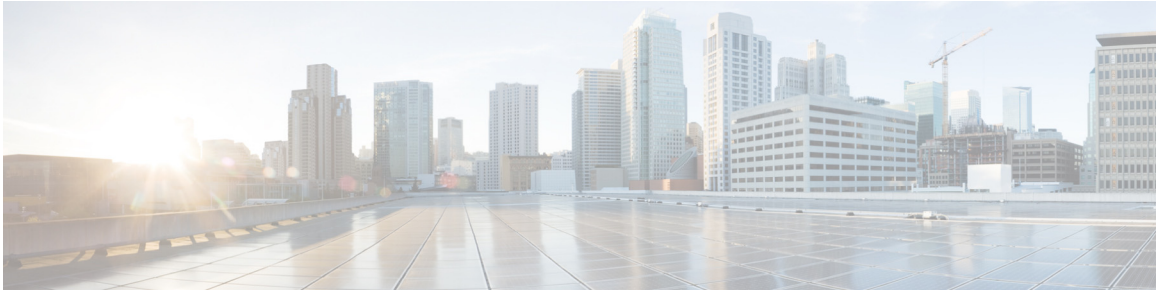
Cisco Intrusion Prevention System Manager Express Configuration Guide for IPS 7.2

April 29, 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-29167-01



Preface

Published: April 29, 2013, OL-29167-01

Revised: February 18, 2014

Contents

This document describes how to install, configure, and use the Intrusion Prevention System Manager Express (IME) for IPS 7.2. It is part of the documentation set for the Cisco Intrusion Prevention System 7.2. It includes a glossary that contains expanded acronyms and pertinent IPS terms. Use this guide with the documents listed in Related Documentation, page iv.

This document contains the following topics:

Audience

This guide is for administrators who need to do the following:

- Install and configure the IME.
- Secure their networks with IPS sensors.
- Prevent intrusion on their networks and monitor subsequent alerts.

Organization

This guide includes the following sections:

Section	Title	Description
1	"Getting Started"	Describes how to get started using Cisco IPS and sensors.
2	"Configuring Device Lists"	Describes how to add and configures devices in the IME.
3	"Configuring Dashboards"	Describes how to add and configure dashboards in the IME.
4	"Configuring RSS Feeds"	Describes how to connect to Cisco RSS feeds in the IME.
5	"Using the Startup Wizard"	Describes how to use the Startup Wizard to set up your sensor using the IME.
6	"Setting Up the Sensor"	Describes how to configure the basic settings of your sensor using the IME.
7	"Configuring Interfaces"	Describes how to configure interfaces on your sensor using the IME.
8	"Configuring Policies"	Describes how to configure polices on your sensor using the IME.
9	"Defining Signatures"	Describes how to configure IPS signatures on your sensor using the IME.
10	"Using the Custom Signature Wizard"	Describes how to use the Signature Wizard to configure signatures using the IME.
11	"Configuring Event Action Rules"	Describes how to configure event action rules policies on your sensor using the IME.
12	"Configuring Anomaly Detection"	Describes how to configure anomaly detection policies on your sensor using the IME.
13	"Configuring Global Correlation"	Describes how to configure global correlation on your sensor using the IME.
14	"Configuring SSH and Certificates"	Describes how to configure SSH and TLS on your sensor using the IME.
15	"Configuring Attack Response Controller for Blocking and Rate Limiting"	Describes how to set up blocking on your sensor using the IME.
16	"Configuring SNMP"	Describes how to configure SNMP on your sensor using the IME.
17	"Configuring External Product Interfaces"	Describes how to set up an external product interface to the CSA MC using the IME.
18	"Managing the Sensor"	Describes how to manage your sensor using the IME.
19	"Monitoring the Sensor"	Describes how to configure monitoring on your sensor using the IME.

Section	Title	Description
20	"Configuring Event Monitoring"	Describes how to set up event monitoring on your sensor using the IME.
21	"Configuring and Generating Reports"	Describes how to configure and generate reports using the IME.
22	"Logging In to the Sensor"	Describes how to log in to the appliances and modules.
23	"Initializing the Sensor"	Describes how to use the **setup** command to initialize your sensor.
24	"Obtaining Software"	Describes how to locate and install the latest Cisco IPS software on Cisco.com.
25	"Upgrading, Downgrading, and Installing System Images"	Describes how to upgrade, downgrade, and install new system images on your sensor.
A	"System Architecture"	Describes the underlying software architecture of the IPS.
B	"Signature Engines"	Lists the IPS signature engines with their options.
C	"Troubleshooting"	Lists troubleshooting procedures and advice.
D	"Open Source License Files Used In Cisco IPS 7.2"	Lists the open source license files that Cisco IPS uses.
	"Glossary"	Lists the IPS terms and acronyms.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

For a complete list of Cisco IPS 7.2 documentation and where to find it, refer to the following URL:

http://www.cisco.com/en/US/docs/security/ips/7.2./roadmap/roadmap7_2.html

For a complete list of the Cisco ASA 5500 series documentation and where to find it, refer to the following URL:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

Obtaining Documentation, Using the Cisco Bug Search Tool, and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Getting Started

This chapter describes the IME and how to get started using it. It contains the following sections:

Introducing the IME

The IME is a network management application that provides system health, events, and collaboration monitoring in addition to reporting and configuration for up to ten sensors. The IME monitors sensor health using customizable dashboards and provides security alerts through RSS feed integration from the Cisco Security Intelligence Operations site. It monitors global correlation data, which you can view in events and reports. It monitors events and lets you sort views by filtering, grouping, and colorization. The IME also supports tools such, as ping, trace route, DNS lookup, and whois lookup for selected events. It contains a flexible reporting network. It embeds the IDM configuration component to allow for a seamless integration between the monitoring and configuration of IPS devices.

Within the IME you can set up your sensors, configure policies, monitor IPS events, and generate reports. The IME works in single application mode—the entire application is installed on one system and you manage everything from that system.

Advisory

The IME contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at the following website:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance, contact us by sending e-mail to export@cisco.com.

Participating in the SensorBase Network

The Cisco IPS contains a security capability, Cisco Global Correlation, which uses the immense security intelligence that we have amassed over the years. At regular intervals, the Cisco IPS receives threat updates from the Cisco SensorBase Network, which contain detailed information about known threats on the Internet, including serial attackers, Botnet harvesters, Malware outbreaks, and dark nets. The IPS uses this information to filter out the worst attackers before they have a chance to attack critical assets. It then incorporates the global threat data in to its system to detect and prevent malicious activity even earlier.

If you agree to participate in the SensorBase Network, Cisco will collect aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other confidential business or personal information. All data is aggregated and sent by secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco will be anonymous and treated as strictly confidential.

Table 1-1 shows how we use the data.

Table 1-1 Cisco Network Participation Data Use

Participation Level	Type of Data	Purpose
Partial	Protocol attributes (TCP maximum segment size and options string, for example)	Tracks potential threats and helps us to understand threat exposure.
	Attack type (signature fired and risk rating, for example)	Used to understand current attacks and attack severity.
	Connecting IP address and port	Identifies attack source.
	Summary IPS performance (CPU utilization, memory usage, inline vs. promiscuous, for example)	Tracks product efficacy.
Full	Victim IP address and port	Detects threat behavioral patterns.

When you enable Partial or Full Network Participation, the Network Participation Disclaimer appears. You must click **Agree** to participate. If you do not have a license installed, you receive a warning telling you that global correlation inspection and reputation filtering are disabled until the sensor is licensed. You can obtain a license at http://www.cisco.com/go/license.

For More Information

- For detailed information on global correlation, see Chapter 14, "Configuring Global Correlation."
- For detailed information on licensing the sensor, see Configuring Licensing, page 20-12.

IME Home Pane

IME Home opens to the Device List pane where you can configure IME devices. It also has the following other features:

- Video help—The IME has an overall feature presentation video that appears when you launch the IME, plus five videos containing procedural help. The video help appears in the pane that it pertains to, but you can also access all video help from **Help > Show Video Help**.

  Note The IME contains video help that requires you to have the Adobe Flash Player Internet Explorer plug-in version 8 or later.

- Notice of whether the clocks on your system and the sensor are synchronized. In the upper left corner, an icon under the Time column indicates whether the sensor time and local system time are synchronized. If they are not, you must make sure you correct the time on the sensor, otherwise the timestamp for monitoring and reporting is not accurate.
- Events per second—In the lower right corner of the Home pane, the EPS (events per second) that the IME has received recently is shown. The EPS count is updated every five seconds.

The IME contains menu features that help you configure various aspects of the IME.

- **File > Import**—Lets you import the alarm data file that you exported from the previous version of the IME or IEV 5.*x*.
- **File > Export**—Lets you export alarm data from the IME database in to a CSV file.
- **View > Reset Layout**—Lets you reset the IME panes to their default view.
- **Tools > Preferences**—Lets you configure how the IME database stores event data, lets you configure a data archive, set up email and enable email notification and automatic reporting, and lets you configure other application settings, such as the location of a network sniffer application, the maximum number of real-time events per view, the maximum number of historical events per view, the event polling interval, and whether to show the feature presentation video at startup. You can also delete the cached DNS names.
- **Tools > Ping, Traceroute, Whois, DNS Lookup**

You can use ping to diagnose basic network connectivity. Ping is a simple way to check if a sensor can communicate back. You can use traceroute to display the route an IP packet takes to a destination. You can use whois to determine the owner of a domain name or an IP address. You can use DNS lookup to translate host names to IP addresses, rather like a phone book.

- **Tools > Change User Password**—Lets you change your existing password in the Change Password dialog box.

- **Tools > Check Database Integrity**—Lets you perform an immediate database integrity check. You receive a Information dialog box informing you if any errors are found.
- **Tools > Repair Database**—Lets you repair any errors that you find in the database. You receive the following Warning dialog box before you can continue:

  ```
  Database repair may cause data loss in certain circumstances. Do you wish to continue?
  ```

- **Tools > IME Console Window**—Lets you use the IME Java console to view and copy logged entries in a text format, which can help you troubleshoot IME errors. To show the virtual machine memory statistics, enter **m** in the console. To perform garbage collection, enter **g** in the console.

For More Information

- For information on correcting the time on the sensor and configuring time on the sensor, see Configuring Time, page 6-7.
- For the procedure to configure data archiving, see Configuring the Data Archive, page 1-8.
- For the procedure to set up email notification, see Configuring Email Notification, page 1-12.
- For detailed information on configuring general options for the IME, see Configuring General Options, page 1-7.

IME System Requirements and Restrictions

For the list of requirements and restrictions for the IME, refer to the Release Notes for your version of the IME at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_release_notes_list.html

IME Demo Mode

The IME provides a demo mode so that you can see the sensor configuration and event monitoring functions without being connected to real devices. We provide a separate IME Demo icon that you can launch from your desktop. IME Demo mode contains sample events and health and security data for demonstrating event monitoring and sensor health and security status.

You can run the IME and IME Demo mode simultaneously, but you can only run one instance of IME Demo mode at a time. You cannot add or delete devices in Demo mode. The dashboard works with simulated data; however, the RSS feed works normally because it relies on Internet connectivity. You can add, edit, or delete event views. The views are filled with simulated events. When the IME is started in demo mode, the IME service continues to receive and store events.

Installing the IME and Migrating Data In to the IME

This section describes how to install and upgrade the IME, and how to migrate data from IEV or a previous version of IME.

Cisco IEV, Cisco IOS IPS, and CSM

If you have a version of Cisco IPS Event Viewer installed, the Install wizard prompts you to remove it before installing the IME.

The IME event monitoring is also supported in IOS-IPS versions that support the Cisco IPS 5.x/6.x signature format. We recommend IOS-IPS 12.4(15)T4 if you intend to use the IME to monitor an IOS IPS device. Some of the new IME functionality including health monitoring is not supported.

Caution Do not install the IME on top of existing installations of CSM. You must uninstall CSM before installing the IME.

Installation Notes and Caveats

Note If you are using Windows 7 or Windows Server 2008, and an IME version earlier than 7.1.1, uninstall IME before upgrading it. Otherwise, just upgrade from your current IME version.

Observe the following when installing or upgrading the IME:

- You can install the IME over all versions of the IME but not over IEV. All alert database and user settings are preserved.
- The IME detects previous versions of IEV and prompts you to manually remove the older version before installing the IME or to install the IME on another system. The installation program then stops.
- Make sure you close any open instances of the IME before upgrading to a new version of the IME.
- Disable any anti-virus or host-based intrusion detection software before beginning the installation, and close any open applications. The installer spawns a command shell application that may trigger your host-based detection software, which causes the installation to fail.
- You must be administrator to install the IME.
- The IME coexists with other instances of the MySQL database. If you have a MySQL database installed on your system, you do NOT have to uninstall it before installing the IME.

Installing or Upgrading the IME

To install the IME, follow these steps:

Step 1 From the Download Software site on Cisco.com, download the IME executable file to your computer, or start the IDM in a browser window, and under Cisco IPS Manager Express, click **download** to install the IME executable file. IME-7.2.1.exe is an example of what the IME executable file might look like.

Step 2 Double-click the executable file. The Cisco IPS Manager Express - InstallShield Wizard appears. You receive a warning if you have a previous version of Cisco IPS Event Viewer installed. Acknowledge the warning, and exit installation. Remove the older version of IEV, and then continue the IME installation

Step 3 Click **Next** to start the IME installation.

Step 4 Accept the license agreement and click **Next**.

Step 5 Click **Next** to choose the destination folder, click **Install** to install the IME, and then click **Finish** to exit the wizard. The Cisco IME and Cisco IME Demo icons are now on your desktop.

Note The first time you start the IME, you are prompted to set up a password.

Migrating IEV Data

To migrate IEV 5.*x* events to the IME, you must exit the installation and manually export the old events by using the IEV 5.*x* export function to move the data to local files. After installing the IME, you can import these files to the new IME system.

Note The IME does not support import and migration functions for IEV 4.*x*.

To export event data from IEV 5.*x* to a local file:

Step 1 From IEV 5.*x*, choose **File > Database Administration > Export Database Tables**.

Step 2 Enter the file name and select the table(s).

Step 3 Click **OK**. The events in the selected table(s) are exported to the specified local file.

Importing IEV Event Data In to IME

To import event data in to the IME, follow these steps:

Step 1 From the IME, choose **File > Import**.

Step 2 Select the file exported from IEV 5.*x* and click **Open**. The contents of the selected file are imported in to the IME.

For More Information

- For the procedure for creating and changing the IME password, see Creating and Changing the IME Password, page 1-6.
- For instructions on how to obtain Cisco IPS software, see Obtaining Cisco IPS Software, page 26-1.

Creating and Changing the IME Password

When you start the IME for the first time, the Password Policy dialog box appears. Enter a password that you will use to access the IME. Reenter the password to confirm, and then click **OK**. From now on when you log in to the IME, enter your password in the Enter IME password field and click **OK**. To change the IME password, choose **Tools > Change User Password**, and enter your existing password, your new password, and then reenter the new password to confirm. When you uninstall and reinstall the IME, you must create a new user password. You do not have to restart the IME after a password change.

Note The IME does not support user roles or multiple sessions, so you do not need to configure a user name.

Password Requirements

The IME password has the following requirements:

- Must contain at least 8 characters and no more than 80.
- Must contain characters from at least three of the following classes:
  - Lower case letters

  - Upper case letters
  - Digits
  - Special characters (! @ $ % & *)
- No single character repeated more than two times consecutively.
- All input must be ASCII characters.

Note The IME performs other checks to make sure that the password is secure. You receive an error message if the password does not pass validation.

Recovering the IME Password

To recover the IME password, follow these steps:

Step 1 Stop the IME client.

Step 2 Delete the hosts.cfg file from the installed directory.

Example

```
C:\Documents and Settings\All Users\Application Data\Cisco Systems\IME\iev\hosts.cfg
```

Note This example location may be different depending on which Windows version you have.

Step 3 Restart the IME client.

Step 4 You are prompted to create a new password.

No events are lost from the database, including new events between the time you deleted hosts.cfg and restarted the IME. However, the event account user name and password will be used for both events and configuration. If you had different user names and passwords for the event and configuration roles, you must edit each device to restore them.

Configuring General Options

In the General dialog box, you can configure certain general options, such as, specifying a network sniffer application, specifying the maximum number of events you want a real time or historical event to contain, specifying the event polling interval, whether you want to see the feature presentation video every time at startup, and whether you want to clear cached DNS names.

A network sniffer application, such as Wireshark, is useful for showing captured data packets for an event. Wireshark is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. For more information, see http://www.wireshark.org.

DNS enables you to convert human-readable names into the IP addresses needed for network packets. To optimize speed, the DNS names are cached. You can clear the DNS lookup results.

Supported User Role

You must be administrator to configure the general settings in the IME.

Field Definitions

The following fields are found in the General dialog box:

- Network Sniffer Application Location—Lets you specify the path to your network sniffer application, or you can click **Browse** and locate the path.
- Maximum Real-time Events Per View—Lets you specify the number of events that a real-time event view should contain. When this number is reached, old events are removed from the view. The default is 2000.
- Maximum Historical Events Per View—Lets you specify the number of events that a historical event view should contain. The default is 50,000.
- Event Polling Interval—Lets you specify the number of seconds per interval for event polling.
- Show feature presentation video at startup—The IME feature video starts up by default every time you start the IME. You can disable it here.
- Delete cached DNS names—Lets you clear cached DNS names.

Configuring the General Settings

To configure the general settings for the IME, follow these steps:

Step 1 From the IME, choose **Tools > Preferences > General**.

Step 2 In the Network Sniffer Application Location field, enter the location of your network sniffer application, or click **Browse** to locate the path.

Step 3 In the Maximum Real-time Events Per View field, enter the number of events you want a real-time event view to contain.

Step 4 In the Maximum Historical Events Per View field, enter the number of events you want a historical event view to contain.

Step 5 In the Event Polling Interval field, enter the number of seconds you want event polling intervals to have.

Step 6 Check the **Show feature presentation video at startup** check box to disable the feature presentation video. The default is enabled.

Step 7 To delete cached DNS names, click **Delete cached DNS names**.

Configuring the Data Archive

The IME uses the MySQL database to store events. You need to archive the database tables periodically to maintain IME performance. You can customize the archive settings in the **Tools > Preferences > Data Archive** dialog box. Each event file contains 1,000,000 events by default and the IME can store up to 400 event files. You can configure IME to send you an email when the event archive reaches a specified limit.

Note You must have an email server configured to receive emails.

Field Definitions

The following fields are found in the Data Archive dialog box:

- Maximum number of events in current event file—Lets you set the maximum number events per current event file. The default is 1,000,000. The range is 1000 to 1,000,000.
- Maximum number of archived files—Lets you set the maximum number of archived files you want to maintain. The default is 100. The range is 10 to 400.
- Enable Notification:
  - When number of archived files reach—Configures the IME to email you when a specified percent of maximum number of archived files is reached. The default is disabled and the default percentage is 80%.

    For example, when you set the maximum number of archived files to 10, and you set the percentage the archived files should reach to 30%, you receive an email when the number of event files created reaches three. Once an email has been sent for a configured percentage, the IME never sends an email again, unless you change the percentage field or the maximum number of archived files field. If you change these two fields, the percent value is recalculated, and once it reaches the new calculation, an email is sent.
  - When number of archived files reach maximum—Configures the IME to email you when the number of archived files reaches the specified maximum. The default is disabled.

    Once the maximum value is reached for every new event archive file creation, an email is sent. To stop receiving notification, uncheck this option. If you change the maximum number of archived files value to a higher value than the old configured value, the notification stops until it reaches the new threshold value. If it is less than the old value, the notifications never stop.
- Enable time schedule for archiving events—Lets you archive event files at certain times.
- Choose the following time schedule:
  - Every—Lets you set the schedule in minutes. The default is 10 minutes.
  - Every—Lets you set the schedule in hours. The default is every hour.
  - Every day at time—Lets you specify a daily time to archive event files.

Configuring Data Archiving

To configure data archiving, follow these steps:

Step 1 From the IME, choose **Tools > Preferences > Data Archive**.

Step 2 In the Maximum number of events in current event file field, enter the number of events you want the current event file to contain. The default is 1,000,000. The range is 1000 to 1,000,000.

Step 3 In the Maximum number of archived files field, enter the number of archived files you want the IME to maintain. The default is 100. The range is 10 to 400.

Step 4 Check the **When number of archived files reach** checkbox and enter a percentage in the % of Max field to receive emails when a specific percent of the maximum number of archived files is reached. The default is enabled and the default percentage is 2%.

Example Email:

```
The configured maximum archived event file limit is 10.
```

```
The configured percentage threshold value for the archived event file is 2%.
This is a notification to inform you that this percent threshold value has been reached.
The oldest event data files are overwritten once the maximum archive file limit is
reached.
```

Step 5 Check the **When number of archived files reach maximum** checkbox to receive emails when the number or archived files reaches the specified maximum number.

Example Email:

```
The configured maximum archived event file limit is 10.
This is a notification to inform you that this limit is just about to be reached.
The next event file creation from the system will overwrite the oldest event file.
```

Example Email:

```
The configured maximum archived event file limit is 10.
This is a notification to inform you that this limit was reached.
The new event file creation from the system is overwriting the oldest event files.
```

Step 6 If you want to use a time schedule to archive events, check the **Enable time schedule for archiving events** check box. The default is enabled.

Step 7 Under Choose the following time schedule, enter the time schedule you want to use, either in minutes, hours, or a specific daily time.

Tip To undo your changes, click **Cancel**.

Step 8 Click **Apply** to apply your changes, save the revised configuration, and continue editing the dialog box, or click **OK** to save the changes and exit the dialog box.

For More Information

For the procedure for setting up an email server for the IME, see Configuring Email Setup, page 1-10.

Configuring Email Setup

In the Email Setup dialog box, you can configure a mail server, and sender and recipient email addresses so that the IME can send email notifications to specified users.

Field Definitions

The following fields are found in the Email Setup dialog box:

- Allow mail to be sent from IME (required for email notifications)—When checked, lets you have the IME send email notifications.
- Send Test Email—Lets you test email setup. You must specify a mail server and sender/recipient email addresses before you can test the email setup.
- Server Settings—Lets you specify the mail server settings:
  - Mail Server (SMTP Host)—Specifies the mail server of your company. Check the **Using SSL** checkbox to use SSL on this server.
  - Using authentication—When checked, enables user authentication.
  - Username—Specifies the username of the user authorized to access the mail server.

  - Password—Specifies the password of the authorized user.
- Sender/Recipient Settings—Lets you specify emails for the senders and recipients:
  - Sender Address—Lets you specify the person who sends the email notifications.
  - Recipient Address(es)—Lets you specify the sensor administrator that you want to receive the email notifications.

Setting Up Email

To set up email, follow these steps:

Step 1 From the IME, choose **Tools > Preferences > Email Setup**.

Step 2 Check the **Allow mail to be sent from IME (required for email notifications)** checkbox.

Step 3 Configure the mail server settings:

a. In the Mail Server (SMTP Host) field, enter the mail server address for your company. Use your company mail server, for example, smtp.mycompany.com.

b. To use SSL, check the **Using SSL** checkbox.

c. To require user authentication, check the **Using authentication** checkbox.

d. In the Username field, enter the username of the user who will access the mail server.

e. In the Password field, enter the password for this user.

Step 4 Configure the sender and recipient settings:

a. In the Sender Address field, enter the email address of the user who will send email from the IME.

b. In the Recipient Address(es) field, enter the email addresses you want to send email notifications to, for example, admin@mycompany.com or ips@mycompany.com.

Tip To undo your changes, click **Cancel**.

Step 5 Click **Apply** to save your changes**.**

Step 6 To test the email setup, **Send a Test Email.**

If you have correctly set up email, you receive an information dialog box stating that the test email has been sent and you should check to see that you received it.

If you have not correctly set up email, you receive an error message stating either that the IME could not connect to the SMTP host because the wrong SMTP server is configured, or that the IME failed to authenticate the server because the user credentials are incorrect.

Step 7 Click **OK** to save your changes and exit the dialog box.

Sample Email Configuration

```
Flag this message
high 2004-0 ICMP Echo Request (10.2.2.2)
Wednesday, March 10, 2010 3:13 PM
From abc@def.com Wed Mar 10 23:13:38 2010
Date:    Wed, 10 Mar 2010 23:13:38 GMT
From:    abc@def.com
To:      jsmith@cisco.com
To:      jimsmith2010@yahoo.com
```

```
Subject: high 2004-0 ICMP Echo Request (10.2.2.2)
```

Configuring Email Notification

Email notifications are sent periodically to the recipient address for the events that correspond to the criteria you defined in the Send notifications for alerts field. By default, email notification is disabled. You must have the email server, sender, and recipient addresses for the email. You must set up email first by entering that information in the **Tools > Preferences > Email Setup** dialog box.

Field Definitions

The following fields are found in the Notifications dialog box:

- Enable email/epage notifications—When checked, enables email notifications.
- Send Test Notification—Lets you test IME email notification. You must have at least one severity level and at least one field selected to test email notification.
- Send notifications for alerts—Lets you specify which level of alerts you want to see and which alerts with the specified risk ratings you want to see.
- Notification Interval—Lets you specify the notification interval in minutes. The default is 10 minutes. The range is 1 to 1440 minutes.
- Notification Type—Lets you choose to send summarized notifications, detailed notifications, or both.
- Maximum number of detailed notifications per interval—Lets you choose how many detailed notifications per interval you want to see.
- Content contains—Lets you choose which content to display in the detailed email notifications:
  - Event ID
  - Severity
  - Device
  - Application name
  - Receive time
  - Event time
  - Sensor local time
  - Signature ID
  - Signature name
  - Signature details
  - Signature version
  - Attacker IP address
  - Attacker locality
  - Victim IP address
  - Victim Port
  - Victim OS
  - Victim Locality

- Summary count
- Initial alert ID
- Summary type
- Is final
- Interface
- VLAN
- Virtual sensor
- Context
- Actions taken
- Alert details
- Risk rating
- Threat rating
- Reputation
- Reputation details
- Protocol

Configuring Email Notification

To configure email notification for the IME, follow these steps:

Step 1 From the IME, choose **Tools > Preferences > Notification**.

Step 2 Check the **Enable email/epage notifications** check box.

Step 3 Choose which types of alerts you want to receive notifications about and in the Risk Rating Range field, enter the risk rating range. The default is 80-100, which is a medium to high risk rating.

Step 4 In the Notification Interval field, enter the interval in minutes. Notification is sent as one summary for each sensor per each interval. The default is 1 to 100 minutes.

Step 5 Under Notification Type, choose what type of notification you want to receive, summarized or detailed.

Step 6 If you choose detailed notifications, under Maximum number of detailed notifications per interval, enter how many detailed notifications you want per summary, and then enter which fields you want in the summary content.

Step 7 In the Content contains field, check the checkbox of each field that you want included in the email notifications.

Step 8 Click **Apply** to save your changes.

Step 9 To test the email notification, click **Send Test Notification**.

If you have correctly set up notification, you receive an information dialog box stating that the test notification has been sent and you should check to see that you received it. If you have not correctly set up notification, you receive an error message.

Step 10 Click **OK** to save your changes and exit the dialog box.

Email Notification Examples

The following example shows the notification sent as one summary for each sensor per each interval:

```
low 9698-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 284
high 35786-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 276
high 40971-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 251
low 8813-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 565
high 21357-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 279
high 41528-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 554
```

The following example shows the detailed information for each event:

```
event_id=1186174940758000000
severity=high
device_name=shark
event_time=1186174940758000000
sig_id=21357
sig_name=Signature Example
```

For More Information

- For more information about risk categories, see Configuring Risk Category, page 12-31.
- For information on how the risk rating is calculated, see Calculating the Risk Rating, page 12-2.

Configuring Reports

The IME send reports once a day, week, or month based on the schedule you configure. By default, automatic reporting is disabled. The IME sends an email with the report as a PDF attachment. The email lets you know the success or failure of the reports you wanted to generate.

Field Definitions

The following fields are found in the Reports dialog box:

- Enable automatic reporting—When checked, enables automatic reporting.
- Send Test Report(s)—Lets you test IME automatic reporting. You must have a time specified, at least one type of report selected, and email notifications set up to test automatic reporting.
- Choose a time schedule—Lets you specify when you want to receive automatic reports:
  - Daily—Specifies a daily automatic report. Choose the time you want to receive it from the drop-down list.
  - Weekly—Specifies a weekly automatic report. Choose the day and time you want to receive it from the drop-down list.
  - Monthly—Specifies a monthly automatic report. Choose time you want to receive it from the drop-down list and enter the day of the month you want to receive it in the Day of each month field.
- Report(s) to include—Lets you choose which types of reports you want to receive.

- Top Attacker Reports—Shows top attacker IP addresses for a specified time. You specify the top number of attacker IP addresses. There are four predefined top attacker reports:
  - Basic Top Attacker
  - Top 10 Attackers Last 1 Hour
  - Top 10 Attackers Last 8 Hours with High Severity
  - Top 20 Critical Attackers Last 24 Hours
- Top Victim Reports—Shows top victim IP addresses for a specified time. You specify the top number of victim IP addresses. There are four predefined top victim reports:
  - Basic Top Victim
  - Top 10 Victims Last 1 Hour
  - Top 10 Victims Last 8 Hours with High Severity
  - Top 20 Victims with Action Denied Attacker
- Top Signature Reports—Shows top signatures fired for a specified time. You specify the top number of signatures. There are four predefined top signature reports:
  - Basic Top Signature
  - Top 10 Signatures Last 1 Hour
  - Top 10 Signatures Last 8 Hours with High Severity
  - Top 20 Critical Signatures Last 24 Hours
- Attacks Over Time Reports—Shows the attacks over a specified time. There are five predefined reports:
  - Basic Over Time Attack
  - Attacks Blocked in Last 24 Hours
  - Attacks Dropped in Last 24 Hours
  - Attacks Over Time Last 1 Hour
  - Critical Attacks Over Last 24 Hours
- Filtered Events vs All Events Reports—Displays a set of events against the total events for a specified time period. There is one predefined report:
  - Negative Reputation Events
  - My Reports—Displays your user-defined reports.
- Preferred chart type—Lets you view the reports as bar charts or pie charts.

Configuring Automatic Reporting

To configure automatic reporting for the IME, follow these steps:

Step 1 From the IME, choose **Tools > Preferences > Reports**.

Step 2 Check the **Enable automatic reporting** check box.

Step 3 Choose a time schedule:

- Daily
- Weekly
- Monthly

Step 4 In the Report(s) to include field, check the checkbox of each report that you want included in the automatic reports.

Step 5 From the Preferred chart type drop-down list, choose either Bar Chart or Pie Chart.

Step 6 Click **Apply** to save your changes.

Step 7 To test the automatic reporting, click **Send Test Report(s)**.

If you have correctly set up automatic reporting, you receive an information dialog box stating that the test report has been sent and you should check to see that you received it. If you have not correctly set up automatic reporting, you receive an error message.

Step 8 Click **OK** to save your changes and exit the dialog box.

Automatic Reports Email Example

```
From: ime@cisco.com [mailto:ime@cisco.com]
Sent: Monday, October 31, 2011 4:30 AM
To: John Smith (jsmith)
Subject: IME Auto-Generated Report - 2011-10-31T04:30:08.085-0500

Please find attached a report summarizing recent sensor activity registered with Cisco
IME.

The following reports were not generated due to missing data:
    - Top 10 Attackers last 8 hours with High Severity
    - Top 20 Critical Attackers last 24 hours
    - Top 10 Victims last 8 hours with High severity
    - Top 20 Victims with Action as denied
    - Top 10 Signatures last 8 hours with High Severity
    - Top 20 Critical Signatures last 24 hours
```

Configuring Device Lists

You can add devices to the IME in the Device List pane and view important information about each device. This chapter describes the Device List pane and how to add devices. It contains the following sections:

Device List Pane

The IME manages up to ten Cisco IPS devices. The upper half of the Device List pane displays pertinent information about each device. You can customize which columns you want to view and which you want to hide by clicking the column button in the far-right corner of the pane to bring up the Choose Columns to Display dialog box.

From Device List pane, you can add, edit, or delete a sensor in the device list. You can start and stop the health and events connections for a sensor and you can view the status of a sensor. You can also obtain information about the sensor by using tools such as ping, trace route, whois, and DNS lookup. You can use the **Add**, **Edit**, **Delete**, **Start**, **Stop**, **Status**, and **Tools** buttons in the Device List table, or you can select the sensor in the table and use the right-click menu.

In the lower half of the Device List pane, the IME health monitoring center displays the details about the sensor you have selected in the upper half of the pane. The data displayed here match the information in the customizable dashboard gadgets.

The Device Details pane contains the following details about the selected sensor:

- Sensor Health—Sensor health and network security health information shown in graph form. You can click **Details** next to the Sensor Health and Network Security graphs to obtain the specifics about the sensor health and network security health.

  If you want to change the sensor health metrics, choose **Details > Configure Sensor Health Metrics**, and you are taken to **Configuration >** *sensor_name* **> Sensor Management > Sensor Health**, where you can reconfigure the health metrics.

If you want to change the threat thresholds, choose **Details > Configure thresholds**, and you are taken to **Configuration >** *sensor_name* **> Policies > IPS Policies**, where you can configure the threat thresholds.

If you want to reset the network security health, choose **Details > Reset Health Status**, and you are taken to **Configuration >** *sensor_name* **> Sensor Monitoring > Properties > Reset Network Security Health**, where you can reset the status and calculation of network security health.

- Sensor Information—Displays the host name, IPS version, whether the sensor is using inline bypass, the total sensing interfaces, the sensor IP address, the device type, the total memory, the total data storage, and the status of Analysis Engine.
- CPU, Memory, and & Load—Displays the CPU, memory, and sensor load usage in graph form.

  Click **Details** next to the Inspection Load graph to see a detailed description of how the inspection load is determined.
- Licensing—Displays all of the pertinent license, signature version, and signature engine version information.
- Interface Status—Displays the interface name, link status, whether it is enabled, the speed, the mode, and the received and transmitted packets.
- Global Correlation Health—Displays the configuration status of global correlation and network participation.

For More Information

- For the procedure for configuring sensor and network security health, see Configuring Sensor Health, page 20-16.
- For the procedure for changing threat thresholds, see Configuring Risk Category, page 8-36.
- For the procedure for resetting network security health, see Resetting Network Security Health, page 21-20.
- For more information about global correlation, see Chapter 14, “Configuring Global Correlation.”

Device List Pane Field Definitions

The following fields are found in the Device List pane:

- Time—If there is a problem with the synchronization between your local system and a sensor that you have added, an icon appears in the time field. If the local system and the sensor are synchronized, the field is empty.

  Note If the time in not synchronized between the sensor and the local system, you do not receive accurate monitoring and reporting.
- Device Name—Displays the name that you gave the sensor.
- IP Address—Displays the IP address of the sensor.
- Device Type—Displays the IPS model name.
- Event Status—Informs you that the IME is connecting to the sensor to receive events.
- Sensor Health—Informs you whether the sensor health is normal or needs attention.
- Global Correlation Status—Informs you of the global correlation status of the sensor.

- Version—Displays the installed Cisco IPS software version.
- License Expiration—Informs you about how many days until the sensor license expires.
- Load—Displays the load percentage.
- Memory—Displays the memory percentage.
- CPU—Displays the percentage the CPU is using.
- Signature Version—Displays the current signature version.

For More Information

- For information about time and the sensor, see Configuring Time, page 6-7.
- For more information about sensor health metrics, see Configuring Sensor Health, page 20-16.
- For more information about global correlation, see Chapter 14, "Configuring Global Correlation."
- For more information about licensing the sensor, see Configuring Licensing, page 20-12.
- For the procedure for obtaining the latest IPS software, see Obtaining Cisco IPS Software, page 26-1.

Add and Edit Device List Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Device List dialog boxes:

- Sensor Name—Specifies the name of the sensor you are adding.
- Sensor IP Address—Specifies the IP address of the sensor you are adding.
- Web Server Port—Specifies the TCP port used by the web server. The default is 443 for HTTP or HTTPS. You receive an error message if you enter a value out of the range of 1 to 65535.
- Communication Protocol—Enables TLS and SSL in the web server. The default is Use encrypted connection (HTTPS). We strongly recommend that you use an encrypted connection.
- Authentication—Lets you specify separate credentials for configuration and event subscription:
  - Configuration User Name—Specifies the name of user account allowed to configure this sensor.
  - Configuration Password—Specifies the password of the user account allowed to configure this sensor.
  - Use the Same Account for Configuration and Event Subscription (This is not recommended)—Lets you have the same account apply to users who can configure and monitor the sensor.

Caution Using the same credentials for both configuration and event retrieval is not as secure as maintaining separate user accounts. We recommend that you maintain separate accounts and that the configuration user name have an administrator user role and the event subscription user name have a viewer user role.

  - Event Subscription User Name—Specifies the name of user account allowed to view events on this sensor.
  - Event Subscription Password—Specifies the password of the user account allowed to view events on this sensor.

- Event Start Time (UTC)—Lets you choose to have the latest alerts retrieved or you can select the start date and time of alerts to retrieve.
- Exclude alerts of the following severity level(s)—Lets you choose to exclude security levels from retrieval. The default is for all security levels to be displayed.

For More Information

For the procedures for recovering sensor passwords, see Recovering the Password, page 20-4.

Adding, Editing, and Deleting Devices

To add, edit, and delete devices, follow these steps:

Step 1 Choose **Home > Devices > Device List**, and then click **Add**.

Step 2 Fill in the required fields in the Add Device dialog box:

a. Enter the sensor name and sensor IP address of the sensor you are adding.

b. To change the default web server port, enter a new port number.

c. Choose the communication protocol.

Note We strongly recommend that you use an encrypted connection.

d. Enter the user name and password of the account that will configure this sensor.

e. Enter the user name and password of the person who will monitor the event subscription for this sensor.

Caution Using the same credentials for both configuration and event retrieval is not as secure as maintaining separate user accounts. We recommend that you maintain separate accounts and that the configuration user name have an administrator user role and the event subscription user name have a viewer user role.

f. Choose the event start time by either checking the **Latest Alerts** check box or entering a start date and time in the Start Date and Start Time fields.

g. Under Exclude alerts of the following severity level(s), check the check boxes of any levels you want to exclude. The default is to have all of the levels configured.

h. Click **OK** to add the sensor to the IME system.

Step 3 Click **Yes** to accept the certificate and continue the HTTPS connection with the sensor. The IME checks the time setting between the IME and the sensor to make sure it is correct. If it is not, you receive a warning message if the sensor time and the IME system are more than five minutes apart. Make sure you synchronize the sensor with your system.

Note If you click **No** you reject the certificate and the IME cannot connect to the sensor.

Caution Having the correct time is very important so that reports, historical events, and the top gadgets are accurate. If the time is not within the range of five minutes, an icon appears next to the device in the Device Lists pane.

Step 4 To edit a device, select it in the list, click **Edit**, make any changes needed, and then click **OK**.

Note You cannot change the Sensor Name because it is a key for the IME database.

Step 5 To delete a device, select it in the list, and then click **Delete**. The device no longer appears in the Device List pane.

For More Information

For more information about correcting time on the sensor, see Correcting Time on the Sensor, page 6-12.

Starting, Stopping, and Displaying Device, Event, Health, and Global Correlation Connection Status

The IME queries the sensor every 10 seconds to obtain health status information as long as you choose **Start > Health Connection**. The IME pulls alerts from the sensor as long as you choose **Start > Events Connection**. The IME sends and receives global correlation data as long as you choose **Start > Global Correlation Connection**.

There are some situations in which you might want to stop the sensor from polling events. For example, you can stop polling events from a specific sensor if you do not want its real-time events interfering when you are analyzing the events of another sensor. Then you can resume after the polling is done. Or you can stop polling health and security if you want to look at a snapshot of the status without the 10-second update.

To start, stop, and display event, health, and global correlation connection status, follow these steps:

Step 1 Select the sensor in the device list for which you want to start or stop event, health, or global correlation connection status.

Step 2 Choose **Start** or **Stop > Health Connection** or **Events Connection** or **Global Correlation Connection**. The column now reads Connected or Not Connected.

Step 3 To display the connection status of the IME to the sensor, the sensor version, and statistics information, select the sensor in the list, and then click **Status**. The following IPS component statistics are displayed in the Device Status dialog box:

- Analysis Engine
- Anomaly Detection
- Event Store
- External Product Interface
- Global Correlation
- Host

- Interface
- Network Access
- Notification
- OS Identification
- SDEE Server
- Transaction Server
- Virtual Sensor
- Web Server

Step 4 To update the contents of the Device Status dialog box, click **Refresh**.

Step 5 To display details about a sensor, select it in the list, and then view the information displayed in the Device Details section of the pane.

To change the health metrics that you see in the Device Details pane, go to **Configuration > *sensor_name* > Sensor Management > Sensor Health**. To change the global correlation metrics that you see in the Device Details pane, go to **Configuration > *sensor_name* > Policies > Global Correlation**.

For More Information

- For more information about sensor health metrics, see Configuring Sensor Health, page 20-16.
- For more information about global correlation, see Chapter 14, "Configuring Global Correlation."

Using Tools for Devices

You can use ping to diagnose basic network connectivity. Ping is a simple way to check if a sensor can communicate back. You can use traceroute to display the route an IP packet takes to a destination. You can use whois to determine the owner of a domain name or an IP address. You can use DNS lookup to translate host names to IP addresses, rather like a phone book.

To use tools for devices, follow these steps

Step 1 Choose **Home > Devices**.

Step 2 To obtain ping statistics for a sensor, select it in the device list table, and then click **Tools > Ping**. The Executing command - ping dialog box appears displaying the ping statistics for that sensor.

Step 3 To find the route of the IP packet, select the sensor in the list, and then click **Tools > Traceroute**. The Executing command - traceroute dialog box appears displaying the trace route statistics for that sensor.

Step 4 To find the whois information, select the sensor in the list, and then click **Tools > WhoIs**. The Executing command - whois dialog box appears displaying the WHOIS statistics for that sensor.

Step 5 To find the DNS information, select the sensor in the list, and then click **Tools > DNS**. The Executing command - dnslookup dialog box appears displaying the DNS lookup statistics for that sensor.

Configuring Dashboards

This chapter describes dashboards, and how to add and delete them. It contains the following topics:

Understanding Dashboards

By default, the Health and Traffic dashboards with default gadgets are displayed. You can customize all dashboards. You can select from the available list of gadgets and drag and drop them into the default dashboards or you can create new dashboards.

To add a dashboard, click **Add Dashboard**. To show the available gadgets you can add to a dashboard, click **Add Gadgets**.

Adding and Deleting Dashboards

To add and delete dashboards and gadgets, follow these steps:

Step 1 Choose **Home > Dashboards**, and then click **Add Dashboard**. A tab appears named Untitled.

Step 2 Double-click **Untitled** and enter the dashboard name on the tab.

Step 3 Click **Add Gadgets**.

Step 4 Drag the desired gadget icons to the dashboard.

Step 5 To customize a gadget, click the **Tool** icon in the upper-right corner and a configuration dialog box appears.

Step 6 To collapse the gadget, click the **Double Arrows** icon in the upper-right corner.

Step 7 To delete the gadget, click the **X** icon in the upper-right corner.

Step 8 To delete the dashboard, click the **X** in the tab.

Caution The Delete Dashboard dialog box appears asking if you are sure you want to delete the dashboard. When you delete a dashboard you lose any gadgets that you created in that dashboard.

IME Gadgets

This section describes the IME gadgets, and contains the following topics:

Sensor Information Gadget

The Sensor Information gadget displays the following sensor information:

- Host Name—Displays the host name that was configured during initialization.
- IPS Version—Displays the current installed IPS version.
- In Bypass—Indicates whether the interfaces are operating in bypass mode.

Note The ASA 5500-X IPS SSP and the ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

- Total Sensing Interfaces—Displays how many sensing interfaces your sensor platform has.

- Analysis Engine Status—Displays the running status of the Analysis Engine. If the Analysis Engine is initializing or being reconfigured, it reads **Processing Transaction**; otherwise the status reads **Running Normally**. Click the **i** icon to view a description of the Analysis Engine status. The following statuses are displayed:
  - Stage—Displays in a progress bar the stage of the Analysis Engine update.
  - Step—Displays in a progress bar any additional steps taken during an Analysis Engine update.
  - Activity—Lets you know when the Analysis Engine activity is complete.

  Note The Stage, Step, and Activity bars disappear once the Analysis Engine update is complete.

- IP Address—Displays the IP address that was configured during initialization.
- Device Type—Displays your IPS sensor platform.
- Total Memory—Displays the total amount of memory available.
- Total Data Storage—Displays the total amount of data storage available.

Changing the Sensor Information Gadget Display

To change the title of the Sensor Information gadget and the sensor whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

- For a detailed description of the Analysis Engine, see Understanding Analysis Engine, page 8-2.
- For a detailed description of bypass mode, see Configuring Bypass Mode, page 7-25.

Sensor Health Gadget

The Sensor Health gadget visually displays sensor health and network security information in two colored meters. The meters are labeled Normal, Needs Attention, or Critical according to an analysis of the specific metrics. The overall health status is set to the highest severity of all the metrics you configured. For example, if you configure eight metrics to determine the sensor health and seven of the eight are green while one is red, the overall sensor health is displayed as red.

Click the **i** icon by the Sensor Health graph to display the specific sensor health metrics, which are grouped according to yellow and red threshold levels.

To change the sensor health metrics, click **Details > Configure Sensor Health Metrics**, and you are taken to **Configuration >** ***sensor_name*** **> Sensor Management > Sensor Health**, where you can reconfigure the health metrics, and enable/disable the sensor health parameters.

The following sensor health metrics and their status are displayed:

- Inspection load
- Missed packet
- Signature update
- License time remaining
- Event retrieval
- Application failed
- In Bypass mode

Note The ASA 5500-X IPS SSP and the ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

- Active interface down
- Global correlation
- Network participation

Click the **i** icon by the Network Security Health graph to display the specific network health metrics and their status. The colors reflect the risk and threat ratings gathered in the last five minutes, which are grouped in green, yellow, and red levels with red being the highest level of risk.

To change the threat thresholds, click **Details > Configure Thresholds**, and you are taken to **Configuration >** ***sensor_name*** **> Policies > IPS Policies**, **> Risk Category** where you can configure the threat thresholds.

To reset the network security health, click **Details > Reset Health Status**, and you are taken to **Configuration >** ***sensor_name*** **> Sensor Monitoring > Properties > Reset Network Security Health**, where you can reset the status and calculation of network security health.

Right-click in the meter to get a menu that lets you change the properties of the meters, print the information contained in the meters, and save the sensor and network health details.

Changing the Sensor Health Gadget Display

To change the title of the Sensor Health gadget and the sensor whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

- For the procedure for changing the threat thresholds, see Configuring Risk Category, page 8-36.
- For more information on bypass mode, see Configuring Bypass Mode, page 7-25.

- For the procedure for configuring sensor and network security health, see Configuring Sensor Health, page 20-16.
- For the procedure for resetting network security health, see Resetting Network Security Health, page 21-20.

Licensing Gadget

The Licensing gadget displays the following pertinent information about your license key and the status of other software updates:

- License Status—Tells you if you have a license key installed and when it expires.
- Signature Version—Displays the installed signature version and information about it. Click the **i** icon to view a description of the Signature Version:
  - Released On—Displays the date this signature version was released.
  - Applied On—Displays the date this signature version was applied.
  - Auto Update Status—Indicates whether automatic update has checked for new versions.
- Engine version—Displays the installed signature engine version and information about it. Click the **i** icon to view a description of Engine Version:
  - Released On—Displays the date this signature engine was released.
  - Applied On—Displays the date this signature engine was applied.
  - Auto Update Status—Displays the last time automatic update checked for updates.

Changing the Licensing Gadget Display

To change the title of the Licensing gadget and the sensor whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

For the procedure for obtaining and installing the license key, see Configuring Licensing, page 20-12.

Interface Status Gadget

The Interface Status gadget displays the following information about each interface:

- Interface—Displays the physical interface name (FastEthernet, GigabitEthernet, or PortChannel).
- Link—Indicates whether the interface is up or down.
- Enabled—Indicates whether the interface is disabled or enabled.

- Speed (Mbps)—Indicates whether the speed of the interface is Auto, 10 Mb, 100 Mb, 1000 Mb, or 10,000 Mb.
- Mode—Indicates whether the interface is in promiscuous, inline interface, inline VLAN pair, or VLAN groups mode.
- Received packets—Displays the total number of packets received on this interface.
- Transmitted packets—Displays the total number of packets transmitted on this interface.

Changing the Interface Status Gadget Display

To change the title of the Interface Status gadget and the device whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

For more information about interfaces, see Chapter 7, "Configuring Interfaces."

Global Correlation Reports Gadget

The Global Correlation Reports gadget displays the following information about reputation:

- Packets Denied Due to Global Correlation—Displays the percentage of malicious packets identified and whether any have been dropped due to global correlation.
- Total Packets Denied—Displays the total number of malicious packets that were identified and which ones were dropped because of global correlation criteria.

Changing the Global Correlation Reports Gadget Display

To change the title of the Global Correlation Reports gadget and the way information is displayed, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Method of display (pie chart, bar chart, or table)

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

- For a description of the reputation feature in global correlation, see Understanding Reputation, page 14-2.
- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 20-16.
- For more information on IME reporting, see Chapter 23, "Configuring and Generating Reports."

Global Correlation Health Gadget

The Global Correlation Health gadget displays the following information about global correlation:

- Global Correlation Updates—Displays the status of global correlation:
  - Status of Last Update Attempt—Indicates whether global correlation is enabled or disabled and whether the last update was successful or failed. Click the **i** icon to view the description of the status.

    Note If the status reads `Disabled`, either global correlation is turned off or the sensor is unlicensed.

  - Time Since Last Successful Update—Indicates how long it has been since the last successful update.
  - Update Interval in Seconds—Indicates how many seconds between update intervals.
  - Update Server—Displays the name of the global correlation server that performs the updates.
  - Update Server Address—Displays the IP address of the global correlation server that performs the updates.
- Counters—Displays the connection attempts:
  - Update Failures Since Last Success—Displays how many failures have occurred since the last successful update.
  - Total Update Attempts—Displays how many times the sensor has tried to update global correlation.
  - Total Update Failures—Displays how many times the updates have failed.
- Current Versions—Displays the versions for the following components that the sensor checks for updates: drop, rule, ip, and config.
- Warnings—Displays the number of warnings about global correlation. Click the **i** icon to view the warnings.
- Network Participation—Displays the status of network participation:
  - Status—Indicates whether connection status is good, has failed one to five times since the last successful connection, or has failed more than five times since the last successful connection. Click the **i** icon to view the description of the status.
- Counters—Displays the connection attempts:
  - Total Connection Attempts—Displays how many times the connection has been attempted.
  - Total Connection Failures—Displays how many times the connection has failed.

  - Connection Failures Since Last Success—Displays how many connection failures have occurred since the last successful connection.
- Connection History—Displays all of the connection attempts and the results (successful or failure).

Changing the Global Correlation Health Gadget Display

To change the title of the Global Correlation Health gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, change the title of the gadget.

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

- For a description of the reputation feature in global correlation, see Understanding Reputation, page 14-2.
- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 20-16.
- For a description of Network Participation, see Understanding Network Participation, page 14-3.

Network Security Gadget

The Network Security gadget displays the following information about your network security:

- Alert counts including Meta and summary alerts.
- Average threat rating and risk rating values.
- Maximum threat rating and risk rating values over a designated time period.

These values are all aggregated by the sensor every 10 seconds and are categorized as green, yellow, or red with green being the most secure and red being the least. The overall network security value represents the least secure value from all virtual sensors. The severity level for a given virtual sensor is calculated as follows:

- Red severity level if one or more red events have been detected on the sensor within the last *n* minutes, where *n* is a configured value that is defaulted to 5 minutes.
- Yellow severity level if one or more yellow events, but no red events, have been detected on the sensor within the last *n* minutes.
- Otherwise the severity level is green.

Chose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > Risk Category** to configure risk categories and the risk values for green, yellow, and red thresholds.

The top graph shows the number of events for each of the categories, such as total, red, yellow, and green events. It counts for alerts by severity or risk category. The lower graph shows the average risks versus the average threats, or the maximum risks versus the maximum threats. This information is categorized per virtual sensor.

Changing the Network Security Gadget Display

To change how the network security values are displayed in the Network Security gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- The device and virtual sensor
- Which graphs to display in the Number of Events graph (all, red, yellow, or green)
- Which graphs to display in the Risk vs. Threat graph (average risk vs. the average threat or the maximum risk vs. the maximum threat).

Step 3 Click **Apply**.

For More Information

For the procedure for changing the threat thresholds, see Configuring Risk Category, page 8-36.

Top Applications Gadget

The Top Applications gadget displays the top ten Layer 4 protocols that the sensor has discovered, which gives you an on overall picture of the traffic mix on the sensor:

- TCP
- UDP
- ICMP
- IP

Changing the Top Applications Gadget Display

To change how the top applications are displayed in the Top Applications gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device whose information you want to display
- Method of display (pie chart, bar chart, or table)
- Virtual sensor whose information you want to display

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

CPU, Memory, & Load Gadget

The CPU, Memory, & Load gadget displays the sensor load, memory usage, and disk usage. If your sensor has multiple CPUs, multiple meters are displayed.

- Inspection Load—Indicates how much traffic inspection capacity the sensor is using. 0 indicates that there is no traffic backup and 100 indicates that the buffers are completely backed up. Click the **i** icon to view the inspection load details. Inspection load is affected by the following factors:
  - Rate of traffic that needs inspection
  - Type of traffic being inspected
  - Number of active connections being inspected
  - Rate of new connections per second
  - Rate of attacks being detected
  - Signatures active on the sensor
  - Custom signatures created on the sensor
- CPU Usage—Indicates how much of the CPU of the sensor is being used. Click the **i** icon to view a description of CPU Usage.
- Memory Usage—Indicates how much memory the system and the Analysis Engine are using:
  - System—Displays the amount of memory used for configuration and event storage. System memory is not used for traffic inspection. The number of configured virtual sensors affects system memory, but changes in traffic or attack rates do not affect system memory. System memory remains stable except when you are configuring the sensor. Click the **i** icon to view a description of system memory.
  - Analysis Engine—Displays the fixed amount of memory allocated to and used by the Analysis Engine, which is part of the SensorApp. The amount of memory that the Analysis Engine is currently using is displayed here. Click the **i** icon to view a description of the Analysis Engine memory.
- Disk Usage—Indicates the amount of disk usage. Click the **i** icon to see the details of each usage.
  - Boot—Displays the amount of boot disk usage, which contains the OS boot image and recovery image. This partitions is used when a system image is installed on the sensor. Click the **i** icon to view a description of the boot partition.
  - System—Displays the amount system disk usage, which contains the system and application files loaded on the sensor. The amount changes after a software update. Click the **i** icon to view a description of the system partition.
  - Application Log—Displays the amount of application log used. Click the **i** icon to view the details.
  - Application Data—Displays the amount of application disk usage, which contains the configuration data and IP log files. The amount changes according to the number of configured virtual sensors and the number of IP logs stored on the device. Click the **i** icon to view the details of the application data partition.

Changing the CPU, Memory, & Load Gadget Display

To change the title of the CPU, Memory, & Load gadget and the sensor whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

RSS Feed Gadget

By default, the RSS Feed gadget is directly fed from the Cisco Security Advisors site on Cisco.com. You can have the RSS Feed gadget display any RSS feed channel that you set up. You can make a gadget for each RSS feed that you want to monitor.

Changing the RSS Feed Gadget Display

To change how the RSS feeds are displayed in the RSS Feed gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Feed Channel URL

Step 3 Click **Apply**.

For More Information

For information on customizing RSS feeds, see Configuring RSS Feeds, page 4-1.

Top Attackers Gadget

The Top Attackers gadget displays the number of events for each top attacker IP address over a specified time. The graph is changed according to the time limit. You can also filter on various conditions to get only the information you want to see. You can also choose to have DNS name resolution for each IP address.

Changing the Top Attackers Display

To change how the top attacker statistics are displayed in the Top Attackers gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Display form (bar chart, pie chart, or table)
- How many top attacker statistics to display at one time (10, 20, or 30)
- Interval to gather the statistics (last one hour, last eight hours, last one day)
- Filter associated with this gadget

Step 3 Check the **Resolve addresses** check box if you want to use DNS name resolution for each IP address.

Step 4 Click **Apply**.

For More Information

For the procedure for configuring filters, see Configuring Filters, page 3-16.

Top Victims Gadget

The Top Victims gadget displays the number of events for each top victim IP address over a specified time. The graph is changed according to the time limit. You can also filter on various conditions to get only the information you want to see. You can also choose to have DNS name resolution for each IP address.

Changing the Top Victims Display

To change how the top victim statistics are displayed in the Top Victims gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Display form (bar chart, pie chart, or table)
- How many top victim statistics to display at one time (10, 20, or 30)
- Interval to gather the statistics (last one hour, last eight hours, last one day)
- Filter associated with this gadget

Step 3 Check the **Resolve addresses** check box if you want to use DNS name resolution for each IP address.

Step 4 Click **Apply**.

For More Information

For the procedure for configuring filters, see Configuring Filters, page 3-16.

Top Signatures Gadget

The Top Signatures gadget displays the top number of signatures over a specified time. The graph is changed according to the time limit. You can also filter on various conditions to get only the information you want to see.

Changing the Top Signatures Display

To change how the top signatures statistics are displayed in the Top Signatures gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Display form (bar chart, pie chart, or table)
- How many top signatures to display at one time (10, 20, or 30)
- Interval to gather the statistics (last one hour, last eight hours, last one day)
- Filter associated with this gadget

Step 3 Click **Apply**.

For More Information

For the procedure for configuring filters, see Configuring Filters, page 3-16.

Attacks Over Time Gadget

The Attacks Over Time gadget displays the number of attacks over a specified time. The graph is changed according to the time limit. You can also filter on various conditions to get only the information you want to see.

Changing the Attacks Over Time Display

To change how the attacks over time statistics are displayed in the Attacks Over Time gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Interval to gather the statistics (last one hour, last eight hours, last one day)
- Filter associated with this gadget

Step 3 Click **Apply**.

For More Information

For the procedure for configuring filters, see Configuring Filters, page 3-16.

Working With a Single Event for Individual Top Attacker and Victim IP Addresses

To work with a single event for a specific IP address for a top attacker or victim, follow these steps:

Step 1 Choose **Home > Dashboards > Dashboard**, and then click the tab of the dashboard for which you want to work with individual attacker or victim IP addresses.

Step 2 From the Events for drop-down list, choose an attacker or victim IP address, for example, **Attacker 51.66.166.10**.

Data are retrieved from the database and displayed. From this window, you can view the attacker or victim settings and change them, and you can view the event details.

Step 3 To work with a single event, select the event in the list, and then click **Event** on the toolbar.

From the Event drop-down list, you can view the following information (it also appears in the lower half of the window under Event Details displayed in tab form):

- Summary—Summarizes all of the information about that event.
- Explanation—Provides the description and related signature information about the signature associated with this event.
- Related Threats—Provides the related threats with a link to more detailed information in MySDN.
- Trigger Packet—Displays information about the packet that triggered the event.
- Context Data—Displays the packet context information.
- Actions Taken—Lists which event actions were deployed.
- Notes—Lets you take action on this event by assigning a designation for it (New, Assigned, Acknowledged, Closed, or Deleted). Add any notes in the Notes field and click **Save Note** to save it.

Step 4 To print the details of this event, click **Show All Details** to display the event details in a printer-friendly window.

Step 5 To add an attribute from a selected event, from the Filter drop-down menu, click **Add to Filter > Attacker IP/Victim IP/Signature ID**. The Filter tab appears in the upper half of the window.

Step 6 To create a filter from this event, from the Filter drop-down menu, click **Create a Filter**.

Step 7 To edit the signature associated with this event, click **Edit Signature**. This takes you to **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures** where you can edit the signature.

Step 8 To create an event action rules filter from this event, click **Create Rule**. This takes you to **Configuration > *sensor_name* > Policies > IPS Policies > Add Event Action Filter** where you can add the event action rules filter.

Step 9 To stop the attacker, from the Stop Attacker drop-down menu, choose one of the following options:

- Using Inline Deny—This takes you to **Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Denied Attackers > Add Denied Attacker**.
- Using Block on another device—This takes you to **Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Host Blocks > Add Host Block**.

Step 10 To use ping, traceroute, DNS, and whois on the IP addresses involved in this event, choose them from the Tools drop-down menu.

You can use ping to diagnose basic network connectivity. Ping is a simple way to check if a sensor can communicate back. You can use traceroute to display the route an IP packet takes to a destination. You can use whois to determine the owner of a domain name or an IP address. You can use DNS lookup to translate host names to IP addresses, rather like a phone book.

Step 11 To save, delete, or copy the event, from the Other drop-down list, choose the action you want to perform.

Step 12 To save any changes that you have made to the view, click **Apply**. To discard any changes, click **Reset**.

For More Information

- For the procedure for adding filter rules, see Configuring Filters, page 3-16.
- For the procedure for adding an event action rules filter, see Adding, Editing, Deleting, Enabling, Disabling, and Moving Event Action Filters, page 12-17.
- For the procedure for adding a denied attacker, see Configuring and Monitoring Denied Attackers, page 17-1.
- For the procedure for adding a host block, see Configuring Host Blocks, page 17-3.
- For more information on using tools, see Using Tools for Devices, page 2-6.

Working With a Single Event for a Top Signature

To work with a single event for a specific Signature ID, follow these steps:

Step 1 Choose **Home > Dashboards > Dashboard**, and then click the tab for the sensor for which you want to work with a specific event for a specific signature.

Step 2 From the Events for drop-down list, choose a signature ID, for example, **SigID 3142**.

Data are retrieved from the database and displayed. From this window, you can view the settings and change them, and you can view the event details.

Step 3 To work with a single event, select the event in the list, and then click **Event**.

From the Event drop-down list, you can view the following information (it appears in the bottom half of the window under Event Details, and the same menu items are displayed in tab form):

- Summary—Summarizes all of the information about that event.
- Explanation—Provides the description and related signature information about the signature associated with this event.
- Related Threats—Provides the related threats with a link to more detailed information in MySDN.
- Trigger Packet—Displays information about the packet that triggered the event.
- Context Data—Displays the packet context information.
- Actions Taken—Lists which event actions were deployed.
- Notes—Lets you take action on this event by assigning a designation for it (New, Assigned, Acknowledged, Closed, or Deleted). Add any notes in the Notes field and click **Save Note** to save it.

Step 4 To print the details of this event, click **Show All Details** to display the event details in a printer-friendly window.

Step 5 To add this event to a filter, from the Filter drop-down menu, click **Add to Filter > Attacker IP/Victim IP/Signature ID**. The Filter tabs appear in the upper half of the window.

Step 6 To create a filter from this event, from the Filter drop-down menu, click **Create a Filter**.

Step 7 To edit the signature associated with this event, click **Edit Signature**. This takes you to **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures** where you can edit the signature.

Step 8 To create an event action rule filter from this event, click **Create Rule**. This takes you to **Configuration > *sensor_name* > Policies > IPS Policies > Add Event Action Filter** where you can add an event action rules filter.

Step 9 To stop the attacker, from the Stop Attacker drop-down menu, choose one of the following options:

- Using Inline Deny—This takes you to **Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Denied Attackers > Add Denied Attacker**.
- Using Block on another device—This takes you to **Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Host Blocks > Add Host Block**.

Step 10 To use Ping, Traceroute, DNS, and WHOIS on the IP addresses involved in this event, choose them from the Tools drop-down menu.

You can use ping to diagnose basic network connectivity. Ping is a simple way to check if a sensor can communicate back. You can use traceroute to display the route an IP packet takes to a destination. You can use whois to determine the owner of a domain name or an IP address. You can use DNS lookup to translate host names to IP addresses, rather like a phone book.

Step 11 To save, delete, or copy the event, from the Other drop-down list, choose the action you want to perform.

For More Information

- For the procedure for adding filter rules, see Configuring Filters, page 3-16.
- For the procedure for adding an event action rules filter, see Adding, Editing, Deleting, Enabling, Disabling, and Moving Event Action Filters, page 12-17.
- For the procedure for adding a denied attacker, see Configuring and Monitoring Denied Attackers, page 17-1.
- For the procedure for adding a host block, see Configuring Host Blocks, page 17-3.
- For more information on using tools, see Using Tools for Devices, page 2-6.

Configuring Filters

Note The Filter tab and Add Filter dialog box fields now support IPv6 and IPv4 addresses.

To configure filters, follow these steps:

Step 1 Choose **Home > Dashboards**, and then click the tab of the dashboard for which you want to configure filter rules.

Step 2 Choose the gadget for which you want to apply filters, for example, the Top Attackers gadget. You can apply filter rules to the Top Attackers, Top Victims, and Top Signatures gadgets.

Step 3 From the Events for drop-down menu, choose the IP address or signature ID to which you want to add a filter.

Step 4 Select the event(s) for which you want to apply filters.

Tip To select more than one item in the list, hold down the **Ctrl** key.

Step 5 Click **View Settings > Filter**.

Step 6 From the Filter Name drop-down menu, choose the filter name for this filter, or click the **Note** icon and then click **Add** to add a new filter:

a. In the Filter Name field, enter a name for this filter.

b. In the Attacker IP field, enter an attacker IP address, or click the **Note** icon and add a unique IP address or a range of IP addresses, and then click **OK**.

c. In the Victim IP field, enter a victim IP address, or click the **Note** icon and add a unique IP address or a range of IP addresses, and then click **OK**.

d. In the Signature Name/ID field, enter a signature name or ID, or click the **Note** icon, and then choose a signature type, and click **OK**.

e. In the Victim Port field, enter a victim port, or click the **Note** icon and enter a victim port that meets the conditions you require, and then click **OK**.

f. Choose the severity levels you want for this filter.

g. In the Risk Rating field, enter the risk rating for this filter, or click the **Note** icon, and then enter the risk rating that meets the conditions you require, and click **OK**.

h. In the Reputation field, enter the reputation score for this filter, or click the **Note** icon, and then enter the reputation that meets the conditions you require, and click **OK**.

i. In the Threat Rating field, enter the threat rating for this filter, or click the **Note** icon, and then enter the threat rating that meets the conditions you require, and click **OK**.

j. In the Actions Taken field, enter the actions you want to trigger this filter, or click the **Note** icon, and then check the check boxes of the actions that you want to trigger this filter, and click **OK**.

k. In the Sensor Name(s) field, enter the names of the sensors that are affected by this filter, or click the **Note** icon, and check the check boxes of the sensor to which this filter applies and click **OK**.

l. In the Virtual Sensor field, enter the virtual sensor to which this filter applies.

m. From the Status drop-down menu, choose on which status you want to filter.

n. In the Victim Locality field, enter the name of any event action rules variable that you created on which you want to filter.

Step 7 To configure grouping, click the **Group By** tab:

a. Check the **Group events based on the following criteria** check box, and then set up the hierarchy of how you want to group the events by selecting the category from the drop-down menus.

b. Under Grouping Preferences, you can check the **Single Level**, **Show Group Columns**, or **Show Count Columns** check boxes. You can only show count columns if you enable Show Group Columns.

Step 8 To add color rules, click the **Color Rules** tab, and then click **Add**.

a. In the Filter Name field, enter a name for this color rules filter.

b. Check the **Enable** check box.

Note If you do not check the **Enable** check box, your color rules filter will not go in to effect.

c. Under Packet Parameters, enter the IP addresses, signature names and/or victim ports for which you want this color rules filter to apply.

d. Under Rating and Action Parameters, enter the severity, risk rating, threat rating, and actions for which you want this color rules filter to apply.

e. Under Other Parameters, enter the sensor name, virtual sensor name, status, and/or victim locality for which you want this color rules filter to apply.

f. Under Color Parameters, choose the foreground and background colors, and the font type for this color rules filter, and then click **OK**.

Tip For aid in entering the correctly formatted values for these fields, click the **Note** icon.

Step 9 To event fields and their order, click the **Fields** tab, and then click **Add >>**, **<< Remove**, **Move Up**, and **Move Down** to chose which fields you want to display and to arrange the fields in the order in which you want to see them.

Step 10 Click the **General** tab, and then in the View Description field enter a description for your view.

Step 11 Click **Save As** to create the new view, and then in the Name field, enter a name for your view. The settings are copied to the new view.

Step 12 Click **Save** to save any changes to the view. Your filter now appears in the Filter Name drop-down menu.

Step 13 To save any changes that you have made to the view, click **Apply**. To discard any changes, click **Reset**.

Manage Filter Rules Dialog Box Field Definitions

The following fields are found in the Manage Filter Rules dialog box:

- Basic Top Attacker Filter—Shows all severity levels (high, medium, low, and informational) for top attacker events.
- Action Denied-Attacker—Shows denied attacker actions, new alarm status, and all severity levels (high, medium, low, and informational) for denied action events.
- Basic Over Time Attack Filter—Shows all severity levels (high, medium, low, and informational) for attacks over time events.
- Basic Top Signature Filter—Shows all severity levels (high, medium, low, and informational) for the top signature events.
- Basic Top Victim Filter—Shows all severity levels (high, medium, low, and informational) for top victims events.
- Related Events Filter—Shows all severity levels (high, medium, low, and informational) for related events.
- Critical Threat—Shows all threat ratings between 75 and 100, new alarm status, and all severity levels (high, medium, low, and informational) for critical events.
- High Severity—Shows all alerts with a new alarm status and high severity level for all events.
- Basic View Filter—Shows all severity levels (high, medium, low, and informational) for all events.
- Basic Filter—Shows new alarm status and all severity levels (high, medium, low, and informational) for all events.

Add and Edit Filter Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Filter dialog boxes:

- Filter Name—Lets you name this filter or pick from the default filters.
- Attacker IP—Attacker IP address you want to include in this filter. The valid values are *ip_address*, *ip_address_range*, for example, 10.0.0.1, !10.0.0.1, !10.1.1.1.

Note The exclamation point (!) means 'does not include.'

- Victim IP—Victim IP address you want to include in this filter. The valid values are *ip_address*, *ip_address_range*, for example, 10.0.0.1, !10.0.0.1, !10.1.1.1.
- Signature Name/ID—Signature Name/ID you want to include in this filter. The valid values are *signature_name* or *signature_id* or *signature_id/subsig_id* or *signature_id_range*, for example:
  - no_checkpoint
  - no_checkpoint, 3320
  - no_checkpoint, 3320/1
  - 3300-400
- Victim Port—Victim port you want to include in this filter. The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Severity—Severity levels you want to include in this filter.
- Risk Rating—Risk rating you want to include in this filter. The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Reputation—Reputation score you want to include in this filter. The valid values are from -10.0 to 10.0.
- Threat Rating—Threat rating you want to include in this filter. The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Action(s) Taken—Lets you choose which actions the filter looks for in the alerts. The actions are a string that you can chose or you can enter free format strings.
- Sensor Name(s)—Lets you assign which sensors are included in this filter.
- Virtual Sensor—Lets you assign which virtual sensors are included in this filter.
- Status—Lets you assign a status to this filter (All, New, Assigned, Closed, Detected, Acknowledged). The Status field is useful, for example, in a situation where you want to save analysis of certain events for later. You can add a note and change the status to 'Acknowledged,' and then later you can filter by status to see all cases that are acknowledged and then do further analysis.
- Victim Locality—An alert attribute in the participants/address alert on which you can filter. It is defined in the event action rules variables.
- Color Parameters—Lets you configure color rules for your events (the following options only appear when you are adding a filter on the Color Rules tab):
  - Foreground—Displays and let you chose the foreground color for your event.
  - Background—Displays and let you chose the background color for your event.
  - Font Type—Lets you chose bold, italic, or both for your event.
  - Preview Text—Displays how the event will look in the view.

Configuring RSS Feeds

This chapter describes RSS feeds and how to configure them. It contains the following topics:

Understanding RSS Feeds

By default three RSS feed channels are set up to come directly from the Cisco Intelligence Operations website. But you can locate any RSS feeds that you want and configure IME to receive them in the **Cisco Security Center > RSS Feeds** pane. You can also have an RSS Feed gadget display the feeds from a specific URL.

RSS feed formats are used to publish frequently updated content such as security information, news items, podcasts, and blog entries. Through IME, you can configure RSS feeds to keep up with the latest in security challenges and security news.

IME supports the following RSS feed formats:

- RSS 0.9x
- RSS 1.0/RDF
- RSS 2.0
- Atom 0.3
- Atom 1.0

You can use these RSS feed formats by using an open source library from Informa.

Use the tool bar in the RRS Feeds pane to configure and organize RSS feeds. You can also use the right-click menu for the same functions.

Configuring RSS Feeds

Although the RSS Feeds icons do not have labels, you can determine which icon is which by using the hover-over help. You can add RSS feed channels and organize them into categories. You can also configure RSS feeds preferences.

Table 4-1 shows the RSS icons and what they configure.

Table 4-1 RSS Icon Descriptions

Icon	Description
	Add Category
	Delete Category
	Rename Category
	Add Channel
	Delete Channel
	Reload Channel
	Move Channel to Another Category
	Rename Channel
	Change Preferences

Configuring RSS Feeds

To configure RSS feeds, follow these steps:

Step 1 Locate the website with the RSS feed that you want to add.

Step 2 Copy the URL of the RSS Feed.

Step 3 Choose **Home > Cisco Security Center > RSS Feeds**, and then click the **Add Channel** icon in the RSS Feeds tool bar.

Step 4 In the Add Channel dialog box, enter the URL of the channel from which you want to receive RSS Feeds. The RSS Feed site appears in the left-hand pane and the items appear in the upper right-hand pane.

Step 5 To view an RSS feed item, select the category in the left-hand pane, and then select the item you want to view in the list in the right-hand pane. The item information appears in the lower right-hand pane. To see more of the item, click **Read more**.

Step 6 To create a new category, click the **Add Category** icon, and in the Add Category dialog box, assign a new category name. The new category appears in the list in the left-hand pane.

Step 7 To move a channel to another category, select it in the right-hand pane, click the **Move Channel** icon, and in the Move Channel dialog box select the new category under which you want the category to appear, and then click **OK**.

Step 8 To move a category under another category, select the channel in the right-hand pane, click the **Move Channel** icon, and in the Move Channel dialog box select the new category to which you want to move the channel, and then click **OK**

Step 9 To delete a category and all of the RSS feeds within it, select the category in the left-hand pane, and then click the **Delete Category** icon. To delete a channel, select it in the upper right-hand pane, and then click the **Delete Channel** icon. You cannot delete the three default Cisco RSS feed categories.

Step 10 To rename a category, select it in the left-hand pane, click the **Rename Category** icon, and then enter the new name in the Rename Category dialog box. To rename a channel, select it in the upper right-hand pane, click the **Rename Channel** icon, and then enter the new name in the Site Name field in the Rename Channel dialog box.

Step 11 To reload a channel, select the category in the left-hand pane, and then click the **Reload Channel** icon.

Step 12 To configure the RSS feeds preferences, click the **Change Preferences** icon.

a. Check the **Allow duplicate channel creation** check box if you want to be able to create duplicate channels.

b. From the drop-down menu, choose how many news items you want to remain in cache. You can choose 10, 30, 50, 100, 300, or 1000.

c. In the Refresh every minutes field, choose how often you want to refresh RSS feeds.

d. To change the default browser, click the **Use following browser** radio button, and enter the browser command line in the Browser command line field, and then click **OK**.

Using the Startup Wizard

This chapter describes the Startup wizard and how to use it to configure your sensor. It contains the following sections:

Startup Wizard Introduction Window

Note You must be administrator to configure basic sensor settings in the Startup wizard.

Because the IME cannot communicate with an unconfigured sensor, you must log in to the sensor CLI and run the **setup** command to configure communication parameters. You can set all communication parameters by using the **setup** command. You can use the Startup Wizard to modify a sensor that has already been configured, but you cannot use the Startup Wizard for initializing a new, unconfigured sensor. You must use the **setup** command for that. Because until you initialize the sensor with the **setup** command, the IME cannot connect to the sensor.

The Startup Wizard leads you through the steps needed to configure the sensor to inspect, respond to, and report on traffic. You can configure basic sensor settings, configure interfaces, create virtual sensors, create policies, assign policies and interfaces to the virtual sensor, associate signature policies with various threat profiles, configure the sensor to automatically download signature and signature engine updates from Cisco.com, and save your changes to the sensor.

You can use the Startup Wizard on all IPS platforms. If a feature is not available on a certain platform, you will not see that configuration window.

Note VLAN groups are not supported in the Startup Wizard.

The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the following features of the Setup Wizard:

- Inline VLAN pairs
- Inline interface pairs
- VLAN groups,
- Setting the time

Note The ASA IPS modules get their time settings from the router, switch, or adaptive security appliance in which they are installed.

- Interface configuration (you must configure interfaces on the adaptive security appliance)

For More Information

You must initialize the sensor before you can choose **Configuration** > ***sensor_name*** > **Sensor Setup** in IME to further configure the sensor. For the procedure for using the **setup** command to initialize the sensor, see Basic Sensor Setup, page 25-4.

Setting up the Sensor

This section describes how to set up the sensor, and contains the following topics:

Sensor Setup Window

In the two Sensor Setup window, you can configure the sensor for basic operation. Most of the fields will already be populated because you assigned the values during initialization. But you can change them here if needed.

Field Definitions

The following fields are found in the Sensor Setup window:

- Network Settings—Lets you set the network settings of the sensor:
  - Host Name—Specifies the name of the sensor. The hostname can be a string of 1 to 64 characters that matches the pattern ^[A-Za-z0-9_/-]+$. The default is sensor. You receive an error message if the name contains a space or exceeds 64 alphanumeric characters.
  - IP Address—Specifies the IP address of the sensor. The default is 192.168.1.2.
  - Subnet Mask—Specifies the mask corresponding to the IP address. The default is 255.255.255.0.
  - Gateway—Specifies the default gateway address. The default is 192.168.1.1.

- HTTP Proxy Server—Lets you enter an HTTP proxy server IP address. You may need proxy servers to download global correlation updates if customer networks use proxy in their networks.
- HTTP Proxy Port—Lets you enter the port number for the HTTP proxy server.
- DNS Primary—Lets you enter the primary DNS server IP address.

Caution For automatic and global correlation updates to function, you must have either a DNS server or an HTTP proxy server configured at all times.

Caution DNS resolution is supported only for accessing the automatic update and global correlation update server.

- Allowed hosts/networks that can access the sensor—Lets you add ACLs:
  - Network—Specifies the IP address of the network you want to add to the access list.
  - Mask—Specifies the netmask of the network you want to add to the access list.

  Note If you change the sensor ACL entries, the IME may lose connection to the sensor when the changes are applied.

- Network Participation—Lets you chose to participate in sending data to the SensorBase Network and at which level you want to participate:
  - Off—No data is contributed to the SensorBase Network.
  - Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
  - Full—All data is contributed to the SensorBase Network.

Add and Edit ACL Entry Dialog Boxes

You can configure the list of hosts or networks that you want to have access to your sensor. The following hosts must have an entry in the access list:

- Hosts that need to Telnet to your sensor.
- Hosts that need to use SSH with your sensor.
- Hosts, such as the IDM and the ASDM, that need to access your sensor from a web browser.
- Management stations, such as the CSM, that need access to your sensor.
- If your sensor is a master blocking sensor, the IP addresses of the blocking forwarding sensors must have an entry in the list.

Field Definitions

The following fields are found in the Add and Edit ACL Entry dialog boxes:

- IP Address—Specifies the IP address of the host or network you want to have access to your sensor.
- Network Mask—Specifies the network mask of the host or network you want to have access to your sensor. The netmask for a single host is 32.

Sensor Setup Window

In the two Sensor Setup windows, you can configure the sensor for basic operation. Most of the fields will already be populated because you assigned the values during initialization. But you can change them here if needed.

Field Definitions

The following fields are found in the Sensor Setup window:

- Current Sensor Date and Time—Sets the time and date for appliances that are not configured with an NTP server:
  - Date—Specifies the sensor local date. When you update the time and date, click **Apply Date/Time to Sensor** to have it go in to effect.
  - Apply Date/Time to Sensor—Immediately updates the time and date on the sensor.

    Note If you cancel the Startup Wizard, the date and time changes remain.

- Time Zone—Sets the zone name and UTC offset:
  - Zone Name—Specifies the local time zone when summertime is not in effect. The default is UTC. You can choose from a predefined set of 37 time zones, or you can create a unique name (24 characters) in the following pattern: ^[A-Za-z0-9()+:,_/-]+$
  - Offset—Specifies the local time zone offset in minutes. The default is 0. If you select a predefined time zone this field is populated automatically.

    Note Changing the time zone offset requires the sensor to reboot.

- NTP Server—Lets you configure the sensor to use an NTP server as its time source:
  - IP Address—Specifies the IP address of the NTP server if you use this to set time on the sensor.
  - Authenticated NTP—Lets you use authenticated NTP, which requires a key and key ID.
  - Key—Specifies the NTP MD5 key type.
  - Key ID—Specifies the ID of the key (1 to 65535) used to authenticate on the NTP server. You receive an error message if the key ID is out of range.

    Note We recommend that you use an NTP server as the sensor time source.

- Summertime—Lets you configure the summer mode:
  - Enable Summertime—Check to enable summertime mode. The default is disabled.
  - Configure Summertime—Click to configure summertime settings.

Configure Summertime Dialog Box

Note You must be administrator to configure time settings.

The following fields are found in the Configure Summertime dialog box:

- Summer Zone Name—Specifies the summertime zone name. The default is UTC. You can choose from a predefined set of 37 time zones, or you can create a unique name (24 characters) in the following pattern: ^[A-Za-z0-9()+:,_/-]+$
- Offset—Specifies the number of minutes to add during summertime. The default is 60. If you choose a predefined time zone, this field is populated automatically.

  Note Changing the time zone offset requires the sensor to reboot.

- Start Time—Specifies the summertime start time setting. The value is hh:mm. You receive an error message if the hours or minutes are out of range.
- End Time—Specifies the summertime end time setting. The value is hh:mm. You receive an error message if the hours or minutes are out of range.
- Summertime Duration—Lets you set whether the duration is recurring or a single date:
  - Recurring—Specifies the duration is in recurring mode.
  - Date—Specifies the duration is in nonrecurring mode.
  - Start—Specifies the start week, day, and month setting.
  - End—Specifies the end week, day, and month setting.

Configuring Sensor Settings

To configure sensor settings in the Startup Wizard, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Startup Wizard > Launch Startup Wizard**, and then click **Next**.

Step 3 In the Host Name field, enter the sensor name.

Step 4 In the IP Address field, enter the sensor IP address.

Step 5 In the Subnet Mask field, enter the network mask address.

Step 6 In the Gateway field, enter the default gateway address.

Note If you change the sensor network settings, the IME loses connection to the sensor when the changes are applied.

Step 7 To configure either an HTTP proxy server or a DNS server to support automatic updates and global correlation, enter the HTTP proxy server IP address in the HTTP Proxy Server field and the port number in the HTTP Proxy Port field, or enter the DNS server IP address in the DNS Primary field. If you do not want to turn on global correlation, click **OK** on the following Warning dialog box:

```
Global correlation requires either an HTTP proxy server or at least one DNS server.
```

If you are using a DNS server, you must configure at least one DNS server and it must be reachable for automatic updates and global correlation updates to be successful. You can configure other DNS servers as backup servers. DNS queries are sent to the first server in the list. If it is unreachable, DNS queries are sent to the next configured DNS server.

Caution For automatic and global correlation updates to function, you must have either a DNS server or an HTTP proxy server configured at all times.

Caution DNS resolution is supported only for accessing the automatic update or global threat correlation update server.

Step 8 To configure the hosts and networks that are allowed to access the sensor, click **Add**:

a. In the IP Address field, enter the IP address of the host you want to have access to the sensor.

b. In the Network Mask field, enter the network mask address of the host you want to have access to the sensor.

c. Click **OK**.

Tip To discard your changes and close the Add ACL Entry dialog box, click **Cancel**.

Step 9 To enable network participation, select the degree of network participation that you want:

- Off—No data is contributed to the SensorBase Network.
- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network.

Note The default is Off. If you chose Partial or Full, you must agree to the Network Participation Disclaimer.

Tip To discard your changes and close the Sensor Setup window, click **Cancel**.

Step 10 Click **Next** to continue to the next Setup window.

Step 11 Under Current Sensor Date and Time, select the current date and time from the drop-down calendar, and then click **OK**, and then click **Apply Date/Time to Sensor**. Date and time indicate the date and time on the local host.

Caution If you accidentally specify the incorrect time, stored events have the wrong time stamp. You must clear the events.

Note If you cancel the Startup Wizard, the date and time changes remain.

Note You cannot change the date or time on IPS modules or if you have configured NTP.

Step 12 Under Time Zone, configure the time zone and offset:

a. In the Zone Name field, choose a time zone from the drop- down list, or enter one that you have created. This is the time zone to be displayed when summertime hours are not in effect.

b. In the Offset field, enter the offset in minutes from UTC. If you choose a predefined time zone name, this field is automatically populated.

Note Changing the time zone offset requires the sensor to reboot.

Step 13 If you are using NTP synchronization, under NTP Server enter the following:

- The IP address of the NTP server in the IP Address field.
- If using authenticated NTP, check the **Authenticated NTP** check box, and then enter the key of the NTP server in the Key field, and the key ID of the NTP server in the Key ID field.

Note If you define an NTP server, the sensor time is set by the NTP server. The CLI **clock set** command produces an error, but time zone and daylight saving time parameters are valid.

Step 14 To enable daylight saving time, check the **Enable Summertime** check box, and then click **Configure Summertime**.

Step 15 Choose the Summer Zone Name from the drop-down list or enter one that you have created. This is the name to be displayed when daylight saving time is in effect.

Step 16 In the Offset field, enter the number of minutes to add during summertime. If you choose a predefined summer zone name, this field is automatically populated.

Step 17 In the Start Time field, enter the time to apply summertime settings.

Step 18 In the End Time field, enter the time to remove summertime settings.

Step 19 Under Summertime Duration, choose whether summertime settings will occur on specified days each year (recurring) or whether they will start and end on specific dates (date):

a. Recurring—Choose the Start and End times from the drop-down lists. The default is the second Sunday in March and the first Sunday in November.

b. Date—Choose the Start and End time from the drop-down lists. The default is January 1 for the start and end time.

Step 20 Click **OK**.

Tip To discard your changes, click **Cancel**.

Step 21 Click **Next** to continue through the Startup Wizard.

Note Changing the network settings may disrupt your connection to the sensor and force you to reconnect with the new address.

Configuring Interfaces

Note You cannot use the Startup Wizard to configure interfaces and virtual sensors for the ASA 5500-X IPS SSP or ASA 5585-X IPS SSP.

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

Interface Summary Window

The Interface Summary window displays the existing interface configuration settings. If an interface is not assigned to a virtual sensor, the Assigned Virtual Sensor column reads “None” and the Details column reads “Backplane” for platforms that have backplane interfaces. The details column reads “Promiscuous” for all other platforms. An interface can be either physical or logical. A physical interface can also be part of a logical interface and can be further subdivided.

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) all have backplane interfaces.

Note You can configure one physical or logical interface during each Startup Wizard session. To configure multiple interfaces, run Startup Wizard multiple times.

You can specify interface configuration in one of five types:

- Promiscuous
- Promiscuous VLAN group (a subinterface)
- Inline interface pair
- Inline interface pair VLAN group (a subinterface)
- Inline VLAN pair (a subinterface)

Note VLAN groups are not supported in the Startup Wizard.

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.

You can click **Finish** to exit the Startup Wizard on this window and commit your changes, or you can continue to configure interfaces and virtual sensors.

Field Definitions

The following fields are found in the Interface Summary window:

- Name—Displays the name of the interface. The values are FastEthernet, GigabitEthernet, Management, or PortChannel for promiscuous interfaces. For inline interfaces, the name is whatever you assigned to the pair.
- Details—Tells you whether the interface is promiscuous, inline, or backplane and whether there are VLAN pairs.
- Assigned Virtual Sensor—Tells you whether the interface or interface pair has been assigned to a virtual sensor.
- Enabled—Tells you whether this interface is enabled or disabled.
- Description—Displays your description of the interface.

Restore Defaults to an Interface Dialog Box

The Restore Default Interface dialog box displays all of the interfaces that are configured or assigned to a virtual sensor. You can select any of the interfaces to be restored. If the selected interface is assigned to a virtual sensor, it is unassigned. If you select an inline interface pair, both physical interfaces are restored to the default and the logical interface is deleted. You cannot select and restore defaults to an inline VLAN pair or VLAN group.

Caution You can only restore defaults to physical interfaces and inline interface pairs.

Traffic Inspection Mode Window

The Traffic Inspection Mode window lets you configure the sensor interfaces as promiscuous, inline interface, or inline VLAN pair mode. If the sensor only has one physical interface, the Inline Interface Pair Mode radio button is disabled. If the sensor does not support inline VLAN pair mode, that option is also disabled.

The following radio buttons are found on the Traffic Inspection Mode window:

- (Keep existing interface configuration)—No changes are made to the interface configuration of the sensor.
- Promiscuous—The sensor is not in the data path of the inspected packets. The sensor cannot modify or drop packets.
- Inline Interface Pair—The sensor is in the data path of the inspected packets. The sensor can modify or drop inspected packets. For inline interface inspection, you must pair two physical interfaces together.

- Inline VLAN Pair—The sensor is in the data path of the inspected packets. The sensor can modify or drop inspected packets. For inline VLAN inspection, you must have one physical interface and an even number of VLANs and the interface must be connected to a trunk port.

Interface Selection Window

On the Interface Selection window, you can choose which interface you want to configure.

Note You can configure one physical or logical interface during each Startup Wizard session. To configure multiple interfaces, run Startup Wizard multiple times.

Inline Interface Pair Window

In the Inline Interface Pair window, you can assign an interface name for two unique interfaces. If your sensor supports hardware bypass, an icon identifies that. If you pair a hardware bypass interface with an interface that does not support hardware bypass, you receive a warning message indicating that hardware bypass is not available.

Note Hardware bypass interfaces allow packet flow to continue even if power is disrupted.

Field Definitions

The following fields are found on the Inline Interface Pair window:

- Inline Interface Name—Lets you assign a name to this inline interface pair.
- First Interface of Pair—Lets you assign the first interface of this pair.
- Second Interface of Pair—Lets you assign the other interface of this pair.

Inline VLAN Pairs Window

If you checked the Inline VLAN Pair Mode radio button in the Interface Inspection Mode window, you can configure inline VLAN pairs on the Inline VLAN Pairs window. If you have already configured inline VLAN pairs, they appear in the table, and you can edit or delete them.

Note You cannot create an inline VLAN pair for an interface that has already been paired with another interface or for an interface that is in promiscuous mode and assigned to a virtual sensor.

To create an inline VLAN pair for an interface that is in promiscuous mode, you must remove the interface from the virtual sensor and then create the inline VLAN pair. You can only pair interfaces that are available.

Note If your sensor does not support inline VLAN pairs, the Inline VLAN Pairs window is not displayed. The ASAIPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support inline VLAN pairs.

Field Definitions

The following fields are found in the Inline VLAN Pairs window:

- Subinterface Number—Displays the subinterface number of the inline VLAN pair. The value is 1 to 255.
- VLAN A—Displays the VLAN number for the first VLAN. The value is 1 to 4095.
- VLAN B—Displays the VLAN number for the second VLAN. The value is 1 to 4095.
- Interface—Displays the name of the inline VLAN pair.
- Virtual Sensor—Displays the name of the virtual sensor for this inline VLAN pair.
- Description—Displays your description of the inline VLAN pair.

Add and Edit Inline VLAN Pair Entry Dialog Boxes

Note You cannot pair a VLAN with itself.

Note The subinterface number and the VLAN numbers should be unique to each physical interface.

The following fields are found in the Add and Edit Inline VLAN Pair Entry dialog boxes:

- Subinterface Number—Lets you assign a subinterface number. You can assign a number from 1 to 255.
- VLAN A—Lets you specify the first VLAN for this inline VLAN pair. You can assign any VLAN from 1 to 4095.
- VLAN B—Lets you specify the other VLAN for this inline VLAN pair. You can assign any VLAN from 1 to 4095.
- Description—Lets you add a description of this inline VLAN pair.

Configuring Inline VLAN Pairs

To configure inline VLAN pairs in the Startup Wizard, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Startup Wizard > Launch Startup Wizard**, and then click **Next**. until you get to the Traffic Inspection Mode window.

Step 3 Click the **Inline VLAN Pair Mode** radio button, click **Next,** and then click **Add**.

Step 4 In the Subinterface Number field, enter a subinterface number (1 to 255) for the inline VLAN pair.

Step 5 In the VLAN 1 field, specify the first VLAN (1 to 4095) for this inline VLAN pair.

Step 6 In the VLAN 2 field, specify the other VLAN (1 to 4095) for this inline VLAN pair.

Step 7 In the Description field, add a description of the inline VLAN pair if desired.

Tip To discard your changes and close the Add Inline VLAN Pair dialog box, click **Cancel**.

Step 8 Click **OK**. The new inline VLAN pair appears in the list in the Inline VLAN Pairs window.

Step 9 To edit an inline VLAN pair, select it, and click **Edit**.

Step 10 You can change the subinterface number, the VLAN numbers, or edit the description.

Tip To discard your changes and close the Edit Inline VLAN Pair dialog box, click **Cancel**.

Step 11 Click **OK**. The edited VLAN pair appears in the list in the Inline VLAN Pairs window.

Step 12 To delete a VLAN pair, select it, and click **Delete**. The VLAN pair no longer appears in the list in the Inline VLAN Pairs window.

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

Step 13 Click **Apply** to apply your changes and save the revised configuration.

Configuring Virtual Sensors

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

Virtual Sensors Window

After you have configured interfaces, you assign them to a virtual sensor in the Virtual Sensors window of the Startup Wizard. By default, the interface is assigned to virtual sensor vs0. You can assign the interface to any existing virtual sensor or you can create a new virtual sensor. To create a virtual sensor, click **Create a Virtual Sensor**. The Add Virtual Sensor dialog box appears and you can configure a virtual sensor.

Note The ASAIPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not have configurable interfaces; therefore, you must use the default virtual sensor. You cannot create a new virtual sensor using the Startup Wizard and you will not see the fields for creating a new virtual sensor.

Field Definitions

The following fields are found in the Virtual Sensors window:

- IPS Policy Summary—Displays the assigned interfaces with assigned policies:
  - Name—Displays the name of the virtual sensor. The default virtual sensor is vs0.

  - Interfaces—Lists the interfaces that you want to assign to a virtual sensor.
  - Signature Policy—Displays the name of the signature policy. The default signature policy is sig0.
  - Event Action Policy—Displays the name of the event action policy. The default event action policy is rules0.
  - Anomaly Detection Policy—Displays the name of the anomaly detection policy. The default anomaly detection policy is ad0.

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

  - Description—Displays the description of the virtual sensor.
- Virtual Sensor Assignments—Lets you assign interfaces and create a virtual sensor for appliances; for modules, the default virtual sensor, vs0, is already assigned.
  - Interface(s)—Lists the available interfaces.
  - Assign Interface to Virtual Sensor—Lists the available virtual sensors. The default sensor is vs0.
  - Create a Virtual Sensor—Displays the Add Virtual Sensor dialog where you can create a virtual sensor with new signature, event action rules, and anomaly detection policies, or you can use the default policies.
- Default Block Policy—Lets you select a risk category for this virtual sensor:
  - Select Virtual Sensor—Lets you choose a virtual sensor to apply the default block policy to. If your sensor does not support virtualization, you will see only vs0 (the default virtual sensor) as a choice.
  - Select a Risk Category—Displays the default risk category used in the deny event action override. Alerts with a risk rating of 90-100 are denied by default. If you do not want to use the default risk category, you can edit the HIGHRISK risk category, or create a new risk category in **Configuration > *sensor_name* > Policies > IPS Policies > Event Action Rules > rules0 > Risk Category**.

Add Virtual Sensor Dialog Box

In the Add Virtual Sensor dialog box, you can create a new signature policy, event action rules policy, and anomaly detection policy, but you cannot configure them. You create the new policy by cloning the default policy. To configure the new policy:

- For new signature policies, choose **Configuration > *sensor_name* > Policies > Signature Definitions > *NewSigPolicy* > Active Signatures**.
- For new event action rules policies, choose **Configuration > *sensor_name* > Policies > Event Action Rules > *NewRulesPolicy***.
- For new anomaly detection policies, choose **Configuration > *sensor_name* > Policies > Anomaly Detections > *NewADPolicy***.

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

Field Definitions

The following fields are found in the Add Virtual Sensor dialog box:

- Virtual Sensor name—Lets you assign a name to the virtual sensor.
- Description—Lets you add a description of the virtual sensor.
- Assign a Signature Policy—Lets you assign a signature policy:
  - Assign a Signature Policy—Lets you assign a signature policy that has already been created.
  - Create a Signature Policy—Lets you create a new signature policy.
- Assign an Event Action Rules Policy—Lets you assign an event action rules policy:
  - Assign an Event Action Rules Policy—Lets you assign an event action rules policy that has already been created.
  - Create an Event Action Rules Policy—Lets you create a new event action rules policy.
- Assign an Anomaly Detection Policy—Lets you assign an anomaly detection policy:
  - Assign an Anomaly Detection Policy—Lets you assign an anomaly detection policy that has already been created.
  - Create an Anomaly Detection Policy—Lets you create a new anomaly detection policy.

For More Information

For the procedure for enabling anomaly detection, see Enabling Anomaly Detection, page 13-4.

Adding a Virtual Sensor

To add a virtual sensor using the Startup Wizard, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Startup Wizard > Launch Startup Wizard**, and then click **Next** until you get to the Virtual Sensors window.

Step 3 Click **Create a Virtual Sensor**.

Step 4 In the Virtual Sensor name field, enter the virtual sensor name.

Step 5 In the Description field, enter a description that will help you identify this virtual sensor.

Step 6 Assign a signature policy by doing one of the following:

a. Click the **Assign a Signature Policy** radio button and chose a signature policy from the drop-down list.

b. Click the **Create a Signature Policy** radio button and enter a name for the signature policy in the field.

Note To configure the new signature policy, choose **Configuration > *sensor_name* >Policies > IPS Policies > Signature Definitions > *NewSigPolicy* > Active Signatures**.

Step 7 Assign an event action rules policy by doing one of the following:

a. Click the **Assign an Event Action Rules Policy** radio button and chose an event action rules policy from the drop-down list.

b. Click the **Create an Event Action Rules Policy** radio button and enter a name for the event action rules policy in the field.

Note To configure the new event action rules policy, choose **Configuration > *sensor_name* >Policies > Event Action Rules > *NewRulesPolicy***.

Step 8 Assign an anomaly detection policy by doing one of the following:

a. Click the **Assign an Anomaly Detection Policy** radio button and chose an anomaly detection policy from the drop-down list.

b. Click the **Create an Anomaly Detection Policy** radio button and enter a name for the anomaly detection policy in the field.

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

Note To configure the new anomaly detection policy, click **Configuration > *sensor_name* > Policies > IPS Policies > Anomaly Detections > *NewADPolicy***.

Step 9 Click **Finish**, and then in the Confirm Configuration Changes dialog box, click **Yes** to save your changes.

Applying Signature Threat Profiles

Note You must be administrator to configure signature threat profiles.

Note Signature threat profiles are supported on the IPS 4345, IPS 4360, IPS 4510, IPS 4520, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP.

In the Signatures window, you can apply threat profiles (specific signature templates) to individual signature policies. A signature threat profile is a predefined signature template that includes customized tunings. These tunings adjust the signature coverage and response actions to enable the sensor to make better choices in various deployment and threat scenarios. You can apply a signature threat profile to one or more signature policies.

The template is dynamic. You can see a description of the template when you select it. Some of the templates may use most or possibly all of the available resources of the sensor for signatures. Some templates are limited to use in virtual sensor vs0, and the sensor may not have enough memory available for using custom signatures. Creating additional virtual sensors and/or custom signatures may cause the

sensor to run out of resources during configuration or while monitoring traffic. Templates also enable additional signatures. Tuning may be required to correct for false positives that may occur on your network when these signatures are added.

Once you apply a signature template to a virtual sensor, you can make modifications to the templates, such as retiring a signature to eliminate a false positive. Your changes are NOT overwritten during signature updates or sensor software upgrades.

However, your changes to signatures settings are removed if the wizard is used to apply a template to the same virtual sensor. The previous configuration is deleted when the template is applied through the wizard.

Caution Applying a signature threat profile overwrites any existing tunings in the corresponding signature policy. You can further customize the signature policy after the signature template has been applied.

Field Definitions

The following fields are found on the Signatures window of the Startup Wizard:

- Policy Name—Displays the names of the signature policies.

  You create and configure signature policies at **Configuration > Policies > Signature Definitions > Add**. Those signature policies are displayed here.
- Threat Profile to Apply—Displays the threat profile that has been applied.
- Select Threat Profile—Lets you apply one of the following signature threat profiles:
  - Keep Existing Tunings
  - Data Center
  - Edge

Note The signature templates are dynamic so the threat profile descriptions change according to the signature set. You can see the descriptions when you apply the template.

Applying Signature Threat Profiles

To apply signature threat profiles to signature policies using the Startup Wizard, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Startup Wizard > Launch Startup Wizard**, and then click **Next** until you get to the Signatures window.

Step 3 In the IPS Signature Policies list, select the signature policy that you want to apply a signature threat profile to.

Step 4 Under Deployment and Threat Profiles, from the Select Threat Profile drop-down list, select one of the following signature templates:

- Keep Existing Tunings
- Data Center
- Edge

Caution Applying a signature threat profile overwrites any existing tunings in the corresponding signature policy. You can further customize the signature policy after the signature template has been applied.

Step 5 Click **Apply Template**, and then click **Finish**.

A dialog box appears stating that the sensor is calculating the changes required to deploy the threat profiles.

Step 6 In the Confirm Configuration Changes dialog box, click **Yes** to save your changes.

Configuring Auto Update

Caution The IPS address has been changed to cisco.com in the URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new address.

You can configure the sensor to automatically download signature and signature engine updates from Cisco.com. When you enable automatic updates, the sensor logs in to Cisco.com and checks for signature and signature engine updates. When an update is available, the sensor downloads the update and installs it. You must have a Cisco.com user account with cryptographic privileges to download Cisco IPS signature and signature engine updates from Cisco.com. The first time you download Cisco software you set up an account with cryptographic privileges.

Caution The sensor does not support communication with Cisco.com through nontransparent proxy servers.

Note Automatic update requires either an HTTP proxy server or at least one DNS server to function.

Field Definitions

The following fields are found on the Auto Update window of the Startup Wizard:

- Enable Signature and Engine Updates from Cisco.com—Lets the sensor go to Cisco.com to download signature and engine updates and install them on the sensor.

  Note You must check the **Enable Signature and Engine Updates from Cisco.com** check box to enable the fields.

- Cisco.com Access—Lets you specify the following options for the Cisco.com server:
  - Username—Specifies the username corresponding to the user account on Cisco.com.
  - Password—Specifies the password for the user account on Cisco.com.
  - Confirm Password—Confirms the password by forcing you to retype the Cisco.com password.

- Schedule—Lets you specify the daily start time:
  - Start Time—Specifies the time to start the update process in 24-hour clock time. This is the time when the sensor will contact Cisco.com and download any new updates.

Configuring Auto Update

Note Automatic update requires either an HTTP proxy server or at least one DNS server to function. Make sure that you have a server configured on Configuration > Startup Wizard > Sensor Setup (Step 2 of ...).

To configure automatic updates from Cisco.com, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Startup Wizard > Auto Update**.

Step 3 To enable signature and engine updates from Cisco.com, check the **Enable Signature and Engine Updates from Cisco.com** check box:

a. In the Username field, enter the username to use when logging in to Cisco.com. A valid value for the username is 1 to 2047 characters.

b. In the Password field, enter the username password for Cisco.com. A valid value for the password is 1 to 2047 characters.

c. In the Confirm Password field, enter the password to confirm it.

d. In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss using the 24-hour clock. The updates occur daily.

Tip To discard your changes, click **Cancel**.

Step 4 Click **Finish** to save your changes.

For More Information

- For the procedure for obtaining software and an account with cryptographic privileges, see Obtaining Cisco IPS Software, page 26-1.
- For a list of the supported FTP and HTTP servers, see Supported FTP and HTTP Servers, page 20-21.
- To configure UNIX-style directory listings for downloading automatic updates, see UNIX-Style Directory Listings, page 20-21.
- For information about the time is takes to install signature updates, see Signature Updates and Installation Time, page 20-21.

Setting Up the Sensor

This chapter provides information for setting up the sensor. It contains the following sections:

Understanding Sensor Setup

After you install the sensor on your network, you must use the **setup** command to initialize it so that you can communicate with it over the network. You cannot use the IME to configure the sensor until you initialize the sensor using the **setup** command.

With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, access control lists, global correlation servers, and time settings. You can continue using advanced setup in the CLI to enable Telnet, configure the web server, and assign and enable virtual sensors and interfaces, or you can use the Startup Wizard in the IME. After you configure the sensor with the **setup** command, you can change the network settings in the IME.

After you initialize the sensor, you can make any changes and configure other network parameters in Sensor Setup.

For More Information

You must initialize the sensor before you can choose **Configuration > *sensor_name* > Sensor Setup** in the IME to further configure the sensor. For the procedure for using the **setup** command to initialize the sensor, see Basic Sensor Setup, page 25-4.

Configuring Network Settings

This section describes how to change the network settings, and contains the following topics:

Network Pane

Note You must be administrator to configure network settings.

After you use the **setup** command to initialize the sensor, the network and communication parameter values appear in the Network pane. If you need to change these parameters, you can do so in the Network pane.

Network Pane Field Definitions

The following fields are found in the Network pane:

- Network Settings—Enables the network parameters for the sensor:
  - Hostname—Specifies the name of the sensor. The hostname can be a string of 1 to 64 characters that matches the pattern ^[A-Za-z0-9_/-]+$. The default is sensor. You receive an error message if the name contains a space or exceeds 64 alphanumeric characters.
  - IP Address—Specifies the IP address of the sensor. The default is 192.168.1.2.
  - Network Mask—Specifies the mask corresponding to the IP address. The default is 255.255.255.0.
  - Default Route—Specifies the default gateway address. The default is 192.168.1.1.
- DNS/Proxy Settings—Lets you configure either an HTTP proxy server or DNS server to support automatic update and global correlation:
  - HTTP Proxy Server—Lets you enter a proxy server IP address. You may need proxy servers to download automatic and global correlation updates if your network uses proxy.
  - HTTP Proxy Port—Lets you enter the port number for the proxy server.
  - DNS Primary—Lets you enter the primary DNS server IP address.
  - DNS Secondary—Lets you enter the secondary DNS server IP address.
  - DNS Tertiary—Lets you enter tertiary DNS server IP address. If you are using a DNS server, you must configure at least one DNS server and it must be reachable for global correlation updates to be successful. You can configure other DNS servers as backup servers. DNS queries are sent to the first server in the list. If it is unreachable, DNS queries are sent to the next configured DNS server.

Caution For automatic and global correlation updates to function, you must have either a DNS server or an HTTP proxy server configured at all times.

Caution DNS resolution is supported only for accessing the automatic and global correlation update server.

- HTTP, FTP, Telnet, SSH, CLI, & Other Options
  - Web Server Port—Specifies the TCP port used by the web server. The default is 443 for HTTPS.

    Note You receive an error message if you enter a value out of the range of 1 to 65535.

- Web Session Timeout—Lets you set the web session (HTTP/HTTPS) inactivity timeout in seconds. The valid range is 600 to 3600 seconds. The default is 3600 seconds.
- Log Web Session Timeout—Lets you log web session inactivity timeouts. The default is disabled.
- Enable TLS/SSL on HTTP—Enables TLS and SSL in the web server. The default is enabled.

  Note We strongly recommend that you enable TLS and SSL.

- FTP Timeout—Sets the amount of time in seconds that the FTP client waits before timing out when the sensor is communicating with an FTP server. The valid range is 1 to 86400 seconds. The default is 300 seconds.
- CLI Session Timeout—Sets the amount of time in minutes that the CLI waits before timing out. Setting the CLI session timeout increases the security of a CLI session. The valid range is 0 to 100,000 minutes. The default is 0, which means that it is an unlimited value and thus will never time out.
- Enable Telnet—Enables or disables Telnet for remote access to the sensor.

  Note Telnet is not a secure access service and therefore is disabled by default.

- Allow Password Recovery—Enables password recovery. The default is enabled.
- Enable SSHv1 Fallback—Enables fallback to SSHv1. The default is disabled. Enable SSHv1.

  Fallback to SSHv1 is provided in case the peer client/server does not support SSHv2. SSHv2 is the default SSH version.
- Login Banner—Lets you add a login banner. There is a 2500-character limit.

Configuring Network Settings

Caution You must have a valid sensor license for automatic signature updates and global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.

To configure network settings, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Network**.

Step 3 To edit the sensor hostname, enter the new name in the Hostname field.

Step 4 To change the sensor IP address, enter the new address in the IP Address field.

Step 5 To change the network mask, enter the new mask in the Network Mask field.

Step 6 To change the default gateway, enter the new address in the Default Route field.

Step 7 To configure either an HTTP proxy server or at least one DNS server to support automatic update and global correlation, enter the HTTP proxy server IP address in the HTTP Proxy Server field and the port number in the HTTP Proxy Port field, or enter the DNS server IP address in the DNS Primary field. If you do not want to turn on global correlation, click **OK** on the following Warning dialog box:

```
DNS or HTTP proxy is required for global correlation inspection and reputation filters,
but no DNS or proxy servers are defined. Do you want to continue?
```

If you are using a DNS server, you must configure at least one DNS server and it must be reachable for automatic and global correlation updates to be successful. You can configure other DNS servers as backup servers. DNS queries are sent to the first server in the list. If it is unreachable, DNS queries are sent to the next configured DNS server.

Caution For automatic and global correlation updates to function, you must have either a DNS server or an HTTP proxy server configured at all times.

Caution DNS resolution is supported only for accessing the automatic and global correlation update server.

Step 8 To change the web server port, enter the new port number in the Web Server Port field.

Note If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IME Use the following format: https://*sensor_ip_address*:*port_number* (for example, https://192.0.2.1:1040).

Step 9 To change the web session timeout, enter the new amount in seconds in the Web Session Timeout field. The valid range is 600 to 3600 seconds. The default is 3600 seconds.

Step 10 To turn on logging for web session inactivity timeouts, check the Log Web Session Timeout checkbox. The default is disabled.

Step 11 To enable or disable TLS/SSL, check the **Enable TLS/SSL on HTTP** check box.

Note We strongly recommend that you enable TLS/SSL.

Note TLS and SSL are protocols that enable encrypted communications between a web browser and the Web Server. When TLS/SSL is enabled, you connect to the IME using https://*sensor_ip_address*. If you disable TLS/SSL, connect to the IME using http://*sensor_ip_address*:*port_number*.

Step 12 To change FTP timeout, enter the new amount in seconds in the FTP Timeout field. The default is 300 seconds.

Step 13 To configure the CLI session timeout, enter the new amount in minutes in the CLI Session Timeout field. The valid range is 0 to 100,000 minutes. The default is 0 minutes, which means it will never time out.

Step 14 To enable or disable remote access, check the **Enable Telnet** check box.

Note Telnet is not a secure access service and therefore is disabled by default. However, SSH is always running on the sensor and it is a secure service.

Step 15 To allow password recovery, check the **Allow Password Recovery** check box.

Note We strongly recommend that you enable password recovery. Otherwise, you must reimage your sensor to gain access if you have a password problem.

Step 16 To allow fallback to SSHv1, check the Enable SSHv1 Fallback check box. The default is enabled.

You should allow fallback to SSHv1 if the peer client/server does not support SSHv2. The default SSH version is SSHv2.

Step 17 To add a login banner, enter the text in the Login Banner field. There is a 2500-character limit.

Tip To undo your changes, click **Reset**.

Step 18 Click **Apply** to apply your changes and save the revised configuration.

Note Changing the network settings may disrupt your connection to the sensor and force you to reconnect with the new address.

For More Information

- For detailed information on global correlation, see Chapter 14, "Configuring Global Correlation."
- For the procedures for recovering the password on the various sensors, see Recovering the Password, page 20-4.

Configuring Allowed Hosts/Networks

This section describes how to add allowed hosts and networks to the system, and contains the following topics:

Allowed Hosts/Networks Pane

Note You must be administrator to configure allowed hosts and networks.

After you use the **setup** command to initialize the sensor, the allowed hosts parameter values appear in the Allowed Hosts/Networks pane. If you need to change these parameters, you can do so in the Allowed Hosts/Networks pane. You use the Allowed Hosts/Networks pane to specify hosts or networks that have permission to access the sensor. By default, there are no entries in the list, and therefore no hosts are permitted until you add them.

You must add the management host, such as the ASDM, IDM, IME, and Cisco Security Manager to the allowed hosts list, otherwise they cannot communicate with the sensor.

Caution When adding, editing, or deleting allowed hosts, make sure that you do not delete the IP address used for remote management of the sensor.

Allowed Hosts/Network Pane and Add and Edit Allowed Host Dialog Boxes Field Definitions

The following fields are found in the Allowed Hosts/Networks pane and Add and Edit Allowed Host dialog boxes:

- IP Address—Specifies the IP address of the host allowed to access the sensor.
- Network Mask—Specifies the mask corresponding to the IP address of the host.

Configuring Allowed Hosts and Networks

To specify hosts and networks that have permission to access your sensor, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Allowed Hosts/Networks**, and then click **Add** to add a host or network to the list. You can add a maximum of 512 allowed hosts.

Step 3 In the IP Address field, enter the IP address of the host or network. You receive an error message if the IP address is already included as part of an existing list entry.

Step 4 In the Network Mask field, enter the network mask of the host or network, or choose a network mask from the drop-down list. the IME requires that a netmask always be provided, whether the IP address is a host or a network. If you do not specify a netmask, you receive the following error: `Network Mask is not valid`. You also receive an error message if the network mask does not match the IP address.

Tip To discard your changes and close the Add Allowed Host dialog box, click **Cancel**.

Step 5 Click **OK**. The new host or network appears in the list in the Allowed Hosts/Networks pane.

Step 6 To edit an existing entry in the list, select it, and click **Edit**.

Step 7 In the IP Address field, edit the IP address of the host or network.

Step 8 In the Network Mask field, edit the network mask of the host or network.

Tip To discard your changes and close the Edit Allowed Host dialog box, click **Cancel**.

Step 9 Click **OK**. The edited host or network appears in the list in the Allowed Hosts/Networks pane.

Step 10 To delete a host or network from the list, select it, and click **Delete**. The host no longer appears in the list in the Allowed Hosts/Networks pane.

Caution All future network connections from the host that you deleted will be denied.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring Time

This section describes time sources and the sensor, and contains the following topics:

Time Pane

Note You must be administrator to configure time settings.

Use the Time pane to configure the sensor local date, time, time zone, summertime (DST), and whether the sensor will use an NTP server for its time source.

Note We recommend that you use an NTP server as the sensor time source.

Time Pane Field Definitions

The following fields are found in the Time pane:

- Sensor Local Date—Specifies the current date on the sensor. The default is January 1, 1970. You receive an error message if the day value is out of range for the month.
- Sensor Local Time—Specifies the current time (hh:mm:ss) on the sensor. The default is 00:00:00. You receive an error message if the hours, minutes, or seconds are out of range.

  Note The date and time fields are disabled if the sensor does not support these fields, or if you have configured NTP settings on the sensor.

- Standard Time Zone—Lets you set the zone name and UTC offset:
  - Zone Name—Specifies the local time zone when summertime is not in effect. The default is UTC. You can choose from a predefined set of 37 time zones, or you can create a unique name (24 characters) in the following pattern: ^[A-Za-z0-9()+:,_/-]+$
  - UTC Offset—Specifies the local time zone offset in minutes. The default is 0. If you select a predefined time zone this field is populated automatically.

    Note Changing the time zone offset requires the sensor to reboot.

- NTP Server—Lets you configure the sensor to use an NTP server as its time source:
  - IP Address—Specifies the IP address of the NTP server if you use this to set time on the sensor.
  - Authenticated NTP—Lets you use authenticated NTP, which requires a key and key ID.
  - Key—Specifies the NTP MD5 key type.
  - Key ID—Specifies the ID of the key (1 to 65535) used to authenticate on the NTP server. You receive an error message if the key ID is out of range.
  - Unauthenticated NTP—Lets you use NTP, but does not require authentication, therefore, no key or key ID.
- Summertime—Lets you enable and configure summertime settings:
  - Enable Summertime—Click to enable summertime mode. The default is disabled.

Configure Summertime Dialog Box Field Definitions

The following fields are found in the Configure Summertime dialog box:

- Summer Zone Name—Specifies the summertime zone name. The default is UTC. You can choose from a predefined set of 37 time zones, or you can create a unique name (24 characters) in the following pattern: ^[A-Za-z0-9()+:,_/-]+$
- Offset—Specifies the number of minutes to add during summertime. The default is 60. If you choose a predefined time zone, this field is populated automatically.

  Note Changing the time zone offset requires the sensor to reboot.

- Start Time—Specifies the summertime start time setting. The value is hh:mm. You receive an error message if the hours or minutes are out of range.
- End Time—Specifies the summertime end time setting. The value is hh:mm. You receive an error message if the hours or minutes are out of range.
- Summertime Duration—Lets you set whether the duration is recurring or a single date:
  - Recurring—Specifies the duration is in recurring mode.
  - Date—Specifies the duration is in nonrecurring mode.
  - Start—Specifies the start week, day, and month setting.
  - End—Specifies the end week, day, and month setting.

Configuring Time on the Sensor

To configure time on the sensor, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Time**.

Step 3 Under Sensor Local Date, select the current date from the drop-down list. Date indicates the date on the local host.

Step 4 Under Sensor Local Time, enter the current time (hh:mm:ss). Time indicates the time on the local host. To see the current time, click **Refresh**.

Caution If you accidentally specify the incorrect time, stored events have the wrong time stamp. You must clear the events.

Note You cannot change the date or time on modules or if you have configured NTP.

Step 5 Under Standard Time Zone, configure the time zone and offset:

a. In the Zone Name field, choose a time zone from the drop-down list, or enter one that you have created. This is the time zone to be displayed when summertime hours are not in effect.

b. In the UTC Offset field, enter the offset in minutes from UTC. If you choose a predefined time zone name, this field is automatically populated.

Note Changing the time zone offset requires the sensor to reboot.

Step 6 If you are using NTP synchronization, under NTP Server enter the following:

- The IP address of the NTP server in the IP Address field.
- If using authenticated NTP, check the **Authenticated NTP** check box, and then enter the key of the NTP server in the Key field, and the key ID of the NTP server in the Key ID field.
- If using unauthenticated NTP, check the **Unauthenticated NTP** check box.

Note If you define an NTP server, the sensor time is set by the NTP server. The CLI **clock set** command produces an error, but time zone and daylight saving time parameters are valid.

Note We recommend that you use an NTP server as the sensor time source.

Step 7 To enable daylight saving time, check the **Enable Summertime** check box.

Step 8 Click **Configure Summertime**.

Step 9 Choose the Summer Zone Name from the drop-down list or enter one that you have created. This is the name to be displayed when daylight saving time is in effect.

Step 10 In the Offset field, enter the number of minutes to add during summertime. If you choose a predefined summer zone name, this field is automatically populated.

Note Changing the time zone offset requires the sensor to reboot.

Step 11 In the Start Time field, enter the time to apply summertime settings.

Step 12 In the End Time field, enter the time to remove summertime settings.

Step 13 Under Summertime Duration, choose whether summertime settings will occur on specified days each year (recurring) or whether they will start and end on specific dates (date):

a. Recurring—Choose the Start and End times from the drop-down lists. The default is the second Sunday in March and the first Sunday in November.

b. Date—Choose the Start and End time from the drop-down lists. The default is January 1 for the start and end time.

Tip To discard your changes and close the Configure Summertime dialog box, click **Cancel**.

Step 14 Click **OK**.

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

Step 15 Click **Apply** to apply your changes and save the revised configuration.

Step 16 If you changed the time and date settings (Step 3 and Step 4), you must also click **Apply Time to Sensor** to save the time and date settings on the sensor.

Time Sources and the Sensor

Note We recommend that you use an NTP server to regulate time on your sensor. You can use authenticated or unauthenticated NTP. For authenticated NTP, you must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server. You can set up NTP during initialization or you can configure NTP through the CLI, IDM, IME, or ASDM.

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings. This section provides a summary of the various ways to set the time on sensors.

The IPS Standalone Appliances

- Use the **clock set** command to set the time. This is the default.
- Configure the appliance to get its time from an NTP time synchronization source.

Note The currently supported Cisco IPS appliances are the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and 4520-XL.

The ASA IPS Modules

- The ASA 5500-X IPS SSP and ASA 5585-X IPS SSP automatically synchronize their clocks with the clock in the adaptive security appliance in which they are installed. This is the default.
- Configure them to get their time from an NTP time synchronization source, such as a Cisco router other than the parent router.

For More Information

- For more information on synchronizing IPS modules with the parent chassis, see Synchronizing IPS Module System Clocks with Parent Device System Clocks, page 6-11.
- For detailed information on configuring NTP, see Configuring NTP, page 6-13.

Synchronizing IPS Module System Clocks with Parent Device System Clocks

The ASAIPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) synchronize their clocks to the parent chassis clock (adaptive security appliance) each time the IPS boots up and any time the parent chassis clock is set. The IPS clock and parent chassis clock tend to drift apart over time. The difference can be as much as several seconds per day. To avoid this problem, make sure that both the IPS clock and the parent clock are synchronized to an external NTP server. If only the IPS clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs.

Verifying the Sensor is Synchronized with the NTP Server

In the Cisco IPS, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the **show statistics host** command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.

To verify the NTP configuration, follow these steps:

Step 1 Log in to the sensor.

Step 2 Generate the host statistics.

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
          2 10373  9014   yes   yes  none    reject   reachable  1
        status = Not Synchronized
     ...
```

Step 3 Generate the hosts statistics again after a few minutes.

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
        *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
         LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f624   yes   yes   ok   sys.peer   reachable  2
          2 10373  9024   yes   yes  none    reject   reachable  2
        status = Synchronized
```

Step 4 If the status continues to read `Not Synchronized`, check with the NTP server administrator to make sure the NTP server is configured correctly.

Correcting Time on the Sensor

If you set the time incorrectly, your stored events will have the incorrect time because they are stamped with the time the event was created. The Event Store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command.

Note You cannot remove individual events.

For More Information

For the procedure for clearing events from Event Store, see Clearing Events, page 6-16.

Configuring NTP

This section describes how to configure a Cisco router to be an NTP server and how to configure the sensor to use an NTP server as its time source. It contains the following topics:

Configuring a Cisco Router to be an NTP Server

The sensor requires an authenticated connection with an NTP server if it is going to use the NTP server as its time source. The sensor supports only the MD5 hash algorithm for key encryption. Use the following procedure to activate a Cisco router to act as an NTP server and use its internal clock as the time source.

Caution The sensor NTP capability is designed to be compatible with Cisco routers acting as NTP servers. The sensor may work with other NTP servers, but is not tested or supported.

Note Remember the NTP server key ID and key values. You need them along with the NTP server IP address when you configure the sensor to use the NTP server as its time source.

To set up a Cisco router to act as an NTP server, follow these steps:

Step 1 Log in to the router.

Step 2 Enter configuration mode.

```
router# configure terminal
```

Step 3 Create the key ID and key value. The key ID can be a number between 1 and 65535. The key value is text (numeric or character). It is encrypted later.

```
router(config)# ntp authentication-key key_ID md5 key_value
```

Example

```
router(config)# ntp authentication-key 100 md5 attack
```

Note The sensor only supports MD5 keys.

Note Keys may already exist on the router. Use the **show running configuration** command to check for other keys. You can use those values for the trusted key in Step 4.

Step 4 Designate the key you just created in Step 3 as the trusted key (or use an existing key). The trusted key ID is the same number as the key ID in Step 3.

```
router(config)# ntp trusted-key key_ID
```

Example

```
router(config)# ntp trusted-key 100
```

Step 5 Specify the interface on the router with which the sensor will communicate.

```
router(config)# ntp source interface_name
```

Example

```
router(config)# ntp source FastEthernet 1/0
```

Step 6 Specify the NTP master stratum number to be assigned to the sensor. The NTP master stratum number identifies the relative position of the server in the NTP hierarchy. You can choose a number between 1 and 15. It is not important to the sensor which number you choose.

```
router(config)# ntp master stratum_number
```

Example

```
router(config)# ntp master 6
```

Configuring the Sensor to Use an NTP Time Source

The sensor requires a consistent time source. We recommend that you use an NTP server. Use the following procedure to configure the sensor to use the NTP server as its time source. You can use authenticated or unauthenticated NTP.

Note For authenticated NTP, you must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server.

Caution The sensor NTP capability is designed to be compatible with Cisco routers acting as NTP servers. The sensor may work with other NTP servers, but is not tested or supported.

To configure the sensor to use an NTP server as its time source, follow these steps:

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

Step 2 Enter configuration mode.

```
sensor# configure terminal
```

Step 3 Enter service host mode.

```
sensor(config)# service host
```

Step 4 Configure unauthenticated NTP:

a. Enter NTP configuration mode.

```
sensor(config-hos)# ntp-option enabled-ntp-unauthenticated
```

b. Specify the NTP server IP address.

```
sensor(config-hos-ena)# ntp-server ip_address
```

c. Verify the unauthenticated NTP settings.

```
sensor(config-hos-ena)# show settings
   enabled-ntp-unauthenticated
   ----------------------------------------------
      ntp-server: 10.89.147.45
   ----------------------------------------------
sensor(config-hos-ena)#
```

Step 5 Configure authenticated NTP:

a. Enter NTP configuration mode.

```
sensor(config-hos)# ntp-option enable
```

b. Specify the NTP server IP address and key ID. The key ID is a number between 1 and 65535. This is the key ID that you already set up on the NTP server.

```
sensor(config-hos-ena)# ntp-servers ip_address key-id key_ID
```

Example

```
sensor(config-hos-ena)# ntp-servers 10.16.0.0 key-id 100
```

c. Specify the key value NTP server. The key value is text (numeric or character). This is the key value that you already set up on the NTP server.

```
sensor(config-hos-ena)# ntp-keys key_ID md5-key key_value
```

Example

```
sensor(config-hos-ena)# ntp-keys 100 md5-key attack
```

d. Verify the NTP settings.

```
sensor(config-hos-ena)# show settings
   enabled
   ----------------------------------------------
      ntp-keys (min: 1, max: 1, current: 1)
      ---------------------------------------------
         key-id: 100
         ---------------------------------------------
            md5-key: attack
         ---------------------------------------------
      ---------------------------------------------
      ntp-servers (min: 1, max: 1, current: 1)
      ---------------------------------------------
         ip-address: 10.16.0.0
         key-id: 100
      ---------------------------------------------
----------------------------------------------
sensor(config-hos-ena)#
```

Step 6 Exit NTP configuration mode.

```
sensor(config-hos-ena)# exit
```

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

Step 7 Press **Enter** to apply the changes or enter **no** to discard them.

Manually Setting the System Clock

Note You do not need to set the system clock if your sensor is synchronized by a valid outside timing mechanism such as an NTP clock source.

Use the **clock set** *hh:mm [:ss] month day year* command to manually set the clock on the appliance. Use this command if no other time sources are available. The **clock set** command does not apply to the following platforms, because they get their time from the adaptive security appliance in which they are installed:

- ASA 5500-X IPS SSP
- ASA 5585-X IPS SSP

To manually set the clock on the appliance, follow these steps:

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

Step 2 Set the clock manually.

```
sensor# clock set 13:21 Mar 29 2011
```

Note The time format is 24-hour time.

Clearing Events

Use the **clear events** command to clear the Event Store.

To clear events from the Event Store, follow these steps:

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

Step 2 Clear the Event Store.

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

Step 3 Enter **yes** to clear the events.

Configuring Authentication

This section describes how to add and remove users on the system and configure AAA RADIUS authentication. It contains the following topics:

Understanding User Roles

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

There are four user roles:

- Viewer—Can view configuration and events, but cannot modify any configuration data except their user passwords.
- Operator—Can view everything and can modify the following options:
  - Signature tuning (priority, disable or enable)
  - Virtual sensor definition
  - Managed routers
  - Their user passwords
- Administrator—Can view everything and can modify all options that operators can modify in addition to the following:
  - Sensor addressing configuration
  - List of hosts allowed to connect as configuration or viewing agents
  - Assignment of physical sensing interfaces
  - Enable or disable control of physical interfaces
  - Add and delete users and passwords
  - Generate new SSH host keys and server certificates

- Service—Only one user with service privileges can exist on a sensor. The service user cannot log in to the IME. The service user logs in to a bash shell rather than the CLI.

  The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed. You should only create an account with the service role for troubleshooting purposes. Only a user with administrator privileges can edit the service account.

  When you log in to the service account, you receive the following warning:

```
************************ WARNING ***********************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
********************************************************************************
```

Note For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.

Understanding the Service Account

You can create a service account for TAC to use during troubleshooting. Although more than one user can have access to the sensor, only one user can have service privileges on a sensor. The service account is for support purposes only.

The root user password is synchronized to the service account password when the service account is created. To gain root access you must log in with the service account and switch to user root with the **su - root** command.

Caution Do not make modifications to the sensor through the service account except under the direction of TAC. If you use the service account to configure the sensor, your configuration is not supported by TAC. Adding services to the operating system through the service account affects proper performance and functioning of the other IPS services. TAC does not support a sensor on which additional services have been added.

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

Note For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.

The Service Account and RADIUS Authentication

If you are using RADIUS authentication and want to create and use a service account, you must create the service account both on your sensor and on the RADIUS server. You must use local authentication to access the service account on the sensor. The service account must be created manually as a local account on the sensor. Then when you configure RADIUS authentication, the service account must also be configured manually on the RADIUS server with the accept message set to ip-role=service.

When you log in to the service account, you are authenticated against both the sensor account and the RADIUS server account. By whatever method you use to access the service account—serial console port, direct monitor/keyboard (for sensors that support it), or a network connection, such as SSH or Telnet—you have to log in using local authentication.

For More Information

For detailed information about the service account, see Understanding the Service Account, page 6-18.

RADIUS Authentication Functionality and Limitations

The current AAA RADIUS implementation has the following functionality and limitations:

- Authentication with a RADIUS server—However, you cannot change the password of the RADIUS server from the IPS.
- Authorization—You can perform role-based authorization by specifying the IPS role of the user on the RADIUS server.
- Accounting—The login attempts of the user and the configuration changes are logged as events locally on the IPS. However, these account messages are not communicated to the RADIUS server.

Authentication Pane

Note You must be administrator to configure authentication.

Caution Make sure you have a RADIUS server already configured before you configure RADIUS authentication on the sensor. IPS has been tested with CiscoSecure ACS 4.2 and 5.1 servers. Refer to your RADIUS server documentation for information on how to set up a RADIUS server.

Use the Authentication pane to configure users who can log in to the sensor. Multiple users are permitted to log in at a time. You can create and remove users from the local sensor. You can only modify one user account at a time. Each user is associated with a role that controls what that user can and cannot modify. The requirements that must be used for user passwords are set in the Passwords pane.

Users are authenticated through AAA either locally or through RADIUS servers. Local authentication is enabled by default. You must configure RADIUS authentication before it is active.

You must specify the user role that is authenticated through RADIUS either by configuring the user role on the RADIUS server or specifying a default user role on the Authentication pane. The username and password are sent in an authentication request to the configured RADIUS server. The response of the server determines whether the login is authenticated.

Note If the sensor is not configured to use a default user role and the sensor user role information in not in the Accept Message of the CiscoSecure ACS server, the sensor rejects RADIUS authentication even if the CiscoSecure ACS server accepts the username and password.

You can configure a primary RADIUS server and a secondary RADIUS server. The secondary RADIUS server authenticates and authorizes users if the primary RADIUS server is unresponsive.

You can also configure the sensor to use local authentication (local fallback) if no RADIUS servers are responding. In this case, the sensor authenticates against the locally configured user accounts. The sensor will only use local authentication if the RADIUS servers are not available, not if the RADIUS server rejects the authentication requests of the user. You can also configure how users connected through the console port are authenticated—through local user accounts, through RADIUS first and if that fails through local user accounts, or through RADIUS alone.

To configure a RADIUS server on the Authentication pane, you must have the IP address, port, and shared secret of the RADIUS server. You must also either have the NAS-ID of the RADIUS server, or have the RADIUS server configured to authenticate clients without a NAS-ID or with the default IPS NAS-ID of cisco-ips.

Authentication Pane Field Definitions

The following fields are found in the Authentication pane:

- User Authentication—Lets you choose either local authentication or authentication using a RADIUS server.
- Local Authentication—Lets you specify the users that have access to this sensor:
  - Username—Specifies the username, which follows the pattern ^[A-Za-z0-9()+:,_/-]+$, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and _, and can contain 1 to 64 characters.
  - Role—Specifies the user role. The values are Administrator, Operator, Service, and Viewer. The default is Viewer.

    Note Only one user with the role of service is allowed.

  - Status—Displays the current user account status, such as active, expired, or locked.
- RADIUS Authentication—Lets you specify RADIUS as the method of authentication:
  - Network Access ID—Identifies the service requesting authentication. The value can be no NAS-ID, cisco-ips, or a NAS-ID already configured on the RADIUS server. The default is cisco-ips.
  - Default User Role—Lets you assign a default user role on the sensor that is only applied when there is NOT a Cisco av pair specifying the user role. The default role values are Administrator, Operator, Viewer, and Unspecified. Service role cannot be the default user role. The default is Unspecified.

Note If you do not want to configure a default user role on the sensor that is applied in the absence of a Cisco av pair, you need to configure the Cisco IOS/PIX 6.x RADIUS Attributes [009\001] cisco-av-pair under the group or user profile with one of the following options: ips-role=administrator, ips-role=operator, ips-role=viewer, ips-role=service, or ips-role=unspecified.

Note If the sensor is not configured to use a default user role and the sensor user role information in not in the Accept Message of the CiscoSecure ACS server, the sensor rejects RADIUS authentication even if the CiscoSecure ACS server accepts the username and password.

Note The default user role is used only when the user has not been configured with a specific role on the ACS server. Local users are always configured with a specific role so the default user role will never apply to locally authenticated users.

Caution Do not add multiple Cisco av-pairs with the same key or you cannot log in. You must have only one instance of ips-role=value. For example, do not use the following configuration:
ips-role= administer
ips-role=ad

  - Allow Local Authentication if all RADIUS Servers are Unresponsive—If checked, lets you default to local authentication if the RADIUS servers are not responding. The default is enabled.

- Primary RADIUS Server—Lets you configure the main RADIUS server:
  - Server IP Address—Specifies the IP address of the RADIUS server.
  - Authentication Port—Specifies the port of the RADIUS server. If not specified, the default RADIUS port is used.
  - Timeout (seconds)—Specifies the number of seconds the sensor waits for a response from a RADIUS server before it considers the server to be unresponsive.
  - Shared Secret—Specifies the secret value configured on the RADIUS server. You must obtain the secret value of the RADIUS server and enter it in the Shared Secret field.

    Note You must have the same secret value configured on both the RADIUS server and the IPS sensor so that the server can authenticate the requests of the client and the client can authenticate the responses of the server.

- Secondary RADIUS Server (optional)—Lets you configure a secondary RADIUS server:
  - Enable a Secondary RADIUS Server—Lets you configure a backup RADIUS server.
  - Server IP Address—Specifies the IP address of the RADIUS server.
  - Authentication Port—Specifies the port of the RADIUS server. If not specified, the default RADIUS port is used.
  - Timeout (seconds)—Specifies the number of seconds the sensor waits for a response from a RADIUS server before it considers the server to be unresponsive.

- Shared Secret—Specifies the secret value configured on the RADIUS server. You must obtain the secret value of the RADIUS server and enter it in the Shared Secret field.

  Note You must have the same secret value configured on both the RADIUS server and the IPS sensor so that the server can authenticate the requests of the client and the client can authenticate the responses of the server.

- Console Authentication—Lets you choose how users connected through the console port are authenticated:

  Note Login sessions created with the ASA **session** command are authenticated as console logins.

  - Local—Indicates that the users connected through the console port are authenticated through local user accounts.
  - RADIUS and Local—Indicates that the users connected through the console port are authenticated through RADIUS first. If RADIUS fails, local authentication is attempted. This is the default.
  - RADIUS—Indicates that the users connected through the console port are authenticated by RADIUS. If you also have Allow Local Authentication if all Radius Servers are Unresponsive enabled, users can also be authenticated through the local user accounts.

Add and Edit User Dialog Boxes Field Definitions

Note You must be administrator to add and edit users.

The following fields found in the Add and Edit User dialog boxes:

- Username—Specifies the username, which follows the pattern ^[A-Za-z0-9()+:,_/-]+$, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and _, and can contain 1 to 64 characters.
- User Role—Specifies the user role. The values are Administrator, Operator, Service, and Viewer. The default is Viewer.

  Note Only one user with the role of service is allowed.

- Password—Specifies the user password, which d must conform to the requirements set by the sensor administrator in the Passwords pane.
- Confirm Password—Lets you confirm the password. You receive an error message if the confirm password does not match the user password.
- Change the password to access the sensor—Lets you change the password of the user. Only available in the Edit dialog box.

Adding, Editing, Deleting Users, and Creating Accounts

To configure users on the sensor, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Authentication**.

Step 3 Next to User Authentication, click the **Local** or **RADIUS Server** radio button to choose the type of user authentication.

Step 4 To configure local authentication, click **Add**.

Step 5 In the Username field, enter the username of the user you are adding.

Step 6 From the User Role drop-down list, choose one of the following user roles:

- Administrator
- Operator
- Viewer
- Service

Note Only one user with the role of service is allowed.

Step 7 In the Password field, enter the new password for that user.

Step 8 In the Confirm Password field, enter the new password for that user.

Tip To discard your changes and close the Add User dialog box, click **Cancel**.

Step 9 Click **OK**. The new user appears in the users list in the Authentication pane.

Step 10 To edit a user, select the user in the users list, and click **Edit**.

Step 11 Make any changes you need to in the Username, User Role, and Password fields.

Tip To discard your changes and close the Edit User dialog box, click **Cancel**.

Step 12 Click **OK**. The edited user appears in the users list in the Authentication pane.

Step 13 To delete a user from the user list, select the user, and click **Delete**. That user is no longer in the users list in the Authentication pane.

Step 14 To configure RADIUS authentication:

a. In the Network Access ID field, enter the NAS-ID. The NAS-ID is an identifier that clients send to servers to communicate the type of service they are attempting to authenticate. The value can be no NAS-ID, cisco-ips, or a NAS-ID already configured on the RADIUS server. The default is cisco-ips.

b. (Optional) Configure a default user role if you are not configuring a Cisco av pair. From the Default User Role drop-down menu, choose the user role for this user. This assigns a default user role on the sensor that is only applied when there is NOT a Cisco av pair specifying the user role. The values are Administrator, Operator, Viewer, or Unspecified. The default is Unspecified.

Note The default user role is used only when the user has not been configured with a specific role on the ACS server. Local users are always configured with a specific role so the default user role will never apply to locally authenticated users.

Note Service cannot be the default role.

c. Configure a Cisco av pair. If you do not want to configure a default user role on the sensor that is applied in the absence of a Cisco av pair, you need to configure the Cisco IOS/PIX 6.x RADIUS Attributes [009\001] cisco-av-pair under the group or user profile with one of the following options:
   - ips-role=viewer
   - ips-role=operator
   - ips-role=administrator
   - ips-role=service
   - ips-role=unspecified

   Note If the sensor is not configured to use a default user role and the sensor user role information in not in the Accept Message of the CiscoSecure ACS server, the sensor rejects RADIUS authentication even if the CiscoSecure ACS server accepts the username and password.

Caution Do not add multiple Cisco av-pairs with the same key or you cannot log in. You must have only one instance of ips-role=value. For example, do not use the following configuration:
ips-role= administer
ips-role=ad

d. If you want to switch over to local authentication if the RADIUS server becomes unresponsive, check the **Allow Local Authentication if all RADIUS Servers are Unresponsive** check box.
e. In the Server IP Address field, enter the RADIUS server IP address.
f. In the Authentication port field, enter the RADIUS server port.
g. In the Timeout (seconds) field, enter the amount of time in seconds you want to wait for the RADIUS server to respond.
h. In the Shared Secret field, enter the secret value that you obtained from the RADIUS server. The shared secret is a piece of data known only to the parties involved in a secure communication.

   Note You must have the same secret value configured on both the RADIUS server and the IPS sensor so that the server can authenticate the requests of the client and the client can authenticate the responses of the server.

i. (Optional) To enable a secondary RADIUS server to perform authentication in case the primary RADIUS server is not responsive, check the **Enable a Secondary RADIUS Server** check box.
j. In the Server IP Address field, enter the IP address of the second RADIUS server.

k. In the Authentication Port field, enter the RADIUS server port.

l. In the Timeout (seconds) field, enter the amount of time in seconds you want to wait for the RADIUS server to respond.

m. In the Shared Secret field, enter the secret value you obtained for this RADIUS server.

n. From the Console Authentication drop-down list, choose the type of console authentication. You can choose Local, RADIUS and Local, or RADIUS.

Note Login sessions created with the ASA **session** command are authenticated as console logins.

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

Step 15 Click **Apply** to apply your changes and save the revised configuration.

Locking User Accounts

Note When you configure account locking, local authentication, as well as RADIUS authentication, is affected. After a specified number of failed attempts to log in locally or in to a RADIUS account, the account is locked locally on the sensor. For local accounts, you can reset the password or use the **unlock user** *username* command to unlock the account. For RADIUS user accounts, you must use the **unlock user** *username* command to unlock the account.

Note For RADIUS users, the attempt limit feature is enforced only after the RADIUS user's first successful login to the sensor.

Use the **attemptLimit** *number* command in authentication submode to lock accounts so that users cannot keep trying to log in after a certain number of failed attempts. The default is 0, which indicates unlimited authentication attempts. For security purposes, you should change this number.

To configure account locking, follow these steps:

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

Step 2 Enter service authentication submode.

```
sensor# configure terminal
sensor(config)# service authentication
```

Step 3 Set the number of attempts users will have to log in to accounts.

```
sensor(config-aut)# attemptLimit 3
```

Step 4 Check your new setting.

```
sensor(config-aut)# show settings
    attemptLimit: 3 defaulted: 0
sensor(config-aut)#
```

Step 5 Set the value back to the system default setting.

```
sensor(config-aut)# default attemptLimit
```

Step 6 Check that the setting has returned to the default.

```
sensor(config-aut)# show settings
    attemptLimit: 0 <defaulted>
sensor(config-aut)#
```

Step 7 Check to see if any users have locked accounts. The account of the user `jsmith` is locked as indicated by the parentheses.

Note When you apply a configuration that contains a non-zero value for attemptLimit, a change is made in the SSH server that may subsequently impact your ability to connect with the sensor. When attemptLimit is non-zero, the SSH server requires the client to support challenge-response authentication. If you experience problems after your SSH client connects but before it prompts for a password, you need to enable challenge-response authentication. Refer to the documentation for your SSH client for instructions.

```
sensor(config-aut)# exit
sensor(config)# exit
sensor# show users all
    CLI ID   User       Privilege
*   1349     cisco      administrator
    5824     (jsmith)   viewer
    9802     tester     operator
```

Step 8 To unlock the account of jsmith, reset the password.

```
sensor# configure terminal
sensor(config)# password jsmith
Enter New Login Password: ******
Re-enter New Login Password: ******
```

For More Information

For the procedure for unlocking user accounts, seeUnlocking User Accounts, page 6-26.

Unlocking User Accounts

Use the **unlock user** *username* command in global configuration mode to unlock local and RADIUS accounts for users who have been locked out after a specified number of failed attempts.

To configure account unlocking, follow these steps:

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

Step 2 Check to see if any users have locked accounts. The account of the user jsmith is locked as indicated by the parentheses.

```
sensor# show users all
    CLI ID   User       Privilege
*   1349     cisco      administrator
    5824     (jsmith)   viewer
    9802     tester     operator
```

Step 3 Enter global configuration mode.

```
sensor# configure terminal
sensor(config)#
```

Step 4 Unlock the account.

```
sensor(config)# unlock user jsmith
```

Step 5 Check your new setting. The account of the user jsmith is now unlocked as indicated by the lack of parenthesis.

```
sensor# show users all
    CLI ID   User       Privilege
*   1349     cisco      administrator
    5824     jsmith     viewer
    9802     tester     operator
```

Configuring Interfaces

This chapter describes the various interface modes and how to configure interfaces on the sensor. It contains the following sections:

Sensor Interfaces

This section describes the sensor interfaces, and contains the following topics:

Understanding Interfaces

The sensor interfaces are named according to the maximum speed and physical location of the interface. The physical location consists of a port number and a slot number. All interfaces that are built-in on the sensor motherboard are in slot 0, and the interface card expansion slots are numbered beginning with

slot 1 for the bottom slot with the slot numbers increasing from bottom to top. Each physical interface can be divided in to VLAN group subinterfaces, each of which consists of a group of VLANs on that interface.

There are three interface roles:

- Command and control
- Sensing
- Alternate TCP reset

There are restrictions on which roles you can assign to specific interfaces and some interfaces have multiple roles. You can configure any sensing interface to any other sensing interface as its TCP reset interface. The TCP reset interface can also serve as an IDS (promiscuous) sensing interface at the same time. The following restrictions apply:

- The TCP reset interface that is assigned to a sensing interface has no effect in inline interface or inline VLAN pair mode, because TCP resets are always sent on the sensing interfaces in those modes.
- There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.
- On the IPS 4500 series, no interface-related configurations are allowed when the SensorApp is down.

Command and Control Interface

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. The command and control interface is permanently enabled. It is permanently mapped to a specific physical interface, which depends on the specific model of sensor. You cannot use the command and control interface as either a sensing or alternate TCP reset interface.

Table 7-1 lists the command and control interfaces for each sensor.

Table 7-1 Command and Control Interfaces

Sensor	Command and Control Interface
ASA 5512-X IPS SSP	Management 0/0
ASA 5515-X IPS SSP	Management 0/0
ASA 5525-X IPS SSP	Management 0/0
ASA 5545-X IPS SSP	Management 0/0
ASA 5555-X IPS SSP	Management 0/0
ASA 5585-X IPS SSP-10	Management 0/0
ASA 5585-X IPS SSP-20	Management 0/0
ASA 5585-X IPS SSP-40	Management 0/0
ASA 5585-X IPS SSP-60	Management 0/0
IPS 4345	Management 0/0
IPS 4345-DC	Management 0/0
IPS 4360	Management 0/0

Table 7-1 Command and Control Interfaces (continued)

Sensor	Command and Control Interface
IPS 4510	Management 0/0[1]
IPS 4520	Management 0/0[1]
IPS 4520-XL	Management 0/0[1]

1. The 4500 series sensors have two management ports, Management 0/0 and Management 0/1, but Management 0/1 is reserved for future use.

Sensing Interfaces

Sensing interfaces are used by the sensor to analyze traffic for security violations. A sensor has one or more sensing interfaces depending on the sensor. Sensing interfaces can operate individually in promiscuous mode or you can pair them to create inline interfaces.

Note On appliances, all sensing interfaces are disabled by default. You must enable them to use them. On modules, the sensing interfaces are permanently enabled.

Some appliances support optional interface cards that add sensing interfaces to the sensor. You must insert or remove these optional cards while the sensor is powered off. The sensor detects the addition or removal of a supported interface card. If you remove an optional interface card, some of the interface configuration is deleted, such as the speed, duplex, description string, enabled/disabled state of the interface, and any inline interface pairings. These settings are restored to their default settings when the card is reinstalled. However, the assignment of promiscuous and inline interfaces to the Analysis Engine is not deleted from the Analysis Engine configuration, but is ignored until those cards are reinserted and you create the inline interface pairs again.

For More Information

- For the number and type of sensing interfaces available for each sensor, see Interface Support, page 7-4.
- For more information on interfaces modes, see Understanding Interface Modes, page 7-10.
- For the procedure for configuring virtual sensors, see Adding, Editing, and Deleting Virtual Sensors, page 8-12.

Interface Support

Table 7-2 describes the interface support for appliances and modules running Cisco IPS.

Table 7-2 Interface Support

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
ASA 5512-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5515-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5525-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5545-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5555-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5585-X IPS SSP-10	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5585-X IPS SSP-20	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5585-X IPS SSP-40	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5585-X IPS SSP-60	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
IPS 4345	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 Gigabitethernet 0/6 GigabitEthernet 0/7	All sensing ports can be paired together	Management 0/0

Table 7-2 Interface Support (continued)

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IPS 4345-DC	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 Gigabitethernet 0/6 GigabitEthernet 0/7	All sensing ports can be paired together	Management 0/0
IPS 4360	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 GigabitEthernet 0/6 GigabitEthernet 0/7	All sensing ports can be paired together	Management 0/0
IPS 4510	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 TenGigabitEthernet 0/6 TenGigabitEthernet 0/7 TenGigabitEthernet 0/8 TenGigabitEthernet 0/9	All sensing ports can be paired together	Management 0/0 Management 0/1[1]

Table 7-2 Interface Support (continued)

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IPS 4520	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 TenGigabitEthernet 0/6 TenGigabitEthernet 0/7 TenGigabitEthernet 0/8 TenGigabitEthernet 0/9	All sensing ports can be paired together	Management 0/0 Management 0/1[1]
IPS 4520-XL	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 TenGigabitEthernet 0/6 TenGigabitEthernet 0/7 TenGigabitEthernet 0/8 TenGigabitEthernet 0/9	All sensing ports can be paired together	Management 0/0 Management 0/1[1]

1. Reserved for future use.

TCP Reset Interfaces

This section explains the TCP reset interfaces and when to use them. It contains the following topics:

- Understanding Alternate TCP Reset Interfaces, page 7-6
- Designating the Alternate TCP Reset Interface, page 7-7

Understanding 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. In some installations when the interface is operating in promiscuous mode, the sensor may not be able to send the TCP reset packets over the same sensing interface on which the attack was detected. In such cases, you can associate the sensing interface with

an alternate TCP reset interface and any TCP resets that would otherwise be sent on the sensing interface when it is operating in promiscuous mode are instead sent out on the associated alternate TCP reset interface.

If a sensing interface is associated with an alternate TCP reset interface, that association applies when the sensor is configured for promiscuous mode but is ignored when the sensing interface is configured for inline mode. any sensing interface can serve as the alternate TCP reset interface for another sensing interface.

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

Table 7-3 lists the alternate TCP reset interfaces.

Table 7-3 Alternate TCP Reset Interfaces

Sensor	Alternate TCP Reset Interface
ASA 5512-X IPS SSP	None
ASA 5515-X IPS SSP	None
ASA 5525-X IPS SSP	None
ASA 5545-X IPS SSP	None
ASA 5555-X IPS SSP	None
ASA 5585-X IPS SSP-10	None
ASA 5585-X IPS SSP-20	None
ASA 5585-X IPS SSP-40	None
ASA 5585-X IPS SSP-60	None
IPS 4345	Any sensing interface
IPS 4345-DC	Any sensing interface
IPS 4360	Any sensing interface
IPS 4510	Any sensing interface
IPS 4520	Any sensing interface
IPS 4520-XL	Any sensing interface

Designating the Alternate TCP Reset Interface

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

You need to designate an alternate TCP reset interface in the following situations:

- When a switch is being monitored with either SPAN or VACL capture and the switch does not accept incoming packets on the SPAN or VACL capture port.
- When a switch is being monitored with either SPAN or VACL capture for multiple VLANs, and the switch does not accept incoming packets with 802.1q headers. The TCP resets need 802.1q headers to tell which VLAN the resets should be sent on.

- When a network tap is used for monitoring a connection. Taps do not permit incoming traffic from the sensor.

Caution You can only assign a sensing interface as an alternate TCP reset interface. You cannot configure the management interface as an alternate TCP reset interface.

Interface Configuration Restrictions

The following restrictions apply to configuring interfaces on the sensor:

- General
  - For IPS standalone appliances with 1 G and 10 G fixed or add-on interfaces, the maximum jumbo frame size is 9216 bytes. For integrated IPS sensors, such as the ASA 5500-X and ASA 5585-X series, refer to the following URL for information:

    http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/interface_start.html#wp1328869

    Note A jumbo frame is an Ethernet packet that is larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS).

  - On the IPS 4500 series, no interface-related configurations are allowed when the SensorApp is down.
- Physical Interfaces
  - On the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) all backplane interfaces have fixed speed, duplex, and state settings. These settings are protected in the default configuration on all backplane interfaces.
  - For nonbackplane FastEthernet interfaces the valid speed settings are 10 Mbps, 100 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit copper interfaces (1000-TX on the IPS 4345, IPS 4360, IPS 4510, and IPS 4520), valid speed settings are 10 Mbps, 100 Mbps, 1000 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit (copper or fiber) interfaces, if the speed is configured for 1000 Mbps, the only valid duplex setting is auto.
  - The command and control interface cannot also serve as a sensing interface.
- Inline Interface Pairs
  - Inline interface pairs can contain any combination of sensing interfaces regardless of the physical interface type (copper versus fiber), speed, or duplex settings of the interface. However, pairing interfaces of different media type, speeds, and duplex settings may not be fully tested or supported.
  - The command and control interface cannot be a member of an inline interface pair.
  - You cannot pair a physical interface with itself in an inline interface pair.
  - A physical interface can be a member of only one inline interface pair.
  - You can only configure bypass mode and create inline interface pairs on sensor platforms that support inline mode.

  - A physical interface cannot be a member of an inline interface pair unless the subinterface mode of the physical interface is **none**.
  - You can configure the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) to operate inline even though they have only one sensing interface.
- Inline VLAN Pairs
  - You cannot pair a VLAN with itself.
  - You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.
  - For a given sensing interface, a VLAN can be a member of only one inline VLAN pair. However, a given VLAN can be a member of an inline VLAN pair on more than one sensing interface.
  - The order in which you specify the VLANs in an inline VLAN pair is not significant.
  - A sensing interface in Inline VLAN Pair mode can have from 1 to 255 inline VLAN pairs.
  - The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support inline VLAN pairs.
  - For the IPS 4510 and IPS 4520, the maximum number of inline VLAN pairs you can create system wide is 150. On all other platforms, the limit is 255 per interface.
- Alternate TCP Reset Interface
  - You can only assign the alternate TCP reset interface to a sensing interface. You cannot configure the command and control interface as an alternate TCP reset interface. The alternate TCP reset interface option is set to **none** as the default and is protected for all interfaces except the sensing interfaces.
  - You can assign the same physical interface as an alternate TCP reset interface for multiple sensing interfaces.
  - A physical interface can serve as both a sensing interface and an alternate TCP reset interface.
  - The command and control interface cannot serve as the alternate TCP reset interface for a sensing interface.
  - A sensing interface cannot serve as its own alternate TCP reset interface.
  - You can only configure interfaces that are capable of TCP resets as alternate TCP reset interfaces.
  - There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.
- VLAN Groups
  - You can configure any single interface for promiscuous, inline interface pair, or inline VLAN pair mode, but no combination of these modes is allowed.
  - You cannot add a VLAN to more than one group on each interface.
  - You cannot add a VLAN group to multiple virtual sensors.
  - An interface can have no more than 255 user-defined VLAN groups.
  - When you pair a physical interface, you cannot subdivide it; you can subdivide the pair.
  - You can use a VLAN on multiple interfaces; however, you receive a warning for this configuration.
  - You can assign a virtual sensor to any combination of one or more physical interfaces and inline VLAN pairs, subdivided or not.

- You can subdivide both physical and logical interfaces into VLAN groups.
- The CLI, IDM, and IME prompt you to remove any dangling references. You can leave the dangling references and continue editing the configuration.
- The CLI, IDM, and IME do not allow configuration changes in Analysis Engine that conflict with the interface configuration.
- The CLI allows configuration changes in the interface configuration that cause conflicts in the Analysis Engine configuration. The IDM and IME do *not* allow changes in the interface configuration that cause conflicts in the Analysis Engine configuration.
- The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support VLAN groups mode.

For More Information

For more information on interface pair combinations, see Interface Support, page 7-4.

Understanding Interface Modes

This section explains the various interface modes, and contains the following topics:

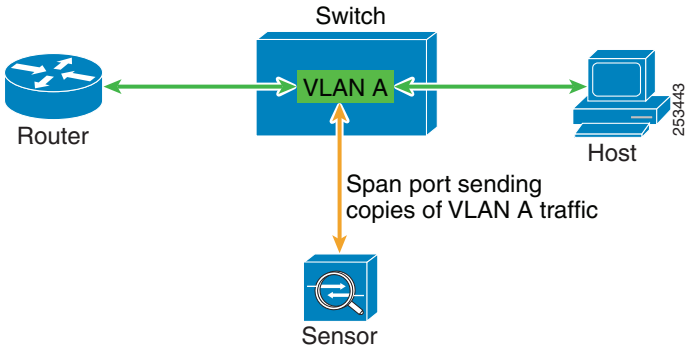
Promiscuous Mode

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. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).

By default, all sensing interfaces are in promiscuous mode. To change an interface from inline interface mode to promiscuous mode, delete any inline interface that contains that interface and delete any inline VLAN pair subinterfaces of that interface from the interface configuration.

Figure 7-1 illustrates promiscuous mode:

Figure 7-1 Promiscuous Mode



IPv6, Switches, and Lack of VACL Capture

VACLs on Catalyst switches do not have IPv6 support. The most common method for copying traffic to a sensor configured in promiscuous mode is to use VACL capture. If you want to have IPv6 support, you can use SPAN ports.

However, you can only configure up to two monitor sessions on a switch unless you use the following configuration:

- Monitor session
- Multiple trunks to one or more sensors
- Restrict per trunk port which VLANs are allowed to perform monitoring of many VLANs to more than two different sensors or virtual sensors within one IPS

The following configuration uses one SPAN session to send all of the traffic on any of the specified VLANs to all of the specified ports. Each port configuration only allows a particular VLAN or VLANs to pass. Thus you can send data from different VLANs to different sensors or virtual sensors all with one SPAN configuration line:

```
clear trunk 4/1-4 1-4094
set trunk 4/1 on dot1q 930
set trunk 4/2 on dot1q 932
set trunk 4/3 on dot1q 960
set trunk 4/4 on dot1q 962
set span 930, 932, 960, 962 4/1-4 both
```

Note The SPAN/Monitor configuration is valuable when you want to assign different IPS policies per VLAN or when you have more bandwidth to monitor than one interface can handle.

For More Information

- For more information on promiscuous mode, see Promiscuous Mode, page 7-10.
- For more information on configuring SPAN/monitor on switches, refer to the following sections in *Catalyst 6500 Series Software Configuration Guide, 8.7*:
  - Configuring SPAN, RSPAN and the Mini Protocol Analyzer

- Configuring SPAN on the Switch
- Configuring Ethernet VLAN Trunks
- Defining the Allowed VLANs on a Trunk

Inline Interface Mode

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. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on Layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (Layers 3 to 7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.

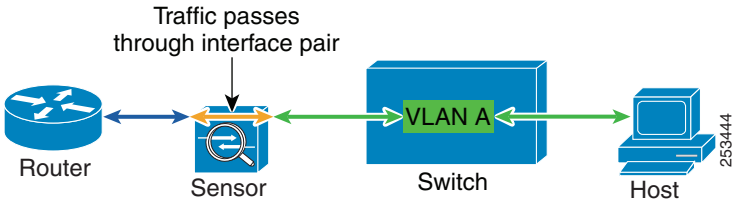
In inline interface pair mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

Note You can configure the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) to operate inline even though they have only one sensing interface.

Note If the paired interfaces are connected to the same switch, you should configure them on the switch as access ports with different access VLANs for the two ports. Otherwise, traffic does not flow through the inline interface.

Figure 7-2 illustrates inline interface pair mode:

Figure 7-2 Inline Interface Pair Mode



Inline VLAN Pair Mode

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support inline VLAN pairs.

Note For the IPS 4500 series, the maximum number of inline VLAN pairs you can create system wide is 150. On all other platforms, the limit is 255 per interface.

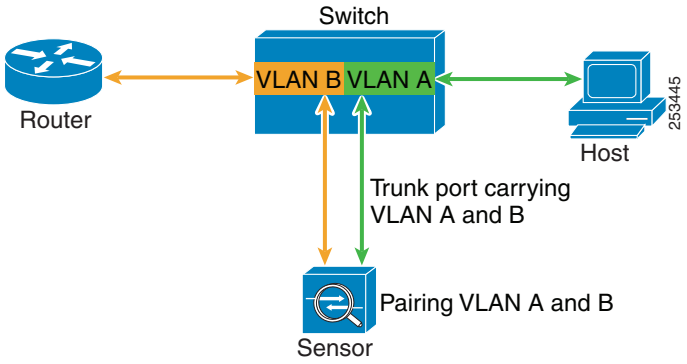
You can associate VLANs in pairs on a physical interface. This is known as inline VLAN pair mode. Packets received on one of the paired VLANs are analyzed and then forwarded to the other VLAN in the pair.

Inline VLAN pair mode is an active sensing mode where a sensing interface acts as an 802.1q trunk port, and the sensor performs VLAN bridging between pairs of VLANs on the trunk. The sensor inspects the traffic it receives on each VLAN in each pair, and can either forward the packets on the other VLAN in the pair, or drop the packet if an intrusion attempt is detected. You can configure an IPS sensor to simultaneously bridge up to 255 VLAN pairs on each sensing interface. The sensor replaces the VLAN ID field in the 802.1q header of each received packet with the ID of the egress VLAN on which the sensor forwards the packet. The sensor drops all packets received on any VLANs that are not assigned to inline VLAN pairs.

Note You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.

Figure 7-3 illustrates inline VLAN pair mode:

Figure 7-3 Inline VLAN Pair Mode



VLAN Groups Mode

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support VLAN groups mode.

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. Analysis Engine supports multiple virtual sensors, each of which can monitor one or more of these interfaces. This lets you apply multiple policies to the same sensor. The advantage is that now you can use a sensor with only a few interfaces as if it had many interfaces.

Note You cannot divide physical interfaces that are in inline VLAN pairs into VLAN groups.

VLAN group subinterfaces associate a set of VLANs with a physical or inline interface. No VLAN can be a member of more than one VLAN group subinterface. Each VLAN group subinterface is identified by a number between 1 and 255. Subinterface 0 is a reserved subinterface number used to represent the entire unvirtualized physical or logical interface. You cannot create, delete, or modify subinterface 0 and no statistics are reported for it.

An unassigned VLAN group is maintained that contains all VLANs that are not specifically assigned to another VLAN group. You cannot directly specify the VLANs that are in the unassigned group. When a VLAN is added to or deleted from another VLAN group subinterface, the unassigned group is updated.

Packets in the native VLAN of an 802.1q trunk do not normally have 802.1q encapsulation headers to identify the VLAN number to which the packets belong. A default VLAN variable is associated with each physical interface and you should set this variable to the VLAN number of the native VLAN or to 0. The value 0 indicates that the native VLAN is either unknown or you do not care if it is specified. If the default VLAN setting is 0, the following occurs:

- Any alerts triggered by packets without 802.1q encapsulation have a VLAN value of 0 reported in the alert.
- Non-802.1q encapsulated traffic is associated with the unassigned VLAN group and it is not possible to assign the native VLAN to any other VLAN group.

Note You can configure a port on a switch as either an access port or a trunk port. On an access port, all traffic is in a single VLAN is called the access VLAN. On a trunk port, multiple VLANs can be carried over the port, and each packet has a special header attached called the 802.1q header that contains the VLAN ID. This header is commonly referred as the VLAN tag. However, a trunk port has a special VLAN called the native VLAN. Packets in the native VLAN do not have the 802.1q headers attached.

Interface Configuration Summary

The Summary pane provides a summary of how you have configured the sensing interfaces—the interfaces you have configured for promiscuous mode, the interfaces you have configured as inline pairs, and the interfaces you have configured as inline VLAN pairs. The content of this pane changes when you change your interface configuration.

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

Field Definitions

The following fields are found in the Summary pane:

- Name—Displays the name of the interface. The values are FastEthernet, GigabitEthernet, Management, or PortChannel for promiscuous interfaces. For inline interfaces, the name is whatever you assigned to the pair.
- Details—Tells you whether the interface is promiscuous, inline, or backplane and whether there are VLAN pairs.

- Assigned Virtual Sensor—Tells you whether the interface or interface pair has been assigned to a virtual sensor.
- Description—Displays your description of the interface.

Configuring Interfaces

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

Interfaces Pane

Note You must be administrator to enable, disable, and edit the interfaces on the sensor.

The Interfaces pane lists the existing physical interfaces on your sensor and their associated settings. The sensor detects the interfaces and populates the interfaces list in the Interfaces pane. If an option is not available for an interface, the field reads N/A or is empty.

To configure the sensor to monitor traffic, you must enable the interface. When you initialized the sensor using the **setup** command, you assigned the interface or the inline pair to a virtual sensor, and enabled the interface or inline pair. If you need to change your interfaces settings, you can do so in the Interfaces pane.To add a virtual sensor and assign it an interface in the Add Virtual Sensor dialog box, choose **Configuration > *sensor_name* > Policies > IPS Policies > Add Virtual Sensor**.

Interfaces Pane Field Definitions

Note If an option is not pertinent or available for an interface, you cannot configure that option. The field is grayed out.

The following fields are found in the Interfaces pane:

- Interface Name—Indicates the name of the interface. The values are FastEthernet, GigabitEthernet, Management, or PortChannel.
- Enabled—Whether or not the interface is enabled.
- Management Interface—Whether or not this interface is a management interface.
- Media Type—Indicates the media type. The media type options are the following:
  - TX—Copper media
  - SX—Fiber media
  - XL—Network accelerator card

  - Backplane interface—An internal interface that connects the module to the backplane of the parent chassis.
- Duplex—Indicates the duplex setting of the interface. The duplex type options are the following:
  - Auto—Sets the interface to auto negotiate duplex.
  - Full—Sets the interface to full duplex.
  - Half—Sets the interface to half duplex.
- Speed—Indicates the speed setting of the interface. The speed type options are the following:
  - Auto—Sets the interface to auto negotiate speed.
  - 10 MB—Sets the interface to 10 MB (for TX interfaces only).
  - 100 MB—Sets the interface to 100 MB (for TX interfaces only).
  - 1000—Sets the interface to 1 GB (for Gigabit interfaces only).
  - 10000—Indicates the interface is set to 10 GB (for PortChannel only).
- Default VLAN—Indicates the VLAN to which the interface is assigned.
- Alternate TCP Reset Interface—If selected, sends TCP resets on an alternate interface when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing.

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

- Description—Lets you provide a description of the interface.

Enabling and Disabling Interfaces

To enable or disable an interface, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Interfaces > Interfaces**.

Step 3 Select the interface and click **Enable**. The interface is enabled. To have the interface monitor traffic, it must also be assigned to a virtual sensor. The Enabled column reads Yes in the list in the Interfaces pane.

Step 4 To disable an interface, select it, and click **Disable**. The Enabled column reads No in the list in the Interfaces pane.

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

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Edit Interface Dialog Box Field Definitions

The following fields are found in the Edit Interface dialog box:

- Interface Name—Name of the interface. The values are FastEthernet, GigabitEthernet, Management, or PortChannel for all interfaces.
- Enabled—Whether or not the interface is enabled.
- Media Type—Indicates the media type. The media types are the following:
  - TX—Copper media
  - SX—Fiber media
  - XL—Network accelerator card
  - Backplane interface—An internal interface that connects the module to the backplane of the parent chassis.
- Duplex—Indicates the duplex setting of the interface. The duplex types are the following:
  - Auto—Sets the interface to auto negotiate duplex.
  - Full—Sets the interface to full duplex.
  - Half—Sets the interface to half duplex.
  - Speed—Indicates the speed setting of the interface. The speed types are the following:
  - Auto—Sets the interface to auto negotiate speed.
  - 10 MB—Sets the interface to 10 MB (for TX interfaces only).
  - 100 MB—Sets the interface to 100 MB (for TX interfaces only).
  - 1000—Sets the interface to 1 GB (for Gigabit interfaces only).
  - 10000—Indicates the interface is set to 10 GB (for PortChannel 0/0 only).
- Default VLAN—Indicates the VLAN to which the interface is assigned.
- Management Interface—Sets this interface as the management interface.
- Use Alternate TCP Reset Interface—If checked, sends TCP resets on an alternate interface when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing.
  - Select Interface—Sets the interface that sends the TCP reset.

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP, ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

- Description—Lets you provide a description of the interface.

Editing Interfaces

To edit the interface settings, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Interfaces > Interfaces**.

Step 3 Select the interface and click **Edit**.

Note You can also double-click the interface and the Edit Interface dialog box appears.

Step 4 You can change the description in the Description field, or change the state from enabled to disabled by checking the **No** or **Yes** check box. You can have the interface use the alternate TCP reset interface by checking the **Use Alternative TCP Reset Interface** check box.

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

Tip To discard your changes and close the Edit Interface dialog box, click **Cancel**.

Step 5 Click **OK**. The edited interface appears in the list in the Interfaces pane.

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

Step 6 Click **Apply** to apply your changes and save the revised configuration.

Configuring Inline Interface Pairs

This section describes how to set up inline interface pairs, and contains the following topics:

Interface Pairs Pane

Note You must be administrator to configure interface pairs.

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

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not need an inline pair for monitoring. You only need to add the physical interface to a virtual sensor.

For More Information

- For the procedure for configuring the ASA 5500-X IPS SSP in inline mode, refer to Configuring the ASA 5500-X IPS SSP.
- For the procedure for configuring the ASA 5585-X IPS SSP in inline mode, refer to Configuring the ASA 5585-X IPS SSP.

Interface Pairs Pane Field Definitions

The following fields are found in the Interface Pairs pane:

- Interface Pair Name—The name you give the interface pair.
- Paired Interfaces—The two interfaces that you have paired (for example, GigabitEthernet 0/0<->GigabitEthernet 0/1).
- Description—Lets you add a description of this interface pair.

Add and Edit Interface Pair Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Interface Pair dialog boxes:

- Interface Pair Name—Indicates the name you give the interface pair.
- Select two interfaces—Lets you select two interfaces from the list to pair (for example, GigabitEthernet 0/0<->GigabitEthernet 0/1).
- Description—Lets you add a description of this interface pair.

Configuring Inline Interface Pairs

To configure inline interface pairs, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Interfaces > Interface Pairs**, and then click **Add**.

Step 3 Enter a name in the Interface Pair Name field. The inline interface name is a name that you create.

Step 4 Select two interfaces to form a pair in the Select two interfaces field. For example, GigabitEthernet 0/0 and GigabitEthernet 0/1.

Step 5 You can add a description of the inline interface pair in the Description field if you want to.

Tip To discard your changes and close the Add Interface pair dialog box, click **Cancel**.

Step 6 Click **OK**. The new inline interface pair appears in the list in the Interface Pairs pane.

Step 7 To edit an inline interface pair, select it, and click **Edit**.

Step 8 You can change the name, choose a new inline interface pair, or edit the description.

Tip To discard your changes and close the Edit Interface Pair dialog box, click **Cancel**.

Step 9 Click **OK**. The edited inline interface pair appears in the list in the Interface Pairs pane.

Step 10 To delete an inline interface pair, select it, and click **Delete**. The inline interface pair no longer appears in the list in the Interface Pairs pane.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring Inline VLAN Pairs

This section describes how to configure inline VLAN pairs, and contains the following topics:

VLAN Pairs Pane

Note You must be administrator to configure inline VLAN pairs.

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support inline VLAN pairs.

The VLAN Pairs pane displays the existing inline VLAN pairs for each physical interface. Click **Add** to create an inline VLAN pair. To create an inline VLAN pair for an interface that is in promiscuous mode, you must remove the interface from the virtual sensor and then create the inline VLAN pair. If the interface is already paired or in promiscuous mode, you receive an error message when you try to create an inline VLAN pair.

Note You cannot create an inline VLAN pair for an interface that has already been paired with another interface or for an interface that is in promiscuous mode and assigned to a virtual sensor.

Note You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.

For More Information

For detailed information on interface configuration restrictions, see Interface Configuration Restrictions, page 7-8.

VLAN Pairs Pane Field Definitions

The following fields are found in the VLAN Pairs pane:

- Interface Name—Displays the name of the inline VLAN pair.
- Subinterface—Displays the subinterface number of the inline VLAN pair. The value is 1 to 255.
- VLAN A—Displays the VLAN number for the first VLAN. The value is 1 to 4095.
- VLAN B—Displays the VLAN number for the second VLAN. The value is 1 to 4095.
- Description—Displays your description of the inline VLAN pair.

Add and Edit VLAN Pair Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Inline VLAN Pair dialog boxes:

- Interface Name—Specifies the name of the interface you want to pair.
- Subinterface Number—Lets you assign a subinterface number. You can assign a number from 1 to 255.
- VLAN A—Lets you specify the first VLAN for this inline VLAN pair. You can assign any VLAN from 1 to 4095.
- VLAN B—Lets you specify the other VLAN for this inline VLAN pair. You can assign any VLAN from 1 to 4095.
- Description—Lets you add a description of this inline VLAN pair.

Note You cannot pair a VLAN with itself. The subinterface number and the VLAN numbers should be unique to each physical interface.

For More Information

For detailed information on interface configuration restrictions, see Interface Configuration Restrictions, page 7-8.

Configuring Inline VLAN Pairs

To configure inline VLAN pairs, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Interfaces > VLAN Pairs**, and then click **Add**.

Step 3 Choose an interface from the **Interface Name** list.

Step 4 In the Subinterface Number field, enter a subinterface number (1 to 255) for the inline VLAN pair.

Step 5 In the VLAN A field, specify the first VLAN (1 to 4095) for this inline VLAN pair.

Step 6 In the VLAN B field, specify the other VLAN (1 to 4095) for this inline VLAN pair.

Step 7 In the Description field, add a description of the inline VLAN pair if desired.

Tip To discard your changes and close the Add VLAN Pair dialog box, click **Cancel**.

Step 8 Click **OK**. The new inline VLAN pair appears in the list in the VLAN Pairs pane.

Step 9 To edit an inline VLAN pair, select it, and click **Edit**.

Step 10 You can change the subinterface number, the VLAN numbers, or edit the description.

Tip To discard your changes and close the Edit VLAN Pair dialog box, click **Cancel**.

Step 11 Click **OK**. The edited VLAN pair appears in the list in the VLAN Pairs pane.

Step 12 To delete a VLAN pair, select it, and click **Delete**. The VLAN pair no longer appears in the list in the VLAN Pairs pane.

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

Step 13 Click **Apply** to apply your changes and save the revised configuration.

Configuring VLAN Groups

This section describes how to configure VLAN groups, and contains the following topics:

VLAN Groups Pane

Note You must be administrator to configure VLAN groups.

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support VLAN groups mode.

In the VLAN Groups pane you can add, edit, or delete VLAN groups that you defined in the sensor interface configuration. 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 VLANs IDs. You then assign each VLAN group to a virtual sensor (but not multiple virtual sensors). You can assign different VLAN groups on the same sensor to different virtual sensors.

After you assign the VLAN IDs to the VLAN group, you must assign the VLAN group to a virtual sensor. The IME cross-validates between the interface and virtual sensor configuration. Any configuration changes in one component that could invalidate the other is blocked.

For More Information

For the procedure for assigning the VLAN group to a virtual sensor, see Adding, Editing, and Deleting Virtual Sensors, page 8-12.

Deploying VLAN Groups

Because a VLAN group of an inline pair does not translate the VLAN ID, an inline paired interface must exist between two switches to use VLAN groups on a logical interface. For an appliance, you can connect the two pairs to the same switch, make them access ports, and then set the access VLANs for the two ports differently. In this configuration, the sensor connects between two VLANs, because each of the two ports is in access mode and carries only one VLAN. In this case the two ports must be in different VLANs, and the sensor bridges the two VLANs, monitoring any traffic that flows between the two VLANs.

You can also connect appliances between two switches. There are two variations. In the first variation, the two ports are configured as access ports, so they carry a single VLAN. In this way, the sensor bridges a single VLAN between the two switches.

In the second variation, the two ports are configured as trunk ports, so they can carry multiple VLANs. In this configuration, the sensor bridges multiple VLANs between the two switches. Because multiple VLANs are carried over the inline interface pair, the VLANs can be divided into groups and each group can be assigned to a virtual sensor.

VLAN Groups Pane Field Definitions

The following fields are found in the VLAN Groups pane:

- Interface Name—Displays the physical or logical interface name of the VLAN group.
- Subinterface—Displays the subinterface number of the VLAN group. The value is 1 to 255.
- VLAN Group—Displays the VLAN number for the VLAN group. The value is 1 to 4095.
- Description—Displays your description of the VLAN group.

Add and Edit VLAN Group Dialog Boxes Field Definitions

The following fields are found in the Add and Edit VLAN Group dialog boxes:

- Interface Name—Specifies the name of the VLAN group.
- Subinterface Number—Specifies the subinterface number of the VLAN group. The value is 1 to 255.
- VLAN Group—Displays the VLAN number for the VLAN group:
  - Unassigned VLANS—Lets you choose all VLANS that have not yet been assigned to a VLAN group.
  - Specify VLAN Group—Lets you specify the VLAN IDs that you want to assign to this VLAN group. The value is 1 to 4095 in a comma-separated pattern of individual VLAN IDs or ranges: 1, 5-8, 10-15.

- Description—Lets you add a description of the VLAN group.

Configuring VLAN Groups

To configure VLAN groups, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Interfaces > VLAN Groups**, and then click **Add**.

Step 3 From the Interface Name drop-down list, choose an interface.

Step 4 In the Subinterface Number field, enter a subinterface number (1 to 255) for the VLAN group.

Step 5 Under VLAN Group, specify the VLAN group for this interface by checking one of the following check boxes:

a. **Unassigned VLANs**—Lets you assign all the VLANs that are not already specifically assigned to a subinterface.

b. **Specify VLAN Group**—Lets you specify the VLANs that you want to assign to this subinterface. You can assign more than one VLAN (1 to 4096) 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 6 You can add a description of the VLAN group in the Description field if you want to.

Tip To discard your changes and close the Add VLAN Group dialog box, click **Cancel**.

Step 7 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 8 To edit a VLAN group, select it, and click **Edit**.

Step 9 You can change the subinterface number, the VLAN group, or edit the description.

Tip To discard your changes and close the Edit VLAN Group dialog box, click **Cancel**.

Step 10 Click **OK**. The edited VLAN group appears in the list in the VLAN Groups pane.

Step 11 To delete a VLAN group, select it, and click **Delete**. The VLAN group no longer appears in the list in the VLAN Groups pane.

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

Step 12 Click **Apply** to apply your changes and save the revised configuration.

Configuring Bypass Mode

This section describes how to configure bypass mode, and contains the following topics:

Bypass Pane

Note You must be administrator to configure bypass mode on the sensor.

Note The ASA 5500-X IPS SSP and the ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

Caution There are security consequences when you put the sensor in bypass mode. When bypass mode is on, the traffic bypasses the sensor and is not inspected; therefore, the sensor cannot prevent malicious attacks.

Caution As with signature updates, when the sensor applies a global correlation update, it may trigger bypass. Whether or not bypass is triggered depends on the traffic load of the sensor and the size of the signature/global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

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, the 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 automatic. By default, bypass mode is set to automatic.

The inline bypass functionality is implemented in software, so it only functions when the operating system is running. If the sensor is powered off or shut down, inline bypass does not work—traffic does not flow through the sensor.

For the IPS 4500 series, when the SensorApp is not running or if bypass mode is on, the following occurs:

- The output from the **packet capture/display** command does not show any packets.
- The **show interface** and **show interface** *interface_name* commands do not show VLAN statistics.

Bypass Pane Field Definitions

The following fields are found in the Bypass pane:

- Auto—Traffic flows through the sensor for inspection unless the monitoring process of the sensor is down. If the monitoring process of the sensor is down, traffic bypasses the sensor until the sensor is running again. The sensor then inspects the traffic. Auto mode is useful during sensor upgrades to ensure that traffic is still flowing while the sensor is being upgraded. Auto mode also helps to ensure traffic continues to pass through the sensor if the monitoring process fails.
- Off—Disables bypass mode. Traffic flows through the sensor for inspection. If the monitoring process of the sensor is down, traffic stops flowing. This means that inline traffic is always inspected.
- On—Traffic bypasses the Analysis Engine and is not inspected. This means that inline traffic is never inspected.

Configuring Traffic Flow Notifications

Note You must be administrator to configure traffic flow notifications.

You can configure the sensor to monitor the flow of packets across an interface and send notification if that flow changes (starts/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.

Field Definitions

The following fields are found in the Traffic Flow Notifications pane:

- Missed Packets Threshold—Specifies the percentage of packets that must be missed during a specified time before a notification is sent.
- Notification Interval—Specifies the interval the sensor checks for the missed packets percentage.
- Interface Idle Threshold—Specifies the number of seconds an interface must be idle and not receiving packets before a notification is sent.

Configuring Traffic Flow Notifications

To configure traffic flow notifications, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Interfaces > Traffic Flow Notifications**.

Step 3 In the Missed Packets Threshold field, specify the percent of missed packets that has to occur before you want to receive notification and enter that amount.

Step 4 In the Notification Interval field, specify the amount of seconds that you want to check for the percentage of missed packets and enter that amount.

Step 5 In the Interface Idle Threshold field, specify 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.

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

Step 6 Click **Apply** to apply your changes and save the revised configuration.

Configuring CDP Mode

Note You must be administrator to configure CDP mode.

Note The ASA 5500-X IPS SSP and the ASA 5585-X IPS SSP do not support CDP mode.

You can configure the sensor to enable or disable the forwarding of CDP packets. This action applies globally to all interfaces.

Cisco Discovery Protocol is a media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. CDP runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.

Field Definitions

The following fields are found in the CDP Mode pane:

- Drop CDP Packets—Specifies that the sensor does not forward CDP packets.
- Forward CDP Packets—Specifies that the sensor forwards CDP packets.

Configuring CDP Mode

To configure CDP mode, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Interfaces > CDP Mode**.

Step 3 From the CDP Mode drop-down list, choose either Drop CDP Packets (default) or Forward CDP Packets.

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

Step 4 Click **Apply** to apply your changes and save the revised configuration.

Configuring Policies

This chapter describes IPS policies and how to configure the virtual sensor. It contains the following sections:

Understanding Security Policies

You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies. The use of multiple security policies lets you create security policies based on different requirements and then apply these customized policies per VLAN or physical interface.

IPS Policies Components

This section describes the various components of IPS Policies, and contains the following sections:

Understanding Analysis Engine

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

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

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. 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:

- ASA 5500-X IPS SSP
- ASA 5585-X IPS SSP
- IPS 4345
- IPS 4345-DC
- IPS 4360
- IPS 4510
- IPS 4520
- IPS 4520-XL

Inline TCP Session Tracking Mode

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the 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.

Understanding Normalizer Mode

Note For the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), normalization is performed by the adaptive security appliance and not the IPS.

Normalization only applies when the sensor is operating in inline mode. The default is strict evasion protection, which is full enforcement of TCP state and sequence tracking. The Normalizer enforces duplicate packets, changed packets, out-of-order packets, and so forth, which helps prevent attackers from evading the IPS.

Asymmetric mode disables most of the Normalizer checks. Use asymmetric mode only when the entire stream cannot be inspected, because in this situation, attackers can now evade the IPS.

Understanding HTTP Advanced Decoding

HTTP advanced decoding facilitates analysis of encoded HTTP return web traffic by using on-the-fly decoding. Changes to HTTP advanced decoding take effect immediately and only affect the new traffic flows.

Restrictions

The following restrictions apply when you enable HTTP advanced decoding:

- Although HTTP advanced decoding does not fire any new signatures, drop packets, or modify traffic, it allows existing signatures to match on content that was previously not detectable because of encodings.
- HTTP advanced decoding only acts on return web response traffic.

Caution Enabling HTTP advanced decoding severely impacts system performance.

Note Because HTTP advanced decoding requires the Regex card and the String XL engine, it is available only to those platforms that have them. HTTP advanced decoding is supported on the IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5585-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, and ASA 5555-X IPS SSP.

Understanding Event Action Overrides

You can add an event action override to change the actions associated with an event based on the risk rating of that event. Event action overrides are a way to add event actions globally without having to configure each signature individually. Each event action has an associated risk rating range. If a signature event occurs and the risk rating for that event falls within the range for an event action, that action is added to the event. For example, if you want any event with a risk rating of 85 or more to generate an SNMP trap, you can set the risk rating range for Request SNMP Trap to 85-100. If you do not want to use action overrides, you can disable the entire event action override component.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Calculating the Risk Rating

A risk rating (RR) is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network. The calculation takes into account the value of the network asset being attacked (for example, a particular server), so it is configured on a per-signature basis using the attack severity rating and the signature fidelity rating, and on a per-server basis using the target value rating. The risk rating is calculated from several components, some of which are configured, some collected, and some derived.

Note The risk rating is associated with alerts not signatures.

Risk ratings let you prioritize alerts that need your attention. These risk rating factors take into consideration the severity of the attack if it succeeds, the fidelity of the signature, the reputation score of the attacker from the global correlation data, and the overall value of the target host to you. The risk rating is reported in the evIdsAlert.

The following values are used to calculate the risk rating for a particular event:

- Signature fidelity rating (SFR)—A weight associated with how well this signature might perform in the absence of specific knowledge of the target. The signature fidelity rating is configured per signature and indicates how accurately the signature detects the event or condition it describes.

  Signature fidelity rating is calculated by the signature author on a per-signature basis. The signature author defines a baseline confidence ranking for the accuracy of the signature in the absence of qualifying intelligence on the target. It represents the confidence that the detected behavior would produce the intended effect on the target platform if the packet under analysis were allowed to be delivered. For example, a signature that is written with very specific rules (specific regular expression) has a higher signature fidelity rating than a signature that is written with generic rules.

Note The signature fidelity rating does not indicate how bad the detected event may be.

- Attack severity rating (ASR)—A weight associated with the severity of a successful exploit of the vulnerability. The attack severity rating is derived from the alert severity parameter (informational, low, medium, or high) of the signature. The attack severity rating is configured per signature and indicates how dangerous the event detected is.

  Note The attack severity rating does not indicate how accurately the event is detected.

- Target value rating (TVR)—A weight associated with the perceived value of the target.

  Target value rating is a user-configurable value (zero, low, medium, high, or mission critical) that identifies the importance of a network asset (through its IP address). You can develop a security policy that is more stringent for valuable corporate resources and looser for less important resources. For example, you could assign a target value rating to the company web server that is higher than the target value rating you assign to a desktop node. In this example, attacks against the company web server have a higher risk rating than attacks against the desktop node. Target value rating is configured in the event action rules policy.

- Attack relevance rating (ARR)—A weight associated with the relevancy of the targeted operating system. Attack relevancy rating is a derived value (relevant, unknown, or not relevant), which is determined at alert time. The relevant operating systems are configured per signature.
- Promiscuous delta (PD)—A weight associated with the promiscuous delta, which can be subtracted from the overall risk rating in promiscuous mode. Promiscuous delta is in the range of 0 to 30 and is configured per signature.

  Note If the trigger packet is not inline, the promiscuous delta is subtracted from the rating.

- Watch list rating (WLR)—A weight associated with the CSA MC watch list in the range of 0 to 100 (CSA MC only uses the range 0 to 35). If the attacker for the alert is found on the watch list, the watch list rating for that attacker is added to the rating.

Figure 8-1 illustrates the risk rating formula:

Figure 8-1 Risk Rating Formula

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

191016

Understanding Threat Rating

Threat rating is risk rating that has been lowered by event actions that have been taken. Nonlogging event actions have a threat rating adjustment. The largest threat rating from all the event actions taken is subtracted from the risk rating. The event actions have the following threat ratings:

- Deny attacker inline—45
- Deny attacker victim pair inline—40

- Deny attacker service pair inline—40
- Deny connection inline—35
- Deny packet inline—35
- Modify packet inline—35
- Request block host—20
- Request block connection—20
- Reset TCP connection—20
- Request rate limit—20

Event Action Summarization

Summarization decreases the volume of alerts sent out from the sensor by providing basic aggregation of events into a single alert. Special parameters are specified for each signature and they influence the handling of the alerts. Each signature is created with defaults that reflect a preferred normal behavior. However, you can tune each signature to change this default behavior within the constraints for each engine type.

The nonalert-generating actions (deny, block, TCP reset) go through the filters for each signature event unsummarized. The alert-generating actions are not performed on these summarized alerts; instead the actions are applied to the one summary alert and then put through the filters.

If you select one of the other alert-generating actions and do not have it filtered out, the alert is created even if you do not select Product Alert. To prevent alerts from being created, you must have all alert-generating actions filtered out.

Summarization and event actions are processed after the Meta engine has processed the component events. This lets the sensor watch for suspicious activity transpiring over a series of events.

Event Action Aggregation

Basic aggregation provides two operating modes. The simple mode involves configuring a threshold number of hits for a signature that must be met before the alert is sent. A more advanced mode is timed-interval counting. In this mode, the sensor tracks the number of hits per second and only sends alerts when that threshold is met. In this example, a hit is a term used to describe an event, which is basically an alert, but it is not sent out of the sensor as an alert until the threshold number of hits has been exceeded.

You can choose from the following summarization options:

- Fire All—Fires an alert each time the signature is triggered. If the threshold is set for summarization, alerts are fired for each execution until summarization occurs. After summarization starts, only one alert every summary interval fires for each address set. Alerts for other address sets are either all seen or separately summarized. The signature reverts to fire all mode after a period of no alerts for that signature.
- Summary—Fires an alert the first time a signature is triggered, and then additional alerts for that signature are summarized for the duration of the summary interval. Only one alert every summary interval should fire for each address set. If the global summary threshold is reached, the signature goes into global summarization mode.
- Global Summarization—Fires an alert for every summary interval. Signatures can be preconfigured for global summarization.

- Fire Once—Fires an alert for each address set. You can upgrade this mode to global summarization mode.

Configuring IPS Policies

This section describes IPS Policies and how to configure a virtual sensor. It contains the following topics:

IPS Policies Pane

The IPS Policies pane displays a list of the virtual sensors in the upper half of the pane. In the upper half of this pane you can add, edit, or delete virtual sensors. For each virtual sensor the following information is displayed:

- Virtual sensor name
- Assigned interfaces or pairs
- Signature definition policy
- Event action rules override policy
  - Risk rating
  - Actions to add
  - Enabled or disabled
- Anomaly detection policy

  Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

- Description of the virtual sensor

  Note The default virtual sensor is vs0. You cannot delete the default virtual sensor.

In the lower half of the pane, you can configure the event action rules for each virtual sensor that you select in the upper half of the pane. You can also configure event action rules in the **Configuration > *sensor_name* > Policies > Event Action rules > rules0** pane. The Event Action Rules part of the pane contains the following tabs:

- Event Action Filters—Lets you remove specifications from an event or discard an entire event and prevent further processing by the sensor.

- IPv4 Target Value Rating—Lets you assign an IPv4 target value rating to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert.
- IPv6 Target Value Rating—Lets you assign an IPv6 target value rating to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert.
- OS Identifications—Lets you associate IP addresses with an OS type, which in turn helps the sensor calculate the attack relevance rating.
- Event Variables—Lets you create event variables to use in event action filters. When you want to use the same value within multiple filters, you can use an event variable.
- Risk Category—Lets you create the risk categories you want to use to monitor sensor and network health and to use in event action overrides.
- Threat Category—Lets you set the red, yellow, and green threat thresholds for network security health statistics.
- General—Lets you configure some global settings that apply to event action rules.

IPS Policies Pane Field Definitions

The following fields are found in the IPS Policies pane:

- Name—Specifies the name of the virtual sensor. The default virtual sensor is vs0.
- Assigned Interfaces (or Pairs)—Specifies the interfaces or interface pairs that belong to this virtual sensor.
- Signature Definition Policy—Specifies the name of the signature definition policy for this virtual sensor. The default signature definition policy is sig0.
- Event Action Override Policy—Specifies the name of the event action rules overrides policy for this virtual sensor. The default event action rules policy is rules0.
  - Risk Rating—Indicates the risk rating range (low, medium, or high risk) that should be used to trigger this event action override.
  - Actions to Add—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
  - Enabled—Indicates whether or not this event action overrides policy is enabled.
- Anomaly Detection Policy—Specifies the name of the anomaly detection policy for this virtual sensor. The default anomaly detection policy is ad0.

  Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

- Description—The description of this virtual sensor.

Add and Edit Virtual Sensor Dialog Boxes Field Definitions

Note You must be administrator or operator to configure a virtual sensor.

You can apply the same policy, for example, sig0, rules0, and ad0, to different virtual sensors. The Add Virtual Sensor dialog box displays only the interfaces that are available to be assigned to this virtual sensor. Interfaces that have already been assigned to other virtual sensors are not shown in this dialog box.

You can also assign event action overrides to virtual sensors, and configure the following modes:

- Anomaly detection operational mode

  Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

- Inline TCP session tracking mode

  Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the inline TCP session tracking mode.

- Normalizer mode

  Note For the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), normalization is performed by the adaptive security appliance and not the IPS.

- HTTP Advanced Decoding

  Note HTTP advanced decoding is supported on the IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5585-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, and ASA 5555-X IPS SSP.

The following fields are found in the Add and Edit Virtual Sensor dialog boxes:

- Virtual Sensor Name—Specifies the name for this virtual sensor.
- Description—Description for this virtual sensor.
- Interfaces—Lets you assign and remove interfaces for this virtual sensor:
  - Assigned—Whether the interfaces or interface pairs have been assigned to the virtual sensor.
  - Name—Specifies the list of available interfaces or interface pairs that you can assign to the virtual sensor (GigabitEthernet or FastEthernet).
  - Details—Lists the mode (inline interface or promiscuous) of the interface and the interfaces of the inline pairs.
- Signature Definition Policy—Specifies the name of the signature definition policy you want to assign to this virtual sensor. The default is sig0.
- Event Action Rules Policy—Specifies the name of the event action rules policy you want to assign to this virtual sensor. The default is rules0.
- Use Event Action Overrides—When checked, lets you configure event action overrides when you click **Add** to open the Add Event Action Override dialog box:
  - Risk Rating—Indicates the level of risk rating for this override.
  - Actions to Add—Indicates the action to add to this override.

  - Enabled—Indicates whether this override is enabled or disabled.

- Anomaly Detection Policy—Displays the name of the anomaly detection policy. The default anomaly detection policy is ad0. Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.
- AD Operational Mode—Specifies the mode that you want the anomaly detection policy to operate in for this virtual sensor. The default is Detect.
- Inline TCP Session Tracking Mode—Specifies the mode used to segregate multiple views of the same stream if the same stream passes through the sensor more than once. The default mode is Virtual Sensor.
  - 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.

    Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the inline TCP session tracking mode.

- Normalizer Mode—Lets you choose which type of normalization you need for traffic inspection:
  - Strict Evasion Protection—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.

  - Asymmetric Mode Protection—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.

    Note For the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), normalization is performed by the adaptive security appliance and not the IPS.

- HTTP Advanced Decoding—Lets you enable HTTP advanced decoding. HTTP advanced decoding analyzes the various encodings that are applied to HTTP return web traffic. The default is Inactive.

Note HTTP advanced decoding is supported on the IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5585-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, and ASA 5555-X IPS SSP.

Add and Edit Event Action Override Dialog Boxes Field Definitions

Note You must be administrator or operator to add or edit event action overrides.

The following fields are found in the Add and Edit Event Action Override dialog boxes:

- Risk Rating—Lets you add the risk rating range, either low, medium, or high risk, that should be used to trigger this event action override. If an event occurs with a risk rating that corresponds to the risk you configure, the event action is added to this event. In add mode, you can create a numeric range by entering it in to the Risk Rating field. In edit mode, you can select the category that you created.
- Available Actions to Add—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
- Assigned—Lets you assign event actions to this override.
- Enabled—Check the check box to enable the action.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Adding, Editing, and Deleting Virtual Sensors

You must assign all interfaces to a virtual sensor and enable them before they can monitor traffic.

To add, edit, and delete virtual sensors, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**, and then click **Add Virtual Sensor**.

Step 3 In the Virtual Sensor Name field, enter a name for the virtual sensor.

Step 4 In the Description field, enter a description of this virtual sensor.

Step 5 To assign the interface to the virtual sensor, check the check box next to the interface you need, and then click **Assign**.

Note Only the available interfaces are listed in the Interfaces list. If other interfaces exist, but have already been assigned to a virtual sensor, they do not appear in this list.

Step 6 Under Signature Definition, choose a signature definition policy from the Signature Definition Policy drop-down list. Unless you want to use the default sig0, you must have already added a signature definition policy by choosing **Configuration > *sensor_name* > Policies > Signature Definitions > Add**.

Step 7 Under Event Action Rule, choose an event action rules policy from the Event Action Rules Policy drop-down list. Unless you want to use the default rules0, you must have already added an event action rules policy by choosing **Configuration > *sensor_name* > Policies > Event Action Rules > Add**.

Step 8 To add event action override to this virtual sensor, check the **Use Event Action Overrides** check box, and then click **Add**.

Note You must check the **Use Event Action Overrides** check box or none of the event action overrides will be enabled regardless of the value you set.

a. Choose the risk rating from the Risk Rating drop-down list.

b. Under the Assigned column, check the check boxes next to the actions you want to assign to this event action override.

c. Under the Enabled column, check the check boxes next to the actions you want enabled.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Tip To discard your changes and close the Add Event Action Override dialog box, click **Cancel**.

d. Click **OK**.

Step 9 (Optional) Under Anomaly Detection, choose an anomaly detection policy from the Anomaly Detection Policy drop-down list. Unless you want to use the default ad0, you must have already added a anomaly detection policy by choosing **Configuration > *sensor_name* > Policies > Anomaly Detections > Add**.

Note Anomaly detection is disabled. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

Step 10 (Optional) Choose the anomaly detection mode (Detect, Inactive, Learn) from the AD Operational Mode drop-down list. The default is Inactive.

Step 11 Under Advanced Options, click the **Double Arrow** icon to change the default values:

a. Choose how the sensor tracks inline TCP sessions (by interface and VLAN, VLAN only, or virtual sensor). The default is virtual sensor. This is almost always the best option to choose.

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support the inline TCP session tracking mode.

b. Choose the Normalizer mode (by strict evasion protection or asymmetric mode protection).

Note For the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), normalization is performed by the adaptive security appliance and not the IPS.

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

Step 12 Enable HTTP advanced decoding by choosing Active from the HTTP Advanced Decoding drop-down list. HTTP advanced decoding is disabled by default.

Note HTTP advanced decoding is supported on the IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5585-X IPS SSP, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, and ASA 5555-X IPS SSP.

Step 13 Click **OK**. The virtual sensor appears in the list in the IPS Policies pane.

Step 14 To edit a virtual sensor, select it in the list, and then click **Edit**.

Step 15 Make any changes needed, and then click **OK**. The edited virtual sensor appears in the list in the upper half of the IPS Policies pane.

Step 16 To remove a virtual sensor, select it, and then click **Delete**. The virtual sensor no longer appears in the upper half of the IPS Policies pane.

Note You cannot delete the default virtual sensor, vs0.

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

Step 17 Click **Apply** to apply your changes and save the revised configuration.

The ASA 5500-X IPS SSP, ASA 5585-X IPS SSP, and Virtual Sensors

This section describes how to configure virtual sensors on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), and contains the following sections:

Understanding the ASA IPS Module and Virtual Sensors

The ASA 5500-X IPS SSP and ASA 5585-X IPS SSP have one sensing interface, PortChannel 0/0. When you create multiple virtual sensors, you must assign this interface to only one virtual sensor. For the other virtual sensors you do not need to designate an interface.

After you create virtual sensors, you must map them to a security context on the adaptive security appliance using the **allocate-ips** command. You can map many security contexts to many virtual sensors.

Note The **allocate-ips** command does not apply to single mode. In this mode, the adaptive security appliance accepts any virtual sensor named in a **policy-map** command.

The **allocate-ips** command adds a new entry to the security context database. A warning is issued if the specified virtual sensor does not exist; however, the configuration is allowed. The configuration is checked again when the **service-policy** command is processed. If the virtual sensor is not valid, the **fail-open** policy is enforced.

ASA IPS Module Configuration Sequence

Follow this sequence to create virtual sensors on the ASA 5500-X IPS SSP and ASA 5585-X IPS SSP, and to assign them to adaptive security appliance contexts:

1. Configure up to four virtual sensors.
2. Assign the sensing interface (PortChannel 0/0) to one of the virtual sensors.
3. (Optional) Assign virtual sensors to different contexts on the adaptive security appliance.
4. Use MPF to direct traffic to the targeted virtual sensor.

Creating Virtual Sensors on the ASA IPS Module

Note You can create four virtual sensors.

Use the **virtual-sensor** *name* command in service analysis engine submode to create virtual sensors on the ASA 5500-X IPS SSP and ASA 5585-X IPS SSP. You assign policies (anomaly detection, event action rules, and signature definition) to the virtual sensor. You can use the default policies, ad0, rules0, or sig0, or you can create new policies.Then you assign the sensing interface, PortChannel 0/0 to one virtual sensor.

The following options apply:

- **anomaly-detection**—Specifies the anomaly detection parameters:
  - **anomaly-detection-name** *name*—Specifies the name of the anomaly detection policy.
  - **operational-mode**—Specifies the anomaly detection mode (**inactive**, **learn**, **detect**).

    Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

- **description**—Provides a description of the virtual sensor.
- **event-action-rules**—Specifies the name of the event action rules policy.
- **signature-definition**—Specifies the name of the signature definition policy.
- **physical-interfaces**—Specifies the name of the physical interface.
- **no**—Removes an entry or selection.

Creating Virtual Sensors

To create a virtual sensor on the ASA 5500-X IPS SSP and ASA 5585-X IPS SSP, 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 if you have enabled anomaly detection. If you do not want to use the default anomaly detection policy, ad0, you must create a new one using the **service anomaly-detection** *name* command, for example, ad1.

```
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 Assign an event action rules policy to this virtual sensor. If you do not want to use the default event action rules policy, rules0, you must create a new one using the **service event-action-rules** *name* command, for example, rules1

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

Step 7 Assign a signature definition policy to this virtual sensor. If you do not want to use the default signature definition policy, sig0, you must create a new one using the **service signature-definition** *name* command, for example sig1.

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

Step 8 Assign the interface to one virtual sensor. By default the sensing interface is already assigned to the default virtual sensor, vs0. You must remove it from the default virtual sensor to assign it to another virtual sensor that you create.

```
sensor(config-ana-vir)# physical-interface PortChannel0/0
```

Step 9 Verify the virtual sensor settings.

```
sensor(config-ana-vir)# show settings
   <protected entry>
   name: vs1
   -----------------------------------------------
      description: virtual sensor 1 default:
      signature-definition: sig0 <protected>
      event-action-rules: rules0 <protected>
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad0 <protected>
         operational-mode: inactive <defaulted>
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 1)
      -----------------------------------------------
```

```
        name: PortChannel0/0
        ---------------------------------------------
      ---------------------------------------------
      inline-TCP-evasion-protection-mode: strict <defaulted>
   ---------------------------------------------
sensor(config-ana-vir)#
```

Step 10 Exit analysis engine mode.

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

Step 11 Press **Enter** to apply the changes or enter **no** to discard them.

Assigning Virtual Sensors to Adaptive Security Appliance Contexts

You can assign multiple virtual sensors to a context. Multiple contexts can share one virtual sensor, and when sharing, the contexts can have different mapped names (aliases) for the same virtual sensor. The following procedure demonstrates how to add three security contexts in multiple mode and how to assign virtual sensors to these security contexts.

Assigning Virtual Sensors to Contexts

To assign virtual sensors to adaptive security appliance contexts in multiple mode for the ASA 5500-X IPS SSP and ASA 5585-X IPS SSP, follow these steps:

Step 1 Log in to the adaptive security appliance.

Step 2 Display the list of available virtual sensors.

```
asa# show ips
Sensor Name      Sensor ID
-----------      ---------
vs0              1
vs1              2
asa#
```

Step 3 Enter configuration mode.

```
asa# configure terminal
asa(config)#
```

Step 4 Enter multiple mode.

```
asa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] yes
asa(config)#
```

Step 5 Add three context modes to multiple mode.

```
asa(config)# admin-context admin
Creating context 'admin'... Done. (13)
asa(config)# context admin
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.101
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.102
asa(config-ctx)#   allocate-interface Management0/0
```

```
asa(config-ctx)#   config-url disk0:/admin.cfg
Cryptochecksum (changed): 0c34dc67 f413ad74 e297464a db211681
INFO: Context admin was created with URL disk0:/admin.cfg
INFO: Admin context will take some time to come up .... please wait.
asa(config-ctx)#
asa(config-ctx)# context c2
Creating context 'c2'... Done. (14)
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.103
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.104
asa(config-ctx)#   config-url disk0:/c2.cfg

WARNING: Could not fetch the URL disk0:/c2.cfg
INFO: Creating context with default config
asa(config-ctx)#
asa(config-ctx)# context c3
Creating context 'c3'... Done. (15)
asa(config-ctx)# all
asa(config-ctx)# allocate-in
asa(config-ctx)# allocate-interface g0/2
asa(config-ctx)# allocate-interface g0/3
asa(config-ctx)#   config-url disk0:/c3.cfg

WARNING: Could not fetch the URL disk0:/c3.cfg
INFO: Creating context with default config
asa(config-ctx)#
```

Step 6 Assign virtual sensors to the security contexts.

```
asa(config)# context admin
asa(config-ctx)#   allocate-ips vs0 adminvs0
asa(config-ctx)# exit
asa(config)# context c2
asa(config-ctx)#   allocate-ips vs1 c2vs1
asa(config)# context c3
asa(config-ctx)# allocate-ips vs0 c3vs0
asa(config-ctx)# allocate-ips vs1 c3vs1
asa(config-ctx)#
```

Step 7 Configure MPF for each context.

Note The following example shows context 3 (c3).

```
asa(config)# context c3
asa/c3(config)# class-map any
asa/c3(config-cmap)# match access-list any
asa/c3(config-cmap)# exit
asa/c3(config)# policy-map ips_out
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips promiscuous fail-close sensor c3vs1
asa/c3(config-pmap-c)# policy-map ips_in
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips inline fail-open sensor c3vs0
asa/c3(config-pmap-c)# service-policy ips_out interface outside
asa/c3(config)# service-policy ips_in interface inside
asa/c3(config)#
```

Step 8 Confirm the configuration.

```
asa/c3(config)# exit
asa(config)# show ips detail
Sensor Name      Sensor ID        Allocated To     Mapped Name
-----------      ---------        ------------     -----------
```

```
vs0             1               admin           adminvs0
                                c3              c3vs0
vs1             2               c2              c2vs1
                                c3              c3vs1
asa(config)#
```

Configuring Event Action Filters

This section describes how to configure event action filters, and contains the following topics:

Understanding Event Action Filters

Event action filters are processed as an ordered list and you can move filters up or down in the list. Filters let the sensor perform certain actions in response to the event without requiring the sensor to perform all actions or remove the entire event. Filters work by removing actions from an event. A filter that removes all actions from an event effectively consumes the event.

Note When filtering sweep signatures, we recommend that you do not filter the destination addresses. If there are multiple destination addresses, only the last address is used for matching the filter.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

Event Action Filters Tab

You can configure event action filters to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor. You can use the variables that you defined on the Event Variables pane to group addresses for your filters.

You must preface the variable with a dollar sign ($) to indicate that you are using a variable rather than a string. Otherwise, you receive the `Bad source and destination` error.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

Event Action Filters Tab Field Definitions

The following fields are found on the Event Action Filters tab:

- Name—Lets you name the filter you are adding. You need to name your filters so that you can move them around in the list and move them to the inactive list if needed.
- Enabled—Indicates whether or not this filter is enabled.
- Sig ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. You can also enter a range of signatures.
- SubSig ID—Identifies the unique numerical value assigned to this subsignature. The subSig ID identifies a more granular version of a broad signature. You can also enter a range of subSig IDs.
- Attacker (IPv4/IPv6/port)—Identifies the IP address and/or port of the host that sent the offending packet. You can also enter a range of addresses or ports.
- Victim (IPv4/IPv6/port)—Identifies the IP address and/or port used by the attacker host. You can also enter a range of addresses or ports.
- Risk Rating—Indicates the risk rating range between 0 and 100 that should be used to trigger this event action filter. If an event occurs with an risk rating that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
- Actions to Subtract—Indicates the actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter.

Add and Edit Event Action Filter Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Event Action Filters dialog boxes:

- Name—Lets you name the filter you are adding. You need to name your filters so that you can move them around in the list and move them to the inactive list if needed.
- Enabled—Lets you enable this filter.
- Signature ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. You can also enter a range of signatures.
- Subsignature ID—Identifies the unique numerical value assigned to this subsignature. The subsignature ID identifies a more granular version of a broad signature. You can also enter a range of subsignature IDs.
- Attacker IPv4 Address—Identifies the IP address of the host that sent the offending packet. You can also enter a range of addresses.
- Attacker IPv6 Address—Identifies the range set of attacker IPv6 addresses of the host that sent the offending packet in the following format:

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  Example—2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888. The second IPv6 address in the range must be greater than or equal to the first IPv6 address.

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

- Attacker Port—Identifies the port used by the attacker host. This is the port from where the offending packet originated. You can also enter a range of ports.
- VictimIPv4 Address—Identifies the IP address of the host being attacked (the recipient of the offending packet). You can also enter a range of addresses.
- VictimIPv6 Address—Identifies the range set of victim IPv6 addresses of the host that is the being attacked (the recipient of the offending packet) in the following format:

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  Example—2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888. The second IPv6 address in the range must be greater than or equal to the first IPv6 address.

  Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

- Victim Port—Identifies the port through which the offending packet was received. You can also enter a range of ports.
- Risk Rating—Indicates the risk rating range between 0 and 100 that should be used to trigger this event action filter. If an event occurs with a risk rating that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
- Actions to Subtract—Opens the Edit Actions dialog box and lets you choose the actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter.
- More Options
  - Active—Lets you add the filter to the filter list so that it takes effect on filtering events.
  - OS Relevance—Lets you filter out events where the attack is not relevant to the victim operating system.
  - Deny Percentage—Determines the percentage of packets to deny for deny attacker features. The valid range is 0 to 100. The default is 100 percent.
  - Stop on Match—Determines whether or not this event will be processed against remaining filters in the event action filters list. If set to No, the remaining filters are processed for a match until a Stop flag is encountered. If set to Yes, no further processing is done. The actions specified by this filter are removed and the remaining actions are performed.
  - Comments—Displays the user comments associated with this filter.

Adding, Editing, Deleting, Enabling, Disabling, and Moving Event Action Filters

Note Global correlation inspection and the reputation filtering deny features do not support IPv6 addresses. For global correlation inspection, the sensor does not receive or process reputation data for IPv6 addresses. The risk rating for IPv6 addresses is not modified for global correlation inspection. Similarly, network participation does not include event data for attacks from IPv6 addresses. And finally, IPv6 addresses do not appear in the deny list.

Note Rate limiting and blocking are not supported for IPv6 traffic. If a signature is configured with a block or rate limit event action and is triggered by IPv6 traffic, an alert is generated but the action is not carried out.

To add, edit, delete, enable, disable, and move event action filters, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the pane, select the virtual sensor in the list for which you want to add event action filters.

Step 4 In the Event Action Rules half of the pane, click the Event Action Filters tab, and then click **Add**.

Step 5 In the Name field, enter a name for the event action filter. A default name is supplied, but you can change it to a more meaningful name.

Step 6 In the Enabled field, click the **Yes** radio button to enable the filter.

Step 7 In the Signature ID field, enter the signature IDs of all signatures to which this filter should be applied. You can use a list (2001, 2004), or a range (2001–2004), or one of the SIG variables you defined on the Event Variables tab. Preface the variable with $.

Step 8 In the SubSignature ID field, enter the subsignature IDs of the subsignatures to which this filter should be applied.

Step 9 In the Attacker IPv4 Address field, enter the IP address of the source host. You can use a variable you defined on the Event Variables tab. Preface the variable with $. You can also enter a range of addresses (for example, 0.0.0.0-255.255.255.255).

Step 10 In the Attacker IPv6 Address field, enter the range set of attacker IPv6 addresses of the source host in the following format:

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>].

The second IPv6 address in the range must be greater than or equal to the first IPv6 address. You can also use a variable you defined on the Event Variables tab. Preface the variable with $.

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Step 11 In the Attacker Port field, enter the port number used by the attacker to send the offending packet.

Step 12 In the Victim IPv4 Address field, enter the IP address of the recipient host. You can use one of the variables if you defined them on the Event Variables tab. Preface the variable with $. You can also enter a range of addresses (for example, 0.0.0.0-255.255.255.255).

Step 13 In the Victim IPv6 Address field, enter the range set of IPv6 address of the recipient host in the following format.

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>].

The second IPv6 address in the range must be greater than or equal to the first IPv6 address. You can use a variable you defined on the Event Variables tab. Preface the variable with $.

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Step 14 In the Victim Port field, enter the port number used by the victim host to receive the offending packet.

Step 15 In the Risk Rating field, enter a risk rating range for this filter. If the risk rating for an event falls within the range you specify, the event is processed against the criteria of this filter.

Step 16 In the Actions to Subtract field, click the note icon to open the Edit Actions dialog box. Check the check boxes of the actions you want this filter to remove from the event.

Tip To choose more than one event action in the list, hold down the **Ctrl** key.

Step 17 In the Active field, click the **Yes** radio button to add this filter to the list so that it takes effect on filtering events.

Step 18 In the OS Relevance drop-down list, choose whether you want to know if the alert is relevant to the operating system that has been identified for the victim.

Step 19 In the Deny Percentage field, enter the percentage of packets to deny for deny attacker features. The default is 100 percent.

Step 20 In the Stop on Match field, click one of the following radio buttons:

a. **Yes**—If you want the Event Action Filters component to stop processing after the actions of this particular filter have been removed. Any remaining filters will not be processed; therefore, no additional actions can be removed from the event.

b. **No**—If you want to continue processing additional filters.

Step 21 In the Comments field, enter any comments that you want to store with this filter, such as the purpose of this filter or why you have configured this filter in a particular way.

Tip To discard your changes and close the Add Event Action Filter dialog box, click **Cancel**.

Step 22 Click **OK**. The new event action filter now appears in the list on the Event Action Filters tab.

Step 23 To edit an existing event action filter, select it in the list, and then click **Edit**.

Step 24 Make any changes needed.

Tip To discard your changes and close the Edit Event Action Filter dialog box, click **Cancel**.

Step 25 Click **OK**. The edited event action filter now appears in the list on the Event Action Filters tab.

Step 26 To delete an event action filter, select it in the list, and then click **Delete**. The event action filter no longer appears in the list on the Event Action Filters tab.

Step 27 To move an event action filter up or down in the list, select it, and then click the **Move Up** or **Move Down** arrow icons.

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

Step 28 Click **Apply** to apply your changes and save the revised configuration.

Configuring IPv4 Target Value Rating

This section describes how to configure IPv4 target value ratings, and contains the following topics:

IPv4 Target Value Rating Tab

Note You must be administrator or operator to add, edit, or delete target value ratings.

You can assign a target value rating to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert. You can assign different target value ratings to different targets. Events with a higher risk rating trigger more severe signature event actions.

IPv4 Target Value Rating Tab Field Definitions

The following fields are found on the IPv4 Target Value Rating tab:

- Target Value Rating (TVR)—Identifies the value assigned to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IP Address—Identifies the IP address of the network asset you want to prioritize with a target value rating.

Add and Edit Target Value Rating Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Target Value Rating dialog boxes:

- Target Value Rating (TVR)—Lets you assign a value to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IPv4 Address(es)—Identifies the IP address of the network asset you want to prioritize with a target value rating.

Adding, Editing, and Deleting IPv4 Target Value Ratings

To add, edit, and delete the IPv4 target value rating for network assets, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure Target Value Ratings.

Step 4 In the Event Action Rules half of the pane, click the IPv4 Target Value Rating tab, and then click **Add**.

Step 5 To assign a target value rating to a new group of assets, follow these steps:

a. From the Target Value Rating (TVR) drop-down list, choose a rating. The values are High, Low, Medium, Mission Critical, or No Value.

b. In the Target IPv4 Address(es) field, enter the IP address of the network asset. To enter a range of IP addresses, enter the lowest address followed by a hyphen and then the highest address in the range. For example: 10.10.2.1-10.10.2.30.

Tip To discard your changes and close the Add Target Value Rating dialog box, click **Cancel**.

Step 6 Click **OK**. The new target value rating for the new asset appears in the list on the IPv4 Target Value Rating tab.

Step 7 To edit an existing target value rating, select it in the list, and then click **Edit**.

Step 8 Make any changes needed.

Tip To discard your changes and close the Edit Target Value Rating dialog box, click **Cancel**.

Step 9 Click **OK**. The edited network asset now appears in the list on the IPv4 Target Value Rating tab.

Step 10 To delete a network asset, select it in the list, and then click **Delete**. The network asset no longer appears in the list on the Ipv4 Target Value Rating tab.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring IPv6 Target Value Rating

This section describes how to configure IPv6 target value ratings, and contains the following topics:

IPv6 Target Value Rating Tab

Note You must be administrator or operator to add, edit, or delete target value ratings.

You can assign a target value rating to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert. You can assign different target value ratings to different targets. Events with a higher risk rating trigger more severe signature event actions.

IPv6 Target Value Rating Tab Field Definitions

The following fields are found on the IPv6 Target Value Rating tab:

- Target Value Rating (TVR)—Identifies the value assigned to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IP Address—Identifies the IP address of the network asset you want to prioritize with a target value rating.

Add and Edit Target Value Rating Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Target Value Rating dialog boxes:

- Target Value Rating (TVR)—Lets you assign a value to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IPv6 Address(es)—Identifies the IPv6 address of the network asset you want to prioritize with a target value rating in the following format:

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  Example—2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888. The second IPv6 address in the range must be greater than or equal to the first IPv6 address.

  Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Adding, Editing, and Deleting IPv6 Target Value Ratings

Note Global correlation inspection and the reputation filtering deny features do not support IPv6 addresses. For global correlation inspection, the sensor does not receive or process reputation data for IPv6 addresses. The risk rating for IPv6 addresses is not modified for global correlation inspection. Similarly, network participation does not include event data for attacks from IPv6 addresses. And finally, IPv6 addresses do not appear in the deny list.

Note Rate limiting and blocking are not supported for IPv6 traffic. If a signature is configured with a block or rate limit event action and is triggered by IPv6 traffic, an alert is generated but the action is not carried out.

To add, edit, and delete the IPv6 target value rating for network assets, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure Target Value Ratings.

Step 4 In the Event Action Rules half of the pane, click the IPv6 Target Value Rating tab, and then click **Add**.

Step 5 To assign a target value rating to a new group of assets, follow these steps:

a. From the Target Value Rating (TVR) drop-down list, choose a rating. The values are High, Low, Medium, Mission Critical, or No Value.

b. In the Target IPv6 Address(es) field, enter the IP address of the network asset.

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>].

You can also use a variable you defined on the Event Variables tab. Preface the variable with $. The second IPv6 address in the range must be greater than or equal to the first IPv6 address.

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Tip To discard your changes and close the Add Target Value Rating dialog box, click **Cancel**.

Step 6 Click **OK**. The new target value rating for the new asset appears in the list on the IPv6 Target Value Rating tab.

Step 7 To edit an existing target value rating, select it in the list, and then click **Edit**.

Step 8 Make any changes needed.

Tip To discard your changes and close the Edit Target Value Rating dialog box, click **Cancel**.

Step 9 Click **OK**. The edited network asset now appears in the list on the IPv6 Target Value Rating tab.

Step 10 To delete a network asset, select it in the list, and then click **Delete**. The network asset no longer appears in the list on the IPv6 Target Value Rating tab.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring OS Identifications

This section describes how to configure OS maps, and contains the following topics:

Understanding Passive OS Fingerprinting

Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK packets exchanged on the network to determine the OS type.

The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk rating of the alert for the attack and/or the sensor may filter the alert for the attack. You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the victim OS, the source of the OS identification, and the relevance to the victim OS in the alert.

Passive OS fingerprinting consists of three components:

- Passive OS learning—Passive OS learning occurs as the sensor observes traffic on the network. Based on the characteristics of TCP SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address.
- User-configurable OS identification—You can configure OS host maps, which take precedence over learned OS maps.

- Computation of attack relevance rating and risk rating—The sensor uses OS information to determine the relevance of the attack signature to the targeted host. The attack relevance is the attack relevance rating component of the risk rating value for the attack alert. The sensor uses the OS type reported in the host posture information imported from the CSA MC to compute the attack relevance rating.

There are three sources of OS information. The sensor ranks the sources of OS information in the following order:

1. Configured OS maps—OS maps you enter. Configured OS maps reside in the event action rules policy and can apply to one or many virtual sensors.

   Note You can specify multiple operating systems for the same IP address. The last one in the list is the operating system that is matched.

2. Imported OS maps—OS maps imported from an external data source. Imported OS maps are global and apply to all virtual sensors.

   Note Currently the CSA MC is the only external data source.

3. Learned OS maps—OS maps observed by the sensor through the fingerprinting of TCP packets with the SYN control bit set. Learned OS maps are local to the virtual sensor that sees the traffic.

When the sensor needs to determine the OS for a target IP address, it consults the configured OS maps. If the target IP address is not in the configured OS maps, the sensor looks in the imported OS maps. If the target IP address is not in the imported OS maps, the sensor looks in the learned OS maps. If it cannot find it there, the sensor treats the OS of the target IP address as unknown.

Note Passive OS fingerprinting is enabled by default and the IPS contains a default vulnerable OS list for each signature.

Configuring Passive OS Fingerprinting

You do not have to configure passive OS fingerprinting for it to function. IPS provides a default vulnerable OS list for each signature and passive analysis is enabled by default.

You can configure the following aspects of passive OS fingerprinting:

- Define OS maps—We recommend configuring OS maps to define the identity of the OS running on critical systems. It is best to configure OS maps when the OS and IP address of the critical systems are unlikely to change.
- Limit the attack relevance rating calculation to a specific IP address range—This limits the attack relevance rating calculations to IP addresses on the protected network.
- Import OS maps—Importing OS maps provides a mechanism for accelerating the learning rate and fidelity of the OS identifications made through passive analysis. If you have an external product interface, such as the CSA MC, you can import OS identifications from it.
- Define event action rules filters using the OS relevance value of the target—This provides a way to filter alerts solely on OS relevance.
- Disable passive analysis—Stops the sensor from learning new OS maps.

- Edit signature vulnerable OS lists—The vulnerable OS list specifies what OS types are vulnerable to each signature. The default, General OS, applies to all signatures that do not specify a vulnerable OS list.

OS Identifications Tab

Note You must be administrator or operator to add, edit, and delete configured OS maps.

Use the OS Identifications tab to configure OS host maps, which take precedence over learned OS maps. On the OS Identifications tab you can add, edit, and delete configured OS maps. You can move them up and down in the list to change the order in which the sensor computes the attack relevance rating and risk rating for that particular IP address and OS type combination.

You can also move OS maps up and down in the list to change the order in which the sensor resolves the OS associated with a particular IP address. Configured OS maps allow for ranges. More specific maps should be at the beginning of the list. Overlap in the IP address range sets is allowed, but the entry closest to the beginning of the list takes precedence. For example, for network 192.168.1.0/24 an administrator might define the following (Table 8-1):

Table 8-1 Example Configured OS Maps

IP Address Range Set	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10,192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

OS Identifications Tab Field Definitions

The following fields are found on the OS Identifications tab:

- Enable passive OS fingerprinting analysis—When checked, lets the sensor perform passive OS analysis.
- Restrict Attack Relevance Ratings (ARR) to these IP addresses—Lets you configure the mapping of OS type to a specific IP address and have the sensor calculate the attack relevance rating for that IP address.
- Configured OS Maps—Displays the attributes of the configured OS maps:
  - Name—Specifies the name you give the configured OS map.
  - Active—Whether this configured OS map is active or inactive.
  - IP Address—Specifies the IP address of this configured OS map.
  - OS Type—Specifies the OS type of this configured OS map.

Add and Edit Configured OS Map Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Configured OS Map dialog boxes:

- Name—Specifies the name of this configured OS map.
- Active—Lets you choose to make the configured OS map active or inactive.
- IP Address—Specifies the IP address associated with this configured OS map. The IP address for configured OS maps (and *only* configured OS maps) can be a set of IP addresses and IP address ranges. The following are all valid IP address values for configured OS maps:
  - 10.1.1.1,10.1.1.2,10.1.1.15
  - 10.1.2.1
  - 10.1.1.1-10.2.1.1,10.3.1.1
  - 10.1.1.1-10.1.1.5
- OS Type—Lets you choose one of the following OS types to associate with the IP address:
  - AIX
  - BSD
  - General OS
  - HP UX
  - IOS
  - IRIX
  - Linux
  - Mac OS
  - Netware
  - Other
  - Solaris
  - UNIX
  - Unknown OS
  - Win NT
  - Windows
  - Windows NT/2K/XP

Adding, Editing, Deleting, and Moving Configured OS Maps

To add, edit, delete, and move configured OS maps, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure OS identifications.

Step 4 In the Event Action Rules half of the pane, click the OS Identifications tab, and then click **Add**.

Step 5 In the Name field, enter a name for the configured OS map.

Step 6 In the Active field, click the **Yes** radio button to add this configured OS map to the list so that it takes effect.

Step 7 In the IP Address field, enter the IP address of the host that you are mapping to an OS. For example, use this format, 10.10.5.5,10.10.2.1-10.10.2.30.

Step 8 From the OS Type drop-down list, choose the OS that will be mapped to the IP address.

Tip To discard your changes and close the Add Configured OS Map dialog box, click **Cancel**.

Step 9 Click **OK**. The new configured OS map now appears in the list on the OS Identifications tab.

Step 10 Check the **Enable passive OS fingerprinting analysis** check box.

Note You must check the **Enable passive OS fingerprinting analysis** check box on the OS Identifications tab or none of the configured OS maps will be enabled regardless of the value you set in the Add Configured OS Map dialog box.

Step 11 To edit a configured OS map, select it in the list, and then click **Edit**.

Step 12 Make any changes needed.

Tip To discard your changes and close the Edit Configured OS Map dialog box, click **Cancel**.

Step 13 Click **OK**. The edited configured OS map now appears in the list on the OS Identifications tab.

Step 14 Check the **Enable passive OS fingerprinting analysis** check box.

Note You must check the **Enable passive OS fingerprinting analysis** check box on the OS Identifications tab or none of the configured OS maps will be enabled regardless of the value you set in the Edit Configured OS Map dialog box.

Step 15 To delete a configured OS map, select it in the list, and then click **Delete**. The configured OS map no longer appears in the list on the OS Identifications tab.

Step 16 To move a configured OS map up or down in the list, select it, and then click the **Move Up** or **Move Down** arrows.

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

Step 17 Click **Apply** to apply your changes and save the revised configuration.

Configuring Event Variables

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

Event Variables Tab

Note You must be administrator or operator to add, edit, or delete event variables.

You can create event variables and then use those variables in event action filters. When you want to use the same value within multiple filters, use a variable. When you change the value of the variable, any filter that uses that variable is updated with the new value.

Note You must preface the event variable with a dollar ($) sign to indicate that you are using a variable rather than a string.

Some variables cannot be deleted because they are necessary to the signature system. If a variable is protected, you cannot select it to edit it. You receive an error message if you try to delete protected variables. You can edit only one variable at a time.

IPv4 Addresses

When configuring IPv4 addresses, specify the full IP address or ranges or set of ranges:

- 192.0.2.3-192.0.2.26
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 192.0.2.3-192.0.2.26

IPv6 Addresses

When configuring IPv6 addresses, use the following format:

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Timesaver If you have an IP address space that applies to your engineering group and there are no Windows systems in that group, and you are not worried about any Windows-based attacks to that group, you could set up a variable to be the IP address space of the engineering group. You could then use this variable to configure a filter that would ignore all Windows-based attacks for this group.

Event Variables Tab Field Definitions

The following fields are found on the Event Variables tab:

- Name—Lets you assign a name to this variable.
- Type—Identifies the variable as an address.
- Value—Lets you add the value(s) represented by this variable.

Add and Edit Event Variable Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Event Variable dialog boxes:

- Name—Lets you assign a name to this variable.
- Type—Identifies the variable as an IPv4 or IPv6 address:
  - address—For IPv4 address use a full IP address or range or set of ranges.
  - ipv6-address—For IPv6 address use the following format: <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

    Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

- Value—Lets you add the value(s) represented by this variable.

Adding, Editing, and Deleting Event Variables

Note Global correlation inspection and the reputation filtering deny features do not support IPv6 addresses. For global correlation inspection, the sensor does not receive or process reputation data for IPv6 addresses. The risk rating for IPv6 addresses is not modified for global correlation inspection. Similarly, network participation does not include event data for attacks from IPv6 addresses. And finally, IPv6 addresses do not appear in the deny list.

Note Rate limiting and blocking are not supported for IPv6 traffic. If a signature is configured with a block or rate limit event action and is triggered by IPv6 traffic, an alert is generated but the action is not carried out.

To add, edit, and delete event variables, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure event variables.

Step 4 In the Event Action Rules half of the pane, click the Event Variables tab, and then click **Add**.

Step 5 In the Name field, enter a name for this variable.

Note A valid name can only contain numbers or letters. You can also use a hyphen (-) or an underscore (_).

Step 6 From the Type drop-down list, choose **address** for an IPv4 address or **ipv6-address** for an IPv6 address.

Step 7 In the Value field, enter the values for this variable.

For IPv4 addresses, specify the full IP address or ranges or set of ranges. For example:

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255

Note You can use commas as delimiters. Make sure there are no trailing spaces after the comma. Otherwise, you receive a `Validation failed` error.

For IPv6 address, use the following format:

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Tip To discard your changes and close the Add Event Variable dialog box, click **Cancel**.

Step 8 Click **OK**. The new variable appears in the list on the Event Variables tab.

Step 9 To edit an existing variable, select it in the list, and then click **Edit**.

Step 10 Make any changes needed.

Tip To discard your changes and close the Edit Event Variable dialog box, click **Cancel**.

Step 11 Click **OK**. The edited event variable now appears in the list on the Event Variables tab.

Step 12 To delete an event variable, select it in the list, and then click **Delete**. The event variable no longer appears in the list on the Event Variables tab.

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

Step 13 Click **Apply** to apply your changes and save the revised configuration.

Configuring Risk Category

This section describes how to configure them risk categories, and contains the following topics:

Risk Category Tab

Note You must be administrator to add and edit risk levels.

On the Risk Category tab, you can use predefined risk categories (HIGHRISK, MEDIUMRISK, AND LOWRISK) or you can define your own labels. Risk categories link a category name to a numeric range defining the risk rating. You specify the low threshold for the category to make sure that the ranges are contiguous. The upper category is either the next higher category or 100.

Note You cannot delete a predefined risk category.

Risk Category Tab Field Definitions

The following fields are found on the Risk Category tab:

- Risk Category Name—Specifies the name of this risk level. The predefined categories have the following values:
  - HIGHRISK—90 (means 90 to 100)
  - MEDIUMRISK—70 (means 70-89)
  - LOWRISK—1 (means 1-69)

- Risk Threshold—Specifies the threshold number for this risk. The value is a number from 0 to 100.
- Risk Range—Specifies the risk rating range for this risk category. The risk rating is a range between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.

Add and Edit Risk Level Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Risk Level dialog boxes:

- Risk Name—Specifies the name of this risk level.
- Risk Threshold—Lets you assign a risk threshold for this risk level. You specify or change only the lower threshold for the category so that the risk categories are contiguous. The upper threshold is either the next higher category or 100.
- Active—Lets you make this risk level active.

Adding, Editing, and Deleting Risk Categories

To add, edit, and delete risk categories, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure risk categories.

Step 4 In the Event Action Rules half of the pane, click the Risk Category tab, and then click **Add**.

Step 5 In the Risk Name field, enter a name for this risk category.

Step 6 In the Risk Threshold field, enter a numerical value for the risk threshold (minimum 0, maximum 100). This number represents the lower boundary of risk. The range appears in the Risk Range field and in the red, yellow, and green threshold fields.

Step 7 To make this risk category active, click the **Yes** radio button.

Tip To discard your changes and close the Add Risk Category dialog box, click **Cancel**.

Step 8 Click **OK**. The new risk category appears in the list on the Risk Category tab.

Step 9 To edit an existing risk category, select it in the list, and then click **Edit**.

Step 10 Make any changes needed.

Tip To discard your changes and close the Edit Risk Category dialog box, click **Cancel**.

Step 11 Click **OK**. The edited risk category now appears in the list on the Risk Category tab.

Step 12 To delete a risk category, select it in the list, and then click **Delete**. The risk category no longer appears in the list on the Risk Category tab.

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

Step 13 Click **Apply** to apply your changes and save the revised configuration.

Configuring Threat Category

Note You must be administrator to configure threat categories.

On the Threat Category tab, you can group threats in red, yellow, and green categories. These red, yellow, and green threshold statistics are used in event action overrides and are also shown in the Network Security Gadget on the Home page.

The red, yellow, and green threshold statistics represent the state of network security with red being the most critical. If you change a threshold, any event action overrides that had the same range as the risk category are changed to reflect the new range. The new category is inserted in to the Risk Category list according to its threshold value and is automatically assigned actions that cover its range.

Field Definitions

The following fields are found on the Threat Category tab:

- Threat Category Thresholds—Lists the numbers for the red, yellow, and green thresholds. The health statistics for network security use these thresholds to determine what level the network security is at (critical, needs attention, or normal). The overall network security value represents the least secure value (green is the most secure and red is the least secure). These color thresholds refer to the Sensor Health gadget on the Home pane:
  - Red Threat Threshold—Sets the red threat threshold. The default is 90.
  - Yellow Threat Threshold—Sets the yellow threat threshold. The default is 70.
  - Green Threat Threshold—Sets the green threat threshold. The default is 1.

For More Information

- For detailed information about the Network Security Gadget, see Network Security Gadget, page 3-8.
- For detailed information about risk category, see Configuring Risk Category, page 8-36.

Configuring General Settings

This section describes how to configure the general settings, and contains the following topics:

General Tab

Note You must be administrator or operator to configure the general settings for event action rules.

You can configure the general settings that apply globally to event action rules, such as whether you want to use the Summarizer and the Meta Event Generator. The Summarizer groups events into a single alert, thus decreasing the number of alerts the sensor sends out. The Meta Event Generator processes the component events, which lets the sensor watch for suspicious activity transpiring over a series of events.

Caution Do not disable the Summarizer or Meta Event Generator except for troubleshooting purposes. If you disable the Summarizer, every signature is set to Fire All with no summarization. If you disable the Meta Event Generator, all Meta engine signatures are disabled.

You can also use threat rating adjustment, event action filters, and you can enable one-way TCP reset. The one-way TCP reset operates for inline mode only and is an automatic addition to the deny packet inline actions. It sends a TCP reset to the victim of the alert, thus creating a black hole for the attacker and clearing the TCP resources of the victim.

Note An inline sensor now denies packets for any alert with a risk rating of greater than or equal to 90. It also issues a one-way TCP reset on TCP alerts with a risk rating of greater than or equal to 90.

You can configure how long you want to deny attackers, the maximum number of denied attackers, and how long you want blocks to last.

General Tab Field Definitions

The following fields are found the on the General tab:

- Use Summarizer—Enables the Summarizer component. By default, the Summarizer is enabled. If you disable it, all signatures are set to Fire All with no summarization. If you configure individual signatures to summarize, this configuration will be ignored if the Summarizer is not enabled.
- Use Meta Event Generator—Enables the Meta Event Generator. By default, the Meta Event Generator is enabled. If you disable the Meta Event Generator, all Meta engine signatures are disabled.
- Use Threat Rating Adjustment—Enables threat rating adjustment, which adjusts the risk rating. If disabled, then risk rating is equal to threat rating. Use Event Action Filters—Enables the event action filter component. You must check this check box to use any filter that is enabled.
- Enable One Way TCP Reset (inline only)—Enables a one-way TCP reset for deny packet inline actions for TCP-based alerts. It sends a TCP reset to the victim of the alert thus clearing the TCP resources of the victim.
- Deny Attacker Duration—Specifies the number of seconds to deny the attacker inline. The valid range is 0 to 518400. The default is 3600.
- Block Action Duration—Specifies the number of minutes to block a host or connection. The valid range is 0 to 10000000. The default is 30.
- Maximum Denied Attackers—Specifies the limit of the number of denied attackers possible in the system at any one time. The valid range is 0 to 100000000. The default is 10000.

Configuring the General Settings

Caution The general settings options operate at a global level, so enabling them affects all sensor processing of these features.

To configure the general settings for event action rules, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Policies > IPS Policies**.

Step 3 Choose **Configuration >** ***sensor_name*** **> Policies > IPS Policies**.

Step 4 In the top half of the IPS Policies pane, select the virtual sensor for which you want to configure general categories.

Step 5 In the Event Action Rules half of the pane, click the General tab.

Step 6 To enable the summarizer feature, check the **Use Summarizer** check box.

Caution Disable the Summarizer for troubleshooting purposes only. Otherwise, make sure the Summarizer is enabled so that all signatures you configure for summarization will actually summarize.

Step 7 To enable the meta event generator, check the **Use Meta Event Generator** check box.

Caution Disable the Meta Event Generator for troubleshooting purposes only. Otherwise, make sure the Meta Event Generator is enabled so that all Meta engine signatures are functional.

Step 8 To enable threat rating adjustment, check the **Use Threat Rating Adjustment** check box.

Step 9 To enable event action filters, check the **Use Event Action Filters** check box.

Note You must check the Use Event Action Filters check box on the General pane so that any event action filters you configured in the **Configuration >** ***sensor_name*** **> Policies > IPS Policies > Event Action Filters** pane are active.

Step 10 To enable one way TCP reset for deny packet inline actions, check the **Enable One Way TCP Reset** check box.

Step 11 In the Deny Attacker Duration field, enter the number of seconds you want to deny the attacker inline.

Step 12 In the Block Action Duration field, enter the number of minutes you want to block a host or connection.

Step 13 In the Maximum Denied Attackers field, enter the maximum number of denied attackers you want at any one time.

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

Step 14 Click **Apply** to apply your changes and save the revised configuration.

Configuring Shared Policies and Group Policies

This chapter describes how to configure and deploy shared policies to multiple sensors and how to group policies for sharing. It contains the following sections:

Configuring Shared Policies

This section describes shared policies and how to configure and deploy them. It contains the following topics:

Understanding Shared Policies

You can configure and deploy shared policies to multiple sensors. Currently only the global correlation policy can be shared. It consists of the inspection/reputation and network participation components. You can create and delete policies from any configuration pane in the IME by clicking **Add Policy** or **Delete Policy** in the upper right corner of the IME.

Shared policies are based on sensor version, not component version. You can use the current configuration of a sensor, another policy, or a template as the source for a new policy. When you use the current configuration of a sensor, the initial current configuration for the policy is taken from the sensor current configuration. When you use another policy as the basis for a new policy, the new policy is a clone of the source policy except for the new name. A template is the default configuration associated with a specified IPS version. You can select a template from any of the sensor versions managed by the IME. For example, if the IME is managing 7.0(2) and 7.0(4) sensors, you can select either of these versions, but IPS 7.0(3) is not an available selection. Only a sensor version can be used as a source template—actual sensors and existing policies may not be used.

After a policy has been created, it does not retain any connection to its source. For example, if you create a policy from a sensor configuration and that sensor configuration is later modified or even if the sensor is deleted, it has no effect on the policy.

Policy Sharing Restrictions

Pay attention to the following when configuring policy sharing:

- You can define up to ten shared policies at any given time.
- Since global correlation was introduced in IPS 7.0, only sensor versions 7.0 and later can be used as a policy source or deployment target.
- At least one sensor or policy must be configured on the IME for a policy to be created.
- Policy names must be less than 64 characters in length.
- Policy names cannot contain characters restricted by Windows (<>^*?":).
- Policy names cannot contain names restricted by Windows (con. nul. aux. prn, etc.).
- New policy names cannot match existing sensor, policy, or policy group names.
- New policy group names cannot match existing sensor or policy names.
- New sensor names cannot match existing sensor, policy, or policy group names.
- No sensor or policy can be named 'Policy Groups,' because this name uniquely identifies the Policy Group tab.

For More Information

For detailed information about global correlation, see Chapter 14, "Configuring Global Correlation."

Add Policy Field Definitions

The following fields are found in the Add Policy dialog box:

- New Policy Name—Specifies the name of the new shared policy.
- Initialize Policy From—Specifies which source you will use for the shared policy.
  - A Device Configuration—Specifies that the policy will be based on a sensor current configuration.
  - Another Policy—Specifies that the policy will be a clone of an existing policy.
  - A Version Template—Specifies that the policy will be a template of a default configuration associated with a specified IPS version.
- Select Source Sensor/Policy/Version—Specifies the sensor, policy, or version that you are choosing from which to initialize the policy.
- The New Policy Will Include These Components—Shows the global correlation components that are a part of this shared policy.

Adding and Deleting Shared Policies

To add and delete shared policies, follow these steps:

Step 1 From the IME, choose **Configuration > Add Policy**. The Add Policy dialog box appears.

Note You can configure shared policies from any configuration pane in the IME.

Step 2 In the New Policy Name field, enter a name for the new policy.

Step 3 Under Initialize Policy From, choose one of the following:

- A Device Configuration
- Another Policy
- A Version Template

Step 4 From the Select Source Sensor drop-down menu, choose the sensor, the policy, or the version that you are applying the policy to.

Step 5 Under The New Policy Will Include These Subcomponents, check the checkboxes of the global correlation components you want to include, and the click **OK**. A tab with the new policy name appears.

Step 6 Select the new policy tab and configure inspection/reputation and network reputation.

Step 7 To delete a shared policy, select the policy tab that you want to delete and click **Delete Policy**. The Delete Policy dialog box appears asking if you are sure you want to delete this policy. Click **Yes** to delete it. The tab is deleted.

For More Information

For detailed information about global correlation, see Chapter 14, "Configuring Global Correlation."

Deploying Shared Policies

To deploy shared policies, follow these steps:

Step 1 From the IME, choose **Configuration >** *shared_policy_name* **> Deployment > Deployment Management > deployment**.

Step 2 Under Select From the Following Sensors and Policy Groups for Deployment, check the checkboxes for the sensors and policy groups that you want to deploy.

Step 3 Under Select From the Following Components for Deployment, since there is currently only one shared policy, global correlation, you accept both inspection/reputation and network participation, or uncheck one of those components and just use one.

Step 4 Click **Apply** and then **Deploy**. The Policy Deployment Results dialog box appears stating the results of the deployment and displays reasons for successful or unsuccessful deployment.

Note If the configuration on the sensor is different than the policy being deployed, you receive a warning that the configuration will be overwritten. You must click **OK** for deployment to proceed. If you do not want to receive this message again, you can disable it in **Tools > Policy Deploy Warning**. If the configuration on the sensor is the same as the policy, the policy is not deployed, and you receive no warning.

For More Information

For detailed information about global correlation, see Chapter 14, "Configuring Global Correlation."

Configuring Policy Groups

You can group multiple sensors for shared policy deployment. Policy groups are only used for shared policy deployment. You create a tree hierarchy of named groups. When you add a sensor to the IME, it is immediately available for insertion into the policy group tree. When you remove a sensor in a group from the IME, it remains in the policy group until you remove it manually. However, no deployment for that sensor can occur until you add it again to the IME.

Pay attention to the following when creating policy groups:

- A group can contain child groups and sensors, but sensors cannot contain children.
- A group or sensor node can only have one parent.
- A group name cannot match any sensor name.
- No matter how many times a sensor happens to appear in various deployed groups, at most one deployment to that sensor can happen.

To manage group policies, follow these steps:

Step 1 From the IME, choose **Configuration > Policy Groups > Group Management > Groups**.

Step 2 Click **Add Group** to add a new group, and in the Enter New Group Name field, enter a name for the new group.

Step 3 Select the new group name and click **Add Sensors** to add sensors to this policy group, The Add Sensors dialog box appears.

Step 4 Under Select From the Following Sensors, check the checkboxes of the sensor(s) you want to include, and then click **OK**. The selected sensor(s) appear under the new policy group.

Step 5 To copy a policy group, select it, click **Copy**, and then click **Paste**. The copied policy group and sensor(s) appear under the selected policy group.

Step 6 To rename a policy group, select it, and then click **Rename**. The Rename Group dialog box appears.

Step 7 In the Enter New Group Name field, enter the new name.

Step 8 To delete a policy group, select it, and then click **Delete**. The policy group is immediately deleted.

Step 9 Click **Move Up** and **Move Down** to rearrange items in the Policy Groups tree.

Step 10 To save your changes, click **Apply**.

Defining Signatures

This chapter explains how to create signature definition policies and how to configure signatures. It contains the following sections:

Understanding Security Policies

Note You must be administrator or operator to add, clone, or delete signature policies.

You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies. The use of multiple security policies lets you create security policies based on different requirements and then apply these customized policies per VLAN or physical interface.

Understanding Signatures

Attacks or other misuses of network resources can be defined as network intrusions. Sensors that use a signature-based technology can detect network intrusions. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as DoS attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define.

The sensor compares the list of signatures with network activity. When a match is found, the sensor takes an action, such as logging the event or sending an alert. Sensors let you modify existing signatures and define new ones.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. 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 tuning your signatures.

To configure a sensor to monitor network traffic for a particular signature, you must enable the signature. By default, the most critical signatures are enabled when you install the signature update. When an attack is detected that matches an enabled signature, the sensor generates an alert, which is stored in the Event Store of the sensor. The alerts, as well as other events, may be retrieved from the Event Store by web-based clients. By default the sensor logs all Informational alerts or higher.

Some signatures have subsignatures, that is, the signature is divided into subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature. For example, if you edit signature 3050 subsignature 1 and change the severity, the severity change applies to only subsignature 1 and not to 3050 2, 3050 3, and 3050 4.

The Cisco IPS contains over 10,000 built-in default signatures. You cannot rename or delete signatures from the list of built-in signatures, but you can retire signatures to remove them from the sensing engine. You can later activate retired signatures; however, this process requires the sensing engines to rebuild their configuration, which takes time and could delay the processing of traffic. You can tune built-in signatures by adjusting several signature parameters. Built-in signatures that have been modified are called tuned signatures.

Note We recommend that you retire any signatures that you are not using. This improves sensor performance.

You can create signatures, which are called custom signatures. Custom signature IDs begin at 60000. You can configure them for several things, such as matching of strings on UDP connections, tracking of network floods, and scans. Each signature is created using a signature engine specifically designed for the type of traffic being monitored.

Event Actions

The Cisco IPS supports the following event actions. Most of the event actions belong to each signature engine unless they are not appropriate for that particular engine.

Alert and Log Actions

- Product Alert—Writes the event to the Event Store as an alert.

Note The Product Alert action is not automatic when you enable alerts for a signature. To have an alert created in the Event Store, you must select Product Alert. If you add a second action, you must include Product Alert if you want an alert sent to the Event Store. Also, every time you configure the event actions, a new list is created and it replaces the old list. Make sure you include all the event actions you need for each signature.

Note There are other event actions that force a Product Alert. These actions use Product Alert as the vehicle for performing the action. Even if Product Alert is not selected or is filtered, the alert is still produced. The actions are the following: Produce Verbose Alert, Request SNMP Trap, Log Attacker Packets, Log Victim Packets, and Log Pair Packets.

Note A Produce Alert event action is added for an event when global correlation has increased the risk rating of an event, and has added either the Deny Packet Inline or Deny Attacker Inline event action.

- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Attacker Packets—Starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Victim Packets—Starts IP logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Pair Packets—Starts IP logging on packets that contain the attacker/victim address pair. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Request SNMP Trap—Sends a request to the Notification Application component of the sensor to perform SNMP notification. This action causes an alert to be written to the Event Store, even if Product Alert is not selected. You must have SNMP configured on the sensor to implement this action.

Deny Actions

- Deny Packet Inline (inline only)—Terminates the packet.

Note You cannot delete the event action override for Deny Packet Inline because it is protected. If you do not want to use that override, disable it.

- Deny Connection Inline (inline only)—Terminates the current packet and future packets on this TCP flow.
- Deny Attacker Victim Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.

Note For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > General Settings**.

- Deny Attacker Service Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
- Deny Attacker Inline (inline only)—Terminates the current packet and future packets from this attacker address for a specified period of time.

- The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.

  Note This is the most severe of the deny actions. It denies current and future packets from a single attacker address. To clear all denied attacker entries, choose **Configuration > *sensor_name* > Sensor Management > Time-Based Actions > Denied Attackers > Clear List**, which permits the addresses back on the network.

- Modify Packet Inline (inline only)—Modifies packet data to remove ambiguity about what the end point might do with the packet.

  Note You cannot use Modify Packet Inline as an action when adding event action filters or overrides.

Other Actions

- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action.

  Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

  Note IPv6 does not support Request Block Connection.

- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action.

  Note IPv6 does not support Request Block Host.

  Note For block actions, to set the duration of the block, choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > General Settings**.

- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action.

  Note Request Rate Limit applies to a select set of signatures.

  Note IPv6 does not support Request Rate Limit.

- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

Understanding Deny Packet Inline

For signatures that have Deny Packet Inline configured as an action or for an event action override that adds Deny Packet Inline as an action, the following actions may be taken:

- Dropped Packet
- Denied Flow
- TCP One Way Reset Sent TCP

The Deny Packet Inline action is represented as a dropped packet action in the alert. When a Deny Packet Inline occurs for a TCP connection, it is automatically upgraded to a Deny Connection Inline action and seen as a denied flow in the alert. If the IPS denies just one packet, the TCP continues to try to send that same packet again and again, so the IPS denies the entire connection to ensure it never succeeds with the resends.

When a Deny Connection Inline occurs, the IPS also automatically sends a TCP one-way reset, which shows up as a TCP one-way reset sent in the alert. When the IPS denies the connection, it leaves an open connection on both the client (generally the attacker) and the server (generally the victim). Too many open connections can result in resource problems on the victim. So the IPS sends a TCP reset to the victim to close the connection on the victim side (usually the server), which conserves the resources of the victim. It also prevents a failover that would otherwise allow the connection to fail over to a different network path and reach the victim. The IPS leaves the attacker side open and denies all traffic from it.

TCP Reset Differences Between IPS Appliances and ASA IPS Modules

The IPS appliance sends TCP reset packets to both the attacker and victim when Reset TCP Connection is selected. The IPS appliance sends a TCP reset packet only to the victim under the following circumstances:

- When a Deny Packet Inline or Deny Connection Inline is selected
- When TCP-based signatures and Reset TCP Connection have NOT been selected

In the case of the ASA IPS modules, the TCP reset request is sent to the ASA, and then the ASA sends the TCP reset packets. The ASA sends TCP reset packets to both the attacker and victim when the Reset TCP Connection is selected. When Deny Packet Inline or Deny Connection Inline is selected, the ASA sends the TCP reset packet to either the attacker or victim depending on the configuration of the signature. Signatures configured to swap the attacker and victim when reporting the alert can cause the ASA to send the TCP reset packet to the attacker.

TCP Normalizer Signature Warning

You receive the following warning if you disable a default-enabled TCP Normalizer signature or remove a default-enabled modify packet inline, deny packet inline, or deny connection inline action:

```
Use caution when disabling, retiring, or changing the event action settings of a <Sig ID>
TCP Normalizer signature for a sensor operating in IPS mode. The TCP Normalizer signature
default values are essential for proper operation of the sensor.
If the sensor is seeing duplicate packets, consider assigning the traffic to multiple
virtual sensors. If you are having problems with asymmetric or out-of-order TCP packets,
consider changing the normalizer mode from strict evasion protection to asymmetric mode
protection. Contact Cisco TAC if you require further assistance.
```

Signature Engines

A signature engine is a component of the Cisco IPS that is designed to support many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of parameters that have allowable ranges or sets of values.

Note The Cisco IPS engines support a standardized Regex.

Cisco IPS contains the following signature engines:

- AIC—Provides thorough analysis of web traffic. The AIC engine provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications, such as instant messaging and gotomypc, that try to tunnel over specified ports. You can also use AIC to inspect FTP traffic and control the commands being issued. There are two AIC engines: AIC FTP and AIC HTTP.
- Atomic—The Atomic engines are combined into four engines with multi-level selections. You can combine Layer 3 and Layer 4 attributes within one signature, for example IP + TCP. The Atomic engine uses the standardized Regex support. The Atomic engines consist of the following types:
  - Atomic ARP—Inspects Layer 2 ARP protocol. The Atomic ARP engine is different because most engines are based on Layer 3 IP protocol.
  - Atomic IP Advanced—Inspects IPv6 Layer 3 and ICMPv6 Layer 4 traffic.
  - Atomic IP—Inspects IP protocol packets and associated Layer 4 transport protocols. This engine lets you specify values to match for fields in the IP and Layer 4 headers, and lets you use Regex to inspect Layer 4 payloads.

    Note All IP packets are inspected by the Atomic IP engine. This engine replaces the 4.x Atomic ICMP, Atomic IP Options, Atomic L3 IP, Atomic TCP, and Atomic UDP engines.

  - Atomic IPv6—Detects two IOS vulnerabilities that are stimulated by malformed IPv6 traffic.
- Fixed—Performs parallel regular expression matches up to a fixed depth, then stops inspection using a single regular expression table. There are three Fixed engines: ICMP, TCP, and UDP.
- Flood—Detects ICMP and UDP floods directed at hosts and networks. There are two Flood engines: Flood Host and Flood Net.
- Meta—Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.
- Multi String—Inspects Layer 4 transport protocols and payloads by matching several strings for one signature. This engine inspects stream-based TCP and single UDP and ICMP packets.
- Normalizer—Configures how the IP and TCP Normalizer functions and provides configuration for signature events related to the IP and TCP Normalizer. Allows you to enforce RFC compliance.
- Service—Deals with specific protocols. The Service engines are divided in to the following protocol types:
  - DNS—Inspects DNS (TCP and UDP) traffic.
  - FTP—Inspects FTP traffic.

- FTP V2—Supports IOS IPS. This signature engine provides a protocol decode engine tuned for IOS IPS. If you try to use this engine, you receive an error message.
- Generic—Decodes custom service and payload, and generically analyzes network protocols.
- H225—Inspects VoIP traffic. Helps the network administrator make sure the SETUP message coming in to the VoIP network is valid and within the bounds that the policies describe. Is also helps make sure the addresses and Q.931 string fields such as url-ids, email-ids, and display information adhere to specific lengths and do not contain possible attack patterns.
- HTTP—Inspects HTTP traffic. The WEBPORTS variable defines inspection port for HTTP traffic.
- HTTP V2—Supports IOS IPS. This signature engine provides a protocol decode engine tuned for IOS IPS. If you try to use this engine, you receive an error message.
- IDENT—Inspects IDENT (client and server) traffic.
- MSRPC—Inspects MSRPC traffic.
- MSSQL—Inspects Microsoft SQL traffic.
- NTP—Inspects NTP traffic.
- P2P—Inspects P2P traffic.
- RPC—Inspects RPC traffic.
- SMB Advanced—Processes Microsoft SMB and Microsoft DCE/RPC (MSRPC) over SMB packets.

Note The SMB engine has been replaced by the SMB Advanced engine. Even though the SMB engine is still visible in IDM, IME, and the CLI, its signatures have been obsoleted; that is, the new signatures have the obsoletes parameter set with the IDs of their corresponding old signatures. Use the new SMB Advanced engine to rewrite any custom signature that were in the SMB engine.

- SMPT V1—Supports IOS IPS.

  This signature engine provides a protocol decode engine tuned for IOS IPS. If you try to use this engine, you receive an error message.
- SNMP—Inspects SNMP traffic.
- SSH—Inspects SSH traffic.
- TNS—Inspects TNS traffic.

- State—Conducts stateful searches of strings in protocols such as SMTP. The state engine has a hidden configuration file that is used to define the state transitions so new state definitions can be delivered in a signature update.
- String—Searches on Regex strings based on ICMP, TCP, or UDP protocol. There are three String engines: String ICMP, String TCP, and String UDP.
- String XL—Searches on Regex strings based on ICMP, TCP, or UDP protocol.The String XL engines provide optimized operation for the Regex accelerator card. There are three String engines: String ICMP XL, String TCP XL, and String UDP XL.

Note The IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP support the String XL engines and the Regex accelerator card.

Note The Regex accelerator card is used for both the standard String engines and the String XL engines. Most standard String engine signatures can be compiled and analyzed by the Regex accelerator card without modification. However, there are special circumstances in which the standard String engine signatures cannot be compiled for the Regex accelerator card. In these situations a new signature is written in a String XL engine using the specific parameters in the String XL engine that do compile on the Regex accelerator card. The new signature in the String XL engine obsoletes the original signature in the standard String engine.

- Sweep—Analyzes sweeps from a single host (ICMP and TCP), from destination ports (TCP and UDP), and multiple ports with RPC requests between two nodes. There are two Sweep engines: Sweep and Sweep Other TCP.
- Traffic Anomaly—Inspects TCP, UDP, and other traffic for worms.
- Traffic ICMP—Analyzes nonstandard protocols, such as TFN2K, LOKI, and DDOS. There are only two signatures with configurable parameters.
- Trojan—Analyzes traffic from nonstandard protocols, such as BO2K andTFN2K. There are three Trojan engines: Bo2k, Tfn2k, and UDP. There are no user-configurable parameters in these engines.

Configuring Signature Definition Policies

This section describes how to configure signature definition policies, and contains the following topics:

Signature Definitions Pane

Note You must be administrator or operator to add, clone, or delete signature policies.

In the Signature Definitions pane, you can add, clone, or delete a signature definition policy. The default signature definition policy is called sig0. When you add a policy, a control transaction is sent to the sensor to create the policy instance. If the response is successful, the new policy instance is added under Signature Definitions. If the control transaction fails, for example because of resource limitations, an error message appears.

If your platform does not support virtual policies, this means you can only have one instance for each component and you cannot create new ones or delete the existing one. In this case, the Add, Clone, and Delete buttons are disabled.

Signature Definitions Pane Field Definitions

The following fields are found in the Signature Definitions pane:

- Policy Name—Identifies the name of this signature definition policy.
- Assigned Virtual Sensor—Identifies the virtual sensor to which this signature definition policy is assigned.

Add and Clone Policy Dialog Boxes Field Definitions

The following field is found in the Add and Clone Policy dialog boxes:

- Name—Specifies the name of the virtual sensor. The default virtual sensor is vs0.
- Assigned Interfaces (or Pairs)—Specifies the interfaces or interface pairs that belong to this virtual sensor.
- Signature Definition Policy—Specifies the name of the signature definition policy for this virtual sensor. The default signature definition policy is sig0.
- Event Action Override Policy—Specifies the name of the event action rules overrides policy for this virtual sensor. The default event action rules policy is rules0.
  - Risk Rating—Indicates the risk rating range (low, medium, or high risk) that should be used to trigger this event action override.
  - Actions to Add—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
  - Enabled—Indicates whether or not this event action overrides policy is enabled.
- Anomaly Detection Policy—Specifies the name of the anomaly detection policy for this virtual sensor. The default anomaly detection policy is ad0.

  Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

- Description—The description of this virtual sensor.

Adding, Cloning, and Deleting Signature Policies

To add, clone, or delete a signature definition policy, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions**, and then click **Add**.

Step 3 In the Policy Name field, enter a name for the signature definition policy.

Tip To discard your changes and close the Add Policy dialog box, click **Cancel**.

Step 4 Click **OK**. The signature definition policy appears in the list in the Signature Definitions pane.

Step 5 To clone an existing signature definition policy, select it in the list, and then click **Clone**. The Clone Policy dialog box appears with "_copy" appended to the existing signature definition policy name.

Step 6 In the Policy Name field, enter a unique name.

Tip To discard your changes and close the Clone Policy dialog box, click **Cancel**.

Step 7 Click **OK**. The cloned signature definition policy appears in the list in the Signature Definitions pane.

Step 8 To remove a signature definition policy, select it, and then click **Delete**. The Delete Policy dialog box appears asking if you are sure you want to delete this policy permanently.

Caution You cannot delete the default signature definition policy, sig0.

Step 9 Click **Yes**. The signature definition policy no longer appears in the list in the Signature Definitions pane.

sig0 Pane

The sig0 menu in the left navigation pane contains the list of signatures listed by categories, for example, by active signatures, signature types, or all signatures. Once you choose a signature type in the menu, the sig0 pane is populated with the tools to configure signatures. You can filter the signatures by a variety of categories, for example, by signature ID, signature name, whether the signature is enabled, severity, fidelity rating, base risk rating, action, type, and engine.

Note You must select a signature category to see the signature configuration and add, clone, or edit signatures.

You can sort the data in each column by clicking the column head. The following columns are shown by default:

- ID
- Name
- Enabled
- Severity
- Fidelity Rating
- Base RR
- Signature Actions (Alert and Log, Deny, and Other)
- Type
- Engine
- Retired

  To change the default column view, click the **Column** icon in the upper right of the pane and check or clear the check boxes in the Choose Columns to Display dialog box. You can also move the columns to a new location by selecting it and dragging it to a different place in the table.

There are configuration buttons grouped around the following configuration actions:

- Signature Configuration—Lets you edit event actions, enable and disable signatures, restore signature defaults, view signature information on MySDN, edit, add, delete, clone, and export signatures.
- Signature Wizard—Lets you use a wizard to create custom signatures.
- Advanced
  - Signature Variables—Lets you set up variables to use within multiple signatures.
  - Miscellaneous—Lets you configure application policy signatures, set up the mode for IP fragmentation and TCP stream reassembly, and configure IP logging.

MySDN

Note Currently when you click **MySDN**, you are redirected to the IntelliShield site, which has replaced MySDN.

MySDN is a repository of information for individual signatures. It provides the following information about a signature:

- Signature ID
- Release version
- Original release date
- Latest release date
- Default enabled
- Default retired
- CVE
- Bugtraq ID
- Alarm severity
- Fidelity
- Description
- Recommended filters
- Benign filters
- IntelliShield alerts

The information from MySDN is available in the lower half of the sig0 pane. Select a signature in the list, and the information appears in the lower half. Or you can select a signature on **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**, and then click **MySDN**. After logging in to Cisco.com, you are taken to the specific information about that signature through the MySDN site ending at the IntelliShield site.

The IME launches MySDN from the last browser window you opened, which is the default setting for Windows. To change this default behavior, in Internet Explorer, choose **Tools > Internet Options**, and then click the **Advanced** tab. Scroll down and uncheck the **Reuse windows for launching shortcuts** check box.

Note The MySDN website has been decommissioned and is no longer available to Cisco.com users. You can get to the information only through the IME.

Configuring Signatures

This section describes how to configure signatures. It contains the following topics:

Sig0 Pane Field Definitions

The following fields are found in the Sig0 pane:

- Filter—Lets you sort the list of signatures by selecting an attribute to filter.
- ID—Identifies the unique numerical value assigned to this signature and subsignature. This value lets the sensor identify a particular signature.
- Name—Identifies the name assigned to the signature.
- Enabled—Identifies whether or not the signature is enabled. A signature must be enabled for the sensor to protect against the traffic specified by the signature.
- Severity—Identifies the severity level that the signature will report: High, Informational, Low, Medium.
- Fidelity Rating—Identifies the weight associated with how well this signature might perform in the absence of specific knowledge of the target.
- Base RR—Displays the base risk rating value of each signature. IDM automatically calculates the base risk rating by multiplying the fidelity rating and the severity factor and dividing them by 100 (Fidelity Rating x Severity Factor /100). Severity Factor has the following values:
  - Severity Factor = 100 if the severity level of the signature is high
  - Severity Factor = 75 if severity level of the signature is medium
  - Severity Factor = 50 if severity level of the signature is low

  - Severity Factor = 25 if severity level of the signature is informational
- Signature Actions—Identifies the actions the sensor will take when this signature fires.
- Type—Identifies whether this signature is a default (built-in), tuned, or custom signature.
- Engine—Identifies the engine that parses and inspects the traffic specified by this signature.
- Retired—Identifies whether or not the signature is retired. A retired signature is removed from the signature engine. You can activate a retired signature to place it back in the signature engine.

Note We recommend that you retire any signatures that you are not using. This improves sensor performance.

Button and Right-Click Menu Functions:

- Edit Actions—Opens the Edit Actions dialog box.
- Enable—Enables the selected signature.
- Disable—Disables the selected signature.
- Set Severity To—Lets you set the severity level that the signature will report: High, Medium, Low or Informational.
- Restore Default—Returns all parameters to the default settings for the selected signature.
- Show Events—Displays the events related to this signature in real time, from the last 10 minutes, or from the last hour.
- MySDN—Takes you to the description of that signature on the MySDN site on Cisco.com.
- Edit—Opens the Edit Signature dialog box. In the Edit Signature dialog box, you can change the parameters associated with the selected signature and effectively *tune* the signature. You can edit only one signature at a time.
- Add—Opens the Add Signature dialog box. In the Add Signature dialog box, you can add the parameters associated with the selected signature and effectively *tune* the signature.
- Delete—Deletes the selected custom signature.You cannot delete built-in signatures.
- Clone—Opens the Clone Signature dialog box. In the Clone Signature dialog box, you can create a signature by changing the prepopulated values of the existing signature you chose to clone.
- Change Status To—Lets you change the status to Active, Retired, Low Memory Retired, Medium Memory Retired.
- Export—Lets you export currently displayed signatures in the table to a comma-separated Excel file (using CSV) or HTML file. You can also use **Ctrl-C** to copy the contents in to a clipboard and later paste in to Notepad or Word using **Ctrl-V**.

Add, Clone, and Edit Signatures Dialog Boxes Field Definitions

The following fields are found in the Add, Clone, and Edit Signature dialog boxes:

- Signature Definition—Defines the signature:
  - Signature ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. The value is 1000 to 65000.
  - SubSignature ID—Identifies the unique numerical value assigned to this subsignature. The subsignature ID identifies a more granular version of a broad signature. The value is 0 to 255.

  - Alert Severity—Lets you choose the severity level of the signature: High, Informational, Low, Medium.
  - Sig Fidelity Rating—Lets you choose the weight associated with how well this signature might perform in the absence of specific knowledge of the target. The value is 0 to 100. The default is 75.
  - Promiscuous Delta—Lets you determine the seriousness of the alert.

Caution We recommend that you do NOT change the promiscuous delta setting for a signature.

- Sig Description—Lets you specify the following attributes that help you distinguish this signature from other signatures:
  - Signature Name—Specifies the name your signature. The default is MySig.
  - Alert Notes—Lets you add alert notes in this field.
  - User Comments—Lets you add your comments about this signature in this field.
  - Alarm Traits—Lets you add the alarm trait in this field. The value is 0 to 65535. The default is 0.
  - Release—Lets you add the software release in which the signature first appeared.
  - Signature Creation Date—Specifies the date this signature was created.
  - Signature Type—Specifies the type of signature (anomaly, component, exploit, other, vulnerability)
- Engine—Lets you choose the engine that parses and inspects the traffic specified by this signature.
- Event Action—Lets you assign the actions the sensor takes when it responds to events.
- Event Counter—Lets you configure how the sensor counts events. For example, you can specify that you want the sensor to send an alert only if the same signature fires 5 times for the same address set:
  - Event Count—Specifies the number of times an event must occur before an alert is generated. The value is 1 to 65535. The default is 1.
  - Event Count Key—Specifies the storage type used to count events for this signature. Choose attacker address, attacker address and victim port, attacker and victim addresses, attacker and victim addresses and ports, or victim address. The default is attacker address.
  - Specify Alert Interval—Specifies the time in seconds before the event count is reset. Choose Yes or No from the drop-down list and then specify the amount of time.
- Alert Frequency—Lets you configure how often the sensor alerts you when this signature is firing. Specify the following parameters for this signature:
  - Summary Mode—Specifies the mode of alert summarization. Choose Fire All, Fire Once, Global Summarize, or Summarize.

    Note When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

  - Summary Interval—Specifies the time in seconds used in each summary alert. The value is 1 to 65535. The default is 15.

  - Summary Key—Specifies the storage type used to summarize alerts. Choose Attacker address, Attacker address and victim port, Attacker and victim addresses, Attacker and victim addresses and ports, or Victim address. The default is Attacker address.
  - Specify Global Summary Threshold—Lets you specify the threshold number of events to take the alert into global summary. Choose Yes or No and then specify the threshold number of events.
- Status—Lets you enable or disable a signature, or retire or unretire a signature:
  - Enabled—Lets you choose whether the signature is enabled or disabled.The default is yes (enabled).
  - Retired—Let you choose whether the signature is retired or not and whether it is low memory retired or medium memory retired. The default is no (not retired). Low memory retired platforms have less that 1 GB of maximum sensor memory. Medium memory retired platforms have at least 1 GB and less than 2 GB of maximum sensor memory. As the signatures are loaded, the value of retired is evaluated based on the platform loading the signatures.
  - Obsoletes—Specifies the list of the signatures that are obsoleted by this signature.
  - Vulnerable OS List—Lets you choose a vulnerable OS for this signature.
- Mars Category—Lets you map this signature to a MARS attack category. This is a static information category that you can view in the alerts.

Edit Actions Dialog Box Field Definitions

An event action is the response of the sensor to an event. Event actions are configurable on a per-signature basis. The following fields are found in the Edit Actions dialog box:

Alert and Log Actions

- Product Alert—Writes the event to the Event Store as an alert.

Note The Product Alert action is not automatic when you enable alerts for a signature. To have an alert created in the Event Store, you must select Product Alert. If you add a second action, you must include Product Alert if you want an alert sent to the Event Store. Also, every time you configure the event actions, a new list is created and it replaces the old list. Make sure you include all the event actions you need for each signature.

Note There are other event actions that force a Product Alert. These actions use Product Alert as the vehicle for performing the action. Even if Product Alert is not selected or is filtered, the alert is still produced. The actions are the following: Produce Verbose Alert, Request SNMP Trap, Log Attacker Packets, Log Victim Packets, and Log Pair Packets.

Note A Produce Alert event action is added for an event when global correlation has increased the risk rating of an event, and has added either the Deny Packet Inline or Deny Attacker Inline event action.

- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.

- Log Attacker Packets—Starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Victim Packets—Starts IP logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Pair Packets—Starts IP logging on packets that contain the attacker/victim address pair. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Request SNMP Trap—Sends a request to the Notification Application component of the sensor to perform SNMP notification. This action causes an alert to be written to the Event Store, even if Product Alert is not selected. You must have SNMP configured on the sensor to implement this action.

Deny Actions

- Deny Packet Inline (inline only)—Terminates the packet.

Note You cannot delete the event action override for Deny Packet Inline because it is protected. If you do not want to use that override, disable it.

- Deny Connection Inline (inline only)—Terminates the current packet and future packets on this TCP flow.
- Deny Attacker Victim Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.

Note For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > General Settings**.

- Deny Attacker Service Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
- Deny Attacker Inline (inline only)—Terminates the current packet and future packets from this attacker address for a specified period of time.
- The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.

Note This is the most severe of the deny actions. It denies current and future packets from a single attacker address. To clear all denied attacker entries, choose **Configuration > *sensor_name* > Sensor Management > Time-Based Actions > Denied Attackers > Clear List**, which permits the addresses back on the network.

- Modify Packet Inline (inline only)—Modifies packet data to remove ambiguity about what the end point might do with the packet.

Note You cannot use Modify Packet Inline as an action when adding event action filters or overrides.

Other Actions

- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action.

  Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

  Note IPv6 does not support Request Block Connection.

- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action.

  Note IPv6 does not support Request Block Host.

  Note For block actions, to set the duration of the block, choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > General Settings**.

- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action.

  Note Request Rate Limit applies to a select set of signatures.

  Note IPv6 does not support Request Rate Limit.

- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

Understanding Deny Packet Inline

For signatures that have Deny Packet Inline configured as an action or for an event action override that adds Deny Packet Inline as an action, the following actions may be taken:

- Dropped Packet
- Denied Flow
- TCP One Way Reset Sent TCP

The Deny Packet Inline action is represented as a dropped packet action in the alert. When a Deny Packet Inline occurs for a TCP connection, it is automatically upgraded to a Deny Connection Inline action and seen as a denied flow in the alert. If the IPS denies just one packet, the TCP continues to try to send that same packet again and again, so the IPS denies the entire connection to ensure it never succeeds with the resends.

When a Deny Connection Inline occurs, the IPS also automatically sends a TCP one-way reset, which shows up as a TCP one-way reset sent in the alert. When the IPS denies the connection, it leaves an open connection on both the client (generally the attacker) and the server (generally the victim). Too many open connections can result in resource problems on the victim. So the IPS sends a TCP reset to the victim to close the connection on the victim side (usually the server), which conserves the resources of the victim. It also prevents a failover that would otherwise allow the connection to fail over to a different network path and reach the victim. The IPS leaves the attacker side open and denies all traffic from it.

TCP Reset Differences Between IPS Appliances and ASA IPS Modules

The IPS appliance sends TCP reset packets to both the attacker and victim when Reset TCP Connection is selected. The IPS appliance sends a TCP reset packet only to the victim under the following circumstances:

- When a Deny Packet Inline or Deny Connection Inline is selected
- When TCP-based signatures and Reset TCP Connection have NOT been selected

In the case of the ASA IPS modules, the TCP reset request is sent to the ASA, and then the ASA sends the TCP reset packets. The ASA sends TCP reset packets to both the attacker and victim when the Reset TCP Connection is selected. When Deny Packet Inline or Deny Connection Inline is selected, the ASA sends the TCP reset packet to either the attacker or victim depending on the configuration of the signature. Signatures configured to swap the attacker and victim when reporting the alert can cause the ASA to send the TCP reset packet to the attacker.

TCP Normalizer Signature Warning

You receive the following warning if you disable a default-enabled TCP Normalizer signature or remove a default-enabled modify packet inline, deny packet inline, or deny connection inline action:

```
Use caution when disabling, retiring, or changing the event action settings of a <Sig ID>
TCP Normalizer signature for a sensor operating in IPS mode. The TCP Normalizer signature
default values are essential for proper operation of the sensor.
If the sensor is seeing duplicate packets, consider assigning the traffic to multiple
virtual sensors. If you are having problems with asymmetric or out-of-order TCP packets,
consider changing the normalizer mode from strict evasion protection to asymmetric mode
protection. Contact Cisco TAC if you require further assistance.
```

For More Information

- For the procedure for configuring the general settings, see Configuring General Settings, page 12-33.
- For the procedure for configuring SNMP, see Chapter 18, “Configuring SNMP.”
- For the procedure for configuring denied attackers, see Configuring and Monitoring Denied Attackers, page 17-1.

Enabling, Disabling, and Retiring Signatures

To enable, disable, and retire signatures, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 To locate a signature, choose a sorting option from the Filter drop-down list. For example, if you are searching for a Flood Host signature, chose **Engine** from the drop-down list, then **Flood Host**, and then select the individual signature. The sig0 pane refreshes and displays only those signatures that match your sorting criteria.

Step 4 To enable or disable an existing signature, select the signature, and follow these steps:

a. View the Enabled column to determine the status of the signature. A signature that is enabled has the check box checked.

b. To enable a signature that is disabled, check the **Enabled** check box.

c. To disable a signature that is enabled, remove the check from the **Enabled** check box.

d. To retire one or more signatures, select the signature(s), right-click, and then click **Change Status To > Retired**.

Note We recommend that you retire any signatures that you are not using. This improves sensor performance.

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

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Adding Signatures

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

To create a custom signature that is not based on an existing signature, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**, and then click **Add**.

Step 3 In the Signature ID field, enter a unique signature ID for the new signature. Custom signature IDs start at 60000.

Step 4 In the Subsignature field, enter a unique subsignature ID for the new signature.

Step 5 From the Alert Severity drop-down list, choose the severity you want to associate with this signature.

Step 6 In the Sig Fidelity Rating field, enter a value between 1 and 100 to represent the signature fidelity rating for this signature.

Step 7 In the Promiscuous Delta field, enter the promiscuous delta (between 0 and 30) that you want to associate with this signature.

Caution We recommend that you do NOT change the promiscuous delta setting for a signature.

Step 8 Complete the Sig Description fields and add any comments about this signature.

Step 9 From the Engine drop-down list, choose the engine the sensor will use to enforce this signature.

Note If you do not know which engine to select, use the Custom Signature Wizard to help you create a custom signature.

Step 10 Assign actions to this signature.

Step 11 Configure the engine-specific parameters for this signature.

Step 12 Configure the Event Counter:

a. In the Event Count field, enter the number of events you want counted (1 to 65535).

b. From the Event Count Key drop-down list, choose the key you want to use.

c. From the Specify Alert Interface drop-down list, choose whether you want to specify the alert interval (Yes or No).

d. If you chose Yes, enter the alert interval (2 to 1000) in the Alert Interval field.

Step 13 Configure the alert frequency.

Step 14 Configure the status of the signature:

a. From the Enabled drop-down list, choose **Yes** to enable the signature.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

b. From the Retired drop-down list, choose **Yes** to make sure the signature is active. This places the signature in the engine.

Note A signature must not be retired for the sensor to actively detect the attack specified by the signature.

c. Choose the vulnerable OS(es).

Tip To select more than one OS, hold down the **Ctrl** key.

Step 15 Choose the MARS category and click **OK**.

Tip To discard your changes and close the Add Signature dialog box, click **Cancel**.

Step 16 Click **OK**. The new signature appears in the list with the Type set to Custom.

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

Step 17 Click **Apply** to apply your changes and save the revised configuration.

Cloning Signatures

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution Some signature values in built-in signature are protected, which means that you cannot copy that value. You can still clone the signature, but you cannot configure certain values. You will receive an error message similar to the following when a signature value cannot be configured:

```
[Obsoletes] is protected, cannot copy the value. [Mars Category] is protected, cannot
copy the value.
```

On the sig0 pane, you can create a signature by cloning an existing signature. This task can save you time when you are creating signatures that are similar. To create a signature by using an existing signature as the starting point, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 To locate a signature, choose a sorting option from the Filter drop-down list. For example, if you are searching for a Flood Host signature, choose **Engine** from the drop-down list, then **Flood Host**, and then select the individual signature. The sig0 pane refreshes and displays only those signatures that match your sorting criteria.

Step 4 Select the signature and click **Clone**.

Step 5 In the Signature field, enter a unique signature ID for the new signature. Custom signature IDs start at 60000.

Step 6 In the Subsignature field, enter a unique subsignature ID for the new signature.

Step 7 Review the parameter values and change the value of any parameter you want to be different for this new signature.

Tip To select more than one OS or event action, hold down the **Ctrl** key.

Step 8 Configure the status of the signature:

a. From the Enabled drop-down list, choose **Yes** to enable the signature.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

b. From the Retired drop-down list, choose **Yes** to make sure the signature is active. This places the signature in the engine.

Note A signature must not be retired for the sensor to actively detect the attack specified by the signature.

Tip To discard your changes and close the Clone Signature dialog box, click **Cancel**.

c. Click **OK**. The cloned signature now appears in the list with the Type set to Custom.

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

Step 9 Click **Apply** to apply your changes and save the revised configuration.

Tuning Signatures

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

You can tune built-in signatures by adjusting several signature parameters. Built-in signatures that have been modified are called *tuned* signatures. On the sig0 pane, you can edit, or *tune* a signature.

To tune an existing signature, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 To locate a signature, choose a sorting option from the Filter drop-down list. For example, if you are searching for a Flood Host signature, choose **Engine** from the drop-down list, then **Flood Host**, and then select the individual signature. The sig0 pane refreshes and displays only those signatures that match your sorting criteria.

Step 4 Select the signature and click **Edit**.

Step 5 Review the parameter values and change the value of any parameter you want to tune.

Tip To select more than one OS, event action, vulnerable OS, or MARS category, hold down the **Ctrl** key.

Step 6 Configure the status of the signature:

a. From the Enabled drop-down list, choose **Yes** to enable the signature.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

b. From the Retired drop-down list, choose **Yes** to make sure the signature is active. This places the signature in the engine.

Note A signature must not be retired for the sensor to actively detect the attack specified by the signature.

Tip To discard your changes and close the Edit Signature dialog box, click **Cancel**.

Step 7 Click **OK**. The edited signature now appears in the list with the Type set to Tuned.

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

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

Assigning Actions to Signatures

On the sig0 pane, you can assign actions to a signature.

To edit actions for a signature or a set of signatures, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 To locate a signature, choose a sorting option from the Filter drop-down list. For example, if you are searching for a Flood Host signature, choose **Engine** from the drop-down list, then **Flood Host**, and then select the individual signature. The sig0 pane refreshes and displays only those signatures that match your sorting criteria.

Step 4 Select the signature(s), and click **Edit Actions**.

Step 5 Check the check boxes next to the actions you want to assign to the signature(s).

Note A check mark indicates that the action is assigned to the selected signature(s). No check mark indicates that the action is not assigned to any of the selected signatures. A gray check mark indicates that the action is assigned to some of the selected signatures.

Tip To select more than one action, hold down the **Ctrl** key.

Choose from the following actions:

- Produce Alert—Writes the event to Event Store as an alert.
- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to Event Store, even if Produce Alert is not selected.
- Log Attacker Packets—Starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to Event Store, even if Produce Alert is not selected.
- Log Victim Packets—Starts IP Logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to Event Store, even if Produce Alert is not selected.
- Log Pair Packets—Starts IP Logging on packets that contain the attacker/victim address pair. This action causes an alert to be written to Event Store, even if Produce Alert is not selected.
- Request SNMP Trap—Sends a request to NotificationApp to perform SNMP notification. This action causes an alert to be written to Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action.
- Deny Packet Inline (inline only)—Does not transmit this packet.
- Deny Connection Inline (inline only)—Does not transmit this packet and future packets on the TCP flow.
- Deny Attacker Victim Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.
- Deny Attacker Service Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
- Deny Attacker Inline (inline only)—Does not transmit this packet and future packets originating from the attacker address for a specified period of time.
- Modify Packet Inline (inline only)—Modifies packet data to remove ambiguity about what the end point might do with the packet.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action.
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action.
- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action.
- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

Tip To discard your changes and close the Assign Actions dialog box, click **Cancel**.

Step 6 Click **OK** to save your changes and close the dialog box. The new action(s) now appears in the Action column.

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

Step 7 Click **Apply** to apply your changes and save the revised configuration.

For More Information

- For the procedure for configuring the general settings, see Configuring General Settings, page 12-33.
- For the procedure for configuring SNMP, see Chapter 18, "Configuring SNMP."
- For the procedure for configuring denied attackers, see Configuring and Monitoring Denied Attackers, page 17-1.

Configuring Alert Frequency

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

You can control how often a signature fires. For example, you may want to decrease the volume of alerts sent out from the sensor. Or you may want the sensor to provide basic aggregation of signature firings into a single alert. Or you may want to counter anti-IPS tools such as "stick," which are designed to send bogus traffic so that the IPS produces thousands of alerts during a very short time.

To configure the alert frequency of a signature, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 Click **Add** to add a signature, choose a signature to clone, and click **Clone**, or choose a signature to edit, and click **Edit**.

Step 4 Configure the event count, key, and alert interval:

a. In the Event Count field, enter a value for the event count. This is the minimum number of hits the sensor must receive before sending one alert for this signature.

b. From the Event Count Key drop-down list, choose an attribute to use as the Event Count Key. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the Event Count Key.

c. If you want to count events based on a rate, choose **Yes** from the Specify Event Interval drop-down list, and then in the Alert Interval field, enter the number of seconds that you want to use for your interval.

Step 5 To control the volume of alerts and configure how the sensor summarizes alerts, choose one of the following options from the Summary Mode drop-down list:

- Fire All—Specifies that you want the sensor to send an alert every time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 6.
- Fire Once—Specifies that you want the sensor to send an alert the first time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 7.
- Summarize—Specifies that you want the sensor to only send summary alerts for this signature instead of sending alerts every time the signature fires. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 8.

- Global Summarize—Specifies that you want the sensor to send an alert the first time a signature fires on an address set, and then only send a global summary alert that includes a summary of all alerts for all address sets over a given time interval. Go to Step 9.

Step 6 Configure the Fire All option:

a. From the Specify Summary Threshold drop-down list, choose **Yes**.

b. In the Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a summary alert for this signature.

c. In the Summary Interval field, enter the number of seconds that you want to use for the time interval.

d. To have the sensor enter global summarization mode, choose **Yes** from the Specify Global Summary Threshold drop-down list.

e. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

f. From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

Step 7 Configure the Fire Once option:

a. From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

b. To have the sensor use global summarization, choose **Yes** from the Specify Global Summary Threshold drop-down list.

c. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert. When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

Note When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

d. In the Summary Interval field, enter the number of seconds during which the sensor counts events for summarization.

Step 8 Configure the Summarize option:

a. In the Summary Interval field, enter the number of seconds during which the sensor counts events for summarization.

b. From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

c. To have the sensor use dynamic global summarization, choose **Yes** from the Specify Global Summary Threshold drop-down list.

d. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

Note When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

Step 9 To configure the Global Summarize option, in the Summary Interval field, enter the number of seconds during which the sensor counts events for summarization.

Step 10 Click **OK** to save your alert behavior changes. You are returned to the sig0 pane.

Tip To discard your changes, click **Cancel**.

Step 11 To apply your alert behavior changes to the signature configuration, click **Apply**. The signature you added or edited is enabled and added to the list of signatures.

Example Meta Engine Signature

Caution A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

Caution A large number of Meta engine signatures could adversely affect overall sensor performance.

The Meta engine defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets. As signature events are generated, the Meta engine inspects them to determine if they match any or several Meta definitions. The Meta engine generates a signature event after all requirements for the event are met.

All signature events are handed off to the Meta engine by the Signature Event Action Processor. The Signature Event Action Processor hands off the event after processing the minimum hits option. Summarization and event action are processed after the Meta engine has processed the component events.

Note The Meta engine is different from other engines in that it takes alerts as input where most engines take packets as input.

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

The following example demonstrates how to create a signature based on the Meta engine. For example, the following custom signature fires when it sees the alerts from signature 2000 subsignature 0 and signature 3000 subsignature 0 on the same source address. The source address selection is a result of the meta key default value of Axxx. You can change the behavior by changing the meta key setting to xxBx (destination address) for example.

To create a signature based on the Meta engine, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**, and then click **Add**.

Step 3 In the Signature ID field, enter a unique signature ID for the new signature. Custom signature IDs start at 60000.

Step 4 In the Subsignature field, enter a unique subsignature ID for the new signature.

Step 5 From the Alert Severity drop-down list, choose the severity you want to associate with this signature.

Step 6 In the Signature Fidelity Rating field, enter a value between 1and 100 to represent the signature fidelity rating for this signature.

Step 7 Leave the default value for the Promiscuous Delta field.

Step 8 Complete the signature description fields and add any comments about this signature.

Step 9 From the Engine drop-down list, choose **Meta**.

Step 10 Configure the Meta engine-specific parameters:

a. From the Event Action drop-down list, choose the actions you want the sensor to take when it responds to an event.

Tip To choose more than one action, hold down the **Ctrl** key.

b. From the Swap Attacker Victim drop-down list, choose **Yes** to swap the destination and source ports in the alert message.

c. In the Meta Reset Interval field, enter the time in seconds to reset the Meta signature. The valid range is 0 to 3600 seconds. The default is 60 seconds.

d. Click the pencil icon next to Component List to insert the new Meta signature. The Component List dialog box appears.

e. Click **Add** to insert the first Meta signature. The Add List Entry dialog box appears.

f. In the Entry Key field, enter a name for the entry, for example, Entry1. The default is MyEntry.

g. In the Component Sig ID field, enter the signature ID of the signature (2000 in this example) on which to match this component.

h. In the Component SubSig ID field, specify the subsignature ID of the signature (0 in this example) on which to match this component.

i. In the Component Count field, enter the number of times this component must fire before it is satisfied.

j. In the Is a NOT component field, choose **Yes** if you want this to be NOT component.

k. Click **OK**. You are returned to the Add List Entry dialog box.

l. Select your entry and click **Select** to move it to the Selected Entries list.

m. Click **OK**.

n. Click **Add** to insert the next Meta signature. The Add List Entry dialog box appears.

o. In the Entry Key field, enter a name for the entry, for example Entry2.

p. In the Component Sig ID field, enter the signature ID of the signature (3000 in this example) on which to match this component.

q. In the Component SubSig ID field, enter the subsignature ID of the signature (0 in this example) on which to match this component.

r. In the Component Count field, enter the number of times this component must fire before it is satisfied.

s. Click **OK**. You are returned to the Add List Entry dialog box.

t. Select your entry and click **Select** to move it to the Selected Entries list.

u. Select the new entry and click **Move Up** or **Move Down** to order the new entry.

Tip Click **Reset Ordering** to return the entries to the Entry Key list.

v. Click **OK**.

w. From the Meta Key drop-down list, choose the storage type for the Meta signature:

- Attacker address
- Attacker and victim addresses
- Attacker and victim addresses and ports
- Victim address

x. In the Unique Victims field, enter the number of unique victims required for this signature. The valid value is 1 to 256. The default is 1.

y. From the Component List in Order drop-down list, choose **Yes** to have the component list fire in order.

Step 11 In the Component List in Order field, you can choose **Yes** to have the component list fire in order. For example, if signature 3000 in the Entry2 component fires before signature 2000 in the Entry1 component, the custom Meta signature will not fire.

Step 12 In the All Components Required field and the All NOT Components Required field, choose **Yes** to use all components and NOT components. This option works with the All NOT Components Required option, if you have NOT components configured as required, the Meta signature will not fire.

Step 13 Configure Event Counter:

a. In the Event Count field, enter the number of events you want counted (1 to 65535).

b. From the Event Count Key drop-down list, choose the key you want to use.

c. From the Specify Alert Interface drop-down list, choose whether you want to specify the alert interval (Yes or No).

d. If you chose Yes, enter the alert interval (2 to 1000) in the Alert Interval field.

Step 14 Configure the alert frequency.

Step 15 Leave the default (**Yes**) for the Enabled field.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

Step 16 Leave the default (**Yes**) for the Retired field. This places the signature in the engine.

Note A signature must not be retired for the sensor to actively detect the attack specified by the signature.

Step 17 From the Vulnerable OS List drop-down list, choose the operating systems that are vulnerable to this signature.

Tip To choose more than one action, hold down the **Ctrl** key.

Step 18 From the Mars Category drop-down list, choose the MARS categories you want this signature to identify.

Tip To choose more than one action, hold down the **Ctrl** key.

Tip To discard your changes and close the Add Signature dialog box, click **Cancel**.

Step 19 Click **OK**. The new signature appears in the list with the Type set to Custom.

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

Step 20 Click **Apply** to apply your changes and save the revised configuration.

For More Information

For detailed information on the Meta engine, see Meta Engine, page B-32.

Example Atomic IP Advanced Engine Signature

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

The following example demonstrates how to create a signature based on the Atomic IP Advanced engine. For example, the following custom signature matches any packets that are IPv6 with a HOP Option Header where the header is type 1 and the length is 8.

To create a signature based on the Atomic IP Advanced engine, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**, and then click **Add**.

Step 3 In the Signature ID field, enter a unique signature ID for the new signature. Custom signature IDs start at 60000.

Step 4 In the Subsignature field, enter a unique subsignature ID for the new signature.

Step 5 From the Alert Severity drop-down list, choose the severity you want to associate with this signature.

Step 6 In the Signature Fidelity Rating field, enter a value between 1and 100 to represent the signature fidelity rating for this signature.

Step 7 Leave the default value for the Promiscuous Delta field.

Step 8 Complete the signature description fields and add any comments about this signature.

Step 9 From the Engine drop-down list, choose **Atomic IP Advanced**.

Step 10 Configure the Atomic IP Advanced engine-specific parameters:

a. From the Event Action drop-down list, choose the actions you want the sensor to take when it responds to an event.

Note IPv6 does not support the following event actions: Request Block Host, Request Block Connection, or Request Rate Limit.

Tip To choose more than one action, hold down the **Ctrl** key.

b. From the IP Version drop-down list, choose **Yes** to enable the IP version, and then from the IP Version drop-down list, choose **IPv6** to enable IPv6.

c. From the HOP Options Header drop-down list, choose **Yes** to enable hop-by-hop options, and then from the HOH Present drop-down list, choose **Have HOH**.

d. From the HOH Options field, choose **Yes**, and then in the HOH Option Type field, enter **1**.

e. In the HOH Option Length drop-down list, choose **Yes** to enable hop-by-hop length, and then in the HOH Option Length field, enter **8**.

Step 11 Configure Event Counter:

a. In the Event Count field, enter the number of events you want counted (1 to 65535).

b. From the Event Count Key drop-down list, choose the key you want to use.

c. From the Specify Alert Interface drop-down list, choose whether you want to specify the alert interval (Yes or No).

d. If you chose Yes, enter the alert interval (2 to 1000) in the Alert Interval field.

Step 12 Configure the alert frequency.

Step 13 Leave the default (**Yes**) for the Enabled field.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

Step 14 Leave the default (**Yes**) for the Retired field. This places the signature in the engine.

Note A signature must not be retired for the sensor to actively detect the attack specified by the signature.

Step 15 From the Vulnerable OS List drop-down list, choose the operating systems that are vulnerable to this signature.

Tip To choose more than one action, hold down the **Ctrl** key.

Step 16 From the Mars Category drop-down list, choose the MARS categories you want this signature to identify.

Tip To choose more than one action, hold down the **Ctrl** key.

Tip To discard your changes and close the Add Signature dialog box, click **Cancel**.

Step 17 Click **OK**. The new signature appears in the list with the Type set to Custom.

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

Step 18 Click **Apply** to apply your changes and save the revised configuration.

For More Information

For more information on the Atomic IP engines, see Atomic Engine, page B-13.

Example String XL TCP Match Offset Signature

Caution A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

Note This procedure also applies to String XLUDP and String XL ICMP signatures, with the exception of the parameter **service-ports,** which does not apply to String XL ICMP signatures.

You can create a custom String XL TCP signature by either cloning an existing String XL TCP signature and then tuning it, or by adding a new signature and assigning the String XL TCP signature engine to it.

The following example demonstrates how to create a custom String XL TCP signature that searches for exact, maximum, or minimum offsets. You can modify the following optional match offset parameters for this custom String XLTCP signature:

- Specify Exact Match Offset {Yes | No}—Enables exact match offset:
  - Exact Match Offset—Specifies the exact stream offset in bytes the regular expression string must report for a match to be valid. The valid value is 0 to 65535.
- Specify Maximum Match Offset {Yes | No}—Enables maximum match offset:
  - Maximum Match Offset—Specifies the maximum stream offset in bytes the regular expression string must report for a match to be valid. The valid value is 0 to 65535.
- Specify Min Match Offset {Yes | No}—Enables minimum match offset:
  - Min Match Offset—Specifies the minimum stream offset in bytes the regular expression string must report for a match to be valid. The valid value is 0 to 65535.

To create a custom String XL TCP signature that searches for matches, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 To create a custom signature by cloning an existing String XL TCP signature, from the Filter drop-down list, choose Engine, and then String TCP XL from the signature engine drop-down list, highlight the signature you want to clone, and then click **Clone**. Continue with Step 5.

Step 4 To create a custom signature based on the String XL TCP engine, click **Add** and in the Engine field in the Add Signature dialog box, click **Click to edit** and choose String XL TCP from the drop-down list. Continue with Step 5.

Step 5 In the Signature ID field, enter a number for the signature. Custom signatures range from 60000 to 65000.

Step 6 In the Subsignature ID field, enter a number for the signature. The default is 0. You can assign a subsignature ID if you are grouping signatures together that are similar.

Step 7 (Optional) In the Severity Alert field, choose the severity to be reported by Event Viewer when the sensor sends an alert. The default is Medium.

Step 8 (Optional) In the Sig Fidelity Rating field, enter a value. The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident. The default is 75.

Step 9 In the Promiscuous Delta field, enter a value. The promiscuous delta is a value used to determine the seriousness of the alert. The valid range is 0 to 30. The default is 0.

Caution We recommend that you do NOT change the promiscuous delta setting for a signature.

Step 10 Under Sig Description specify the attributes that uniquely identify this signature:

a. (Optional) In the Signature Name field, enter a name for the signature. A default name, My Sig, appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

Note The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

b. (Optional) In the Alert Notes field, enter text to be added to the alert. You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated. The default is My Sig Info.

c. (Optional) In the User Comments field, enter text that describes this signature. You can add any text that you find useful here. This field does not affect the signature or alert in any way. The default is Sig Comment.

Step 11 Under Engine, assign the engine-specific parameters:

a. (Optional) In the Event Action field, assign the event actions you want the signature to report. The default is Produce Alert. You can assign more actions, such as deny or block, based on your security policy.

Tip To select more than one action, hold down the **Ctrl** key.

b. (Optional) In the Strip Telnet Options field, choose **Yes** from the drop-down list to strip the Telnet option characters from the data before the pattern is searched.

c. From the Direction drop-down list, choose the direction of the traffic:

- From Service—Traffic from service port destined to client port.
- To Service—Traffic from client port destined to service port.

d. In the Service Ports field, enter the port number, for example, 80. The value is a comma-separated list of ports or port ranges where the target service resides.

Step 12 To specify the regular expression, in the Specify Raw Regex String, choose **No** from the drop-down list.

Note Raw Regex is regular expression syntax used for raw mode processing. It is expert mode only and targeted for use by the Cisco IPS signature development team or only those who are under supervision by the Cisco IPS signature development team. You can configure a String XL signature in either regular Regex or raw Regex.

a. In the Regex String field, enter the string this signature will be looking for in the TCP packet, for example, tcpstring.

b. (Optional) In the Specify Minimum Match Length field, choose **Yes** from the drop-down list to enable minimum match length, and then in the Minimum Match Length field, enter the minimum number of bytes the regular expression string must match (0 to 65535).

c. (Optional) In the Swap Attacker Victim field, choose **Yes** from the drop-down list to swap the attacker and victim addresses and ports (source and destination) in the alert message and for any actions taken.

Step 13 (Optional) In the Specify Exact Match Offset field, choose **Yes** from the drop-down list to enable exact match offset, and then in the Exact Match Offset field, enter the exact offset the regular expression must trigger to be considered a match for this signature (0 to 65535).

Note If you have exact match offset set to Yes, you cannot configure maximum or minimum match offset. If you have exact match offset set to No, you can configure both maximum and minimum match offset at the same time.

Step 14 (Optional) In the Specify Max Match Offset field, choose **Yes** from the drop-down list to enable maximum match offset, and then in the Specify Max Match Offset field, enter the maximum offset at which the regular expression must trigger to be considered a match for this signature (0 to 65535).

Step 15 (Optional) In the Specify Min Match Offset field, choose **Yes** from the drop-down list to enable minimum match offset, and then in the Specify Min Match Offset field, enter the minimum offset at which the regular expression must trigger to be considered a match for this signature (0 to 65535).

Step 16 (Optional) Under Alert Frequency, you can change the default alert frequency.

Step 17 Click **OK** to create your custom signature. The signature you created is enabled and added to the list of signatures.

Tip To discard your changes, click **Cancel**.

For More Information

- For more information about the String XL engine, see String XL Engines, page B-63.
- For information about regular expression syntax, see Regular Expression Syntax, page B-9.

Example String XL TCP Engine Minimum Match Length Signature

Caution A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

Note This procedure also applies to String XLUDP and String XL ICMP signatures, with the exception of the parameter **service-ports,** which does not apply to String XL ICMP signatures.

You can create a custom String XL TCP signature by either cloning an existing String XL TCP signature and then tuning it, or by adding a new signature and assigning the String XL TCP signature engine to it.

You can configure the following options to work with a specific Regex string:

- Dot All {Yes | No}—If set to Yes, matches [\x00-\xFF] including \n; if set to No, matches anything in the range [\x00-\xFF] except \n. No is the default.
- End Optional {Yes | No}—Specifies that at the end of a packet, if all other conditions are satisfied but the end is not seen, a match is reported if the minimum is exceeded
- No Case {Yes | No}—Specifies to treat all alphabetic characters in the expression as case insensitive.
- Stingy {Yes | No}—Specifies to stop looking for larger matches after the first completed match.

Note Stingy can only be used with Min Match Length; otherwise, it is ignored

- UTF-8 {True | False}—Treats all legal UTF-8 byte sequences in the expression as a single character.

The following example demonstrates how to create a custom String XL TCP signature that searches for minimum match length with stingy, dot all, and UTF-8 turned on. To create a custom signature based on the String XL TCP engine that searches for minimum match length with stingy, dot all, and UTF-8 turned on, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 To create a custom signature by cloning an existing String XL TCP signature, from the Filter drop-down list, choose Engine, and then String TCP XL from the signature engine drop-down list, then highlight the signature you want to clone, and click **Clone**. Continue with Step 5.

Step 4 To create a custom signature based on the String XL TCP engine, click **Add** and in the Engine field in the Add Signature dialog box, click **Click to edit** and choose String XL TCP from the drop-down list. Continue with Step 5.

Step 5 In the Signature ID field, enter a number for the signature. Custom signatures range from 60000 to 65000.

Step 6 In the Subsignature ID field, enter a number for the signature. The default is 0. You can assign a subsignature ID if you are grouping signatures together that are similar.

Step 7 (Optional) In the Severity Alert field, choose the severity to be reported by Event Viewer when the sensor sends an alert. The default is Medium.

Step 8 (Optional) In the Sig Fidelity Rating field, enter a value. The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident. The default is 75.

Step 9 In the Promiscuous Delta field, enter a value. The promiscuous delta is a value used to determine the seriousness of the alert. The valid range is 0 to 30. The default is 0.

Caution We recommend that you do NOT change the promiscuous delta setting for a signature.

Step 10 Under Sig Description specify the attributes that uniquely identify this signature:

a. (Optional) In the Signature Name field, enter a name for the signature. A default name, My Sig, appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

Note The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

b. (Optional) In the Alert Notes field, enter text to be added to the alert. You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated. The default is My Sig Info.

c. (Optional) In the User Comments field, enter text that describes this signature. You can add any text that you find useful here. This field does not affect the signature or alert in any way. The default is Sig Comment.

Step 11 Under Engine, assign the engine-specific parameters:

a. (Optional) In the Event Action field, assign the event actions you want the signature to report. The default is Produce Alert. You can assign more actions, such as deny or block, based on your security policy.

Tip To select more than one action, hold down the **Ctrl** key.

b. (Optional) In the Strip Telnet Options field, choose **Yes** from the drop-down list to strip the Telnet option characters from the data before the pattern is searched.

c. From the Direction drop-down list, choose the direction of the traffic:

- From Service—Traffic from service port destined to client port.
- To Service—Traffic from client port destined to service port.

d. In the Service Ports field, enter the port number, for example, 23. The value is a comma-separated list of ports or port ranges where the target service resides.

Step 12 To specify the regular expression, in the Specify Raw Regex String, choose **No** from the drop-down list.

Note Raw Regex is regular expression syntax used for raw mode processing. It is expert mode only and targeted for use by the Cisco IPS signature development team or only those who are under supervision by the Cisco IPS signature development team. You can configure a String XL signature in either regular Regex or raw Regex.

a. In the Regex String field, enter the string this signature will be looking for in the TCP packet (for example, ht+p[\r].).

b. (Optional) In the Specify Minimum Match Length field, choose **Yes** from the drop-down list to enable minimum match length, and then in the Minimum Match Length field, enter the minimum number of bytes the regular expression string must match (0 to 65535).

c. (Optional) In the Swap Attacker Victim field, choose **Yes** from the drop-down list to swap the attacker and victim addresses and ports (source and destination) in the alert message and for any actions taken.

Step 13 (Optional) Turn on the following options by choosing **Yes** in the drop-down list:

- Dot All
- Stingy
- UTF-8

Step 14 (Optional) Under Alert Frequency, you can change the default alert frequency.

Step 15 Click **OK** to create your custom signature. The signature you created is enabled and added to the list of signatures.

Tip To discard your changes, click **Cancel**.

For More Information

- For more information about the String XL engine, see String XL Engines, page B-63.
- For information about regular expression syntax, see Regular Expression Syntax, page B-9.

Configuring Signature Variables

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

Signature Variables Tab

Note You must be administrator or operator to configure signature variables.

When you want to use the same value within multiple signatures, use a variable. When you change the value of a variable, that variable is updated in all signatures in which it appears. This saves you from having to change the variable repeatedly as you configure signatures.

Note You must preface the variable with a dollar ($) sign to indicate that you are using a variable rather than a string.

Some variables cannot be deleted because they are necessary to the signature system. If a variable is protected, you cannot select it to edit it. You receive an error message if you try to delete protected variables. You can edit only one variable at a time.

Signature Variables Field Definitions

The following fields are found on the Signature Variables tab and in the Add and Edit Signature Variable dialog boxes:

- Name—Identifies the name assigned to this variable.
- Type—Identifies the variable as a web port or IP address range.
- Value—Identifies the value(s) represented by this variable.

Note To designate multiple port numbers for a single variable, place a comma between the entries. For example, 80, 3128, 8000, 8010, 8080, 8888, 24326.

Adding, Editing, and Deleting Signature Variables

To add, edit, and delete signature variables, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures > Advanced > Signature Variables**, and then click **Add** to create a variable.

Step 3 In the Name field, enter the name of the signature variable. From the Type drop-down list, choose the type of signature variable.

Note A valid name can only contain numbers or letters. You can also use a hyphen (-) or underscore (_).

Step 4 In the Value field, enter the value for the new signature variable. The web-ports type has a predefined set of ports where web servers are running, but you can edit the value. This variable affects all signatures that have web ports. The default is 80, 3128, 8000, 8010, 8080, 8888, 24326.

Note You can use commas as delimiters. Make sure there are no trailing spaces after the comma. Otherwise, you receive a `Validation failed` error.

Tip To discard your changes and close the Add Signature Variable dialog box, click **Cancel**.

Step 5 Click **OK**. The new variable appears in the signature variables list on the Signature Variables tab.

Step 6 To edit an existing variable, select it in the signature variables list, and then click **Edit**.

Step 7 Make any changes needed in the Value field.

Tip To discard your changes and close the Edit Signature Variable dialog box, click **Cancel**.

Step 8 Click **OK**. The edited variable appears in the signature variables list on the Signature Variables tab.

Step 9 To delete a variable, select it in the signature variables list, and then click **Delete**. The variable no longer appears in the signature variables list on the Signature Variables tab.

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

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Configuring Miscellaneous Settings

This section describes the Miscellaneous tab and how to configure Application Inspection and Control (AIC) signatures, IP fragment reassembly signatures, TCP stream reassembly signatures, and IP logging. It contains the following topics:

Miscellaneous Tab

Note You must be administrator or operator to configure the parameters on the Miscellaneous tab.

On the Miscellaneous tab, you can perform the following tasks:

- Configure the application policy parameters (also known as AIC signatures)

  You can configure the sensor to provide Layer 4 to Layer 7 packet inspection to prevent malicious attacks related to web services. You first set up the AIC parameters, then you can either use the default AIC signatures or tune them.

- Configure IP fragment reassembly options

  You can configure the sensor to reassemble a datagram that has been fragmented over multiple packets. You can specify boundaries that the sensor uses to determine how many datagrams and how long to wait for more fragments of a datagram. The goal is to ensure that the sensor does not allocate all its resources to datagrams that cannot be completely reassembled, either because the sensor missed some frame transmissions or because an attack has been launched that is based on generating random fragment datagrams. You first choose the method the sensor will use to perform IP fragment reassembly, then you can tune the IP fragment reassembly signatures, which are part of the Normalizer engine.

- Configure TCP stream reassembly

  You can configure the sensor to monitor only TCP sessions that have been established by a complete three-way handshake. You can also configure how long to wait for the handshake to complete, and how long to keep monitoring a connection where no more packets have been seen. The goal is to prevent the sensor from creating alerts where a valid TCP session has not been established. There are known attacks against sensors that try to get the sensor to generate alerts by simply replaying pieces of an attack. The TCP session reassembly feature helps to mitigate these types of attacks against the sensor. You first choose the method the sensor will use to perform TCP stream reassembly, then you can tune TCP stream reassembly signatures, which are part of the Normalizer engine.

Note For signature 3050 Half Open SYN Attack, if you choose Modify Packet Inline as the action, you can see as much as 20 to 30% performance degradation while the protection is active. The protection is only active during an actual SYN flood.

- Configure IP logging options

  You can configure a sensor to generate an IP session log when the sensor detects an attack. When IP logging is configured as a response action for a signature and the signature is triggered, all packets to and from the source address of the alert are logged for a specified period of time.

For More Information

- For the procedure for setting up the AIC parameters, see Configuring Application Policy, page 10-49.
- For an example procedure for tuning AIC signatures, see Tuning an AIC Signature, page 10-50.
- For the procedure for configuring the method the sensor uses for performing IP fragment reassembly, see Configuring the IP Fragment Reassembly Mode, page 10-53.
- For an example procedure for tuning an IP fragment reassembly signature, see Tuning an IP Fragment Reassembly Signature, page 10-53.
- For the procedure for configuring the method the sensor uses to perform TCP stream reassembly, see Configuring the TCP Stream Reassembly Mode, page 10-59.
- For an example procedure for tuning a TCP stream reassembly signature, see Tuning a TCP Stream Reassembly Signature, page 10-60.
- For the procedure for configuring IP logging, see Configuring IP Logging, page 10-61.

Miscellaneous Tab Field Definitions

The following fields and buttons are found on the Miscellaneous tab:

- Application Policy—Lets you configure application policy enforcement:
  - Enable HTTP —Enables protection for web services. Check the **Yes** check box to require the sensor to inspect HTTP traffic for compliance with the RFC.
  - Max HTTP Requests—Specifies the maximum number of outstanding HTTP requests per connection.
  - AIC Web Ports—Specifies the variable for ports to look for AIC traffic.
  - Enable FTP—Enables protection for web services. Check the **Yes** check box to require the sensor to inspect FTP traffic.
- Fragment Reassembly—Lets you configure the mode for IP fragment reassembly:
  - IP Reassembly Mode—Identifies the method the sensor uses to reassemble the fragments, based on the operating system.
- Stream Reassembly—Lets you configure the mode for TCP stream reassembly:
  - TCP Handshake Required—Specifies that the sensor should only track sessions for which the three-way handshake is completed.
  - TCP Reassembly Mode—Specifies the mode the sensor should use to reassemble TCP sessions with the following options:

  - Asymmetric—Can only see one direction of bidirectional traffic flow.

    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.
  - Loose—Use in environments where packets might be dropped.
- IP Log—Lets you configure the sensor to stop an in-progress IP Log when any one of the following thresholds is reached:
  - Max IP Log Packets—Identifies the maximum number of packets per log. Valid values are 0 to 65535 packets. The default is 0 packets.
  - IP Log Time—Identifies the duration in seconds to log. Valid values are 30 to 300 seconds. The default is 30 seconds.
  - Max IP Log Bytes—Identifies the maximum size in bytes per log. Valid values are 0 to 2147483647 bytes. The default is 0 bytes.

Configuring Application Policy Signatures

This section describes Application Policy (AIC) signatures and how to configure them. It contains the following topics:

Understanding AIC Signatures

AIC has the following categories of signatures:

- HTTP request method
  - Define request method
  - Recognized request methods
- MIME type
  - Define content type
  - Recognized content type

- Define web traffic policy

  There is one predefined signature, 12674, that specifies the action to take when noncompliant HTTP traffic is seen. The parameter Alarm on Non HTTP Traffic enables the signature. By default this signature is enabled.
- Transfer encodings
  - Associate an action with each method
  - List methods recognized by the sensor
  - Specify which actions need to be taken when a chunked encoding error is seen
- FTP commands
  - Associates an action with an FTP command.

For More Information

- For more information on the AIC engine, see AIC Engine, page B-10.
- For a list of AIC request method signature IDs and descriptions, see AIC Request Method Signatures, page 10-44.
- For a list of AIC MIME define content type signature IDs and descriptions, see AIC MIME Define Content Type Signatures, page 10-45.
- For a list of AIC transfer encoding signature IDs and descriptions, see AIC Transfer Encoding Signatures, page 10-48.
- For a list of AIC FTP commands signature IDs and descriptions, see AIC FTP Commands Signatures, page 10-48.

AIC Engine and Sensor Performance

Application policy enforcement is a unique sensor feature. Rather than being based on traditional IPS technologies that inspect for exploits, vulnerabilities, and anomalies, AIC policy enforcement is designed to enforce HTTP and FTP service policies. The inspection work required for this policy enforcement is extreme compared with traditional IPS inspection work. A large performance penalty is associated with using this feature. When AIC is enabled, the overall bandwidth capacity of the sensor is reduced.

AIC policy enforcement is disabled in the IPS default configuration. If you want to activate AIC policy enforcement, we highly recommend that you carefully choose the exact policies of interest and disable those you do not need. Also, if your sensor is near its maximum inspection load capacity, we recommend that you not use this feature since it can oversubscribe the sensor. We recommend that you use the adaptive security appliance firewall to handle this type of policy enforcement.

For More Information

For more information on the AIC signature engine, see AIC Engine, page B-10.

AIC Request Method Signatures

The HTTP request method has two categories of signatures:

- Define request method—Allows actions to be associated with request methods. You can expand and modify the signatures (Define Request Method).
- Recognized request methods—Lists methods that are recognized by the sensor (Recognized Request Methods).

Table 10-1 lists the predefined define request method signatures. Enable the signatures that have the predefined method you need.

Table 10-1 Request Method Signatures

Signature ID	Define Request Method
12676	Request Method Not Recognized
12677	Define Request Method PUT
12678	Define Request Method CONNECT
12679	Define Request Method DELETE
12680	Define Request Method GET
12681	Define Request Method HEAD
12682	Define Request Method OPTIONS
12683	Define Request Method POST
12685	Define Request Method TRACE
12695	Define Request Method INDEX
12696	Define Request Method MOVE
12697	Define Request Method MKDIR
12698	Define Request Method COPY
12699	Define Request Method EDIT
12700	Define Request Method UNEDIT
12701	Define Request Method SAVE
12702	Define Request Method LOCK
12703	Define Request Method UNLOCK
12704	Define Request Method REVLABEL
12705	Define Request Method REVLOG
12706	Define Request Method REVADD
12707	Define Request Method REVNUM
12708	Define Request Method SETATTRIBUTE
12709	Define Request Method GETATTRIBUTENAME
12710	Define Request Method GETPROPERTIES
12711	Define Request Method STARTENV
12712	Define Request Method STOPREV

For More Information

For the procedure for enabling signatures, see Enabling, Disabling, and Retiring Signatures, page 10-19.

AIC MIME Define Content Type Signatures

There are two policies associated with MIME types:

- Define content type—Associates specific actions for the following cases (Define Content Type):
  - Deny a specific MIME type, such as an image/jpeg
  - Message size violation
  - MIME-type mentioned in header and body do not match
- Recognized content type (Recognized Content Type)

Table 10-2 lists the predefined define content type signatures. Enable the signatures that have the predefined content type you need. You can also create custom define content type signatures.

Table 10-2 Define Content Type Signatures

Signature ID	Signature Description
12621	Content Type image/gif Invalid Message Length
12622 2	Content Type image/png Verification Failed
12623 0 12623 1 12623 2	Content Type image/tiff Header Check Content Type image/tiff Invalid Message Length Content Type image/tiff Verification Failed
12624 0 12624 1 12624 2	Content Type image/x-3ds Header Check Content Type image/x-3ds Invalid Message Length Content Type image/x-3ds Verification Failed
12626 0 12626 1 12626 2	Content Type image/x-portable-bitmap Header Check Content Type image/x-portable-bitmap Invalid Message Length Content Type image/x-portable-bitmap Verification Failed
12627 0 12627 1 12627 2	Content Type image/x-portable-graymap Header Check Content Type image/x-portable-graymap Invalid Message Length Content Type image/x-portable-graymap Verification Failed
12628 0 12628 1 12628 2	Content Type image/jpeg Header Check Content Type image/jpeg Invalid Message Length Content Type image/jpeg Verification Failed
12629 0 12629 1	Content Type image/cgf Header Check Content Type image/cgf Invalid Message Length
12631 0 12631 1	Content Type image/x-xpm Header Check Content Type image/x-xpm Invalid Message Length
12633 0 12633 1 12633 2	Content Type audio/midi Header Check Content Type audio/midi Invalid Message Length Content Type audio/midi Verification Failed
12634 0 12634 1 12634 2	Content Type audio/basic Header Check Content Type audio/basic Invalid Message Length Content Type audio/basic Verification Failed

Table 10-2 Define Content Type Signatures (continued)

Signature ID	Signature Description
12635 0 12635 1 12635 2	Content Type audio/mpeg Header Check Content Type audio/mpeg Invalid Message Length Content Type audio/mpeg Verification Failed
12636 0 12636 1 12636 2	Content Type audio/x-adpcm Header Check Content Type audio/x-adpcm Invalid Message Length Content Type audio/x-adpcm Verification Failed
12637 0 12637 1 12637 2	Content Type audio/x-aiff Header Check Content Type audio/x-aiff Invalid Message Length Content Type audio/x-aiff Verification Failed
12638 0 12638 1 12638 2	Content Type audio/x-ogg Header Check Content Type audio/x-ogg Invalid Message Length Content Type audio/x-ogg Verification Failed
12639 0 12639 1 12639 2	Content Type audio/x-wav Header Check Content Type audio/x-wav Invalid Message Length Content Type audio/x-wav Verification Failed
12641 0 12641 1 12641 2	Content Type text/html Header Check Content Type text/html Invalid Message Length Content Type text/html Verification Failed
12642 0 12642 1	Content Type text/css Header Check Content Type text/css Invalid Message Length
12643 0 12643 1	Content Type text/plain Header Check Content Type text/plain Invalid Message Length
12644 0 12644 1	Content Type text/richtext Header Check Content Type text/richtext Invalid Message Length
12645 0 12645 1 12645 2	Content Type text/sgml Header Check Content Type text/sgml Invalid Message Length Content Type text/sgml Verification Failed
12646 0 12646 1 12646 2	Content Type text/xml Header Check Content Type text/xml Invalid Message Length Content Type text/xml Verification Failed
12648 0 12648 1 12648 2	Content Type video/flc Header Check Content Type video/flc Invalid Message Length Content Type video/flc Verification Failed
12649 0 12649 1 12649 2	Content Type video/mpeg Header Check Content Type video/mpeg Invalid Message Length Content Type video/mpeg Verification Failed
12650 0 12650 1	Content Type text/xmcd Header Check Content Type text/xmcd Invalid Message Length
12651 0 12651 1 12651 2	Content Type video/quicktime Header Check Content Type video/quicktime Invalid Message Length Content Type video/quicktime Verification Failed
12652 0 12652 1	Content Type video/sgi Header Check Content Type video/sgi Verification Failed

Table 10-2 Define Content Type Signatures (continued)

Signature ID	Signature Description
12653 0 12653 1	Content Type video/x-avi Header Check Content Type video/x-avi Invalid Message Length
12654 0 12654 1 12654 2	Content Type video/x-fli Header Check Content Type video/x-fli Invalid Message Length Content Type video/x-fli Verification Failed
12655 0 12655 1 12655 2	Content Type video/x-mng Header Check Content Type video/x-mng Invalid Message Length Content Type video/x-mng Verification Failed
12656 0 12656 1 12656 2	Content Type application/x-msvideo Header Check Content Type application/x-msvideo Invalid Message Length Content Type application/x-msvideo Verification Failed
12658 0 12658 1	Content Type application/ms-word Header Check Content Type application/ms-word Invalid Message Length
12659 0 12659 1	Content Type application/octet-stream Header Check Content Type application/octet-stream Invalid Message Length
12660 0 12660 1 12660 2	Content Type application/postscript Header Check Content Type application/postscript Invalid Message Length Content Type application/postscript Verification Failed
12661 0 12661 1	Content Type application/vnd.ms-excel Header Check Content Type application/vnd.ms-excel Invalid Message Length
12662 0 12662 1	Content Type application/vnd.ms-powerpoint Header Check Content Type application/vnd.ms-powerpoint Invalid Message Length
12663 0 12663 1 12663 2	Content Type application/zip Header Check Content Type application/zip Invalid Message Length Content Type application/zip Verification Failed
12664 0 12664 1 12664 2	Content Type application/x-gzip Header Check Content Type application/x-gzip Invalid Message Length Content Type application/x-gzip Verification Failed
12665 0 12665 1	Content Type application/x-java-archive Header Check Content Type application/x-java-archive Invalid Message Length
12666 0 12666 1	Content Type application/x-java-vm Header Check Content Type application/x-java-vm Invalid Message Length
12667 0 12667 1 12667 2	Content Type application/pdf Header Check Content Type application/pdf Invalid Message Length Content Type application/pdf Verification Failed
12668 0 12668 1	Content Type unknown Header Check Content Type unknown Invalid Message Length
12669 0 12669 1	Content Type image/x-bitmap Header Check Content Type image/x-bitmap Invalid Message Length
12673 0	Recognized content type

For More Information

For the procedure for enabling signatures, see Enabling, Disabling, and Retiring Signatures, page 10-19

AIC Transfer Encoding Signatures

There are three policies associated with transfer encoding:

- Associate an action with each method (Define Transfer Encoding)
- List methods recognized by the sensor (Recognized Transfer Encodings)
- Specify which actions need to be taken when a chunked encoding error is seen (Chunked Transfer Encoding Error)

Table 10-3 lists the predefined transfer encoding signatures. Enable the signatures that have the predefined transfer encoding method you need.

Table 10-3 Transfer Encoding Signatures

Signature ID	Transfer Encoding Method
12686	Recognized Transfer Encoding
12687	Define Transfer Encoding Deflate
12688	Define Transfer Encoding Identity
12689	Define Transfer Encoding Compress
12690	Define Transfer Encoding GZIP
12693	Define Transfer Encoding Chunked
12694	Chunked Transfer Encoding Error

For More Information

For the procedure for enabling signatures, see Enabling, Disabling, and Retiring Signatures, page 10-19

AIC FTP Commands Signatures

Table 10-4 lists the predefined FTP commands signatures. Enable the signatures that have the predefined FTP command you need.

Table 10-4 FTP Commands Signatures

Signature ID	FTP Command
12900	Unrecognized FTP command
12901	Define FTP command abor
12902	Define FTP command acct
12903	Define FTP command allo
12904	Define FTP command appe
12905	Define FTP command cdup
12906	Define FTP command cwd
12907	Define FTP command dele

Table 10-4 FTP Commands Signatures (continued)

Signature ID	FTP Command
12908	Define FTP command help
12909	Define FTP command list
12910	Define FTP command mkd
12911	Define FTP command mode
12912	Define FTP command nlst
12913	Define FTP command noop
12914	Define FTP command pass
12915	Define FTP command pasv
12916	Define FTP command port
12917	Define FTP command pwd
12918	Define FTP command quit
12919	Define FTP command rein
12920	Define FTP command rest
12921	Define FTP command retr
12922	Define FTP command rmd
12923	Define FTP command rnfr
12924	Define FTP command rnto
12925	Define FTP command site
12926	Define FTP command smnt
12927	Define FTP command stat
12928	Define FTP command stor
12929	Define FTP command stou
12930	Define FTP command stru
12931	Define FTP command syst
12932	Define FTP command type
12933	Define FTP command user

For More Information

For the procedure for enabling signatures, see Enabling, Disabling, and Retiring Signatures, page 10-19

Configuring Application Policy

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

To configure the application policy parameters, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures > Advanced > Miscellaneous**.

Step 3 In the Enable HTTP field, choose **Yes** from the drop-down list to enable inspection of HTTP traffic.

Step 4 In the Max HTTP Requests field, enter the number of outstanding HTTP requests per connection that can be outstanding without having received a response from the server.

Step 5 In the AIC Web Ports field, enter the ports that you want to be active.

Step 6 In the Enable FTP field choose **Yes** from the drop-down list to enable inspection of FTP traffic.

Note If you enable the application policy for HTTP or FTP, the sensor checks to be sure the traffic is compliant with the RFC.

Tip To discard your changes, click **Cancel**.

Step 7 Click **OK**.

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

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

Tuning an AIC Signature

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

The following example demonstrates how to tune an AIC signature, a Recognized Content Type (MIME) signature, specifically, signature 12,623 1 Content Type image/tiff Invalid Message Length.

To tune a MIME-type policy signature, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 From the Filter drop-down list, choose **Engine** and then choose **AIC HTTP** as the engine.

Step 4 Scroll down the list and select Sig ID 12,623 Subsig ID 1 Content Type image/tiff Invalid Message Length, and click **Edit**.

Tip You can click the Sig ID column head to have the signature IDs appear in order.

Step 5 Under Status, choose **Yes** from the drop-down list in the Enabled field.

Step 6 Under Engine, choose one of the options, for example, **Length**, in the Content Type Details field.

Step 7 In the Length field, make the length smaller by changing the default to 30,000.

Tip To discard your changes and close the Edit Signature dialog box, click **Cancel**.

Step 8 Click **OK**, and then click **Apply** to save your changes.

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

Configuring IP Fragment Reassembly Signatures

This section describes IP fragment reassembly, lists the IP fragment reassembly signatures with their configurable parameters, and describes how to configure them. It contains the following topics:

- Understanding IP Fragment Reassembly Signatures, page 10-51
- IP Fragment Reassembly Signatures and Configurable Parameters, page 10-52
- Configuring the IP Fragment Reassembly Mode, page 10-53
- Tuning an IP Fragment Reassembly Signature, page 10-53

Understanding IP Fragment Reassembly Signatures

You can configure the sensor to reassemble a datagram that has been fragmented over multiple packets. You can specify boundaries that the sensor uses to determine how many datagram fragments it reassembles and how long to wait for more fragments of a datagram. The goal is to ensure that the sensor does not allocate all its resources to datagrams that cannot be completely reassembled, either because the sensor missed some frame transmissions or because an attack has been launched that is based on generating random fragmented datagrams.

Note You configure the IP fragment reassembly per signature.

For More Information

For more information on the Normalizer engine, see Normalizer Engine, page B-35.

IP Fragment Reassembly Signatures and Configurable Parameters

Table 10-5 lists IP fragment reassembly signatures with the parameters that you can configure for IP fragment reassembly. The IP fragment reassembly signatures are part of the Normalizer engine.

Table 10-5 IP Fragment Reassembly Signatures

Signature ID and Name	Description	Parameter With Default Value and Range	Default Action
1200 IP Fragmentation Buffer Full	Fires when the total number of fragments in the system exceeds the threshold set by Max Fragments.	Specify Max Fragments 10000 (0-42000)	Deny Packet Inline Produce Alert[1]
1201 IP Fragment Overlap	Fires when the fragments queued for a datagram overlap each other.	—[2]	Deny Packet Inline Produce Alert[1]
1202 IP Fragment Overrun - Datagram Too Long	Fires when the fragment data (offset and size) exceeds the threshold set with Max Datagram Size.	Specify Max Datagram Size 65536 (2000-65536)	Deny Packet Inline Produce Alert[3]
1203 IP Fragment Overwrite - Data is Overwritten	Fires when the fragments queued for a datagram overlap each other and the overlapping data is different.[4]	—	Deny Packet Inline Produce Alert[5]
1204 IP Fragment Missing Initial Fragment	Fires when the datagram is incomplete and missing the initial fragment.	—	Deny Packet Inline Produce Alert[6]
1205 IP Fragment Too Many Datagrams	Fires when the total number of partial datagrams in the system exceeds the threshold set by Max Partial Datagrams.	Specify Max Partial Datagrams 1000 (0-10000)	Deny Packet Inline Produce Alert[7]
1206 IP Fragment Too Small	Fires when there are more than Max Small Frags of a size less than Min Fragment Size in one datagram.[8]	Specify Max Small Frags 2 (8-1500) Specify Min Fragment Size 400 (1-8)	Deny Packet Inline Produce Alert[9]
1207 IP Fragment Too Many Fragments in a Datagram	Fires when there are more than Max Fragments per Datagram in one datagram.	Specify Max Fragments per Datagram 170 (0-8192)	Deny Packet Inline Produce Alert[6]
1208 IP Fragment Incomplete Datagram	Fires when all of the fragments for a datagram have not arrived during the Fragment Reassembly Timeout.[10]	Specify Fragment Reassembly Timeout 60 (0-360)	Deny Packet Inline Produce Alert[6]
1225 Fragment Flags Invalid	Fires when a bad combination of fragment flags is detected.	—[11]	—

1. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packets and all associated fragments for this datagram. If you disable this signature, the default values are still used and packets are dropped (inline mode) or not analyzed (promiscuous mode) and no alert is sent.
2. This signature does not fire when the datagram is an exact duplicate. Exact duplicates are dropped in inline mode regardless of the settings. Modify Packet Inline removes the overlapped data from all but one fragment so there is no ambiguity about how the endpoint treats the datagram. Deny Connection Inline has no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
3. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram. Regardless of the actions set the datagram is not processed by the IPS if the datagram is larger than the Max Datagram size.
4. This is a very unusual event.
5. Modify Packet Inline removes the overlapped data from all but one fragment so there is no ambiguity about how the endpoint treats the datagram. Deny Connection Inline has no effect on this signature. Deny Packet Inline drops the packets and all associated fragments for this datagram.

6. IPS does not inspect a datagram missing the first fragments regardless of the settings. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
7. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
8. IPS does not inspect the datagram if this signature is on and the number of small fragments is exceeded.
9. Modify Packet Inline and Deny Connection Inline have no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.
10. The timer starts when the packet for the datagram arrives.
11. Modify Packet Inline modifies the flags to a valid combination. Deny Connection Inline has no effect on this signature. Deny Packet Inline drops the packet and all associated fragments for this datagram.

Configuring the IP Fragment Reassembly Mode

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Note You can configure the IP fragment reassembly mode if your sensor is operating in promiscuous mode. If your sensor is operating inline mode, the method is NT only.

To configure the mode the sensor uses for IP fragment reassembly, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures > Advanced > Miscellaneous**.

Step 3 Under Fragment Reassembly, from the IP Reassembly Mode field choose the operating system you want to use to reassemble the fragments.

Tip To discard your changes and close the Advanced dialog box, click **Cancel**.

Step 4 Click **OK**, and then **Apply** to apply your changes and save the revised configuration

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

Tuning an IP Fragment Reassembly Signature

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

The following procedure demonstrates how to tune an IP fragment reassembly signature, specifically, signature 1200 0 IP Fragmentation Buffer Full.

To tune an IP fragment reassembly signature, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 In the Filter field, choose **Engine** from the drop-down list, and then choose **Normalizer** as the engine.

Step 4 Select the IP fragment reassembly signature you want to configure in the list, for example, Sig ID 1200 Subsig ID 0 IP Fragmentation Buffer Full, and then click **Edit**.

Step 5 Change the default setting of any IP fragment reassembly parameters that can be configured for signature 1200. For example, in the Max Fragments field change the setting from the default of 10000 to 20000. For signature 1200, you can also change the parameters of these options:

- Specify TCP Idle Timeout
- Specify Service Ports
- Specify SYN Flood Max Embryonic

Tip To discard your changes and close the Edit Signature dialog box, click **Cancel**.

Step 6 Click **OK**, and then **Apply** to apply your changes and save the revised configuration

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

Configuring TCP Stream Reassembly Signatures

This section describes TCP stream reassembly, lists the TCP stream reassembly signatures with the configurable parameters, describes how to configure TCP stream signatures, and how to configure the mode for TCP stream reassembly. This section contains the following topics:

Understanding TCP Stream Reassembly Signatures

You can configure the sensor to monitor only TCP sessions that have been established by a complete three-way handshake. You can also configure how long to wait for the handshake to complete, and how long to keep monitoring a connection where no more packets have been seen. The goal is to prevent the sensor from creating alerts where a valid TCP session has not been established. There are known attacks against sensors that try to get the sensor to generate alerts by simply replaying pieces of an attack. The TCP session reassembly feature helps to mitigate these types of attacks against the sensor.

You configure TCP stream reassembly parameters per signature. You can configure the mode for TCP stream reassembly.

For More Information

For more information on Normalizer engine, see Normalizer Engine, page B-35.

TCP Stream Reassembly Signatures and Configurable Parameters

Table 10-6 lists TCP stream reassembly signatures with the parameters that you can configure for TCP stream reassembly. TCP stream reassembly signatures are part of the Normalizer engine.

Table 10-6 TCP Stream Reassembly Signatures

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1301 TCP Session Inactivity Timeout[1]	Fires when a TCP session has been idle for a TCP Idle Timeout.	TCP Idle Timeout 3600 (15-3600)	—[2]
1302 TCP Session Embryonic Timeout[3]	Fires when a TCP session has not completes the three-way handshake in TCP embryonic timeout seconds.	TCP Embryonic Timeout 15 (3-300)	—[4]
1303 TCP Session Closing Timeout[5]	Fires when a TCP session has not closed completely in TCP Closed Timeout seconds after the first FIN.	TCP Closed Timeout 5 (1-60)	—[6]
1304 TCP Session Packet Queue Overflow	This signature allows for setting the internal TCP Max Queue size value for the Normalizer engine. As a result it does not function in promiscuous mode. By default this signature does not fire an alert. If a custom alert event is associated with this signature and if the queue size is exceeded, an alert fires. **Note** The IPS signature team discourages modifying this value.	TCP Max Queue 32 (0-128) TCP Idle Timeout 3600	—[7]
1305 TCP Urg Flag Set[8]	Fires when the TCP urgent flag is seen	TCP Idle Timeout 3600	Modify Packet Inline[9]

Table 10-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1306 0 TCP Option Other	Fires when a TCP option in the range of TCP Option Number is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Option Number 6-7,9-255 (Integer Range Allow Multiple 0-255 constraints) TCP Idle Timeout 3600	Modify Packet Inline Produce Alert[10]
1306 1 TCP SACK Allowed Option	Fires when a TCP selective ACK allowed option is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline[11]
1306 2 TCP SACK Data Option	Fires when a TCP selective ACK data option is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline[12]
1306 3 TCP Timestamp Option	Fires when a TCP timestamp option is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline[13]
1306 4 TCP Window Scale Option	Fires when a TCP window scale option is seen. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline[14]
1306 5 TCP MSS Option	Fires when a TCP MSS option is detected. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline
1306 6 TCP option data after EOL option	Fires when the TCP option list has data after the EOL option. All 1306 signatures fire an alert and do not function in promiscuous mode.	TCP Idle Timeout 3600	Modify Packet Inline
1307 TCP Window Variation	Fires when the right edge of the recv window for TCP moves to the right (decreases).	TCP Idle Timeout 3600	Deny Connection Inline Produce Alert[15]
1308 TTL Evasion[16]	Fires when the TTL seen on one direction of a session is higher than the minimum that has been observed.	TCP Idle Timeout 3600	Modify Packet Inline[17]

Table 10-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1309 TCP Reserved Flags Set	Fires when the reserved bits (including bits used for ECN) are set on the TCP header.	TCP Idle Timeout 3600	Modify Packet Inline Produce Alert[18]
1311 TCP Packet Exceeds MSS	Fires when a packet exceeds the MSS that was exchanged during the three-way handshake.	TCP Idle Timeout 3600	Produce Alert[19]
1312 TCP MSS Below Minimum	Fires when the MSS value in a packet containing a SYN flag is less that TCP Min MSS.	TCP Min MSS 400 (0-16000) TCP Idle Timeout 3600	Modify Packet Inline[20]
1313 TCP Max MSS	Fires when the MSS value in a packet containing a SYN flag exceed TCP Max MSS	TCP Max MSS1460 (0-16000)	Modify Packet Inline disabled[21]
1314 TCP Data SYN	Fires when TCP payload is sent in the SYN packet.	—	Deny Packet Inline disabled[22]
1315 ACK Without TCP Stream	Fires when an ACK packet is sent that does not belong to a stream.	—	Produce Alert disabled[23]
1317 Zero Window Probe	Fires when a zero window probe packet is detected.	Modify Packet Inline removes data from the Zero Window Probe packet.	Modify Packet Inline
1330[24] 0 TCP Drop - Bad Checksum	Fires when TCP packet has bad checksum.	Modify Packet Inline corrects the checksum.	Deny Packet Inline
1330 1 TCP Drop - Bad TCP Flags	Fires when TCP packet has bad flag combination.	—	Deny Packet Inline
1330 2 TCP Drop - Urgent Pointer With No Flag	Fires when TCP packet has a URG pointer and no URG flag.	Modify Packet Inline clears the pointer.	Modify Packet Inline disabled
1330 3 TCP Drop - Bad Option List	Fires when TCP packet has a bad option list.	—	Deny Packet Inline
1330 4 TCP Drop - Bad Option Length	Fires when TCP packet has a bad option length.	—	Deny Packet Inline
1330 5 TCP Drop - MSS Option Without SYN	Fires when TCP MSS option is seen in packet without the SYN flag set.	Modify Packet Inline clears the MSS option.	Modify Packet Inline
1330 6 TCP Drop - WinScale Option Without SYN	Fires when TCP window scale option is seen in packet without the SYN flag set.	Modify Packet Inline clears the window scale option.	Modify Packet Inline

Table 10-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1330 7 TCP Drop - Bad WinScale Option Value	Fires when a TCP packet has a bad window scale value.	Modify Packet Inline sets the value to the closest constraint value.	Modify Packet Inline
1330 8 TCP Drop - SACK Allow Without SYN	Fires when the TCP SACK allowed option is seen in a packet without the SYN flags set.	Modify Packet Inline clears the SACK allowed option.	Modify Packet Inline
1330 9 TCP Drop - Data in SYN|ACK	Fires when TCP packet with SYN and ACK flags set also contains data.	—	Deny Packet Inline
1330 10 TCP Drop - Data Past FIN	Fires when TCP data is sequenced after FIN.	—	Deny Packet Inline
1330 11 TCP Drop - Timestamp not Allowed	Fires when TCP packet has timestamp option when timestamp option is not allowed.	—	Deny Packet Inline
1330 12 TCP Drop - Segment Out of Order	Fires when TCP segment is out of order and cannot be queued.	—	Deny Packet Inline
1330 13 TCP Drop - Invalid TCP Packet	Fires when TCP packet has invalid header.	—	Deny Packet Inline
1330 14 TCP Drop - RST or SYN in window	Fires when TCP packet with RST or SYN flag was sent in the sequence window but was not the next sequence.	—	Deny Packet Inline
1330 15 TCP Drop - Segment Already ACKed	Fires when TCP packet sequence is already ACKed by peer (excluding keepalives).	—	Deny Packet Inline
1330 16 TCP Drop - PAWS Failed	Fires when TCP packet fails PAWS check.	—	Deny Packet Inline
1330 17 TCP Drop - Segment out of State Order	Fires when TCP packet is not proper for the TCP session state.	—	Deny Packet Inline
1330 18 TCP Drop - Segment out of Window	Fires when TCP packet sequence number is outside of allowed window.	—	Deny Packet Inline
3050 Half Open SYN Attack		syn-flood-max-embryonic 5000	
3250 TCP Hijack		max-old-ack 200	
3251 TCP Hijack Simplex Mode		max-old-ack 100	

1. The timer is reset to 0 after each packet on the TCP session. by default, this signature does not produce an alert. You can choose to produce alerts for expiring TCP connections if desired. A statistic of total number of expired flows is updated any time a flow expires.

2. Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
3. The timer starts with the first SYN packet and is not reset. State for the session is reset and any subsequent packets for this flow appear to be out of order (unless it is a SYN).
4. Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
5. The timer starts with the first FIN packet and is not reset. State for the session is reset and any subsequent packets for this flow appear to be out of order (unless it is a SYN).
6. Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
7. Modify Packet Inline and Deny Packet Inline have no effect on this signature. Deny Connection Inline drops the current packet and the TCP session.
8. Phrak 57 describes a way to evade security policy using URG pointers. You can normalize the packet when it is in inline mode with this signature.
9. Modify Packet Inline strips the URG flag and zeros the URG pointer from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
10. Modify Packet Inline strips the selected option(s) from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
11. Modify Packet Inline strips the selected ACK allowed option from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
12. Modify Packet Inline strips the selected ACK allowed option from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
13. Modify Packet Inline strips the timestamp option from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
14. Modify Packet Inline strips the window scale option from the packet. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
15. Modify Packet Inline has no effect on this signature. Deny Connection Inline drops the current packet and the TCP connection. Deny Packet Inline drops the packet.
16. This signature is used to cause TTLs to monotonically decrease for each direction on a session. For example, if TTL 45 is the lowest TTL seen from A to B, then all future packets from A to B will have a maximum of 45 if Modify Packet Inline is set. Each new low TTL becomes the new maximum for packets on that session.
17. Modify Packet Inline ensures that the IP TTL monotonically decreases. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
18. Modify Packet Inline clears all reserved TCP flags. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
19. Modify Packet Inline has no effect on this signature. Deny Connection Inline drops the current packet and the TCP connection. Deny Packet Inline drops the packet.
20. 2.4.21-15.EL.cisco.1 Modify Packet Inline raises the MSS value to TCP Min MSS. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet 2.4.21-15.EL.cisco.1.
21. Modify Packet Inline lowers the MSS value to TCP Max MSS. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet 2.4.21-15.EL.cisco.1.
22. Modify Packet Inline has no effect on this signature. Deny Connection Inline drops the current packet and the TCP session. Deny Packet Inline drops the packet.
23. Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature. By default, the 1330 signatures drop packets for which this signature sends alerts.
24. These subsignatures represent the reasons why the Normalizer might drop a TCP packet. By default these subsignatures drop packets. These subsignatures let you permit packets that fail the checks in the Normalizer through the IPS. The drop reasons have an entry in the TCP statistics. By default these subsignatures do not produce an alert.

Configuring the TCP Stream Reassembly Mode

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Note The parameters TCP Handshake Required and TCP Reassembly Mode only impact sensors inspecting traffic in promiscuous mode, not inline mode. To configure asymmetric options for sensors inspecting inline traffic, use the Normalizer Mode parameter.

To configure the TCP stream reassembly mode, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures > Advanced > Miscellaneous**.

Step 3 Under Stream Reassembly, in TCP Handshake Required field, choose **Yes**. Choosing TCP Handshake Required specifies that the sensor should only track sessions for which the three-way handshake is completed.

Step 4 In the TCP Reassembly Mode field, from the drop-down list, choose the mode the sensor should use to reassemble TCP sessions:

- **Asymmetric**—Lets the sensor synchronize state with the flow and maintain inspection for those engines that do not require both directions.
- **Strict**—If a packet is missed for any reason, all packets after the missed packet are processed.
- **Loose**—Use in environments where packets might be dropped.

Tip To discard your changes and close the Advanced dialog box, click **Cancel**.

Step 5 Click **OK**, and then **Apply** to apply your changes and save the revised configuration

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

For More Information

For information on asymmetric inspection options for sensors configured in inline mode, see Inline TCP Session Tracking Mode, page 8-3 and Adding, Editing, and Deleting Virtual Sensors, page 8-12.

Tuning a TCP Stream Reassembly Signature

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution For signature 3050 Half Open SYN Attack, if you choose Modify Packet Inline as the action, you can see as much as 20 to 30% performance degradation while the protection is active. The protection is only active during an actual SYN flood.

The following procedure demonstrates how to tune a TCP stream reassembly signatures, for example, signature 1313 0 TCP MSS Exceeds Maximum.

To tune a TCP stream reassembly signature, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**.

Step 3 From the Filter drop-down list, choose **Engine** and then choose **Normalizer**.

Step 4 Select the TCP fragment reassembly signature you want to configure in the list, for example, Sig ID 1313 Subsig ID 0 TCP MSS Exceeds Maximum, and click **Edit**.

Step 5 Change the default setting of any configurable IP fragment reassembly parameters for signature 1313. For example, in the TCP Max MSS field, change the setting from the default of 1460 to 1380. Changing this parameter from the default of 1460 to 1380 helps prevent fragmentation of traffic going through a VPN tunnel.

Step 6 For signature 1313 0, you can also change the parameters of these options:

- Specify Hijack Max Old Ack
- Specify TCP Idle Timeout
- Specify Service Ports
- Specify SYN Flood Max Embryonic

Tip To discard your changes and close the Edit Signature dialog box, click **Cancel**.

Step 7 Click **OK**, and then **Apply** to apply your changes and save the revised configuration

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

Configuring IP Logging

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

You can configure a sensor to generate an IP session log when the sensor detects an attack. When IP logging is configured as a response action for a signature and the signature is triggered, all packets to and from the source address of the alert are logged for a specified period of time.

Note IP logging allows a maximum limit of 20 concurrent IP log files. Once the limit of 20 is reached, you receive the following message in main.log: `Cid/W errWarnIpLogProcessor::addIpLog: Ran out of file descriptors.`

When the sensor meets any one of the IP logging conditions, it stops IP logging.

To configure IP logging parameters, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures > Advanced > Miscellaneous**.

Step 3 Under IP Log in the Max IP Log Packets field, enter the maximum number of packets per log. The range is 0 to 65535. The default is 0 packets.

Step 4 In the IP Log Time field, enter the duration in seconds you want the sensor to log. A valid value is 30 to 300 seconds. The default is 30 seconds.

Step 5 In the Max IP Log Bytes field, enter the maximum size in bytes per log. The range is 0 to 2147483647 bytes. The default is 0 bytes.

Tip To discard your changes and close the Advanced dialog box, click **Cancel**.

Step 6 Click **OK**, and then **Apply** to apply your changes and save the revised configuration

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

Using the Custom Signature Wizard

This chapter describes the Custom Signature Wizard and how to use it to create custom signatures. It contains the following sections:

Understanding the Custom Signature Wizard

Note You must be administrator or operator to create custom signatures.

The Custom Signature Wizard guides you through a step-by-step process for creating custom signatures. There are two possible sequences—using a signature engine to create your custom signature or creating the custom signature without a signature engine.

For More Information

For more information on the individual signature engines, see Appendix B, "Signature Engines."

Using a Signature Engine

The following sequence applies if you use a signature engine to create your custom signature:

Step 1 Choose a signature engine:

- Atomic IP
- Atomic IP Advanced
- Service HTTP
- Service MSRPC

- Service RPC
- State (SMTP, ...)
- String ICMP
- String TCP
- String UDP
- Sweep

Step 2 Assign the signature identification parameters:

- Signature ID
- Subsignature ID
- Signature Name
- Alert Notes (optional)
- User Comments (optional)

Step 3 Assign the engine-specific parameters. The parameters differ for each signature engine, although there is a group of master parameters that applies to each engine.

Step 4 Assign the alert response:

- Signature Fidelity Rating
- Severity of the Alert

Step 5 Assign the alert behavior. You can accept the default alert behavior. To change it, click **Advanced**, which opens the Advanced Alert Behavior wizard. With this wizard you can configure how you want to handle alerts for this signature.

Step 6 Click **Finish**.

Signature Engines Not Supported for the Custom Signature Wizard

The Custom Signature Wizard in Cisco IPS does not support creating custom signatures based on the following signature engines:

- AIC FTP
- AIC HTTP
- Atomic ARP
- Atomic IP6
- Fixed ICMP
- Fixed TCP
- Fixed UDP
- Flood Host
- Flood Net
- Meta

- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H225
- Service IDENT
- Service MSSQL
- Service NTP
- Service P2P
- Service SMB Advanced
- Service SNMP
- Service SSH
- Service TNS
- String XL ICMP
- String XL TCP
- String XL UDP
- Traffic ICMP
- Traffic Anomaly
- Trojan Bo2k
- Trojan Tfn2k
- Trojan UDP

You can create custom signatures based on these existing signature engines by cloning an existing signature from the engine you want.

Note The IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP support the String XL engines and the Regex accelerator card.

For More Information

- For more information on using the CLI to create custom signatures using these signature engines, refer to *Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.2*.
- For more information on cloning signatures, see Cloning Signatures, page 10-21.

Not Using a Signature Engine

The following sequence applies if you are not using a signature engine to create your custom signature:

Step 1 Specify the protocol you want to use:

- IP—Go to Step 3.
- ICMP—Go to Step 2.
- UDP—Go to Step 2.
- TCP—Go to Step 2.

Step 2 For ICMP and UDP protocols, select the traffic type and inspect data type. For TCP protocol, select the traffic type.

Step 3 Assign the signature identification parameters:

- Signature ID
- Subsignature ID
- Signature Name
- Alert Notes (optional)
- User Comments (optional)

Step 4 Assign the engine-specific parameters. The parameters differ for each signature engine, although there is a group of master parameters that applies to each engine.

Step 5 Assign the alert response:

- Signature Fidelity Rating
- Severity of the Alert

Step 6 Assign the alert behavior. You can accept the default alert behavior. To change it, click **Advanced**, which opens the Advanced Alert Behavior wizard. With this wizard you can configure how you want to handle alerts for this signature.

Step 7 Click **Finish**.

Creating Custom Signatures

Caution Adding a custom signature can affect sensor performance. To monitor the effect the new signature has on the sensor, choose **Configuration > *sensor_name* > Interface Configuration > Traffic Flow Notifications** and configure the Missed Packet Threshold and Notification Interval options to judge how the sensor is handling the new signature.

The Custom Signature Wizard provides a step-by-step procedure for configuring custom signatures.

To create custom signatures using the Custom Signature Wizard, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Signature Wizard**.

Step 3 If you know the specific signature engine you want to use to create the new signature, click the **Yes** radio button, choose the engine from the Select Engine drop-down list, and then click **Next.** Go to Step 12. If you do not know what engine you should use, click the **No** radio button, and then click **Next**.

Step 4 Click the radio button that best matches the type of traffic you want this signature to inspect, and then click **Next**:

- IP (for IP, go to Step 12.)
- ICMP (for ICMP, go to Step 5.)
- UDP (for UDP, go to Step 6.)
- TCP (for TCP, go to Step 8.)

Step 5 In the ICMP Traffic Type window, click one of the following radio buttons, and then click **Next**:

- Single Packet—You are creating a signature to inspect a single packet for an attack using either the Atomic IP engine (for Header Data) or the String ICMP engine. Go to Step 11.
- Sweeps—You are creating a signature to detect a sweep attack using the sweep engine for your new signature. Go to Step 12.

Step 6 In the UDP Traffic Type window, click one of the following radio buttons, and then click **Next**:

- Single Packet—You are creating a signature to inspect a single packet for an attack using either the Atomic IP engine (for Header Data) or the String UDP engine. Go to Step 11.
- Sweeps—You are creating a signature to detect a sweep attack using the sweep engine for the signature. Go to Step 7.

Step 7 In the UDP Sweep Type window, click one of the following radio buttons, and then click **Next**:

- Host Sweep—You are creating a signature that uses a sweep to search for open ports on a host. The sweep engine is used to create the new signature and the storage key is set to Axxx. Go to Step 12.
- Port Sweep—You are creating a signature that uses a sweep to search for hosts on a network. The sweep engine is used to create the new signature and the storage key is set to AxBx. Go to Step 12.

Step 8 In the TCP Traffic Type window, click one of the following radio buttons, and then click **Next**:

- Single Packet—You are creating a signature to inspect a single packet for an attack. The atomic IP engine is used to create the signature. Go to Step 12.
- Single TCP Connection—You are creating a signature to detect an attack in a single TCP connection. Go to Step 9.
- Multiple Connections—You are creating a signature to inspect multiple connections for an attack. Go to Step 10.

Step 9 In the Service Type window, click one of the following radio buttons, click **Next**, and then go to Step 12:

- HTTP—You are creating a signature to detect an attack that uses the HTTP service. The service HTTP engine is used to create the signature.
- SMTP—You are creating a signature to detect an attack that uses the SMTP service. The SMTP engine is used to create the signature.

- RPC—You are creating a signature to detect an attack that uses the RPC service. The service RPC engine is used to create the signature.
- MSRPC—You are creating a signature to detect an attack that uses the MSRPC service. The service MSRPC engine is used to create the signature.
- Other—You are creating a signature to detect an attack that uses a service other than HTTP, SMTP, or RPC. The string TCP engine is used to create the signature.

Step 10 On the TCP Sweep Type window, click one of the following radio buttons, click **Next**, and then go to Step 12:

- Host Sweep—You are creating a signature that uses a sweep to search for open ports on a host. The sweep engine is used to create the signature and the storage key is set to Axxx.
- Port Sweep—You are creating a signature that uses a sweep to search for hosts on a network. The Sweep engine is used to create the new signature and the storage key is set to AxBx.

Step 11 In the Inspect Data window, for a single packet, click one of the following radio buttons, click **Next**, and then go to Step 12:

- Header Data Only—Specifies the header as the portion of the packet you want the sensor to inspect.
- Payload Data Only—Specifies the payload as the portion of the packet you want the sensor to inspect.

Step 12 In the Signature Identification window, specify the attributes that uniquely identify this signature, and then click **Next**:

a. In the Signature ID field, enter a number for this signature. Custom signatures range from 60000 to 65000.

b. In the Subsignature ID field, enter a number for this signature. The default is 0.

You can assign a subsignature ID if you are grouping signatures together that are similar.

c. In the Signature Name field, enter a name for this signature. A default name appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

Note The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

d. (Optional) In the Alert Notes field, enter text to be added to the alert. You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated.

e. (Optional) In the User Comments field, enter text that describes this signature. You can add any text that you find useful here. This field does not affect the signature or alert in any way.

Step 13 Assign values to the engine-specific parameters, and then click **Next**.

Step 14 In the Alert Response window, specify the following alert response options:

a. In the Signature Fidelity Rating field, enter a value. The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident.

b. From the Severity of the Alert drop-down list, choose the severity to be reported by Event Viewer when the sensor sends an alert:

- High
- Informational

- Low
- Medium

Step 15 To accept the default alert behavior, click **Finish** and go to Step 22. To change the default alert behavior, click **Advanced** and continue with Step 16.

Note You can control how often this signature fires. For example, you may want to decrease the volume of alerts sent out from the sensor. Or you may want the sensor to provide basic aggregation of signature firings into a single alert. Or you may want to counter anti-IPS tools such as "stick," which are designed to send bogus traffic so that the IPS produces thousands of alerts during a very short time.

Step 16 Configure the event count, key, and interval:

a. In the Event Count field, enter a value for the event count. This is the minimum number of hits the sensor must receive before sending one alert for this signature.

b. From the Event Count Key drop-down list, choose an attribute to use as the event count key. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the event count key.

c. If you want to count events based on a rate, check the **Use Event Interval** check box, and then in the Event Interval (seconds) field, enter the number of seconds that you want to use for your interval.

d. Click **Next** to continue. The Alert Summarization window appears.

Step 17 To control the volume of alerts and configure how the sensor summarizes alerts, click one of the following radio buttons:

- Alert Every Time the Signature Fires—Specifies that you want the sensor to send an alert every time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 18.
- Alert the First Time the Signature Fires—Specifies that you want the sensor to send an alert the first time the signature detects malicious traffic. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 19.
- Send Summary Alerts—Specifies that you want the sensor to only send summary alerts for this signature instead of sending alerts every time the signature fires. You can then specify additional thresholds that let the sensor dynamically adjust the volume of alerts. Go to Step 20.
- Send Global Summary Alerts—Specifies that you want the sensor to send an alert the first time a signature fires on an address set, and then only send a global summary alert that includes a summary of all alerts for all address sets over a given time interval. Go to Step 21.

Note When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

Step 18 Configure the Alert Every Time the Signature Fires option:

a. From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

b. To use dynamic summarization, check the **Use Dynamic Summarization** check box. Dynamic summarization lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.

c. In the Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a summary alert for this signature.

d. In the Summary Interval (seconds) field, enter the number of seconds that you want to use for the time interval.

e. To have the sensor enter global summarization mode, check the **Specify Global Summary Threshold** check box.

f. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

Step 19 Configure the Alert the First Time the Signature Fires option:

a. From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

b. To have the sensor use dynamic global summarization, check the **Use Dynamic Global Summarization** check box.

c. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

Note When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

d. In the Global Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

Step 20 Configure the Send Summary Alerts option:

a. In the Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

b. From the Summary Key drop-down list, choose the type of summary key. The summary key identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, choose Attacker address as the summary key.

c. To have the sensor use dynamic global summarization, check the **Use Dynamic Global Summarization** check box.

d. In the Global Summary Threshold field, enter the minimum number of hits the sensor must receive before sending a global summary alert.

Note When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

Step 21 In the Global Summary Interval (seconds) field, enter the number of seconds during which the sensor counts events for summarization.

Step 22 Click **Finish** to save your alert behavior changes.

Step 23 Click **Finish** to save your custom signature.

Step 24 Click **Yes** to create the custom signature. The signature you created is enabled and added to the list of signatures.

Tip To discard your changes, click **Cancel**.

Custom Signature Wizard Field Definitions

This section describes the Custom Signature Wizard windows and lists the field definitions for the Custom Signature Wizard. It also contains procedure for creating three example custom signatures. It contains the following topics:

- Alert Response Window, page 11-26
- Alert Behavior Window, page 11-26

Welcome Window

The following fields are found in the Welcome window of the Custom Signature Wizard:

- Yes—Activates the Select Engine field and lets you choose from a list of signature engines.
- Select Engine—Displays the list of available signature engines. If you know which signature engine you want to use to create a signature, click **Yes**, and choose one of the following engine types from the drop-down list:
  - Atomic IP—Lets you create an Atomic IP signature.
  - Service HTTP—Lets you create a signature for HTTP traffic.
  - Service MSRPC—Lets you create a signature for MSRPC traffic.
  - Service RPC—Lets you create a signature for RPC traffic.
  - State SMTP—Lets you create a signature for SMTP traffic.
  - String ICMP—Lets you create a signature for an ICMP string.
  - String TCP—Lets you create a signature for a TCP string.
  - String UDP—Lets you create a signature for a UDP string.
  - Sweep—Lets you create a signature for a sweep.
- No—Lets you continue with the advanced engine selection screens of the Custom Signature Wizard.

Protocol Type Window

You can define a signature that looks for malicious behavior in a certain protocol. You can have the following protocols decoded and inspected by your signature:

- IP
- ICMP
- UDP
- TCP

Field Definitions

The following fields are found in the Protocol Type window of the Custom Signature Wizard:

- IP—Creates a signature to decode and inspect IP traffic.
- ICMP—Creates a signature to decode and inspect ICMP traffic.
- UDP—Creates a signature to decode and inspect UDP traffic.
- TCP—Creates a signature to decode and inspect TCP traffic.

Signature Identification Window

The signature identification parameters describe the signature but do not affect the behavior of the signature. You must have a signature ID, subsignature ID, and a signature name. The other fields are optional.

Field Definitions

The following fields are found in the Signature Identification window of the Custom Signature Wizard:

- Signature ID—Identifies the unique numerical value assigned to this signature. The signature ID lets the sensor identify a particular signature. The signature ID is reported to the Event Viewer when an alert is generated. The valid range is between 60000 and 65000.
- SubSignature ID—Identifies the unique numerical value assigned to this subsignature. The subsignature ID identifies a more granular version of a broad signature. The valid value is between 0 and 255. The subsignature is reported to the Event Viewer when an alert is generated.
- Signature Name—Identifies the name assigned to this signature. Reported to the Event Viewer when an alert is generated.
- Alert Notes—(Optional) Specifies the text that is associated with the alert if this signature fires. Reported to the Event Viewer when an alert is generated.
- User Comments—(Optional) Specifies notes or other comments about this signature that you want stored with the signature parameters.

Service MSRPC Engine Parameters Window

The Service MSRPC engine processes MSRPC packets. MSRPC allows for cooperative processing between multiple computers and their application software in a networked environment. It is a transaction-based protocol, implying that there is a sequence of communications that establishes the channel and passes processing requests and replies.

MSRPC is an ISO Layer 5-6 protocol and is layered on top of other transport protocols such as UDP, TCP, and SMB. The MSRPC engine contains facilities to allow for fragmentation and reassembly of the MSRPC PDUs.

This communication channel is the source of recent Windows NT, Windows 2000, and Window XP security vulnerabilities. The Service MSRPC engine only decodes the DCE and RPC protocol for the most common transaction types.

Field Definitions

The following fields are found in the MSRPC Engine Parameters window of the Custom Signature Wizard. These options enable you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- Specify Regex String—(Optional) Lets you specify an exact match offset, including the minimum and maximum match offset, Regex string, and minimum match length.
- Protocol—Lets you specify TCP or UDP as the protocol.

- Specify Operation—(Optional) Lets you specify an operation.
- Specify UUID—(Optional) Lets you specify a UUID.

ICMP Traffic Type Window

The following fields are found in the ICMP Traffic Type window of the Custom Signature Wizard:

- Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Sweeps—Specifies that you are creating a signature to detect a sweep attack.

Inspect Data Window

The following fields are found in the Inspect Data window of the Custom Signature Wizard:

- Header Data Only—Specifies the header as the portion of the packet you want the sensor to inspect.
- Payload Data Only—Specifies the payload as the portion of the packet you want the sensor to inspect.

UDP Traffic Type Window

The following fields are found in the UDP Traffic Type window of the Custom Signature Wizard:

- Single Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Sweeps—Specifies that you are creating a signature to detect a sweep attack.

UDP Sweep Type Window

The following fields are found in the UDP Sweep Type window of the Custom Signature Wizard:

- Host Sweep—Identifies a sweep that searches for hosts on a network.
- Port Sweep—Identifies a sweep that searches for open ports on a host.

TCP Traffic Type Window

The following fields are found in the TCP Traffic Type window of the Custom Signature Wizard:

- Single Packet—Specifies that you are creating a signature to inspect a single packet for an attack.
- Single TCP Connection—Specifies that you are creating a signature to inspect a single TCP connection for an attack.
- Multiple Connections—Specifies that you are creating a signature to inspect multiple connections for an attack.

Service Type Window

The following fields are found in the Service Type window of the Custom Signature Wizard:

- HTTP—Specifies you are creating a signature to describe an attack that uses the HTTP service.
- SMTP—Specifies you are creating a signature to describe an attack that uses the SMTP service.
- RPC—Specifies you are creating a signature to describe an attack that uses the RPC service.
- MSRPC—Specifies you are creating a signature to describe an attack that uses the MSRPC service.
- Other—Specifies you are creating a signature to describe an attack that uses a service other than HTTP, SMTP, RPC, or MSRPC.

TCP Sweep Type Window

The following fields are found in the TCP Sweep Type window of the Custom Signature Wizard:

- Host Sweep—Identifies a sweep that searches for hosts on a network.
- Port Sweep—Identifies a sweep that searches for open ports on a host.

Atomic IP Engine Parameters Window

The Atomic IP engine defines signatures that inspect IP protocol headers and associated Layer 4 transport protocols (TCP, UDP, and ICMP) and payloads. The Atomic engines do not store persistent data across packets. Instead they can fire an alert from the analysis of a single packet.

Field Definitions

The following fields are found in the Atomic IP Engine Parameters window of the Custom Signature Wizard. These options let you create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- Fragment Status—Indicates if you want to inspect fragmented or unfragmented traffic.
- Specify Layer 4 Protocol—(Optional) Lets you choose whether or not a specific protocol applies to this signature. If you choose Yes, you can choose from the following protocols:
  - ICMP Protocol—Lets you specify an ICMP sequence, type, code, identifier, and total length.
  - Other IP Protocols—Lets you specify an identifier.
  - TCP Protocol—Lets you set the TCP flags, window size, mask, payload length, urgent pointer, header length, reserved attribute, and port range for the source and destination.
  - UDP Protocol—Lets you specify a valid UDP length, length mismatch, and port range for the source and destination.
- Specify Payload Inspection—(Optional) Lets you specify the following payload inspection options.
- Specify IP Payload Length—(Optional) Lets you specify the payload length.
- Specify IP Header Length—(Optional) Lets you specify the header length.

- Specify IP Type of Service—(Optional) Lets you specify the type of service.
- Specify IP Time-to-Live—(Optional) Lets you specify the time-to-live for the packet.
- Specify IP Version—(Optional) Lets you specify the IP version.
- Specify IP Identifier—(Optional) Lets you specify an IP identifier.
- Specify IP Total Length—(Optional) Lets you specify the total IP length.
- Specify IP Option Inspection—(Optional) Lets you specify the following IP inspection options:
  - IP Option—Specifies the IP option code to match.
  - IP Option Abnormal Options—Specifies the malformed list of options.
- Specify IP Addr Options—(Optional) Lets you specify the following IP Address options:
  - Address with Localhost—Identifies traffic where the local host address is used as either the source or destination.
  - IP Address—Lets you specify the source or destination address. Use the following syntax: x.x.x.x-z.z.z.z, i.e. 10.10.10.1-10.10.10.254.
  - RFC 1918 Address—Identifies the type of address as RFC 1918.
  - Src IP Equal Dst IP—Identifies traffic where the source and destination addresses are the same.

Example Atomic IP Advanced Engine Signature

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

The following example demonstrates how to create a signature based on the Atomic IP Advanced engine. For example, the following custom signature matches any packets that are IPv6 with a HOP Option Header where the header is type 1 and the length is 8.

To create a signature based on the Atomic IP Advanced engine, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures**, and then click **Add**.

Step 3 In the Signature ID field, enter a unique signature ID for the new signature. Custom signature IDs start at 60000.

Step 4 In the Subsignature field, enter a unique subsignature ID for the new signature.

Step 5 From the Alert Severity drop-down list, choose the severity you want to associate with this signature.

Step 6 In the Signature Fidelity Rating field, enter a value between 1and 100 to represent the signature fidelity rating for this signature.

Step 7 Leave the default value for the Promiscuous Delta field.

Step 8 Complete the signature description fields and add any comments about this signature.

Step 9 From the Engine drop-down list, choose **Atomic IP Advanced**.

Step 10 Configure the Atomic IP Advanced engine-specific parameters:

a. From the Event Action drop-down list, choose the actions you want the sensor to take when it responds to an event.

Note IPv6 does not support the following event actions: Request Block Host, Request Block Connection, or Request Rate Limit.

Tip To choose more than one action, hold down the **Ctrl** key.

b. From the IP Version drop-down list, choose **Yes** to enable the IP version, and then from the IP Version drop-down list, choose **IPv6** to enable IPv6.

c. From the HOP Options Header drop-down list, choose **Yes** to enable hop-by-hop options, and then from the HOH Present drop-down list, choose **Have HOH**.

d. From the HOH Options field, choose **Yes**, and then in the HOH Option Type field, enter **1**.

e. In the HOH Option Length drop-down list, choose **Yes** to enable hop-by-hop length, and then in the HOH Option Length field, enter **8**.

Step 11 Configure Event Counter:

a. In the Event Count field, enter the number of events you want counted (1 to 65535).

b. From the Event Count Key drop-down list, choose the key you want to use.

c. From the Specify Alert Interface drop-down list, choose whether you want to specify the alert interval (Yes or No).

d. If you chose Yes, enter the alert interval (2 to 1000) in the Alert Interval field.

Step 12 Configure the alert frequency.

Step 13 Leave the default (**Yes**) for the Enabled field.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

Step 14 Leave the default (**Yes**) for the Retired field. This places the signature in the engine.

Note A signature must not be retired for the sensor to actively detect the attack specified by the signature.

Step 15 From the Vulnerable OS List drop-down list, choose the operating systems that are vulnerable to this signature.

Tip To choose more than one action, hold down the **Ctrl** key.

Step 16 From the Mars Category drop-down list, choose the MARS categories you want this signature to identify.

Tip To choose more than one action, hold down the **Ctrl** key.

Tip To discard your changes and close the Add Signature dialog box, click **Cancel**.

Step 17 Click **OK**. The new signature appears in the list with the Type set to Custom.

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

Step 18 Click **Apply** to apply your changes and save the revised configuration.

For More Information

For more information on the Atomic IP engines, see Atomic Engine, page B-13.

Service HTTP Engine Parameters Window

The Service HTTP engine is a service-specific string-based pattern-matching inspection engine. The HTTP protocol is one of the most commonly used in networks of today. In addition, it requires the most amount of preprocessing time and has the most number of signatures requiring inspection making it critical to the overall performance of the system.

The Service HTTP engine uses a Regex library that can combine multiple patterns into a single pattern-matching table allowing a single search through the data. This engine searches traffic directed only to web services, or HTTP requests. You cannot inspect return traffic with this engine. You can specify separate web ports of interest in each signature in this engine.

HTTP deobfuscation is the process of decoding an HTTP message by normalizing encoded characters to ASCII equivalent characters. It is also known as ASCII normalization.

Before an HTTP packet can be inspected, the data must be deobfuscated or normalized to the same representation that the target system sees when it processes the data. It is ideal to have a customized decoding technique for each host target type, which involves knowing what operating system and web server version is running on the target. The Service HTTP engine has default deobfuscation behavior for the Microsoft IIS web server.

Field Definitions

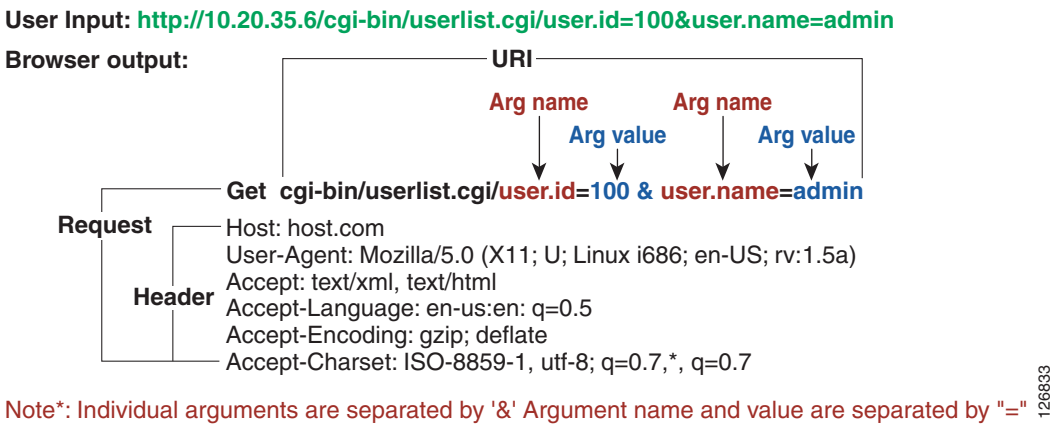
The following fields are found in the Service HTTP Engine Parameters window of the Custom Signature Wizard. These options let you create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- De Obfuscate—Specifies whether or not to apply anti-evasive HTTP deobfuscation before searching. The default is Yes.

- Max Field Sizes—(Optional) Lets you specify maximum URI, Arg, Header, and Request field lengths. The following figure demonstrates the maximum field sizes:



- Regex—Lets you specify a regular expression for the URI, Arg, Header, and Request Regex.
- Service Ports—Identifies the specific service ports used by the traffic. The value is a comma-separated list of ports.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.

Example Service HTTP Engine Signature

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

Use the Custom Signature Wizard to create a custom Service HTTP engine signature.

To create a custom Service HTTP signature, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Signature Wizard**.

Step 3 Click the **Yes** radio button, choose **Service HTTP** from the Select Engine drop-down list, and then click **Next.**

Step 4 To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:

a. In the Signature ID field, enter a number for the signature. Custom signatures range from 60000 to 65000.

b. In the Subsignature ID field, enter a number for the signature. The default is 0. You can assign a subsignature ID if you are grouping signatures together that are similar.

c. In the Signature Name field, enter a name for the signature. A default name, My Sig, appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

Note The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

d. (Optional) In the Alert Notes field, enter text to be added to the alert. You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated. The default is My Sig Info.

e. (Optional) In the User Comments field, enter text that describes this signature, and then click **Next**. You can add any text that you find useful here. This field does not affect the signature or alert in any way. The default is Sig Comment.

Step 5 Assign the event actions. The default is Produce Alert. You can assign more actions, such as deny or block, based on your security policy.

Tip To select more than one action, hold down the **Ctrl** key.

Step 6 In the De Obfuscate field, choose **Yes** from the drop-down list to configure the signature to apply anti-evasive deobfuscation before searching.

Step 7 (Optional) Under Max Field Sizes you can configure the following optional parameters for maximum field sizes:

- Specify Max URI Field Length—Enables the maximum URI field length.
- Specify Max Arg Field Length—Enables maximum argument field length.
- Specify Max Header Field Length—Enables maximum header field length.
- Specify Max Request Field Length—Enables maximum request field length.

Step 8 Under Regex, configure the Regex parameters:

a. In the Specify URI Regex field, choose **Yes** from the drop-down list.

b. In the URI Regex field, enter the URI Regex, for example, [Mm][Yy][Ff][Oo][Oo].

c. You can specify values for the following optional parameters:

- Specify Arg Name Regex—Enables searching the Arguments field for a specific regular expression.
- Specify Header Regex—Enables searching the Header field for a specific regular expression.
- Specify Request Regex—Enables searching the Request field for a specific regular expression.

Step 9 In the Service Ports field, enter the port number. For example, you can use the web ports variable, $WEBPORTS. The value is a comma-separated list of ports or port ranges where the target service resides.

Step 10 (Optional) In the Swap Attacker Victim field, choose **Yes** from the drop-down list to have the address (and ports) source and destination in the alert message swapped.

Step 11 Click **Next**.

Step 12 (Optional) You can change the following default alert response options:

a. In the Signature Fidelity Rating field, enter a value. The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident. The default is 75.

b. In the Severity of the Alert field, choose the severity to be reported by Event Viewer when the sensor sends an alert. The default is Medium.

Step 13 Click **Next**.

Step 14 To change the default alert behavior, click **Advanced**. Otherwise click **Finish** and your custom signature is created. The Create Custom Signature dialog box appears and asks if you want to create and apply this custom signature to the sensor.

Tip To discard your changes, click **Cancel**.

Step 15 Click **Yes** to create the custom signature. The signature you created is enabled and added to the list of signatures.

Service RPC Engine Parameters Window

The Service RPC engine specializes in RPC protocol and has full decode as an anti-evasive strategy. It can handle fragmented messages (one message in several packets) and batch messages (several messages in a single packet).

The RPC portmapper operates on port 111. Regular RPC messages can be on any port greater than 550. RPC sweeps are like TCP port sweeps, except that they only count unique ports when a valid RPC message is sent. RPC also runs on UDP.

Field Definitions

The following fields are found in the Service RPC Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- Direction—Indicates whether the sensor is watching traffic destined to or coming from the service port. The default is To Service.
- Protocol—Lets you specify TCP or UDP as the protocol.
- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.
- Specify Regex String—Lets you specify a Regex string to search for.
- Specify Port Map Program—Identifies the program number sent to the port mapper of interest for this signature. The valid range is 0 to 999999999.

- Specify RPC Program—Identifies the RPC program number of interest for this signature. The valid range is 0 to 1000000.
- Specify Spoof Src—Fires the alarm when the source address is set to 127.0.0.1.
- Specify RPC Max Length—Identifies the maximum allowed length of the whole RPC message. Lengths longer than this cause an alert. The valid range is 0 to 65535.
- Specify RPC Procedure—Identifies the RPC procedure number of interest for this signature. The valid range is 0 to 1000000.

State Engine Parameters Window

The State engine provides state-based regular expression-based pattern inspection of TCP streams. A state engine is a device that stores the state of an event and at a given time can operate on input to transition from one state to another and/or cause an action or output to take place. State machines are used to describe a specific event that causes an output or alarm. There are three state machines in the State engine: SMTP, Cisco Login, and LPR Format String.

Field Definitions

The following fields are found in the State Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- State Machine—Identifies the name of the state to restrict the match of the regular expression string. The options are: Cisco Login, LPR Format String, and SMTP.
- State Name—Identifies the name of the state. The options are: Abort, Mail Body, Mail Header, SMTP Commands, and Start.
- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match. The valid range is 0 to 65535.
- Regex String—Identifies the regular expression string that triggers a state transition.
- Direction—Identifies the direction of the data stream to inspect for the transition. The default is To Service.
- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.
- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offset.

String ICMP Engine Parameters Window

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data. There are three String engines: String ICMP, String TCP, and String UDP.

Field Definitions

The following fields are found in the String ICMP Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to the end of the match. The valid range is 0 to 65535.
- Regex String—Identifies the regular expression string to search for in a single packet.
- Direction—Identifies the direction of the data stream to inspect for the transition. The default is To Service.
- ICMP Type—The ICMP header TYPE value. The valid range is 0 to 18. The default is 0-18.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.
- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offsets.

String TCP Engine Parameters Window

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data. There are three String engines: String ICMP, String TCP, and String UDP.

Field Definitions

The following fields are found in the String TCP Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- Strip Telnet Options—Strips the Telnet option control characters from the data stream before the pattern is searched. This is primarily used as an anti-evasion tool. The default is No.
- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match. The valid range is 0 to 65535.
- Regex String—Identifies the regular expression string to search for in a single packet.
- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.
- Direction—Identifies the direction of the data stream to inspect for the transition. The default is To Service.
- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offsets.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.

Example String TCP Engine Signature

Tip An empty check box indicates the default value is being used. Check the check box to configure that parameter. Click the value field to change the parameter. A green check indicates that a user-defined value is being used. Click the green check to change the value back to the default.

Caution A custom signature can affect the performance of your sensor. Test the custom signature against a baseline sensor performance for your network to determine the overall impact of the signature.

Use the Custom Signature Wizard to create a custom String TCP engine signature. The following procedure also applies to creating custom String ICMP and UDP signatures.

To create a custom String TCP signature, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Signature Wizard**.

Step 3 Click the **Yes** radio button, choose **String TCP** from the Select Engine drop-down list, and then click **Next.** The Signature Identification window appears.

Step 4 To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:

a. In the Signature ID field, enter a number for the signature. Custom signatures range from 60000 to 65000.

b. In the Subsignature ID field, enter a number for the signature. The default is 0. You can assign a subsignature ID if you are grouping signatures together that are similar.

c. In the Signature Name field, enter a name for the signature. A default name, My Sig, appears in the Signature Name field. Change it to a name that is more specific for your custom signature.

Note The signature name, along with the signature ID and subsignature ID, is reported to Event Viewer when an alert is generated.

d. (Optional) In the Alert Notes field, enter text to be added to the alert. You can add text to be included in alerts associated with this signature. These notes are reported to Event Viewer when an alert is generated. The default is My Sig Info.

e. (Optional) In the User Comments field, enter text that describes this signature. You can add any text that you find useful here. This field does not affect the signature or alert in any way. The default is Sig Comment.

f. Click **Next**. The Engine Specific Parameters window appears.

Step 5 Assign the event actions. The default is Produce Alert. You can assign more actions, such as deny or block, based on your security policy.

Tip To select more than one action, hold down the **Ctrl** key.

Step 6 (Optional) In the Strip Telnet Options field, choose **Yes** from the drop-down list to strip the Telnet option characters from the data before the pattern is searched.

Step 7 (Optional) In the Specify Min Match Length field, choose **Yes** from the drop-down list to enable minimum match length, and then in the Min Match Length field, enter the minimum number of bytes the regular expression string must match (0 to 65535).

Step 8 In the Regex String field, enter the string this signature will be looking for in the TCP packet.

Step 9 In the Service Ports field, enter the port number, for example, 23. The value is a comma-separated list of ports or port ranges where the target service resides.

Step 10 From the Direction drop-down list, choose the direction of the traffic:

- From Service—Traffic from service port destined to client port.
- To Service—Traffic from client port destined to service port.

Step 11 (Optional) In the Specify Exact Match Offset field, choose **Yes** from the drop-down list to enable exact match offset. The exact match offset is the exact stream offset the regular expression string must report for a match to be valid (0 to 65535).

a. In the Specify Max Match Offset field, enter the maximum value.

b. In the Specify Min Match Offset field, enter the minimum value.

Step 12 In the Swap Attacker Victim field, choose **Yes** from the drop-down list to swap the address (and ports) source and destination in the alert message, and then click **Next**.

Step 13 (Optional) You can change the following default alert response options:

a. In the Signature Fidelity Rating field, enter a value. The signature fidelity rating is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident. The default is 75.

b. In the Severity of the Alert field, choose the severity to be reported by Event Viewer when the sensor sends an alert. The default is Medium.

Step 14 Click **Next**.

Step 15 To change the default alert behavior, click **Advanced**. Otherwise click **Finish** and your custom signature is created. The Create Custom Signature dialog box appears and asks if you want to create and apply this custom signature to the sensor.

Tip To discard your changes, click **Cancel**.

Step 16 Click **Yes** to create the custom signature. The signature you created is enabled and added to the list of signatures.

For More Information

For more information about regular expression syntax, see Regular Expression Syntax, page B-9.

String UDP Engine Parameters Window

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data. There are three String engines: String ICMP, String TCP, and String UDP.

Field Definitions

The following fields are found in the String UDP Engine Parameters window of the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- Specify Min Match Length—Identifies the minimum number of bytes the regular expression string must match from the start of the match to end of the match. The valid range is 0 to 65535.
- Regex String—Identifies the regular expression string to search for in a single packet.
- Service Ports—Identifies ports or port ranges where the target service may reside. The valid value is a comma-separated list of ports or port ranges.
- Direction—Identifies the direction of the data stream to inspect for the transition.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.
- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match. If you choose Yes, you can set the exact match offset. The valid range is 0 to 65535. If you choose No, you can set the minimum and maximum match offset.

Sweep Engine Parameters Window

The Sweep engine analyzes traffic between two hosts or from one host to many hosts. You can tune the existing signatures or create custom signatures. The Sweep engine has protocol-specific parameters for ICMP, UDP, and TCP.

The alert conditions of the Sweep engine ultimately depend on the count of the unique parameter. The unique parameter is the threshold number of distinct hosts or ports depending on the type of sweep. The unique parameter triggers the alert when more than the unique number of ports or hosts is seen on the address set within the time period. The processing of unique port and host tracking is called counting.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

A unique parameter must be specified for all signatures in the Sweep engine. A limit of 2 through 40 (inclusive) is enforced on the sweeps. 2 is the absolute minimum for a sweep, otherwise, it is not a sweep (of one host or port). 40 is a practical maximum that must be enforced so that the sweep does not consume excess memory. More realistic values for unique range between 5 and 15.

TCP sweeps must have a TCP flag and mask specified to determine which sweep inspector slot in which to count the distinct connections. ICMP sweeps must have an ICMP type specified to discriminate among the various types of ICMP packets.

Data Node

When an activity related to Sweep engine signatures is seen, the IPS uses a data node to determine when it should stop monitoring for a particular host. The data node contains various persistent counters and variables needed for cross-packet reassembly of streams and for tracking the inspection state on a per-stream/per-source/per-destination basis The data node containing the sweep determines when the sweep should expire. The data node stops a sweep when the data node has not seen any traffic for *x* number of seconds (depending on the protocol).

There are several adaptive timeouts for the data nodes. The data node expires after 30 seconds of idle time on the address set after all of the contained objects have been removed. Each contained object has various timeouts, for example, TCP Stream has a one-hour timeout for established connections. Most other objects have a much shorter expiration time, such as 5 or 60 seconds.

Field Definitions

The following fields are found in the Sweep Engine Parameters window in the Custom Signature Wizard. These options allow you to create a signature to detect a very general or very specific type of traffic.

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected. The default is Produce Alert.

Tip To select more than one action, hold down the **Ctrl** key.

- Unique—Identifies the threshold number of unique host connections. The alarm fires when the unique number of host connections is exceeded during the interval.
- Protocol—Identifies the protocol:
  - ICMP—Lets you specify the ICMP storage type and choose one of these storage keys: attacker address, attacker address and victim port, or attacker and victim addresses.
  - TCP—Lets you choose suppress reverse, inverted sweep, mask, TCP flags, fragment status, storage key, or specify a port range.
  - UDP—Lets you choose a storage key, or specify a port range.
- Src Addr Filter—Processes packets that do not have a source IP address (or addresses) defined in the filter values.

- Dst Addr Filter—Processes packets that do not have a destination IP address (or addresses) defined in the filter values.
- Swap Attacker Victim—Specifies whether to swap the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken. The default is No.

Alert Response Window

The following fields are found in the Alert Response window of the Custom Signature Wizard:

- Signature Fidelity Rating—A weight associated with how well this signature might perform in the absence of specific knowledge of the target.

  Note Signature fidelity rating is calculated by the signature author on a per-signature basis. A signature that is written with very specific rules (specific Regex) will have a higher signature fidelity rating than a signature that is written with generic rules.

- Severity of the Alert—The severity at which the alert is reported:
  - High—The most serious security alert.
  - Medium—A moderate security alert.
  - Low—The least security alert.
  - Information—Denotes network activity, not a security alert.

Alert Behavior Window

Normal alert behavior for the sensor is to send the first alert for each address set, and then to send a summary of all the alerts for this address set over the next 15 seconds. Click **Advanced** to change this alert behavior.

This section describes the Advanced Alert Behavior Wizard, and contains the following topics:

Event Count and Interval Window

The following fields are found in the Event Count and Interval window of the Advanced Alert Behavior wizard:

- Event Count—Identifies the minimum number of hits the sensor must receive before sending one alert for this signature.
- Event Count Key—Identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Event Count Key.

- Use Event Interval—Specifies that you want the sensor to count events based on a rate. For example, if set your Event Count to 500 events and your Event Interval to 30 seconds, the sensor sends you one alert if 500 events are received within 30 seconds of one another.
- Event Interval (seconds)—Identifies the time interval during which the sensor counts events for rate-based counting.

Alert Summarization Window

The following fields are found in the Alert Summarization window of the Advanced Alert Behavior wizard:

- Alert Every Time the Signature Fires—Specifies that you want the sensor to send an alert every time the signature detects malicious traffic. You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.
- Alert the First Time the Signature Fires—Specifies that you want the sensor to send an alert the first time the signature detects malicious traffic. You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.
- Send Summary Alerts—Specifies that you want the sensor to only send summary alerts for this signature, instead of sending alerts every time the signature fires. You can then specify additional thresholds that allow the sensor to dynamically adjust the volume of alerts.
- Send Global Summary Alerts—Specifies that you want the sensor to send an alert the first time a signature fires on an address set, and then only send a global summary alert that includes a summary of all alerts for all address sets over a given time interval.

Alert Dynamic Response Fire All Window

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Alert Every Time the Signature Fires:

- Summary Key—Identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.
- Use Dynamic Summarization—Lets the sensor dynamically enter summarization mode:
  - Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a summary.
  - Summary Interval (seconds)—Specifies that you want to count events based on a rate and identifies the number of seconds that you want to use for the time interval.

Note When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert for each signature to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior. A global summary counts signature firings on all attacker IP addresses and ports and all victim IP addresses and ports.

- Specify Summary Threshold—Lets you choose a summary threshold:
  - Global Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

Alert Dynamic Response Fire Once Window

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Alert the First Time the Signature Fires:

- Summary Key—Identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.
- Use Dynamic Global Summarization—Lets the sensor dynamically enter global summarization mode:
  - Global Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

    Note When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single alert the first time a signature fires to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

  - Global Summary Interval (seconds)—Identifies the time interval during which the sensor counts events for summarization.

Alert Dynamic Response Summary Window

The following fields are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you choose Summary:

Note When multiple contexts from the adaptive security appliance are contained in one virtual sensor, the summary alerts contain the context name of the last context that was summarized. Thus, the summary is the result of all alerts of this type from all contexts that are being summarized.

- Summary Interval (seconds)—Identifies the time interval during which the sensor counts events for summarization.
- Summary Key—Identifies the attribute to use for counting events. For example, if you want the sensor to count events based on whether or not they are from the same attacker, select Attacker Address as the Summary Key.
- Use Dynamic Global Summarization—Allows the sensor to dynamically enter global summarization mode:
  - Global Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

    Note When the alert rate exceeds a specified number of signatures in a specified number of seconds, the sensor changes from sending a single summary alert to sending a single global summary alert. When the rate during the interval drops below this threshold, the sensor reverts to its configured alert behavior.

Global Summarization Window

The following field is found in the Global Summarization window of the Advanced Alert Behavior wizard:

- Global Summary Interval (seconds)—Identifies the time interval during which the sensor counts events for summarization.

Configuring Event Action Rules

Note In the Event Action Rules pane, you can create event action rules policies and configure them. You can also configure event action rules in the lower half of the IPS Policies pane: **Configuration > *sensor_name* > Policies > IPS Policies**.

This chapter explains how to add event action rules policies and how to configure event action rules. It contains the following sections:

Understanding Security Policies

You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies. The use of multiple security policies lets you create security policies based on different requirements and then apply these customized policies per VLAN or physical interface.

Event Action Rules Components

This section describes the various components of event action rules, and contains the following topics:

Understanding Event Action Rules

In the Event Action Rules pane, you can add, clone, or delete an event action rules policy. The default event action rules policy is rules0. When you add a policy, a control transaction is sent to the sensor to create the policy instance. If the response is successful, the new policy instance is added under Event Action Rules. If the control transaction fails, for example because of resource limitations, an error message appears.

If your platform does not support virtual policies, this means you can only have one instance for each component and you cannot create new ones or delete the existing one. In this case, the Add, Clone, and Delete buttons are disabled.

Calculating the Risk Rating

A risk rating (RR) is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network. The calculation takes into account the value of the network asset being attacked (for example, a particular server), so it is configured on a per-signature basis using the attack severity rating and the signature fidelity rating, and on a per-server basis using the target value rating. The risk rating is calculated from several components, some of which are configured, some collected, and some derived.

Note The risk rating is associated with alerts not signatures.

Risk ratings let you prioritize alerts that need your attention. These risk rating factors take into consideration the severity of the attack if it succeeds, the fidelity of the signature, the reputation score of the attacker from the global correlation data, and the overall value of the target host to you. The risk rating is reported in the evIdsAlert.

The following values are used to calculate the risk rating for a particular event:

- Signature fidelity rating (SFR)—A weight associated with how well this signature might perform in the absence of specific knowledge of the target. The signature fidelity rating is configured per signature and indicates how accurately the signature detects the event or condition it describes.

Signature fidelity rating is calculated by the signature author on a per-signature basis. The signature author defines a baseline confidence ranking for the accuracy of the signature in the absence of qualifying intelligence on the target. It represents the confidence that the detected behavior would produce the intended effect on the target platform if the packet under analysis were allowed to be delivered. For example, a signature that is written with very specific rules (specific regular expression) has a higher signature fidelity rating than a signature that is written with generic rules.

Note The signature fidelity rating does not indicate how bad the detected event may be.

- Attack severity rating (ASR)—A weight associated with the severity of a successful exploit of the vulnerability. The attack severity rating is derived from the alert severity parameter (informational, low, medium, or high) of the signature. The attack severity rating is configured per signature and indicates how dangerous the event detected is.

  Note The attack severity rating does not indicate how accurately the event is detected.

- Target value rating (TVR)—A weight associated with the perceived value of the target.

  Target value rating is a user-configurable value (zero, low, medium, high, or mission critical) that identifies the importance of a network asset (through its IP address). You can develop a security policy that is more stringent for valuable corporate resources and looser for less important resources. For example, you could assign a target value rating to the company web server that is higher than the target value rating you assign to a desktop node. In this example, attacks against the company web server have a higher risk rating than attacks against the desktop node. Target value rating is configured in the event action rules policy.

- Attack relevance rating (ARR)—A weight associated with the relevancy of the targeted operating system. Attack relevancy rating is a derived value (relevant, unknown, or not relevant), which is determined at alert time. The relevant operating systems are configured per signature.
- Promiscuous delta (PD)—A weight associated with the promiscuous delta, which can be subtracted from the overall risk rating in promiscuous mode. Promiscuous delta is in the range of 0 to 30 and is configured per signature.

  Note If the trigger packet is not inline, the promiscuous delta is subtracted from the rating.

- Watch list rating (WLR)—A weight associated with the CSA MC watch list in the range of 0 to 100 (CSA MC only uses the range 0 to 35). If the attacker for the alert is found on the watch list, the watch list rating for that attacker is added to the rating.

Figure 12-1 illustrates the risk rating formula:

Figure 12-1 Risk Rating Formula

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

191016

Understanding Threat Rating

Threat rating is risk rating that has been lowered by event actions that have been taken. Nonlogging event actions have a threat rating adjustment. The largest threat rating from all the event actions taken is subtracted from the risk rating. The event actions have the following threat ratings:

- Deny attacker inline—45
- Deny attacker victim pair inline—40
- Deny attacker service pair inline—40
- Deny connection inline—35
- Deny packet inline—35
- Modify packet inline—35
- Request block host—20
- Request block connection—20
- Reset TCP connection—20
- Request rate limit—20

Understanding Event Action Overrides

You can add an event action override to change the actions associated with an event based on the risk rating of that event. Event action overrides are a way to add event actions globally without having to configure each signature individually. Each event action has an associated risk rating range. If a signature event occurs and the risk rating for that event falls within the range for an event action, that action is added to the event. For example, if you want any event with a risk rating of 85 or more to generate an SNMP trap, you can set the risk rating range for Request SNMP Trap to 85-100. If you do not want to use action overrides, you can disable the entire event action override component.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Understanding Event Action Filters

Event action filters are processed as an ordered list and you can move filters up or down in the list. Filters let the sensor perform certain actions in response to the event without requiring the sensor to perform all actions or remove the entire event. Filters work by removing actions from an event. A filter that removes all actions from an event effectively consumes the event.

Note When filtering sweep signatures, we recommend that you do not filter the destination addresses. If there are multiple destination addresses, only the last address is used for matching the filter.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

Event Action Summarization

Summarization decreases the volume of alerts sent out from the sensor by providing basic aggregation of events into a single alert. Special parameters are specified for each signature and they influence the handling of the alerts. Each signature is created with defaults that reflect a preferred normal behavior. However, you can tune each signature to change this default behavior within the constraints for each engine type.

The nonalert-generating actions (deny, block, TCP reset) go through the filters for each signature event unsummarized. The alert-generating actions are not performed on these summarized alerts; instead the actions are applied to the one summary alert and then put through the filters.

If you select one of the other alert-generating actions and do not have it filtered out, the alert is created even if you do not select Product Alert. To prevent alerts from being created, you must have all alert-generating actions filtered out.

Summarization and event actions are processed after the Meta engine has processed the component events. This lets the sensor watch for suspicious activity transpiring over a series of events.

Event Action Aggregation

Basic aggregation provides two operating modes. The simple mode involves configuring a threshold number of hits for a signature that must be met before the alert is sent. A more advanced mode is timed-interval counting. In this mode, the sensor tracks the number of hits per second and only sends alerts when that threshold is met. In this example, a hit is a term used to describe an event, which is basically an alert, but it is not sent out of the sensor as an alert until the threshold number of hits has been exceeded.

You can choose from the following summarization options:

- Fire All—Fires an alert each time the signature is triggered. If the threshold is set for summarization, alerts are fired for each execution until summarization occurs. After summarization starts, only one alert every summary interval fires for each address set. Alerts for other address sets are either all seen or separately summarized. The signature reverts to fire all mode after a period of no alerts for that signature.
- Summary—Fires an alert the first time a signature is triggered, and then additional alerts for that signature are summarized for the duration of the summary interval. Only one alert every summary interval should fire for each address set. If the global summary threshold is reached, the signature goes into global summarization mode.
- Global Summarization—Fires an alert for every summary interval. Signatures can be preconfigured for global summarization.
- Fire Once—Fires an alert for each address set. You can upgrade this mode to global summarization mode.

Signature Event Action Processor

The Signature Event Action Processor coordinates the data flow from the signature event in the Alarm Channel to processing through the Signature Event Action Override, the Signature Event Action Filter, and the Signature Event Action Handler. It consists of the following components:

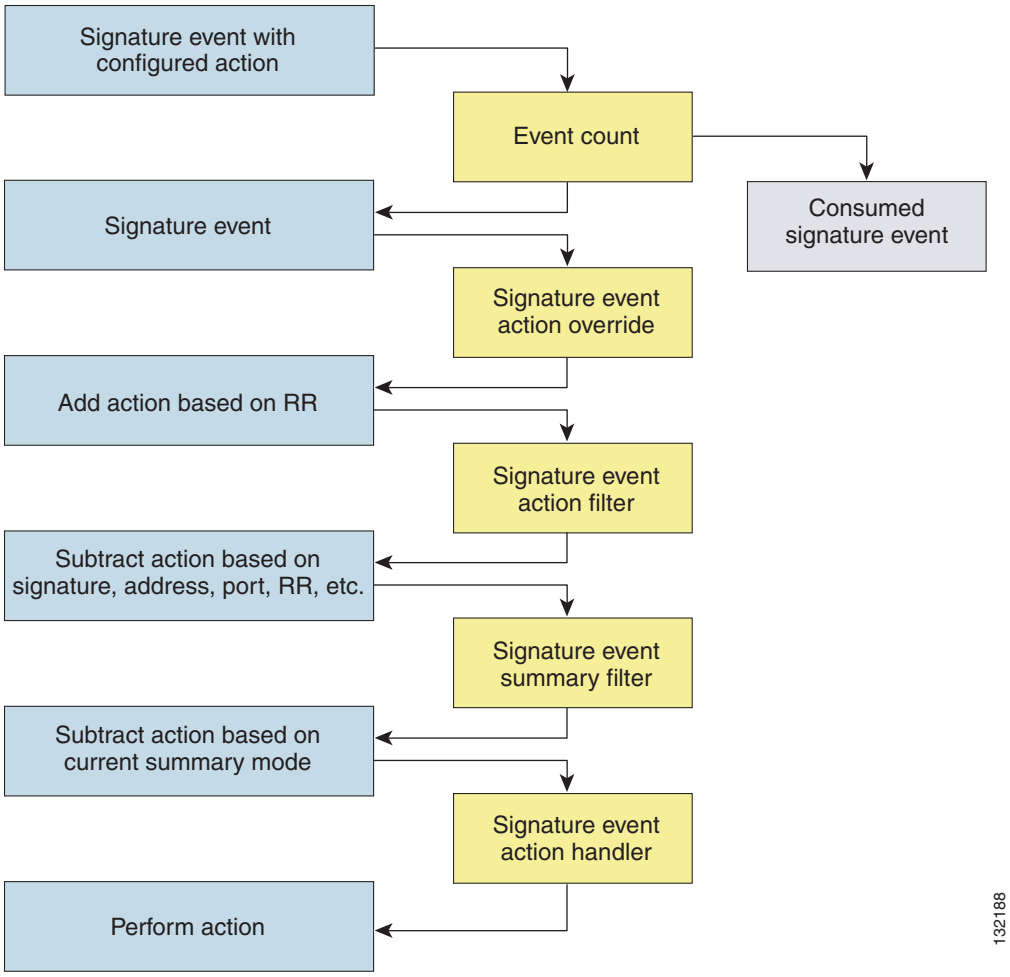
- Alarm Channel—The unit that represents the area to communicate signature events from the SensorApp inspection path to signature event handling.
- Signature Event Action Override—Adds actions based on the risk rating value. Signature Event Action Override applies to all signatures that fall in the range of the configured risk rating threshold. Each Signature Event Action Override is independent and has a separate configuration value for each action type.
- Signature Event Action Filter—Subtracts actions based on the signature ID, addresses, and risk rating of the signature event. The input to the Signature Event Action Filter is the signature event with actions possibly added by the Signature Event Action Override.

  Note The Signature Event Action Filter can only subtract actions, it cannot add new actions.

  The following parameters apply to the Signature Event Action Filter:
  - Signature ID
  - Subsignature ID
  - Attacker address
  - Attacker port
  - Victim address
  - Victim port
  - Risk rating threshold range
  - Actions to subtract
  - Sequence identifier (optional)
  - Stop-or-continue bit
  - Enable action filter line bit
  - Victim OS relevance or OS relevance
- Signature Event Action Handler—Performs the requested actions. The output from the Signature Event Action Handler is the actions being performed and possibly an evIdsAlert written to the Event Store.

Figure 12-2 on page 12-7 illustrates the logical flow of the signature event through the Signature Event Action Processor and the operations performed on the action for this event. It starts with the signature event with configured action received in the Alarm Channel and flows top to bottom as the signature event passes through the functional components of the Signature Event Action Processor.

Figure 12-2 Signature Event Through Signature Event Action Processor



Event Actions

The Cisco IPS supports the following event actions. Most of the event actions belong to each signature engine unless they are not appropriate for that particular engine.

Alert and Log Actions

- Product Alert—Writes the event to the Event Store as an alert.

Note The Product Alert action is not automatic when you enable alerts for a signature. To have an alert created in the Event Store, you must select Product Alert. If you add a second action, you must include Product Alert if you want an alert sent to the Event Store. Also, every time you configure the event actions, a new list is created and it replaces the old list. Make sure you include all the event actions you need for each signature.

Note There are other event actions that force a Product Alert. These actions use Product Alert as the vehicle for performing the action. Even if Product Alert is not selected or is filtered, the alert is still produced. The actions are the following: Produce Verbose Alert, Request SNMP Trap, Log Attacker Packets, Log Victim Packets, and Log Pair Packets.

Note A Produce Alert event action is added for an event when global correlation has increased the risk rating of an event, and has added either the Deny Packet Inline or Deny Attacker Inline event action.

- Produce Verbose Alert—Includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Attacker Packets—Starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Victim Packets—Starts IP logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Log Pair Packets—Starts IP logging on packets that contain the attacker/victim address pair. This action causes an alert to be written to the Event Store, even if Product Alert is not selected.
- Request SNMP Trap—Sends a request to the Notification Application component of the sensor to perform SNMP notification. This action causes an alert to be written to the Event Store, even if Product Alert is not selected. You must have SNMP configured on the sensor to implement this action.

Deny Actions

- Deny Packet Inline (inline only)—Terminates the packet.

Note You cannot delete the event action override for Deny Packet Inline because it is protected. If you do not want to use that override, disable it.

- Deny Connection Inline (inline only)—Terminates the current packet and future packets on this TCP flow.
- Deny Attacker Victim Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.

Note For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > General Settings**.

- Deny Attacker Service Pair Inline (inline only)—Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
- Deny Attacker Inline (inline only)—Terminates the current packet and future packets from this attacker address for a specified period of time.

- The sensor maintains a list of attackers being denied by the system. To remove an entry from the denied attacker list, you can view the list of attackers and clear the entire list, or you can wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is being denied, but issues another attack, the timer for attacker A is reset and attacker A remains in the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.

  Note This is the most severe of the deny actions. It denies current and future packets from a single attacker address. To clear all denied attacker entries, choose **Configuration > *sensor_name* > Sensor Management > Time-Based Actions > Denied Attackers > Clear List**, which permits the addresses back on the network.

- Modify Packet Inline (inline only)—Modifies packet data to remove ambiguity about what the end point might do with the packet.

  Note You cannot use Modify Packet Inline as an action when adding event action filters or overrides.

Other Actions

- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action.

  Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

  Note IPv6 does not support Request Block Connection.

- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action.

  Note IPv6 does not support Request Block Host.

  Note For block actions, to set the duration of the block, choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > General Settings**.

- Request Rate Limit—Sends a rate limit request to ARC to perform rate limiting. You must have rate limiting devices configured to implement this action.

  Note Request Rate Limit applies to a select set of signatures.

  Note IPv6 does not support Request Rate Limit.

- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow. Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

Understanding Deny Packet Inline

For signatures that have Deny Packet Inline configured as an action or for an event action override that adds Deny Packet Inline as an action, the following actions may be taken:

- Dropped Packet
- Denied Flow
- TCP One Way Reset Sent TCP

The Deny Packet Inline action is represented as a dropped packet action in the alert. When a Deny Packet Inline occurs for a TCP connection, it is automatically upgraded to a Deny Connection Inline action and seen as a denied flow in the alert. If the IPS denies just one packet, the TCP continues to try to send that same packet again and again, so the IPS denies the entire connection to ensure it never succeeds with the resends.

When a Deny Connection Inline occurs, the IPS also automatically sends a TCP one-way reset, which shows up as a TCP one-way reset sent in the alert. When the IPS denies the connection, it leaves an open connection on both the client (generally the attacker) and the server (generally the victim). Too many open connections can result in resource problems on the victim. So the IPS sends a TCP reset to the victim to close the connection on the victim side (usually the server), which conserves the resources of the victim. It also prevents a failover that would otherwise allow the connection to fail over to a different network path and reach the victim. The IPS leaves the attacker side open and denies all traffic from it.

TCP Reset Differences Between IPS Appliances and ASA IPS Modules

The IPS appliance sends TCP reset packets to both the attacker and victim when Reset TCP Connection is selected. The IPS appliance sends a TCP reset packet only to the victim under the following circumstances:

- When a Deny Packet Inline or Deny Connection Inline is selected
- When TCP-based signatures and Reset TCP Connection have NOT been selected

In the case of the ASA IPS modules, the TCP reset request is sent to the ASA, and then the ASA sends the TCP reset packets. The ASA sends TCP reset packets to both the attacker and victim when the Reset TCP Connection is selected. When Deny Packet Inline or Deny Connection Inline is selected, the ASA sends the TCP reset packet to either the attacker or victim depending on the configuration of the signature. Signatures configured to swap the attacker and victim when reporting the alert can cause the ASA to send the TCP reset packet to the attacker.

TCP Normalizer Signature Warning

You receive the following warning if you disable a default-enabled TCP Normalizer signature or remove a default-enabled Modify Packet Inline, Deny Packet Inline, or Deny Connection Inline action:

```
Use caution when disabling, retiring, or changing the event action settings of a <Sig ID>
TCP Normalizer signature for a sensor operating in IPS mode. The TCP Normalizer signature
default values are essential for proper operation of the sensor.
If the sensor is seeing duplicate packets, consider assigning the traffic to multiple
virtual sensors. If you are having problems with asymmetric or out-of-order TCP packets,
consider changing the normalizer mode from strict evasion protection to asymmetric mode
protection. Contact Cisco TAC if you require further assistance.
```

Understanding Deny Packet Inline and Reset TCP Connection

Pay attention to the following when configuring Deny Packet Inline and Reset TCP Connection:

- If you want to deny attack packets from reaching the victim and also reset the TCP connection for that flow, then you must configure BOTH Deny Packet Inline AND Reset TCP Connection.
- Configuring Reset TCP Connection alone only resets the TCP connection but the attack packet is not denied from reaching the victim.
- Configuring Deny Packet Inline alone only denies the attack packet from reaching the victim. It does not trigger a TCP reset.

For More Information

- For the procedure for configuring the general settings, see Configuring the General Settings, page 12-34.
- For the procedure for configuring SNMP, see Chapter 18, "Configuring SNMP."
- For the procedure for configuring denied attackers, see Configuring and Monitoring Denied Attackers, page 17-1.

Configuring Event Action Rules Policies

This section describes how to create event action rules policies, and contains the following topics:

Event Action Rules Pane

Note You must be administrator or operator to add, clone, or delete event action rules policies.

In the Event Action Rules pane, you can add, clone, or delete an event action rules policy. The default event action rules policy is rules0. When you add a policy, a control transaction is sent to the sensor to create the policy instance. If the response is successful, the new policy instance is added under Event Action Rules. If the control transaction fails, for example because of resource limitations, an error message appears.

If your platform does not support virtual policies, this means you can only have one instance for each component and you cannot create new ones or delete the existing one. In this case, the Add, Clone, and Delete buttons are disabled.

Event Action Rules Pane Field Definitions

The following fields are found in the Event Action Rules pane:

- Policy Name—Identifies the name of this event action rules policy.
- Assigned Virtual Sensor—Identifies the virtual sensor for which this event action rules policy is assigned.

Add and Clone Policy Dialog Boxes Field Definitions

The following field is found in the Add and Clone Policy dialog boxes:

- Policy Name—Lets you create a unique name for the new policy.

Adding, Cloning, and Deleting Event Action Rules Policies

To add, clone, or delete an event action rules policy, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Event Action Rules**, and then click **Add**.

Step 3 In the Policy Name field, enter a name for the event action rules policy.

Tip To discard your changes and close the dialog box, click **Cancel**.

Step 4 Click **OK**. The event action rules policy appears in the list in the Event Action Rules pane.

Step 5 To clone an existing event action rules policy, select it in the list, and then click **Clone**. The Clone Policy dialog box appears with "_copy" appended to the existing event action rules policy name.

Step 6 In the Policy Name field, enter a unique name.

Tip To discard your changes and close the dialog box, click **Cancel**.

Step 7 Click **OK**. The cloned event action rules policy appears in the list in the Event Action Rules pane.

Step 8 To remove an event action rules policy, select it, and then click **Delete**. The Delete Policy dialog box appears asking if you are sure you want to delete this policy permanently.

Caution You cannot delete the default event action rules policy, rules0.

Step 9 Click **Yes**. The event action rules policy no longer appears in the list in the Event Action Rules pane.

rules0 Pane

The Event Action Rules (rules0) pane contains seven tabs on which you can configure event action overrides, event action filters, target value ratings, OS identifications, event variables, risk categories, and general settings for the event action rules policies that you added in the **Configuration > *sensor_name* > Policies > Event Action Rules** pane.

You can also configure event action rules in the lower half of the **Configuration > *sensor_name* > Policies > IPS Policies** pane.

Configuring Event Action Overrides

This section describes how to configure event action overrides, and contains the following topics:

Event Action Overrides Tab

Note You must be administrator or operator to add or edit event action overrides.

On the Event Action Overrides tab, you can add an event action override to change the actions associated with an event based on specific details about that event.

Event Action Overrides Tab Field Definitions

The following fields are found on the Event Action Overrides tab:

- Use Event Action Overrides—If checked, lets you use any event action override that is enabled.
- Risk Rating—Indicates the risk rating level that should be used to trigger this event action override.

  If an event occurs with a risk rating that matches this level, the event action is added to this event.
- Actions to Add—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
- Enabled—Indicates whether or not the override is enabled.

Add and Edit Event Action Override Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Event Action Override dialog boxes:

- Risk Rating—Indicates the risk rating range, either low, medium, or high risk, that should be used to trigger this event action override. If an event occurs with a risk rating that corresponds to the risk you configure, the event action is added to this event.

- Available Actions to Add—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
- Enabled—Check the check box to enable the action when the event action override is triggered.

Adding, Editing, Deleting, Enabling, and Disabling Event Action Overrides

To add, edit, delete, enable, and disable event action overrides, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration** > *sensor_name* > **Policies > Event Action Rules > rules0 > Event Action Overrides**.

Step 3 To create a event action override, click **Add**.

Step 4 From the Risk Rating drop-down menu, assign a risk rating range to this network asset.

Step 5 From the Available Actions to Add list, check the event actions to which this event action override will correspond.

Step 6 Check the Enabled check boxes for the actions you want to enable in the override.

Tip To discard your changes and close the Add Event Action Override dialog box, click **Cancel**.

Step 7 Click **OK**. The new event action override now appears in the list on the Event Action Overrides tab.

Step 8 Check the **Use Event Action Overrides** check box.

Note You must check the **Use Event Action Overrides** check box on the Event Action Overrides tab or none of the event action overrides will be enabled regardless of the value you set.

Step 9 To edit an existing event action override, select it in the list, and then click **Edit**. Make any changes needed.

Tip To discard your changes and close the Edit Event Action Override dialog box, click **Cancel**.

Step 10 Click **OK**. The edited event action override now appears in the list on the Event Action Overrides tab.

Step 11 Check the **Use Event Action Overrides** check box.

Note You must check the **Use Event Action Overrides** check box on the Event Action Overrides tab or none of the event action overrides will be enabled regardless of the value you set.

Step 12 To delete an event action override, select it in the list, and then click **Delete**. The event action override no longer appears in the list on the Event Action Overrides tab.

Step 13 To enable or disable an event action override, select it in the list, and then click **Edit**.

Step 14 To disable an event action override, clear the **Enabled** check boxes for any event actions that you have assigned to that event action override. To enable an event action override, check any **Enabled** check boxes for any event actions that you have assigned to that event action override.

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

Step 15 Click **Apply** to apply your changes and save the revised configuration.

Configuring Event Action Filters

This section describes how to configure event action filters, and contains the following topics:

Event Action Filters Tab

Note You must be administrator or operator to add, edit, enable, disable, or delete event action filters.

You can configure event action filters to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor. You can use the variables that you defined on the Event Variables pane to group addresses for your filters.

You must preface the variable with a dollar sign ($) to indicate that you are using a variable rather than a string. Otherwise, you receive the `Bad source and destination` error.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

Event Action Filters Tab Field Definitions

The following fields are found on the Event Action Filters tab:

- Name—Lets you name the filter you are adding. You need to name your filters so that you can move them around in the list and move them to the inactive list if needed.
- Enabled—Indicates whether or not this filter is enabled.
- Sig ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. You can also enter a range of signatures.
- SubSig ID—Identifies the unique numerical value assigned to this subsignature. The subSig ID identifies a more granular version of a broad signature. You can also enter a range of subSig IDs.
- Attacker (IPv4/IPv6/port)—Identifies the IP address and/or port of the host that sent the offending packet. You can also enter a range of addresses or ports.

- Victim (IPv4/IPv6/port)—Identifies the IP address and/or port used by the attacker host. You can also enter a range of addresses or ports.
- Risk Rating—Indicates the risk rating range between 0 and 100 that should be used to trigger this event action filter. If an event occurs with an risk rating that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
- Actions to Subtract—Indicates the actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter.

Add and Edit Event Action Filter Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Event Action Filter dialog boxes:

- Name—Lets you name the filter you are adding. You need to name your filters so that you can move them around in the list and move them to the inactive list if needed.
- Enabled—Lets you enable this filter.
- Signature ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature. You can also enter a range of signatures.
- Subsignature ID—Identifies the unique numerical value assigned to this subsignature. The subsignature ID identifies a more granular version of a broad signature. You can also enter a range of subsignature IDs.
- Attacker IPv4 Address—Identifies the IP address of the host that sent the offending packet. You can also enter a range of addresses.
- Attacker IPv6 Address—Identifies the range set of attacker IPv6 addresses of the host that sent the offending packet in the following format:

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  Example—2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888. The second IPv6 address in the range must be greater than or equal to the first IPv6 address.

  Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

- Attacker Port—Identifies the port used by the attacker host. This is the port from where the offending packet originated. You can also enter a range of ports.
- VictimIPv4 Address—Identifies the IP address of the host being attacked (the recipient of the offending packet). You can also enter a range of addresses.
- VictimIPv6 Address—Identifies the range set of victim IPv6 addresses of the host that is the being attacked (the recipient of the offending packet) in the following format:

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  Example—2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888. The second IPv6 address in the range must be greater than or equal to the first IPv6 address.

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

- Victim Port—Identifies the port through which the offending packet was received. You can also enter a range of ports.
- Risk Rating—Indicates the risk rating range between 0 and 100 that should be used to trigger this event action filter. If an event occurs with a risk rating that falls within the minimum-maximum range you configure here, the event is processed against the rules of this event filter.
- Actions to Subtract—Opens the Edit Actions dialog box and lets you choose the actions that should be removed from the event, should the conditions of the event meet the criteria of the event action filter.
- More Options
  - Active—Lets you add the filter to the filter list so that it takes effect on filtering events.
  - OS Relevance—Lets you filter out events where the attack is not relevant to the victim operating system.
  - Deny Percentage—Determines the percentage of packets to deny for deny attacker features. The valid range is 0 to 100. The default is 100 percent.
  - Stop on Match—Determines whether or not this event will be processed against remaining filters in the event action filters list. If set to No, the remaining filters are processed for a match until a Stop flag is encountered. If set to Yes, no further processing is done. The actions specified by this filter are removed and the remaining actions are performed.
  - Comments—Displays the user comments associated with this filter.

Adding, Editing, Deleting, Enabling, Disabling, and Moving Event Action Filters

To add, edit, delete, enable, disable, and move event action filters, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > Event Action Filters**, and then click **Add**.

Step 3 In the Name field, enter a name for the event action filter. A default name is supplied, but you can change it to a more meaningful name.

Step 4 In the Enabled field, click the **Yes** radio button to enable the filter.

Step 5 In the Signature ID field, enter the signature IDs of all signatures to which this filter should be applied. You can use a list (2001, 2004), or a range (2001–2004), or one of the SIG variables you defined on the Event Variables tab. Preface the variable with $.

Step 6 In the SubSignature ID field, enter the subsignature IDs of the subsignatures to which this filter should be applied.

Step 7 In the Attacker IPv4 Address field, enter the IP address of the source host. You can use a variable you defined on the Event Variables tab. Preface the variable with $. You can also enter a range of addresses (for example, 0.0.0.0-255.255.255.255).

Step 8 In the Attacker IPv6 Address field, enter the range set of attacker IPv6 addresses of the source host in the following format:

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>].

The second IPv6 address in the range must be greater than or equal to the first IPv6 address. You can also use a variable you defined on the Event Variables tab. Preface the variable with $.

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Step 9 In the Attacker Port field, enter the port number used by the attacker to send the offending packet.

Step 10 In the Victim IPv4 Address field, enter the IP address of the recipient host. You can use one of the variables if you defined them on the Event Variables tab. Preface the variable with $. You can also enter a range of addresses (for example, 0.0.0.0-255.255.255.255).

Step 11 In the Victim IPv6 Address field, enter the range set of IPv6 address of the recipient host in the following format.

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>].

The second IPv6 address in the range must be greater than or equal to the first IPv6 address. You can use a variable you defined on the Event Variables tab. Preface the variable with $.

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Step 12 In the Victim Port field, enter the port number used by the victim host to receive the offending packet.

Step 13 In the Risk Rating field, enter a risk rating range for this filter. If the risk rating for an event falls within the range you specify, the event is processed against the criteria of this filter.

Step 14 In the Actions to Subtract field, click the note icon to open the Edit Actions dialog box. Check the check boxes of the actions you want this filter to remove from the event.

Tip To choose more than one event action in the list, hold down the **Ctrl** key.

Step 15 In the Active field, click the **Yes** radio button to add this filter to the list so that it takes effect on filtering events.

Step 16 In the OS Relevance drop-down list, choose whether you want to know if the alert is relevant to the operating system that has been identified for the victim.

Step 17 In the Deny Percentage field, enter the percentage of packets to deny for deny attacker features. The default is 100 percent.

Step 18 In the Stop on Match field, click one of the following radio buttons:

a. **Yes**—If you want the Event Action Filters component to stop processing after the actions of this particular filter have been removed. Any remaining filters will not be processed; therefore, no additional actions can be removed from the event.

b. **No**—If you want to continue processing additional filters.

Step 19 In the Comments field, enter any comments that you want to store with this filter, such as the purpose of this filter or why you have configured this filter in a particular way.

Tip To discard your changes and close the Add Event Action Filter dialog box, click **Cancel**.

Step 20 Click **OK**. The new event action filter now appears in the list on the Event Action Filters tab.

Step 21 To edit an existing event action filter, select it in the list, and then click **Edit**.

Step 22 Make any changes needed.

Tip To discard your changes and close the Edit Event Action Filter dialog box, click **Cancel**.

Step 23 Click **OK**. The edited event action filter now appears in the list on the Event Action Filters tab.

Step 24 To delete an event action filter, select it in the list, and then click **Delete**. The event action filter no longer appears in the list on the Event Action Filters tab.

Step 25 To move an event action filter up or down in the list, select it, and then click the **Move Up** or **Move Down** arrow icons.

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

Step 26 Click **Apply** to apply your changes and save the revised configuration.

Configuring IPv4 Target Value Rating

This section describes how to configure IPv4 target value ratings, and contains the following topics:

IPv4 Target Value Rating Tab

Note You must be administrator or operator to add, edit, or delete target value ratings.

You can assign a target value rating to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert. You can assign different target value ratings to different targets. Events with a higher risk rating trigger more severe signature event actions.

IPv4 Target Value Rating Tab Field Definitions

The following fields are found on the IPv4 Target Value Rating tab:

- Target Value Rating (TVR)—Identifies the value assigned to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IP Address—Identifies the IP address of the network asset you want to prioritize with a target value rating.

Add and Edit Target Value Rating Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Target Value Rating dialog boxes:

- Target Value Rating (TVR)—Lets you assign a value to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IPv4 Address(es)—Identifies the IP address of the network asset you want to prioritize with a target value rating.

Adding, Editing, and Deleting IPv4 Target Value Ratings

To add, edit, and delete the IPv4 target value rating for network assets, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > IPv4 Target Value Rating**, and then click **Add**.

Step 3 To assign a target value rating to a new group of assets, follow these steps:

a. From the Target Value Rating (TVR) drop-down list, choose a rating. The values are High, Low, Medium, Mission Critical, or No Value.

b. In the Target IPv4 Address(es) field, enter the IP address of the network asset. To enter a range of IP addresses, enter the lowest address followed by a hyphen and then the highest address in the range. For example: 10.10.2.1-10.10.2.30.

Tip To discard your changes and close the Add Target Value Rating dialog box, click **Cancel**.

Step 4 Click **OK**. The new target value rating for the new asset appears in the list on the IPv4 Target Value Rating tab.

Step 5 To edit an existing target value rating, select it in the list, and then click **Edit**.

Step 6 Make any changes needed.

Tip To discard your changes and close the Edit Target Value Rating dialog box, click **Cancel**.

Step 7 Click **OK**. The edited network asset now appears in the list on the IPv4 Target Value Rating tab.

Step 8 To delete a network asset, select it in the list, and then click **Delete**. The network asset no longer appears in the list on the Ipv4 Target Value Rating tab.

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

Step 9 Click **Apply** to apply your changes and save the revised configuration.

Configuring IPv6 Target Value Rating

This section describes how to configure IPv6 target value ratings, and contains the following topics:

IPv6 Target Value Rating Tab

Note You must be administrator or operator to add, edit, or delete target value ratings.

You can assign a target value rating to your network assets. The target value rating is one of the factors used to calculate the risk rating value for each alert. You can assign different target value ratings to different targets. Events with a higher risk rating trigger more severe signature event actions.

IPv6 Target Value Rating Tab Field Definitions

The following fields are found on the IPv6 Target Value Rating tab:

- Target Value Rating (TVR)—Identifies the value assigned to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IP Address—Identifies the IP address of the network asset you want to prioritize with a target value rating.

Add and Edit IPv6 Target Value Rating Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Target Value Rating dialog boxes:

- Target Value Rating (TVR)—Lets you assign a value to this network asset. The value can be High, Low, Medium, Mission Critical, or No Value.
- Target IPv6 Address(es)—Identifies the IPv6 address of the network asset you want to prioritize with a target value rating in the following format:

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  Example—2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888. The second IPv6 address in the range must be greater than or equal to the first IPv6 address.

  Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Adding, Editing, and Deleting IPv6 Target Value Ratings

To add, edit, and delete the IPv6 target value rating for network assets, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > IPv6 Target Value Rating**, and then click **Add**.

Step 3 To assign a target value rating to a new group of assets, follow these steps:

a. From the Target Value Rating (TVR) drop-down list, choose a rating. The values are High, Low, Medium, Mission Critical, or No Value.

b. In the Target IPv6 Address(es) field, enter the IP address of the network asset.

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>].

You can also use a variable you defined on the Event Variables tab. Preface the variable with $. The second IPv6 address in the range must be greater than or equal to the first IPv6 address.

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Tip To discard your changes and close the Add Target Value Rating dialog box, click **Cancel**.

Step 4 Click **OK**. The new target value rating for the new asset appears in the list on the IPv6 Target Value Rating tab.

Step 5 To edit an existing target value rating, select it in the list, and then click **Edit**.

Step 6 Make any changes needed.

Tip To discard your changes and close the Edit Target Value Rating dialog box, click **Cancel**.

Step 7 Click **OK**. The edited network asset now appears in the list on the IPv6 Target Value Rating tab.

Step 8 To delete a network asset, select it in the list, and then click **Delete**. The network asset no longer appears in the list on the IPv6 Target Value Rating tab.

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

Step 9 Click **Apply** to apply your changes and save the revised configuration.

Configuring OS Identifications

This section describes how to configure OS identifications, and contains the following topics:

OS Identifications Tab

Note You must be administrator or operator to add, edit, and delete configured OS maps.

Use the OS Identifications tab to configure OS host maps, which take precedence over learned OS maps. On the OS Identifications tab you can add, edit, and delete configured OS maps. You can move them up and down in the list to change the order in which the sensor computes the attack relevance rating and risk rating for that particular IP address and OS type combination.

You can also move OS maps up and down in the list to change the order in which the sensor resolves the OS associated with a particular IP address. Configured OS maps allow for ranges. More specific maps should be at the beginning of the list. Overlap in the IP address range sets is allowed, but the entry closest to the beginning of the list takes precedence. For example, for network 192.168.1.0/24 an administrator might define the following (Table 12-1):

Table 12-1 Example Configured OS Maps

IP Address Range Set	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10,192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

Understanding Passive OS Fingerprinting

Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK packets exchanged on the network to determine the OS type.

The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk rating of the alert for the attack and/or the sensor may filter the alert for the attack. You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the victim OS, the source of the OS identification, and the relevance to the victim OS in the alert.

Passive OS fingerprinting consists of three components:

- Passive OS learning—Passive OS learning occurs as the sensor observes traffic on the network. Based on the characteristics of TCP SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address.
- User-configurable OS identification—You can configure OS host maps, which take precedence over learned OS maps.
- Computation of attack relevance rating and risk rating—The sensor uses OS information to determine the relevance of the attack signature to the targeted host. The attack relevance is the attack relevance rating component of the risk rating value for the attack alert. The sensor uses the OS type reported in the host posture information imported from the CSA MC to compute the attack relevance rating.

There are three sources of OS information. The sensor ranks the sources of OS information in the following order:

1. Configured OS maps—OS maps you enter. Configured OS maps reside in the event action rules policy and can apply to one or many virtual sensors.

   Note You can specify multiple operating systems for the same IP address. The last one in the list is the operating system that is matched.

2. Imported OS maps—OS maps imported from an external data source. Imported OS maps are global and apply to all virtual sensors.

Note Currently the CSA MC is the only external data source.

3. Learned OS maps—OS maps observed by the sensor through the fingerprinting of TCP packets with the SYN control bit set. Learned OS maps are local to the virtual sensor that sees the traffic.

When the sensor needs to determine the OS for a target IP address, it consults the configured OS maps. If the target IP address is not in the configured OS maps, the sensor looks in the imported OS maps. If the target IP address is not in the imported OS maps, the sensor looks in the learned OS maps. If it cannot find it there, the sensor treats the OS of the target IP address as unknown.

Note Passive OS fingerprinting is enabled by default and the IPS contains a default vulnerable OS list for each signature.

Configuring Passive OS Fingerprinting

You do not have to configure passive OS fingerprinting for it to function. IPS provides a default vulnerable OS list for each signature and passive analysis is enabled by default.

You can configure the following aspects of passive OS fingerprinting:

- Define OS maps—We recommend configuring OS maps to define the identity of the OS running on critical systems. It is best to configure OS maps when the OS and IP address of the critical systems are unlikely to change.
- Limit the attack relevance rating calculation to a specific IP address range—This limits the attack relevance rating calculations to IP addresses on the protected network.
- Import OS maps—Importing OS maps provides a mechanism for accelerating the learning rate and fidelity of the OS identifications made through passive analysis. If you have an external product interface, such as the CSA MC, you can import OS identifications from it.
- Define event action rules filters using the OS relevance value of the target—This provides a way to filter alerts solely on OS relevance.
- Disable passive analysis—Stops the sensor from learning new OS maps.
- Edit signature vulnerable OS lists—The vulnerable OS list specifies what OS types are vulnerable to each signature. The default, General OS, applies to all signatures that do not specify a vulnerable OS list.

OS Identifications Tab Field Definitions

The following fields are found on the OS Identifications tab:

- Enable passive OS fingerprinting analysis—When checked, lets the sensor perform passive OS analysis.
- Restrict Attack Relevance Ratings (ARR) to these IP addresses—Lets you configure the mapping of OS type to a specific IP address and have the sensor calculate the attack relevance rating for that IP address.
- Configured OS Maps—Displays the attributes of the configured OS maps:
  - Name—Specifies the name you give the configured OS map.

  - Active—Whether this configured OS map is active or inactive.
  - IP Address—Specifies the IP address of this configured OS map.
  - OS Type—Specifies the OS type of this configured OS map.

Add and Edit Configured OS Map Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Configured OS Map dialog boxes:

- Name—Specifies the name of this configured OS map.
- Active—Lets you choose to make the configured OS map active or inactive.
- IP Address—Specifies the IP address associated with this configured OS map. The IP address for configured OS maps (and *only* configured OS maps) can be a set of IP addresses and IP address ranges. The following are all valid IP address values for configured OS maps:
  - 10.1.1.1,10.1.1.2,10.1.1.15
  - 10.1.2.1
  - 10.1.1.1-10.2.1.1,10.3.1.1
  - 10.1.1.1-10.1.1.5
- OS Type—Lets you choose one of the following OS types to associate with the IP address:
  - AIX
  - BSD
  - General OS
  - HP UX
  - IOS
  - IRIX
  - Linux
  - Mac OS
  - Netware
  - Other
  - Solaris
  - UNIX
  - Unknown OS
  - Win NT
  - Windows
  - Windows NT/2K/XP

Adding, Editing, Deleting, and Moving Configured OS Maps

To add, edit, delete, and move configured OS maps, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > OS Identifications**, and then click **Add**.

Step 3 In the Name field, enter a name for the configured OS map.

Step 4 In the Active field, click the **Yes** radio button to add this configured OS map to the list so that it takes effect.

Step 5 In the IP Address field, enter the IP address of the host that you are mapping to an OS. For example, use this format, 10.10.5.5,10.10.2.1-10.10.2.30.

Step 6 From the OS Type drop-down list, choose the OS that will be mapped to the IP address.

Tip To discard your changes and close the Add Configured OS Map dialog box, click **Cancel**.

Step 7 Click **OK**. The new configured OS map now appears in the list on the OS Identifications tab.

Step 8 Check the **Enable passive OS fingerprinting analysis** check box.

Note You must check the **Enable passive OS fingerprinting analysis** check box on the OS Identifications tab or none of the configured OS maps will be enabled regardless of the value you set in the Add Configured OS Map dialog box.

Step 9 To edit a configured OS map, select it in the list, and then click **Edit**.

Step 10 Make any changes needed.

Tip To discard your changes and close the Edit Configured OS Map dialog box, click **Cancel**.

Step 11 Click **OK**. The edited configured OS map now appears in the list on the OS Identifications tab.

Step 12 Check the **Enable passive OS fingerprinting analysis** check box.

Note You must check the **Enable passive OS fingerprinting analysis** check box on the OS Identifications tab or none of the configured OS maps will be enabled regardless of the value you set in the Edit Configured OS Map dialog box.

Step 13 To delete a configured OS map, select it in the list, and then click **Delete**. The configured OS map no longer appears in the list on the OS Identifications tab.

Step 14 To move a configured OS map up or down in the list, select it, and then click the **Move Up** or **Move Down** arrows.

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

Step 15 Click **Apply** to apply your changes and save the revised configuration.

Configuring Event Variables

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

Event Variables Tab

Note You must be administrator or operator to add, edit, or delete event variables.

You can create event variables and then use those variables in event action filters. When you want to use the same value within multiple filters, use a variable. When you change the value of the variable, any filter that uses that variable is updated with the new value.

Note You must preface the event variable with a dollar ($) sign to indicate that you are using a variable rather than a string.

Some variables cannot be deleted because they are necessary to the signature system. If a variable is protected, you cannot select it to edit it. You receive an error message if you try to delete protected variables. You can edit only one variable at a time.

IPv4 Addresses

When configuring IPv4 addresses, specify the full IP address or ranges or set of ranges:

- 192.0.2.3-192.0.2.26
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 192.0.2.3-192.0.2.26

IPv6 Addresses

When configuring IPv6 addresses, use the following format:

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Timesaver If you have an IP address space that applies to your engineering group and there are no Windows systems in that group, and you are not worried about any Windows-based attacks to that group, you could set up a variable to be the IP address space of the engineering group. You could then use this variable to configure a filter that would ignore all Windows-based attacks for this group.

Event Variables Tab Field Definitions

The following fields are found on the Event Variables tab:

- Name—Lets you assign a name to this variable.
- Type—Identifies the variable as an address.
- Value—Lets you add the value(s) represented by this variable.

Add and Edit Event Variable Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Event Variable dialog boxes:

- Name—Lets you assign a name to this variable.
- Type—Identifies the variable as an IPv4 or IPv6 address:
  - address—For IPv4 address use a full IP address or range or set of ranges.
  - ipv6-address—For IPv6 address use the following format: <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

    Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

- Value—Lets you add the value(s) represented by this variable.

Adding, Editing, and Deleting Event Variables

To add, edit, and delete event variables, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > Event Variables**, and then click **Add**.

Step 3 In the Name field, enter a name for this variable.

Note A valid name can only contain numbers or letters. You can also use a hyphen (-) or an underscore (_).

Step 4 From the Type drop-down list, choose **address** for an IPv4 address or **ipv6-address** for an IPv6 address.

Step 5 In the Value field, enter the values for this variable.

For IPv4 addresses, specify the full IP address or ranges or set of ranges. For example:

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255

Note You can use commas as delimiters. Make sure there are no trailing spaces after the comma. Otherwise, you receive a `Validation failed` error.

For IPv6 address, use the following format:

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

Note IPv6 addresses are 128 bits represented in hexadecimal and divided into eight 16-bit groups separated by colons. You can skip the leading zeros and you can represent the zeroed groups in the middle with a double colon (::). You must start the address with the 2001:db8 prefix.

Tip To discard your changes and close the Add Event Variable dialog box, click **Cancel**.

Step 6 Click **OK**. The new variable appears in the list on the Event Variables tab.

Step 7 To edit an existing variable, select it in the list, and then click **Edit**.

Step 8 Make any changes needed.

Tip To discard your changes and close the Edit Event Variable dialog box, click **Cancel**.

Step 9 Click **OK**. The edited event variable now appears in the list on the Event Variables tab.

Step 10 To delete an event variable, select it in the list, and then click **Delete**. The event variable no longer appears in the list on the Event Variables tab.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring Risk Category

This section describes how to configure risk categories, and contains the following topics:

Risk Category Tab

Note You must be administrator to add and edit risk levels.

On the Risk Category tab, you can use predefined risk categories (HIGHRISK, MEDIUMRISK, AND LOWRISK) or you can define your own labels. Risk categories link a category name to a numeric range defining the risk rating. You specify the low threshold for the category to make sure that the ranges are contiguous. The upper category is either the next higher category or 100.

Note You cannot delete a predefined risk category.

Risk Category Tab Field Definitions

The following fields are found on the Risk Category tab:

- Risk Category Name—Specifies the name of this risk level. The predefined categories have the following values:
  - HIGHRISK—90 (means 90 to 100)
  - MEDIUMRISK—70 (means 70-89)
  - LOWRISK—1 (means 1-69)
- Risk Threshold—Specifies the threshold number for this risk. The value is a number from 0 to 100.
- Risk Range—Specifies the risk rating range for this risk category. The risk rating is a range between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.

Add and Edit Risk Level Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Risk Level dialog boxes:

- Risk Name—Specifies the name of this risk level.
- Risk Threshold—Lets you assign a risk threshold for this risk level. You specify or change only the lower threshold for the category so that the risk categories are contiguous. The upper threshold is either the next higher category or 100.
- Active—Lets you make this risk level active.

Adding, Editing, and Deleting Risk Categories

To add, edit, and delete risk categories, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > Risk Category**, and then click **Add**.

Step 3 In the Risk Name field, enter a name for this risk category.

Step 4 In the Risk Threshold field, enter a numerical value for the risk threshold (minimum 0, maximum 100). This number represents the lower boundary of risk. The range appears in the Risk Range field and in the red, yellow, and green threshold fields.

Step 5 To make this risk category active, click the **Yes** radio button.

Tip To discard your changes and close the Add Risk Category dialog box, click **Cancel**.

Step 6 Click **OK**. The new risk category appears in the list on the Risk Category tab.

Step 7 To edit an existing risk category, select it in the list, and then click **Edit**.

Step 8 Make any changes needed.

Tip To discard your changes and close the Edit Risk Category dialog box, click **Cancel**.

Step 9 Click **OK**. The edited risk category now appears in the list on the Risk Category tab.

Step 10 To delete a risk category, select it in the list, and then click **Delete**. The risk category no longer appears in the list on the Risk Category tab.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring Threat Category

Note You must be administrator to configure threat categories.

On the Threat Category tab, you can group threats in red, yellow, and green categories. These red, yellow, and green threshold statistics are used in event action overrides and are also shown in the Network Security Gadget on the Home page.

The red, yellow, and green threshold statistics represent the state of network security with red being the most critical. If you change a threshold, any event action overrides that had the same range as the risk category are changed to reflect the new range. The new category is inserted in to the Risk Category list according to its threshold value and is automatically assigned actions that cover its range.

Field Definitions

The following fields are found on the Threat Category tab:

- Threat Category Thresholds—Lists the numbers for the red, yellow, and green thresholds. The health statistics for network security use these thresholds to determine what level the network security is at (critical, needs attention, or normal). The overall network security value represents the least secure value (green is the most secure and red is the least secure). These color thresholds refer to the Sensor Health gadget on the Home pane:
  - Red Threat Threshold—Sets the red threat threshold. The default is 90.
  - Yellow Threat Threshold—Sets the yellow threat threshold. The default is 70.
  - Green Threat Threshold—Sets the green threat threshold. The default is 1.

For More Information

- For detailed information about the Network Security Gadget, see Network Security Gadget, page 3-8.
- For detailed information about risk category, see Configuring Risk Category, page 12-31.

Configuring General Settings

This section describes how to configure the general settings, and contains the following topics:

General Tab

Note You must be administrator or operator to configure the general settings for event action rules.

You can configure the general settings that apply globally to event action rules, such as whether you want to use the Summarizer and the Meta Event Generator. The Summarizer groups events into a single alert, thus decreasing the number of alerts the sensor sends out. The Meta Event Generator processes the component events, which lets the sensor watch for suspicious activity transpiring over a series of events.

Caution Do not disable the Summarizer or Meta Event Generator except for troubleshooting purposes. If you disable the Summarizer, every signature is set to Fire All with no summarization. If you disable the Meta Event Generator, all Meta engine signatures are disabled.

You can also use threat rating adjustment, event action filters, and you can enable one-way TCP reset. The one-way TCP reset operates for inline mode only and is an automatic addition to the deny packet inline actions. It sends a TCP reset to the victim of the alert, thus creating a black hole for the attacker and clearing the TCP resources of the victim.

Note An inline sensor now denies packets for any alert with a risk rating of greater than or equal to 90. It also issues a one-way TCP reset on TCP alerts with a risk rating of greater than or equal to 90.

You can configure how long you want to deny attackers, the maximum number of denied attackers, and how long you want blocks to last.

General Tab Field Definitions

The following fields are found the on the General tab:

- Use Summarizer—Enables the Summarizer component. By default, the Summarizer is enabled. If you disable it, all signatures are set to Fire All with no summarization. If you configure individual signatures to summarize, this configuration will be ignored if the Summarizer is not enabled.
- Use Meta Event Generator—Enables the Meta Event Generator. By default, the Meta Event Generator is enabled. If you disable the Meta Event Generator, all Meta engine signatures are disabled.
- Use Threat Rating Adjustment—Enables threat rating adjustment, which adjusts the risk rating. If disabled, then risk rating is equal to threat rating. Use Event Action Filters—Enables the event action filter component. You must check this check box to use any filter that is enabled.
- Enable One Way TCP Reset (inline only)—Enables a one-way TCP reset for deny packet inline actions for TCP-based alerts. It sends a TCP reset to the victim of the alert thus clearing the TCP resources of the victim.
- Deny Attacker Duration—Specifies the number of seconds to deny the attacker inline. The valid range is 0 to 518400. The default is 3600.
- Block Action Duration—Specifies the number of minutes to block a host or connection. The valid range is 0 to 10000000. The default is 30.
- Maximum Denied Attackers—Specifies the limit of the number of denied attackers possible in the system at any one time. The valid range is 0 to 100000000. The default is 10000.

Configuring the General Settings

Caution The general settings options operate at a global level, so enabling them affects all sensor processing of these features.

To configure the general settings for event action rules, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > General**.

Step 3 To enable the summarizer feature, check the **Use Summarizer** check box.

Caution Disable the Summarizer for troubleshooting purposes only. Otherwise, make sure the Summarizer is enabled so that all signatures you configure for summarization will actually summarize.

Step 4 To enable the meta event generator, check the **Use Meta Event Generator** check box.

Caution Disable the Meta Event Generator for troubleshooting purposes only. Otherwise, make sure the Meta Event Generator is enabled so that all Meta engine signatures are functional.

Step 5 To enable threat rating adjustment, check the **Use Threat Rating Adjustment** check box.

Step 6 To enable event action filters, check the **Use Event Action Filters** check box.

Note You must check the Use Event Action Filters check box on the General pane so that any event action filters you configured in the **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > Event Action Filters** pane are active.

Step 7 To enable one way TCP reset for deny packet inline actions, check the **Enable One Way TCP Reset** check box.

Step 8 In the Deny Attacker Duration field, enter the number of seconds you want to deny the attacker inline.

Step 9 In the Block Action Duration field, enter the number of minutes you want to block a host or connection.

Step 10 In the Maximum Denied Attackers field, enter the maximum number of denied attackers you want at any one time.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

For More Information

- For detailed information about threat rating, see Understanding Threat Rating, page 12-4.
- For detailed information about risk rating, see Calculating the Risk Rating, page 12-2.

Configuring Anomaly Detection

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

This chapter describes how to create multiple security policies and apply them to individual virtual sensors. It contains the following sections:

Understanding Security Policies

You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies. The use of multiple security policies lets you create security policies based on different requirements and then apply these customized policies per VLAN or physical interface.

Anomaly Detection Components

The following section describes the various components of anomaly detection, and contains the following topics:

Understanding Anomaly Detection

The anomaly detection component of the sensor detects worm-infected hosts. This enables the sensor to be less dependent on signature updates for protection again worms and scanners, such as Code Red and SQL Slammer and so forth. The anomaly detection component lets the sensor learn normal activity and send alerts or take 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 detects the following two situations:

- When the network starts on the path of becoming congested by worm traffic.
- When a single worm-infected source enters the network and starts scanning for other vulnerable hosts.

Worms

Caution Anomaly detection assumes it gets traffic from both directions. If the sensor is configured to see only one direction of traffic, you should turn off anomaly detection. Otherwise, when anomaly detection is running in an asymmetric environment, it identifies all traffic as having incomplete connections, that is, as scanners, and sends alerts for all traffic flows. Using asymmetric mode protection with anomaly detection enabled causes excessive resource usage and possible false positives for anomaly detection signatures.

Worms are automated, self-propagating, intrusion agents that make copies of themselves and then facilitate their spread. Worms 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 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 scanners. To spread, a worm must find new hosts. It finds them by scanning the Internet or network 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 destination IP addresses.

The events that are important for TCP protocol are nonestablished 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 nonestablished 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 only in 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 timeout 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 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 is not detected by the anomaly detection worm policies. Worms that receive a mailing list from probing files within the infected host and email this list are also not detected, because no Layer 3/Layer 4 anomaly is generated.

For More Information

- For more information about how worms operate, see Worms, page 13-2.
- For the procedure for turning off anomaly detection, refer to Disabling Anomaly Detection, page 13-35.

Anomaly Detection Modes

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

If you have anomaly detection enabled, it 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.

Anomaly detection has the following modes:

- Learning accept mode—Anomaly detection conducts an initial learning accept mode for the default period of 24 hours. We assume that during this phase no attack is being carried out. Anomaly detection creates an initial baseline, known as a knowledge base (KB), of the network traffic. The default interval value for periodic schedule is 24 hours and the default action is rotate, meaning that a new KB is saved and loaded, and then replaces the initial KB after 24 hours.

  Note Anomaly detection does not detect attacks when working with the initial KB, which is empty. After the default of 24 hours, a KB is saved and loaded and now anomaly detection also detects attacks.

Note Depending on your network complexity, you may want to have anomaly detection in learning accept mode for longer than the default 24 hours.

- Detect mode—For ongoing operation, the sensor should remain in detect mode. This is for 24 hours a day, 7 days a week. Once a KB is created and replaces the initial KB, anomaly detection detects attacks based on it. It looks at the network traffic flows that violate thresholds in the KB and sends alerts. As anomaly detection looks for anomalies, it also records gradual changes to the KB that do not violate the thresholds and thus creates a new KB. The new KB is periodically saved and takes the place of the old one thus maintaining an up-to-date KB.
- Inactive mode—You can turn anomaly detection off by putting it in inactive mode. Under certain circumstances, anomaly detection should be in inactive mode, for example, if the sensor is running in an asymmetric environment. Because anomaly detection assumes it gets traffic from both directions, if the sensor is configured to see only one direction of traffic, anomaly detection identifies all traffic as having incomplete connections, that is, as scanners, and sends alerts for all traffic flows. Having anomaly detection running also lowers performance.

Example

The following example summarizes the default anomaly detection configuration. If you add a virtual sensor at 11:00 pm and do not change the default anomaly detection configuration, anomaly detection begins working with the initial KB and only performs learning. Although it is in detect mode, it cannot detect attacks until it has gathered information for 24 hours and replaced the initial KB. At the first start time (10:00 am by default), and the first interval (24 hours by default), the learning results are saved to a new KB and this KB is loaded and replaces the initial KB. Because the anomaly detection is in detect mode by default, now that anomaly detection has a new KB, the anomaly detection begins to detect attacks.

For More Information

- For the procedure for enabling anomaly detection, see Enabling Anomaly Detection, page 13-4.
- For more information on how worms operate, see Worms, page 13-2.
- For the procedure for configuring the sensor to be in different anomaly detection modes, see Adding, Editing, and Deleting Virtual Sensors, page 8-12.

Enabling Anomaly Detection

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

To enable anomaly detection, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > IPS Policies**.

Step 3 Select the virtual sensor for which you want to turn on anomaly detection, and then click **Edit**.

Step 4 Under Anomaly Detection, choose an anomaly detection policy from the Anomaly Detection Policy drop-down list. Unless you want to use the default ad0, you must have already added a anomaly detection policy by choosing **Configuration > *sensor_name* > Policies > Anomaly Detections > Add**.

Step 5 Choose Detect as the anomaly detection mode from the AD Operational Mode drop-down list. The default is Inactive.

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

Step 6 Click **OK**.

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

Step 7 Click **Apply** to apply your changes and save the revised configuration.

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, internal, illegal, and external, each with its own thresholds.

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.

For More Information

For more information about configuring anomaly detection zones, see Configuring the Internal Zone, page 13-15, Configuring the Illegal Zone, page 13-22, and Configuring the Illegal Zone, page 13-22.

Anomaly Detection Configuration Sequence

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

You can configure the detection part of anomaly detection. You can configure a set of thresholds that override the KB learned thresholds. However, anomaly detection continues learning regardless of how you configure the detection. You can also import, export, and load a KB and you can view a KB for data.

Follow this sequence when configuring anomaly detection:

1. Create an anomaly detection policy to add to the virtual sensors. Or you can use the default anomaly detection policy, ad0.

2. Add the anomaly detection policy to your virtual sensors.
3. Enable anomaly detection.
4. Configure the anomaly detection zones and protocols.
5. For the first 24 hours anomaly detection performs learning to create a populated KB. The initial KB is empty and during the default 24 hours, anomaly detection collects data to use to populate the KB. If you want the learning period to be longer than the default period of 24 hours, you must manually set the mode to learning accept.
6. Let the sensor run in learning accept mode for at least 24 hours (the default). You should let the sensor run in learning accept mode for at least 24 hours so it can gather information on the normal state of the network for the initial KB. However, you should change the amount of time for learning accept mode according to the complexity of your network. After the time period, the sensor saves the initial KB as a baseline of the normal activity of your network.

   Note We recommend leaving the sensor in learning accept mode for at least 24 hours, but letting the sensor run in learning accept mode for longer, even up to a week, is better.

7. If you manually set anomaly detection to learning accept mode, switch back to detect mode.
8. Configure the anomaly detection parameters:
   - Configure the worm timeout and which source and destination IP addresses should be bypassed by anomaly detection. After this timeout, the scanner threshold returns to the configured value.
   - Decide whether you want to enable automatic KB updates when anomaly detection is in detect mode.
   - Configure the 18 anomaly detection worm signatures to have more event actions than just the default Produce Alert. For example, configure them to have Deny Attacker event actions.

For More Information

- For the procedure for enabling anomaly detection, see Enabling Anomaly Detection, page 13-4.
- For the procedures for putting anomaly detection in different modes, see Adding, Editing, and Deleting Virtual Sensors, page 8-12.
- For the procedure for configuring a new anomaly detection policy, see Configuring Anomaly Detections Policies, page 13-9.
- For more information on configuring zones, see Configuring the Internal Zone, page 13-15, Configuring the Illegal Zone, page 13-22, and Configuring the Illegal Zone, page 13-22.
- For more information on anomaly detection modes, see Anomaly Detection Modes, page 13-3.
- For more information about configuring learning accept mode, see Configuring Learning Accept Mode, page 13-12.
- For more information on configuring anomaly detection signatures, see Anomaly Detection Signatures, page 13-7.
- For more information on Deny Attacker event actions, see Event Actions, page 12-7.

Anomaly Detection Signatures

The Traffic Anomaly engine contains nine anomaly detection signatures covering three protocols (TCP, UDP, and other). Each signature has two subsignatures, one for the scanner and the other for the worm-infected host (or a scanner under worm attack). When anomaly detection discovers an anomaly, it triggers an alert for these signatures. All anomaly detection signatures are enabled by default and the alert severity for each one is set to high.

When a scanner is detected but no histogram anomaly occurred, the scanner signature fires for that attacker (scanner) IP address. If the histogram signature is triggered, the attacker addresses that are doing the scanning each trigger the worm signature (instead of the scanner signature). The alert details state which threshold is being used for the worm detection now that the histogram has been triggered. From that point on, all scanners are detected as worm-infected hosts.

The following anomaly detection event actions are possible:

- Produce Alert—Writes the event to the Event Store.
- Deny Attacker Inline—(Inline only) Does not transmit this packet and future packets originating from the attacker address for a specified period of time.
- Log Attacker Packets—Starts IP logging for packets that contain the attacker address.
- Deny Attacker Service Pair Inline—Blocks the source IP address and the destination port.
- SNMP Trap—Sends a request to NotificationApp to perform SNMP notification.
- Request Block Host—Sends a request to ARC to block this host (the attacker).

Table 13-1 lists the anomaly detection worm signatures.

Table 13-1 Anomaly Detection Worm Signatures

Signature ID	Subsignature ID	Name	Description
13000	0	Internal TCP Scanner	Identified a single scanner over a TCP protocol in the internal zone.
13000	1	Internal TCP Scanner	Identified a worm attack over a TCP protocol in the internal zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.
13001	0	Internal UDP Scanner	Identified a single scanner over a UDP protocol in the internal zone.
13001	1	Internal UDP Scanner	Identified a worm attack over a UDP protocol in the internal zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13002	0	Internal Other Scanner	Identified a single scanner over an Other protocol in the internal zone.
13002	1	Internal Other Scanner	Identified a worm attack over an Other protocol in the internal zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.

Table 13-1 Anomaly Detection Worm Signatures (continued)

Signature ID	Subsignature ID	Name	Description
13003	0	External TCP Scanner	Identified a single scanner over a TCP protocol in the external zone.
13003	1	External TCP Scanner	Identified a worm attack over a TCP protocol in the external zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.
13004	0	External UDP Scanner	Identified a single scanner over a UDP protocol in the external zone.
13004	1	External UDP Scanner	Identified a worm attack over a UDP protocol in the external zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13005	0	External Other Scanner	Identified a single scanner over an Other protocol in the external zone.
13005	1	External Other Scanner	Identified a worm attack over an Other protocol in the external zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.
13006	0	Illegal TCP Scanner	Identified a single scanner over a TCP protocol in the illegal zone.
13006	1	Illegal TCP Scanner	Identified a worm attack over a TCP protocol in the illegal zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.
13007	0	Illegal UDP Scanner	Identified a single scanner over a UDP protocol in the illegal zone.
13007	1	Illegal UDP Scanner	Identified a worm attack over a UDP protocol in the illegal zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13008	0	Illegal Other Scanner	Identified a single scanner over an Other protocol in the illegal zone.
13008	1	Illegal Other Scanner	Identified a worm attack over an Other protocol in the illegal zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.

For More Information

For the procedure for assigning actions to signatures, see Assigning Actions to Signatures, page 10-23.

Configuring Anomaly Detections Policies

This section describes how to create anomaly detection policies, and contains the following topics:

Anomaly Detections Pane

Note You must be administrator or operator to add, clone, or delete anomaly detection policies.

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

In the Anomaly Detections pane, you can add, clone, or delete an anomaly detection policy. The default anomaly detection policy is ad0. When you add a policy, a control transaction is sent to the sensor to create the new policy instance. If the response is successful, the new policy instance is added under Anomaly Detections. If the control transaction fails, for example because of resource limitations, an error message appears.

If your platform does not support virtual policies, this means you can only have one instance for each component and you cannot create new ones or delete the existing one. In this case, the Add, Clone, and Delete buttons are disabled.

For More Information

For the procedure for enabling anomaly detection, see Enabling Anomaly Detection, page 13-4.

Anomaly Detections Pane Field Definitions

The following fields are found in the Anomaly Detections pane:

- Policy Name—Identifies the name of this anomaly detection policy.
- Assigned Virtual Sensor—Identifies the virtual sensor to which this anomaly detection policy is assigned.

Add and Clone Policy Dialog Boxes Field Definitions

The following field is found in the Add and Clone Policy dialog boxes:

- Policy Name—Identifies the name of this anomaly detection policy.

Adding, Cloning, and Deleting Anomaly Detection Policies

To add, clone, or delete an anomaly detection policy, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Anomaly Detections**, and then click **Add**.

Step 3 In the Policy Name field, enter a name for the anomaly detection policy.

Tip To discard your changes and close the dialog box, click **Cancel**.

Step 4 Click **OK**. The anomaly detection policy appears in the list in the Anomaly Detections pane.

Step 5 To clone an existing anomaly detection policy, select it in the list, and then click **Clone**. The Clone Policy dialog box appears with "_copy" appended to the existing anomaly detection policy name.

Step 6 In the Policy Name field, enter a unique name.

Tip To discard your changes and close the dialog box, click **Cancel**.

Step 7 Click **OK**. The cloned anomaly detection policy appears in the list in the Anomaly Detections pane.

Step 8 To remove an anomaly detection policy, select it, and then click **Delete**. The Delete Policy dialog box appears asking if you are sure you want to delete this policy permanently.

Caution You cannot delete the default anomaly detection policy, ad0.

Step 9 Click **Yes**. The anomaly detection policy no longer appears in the list in the Anomaly Detections pane.

ad0 Pane

The ad0 pane (default) contains the tools to configure anomaly detection. There are five tabs:

- Operation Settings—Lets you set the worm timeout and which source and destination IP addresses you want the sensor to ignore during anomaly detection processing.
- Learning Accept Mode—Lets you enable the sensor to automatically accept the learning KB, and to configure a schedule for accepting the learned KB.
- Internal Zone—Lets you configure the destination IP addresses and the threshold of the internal zone.
- Illegal Zone—Lets you configure the destination IP addresses and the threshold of the illegal zone.
- External Zone—Lets you configure the threshold of the external zone.

Configuring Operation Settings

This section describes how to configure operation settings, and contains the following topics:

Operation Settings Tab

Note You must be administrator or operator to configure anomaly detection operation settings.

On the Operation Settings tab, you can set the worm detection timeout. After this timeout, the scanner threshold returns to the configured value. You can also configure source and destination IP addresses that you want the sensor to ignore when anomaly detection is gathering information for a KB. Anomaly detection does not track these source and destination IP addresses and the KB thresholds are not affected by these IP addresses.

Operating Settings Tab Field Definitions

The following fields are found on the Operation Settings tab:

- Worm Timeout—Lets you enter the time in seconds for the worm termination timeout. The range is 120 to 10,000,000 seconds. The default is 600 seconds.
- Configure IP address ranges to ignore during anomaly detection processing—Lets you enter IP addresses that should be ignored while anomaly detection is processing:
  - Enable ignored IP Addresses—If checked, enables the list of ignored IP addresses.
  - Source IP Addresses—Lets you enter the source IP addresses that you want anomaly detection to ignore.
  - Destination IP Addresses—Lets you enter the destination IP addresses that you want anomaly detection to ignore.

Configuring Anomaly Detection Operation Settings

To configure anomaly detection operation settings, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration** > ***sensor_name*** > **Policies** > **Anomaly Detections** > **ad0** > **Operation Settings**.

Step 3 In the Worm Timeout field, enter the number of seconds you want to wait for a worm detection to time out. The range is 120 to 10,000,000 seconds. The default is 600 seconds.

Step 4 To enable the list of ignored IP addresses, check the **Enable ignored IP Addresses** check box.

Note You must check the **Enable ignored IP Addresses** check box or none of the IP addresses you enter will be ignored.

Step 5 In the Source IP Addresses field, enter the addresses or range of source IP addresses that you want anomaly detection to ignore. The valid form is 10.10.5.5,10.10.2.1-10.10.2.30.

Step 6 In the Destination IP Addresses field, enter the addresses or range of destination IP addresses that you want anomaly detection to ignore.

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

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Configuring Learning Accept Mode

This section describes how to configure learning accept mode, and contains the following topics:

Learning Accept Mode Tab

Note You must be administrator or operator to configure learning accept mode.

Use the Learning Accept Mode tab to configure whether you want the sensor to create a new KB every so many hours. You can configure whether the KB is created and loaded (Rotate) or saved (Save Only). You can schedule how often and when the KB is loaded or saved.

The default generated filename is *YYYY-Mon-dd-hh_mm_ss*, where *Mon* is a three-letter abbreviation of the current month.

The KB and Histograms

The KB has a tree structure, and contains the following information:

- KB name
- Zone name
- Protocol
- Service

The KB holds a scanner threshold and a histogram for each service. If you have learning accept mode set to auto and the action set to rotate, a new KB is created every 24 hours and used in the next 24 hours. If you have learning accept mode set to auto and the action is set to save only, a new KB is created, but the current KB is used. If you do not have learning accept mode set to auto, no KB is created.

Note Learning accept mode uses the sensor local time.

The scanner threshold defines the maximum number of zone IP addresses that a single source IP address can scan. The histogram threshold defines the maximum number of source IP addresses that can scan more than the specified numbers of zone IP addresses.

Anomaly detection identifies a worm attack when there is a deviation from the histogram that it has learned when no attack was in progress (that is, when the number of source IP addresses that concurrently scan more than the defined zone destination IP address is exceeded). For example, if the scanning threshold is 300 and the histogram for port 445, if anomaly detection identifies a scanner that scans 350 zone destination IP addresses, it produces an action indicating that a mass scanner was detected. However, this scanner does not yet verify that a worm attack is in progress. Table 13-2 describes this example.

Table 13-2 Example Histogram

Number of source IP addresses	10	5	2
Number of destination IP addresses	5	20	100

When anomaly detection identifies six concurrent source IP addresses that scan more than 20 zone destination IP addresses on port 445, it produces an action with an unspecified source IP address that indicates anomaly detection has identified a worm attack on port 445. The dynamic filter threshold, 20, specifies the new internal scanning threshold and causes anomaly detection to lower the threshold definition of a scanner so that anomaly detection produces additional dynamic filters for each source IP address that scans more than the new scanning threshold (20).

You can override what the KB learned per anomaly detection policy and per zone. If you understand your network traffic, you may want to use overrides to limit false positives.

Triggering the High Category Histogram Before the Single-Scanner Threshold

Based on the default histogram (nonlearned knowledge base [KB]) values, histogram-based detection can occur before single-scanner detection.

Single scanner detection is based on the scanner threshold settings. The scanner threshold setting is a single number for that port or protocol and zone. Any single IP address scanning more than that number of hosts of that port or protocol in that zone is alerted as a scanner.

There is a histogram for that port or protocol and zone that tracks how many systems normally scan a smaller number of hosts (10 hosts, 20 hosts, or 100 hosts). When more than that normal number of scanners are seen, then a worm is declared and all IPs scanning more than the associated number of hosts are alerted on as being a worm scanner.

Note An IP source address can be alerted on as being a worm scanner without ever reaching the scanner threshold. The scanner threshold is used to detect single systems scanning a large number of hosts and is tracked separately from the algorithms for detecting worms.

Learning Accept Mode Tab Field Definitions

The following fields are found on the Learning Accept Mode tab:

- Automatically accept learning knowledge base—If checked, the sensor automatically updates the KB. If not checked, anomaly detection does not automatically create a new KB.
- Action—Lets you specify whether to rotate or save the KB. If you choose Save Only, the new KB is created. You can examine it and decide whether to load it into anomaly detection. If you choose Rotate, the new KB is created and loaded according to the schedule you define.
- Schedule—Lets you choose Calendar Schedule or Periodic Schedule:
  - Periodic Schedule—Lets you configure the first learning snapshot time of day and the interval of the subsequent snapshots. The default is the periodic schedule in 24-hour format.
  - Start Time—Enter the time you want the new KB to start.The valid format is hh:mm:ss.
  - Learning Interval—Enter how long you want anomaly detection to learn from the network before creating a new KB.
  - Calendar Schedule—Lets you configure the days and times of the day for the KB to be created.
  - Times of Day—Click **Add** and enter the times of day in the Add Start Time dialog box.
  - Days of the Week—Check the check boxes of the days of the week you want to configure.

Add and Edit Start Time Dialog Boxes Field Definitions

The following field is found in the Add and Edit Start Time dialog boxes:

- Start Time—Lets you enter the start time for learning accept mode in hours, minutes, and seconds. The valid form is hh:mm:ss in 24-hour time.

Configuring Learning Accept Mode

To configure learning accept mode for anomaly detection, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Anomaly Detections > ad0 > Learning Accept Mode**.

Step 3 To have anomaly detection automatically update the KB, check the **Automatically accept learning knowledge base** check box.

Step 4 From the Action drop-down list, choose one of the following action types:

- Rotate—New KB is created and loaded. This is the default.
- Save Only—New KB is created but not loaded. You can view it to decide if you want to load it.

Step 5 From the Schedule drop-down list, choose one of the following schedule types:

- Calendar Schedule—Go to Step 6.
- Periodic Schedule—Go to Step 7.

Step 6 To configure the calendar schedule:

a. Click **Add** to add the start time.

b. Enter the start time in hours, minutes, and seconds using the 24-hour time format.

Tip To discard your changes and close the Add Start Time dialog box, click **Cancel**.

c. Click **OK**.

d. In the Days of the Week field, check the check boxes of the days you want the anomaly detection module to capture KB snapshots.

Step 7 To configure the periodic schedule (the default):

a. In the Start Time fields, enter the start time in hours, minutes, and seconds using the 24-hour time format.

b. In the Learning Interval field, enter the interval of the subsequent KB snapshots.

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

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

Configuring the Internal Zone

This section describes how to configure the internal zone, and contains the following topics:

Internal Zone Tab

Note You must be administrator or operator to configure the internal zone.

The Internal Zone tab has four tabs:

- General—Lets you enable the internal zone and specify which subnets it contains.
- TCP Protocol—Lets you enable TCP protocol and configure your own thresholds and histograms.
- UDP Protocol—Lets you enable UDP protocol and configure your own thresholds and histograms.

- Other Protocols—Lets you enable other protocols and your own thresholds and histograms.

The internal zone should represent your internal network. It should receive all the traffic that comes to your IP address range.

General Tab

On the General tab, you enable the zone. If the zone is disabled, packets to this zone are ignored. By default the zone is enabled.

You then add the IP addresses that belong to this zone. If you do not configure IP addresses for all zones, all packets are sent to the default zone, the external zone.

Field Definitions

The following fields are found on the General tab:

- Enable the Internal Zone—If checked, enables the internal zone.
- Service Subnets—Lets you enter the subnets that you want to apply to the internal zone. The valid format is 10.10.5.5,10.10.2.1-10.10.2.30.

TCP Protocol Tab

On the TCP Protocol tab, you enable or disable TCP protocol for the internal zone. You can configure a destination port for the TCP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the TCP Protocol tab:

- Enable the TCP Protocol—If checked, enables TCP protocol.
- Destination Port Map tab—Lets you associate a specific port with the TCP protocol:
  - Port Number—Displays the configured port number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold settings.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms. Default thresholds are used for services that are not in the KB and were not overridden by the configuration:
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
  - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Destination Port Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Destination Port dialog boxes:

- Destination Port number—Lets you enter the destination port number. The valid range is 0 to 65535.
- Enable the Service—If checked, enables the service.
- Override Scanner Settings—If checked, overrides the default scanner settings and lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
  - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
  - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Add and Edit Histogram Dialog Boxes Field Definitions

The following fields are found on the Add and Edit Histogram dialog boxes:

- Number of Destination IP Addresses—Lets you add a high, medium, or low number of destination IP addresses. Low is 5 destination IP addresses, medium is 20, and high is 100.
- Number of Source IP Addresses—Lets you add the number of source IP addresses. The valid range is 0 to 4096.

UDP Protocol Tab

On the UDP Protocol tab, you enable or disable UDP protocol for the internal zone. You can configure a destination port for the UDP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the UDP Protocol tab:

- Enable the UDP Protocol—If checked, enables UDP protocol.
- Destination Port Map tab—Lets you associate a specific port with the UDP protocol:
  - Port Number—Displays the configured port number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms:
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.

  - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Other Protocols Tab

On the Other Protocols tab, you enable or disable other protocols for the internal zone. You can configure a protocol number map for the other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the Other Protocols tab:

- Enable Other Protocols—If checked, enables the other protocols.
- Protocol Number Map tab—Lets you associate a specific protocol number with the other protocols:
  - Protocol Number—Displays the configured protocol number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms.
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
  - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Protocol Number Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Protocol Number dialog boxes:

- Protocol number—Lets you enter a protocol number.
- Enable the Service—Lets you enable the service.
- Override Scanner Settings—If checked, lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
  - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
  - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Configuring the Internal Zone

To configure the internal zone for anomaly detection, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Anomaly Detections > ad0 > Internal Zone**, and then click the **General** tab.

Step 3 To enable the internal zone, check the **Enable the Internal Zone** check box.

Note You must check the **Enable the Internal Zone** check box or any protocols that you configure will be ignored.

Step 4 In the Service Subnets field, enter the subnets to which you want the internal zone to apply. The valid format is 10.10.5.5,10.10.2.1-10.10.2.30.

Step 5 To configure TCP protocol, click the **TCP Protocol** tab.

Step 6 To enable TCP protocol, check the **Enable the TCP Protocol** check box.

Note You must check the **Enable the TCP Protocol** check box or the TCP protocol configuration will be ignored.

Step 7 Click the **Destination Port Map** tab, and then click **Add** to add a destination port.

Step 8 In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

Step 9 To enable the service on that port, check the **Enable the Service** check box.

Step 10 To override the scanner values for that port, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 11 To add a histogram for the new scanner settings, click **Add**.

Step 12 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 13 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 14 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.

Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 15 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 16 To edit the destination port map, select it in the list, and click **Edit**.

Step 17 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 18 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list Destination Port Map tab.

Step 19 To edit the default thresholds, click the **Default Thresholds** tab.

Step 20 Select the threshold histogram you want to edit, and click **Edit**.

Step 21 From the Number of Destination IP Addresses the drop down list, change the value (High, Medium, or Low).

Step 22 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

Step 23 To configure UDP protocol, click the **UDP Protocol** tab.

Step 24 To enable UDP protocol, check the **Enable the UDP Protocol** check box.

Note You must check the **Enable the UDP Protocol** check box or the UDP protocol configuration will be ignored.

Step 25 Click the **Destination Port Map** tab, and then click **Add** to add a destination port.

Step 26 In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

Step 27 To enable the service on that port, check the **Enable the Service** check box.

Step 28 To override the scanner values for that port, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 29 To add a histogram for the new scanner settings, click **Add**.

Step 30 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 31 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 32 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.

Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 33 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 34 To edit the destination port map, select it in the list, and click **Edit**.

Step 35 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 36 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list on the Destination Port Map tab.

Step 37 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 38 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 39 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.The edited threshold histogram appears in the list on the Default Thresholds tab.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

Step 40 To configure Other protocols, click the **Other Protocols** tab.

Step 41 To enable other protocols, check the **Enable Other Protocols** check box.

Note You must check the **Enable Other Protocol**s check box or the other protocols configuration will be ignored.

Step 42 Click the **Protocol Number Map** tab, and then click **Add** to add a protocol number.

Step 43 In the Protocol Number field, enter the protocol number. The valid range is 0 to 255.

Step 44 To enable the service of that protocol, check the **Enable the Service** check box.

Step 45 To override the scanner values for that protocol, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 46 To add a histogram for the new scanner settings, click **Add**.

Step 47 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 48 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 49 Click **OK**. The new scanner setting appears in the list in the Add Protocol Number dialog box.

Tip To discard your changes and close the Add Protocol Number dialog box, click **Cancel**.

Step 50 Click **OK**. The new protocol number map appears in the list on the Protocol Number Map tab.

Step 51 To edit the protocol number map, select it in the list, and click **Edit**.

Step 52 Make any changes to the fields and click **OK**. The edited protocol number map appears in the list on the Protocol Number Map tab.

Step 53 To delete a protocol number map, select it, and click **Delete**. The protocol number map no longer appears in the list on the Protocol Number Map tab.

Step 54 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 55 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 56 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

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

Step 57 Click **Apply** to apply your changes and save the revised configuration.

Configuring the Illegal Zone

This section describes how to configure the illegal zone, and contains the following topics:

Illegal Zone Tab

Note You must be administrator or operator to configure the illegal zone.

The Illegal Zone tab has four tabs:

- General—Lets you enable the illegal zone and specify which subnets it contains.
- TCP Protocol—Lets you enable TCP protocol and configure your own thresholds and histograms.
- UDP Protocol—Lets you enable UDP protocol and configure your own thresholds and histograms.
- Other Protocols—Lets you enable other protocols and your own thresholds and histograms.

The illegal zone should represent 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.

General Tab

On the General tab, you enable the zone. If the zone is disabled, packets to this zone are ignored. By default the zone is enabled.

You then add the IP addresses that belong to this zone. If you do not configure IP addresses for all zones, all packets are sent to the default zone, the external zone.

Field Definitions

The following fields are found on the General tab:

- Enable the Internal Zone—If checked, enables the internal zone.
- Service Subnets—Lets you enter the subnets that you want to apply to the internal zone. The valid format is 10.10.5.5,10.10.2.1-10.10.2.30.

TCP Protocol Tab

On the TCP Protocol tab, you enable or disable TCP protocol for the illegal zone. You can configure a destination port for the TCP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the TCP Protocol tab:

- Enable the TCP Protocol—If checked, enables TCP protocol.
- Destination Port Map tab—Lets you associate a specific port with the TCP protocol:
  - Port Number—Displays the configured port number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold settings.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms. Default thresholds are used for services that are not in the KB and were not overridden by the configuration:
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
  - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Destination Port Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Destination Port dialog boxes:

- Destination Port number—Lets you enter the destination port number. The valid range is 0 to 65535.
- Enable the Service—If checked, enables the service.

- Override Scanner Settings—If checked, overrides the default scanner settings and lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
  - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
  - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Add and Edit Histogram Dialog Boxes Field Definitions

The following fields are found on the Add and Edit Histogram dialog boxes:

- Number of Destination IP Addresses—Lets you add a high, medium, or low number of destination IP addresses. Low is 5 destination IP addresses, medium is 20, and high is 100.
- Number of Source IP Addresses—Lets you add the number of source IP addresses. The valid range is 0 to 4096.

UDP Protocol Tab

On the UDP Protocol tab, you enable or disable UDP protocol for the illegal zone. You can configure a destination port for the UDP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the UDP Protocol tab:

- Enable the UDP Protocol—If checked, enables UDP protocol.
- Destination Port Map tab—Lets you associate a specific port with the UDP protocol:
  - Port Number—Displays the configured port number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms:
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
  - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Other Protocols Tab

On the Other Protocols tab, you enable or disable Other protocols for the illegal zone. You can configure a protocol number map for the Other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the Other Protocols tab:

- Enable Other Protocols—If checked, enables the other protocols.
- Protocol Number Map tab—Lets you associate a specific protocol number with the other protocols:
  - Protocol Number—Displays the configured protocol number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms.
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
  - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Protocol Number Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Protocol Number dialog boxes:

- Protocol number—Lets you enter a protocol number.
- Enable the Service—Lets you enable the service.
- Override Scanner Settings—If checked, lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
  - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
  - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Configuring the Illegal Zone

To configure the illegal zone for anomaly detection, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration** > ***sensor_name*** > **Policies** > **Anomaly Detections** > **ad0** > **Illegal Zone**.

Step 3 Click the **General** tab.

Step 4 To enable the illegal zone, check the **Enable the Illegal Zone** check box.

Note You must check the **Enable the Illegal Zone** check box or any protocols that you configure will be ignored.

Step 5 In the Service Subnets field, enter the subnets to which you want the illegal zone to apply. The valid format is 10.10.5.5,10.10.2.1-10.10.2.30.

Step 6 To configure TCP protocol, click the **TCP Protocol** tab.

Step 7 To enable TCP protocol, check the **Enable the TCP Protocol** check box.

Note You must check the **Enable the TCP Protocol** check box or the TCP protocol configuration will be ignored.

Step 8 Click the **Destination Port Map** tab, and then click **Add** to add a destination port.

Step 9 In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

Step 10 To enable the service on that port, check the **Enable the Service** check box.

Step 11 To override the scanner values for that port, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 12 To add a histogram for the new scanner settings, click **Add**.

Step 13 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 14 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 15 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.

Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 16 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 17 To edit the destination port map, select it in the list, and click **Edit**.

Step 18 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 19 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list Destination Port Map tab.

Step 20 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 21 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 22 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the **Default Thresholds** tab.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

Step 23 To configure UDP protocol, click the **UDP Protocol** tab.

Step 24 To enable UDP protocol, check the **Enable the UDP Protocol** check box.

Note You must check the **Enable the UDP Protocol** check box or the UDP protocol configuration will be ignored.

Step 25 Click the **Destination Port Map** tab, and then click **Add** to add a destination port.

Step 26 In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

Step 27 To enable the service on that port, check the **Enable the Service** check box.

Step 28 To override the scanner values for that port, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 29 To add a histogram for the new scanner settings, click **Add**.

Step 30 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 31 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 32 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.

Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 33 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 34 To edit the destination port map, select it in the list, and click **Edit**.

Step 35 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 36 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list on the Destination Port Map tab.

Step 37 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 38 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 39 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

The edited threshold histogram appears in the list on the Default Thresholds tab.

Step 40 To configure Other protocols, click the **Other Protocol**s tab.

Step 41 To enable other protocols, check the **Enable Other Protocols** check box.

Note You must check the **Enable Other Protocol**s check box or the other protocols configuration will be ignored.

Step 42 Click the **Protocol Number Map** tab, and then click **Add** to add a protocol number.

Step 43 In the Protocol Number field, enter the protocol number. The valid range is 0 to 255.

Step 44 To enable the service of that protocol, check the **Enable the Service** check box.

Step 45 To override the scanner values for that protocol, check the **Override Scanner** Settings check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 46 To add a histogram for the new scanner settings, click **Add**.

Step 47 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 48 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 49 Click **OK**. The new scanner setting appears in the list in the Add Protocol Number dialog box.

Tip To discard your changes and close the Add Protocol Number dialog box, click **Cancel**.

Step 50 Click **OK**. The new protocol number map appears in the list on the Protocol Number Map tab.

Step 51 To edit the protocol number map, select it in the list, and click **Edit**.

Step 52 Make any changes to the fields and click **OK**. The edited protocol number map appears in the list on the Protocol Number Map tab.

Step 53 To delete a protocol number map, select it, and click **Delete**. The protocol number map no longer appears in the list on the Protocol Number Map tab.

Step 54 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 55 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 56 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

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

Step 57 Click **Apply** to apply your changes and save the revised configuration.

Configuring the External Zone

This section describes how to configure external zone, and contains the following topics:

External Zone Tab

Note You must be administrator or operator to configure the external zone.

The External Zone tab has three tabs:

- TCP Protocol—Lets you enable TCP protocol and configure your own thresholds and histograms.
- UDP Protocol—Lets you enable UDP protocol and configure your own thresholds and histograms.
- Other Protocols—Lets you enable other protocols and your own thresholds and histograms.

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.

TCP Protocol Tab

On the TCP Protocol tab, you enable or disable TCP protocol for the external zone. You can configure a destination port for the TCP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the TCP Protocol tab:

- Enable the TCP Protocol—If checked, enables TCP protocol.
- Destination Port Map tab—Lets you associate a specific port with the TCP protocol:
  - Port Number—Displays the configured port number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold settings.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms. Default thresholds are used for services that are not in the KB and were not overridden by the configuration:
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
  - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Destination Port Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Destination Port dialog boxes:

- Destination Port number—Lets you enter the destination port number. The valid range is 0 to 65535.
- Enable the Service—If checked, enables the service.
- Override Scanner Settings—If checked, overrides the default scanner settings and lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
  - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
  - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Add and Edit Histogram Dialog Boxes Field Definitions

The following fields are found on the Add and Edit Histogram dialog boxes:

- Number of Destination IP Addresses—Lets you add a high, medium, or low number of destination IP addresses. Low is 5 destination IP addresses, medium is 20, and high is 100.
- Number of Source IP Addresses—Lets you add the number of source IP addresses. The valid range is 0 to 4096.

UDP Protocol Tab

On the UDP Protocol tab, you enable or disable UDP protocol for the external zone. You can configure a destination port for the UDP protocol. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the UDP Protocol tab:

- Enable the UDP Protocol—If checked, enables UDP protocol.
- Destination Port Map tab—Lets you associate a specific port with the UDP protocol:
  - Port Number—Displays the configured port number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms:
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.
  - Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Other Protocols Tab

On the Other Protocols tab, you enable or disable Other protocols for the external zone. You can configure a protocol number map for the Other protocols. You can either use the default thresholds or override the scanner settings and add your own thresholds and histograms.

Field Definitions

The following fields are found on the Other Protocols tab:

- Enable Other Protocols—If checked, enables the other protocols.
- Protocol Number Map tab—Lets you associate a specific protocol number with the other protocols:
  - Protocol Number—Displays the configured protocol number.
  - Service Enabled—Whether or not the service is enabled.
  - Scanner Overridden—Whether or not the scanner has been overridden.
  - Overridden Scanner Settings Threshold—Displays the configured threshold setting.
  - Overridden Scanner Settings Histogram—Displays the configured histogram.
- Default Thresholds tab—Displays the default thresholds and histograms.
  - Scanner Threshold—Lets you change the scanner threshold.
  - Threshold Histogram Number of Destination IP Addresses—Displays the number of destination IP addresses grouped as low, medium, and high.

- Threshold Histogram Number of Source IP Addresses—Displays the number of source IP addresses associated with each group of destination IP addresses.

Add and Edit Protocol Number Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Protocol Number dialog boxes:

- Protocol number—Lets you enter a protocol number.
- Enable the Service—Lets you enable the service.
- Override Scanner Settings—If checked, lets you add, edit, delete, and select all histograms.
- Scanner Threshold—Lets you set the scanner threshold. The valid range is 5 to 1000. The default is 100.
- Threshold Histogram—Displays the histograms that you added:
  - Number of Destination IP Addresses—Displays the number of destination IP addresses that you added.
  - Number of Source IP Addresses—Displays the number of source IP addresses that you added.

Configuring the External Zone

To configure the external zone for anomaly detection, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Policies > Anomaly Detections > ad0 > External Zone**.

Step 3 To enable the external zone, check the **Enable the External Zone** check box.

Note You must check the **Enable the External Zone** check box or any protocols that you configure will be ignored.

Step 4 To configure TCP protocol, click the **TCP Protocol** tab.

Step 5 To enable TCP protocol, check the **Enable the TCP Protocol** check box.

Note You must check the **Enable the TCP Protocol** check box or the TCP protocol configuration will be ignored.

Step 6 Click the **Destination Port Map** tab, and then click **Add** to add a destination port.

Step 7 In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

Step 8 To enable the service on that port, check the **Enable the Service** check box.

Step 9 To override the scanner values for that port, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 10 To add a histogram for the new scanner settings, click **Add**.

Step 11 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 12 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 13 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.

Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 14 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 15 To edit the destination port map, select it in the list, and click **Edit**.

Step 16 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 17 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list Destination Port Map tab.

Step 18 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 19 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 20 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

Step 21 To configure UDP protocol, click the **UDP Protocol** tab.

Step 22 To enable UDP protocol, check the **Enable the UDP Protocol** check box.

Note You must check the **Enable the UDP Protocol** check box or the UDP protocol configuration will be ignored.

Step 23 Click the **Destination Port Map** tab, then click **Add** to add a destination port.

Step 24 In the Destination Port Number field, enter the destination port number. The valid range is 0 to 65535.

Step 25 To enable the service on that port, check the **Enable the Service** check box.

Step 26 To override the scanner values for that port, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 27 To add a histogram for the new scanner settings, click **Add**.

Step 28 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 29 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 30 Click **OK**. The new scanner setting appears in the list in the Add Destination Port dialog box.

Tip To discard your changes and close the Add Destination Port dialog box, click **Cancel**.

Step 31 Click **OK**. The new destination port map appears in the list on the Destination Port Map tab.

Step 32 To edit the destination port map, select it in the list, and click **Edit**.

Step 33 Make any changes to the fields and click **OK**. The edited destination port map appears in the list on the Destination Port Map tab.

Step 34 To delete a destination port map, select it, and click **Delete**. The destination port map no longer appears in the list on the Destination Port Map tab.

Step 35 To edit the default thresholds, click the **Default Thresholds** tab, select the threshold histogram you want to edit, and then click **Edit**.

Step 36 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 37 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

Step 38 To configure Other protocols, click the **Other Protocol**s tab.

Step 39 To enable other protocols, check the **Enable Other Protocols** check box.

Note You must check the **Enable Other Protocol**s check box or the other protocols configuration will be ignored.

Step 40 Click the **Protocol Number Map** tab, and then click **Add** to add a protocol number.

Step 41 In the Protocol Number field, enter the protocol number. The valid range is 0 to 255.

Step 42 To enable the service of that protocol, check the **Enable the Service** check box.

Step 43 To override the scanner values for that protocol, check the **Override Scanner Settings** check box. You can use the default scanner values, or you can override them and configure your own scanner values.

Step 44 To add a histogram for the new scanner settings, click **Add**.

Step 45 From the Number of Destination IP Addresses drop-down list, choose the value (High, Medium, or Low).

Step 46 In the Number of Source IP Addresses field, enter the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096.

Tip To discard your changes and close the Add Histogram dialog box, click **Cancel**.

Step 47 Click **OK**. The new scanner setting appears in the list in the Add Protocol Number dialog box.

Tip To discard your changes and close the Add Protocol Number dialog box, click **Cancel**.

Step 48 Click **OK**. The new protocol number map appears in the list on the Protocol Number Map tab.

Step 49 To edit the protocol number map, select it in the list, and click **Edit**.

Step 50 Make any changes to the fields and click **OK**. The edited protocol number map appears in the list on the Protocol Number Map tab.

Step 51 To delete a protocol number map, select it, and click **Delete**. The protocol number map no longer appears in the list on the Protocol Number Map tab.

Step 52 To edit the default thresholds, click the **Default Thresholds** tab.

Step 53 Select the threshold histogram you want to edit, and click **Edit**.

Step 54 From the Number of Destination IP Addresses drop-down list, change the value (High, Medium, or Low).

Step 55 In the Number of Source IP Addresses field, edit the number of source IP addresses you want associated with this histogram. The valid range is 0 to 4096. The edited threshold histogram appears in the list on the Default Thresholds tab.

Tip To discard your changes and close the Edit Histogram dialog box, click **Cancel**.

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

Step 56 Click **Apply** to apply your changes and save the revised configuration.

Disabling Anomaly Detection

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

If you have anomaly detection enabled and you have your sensor configured to see only one direction of traffic, you should disable anomaly detection. Otherwise, you will receive many alerts, because anomaly detection sees asymmetric traffic as having incomplete connections, that is, like worm scanners, and fires alerts.

To disable anomaly detection, follow these steps:

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

Step 2 Enter analysis engine submode.

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

Step 3 Enter the virtual sensor name that contains the anomaly detection policy you want to disable.

```
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)#
```

Step 4 Disable anomaly detection operational mode.

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# operational-mode inactive
sensor(config-ana-vir-ano)#
```

Step 5 Exit analysis engine submode.

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

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

Configuring Global Correlation

This chapter provides information for configuring global correlation. It contains the following sections:

Understanding Global Correlation

You can configure global correlation so that your sensors are aware of network devices with a reputation for malicious activity, and can take action against them. Participating IPS devices in a centralized Cisco threat database, the SensorBase Network, receive and absorb global correlation updates. The reputation information contained in the global correlation updates is factored in to the analysis of network traffic, which increases IPS efficacy, since traffic is denied or allowed based on the reputation of the source IP address. The participating IPS devices send data back to the Cisco SensorBase Network, which results in a feedback loop that keeps the updates current and global.

You can configure the sensor to participate in the global correlation updates and/or in sending telemetry data or you can turn both services off. You can view reputation scores in events and see the reputation score of the attacker. You can also view statistics from the reputation filter. You can filter the events based on reputation scores and generate reports based on them.

Participating in the SensorBase Network

The Cisco IPS contains a security capability, Cisco Global Correlation, which uses the immense security intelligence that we have amassed over the years. At regular intervals, the Cisco IPS receives threat updates from the Cisco SensorBase Network, which contain detailed information about known threats on the Internet, including serial attackers, Botnet harvesters, Malware outbreaks, and dark nets. The IPS uses this information to filter out the worst attackers before they have a chance to attack critical assets. It then incorporates the global threat data in to its system to detect and prevent malicious activity even earlier.

If you agree to participate in the SensorBase Network, Cisco will collect aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other confidential business or personal information. All data is aggregated and sent by secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco will be anonymous and treated as strictly confidential.

Table 14-1 shows how we use the data.

Table 14-1 Cisco Network Participation Data Use

Participation Level	Type of Data	Purpose
Partial	Protocol attributes (TCP maximum segment size and options string, for example)	Tracks potential threats and helps us to understand threat exposure.
	Attack type (signature fired and risk rating, for example)	Used to understand current attacks and attack severity.
	Connecting IP address and port	Identifies attack source.
	Summary IPS performance (CPU utilization, memory usage, inline vs. promiscuous, for example)	Tracks product efficacy.
Full	Victim IP address and port	Detects threat behavioral patterns.

When you enable Partial or Full Network Participation, the Network Participation Disclaimer appears. You must click **Agree** to participate. If you do not have a license installed, you receive a warning telling you that global correlation inspection and reputation filtering are disabled until the sensor is licensed. You can obtain a license at http://www.cisco.com/go/license.

For More Information

For information on how to obtain and install a sensor license, see Configuring Licensing, page 20-12.

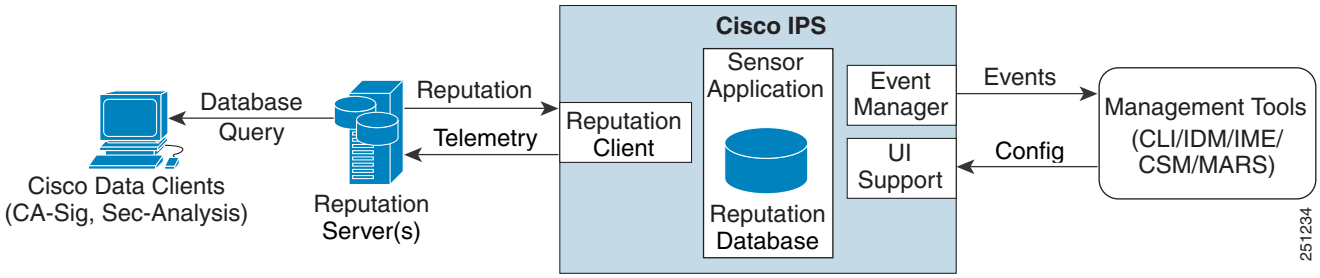
Understanding Reputation

Similar to human social interaction, reputation is an opinion toward a device on the Internet. It enables the installed base of IPS sensors in the field to collaborate using the existing network infrastructure. A network device with reputation is most likely either malicious or infected. You can view reputation information and statistics in the IDM, IME, or the CLI.

The IPS sensor collaborates with the global correlation servers (also known as reputation servers) to improve the efficacy of the sensor.

Figure 14-1 shows the role of the sensor and the global correlation servers.

Figure 14-1 IPS Management and Global Correlation Server Interaction



The global correlation servers provide information to the sensor about certain IP addresses that may identify malicious or infected hosts. The sensor uses this information to determine which actions, if any, to perform when potentially harmful traffic is received from a host with known reputation. Because the global correlation database changes rapidly, the sensor must periodically download global correlation updates from the global correlation servers.

Caution As with signature updates, when the sensor applies a global correlation update, it may trigger bypass. Whether or not bypass is triggered depends on the traffic load of the sensor and the size of the signature/global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

For More Information

For more information about viewing global correlation statistics, see Viewing Statistics, page 21-22.

Understanding Network Participation

Network participation lets us collect nearly real-time data from sensors around the world. Sensors installed at customer sites can send data to the SensorBase Network. These data feed in to the global correlation database to increase reputation fidelity. Communication between sensors and the SensorBase Network involves an HTTPS request and response over TCP/IP. Network participation gathers the following data:

- Signature ID
- Attacker IP address
- Attacker port
- Maximum segment size
- Victim IP address
- Victim port
- Signature version
- TCP options string

- Reputation score
- Risk rating
- Data gathered from the sensor health metrics

The statistics for network participation show the hits and misses for alerts, the reputation actions, and the counters of packets that have been denied.

Note Network participation requires a network connection to the Internet.

There are three modes for network participation:

- Off—The network participation server does not collect data, track statistics, or try to contact the Cisco SensorBase Network.
- Partial Participation—The network participation server collects data, tracks statistics, and communicates with the SensorBase Network. Data considered to be potentially sensitive is filtered out and never sent.
- Full Participation—The network participation server collects data, tracks statistics, and communicates with the SensorBase Network. All data collected is sent except the IP addresses that you exclude from the network participation data.

Caution As with signature updates, when the sensor applies a global correlation update, it may trigger bypass. Whether or not bypass is triggered depends on the traffic load of the sensor and the size of the signature/global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

For More Information

- For more information on network participation, see Configuring Network Participation, page 14-10.
- For more information on bypass mode, see Configuring Bypass Mode, page 7-25.

Understanding Efficacy

Obtaining data from participating IPS clients and using that in conjunction with the existing corpus of threat knowledge improves the efficacy of the IPS. We measure efficacy based on the following:

- False positives as a percentage of actionable events
- False negatives as a percentage of threats that do not result in actionable events
- Actionable events as a percentage of all events

The IPS signature team uses the data to improve signature fidelity and the IPS engineering team uses the data to better understand the various types of sensor deployment.

For More Information

For more information about reputation and risk rating, see Reputation and Risk Rating, page 14-5.

Reputation and Risk Rating

Risk rating is the concept of the probability that a network event is malicious. You assign a numerical quantification of the risk associated with a particular event on the network. By default, an alert with an extreme risk rating shuts down traffic. Reputation indicates the probability that a particular attacker IP address will initiate malicious behavior based on its known past activity. A certain score is computed for this reputation by the Alarm Channel and added to risk rating, thus improving the efficacy of the IPS. When the attacker has a bad reputation score, an incremental risk is added to the risk rating to make it more aggressive.

The Alarm Channel handles signature events from the data path. The alert processing units have multiple aggregation techniques, action overrides, action filters, attacker reputation, and per-action custom handling methods. We use the large reputation data from the reputation participation client to score attackers in the Alarm Channel and then use this score to influence the risk rating and actions of the alert.

For More Information

- For a detailed description of risk rating, see Calculating the Risk Rating, page 12-2.
- For a detailed description of threat rating, see Understanding Threat Rating, page 12-4.
- For a detailed description of event action filters, see Understanding Event Action Filters, page 12-4.
- For a detailed description of the Alarm Channel, see Understanding the SensorApp, page A-23.
- For a detailed description of event action aggregation, see Event Action Aggregation, page 12-5.

Global Correlation Features and Goals

There are three main features of global correlation:

- Global Correlation Inspection—We use the global correlation reputation knowledge of attackers to influence alert handling and deny actions when attackers with a bad score are seen on the sensor.
- Reputation Filtering—Applies automatic deny actions to packets from known malicious sites.
- Network Reputation—Sensor sends alert and TCP fingerprint data to the SensorBase Network.

Global correlation has the following goals:

- Dealing intelligently with alerts thus improving efficacy.
- Improving protection against known malicious sites.
- Sharing telemetry data with the SensorBase Network to improve visibility of alerts and sensor actions on a global scale.
- Simplifying configuration settings.
- Automatic handling of the uploads and downloads of the information.

Global Correlation Requirements

Global correlation has the following requirements:

- Valid license—You must have a valid sensor license for automatic signature updates and global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.
- Network Participation disclaimer—You must agree to the disclaimer to participate.
- External connectivity for the sensor and a DNS server—The global correlation features of Cisco IPS require the sensor to connect to the Cisco SensorBase Network. Domain name resolution is also required for these features to function. You can either configure the sensor to connect through an HTTP proxy server that has a DNS client running on it, or you can assign an Internet routeable address to the management interface of the sensor and configure the sensor to use a DNS server. In Cisco IPS the HTTP proxy and DNS servers are used only by the global correlation features.

  If you are connecting through an HTTP proxy, make sure you have the following configuration:

  - The proxy must allow HTTP requests from the IPS systems to http://updates.ironport.com/ibrs/ on port 80.
  - The proxy must allow HTTPS requests from the IPS systems to update-manifests.ironport.com on port 443.
  - The firewall must allow access from the proxy to the internet (any destination address) on ports 80 and 443.

  If you are NOT connecting through the HTTP proxy:

  - The firewall must allow access from each IPS to the Internet (any destination address) on ports 80 and 443.

  Note The IPS does not support the use of authenticated proxies.

- Sensors deployed in an environment with a slow command and control connection will be slow to download global correlation updates.
- No IPv6 address support—Global correlation inspection and the reputation filtering deny features do not support IPv6 addresses. For global correlation inspection, the sensor does not receive or process reputation data for IPv6 addresses. The risk rating for IPv6 addresses is not modified for global correlation inspection. Similarly, network participation does not include event data for attacks from IPv6 addresses. And finally, IPv6 addresses do not appear in the deny list.
- Sensor in inline mode—The sensor must operate in inline mode so that the global correlation features can increase efficacy by being able to use the inline deny actions.
- Sensor that supports the global correlation features
- IPS version that supports the global correlation features

For More Information

- For information on how to obtain and install a sensor license, see Configuring Licensing, page 20-12.
- For information about the Network Participation disclaimer, see Participating in the SensorBase Network, page 14-2.

- For information about configuring a DNS or HTTP proxy server to support global correlation, see Configuring Network Settings, page 6-1.
- For information on troubleshooting global correlation, see Troubleshooting Global Correlation, page 14-11.

Understanding Global Correlation Sensor Health Metrics

For global correlation, the following metrics are added to sensor health monitoring:

- Green indicates that the last update was successful.
- Yellow indicates that there has not been a successful update within the past day (86,400 seconds).
- Red indicates that there has not been a successful update within the last three days (259,200 seconds).

For network participation, the following metrics are added to sensor health monitoring:

- Green indicates that the last connection was successful.
- Yellow indicates that less than 6 connections failed in a row.
- Red indicates that more than 6 connections failed in a row.

You can view the metrics in the Sensor Health gadget and the Global Correlation Health gadget.

Global correlation health status defaults to red and changes to green after a successful global correlation update. Successful global correlation updates require a DNS server or an HTTP proxy server. Global correlation health and overall sensor health status are red until you configure a DNS or HTTP proxy server on the sensor. If the sensor is deployed in an environment where a DNS or HTTP proxy server is not available, you can address the red global correlation health and overall sensor health status by disabling global correlation and configuring sensor health status not to include global correlation health status.

For More Information

- For more information about the sensor health metrics, see Configuring Sensor Health, page 20-16.
- For the procedure for disabling global correlation, see Disabling Global Correlation, page 14-12.
- For more information on the Sensor Health and Global Correlation Health gadgets, see IME Gadgets, page 3-2.

Configuring Global Correlation Inspection and Reputation Filtering

This section describes how to set up global correlation inspection and reputation, and contains the following topics:

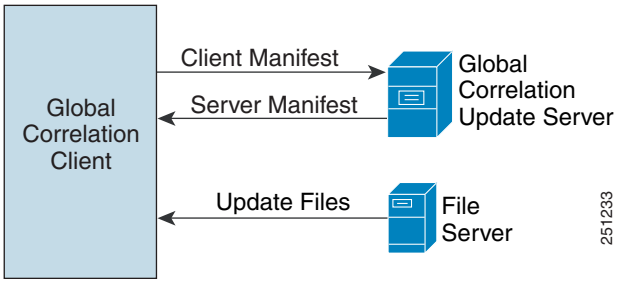
Inspection/Reputation Pane

Note You must be administrator or operator to configure inspection/reputation settings.

In the Inspection/Reputation pane you can configure the sensor to use updates from the SensorBase Network to adjust the risk rating. The client determines which updates are available and applicable to the sensor by communicating with the global correlation update server and a file server, which is a two-phase process. In the first phase the sensor sends a client manifest to the global correlation update sever via an HTTPS POST request. The server then returns the server manifest document in the HTTPS response. In the next phase the sensor identifies the updates that are available and how to obtain them from a file server. The sensor downloads the encrypted update files via HTTP from the file server using the information in the server manifest. The integrity of these update files has been verified by comparing its MD5 hash with the hash value specified in the server manifest.

Figure 14-2 demonstrates how the global correlation update client obtains the files.

Figure 14-2 Global Correlation Update Client



Caution You must have a valid sensor license for automatic signature updates and global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.

Once you configure global correlation, updates are automatic and happen at regular intervals, approximately every five minutes by default, but this interval may be modified by the global correlation server. The sensor gets a full update and then applies an incremental update periodically.

You configure an HTTP proxy or a DNS server in the Network pane. If you turn on global correlation, you can choose how aggressively you want the deny actions to be enforced against malicious hosts. You can then enable reputation filtering to deny access to known malicious hosts. If you only want a report of what could have happened, you can enable **Test Global Correlation**. This puts the sensor in audit mode, and actions the sensor would have performed are generated in the events.

To view the status of global correlation in the Sensor Health gadget, click **Details**. The status of global correlation reads Normal, Needs Attention, or Critical.

Caution As with signature updates, when the sensor applies a global correlation update, it may trigger bypass. Whether or not bypass is triggered depends on the traffic load of the sensor and the size of the signature/global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

Inspection/Reputation Pane Field Definitions

The following fields are found in the Inspection/Reputation pane:

- Global Correlation Inspection—Lets you turn global correlation off and on. When turned on, the sensor uses updates from the SensorBase Network to adjust the risk rating. The default is On, however, you must have a DNS server or proxy server configured for global correlation inspection to take effect.

  There are three modes that let you determine how aggressively the sensor uses global correlation information to initiate deny actions:

  - Permissive—Has the least aggressive effect on deny actions.
  - Standard—Has a moderately aggressive effect on deny actions. This is the default.
  - Aggressive—Has a very aggressive effect on deny actions.
- Reputation Filtering—Lets you turn reputation filtering on and off. When turned on, the sensor denies access to malicious hosts that are listed in the global correlation database. The default is On.
- Test Global Correlation—Enables reporting of deny actions that are affected by global correlation. Allows you to test the global correlation features without actually denying any hosts.

For More Information

- For information on how to obtain and install a sensor license, see Configuring Licensing, page 20-12.
- For more information about the sensor health metrics, see Configuring Sensor Health, page 20-16.

Configuring Global Correlation Inspection and Reputation Filtering

To configure global correlation inspection and reputation filtering, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Policies > Global Correlation > Inspection/Reputation**.

Step 3 To turn on global correlation inspection and reputation filtering, click the **On** radio button. Global correlation inspection and reputation filtering are turned off by default.

Step 4 From the drop-down list, choose how you want the sensor to use global correlation information to initiate deny actions:

- Permissive—Has the least aggressive effect on deny actions.
- Standard—Has a moderately aggressive effect on deny actions.
- Aggressive—Has a very aggressive effect on deny actions.

Step 5 To turn on reputation filtering, click the **On** radio button. Reputation filtering is turned off by default.

Step 6 To test global correlation, but not let global correlation influence whether traffic is denied, click the **Test Global Correlation** check box. This gives you reports as if global correlation inspection and reputation filtering were on.

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

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Configuring Network Participation

This section describes how to configure network participation, and contains the following topics:

Network Participation Pane

Note You must be administrator or operator to configure network participation.

In the Network Participation pane, you can configure the sensor to send data to the SensorBase Network. You can configure the sensor to fully participate and send all data to the SensorBase Network. Or you can configure the sensor to collect the data but to omit potentially sensitive data, such as the destination IP address of trigger packets.

Note Configuring the sensor for partial network participation limits a third party from extracting reconnaissance information about your internal network from the global correlation database.

Network Participation Pane Field Definitions

The following fields are found in the Network Participation pane:

- Off—No data is contributed to the SensorBase Network.
- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network except the attacker/victim IP addresses that you exclude.

Configuring Network Participation

To configure network participation, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Policies > Global Correlation > Network Participation**.

Step 3 To turn on network participation, click the **Partial** or **Full** radio button:

- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network except any attacker/victim IP addresses that you exclude.

Caution You must accept the disclaimer to participate in network participation.

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

Step 4 Click **Apply** to apply your changes and save the revised configuration.

Troubleshooting Global Correlation

Make sure you observe the following when configuring global correlation:

- Because global correlation updates occur through the sensor management interface, firewalls must allow port 443/80 traffic.
- You must have an HTTP proxy server or a DNS server configured to allow global correlation features to function.
- If you have an HTTP proxy server configured, the proxy must allow port 443/80 traffic from IPS systems.
- You must have a valid IPS license to allow global correlation features to function.
- Global correlation features only contain external IP addresses, so if you position a sensor in an internal lab, you may never receive global correlation information.
- Make sure your sensor supports the global correlation features.
- Make sure your IPS version supports the global correlation features.

Disabling Global Correlation

If your sensor is deployed in an environment where a DNS server or HTTP proxy server is not available, you may want to disable global correlation so that global correlation health does not appear as red in the overall sensor health, thus indicating a problem. You can also configure sensor health to exclude global correlation status.

To disable global correlation inspection, reputation filtering, and network participation, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Policies > Global Correlation > Inspection/Reputation**.

Step 3 To disable global correlation inspection and reputation filtering, click the **Off** radio button.

Step 4 To disable reputation filtering, click the **Off** radio button.

Step 5 Choose **Configuration > *sensor_name* > Policies > Global Correlation > Network Participation**

Step 6 To disable network participation, click the **Off** radio button.

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

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Configuring SSH and Certificates

This chapter describes how to configure SSH and certificates for your sensor, and it contains the following sections:

Understanding SSH

SSH provides strong authentication and secure communications over channels that are not secure. SSH encrypts your connection to the sensor and provides a key so you can validate that you are connecting to the correct sensor. SSH also provides authenticated and encrypted access to other devices that the sensor connects to for blocking. The IPS supports managing both SSHv1 and SSHv2. The default is SSHv2, but you can configure the sensor to fallback to SSHv1 if the peer client/server does not support SSHv2.

SSH authenticates the hosts or networks using one or both of the following:

- Password
- User RSA public key

Note SSH never sends passwords in clear text.

SSH protects against the following:

- IP spoofing—A remote host sends out packets pretending to come from another trusted host.

  Note SSH even protects against a spoofer on the local network who can pretend he is your router to the outside.

- IP source routing—A host pretends an IP packet comes from another trusted host.
- DNS spoofing—An attacker forges name server records.
- Interception of clear text passwords and other data by intermediate hosts.
- Manipulation of data by those in control of intermediate hosts.
- Attacks based on listening to X authentication data and spoofed connection to the X11 server.

Configuring Authorized RSA Keys

This section describes how to configure authorized RSA keys for the sensor, and contains the following topics:

Authorized RSA Keys Pane

Note You must be administrator to add or edit authorized RSA keys. If you have operator or viewer privileges and you try to add or edit an authorized key, you receive the `Delivery Failed` message.

Use the Authorized RSA Keys pane to manage public keys for SSHv2 clients allowed to use RSA authentication to log in to the local SSH server. The Authorized RSA Keys pane displays the public keys of all SSH clients allowed to access the sensor. You can view only your key and not the keys of other users.

Each user who can log in to the sensor has a list of authorized keys compiled from each client the user logs in with. When using SSHv2 to log in to the sensor, you can use RSA authentication rather than using passwords.

Authorized RSA Keys Pane Field Definitions

The following fields are found in the Authorized RSA Keys pane:

- ID—Specifies a unique string (1 to 256 characters) to identify the key. You receive an error message if the ID contains a space or exceeds 256 alphanumeric characters.
- Public Key—Specifies the public key of the SSHv2 client.

Add and Edit Authorized RSA Key Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Authorized RSA Key dialog boxes:

- ID—Specifies a unique string (1 to 256 characters) to identify the key. You receive an error message if the ID contains a space or exceeds 256 alphanumeric characters.
- Public Key—Specifies the public key of the SSHv2 client.

Defining Authorized RSA Keys

To define public RSA keys, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SSH > Authorized RSA Keys,** and then click **Add** to add a public key to the list. You can add a maximum of 50 SSHv2 authorized keys.

Step 3 In the ID field, enter a unique ID to identify the key.

Step 4 In the Public Key field, enter the public key.

Note You generate the key on the SSH client and enter it in the Public Key field.

Tip To discard your changes and close the Add Authorized RSA Key dialog box, click **Cancel**.

Step 5 Click **OK**. The new key appears in the authorized keys list in the Authorized RSA Keys pane.

Step 6 To edit an existing entry in the authorized keys list, select it, and click **Edit**.

Step 7 Edit the ID and Public Key fields.

Caution You cannot modify the ID field after you have created an entry.

Tip To discard your changes and close the Edit Authorized RSA Key dialog box, click **Cancel**.

Step 8 Click **OK**. The edited key appears in the authorized keys list in the Authorized RSA Keys pane.

Step 9 To delete a public key from the list, select it, and click **Delete**. The key no longer appears in the authorized keys list in the Authorized RSA Keys pane.

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

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Configuring Authorized RSA1 Keys

This section describes how to configure authorized RSA keys for the sensor, and contains the following topics:

Authorized RSA1 Keys Pane

Note You must be administrator to add or edit authorized keys. If you have operator or viewer privileges and you try to add or edit an authorized key, you receive the `Delivery Failed` message.

Use the Authorized RSA1 Keys pane to specify SSHv1 public keys for a client allowed to use RSA authentication to log in to the local SSH server. The Authorized RSA1 Keys pane displays the public keys of all SSH clients allowed to access the sensor. You can view only your key and not the keys of other users.

Each user who can log in to the sensor has a list of authorized keys compiled from each client the user logs in with. When using SSHv1 to log in to the sensor, you can use the RSA authentication rather than using passwords.

Use an RSA key generation tool on the client where the private key is going to reside. Then, display the generated public key as a set of three numbers (modulus length, public exponent, public modulus) and enter those numbers in the fields on the Authorized RSA1 Keys pane.

Authorized RSA1 Keys Pane Field Definitions

The following fields are found in the Authorized RSA1 Keys pane:

- ID—Specifies a unique string (1 to 256 characters) to identify the key. You receive an error message if the ID contains a space or exceeds 256 alphanumeric characters.
- Modulus Length—Specifies the number of significant bits (511 to 2048) in the modulus. You receive an error message if the length is out of range.
- Public Exponent—Used by the RSA algorithm to encrypt data. The valid range is 3 to 2147483647. You receive an error message if the exponent is out of range.
- Public Modulus—Used by the RSA algorithm to encrypt data. The public modulus is a string of 1 to 2048 numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). You receive an error message if the modulus is out of range or if you use characters rather than numbers. The numbers must match the following pattern: ^[0-9][0-9]*$.

Add and Edit Authorized RSA1 Key Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Authorized RSA1 Key dialog boxes:

- ID—Specifies a unique string (1 to 256 characters) to identify the key. You receive an error message if the ID contains a space or exceeds 256 alphanumeric characters.
- Modulus Length—Specifies the number of significant bits (511 to 2048) in the modulus. You receive an error message if the length is out of range.
- Public Exponent—Used by the RSA algorithm to encrypt data. The valid range is 3 to 2147483647. You receive an error message if the exponent is out of range.
- Public Modulus—Used by the RSA algorithm to encrypt data. The public modulus is a string of 1 to 2048 numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). You receive an error message if the modulus is out of range or if you use characters rather than numbers. The numbers must match the following pattern: ^[0-9][0-9]*$.

Defining Authorized RSA1 Keys

To define public RSA1 keys, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SSH > Authorized RSA1 Keys,** and then click **Add** to add a public key to the list. You can add a maximum of 50 SSH authorized keys.

Step 3 In the ID field, enter a unique ID to identify the key.

Step 4 In the Modulus Length field, enter an integer. The modulus length is the number of significant bits in the modulus. The strength of an RSA key relies on the size of the modulus. The more bits the modulus has, the stronger the key.

Note If you do not know the modulus length, public exponent, and public modulus, use an RSA key generation tool on the client where the private key is going to reside. Display the generated public key as a set of three numbers (modulus length, public exponent, and public modulus) and enter those numbers in Steps 4 through 6.

Step 5 In the Public Exponent field, enter an integer. The RSA algorithm uses the public exponent to encrypt data. The valid value for the public exponent is a number between 3 and 2147483647.

Step 6 In the Public Modulus field, enter a value. The public modulus is a string value of numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). The RSA algorithm uses the public modulus to encrypt data.

Tip To discard your changes and close the Add Authorized RSA1 Key dialog box, click **Cancel**.

Step 7 Click **OK**. The new key appears in the authorized keys list in the Authorized RSA1 Keys pane.

Step 8 To edit an existing entry in the authorized keys list, select it, and click **Edit**.

Step 9 Edit the Modulus Length, Public Exponent, and Public Modulus fields.

Caution You cannot modify the ID field after you have created an entry.

Tip To discard your changes and close the Edit Authorized RSA1 Key dialog box, click **Cancel**.

Step 10 Click **OK**. The edited key appears in the authorized keys list in the Authorized RSA1 Keys pane.

Step 11 To delete a public key from the list, select it, and click **Delete**. The key no longer appears in the authorized keys list in the Authorized RSA1Keys pane.

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

Step 12 Click **Apply** to apply your changes and save the revised configuration.

Configuring Known Host RSA Keys

This section describes how to configure known host RSA keys, and contains the following topics:

Known Host RSA Keys Pane

Note You must be administrator to add or edit known host RSA keys.

Use the Known Host RSA Keys pane to define public keys for the blocking devices that the sensor manages, and for SSH (SCP) servers that are used for downloading updates or copying files. You must get each device and server to report its public key so that you have the information you need to configure the Known Host RSA Keys pane. If you cannot obtain the public key in the correct format, click **Retrieve Host Key** in the Add Known Host RSA Keys dialog box.

The IME attempts to retrieve the known host key from the host specified by the IP address. If successful, The IME populates the Add Known Host RSA Key pane with the key.

Note **Retrieve Host Key** is available only in the Add dialog box. You receive an error message if the IP address is invalid.

Known Host RSA Keys Pane Field Definitions

The following fields are found in the Known Host RSA Keys pane:

- IP Address—Specifies the IP address of the host for which you are adding keys.
- Public Key—Specifies the RSA host key.

Add and Edit Known Host RSA Key Dialog Boxes Field Definitions

The following fields and button are found in the Add and Edit Known Host RSA Key dialog boxes:

- IP Address—Specifies the IP address of the host for which you are adding keys.
- Public Key—Specifies the RSA host key.
- Retrieve Host Key—Lets the IME try to retrieve the known host key from the host specified by the IP address. If successful, The IME populates the Add Known Host RSA Key pane with the key.

Note **Retrieve Host Key** is available only in the Add dialog box. You receive an error message if the IP address is invalid.

Defining Known Host RSA Keys

To define known host RSA keys, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SSH > Known Host RSA Keys**, and then click **Add** to add a known host RSA key to the list.

Step 3 In the IP Address field, enter the IP address of the host for which you are adding a key.

Step 4 If you know the public key, enter it in the Public key field, or click **Retrieve Host Key** to obtain the known host key. The IME attempts to retrieve the key from the host whose IP address you entered in Step 3. If the attempt is successful, go to Step 5.

Caution Validate that the key that was retrieved is correct for the specified address to make sure the server IP address is not being spoofed.

Tip To discard your changes and close the Add Known Host RSA Key dialog box, click **Cancel**.

Step 5 Click **OK**. The new key appears in the known host keys list in the Known Host RSA Keys pane.

Step 6 To edit an existing entry in the authorized keys list, select it, and click **Edit**.

Step 7 Edit the ID and the Public Key fields.

Caution You cannot modify the ID field after you have created an entry.

Tip To discard your changes and close the Edit Known Host RSA Key dialog box, click **Cancel**.

Step 8 Click **OK**. The edited key appears in the known host keys list in the Known Host RSA Keys pane.

Step 9 To delete a public key from the list, select it, and click **Delete**. The key no longer appears in the known host keys list in the Known Host RSA Keys pane.

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

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Configuring Known Host RSA1 Keys

This section describes how to configure known host RSA1 keys, and contains the following topics:

Known Host RSA1 Keys Pane

Note You must be administrator to add or edit known host RSA1 keys.

Use the Known Host RSA1 Keys pane to define public keys for the blocking devices that the sensor manages, and for SSH (SCP) servers that are used for downloading updates or copying files. You must get each device and server to report its public key so that you have the information you need to configure the Known Host RSA1 Keys pane. If you cannot obtain the public key in the correct format, click **Retrieve Host Key** in the Add Known Host RSA1 Keys dialog box.

The IME attempts to retrieve the known host key from the host specified by the IP address. If successful, The IME populates the Add Known Host RSA1 Key pane with the key.

Note **Retrieve Host Key** is available only in the Add dialog box. You receive an error message if the IP address is invalid.

Known Host RSA1 Keys Pane Field Definitions

The following fields are found in the Known Host RSA1 Keys pane:

- IP Address—Specifies the IP address of the host for which you are adding keys.
- Modulus Length—Specifies the number of significant bits (511 to 2048) in the modulus. You receive an error message if the length is out of range.
- Public Exponent—Used by the RSA algorithm to encrypt data. The valid range is 3 to 2147483647. You receive an error message if the exponent is out of range.
- Public Modulus—Used by the RSA algorithm to encrypt data. The public modulus is a string of 1 to 2048 numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). You receive an error message if the modulus is out of range or if you use characters rather than numbers. The numbers must match the following pattern: ^[0-9][0-9]*$.

Add and Edit Known Host RSA1 Key Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Known Host RSA1 Key dialog boxes:

Use the Known Host RSA1 Keys pane to define public keys for the blocking devices that the sensor manages, and for SSH (SCP) servers that are used for downloading updates or copying files. You must get each device and server to report its public key so that you have the information you need to configure the Known Host RSA1 Keys pane. If you cannot obtain the public key in the correct format, click **Retrieve Host Key** in the Add Known Host RSA1 Keys dialog box.

The IME attempts to retrieve the known host key from the host specified by the IP address. If successful, The IME populates the Add Known Host RSA1 Key pane with the key.

Note **Retrieve Host Key** is available only in the Add dialog box. You receive an error message if the IP address is invalid.

Defining Known Host RSA1 Keys

To define known host RSA1 keys, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SSH > Known Host RSA1 Keys**, and then click **Add** to add a known host key to the list.

Step 3 In the IP Address field, enter the IP address of the host for which you are adding a key.

Step 4 Click **Retrieve Host Key**. The IME attempts to retrieve the key from the host whose IP address you entered in Step 3. If the attempt is successful, go to Step 8. If the attempt is not successful, complete Steps 5 through 7.

Caution Validate that the key that was retrieved is correct for the specified address to make sure the server IP address is not being spoofed.

Step 5 In the Modulus Length field, enter an integer. The modulus length is the number of significant bits in the modulus. The strength of an RSA key relies on the size of the modulus. The more bits the modulus has, the stronger the key.

Step 6 In the Public Exponent field, enter an integer. The RSA algorithm uses the public exponent to encrypt data.

Step 7 In the Public Modulus field, enter a value. The public modulus is a string value of numbers (where modulus is (2 ^ length) < modulus < (2 ^ (length + 1))). The RSA algorithm uses the public modulus to encrypt data.

Tip To discard your changes and close the Add Known Host RSA1 Key dialog box, click **Cancel**.

Step 8 Click **OK**. The new key appears in the known host keys list in the Known Host RSA1 Keys pane.

Step 9 To edit an existing entry in the authorized keys list, select it, and click **Edit**.

Step 10 Edit the Modulus Length, Public Exponent, and Public Modulus fields.

Caution You cannot modify the ID field after you have created an entry.

Tip To discard your changes and close the Edit Known Host RSA1 Key dialog box, click **Cancel**.

Step 11 Click **OK**. The edited key appears in the known host keys list in the Known Host RSA1 Keys pane.

Step 12 To delete a public key from the list, select it, and click **Delete**. The key no longer appears in the known host keys list in the Known Host RSA1 Keys pane.

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

Step 13 Click **Apply** to apply your changes and save the revised configuration.

Generating the Sensor Key

Note You must be administrator to generate sensor SSH host keys.

The server uses the SSH host key to prove its identity. Clients know they have contacted the correct server when they see a known key. The sensor generates an SSHv1 or SSHv2 host key the first time it starts up. It is displayed in the Sensor Key pane along with the Bubble Babble. Click **Generate Key** to replace that key with a new key.

Note If you generate a new key, you must update the known hosts tables on remote systems with the new key to prevent connection failures.

Field Definitions

The Sensor Key pane displays the current sensor RSA1 (SSHv1) and RSA (SSHv2) host keys. Press **Generate Key** to generate a new sensor SSH host key.

Displaying and Generating the Sensor SSH Host Key

Caution The new key replaces the existing key, which requires you to update the known hosts tables on remote systems with the new host key so that future connections succeed.

To display and generate sensor SSH host keys, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SSH > Sensor Key**. The sensor SSH host key is displayed.

Step 3 To generate a new sensor SSH host key, click **Generate Key**. A dialog box displays the following warning:

```
Generating a new SSH host key requires you to update the known hosts tables on remote
systems with the new key so that future connections succeed. Do you want to continue?
```

Step 4 Click **OK** to continue. A new host key is generated and the old host key is deleted. A status message states the key was updated successfully.

Understanding Certificates

Note The IDM configuration component is embedded in IME.

The Cisco IPS contains a web server that is running the IDM. Management stations connect to this web server. Blocking forwarding sensors also connect to the web server of the master blocking sensor. To provide security, this web server uses an encryption protocol known as TLS, which is closely related to SSL protocol. When you enter a URL into the web browser that starts with `https://ip_address`, the web browser responds by using either TLS or SSL protocol to negotiate an encrypted session with the host.

Caution The web browser initially rejects the certificate presented by the IDM because it does not trust the certificate authority (CA).

Note The IDM is enabled by default to use TLS and SSL.We highly recommend that you use TLS and SSL.

The process of negotiating an encrypted session in TLS is called "handshaking," because it involves a number of coordinated exchanges between client and server. The server sends its certificate to the client. The client performs the following three-part test on this certificate:

1. Is the issuer identified in the certificate trusted?

   Every web browser ships with a list of trusted third-party CAs. If the issuer identified in the certificate is among the list of CAs trusted by your browser, the first test is passed.

2. Is the date within the range of dates during which the certificate is considered valid?

   Each certificate contains a Validity field, which is a pair of dates. If the date falls within this range of dates, the second test is passed.

3. Does the common name of the subject identified in the certificate match the URL hostname?

   The URL hostname is compared with the subject common name. If they match, the third test is passed.

When you direct your web browser to connect with the IDM, the certificate that is returned fails because the sensor issues its own certificate (the sensor is its own CA) and the sensor is not already in the list of CAs trusted by your browser.

When you receive an error message from your browser, you have three options:

- Disconnect from the site immediately.
- Accept the certificate for the remainder of the web browsing session.
- Add the issuer identified in the certificate to the list of trusted CAs of the web browser and trust the certificate until it expires.

The most convenient option is to permanently trust the issuer. However, before you add the issuer, use out-of-band methods to examine the fingerprint of the certificate. This prevents you from being victimized by an attacker posing as a sensor. Confirm that the fingerprint of the certificate appearing in your web browser is the same as the one on your sensor.

Caution If you change the organization name or hostname of the sensor, a new certificate is generated the next time the sensor is rebooted. The next time your web browser connects to the IDM, you will receive the manual override dialog boxes. You must perform the certificate fingerprint validation again for Internet Explorer and Firefox.

For More Information

For more information about the master blocking sensor, see Configuring the Master Blocking Sensor, page 16-23/

Configuring Trusted Hosts

This section describes how to configure trusted hosts, and contains the following sections.

Trusted Hosts Pane

Note You must be administrator to add trusted hosts.

Use the Trusted Hosts pane to add certificates for master blocking sensors and for TLS and SSL servers that the sensor uses for downloading updates. You can also use it to add the IP addresses of external product interfaces, such as CSA MC, that the sensor communicates with.

The Trusted Hosts pane lists all trusted host certificates that you have added. You can add certificates by entering an IP address. The IME retrieves the certificate and displays its fingerprint. If you accept the fingerprint, the certificate is trusted. You can add and delete entries from the list, but you cannot edit them.

Trusted Hosts Pane Field Definitions

The following fields are found in the Trusted Hosts pane:

- IP Address—Specifies the IP address of the trusted host.
- SHA1—Specifies the Secure Hash Algorithm. SHA1 is a cryptographic message digest algorithm.

Add Trusted Host Dialog Box Field Definitions

The following fields are found in the Add Trusted Host dialog box:

- IP Address—Specifies the IP address of the trusted host.
- Port—(Optional) Specifies the port number of where to obtain the host certificate.

Adding Trusted Hosts

To add trusted hosts, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Certificates > Trusted Hosts**, and then click **Add** to add a trusted host to the list.

Step 3 In the IP Address field, enter the IP address of the trusted host you are adding.

Step 4 In the Port field, enter a port number if the sensor is using a port other than 443.

Tip To discard your changes and close the Add Trusted Host dialog box, click **Cancel**.

Step 5 Click **OK**. The IME retrieves the certificate from the host whose IP address you entered in Step 3. The new trusted host appears in the trusted hosts list in the Trusted Hosts pane. A dialog box informs you that the IME is communicating with the sensor:

```
Communicating with the sensor, please wait ...
```

A dialog box provides status about whether the IME was successful in adding a trusted host:

```
The new host was added successfully.
```

Step 6 Verify that the fingerprint is correct by comparing the displayed values with a securely obtained value, such as through direct terminal connection or on the console. If you find any discrepancies, delete the trusted host immediately.

Step 7 To view an existing entry in the trusted hosts list, select it, and click **View**. The View Trusted Host dialog box appears. The certificate data is displayed. Data displayed in this dialog box is read-only.

Step 8 Click **OK**.

Step 9 To delete a trusted host from the list, select it, and click **Delete**. The trusted host no longer appears in the trusted hosts list in the Trusted Hosts pane.

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

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Generating the Server Certificate

Note You must be administrator to generate server certificates.

The Server Certificate pane displays the sensor server X.509 certificate. You can generate a new server self-signed X.509 certificate from this pane. A certificate is generated when the sensor is first started. Click **Generate Certificate** to generate a new host certificate.

Caution The sensor IP address is included in the certificate. If you change the sensor IP address, you must generate a new certificate.

Field Definitions

The Server Certificate pane displays the current server X.509 certificate. Click **Generate Certificate** to generate a new sensor X.509 certificate.

Displaying and Generating the Server Certificate

Note Write down the new fingerprint. Later you will need it to verify what is displayed in your web browser when you connect, or when you are adding the sensor as a trusted host. If the sensor is a master blocking sensor, you must update the trusted hosts table on the remote sensors that are sending blocks to the master blocking sensor.

To display and generate the sensor server X.509 certificate, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Certificate > Server Certificate**. The sensor server X.509 certificate is displayed.

Step 3 To generate a new sensor server X.509 certificate, click **Generate Certificate**. A dialog box displays the following warning:

```
Generating a new server certificate requires you to verify the new fingerprint the next
time you connect or when you add the sensor as a trusted host. Do you want to continue?
```

Step 4 Click **OK** to continue. A new server certificate is generated and the old server certificate is deleted.

Configuring Attack Response Controller for Blocking and Rate Limiting

Note ARC is formerly known as Network Access Controller. Although the name has been changed, the IME and the CLI contain references to Network Access Controller, **nac**, and **network-access**.

This chapter describes how to configure blocking on your sensor. It contains the following sections:

ARC Components

This section describes the various components of the ARC, and contains the following topics:

Understanding Blocking

The ARC is responsible for managing network devices in response to suspicious events by blocking access from attacking hosts and networks. The ARC blocks the IP address on the devices it is managing. It sends the same block to all the devices it is managing, including any other master blocking sensors. The ARC monitors the time for the block and removes the block after the time has expired.

The ARC completes the action response for a new block in no more than 7 seconds. In most cases, it completes the action response in less time. To meet this performance goal, you should not configure the sensor to perform blocks at too high a rate or to manage too many blocking devices and interfaces. We recommend that the maximum number of blocks not exceed 250 and the maximum number of blocking items not exceed 10. To calculate the maximum number of blocking items, a security appliance counts as one blocking item per blocking context. A router counts as one blocking item per blocking interface/direction. A switch running Catalyst software counts as one blocking item per blocking VLAN. If the recommended limits are exceeded, the ARC may not apply blocks in a timely manner or may not be able to apply blocks at all.

Caution Blocking is not supported on the FWSM in multiple mode admin context.

For security appliances configured in multi-mode, Cisco IPS does not include VLAN information in the block request. Therefore you must make sure the IP addresses being blocked are correct for each security appliance. For example, the sensor is monitoring packets on a security appliance customer context that is configured for VLAN A, but is blocking on a different security appliance customer context that is configured for VLAN B. Addresses that trigger blocks on VLAN A may refer to a different host on VLAN B.

There are three types of blocks:

- Host block—Blocks all traffic from a given IP address.
- Connection block—Blocks traffic from a given source IP address to a given destination IP address and destination port. Multiple connection blocks from the same source IP address to either a different destination IP address or destination port automatically switch the block from a connection block to a host block.
- Network block—Blocks all traffic from a given network. You can initiate host and connection blocks manually or automatically when a signature is triggered. You can only initiate network blocks manually.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Caution Do not confuse blocking with the ability of the sensor to drop packets. The sensor can drop packets when the following actions are configured for a sensor in inline mode: deny packet inline, deny connection inline, and deny attacker inline.

For automatic blocks, you must check the Request Block Host or Request Block Connection check boxes as the event action for particular signatures, and add them to any event action overrides you have configured, so that the SensorApp sends a block request to the ARC when the signature is triggered. When the ARC receives the block request from the SensorApp, it updates the device configurations to block the host or connection.

On Cisco routers and Catalyst 6500 series switches, ARC creates blocks by applying ACLs or VACLs. ACLs and VACLs permit or deny passage of data packets through interface directions or VLANs. Each ACL or VACL contains permit and deny conditions that apply to IP addresses. The security appliances do not use ACLs or VACLs. The built-in **shun** and **no shun** command is used.

Caution The ACLs that ARC makes should never be modified by you or any other system. These ACLs are temporary and new ACLs are constantly being created by the sensor. The only modifications that you can make are to the Pre- and Post-Block ACLs.

You need the following information for the ARC to manage a device:

- Login user ID (if the device is configured with AAA).
- Login password.
- Enable password (not needed if the user has enable privileges).
- Interfaces to be managed (for example, ethernet0, vlan100).
- Any existing ACL or VACL information you want applied at the beginning (Pre-Block ACL or VACL) or end (Post-Block ACL or VACL) of the ACL or VACL that will be created. This does not apply to the security appliances because they do not use ACLs to block.
- Whether you are using Telnet or SSH to communicate with the device.
- IP addresses (host or range of hosts) you never want blocked.
- How long you want the blocks to last.

Tip To see the status of the ARC, in the IME choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Statistics**.

Note Rate limiting and blocking are not supported for IPv6 traffic. If a signature is configured with a block or rate limit event action and is triggered by IPv6 traffic, an alert is generated but the action is not carried out.

For More Information

- For the procedure to add Request Block Host or Request Block Connection event actions to a signatures, see Assigning Actions to Signatures, page 10-23.
- For the procedure for configuring overrides that add the Request Block Host or Request Block Connection event actions to alerts of specific risk rating, see Adding, Editing, Deleting, Enabling, and Disabling Event Action Overrides, page 12-14.
- For more information on Pre- and Post-Block ACLs, see How the Sensor Manages Devices, page 16-17.

Understanding Rate Limiting

The 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. The ARC can configure rate limits on network devices running Cisco IOS 12.3 or later. Master blocking sensors can also forward rate limit requests to blocking forwarding sensors.

To add a rate limit, you specify the following:

- Source address and/or destination address for any rate limit
- Source port and/or destination port for rate limits with TCP or UDP protocol

You can also tune rate limiting signatures. You must also set the action to Request Rate Limit and set the percentage for these signatures.

Note Rate limiting and blocking are not supported for IPv6 traffic. If a signature is configured with a block or rate limit event action and is triggered by IPv6 traffic, an alert is generated but the action is not carried out.

Table 16-1 lists the supported rate limiting signatures and parameters.

Table 16-1 Rate Limiting Signatures

Signature ID	Signature Name	Protocol	Destination IP Address Allowed	Data
2152	ICMP Flood Host	ICMP	Yes	echo-request
2153	ICMP Smurf Attack	ICMP	Yes	echo-reply
4002	UDP Flood Host	UDP	Yes	none
6901	Net Flood ICMP Reply	ICMP	No	echo-reply
6902	Net Flood ICMP Request	ICMP	No	echo-request
6903	Net Flood ICMP Any	ICMP	No	None
6910	Net Flood UDP	UDP	No	None
6920	Net Flood TCP	TCP	No	None
3050	TCP HalfOpenSyn	TCP	No	halfOpenSyn

Tip To see the status of the ARC, in the IME choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Statistics**.

For More Information

- For the procedure for configuring rate limiting on a router, see Configuring the Router Blocking and Rate Limiting Device Interfaces, page 16-19.
- For the procedure for configuring a sensor to be a master blocking sensor, see Configuring the Master Blocking Sensor, page 16-25.

Understanding Service Policies for Rate Limiting

You must not apply a service policy to an interface/direction that is configured for rate limiting. If you do so, the rate limit action will fail. Before configuring rate limits, confirm that there is no service policy on the interface/direction, and remove it if one exists. The ARC does not remove the existing rate limit unless it is one that the ARC had previously added.

Rate limits use ACLs, but not in the same way as blocks. Rate limits use **acls** and **class-map** entries to identify traffic, and **policy-map** and **service-policy** entries to police the traffic.

Before Configuring the ARC

Caution Two sensors cannot control blocking or rate limiting on the same device. If this situation is needed, configure one sensor as the master blocking sensor to manage the devices and the other sensors can forward their requests to the master blocking sensor.

Note When you add a master blocking sensor, you reduce the number of blocking devices per sensor. For example, if you want to block on 10 security appliances and 10 routers with one blocking interface/direction each, you can assign 10 to the sensor and assign the other 10 to a master blocking sensor.

Before you configure the ARC for blocking or rate limiting, make sure you do the following:

- Analyze your network topology to understand which devices should be blocked by which sensor, and which addresses should never be blocked.
- Gather the usernames, device passwords, enable passwords, and connections types (Telnet or SSH) needed to log in to each device.
- Know the interface names on the devices.
- Know the names of the Pre-Block ACL or VACL and the Post-Block ACL or VACL if needed.
- Understand which interfaces should and should not be blocked and in which direction (in or out). You do not want to accidentally shut down an entire network.

Supported Devices

Caution If the recommended limits are exceeded, the ARC may not apply blocks in a timely manner or may not be able to apply blocks at all.

By default, the ARC supports up to 250 devices in any combination. The following devices are supported for blocking by the ARC:

- Cisco series routers using Cisco IOS 11.2 or later (ACLs):
  - Cisco 1600 series router
  - Cisco 1700 series router
  - Cisco 2500 series router

  - Cisco 2600 series router
  - Cisco 2800 series router
  - Cisco 3600 series router
  - Cisco 3800 series router
  - Cisco 7200 series router
  - Cisco 7500 series router
- Catalyst 5000 switches with RSM with IOS 11.2(9)P or later (ACLs)
- Catalyst 6500 switches and 7600 routers with IOS 12.1(13)E or later (ACLs)
- Catalyst 6500 switches 7600 routers with Catalyst software version 7.5(1) or later (VACLs)
  - Supervisor Engine 1A with PFC
  - Supervisor Engine 1A with MSFC1
  - Supervisor Engine 1A with MFSC2
  - Supervisor Engine 2 with MSFC2
  - Supervisor Engine 720 with MSFC3

Note We support VACL blocking on the Supervisor Engine and ACL blocking on the MSFC.

- PIX Firewall with version 6.0 or later (**shun** command)
  - 501
  - 506E
  - 515E
  - 525
  - 535
- ASA with version 7.0 or later (**shun** command)
  - ASA 5510
  - ASA 5520
  - ASA 5540
- FWSM 1.1 or later (**shun** command)

You configure blocking using either ACLs, VACLS, or the **shun** command. All firewall and ASA models support the **shun** command.

The following devices are supported for rate limiting by the ARC:

- Cisco series routers using Cisco IOS 12.3 or later:
  - Cisco 1700 series router
  - Cisco 2500 series router
  - Cisco 2600 series router
  - Cisco 2800 series router
  - Cisco 3600 series router
  - Cisco 3800 series router

- Cisco 7200 series router
- Cisco 7500 series router

Caution The ARC cannot perform rate limits on 7500 routers with VIP. The ARC reports the error but cannot rate limit.

Configuring Blocking Properties

This section describes how to configure blocking properties for the sensor, and contains the following topics:

Blocking Properties Pane

Note You must be administrator or operator to add, edit, or delete IP addresses never to be blocked.

Use the Blocking Properties pane to configure the basic settings required to enable blocking and rate limiting.

Understanding Blocking Properties

The ARC controls blocking and rate limiting actions on managed devices. You must tune your sensor to identify hosts and networks that should never be blocked, not even manually. You may have a trusted network device whose normal, expected behavior appears to be an attack. Such a device should never be blocked, and trusted, internal networks should never be blocked. Properly tuning signatures reduces the number of false positives and helps ensure proper network operations. Tuning and filtering signatures prevents alarms from being generated. If an alarm is not generated, the associated block does not occur.

Note Never Block Address does not apply to rate limiting. This option applies only to the Request Block Host or Request Block Connection event actions. It does not apply to the Deny Attacker Inline, Deny Connection Inline, or Deny Packet Inline event actions. Use event action rules to filter out the hosts that you do not want blocked, denied, or dropped.

If you specify a netmask, this is the netmask of the network that should never be blocked. If no netmask is specified, only the IP address you specify will never be blocked.

Caution We recommend that you do not permit the sensor to block itself, because it may stop communicating with the blocking device. You can configure this option if you can ensure that if the sensor creates a rule to block its own IP address, it will not prevent the sensor from accessing the blocking device.

By default, blocking is enabled on the sensor. If the ARC is managing a device and you need to manually configure something on that device, you should disable blocking first. You want to avoid a situation in which both you and the ARC could be making a change at the same time on the same device. This could cause the device or the ARC to fail.

By default, only blocking is supported on Cisco IOS devices. You can override the blocking default by selecting rate limiting or blocking plus rate limiting.

Blocking Properties Pane Field Definitions

The following fields are found in the Blocking Properties pane:

- Enable blocking— Specifies whether or not to enable blocking of hosts. The default is enabled. You receive an error message if Enable blocking is disabled and nondefault values exist in the other fields.

  Note When you enable blocking, you also enable rate limiting. When you disable blocking, you also disable rate limiting. This means that the ARC cannot add new or remove existing blocks or rate limits.

  Note Even if you do not enable blocking, you can configure all other blocking settings.

- Allow sensor IP address to be blocked—Specifies whether or not the sensor IP address can be blocked. The default is disabled.
- Log all block events and errors—Configures the sensor to log events that follow blocks from start to finish and any error messages that occur. When a block is added to or removed from a device, an event is logged. You may not want all these events and errors to be logged. Disabling this option suppresses new events and errors. The default is enabled.

  Note Log all block events and errors also applies to rate limiting.

- Enable NVRAM write—Configures the sensor to have the router write to NVRAM when the ARC first connects. If enabled, NVRAM is written each time the ACLs are updated. The default is disabled.

  Note Enabling NVRAM writing ensures that all changes for blocking and rate limiting are written to NVRAM. If the router is rebooted, the correct blocks and rate limits will still be active. If NVRAM writing is disabled, a short time without blocking or rate limiting occurs after a router reboot. Not enabling NVRAM writing increases the life of the NVRAM and decreases the time for new blocks and rate limits to be configured.

- Enable ACL Logging—Causes the ARC to append the log parameter to block entries in the ACL or VACL. This causes the device to generate syslog events when packets are filtered. This option only applies to routers and switches. The default is disabled.
- Maximum Block Entries—Specifies the maximum number of entries to block. The value is 1 to 65535. The default is 250.
- Maximum Interfaces—Configures the maximum number of interfaces for performing blocks.

  For example, a PIX 500 series security appliance counts as one interface. A router with one interface counts as one, but a router with two interfaces counts as two. The maximum number of interfaces is 250 per device. The default is 250.

  Note You use Maximum Interfaces to set an upper limit on the number of devices and interfaces that the ARC can manage. The total number of blocking devices (not including master blocking sensors) cannot exceed this value. The total number of blocking items also cannot exceed this value, where a blocking item is one security appliance context, one router blocking interface/direction, or one Catalyst Software switch blocking VLAN.

  Note In addition, the following maximum limits are fixed and you cannot change them: 250 interfaces per device, 250 security appliances, 250 routers, 250 Catalyst Software switches, and 100 master blocking sensors.

- Maximum Rate Limit Entries—Specifies the maximum number of rate limit entries. The maximum rate limit should be equal to or less than the maximum blocking entries. If you configure more rate limit entries than block entries, you receive an error. The value is 1 to 32767. The default is 250.
- Never Block Addresses—Lets you configure IP addresses that you want the sensor to avoid blocking:

  Note Never Block Address does not apply to rate limiting. This option applies only to the Request Block Host and Request Block Connection event actions. It does not apply to the Deny Attacker Inline, Deny Connection Inline, or Deny Packet Inline event actions. Use event action rules to filter out the hosts that you do not want blocked, denied, or dropped.

  - IP Address—Specifies the IP address to never block.
  - Mask—Specifies the mask corresponding to the IP address never to block.

Configuring Blocking Properties

To configure blocking properties, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Blocking > Blocking Properties**.

Step 3 Check the **Enable blocking** check box to enable blocking and rate limiting.

Note For blocking or rate limiting to operate, you must set up devices to do the blocking or rate limiting.

Step 4 Do not check the **Allow the sensor IP address to be blocked** check box unless necessary.

Caution We recommend that you do not allow the sensor to block itself, because it may stop communicating with the blocking device. You can select this option if you can ensure that if the sensor creates a rule to block its own IP address, it will not prevent the sensor from accessing the blocking device.

Step 5 Check the **Log all block events and errors** check box if you want the blocking events and errors logged.

Step 6 Check the **Enable NVRAM write** check box if you want the sensor to have the router write to NVRAM when the ARC first connects.

Step 7 Check the **Enable ACL logging** check box if you want the ARC to append the log parameter to block entries in the ACL or VACL.

Step 8 In the Maximum Block Entries field, enter how many blocks are to be maintained simultaneously (1 to 65535).

Note We do not recommend setting the maximum block entries higher than 250.

Note The number of blocks will not exceed the maximum block entries. If the maximum is reached, new blocks will not occur until existing blocks time out and are removed.

Step 9 Enter the number of interfaces you want to have performing blocks in the Maximum Interfaces field.

Step 10 Enter the number of rate limit entries (1 to 32767) you want in the Maximum Rate Limit Entries field.

Caution The maximum rate limit should be equal to or less than the maximum blocking entries. If you configure more rate limit entries than block entries, you receive an error.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Add and Edit Never Block Address Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Never Block Address dialog boxes:

- IP Address—Specifies the IP address to never block.
- Mask—Specifies the mask corresponding to the IP address never to block.

Adding, Editing, and Deleting IP Addresses Never to be Blocked

To add, edit, and delete an IP address never to be blocked, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Blocking > Blocking Properties**, and click **Add** to add a host or network to the list of addresses never to be blocked.

Step 3 In the IP Address field, enter the IP address of the host or network.

Step 4 In the Network Mask field, enter the network mask of the host or network, or select a network mask from the list.

Tip To discard your changes and close the Add Never Block Address dialog box, click **Cancel**.

Step 5 Click **OK**. You receive an error message if the entries are identical. The new host or network appears in the Never Block Addresses list in the Blocking Properties pane.

Step 6 To edit an existing entry in the never block addresses list, select it, and click **Edit**.

Step 7 In the IP Address field, edit the IP address of the host or network.

Step 8 In the Network Mask field, edit the network mask of the host or network.

Tip To discard your changes and close the Edit Never Block Address dialog box, click **Cancel**.

Step 9 Click **OK**. The edited host or network appears in the Never Block Addresses list in the Allowed Hosts pane.

Step 10 To delete a host or network from the list, select it, and click **Delete**. The host no longer appears in the Never Block Addresses list in the Blocking Properties pane.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring Device Login Profiles

This section describes how to configure device login profiles, and contains the following topics:

Device Login Profiles Pane

Note You must be administrator or operator to add or edit device login profiles.

Use the Device Login Profiles pane to configure the profiles that the sensor uses when logging in to blocking devices. You must set up device login profiles for the other hardware that the sensor manages. The device login profiles contain username, login password, and enable password information under a name that you create. For example, routers that all share the same passwords and usernames can be under one device login profile name.

Note You must have a device login profile created before configuring the blocking devices.

Device Login Profiles Pane Field Definitions

The following fields are found on the Device Login Profiles pane:

- Profile Name—Specifies the name of the profile.
- Username—Specifies the username used to log in to the blocking device.
- Login Password—Specifies the login password used to log in to the blocking device.

  Note If a password exists, it is displayed with a fixed number of asterisks.

- Enable Password—Specifies the enable password used on the blocking device.

  Note If a password exists, it is displayed with a fixed number of asterisks.

Add and Edit Device Login Profile Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Device Login Profile dialog boxes.

- Profile Name—Specifies the name of the profile.
- Username—Specifies the username used to log in to the blocking device.
- Login Password—Specifies the login password used to log in to the blocking device.

  Note If a password exists, it is displayed with a fixed number of asterisks.

- Enable Password—Specifies the enable password used on the blocking device.

  Note If a password exists, it is displayed with a fixed number of asterisks.

Configuring Device Login Profiles

To configure device login profiles, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Blocking > Device Login Profiles**, and click **Add** to add a profile.

Step 3 In the Profile Name field, enter the profile name.

Step 4 (Optional) In the Username field, enter the username used to log in to the blocking device.

Step 5 (Optional) In the New Password field, enter the login password.

Step 6 (Optional) In the Confirm New Password field, enter the login password again to confirm it.

Step 7 (Optional) In the New Password field, enter the enable password.

Step 8 (Optional) In the Confirm New Password field, enter the enable password again to confirm it.

Tip To discard your changes and close the Add Device Login Profile dialog box, click **Cancel**.

Step 9 Click **OK**. You receive an error message if the profile name already exists. The new device login profile appears in the list in the Device Login Profile pane.

Step 10 To edit an existing entry in the device login profile list, select it, and click **Edit**.

Step 11 In the Username field, edit the username used to log in to the blocking device.

Step 12 Check the **Change the login password check box** to change the login password.

Step 13 In the New Password field, enter the new login password.

Step 14 In the Confirm New Password field, enter the new login password to confirm it.

Step 15 Check the **Change the enable password** check box to change the enable password.

Step 16 In the New Password field, enter the new enable password.

Step 17 In the Confirm New Password field, enter the enable password to confirm it.

Tip To discard your changes and close the Edit Device Login Profile dialog box, click **Cancel**.

Step 18 Click **OK**. The edited device login profile appears in the list in the Device Login Profile pane.

Step 19 To delete a device login profile from the list, select it, and click **Delete**. The device login profile no longer appears in the list in the Device Login Profile pane.

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

Step 20 Click **Apply** to apply your changes and save the revised configuration.

Configuring Blocking Devices

This section describes how to configure blocking devices, and contains the following topics:

Blocking Device Pane

Note You must be administrator or operator to configure blocking devices.

Use the Blocking Devices pane to configure the devices that the sensor uses to implement blocking and rate limiting. You can configure your sensor to block an attack by generating ACL rules for deployment to a Cisco IOS router, or a Catalyst 6500 switch, or by generating shun rules on a security appliance. The router, switch, or security appliance is called a blocking device.

Rate limits use ACLs, but not in the same way as blocks. Rate limits use ACLs and class-map entries to identify traffic, and policy-map and service-policy entries to police the traffic.

Caution A single sensor can manage multiple devices but multiple senors cannot manage a single device. For that you must use a master blocking sensor.

You must specify a device login profile for each device that the sensor manages before you can configure the devices in the Blocking Devices pane.

Blocking Devices Pane Field Definitions

The following fields are found in the Blocking Devices pane:

- IP Address—Specifies the IP address of the blocking device.
- Sensor's NAT Address—Specifies the NAT address of the sensor.
- Device Login Profile—Specifies the device login profile used to log in to the blocking device.
- Device Type—Specifies the type of device (Cisco Router, Cat 6K, PIX/ASA). The default is Cisco Router.
- Response Capabilities—Specifies whether the device uses blocking or rate limiting or both.
- Communication—Specifies the communication mechanism used to log in to the blocking device (SSH 3DES and Telnet). The default is SSH 3DES.

Add and Edit Blocking Device Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Blocking Device dialog boxes:

- IP Address—Specifies the IP address of the blocking device.

- Sensor's NAT Address—Specifies the NAT address of the sensor.
- Device Login Profile—Specifies the device login profile used to log in to the blocking device.
- Device Type—Specifies the type of device (Cisco Router, Cat 6K, PIX/ASA). The default is Cisco Router.
- Response Capabilities—Specifies whether the device uses blocking or rate limiting or both.
- Communication—Specifies the communication mechanism used to log in to the blocking device (SSH 3DES and Telnet). The default is SSH 3DES.

Adding, Editing, and Deleting Blocking and Rate Limiting Devices

To add, edit, or delete blocking and rate limiting devices, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Blocking > Blocking Devices**, and click **Add** to add a blocking device. You receive an error message if you have not configured the device login profile.

Step 3 In the IP Address field, enter the IP address of the blocking device.

Step 4 (Optional) In the Sensor's NAT Address field, enter the NAT address of the sensor.

Step 5 From the Device Login Profile drop-down list, choose the device login profile.

Step 6 From the Device Type drop-down list, choose the device type.

Step 7 In the Response Capabilities field, check the **Block** and/or **Rate Limit** check boxes to specify whether the device will perform blocking, rate limiting, or both.

Note You must select the blocking and rate limiting actions for particular signatures so that SensorApp sends a block or rate limit request to ARC when the signature is triggered.

Step 8 From the Communication drop-down list, choose the communication type. If you choose SSH 3DES, go to Step 11.

Tip To discard your changes and close the Add Blocking Device dialog box, click **Cancel**.

Step 9 Click **OK**. You receive an error message if the IP address has already been added. The new device appears in the list in the Blocking Devices pane.

Step 10 If you choose SSH 3DES, you must add the device to the known hosts list:

Note If you select SSH 3DES, the blocking device must have a feature set or license that supports 3DES encryption.

Note You can also choose **Configuration > *sensor_name* > Sensor Management > SSH > Known Host Keys > Add Known Host Key** to add the device to the known hosts list.

a. Telnet to your sensor and log in to the CLI.

b. Enter global configuration mode:

```
sensor# configure terminal
```

c. Obtain the public key:

```
sensor(config)# ssh host-key blocking_device_ip_address
```

d. You are prompted to confirm adding the public key to the known hosts list:

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

e. Enter **yes**.

f. Exit global configuration mode and the CLI:

```
sensor(config)# exit
sensor# exit
```

Step 11 To edit an existing entry in the blocking devices list, select it, and click **Edit**.

Step 12 Edit the NAT address of the sensor if desired.

Step 13 Change the device login profile if desired.

Step 14 Change the device type if desired.

Step 15 Change whether the device will perform blocking or rate limiting if desired.

Step 16 Change the communication type if desired.

Tip To discard your changes and close the Edit Blocking Device dialog box, click **Cancel**.

Step 17 Click **OK**. The edited blocking device appears in the list in the Blocking Device pane.

Step 18 To delete a blocking device from the list, select it, and click **Delete**. The blocking device no longer appears in the list in the Blocking Device pane.

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

Step 19 Click **Apply** to apply your changes and save the revised configuration.

Configuring Router Blocking Device Interfaces

This section describes how to configure router blocking device interfaces, and contains the following topics:

Router Blocking Device Interfaces Pane

Note You must be administrator or operator to configure the router blocking device interfaces.

You must configure the blocking or rate limiting interfaces on the router and specify the direction of traffic you want blocked or rate-limited in the Router Blocking Device Interfaces pane.

Understanding Router Blocking Device Interfaces

Note Pre-Block and Post-Block ACLS do not apply to rate limiting.

You create and save Pre-Block and Post-Block ACLs in your router configuration. These ACLs must be extended IP ACLs, either named or numbered. See your router documentation for more information on creating ACLs. Enter the names of these ACLs that are already configured on your router in the Pre-Block ACL and Post-Block ACL fields.

The Pre-Block ACL is mainly used for permitting what you do not want the sensor to ever block. When a packet is checked against the ACL, the first line that gets matched determines the action. If the first line matched is a permit line from the Pre-Block ACL, the packet is permitted even though there may be a deny line (from an automatic block) listed later in the ACL. The Pre-Block ACL can override the deny lines resulting from the blocks.

The Post-Block ACL is best used for additional blocking or permitting that you want to occur on the same interface or direction. If you have an existing ACL on the interface or direction that the sensor will manage, that existing ACL can be used as a Post-Block ACL. If you do not have a Post-Block ACL, the sensor inserts **permit ip any any** at the end of the new ACL.

When the sensor starts up, it reads the contents of the two ACLs. It creates a third ACL with the following entries:

- A **permit** line for the sensor IP address
- Copies of all configuration lines of the Pre-Block ACL
- A **deny** line for each address being blocked by the sensor
- Copies of all configuration lines of the Post-Block ACL

The sensor applies the new ACL to the interface and direction that you designate.

Note When the new ACL is applied to an interface or direction of the router, it removes the application of any other ACL to that interface or direction.

How the Sensor Manages Devices

Note ACLs do not apply to rate limiting devices.

The ARC uses ACLs on Cisco routers and switches to manage those devices. These ACLs are built as follows:

1. A **permit** line with the sensor IP address or, if specified, the NAT address of the sensor.

   Note If you permit the sensor to be blocked, this line does not appear in the ACL.

2. Pre-Block ACL (if specified). This ACL must already exist on the device.

   Note The ARC reads the lines in the ACL and copies these lines to the beginning of the ACL.

3. Any active blocks.
4. Either specify a Post-Block ACL, which must already exist on the device, or specify **permit ip any any** (do not use if a Post-Block ACL is specified). The ARC reads the lines in the ACL and copies these lines to the end of the ACL.

   Note Make sure the last line in the ACL is **permit ip any any** if you want all unmatched packets to be permitted.

The ARC uses two ACLs to manage devices. Only one is active at any one time. It uses the offline ACL name to build the new ACL, then applies it to the interface. The ARC then reverses the process on the next cycle.

Caution The ACLs that the ARC makes should never be modified by you or any other system. These ACLs are temporary and new ACLs are constantly being created by the sensor. The only modifications that you can make are to the Pre- and Post-Block ACLs.

If you need to modify the Pre-Block or Post-Block ACL, do the following:

1. Disable blocking on the sensor.
2. Make the changes to the configuration of the device.
3. Reenable blocking on the sensor.

When blocking is reenabled, the sensor reads the new device configuration.

Caution A single sensor can manage multiple devices, but you cannot use multiple sensors to control a single device. In this case, use a master blocking sensor.

For More Information

- For the procedure for enabling blocking, see Configuring Blocking Properties, page 16-9.
- For the procedure for configuring the sensor to be a master blocking sensor, see Configuring the Master Blocking Sensor, page 16-25.

Router Blocking Device Interfaces Pane Field Definitions

The following fields are found in the Router Blocking Device Interfaces pane:

- Router Blocking Device—Specifies the IP address of the router blocking or rate limiting device.
- Blocking Interface—Specifies the interface to be used on the router blocking or rate limiting device. A valid value is 1 to 64 characters in the format a-z, A-Z, 0-9 and the special characters "." and "/."
- Direction—Specifies the direction to apply the blocking ACL. A valid value is In or Out.
- Pre-Block ACL—Specifies the ACL to apply before the blocking ACL. A valid value is 0 to 64 characters. This field does not apply to rate limiting.
- Post-Block ACL—Specifies the ACL to apply after the blocking ACL. A valid value is 0 to 64 characters. This field does not apply to rate limiting

Note The Post-Block ACL cannot be the same as the Pre-Block ACL.

Add and Edit Router Blocking Device Interface Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Router Blocking Device Interface dialog boxes:

- Router Blocking Device—Specifies the IP address of the router blocking or rate limiting device.
- Blocking Interface—Specifies the interface to be used on the router blocking or rate limiting device. A valid value is 1 to 64 characters in the format a-z, A-Z, 0-9 and the special characters "." and "/."
- Direction—Specifies the direction to apply the blocking ACL. A valid value is In or Out.
- Pre-Block ACL—Specifies the ACL to apply before the blocking ACL. A valid value is 0 to 64 characters. This field does not apply to rate limiting.
- Post-Block ACL—Specifies the ACL to apply after the blocking ACL. A valid value is 0 to 64 characters. This field does not apply to rate limiting

Note The Post-Block ACL cannot be the same as the Pre-Block ACL.

Configuring the Router Blocking and Rate Limiting Device Interfaces

To configure router blocking and rate limiting device interfaces, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Blocking > Router Blocking Device Interfaces**, and click **Add** to add a router blocking or rate limiting device interface.

Step 3 In the Router Blocking Device drop-down list, choose the IP address of the router blocking or rate limiting device.

Step 4 In the Blocking Interface field, enter the blocking or rate limiting interface name.

Step 5 From the Direction drop-down list, choose the direction (in or out).

Step 6 (Optional) In the Pre-Block ACL field, enter the name of the Pre-Block ACL.

Note This step does not apply to rate limiting devices.

Step 7 (Optional) In the Post-Block ACL field, enter the name of the Post-Block ACL.

Note This step does not apply to rate limiting devices.

Tip To discard your changes and close the Add Router Blocking Device Interface dialog box, click **Cancel**.

Step 8 Click **OK**. You receive an error message if the IP address/interface/direction combination already exists. The new interface appears in the list in the Router Blocking Device Interfaces pane.

Step 9 To edit an existing entry in the router blocking device interfaces list, select it, and click **Edit**.

Step 10 Edit the blocking or rate limiting interface name, if needed.

Step 11 Change the direction, if needed.

Step 12 Edit the Pre-Block ACL name, if needed.

Step 13 Edit the Post-Block ACL name, if needed.

Tip To discard your changes and close the Edit Router Blocking Device Interface dialog box, click **Cancel**.

Step 14 Click **OK**. The edited router blocking or rate limiting device interface appears in the list in the Router Blocking Device Interfaces pane.

Step 15 To delete a router blocking or rate limiting device interface from the list, select it, and click **Delete**. The router blocking or rate limiting device interface no longer appears in the list in the Router Blocking Device Interfaces pane.

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

Step 16 Click **Apply** to apply your changes and save the revised configuration.

Configuring Cat 6K Blocking Device Interfaces

This section describes how to configure Catalyst 6500 Series interfaces, and contains the following topics:

- Add and Edit Cat 6K Blocking Device Interface Dialog Boxes Field Definitions, page 16-22
- Configuring Cat 6K Blocking Device Interfaces, page 16-22

Cat 6K Blocking Device Interfaces Pane

Note You must be administrator or operator to configure the Catalyst 6500 series switches blocking device interfaces.

You specify the VLAN ID and VACLs on the blocking Catalyst 6500 series switch in the Cat 6K Blocking Device Interfaces pane.

Understanding Cat 6K Blocking Device Interfaces

You can configure the ARC to block using VACLs on the switch itself when running Cisco Catalyst software, or to block using router ACLs on the MSFC or on the switch itself when running Cisco IOS software. This section describes blocking using VACLs. You cannot configure switches that use VACLs to perform rate limiting. You must configure the blocking interfaces on the Catalyst 6500 series switch and specify the VLAN of traffic you want blocked.

You create and save Pre-Block and Post-Block VACLs in your switch configuration. These VACLs must be extended IP VACLs, either named or numbered. See your switch documentation for more information on creating VACLs. Enter the names of these VACLs that are already configured on your switch in the Pre-Block VACL and Post-Block VACL fields.

The Pre-Block VACL is used mainly for permitting what you do not want the sensor to ever block. When a packet is checked against the VACL, the first line that gets matched determines the action. If the first line matched is a permit line from the Pre-Block VACL, the packet is permitted even though there may be a deny line (from an automatic block) listed later in the VACL. The Pre-Block VACL can override the deny lines resulting from the blocks.

The Post-Block VACL is best used for additional blocking or permitting that you want to occur on the same VLAN. If you have an existing VACL on the VLAN that the sensor will manage, the existing VACL can be used as a Post-Block VACL. If you do not have a Post-Block V ACL, the sensor inserts **permit ip any any** at the end of the new VACL.

When the sensor starts up, it reads the contents of the two VACLs. It creates a third VACL with the following entries:

- A **permit** line for the sensor IP address
- Copies of all configuration lines of the Pre-Block VACL
- A **deny** line for each address being blocked by the sensor
- Copies of all configuration lines of the Post-Block VACL

The sensor applies the new VACL to the VLAN that you designate.

Note When the new VACL is applied to a VLAN of the switch, it removes the application of any other VACL to that VLAN.

For More Information

For blocking using router ACLs, see Configuring the Router Blocking and Rate Limiting Device Interfaces, page 16-19.

Cat 6K Blocking Device Interfaces Pane Field Definitions

The following fields are found in the Cat 6K Blocking Device Interfaces pane:

- Cat 6K Blocking Device—Specifies the IP address of the Catalyst 6500 series switch blocking device.
- VLAN ID—Specifies the VLAN ID to be used on the Catalyst 6500 series switch blocking device. The value is 1 to 4094.
- Pre-Block VACL—Specifies the VACL to apply before the blocking VACL. The value is 0 to 64 characters.
- Post-Block VACL—Specifies the VACL to apply after the blocking VACL. The value is 0 to 64 characters.

Note The Post-Block VACL cannot be the same as the Pre-Block VACL.

Add and Edit Cat 6K Blocking Device Interface Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Cat 6K Blocking Device Interface dialog boxes:

- Cat 6K Blocking Device—Specifies the IP address of the Catalyst 6500 series switch blocking device.
- VLAN ID—Specifies the VLAN ID to be used on the Catalyst 6500 series switch blocking device. The value is 1 to 4094.
- Pre-Block VACL—Specifies the VACL to apply before the blocking VACL. The value is 0 to 64 characters.
- Post-Block VACL—Specifies the VACL to apply after the blocking VACL. The value is 0 to 64 characters.

Note The Post-Block VACL cannot be the same as the Pre-Block VACL.

Configuring Cat 6K Blocking Device Interfaces

To configure Catalyst 6500 series switch blocking device interfaces, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Blocking > Cat 6K Blocking Device Interfaces**, and click **Add** to add a Catalyst 6500 series switch blocking device interface.

Step 3 From the Cat 6K Blocking Device drop-down list, choose the IP address of the Catalyst 6500 series switch.

Step 4 In the VLAN ID field, enter the VLAN ID.

Step 5 (Optional) In the Pre-Block VACL field, enter the name of the Pre-Block VACL.

Step 6 (Optional) In the Post-Block VACL field, enter the name of the Post-Block VACL.

Tip To discard your changes and close the Add Cat 6K Blocking Device Interface dialog box, click **Cancel**.

Step 7 Click **OK**. You receive an error message if the IP address/VLAN combination already exists. The new interface appears in the list in the Cat 6K Blocking Device Interfaces pane.

Step 8 To edit an existing entry in the Catalyst 6500 series switch blocking device interfaces list, select it, and click **Edit**.

Step 9 Edit the VLAN ID, if needed.

Step 10 Edit the Pre-Block VACL name, if needed.

Step 11 Edit the Post-Block VACL name, if needed.

Tip To discard your changes and close the Edit Cat 6K Blocking Device Interface dialog box, click **Cancel**.

Step 12 Click **OK**. The edited Catalyst 6500 series switch blocking device interface appears in the list in the Cat 6K Blocking Device Interfaces pane.

Step 13 To delete a Catalyst 6500 series switch blocking device interface from the list, select it, and click **Delete**. The Catalyst 6500 series switch blocking device interface no longer appears in the list in the Cat 6K Blocking Device Interfaces pane.

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

Step 14 Click **Apply** to apply your changes and save the revised configuration.

Configuring the Master Blocking Sensor

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

Master Blocking Sensor Pane

Note You must be administrator or operator to configure the master blocking sensor.

You specify the master blocking sensor that is used to configure the blocking devices in the Master Blocking Sensor pane.

Understanding the Master Blocking Sensor

Multiple sensors (blocking forwarding sensors) can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The master blocking sensor is the ARC running on a sensor that controls blocking on one or more devices on behalf of one or more other sensors. The ARC on a master blocking sensor controls blocking on devices at the request of the ARCs running on other sensors. Master blocking sensors can also forward rate limits.

Caution Two sensors cannot control blocking or rate limiting on the same device. If this situation is needed, configure one sensor as the master blocking sensor to manage the devices and the other sensors can forward their requests to the master blocking sensor.

When you add a master blocking sensor, you reduce the number of blocking devices per sensor. For example, if you want to block on 10 firewalls and 10 routers with one blocking interface/direction each, you can assign 10 to the sensor and assign the other 10 to a master blocking sensor.

On the blocking forwarding sensor, identify which remote host serves as the master blocking sensor; on the master blocking sensor you must add the blocking forwarding sensors to its access list.

If the master blocking sensor requires TLS for web connections, you must configure the ARC of the blocking forwarding sensor to accept the X.509 certificate of the master blocking sensor remote host. Sensors by default have TLS enabled, but you can change this option.

Note Typically the master blocking sensor is configured to manage the network devices. Blocking forwarding sensors are not normally configured to manage other network devices, although doing so is permissible.

Even if you have no devices configured for blocking or rate limiting, a sensor that is configured for blocking or rate limiting can forward blocking and rate limiting requests to a master blocking sensor. When a signature fires that has blocking or rate limit requests configured as event actions, the sensor forwards the block or rate limit request to the master blocking sensor, which then performs the block or rate limit.

Caution Only one sensor should control all blocking interfaces on a device.

Master Blocking Sensor Pane Field Definitions

The following fields are found in the Master Blocking Sensor pane:

- IP Address—Specifies the IP address of the master blocking sensor.
- Port—Specifies the port on which to connect to the master blocking sensor. The default is 443.
- Username—Specifies the username used to log in to the master blocking sensor. The username follows the pattern ^[A-Za-z0-9()+:,_/-]+$, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and _, and can contain 1 to 64 characters.
- TLS Used—Specifies whether or not TLS is being used.

Add and Edit Master Blocking Sensor Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Master Blocking Sensor dialog boxes:

- IP Address—Specifies the IP address of the master blocking sensor. You receive a warning if the IP address already exists.
- Port (optional)—Specifies the port on which to connect on the master blocking sensor. The default is 443.
- Username—Specifies the username used to log in to the master blocking sensor. A valid value is 1 to 16 characters.
- Change the password—Lets you change the password.
- New Password—Specifies the login password used to log in to the master blocking sensor.
- Confirm Password—Confirms the login password.
- Use TLS—Specifies whether or not to use TLS.

Configuring the Master Blocking Sensor

To configure the master blocking sensor, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Blocking > Master Blocking Sensor**, and click **Add** to add an master blocking sensor.

Step 3 In the IP Address field, enter the IP address of the master blocking sensor.

Step 4 (Optional) In the Port field, enter the port number. The default is 443.

Step 5 In the Username field, enter the username.

Step 6 In the New Password field, enter the password for the user.

Step 7 In the Confirm New Password field, enter the password to confirm it.

Step 8 Check the **TLS** check box.

Tip To discard your changes and close the Add Master Blocking Sensor dialog box, click **Cancel**.

Step 9 Click **OK**. You receive an error message if the IP address has already been added. The new master blocking sensor appears in the list in the Master Blocking Sensor pane.

Step 10 If you selected TLS, configure the ARC of the blocking forwarding sensor to accept the TLS/SSL X.509 certificate of the master blocking sensor remote host:

Note You can also choose **Configuration > *sensor_name* > Sensor Management > Certificates > Trusted Hosts > Add Trusted Host** to configure the blocking forwarding sensor to accept the X.509 certificate.

a. Log in to the CLI of the blocking forwarding sensor using an account with administrator privileges.

b. Enter global configuration mode.

```
sensor# configure terminal
```

c. Add the trusted host.

```
sensor(config)# tls trusted-host ip-address master_blocking_sensor_ip_address
```

You are prompted to confirm adding the trusted host:

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

d. Enter **yes** to add the host.

e. Exit global configuration mode and the CLI.

```
sensor(config)# exit
sensor# exit
```

You are prompted to accept the certificate based on the fingerprint of the certificate. Sensors provide only self-signed certificates (instead of certificates signed by a recognized certificate authority). You can verify the host sensor certificate of the master blocking sensor by logging in to the host sensor and entering the **show tls fingerprint** command to see that the fingerprints of the host certificate match.

Step 11 To edit an existing entry in the master blocking sensor list, select it, and click **Edit**.

Step 12 (Optional) Edit the port.

Step 13 Edit the username, if needed.

Step 14 To change the password for this user, check the **Change the password** check box:

a. In the New Password field, enter the new password.

b. In the Confirm New Password field, enter the new password to confirm it.

Step 15 Check or uncheck the **TLS** check box, if needed.

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

Step 16 Click **OK**. The edited master blocking sensor appears in the list in the Master Blocking Sensor pane.

Step 17 To delete a master blocking sensor from the list, select it, and click **Delete**. The master blocking sensor no longer appears in the list in the Master Blocking Sensor pane.

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

Step 18 Click **Apply** to apply your changes and save the revised configuration.

Managing Time-Based Actions

The IME lets you manage time-based actions, such as configuring and viewing the list of denied attackers, configuring IP logging, setting up host and network blocks, and configuring and managing rate limiting. This section describes how to manage time-based actions, and contains the following topics:

Configuring and Monitoring Denied Attackers

This section describes how to monitor the denied attackers list, and contains the following topics:

Denied Attackers Pane

Note You must be administrator to monitor and clear the denied attackers list.

The Denied Attackers pane displays all IP addresses and the hit count for denied attackers. You can reset the hit count for all IP addresses or clear the list of denied attackers. You can also configure denied attackers to be monitored.

Note Resetting and clearing apply to all items in the table.

Denied Attackers Pane Field Definitions

The following fields are found in the Denied Attackers pane:

- Virtual Sensor—Indicates the virtual sensor that is denying the attacker.
- Attacker IP—Specifies the IP address of the attacker the sensor is denying.
- Victim IP—Specifies the IP address of the victim the sensor is denying.
- Port—Specifies the port of the host the sensor is denying.
- Protocol—Specifies the protocol that the attacker is using.
- Requested Percentage—Specifies the percentage of traffic that you configured to be denied by the sensor in inline mode.
- Actual Percentage—Specifies the percentage of traffic in inline mode that the sensor actually denies.

  Note The sensor tries to deny exactly the percentage you requested, but because of percentage fractions, the sensor is sometimes below the requested threshold.

- Hit Count—Displays the hit count for that denied attacker.

Monitoring the Denied Attackers List and Adding Denied Attackers

To view the list of denied attackers, their hit counts, to add and delete denied attackers, and to clear the list of denied attackers and reset the hit count, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Time-Based Actions > Denied Attackers**.

Step 3 To refresh the list, click **Refresh**.

Step 4 To clear the entire list of denied attackers, click **Clear List**.

Step 5 To have the hit count start over for all denied attackers, click **Reset All Hit Counts**.

Step 6 To add a denied attacker to the list to be monitored, click **Add**.

Step 7 In the Attacker IP field, enter the attacker IP address.

Note You can enter IPv4 and IPv6 IP addresses.

Step 8 Click the **Specify Victim Address or Port** check box, and enter the IP address and port number.

Step 9 Click the **Specify Virtual Sensor** check box and choose the virtual sensor from the drop-down list.

Tip To discard your changes and return to the Denied Attackers pane, click **Cancel**.

Step 10 Click **OK** to save your changes. The denied attacker appears in the Denied Attacker list.

Step 11 To delete a denied attacker from the list, select it, and then click **Delete**.

Configuring Host Blocks

This section describes how to configure host blocks, and contains the following topics:

Host Blocks Pane

Note You must be administrator or operator to configure active host blocks.

Use the Host Blocks pane to configure and manage blocking of hosts. A host block denies traffic from a specific host permanently (until you remove the block) or for a specified amount of time. You can base the block on a connection by specifying the destination IP address and the destination protocol and port. A host block is defined by its source IP address. If you add a block with the same source IP address as an existing block, the new block overwrites the old block.

If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the host block remains in effect until the sensor is rebooted or the block is deleted.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Host Block Pane Field Definitions

The following fields are found in the Host Blocks pane:

- Source IP—Specifies the source IP address for the block.
- Destination IP—Specifies the destination IP address for the block.
- Destination Port—Specifies the destination port for the block.
- Protocol—Specifies the type of protocol (TCP, UDP, or ANY). The default is ANY.
- Minutes Remaining—Specifies the time remaining for the blocks in minutes.
- Timeout (minutes)—Specifies the original timeout value for the block in minutes. A valid value is between 1 to 70560 minutes (49 days).
- VLAN—Specifies the VLAN that carried the data that fired the signature.

Note Even though the VLAN ID is included in the block request, it is not passed to the security appliance. Sensors cannot block on FWSM 2.1 or greater when logged in to the admin context.

- Connection Block Enabled—Specifies whether or not to block the connection for the host.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Add Host Block Dialog Box Field Definitions

The following fields are found in the Add Active Host Block dialog box:

- Source IP—Specifies the source IP address for the block.
- Enable connection blocking—Specifies whether or not to block the connection for the host.
- Connection Blocking—Lets you configure parameters for connection blocking:
  - Destination IP—Specifies the destination IP address for the block.
  - Destination Port (optional)—Specifies the destination port for the block.
  - Protocol (optional)—Specifies the type of protocol (TCP, UDP, or ANY). The default is ANY.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

- VLAN (optional)—Specifies the VLAN that carried the data that fired the signature.

Note Even though the VLAN ID is included in the block request, it is not passed to the security appliance. Sensors cannot block on FWSM 2.1 or later when logged in to the admin context.

- Enable Timeout—Lets you set a timeout value for the block in minutes.
- Timeout—Specifies the number of minutes for the block to last. A valid value is between 1 and 70560 minutes (49 days).
- No Timeout—Lets you choose to have no timeout for the block.

Adding, Deleting, and Managing Host Blocks

To add, delete, and manage host blocks, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Time-Based Actions > Host Blocks**, and then click **Add** to add a host block.

Step 3 In the Source IP field, enter the source IP address of the host you want blocked.

Step 4 To make the block connection-based, check the **Enable Connection Blocking** check box:

Note A connection block blocks traffic from a given source IP address to a given destination IP address and destination port.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

a. In the Destination IP field, enter the destination IP address.

b. (Optional) In the Destination Port field, enter the destination port.

c. (Optional) From the Protocol drop-down list, choose the protocol.

Step 5 (Optional) In the VLAN field, enter the VLAN for the connection block.

Step 6 Configure the timeout:

- To configure the block for a specified amount of time, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes.
- T o not configure the block for a specified amount of time, click the **No Timeout** radio button.

Tip To discard your changes and close the Add Host Block dialog box, click **Cancel**.

Step 7 Click **Apply**. The new host block appears in the list in the Host Blocks pane.

Step 8 Click **Refresh** to refresh the contents of the host blocks list.

Step 9 To delete a block, select a host block in the list, and click **Delete**. The Delete Host Block dialog box asks if you are sure you want to delete this block.

Tip To discard your changes and close the Delete Host Block dialog box, click **Cancel**.

Step 10 Click **Yes** to delete the block. The host block no longer appears in the list in the Host Blocks pane.

Configuring Network Blocks

This section describes how to configure network blocks, and contains the following topics:

Network Blocks Pane

Note You must be administrator or operator to configure network blocks.

Use the Network Blocks pane to configure and manage blocking of networks. A network block denies traffic from a specific network permanently (until you remove the block) or for a specified amount of time. A network block is defined by its source IP address and netmask. The netmask defines the blocked subnet. A host subnet mask is accepted also.

If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the block remains in effect until the sensor is rebooted or the block is deleted.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Network Blocks Pane Field Definitions

The following fields are found in the Network Blocks pane:

- IP Address—Specifies the IP address for the block.
- Mask—Specifies the network mask for the block.
- Minutes Remaining—Specifies the time remaining for the blocks in minutes.
- Timeout (minutes)—Specifies the original timeout value for the block in minutes. A valid value is between 1 and 70560 minutes (49 days).

Add Network Block Dialog Box Field Definitions

The following fields are found in the Add Network Block dialog box:

- Source IP—Specifies the IP address for the block.
- Netmask—Specifies the network mask for the block.
- Enable Timeout—Specifies the timeout value for the block in minutes.
- Timeout—Specifies the duration of the block in minutes. A valid value is between 1 and 70560 minutes (49 days).
- No Timeout—Lets you choose to have no timeout for the block.

Adding, Deleting, and Managing Network Blocks

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

To add, delete, and manage network blocks, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Time-Based Actions > Network Blocks**, and then click **Add** to add a network block.

Step 3 In the Source IP field, enter the source IP address of the network you want blocked.

Step 4 From the Netmask drop-down list, choose the netmask.

Step 5 Configure the timeout:

- To configure the block for a specified amount of time, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes.
- To not configure the block for a specified amount of time, click the **No Timeout** radio button.

Tip To undo your changes and close the Add Network Block dialog box, click **Cancel**.

Step 6 Click **Apply**. You receive an error message if a block has already been added. The new network block appears in the list in the Network Blocks pane.

Step 7 Click **Refresh** to refresh the contents of the network blocks list.

Step 8 Select a network block in the list and click **Delete** to delete that block. The Delete Network Block dialog box asks if you are sure you want to delete this block.

Step 9 Click **Yes** to delete the block. The network block no longer appears in the list in the Network Blocks pane.

Configuring Rate Limits

This section describes how to configure and manage rate limits, and contains the following topics:

Rate Limits Pane

Note You must be administrator to add rate limits.

Use the Rate Limits pane to configure and manage rate limiting. A rate limit restricts the amount of a specified type of traffic that is allowed on a network device interface to a percentage of maximum bandwidth capacity. Traffic that exceeds this percentage is dropped by the network device. A rate limit can restrict traffic to a specified target host, or to all traffic that crosses the configured interface/directions. You can use rate limits permanently or for a specified amount of time. A rate limit is identified by a protocol, an optional destination address, and an optional data value.

Because the rate limit is specified as a percent, it may translate to different actual limits on interfaces with different bandwidth capacities. A rate limit percent value must be an integer between 1 and 100 inclusive.

Rate Limits Pane Field Definitions

The following fields are found in the Rate Limits pane:

- Protocol—Specifies the protocol of the traffic that is rate limited.
- Rate—Specifies the percent of maximum bandwidth that is allowed for the rate-limited traffic. Matching traffic that exceeds this rate will be dropped.
- Source IP—Specifies the source host IP address of the rate-limited traffic.
- Source Port—Specifies the source host port of the rate-limited traffic.
- Destination IP—Specifies the destination host IP address of the rate-limited traffic.
- Destination Port—Specifies the destination host port of the rate-limited traffic.
- Data—Specifies the additional identifying information needed to more precisely qualify traffic for a given protocol. For example, echo-request narrows the ICMP protocol traffic to rate-limit pings.
- Minutes Remaining—Specifies the remaining minutes that this rate limit is in effect.
- Timeout (minutes)—Specifies the total number of minutes for this rate limit.

Add Rate Limit Dialog Box Field Definitions

The following fields are found in the Add Rate Limit dialog box:

- Protocol—Specifies the protocol of the traffic that is rate-limited (ICMP, TCP, or UDP).
- Rate (1-100)—Specifies the percentage of the maximum bandwidth allowed for the rate-limited traffic.
- Source IP (optional)—Specifies the source host IP address of the rate-limited traffic.
- Source Port (optional)—Specifies the source host port of the rate-limited traffic.
- Destination IP (optional)—Specifies the destination host IP address of the rate-limited traffic.
- Destination Port (optional)—Specifies the destination host port of the rate-limited traffic.
- Use Additional Data—Lets you choose whether to specify more data, such as echo-reply, echo-request, or halfOpenSyn.
- Timeout—Lets you choose whether to enable timeout:
  - No Timeout—Specifies that timeout not enabled.
  - Enable Timeout—Lets you specify the timeout in minutes (1 to 70560).

Adding, Deleting, and Managing Rate Limiting

To add, delete, and manage rate limiting, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Time-Based Actions > Rate Limits**, and then click **Add** to add a rate limit.

Step 3 From the Protocol drop-down list, choose the protocol (ICMP, TCP, or UDP) of the traffic you want rate limited.

Step 4 In the Rate field, enter the rate limit (1 to 100) percent.

Step 5 (Optional) In the Source IP field, enter the source IP address.

Step 6 (Optional) In the Source Port field, enter the source port.

Step 7 (Optional) In the Destination IP field, enter the destination IP address.

Step 8 (Optional) In the Destination Port field, enter the destination port.

Step 9 (Optional) To configure the rate limit to use additional data, check the **Use Additional Data** check box.

Step 10 From the Select Data drop-down list, choose the additional data (echo-reply, echo-request, or halfOpenSyn).

Step 11 Configure the timeout:

- If you do not want to configure the rate limit for a specified amount of time, click the **No Timeout** radio button.
- If you want to configure a timeout in minutes, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes (1 to 70560).

Tip To discard your changes and close the Add Rate Limit dialog box, click **Cancel**.

Step 12 Click **Apply**. The new rate limit appears in the list in the Rate Limits pane.

Step 13 Click **Refresh** to refresh the contents of the Rate Limits list.

Step 14 To delete a rate limit, select a rate limit from the list, and click **Delete**. The Delete Rate Limit dialog box asks if you are sure you want to delete this rate limit.

Tip To close the Delete Rate Limit dialog box, click **No**.

Step 15 Click **Yes** to delete the rate limit. The rate limit no longer appears in the rate limits list.

For More Information

For the procedure for assigning actions to signatures, see Assigning Actions to Signatures, page 10-23.

Configuring IP Logging

This section describes how to configure IP logging, and contains the following topics:

Understanding IP Logging

Caution Turning on IP logging slows system performance.

The simplest IP logging consists of an IP address. You can configure the sensor to capture all IP traffic associated with a host you specify by IP address. The sensor begins collecting as soon as it sees the first IP packet with this IP address and continues collecting depending on the parameters that you have set. You can specify in minutes how long you want the IP traffic to be logged at the IP address, and/or how many packets you want logged, and/or how many bytes you want logged. The sensor stops logging IP traffic at the first parameter you specify.

Log files are in one of three states:

- Added—When IP logging is added
- Started—When the sensor sees the first packet, the log file is opened and placed into the Started state.
- Completed—When the IP logging limit is reached.

The number of files in all three states is limited to 20. The IP logs are stored in a circular buffer that is never filled because new IP logs overwrite the old ones. Once the limit of 20 is reached, you receive the following message in main.log: `Cid/W errWarnIpLogProcessor::addIpLog: Ran out of file descriptors.`

Note Logs remain on the sensor until the sensor reclaims them. You cannot manage IP log files on the sensor.

You can copy IP log files to an FTP or SCP server so that you can view them with a sniffing tool such as WireShark or TCPDUMP. The files are stored in PCAP binary form with the pcap file extension.

IP Logging Pane

Note You must be administrator to configure IP logging.

The IP Logging pane displays all IP logs that are available for downloading on the system. IP logs are generated in two ways:

- When you add IP logs in the Add IP Logging dialog box
- When you select one of the following as the event action for a signature:
  - Log Attacker Packets
  - Log Pair Packets
  - Log Victim Packets

When the sensor detects an attack based on this signature, it creates an IP log. The event alert that triggered the IP log appears in the IP logging table.

Caution You must have packet logging enabled on the Packet Logging pane (**Configuration** > ***sensor_name*** > **Sensor Management > Packet Logging**) to configure IP logging.

IP Logging Pane Field Definitions

The following fields are found in the IP Logging pane:

- Log ID—Specifies the ID of the IP log.
- Virtual Sensor—Specifies the virtual sensor with which the IP log is associated.
- IP Address—Specifies the IP address of the host for which the log is being captured.
- Status—Specifies the status of the IP log. Valid values are added, started, or completed.
- Start Time—Specifies the timestamp of the first captured packet.
- Current End Time—Specifies the timestamp of the last captured packet. There is no timestamp if the capture is not complete.
- Alert ID—Specifies the ID of the event alert, if any, that triggered the IP log.
- Packets Captured—Specifies the current count of the packets captured.
- Bytes Captured—Specifies the current count of the bytes captured.

Add and Edit IP Logging Dialog Boxes Field Definitions

The following fields are found on the Add and Edit IP Logging dialog boxes:

- Virtual Sensor—Specifies the virtual sensor from which you want to capture IP logs.
- IP Address—Specifies the IP address of the host for which the log is being captured.

Note You can enter IPv4 and IPv6 IP addresses.

Note If IP logging is already enabled for a particular IP address and virtual sensor, that IP log is overwritten with the new IP log.

- Maximum Values—Lets you set the values for IP logging:
  - Duration—Specifies the maximum duration to capture packets. The range is 1 to 60 minutes. The default is 10 minutes.
  - Packets (optional)—Specifies the maximum number of packets to capture. The range is 0 to 4294967295 packets.
  - Bytes (optional)—Specifies the maximum number of bytes to capture. The range is 0 to 4294967295 bytes.

Configuring IP Logging

To log IP traffic for a particular host, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Time-Based Actions > IP Logging**, and then click **Add**.

Step 3 From the Virtual Sensor drop-down list, choose for which virtual sensor you want to turn on IP logging.

Step 4 In the IP Address field, enter the IP address of the host from which you want IP logs to be captured. You receive an error message if a capture is being added that exists and is in the Added or Started state.

Note You can enter IPv4 and IPv6 IP addresses.

Note If IP logging is already enabled for a particular IP address and virtual sensor, that IP log is overwritten with the new IP log.

Step 5 In the Duration field, enter how many minutes you want IP logs to be captured. The range is 1 to 60 minutes. The default is 10 minutes.

Step 6 (Optional) In the Packets field, enter how many packets you want to be captured. The range is 0 to 4294967295 packets.

Step 7 (Optional) in the Bytes field, enter how many bytes you want to be captured. The range is 0 to 4294967295 packets.

Tip To discard your changes, and close the Add IP Log dialog box, click **Cancel**.

Step 8 Click **Apply** to apply your changes and save the revised configuration. The IP log with a log ID appears in the list in the IP Logging pane.

Step 9 To stop IP logging, select the log ID for the log you want to stop, and click **Stop**.

Step 10 Click **OK** to stop IP logging for that log.

Step 11 To download an IP log, select the log ID, and click **Download**.

Step 12 Save the log to your local machine. You can view it with WireShark.

Configuring SNMP

This chapter describes how to configure the sensor to use SNMP and SNMP traps. It contains the following sections:

Understanding SNMP

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is a simple request/response protocol. The network-management system issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations: Get, GetNext, Set, and Trap.

You can configure the sensor for monitoring by SNMP. SNMP defines a standard way for network management stations to monitor the health and status of many types of devices, including switches, routers, and sensors.

You can configure the sensor to send SNMP traps. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. Trap-directed notification has the following advantage—if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event.

After receiving the event, the manager displays it and can take an action based on the event. For instance, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Note Trap-directed notification results in substantial savings of network and agent resources by eliminating frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent cannot send a trap if the device has had a catastrophic outage.

You can use SNMPv2 and SNMPv3 protocol concurrently. If the SNMP request contains version 3 user information, then you get a version 3 reply (provided the same user is configured as a version 3 user in the IPS). If the SNMP request is a version 2 request, the IPS returns the response (provided the correct version 2 community string is configured). Support for SNMPv3 is valid for IPS 7.2(2)E4 and later.

Note Encryption of the SNMPv3 payload uses AES-128 and authentication of the user password uses HMAC-SHA-96.

For More Information

For the procedure for having the sensor send SNMP traps, see Assigning Actions to Signatures, page 10-23.

Configuring SNMP General Configuration

Note You must be administrator to configure the sensor to use SNMP.

Use the General Configuration pane to configure the sensor to use SNMP.

Field Definitions

The following fields are found in the SNMP General Configuration pane:

- Enable SNMP Gets/Sets—If checked, allows SNMP gets and sets.
- SNMP Agent Parameters—Configures the parameters for SNMP agent:
  - Read-Only Community String—Specifies the community string for read-only access.
  - Read-Write Community String—Specifies the community string for read and write access.
  - Sensor Contact—Specifies the contact person, contact point, or both for the sensor.
  - Sensor Location—Specifies the location of the sensor.
  - Sensor Agent Port—Specifies the IP port of the sensor. The default is 161.
  - Sensor Agent Protocol—Specifies the IP protocol of the sensor. The default is UDP.

Configuring General Parameters

Caution To have the sensor send SNMP traps, you must also select **Request SNMP Trap** as the event action when you configure signatures.

To set the general SNMP parameters, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SNMP > General Configuration**.

Step 3 To enable SNMP so that the SNMP management workstation can issue requests to the sensor SNMP agent, check the **Enable SNMP Gets/Sets** check box.

Step 4 Configure the SNMP agent parameters. These are the values that the SNMP management workstation can request from the sensor SNMP agent.

a. In the Read-Only Community String field, enter the read-only community string. The read-only community string helps to identify the sensor SNMP agent.

b. In the Read-Write Community String field, enter the read-write community string. The read-write community string helps to identify the sensor SNMP agent.

Note The management workstation sends SNMP requests to the sensor SNMP agent, which resides on the sensor. If the management workstation issues a request and the community string does not match what is on the senor, the sensor will reject it.

c. In the Sensor Contact field, enter the sensor contact user ID.

d. In the Sensor Location field, enter the location of the sensor.

e. In the Sensor Agent Port field, enter the port of the sensor SNMP agent. The default SNMP port number is 161.

f. From the Sensor Agent Protocol drop-down list, choose the protocol the sensor SNMP agent will use. The default protocol is UDP.

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

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Configuring SNMPv3 Users

This section describes how to configure SNMPv3 users, and contains the following topics:

SNMPv3 Users Pane

Note You must be administrator or operator to configure SNMPv3 users on the sensor.

Note Support for SNMPv3 is valid for IPS 7.2(2)E4 and later.

The SNMPv3 Users pane displays the username, access control, security level, authentication protocol, and privacy protocol of all SNMPv3 users configured on the system. In the SNMPv3 Users pane, you can add, edit, and delete SNMPv3 users. You can configure a maximum of 25 SNMPv3 users on the system.

Note You can also associate SNMPv3 users with SNMP trap destinations. If no SNMPv3 user is associated with a trap, then an SNMPv2 trap is sent.

SNMPv3 protocol introduces new security features, such as authentication and encryption that were missing from the previous versions. The security model supported by the sensor is USM (User-based Security Model). The U stands for User-based, because it contains a list of users and their attributes.

Note Encryption of the SNMPv3 payload uses AES-128 and authentication of the user password uses HMAC-SHA-96.

Note We recommend that you configure SNMPv3 users with security levels that require authentication, such as authPriv and authNoPriv, with authPriv being the most highly recommended. Configuring SNMPv3 users with the noAuthNoPriv security level is NOT recommended.

SNMPv3 Users Pane Field Definitions

The following fields are found in the SNMPv3 Users pane:

- Username—Displays the username on the host that belongs to the SNMP agent.
- Access Control—Displays the access control (rouser or rwuser) of the SNMPv3 user.
- Security Level—Displays one of the following security models for the SNMPv3 user:
  - noAuthNoPriv—No Authentication and No Privacy, which means that no security is applied to messages.
  - authNoPriv—Authentication but No Privacy, which means that messages are authenticated.
  - authPriv—Authentication and Privacy, which means that messages are authenticated and encrypted.
- Authentication Protocol—Displays the authentication protocol (SHA or none) for the SNMPv3 user.
- Privacy Protocol—Displays the privacy or encryption algorithm used (AES or none) for the SNMPv3 user.

Add and Edit SNMPv3 User Dialog Boxes Field Definitions

The following fields are found in the Add and Edit SNMPv3 User dialog boxes:

- Username—Specifies a username for this SNMPv3 user. The maximum number of characters is 32.
- Access Control—Specifies the access control for this SNMPv3 user:
  - rouser—Read-only user.
  - rwuser—Read-write user.

Note Both rouser and rwuser can do 'get' operations, but rwuser access control is mandatory to do 'set' operations.

- Security Level—Specifies the security level for this SNMPv3 user:
  - noAuthNoPriv—No Authentication and No Privacy, which means that no security is applied to messages.
  - authNoPriv—Authentication but No Privacy, which means that messages are authenticated.
  - authPriv—Authentication and Privacy, which means that messages are authenticated and encrypted.

Note We recommend that you configure SNMPv3 users with security levels that require authentication, such as authPriv and authNoPriv, with authPriv being the most highly recommended. Configuring SNMPv3 users with the noAuthNoPriv security level is NOT recommended.

- Authentication Protocol—Specifies the authentication protocol (SHA or none) for this SNMPv3 user.
- Authentication Passphrase—Lets you assign an authentication passphrase for this SNMPv3 user. The valid range is 8 to 257 characters; no spaces or double quotes allowed.
- Confirm Authentication Passphrase—Lets you confirm the passphrase.
- Privacy Protocol—Specifies the privacy protocol (AES or none) for this SNMPv3 user.
- Privacy Passphrase—Lets you assign a privacy passphrase for this SNMPv3 user. The valid range is 8 to 257 characters; no spaces or double quotes allowed.
- Confirm Privacy Passphrase—Lets you confirm the passphrase

Caution The same passphrase value for both authentication and privacy is allowed, although it is not a recommended security practice.

Configuring SNMPv3 Users

To configure SNMPv3 users, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SNMP > SNMPv3 Users**, and then click **Add**.

Step 3 In the Add SNMPv3 User dialog box, set the following user parameters:

a. In the Username field, enter the username of the SNMPv3 user. The maximum number of characters is 32.

b. In the Access Control field, select rouser or rwuser, from the drop-down list.

c. In the Security Level field, select one of the following security levels from the drop-down list:
   - noAuthNoPriv—No Authentication and No Privacy, which means that no security is applied to messages.
   - authNoPriv—Authentication but No Privacy, which means that messages are authenticated.
   - authPriv—Authentication and Privacy, which means that messages are authenticated and encrypted.

   Note We recommend that you configure SNMPv3 users with security levels that require authentication, such as authPriv and authNoPriv, with authPriv being the most highly recommended. Configuring SNMPv3 users with the noAuthNoPriv security level is NOT recommended.

d. In the Authentication Protocol field, select SHA or None from the drop-down list.

e. In the Authentication Passphrase field, enter a passphrase and then confirm it in the Confirm Authentication Passphrase field.

f. In the Privacy Protocol field, select AES or None from the drop-down list.

g. In the Privacy Passphrase field, enter a passphrase and then confirm it in the Confirm Privacy Passphrase field.

Tip To discard your changes and close the Add SNMPv3 User dialog box, click **Cancel**.

Step 4 Click **OK**. The new SNMPv3 user appears in the list in the SNMPv3 Users pane.

Step 5 To edit an SNMPv3 user, select it, and click **Edit**.

Step 6 Edit the any of the fields, if needed.

Tip To discard your changes and close the Edit SNMPv3 User dialog box, click **Cancel**.

Step 7 Click **OK**. The edited SNMPv3 User appears in the list in the SNMPv3 Users pane.

Step 8 To delete an SNMPv3 user, select it, and click **Delete**. The SNMPv3 user no longer appears in the list in the SNMPv3 Users pane.

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

Step 9 Click **Apply** to apply your changes and save the revised configuration.

Configuring SNMP Traps

This section describes how to configure SNMP traps, and contains the following topics:

- Add and Edit SNMP Trap Destination Dialog Boxes Field Definitions, page 18-8
- Configuring SNMP Traps, page 18-8

Traps Configuration Pane

Note You must be administrator to configure SNMP traps on the sensor.

Use the Traps Configuration pane to set up SNMP traps and trap destinations on the sensor. An SNMP trap is a notification. You configure the sensor to send traps based on whether the event is fatal, an error, or a warning.

Note You can also associate SNMPv3 users with SNMP trap destinations. If no SNMPv3 user is associated with a trap, then an SNMPv2 trap is sent. For example, if a version 3 user is associated with a trap destination, all traps for that destination will be version 3 traps using the configured user. No version 2 trap is sent to that trap destination. If a version 3 user is not configured, then a version 2 trap is sent. Traps can be sent to one destination using version 3 and to another destination using version 2. Support for SNMPv3 is valid for IPS 7.2(2)E4 and later.

Traps Configuration Pane Field Definitions

The following fields are found in the Traps Configuration pane:

- Enable SNMP Traps—If checked, indicates the remote server will use a pull update.
- SNMP Traps—Let you choose the error events to notify through SNMP:
  - Fatal—Generates traps for all fatal error events.
  - Error—Generates traps for all error error events.
  - Warning—Generates traps for all warning error events.
- Enable detailed traps for alerts—If checked, includes the full text of the alert in the trap. Otherwise, sparse mode is used. Sparse mode includes less than 484 bytes of text for the alert.
- Send traps when health metrics change—If checked, sends SNMP traps containing information about the overall health of the sensor.

  Note To receive sensor health information through SNMP traps, you must have the sensor health metrics enabled. Choose **Configuration > *sensor_name* > Sensor Management > Sensor Health** to enable sensor health metrics.

- Default Trap Community String—Specifies the community string used for the traps if no specific string has been set for the trap.
- SNMP Trap Destinations—Specifies the destination for the trap. You must specify the following information about the destination:
  - IP Address—Specifies the IP address of the trap destination.
  - UDP Port—Specifies the UDP port of the trap destination.
  - Trap Community String—Specifies the trap community string.

– SNMPv3 User—Specifies the SNMPv3 user of the trap destination.

  If no SNMPv3 user is specified, SNMPv2 is used.

Add and Edit SNMP Trap Destination Dialog Boxes Field Definitions

The following fields are found in the Add and Edit SNMP Trap Destination dialog boxes:

- IP Address—Specifies the IP address of the trap destination.
- UDP Port—Specifies the UDP port of the trap destination. The default is port 162.
- Trap Community String—Specifies the trap community string.
- SNMPv3 User—Specifies the SNMPv3 user of the trap destination.

  If no SNMPv3 user is specified, SNMPv2 is used.

Configuring SNMP Traps

Caution To have the sensor send SNMP traps, you must also select **Request SNMP Trap** as the event action when you configure signatures.

Caution To have the sensor send SNMP traps, you must also select **Request SNMP Trap** as the event action when you configure signatures.

To configure SNMP traps, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SNMP > Traps Configuration**.

Step 3 To enable SNMP traps, check the **Enable SNMP Traps** check box.

Step 4 Set the parameters for the SNMP trap:

a. Check the error events you want to be notified about through SNMP traps. You can choose to have the sensor send an SNMP trap based on one or all of the following events: fatal, error, warning.

b. To receive detailed SNMP traps, check the **Enable detailed traps for alerts** check box.

c. To receive SNMP traps containing sensor health metrics, check the **Send traps when health metrics change** check box.

Note To receive sensor health information through SNMP traps, you must have the sensor health metrics enabled. Choose **Configuration > *sensor_name* > Sensor Management > Sensor Health** to enable sensor health metrics.

d. In the Default Trap Community String field, enter the community string to be included in the detailed traps.

Step 5 Set the parameters for the SNMP trap destinations so the sensor knows which management workstations to send them to:

a. Click **Add**.

b. In the IP Address field, enter the IP address of the SNMP management station.

c. In the UDP Port field, enter the UDP port of the SNMP management station.

d. In the Trap Community String field, enter the trap Community string.

Note The community string appears in the trap and is useful if you are receiving multiple types of traps from multiple agents. For example, a router or sensor could be sending the traps, and if you put something that identifies the router or sensor specifically in your community string, you can filter the traps based on the community string.

e. From the SNMPv3 User drop-down list, select the trap-v3user associated with this trap.

If no SNMPv3 user is specified, SNMPv2 is used.

Tip To discard your changes and close the Add SNMP Trap Destination dialog box, click **Cancel**.

Step 6 Click **OK**. The new SNMP trap destination appears in the list in the Traps Configuration pane.

Step 7 To edit an SNMP trap destination, select it, and click **Edit**.

Step 8 Edit the **U**DP Port and Trap Community String fields, and change the SNMPv3 user, if needed.

Tip To discard your changes and close the Edit SNMP Trap Destination dialog box, click **Cancel**.

Step 9 Click **OK**. The edited SNMP trap destination appears in the list in the Traps Configuration pane.

Step 10 To delete an SNMP trap destination, select it, and click **Delete**. The SNMP trap destination no longer appears in the list in the Traps Configuration pane.

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

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Supported MIBs

Note To receive sensor health information through SNMP traps, you must have the sensor health metrics enabled. Choose **Configuration > *sensor_name* > Sensor Management > Sensor Health** to enable sensor health metrics.

The following private MIBs are supported on the sensor:

- CISCO-CIDS-MIB

  The CISCO-CIDS-MIB has been updated to include SNMP health data.
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

You can obtain these private Cisco MIBs under the heading SNMP v2 MIBs at this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Note MIB II is available on the sensor, but we do not support it. We know that some elements are not correct (for example, the packet counts from the IF MIB on the sensing interfaces). While you can use elements from MIB II, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

Note CISCO-PROCESS-MIB is available on the sensor, but we do not support it. We know that some elements are not available. While you can use elements from CISCO-PROCESS-MIB, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

Configuring External Product Interfaces

This chapter explains how to configure external product interfaces. It contains the following sections:

Understanding External Product Interfaces

Note In Cisco IPS, you can only add interfaces to the CSA MC.

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. For example, the types of information that can be received from external products include host profiles (the host OS configuration, application configuration, and security posture) and IP addresses that have been identified as causing malicious network activity.

Understanding CSA MC

The CSA MC enforces a security policy on network hosts. It has two components:

- Agents that reside on and protect network hosts.
- Management Console (MC)—An application that manages agents. It downloads security policy updates to agents and uploads operational information from agents.

The CSA MC receives host posture information from the CSA agents it manages. It also maintains a watch list of IP addresses that it has determined should be quarantined from the network. The CSA MC sends two types of events to the sensor—host posture events and quarantined IP address events.

Host posture events (called imported OS identifications in IPS) contain the following information:

- Unique host ID assigned by the CSA MC
- CSA agent status
- Host system hostname
- Set of IP addresses enabled on the host
- CSA software version
- CSA polling status
- CSA test mode status
- NAC posture

For example, when an OS-specific signature fires whose target is running that OS, the attack is highly relevant and the response should be greater. If the target OS is different, then the attack is less relevant and the response may be less critical. The signature attack relevance rating is adjusted for this host.

The quarantined host events (called the watch list in IPS) contain the following information:

- IP address
- Reason for the quarantine
- Protocol associated with a rule violation (TCP, UDP, or ICMP)
- Indicator of whether a rule-based violation was associated with an established session or a UDP packet.

For example, if a signature fires that lists one of these hosts as the attacker, it is presumed to be that much more serious. The risk rating is increased for this host. The magnitude of the increase depends on what caused the host to be quarantined.

The sensor uses the information from these events to determine the risk rating increase based on the information in the event and the risk rating configuration settings for host postures and quarantined IP addresses.

Note The host posture and watch list IP address information is not associated with a virtual sensor, but is treated as global information.

Secure communications between the CSA MC and the IPS sensor are maintained through SSL/TLS. The sensor initiates SSL/TLS communications with the CSA MC. This communication is mutually authenticated. The CSA MC authenticates by providing X.509 certificates. The sensor uses username/password authentication.

Note You can only enable two CSA MC interfaces.

Caution You must add the CSA MC as a trusted host so the sensor can communicate with it. To add the CSA MC as a trusted host, choose **Configuration > *sensor_name* > Sensor Management > Certificates > Trusted Hosts > Add**.

For More Information

For the procedure to add a trusted host, see Adding Trusted Hosts, page 15-13.

External Product Interface Issues

When the external product interface receives host posture and quarantine events, the following issues can arise:

- The sensor can store only a certain number of host records:
  - If the number of records exceeds 10,000, subsequent records are dropped.
  - If the 10,000 limit is reached and then it drops to below 9900, new records are no longer dropped.
- Hosts can change an IP address or appear to use another host IP address, for example, because of DHCP lease expiration or movement in a wireless network. In the case of an IP address conflict, the sensor presumes the most recent host posture event to be the most accurate.
- A network can include overlapping IP address ranges in different VLANs, but host postures do not include VLAN ID information. You can configure the sensor to ignore specified address ranges.
- A host can be unreachable from the CSA MC because it is behind a firewall. You can exclude unreachable hosts.
- The CSA MC event server allows up to ten open subscriptions by default. You can change this value. You must have an administrative account and password to open subscriptions.
- CSA data is not virtualized; it is treated globally by the sensor.
- Host posture OS and IP addresses are integrated into passive OS fingerprinting storage. You can view them as imported OS profiles.
- You cannot see the quarantined hosts.
- The sensor must recognize each CSA MC host X.509 certificate. You must add them as a trusted host.
- You can configure a maximum of two external product devices.

For More Information

- For more information on working with OS maps and identifications, see Adding, Editing, Deleting, and Moving Configured OS Maps, page 12-27 and Configuring OS Identifications, page 21-17.
- For the procedure for adding trusted hosts, see Adding Trusted Hosts, page 15-13.

Configuring the CSA MC to Support IPS Interfaces

Note For more detailed information about host posture events and quarantined IP address events, refer to *Using Management Center for Cisco Security Agents 5.1*.

You must configure the CSA MC to send host posture events and quarantined IP address events to the sensor. To configure the CSA MC to support IPS interfaces, follow these steps:

Step 1 Choose **Events > Status Summary**.

Step 2 In the Network Status section, click **No** beside **Host history collection enabled**, and then click **Enable** in the popup window.

Note Host history collection is enabled globally for the system. This feature is disabled by default because the MC log file tends to fill quickly when it is turned on.

Step 3 Choose **Systems > Groups** to create a new group (with no hosts) to use in conjunction with administrator account you will next create.

Step 4 Choose **Maintenance > Administrators > Account Management** to create a new CSA MC administrator account to provide IPS access to the MC system.

Step 5 Create a new administrator account with the role of **Monitor**. This maintains the security of the MC by not allowing this new account to have configure privileges.

Note Remember the username and password for this administrator account because you need them to configure external product interfaces on the sensor.

Step 6 Choose **Maintenance > Administrators > Access Control** to further limit this administrator account.

Step 7 In the Access Control window, select the administrator you created and select the group you created.

Note When you save this configuration, you further limit the MC access of this new administrator account with the purpose of maintaining security on the CSA MC.

Configuring External Product Interfaces

This section describes the External Product Interfaces pane, and contains the following topics:

External Product Interfaces Pane

Note You must be administrator to add, edit, and delete external product interfaces and posture ACLs.

Use the External Product Interfaces pane to add the interfaces of the CSA MC so that the sensor can receive and process information from the CSA MC.

Caution You must add the external product as a trusted host so the sensor can communicate with it. To add a trusted host, choose **Configuration > *sensor_name* > Sensor Management > Certificates > Trusted Hosts > Add**.

External Product Interfaces Pane Field Definitions

The following fields are found in the External Product Interfaces pane:

- IP Address—Specifies the IP address of the external product.
- Enabled—Indicates whether the external product interface is enabled.
- Port—Specifies the port being used for communications.
- TLS Used—Indicates whether secure communications are being used.
- Username—Specifies the user login name that connects to the CSA MC.
- Host Posture Settings—Indicates how host postures received from the CSA MC should be handled:
  - Enabled—Indicates that receipt of the host postures is enabled. If disabled, the host posture information received from a CSA MC is deleted.
  - Allow Unreachable—Allows/denies the receipt of host posture information for hosts that are not reachable by the CSA MC.

    A host is not reachable if the CSA MC cannot establish a connection with the host on any IP addresses in the host 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 CSA MC are also not reachable by the IPS, for example if the IPS and the CSA MC are on the same network segment.
  - Posture ACLs—Specifies network address ranges for which host postures are allowed or denied. This option provides a mechanism for filtering postures that have IP addresses that may not be visible to the IPS or may be duplicated across the network.
- Watch List Settings—Indicates how watch list settings received from the CSA MC should be handled:
  - Enabled—Indicates that receipt of the watch list is enabled. If disabled, the watch list information received from a CSA MC is deleted.
  - Manual RR Increase—Indicates by what percentage the manual watch list risk rating should be increased.
  - Session RR Increase—Indicates by what percentage the session-based watch list risk rating should be increased.
  - Packet RR Increase—Indicates by what percentage the packet-based watch list risk rating should be increased.
- SDEE URL—Indicates the URL on the CSA MC the IPS uses to retrieve information using SDEE communication. You must configure the URL based on the software version of the CSA MC that the IPS is communicating with as follows:
  - For the CSA MC version 5.0, use /csamc50/sdee-server.
  - For the CSA MC version 5.1, use /csamc51/sdee-server.
  - For the CSA MC version 5.2 and later, use /csamc/sdee-server (the default value).

Add and Edit External Product Interface Dialog Boxes Field Definitions

The following fields are found in the Add and Edit External Product Interface dialog boxes:

- External Product's IP Address—Specifies the IP address of the external product.
- Enable receipt of information—Enables the sensor to receive information from the external product interface.

Note If not checked, all host posture and quarantine information from this device is purged from the sensor.

- Communication Settings—Lets you see the SDEE URL and TLS, and lets you change the port:
  - SDEE URL—Specifies the URL on the CSA MC the IPS uses to retrieve information using SDEE communication. You must configure the URL based on the software version of the CSA MC that the IPS is communicating with. For the CSA MC version 5.0, use /csamc50/sdee-server. For the CSA MC version 5.1, use /csamc51/sdee-server. For the CSA MC version 5.2 and later, use /csamc/sdee-server (the default value).
  - Port—Specifies the port being used for communications.
  - Use TLS—Indicates that secure communications are being used. You cannot change this value.
- Login Settings—Lets you specify the credentials required to log in to the CSA MC:
  - Username—Lets you enter the username used to log in to the CSA MC.
  - Password—Lets you assign a password to the user.
  - Confirm Password—Lets you confirm the password.
- Watch List Settings—Lets you configure how watch list settings received from the CSA MC should be handled:
  - Enable receipt of watch list—Enables/disables the receipt of the watch list information. The watch list information received from a CSA MC is deleted when disabled.
  - Manual Watch List RR Increase—Lets you increase the percentage of the manual watch list risk rating.
  - Session-based Watch List RR Increase—Lets you increase the percentage of the session-based watch list risk rating.
  - Packet-based Watch List RR Increase—Lets you increase the percentage of the packet-based watch list risk rating.
- Host Posture Settings—Specifies how host postures received from the CSA MC should be handled:
  - Enable receipt of host postures—Enables/disables the receipt of the host posture information. The host posture information received from a CSA MC is deleted when disabled.
  - Allow unreachable hosts' postures—Allows/denies the receipt of host posture information for hosts that are not reachable by the CSA MC. A host is not reachable if the CSA MC cannot establish a connection with the host on any 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 CSA MC are also not reachable by the IPS, for example if the IPS and the CSA MC are on the same network segment.

- Permitted and Denied Host Posture Addresses—Lets you add host posture ACLs that will be permitted or denied:
  - Name—Specifies the name of the posture ACL.
  - Active—Indicates whether this posture ACL is active.
  - IP Address—Specifies the IP address of the posture ACL.
  - Network Mask—Specifies the network mask of the posture ACL.
  - Action—Specifies the action (deny or permit) the posture ACL will take.

Add and Edit Posture ACL Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Posture ACL dialog boxes:

- Name—Specifies the name of the posture ACL.
- Active—Specifies whether this posture ACL is active.
- IP Address—Specifies the IP address of the posture ACL.
- Network Mask—Specifies the network mask of the posture ACL.
- Action—Specifies the action (deny or permit) the posture ACL will take.

Adding, Editing, and Deleting External Product Interfaces and Posture ACLs

Caution In Cisco IPS the only external product interfaces you can add are CSA MC interfaces. Cisco IPS supports two CSA MC interfaces.

Note Make sure you add the external product as a trusted host so the sensor can communicate with it. To add a trusted host, choose **Configuration > *sensor_name* > Sensor Management > Certificates > Trusted Hosts > Add**.

To add an external product interface, follow these steps:

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

Step 2 Choose **Configuration >*sensor_name* > Sensor Management > External Product Interfaces**, and click **Add** to add an external product interface.

Step 3 In the External Product's IP Address field, enter the IP address of the external product.

Step 4 Check the **Enable receipt of information** check box to allow information to be passed from the external product to the sensor.

Step 5 In the Port field, change the default port 443 if needed.

Note Under Communication Settings, you can only change the Port value.

Step 6 Configure the login settings:

a. In the Username field, enter the username of the user who can log in to the external product.

b. In the Password field, enter the password the user will use.

c. In the Confirm Password field, enter the password again.

Note Steps 7 through 15 are optional. If you do not perform Steps 7 though 15, the default values are used receive all of the CSA MC information with no filters applied.

Step 7 (Optional) Configure the watch list settings:

a. Check the **Enable receipt of watch list** check box to allow the watch list information to be passed from the external product to the sensor.

Note If you do not check the **Enable receipt of watch list** check box, the watch list information received from a CSA MC is deleted.

b. In the Manual Watch List RR 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 8 (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.

Note If you do not check the **Enable receipt of host postures** check box, the host posture information received from a CSA MC is deleted.

Step 9 (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.

Note A host is not reachable if the CSA MC cannot establish a connection with the host on any of the IP addresses in the host 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 CSA MC are also not reachable by the IPS, for example if the IPS and the CSA MC are on the same network segment.

Step 10 (Optional) To add a posture ACL, click **Add**.

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) In the Name field, enter a name for the posture ACL.

Step 12 (Optional) In the Active field, click the **Yes** radio button to make the posture ACL active.

Step 13 (Optional) In the IP Address field, enter the IP address the posture ACL will use.

Step 14 (Optional) In the Network Mask field, enter the network mask the posture ACL will use.

Step 15 (Optional) In the Action drop-down list, choose the action (Deny or Permit) the posture ACL will take.

Tip To undo your changes and close the Add Posture ACL dialog box, click **Cancel**.

Step 16 (Optional) Click **OK**. The new posture ACL appears in the Host Posture Setting 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.

Step 17 To edit an existing posture ACL, select it, and click **Edit**.

Step 18 Edit the IP Address, Network Mask, and Action fields or change the active state to inactive by clicking the **No** radio button.

Tip To discard your changes and close the Edit Posture ACL dialog box, click **Cancel**.

Step 19 Click **OK**. The edited posture ACL appears in the Host Posture Setting list in the Add External Product Interface dialog box.

Step 20 To delete a posture ACL from the list, select it, and click **Delete**. The posture ACL no longer appears in the Host Posture Setting list in the Add External Product Interface dialog box.

Step 21 Click **OK**. The external product interface now appears in the Management Center for Cisco Security Agents list in the External Product Interfaces pane.

Tip To discard your changes and close the Add External Product Interface dialog box, click **Cancel**.

Step 22 To edit the external product interface, select it, and click **Edit**.

Step 23 Make any changes needed to the fields in the dialog box.

Tip To discard your changes and close the Edit External Product Interface dialog box, click **Cancel**.

Step 24 Click **OK**. The edited external product interface appears in the Management Center for Cisco Security Agents list in the External Product Interfaces pane.

Step 25 To delete an external product interface, select it, and click **Delete**. The external product interface no longer appears in the Management Center for Cisco Security Agents list in the External Product Interfaces pane.

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

Step 26 Click **Apply** to apply your changes and save the revised configuration.

Troubleshooting External Product Interfaces

To troubleshoot external product interfaces, check the following:

- Make sure the interface is active by checking the output from the **show statistics external-product-interface** command in the CLI, or choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Statistics** in the IME and check the Interface state line in the response.
- Make sure you have added the CSA MC IP address to the trusted hosts. If you forgot to add it, add it, wait a few minutes and then check again.
- Confirm subscription login information by opening and closing a subscription on the CSA MC using the browser.
- Check the Event Store for the CSA MC subscription errors.

For More Information

- For the procedure for adding trusted hosts, see Adding Trusted Hosts, page 15-13.
- For the procedure for displaying events, see Monitoring Events, page 21-1.

Managing the Sensor

This chapter describes how to manage your sensor, for example, how to set passwords, obtain and install license keys, set up IP logging variables, update your sensor with the latest software, restore sensor defaults, reboot the sensor, and shut down the sensor.

This chapter contains the following sections:

Configuring Passwords

This section describes how to set up passwords for users on the sensor, and contains the following topics:

Passwords Pane

As sensor administrator, you can configure how passwords are created in the Passwords pane. All user-created passwords must conform to the policy that you set in the Passwords pane.

Caution If the password policy includes minimum numbers of character sets, such as upper case or number characters, the sum of the minimum number of required character sets cannot exceed the minimum password size. For example, you cannot set a minimum password size of eight and also require that passwords must contain at least five lowercase and five uppercase characters.

Passwords Pane Field Definitions

The following fields are found in the Passwords pane:

- Attempt Limit—Lets you lock accounts so that users cannot keep trying to log in after a certain number of failed attempts. The default is 0, which indicates unlimited authentication attempts. For security purposes, you should change this number.
- Size Range—Specifies the range for the minimum and maximum allowed size for a password. For IPS 7.2(1)E4, a valid password is 8 to 32 characters long. For IPS 7.2(2)E4 and later, a valid password is 6 to 127 characters long.
- Minimum Digit Characters—Specifies the minimum number of numeric digits that you specify must be in a password.
- Minimum Upper Case Characters—Specifies the maximum number of upper-case alphabet characters that you specify must be in a password.
- Minimum Lower Case Characters—Specifies the minimum number of lower-case alphabet characters that you specify must be in a password.
- Minimum Other Characters—Specifies the minimum number of non-alphanumeric printable characters that you specify must be in a password.
- Number of Historical Passwords—Specifies the number of historical passwords you want the sensor to remember for each account. Any attempt to change the password of an account fails if the new password matches any of the remembered passwords. When this value is 0, no previous passwords are remembered.

For More Information

For the procedures for recovering passwords for the various sensors, see Recovering the Password, page 20-4.

Configuring Password Requirements

To configure password requirements, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Passwords**.

Step 3 In the Attempt Limit field, enter how many attempts a user has to enter the correct password.

Note The default is 0, which indicates unlimited authentication attempts. For security purposes, you should change this number.

Step 4 In the Size Range field, enter how long the password can be. For IPS 7.2(1)E4, a valid password is 8 to 32 characters long. For IPS 7.2(2)E4 and later, a valid password is 6 to 127 characters long.

Step 5 In the Minimum Digit Characters field, enter the minimum number of numeric digits a password can have.

Step 6 In the Minimum Upper Case Characters field, enter the least number of upper case characters the password can have.

Step 7 In the Minimum Lower Case Characters field, enter the least number of lower case characters the password can have.

Caution If the password policy includes minimum numbers of character sets, such as upper case or number characters, the sum of the minimum number of required character sets cannot exceed the minimum password size. For example, you cannot set a minimum password size of eight and also require that passwords must contain at least five lowercase and five uppercase characters.

Step 8 In the Minimum Other Characters field, enter the least number of other characters the password can have.

Step 9 In the Number of Historical Passwords field, enter the number of historical passwords you want the sensor to remember for each account.

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

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Configuring Packet Logging

Note Make sure that the user is configured with the appropriate Cisco av-pair on the RADIUS server. This pair would be in the form “permit-packet-logging=true/false.”

On the Packet Logging pane, you can restrict the use of packet capture-related commands—packet capture/display, IP logging—for local and AAA RADIUS users. RADIUS users with the correct av-pair are authorized to execute packet capture, packet display, and IP logging commands. Local users with the correct permissions can use the packet capture and IP log commands. To restrict all users from executing packet capture and IP log commands, uncheck the **Permit packet capture and iplog commands** checkbox. To allow AAA RADIUS users with the correct av-pair and local users with the correct privilege levels to execute all packet capture and IP log commands, check the **Permit packet capture and iplog commands** checkbox. The default is to permit packet capture and IP log commands.

When you modify the permit packet capture and IP log command option, you receive the following warning:

```
Modified packet settings would take effect only for new sessions, existing sessions will
continue with previous settings.
```

The IP Logging pane (**Sensor Management > Time-Based Actions > IP Logging**) reflects the packet capture command restriction. The current user is verified for the appropriate permissions to add, edit, download, or stop IP logging. Once the user is verified, IP logging is enabled. If the user does not have the appropriate permissions, the following error message is displayed:

```
You do not have sufficient permissions to perform this action. Packet and IP logging have
been restricted for this user.
```

For More Information

- For more information about IP logging, see Configuring IP Logging, page 17-10.
- For detailed information about AAA RADIUS authentication, see Configuring Authentication, page 6-17.

Recovering the Password

This section describes how to recover the password on the sensor, and contains the following topics:

Understanding Password Recovery

Note Administrators may need to disable the password recovery feature for security reasons.

Password recovery implementations vary according to IPS platform requirements. Password recovery is implemented only for the cisco administrative account and is enabled by default. The IPS administrator can then recover user passwords for other accounts using the CLI. The cisco user password reverts to **cisco** and must be changed after the next login.

Table 20-1 lists the password recovery methods according to platform.

Table 20-1 Password Recovery Methods According to Platform

Platform	Description	Recovery Method
4300 series sensors 4500 series sensors	Standalone IPS appliances	GRUB prompt or ROMMON
ASA 5500-X IPS SSP ASA 5585-X IPS SSP	ASA 5500 series adaptive security appliance IPS modules	Adaptive security appliance CLI command

For More Information

For the procedure for disabling password recovery, see Disabling Password Recovery, page 20-10.

Recovering the Appliance Password

There are two ways to recover the password for appliances—using the GRUB menu or ROMMON. This section describes how to recover the password on appliances, and contains the following topics:

- Using the GRUB Menu, page 20-5
- Using ROMMON, page 20-5

Using the GRUB Menu

Note You must have a terminal server or direct serial connection to the appliance to use the GRUB menu to recover the password.

For the IPS 4355, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL appliances, the password recovery is found in the GRUB menu, which appears during bootup. When the GRUB menu appears, press any key to pause the boot process.

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance to see the GRUB menu.

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
-------------------------------------------
0: Cisco IPS
1: Cisco IPS Recovery
2: Cisco IPS Clear Password (cisco)
-------------------------------------------

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    Commands before booting, or 'c' for a command-line.

    Highlighted entry is 0:
```

Step 2 Press any key to pause the boot process.

Step 3 Choose **`2: Cisco IPS Clear Password (cisco)`**. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

For More Information

For the procedure for connecting an appliance t a terminal server, see Troubleshooting Loose Connections, page C-23.

Using ROMMON

For the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL, you can use the ROMMON to recover the password. To access the ROMMON CLI, reboot the sensor from a terminal server or direct connection and interrupt the boot process.

Note After recovering the password, you must reset the confreg to **0**, otherwise, when you try to upgrade the sensor, the upgrade fails because when the sensor reboots, it goes to password recovery (**confreg 0x7**) rather than to the upgrade option.

To recover the password using the ROMMON CLI, follow these steps:

Step 1 Reboot the appliance.

Step 2 To interrupt the boot process, press **ESC** or **Control-R** (terminal server) or send a **BREAK** command (direct connection). The boot code either pauses for 10 seconds or displays something similar to one of the following:

- `Evaluating boot options`
- `Use BREAK or ESC to interrupt boot`

Step 3 Enter the following commands to reset the password:

```
confreg 0x7
boot
```

Sample ROMMON session:

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS-4360-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

Step 4 Enter the following command to reset the confreg value to 0:

```
confreg 0
```

For More Information

For the procedure for connecting an appliance to a terminal server, see Connecting an Appliance to a Terminal Server, page 24-3..

Recovering the ASA 5500-X IPS SSP Password

You can reset the password to the default (**cisco**) for the ASA 5500-X IPS SSP using the CLI or the ASDM. Resetting the password causes it to reboot. IPS services are not available during a reboot.

Note To reset the password, you must have ASA 8.6.1 or later.

Use the **sw-module module ips password-reset** command to reset the password to the default **cisco**. If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

To reset the password on the ASA 5500-X IPS SSP, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command:

```
asa# sw-module module ips password-reset
Reset the password on module ips? [confirm]
```

Step 2 Press **Enter** to confirm.

```
Password-Reset issued for module ips.
```

Step 3 Verify the status of the module. Once the status reads `Up`, you can session to the ASA 5500-X IPS SSP.

```
asa# show module ips
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
ips ASA 5555-X IPS Security Services Processor   ASA5555-IPS        FCH151070GR

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
ips 503d.e59c.7c4c to 503d.e59c.7c4c  N/A          N/A          7.2(1)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- -------------------------
ips IPS                            Up               7.2(1)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
ips Up                 Up

Mod License Name   License Status  Time Remaining
--- -------------- --------------- ---------------
ips IPS Module     Enabled         210 days
```

Step 4 Session to the ASA 5500-X IPS SSP.

```
asa# session ips
Opening command session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-^X'.
```

Step 5 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
Password: cisco

You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
```

Step 6 Enter your new password twice.

```
New password: new password
Retype new password: new password
```

```
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on this IPS platform. The system will continue to
operate with the currently installed signature set. A valid license must be obtained in
order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a
new license or install a license.

asa-ssp#
```

Using the ASDM

To reset the password in the ASDM, follow these steps:

Step 1 From the ASDM menu bar, choose **Tools > IPS Password Reset**.

Note This option does not appear in the menu if there is no IPS present.

Step 2 In the IPS Password Reset confirmation dialog box, click **OK** to reset the password to the default (**cisco**). A dialog box displays the success or failure of the password reset. If the reset fails, make sure you have the correct ASA and IPS software versions.

Step 3 Click **Close** to close the dialog box. The sensor reboots.

Recovering the ASA 5585-X IPS SSP Password

Note To reset the password, you must have ASA 8.2.(4.4) or later or ASA 8.4.2 or later. The ASA 5585-X IPS SSP is not supported in ASA 8.3(*x*).

You can reset the password to the default (**cisco**) for the ASA 5585-X IPS SSP using the CLI or the ASDM. Resetting the password causes it to reboot. IPS services are not available during a reboot.

Use the **hw-module module** *slot_number* **password-reset** command to reset the password to the default **cisco**. If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

To reset the password on the ASA 5585-X IPS SSP, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command:

```
asa# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm]
```

Step 2 Press **Enter** to confirm.

```
Password-Reset issued for slot 1.
```

Step 3 Verify the status of the module. Once the status reads `Up`, you can session to the ASA 5585-X IPS SSP.

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5585-X IPS Security Services Processor-4 ASA5585-SSP-IPS40  JAF1436ABSG

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 5475.d029.8c74 to 5475.d029.8c7f  0.1          2.0(12)3     7.2(1)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- -------------------------
  1 IPS                            Up               7.2(1)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

Step 4 Session to the ASA 5585-X IPS SSP.

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 5 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
Password: cisco

You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
```

Step 6 Enter your new password twice.

```
New password: new password
Retype new password: new password

***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.
```

```
***LICENSE NOTICE***
There is no license key installed on this IPS platform. The system will continue to
operate with the currently installed signature set. A valid license must be obtained in
order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a
new license or install a license.
ips_ssp#
```

Using the ASDM

To reset the password in the ASDM, follow these steps:

Step 1 From the ASDM menu bar, choose **Tools > IPS Password Reset**.

Note This option does not appear in the menu if there is no IPS present.

Step 2 In the IPS Password Reset confirmation dialog box, click **OK** to reset the password to the default (**cisco**). A dialog box displays the success or failure of the password reset. If the reset fails, make sure you have the correct ASA and IPS software versions.

Step 3 Click **Close** to close the dialog box. The sensor reboots.

Disabling Password Recovery

Caution If you try to recover the password on a sensor on which password recovery is disabled, the process proceeds with no errors or warnings; however, the password is not reset. If you cannot log in to the sensor because you have forgotten the password, and password recovery is set to disabled, you must reimage your sensor.

Password recovery is enabled by default. You can disable password recovery through the CLI or IME.

Disabling Password Recovery Using the CLI

To disable password recovery in the CLI, follow these steps:

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

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Enter host mode.

```
sensor(config)# service host
```

Step 4 Disable password recovery.

```
sensor(config-hos)# password-recovery disallowed
```

Disabling Password Recovery Using the IME

To disable password recovery in the IME, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Network**.

Step 3 To disable password recovery, uncheck the **Allow Password Recovery** check box.

Troubleshooting Password Recovery

When you troubleshoot password recovery, pay attention to the following:

- You cannot determine whether password recovery has been disabled in the sensor configuration from the ROMMON prompt, GRUB menu, switch CLI, or router CLI. If you attempt password recovery, it always appears to succeed. If it has been disabled, the password is not reset to **cisco**. The only option is to reimage the sensor.
- You can disable password recovery in the host configuration. For the platforms that use external mechanisms, such as ROMMON, although you can run commands to clear the password, if password recovery is disabled in the IPS, the IPS detects that password recovery is not allowed and rejects the external request.
- To check the state of password recovery, use the **show settings | include password** command.

Verifying the State of Password Recovery

Use the **show settings | include password** command to verify whether password recovery is enabled.

To verify whether password recovery is enabled, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

Step 3 Verify the state of password recovery by using the **include** keyword to show settings in a filtered output.

```
sensor(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
sensor(config-hos)#
```

Configuring Licensing

This section describes how to obtain and install the license key, and contains the following topics:

Licensing Pane

Note You must be administrator to view license information in the Licensing pane and to install the sensor license key.

In the Licensing pane, you can obtain and install the sensor license key. The Licensing pane displays the status of the current license.

Understanding Licensing

Although the sensor functions without the license key, you must have a license key to obtain signature updates and use the global correlation features. To obtain a license key, you must have the following:

- Cisco Service for IPS service contract—Contact your reseller, Cisco service or product sales to purchase a contract.
- Your IPS device serial number—To find the IPS device serial number in the IME, choose **Configuration > *sensor_name* > Sensor Management > Licensing**.
- Valid Cisco.com username and password.

Trial license keys are also available. If you cannot get your sensor licensed because of problems with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the license key from a license key provided in a local file. Go to http://www.cisco.com/go/license and click **IPS Signature Subscription Service** to apply for a license key.

You can view the status of the license key in these places:

- The IME Home page in the Device Details section on the Licensing tab
- License Notice at CLI login

Whenever you start the IME or the CLI, you are informed of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use the IME and the CLI, but you cannot download signature updates.

If you already have a valid license on the sensor, you can click **Download** on the License pane to download a copy of your license key to the computer that the IME is running on and save it to a local file. You can then replace a lost or corrupted license, or reinstall your license after you have reimaged the sensor.

Service Programs for IPS Products

You must have a Cisco Services for IPS service contract for any IPS product so that you can download a license key and obtain the latest IPS signature updates. If you have a direct relationship with Cisco Systems, contact your account manager or service account manager to purchase the Cisco Services for IPS service contract. If you do not have a direct relationship with Cisco Systems, you can purchase the service account from a one-tier or two-tier partner.

When you purchase the following IPS products you must also purchase a Cisco Services for IPS service contract:

- IPS 4345
- IPS 4345-DC
- IPS 4360
- IPS 4510
- IPS 4520
- IPS 4520-XL

When you purchase an ASA 5500 series adaptive security appliance product that does not contain IPS, you must purchase a SMARTnet contract.

Note SMARTnet provides operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

When you purchase an ASA 5500 series adaptive security appliance product that ships with an IPS module installed, or if you purchase one to add to your ASA 5500 series adaptive security appliance product, you must purchase the Cisco Services for IPS service contract.

Note Cisco Services for IPS provides IPS signature updates, operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

For example, if you purchase an ASA 5585-X and then later want to add IPS and purchase an ASA-IPS10-K9, you must now purchase the Cisco Services for IPS service contract. After you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key.

Caution If you ever send your product for RMA, the serial number changes. You must then get a new license key for the new serial number.

Licensing Pane Field Definitions

The following fields are found in the Licensing pane:

- Current License—Provides the status of the current license:
  - License Status—Displays the current license status of the sensor.
  - Expiration Date—Displays the date when the license key expires (or has expired). If the key is invalid, no date is displayed.
  - Serial Number—Displays the serial number of the sensor.
  - Product ID—Displays the product ID of your sensor.
- Update License—Specifies from where to obtain the new license key:
  - Cisco.com—Contacts the license server at Cisco.com for a license key.
  - License File—Specifies that a license file be used.
  - Local File Path—Indicates where the local file is that contains the license key.

Obtaining and Installing the License Key

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

To obtain and install the license key, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Licensing**.

Step 3 The Licensing pane displays the status of the current license. If you have already installed your license, you can click **Download** to save it if needed.

Step 4 Obtain a license key by doing one of the following:

- Click the **Cisco.com** radio button to obtain the license from Cisco.com. the IME contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 5.
- Click the **License File** radio button to use a license file. To use this option, you must apply for a license key at this URL: www.cisco.com/go/license. The license key is sent to you in e-mail and you save it to a drive that the IME can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.

Step 5 Click **Update License**, and in the Licensing dialog box, click **Yes** to continue. The Status dialog box informs you that the sensor is trying to connect to Cisco.com. An Information dialog box confirms that the license key has been updated.

Step 6 Click **OK**.

Step 7 Log in to Cisco.com.

Step 8 Go to www.cisco.com/go/license.

Step 9 Fill in the required fields. Your license key will be sent to the e-mail address you specified.

Caution You must have the correct IPS device serial number and product identifier (PID) because the license key only functions on the device with that number.

Step 10 Save the license key to a hard-disk drive or a network drive that the client running the IME can access.

Step 11 Log in to the IME.

Step 12 Choose **Configuration > *sensor_name* > Sensor Management > Licensing.**

Step 13 Under Update License, click the **License File** radio button.

Step 14 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

Step 15 Browse to the license file and click **Open**.

Step 16 Click **Update License**.

Licensing the ASA 5500-X IPS SSP

For the ASA 5500-X series adaptive security appliances with the IPS SSP, the ASA requires the IPS Module license. To view your current ASA licenses, in ASDM choose **Home > Device Dashboard > Device Information > Device License**. For more information about ASA licenses, refer to the licensing chapter in the configuration guide. After you obtain the ASA IPS Module license, you can obtain and install the IPS license key.

For More Information

- For more information about getting started using the ASA 5500-X IPS SSP, refer to the *Cisco IPS Module on the ASA Quick Start Guide*.
- For the procedures for obtaining and installing the IPS License key, see Obtaining and Installing the License Key, page 20-14.

Uninstalling the License Key

Use the **erase license-key** command to uninstall the license key on your sensor. This allows you to delete an installed license key from a sensor without restarting the sensor or logging into the sensor using the service account.

To uninstall the license key, follow these steps:

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

Step 2 Uninstall the license key on the sensor.

```
sensor# erase license-key
Warning: Executing this command will remove the license key installed on the sensor.

You must have a valid license key installed on the sensor to apply the Signature Updates
and use the Global Correlation features.

Continue? []: yes
sensor#
```

Step 3 Verify the sensor key has been uninstalled.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0        2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
No license present
Sensor up-time is 3 days.
Using 14470M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.1M out of 376.1M bytes of available disk space (24%
 usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

  IPS-K9-7.2-1-E4   11:17:07 UTC Thu Jan 10 2013

Recovery Partition Version 1.1 - 7.2(1)E4

Host Certificate Valid from: 17-Apr-2013 to 18-Apr-2015
sensor#
```

Configuring Sensor Health

Note You must be administrator to configure sensor health metrics.

In the Sensor Health pane, you can configure the metrics that are used to determine the health and network security status of the IPS. The results show up in the Home pane in the various gadgets. If you do not select a metric by checking the check box, it does not show up in the health and network security status results. You can accept the default configuration or edit the values.

The overall health is set to the most critical settings of any of the metrics. For instance, if all the selected metrics are green except for one that is red, the overall health becomes red. The IPS produces a health and security status event when the overall health status of the IPS changes.

The security status of the sensor is determined for each virtual sensor using the threat ratings of events detected by the virtual sensors. The security status of the virtual sensor is raised when the virtual sensor detects an event with a threat rating that exceeds the threshold for that virtual sensor. Once a threshold has been exceeded, the security status remains at a critical level until the configured amount of time has passed with no more events being detected at the higher level.

ASA 5500-X IPS SSP and Memory Usage

For the ASA 5500-X IPS SSP, the memory usage is 93%. The default health thresholds for the sensor are 80% for yellow and 91% for red, so the sensor health will be shown as red on these platforms even for normal operating conditions. You can tune the threshold percentage for memory usage so that it reads more accurately for these platforms by configuring the Memory Usage option in the sensor health metrics.

Note Make sure you have the Memory Usage option in the sensor health metrics enabled.

Table 20-2 lists the Yellow Threshold and the Red Threshold health values.

Table 20-2 ASA 5500-X IPS SSP Memory Usage Values

Platform	Yellow	Red	Memory Used
ASA 5512-X IPS SSP	85%	91%	28%
ASA 5515-X IPS SSP	88%	92%	14%
ASA 5525-X IPS SSP	88%	92%	14%
ASA 5545-X IPS SSP	93%	96%	13%
ASA 5555-X IPS SSP	95%	98%	17%

Field Definitions

The following fields are found in the Sensor Health pane:

- Inspection Load—Lets you set a threshold for inspection load and whether this metric is applied to the overall sensor health rating.
- Missed Packet—Lets you set a threshold percentage for missed packets and whether this metric is applied to the overall sensor health rating.
- Memory Usage—Lets you set a threshold percentage for memory usage and whether this metric is applied to the overall sensor health rating.
- Signature Update—Lets you set a threshold for when the last signature update was applied and whether this metric is applied to the overall sensor health rating.
- License Expiration—Lets you set a threshold for when the license expires and whether this metric is applied to the overall sensor health rating.
- Event Retrieval—Lets you set a threshold for when the last event was retrieved and whether this metric is applied to the overall sensor health rating.

Note The event retrieval metric keeps track of when the last event was retrieved by an external monitoring application such as the IME. Disable Event Retrieval if you are not doing external event monitoring.

- Network Participation—Lets you choose whether the network participation health metrics contribute to the overall sensor health rating.
- Global Correlation—Let you choose whether the global correlation health metrics contribute to the overall sensor health rating.
- Application Failure—Lets you choose to have an application failure applied to the overall sensor health rating.
- IPS in Bypass Mode—Let you choose to know if bypass mode is active and have that apply to the overall sensor health rating.
- One or More Active Interfaces Down—Lets you choose to know if one or more enabled interfaces are down and have that apply to the overall sensor health rating.
- Yellow Threshold—Lets you set the lowest threshold in percentage, days, seconds, or failures for yellow.
- Red Threshold—Lets you set the lowest threshold in percentage, days, seconds, or failures for red.

For More Information

- For more detailed information on IME gadgets, see IME Gadgets, page 3-2.
- For a description of the IME Home pane, see IME Home Pane, page 1-3.

Configuring IP Logging Variables

Note You must be administrator to configure the IP logging variable.

You can configure the IP logging variable, Maximum Open IP Log Files, which applies to the general operation of the sensor.

Field Definitions

The following field is found in the IP Logging Variables pane:

- Maximum Open IP Log Files—Specifies the maximum number of concurrently open IP log files. The valid range is from 20 to 100. The default is 20.

Configuring Service Activity

Note You must be administrator to enable collection of service activity data.

In the Service Activity pane, you can enable the Analysis Engine to collect service activity data and you can specify the number of service activities for which you want data collected. The information is given as a per-port count of packets and bytes. The output is displayed in the Statistics pane.

Caution Collecting service activity data slows down sensor performance.

Field Definitions

The following field is found in the Service Activity pane:

- Collect Service Activity Data—Lets the Analysis Engine collect service activity data. The default is 15. The valid range is 10 to 65536.

Displaying SDEE Subscriptions

Note You must be administrator to delete SDEE subscription IDs.

Note Support for SDEE subscription is valid for IPS 7.2(2)E4 and later.

The SDEE Subscriptions pane displays the details of the SDEE client subscriptions on the sensor. You can view the SDEE subscription ID, the status (expired or valid) of the subscription, the IP address of each SDEE client for each listed subscription, and see the last time the subscription was read. The SDEE server automatically deletes SDEE subscriptions that appear to be idle or left open for 24 hours, although the timer checks for expired subscriptions every 12 hours. You can clear/refresh the pane by clicking **Refresh**. To delete an item in the SDEE Subscriptions pane, select it in the list, and click **Delete**.

SDEE is part of the IPS communications systems. The Cisco IPS produces various types of events including intrusion alerts and status events. The IPS communicates events to clients such as management applications using the proprietary IPS-industry leading protocol, SDEE, which is a product-independent standard for communicating security device events. SDEE adds extensibility features that are needed for communicating events generated by various types of security devices.

Systems that use SDEE to communicate events to clients are referred to as SDEE providers. SDEE specifies that events can be transported using the HTTP or HTTP over SSL and TLS protocols. When HTTP or HTTPS is used, SDEE providers act as HTTP servers, while SDEE clients are the initiators of HTTP requests.

The IPS includes the web server, which processes HTTP or HTTPS requests. The web server uses run-time loadable servlets to process the different types of HTTP requests. Each servlet handles HTTP requests that are directed to the URL associated with the servlet. The SDEE server is implemented as a web server servlet.

The SDEE server only processes authorized requests. A request is authorized if is originates from a web server to authenticate the identity of the client and determine the privilege level of the client.

Field Definitions

The following fields are found in the SDEE Subscriptions pane:

- ID—Displays the ID of the SDEE subscription.
- Status—Displays a status of open or read pending:
  - Open—A subscription is in an open state when it is open but an event retrieval request in not blocked waiting to retrieve events.
  - Read Pending—A subscription is in a read pending state when the IPS has received an event retrieval request and the request is blocked waiting for events to be generated. Read pending is a normal state for a subscription to be in.
- IP Address—Displays the IP address of each SDEE client for each listed subscription.

- State—Displays whether the SDEE subscription is valid or expired. An expired subscription means that the last time the subscription was read was 24 hours ago and therefore it is not in a read pending state. Read operations on an expired subscription are not allowed.
- Last Read Time—Displays the last time the SDEE server read the subscriptions and events were returned to you.

Configuring Automatic Update

This section describes how to configure your sensor for automatic software updates, and contains the following topics:

Auto/Cisco.com Update Pane

Note You must be administrator to view the Auto Update pane and to configure automatic updates.

On the Auto/Cisco.com Update pane, you can immediately update the sensor, or you can configure the sensor to automatically download signature and signature engine updates from a remote server or the Cisco server. If you click Update Now, and you do not have the remote or Cisco server settings configured, you must configure them before automatic update will occur. If the settings are already configured, automatic update begins immediately.

When you enable automatic updates, the sensor logs in to the server and checks for signature and signature engine updates according to the schedule you configure. When an update is available, the sensor downloads the update and installs it. You must have a Cisco.com user account with cryptographic privileges to download Cisco IPS signature and signature engine updates from Cisco.com. The first time you download Cisco software you set up an account with cryptographic privileges.

Pay attention to the following:

- Automatic updates do not work with Windows FTP servers configured with DOS-style paths. Make sure the server configuration has the UNIX-style path option enabled rather than DOS-style paths.
- The IPS address has been changed to cisco.com in the URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new address.
- For IPS 7.2(1)E4, while executing an immediate upgrade, you cannot use the IDM, IME, or CLI, or start any new sessions until the upgrade is complete. For IPS 7.2(2)E4 and later, you can use the IDM, IME, and CLI immediately after you begin an automatic update because the automatic update is now executed as background process.
- Automatic update requires either an HTTP proxy server or at least one DNS server to function. Make sure that you have a server configured on Configuration > Sensor Setup > Network.

- If you have both remote and Cisco servers settings configured, update from Cisco.com will be disabled. The sensor prefers automatic updates from a remote server to updates from Cisco.com.
- While executing an immediate upgrade, you cannot use the IME, or start any new sessions until the upgrade is complete.
- The sensor does not support communication with Cisco.com through nontransparent proxy servers.

For More Information

For the procedure for obtaining software and an account with cryptographic privileges, see Obtaining Cisco IPS Software, page 26-1.

Supported FTP and HTTP Servers

The following FTP servers are supported for IPS software updates:

- WU-FTPD 2.6.2 (Linux)
- Solaris 2.8
- Sambar 6.0 (Windows 2000)
- Serv-U 5.0 (Windows 2000)
- MS IIS 5.0 (Windows 2000)

The following HTTP/HTTPS servers are supported for IPS software updates:

- CSM - Apache Server (Tomcat)
- CSM - Apache Server (JRun)

UNIX-Style Directory Listings

To configure automatic update using an FTP server, the FTP server must provide directory listing responses in UNIX style. MS-DOS style directory listing is not supported by the sensor automatic update feature.

Note If the server supplies MS-DOS style directory listings, the sensor cannot parse the directory listing and does not know that there is a new update available.

To change Microsoft IIS to use UNIX-style directory listings, follow these steps:

Step 1 Choose **Start > Program Files > Administrative Tools**.

Step 2 Click the **Home Directory** tab.

Step 3 Click the **UNIX directory listings style** radio button.

Signature Updates and Installation Time

There is a short period of time that traffic is not inspected while you are performing signature updates. However, traffic continues to flow if you have bypass enabled.

When a signature update adds or modifies signatures that contain regular expressions, the regular expression cache tables used by SensorApp have to be recompiled. The amount of recompile time varies by platform, number of signatures modified and/or added, and type of signatures modified and/or added.

If a signature update only adds one or two new signatures on a high-end platform, the recompile can be as fast as a few seconds.

The recompile takes several minutes and even up to a half hour under the following conditions:

- When a signature update adds a large number of signatures, for example, when you are skipping several signature levels to install a newer one, for example, installing S258 on top of S240.
- When a signature update modifies a large number of signatures, for example when a large number of older signatures is disabled and/or retired.

During the recompile, SensorApp stops monitoring packets. The interface driver detects this when the packet buffers begin filling up on the way to SensorApp and the driver stops receiving packets from SensorApp. If the sensor is in inline mode, the driver either turns on bypass if the bypass option is set to Auto, or brings down the interface links if bypass is set to Off.

Note Some packets can be dropped before the bypass setting begins operating. Once SensorApp completes the recompile of the regular expression cache files, SensorApp reconnects to the driver and begins monitoring again, and the driver begins passing packets to SensorApp for analysis, and if necessary, also brings the interface links back up.

For More Information

For more information on bypass mode, see Configuring Bypass Mode, page 7-25.

Auto/Cisco.com Update Pane Field Definitions

Note For IPS 7.2(1)E4, while executing an immediate upgrade, you cannot use the IDM, IME, or CLI, or start any new sessions until the upgrade is complete. For IPS 7.2(2)E4 and later, you can use the IDM, IME, and CLI immediately after you begin an automatic update because the automatic update is now executed as background process.

The following fields are found in the Auto/Cisco.com Update pane:

- Update Now—Lets you trigger an update immediately if you have automatic upgrade settings configured.

Remote Server Settings

- Enable auto-update from a remote server—Lets the sensor install updates stored on a remote server.

  Note If **Enable auto-update from a remote server** is not checked, all fields are disabled and cleared. You cannot toggle this on or off without losing all other settings.

- Remote Server Access—Lets you specify the following options for the remote server:
  - IP Address—Identifies the IP address of the remote server.
  - Username—Identifies the username corresponding to the user account on the remote server.

  - Password—Identifies the password for the user account on the remote server.
  - Confirm Password—Confirms the password by forcing you to retype the remote server password.
  - File Copy Protocol—Specifies whether to use FTP or SCP.
  - Directory—Identifies the path to the update on the remote server.
- Schedule—Lets you specify the following schedule options:
  - Start Time—Identifies the time to start the update process. This is the time when the sensor will contact the remote server and search for an available update.
  - Frequency—Specifies whether to perform updates on an hourly or weekly basis.
  - Hourly—Specifies to check for an update every n hours.
  - Daily—Specifies the days of the week to perform the updates.

Cisco Server Settings

- Enable signature and engine updates from Cisco—Lets the sensor go to Cisco.com to download signature and engine updates.
- Cisco Server Access—Lets you specify the following options for the Cisco.com server:
  - URL—Automatically populated with the correct URL when you check the **Enable signature and engine updates from Cisco** check box.
  - Username—Identifies the username corresponding to the user account on Cisco.com.
  - Password—Identifies the password for the user account on Cisco.com.
  - Confirm Password—Confirms the password by forcing you to retype the Cisco.com password.
- Schedule—Lets you specify the following schedule options:
  - Start Time—Identifies the time to start the update process. This is the time when the sensor will contact the remote server and search for an available update.
  - Frequency—Specifies whether to perform updates on an hourly or weekly basis.
  - Hourly—Specifies to check for an update every n hours.
  - Daily—Specifies the days of the week to perform the updates.

Auto Update Info

- Refresh—Refreshes the auto update information.
- Last Directory Read Attempt—Displays the last time the sensor accessed the automatic update directory to check for new updates.
- Last Download Attempt—Displays the last time the sensor tried to download updates.
- Last Install Attempt—Displays the last time the sensor tried to install updates.
- Last Directory Read—Displays the last directory that was accessed.
- Last Update Status—Displays the status of the last update.
- Next Attempt—Displays the next time the sensor will try to download updates.

Configuring Auto Update

Caution The IPS address has been changed to cisco.com in the URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new address.

Note For IPS 7.2(1)E4, while executing an immediate upgrade, you cannot use the IDM, IME, or CLI, or start any new sessions until the upgrade is complete. For IPS 7.2(2)E4 and later, you can use the IDM, IME, and CLI immediately after you begin an automatic update because the automatic update is now executed as background process.

To configure automatic updates from a remote server or Cisco.com, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Auto/Cisco.com Update**.

Step 3 To trigger an immediate automatic upgrade, click **Update Now**.

Note You must have automatic update settings configured to trigger an immediate update.

Step 4 To enable automatic updates from a remote server, check the **Enable Auto Update from a Remote Server** check box:

a. In the IP Address field, enter the IP address of the remote server where you have downloaded and stored updates.

b. To identify the protocol used to connect to the remote server, from the File Copy Protocol drop-down list, choose either FTP or SCP.

c. In the Directory field, enter the path to the directory on the remote server where the updates are located. A valid value for the path is 1 to 128 characters.

d. In the Username field, enter the username to use when logging in to the remote server. A valid value for the username is 1 to 2047 characters.

e. In the Password field, enter the username password on the remote server. A valid value for the password is 1 to 2047 characters.

f. In the Confirm Password field, enter the password to confirm it.

g. For hourly updates, check the **Hourly** check box, and follow these steps:

- In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.
- In the Every_hours field, enter the hour interval at which you want every update to occur. The valid value is 1 to 8760.

  For example, if you enter 5, every 5 hours the sensor looks at the directory of files on the server. If there is an available update candidate, it is downloaded and installed. Only one update is installed per cycle even if there are multiple available candidates. The sensor determines the most recent update that can be installed and installs that file.

h. For weekly updates, check the **Daily** check box, and follow these steps:

- In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.

- In the Days field, check the day(s) you want the sensor to check for and download available updates.

Step 5 To enable signature and engine updates from Cisco.com, check the **Enable Signature and Engine Updates from Cisco.com** check box:

a. In the Username field, enter the username to use when logging in to Cisco.com. A valid value for the username is 1 to 2047 characters.

b. In the Password field, enter the username password for Cisco.com. A valid value for the password is 1 to 2047 characters.

c. In the Confirm Password field, enter the password to confirm it.

d. For hourly updates, check the **Hourly** check box, and follow these steps:

- In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.
- In the Every_hours field, enter the hour interval at which you want every update to occur. The valid value is 1 to 8760.

  For example, if you enter 5, every 5 hours the sensor looks at the directory of files on the server. If there is an available update candidate, it is downloaded and installed. Only one update is installed per cycle even if there are multiple available candidates. The sensor determines the most recent update that can be installed and installs that file.

e. For weekly updates, check the **Daily** check box, and follow these steps:

- In the Start Time field, enter the time you want the updates to start. The valid value is hh:mm:ss.
- In the Days field, check the day(s) you want the sensor to check for and download available updates.

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

Step 6 Click **Apply** to save your changes.

Manually Updating the Sensor

This section describes how to manually update the sensor, and contains the following topics:

Update Sensor Pane

Note You must be administrator to view the Update Sensor pane and to update the sensor with service packs and signature updates.

In the Update Sensor pane, you can immediately apply service pack and signature updates. Sensor upgrade/update package filenames have the .pkg extension.

Note To manually update the sensor, you must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

Caution You cannot apply system image files on the Update Sensor pane. You must follow the procedures for reimaging your sensor. System image filenames have the .img or .aip extension.

For More Information

- For information on signature updates and how long it can take to install them, see Signature Updates and Installation Time, page 20-21.
- For the procedure for obtaining software files on Cisco.com, see Obtaining Cisco IPS Software, page 26-1

Update Sensor Pane Field Definitions

The following fields are found in the Update Sensor pane:

- Update is located on a remote server and is accessible by the sensor—Lets you specify the following options:
  - URL—Identifies the type of server where the update is located. Specify whether to use FTP, HTTP, HTTPS, or SCP.
  - ://—Identifies the path to the update on the remote server.
  - Username—Identifies the username corresponding to the user account on the remote server.
  - Password—Identifies the password for the user account on the remote server.
- Update is located on this client—Lets you specify the following options:
  - Local File Path—Identifies the path to the update file on this local client.
  - Browse Local—Opens the Browse dialog box for the file system on this local client. From this dialog box, you can navigate to the update file.

Updating the Sensor

Note To manually update the sensor, you must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

To immediately apply a service pack and signature update, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Update Sensor**.

Step 3 To pull an update down from a remote server and install it on the sensor, follow these steps:

a. Check the **Update is located on a remote server and is accessible by the sensor** check box.

b. In the URL field, enter the URL where the update can be found.

Note You must have already downloaded the update from Cisco.com and put it on the FTP server.

The following URL types are supported:

- FTP:—Source URL for an FTP network server.

  The syntax for this prefix is the following:

  `ftp://location/relative_directory/filename`

  or

  `ftp://location//absolute_directory/filename`

- HTTPS:—Source URL for a web server.

  Note Before using the HTTPS protocol, set up a TLS trusted host.

  The syntax for this prefix is the following:

  `https://location/directory/filename`

- SCP:—Source URL for a SCP network server.

  The syntax for this prefix is the following:

  `scp://location/relative_directory/filename`

  or

  `scp://location/absolute_directory/filename`

- HTTP:—Source URL for a web server.

  The syntax for this prefix is the following:

  `http://location/directory/filename`

  The following example shows the FTP protocol:

  `ftp://user@ip_address/UPDATES/file_name.rpm.pkg`

c. In the Username field, enter the username for an account on the remote server.

d. In the Password field, enter the password associated with this account on the remote server.

Step 4 To push from the local client and install it on the sensor, follow these steps:

a. Check the **Update is located on this client** check box.

b. Specify the path to the update file on the local client or click **Browse Local** to navigate through the files on the local client.

Step 5 Click **Update Sensor**. The Update Sensor dialog box tells you that if you want to update, you will lose your connection to the sensor and you must log in again.

Step 6 Click **OK** to update the sensor.

Note The IME and CLI connections are lost during the following updates: service pack, minor, major, and engineering patch. If you are applying one of these updates, the installer restarts the IPS applications. A reboot of the sensor is possible. You do not lose the connection when applying signature updates and you do not need to reboot the system.

Tip To discard your changes and close the dialog box, click **Cancel**.

For More Information

For the procedure for obtaining software files on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.

Restoring Defaults

Note You must be administrator to view the Restore Defaults pane and to restore the sensor defaults.

On the Restore Defaults pane, you can restore the default configuration at any time to your sensor.

Warning **Restoring the defaults removes the current application settings and restores the default settings. Your network settings also return to the defaults and you immediately lose connection to the sensor.**

To restore the default configuration, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Restore Defaults**.

Step 3 To restore the default configuration, click **Restore Defaults**.

Step 4 In the Restore Defaults dialog box, click **OK**.

Note Restoring defaults resets the IP address, netmask, default gateway, and access list. The password and time are not reset. Manual and automatic blocks also remain in effect. You must manually reboot your sensor.

Rebooting the Sensor

Note You must be administrator to see the Reboot Sensor pane and to reboot the sensor.

You can shut down and restart the sensor from the Reboot Sensor pane.

To reboot the sensor, follow these steps:

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

Step 2 Choose **Configuration > Sensor Management > Reboot Sensor**, and then click **Reboot Sensor**.

Step 3 To shut down and restart the sensor, click **OK**. The sensor applications shut down and then the sensor reboots. After the reboot, you must log back in.

Note There is a 30-second delay during which users who are logged in to the CLI are notified that the sensor applications are going to shut down.

Shutting Down the Sensor

Note You must be administrator to view the Shut Down Sensor pane and to shut down the sensor.

You can shut down the IPS applications and then put the sensor in a state in which it is safe to power it off.

To shut down the sensor, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > Shut Down Sensor**, and then click **Shut Down Sensor**.

Step 3 In the Shut Down Sensor dialog box, click **OK**. The sensor applications shut down and any open connections to the sensor are closed.

Note There is a 30-second delay during which users who are logged in to the CLI are notified that the sensor applications are going to shut down.

Monitoring the Sensor

The IME lets you monitor all aspects of the sensor, including performance, statistics, and connections. You can monitor OS identifications and anomaly detection. This section describes how to monitor your sensor, and contains the following topics:

Monitoring Events

This section describes how to filter and view event data on your sensor, and contains the following topics:

Events Pane

The Events pane lets you filter and view event data. You can filter events based on type, time, or both. By default all alert and error events are displayed for the past one hour. To access these events, click **View**.

When you click **View**, the IME defines a time range for the events if you have not already configured one If you do not specify an end time of the range, it is defined as the moment you click **View**.

To prevent system errors when retrieving large numbers of events from the sensor, the IME limits the number of events you can view at one time (the maximum number of rows per page is 500). Click **Back** and **Next** to view more events.

Events Pane Field Definitions

The following fields are found in the Events pane:

- Show Alert Events—Lets you configure the level of alert you want to view. The default is all levels enabled.
  - Informational
  - Low
  - Medium
  - High
- Threat Rating (0-100)—Lets you change the range (minimum and maximum levels) of the threat rating value.
- Show Error Events—Lets you configure the type of errors you want to view. The default is all levels enabled.
  - Warning
  - Error
  - Fatal
- Show Attack Response Controller events—Shows ARC (formerly known as Network Access Controller) events. The default is disabled.

  Note NAC is now known as ARC; however, in Cisco IPS, the name change has not been completed throughout the IME and the CLI.

- Show status events—Shows status events. The default is disabled.
- Select the number of the rows per page—Lets you determine how many rows you want to view per page. The valid range is 100 to 500. The default is 100.
- Show all events currently stored on the sensor—Retrieves all events stored on the sensor.
- Show past events—Lets you go back a specified number of hours or minutes to view past events.
- Show events from the following time range—Retrieves events from the specified time range.

For More Information

For a detailed explanation of threat rating, see Understanding Threat Rating, page 12-4.

Event Viewer Pane Field Definitions

The following fields are found on the Event Viewer pane:

- #—Identifies the order number of the event in the results query.
- Type—Identifies the type of event as Error, NAC, Status, or Alert.
- Sensor UTC Time—Identifies when the event occurred.
- Sensor Local Time—Displays the local time of the sensor.
- Event ID—Displays the numerical identifier the sensor has assigned to the event.
- Events—Briefly describes the event.
- Sig ID—Identifies the signature that fired and caused the alert event.
- Performed Actions—Displays the actions the sensor has taken.

Configuring Event Display

To configure how you want events to be displayed, follow these steps:

Step 1 Log in to the IME.

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Events**.

Step 3 Under Show Alert Events, check the check boxes of the levels of alerts you want to be displayed.

Step 4 In the Threat Rating field, enter the minimum and maximum range of threat rating.

Step 5 Under Show Error Events, check the check boxes of the types of errors you want to be displayed.

Step 6 To display ARC (formerly known as Network Access Controller) events, check the **Show Attack Response Controller events** check box.

Step 7 To display status events, check the **Show status events** check box.

Step 8 In the Select the number of the rows per page field, enter the number of rows per page you want displayed. The default is 100. The values are 100, 200, 300, 400, or 500.

Step 9 To set a time for events to be displayed, click one of the following ratio buttons:

- **Show all events currently stored on the sensor**
- **Show past events—**Enter the hours and minutes you want to go back to view past events.
- **Show events from the following time range—**Enter a start and end time.

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

Step 10 Click **View** to display the events you configured.

Step 11 To sort up and down in a column, click the right-hand side to see the up and down arrow.

Step 12 Click **Next** or **Back** to page by one hundred.

Step 13 To view details of an event, select it, and click **Details**. The details for that event appear in another dialog box. The dialog box has the Event ID as its title.

Clearing Event Store

Note The Event Store has a fixed size of 30 MB for all platforms.

Use the **clear events** command to clear the Event Store.

To clear events from the Event Store, follow these steps:

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

Step 2 Clear the Event Store.

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

Step 3 Enter **yes** to clear the events.

Displaying Inspection Load Statistics

Note You must be administrator to monitor inspection load statistics.

The Inspection Load Statistics pane displays the inspection load history across varying time periods. Historical peak and average values of the inspection load are displayed minute-by-minute (up to the last 60 minutes) or hour-by-hour (up to the last 72 hours).

The Inspection Load Statistics pane has two parts—a graphical chart on the top and a table on the bottom. The chart graphically displays the time versus the peak/average range. The table displays the raw peak/average values corresponding to the time value. You can hide each part of the pane by clicking the collapse toggle on the left side of the divider.

You can change the time scale of the statistics from the Type drop-down menu in the upper left corner. And you can export the statistics to a CSV or HTML file by clicking **Export**. Or you can right click on the graph to save and print the file.

Field Definitions

The following fields are found in the Inspection Load Statistics pane:

- Type—Lets you choose how to display inspection load statistics:
  - Inspection Load Per Minute (Last 60 Minutes)—Shows the statistics per minute over the last hour.
  - Inspection Load Per Hour (Last 72 Hours)—Shows the statistics per hour over the last three days.
- Export—Lets you export the data to one of the following file formats:
  - to CSV file
  - to HTML file

- Last Updated—Displays the date and time that the inspection load statistics were last updated.

Displaying Inspection Load Statistics

To configure how you want inspection load statistics to be displayed, follow these steps:

Step 1 Log in to the IME.

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Inspection Load Statistics**.

Step 3 From the Type drop-down list, select which view of the inspection load statistics you want to be displayed.

- Inspection Load Per Minute (Last 60 Minutes)—Shows the statistics per minute over the last hour.
- Inspection Load Per Hour (Last 72 Hours)—Shows the statistics per hour over the last three days.

Step 4 To collapse either the graph or the table, click the collapse toggle on the left side on the divider. To show the graph or table again, click the collapse toggle and then put your cursor on the divider and resize the pane.

Step 5 To export data from the Inspection Load Statistics pane, click **Export** and choose one of the following file formats:

- to CSV file
- to HTML file

Step 6 A Save dialog box appears. Enter a filename and choose which folder you want to save the file in and click **Save**.

Step 7 To refresh the view, click **Refresh**.

Step 8 You can left click on the pane and from the popup menu you can save or print the statistics.

Displaying Interface Statistics

In the Interface Statistics pane you can view the historical interface statistics in chart or table format. All interfaces including the management interface are presented. You can view the data for all interfaces together and the various counters for the last 60 minutes or for the last 72 hours. And you can export the statistics to a CSV or HTML file by clicking **Export**. Or you can right click on the graph to save and print the file.

For each interface you can see the following statistics in either minutes or hours:

- Total packets received
- Total bytes received
- FIFO overruns
- Received errors
- Received Mbps
- Missed packets (in terms of percentage)
- Average load (in terms of percentage)
- Peak Load (in terms of percentage)

Field Definitions

The following fields are found in the Interface Statistics pane:

- Interface—Lets you choose the interface for which you want to display statistics.
- Parameter—Lets you sort the statistics by parameter.
- Interval—Lets you choose the last 60 minutes or 72 hours as the time interval in which to display the statistics.

Displaying Interface Statistics

To configure how you want interface statistics to be displayed, follow these steps:

Step 1 Log in to the IME.

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Interface Statistics**.

Step 3 From the Interface drop-down list, select the interface you want to display statistics for.

Step 4 From the Parameter drop-down list, select the way you want the statistics sorted:

- Average load percentage
- Peak load percentage
- Missed packet percentage
- Packets received
- Bytes received
- Bytes per second
- Received errors
- FIFO overruns

Step 5 From the Interval drop-down menu, select the time interval for which to display the statistics:

- Last 60 minutes
- Last 72 hours

Step 6 To collapse either the graph or the table, click the collapse toggle on the left side on the divider. To show the graph or table again, click the collapse toggle and then put your cursor on the divider and resize the pane.

Step 7 To export data from the Interface Statistics pane, click **Export** and choose one of the following file formats:

- to CSV file
- to HTML file

Step 8 A Save dialog box appears. Enter a filename and choose which folder you want to save the file in and click **Save**.

Step 9 To refresh the view, click **Refresh**.

Step 10 You can left click on the pane and from the popup menu you can save or print the statistics.

Monitoring Anomaly Detection KBs

This section describes how to work with anomaly detection KBs, and contains the following topics:

Anomaly Detection Pane

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

Note You must be administrator to monitor anomaly detection KBs.

The Anomaly Detection pane displays the KBs for all virtual sensors. In the Anomaly Detection pane, you can perform the following actions:

- Show thresholds of specific KBs
- Compare KBs
- Load a KB
- Make the KB the current KB
- Rename a KB
- Download a KB
- Upload a KB
- Delete a KB or all KBs

Note The Anomaly Detection buttons are active if only one row in the list is selected, except for Compare KBs, which can have two rows selected. If any other number of rows is selected, none of the buttons is active.

Understanding KBs

The KB has a tree structure, and contains the following information:

- KB name
- Zone name
- Protocol
- Service

The KB holds a scanner threshold and a histogram for each service. If you have learning accept mode set to auto and the action set to rotate, a new KB is created every 24 hours and used in the next 24 hours. If you have learning accept mode set to auto and the action is set to save only, a new KB is created, but the current KB is used. If you do not have learning accept mode set to auto, no KB is created.

Note Learning accept mode uses the sensor local time.

The scanner threshold defines the maximum number of zone IP addresses that a single source IP address can scan. The histogram threshold defines the maximum number of source IP addresses that can scan more than the specified numbers of zone IP addresses.

Anomaly detection identifies a worm attack when there is a deviation from the histogram that it has learned when no attack was in progress (that is, when the number of source IP addresses that concurrently scan more than the defined zone destination IP address is exceeded). For example, if the scanning threshold is 300 and the histogram for port 445, if anomaly detection identifies a scanner that scans 350 zone destination IP addresses, it produces an action indicating that a mass scanner was detected. However, this scanner does not yet verify that a worm attack is in progress. Table 21-1 describes this example.

Table 21-1 Example Histogram

Number of source IP addresses	10	5	2
Number of destination IP addresses	5	20	100

When anomaly detection identifies six concurrent source IP addresses that scan more than 20 zone destination IP addresses on port 445, it produces an action with an unspecified source IP address that indicates anomaly detection has identified a worm attack on port 445. The dynamic filter threshold, 20, specifies the new internal scanning threshold and causes anomaly detection to lower the threshold definition of a scanner so that anomaly detection produces additional dynamic filters for each source IP address that scans more than the new scanning threshold (20).

You can override what the KB learned per anomaly detection policy and per zone. If you understand your network traffic, you may want to use overrides to limit false positives.

Triggering the High Category Histogram Before the Single-Scanner Threshold

Based on the default histogram (nonlearned knowledge base [KB]) values, histogram-based detection can occur before single-scanner detection.

Single scanner detection is based on the scanner threshold settings. The scanner threshold setting is a single number for that port or protocol and zone. Any single IP address scanning more than that number of hosts of that port or protocol in that zone is alerted as a scanner.

There is a histogram for that port or protocol and zone that tracks how many systems normally scan a smaller number of hosts (10 hosts, 20 hosts, or 100 hosts). When more than that normal number of scanners are seen, then a worm is declared and all IPs scanning more than the associated number of hosts are alerted on as being a worm scanner.

Note An IP source address can be alerted on as being a worm scanner without ever reaching the scanner threshold. The scanner threshold is used to detect single systems scanning a large number of hosts and is tracked separately from the algorithms for detecting worms.

Anomaly Detection Pane Field Definitions

The following fields and buttons are found in the Anomaly Detection pane:

Field Definitions

- Virtual Sensor—Displays the virtual sensor to which the KB belongs.
- Knowledge Base Name—Displays the name of the KB.

Note By default, the KB is named by its date. The default name is the date and time (year-month-day-hour_minutes_seconds). The initial KB is the first KB, the one that has the default thresholds.

- Current—Yes indicates the currently loaded KB.
- Size—Indicates the size in KB of the KB. The range is usually less than 1 KB to 500-700 KB.
- Created—Displays the date the KB was created.

Button Functions

- Show Thresholds—Opens the Thresholds window for the selected KB. In this window, you can view the scanner thresholds and histograms for the selected KB.
- Compare KBs—Opens the Compare Knowledge Bases dialog box. In this dialog box, you can choose which KB you want to compare to the selected KB. It opens the Differences between knowledge bases *KB name* and *KB name* window.
- Load—Loads the selected KB, which makes it the currently used KB.
- Save Current—Opens the Save Knowledge Base dialog box. In this dialog box, you can save a copy of the selected KB.
- Rename—Opens the Rename Knowledge Base dialog box. In this dialog box, you can rename the selected KB.
- Download—Opens the Download Knowledge Base From Sensor dialog box. In this dialog box, you can download a KB from a remote sensor.
- Upload—Opens the Upload Knowledge Base to Sensor dialog box. In this dialog box, you can upload a KB to a remote sensor.
- Delete—Deletes the selected KB.
- Delete All—Deletes all of the KBs.
- Refresh—Refreshes the Anomaly Detection pane.

Showing Thresholds

This section describes how to display KB threshold information, and contains the following topics:

- Threshold for KB_Name Window, page 21-10
- Thresholds for KB_Name Window Field Definitions, page 21-10
- Monitoring the KB Thresholds, page 21-10

Threshold for KB_Name Window

In the Thresholds for *KB_Name* window, the following threshold information is displayed for the selected KB:

- Zone name
- Protocol
- Learned scanner threshold
- User scanner threshold
- Learned histogram
- User histogram

You can filter the threshold information by zone, protocols, and ports. For each combination of zone and protocol, two thresholds are displayed: the Scanner Threshold and the Histogram threshold either for the learned (default) mode or the user-configurable mode.

Thresholds for *KB_Name* Window Field Definitions

The following fields are found in the Thresholds for *KB_Name* window:

- Filters—Lets you filter the threshold information by zone or protocol:
  - Zones—Specifies to filter to filter by all zones, external only, illegal only, or internal only.
  - Protocols—Filter by all protocols, TCP only, UDP only, or other only.

Note If you choose a specific protocol, you can also filter on all ports or a single port (TCP and UDP), all protocols, or a single protocol (other).

- Zone—Lists the zone name (external, internal, or illegal).
- Protocol—Lists the protocol (TCP, UDP, or Other).
- Scanner Threshold (Learned)—Lists the learned value for the scanner threshold.
- Scanner Threshold (User)—Lists the user-configured value for the scanner threshold.
- Histogram (Learned)—Lists the learned value for the histogram.
- Histogram (User)—Lists the user-configured value for the histogram.

Monitoring the KB Thresholds

To monitor KB thresholds, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 To refresh the Anomaly Detection pane with the latest KB information, click **Refresh**.

Step 4 To display the thresholds for a KB, select the KB in the list and click **Show Thresholds**. The Thresholds for *KB_Name* window appears. The default display shows all zones and all protocols.

Step 5 To filter the display to show only one zone, choose the zone from the Zones drop-down list.

Step 6 To filter the display to show only one protocol, choose the protocol from the Protocols drop-down list. The default display shows all ports for the TCP or UDP protocol and all protocols for the Other protocol.

Step 7 To filter the display to show a single port for TCP or UPD, click the **Single Port** radio button and enter the port number in the Port field.

Step 8 To filter the display to show a single protocol for Other protocol, click the **Single Protocol** radio button and enter the protocol number in the Protocol field.

Step 9 To refresh the window with the latest threshold information, click **Refresh**.

Comparing KBs

This section describes how to compare KBs, and contains the following topics:

Compare Knowledge Base Dialog Box

You can compare two KBs and display the differences between them. You can also display services where the thresholds differ more than the specified percentage. The Details of Difference column shows in which KB certain ports or protocols appear, or how the threshold percentages differ.

Field Definitions

The following field is found in the Compare Knowledge Bases dialog box:

- Drop-down list containing all KBs.

Differences between knowledge bases *KB_Name* and *KB_Name* Window

The Differences between knowledge base *KB_Name* and *KB_Name* window displays the following types of information:

- Zone
- Protocol
- Details of Difference

You can specify the percentage of the difference that you want to see. The default is 10%.

Field Definitions

The following fields are found in the Differences between knowledge bases *KB_Name* and *KB_Name* window:

- Specify Percentage of Difference—Lets you change the default from 10% to show different percentages of differences.
- Zone—Displays the zone for the KB differences (internal, illegal, or external).
- Protocol—Displays the protocol for the KB differences (TCP, UDP, or Other).

- Details of Difference—Displays the details of difference in the second KB.

Difference Thresholds between knowledge bases *KB_Name* and *KB_Name* Window

The Difference Thresholds between knowledge base *KB_Name* and *KB_Name* window displays the following types of information:

- Knowledge base name
- Zone name
- Protocol
- Scanner threshold (learned and user-configured)
- Histogram (learned and user-configured)

Field Definitions

The Difference Thresholds between knowledge base *KB_Name* and *KB_Name* window displays the following types of information:

- Knowledge Base—Displays the KB name.
- Zone—Displays the name of the zone (internal, illegal, or external).
- Protocol—Displays the protocol (TCP, UDP, or Other).
- Scanner Threshold (Learned)—Lists the learned value for the scanner threshold.
- Scanner Threshold (User)—Lists the user-configured value for the scanner threshold.
- Histogram (Learned)—Lists the learned value for the histogram.
- Histogram (User)—Lists the user-configured value for the histogram.

Comparing KBs

To compare two KBs, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 To refresh the Anomaly Detection pane with the most recent KB information, click **Refresh**.

Step 4 Select one KB in the list that you want to compare and click **Compare KBs**.

Step 5 From the drop-down list, choose the other KB you want in the comparison.

Note Or you can choose KBs in the list by holding the **Ctrl** key and selecting two KBs.

Step 6 Click **OK**. The Differences between knowledge bases *KB_Name* and *KB_Name* window appears.

Note If there are no differences between the two KBs, the list is empty.

Step 7 To change the percentage of difference from the default of 10%, enter a new value in the Specify Percentage of Difference field.

Step 8 To view more details of the difference, select the row and then click **Details**. The Difference Thresholds between knowledge bases *KB_Name* and *KB_Name* window appears displaying the details.

Saving the Current KB

This section describes how to save, load, or delete the current KB, and contains the following topics:

Save Knowledge Base Dialog Box

You can save a KB under a different name. An error is generated if anomaly detection is not active when you try to save the KB. If the KB name already exists, whether you chose a new name or use the default, the old KB is overwritten. Also, the size of KB files is limited, so if a new KB is generated and the limit is reached, the oldest KB (as long as it is not the current or initial KB) is deleted.

Note You cannot overwrite the initial KB.

Field Definitions

The following fields are found in the Save Knowledge Base dialog box:

- Virtual Sensor—Lets you choose the virtual sensor for the saved KB.
- Save As—Lets you accept the default name or enter a new name for the saved KB.

Loading a KB

Note Loading a KB sets it as the current KB.

To load a KB, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 Select the KB in the list that you want to load and click **Load**. The Load Knowledge Base dialog box appears asking if you are sure you want to load the knowledge base.

Step 4 Click **Yes**. The Current column now read Yes for this KB.

Saving a KB

To save a KB with a new KB and virtual sensor, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 Select the KB in the list that you want to save as a new KB and click **Save Current**.

Step 4 From the Virtual Sensor drop-down list, choose the virtual sensor to which you want this KB to apply.

Step 5 In the Save As field, either accept the default name, or enter a new name for the KB.

Tip To discard your changes and close the Save Knowledge Base dialog box, click **Cancel**.

Step 6 Click **Apply**. The KB with the new name appears in the list in the Anomaly Detection pane.

Deleting a KB

Note You cannot delete the KB that is loaded as the current KB, nor can you delete the initial KB.

To delete a KB, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 Select the KB in the list that you want to delete and click **Delete**. The Delete Knowledge Base dialog box appears asking if you are sure you want to delete the knowledge base.

Step 4 Click **Yes**. The KB no longer appears in the list in the Anomaly Detection pane.

Renaming a KB

The following field is found in the Rename Knowledge Base dialog box:

- New Name—Lets you enter a new name for the selected KB.

Note You cannot rename the initial KB.

To rename a KB, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 Select the KB in the list that you want to rename and click **Rename**.

Step 4 In the New Name field, enter the new name for the KB.

Step 5 Click **Apply**. The newly named KB appears in the list in the Anomaly Detection pane.

Downloading a KB

You can download a KB to a remote location using FTP or SCP protocol. You must have the remote URL, username, and password.

Field Definitions

The following fields are found in the Download Knowledge Base From Sensor dialog box.

- File Transfer Protocol—Lets you choose SCP or FTP as the file transfer protocol.
- IP address—Specifies the IP address of the remote sensor from which you are downloading the KB.
- Directory—Specifies the path where the KB resides on the remote sensor.
- File Name—Specifies the filename of the KB.
- Username—Specifies the username corresponding to the user account on the remote sensor.
- Password—Specifies the password for the user account on the remote sensor.

Downloading a KB

To download a KB from a sensor, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 To download a KB from a sensor, click **Download**.

Step 4 From the File Transfer Protocol drop-down list, choose the protocol you want to use (SCP or FTP).

Step 5 In the IP address field, enter the IP address of the sensor from which you are downloading the KB.

Step 6 In the Directory field, enter the path where the KB resides on the sensor.

Step 7 In the File Name field, enter the filename of the KB.

Step 8 In the Username field, enter the username corresponding to the user account on the sensor.

Step 9 In the Password field, enter the password for the user account on the sensor.

Tip To discard your changes and close the dialog box, click **Cancel**.

Step 10 Click **Apply**. The new KB appears in the list in the Anomaly Detection pane.

Uploading a KB

You can upload a KB from a remote location using FTP or SCP protocol. You must have the remote URL, username, and password.

Field Definitions

The following fields are found in the Upload Knowledge Base to Sensor dialog box:

- File Transfer Protocol—Lets you choose SCP or FTP as the file transfer protocol.
- IP address—Specifies the IP address of the remote sensor to which you are uploading the KB.
- Directory—Specifies the path where the KB resides on the sensor.
- File Name—Specifies the filename of the KB.
- Virtual Sensor—Specifies the virtual sensor with which you want to associate this KB.
- Save As—Lets you save the KB as a new file name.
- Username—Specifies the username corresponding to the user account on the sensor.
- Password—Specifies the password for the user account on the sensor.

Uploading a KB

To upload a KB to a sensor, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 To upload a KB to a sensor, click **Upload**.

Step 4 From the File Transfer Protocol drop-down list, choose the protocol you want to use (SCP or FTP).

Step 5 In the IP address field, enter the IP address of the sensor to which you are downloading the KB.

Step 6 In the Directory field, enter the path where the KB resides on the sensor.

Step 7 In the File Name field, enter the filename of the KB.

Step 8 From the Virtual Sensor drop-down list, choose the virtual sensor to which you want this KB to apply.

Step 9 In the Save As field, enter the name of the new KB.

Step 10 In the Username field, enter the username corresponding to the user account on the sensor.

Step 11 In the Password field, enter the password for the user account on the sensor.

Tip To discard your changes and close the dialog box, click **Cancel**.

Step 12 Click **Apply**. The new KB appears in the list in the Anomaly Detection pane.

Configuring OS Identifications

This section describes how to display learned OS and imported OS maps for the sensor, and contains the following topics:

Configuring Learned Operating Systems

Note You must administrator or operator to clear the list or delete entries in the Learned OS pane.

The Learned OS pane displays the learned OS maps that the sensor has learned from observing traffic on the network. The sensor inspects TCP session negotiations to determine the OS running on each host.

To clear the list or delete one entry, select the row and click **Delete**. Click **Refresh** to update the list. Click **Export** to export currently displayed learned OSes in the table to a comma-separated Excel file (using CSV) or HTML file. You can also use **Ctrl-C** to copy the contents in to a clipboard and later paste in to Notepad or Word using **Ctrl-V**.

Note If passive OS fingerprinting is still enabled and hosts are still communicating on the network, the learned OS maps are immediately repopulated.

Field Definitions

The following fields are found in the Learned OS Pane:

- Virtual Sensor—Specifies the virtual sensor with which the OS value is associated.
- Host IP Address—Specifies the IP address to which the OS value is mapped.
- OS Type—Specifies the OS type associated with the IP address.

Deleting Values and Clearing the Learned OS List

To delete a learned OS value or to clear the entire list, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > OS Identifications > Learned OS**.

Step 3 To delete one entry in the list, select it, and click **Delete**. The learned OS value no longer appears in the list on the Learned OS pane.

Step 4 To get the most recent list of learned OS values, click **Refresh**. The learned OS list is refreshed.

Step 5 To clear all learned OS values, click **Clear List**. The learned OS list is now empty.

Step 6 To save the learned OS list to CSV and HTML formats, click **Export**. You can also use **Ctrl-C** to copy the contents of the Learned OS pane and then use **Ctrl-V** to copy the contents in a NotePad or Word.

For More Information

For detailed information on adding, editing, deleting, and moving configured OS maps, see Adding, Editing, Deleting, and Moving Configured OS Maps, page 12-27.

Configuring Imported Operating Systems

Note You must administrator or operator to clear the list or delete entries in the Imported OS pane.

The Imported OS pane displays the OS maps that the sensor has imported from CSA MC if you have CSA MC set up as an external interface product. Choose **Configuration > External Product Interfaces** to add an external product interface. To clear the list or delete one entry, select the row, and then click **Delete**.

Field Definitions

The following fields are found in the Imported OS Pane:

- Host IP Address—Specifies the IP address to which the OS value is mapped.
- OS Type—Specifies the OS type associated with the IP address.

Deleting Values and Clearing the Imported OS List

To delete an imported OS value or to clear the entire list, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Dynamic Data > OS Identifications > Imported OS**.

Step 3 To delete one entry in the list, select it, and click **Delete**. The imported OS value no longer appears in the list on the Imported OS pane.

Step 4 To clear all imported OS values, click **Clear List**. The imported OS list is now empty.

Step 5 To update the pane with current imported OS values, click **Refresh**.

For More Information

For detailed information about external product interfaces, see Chapter 19, "Configuring External Product Interfaces."

Clearing Flow States

This section describes how to clear sensor databases, and contains the following topics:

Clear Flow States Pane

Caution Clearing the alerts database deletes any summary alerts in progress, which prevents a final summary alert. We recommend that you only clear the alerts database for troubleshooting purposes.

The Clear Flow States pane lets you clear the database of some or all of its contents, for example, the nodes, alerts, or inspectors databases. If you do not provide the virtual sensor name, all virtual sensor databases are cleared.

Clearing the nodes in the database causes the sensor to start fresh as if from a restart. All open TCP stream information is deleted and new TCP stream nodes are created as new packets are received.

When you clear the inspectors database, the TCP and state information is retained, but all inspection records that might lead to a future alert are deleted. New inspection records are created as new packets are retrieved.

When you clear the alerts database, the alerts database is cleared entirely.

Clear Flow States Pane Field Definitions

The following fields are found in the Clear Flow States pane:

- Clear Nodes—Clears the overall packet database elements, including the packet nodes, TCP session information, and inspector lists.
- Clear Inspectors—Clears inspector lists contained within the nodes. Does not clear TCP session information or nodes. Inspector lists represent the packet work and observations collected during the sensor up time.
- Clear Alerts (not recommended)—Clears the alerts database, including the alerts nodes, Meta inspector information, summary state, and event count structures.

Caution Clearing the alerts database deletes any summary alerts in progress, which prevents a final summary alert. We recommend that you only clear the alerts database for troubleshooting purposes.

- Clear All—Clears all of the virtual sensor databases.
- Specify a Single Virtual Sensor (otherwise all virtual sensors will be cleared)—Lets you clear the database of a specific virtual sensor.

Clearing Flow States

To clear flow states, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Properties > Clear Flow States**.

Step 3 Click the radio buttons of the values you want to clear:

- Clear Nodes
- Clear Inspectors

- Clear Alerts (not recommended)
- Clear All

Caution Clearing the alerts database deletes any summary alerts in progress, which prevents a final summary alert. We recommend that you only clear the alerts database for troubleshooting purposes.

Step 4 To clear the flow state of one virtual sensor, check the **Specify a Single Virtual Sensor (otherwise all virtual sensors will be cleared)** check box. To clear the flow state for all virtual sensors, go to Step 6.

Step 5 From the drop-down list, select the virtual sensor for which you want to clear the flow state.

Step 6 Click **Clear Flow State Now**.

Resetting Network Security Health

Note You must be administrator to reset network security health.

The Reset Network Security Health pane lets you reset the status and calculation of network security health. This clears the Network Security Health gadget on the Home page. If you do not provide the virtual sensor name, all virtual sensor network security health information is cleared.

Field Definition

The following field is found in the Reset Network Security Health pane:

- Specify a Single Virtual Sensor (otherwise network security for all virtual sensors will be reset)—Lets you clear the network security data for a specific virtual sensor.

Resetting Network Security Health Data

To reset network security health data, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Properties > Reset Network Security Health**.

Step 3 To reset the network security health of one virtual sensor, check the **Specify a Single Virtual Sensor (otherwise network security for all virtual sensors will be reset)** check box. To reset the data for all virtual sensors, go to Step 5.

Step 4 From the drop-down list, select the virtual sensor for which you want to clear network security health data.

Step 5 Click **Reset Network Security Health Now**. The data in the Network Security Health gadget on the Home page are cleared.

Note To change the threat thresholds displayed in the Network Security gadget, choose **Configuration > *sensor_name* > Event Action Rules > rules0 > Risk Category**.

For More Information

- For more information on the Sensor Health gadget, which contains network security data, see Sensor Health Gadget, page 3-3.
- For the procedure for configuring sensor health, see Configuring Sensor Health, page 20-16.
- For the procedure for configuring risk categories, see Configuring Risk Category, page 12-31.

Generating a Diagnostics Report

Note You must be administrator to run diagnostics.

Note Generating a diagnostics report can take a few minutes.

You can obtain diagnostics information on your sensors for troubleshooting purposes. The diagnostics report contains internal system information, such as logs, status, configuration, and so forth, that is intended for TAC to use when troubleshooting the sensor. You can view the report in the Diagnostics Report pane or you can click **Save** and save it to the hard-disk drive.

Button Definitions

The following buttons are found in the Diagnostics Report pane:

- Save—Opens the Save As dialog box so you can save a copy of the diagnostics report to your hard-disk drive.
- Generate Report—Starts the diagnostics process. This process can take several minutes to complete. After the process is complete, a report is generated and the display is refreshed with the updated report.

Generating a Diagnostics Report

Caution After you start the diagnostics process, do not click any other options in IME or leave the Diagnostics pane. This process must be completed before you can perform any other tasks for the sensor.

To run diagnostics, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Diagnostics Report**, and then click **Generate Report**.

Note The diagnostics process can take some time to complete. When the process has finished running, the display is refreshed with the updated results.

Step 3 To save this report as a file, click **Save**. The **Save As** dialog box opens and you can save the report to your hard-disk drive.

Viewing Statistics

Note You must be administrator or operator to view sensor statistics

The Statistics pane shows statistics for your sensor. You can display all applications by checking the **Check All** check box in the upper right-hand corner, or you can select specific applications to display statistics by checking the checkbox for each application you want to display. You can copy and save statistics to a file of your choice or automatically to this filename, statistics-*year-date*-T*time*.txt.

The Statistics pane displays the following applications running on your sensor:

- Analysis Engine

  The Analysis Engine section also contains global correlation statistics.
- Anomaly Detection
- Event Store
- External Product Interface
- Host
- Interface Configuration
- Logger
- Network Access (now known as Attack Response Controller)
- Notification
- OS Identification
- Transaction Server
- Virtual Sensor
- Web Server

Note Look at the statistics for the virtual sensor to determine the load value over a longer period of time. The statistics for Analysis Engine show values over a shorter period of time. If you compare the output, the values will appear to be inconsistent due to the different time periods. To get an accurate comparison between them, compare the processing load percentage from the statistics for the virtual sensor and the one-minute averaged value from the statistics for Analysis Engine.

Buttons

The following buttons are found in the Statistics pane:

- Refresh—Displays the most recent information about the sensor applications, including the Analysis Engine, Anomaly Detection, Event Store, External Product Interface, Host, Interface Configuration, Logger, Network Access, Notification, OS Identification, Transaction Server, Virtual Sensor, and Web server.

  Note Network Access Controller, now known as Attack Response Controller beginning with Cisco IPS 5.1, is still listed as Network Access in the statistics output.

- Copy—Lets you copy the entire displayed statistics or highlighted statistics to a file of your choice.
- Save—Lets you save entire displayed statistics or highlighted statistics to a file with the following filename, statistics-*year-date*-T*time*.txt.

Viewing Statistics

To show statistics for your sensor, follow these steps:

Step 1 Log in to IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Statistics**.

Step 3 To view all sensor application statistics, check the **Check All** check box in the upper right-hand corner of the Statistics pane. The sensor statistics appear in the pane below.

a. To copy the entire sensor statistics in the Statistics pane, click **Copy**. You can then paste the copied statistics into a document of your choice.

b. To save the entire sensor statistics, click **Save**. A dialog box appears with the following filename, for example, statistics-2014-01-22T110430CST.txt. You can choose where you want to save the file.

Step 4 To view specific sensor application statistics, click the down arrows in the upper right-hand corner of the Statistics pane to display all sensor application, and then check the check box next to the applications whose statistics you want to display.

a. To copy specific statistics, highlight the statistics, and then click **Copy**. You can then paste the copied statistics into a document of your choice.

b. To save specific statistics, highlight the statistics, and then click **Save.** A dialog box appears with the following filename, for example, statistics-2014-01-22T110430CST.txt. You can choose where you want to save the file.

Step 5 To have the statistics reset every time you refresh them, check the **Reset statistics after refresh** check box. To update statistics as they change, click **Refresh**.

Viewing System Information

The System Information pane displays the following information:

- TAC contact information
- Platform information
- Booted partition

- Software version
- Status of applications (MainApp, Analysis Engine, and CollaborationApp)
- Upgrades installed
- PEP information
- Memory usage
- Disk usage

Button Definitions

The following button is found on the System Information pane:

- Refresh—Displays the most recent information about the sensor, including the software version and PEP information.

Viewing System Information

To view system information, follow these steps:

Step 1 Log in to the IME using an account with administrator or operator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > System Information**. The System Information pane displays information about the system.

Step 3 Click **Refresh**. The pane refreshes and displays new information.

Configuring Event Monitoring

This chapter describes IME event monitoring and how to configure it. It contains the following sections:

Understanding Event Monitoring

The Event Monitoring pane contains views of events—events either in real time or historical time (events stored in the database). IME contains predefined views and you can also create your own views. You cannot delete or save changes to the predefined views. The left-hand side of the Event Monitoring pane is a view tree, and the right-hand side lets you configure the view and display it.

The right-hand side of the Event Monitoring pane consists of three parts:

- View Settings—Contains five tabs you can use to specify what events you want to see and how you want to see them. You can view events by filters, groups, colors, fields, and view types.

  You can use filters to details your view. You can use grouping to arrange the data in your view. You can use color so that certain specific data stand out. For example, if you are looking for events from a certain attacker IP address, you can highlight the events with the severity level as high and then apply a certain color to those events. You can choose which fields you want to display and in which order.
- Events table—Displays the events in your view. You can interface with events by selecting a row and then performing various actions using the toolbar or the right-click menu.
- Event Details—Select a single row in the Events table and the details for that event are displayed in the Event Details section of the pane.

Group By, Color Rules, Fields, and General Tabs

On the Group By tab, you can group events based on the attributes of an event. Up to four levels of nested grouping are allowed. For example, you can group on severity, then on Attacker IP address, and so forth. The selection criteria is the same as that for creating filters.

On the Color Rules tab, you can select events based on specific criteria and then apply different background and foreground colors to those events. The selection criteria is the same as that for creating filters. You must apply the colors from top to bottom. At the first match, the color rule is applied.

On the Fields tab, you can add and remove which fields you want to see in the event data, and you can move them up and down in the list in the order in which you want to see them. The selection criteria is the same as that for creating filters.

On the General tab, you can choose the view and give it a description. The available views are the predefined ones and the ones you have created that appear in the Event Views tree in the left-hand side of the Event Monitoring pane.

Understanding Filters

Note The Filter tab and Add Filter dialog box fields now support IPv6 and IPv4 addresses.

You can configure filtering properties for specific views in IME, thus allowing you to view only the events you want to see. If you do not apply filters to events, you see all events; otherwise, with a filter applied, you see only the events that match the criteria specified in the filter.

You can create filters based on a variety of criteria so that only the information you want to see is shown in your view. You can group events in single levels or columns, or according to the following criteria:

- Severity
- Date
- Time
- Device
- Signature Name
- Signature ID
- Attacker IP address
- Victim IP address
- Actions taken
- Victim port
- Threat rating
- Risk rating
- Reputation

Timesaver For example, if you are interested in all events that have high severity, you can create a filter with the **High** check box checked in the Severity section of the filter. This filter will then show only events that have a high severity.

You can use predefined filters or add new ones. You cannot edit or delete the predefined filters. You can enter comma-separated values in each field. Each field supports single entries, ranges, and NOT operations. For example, the attacker IP address supports the following formats:

- 10.1.1.1,10.1.1.5
- 10.1.1.1-10.1.1.15
- ! 10.1.1.1

Note The exclamation point (!) means 'does not include.'

Using filters, you can run queries, such as the following:

- Show events with attacker IP 10.1.1.1 or 10.1.1.5 and Sig ID 5042
- Show events with the risk rating 75-100 and attacker IP address 192.2.3.3

The Manage Filter Rules dialog box displays these filter definitions. Risk rating, threat rating, and destination port fields support the following formats:

- =
- !=
- >
- >=
- <
- <=
- in the range
- not in the range

Filter Tab and Add Filter Dialog Box Field Definitions

The following fields are found on the Filter tab and in the Add Filter dialog box:

- Filter Name—Lets you name this filter or pick from the default filters.
- Attacker IP—Attacker IP address you want to include in this filter. The valid values are *ip_address*, *ip_address_range*, for example, 10.0.0.1, !10.0.0.1, !10.1.1.1.

  Note The exclamation point (!) means 'does not include.'

- Victim IP—Victim IP address you want to include in this filter. The valid values are *ip_address*, *ip_address_range*, for example, 10.0.0.1, !10.0.0.1, !10.1.1.1.

- Signature Name/ID—Signature Name/ID you want to include in this filter. The valid values are *signature_name* or *signature_id* or *signature_id/subsig_id* or *signature_id_range*, for example:
  - no_checkpoint
  - no_checkpoint, 3320
  - no_checkpoint, 3320/1
  - 3300-400
- Victim Port—Victim port you want to include in this filter. The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Severity—Severity levels you want to include in this filter.
- Risk Rating—Risk rating you want to include in this filter. The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Reputation—Reputation score you want to include in this filter. The valid values are from -10.0 to 10.0.
- Threat Rating—Threat rating you want to include in this filter. The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Action(s) Taken—Lets you choose which actions the filter looks for in the alerts. The actions are a string that you can chose or you can enter free format strings.
- Sensor Name(s)—Lets you assign which sensors are included in this filter.
- Virtual Sensor—Lets you assign which virtual sensors are included in this filter.
- Status—Lets you assign a status to this filter (All, New, Assigned, Closed, Detected, Acknowledged). The Status field is useful, for example, in a situation where you want to save analysis of certain events for later. You can add a note and change the status to 'Acknowledged,' and then later you can filter by status to see all cases that are acknowledged and then do further analysis.
- Victim Locality—An alert attribute in the participants/address alert on which you can filter. It is defined in the event action rules variables.
- Color Parameters—Lets you configure color rules for your events (the following options only appear when you are adding a filter on the Color Rules tab):
  - Foreground—Displays and let you chose the foreground color for your event.
  - Background—Displays and let you chose the background color for your event.
  - Font Type—Lets you chose bold, italic, or both for your event.
  - Preview Text—Displays how the event will look in the view.

Working With Event Views

To work with event views, follow these steps:

Step 1 Choose **Event Monitoring > Event Monitoring > Event Views**.

Five predefined views appear in the left-hand side of the Event Monitoring pane: Basic View, Blocked Attacks View, Dropped Attacks View, Grouped Severity View, and Real-Time Colored View. The events appear in the lower half of the View pane.

Step 2 To create a view, click **New**.

Step 3 In the New View dialog box, enter a name for the view in the Name field, and then click **OK**. The new view now appears in the left part of the pane under My Views. You can work with a single event and apply and create filters for your view.

For More Information

- For the procedure for working with a single event, see Working With a Single Event, page 22-5.
- For the procedure for applying and creating filters for your view, see Configuring Filters for Event Views, page 22-6.

Working With a Single Event

To work with a single event, follow these steps:

Step 1 Chose **Event Monitoring > Event Monitoring > Event Views > Basic View**.

Step 2 Configure the time period from which you want to gather events.

Step 3 To work with a single event, select the event in the list, and then click **Event** on the toolbar.

From the Event drop-down list, you can view the following information (it also appears in the lower half of the window under Event Details displayed in tab form):

- Summary—Summarizes all of the information about that event.
- Explanation—Provides the description and related signature information about the signature associated with this event.
- Related Threats—Provides the related threats with a link to more detailed information in MySDN.
- Trigger Packet—Displays information about the packet that triggered the event.
- Context Data—Displays the packet context information.
- Actions Taken—Lists which event actions were deployed.
- Notes—Lets you take action on this event by assigning a designation for it (New, Assigned, Acknowledged, Closed, or Deleted). Add any notes in the Notes field and click **Save Note** to save it.

Step 4 To print the details of this event, click **Show All Details** to display the event details in a printer-friendly window.

Step 5 To add an attribute from a selected event, from the Filter drop-down menu, click **Add to Filter > Attacker IP/Victim IP/Signature ID**. The Filter tab appears in the upper half of the window.

Step 6 To create a filter from this event, from the Filter drop-down menu, click **Create a Filter**.

Step 7 To edit the signature associated with this event, click **Edit Signature**. This takes you to **Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures** where you can edit the signature.

Step 8 To create an event action rules filter from this event, click **Create Rule**. This takes you to **Configuration > *sensor_name* > Policies > IPS Policies > Add Event Action Filter** where you can add the event action rules filter.

Step 9 To stop the attacker, from the Stop Attacker drop-down menu, choose one of the following options:

- Using Inline Deny—This takes you to **Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Denied Attackers > Add Denied Attacker**.

- Using Block on another device—This takes you to **Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Host Blocks > Add Host Block**.

Step 10 To use ping, traceroute, DNS, and whois on the IP addresses involved in this event, choose them from the Tools drop-down menu.

You can use ping to diagnose basic network connectivity. Ping is a simple way to check if a sensor can communicate back. You can use traceroute to display the route an IP packet takes to a destination. You can use whois to determine the owner of a domain name or an IP address. You can use DNS lookup to translate host names to IP addresses, rather like a phone book.

Step 11 To save, delete, or copy the event, from the Other drop-down list, choose the action you want to perform.

Step 12 To save any changes that you have made to the view, click **Apply**. To discard any changes, click **Reset**.

For More Information

- For the procedure for adding filters, see Configuring Filters for Event Views, page 22-6.
- For the procedure for adding an event action rules filter, see Adding, Editing, Deleting, Enabling, Disabling, and Moving Event Action Filters, page 12-17.
- For the procedure for adding a denied attacker, see Configuring and Monitoring Denied Attackers, page 17-1.
- For the procedure for adding a host block, see Configuring Host Blocks, page 17-3.
- For more information on these tools, see Using Tools for Devices, page 2-6.

Configuring Filters for Event Views

Note The Filter tab and Add Filter dialog box fields now support IPv6 and IPv4 addresses.

To configure filters, follow these steps:

Step 1 Chose **Event Monitoring** and then click **New**.

Tip To select more than one item in the list, hold down the **Ctrl** key.

Step 2 In the New View dialog box, enter the name of the new view. The new view appears under My Views in the View tree.

Step 3 Click **View Settings > Filter**.

Step 4 From the Filter Name drop-down menu, choose the filter name for this filter, or click the **Note** icon and then click **Add** to add a new filter:

a. In the Filter Name field, enter a name for this filter.

b. In the Attacker IP field, enter an attacker IP address, or click the **Note** icon and add a unique IP address or a range of IP addresses, and then click **OK**.

c. In the Victim IP field, enter a victim IP address, or click the **Note** icon and add a unique IP address or a range of IP addresses, and then click **OK**.

d. In the Signature Name/ID field, enter a signature name or ID, or click the **Note** icon, and then choose a signature type, and click **OK**.

e. In the Victim Port field, enter a victim port, or click the **Note** icon and enter a victim port that meets the conditions you require, and then click **OK**.

f. Choose the severity levels you want for this filter.

g. In the Risk Rating field, enter the risk rating for this filter, or click the **Note** icon, and then enter the risk rating that meets the conditions you require, and click **OK**.

h. In the Reputation field, enter the reputation score for this filter, or click the **Note** icon, and then enter the reputation that meets the conditions you require, and click **OK**.

i. In the Threat Rating field, enter the threat rating for this filter, or click the **Note** icon, and then enter the threat rating that meets the conditions you require, and click **OK**.

j. In the Actions Taken field, enter the actions you want to trigger this filter, or click the **Note** icon, and then check the check boxes of the actions that you want to trigger this filter, and click **OK**.

k. In the Sensor Name(s) field, enter the names of the sensors that are affected by this filter, or click the **Note** icon, and check the check boxes of the sensor to which this filter applies and click **OK**.

l. In the Virtual Sensor field, enter the virtual sensor to which this filter applies.

m. From the Status drop-down menu, choose on which status you want to filter.

n. In the Victim Locality field, enter the name of any event action rules variable that you created on which you want to filter.

Step 5 To configure grouping, click the **Group By** tab:

a. Check the **Group events based on the following criteria** check box, and then set up the hierarchy of how you want to group the events by selecting the category from the drop-down menus.

b. Under Grouping Preferences, you can check the **Single Level**, **Show Group Columns**, or **Show Count Columns** check boxes. You can only show count columns if you enable Show Group Columns.

Step 6 To add color rules, click the **Color Rules** tab, and then click **Add**.

a. In the Filter Name field, enter a name for this color rules filter.

b. Check the **Enable** check box.

Note If you do not check the **Enable** check box, your color rules filter will not go in to effect.

c. Under Packet Parameters, enter the IP addresses, signature names and/or victim ports for which you want this color rules filter to apply.

d. Under Rating and Action Parameters, enter the severity, risk rating, threat rating, and actions for which you want this color rules filter to apply.

e. Under Other Parameters, enter the sensor name, virtual sensor name, status, and/or victim locality for which you want this color rules filter to apply.

f. Under Color Parameters, choose the foreground and background colors, and the font type for this color rules filter, and then click **OK**.

Tip For aid in entering the correctly formatted values for these fields, click the **Note** icon.

Step 7 To event fields and their order, click the **Fields** tab, and then click **Add >>**, **<< Remove**, **Move Up**, and **Move Down** to chose which fields you want to display and to arrange the fields in the order in which you want to see them.

Step 8 Click the **General** tab, and then in the View Description field enter a description for your view.

Step 9 Click **Save As** to create the new view, and then in the Name field, enter a name for your view. The settings are copied to the new view.

Step 10 Click **Save** to save any changes to the view. Your filter now appears in the Filter Name drop-down menu.

Step 11 To save any changes that you have made to the view, click **Apply**. To discard any changes, click **Reset**.

Configuring and Generating Reports

This chapter describes IME reports and how to configure and generate them. It contains the following topics:

Understanding IME Reporting

The IME lets you create different reports that you can customize using different filters. A report consists of a window with a bar or pie chart along with the tabular data used for the graphs. There are IME report types, user-defined reports, and demo reports that are predefined examples of reports.

The Reports window is divided in to two parts: the left-hand pane, the Report tree, shows the reports list in the form of a tree, and the right-hand pane, the Report Settings pane, contains the report. The Report tree contains a set of predefined reports, such as Basic Top Attacker, and place to store user-defined reports under the My Reports node. When you select a report in the list and click **Generate Report**, the corresponding report containing a graph and a table is displayed in the lower half of the Report Settings pane. The Reports Setting pane contains two tabs, General and Filter, which let you customize the report.

You can also save the reports as PDF or RTF files and print them in the IME. And you can set up automatic reporting and have the IME send you the reports you want automatically. The IME summarizes which reports were successfully generated and then attaches them as a PDF to the email. To set up automatic reporting, go to **Preferences > Tools > Reports**.

Note The Filter tab and Add Filter dialog box fields now support IPv6 and IPv4 addresses.

These are the IME report types:

- Top Attacker Reports—Shows top attacker IP addresses for a specified time. You specify the top number of attacker IP addresses. There are four predefined top attacker reports:
  - Basic Top Attacker
  - Top 10 Attackers Last 1 Hour
  - Top 10 Attackers Last 8 Hours with High Severity
  - Top 20 Critical Attackers Last 24 Hours

- Top Victim Reports—Shows top victim IP addresses for a specified time. You specify the top number of victim IP addresses. There are four predefined top victim reports:
  - Basic Top Victim
  - Top 10 Victims Last 1 Hour
  - Top 10 Victims Last 8 Hours with High Severity
  - Top 20 Victims with Action Denied Attacker
- Top Signature Reports—Shows top signatures fired for a specified time. You specify the top number of signatures. There are four predefined top signature reports:
  - Basic Top Signature
  - Top 10 Signatures Last 1 Hour
  - Top 10 Signatures Last 8 Hours with High Severity
  - Top 20 Critical Signatures Last 24 Hours
- Attacks Over Time Reports—Shows the attacks over a specified time. There are five predefined reports:
  - Basic Over Time Attack
  - Attacks Blocked in Last 24 Hours
  - Attacks Dropped in Last 24 Hours
  - Attacks Over Time Last 1 Hour
  - Critical Attacks Over Last 24 Hours
- Filtered Events vs. All Events Reports—Displays a set of events against the total events for a specified time period. There is one predefined report:
  - Negative Reputation Events
- Global Correlation Reports—Displays the global correlation reports since the sensor has been running. There are two predefined global correlation reports:
  - Reputation Filter
  - Global Correlation
- Specialized Reports—Displays the specialized reports. There is one predefined specialized report:
  - Obfuscated Traffic/Attacks—This report contains statistics on suspect and explicit traffic obfuscation activity. It combines a top attacker report with a top event report. Traffic obfuscation is way of getting attacks through the security device. With the strong obfuscation detection and cleansing capabilities of the Cisco IPS, you can detect traffic obfuscation and deal with potential threats.

Configuring and Generating Reports

Note The Filter tab and Add Filter dialog box fields now support IPv6 and IPv4 addresses.

You can customize your report by configuring the number of items you want in your report and what the time interval should be. You can also use DNS to resolve the IP addresses. You can also use filters to further refine the type of information you want your report to contain.

To configure and generate reports, follow these steps:

Step 1 In the Report tree, click **New**, and then in the New Report dialog box, enter the name of the new report, choose the type of report from the drop-down list, and then click **OK**. Your new report shows up under My Reports in the Report tree.

Step 2 Select your report, and on the **General** tab, configure the settings for your report:

a. In the Report Description field, enter a description for this report.

b. In the Top field, enter how many top events you want to see in this report.

c. Check the **Resolve Addresses Using DNS** check box, if you want to use DNS address resolution.

d. Configure the time interval for this report, either the duration or enter a custom time.

Step 3 On the **Filter** tab, from the Filter Name drop-down menu, choose the filter name, or to add a filter, click the **Note** icon.

Step 4 In the Manage Filter Rules dialog box, configure the filter fields for your report.

Step 5 Click **Generate Report**. Your report shows up in the bottom half of the Report Settings pane, displaying the statistics in graph and table form.

Step 6 To customize the display, choose Bar or Pie Chart in the **Display Type** drop-down menu.

Step 7 Click **Print** to print the report, or click **Save** to save the report in PDF or RFT format to your hard-disk drive.

Step 8 To see events for a single IP address, choose the IP address from the Events for drop-down list.

For More Information

- For the procedure for creating a filter, see Configuring Filters, page 3-16.
- For the procedure for configuring events for single IP addresses, see Working With a Single Event for Individual Top Attacker and Victim IP Addresses, page 3-14.
- For the procedure for configuring events for single signatures, see Working With a Single Event for a Top Signature, page 3-15.

Logging In to the Sensor

Note All IPS platforms allow ten concurrent CLI sessions.

This chapter explains how to log in to the various Cisco IPS platforms, and contains the following sections:

Supported User Roles

You can log in with the following user privileges:

- Administrator
- Operator
- Viewer
- Service

The service role does not have direct access to the CLI. Service account users are logged directly into a bash shell. Use this account for support and troubleshooting purposes only. Unauthorized modifications are not supported and will require the sensor to be reimaged to guarantee proper operation. You can create only one user with the service role.

When you log in to the service account, you receive the following warning:

```
******************************** WARNING ****************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be re-imaged
to guarantee proper operation.
*********************************************************************************
```

Note The service role is a special role that allows you to bypass the CLI if needed. Only a user with administrator privileges can edit the service account.

For More Information

- For more information about the service account, see Understanding the Service Account, page 6-18.
- For the procedures for adding and deleting users, see Configuring Authentication, page 6-17.

Logging In to the Appliance

Note You can log in to the appliance from a console port. The currently supported Cisco IPS appliances are the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL.

To log in to the appliance, follow these steps:

Step 1 Connect a console port to the sensor to log in to the appliance.

Step 2 Enter your username and password at the login prompt.

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the appliance.You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
sensor#
```

For More Information

- For the procedure for connecting an appliance to a terminal server, see Connecting an Appliance to a Terminal Server, page 24-3.
- For the procedure for using the **setup** command to initialize the appliance, see Basic Sensor Setup, page 25-4

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For terminal servers with RJ-45 connections, connect a rollover cable from the console port on the appliance to a port on the terminal server.
- For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.

Step 2 Configure the line and port on the terminal server. In enable mode, enter the following configuration, where # is the line number of the port to be configured.

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance. If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

Logging In to the ASA 5500-X IPS SSP

You log in to the ASA 5500-X IPS SSP from the adaptive security appliance.

To session in to the ASA 5500-X IPS SSP from the adaptive security appliance, follow these steps:

Step 1 Log in to the adaptive security appliance.

Note If the adaptive security appliance is operating in multi-mode, use the **change system** command to get to the system level prompt before continuing.

Step 2 Session to the IPS. You have 60 seconds to log in before the session times out.

```
asa# session ips
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 3 Enter your username and password at the login prompt.

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the module. You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on this IPS platform.
The system will continue to operate with the currently installed
signature set. A valid license must be obtained in order to apply
signature updates. Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.

asa-ips#
```

Step 4 To escape from a session and return to the adaptive security appliance prompt, do one of the following:

- Enter **exit**.
- Press **CTRL-Shift-6-x** (represented as **CTRL^X**).

For More Information

For the procedure for using the **setup** command to initialize the ASA 5500-X IPS SSP, see Basic Sensor Setup, page 25-4.

Logging In to the ASA 5585-X IPS SSP

You log in to the ASA 5585-X IPS SSP from the adaptive security appliance.

To session in to the ASA 5585-X IPS SSP from the adaptive security appliance, follow these steps:

Step 1 Log in to the adaptive security appliance.

Note If the adaptive security appliance is operating in multi-mode, use the **change system** command to get to the system level prompt before continuing.

Step 2 Session to the ASA 5585-X IPS SSP. You have 60 seconds to log in before the session times out.

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 3 Enter your username and password at the login prompt.

Note The default username and password are both **cisco**. You are prompted to change them the first time you log in to the module. You must first enter the UNIX password, which is **cisco**. Then you must enter the new password twice.

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
ips-ssp#
```

Step 4 To escape from a session and return to the adaptive security appliance prompt, do one of the following:

- Enter **exit**.
- Press **CTRL-Shift-6-x** (represented as **CTRL^X**).

For More Information

For the procedure for using the **setup** command to initialize the ASA 5585-X IPS SSP, see Basic Sensor Setup, page 25-4.

Logging In to the Sensor

Note After you have initialized the sensor using the **setup** command and enabled Telnet, you can use SSH or Telnet to log in to the sensor.

To log in to the sensor using Telnet or SSH, follow these steps:

Step 1 To log in to the sensor over the network using SSH or Telnet.

```
ssh sensor_ip_address
telnet sensor_ip_address
```

Step 2 Enter your username and password at the login prompt.

```
login: ******
Password: ******
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable law s and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
sensor#
```

For More Information

For the procedure for initializing the sensor, see Basic Sensor Setup, page 25-4

Initializing the Sensor

This chapter describes how to use the **setup** command to initialize the sensor, and contains the following sections:

Understanding Initialization

Note You must be administrator to use the **setup** command.

After you install the sensor on your network, you must use the **setup** command to initialize it so that you can communicate with it over the network. You cannot use the IME to configure the sensor until you initialize the sensor using the **setup** command.

With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, access control lists, global correlation servers, and time settings. You can continue using advanced setup in the CLI to enable Telnet, enable SSHv1 fallback, configure the web server, and assign and enable virtual sensors and interfaces, or you can use the Startup Wizard in the IME. After you configure the sensor with the **setup** command, you can change the network settings in the IME.

Caution You must have a valid sensor license for automatic signature updates and global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.

For More Information

For the procedure for initializing the sensor using the **setup** command, see Basic Sensor Setup, page 25-4.

Simplified Setup Mode

The sensor automatically calls the **setup** command when you connect to the sensor using a console cable and the sensor basic network settings have not yet been configured. The sensor does not call automatic setup under the following conditions:

- When initialization has already been successfully completed.
- If you have recovered or downgraded the sensor.
- If you have set the host configuration to default after successfully configuring the sensor using automatic setup.

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. The values shown in brackets next to each prompt are the default values last set.

System Configuration Dialog

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. The values shown in brackets next to each prompt are the current values.

You must go through the entire System Configuration Dialog until you come to the option that you want to change. To accept default settings for items that you do not want to change, press **Enter**.

To return to the EXEC prompt without making changes and without going through the entire System Configuration Dialog, press **Ctrl-C**. The System Configuration Dialog also provides help text for each prompt. To access the help text, enter **?** at a prompt.

When you complete your changes, the System Configuration Dialog shows you the configuration that you created during the setup session. It also asks you if you want to use this configuration. If you enter **yes**, the configuration is saved. If you enter **no**, the configuration is not saved and the process begins again. There is no default for this prompt; you must enter either **yes** or **no**.

You can configure daylight savings time either in recurring mode or date mode. If you choose recurring mode, the start and end days are based on week, day, month, and time. If you choose date mode, the start and end days are based on month, day, year, and time. Choosing disable turns off daylight savings time.

Note You only need to set the date and time in the System Configuration Dialog if the system is an appliance and is NOT using NTP.

Note The System Configuration Dialog is an interactive dialog. The default settings are displayed.

Example 25-1 shows a sample System Configuration Dialog.

Example 25-1 Example System Configuration Dialog

```
    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
```

```
Default settings are in square brackets '[]'.



Current time: Wed Mar 6 00:07:23 2013

Setup Configuration last modified:

Enter host name[sensor]:
Enter IP interface[192.168.1.2/24,192.168.1.1]:
Modify current access list?[no]:
Current access list entries:
  [1] 0.0.0.0/0
Delete:
Permit:
Use DNS server for Auto-Updates from www.cisco.com and Global Correlation?[no]:
  DNS server IP address[171.68.226.120]:
Use HTTP proxy server for Auto-Updates from www.cisco.com and Global Correlation?[no]:
  HTTP proxy server IP address:
  HTTP proxy server Port number:
Modify system clock settings?[no]:
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]:
    NTP Server IP Address[]:
    Use NTP Authentication?[no]:
      NTP Key ID[]:
      NTP Key Value[]:
Modify system date and time?[no]:
  Local Date as YYYY-MM-DD[2013-03-06]:
  Local Time as HH:MM:SS[]:
Participation in the SensorBase Network allows Cisco to collect aggregated statistics
about traffic sent to your IPS.
SensorBase Network Participation level?[off]:

If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS.
This includes summary data on the Cisco IPS network traffic properties and how this
traffic was handled by the Cisco appliances.  We do not collect the data content of
traffic or other sensitive business or personal information.  All data is aggregated and
sent via secure HTTP to the Cisco SensorBase Network servers in periodic intervals.  All
data shared with Cisco will be anonymous and treated as strictly confidential.
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
  * Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
```

```
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs. promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
  * Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

Basic Sensor Setup

You can perform basic sensor setup using the **setup** command, and then finish setting up the sensor using the CLI, IDM, or IME.

To perform basic sensor setup using the **setup** command, follow these steps:

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

Note Both the default username and password are **cisco**.

Step 2 The first time you log in to the sensor you are prompted to change the default password. Passwords must be at least eight characters long and be strong, that is, not be a dictionary word. After you change the password, basic setup begins.

Step 3 Enter the `setup` command. The System Configuration Dialog is displayed.

Step 4 Specify the hostname. The hostname is a case-sensitive character string up to 64 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable. The default is sensor.

Step 5 Specify the IP interface. The IP interface is in the form of IP Address/Netmask,Gateway: *X.X.X.X/nn*,*Y.Y.Y.Y*, where *X.X.X.X* specifies the sensor IP address as a 32-bit address written as 4 octets separated by periods, *nn* specifies the number of bits in the netmask, and *Y.Y.Y.Y* specifies the default gateway as a 32-bit address written as 4 octets separated by periods.

Step 6 Enter `yes` to modify the network access list:

a. If you want to delete an entry, enter the number of the entry and press **Enter**, or press **Enter** to get to the Permit line.

b. Enter the IP address and netmask of the network you want to add to the access list.

Note For example, 10.0.0.0/8 permits all IP addresses on the 10.0.0.0 network (10.0.0.0-10.255.255.255) and 10.1.1.0/24 permits only the IP addresses on the 10.1.1.0 subnet (10.1.1.0-10.1.1.255). If you want to permit access to a single IP address than the entire network, use a 32-bit netmask. For example, 10.1.1.1/32 permits just the 10.1.1.1 address.

c. Repeat Step b until you have added all networks that you want to add to the access list, and then press **Enter** at a blank permit line to go to the next step.

Step 7 You must configure a DNS server or an HTTP proxy server for automatic updates from www.cisco.com and global correlation to operate:

a. Enter `yes` to add a DNS server, and then enter the DNS server IP address.

b. Enter **yes** to add an HTTP proxy server, and then enter the HTTP proxy server IP address and port number.

Caution You must have a valid sensor license for automatic signature updates and global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.

Step 8 Enter **yes** to modify the system clock settings:

a. Enter **yes** to modify summertime settings.

Note Summertime is also known as DST. If your location does not use Summertime, go to Step m.

b. Enter **yes** to choose the USA summertime defaults, or enter **no** and choose recurring, date, or disable to specify how you want to configure summertime settings. The default is recurring.

c. If you chose recurring, specify the month you want to start summertime settings. Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december. The default is march.

d. Specify the week you want to start summertime settings. Valid entries are first, second, third, fourth, fifth, and last. The default is second.

e. Specify the day you want to start summertime settings. Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

f. Specify the time you want to start summertime settings. The default is 02:00:00.

Note The default recurring summertime parameters are correct for time zones in the United States. The default values specify a start time of 2:00 a.m. on the second Sunday in March, and a stop time of 2:00 a.m. on the first Sunday in November. The default summertime offset is 60 minutes.

g. Specify the month you want summertime settings to end. Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december. The default is november.

h. Specify the week you want the summertime settings to end. Valid entries are first, second, third, fourth, fifth, and last. The default is first.

i. Specify the day you want the summertime settings to end. Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

j. Specify the time you want summertime settings to end. The default is 02:00:00.

k. Specify the DST zone. The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+:,_/-]+$.

l. Specify the summertime offset. Specify the summertime offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian). The default is 60.

m. Enter **yes** to modify the system time zone.

n. Specify the standard time zone name. The zone name is a character string up to 24 characters long.

o. Specify the standard time zone offset. Specify the standard time zone offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian). The default is 0.

p. Enter **yes** if you want to use NTP. To use authenticated NTP, you need the NTP server IP address, the NTP key ID, and the NTP key value. If you do not have those at this time, you can configure NTP later. Otherwise, you can choose unauthenticated NTP.

Step 9 Enter **off**, **partial**, or **full** to participate in the SensorBase Network Participation:

- Off—No data is contributed to the SensorBase Network.
- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network except the attacker/victim IP addresses that you exclude.

The SensorBase Network Participation disclaimer appears. It explains what is involved in participating in the SensorBase Network.

Step 10 Enter **yes** to participate in the SensorBase Network.

```
The following configuration was entered.
service host
network-settings
host-ip 192.168.1.2/24, 192.168.1.1
host-name sensor
telnet-option disabled
sshv1-fallback disabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
dns-primary-server enabled
address 171.68.226.120
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.170
port 8080
exit
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month march
week-of-month second
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month november
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
exit
ntp-option enabled
ntp-keys 1 md5-key 8675309
ntp-servers 10.10.1.2 key-id 1
exit
service global-correlation
network-participation full
```

```
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
```

Step 11 Enter **2** to save the configuration (or **3** to continue with advanced setup using the CLI).

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 12 If you changed the time setting, enter **yes** to reboot the sensor.

For More Information

- For the procedure for obtaining the most recent service pack and signature update, see Obtaining Cisco IPS Software, page 26-1.
- For the procedures for continuing with advanced setup for all sensors, see Advanced Setup, page 25-7.

Advanced Setup

This section describes how to continue with Advanced Setup in the CLI for the sensor. It contains the following sections:

Appliance Advanced Setup

Note The currently supported Cisco IPS appliances are the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL.

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

Note Adding new subinterfaces is a two-step process. You first organize the interfaces when you edit the virtual sensor configuration. You then choose which interfaces and subinterfaces are assigned to which virtual sensors.

The interfaces change according to the appliance model, but the prompts are the same for all models.

To continue with advanced setup for the appliance, follow these steps:

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

Step 2 Enter the `setup` command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter `3` to access advanced setup.

Step 4 Specify the Telnet server status. The default is disabled.

Step 5 Specify the SSHv1 fallback setting. The default is disabled.

Step 6 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 7 Enter `yes` to modify the interface and virtual sensor configuration and to see the current interface configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Promiscuous:
   GigabitEthernet0/0
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs1
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs2
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 8 Enter `1` to edit the interface configuration.

Note The following options let you create and delete interfaces. You assign the interfaces to virtual sensors in the virtual sensor configuration. If you are using promiscuous mode for your interfaces and are not subdividing them by VLAN, no additional configuration is necessary.

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 9 Enter **2** to add inline VLAN pairs and display the list of available interfaces.

Caution The new VLAN pair is not automatically added to a virtual sensor.

```
Available Interfaces
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Step 10 Enter **1** to add an inline VLAN pair to GigabitEthernet 0/0, for example.

```
Inline Vlan Pairs for GigabitEthernet0/0
   None
```

Step 11 Enter a subinterface number and description.

```
Subinterface Number:
Description[Created via setup by user asmith]:
```

Step 12 Enter numbers for VLAN 1 and 2.

```
Vlan1[]: 200
Vlan2[]: 300
```

Step 13 Press **Enter** to return to the available interfaces menu.

Note Entering a carriage return at a prompt without a value returns you to the previous menu.

```
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Note At this point, you can configure another interface, for example, GigabitEthernet 0/1, for inline VLAN pair.

Step 14 Press **Enter** to return to the top-level interface editing menu.

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 15 Enter **4** to add an inline interface pair and see these options.

```
Available Interfaces
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3
```

Step 16 Enter the pair name, description, and which interfaces you want to pair.

```
Pair name: newPair
Description[Created via setup by user asmith:
Interface1[]: GigabitEthernet0/1
Interface2[]: GigabitEthernet0/2
Pair name:
```

Step 17 Press **Enter** to return to the top-level interface editing menu.

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 18 Press **Enter** to return to the top-level editing menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 19 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 20 Enter **2** to modify the virtual sensor configuration, vs0.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/3
   [2] GigabitEthernet0/0
  Inline Vlan Pair:
   [3] GigabitEthernet0/0:1  (Vlans: 200, 300)
  Inline Interface Pair:
   [4] newPair (GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

Step 21 Enter **3** to add inline VLAN pair GigabitEthernet0/0:1.

Step 22 Enter **4** to add inline interface pair NewPair.

Step 23 Press **Enter** to return to the top-level virtual sensor menu.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
```

```
  Event Action Rules: rules0
  Signature Definitions: sig0
  Inline Vlan Pair:
   GigabitEthernet0/0:1  (Vlans: 200, 300)
  Inline Interface Pair:
   newPair (GigabitEthernet0/1, GigabitEthernet0/2)

  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option: GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

Step 24 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 25 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 26 Enter **yes** to disable automatic threat prevention on all virtual sensors.

Step 27 Press **Enter** to exit the interface and virtual sensor configuration.

```
The following configuration was entered.
service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option disabled
sshv1-fallback disabled
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user asmith
vlan1 200
```

```
vlan2 300
exit
exit
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
physical-interfaces GigabitEthernet0/2
admin-state enabled
exit
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
inline-interfaces newPair
description Created via setup by user asmith
interface1 GigabitEthernet0/1
interface2 GigabitEthernet0/2
exit
exit
service analysis-engine
virtual-sensor newVs
description Created via setup by user cisco
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/0
exit
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 1
logical-interface newPair
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 28 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 29 Reboot the appliance.

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 30 Enter **yes** to continue the reboot.

Step 31 Apply the most recent service pack and signature update. You are now ready to configure your appliance for intrusion prevention.

For More Information

For the procedure for obtaining the most recent service pack and signature update, see Obtaining Cisco IPS Software, page 26-1.

ASA 5500-X IPS SSP Advanced Setup

Note The currently supported Cisco ASA adaptive security appliances with the IPS SSP are the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.

Note The ASA 5500-X IPS SSP is supported in ASA 8.6.1 and later.

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

To continue with advanced setup for the ASA 5500-X IPS SSP, follow these steps:

Step 1 Session in to the IPS using an account with administrator privileges.

```
asa# session ips
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the SSHv1 fallback setting. The default is disabled.

Step 6 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 7 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel 0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
```

```
Option:
```

Step 8 Enter `1` to edit the interface configuration.

Note You do not need to configure interfaces on the ASA 5500-X IPS SSP. You should ignore the modify interface default VLAN setting. The separation of traffic across virtual sensors is configured differently for the ASA 5500-X IPS SSP than for other sensors.

```
  [1] Modify interface default-vlan.
Option:
```

Step 9 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 10 Enter `2` to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 11 Enter `2` to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel 0/0
Add Interface:
```

Step 12 Enter `1` to add PortChannel 0/0 to virtual sensor vs0.

Note Multiple virtual sensors are supported. The adaptive security appliance can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign PortChannel 0/0. We recommend that you assign PortChannel 0/0 to vs0, but you can assign it to another virtual sensor if you want to.

Step 13 Press **Enter** to return to the main virtual sensor menu.

Step 14 Enter `3` to create a virtual sensor.

```
Name[]:
```

Step 15 Enter a name and description for your virtual sensor.

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
```

```
Option[2]:
```

Step 16 Enter **1** to use the existing anomaly-detection configuration, ad0.

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

Step 17 Enter **2** to create a signature-definition configuration file.

Step 18 Enter the signature-definition configuration name, **newSig**.

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

Step 19 Enter **1** to use the existing event-action-rules configuration, rules0.

Note If PortChannel 0/0 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

Step 20 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 21 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 22 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name asa-ips
telnet-option disabled
sshv1-fallback disabled
```

```
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 23 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 24 Reboot the ASA 5500-X IPS SSP.

```
asa-ips# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 25 Enter **yes** to continue the reboot.

Step 26 After reboot, log in to the sensor, and display the self-signed X.509 certificate (needed by TLS).

```
asa-ips# show tls fingerprint
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 27 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this ASA 5500-X IPS SSP with a web browser.

Step 28 Apply the most recent service pack and signature update. You are now ready to configure the ASA 5500-X IPS SSP for intrusion prevention.

For More Information

- For the procedure for obtaining the most recent service pack and signature update, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for enabling anomaly detection, see Enabling Anomaly Detection, page 13-4.

ASA 5585-X IPS SSP Advanced Setup

Note The ASA 5585-X IPS SSP is supported in ASA 8.2(4.4) and later as well as ASA 8.4(2) and later. It is not supported in ASA 8.3(*x*).

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

To continue with advanced setup for the ASA 5585-X IPS SSP, follow these steps:

Step 1 Session in to the ASA 5585-X IPS SSP using an account with administrator privileges.

```
asa# session 1
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the SSHv1 fallback setting. The default is disabled.

Step 6 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 7 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 8 Enter **1** to edit the interface configuration.

Note You do not need to configure interfaces on the ASA 5585-X IPS SSP. You should ignore the modify interface default VLAN setting. The separation of traffic across virtual sensors is configured differently for the ASA 5585-X IPS SSP than for other sensors.

```
  [1] Modify interface default-vlan.
Option:
```

Step 9 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 10 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 11 Enter **2** to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel0/0
Add Interface:
```

Step 12 Enter **1** to add PortChannel 0/0 to virtual sensor vs0.

Note Multiple virtual sensors are supported. The adaptive security appliance can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign PortChannel 0/0. We recommend that you assign PortChannel 0/0 to vs0, but you can assign it to another virtual sensor if you want to.

Step 13 Press **Enter** to return to the main virtual sensor menu.

Step 14 Enter **3** to create a virtual sensor.

```
Name[]:
```

Step 15 Enter a name and description for your virtual sensor.

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

Step 16 Enter **1** to use the existing anomaly-detection configuration, ad0.

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

Step 17 Enter **2** to create a signature-definition configuration file.

Step 18 Enter the signature-definition configuration name, **newSig**.

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

Step 19 Enter **1** to use the existing event action rules configuration, rules0.

Note If PortChannel 0/0 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

Step 20 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 21 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 22 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name ips-ssp
telnet-option disabled
sshv1-fallback disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
```

```
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 23 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 24 Reboot the ASA 5585-X IPS SSP.

```
ips-ssp# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 25 Enter **yes** to continue the reboot.

Step 26 After reboot, log in to the sensor, and display the self-signed X.509 certificate (needed by TLS).

```
ips-ssp# show tls fingerprint
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 27 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this ASA 5585-X IPS SSP with a web browser.

Step 28 Apply the most recent service pack and signature update. You are now ready to configure your ASA 5585-X IPS SSP for intrusion prevention.

For More Information

- For the procedure for obtaining the most recent service pack and signature update, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for enabling anomaly detection, see Enabling Anomaly Detection, page 13-4.

Verifying Initialization

Note The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS version you have installed.

To verify that you initialized your sensor, follow these steps:

Step 1 Log in to the sensor.

Step 2 View your configuration.

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Fri Apr 19 19:01:05 2013
! ------------------------------
! Version 7.2(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S697.0   2013-02-15
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
inline-interfaces pair0
interface1 GigabitEthernet0/0
interface2 GigabitEthernet0/1
exit
bypass-mode auto
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.106.133.159/23,10.106.132.1
host-name q4360-159
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
```

```
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
websession-inactivity-timeout 3600
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
logical-interface pair0
exit
exit
```

Note You can also use the **more current-config** command to view your configuration.

Step 3 Display the self-signed X.509 certificate (needed by TLS).

```
sensor# show tls fingerprint
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 4 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when connecting to this sensor with a web browser.

For More Information

For the procedure for logging in to the sensor, see Chapter 24, “Logging In to the Sensor.”

Obtaining Software

This chapter describes how to obtain and install the latest Cisco IPS software, and contains the following topics:

IPS 7.2(*x*)E4 File List

The currently supported IPS 7.2(*x*)E4 versions are 7.2(1)E4 and IPS 7.2(2)E4. For a list of the specific IPS filenames and the IPS versions that each sensor supports, refer to the Release Notes for your IPS version found at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_release_notes_list.html

Obtaining Cisco IPS Software

You can find major and minor updates, service packs, signature and signature engine updates, system and recovery files, firmware upgrades, and Readmes on the Download Software site on Cisco.com. Signature updates are posted to Cisco.com approximately every week, more often if needed. Service packs are posted to Cisco.com in a release train format, a new release every three months. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.

You must have an account with cryptographic access before you can download software. You set this account up the first time you download IPS software from the Download Software site.

Note You must be logged in to Cisco.com to download software. You must have an active IPS maintenance contract and a Cisco.com password to download software. You must have a sensor license to apply signature updates.

Downloading Cisco IPS Software

To download software on Cisco.com, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 From the Support drop-down menu, choose **Download Software**.

Step 3 Under Select a Software Product Category, choose **Security Software**.

Step 4 Choose **Intrusion Prevention System (IPS)**.

Step 5 Enter your username and password.

Step 6 In the Download Software window, choose **IPS Appliances > Cisco Intrusion Prevention System** and then click the version you want to download.

Note You must have an IPS subscription service license to download software.

Step 7 Click the type of software file you need. The available files appear in a list in the right side of the window. You can sort by file name, file size, memory, and release date. And you can access the Release Notes and other product documentation.

Step 8 Click the file you want to download. The file details appear.

Step 9 Verify that it is the correct file, and click **Download**.

Step 10 Click **Agree** to accept the software download rules. The File Download dialog box appears. The first time you download a file from Cisco.com, you must fill in the Encryption Software Export Distribution Authorization form before you can download the software.

a. Fill out the form and click **Submit**. The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.

b. Read the policy and click **I Accept**. The Encryption Software Export/Distribution Form appears.

If you previously filled out the Encryption Software Export Distribution Authorization form, and read and accepted the Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again.

Step 11 Open the file or save it to your computer.

Step 12 Follow the instructions in the Readme or the Release Notes to install the update.

For More Information

- For more information about IPS maintenance contracts and the procedure for obtaining and installing the license key, see Configuring Licensing, page 20-12.
- For an explanation of the IPS file versioning scheme, see IPS Software Versioning, page 26-3.

IPS Software Versioning

When you download IPS software images from Cisco.com, you should understand the versioning scheme so that you know which files are base files, which are cumulative, and which are incremental.

Note The software version installed on your sensor is listed on the Sensor Information tab in the Device List pane in IME.

Major Update

A major update contains new functionality or an architectural change in the product. For example, the Cisco IPS 7.2 base version includes everything (except deprecated features) since the previous major release (the minor update features, service pack fixes, and signature updates) plus any new changes. Major update 7.2(1) requires 5.1(6) and later. With each major update there are corresponding system and recovery packages.

Note The 7.2(1) major update is used to upgrade 5.1(6) and later sensors to 7.2(1) If you are reinstalling 7.2(1) on a sensor that already has 7.2(1) installed, use the system image or recovery procedures rather than the major update.

Minor Update

A minor update is incremental to the major version. Minor updates are also base versions for service packs. The first minor update for 7.2 is 7.3. Minor updates are released for minor enhancements to the product. Minor updates contain all previous minor features (except deprecated features), service pack fixes, signature updates since the last major version, and the new minor features being released. You can install the minor updates on the previous major or minor version (and often even on earlier versions). The minimum supported version needed to upgrade to the newest minor version is listed in the Readme that accompanies the minor update. With each minor update there are corresponding system and recovery packages.

Service Pack

A service packs is cumulative following a base version release (minor or major). Service packs are released in a train release format with several new features per train. Service packs contain all service pack fixes since the last base version (minor or major) and the new features and defect fixes being released. Service packs require the minor version. The minimum supported version needed to upgrade to the newest service pack is listed in the Readme that accompanies the service pack. Service packs also include the latest engine update. For example, if service pack 7.2(3) is released, and E4 is the latest engine level, the service pack is released as 7.2(3)E4.

Patch Release

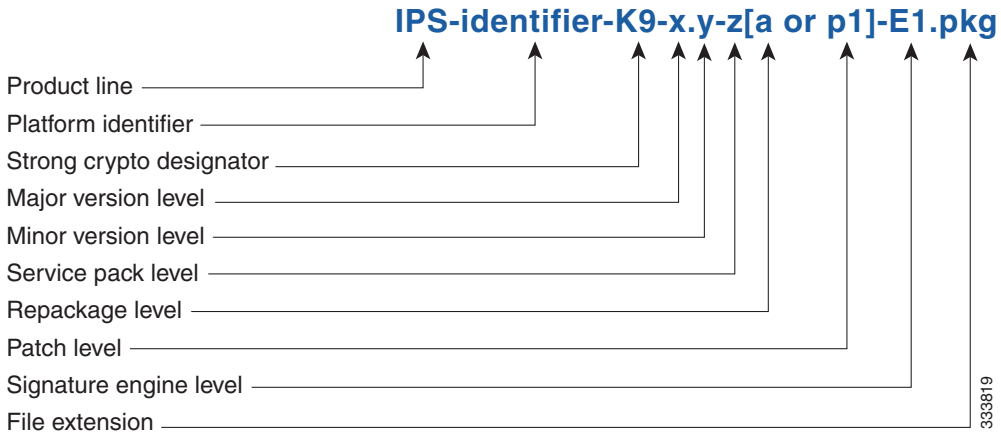
A patch release is used to address defects that are identified in the upgrade binaries after a software release. Rather than waiting until the next major or minor update, or service pack to address these defects, a patch can be posted. Patches include all prior patch releases within the associated service pack level. The patches roll into the next official major or minor update, or service pack.

Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 7.2(1p1) requires 7.2(1).

Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 7.2(1p1) to 7.2(1p2) without first uninstalling 7.2(1p1).

Figure 26-1 illustrates what each part of the IPS software file represents for major and minor updates, service packs, and patch releases.

Figure 26-1 IPS Software File Name for Major and Minor Updates, Service Packs, and Patch Releases



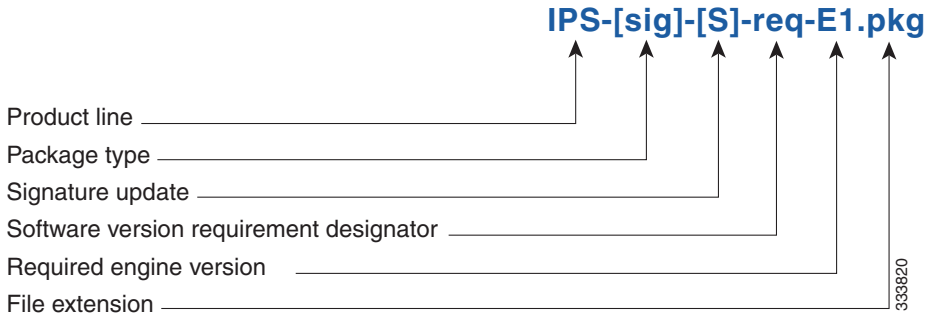
Signature Update and Signature Engine Update

A signature update is a package file containing a set of rules designed to recognize malicious network activities. Signature updates are released independently from other software updates. Each time a major or minor update is released, you can install signature updates on the new version and the next oldest version for a period of at least six months. Signature updates are dependent on a required signature engine version. Because of this, a *req* designator lists the signature engine required to support a particular signature update.

A signature engine update is an executable file containing binary code to support new signature updates. Signature engine files require a specific service pack, which is also identified by the *req* designator.

Figure 26-2 illustrates what each part of the IPS software file represents for signature updates.

Figure 26-2 IPS Software File Name for Signature Updates and Signature Engine Updates



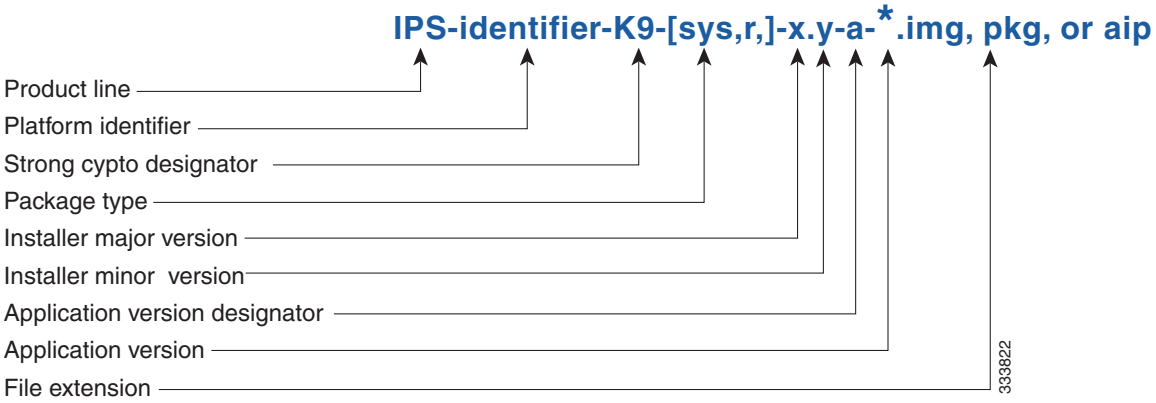
Recovery and System Image Files

Recovery and system image files contain separate versions for the installer and the underlying application. The installer version contains a major and minor version field. The major version is incremented by one of any major changes to the image installer, for example, switching from .tar to rpm or changing kernels. The minor version can be incremented by any one of the following:

- Minor change to the installer, for example, a user prompt added.
- Repackages require the installer minor version to be incremented by one if the image file must be repackaged to address a defect or problem with the installer.

Figure 26-3 illustrates what each part of the IPS software file represents for recovery and system image filenames.

Figure 26-3 IPS Software File Name for Recovery and System Image Files



For More Information

For a table listing the types of files with examples of filenames and corresponding software releases, see Software Release Examples, page 26-5.

Software Release Examples

Table 26-1 lists Cisco IPS software release examples.

Table 26-1 Cisco IPS Software Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Signature and signature engine update[1]	Weekly for signatures, as needed for signature engine	sig	S669	IPS-sig-S669-req-E4.pkg
Service packs[2]	Every three months	—	7.2(2)	IPS-*identifier*-K9-7.2-2-E4.pkg
Minor version update[3]	Annually	—	7.2(1)	IPS-*identifier*-K9-7.2-1-E4.pkg
Major version update[4]	Annually	—	8.0(1)	IPS-*identifier*-K9-8.0-1-E4.pkg
Patch release[5]	As needed	patch	7.2(1p1)	IPS-*identifier*-K9-patch-7.2-1pl-E4.pkg

Table 26-1 Cisco IPS Software Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Recovery package[6]	Annually or as needed	r	1.1-7.2(1)	IPS-*identifier*-K9-r-1.1-a-7.2-1-E4.pkg
System image[7]	Annually	sys	Separate file per sensor platform	IPS-SSP_60-K9-sys-1.1-a-7.2-2-E4.img IPS-4345-K9-sys-1.1-a-7.2-2-E4.img IPS-SSP_5545-K9-sys-1.1-a-7.2-2-E4.aip IPS-4510-K9-sys-1.1-a-7.2-2-E4.img

1. Signature updates include the latest cumulative IPS signatures. Signature engine updates add new engines or engine parameters that are used by new signatures in later signature updates.
2. Service packs include new features and defect fixes.
3. Minor versions include new minor version features and/or minor version functionality.
4. Major versions include new major version functionality or new architecture.
5. Patch releases are for interim fixes.
6. The r 1.1 can be revised to r 1.2 if it is necessary to release a new recovery package that contains the same underlying application image. If there are defect fixes for the installer, for example, the underlying application version may still be 7.2(3), but the recovery partition image will be r 1.2.
7. The system image includes the combined recovery and application image used to reimage an entire sensor.

Table 26-2 describes the platform identifiers used in platform-specific names.

Table 26-2 Platform Identifiers

Sensor Family	Identifier
ASA 5500-X series	SSP_5512 SSP_5515 SSP_5525 SSP_5545 SSP_5555
ASA 5585-X series	SSP_10 SSP_20 SSP_40 SSP_60
IPS 4345 series	4345
IPS 4360 series	4360
IPS 4510 series	4510
IPS 4520 series	4520

For More Information

- For instructions on how to access these files on Cisco.com, see Obtaining Cisco IPS Software, page 26-1
- For procedures for installing the various software files, see Chapter 27, "Upgrading, Downgrading, and Installing System Images."

Accessing IPS Documentation

You can find IPS documentation at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

Or to access IPS documentation from Cisco.com, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 Click **Support**.

Step 3 Under Support at the bottom of the page, click **Documentation**.

Step 4 Choose **Products > Security > Intrusion Prevention System (IPS) > IPS Appliances > Cisco IPS 4200 Series Sensors**. The Cisco IPS 4200 Series Sensors page appears. All of the most up-to-date IPS documentation is on this page.

Note Although you will see references to other IPS documentation sites on Cisco.com, this is the site with the most complete and up-to-date IPS documentation.

Step 5 Click one of the following categories to access Cisco IPS documentation:

- **Download Software**—Takes you to the Download Software site.

  Note You must be logged into Cisco.com to access the software download site.

- **Release and General Information**—Contains documentation roadmaps and release notes.
- **Reference Guides**—Contains command references and technical references.
- **Design**—Contains design guide and design tech notes.
- **Install and Upgrade**—Contains hardware installation and regulatory guides.
- **Configure**—Contains configuration guides for IPS CLI, IDM, and IME.
- **Troubleshoot and Alerts**—Contains TAC tech notes and field notices.

Cisco Security Intelligence Operations

The Cisco Security Intelligence Operations site on Cisco.com provides intelligence reports about current vulnerabilities and security threats. It also has reports on other security topics that help you protect your network and deploy your security systems to reduce organizational risk.

You should be aware of the most recent security threats so that you can most effectively secure and manage your network. Cisco Security Intelligence Operations contains the top ten intelligence reports listed by date, severity, urgency, and whether there is a new signature available to deal with the threat.

Cisco Security Intelligence Operations contains a Security News section that lists security articles of interest. There are related security tools and links.

You can access Cisco Security Intelligence Operations at this URL:

http://tools.cisco.com/security/center/home.x

Cisco Security Intelligence Operations is also a repository of information for individual signatures, including signature ID, type, structure, and description.

You can search for security alerts and signatures at this URL:

http://tools.cisco.com/security/center/search.x

Upgrading, Downgrading, and Installing System Images

This chapter describes how to upgrade, downgrade, and install system images. It contains the following sections:

Upgrade Notes and Caveats

Pay attention to the following upgrade notes and caveats when upgrading your sensor:

- Anomaly detection has been disabled by default. If you did not configure the operation mode manually before the upgrade, it defaults to inactive after you upgrade to IPS 7.2(1)E4 or later. If you configured the operation mode to detect, learn, or inactive, the tuned value is preserved after the upgrade.
- You must have a valid maintenance contract per sensor to download software upgrades from Cisco.com.
- You must be running IPS 7.1(1)E4 to upgrade to IPS 7.2(x)E4 or later.
- This service pack automatically reboots the sensor to apply the changes. During reboot, inline network traffic is disrupted.
- You cannot uninstall IPS 7.2(x)E4. To revert to a previous version, you must reimage the sensor using the appropriate system image file.
- You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.2 to 7.1. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.1, you must reimage the sensor.

- After upgrading to 7.2(x)E4, you cannot automatically update the sensor to IPS 7.3(1) E4 using the CLI, IDM, or IME, because SNMPv3 support is not available in IPS 7.3(1)E4. You can however, manually update to 7.3(1)E4 using the CLI, which warns you that the SNMP configuration will be removed from the sensor.
- If a client connecting to a sensor that is using SSH does not support SSHv2, or if SSHv2 is disabled, the management connectivity is lost after upgrading to IPS 7.2(x)E4 from any 7.1(x) version because SSHv1 is disabled by default in IPS 7.2(x)E4.
- You cannot downgrade the sensor using the recovery partition. To downgrade to an earlier version, you must install the appropriate system image file (.img file).
- All user configuration settings are lost when you install the system image. Before trying to recover the sensor by installing the system image, try to recover by using the **recover application-partition** command or by selecting the recovery partition during sensor bootup.
- For IPS 7.2(1)E4, while executing an immediate upgrade, you cannot use the IDM, IME, or CLI, or start any new sessions until the upgrade is complete. For IPS 7.2(2)E4 and later, you can use the IDM, IME, and CLI immediately after you begin an automatic update because the automatic update is now executed as background process.

For More Information

- For the procedure for accessing downloads on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for using the **upgrade** command to upgrade the sensor, see Upgrading the Sensor, page 27-3.
- For the procedure for configuring automatic upgrades on the sensor, see Configuring Automatic Upgrades, page 27-8.
- For the procedure for using the **recover** command, see Recovering the Application Partition, page 27-14.
- For the procedure for installing the IPS 4345 and IPS 4360 system image, see Installing the IPS 4300 Series System Images, page 27-17.
- For the procedure for installing the IPS 4510 and IPS 4520 system image, see Installing the IPS 4500 Series System Images, page 27-20.
- For the procedure for installing the ASA 5500-X IPS SSP system image, see Installing the ASA 5500-X IPS SSP System Image, page 27-23.
- For the procedure for installing the ASA 5585-X IPS SSP system image, see Installing the ASA 5585-X IPS SSP System Image, page 27-24.

Understanding Upgrades, Downgrades, and System Images

You can upgrade and downgrade the software on the sensor. Upgrading applies a service pack, signature update, signature engine update, minor version, major version, or recovery partition file. Downgrading removes the last applied service pack or signature update from the sensor.

You can recover the application partition image on your sensor if it becomes unusable. Using the **recover** command lets you retain your host settings while other settings revert to the factory defaults.

To install a new system image on the sensor, use ROMMON, the bootloader file, or the maintenance partition depending on which platform you have. When you install a new system image on your sensor, all accounts are removed and the default cisco account is reset to use the default password **cisco**. After installing the system image, you must initialize the sensor again.

After you reimage and initialize your sensor, upgrade your sensor with the most recent service pack, signature update, signature engine update, minor update, major update, and recovery partition files.

Pay attention to the following:

- You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.2 to 7.1. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.1, you must reimage the sensor.
- After you upgrade any IPS software on your sensor, you must restart the IME to see the latest software features.
- You cannot downgrade the sensor using the recovery partition. To downgrade to an earlier version, you must install the appropriate system image file (.img file).
- During a signature upgrade all signature configurations are retained, both the signature tunings as well as the custom signatures. During a signature downgrade the current signature configuration is replaced with the old signature configuration. So if the last signature set had custom signatures and/or signature tunings, these are restored during the downgrade.

For More Information

- For the procedure for initializing the sensor, see Chapter 25, "Initializing the Sensor."
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.
- For the procedures for reimaging the various sensors, see Installing System Images, page 27-15.

Supported FTP and HTTP/HTTPS Servers

The following FTP servers are supported for IPS software updates:

- WU-FTPD 2.6.2 (Linux)
- Solaris 2.8
- Sambar 6.0 (Windows 2000)
- Serv-U 5.0 (Windows 2000)
- MS IIS 5.0 (Windows 2000)

The following HTTP/HTTPS servers are supported for IPS software updates:

- CSM - Apache Server (Tomcat)
- CSM - Apache Server (JRun)

For More Information

- For the procedure for downloading IPS software updates from Cisco.com, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for configuring automatic updates, see Configuring Automatic Upgrades, page 27-8.

Upgrading the Sensor

Note For the IME procedure for upgrading the sensor, see Manually Updating the Sensor, page 20-25.

This section explains how to use the **upgrade** command to upgrade the software on the sensor. It contains the following topics:

IPS 7.2 Upgrade Files

The currently supported IPS 7.2(*x*) versions are 7.2(1)E4 and 7.2(2)E4. For a list of the specific IPS filenames and the IPS versions that each sensor supports, refer to the Release Notes for your IPS version found at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_release_notes_list.html

For More Information

For the procedure for obtaining IPS files on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.

Upgrade Notes and Caveats

For a list of the upgrade notes and caveats for each IPS version, refer to the Release Notes for your IPS version found at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_release_notes_list.html

Manually Upgrading the Sensor

Caution You must log in to Cisco.com using an account with cryptographic privileges to download software. The first time you download software on Cisco.com, you receive instructions for setting up an account with cryptographic privileges.

Note During a signature upgrade all signature configurations are retained, both the signature tunings as well as the custom signatures. During a signature downgrade the current signature configuration is replaced with the old signature configuration. So if the last signature set had custom signatures and/or signature tunings, these are restored during the downgrade.

Caution Do not change the filename. You must preserve the original filename for the sensor to accept the update.

Note For the IME procedure for upgrading the sensor, see Manually Updating the Sensor, page 20-25.

Use the **upgrade** *source-url* command to apply service pack, signature update, engine update, minor version, major version, or recovery partition file upgrades. The following options apply:

- *source-url*—Specifies the location of the source file to be copied:
  - ftp:—Source URL for an FTP network server. The syntax for this prefix is:

    ftp://[[username@]location][/relativeDirectory]/filename

    ftp://[[username@]location][//absoluteDirectory]/filename

    Note You are prompted for a password.

  - scp:—Source URL for the SCP network server. The syntax for this prefix is:

    scp://[[username@]location][/relativeDirectory]/filename

    scp://[[username@]location][//absoluteDirectory]/filename

    Note You are prompted for a password. You must add the remote host to the SSH known hosts list.

  - http:—Source URL for the web server. The syntax for this prefix is:

    http://[[username@]location][/directory]/filename

    Note The directory specification should be an absolute path to the desired file.

  - https:—Source URL for the web server. The syntax for this prefix is:

    https://[[username@]location][/directory]/filename

    Note The directory specification should be an absolute path to the desired file. The remote host must be a TLS trusted host.

Upgrading the Sensor

Note The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS version you have installed.

To upgrade the sensor, follow these steps:

Step 1 Download the appropriate file to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Upgrade the sensor.

```
sensor(config)# upgrade url/IPS-SSP_10-K9-7.2-1-E4.pkg
```

The URL points to where the update file is located, for example, to retrieve the update using FTP, enter the following:

```
sensor(config)# upgrade ftp://username@ip_address//directory/IPS-SSP_10-K9-7.2-1-E4.pkg
```

Step 5 Enter the password when prompted.

```
Enter password: ********
```

Step 6 Enter **yes** to complete the upgrade.

Note Major updates, minor updates, and service packs may force a restart of the IPS processes or even force a reboot of the sensor to complete installation.

Note The operating system is reimaged and all files that have been placed on the sensor through the service account are removed.

Step 7 Verify your new sensor version.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0        2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
No license present
Sensor up-time is 3 days.
Using 14470M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.1M out of 376.1M bytes of available disk space (24%
 usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

  IPS-K9-7.2-1-E4   11:17:07 UTC Thu Jan 10 2013
```

```
Recovery Partition Version 1.1 - 7.2(1)E4

Host Certificate Valid from: 17-Apr-2013 to 18-Apr-2015
sensor#
```

For More Information

- For the location of the specific IPS upgrade filenames for each IPS version, see IPS 7.2 Upgrade Files, page 27-4.
- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 27-3.
- For the procedure for locating software on Cisco.com and obtaining an account with cryptographic privilege, see Obtaining Cisco IPS Software, page 26-1.

Upgrading the Recovery Partition

Note Recovery partition images are generated for major and minor updates and only in rare situations for service packs or signature updates.

Note You cannot downgrade the sensor using the recovery partition. To downgrade to an earlier version, you must install the appropriate system image file (.img file).

Use the **upgrade** command to upgrade the recovery partition with the most recent version so that it is ready if you need to recover the application partition on your sensor. Recovery partition images are generated for major and minor updates and only in rare situations for service packs or signature updates.

To upgrade the recovery partition on your sensor, follow these steps:

Step 1 Download the appropriate recovery partition image file to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Caution Some browsers add an extension to the filename. The filename of the saved file must match what is displayed on the download page or you cannot use it to upgrade the recovery partition.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Upgrade the recovery partition.

```
sensor(config)#
upgrade scp://user@server_ipaddress//upgrade_path/IPS-SSP_10-K9-r-1.1-a-7.2-1-E4.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-SSP_10-K9-r-1.1-a-7.2-1-E4.pkg
```

Step 5 Enter the server password. The upgrade process begins.

Note This procedure only reimages the recovery partition. The application partition is not modified by this upgrade. To reimage the application partition after the recovery partition, use the **recover application-partition** command.

For More Information

- For the location of the list of specific recovery image files, see IPS 7.2 Upgrade Files, page 27-4.
- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 27-3.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for using the **recover** command, see Upgrading the Recovery Partition, page 27-7.

Configuring Automatic Upgrades

This section describes how to configure the sensor to automatically look for upgrades in the upgrade directory. It contains the following topics:

Understanding Automatic Upgrades

Caution The IPS address has been changed to cisco.com in the URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new address.

You can configure the sensor to look for new upgrade files in your upgrade directory automatically. For example, several sensors can point to the same remote FTP server directory with different update schedules, such as every 24 hours, or Monday, Wednesday, and Friday at 11:00 pm.

You specify the following information to schedule automatic upgrades:

- Server IP address
- Path of the directory on the file server where the sensor checks for upgrade files
- File copy protocol (SCP or FTP)
- Username and password
- Upgrade schedule

You must download the software upgrade from Cisco.com and copy it to the upgrade directory before the sensor can poll for automatic upgrades.

For More Information

- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for adding the SCP server to the SSH known hosts list, see Configuring Known Host RSA1 Keys, page 15-8.

Automatically Upgrading the Sensor

Note For the IME procedure for automatically upgrading the sensor, see Configuring Automatic Update, page 20-20.

Use the **auto-upgrade-option enabled** command in the service host submode to configure automatic upgrades.

The following options apply:

- **cisco-server {disabled | enabled}**—Enables automatic signature and engine updates from Cisco.com.
- **cisco-url** *cisco_url*—Specifies the Cisco server locator service. You do not need to change this unless the www.cisco.com IP address changes.
- **default**— Sets the value back to the system default setting.
- **directory** *directory*— Specifies the directory where upgrade files are located on the file server. A leading '/' indicates an absolute path.
- **file-copy-protocol {ftp | scp}**— Specifies the file copy protocol used to download files from the file server.

  Note If you use SCP, you must use the **ssh host-key** command to add the server to the SSH known hosts list so the sensor can communicate with it through SSH.

- **ip-address** *ip_address*—Specifies the IP address of the file server.
- **password** *password*—Specifies the user password for Cisco server authentication.
- **schedule-option**—Specifies the schedules for when Cisco server automatic upgrades occur. Calendar scheduling starts upgrades at specific times on specific days. Periodic scheduling starts upgrades at specific periodic intervals.
  - **calendar-schedule**—Configures the days of the week and times of day that automatic upgrades will be performed.
  - **days-of-week**—Specifies the days of the week on which auto-upgrades will be performed. You can select multiple days: *sunday* through *saturday* are the valid values.
  - **no**—Removes an entry or selection setting.
  - **times-of-day**—Specifies the times of day at which auto-upgrades will begin. You can select multiple times. The valid value is *hh:mm[:ss]*.
  - **periodic-schedule**—Specifies the time that the first automatic upgrade should occur, and how long to wait between automatic upgrades.
  - **interval**—Specifies the number of hours to wait between automatic upgrades. Valid values are 0 to 8760.

  - **start-time**—Specifies the time of day to start the first automatic upgrade. The valid value is *hh:mm[:ss]*.
- **user-name** *user_name*—Specifies the username for server authentication.
- **user-server {disabled | enabled}**—Enables automatic upgrades from a user-defined server.

Configuring Automatic Upgrades

If you get an unauthorized error message while configuring an automatic update, make sure you have the correct ports open on any firewalls between the sensor and Cisco.com. For example, you need port 443 for the initial automatic update connection to www.cisco.com, and you need port 80 to download the chosen package from a Cisco file server. The IP address may change for the Cisco file server, but you can find it in the lastDownloadAttempt section in the output of the **show statistics host** command.

Caution The IPS address has been changed to cisco.com in the URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new address.

Note To check the status of the last automatic update or the next scheduled automatic update, run the **show statistics host** command and check the Auto Update Statistics section.

To schedule automatic upgrades, follow these steps:

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

Step 2 Enter automatic upgrade submode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# auto-upgrade
sensor(config-hos-aut)#
```

Step 3 Configure the sensor to automatically look for new upgrades either on Cisco.com or on your file server:

a. On Cisco.com. Continue with Step 4.

```
sensor(config-hos-aut)# cisco-server enabled
```

b. From your server.

```
sensor(config-hos-aut)# user-server enabled
```

c. Specify the IP address of the file server.

```
sensor(config-hos-ena)# ip-address 10.1.1.1
```

d. Specify the directory where the upgrade files are located on the file server.

```
sensor(config-hos-ena)# directory /tftpboot/sensor_updates
```

e. Specify the file server protocol.

```
sensor(config-hos-ena)# file-copy-protocol ftp
```

Note If you use SCP, you must use the **ssh host-key** command to add the server to the SSH known hosts list so the sensor can communicate with it through SSH.

Step 4 Specify the username for authentication.

```
sensor(config-hos-ena)# user-name tester
```

Step 5 Specify the password of the user.

```
sensor(config-hos-ena)# password
Enter password[]: ******
Re-enter password: ******
```

Step 6 Specify the scheduling:

a. For calendar scheduling (starts upgrades at specific times on specific day):

```
sensor(config-hos-ena)# schedule-option calendar-schedule
sensor(config-hos-ena-cal)# days-of-week sunday
sensor(config-hos-ena-cal)# times-of-day 12:00:00
```

b. For periodic scheduling (starts upgrades at specific periodic intervals):

```
sensor(config-hos-ena)# schedule-option periodic-schedule
sensor(config-hos-ena-per)# interval 24
sensor(config-hos-ena-per)# start-time 13:00:00
```

Step 7 Verify the settings.

```
sensor(config-hos-ena)# show settings
   enabled
   ----------------------------------------------
      schedule-option
      ---------------------------------------------
         periodic-schedule
         ---------------------------------------------
            start-time: 13:00:00
            interval: 24 hours
         ---------------------------------------------
      ---------------------------------------------
      ip-address: 10.1.1.1
      directory: /tftpboot/update/6.1_dummy_updates
      user-name: tester
      password: <hidden>
      file-copy-protocol: ftp default: scp
   ----------------------------------------------
sensor(config-hos-ena)#
```

Step 8 Exit automatic upgrade submode.

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

Step 9 Press **Enter** to apply the changes or type **no** to discard them.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 27-3.
- For the procedure for adding the SCP server to the SSH known hosts list, see Defining Known Host RSA1 Keys, page 15-9.

Applying an Immediate Update

Caution For IPS 7.2(1)E4, while executing an immediate upgrade, you cannot use the IDM, IME, or CLI, or start any new sessions until the upgrade is complete. For IPS 7.2(2)E4 and later, you can use the IDM, IME, and CLI immediately after you begin an automatic update because the automatic update is now executed as background process.

Use the **autoupdatenow** command to remove perform an immediate update on the sensor. You receive a warning that this command performs an update on the sensor immediately. After executing this command, disable the **user-server/cisco-server** options in the auto-upgrade settings in the service host submode, if you do not want scheduled automatic updates.

Note You must have either a DNS or HTTP proxy server configured to download automatic updates from cisco.com.

Note You must have automatic update configured and a valid license to apply updates.

To perform an immediate update on the sensor, follow these steps:

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

Step 2 Start immediate automatic update.

```
sensor# autoupdatenow
Warning: Executing this command will perform an auto-upgrade on the sensor immediately.
Before executing this command, you must have a valid license to apply the Signature
AutoUpdates and auto-upgrade settings configured.After executing this command please
disable user-server/cisco-server inside 'auto-upgrade' settings, if you don't want
scheduled auto-updates
Continue? []:
```

Step 3 Enter **yes** to continue. The update is applied.

For More Information

- For the procedure for configuring automatic update, see Configuring Automatic Upgrades, page 27-8.
- For the procedure for configuring DNS and HTTP proxy servers, see Configuring Network Settings, page 6-3.

Downgrading the Sensor

Caution You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.2 to 7.1. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.1, you must reimage the sensor.

Note You cannot downgrade the sensor using the recovery partition. To downgrade to an earlier version, you must install the appropriate system image file (.img file).

Use the **downgrade** command to remove the last applied signature upgrade or signature engine upgrade from the sensor. The signature upgrade includes threat profiles. When you downgrade the signature update, the threat profile reverts to the one found in the previous signature upgrade.

To remove the last applied signature update or signature engine update from the sensor, follow these steps:

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

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Downgrade the sensor.

```
sensor(config)# downgrade
Warning: Executing this command will downgrade the system to IPS-K9-7.2-1-E4.
Configuration changes made since the last upgrade will be lost and the system may be
rebooted. Signature threat profile mapping to signature instances will be reverted to the
previous configuration.
Continue with downgrade? []: yes

Broadcast Message from root@qa-ff-4510-133-163
        (somewhere) at 23:47 ...

Un-installing IPS-sig-S750-req-E4.



Broadcast Message from root@qa-ff-4510-133-163
        (somewhere) at 23:47 ...

Un-install complete.
sensor(config)# exit
sensor#
```

Step 4 Display the current version after the downgrade.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0        2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
No license present
Sensor up-time is 3 days.
Using 14470M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.1M out of 376.1M bytes of available disk space (24%
 usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
```

```
 usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

* IPS-K9-7.2-1-E4       07:40:07 UTC Sun Jan 20 2013
  IPS-sig-S750-req-E4.pkg   16:57:01 UTC Sat Jan 11 2014

Recovery Partition Version 1.1 - 7.2(1)E4

Host Certificate Valid from: 10-Jan-2014 to 11-Jan-2016

sensor#
```

Step 5 If there is no recently applied service pack or signature update, the **downgrade** command is not available.

```
sensor(config)# downgrade
No downgrade available.
sensor(config)#
```

Recovering the Application Partition

You can recover the application partition image for the sensor if it becomes unusable. Some network configuration information is retained when you use this method, which lets you have network access after the recovery is performed. Use the **recover application-partition** command to boot to the recovery partition, which automatically recovers the application partition on your sensor. If you have upgraded your recovery partition to the most recent version before you recover the application partition image, you can install the most up-to-date software image.

Because you can execute the **recover application-partition** command through a Telnet or SSH connection, we recommend using this command to recover sensors that are installed at remote locations.

Note When you reconnect to the sensor after recovery, you must log in with the default username and password **cisco**.

Recovering the Application Partition Image

To recover the application partition image, follow these steps:

Step 1 Download the recovery partition image file to an FTP, HTTP, or HTTPS server that is accessible from your sensor.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Recover the application partition image.

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all applications and re-image the node to
version 7.1(x)E4. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:
```

Step 5 Enter **yes** to continue. Shutdown begins immediately after you execute the **recover** command. Shutdown can take a while, and you will still have access to the CLI, but access will be terminated without warning.

The application partition is reimaged using the image stored on the recovery partition. You must now initialize the sensor with the **setup** command.The IP address, netmask, access lists, time zone, and offset are saved and applied to the reimaged application partition. If you executed the **recover application-partition** command remotely, you can SSH to the sensor with the default username and password (**cisco/cisco**) and then initialize the sensor again with the **setup** command. You cannot use Telnet until you initialize the sensor because Telnet is disabled by default.

For More Information

- For the location for the list of application partition image files, see IPS 7.2 Upgrade Files, page 27-4.
- For more information about TFTP servers, see TFTP Servers, page 27-16.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for using the **setup** command, see Basic Sensor Setup, page 25-4.
- For the procedure for upgrading the recovery partition to the most recent version, see Upgrading the Recovery Partition, page 27-7.

Installing System Images

Caution All user configuration settings are lost when you install the system image. Before trying to recover the sensor by installing the system image, try to recover by using the **recover application-partition** command or by selecting the recovery partition during sensor bootup.

This section contains the procedures for installing system images on the appliances and modules. It contains the following topics:

- Installing the ASA 5500-X IPS SSP System Image, page 27-23
- Installing the ASA 5585-X IPS SSP System Image, page 27-24

ROMMON

Some Cisco sensors include a preboot CLI called ROMMON, which lets you boot images on sensors where the image on the primary device is missing, corrupt, or otherwise unable to boot the normal application. ROMMON is particularly useful for recovering remote sensors as long as the serial console port is available.

Access to ROMMON is available only through the serial console port, a Cisco-standard asynchronous RS-232C DTE available in an RJ-45F connector on the sensor chassis. The serial port is configured for 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

For More Information

For the procedure for using a terminal server, see Connecting an Appliance to a Terminal Server, page 27-16.

TFTP Servers

ROMMON uses TFTP to download an image and launch it. TFTP does not address network issues such as latency or error recovery. It does implement a limited packet integrity check so that packets arriving in sequence with the correct integrity value have an extremely low probability of error. But TFTP does not offer pipelining so the total transfer time is equal to the number of packets to be transferred times the network average RTT. Because of this limitation, we recommend that the TFTP server be located on the same LAN segment as the sensor. Any network with an RTT less than a 100 milliseconds should provide reliable delivery of the image. Be aware that some TFTP servers limit the maximum file size that can be transferred to ~32 MB.

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For terminal servers with RJ-45 connections, connect a rollover cable from the console port on the appliance to a port on the terminal server.
- For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.

Step 2 Configure the line and port on the terminal server. In enable mode, enter the following configuration, where # is the line number of the port to be configured.

```
config t
line #
login
transport input all
```

```
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance. If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

Installing the IPS 4300 Series System Images

Note This procedure is for IPS 4345, but is also applicable to IPS 4360. The system image for IPS 4360 has "4360" in the filename.

You can install the IPS 4345 and IPS 4360 system image by using the ROMMON on the appliance to TFTP the system image on to the compact flash device. To install the IPS 4345 and IPS 4360 system image, follow these steps:

Step 1 Download the IPS 4345 system image file to the tftp root directory of a TFTP server that is accessible from your IPS 4345.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4345.

Step 2 Boot the IPS 4345.

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 1.0(5)0 09/14/04 12:23:35.90

Low Memory: 631 KB
High Memory: 2048 MB
PCI Device Table.
Bus Dev Func VendID DevID Class              Irq
00  00  00   8086   2578  Host Bridge
00  01  00   8086   2579  PCI-to-PCI Bridge
00  03  00   8086   257B  PCI-to-PCI Bridge
```

```
00  1C  00   8086   25AE  PCI-to-PCI Bridge
00  1D  00   8086   25A9  Serial Bus         11
00  1D  01   8086   25AA  Serial Bus         10
00  1D  04   8086   25AB  System
00  1D  05   8086   25AC  IRQ Controller
00  1D  07   8086   25AD  Serial Bus         9
00  1E  00   8086   244E  PCI-to-PCI Bridge
00  1F  00   8086   25A1  ISA Bridge
00  1F  02   8086   25A3  IDE Controller     11
00  1F  03   8086   25A4  Serial Bus         5
00  1F  05   8086   25A6  Audio              5
02  01  00   8086   1075  Ethernet           11
03  01  00   177D   0003  Encrypt/Decrypt    9
03  02  00   8086   1079  Ethernet           9
03  02  01   8086   1079  Ethernet           9
03  03  00   8086   1079  Ethernet           9
03  03  01   8086   1079  Ethernet           9
04  02  00   8086   1209  Ethernet           11
04  03  00   8086   1209  Ethernet           5

Evaluating BIOS Options ...
Launch BIOS Extension to setup ROMMON

Cisco Systems ROMMON Version (1.0(5)0) #1: Tue Sep 14 12:20:30 PDT 2004

Platform IPS-4345-K9
Management0/0

MAC Address: 0000.c0ff.ee01
```

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon> set

ROMMON Variable Settings:
      ADDRESS=0.0.0.0
      SERVER=0.0.0.0
      GATEWAY=0.0.0.0
      PORT=Management0/0
      VLAN=untagged
      IMAGE=
      CONFIG=
```

The variables have the following definitions:

- Address—Local IP address of the IPS 4345.
- Server—TFTP server IP address where the application image is stored.
- Gateway—Gateway IP address used by the IPS 4345.
- Port—Ethernet interface used for the IPS 4345 management.

- VLAN—VLAN ID number (leave as untagged).
- Image—System image file/path name.
- Config—Unused by these platforms.

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, change the interface used for the TFTP download.

Note The default interface used for TFTP downloads is Management 0/0, which corresponds to the MGMT interface of the IPS 4345.

```
rommon> PORT=interface_name
```

Step 6 If necessary, assign an IP address for the local port on the IPS 4345.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the IPS 4345.

Step 7 Assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 8 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 9 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 10 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path file_name
```

Caution Make sure that you enter the **IMAGE** command in all uppercase. You can enter the other ROMMON commands in either lower case or upper case, but the **IMAGE** command specifically must be all uppercase.

UNIX Example

```
rommon> IMAGE=system_images/IPS-4345-K9-sys-1.1-a-7.2-1-E4.img
```

Note The path is relative to the default tftpboot directory of the UNIX TFTP server. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows Example

```
rommon> IMAGE=system_images/IPS-4345-K9-sys-1.1-a-7.2-1-E4.img
```

Step 11 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 12 Download and install the system image.

```
rommon> tftp
```

Caution To avoid corrupting the system image, do not remove power from the IPS 4345 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on the IPS 4345. Be sure to use the IPS 4345 image.

For More Information

- For the location of the list of specific recovery image files, see IPS 7.2 Upgrade Files, page 27-4.
- For more information about TFTP servers, see TFTP Servers, page 27-16.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.

Installing the IPS 4500 Series System Images

Note The following procedure references the IPS 4510 but it also refers to the IPS 4520 and IPS 4520-XL.

Note Use the 4520 files to upgrade the IPS 4520-XL.

You can install the IPS 4500 series system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

To install the IPS 4510 system image, follow these steps:

Step 1 Download the IPS 4510 system image file to the tftp root directory of a TFTP server that is accessible from your IPS 4510.

Note Make sure you can access the TFTP server location from the network connected to the Management port of your IPS 4510.

Step 2 Boot the IPS 4510.

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon> set

ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

The variables have the following definitions:

- Address—Specifies the local IP address of the IPS 4510.
- Server—Specifies the TFTP server IP address where the application image is stored.
- Gateway—Specifies the gateway IP address used by the IPS 4510.
- Port—Specifies the Ethernet interface used for IPS 4510 management.
- VLAN—Specifies the VLAN ID number (leave as untagged).
- Image—Specifies the system image file/path name.
- Config—Unused by these platforms.

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, assign an IP address for the Managment port on the IPS 4510.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the IPS 4510.

Step 6 If necessary, assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 7 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path/file_name
```

UNIX Example

```
rommon> IMAGE=/system_images/IPS-4510-K9-sys-1.1-a-7.2.-1-E4.img
```

Note The path is relative to the UNIX TFTP server default tftpboot directory. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows Example

```
rommon> IMAGE=\system_images\IPS-4510-K9-sys-1.1-a-7.2.-1-E4.img
```

Step 10 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 11 Download and install the system image.

```
rommon> tftp
```

Caution To avoid corrupting the system image, do not remove power from the IPS 4510 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on the IPS 4510. Be sure to use the IPS 4510 image.

For More Information

- For the location of the list of specific recovery image files, see IPS 7.2 Upgrade Files, page 27-4.
- For more information about TFTP servers, see TFTP Servers, page 27-16.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.

Installing the ASA 5500-X IPS SSP System Image

Note Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

Note The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS version you have installed.

To install the system image on the ASA 5500-X IPS SSP, follow these steps:

Step 1 Download the IPS system image file corresponding to your ASA platform to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of the adaptive security appliance.

Step 2 Log in to the adaptive security appliance.

Step 3 Enter enable mode.

```
asa> enable
```

Step 4 Copy the IPS image to the disk0 flash of the adaptive security appliance.

```
asa# copy tftp://192.0.2.0/directory/IPS-5545-K9-sys-1.1-a-7.2.-1-E4.aip disk0:
```

Step 5 Image the ASA 5500-X IPS SSP.

```
asa# sw-module module ips recover configure image
disk0:/IPS-SSP_5545-K9-sys-1.1-a-7.2.-1-E4.aip
```

Step 6 Execute the recovery. This transfers the image from the TFTP server to the ASA 5500-X IPS SSP and restarts it.

```
asa# sw-module module ips recover boot
```

Step 7 Periodically check the recovery until it is complete.

```
asa# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 Cisco ASA 5545 Appliance with 8 GE ports, 1  ASA5545            ABC1234D56E
  1 IPS 5545 Intrusion Protection System         IPS5545            ABC1234D56E

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---  --------------------------------- ------------ ------------ -------------
0    503d.e59c.6dc1 to 503d.e59c.6dca  1.0                       8.6.1
ips  503d.e59c.6dcb to 503d.e59c.6dcb  N/A          N/A          7.2.(1)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               7.2.(1)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
```

```
  1 Up                 Up

asa#
```

Note The Status field in the output indicates the operational status of the ASA 5500-X IPS SSP. An ASA 5500-X IPS SSP operating normally shows a status of "Up." While the adaptive security appliance transfers an application image to the ASA 5500-X IPS SSP, the Status field in the output reads "Recover." When the adaptive security appliance completes the image transfer and restarts the ASA 5500-X IPS SSP, the newly transferred image is running.

Note To debug any errors that may happen in the recovery process, use the **debug module-boot** command to enable debugging of the system reimaging process.

Step 8 Session to the ASA 5500-X IPS SSP and initialize it with the **setup** command.

For More Information

- For the location of the list of specific recovery image files, see IPS 7.2 Upgrade Files, page 27-4.
- For more information about TFTP servers, see TFTP Servers, page 27-16.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 26-1.

Installing the ASA 5585-X IPS SSP System Image

This section describes how to install the ASA 5585-X IPS SSP system image using the **hw-module** command or ROMMON, and contains the following topics:

- Installing the ASA 5585-X IPS SSP System Image Using the hw-module Command, page 27-24
- Installing the ASA 5585-X IPS SSP System Image Using ROMMON, page 27-27

Installing the ASA 5585-X IPS SSP System Image Using the hw-module Command

Note Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

Note This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

Note The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS version you have installed.

To install the system image, transfer the software image from a TFTP server to the ASA 5585-X IPS SSP using the adaptive security appliance CLI. The adaptive security appliance can communicate with the ROMMON application of the ASA 5585-X IPS SSP to transfer the image.

To install the ASA 5585-X IPS SSP software image, follow these steps:

Step 1 Download the ASA 5585-X IPS SSP system image file to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your adaptive security appliance.

Step 2 Log in to the adaptive security appliance.

Step 3 Enter enable mode.

```
asa# enable
```

Step 4 Configure the recovery settings for the ASA 5585-X IPS SSP.

```
asa (enable)# hw-module module 1 recover configure
```

Note If you make an error in the recovery configuration, use the **hw-module module 1 recover stop** command to stop the system reimaging and then you can correct the configuration.

Step 5 Specify the TFTP URL for the software image.

```
Image URL [tftp://0.0.0.0/]:
```

Example

```
Image URL [tftp://0.0.0.0/]: tftp://192.0.2.0/IPS-SSP_40-K9-sys-1.1-a-7.2.-1-E4.img
```

Step 6 Specify the command and control interface of the ASA 5585-X IPS SSP.

Note The port IP address is the management IP address of the ASA 5585-X IPS SSP.

```
Port IP Address [0.0.0.0]:
```

Example

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

Step 7 Leave the VLAN ID at 0.

```
VLAN ID [0]:
```

Step 8 Specify the default gateway of the ASA 5585-X IPS SSP.

```
Gateway IP Address [0.0.0.0]:
```

Example

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

Step 9 Execute the recovery. This transfers the software image from the TFTP server to the ASA 5585-X IPS SSP and restarts it.

```
asa# hw-module module 1 recover boot
```

Step 10 Periodically check the recovery until it is complete.

Note The status reads `Recovery` during recovery and reads `Up` when installation is complete.

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-10 with 8GE
Model:              ASA5585-SSP-IPS40
Hardware version:   1.0
Serial Number:      JAF1350ABSL
Firmware version:   2.0(1)3
Software version:   7.2.(1)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2.(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.0
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       10.89.148.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa#
```

Note The Status field in the output indicates the operational status of the ASA 5585-X IPS SSP. An ASA 5585-X IPS SSP operating normally shows a status of “Up.” While the adaptive security appliance transfers the software image to the ASA 5585-X IPS SSP, the Status field in the output reads “Recover.” When the adaptive security appliance completes the software image transfer and restarts the ASA 5585-X IPS SSP, the newly transferred image is running.

Note To debug any errors that may happen during this process, use the **debug module-boot** command to enable debugging of the software installation process.

Step 11 Session to the ASA 5585-X IPS SSP.

Step 12 Enter **cisco** three times and your new password twice.

Step 13 Initialize the ASA 5585-X IPS SSP with the **setup** command.

Installing the ASA 5585-X IPS SSP System Image Using ROMMON

You can install the ASA 5585-X IPS SSP system image by using the ROMMON on the adaptive security appliance to TFTP the system image onto the ASA 5585-X IPS SSP.

To install the ASA 5585-X IPS SSP system image, follow these steps:

Step 1 Download the ASA 5585-X IPS SSP system image file to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your adaptive security appliance.

Step 2 Boot the ASA 5585-X IPS SSP.

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 0.0(2)10 11:16:38 04/15/10
Com KbdBuf SMM UsbHid Msg0 Prompt Pmrt Cache1 LowM ExtM HugeM Cache2 Flg Siz0 Amrt PMM
PnpDsp Smbios Lpt0 Npx1 Apm Lp1 Acpi Typ Dbg Enb Mp MemReduce MemSync1 CallRoms MemSync2
DriveInit


Total memory : 12 GB
Total number of CPU cores : 8
Com Lp1 Admgr2 Brd10 Plx2 OEM0=7EFF5C74
Cisco Systems ROMMON Version (1.0(12)10) #0: Thu Apr  8 00:12:33 CDT 2010

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Management0/0
Link is UP
MAC Address: 5475.d029.7fa9
```

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon #0> set
ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
```

```
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20
```

The variables have the following definitions:

- Address—Specifies the local IP address of the ASA 5585-X IPS SSP.
- Server—Specifies the TFTP server IP address where the application image is stored.
- Gateway—Specifies the gateway IP address used by the ASA 5585-X IPS SSP.
- Port—Specifies the ethernet interface used for the ASA 5585-X IPS SSP management.
- VLAN—Specifies the VLAN ID number (leave as untagged).
- Image—Specifies the system image file/path name.
- Config—Specifies the unused by these platforms.

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, change the interface used for the TFTP download.

Note The default interface used for TFTP downloads is Management 0/0, which corresponds to the management interface of the ASA 5585-X IPS SSP.

```
rommon> PORT=interface_name
```

Step 6 If necessary, assign an IP address for the local port on the ASA 5585-X IPS SSP.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the ASA 5585-X IPS SSP.

Step 7 If necessary, assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 8 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 9 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands.

```
rommon> ping server_ip_address
rommon> ping server
```

Step 10 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path/file_name
```

Caution Make sure that you enter the **IMAGE** command in all uppercase. You can enter the other ROMMON commands in either lower case or upper case, but the **IMAGE** command specifically must be all uppercase.

UNIX Example

```
rommon> IMAGE=/system_images/IPS-SSP_10-K9-sys-1.1-a-7.2.-1-E4.img
```

Note The path is relative to the default tftpboot directory of the UNIX TFTP server. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows Example

```
rommon> IMAGE=\system_images\IPS-SSP_10-K9-sys-1.1-a-7.2.-1-E4.img
```

Step 11 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 12 Download and install the system image.

```
rommon> tftp
```

Note If the network settings are correct, the system downloads and boots the specified image on the ASA 5585-X IPS SSP. Be sure to use the ASA 5585-X IPS SSP image.

Caution To avoid corrupting the system image, do not remove power from the ASA 5585-X IPS SSP while the system image is being installed.

System Architecture

This appendix describes the Cisco IPS system architecture, and contains the following topics:

Purpose of Cisco IPS

The purpose of the Cisco IPS is to detect and prevent malicious network activity. You can install the Cisco IPS software on two platforms: appliances and the modules. The Cisco IPS contains a management application and a monitoring application. The IDM is a network management JAVA application that you can use to manage and monitor the IPS. The IME is an IPS network monitoring JAVA application that you can use to view IPS events. The IME also contains the IDM configuration component. The IDM and the IME communicate with the IPS using HTTP or HTTPS and are hosted on your computer.

System Design

The Cisco IPS software runs on the Linux operating system. We have hardened the Linux OS by removing unnecessary packages from the OS, disabling unused services, restricting network access, and removing access to the shell.

Figure A-1 illustrates the system design for IPS software.

Figure A-1 System Design for the IPS

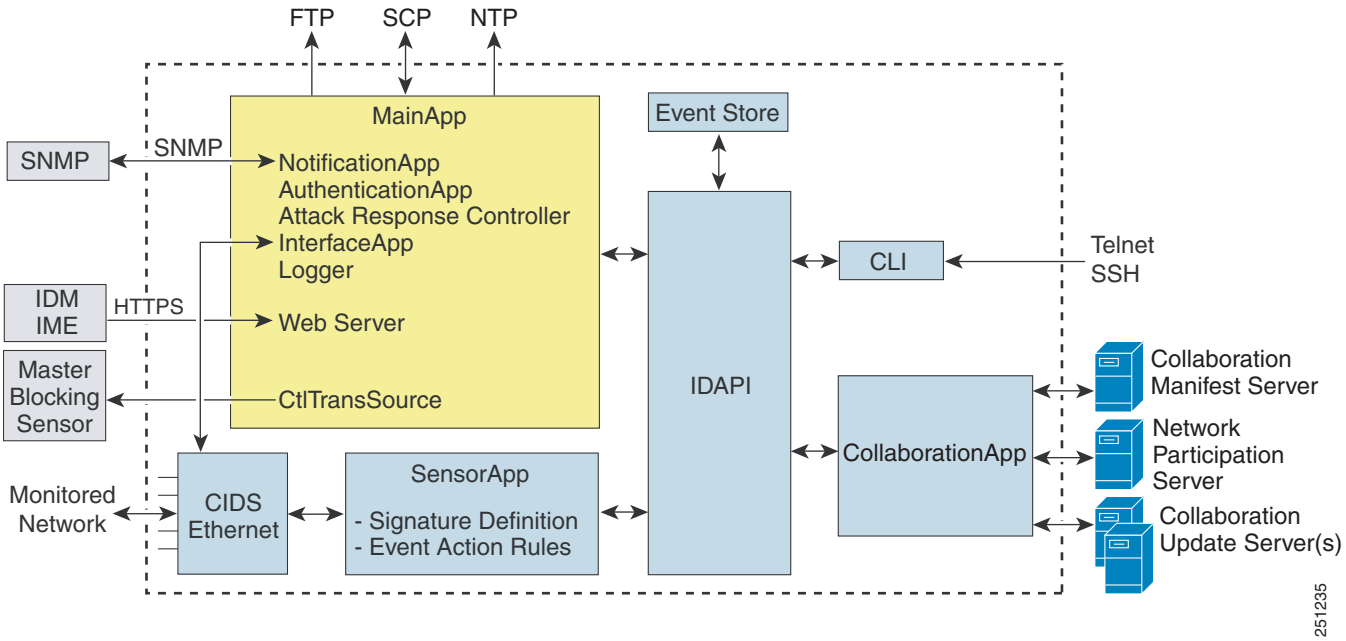
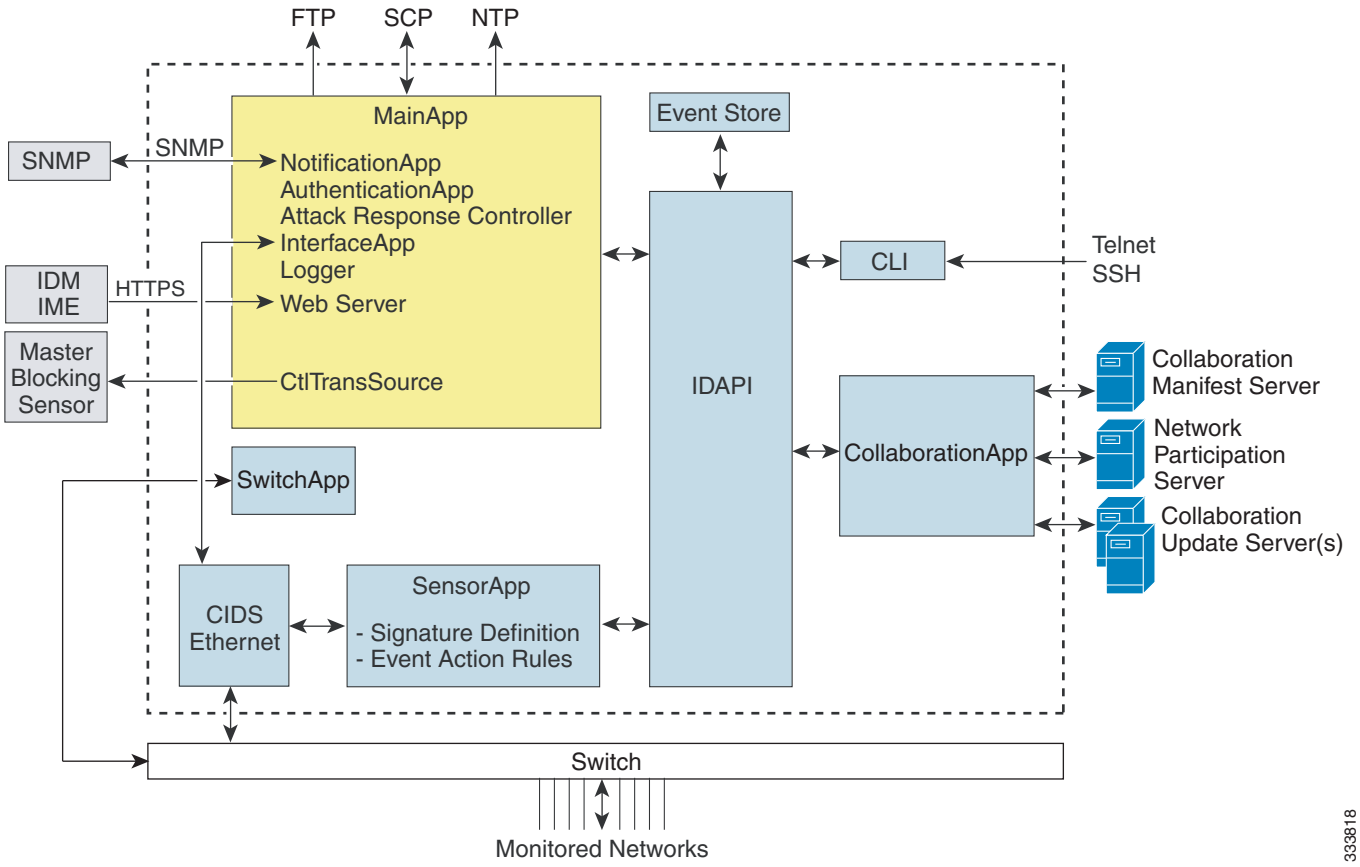


Figure A-2 illustrates the system design for IPS software for the IPS 4500 series sensors.

Figure A-2 System Design for IPS 4500 Series Sensors



For More Information

- For more information on the MainApp, see MainApp, page A-5.
- For more information on the SensorApp, see SensorApp, page A-22.
- For more information on the CollaborationApp, see CollaborationApp, page A-27.
- For detailed information on the CLI, see CLI, page A-30.
- For detailed information on the SwitchApp, see SwitchApp, page A-29.

System Applications

Note Each application has its own configuration file in XML format.

The Cisco IPS software includes the following applications:

- MainApp—Initializes the system, starts and stops the other applications, configures the OS, and performs upgrades. It contains the following components:
  - ctlTransSource (Control Transaction server)—Allows sensors to send control transactions. This is used to enable the master blocking sensor capability of Attack Response Controller (formerly known as Network Access Controller).
  - Event Store—An indexed store used to store IPS events (error, status, and alert system messages) that is accessible through the CLI, IDM, IME, ASDM, or SDEE.

    Note The Event Store has a fixed size of 30 MB for all platforms.

  - InterfaceApp—Handles bypass and physical settings and defines paired interfaces. Physical settings are speed, duplex, and administrative state.
  - Logger—Writes all the log messages of the application to the log file and the error messages of the application to the Event Store.
  - Attack Response Controller (formerly known as Network Access Controller) —Manages remote network devices (firewalls, routers, and switches) to provide blocking capabilities when an alert event has occurred. The ARC creates and applies ACLs on the controlled network device or uses the **shun** command (firewalls).
  - NotificationApp—Sends SNMP traps when triggered by alert, status, and error events. The NotificationApp uses the public domain SNMP agent. SNMP GETs provide information about the general health of the sensor.
  - Web server (HTTP SDEE server)—Provides a web interface and communication with the other IPS devices through the SDEE protocol using several servlets to provide the IPS services.
  - AuthenticationApp—Verifies that users are authorized to perform CLI, IDM, IME, ASDM, or SDEE actions.
- SensorApp (Analysis Engine)—Performs packet capture and analysis.
- CollaborationApp—Interfaces with the MainApp and the SensorApp using various interprocess communication technologies including IDAPI control transactions, semaphores, shared memory, and file exchange.
- CLI—The interface that is run when you successfully log in to the sensor through Telnet or SSH. All accounts created through the CLI will use the CLI as their shell (except the service account—only one service account is allowed). Allowed CLI commands depend on the privilege of the user.

All Cisco IPS applications communicate with each other through a common API called the IDAPI. Remote applications (other sensors, management applications, and third-party software) communicate with sensors through the SDEE protocol.

The sensor has the following partitions:

- Application partition—A full IPS system image.
- Recovery partition—A special purpose image used for recovery of the sensor. Booting into the recovery partition enables you to completely reimage the application partition. Network settings are preserved, but all other configuration is lost.

User Interaction

You interact with the Cisco IPS in the following ways:

- Configure device parameters

  You generate the initial configuration for the system and its features. This is an infrequent task, usually done only once. The system has reasonable default values to minimize the number of modifications you must make. You can configure Cisco IPS through the CLI, IDM, IME, CSM, ASDM, or through another application using SDEE.

- Tune

  You make minor modifications to the configuration, primarily to Analysis Engine, which is the portion of the application that monitors network traffic. You can tune the system frequently after initially installing it on the network until it is operating efficiently and only producing information you find useful. You can create custom signatures, enable features, or apply a service pack or signature update. You can tune Cisco IPS through the CLI, IDM, IME, CSM, ASDM, or through another application using SDEE.

- Update

  You can schedule automatic updates or apply updates immediately to the applications and signature data files. You can update Cisco IPS through the CLI, IDM, IME, CSM, ASDM, or through another application using SDEE.

- Retrieve information

  You can retrieve data (status messages, errors, and alerts) from the system through the CLI, IDM, IME, CSM, ASDM, or another application using SDEE.

Security Features

Cisco IPS has the following security features:

- Network access is restricted to hosts who are specifically allowed access.
- All remote hosts who attempt to connect through the web server, SSH and SCP or Telnet will be authenticated.
- By default Telnet access is disabled. You can choose to enable Telnet.
- By default SSH access is enabled.
- An FTP server does not run on the sensor. You can use SCP to remotely copy files.
- By default the web server uses TLS or SSL. You can choose to disable TLS and SSL.
- Unnecessary services are disabled.
- Only the SNMP set required by the Cisco MIB Police is allowed within the CISCO-CIDS-MIB. OIDs implemented by the public domain SNMP agent will be writeable when specified by the MIB.

MainApp

This section describes the MainApp, and contains the following topics:

Understanding the MainApp

The MainApp includes all IPS components except SensorApp and the CLI. It is loaded by the operating system at startup and loads SensorApp. The MainApp then brings the following subsystem components up:

- Authentication
- Logger
- ARC
- Web Server
- Notification (SNMP)
- External Product Interface
- Interface manager
- Event Store
- Health and security monitoring

MainApp Responsibilities

The MainApp has the following responsibilities:

- Validate the Cisco-supported hardware platform
- Report software version and PEP information
- Start, stop, and report the version of the IPS components
- Configure the host system settings
- Manage the system clock
- Manage the Event Store
- Install and uninstall software upgrades

Note In the Cisco IPS, the MainApp can automatically download signature and signature engine updates from Cisco.com.

- Shut down or reboot the operating system

The MainApp responds to the **show version** command by displaying the following information:

- Sensor build version
- MainApp version
- Version of each running application
- Version and timestamp of each installed upgrade
- Next downgrade version of each installed upgrade
- Platform version
- Version of sensor build on the other partition

The MainApp also gathers the host statistics and reports the health and security monitoring status.

Event Store

This section describes the Event Store, and contains the following topics:

- Understanding the Event Store, page A-7
- Event Data Structures, page A-8
- IPS Events, page A-9

Understanding the Event Store

Note The Event Store has a fixed size of 30 MB for all platforms.

Each IPS event is stored in the Event Store with a time stamp and a unique, monotonic, ascending ID. This time stamp is the primary key used to index the event into the fixed-size, indexed Event Store. When the circular Event Store has reached its configured size, the oldest event or events are overwritten by the new event being stored. The SensorApp is the only application that writes alert events into the Event Store. All applications write log, status, and error events into the Event Store.

The fixed-sized, indexed Event Store allows simple event queries based on the time, type, priority, and a limited number of user-defined attributes. If each event is assigned a priority of low, medium, or high, a single event query can specify a list of desired event types, intrusion event priorities, and a time range.

Table A-1 shows some examples:

Table A-1 IPS Event Examples

IPS Event Type	Intrusion Event Priority	Start Time Stamp Value	Stop Time Stamp Value	Meaning
status	—	0	Maximum value	Get all status events that are stored.
error status	—	0	65743	Get all error and status events that were stored before time 65743.
status	—	65743	Maximum value	Get status events that were stored at or after time 65743.

Table A-1 IPS Event Examples (continued)

IPS Event Type	Intrusion Event Priority	Start Time Stamp Value	Stop Time Stamp Value	Meaning
intrusion attack response	low	0	Maximum value	Get all intrusion and attack response events with low priority that are stored.
attack response error status intrusion	medium high	4123000000	4123987256	Get attack response, error, status, and intrusion events with medium or high priority that were stored between time 4123000000 and 4123987256.

The size of the Event Store allows sufficient buffering of the IPS events when the sensor is not connected to an IPS event consumer. Sufficient buffering depends on your requirements and the capabilities of the nodes in use. The oldest events in the circular buffer are replaced by the newest events.

Event Data Structures

The various functional units communicate the following seven types of data:

- Intrusion events—Produced by the SensorApp. The sensor detects intrusion events.
- Error events—Caused by hardware or software malfunctions.
- Status events—Reports of a change in the status of the application, for example, that its configuration has been updated.
- Control transaction log events—The sensor logs the result of a control transaction.
- Attack response events—Actions for the ARC, for example, a block request.
- Debug events—Highly detailed reports of a change in the status of the application used for debugging.
- Control transaction data—Data associated with control transactions, for example, diagnostic data from an application, session logs, and configuration data to or from an application.

All seven types of data are referred to collectively as *IPS data*. The six event types—intrusion, error, status, control transaction log, network access, and debug—have similar characteristics and are referred to collectively as *IPS events*. IPS events are produced by the several different applications that make up the IPS and are subscribed to by other IPS applications. IPS events have the following characteristics:

- They are spontaneously generated by the application instances configured to do so. There is no request from another application instance to generate a particular event.
- They have no specific destination. They are stored and then retrieved by one or more application instances.

Control transactions involve the following types of requests:

- Request to update the configuration data of an application instance
- Request for the diagnostic data of an application instance
- Request to reset the diagnostic data of an application instance
- Request to restart an application instance
- Request for ARC, such as a block request

Control transactions have the following characteristics:

- They always consist of a request followed by a response.

  The request and response may have an arbitrary amount of data associated with them. The response always includes at least a positive or negative acknowledgment.

- They are point-to-point transactions.

  Control transactions are sent by one application instance (the initiator) to another application instance (the responder).

IPS data is represented in XML format as an XML document. The system stores user-configurable parameters in several XML files.

IPS Events

IPS applications generate IPS events to report the occurrence of some stimulus. The events are the data, such as the alerts generated by SensorApp or errors generated by any application. Events are stored in a local database known as the Event Store.

There are five types of events:

- evAlert—Alert event messages that report when a signature is triggered by network activity.
- evStatus—Status event messages that report the status and actions of the IPS applications.
- evError— Error event messages that report errors that occurred while attempting response actions.
- evLogTransaction—Log transaction messages that report the control transactions processed by each sensor application.
- evShunRqst—Block request messages that report when ARC issues a block request.

You can view the status and error messages using the CLI, IME, and ASDM. The SensorApp and ARC log response actions (TCP resets, IP logging start and stop, blocking start and stop, trigger packet) as status messages.

NotificationApp

The NotificationApp allows the sensor to send alerts and system error messages as SNMP traps. It subscribes to events in the Event Store and translates them into SNMP MIBs and sends them to destinations through a public-domain SNMP agent. The NotificationApp supports sending sets and gets. The SNMP GETs provide information about basic sensor health.

The NotificationApp has been modified in IPS 7.2(2)E4 and later to support SNMPv3. SNMPv3 configuration, such as access control (rwuser and rouser) security level (authPriv, noAuthNoPriv, authNoPriv), authentication protocol (SHA or none), and privacy protocol (AES or none), has been added. The administrator can also associate SNMPv3 users with trap destinations.

The NotificationApp sends the following information from the evAlert event in sparse mode:

- Originator information
- Event ID
- Event severity
- Time (UTC and local time)
- Signature name
- Signature ID

- Subsignature ID
- Participant information
- Alarm traits

The NotificationApp sends the following information from the evAlert event in detail mode:

- Originator information
- Event ID
- Event severity
- Time (UTC and local time)
- Signature name
- Signature ID
- Subsignature ID
- Version
- Summary
- Interface group
- VLAN
- Participant information
- Actions
- Alarm traits
- Signature
- IP log IDs

The NotificationApp determines which evError events to send as a trap according to the filter that you define. You can filter based on error severity (error, fatal, and warning). The NotificationApp sends the following information from the evError event:

- Originator information
- Event ID
- Event severity
- Time (UTC and local time)
- Error message

The NotificationApp supports GETs for the following general health and system information from the sensor:

- Packet loss
- Packet denies
- Alarms generated
- Fragments in FRP
- Datagrams in FRP
- TCP streams in embryonic state
- TCP streams in established state
- TCP streams in closing state

- TCP streams in system
- TCP packets queued for reassembly
- Total nodes active
- TCP nodes keyed on both IP addresses and both ports
- UDP nodes keyed on both IP addresses and both ports
- IP nodes keyed on both IP addresses
- Sensor memory critical stage
- Interface status
- Command and control packet statistics
- Fail-over state
- System uptime
- CPU usage
- Memory usage for the system
- PEP

Note Not all IPS platforms support PEP.

The NotificationApp provides the following statistics:

- Number of error traps
- Number of event action traps
- Number of SNMP GET requests
- Number of SNMP SET requests

CtlTransSource

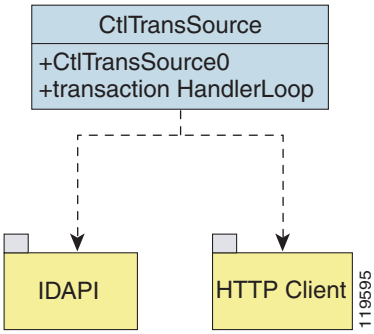
The CtlTransSource is an application that forwards locally initiated remote control transactions to their remote destinations using HTTP protocol. The CtlTransSource initiates either TLS or non-TLS connections and communicates remote control transactions to HTTP servers over these connections.

The CtlTransSource must establish sufficient credentials on the remote HTTP server to execute a remote control transaction. It establishes its credentials by presenting an identity to the HTTP server on the remote node in the form of a username and password (basic authentication). When the authentication is successful, the requestor is assigned a cookie containing a user authentication that must be presented with each request on that connection.

The transactionHandlerLoop method in the CtlTransSource serves as a proxy for remote control transaction. When a local application initiates a remote control transaction, IDAPI initially directs the transaction to the CtlTransSource. The transactionHandlerLoop method is a loop that waits on remote control transactions that are directed to the CtlTransSource.

Figure A-3 shows the transactionHandlerLoop method in the CtlTransSource.

Figure A-3 CtlTransSource



When the transactionHandlerLoop receives a remotely addressed transaction, it tries to forward the remote control transaction to its remote destination. The transactionHandlerLoop formats the transaction into a control transaction message. The transactionHandlerLoop uses the HttpClient classes to issue the control transaction request to the HTTP server on the remote node. The remote HTTP server handles the remote control transaction and returns the appropriate response message in an HTTP response. If the remote HTTP server is an IPS web server, the web server uses the CtlTransSource servlet to process the remote control transactions.

The transactionHandlerLoop returns either the response or a failure response as the response of the control transaction to the initiator of the remote control transaction. If the HTTP server returns an unauthorized status response (indicating the HTTP client has insufficient credentials on the HTTP server), the transactionHandlerLoop reissues the transaction request using the designated username and password of the CtlTransSource to authenticate the identity of the requestor. The transactionHandlerLoop continues to loop until it receives a control transaction that directs it to exit or until its exit event is signaled.

Attack Response Controller

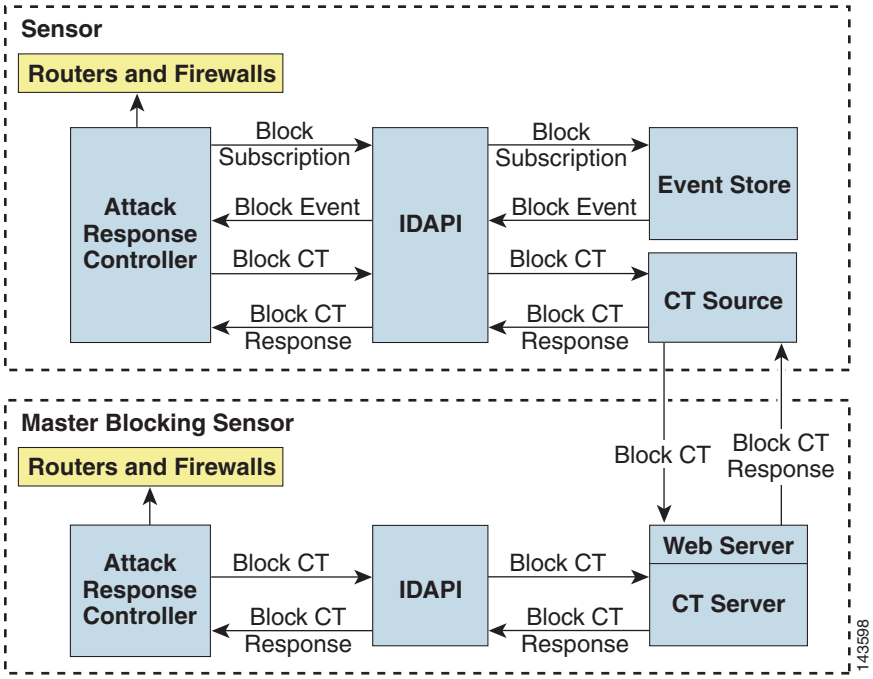
This section describes the Attack Response Controller (ARC), and contains the following topics:

Understanding the ARC

The main responsibility of the ARC is to block events. When it responds to a block, it either interacts with the devices it is managing directly to enable the block or it sends a block request through the Control Transaction Server to a master blocking sensor. The web server on the master blocking sensor receives the control transaction and passes it to the Control Transaction Server, which passes it to the ARC. The ARC on the master blocking sensor then interacts with the devices it is managing to enable the block.

Figure A-4 illustrates the ARC.

Figure A-4 ARC



Note An ARC instance can control 0, 1, or many network devices. The ARC does not share control of any network device with other ARC applications, IPS management software, other network management software, or system administrators. Only one ARC instance is allowed to run on a given sensor.

The ARC initiates a block in response to one of the following:

- An alert event generated from a signature that is configured with a block action
- A block configured manually through the CLI, IDM, IME, or ASDM
- A block configured permanently against a host or network address

When you configure the ARC to block a device, it initiates either a Telnet or SSH connection with the device. The ARC maintains the connection with each device. After the block is initiated, the ARC pushes a new set of configurations or ACLs (one for each interface direction) to each controlled device. When a block is completed, all configurations or ACLs are updated to remove the block.

ARC Features

The ARC has the following features:

- Communication through Telnet and SSH 1.5 with 3DES (the default) or DES encryption

  Only the protocol specified in the ARC configuration for that device is attempted. If the connection fails for any reason, the ARC attempts to reestablish it.

- Preexisting ACLs on routers and VACLs on switches

  If a preexisting ACL exists on a router interface or direction that is controlled by the ARC, you can specify that this ACL be merged into the ARC-generated configuration, either before any blocks by specifying a preblock ACL or after any blocks by specifying a postblock ACL. The Catalyst 6000 VACL device types can have a preblock and postblock VACL specified for each interface that the ARC controls. The firewall device types use a different API to perform blocks and the ARC does not have any effect on preexisting ACLs on the firewalls.

  Note Catalyst 5000 RSM and Catalyst 6000 MSFC2 network devices are supported in the same way as Cisco routers.

- Forwarding blocks to a list of remote sensors

  The ARC can forward blocks to a list of remote sensors, so that multiple sensors can in effect collectively control a single network device. Such remote sensors are referred to as master blocking sensors.

- Specifying blocking interfaces on a network device

  You can specify the interface and direction where blocking is performed in the ARC configuration for routers. You can specify the interface where blocking is performed in the VACL configuration. The ARC can simultaneously control up to 250 interfaces.

  Note Cisco firewalls do not block based on interface or direction, so this configuration is never specified for them.

- Blocking hosts or networks for a specified time

  The ARC can block a host or network for a specified number of minutes or indefinitely. The ARC determines when a block has expired and unblocks the host or network at that time.

- Logging important events

  The ARC writes a confirmation event when block or unblock actions are completed successfully or if any errors occur. The ARC also logs important events such as loss and recovery of a network device communication session, configuration errors, and errors reported by the network device.

- Maintaining the blocking state across ARC restarts

  The ARC reapplies blocks that have not expired when a shutdown or restart occurs. The ARC removes blocks that have expired while it was shut down.

  Note The ARC can only maintain the blocking state successfully if no one changes the system time while the application is shut down.

- Maintaining blocking state across network device restarts

  The ARC reapplies blocks and removes expired blocks as needed whenever a network device is shut down and restarted. The ARC is not affected by simultaneous or overlapping shutdowns and restarts of the ARC.

- Authentication and authorization

  The ARC can establish a communications session with a network device that uses AAA authentication and authorization including the use of remote TACACS+ servers.

- Two types of blocking

  The ARC supports host blocks and network blocks. Host blocks are connection based or unconditional. Network blocks are always unconditional.

- NAT addressing

  The ARC can control network devices that use a NAT address for the sensor. If you specify a NAT address when you configure a network device, that address is used instead of the local IP address when the sensor address is filtered from blocks on that device.

- Single point of control

  The ARC does not share control of network devices with administrators or other software. If you must update a configuration, shut down ARC until the change is complete. You can enable or disable the ARC through the CLI or any Cisco IPS manager. When the ARC is reenabled, it completely reinitializes itself, including rereading the current configuration for each controlled network device.

  Note We recommend that you disable the ARC from blocking when you are configuring any network device, including firewalls.

- Maintains up to 250 active blocks at any given time

  The ARC can maintain up to 250 active blocks at a time. Although the ARC can support up to 65535 blocks, we recommend that you allow no more than 250 at a time.

  Note The number of blocks is not the same as the number of interface and directions.

Supported Blocking Devices

The ARC can control the following devices:

- Cisco routers running Cisco IOS 11.2 or later

  Note To perform rate limiting, the routers must be running Cisco IOS 12.3 or later.

- Catalyst 5000 series switches with Supervisor Engine software 5.3(1) or later running on the supervisor engine, and IOS 11.2(9)P or later running on the RSM.

  Note You must have the RSM because blocking is performed on the RSM.

- Catalyst 6000 series switches with PFC installed running Catalyst software 5.3 or later

- Catalyst 6000 MSFC2 with Catalyst software 5.4(3) or later and Cisco IOS 12.1(2)E or later on the MSFC2
- Cisco ASA 5500 series models: ASA 5510, ASA 5520, and ASA 5540
- FWSM

Note The FWSM cannot block in multi-mode admin context.

ACLs and VACLs

If you want to filter packets on an interface or direction that the ARC controls, you can configure the ARC to apply an ACL before any blocks (preblock ACL) and to apply an ACL after any blocks (postblock ACL). These ACLs are configured on the network device as inactive ACLs. You can define preblock and postblock ACLs for each interface and direction. The ARC retrieves and caches the lists and merges them with the blocking ACEs whenever it updates the active ACL on the network device. In most cases, you will want to specify a preexisting ACL as the postblock ACL so that it does not prevent any blocks from taking effect. ACLs work by matching a packet to the first ACE found. If this first ACE permits the packet, a subsequent deny statement will not be found.

You can specify different preblock and postblock ACLs for each interface and direction, or you can reuse the same ACLs for multiple interfaces and directions. If you do not want to maintain a preblock list, you can use the never block option and always block hosts and networks by using existing configuration statements. A forever block is a normal block with a timeout value of -1.

The ARC only modifies ACLs that it owns. It does not modify ACLs that you have defined. The ACLs maintained by ARC have a specific format that should not be used for user-defined ACLs. The naming convention is **IPS_<**interface_name**>_[in | out]_[0 | 1]**. <interface_name> corresponds to the name of the blocking interface as given in the ARC configuration.

For Catalyst switches, it is a blocking interface VLAN number. Do not use these names for preblock and postblock ACLs. For Catalyst 6000 VACLs, you can specify a preblock and postblock VACL and only the interface is specified (direction is not used in VLANs). For firewalls, you cannot use preblock or postblock ACLs because the firewall uses a different API for blocking. Instead you must create ACLs directly on the firewalls.

Maintaining State Across Restarts

When the sensor shuts down, the ARC writes all blocks and rate limits (with starting timestamps) to a local file (nac.shun.txt) that is maintained by the ARC. When the ARC starts, this file is used to determine if any block updates should occur at the controlled network devices. Any unexpired blocks found in the file are applied to the network devices at startup. When the ARC shuts down, no special actions on the ACLs are taken even if outstanding blocks are in effect. The nac.shun.txt file is accurate only if the system time is not changed while the ARC is not running.

Caution Do not make manual changes to the nac.shun.txt file.

The following scenarios demonstrate how the ARC maintains state across restarts.

Scenario 1

There are two blocks in effect when the ARC stops and one of them expires before the ARC restarts. When the ARC restarts, it first reads the nac.shun.txt file. It then reads the preblock and postblock ACLs or VACLs. The active ACL or VACL is built in the following order:

1. The **allow** *sensor_ ip_address* command (unless the **allow sensor shun** command has been configured)
2. Preblock ACL
3. The **always block** command entries from the configuration
4. Unexpired blocks from nac.shun.txt
5. Postblock ACL

When a host is specified as never block in the ARC configuration, it does not get translated into permit statements in the ACL. Instead, it is cached by the ARC and used to filter incoming addShunEvent events and addShunEntry control transactions.

Scenario 2

There are no preblock or postblock ACLs specified, but there is an existing active ACL. The new ACL is built in the following order:

1. The **allow** *sensor_ ip_address* command (unless the **allow sensor shun** command has been configured)
2. The **always block** command entries from the configuration
3. Unexpired blocks from nac.shun.txt
4. The **permit IP any any** command

Connection-Based and Unconditional Blocking

The ARC supports two types of blocking for hosts and one type of blocking for networks. Host blocks are connection-based or unconditional. Network blocks are always unconditional.

When a host block is received, the ARC checks for the connectionShun attribute on the host block. If connectionShun is set to true, the ARC performs connection blocking. Any host block can contain optional parameters, such as destination IP address, source port, destination port, and protocol. For a connection block to take place, at least the source and destination IP address must be present. If the source port is present on a connection block, it is ignored and not included in the block.

Under the following conditions, the ARC forces the block to be unconditional, converting the block from connection type if necessary:

- A block of any type is active for a specified source IP address
- A new block of any type is received for that source IP address
- The new block differs in any of its optional parameters (except the source port) from the old block

When a block is updated (for example, when a new block arrives while an existing block for that source IP address or network is already in effect), the remaining minutes of the existing block are determined. If the time for the new block is less than or equal to the remaining minutes, no action is taken. Otherwise, the new block timeout replaces the existing block timeout.

Caution Cisco firewalls do not support connection blocking of hosts. When a connection block is applied, the firewall treats it like an unconditional block. Cisco firewalls also do not support network blocking. ARC never tries to apply a network block to a Cisco firewall.

Blocking with Cisco Firewalls

The ARC performs blocks on firewalls using the **shun** command. The **shun** command has the following formats:

- To block an IP address:

  shun srcip [*destination_ip_address source_port destination_port* [*port*]]

- To unblock an IP address:

  no shun ip

- To clear all blocks:

  clear shun

- To show active blocks or to show the global address that was actually blocked:

  show shun [*ip_address*]

The ARC uses the response to the **show shun** command to determine whether the block was performed. The **shun** command does not replace existing ACLs, conduits, or outbound commands, so there is no need to cache the existing firewall configuration, nor to merge blocks into the firewall configuration.

Caution Do not perform manual blocks or modify the existing firewall configuration while ARC is running.

If the **block** command specifies only the source IP address, existing active TCP connections are not broken, but all incoming packets from the blocked host are dropped.

When the ARC first starts up, the active blocks in the firewall are compared to an internal blocking list. Any blocks that do not have a corresponding internal list entry are removed.

The ARC supports authentication on a firewall using local usernames or a TACACS+ server. If you configure the firewall to authenticate using AAA but without the TACACS+ server, the ARC uses the reserved username *pix* for communications with the firewall.

If the firewall uses a TACACS+ server for authentication, you use a TACACS+ username. In some firewall configurations that use AAA logins, you are presented with three password prompts: the initial firewall password, the AAA password, and the enable password. The ARC requires that the initial firewall password and the AAA password be the same.

When you configure a firewall to use NAT or PAT and the sensor is checking packets on the firewall outside network, if you detect a host attack that originates on the firewall inside network, the sensor tries to block the translated address provided by the firewall. If you are using dynamic NAT addressing, the block can be ineffective or cause innocent hosts to be blocked. If you are using PAT addressing, the firewall could block the entire inside network. To avoid these situations, position your sensor on the inside interface or do not configure the sensor to block.

Blocking with Catalyst Switches

Catalyst switches with a PFC filter packets using VACLs. VACLs filter all packets between VLANs and within a VLAN. MSFC router ACLs are supported when WAN cards are installed and you want the sensor to control the interfaces through the MSFC2.

Note An MSFC2 card is not a required part of a Catalyst switch configuration for blocking with VACLs.

Caution When you configure the ARC for the Catalyst switch, do not specify a direction with the controlled interface. The interface name is a VLAN number. Preblock and postblock lists should be VACLs.

The following commands apply to the Catalyst VACLs:

- To view an existing VACL:

  `show security acl info` *acl_name*

- To block an address (*address_spec* is the same as used by router ACLs):

  `set security acl ip` *acl_name* **`deny`** *address_spec*

- To activate VACLs after building the lists:

  `commit security acl all`

- To clear a single VACL:

  `clear security acl map` *acl_name*

- To clear all VACLs:

  `clear security acl map all`

- To map a VACL to a VLAN:

  `set sec acl` *acl_name vlans*

Logger

The sensor logs all events (alert, error, status, and debug messages) in a persistent, circular buffer. The sensor also generates IP logs. The messages and IP logs are accessible through the CLI, IDM, and ASDM.

The IPS applications use the Logger to log messages. The Logger sends log messages at any of five levels of severity: debug, timing, warning, error, and fatal. The Logger writes the log messages to /usr/cids/idsRoot/log/main.log, which is a circular text file. New messages overwrite older messages when the file reaches its maximum size; therefore the last message written may not appear at the end of the main.log. Search for the string "= END OF FILE =" to locate the last line written to the main.log.

The main.log is included in the **show tech-support** command output. If the message is logged at warning level or above (error or fatal), the Logger converts the message to an evError event (with the corresponding error severity) and inserts it in the Event Store.

The Logger receives all syslog messages, except cron messages, that are at the level of informational and above (*.info;cron.none), and inserts them in to the Event Store as evErrors with the error severity set to Warning. The Logger and application logging are controlled through the service logger commands.

The Logger can control what log messages are generated by each application by controlling the logging severity for different logging zones. You would only access the individual-zone-control of the logger service at the request and supervision of a TAC engineer or developer. For troubleshooting purposes, TAC might request that you turn on debug logging.

AuthenticationApp

This section describes the AuthenticationApp, and contains the following topics:

Understanding the AuthenticationApp

The AuthenticationApp has the following responsibilities:

- To authenticate the identity of a user
- To administer the accounts, privileges, keys, and certificates of the user
- To configure which authentication methods are used by the AuthenticationApp and other access services on the sensor

Authenticating Users

You must configure authentication on the sensor to establish appropriate security for user access. When you install a sensor, an initial cisco account with an expired password is created. A user with administrative access to the sensor accesses the sensor through the CLI or an IPS manager, such as the IDM or the ASDM, by logging in to the sensor using the default administrative account (**cisco**). In the CLI, the administrator is prompted to change the password. IPS managers initiate a setEnableAuthenticationTokenStatus control transaction to change the password of an account.

Through the CLI or an IPS manager, the administrator configures which authentication method is used, such as username and password or an SSH authorized key. The application servicing the administrator initiates a setAuthenticationConfig control transaction to establish the authentication configuration.

The authentication configuration includes a login attempt limit value that is used to specify how account locking is handled. Account locking is invoked when the number of consecutive failed login attempts for a given account exceeds the login attempt limit value. After an account is locked, all further attempts to log in to that account are rejected. The account is unlocked by resetting the authentication token of the account using the setEnableAuthenticationTokenStatus control transaction. The account locking feature is disabled when the login attempt limit value is set to zero.

The administrator can add additional user accounts either through the CLI or an IPS manager.

Configuring Authentication on the Sensor

When a user tries to access the sensor through a service such as web server or the CLI, the identity of the user must be authenticated and the privileges of the user must be established. The service that is providing access to the user initiates an execAuthenticateUser control transaction request to the

AuthenticationApp to authenticate the identity of the user. The control transaction request typically includes the username and a password, or the identity of the user can be authenticated using an SSH authorized key.

The AuthenticationApp responds to the execAuthenticateUser control transaction request by attempting to authenticate the identity of the user. The AuthenticationApp returns a control transaction response that contains the authentication status and privileges of the user. If the identity of the user cannot be authenticated, the AuthenticationApp returns an unauthenticated status and anonymous user privileges in the control transaction response. The control transaction response also indicates if the account password has expired. User interface applications that authenticate users by initiating an execAuthenticateUser control transaction prompt the user to change the password.

The AuthenticationApp uses the underlying operating system to confirm the identity of a user. All the IPS applications send control transactions to the AuthenticationApp, which then uses the operating system to form its responses.

Remote shell services, Telnet and SSH, are not IPS applications. They call the operating system directly. If the user is authenticated, it launches the IPS CLI. In this case, the CLI sends a special form of the execAuthenticateUser control transaction to determine the privilege level of the logged-in user. The CLI then tailors the commands it makes available based on this privilege level.

Managing TLS and SSH Trust Relationships

Encrypted communications over IP networks provide data privacy by making it impossible for a passive attacker to discover from the packets exchanged alone the secret key needed to decrypt the data in the packets.

However, an equally dangerous attack vector is for an impostor to pretend to be the server end of the connection. All encryption protocols provide a means for clients to defend themselves from these attacks. IPS supports two encryption protocols, SSH and TLS, and the AuthenticationApp helps manage trust when the sensor plays either the client or server role in encrypted communications.

The IPS web server and SSH server are server endpoints of encrypted communications. They protect their identities with a private key and offer a public key to clients that connect to them. For TLS this public key is included inside an X.509 certificate, which includes other information. Remote systems that connect to the sensor should verify that the public key received during connection establishment is the key they expect.

Clients must maintain a list of trusted public keys to protect themselves from man-in-the-middle attacks. The exact procedure by which this trust is established varies depending on the protocol and client software. In general, the client displays a fingerprint of 16 or 20 bytes. The human operator who is configuring the client to establish trust should use an out-of-band method to learn the key fingerprints of the server before attempting to establish trust. If the fingerprints match, the trust relationship is established and henceforth the client can automatically connect with that server and be confident that the remote server is not an impostor.

You can use the **show ssh server-key** and **show tls fingerprint** to display the key fingerprints of the sensor. By recording the output of these commands when directly connected to the sensor console, you can reliably use this information to confirm the identity of the sensor over the network later when establishing trust relationships.

For example, when you initially connect to a sensor through the Microsoft Internet Explorer web browser, a security warning dialog box indicates that the certificate is not trusted. Using the user interface of Internet Explorer, you can inspect the certificate thumbprint, a value that should exactly match the SHA1 fingerprint displayed by the **show tls fingerprint** command. After verifying this, add this certificate to the list of trusted CAs of the browser to establish permanent trust.

Each TLS client has different procedures for establishing this trust. The sensor itself includes a TLS client that is used to send control transactions to other sensors and download upgrades and configuration files from other TLS web servers. Use the **tls trusted-host** command to establish trust of the TLS servers with which the sensor communicates.

Similarly, the sensor includes an SSH client that is used to communicate with managed network devices, download upgrades, and copy configurations and support files to remote hosts. Use the **ssh host-key** command to establish trust relationships with the SSH servers the sensor will contact.

You can manage the list of TLS trusted certificates and SSH known hosts through the commands **service trusted-certificates** and **service ssh-known-hosts**.

X.509 certificates include additional information that can increase the security of the trust relationship; however, these can lead to confusion. For example, an X.509 certificate includes a validity period during which the certificate can be trusted. Typically this period is a number of years starting at the moment the certificate is created. To ensure that an X.509 certificate is valid at the moment it is being used requires that the client system maintain an accurate clock.

X.509 certificates are also tied to a particular network address. Sensors fill this field with the IP address of the command and control interface of the sensor. Consequently, if you change the command and control IP address of the sensor, the X.509 certificate of the server is regenerated. You must reconfigure all clients on the network that trusted the old certificate to locate the sensor at its new IP address and trust the new certificate.

By using the SSH known hosts and TLS trusted certificates services in the AuthenticationApp, you can operate sensors at a high level of security.

Web Server

The web server provides SDEE support, which enables the sensor to report security events, receive IDIOM transactions, and serve IP logs. The web server supports HTTP 1.0 and 1.1. Communications with the web server often include sensitive information, such as passwords, that would severely compromise the security of the system if an attacker were able to eavesdrop. For this reason, sensors ship with TLS enabled. The TLS protocol is an encryption protocol that is compatible with SSL.

Note We deprecated the RDEP event sever service in IPS 6.1, and deleted it from the IPS 7.0(1) system architecture. The web server now uses the SDEE event server.

SensorApp

This section describes the SensorApp, and contains the following topics:

Understanding the SensorApp

The SensorApp performs packet capture and analysis. Policy violations are detected through signatures in the SensorApp and the information about the violations is forwarded to the Event Store in the form of an alert. Packets flow through a pipeline of processors fed by a producer designed to collect packets from the network interfaces on the sensor. Event actions can be associated with an event risk rating threshold that must be surpassed for the actions to take place. Some of the processors call inspectors to perform signature analysis. All inspectors can call the alarm channel to produce alerts as needed.

The SensorApp supports the following processors:

- Time Processor—This processor processes events stored in a time-slice calendar. Its primary task is to make stale database entries expire and to calculate time-dependent statistics.
- Deny Filters Processor—This processor handles the deny attacker functions. It maintains a list of denied source IP addresses. Each entry in the list expires based on the global deny timer, which you can configure in the virtual sensor configuration.
- Signature Event Action Processor—This processor processes event actions. Event actions can be associated with an event risk rating threshold that must be surpassed for the actions to take place. It supports the following event actions:
  - Reset TCP flow
  - IP log
  - Deny packets
  - Deny flow
  - Deny attacker
  - Alert
  - Block host
  - Block connection
  - Generate SNMP trap
  - Capture trigger packet
- Statistics Processor—This processor keeps track of system statistics such as packet counts and packet arrival rates.
- Layer 2 Processor—This processor processes layer 2-related events. It also identifies malformed packets and removes them from the processing path. You can configure actionable events for detecting malformed packets such as alert, capture packet, and deny packet. The layer 2 processor updates statistics about packets that have been denied because of the policy you have configured.
- Database Processor—This processor maintains the signature state and flow databases.
- Fragment Reassembly Processor—This processor reassembles fragmented IP datagrams. It is also responsible for normalization of IP fragments when the sensor is in inline mode.
- Stream Reassembly Processor—This processor reorders TCP streams to ensure the arrival order of the packets at the various stream-based inspectors. It is also responsible for normalization of the TCP stream. The normalizer engine lets you enable or disable alert and deny actions.

  The TCP Stream Reassembly Processor normalizer has a hold-down timer, which lets the stream state rebuild after a reconfiguration event. You cannot configure the timer. During the hold-down interval, the system synchronizes stream state on the first packet in a stream that passes through the system. When the hold down has expired, sensorApp enforces your configured policy. If this policy calls for a denial of streams that have not been opened with a 3-way handshake, established streams

that were quiescent during the hold-down period will not be forwarded and will be allowed to timeout. Those streams that were synchronized during the hold-down period are allowed to continue.

- Signature Analysis Processor—This processor dispatches packets to the inspectors that are not stream-based and that are configured for interest in the packet in process.
- Slave Dispatch Processor—A process found only on dual CPU systems.

The SensorApp also supports the following units:

- Analysis Engine—The Analysis Engine handles sensor configuration. It maps the interfaces and also the signature and alarm channel policy to the configured interfaces.
- Alarm Channel—The Alarm Channel processes all signature events generated by the inspectors. Its primary function is to generate alerts for each event it is passed.

Inline, Normalization, and Event Risk Rating Features

The SensorApp contains the following inline, normalization, and event risk rating features:

- Processing packets inline

  When the sensor is processing packets in the data path, all packets are forwarded without any modifications unless explicitly denied by policy configuration. Because of TCP normalization it is possible that some packets will be delayed to ensure proper coverage. When policy violations are encountered, the SensorApp allows for the configuration of actions. Additional actions are available in inline mode, such as deny packet, deny flow, and deny attacker.

  All packets that are unknown or of no interest to the IPS are forwarded to the paired interface with no analysis. All bridging and routing protocols are forwarded with no participation other than a possible deny due to policy violations. There is no IP stack associated with any interface used for inline (or promiscuous) data processing. The current support for 802.1q packets in promiscuous mode is extended to inline mode.

- IP normalization

  Intentional or unintentional fragmentation of IP datagrams can serve to hide exploits making them difficult or impossible to detect. Fragmentation can also be used to circumvent access control policies like those found on firewalls and routers. And different operating systems use different methods to queue and dispatch fragmented datagrams. If the sensor has to check for all possible ways that the end host will reassemble the datagrams, it makes the sensor vulnerable to denial of service attacks. Reassembling all fragmented datagrams inline and only forwarding completed datagrams, refragmenting the datagram if necessary, is the solution to this problem. The IP Fragmentation Normalization unit performs this function.

- TCP normalization

  Through intentional or natural TCP session segmentation, some classes of attacks can be hidden. To make sure policy enforcement can occur with no false positives and false negatives, the state of the two TCP endpoints must be tracked and only the data that is actually processed by the real host endpoints should be passed on. Overlaps in a TCP stream can occur, but are extremely rare except for TCP segment retransmits. Overwrites in the TCP session should not occur. If overwrites do occur, someone is intentionally trying to elude the security policy or the TCP stack implementation is broken. Maintaining full information about the state of both endpoints is not possible unless the sensor acts as a TCP proxy. Instead of the sensor acting as a TCP proxy, the segments will be ordered properly and the normalizer will look for any abnormal packets associated with evasion and attacks.

- Event risk rating

  Event risk rating helps reduce false positives from the system and gives you more control over what causes an alarm. The event risk rating incorporates the following additional information beyond the detection of a potentially malicious action:

  - Severity of the attack if it were to succeed
  - Fidelity of the signature
  - Relevance of the potential attack with respect to the target host
  - Overall value of the target host

SensorApp New Features

The SensorApp contains the following new features:

- Policy table—Provides a list of risk category settings (high, medium, and low).
- Evasion protection—Lets an inline interface mode sensor switch from strict mode to asymmetric mode for the Normalizer.
- Sensor health meter—Provides sensor-wide health statistics.
- Top services—Provides the top ten instances of the TCP, UDP, ICMP, and IP protocols.
- Security meter—Profiles alerts into threat categories and reports this information in red, yellow, and green buckets. You can configure the transition points for these buckets.
- Clear Flow state—Lets you clear the database, which causes the sensor to start fresh just as in a restart.
- Restart status—Reports periodically the current start and restart stages of the sensor.

Packet Flow

Packets are received by the NIC and placed in the kernel user-mapped memory space by the IPS-shared driver. The packet is prepended by the IPS header. Each packet also has a field that indicates whether to pass or deny the packet when it reaches Signature Event Action Processor.

The producer pulls packets from the shared-kernel user-mapped packet buffer and calls the process function that implements the processor appropriate to the sensor model. The following orders occur:

- Single processor execution

  Time Processor --> Layer 2 Processor --> Deny Filters Processor --> Fragment Reassembly Processor --> Statistics Processor --> Database Processor --> Signature Analysis Processor --> Stream Reassembly Processor --> Signature Event Action Processor

- Dual processor execution

  Execution Thread 1 Time Processor --> Layer 2 Processor --> Deny Filters Processor --> Fragment Reassembly Processor --> Statistics Processor --> Database Processor --> Signature Analysis Processor --> Slave Dispatch Processor --> | Execution Thread 2 Database Processor --> Stream Reassembly Processor --> Signature Event Action Processor

Signature Event Action Processor

The Signature Event Action Processor coordinates the data flow from the signature event in the Alarm Channel to processing through the Signature Event Action Override, the Signature Event Action Filter, and the Signature Event Action Handler. It consists of the following components:

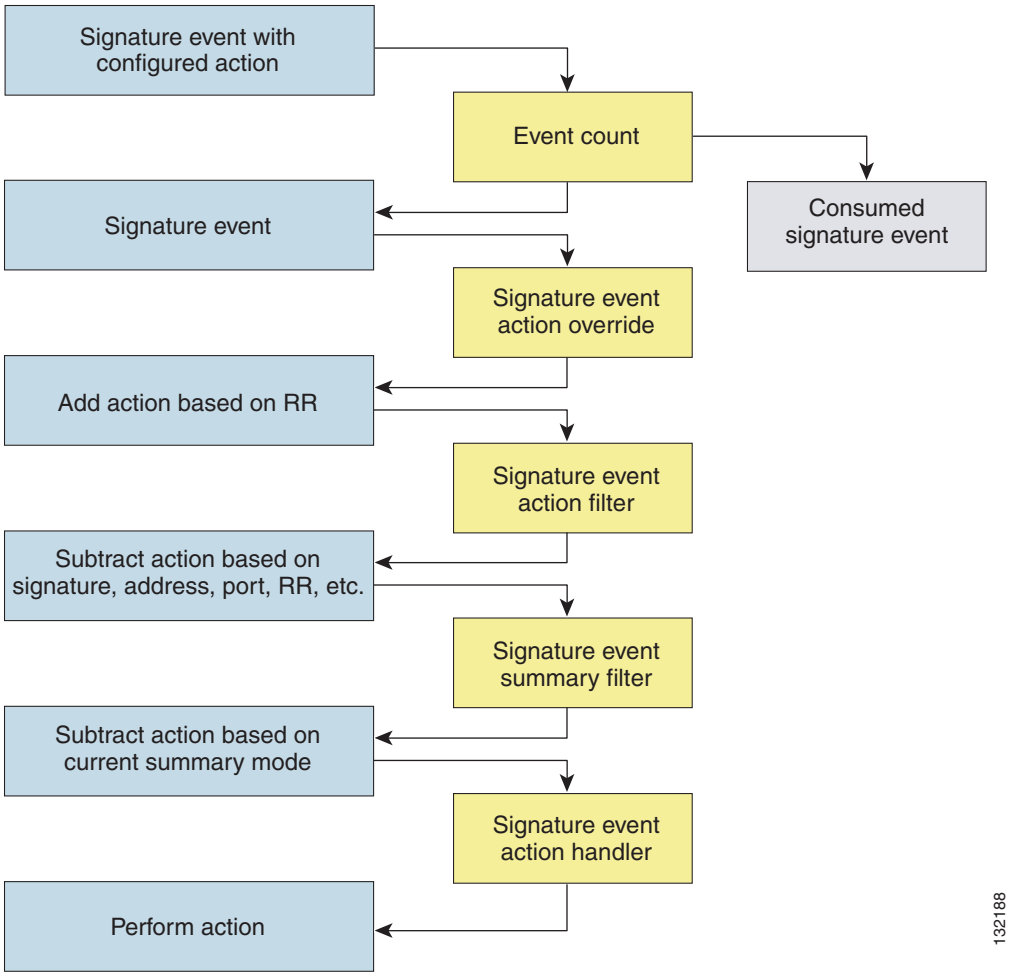
- Alarm Channel—The unit that represents the area to communicate signature events from the SensorApp inspection path to signature event handling.
- Signature Event Action Override—Adds actions based on the risk rating value. Signature Event Action Override applies to all signatures that fall in the range of the configured risk rating threshold. Each Signature Event Action Override is independent and has a separate configuration value for each action type.
- Signature Event Action Filter—Subtracts actions based on the signature ID, addresses, and risk rating of the signature event. The input to the Signature Event Action Filter is the signature event with actions possibly added by the Signature Event Action Override.

  Note The Signature Event Action Filter can only subtract actions, it cannot add new actions.

  The following parameters apply to the Signature Event Action Filter:
  - Signature ID
  - Subsignature ID
  - Attacker address
  - Attacker port
  - Victim address
  - Victim port
  - Risk rating threshold range
  - Actions to subtract
  - Sequence identifier (optional)
  - Stop-or-continue bit
  - Enable action filter line bit
  - Victim OS relevance or OS relevance
- Signature Event Action Handler—Performs the requested actions. The output from the Signature Event Action Handler is the actions being performed and possibly an evIdsAlert written to the Event Store.

Figure A-5 on page A-27 illustrates the logical flow of the signature event through the Signature Event Action Processor and the operations performed on the action for this event. It starts with the signature event with configured action received in the Alarm Channel and flows top to bottom as the signature event passes through the functional components of the Signature Event Action Processor.

Figure A-5 Signature Event Through Signature Event Action Processor



CollaborationApp

This section describes the CollaborationApp, and contains the following topics:

- Understanding the CollaborationApp, page A-27
- Update Components, page A-28
- Error Events, page A-29

Understanding the CollaborationApp

The CollaborationApp is a peer of the MainApp and the SensorApp. It interfaces with them using various interprocess communication technologies, such as IDAPI control transactions, semaphores, shared memory, and file exchange.

Reputation updates are exchanged between the Global Correlation server and the CollaborationApp. The CollaborationApp communicates with the sensors using four update components:

- Set of rules score weight values
- Set of IP addresses and address ranges, which together with the rules and alerts provide the information needed to calculate reputation scores
- List of IP addresses and address ranges for which traffic should always be denied
- Network participation configuration, which allows the server to control the rate at which sensors send telemetry date to the server

The sensor sends collaboration information to the Network Participation server. The sensor queries the Global Correlation server for a list of what collaboration updates are available and from which Global Correlation server to download the update files.

Note The SensorApp starts before the CollaborationApp, but they initialize asynchronously. Therefore, it is possible that the Reputation Update server may download and attempt to apply one or more global correlation updates before the SensorApp is ready to accept the update. The update server may download and partially process the update, but it must wait until the SensorApp is ready before it can commit the update.

For More Information

For detailed information on global correlation and how to configure it, see Chapter 14, "Configuring Global Correlation."

Update Components

The Global Correlation Update client exchanges manifests with the Global Correlation Update server. It parses the server manifest to determine what new updates are available for download and where they reside, and then builds a list of updates to be installed. If all updates are applied successfully, then the Global Correlation Update client commits the applied updates for each component, notifies SensorApp that new updates are available, and updates the client manifest to reflect the latest committed updates for each component.

The client manifest contains the UDI of the sensor, which includes the serial number of the sensor, and an encrypted shared secret that the server uses to verify the sensor is an authentic Cisco IPS sensor. The server manifest contains a list of update files available for each component. For each update file in the list, the server manifest contains data, such as the update version, type, order, location, file transfer protocol, and so forth.

There are two types of updates files: a full update file that replaces any existing data in the database of the component, and an incremental update that modifies the existing reputation data by adding, deleting, or replacing information. When all update files have been applied for all components, the temporary databases are committed by replacing the working databases.

Authentication and authorization are achieved though the secret encryption mechanism and decryption key management. The Global Correlation Update server authenticates the sensor using the shared secret encryption mechanism contained in the client manifest. The Global Correlation Update client authorizes sensors using decryption key management. Sensors that have been authenticated by the Global Correlation Update server are sent valid keys in the server manifest so that they can decrypt the update files.

Caution You receive a warning message if you have enabled global correlation, but you have not configured a DNS or HTTP proxy server. This warning is a reminder to either disable global correlation or add a DNS or HTTP proxy server.

For More Information

For the procedure for adding a DNS or HTTP proxy server to support global correlation, seeConfiguring Network Settings, page 6-1.

Error Events

Whenever a global correlation update fails, an evError event is generated. The error message is included in sensor statistics. The following conditions result in a status message with the severity of Error:

- The sensor is unlicensed
- No DNS or HTTP proxy server is configured
- The manifest exchange failed
- An update file download failed
- Applying or committing the update failed

An evError event is generated with the severity level of Warning if you edit and save either the host or global correlation configurations so that global correlation is enabled, but no DNS or HTTP proxy servers are configured.

For More Information

For the procedure for displaying sensor statistics, see Viewing Statistics, page 21-22.

SwitchApp

The 4500 series sensors have a built in switch that provides the external monitoring interfaces of the sensor. The SwitchApp is part of the IPS 4500 series design that enables the InterfaceApp and sensor initialization scripts to communicate with and control the switch. Any application that needs to get or set information on the switch must communicate with the SwitchApp. Additionally the SwitchApp implements the following:

- Detects bypass—When the SensorApp is not monitoring, the SwitchApp places the switch in bypass mode and then back to inspection mode once the SensorApp is up and running normally.
- Collects port statistics—The SwitchApp monitors the switch and collects statistics on the external interfaces of the switch for reporting by InterfaceApp.
- Handles the external interface configuration—When you update the interface configuration, the configuration is sent to the InterfaceApp, which updates the interface configuration for SwitchApp, which then forwards that configuration on to the switch.

CLI

This section describes the Cisco IPS CLI, and contains the following topics:

Understanding the CLI

The CLI provides the sensor user interface for all direct node access such as Telnet, SSH, and serial interface. You configure the sensor applications with the CLI. Direct access to the underlying OS is allowed through the service role.

User Roles

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

There are four user roles:

- Viewer—Can view configuration and events, but cannot modify any configuration data except their user passwords.
- Operator—Can view everything and can modify the following options:
  - Signature tuning (priority, disable or enable)
  - Virtual sensor definition
  - Managed routers
  - Their user passwords
- Administrator—Can view everything and can modify all options that operators can modify in addition to the following:
  - Sensor addressing configuration
  - List of hosts allowed to connect as configuration or viewing agents
  - Assignment of physical sensing interfaces
  - Enable or disable control of physical interfaces
  - Add and delete users and passwords
  - Generate new SSH host keys and server certificates
- Service—Only one user with service privileges can exist on a sensor. The service user cannot log in to the IME. The service user logs in to a bash shell rather than the CLI.

  The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed. You should only create an account with the service role for troubleshooting purposes. Only a user with administrator privileges can edit the service account.

When you log in to the service account, you receive the following warning:

```
************************ WARNING ************************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
*********************************************************************************
```

Note For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.

Service Account

The service account is a support and troubleshooting tool that enables TAC to log in to a native operating system shell rather than the CLI shell. It does not exist on the sensor by default. You must create it so that it is available for TAC to use for troubleshooting your sensor.

Only one service account is allowed per sensor and only one account is allowed a service role. When the password of the service account is set or reset, the password of the root account is set to the same password. This allows the service account user to su to root using the same password. When the service account is removed, the password of the root account is locked.

The service account is not intended to be used for configuration purposes. Only modifications made to the sensor through the service account under the direction of TAC are supported. Cisco Systems does not support the addition and/or running of an additional service to the operating system through the service account, because it affects proper performance and proper functioning of the other IPS services. TAC does not support a sensor on which additional services have been added.

You can track logins to the service account by checking the log file /var/log/.tac, which is updated with a record of service account logins.

Note The Cisco IPS incorporates several troubleshooting features that are available through the CLI, IDM, or IME. The service account is not necessary for most troubleshooting situations. You may need to create the service account at the direction of TAC to troubleshoot a very unique problem. The service account lets you bypass the protections built into the CLI and allows root privilege access to the sensor, which is otherwise disabled. We recommend that you do not create a service account unless it is needed for a specific reason. You should remove the service account when it is no longer needed.

Communications

This section describes the communications protocols used by Cisco IPS, and contains the following topics:

- SDEE, page A-33
- CIDEE, page A-34

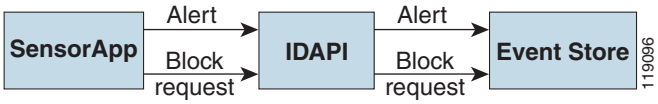
IDAPI

IPS applications use an interprocess communication API called the IDAPI to handle internal communications. The IDAPI reads and writes event data and provides a mechanism for control transactions. The IDAPI is the interface through which all the applications communicate.

The SensorApp captures and analyzes the network traffic on its interfaces. When a signature is matched, the SensorApp generates an alert, which is stored in the Event Store. If the signature is configured to perform the blocking response action, the SensorApp generates a block event, which is also stored in the Event Store.

Figure A-6 illustrates the IDAPI interface.

Figure A-6 IDAPI



Each application registers to the IDAPI to send and receive events and control transactions. The IDAPI provides the following services:

- Control transactions
  - Initiates the control transaction.
  - Waits for the inbound control transaction.
  - Responds to the control transaction.
- IPS events
  - Subscribes to remote IPS events, which are stored in the Event Store when received.
  - Reads IPS events from the Event Store.
  - Writes IPS events to the Event Store.

The IDAPI provides the necessary synchronization mechanisms to guarantee atomic data accesses.

IDIOM

IDIOM is a data format standard that defines the event messages that are reported by the IPS as well as the operational messages that are used to configure and control intrusion detection systems. These messages consist of XML documents that conform to the IDIOM XML schema.

IDIOM supports two types of interactions: event and control transaction. Event interactions are used to exchange IPS events such as alerts. IDIOM uses two types of messages for event interactions: event and error messages. Control transactions provide a means for one host to initiate an action in, change the state of, or read the state of another host. Control transactions utilize four types of IDIOM messages: request, response, configuration, and error messages. Events and control transactions that are communicated between application instances within a host are known as local events or local control

transactions, or collectively, local IDIOM messages. Events and control transactions that are communicated between different hosts are known as remote events and remote control transactions, or collectively, remote IDIOM messages.

Note IDIOM for the most part has been superseded by IDCONF, SDEE, and CIDEE.

IDCONF

The Cisco IPS manages its configuration using XML documents. IDCONF specifies the XML schema including the Cisco IPS control transactions. The IDCONF schema does not specify the contents of the configuration documents, but rather the framework and building blocks from which the configuration documents are developed. It provides mechanisms that let the IPS managers and CLI ignore features that are not configurable by certain platforms or functions through the use of the feature-supported attribute.

IDCONF messages are wrapped inside IDIOM request and response messages.

The following is an IDCONF example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<request xmlns="http://www.cisco.com/cids/idiom" schemaVersion="2.00">
  <editConfigDelta xmlns="http://www.cisco.com/cids/idconf">
    <component name="userAccount">
      <config typedefsVersion="2004-03-01" xmlns="http://www.cisco.com/cids/idconf">
        <struct>
           <map name="user-accounts‟ editOp=“merge”>
             <mapEntry>
               <key>
                <var name="name">cisco</var>
              </key>
               <struct>
                <struct name="credentials">
                  <var name="role">administrator</var>
                </struct>
               </struct>
            </mapEntry>
          </map>
        </struct>
      </config>
    </component>
  </editDefaultConfig>
</request>
```

SDEE

The Cisco IPS produces various types of events including intrusion alerts and status events. The IPS communicates events to clients such as management applications using the proprietary IPS-industry leading protocol, SDEE, which is a product-independent standard for communicating security device events. SDEE adds extensibility features that are needed for communicating events generated by various types of security devices.

Systems that use SDEE to communicate events to clients are referred to as SDEE providers. SDEE specifies that events can be transported using the HTTP or HTTP over SSL and TLS protocols. When HTTP or HTTPS is used, SDEE providers act as HTTP servers, while SDEE clients are the initiators of HTTP requests.

The IPS includes the web server, which processes HTTP or HTTPS requests. The web server uses run-time loadable servlets to process the different types of HTTP requests. Each servlet handles HTTP requests that are directed to the URL associated with the servlet. The SDEE server is implemented as a web server servlet.

The SDEE server only processes authorized requests. A request is authorized if is originates from a web server to authenticate the identity of the client and determine the privilege level of the client.

CIDEE

CIDEE specifies the extensions to SDEE that are used by the Cisco IPS. The CIDEE standard specifies all possible extensions that are supported by the Cisco IPS. Specific systems may implement a subset of CIDEE extensions. However, any extension that is designated as being required MUST be supported by all systems. CIDEE specifies the Cisco IPS-specific security device events and the IPS extensions to the SDEE evIdsAlert element.

CIDEE supports the following events:

- evError—Error event

  Generated by the CIDEE provider when the provider detects an error or warning condition. The evError event contains error code and textual description of the error.

- evStatus—Status message event

  Generated by CIDEE providers to indicate that something of potential interest occurred on the host. Different types of status messages can be reported in the status event—one message per event. Each type of status message contains a set of data elements that are specific to the type of occurrence that the status message is describing. The information in many of the status messages are useful for audit purposes. Errors and warnings are not considered status information and are reported using evError rather than evStatus.

- evShunRqst—Block request event

  Generated to indicate that a block action is to be initiated by the service that handles network blocking.

The following is a CDIEE extended event example:

```
<sd:events xmlns:cid="http://www.cisco.com/cids/2004/04/cidee"
xmlns:sd="“http://example.org/2003/08/sdee”>
 <sd:evIdsAlert eventId="1042648730045587005" vendor="Cisco‟ severity="medium">
  <sd:originator>
    <sd:hostId>Beta4Sensor1</sd:hostId>
    <cid:appName>sensorApp</cid:appName>
    <cid:appInstanceId>8971</cid:appInstanceId>
  </sd:originator>
  <sd:time offset="0" timeZone="UTC">1043238671706378000</sd:time>
  <sd:signature description="IOS Udp Bomb" id="4600" cid:version="S37">
    <cid:subsigId>0</cid:subsigId>
  </sd:signature> …
```

Cisco IPS File Structure

The Cisco IPS has the following directory structure:

- /usr/cids/idsRoot—Main installation directory.
- /usr/cids/idsRoot/shared—Stores files used during system recovery.

- /usr/cids/idsRoot/var—Stores files created dynamically while the sensor is running.
- /usr/cids/idsRoot/var/updates—Stores files and logs for update installations.
- /usr/cids/idsRoot/var/virtualSensor—Stores files used by SensorApp to analyze regular expressions.
- /usr/cids/idsRoot/var/eventStore—Contains the Event Store application.
- /usr/cids/idsRoot/var/core—Stores core files that are created during system crashes.
- /usr/cids/idsRoot/var/iplogs—Stores IP log file data.
- /usr/cids/idsRoot/bin—Contains the binary executables.
- /usr/cids/idsRoot/bin/authentication—Contains the authentication application.
- /usr/cids/idsRoot/bin/cidDump—Contains the script that gathers data for tech support.
- /usr/cids/idsRoot/bin/cidwebserver—Contains the web server application.
- /usr/cids/idsRoot/bin/cidcli—Contains the CLI application.
- /usr/cids/idsRoot/bin/nac—Contains the ARC application.
- /usr/cids/idsRoot/bin/logApp—Contains the logger application.
- /usr/cids/idsRoot/bin/mainApp—Contains the main application.
- /usr/cids/idsRoot/bin/sensorApp—Contains the sensor application.
- /usr/cids/idsRoot/bin/collaborationApp—Contains the collaboration application.
- /usr/cids/idsRoot/bin/switchApp—Contains the switch application.
- /usr/cids/idsRoot/etc—Stores sensor configuration files.
- /usr/cids/idsRoot/htdocs—Contains the IDM files for the web server.
- /usr/cids/idsRoot/lib—Contains the library files for the sensor applications.
- /usr/cids/idsRoot/log—Contains the log files for debugging.
- /usr/cids/idsRoot/tmp—Stores the temporary files created during run time of the sensor.

Summary of Cisco IPS Applications

Table A-2 gives a summary of the applications that make up the IPS.

Table A-2 Summary of Applications

Application	Description
AuthenticationApp	Authorizes and authenticates users based on IP address, password, and digital certificates.
Attack Response Controller	An ARC is run on every sensor. Each ARC subscribes to network access events from its local Event Store. The ARC configuration contains a list of sensors and the network access devices that its local ARC controls. If an ARC is configured to send network access events to a master blocking sensor, it initiates a network access control transaction to the remote ARC that controls the device. These network access action control transactions are also used by IPS managers to issue occasional network access actions.

Table A-2 Summary of Applications (continued)

Application	Description
CLI	Accepts command line input and modifies the local configuration using the IDAPI.
CollaborationApp	Shares information with other devices through a global correlation database to improve the combined efficacy of all the devices.
Control Transaction Server[1]	Accepts control transactions from a remote client, initiates a local control transaction, and returns the response to the remote client.
Control Transaction Source[2]	Waits for control transactions directed to remote applications, forwards the control transactions to the remote node, and returns the response to the initiator.
IDM	The Java applet that provides an HTML IPS management interface.
IME	The Java applet that provides an interface for viewing and archiving events.
InterfaceApp	Handles bypass and physical settings and defines paired interfaces. Physical settings are speed, duplex, and administrative state.
Logger	Writes all the log messages of the application to the log file and the error messages of the application to the Event Store.
MainApp	Reads the configuration and starts applications, handles starting and stopping of applications and node reboots, handles software upgrades.
NotificationApp	Sends SNMP traps when triggered by alert, status, and error events. NotificationApp uses the public domain SNMP agent. SNMP GETs provide information about the general health of the sensor.
SDEE Server[3]	Accepts requests for events from remote clients.
SensorApp	Captures and analyzes traffic on the monitored network and generates intrusion and network access events. Responds to IP logging control transactions that turn logging on and off and that send and delete IP log files.
SwitchApp	Part of the IPS 4500 series design that enables the InterfaceApp and sensor initialization scripts to communicate with and control the built-in switch. Any application that needs to get or set information on the switch must communicate with the SwitchApp.
Web Server	Waits for remote HTTP client requests and calls the appropriate servlet application.

1. This is a web server servlet.
2. This is a remote control transaction proxy.
3. This is a web server servlet.

Signature Engines

This appendix describes the IPS signature engines. It contains the following sections:

Understanding Signature Engines

A signature engine is a component of the Cisco IPS that is designed to support many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of parameters that have allowable ranges or sets of values.

Note The Cisco IPS engines support a standardized Regex.

Cisco IPS contains the following signature engines:

- AIC—Provides thorough analysis of web traffic. The AIC engine provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications, such as instant messaging and gotomypc, that try to tunnel over specified ports. You can also use AIC to inspect FTP traffic and control the commands being issued. There are two AIC engines: AIC FTP and AIC HTTP.
- Atomic—The Atomic engines are combined into four engines with multi-level selections. You can combine Layer 3 and Layer 4 attributes within one signature, for example IP + TCP. The Atomic engine uses the standardized Regex support. The Atomic engines consist of the following types:
  - Atomic ARP—Inspects Layer 2 ARP protocol. The Atomic ARP engine is different because most engines are based on Layer 3 IP protocol.
  - Atomic IP Advanced—Inspects IPv6 Layer 3 and ICMPv6 Layer 4 traffic.
  - Atomic IP—Inspects IP protocol packets and associated Layer 4 transport protocols. This engine lets you specify values to match for fields in the IP and Layer 4 headers, and lets you use Regex to inspect Layer 4 payloads.

    Note All IP packets are inspected by the Atomic IP engine. This engine replaces the 4.x Atomic ICMP, Atomic IP Options, Atomic L3 IP, Atomic TCP, and Atomic UDP engines.

  - Atomic IPv6—Detects two IOS vulnerabilities that are stimulated by malformed IPv6 traffic.
- Fixed—Performs parallel regular expression matches up to a fixed depth, then stops inspection using a single regular expression table. There are three Fixed engines: ICMP, TCP, and UDP.
- Flood—Detects ICMP and UDP floods directed at hosts and networks. There are two Flood engines: Flood Host and Flood Net.
- Meta—Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.
- Multi String—Inspects Layer 4 transport protocols and payloads by matching several strings for one signature. This engine inspects stream-based TCP and single UDP and ICMP packets.
- Normalizer—Configures how the IP and TCP Normalizer functions and provides configuration for signature events related to the IP and TCP Normalizer. Allows you to enforce RFC compliance.
- Service—Deals with specific protocols. The Service engines are divided in to the following protocol types:
  - DNS—Inspects DNS (TCP and UDP) traffic.
  - FTP—Inspects FTP traffic.
  - FTP V2—Supports IOS IPS. This signature engine provides a protocol decode engine tuned for IOS IPS. If you try to use this engine, you receive an error message.
  - Generic—Decodes custom service and payload, and generically analyzes network protocols.
  - H225—Inspects VoIP traffic. Helps the network administrator make sure the SETUP message coming in to the VoIP network is valid and within the bounds that the policies describe. Is also helps make sure the addresses and Q.931 string fields such as url-ids, email-ids, and display information adhere to specific lengths and do not contain possible attack patterns.
  - HTTP—Inspects HTTP traffic. The WEBPORTS variable defines inspection port for HTTP traffic.

- HTTP V2—Supports IOS IPS. This signature engine provides a protocol decode engine tuned for IOS IPS. If you try to use this engine, you receive an error message.
- IDENT—Inspects IDENT (client and server) traffic.
- MSRPC—Inspects MSRPC traffic.
- MSSQL—Inspects Microsoft SQL traffic.
- NTP—Inspects NTP traffic.
- P2P—Inspects P2P traffic.
- RPC—Inspects RPC traffic.
- SMB Advanced—Processes Microsoft SMB and Microsoft DCE/RPC (MSRPC) over SMB packets.

Note The SMB engine has been replaced by the SMB Advanced engine. Even though the SMB engine is still visible in IDM, IME, and the CLI, its signatures have been obsoleted; that is, the new signatures have the obsoletes parameter set with the IDs of their corresponding old signatures. Use the new SMB Advanced engine to rewrite any custom signature that were in the SMB engine.

- SMPT V1—Supports IOS IPS.

  This signature engine provides a protocol decode engine tuned for IOS IPS. If you try to use this engine, you receive an error message.
- SNMP—Inspects SNMP traffic.
- SSH—Inspects SSH traffic.
- TNS—Inspects TNS traffic.

- State—Conducts stateful searches of strings in protocols such as SMTP. The state engine has a hidden configuration file that is used to define the state transitions so new state definitions can be delivered in a signature update.
- String—Searches on Regex strings based on ICMP, TCP, or UDP protocol. There are three String engines: String ICMP, String TCP, and String UDP.
- String XL—Searches on Regex strings based on ICMP, TCP, or UDP protocol.The String XL engines provide optimized operation for the Regex accelerator card. There are three String engines: String ICMP XL, String TCP XL, and String UDP XL.

Note The IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP support the String XL engines and the Regex accelerator card.

Note The Regex accelerator card is used for both the standard String engines and the String XL engines. Most standard String engine signatures can be compiled and analyzed by the Regex accelerator card without modification. However, there are special circumstances in which the standard String engine signatures cannot be compiled for the Regex accelerator card. In these situations a new signature is written in a String XL engine using the specific parameters in the String XL engine that do compile on the Regex accelerator card. The new signature in the String XL engine obsoletes the original signature in the standard String engine.

- Sweep—Analyzes sweeps from a single host (ICMP and TCP), from destination ports (TCP and UDP), and multiple ports with RPC requests between two nodes. There are two Sweep engines: Sweep and Sweep Other TCP.
- Traffic Anomaly—Inspects TCP, UDP, and other traffic for worms.
- Traffic ICMP—Analyzes nonstandard protocols, such as TFN2K, LOKI, and DDOS. There are only two signatures with configurable parameters.
- Trojan—Analyzes traffic from nonstandard protocols, such as BO2K andTFN2K. There are three Trojan engines: Bo2k, Tfn2k, and UDP. There are no user-configurable parameters in these engines.

Master Engine

The Master engine provides structures and methods to the other engines and handles input from configuration and alert output. This section describes the Master engine, and contains the following topics:

- General Parameters, page B-4
- Alert Frequency, page B-7
- Event Actions, page B-8

General Parameters

The following parameters are part of the Master engine and apply to all signatures (if it makes sense for that signature engine).

Table B-1 lists the general master engine parameters.

Table B-1 Master Engine Parameters

Parameter	Description	Value
Signature ID	Specifies the ID of this signature.	*number*
Sub Signature ID	Specifies the sub ID of this signature	*number*
Alert Severity	Specifies the severity of the alert: • Dangerous alert • Medium-level alert • Low-level alert • Informational alert	High Medium Low Informational (default)

Table B-1 Master Engine Parameters (continued)

Parameter	Description	Value
Sig Fidelity Rating	Specifies the rating of the fidelity of this signature.	0 to 100 (default = 100)
Promiscuous Delta	Specifies the delta value used to determine the seriousness of the alert.	0 to 30 (default = 5)
Signature Name	Specifies the name of the signature.	*sig-name*
Alert Notes	Provides additional information about this signature that will be included in the alert message.	*alert-notes*
User Comments	Provides comments about this signature.	*comments*
Alert Traits	Specifies traits you want to document about this signature.	0 to 65335
Release	Provides the release in which the signature was most recently updated.	*release*
Signature Creation Date	Specifies the date the signature was created.	—
Signature Type	Specifies the signature category.	Anomaly Component Exploit Other
Engine	Specifies the engine to which the signature belongs. **Note** The engine-specific parameters appear under the Engine category.	—
Event Count	Specifies the number of times an event must occur before an alert is generated.	1 to 65535 (default = 1)
Event Count Key	Specifies the storage type on which to count events for this signature: • Attacker address • Attacker and victim addresses • Attacker address and victim port • Victim address • Attacker and victim addresses and ports	Axxx AxBx Axxb xxBx AaBb
Specify Alert Interval {Yes | No}	Enables the alert interval: • Alert Interval—Specifies the time in seconds before the event count is reset.	2 to 1000
Status	Specifies whether the signature is enabled or disabled, active or retired.	Enabled | Retired {Yes | No}
Obsoletes	Indicates that a newer signature has disabled an older signature.	—

Table B-1 Master Engine Parameters (continued)

Parameter	Description	Value
Vulnerable OS List	When combined with passive OS fingerprinting, it allows the IPS to determine if it is likely a given attack is relevant to the target system.	AIX BSD General OS HP-UX IOS IRIX Linux Mac OS Netware Other Solaris UNIX Windows Windows NT Windows NT/2K/XP
Mars Category {Yes| No}	Maps signatures to a MARS attack category.[1]	—

1. This is a static information category that you can set in the configuration and view in the alerts.Refer to the MARS documentation for more information.

Promiscuous Delta

The promiscuous delta lowers the risk rating of certain alerts in promiscuous mode. Because the sensor does not know the attributes of the target system and in promiscuous mode cannot deny packets, it is useful to lower the prioritization of promiscuous alerts (based on the lower risk rating) so the administrator can focus on investigating higher risk rating alerts. In inline mode, the sensor can deny the offending packets so that they never reach the target host, so it does not matter if the target was vulnerable. Because the attack was not allowed on the network, the IPS does not subtract from the risk rating value. Signatures that are not service, OS, or application-specific have 0 for the promiscuous delta. If the signature is specific to an OS, service, or application, it has a promiscuous delta of 5, 10, or 15 calculated from 5 points for each category.

Caution We recommend that you do NOT change the promiscuous delta setting for a signature.

Obsoletes

The Cisco signature team uses the obsoletes field to indicate obsoleted, older signatures that have been replaced by newer, better signatures, and to indicate disabled signatures in an engine when a better instance of that engine is available. For example, some String XL hardware-accelerated signatures now replace equivalent signatures that were defined in the String engine.

Vulnerable OS List

When you combine the vulnerable OS setting of a signature with passive OS fingerprinting, the IPS can determine if it is likely that a given attack is relevant to the target system. If the attack is found to be relevant, the risk rating value of the resulting alert receives a boost. If the relevancy is unknown, usually because there is no entry in the passive OS fingerprinting list, then no change is made to the risk rating. If there is a passive OS fingerprinting entry and it does not match the vulnerable OS setting of a signature, the risk rating value is decreased. The default value by which to increase or decrease the risk rating is +/- 10 points.

For More Information

- For more information about promiscuous mode, see Promiscuous Mode, page 7-10.
- For more information about passive OS fingerprinting, see Configuring OS Identifications, page 12-23.

Alert Frequency

The purpose of the alert frequency parameter is to reduce the volume of the alerts written to the Event Store to counter IDS DoS tools, such as stick. There are four modes: Fire All, Fire Once, Summarize, and Global Summarize. The summary mode is changed dynamically to adapt to the current alert volume. For example, you can configure the signature to Fire All, but after a certain threshold is reached, it starts summarizing.

Table B-2 lists the alert frequency parameters.

Table B-2 Master Engine Alert Frequency Parameters

Parameter	Description	Value
Summary Mode	Specifies the mode used for summarization: • Fire All—Fires an alert on all events. • Fire Once—Fires an alert only once. • Global Summarize—Summarizes an alert so that it only fires once regardless of how many attackers or victims. • Summarize—Summarizes alerts.	Fire All Fire Once Global Summarize Summarize
Specify Summary Threshold {Yes | No}	Enables summary threshold mode: • Summary Threshold—Specifies the threshold number of alerts to send a signature into summary mode. • Summary Interval—Specifies the time in seconds used in each summary alert.	0 to 65535 1 to 1000
Specify Global Summary Threshold {Yes | No}	Enables global summary threshold mode: • Global Summary Threshold—Specifies the threshold number of events to take alerts into global summary.	1 to 65535
Summary Key	Specifies the storage type on which to summarize this signature: • Attacker address • Attacker and victim addresses • Attacker address and victim port • Victim address • Attacker and victim addresses and ports	Axxx AxBx Axxb xxBx AaBb

Event Actions

The Cisco IPS supports the following event actions. Most of the event actions belong to each signature engine unless they are not appropriate for that particular engine.

Alert and Log Actions

- Product Alert—Writes an alert to Event Store.
- Produce Verbose Alert—Includes an encoded dump (possibly truncated) of the offending packet in the alert.
- Log Attacker Packets—Starts IP logging of packets containing the attacker address and sends an alert.
- Log Victim Packets—Starts IP logging of packets containing the victim address and sends an alert.
- Log Attacker/Victim Pair Packets (inline mode only)—Starts IP logging of packets containing the attacker/victim address pair.
- Request SNMP Trap—Sends request to the NotificationApp to perform SNMP notification.

Deny Actions

- Deny Packet Inline (inline mode only)—Does not transmit this packet.

  Note You cannot delete the event action override for Deny Packet Inline because it is protected. If you do not want to use that override, disable it.

- Deny Connection Inline (inline mode only)—Does not transmit this packet and future packets on the TCP Flow.
- Deny Attacker Victim Pair Inline (inline mode only)—Does not transmit this packet and future packets on the attacker/victim address pair for a specified period of time.
- Deny Attacker Service Pair Inline (inline mode only)—Does not transmit this packet and future packets on the attacker address victim port pair for a specified period of time.
- Deny Attacker Inline (inline mode only)—Does not transmit this packet and future packets from the attacker address for a specified period of time.

  Note This is the most severe of the deny actions. It denies the current and future packets from a single attacker address. Each deny address times out for *X* seconds from the first event that caused the deny to start, where X is the amount of seconds that you configured. You can clear all denied attacker entries by choosing **Configuration > sensor_name > Sensor Management > Time-Based Actions > Denied Attackers > Clear List**, which permits the addresses back on the network.

- Modify Packet Inline (inline mode only)—Modifies packet data to remove ambiguity about what the end point might do with the packet.

  Note The event action Modify Packet Inline is part of the Normalizer engine. It scrubs the packet and corrects irregular issues such as bad checksum, out of range values, and other RFC violations.

Other Actions

Note IPv6 does not support the following event actions: Request Block Host, Request Block Connection, or Request Rate Limit.

- Request Block Connection—Requests the ARC to block this connection.
- Request Block Host—Requests the ARC to block this attacker host.
- Request Rate Limit—Requests the ARC to perform rate limiting.
- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow.

Regular Expression Syntax

Regular expressions (Regex) are a powerful and flexible notational language that allow you to describe text. In the context of pattern matching, regular expressions allow a succinct description of any arbitrary pattern.

Table B-3 lists the IPS signature Regex syntax.

Table B-3 Signature Regular Expression Syntax

Metacharacter	Name	Description
?	Question mark	Repeat 0 or 1 times.
*	Star, asterisk	Repeat 0 or more times.
+	Plus	Repeat 1 or more times.
{x}	Quantifier	Repeat exactly *X* times.
{x,}	Minimum quantifier	Repeat at least *X* times.
.	Dot	Any one character except new line (0x0A).
[abc]	Character class	Any character listed.
[^abc]	Negated character class	Any character not listed.
[a-z]	Character range class	Any character listed inclusively in the range.
( )	Parenthesis	Used to limit the scope of other metacharacters.
|	Alternation, or	Matches either expression it separates.
^	caret	The beginning of the line.
char	Escaped character	When *char* is a metacharacter or not, matches the literal *char*.
char	Character	When char is not a metacharacter, matches the literal char.
\r	Carriage return	Matches the carriage return character (0x0D).
\n	New line	Matches the new line character (0x0A).
\t	Tab	Matches the tab character (0x09).
\f	Form feed	Matches the form feed character (0x0C).

Table B-3 Signature Regular Expression Syntax (continued)

Metacharacter	Name	Description
\xNN	Escaped hexadecimal character	Matches character with the hexadecimal code 0xNN (0<=N<=F).
\NNN	Escaped octal character	Matches the character with the octal code NNN (0<=N<=8).

All repetition operators will match the shortest possible string as opposed to other operators that consume as much of the string as possible thus giving the longest string match.

Table B-4 lists examples of Regex patterns.

Table B-4 Regex Patterns

To Match	Regular Expression
Hacker	Hacker
Hacker or hacker	[Hh]acker
Variations of bananas, banananas, bananananananas	ba(na)+s
foo and bar on the same line with anything except a new line between them	foo.*bar
Either foo or bar	foo|bar
Either moon or soon	(m|s)oon

AIC Engine

The Application Inspection and Control (AIC) engine inspects HTTP web traffic and enforces FTP commands. This section describes the AIC engine and its parameters, and contains the following topics:

- Understanding the AIC Engine, page B-10
- AIC Engine and Sensor Performance, page B-11
- AIC Engine Parameters, page B-11

Understanding the AIC Engine

AIC provides thorough analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications, such as instant messaging and gotomypc, that try to tunnel over specified ports. Inspection and policy checks for P2P and instant messaging are possible if these applications are running over HTTP. AIC also provides a way to inspect FTP traffic and control the commands being issued. You can enable or disable the predefined signatures or you can create policies through custom signatures.

Note The AIC engines run when HTTP traffic is received on AIC web ports. If traffic is web traffic, but not received on the AIC web ports, the Service HTTP engine is executed. AIC inspection can be on any port if it is configured as an AIC web port and the traffic to be inspected is HTTP traffic.

AIC Engine and Sensor Performance

Application policy enforcement is a unique sensor feature. Rather than being based on traditional IPS technologies that inspect for exploits, vulnerabilities, and anomalies, AIC policy enforcement is designed to enforce HTTP and FTP service policies. The inspection work required for this policy enforcement is extreme compared with traditional IPS inspection work. A large performance penalty is associated with using this feature. When AIC is enabled, the overall bandwidth capacity of the sensor is reduced.

AIC policy enforcement is disabled in the IPS default configuration. If you want to activate AIC policy enforcement, we highly recommend that you carefully choose the exact policies of interest and disable those you do not need. Also, if your sensor is near its maximum inspection load capacity, we recommend that you not use this feature since it can oversubscribe the sensor. We recommend that you use the adaptive security appliance firewall to handle this type of policy enforcement.

AIC Engine Parameters

The AIC engines define signatures for deep inspection of web traffic. They also define signatures that authorize and enforce FTP commands. There are two AIC engines: AIC HTTP and AIC FTP. The AIC engines have the following features:

- Web traffic:
  - RFC compliance enforcement
  - HTTP request method authorization and enforcement
  - Response message validation
  - MIME type enforcement
  - Transfer encoding type validation
  - Content control based on message content and type of data being transferred
  - URI length enforcement
  - Message size enforcement according to policy configured and the header
  - Tunneling, P2P and instant messaging enforcement.

    This enforcement is done using regular expressions. There are predefined signature but you can expand the list.
- FTP traffic:
  - FTP command authorization and enforcement

Table B-5 lists the parameters that are specific to the AIC HTTP engine.

Table B-5 AIC HTTP Engine Parameters

Parameter	Description
Signature Type	Specifies the type of AIC signature.
Content Types	Specifies an AIC signature that deals with MIME types: • Define Content Type—Associates actions such as denying a specific MIME type (image/gif), defining a message-size violation, and determining that the MIME-type mentioned in the header and body do not match. • Define Recognized Content Types—Lists content types recognized by the sensor.
Define Web Traffic Policy	Specifies the action to take when noncompliant HTTP traffic is seen. Alarm on Non-HTTP Traffic {Yes | No} enables the signature. This signature is disabled by default.
Max Outstanding Requests Overrun	Specifies the maximum allowed HTTP requests per connection (1 to 16).
Msg Body Pattern	Uses Regex to define signatures that look for specific patterns in the message body.
Request Methods	Specifies the AIC signature that allows actions to be associated with HTTP request methods: • Define Request Method—Specifies get, put, and so forth. • Recognized Request Methods—Lists methods recognized by the sensor.
Transfer Encoding	Specifies the AIC signature that deals with transfer encodings: • Define Transfer Encoding—Associates an action with each method, such as compress, chunked, and so forth. • Recognized Transfer Encodings—Lists methods recognized by the sensor. • Chunked Transfer Encoding—Specifies actions to be taken when a chunked encoding error is seen.

Table B-6 lists the parameters that are specific to the AIC FTP engine.

Table B-6 AIC FTP Engine Parameters

Parameter	Description
Signature Type	Specifies the type of AIC signature.
FTP Commands	Associates an action with an FTP command: • FTP Command—Lets you choose the FTP command you want to inspect.
Unrecognized FTP Command	Inspects unrecognized FTP commands.

For More Information

- For the procedures for configuring AIC engine signatures, see Configuring Application Policy Signatures, page 10-42.
- For an example of a custom AIC signature, see Tuning an AIC Signature, page 10-50.
- For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Atomic Engine

The Atomic engine contains signatures for simple, single packet conditions that cause alerts to be fired. This section describes the Atomic engine, and contains the following topics:

Atomic ARP Engine

The Atomic ARP engine defines basic Layer 2 ARP signatures and provides more advanced detection of the ARP spoof tools dsniff and ettercap.

Table B-7 lists the parameters that are specific to the Atomic ARP engine.

Table B-7 Atomic ARP Engine Parameters

Parameter	Description	Value
Specify ARP Operation {Yes | No}	(Optional) Enables ARP operation: • ARP Operation—Specifies the type of ARP operation to inspect.	0 to 65535
Specify Mac Flip Times {Yes | No}	(Optional) Enables MAC address flip times: • Mac Flip Times—Specifies how many times to flip the MAC address in the alert.	0 to 65535
Specify Request Inbalance {Yes | No}	(Optional) Enables request inbalance: • Request Inbalance—Specifies the value for firing an alert when there are this many more requests than replies on the IP address.	0 to 65535

Table B-7 Atomic ARP Engine Parameters (continued)

Parameter	Description	Value
Specify Type of ARP Sig {Yes | No}	(Optional) Enables the ARP signature type: • Type of ARP Sig—Specifies the type of ARP signatures you want to fire on: – Destination Broadcast—Fires an alert for this signature when it sees an ARP destination address of 255.255.255.255. – Same Source and Destination—Fires an alert for this signature when it sees an ARP destination address with the same source and destination MAC address – Source Broadcast (default)—Fires an alert for this signature when it sees an ARP source address of 255.255.255.255. – Source Multicast—Fires an alert for this signature when it sees an ARP source MAC address of 01:00:5e:(00-7f).	Dst Broadcast Same Src and Dst Src Broadcast Src Multicast
Storage Key	Specifies the type of address key used to store persistent data: • Attacker address • Attacker and victim addresses • Victim address • Global	Axxx AxBx xxBx xxxx

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Atomic IP Advanced Engine

The Atomic IP Advanced engine parses and interprets the IPv6 header and its extensions, the IPv4 header and its options, ICMP, ICMPv6, TCP, and UDP, and seeks out anomalies that indicate unusual activity.

Atomic IP Advanced engine signatures do the following:

- Inspect for anomalies in IP addresses, for example, spoofed addresses.
- Inspect for bad information in the length fields of the packet.
- Fire informational alerts about the packet.
- Fire higher severity alerts for the limited set of known vulnerabilities.
- Duplicate any IPv6-specific signatures in Engine Atomic IP that can also apply to IPv6.
- Provide default signatures for identifying tunneled traffic based on IP address, port, protocol, and limited information from the packet data.

Only the outermost IP tunnel is identified. When an IPv6 tunnel or IPv6 traffic inside of an IPv4 tunnel is detected, a signature fires an alert. All of the other IPv6 traffic in embedded tunnels is not inspected. The following tunneling methods are supported, but not individually detected. For example, ISATAP, 6to4, and manual IPv6 RFC 4213 tunnels all appear as IPv6 in IPv4, which is detected by signature 1007:

- ISATAP
- 6to4 (RFC 3056)
- Manually configured tunnels (RFC 4213)
- IPv6 over GRE
- Teredo (IPv6) inside UDP
- MPLS (unencrypted)
- IPv6 over IPv6

IPv6 supports the following:

- Denying by source IP address, destination IP address, or IP address pair
- Alerts
- Resetting the TCP connection
- Logging

Atomic IP Advanced Engine Restrictions

The Atomic IP Advanced engine contains the following restrictions:

- Cannot detect the Layer 4 field of the packets if the packets are fragmented so that the Layer 4 identifier does not appear in the first packet.
- Cannot detect Layer 4 attacks in flows with packets that are fragmented by IPv6 because there is no fragment reassembly.
- Cannot detect attacks with tunneled flows.
- Limited checks are provided for the fragmentation header.
- There is no support for IPv6 on the management (command and control) interface.
- If there are illegal duplicate headers, a signature fires, but the individual headers cannot be separately inspected.
- Anomaly detection does not support IPv6 traffic; only IPv4 traffic is directed to the anomaly detection processor.
- Rate limiting and blocking are not supported for IPv6 traffic. If a signature is configured with a block or rate limit event action and is triggered by IPv6 traffic, an alert is generated but the action is not carried out.

Note The second number in the ranges must be greater than or equal to the first number.

Table B-8 lists the parameters that are specific to the Atomic IP Advanced engine.

Table B-8 Atomic IP Advanced Engine Parameters

Parameter	Description	Value
Global		
Fragment Status	Specifies whether or not fragments are wanted.	Any | No Fragments | Want Fragments
Encapsulation {Yes | No}	(Optional) Enables any encapsulation before the start of Layer 3 for the packet:[1] • Encapsulation—Specifies the type of encapsulation to inspect.	None | MPLS | GRE | Ipv4 in IPv6 | IP IP | Any
IP Version {Yes | No}	(Optional) Enables the IP protocol version: • IP Version—Specifies IPv4 or IPv6.	IPv4 | IPv6
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)
Regex		
Specify Regex Inspection	(Optional) Enables Regex inspection.	Yes | No
Regex Search Scope	Specifies the start and end points for the regular expression search.	ipv6-doh-only ipv6-doh-plus ipv6-hoh-only ipv6-hoh-plus ipv6-rh-only ipv6-rh-plus layer3-only layer3-plus layer4
Regex String	Specifies the regular expression to search for in a single TCP packet.	*string*
Specify Exact Match Offset {Yes | No}	Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the Regex String must report for a match to be valid.	0 to 65535
Specify Min Match Length {Yes | No}	Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the Regex String must match.	0 to 65535
Specify Min Match Offset {Yes | No}	Enables minimum match offset: • Min Match Offset—Specifies the minimum stream offset the Regex String must report for a match to be valid.	0 to 65535

Table B-8 Atomic IP Advanced Engine Parameters (continued)

Parameter	Description	Value
Specify Max Match Offset {Yes | No}	Enables maximum match offset: • Max Match Offset—Specifies the maximum stream offset the Regex String must report for a match to be valid.	0 to 65535
IPv6		
Authentication Header {Yes | No}	(Optional) Enables inspection of the authentication header: • AH Present—Inspects the authentication header: – AH Length—Specifies the length of the authentication header to inspect. – AH Next Header—Specifies the value of the authentication header to inspect.	Have AH | No AH • 0 to 1028 • 0 to 255
Destination Options Header {Yes | No}	(Optional) Enables inspection of the destination options header: • DOH Present —Inspects the destination options header: – DOH Count —Specifies the number of destination options headers to inspect. – DOH Length—Specifies the length of destination options headers to inspect. – DOH Next Header—Specifies the number of next destination options headers to inspect. – DOH Option Type—Specifies the type of destination options headers to inspect. – DOH Option Length —Specifies the length of destination options headers to inspect.	Have DOH | No DO • 0 to 2 • 8 to 2048 • 0 to 255 • 0 to 255 • 0 to 255
Specify ESP Header {Yes | No}	(Optional) Enables inspection of the ESP header: • ESP Present—Inspects the ESP header.	Have ESP | No ESP
Specify First Next Header {Yes | No}	(Optional) Enables inspection of the first next header: • First Next Header—Specifies the value of the first next header to inspect.	0 to 255

Table B-8 Atomic IP Advanced Engine Parameters (continued)

Parameter	Description	Value
Specify Flow Label {Yes | No}	(Optional) Enables inspection of the flow label: • Flow Label—Specifies the value of the flow label to inspect.	0 to 1048575
Specify Headers Out of Order {Yes | No}	(Optional) Enables inspection of out-of-order headers: • Headers Out of Order—Inspects headers that are out of order.	Yes | No
Specify Headers Repeated {Yes | No}	(Optional) Enables inspection of repeated headers: • Headers Repeated—Inspects repeated headers.	Yes | No
Specify Hop Limit {Yes | No}	(Optional) Enables hop limit: • Hop Limit—Specifies the value of the hop limit to inspect.	0 to 255
Specify Hop Options Header {Yes | No}	(Optional) Enables inspection of the hop-by-hop options header: • HOH Present—Inspects the hop-by-hop options header.	Have HOH | No HOH
Specify IPv6 Address Options {Yes | No}	(Optional) Enables the IPv6 address options: • IPv6 Address Options—Specifies the IPv6 address options: – Address With Localhost—IP address with ::1. – Documentation Address—IP address with 2001:db8::/32 prefix. – IPv6 Address—IP address. – Link Local Address—Inspects for an IPv6 link local address. – Multicast Destination—Inspects for a destination multicast address. – Multicast Source—Inspects for a source multicast address. – Not Link Local Address—Inspects for an address that is not link-local. – Not Valid Address—Inspects for an address that is not reserved for link-local, global, or multicast. – Source IP Equals Destination IP—Source and destination addresses are the same.	Yes | No

Table B-8 Atomic IP Advanced Engine Parameters (continued)

Parameter	Description	Value
Specify IPv6 Data Length {Yes | No}	(Optional) Enables inspection of IPv6 data length: • IPv6 Data Length—Specifies the IPv6 data length to inspect.	0 to 65535
Specify IPv6 Header Length {Yes | No}	(Optional) Enables inspection of IPv6 header length: • Pv6 Header Length—Specifies the length of the IPv6 header to inspect.	0 to 65535
Specify IPv6 Total Length {Yes | No}	(Optional) Enables inspection of IPv6 total length: • IPv6 Total Length—Specifies the IPv6 total length to inspect.	0 to 65535
Specify IPv6 Payload Length {Yes | No}	(Optional) Enables inspection of IPv6 payload length: • IPv6 Payload Length—Specifies the IPv6 payload length to inspect.	0 to 65535
Specify Routing Header {Yes | No}	(Optional) Enables inspection of the routing header: • RH Present—Inspects the routing header.	Have RH | No RH
Specify Traffic Class {Yes | No}	(Optional) Enables inspection of the traffic class: • Traffic Class—Specifies the value of the traffic class to inspect.	0 to 255
IPV4		
Specify IP Addr Options {Yes | No}	(Optional) Enables IP address options: • IP Addr Options—Specifies the IP address options.	Address With Localhost IP Address[2] RFC 1918 Address Src IP Eq Dst IP
Specify IP Header Length {Yes | No}	(Optional) Enables inspection of the IP header length: • IP Header Length—Specifies the length of the IP header to inspect.	0 to 16
Specify IP Identifier {Yes | No}	(Optional) Enables inspection of the IP identifier: • IP Identifier—Specifies the IP ID to inspect.	0 to 255

Table B-8 Atomic IP Advanced Engine Parameters (continued)

Parameter	Description	Value
Specify IP Option Inspection {Yes | No}	(Optional) Enables inspection of the IP options: • IP Option Inspection—Specifies the value of the IP option: – IP Option—IP OPTION code to match. – IP Option Abnormal Options—The list of options is malformed.	0 to 65535
Specify IP Payload Length {Yes | No}	(Optional) Enables inspection of the IP payload length: • IP Payload Length—Specifies the length of the IP payload to inspect.	0 to 65535
Specify IP Type of Service {Yes | No}	(Optional) Enables inspection of the IP type of service: • IP Type of Service—Specifies the IP type of service to inspect.	0 to 255
Specify IP Total Length {Yes | No}	(Optional) Enables inspection of the IP total length: • IP Total Length—Specifies the total length of the IP packet to inspect.	0 to 65535
Specify IP Time-to-Live {Yes | No}	(Optional) Enables inspection of the IP time-to-live: • IP Time-to-Live—Specifies the value of the IP TTL to inspect.	0 to 255
Specify IP Version {Yes | No}	(Optional) Enables inspection of the IP version: • IP Version—Specifies which IP version to inspect.	0 to 16
L4 Protocol		
Specify L4 Protocol {Yes | No}	(Optional) Enables inspection of Layer 4 protocol: • L4 Protocol—Specifies which Layer 4 protocol to inspect.	ICMP Protocol ICMPv6 Protocol TCP Protocol UDP Protocol Other IP Protocols
L4 Protocol Other		
Specify Other IP Protocol ID	(Optional) Enables inspection of other Layer 4 protocols: • Other IP Protocol ID—Specifies which single IP protocol ID or single range of IP protocol IDs for which to send alerts.	0 to 255

Table B-8 Atomic IP Advanced Engine Parameters (continued)

Parameter	Description	Value
L4 Protocol ICMP		
Specify ICMP Code {Yes | No}	(Optional) Enables inspection of Layer 4 ICMP code: • ICMP Code—Specifies the value of the ICMP header CODE.	0 to 65535
Specify ICMP ID {Yes | No}	(Optional) Enables inspection of Layer 4 ICMP ID: • ICMP ID—Specifies the value of the ICMP header IDENTIFIER.	0 to 65535
Specify ICMP Sequence {Yes | No}	(Optional) Enables inspection of Layer 4 ICMP sequence: • ICMP Sequence—Specifies the ICMP sequence for which to look.	0 to 65535
Specify ICMP Type {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMP header type: • ICMP Type—Specifies the value of the ICMP header TYPE.	0 to 65535
L4 Protocol ICMPv6		
Specify ICMPv6 Code	(Optional) Enables inspection of the Layer 4 ICMPv6 code: • ICMPv6 Code—Specifies the value of the ICMPv6 header CODE.	0 to 255
Specify ICMPv6 ID {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMPv6 identifier: • ICMPv6 ID—Specifies the value of the ICMPv6 header IDENTIFIER.	0 to 65535
Specify ICMPv6 Length {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMPv6 length: • ICMPv6 Length—Specifies the value of the ICMPv6 header LENGTH.	0 to 65535
Specify ICMPv6 MTU Field {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMPv6 MTU field: • ICMPv6 MTU Field—Specifies the value of the ICMPv6 header MTU field.	4,294,967,295
Specify ICMPv6 Option Type {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMPv6 type: • ICMPv6 Option Type—Specifies the ICMPv6 option type to inspect.	0 to 255

Table B-8 Atomic IP Advanced Engine Parameters (continued)

Parameter	Description	Value
Specify ICMPv6 Option Length {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMPv6 option length: • ICMPv6 Option Length—Specifies the ICMPv6 option length to inspect.	0 to 255
Specify ICMPv6 Sequence {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMPv6 sequence: • ICMPv6 Sequence—Specifies the value of the ICMPv6 header SEQUENCE.	0 to 65535
Specify ICMPv6 Type {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMPv6 type: • ICMPv6 Type—Specifies the value of the ICMPv6 header TYPE.	0 to 255
L4 Protocol TCP and UDP		
Specify Destination Port {Yes | No}	(Optional) Enables the destination port for use: • Destination Port—Specifies the destination port of interest for this signature.	0 to 65535
Specify Source Port {Yes | No}	(Optional) Enables source port for use: • Source Port—Specifies the source port of interest for this signature.	0 to 65535
Specify TCP Mask {Yes | No}	(Optional) Enables the TCP mask for use: • TCP Mask—Specifies the mask used in TCP flags comparison: – URG bit – ACK bit – PSH bit – RST bit – SYN bit – FIN bit	URG ACK PSH RST SYN FIN
Specify TCP Flags {Yes | No}	(Optional) Enables TCP flags for use: • TCP Flags—Specifies the TCP flags to match when masked by mask: – URG bit – ACK bit – PSH bit – RST bit – SYN bit – FIN bit	URG ACK PSH RST SYN FIN

Table B-8 Atomic IP Advanced Engine Parameters (continued)

Parameter	Description	Value
Specify TCP Reserved {Yes | No}	(Optional) Enables TCP reserved for use: • TCP Reserved—Specifies the value of TCP reserved.	0 to 63
Specify TCP Header Length {Yes | No}	(Optional) Enables inspection of the Layer 4 TCP header length: • TCP Header Length—Specifies the length of the TCP header used in inspection.	0 to 60
Specify TCP Payload Length {Yes | No}	(Optional) Enables inspection of the Layer 4 TCP payload length: • TCP Payload Length—Specifies the length of the TCP payload.	0 to 65535
Specify TCP URG Pointer {Yes | No}	(Optional) Enables inspection of the Layer 4 TCP URG pointer: • TCP URG Pointer—Specifies the value of the TCP URG flag inspection.	0 to 65535
Specify TCP Window Size {Yes | No}	(Optional) Enables inspection of the Layer 4 TCP window size: • TCP Window Size—Specifies the window size of the TCP packet.	0 to 65535
Specify UDP Valid Length {Yes | No}	(Optional) Enables inspection of the Layer 4 UDP valid length: • UDP Valid Length—Specifies the UDP packet lengths that are considered valid and should not be inspected.	0 to 65535
Specify UDP Length Mismatch {Yes | No}	(Optional) Enables inspection of the Layer 4 UDP length mismatch: • UDP Length Mismatch—Fires an alert when IP Data length is less than the UDP Header length.	0 to 65535

1. When a packet is GRE, IPIP, IPv4inIPv6, or MPL the sensor skips the Layer 3 encapsulation header and the encapsulation header, and all inspection is done starting from the second Layer 3. The encapsulation enumerator allows the engine to look backward to see if there is an encapsulation header before the Layer 3 in question.
2. Use the following syntax: x.x.x.x-z.z.z.z, for example, 10.10.10.1-10.10.10.254.

For More Information

- For an example custom Atomic IP Advanced signature, see Example Atomic IP Advanced Engine Signature, page 10-30.
- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Atomic IP Engine

The Atomic IP engine defines signatures that inspect IP protocol headers and associated Layer 4 transport protocols (TCP, UDP, and ICMP) and payloads. The Atomic engines do not store persistent data across packets. Instead they can fire an alert from the analysis of a single packet.

Table B-9 lists the parameters that are specific to the Atomic IP engine.

Table B-9 Atomic IP Engine Parameters

Parameter	Description	Value
Specify IP Addr Options {Yes | No}	(Optional) Enables IP address options: • IP Addr Options—Specifies the IP address options.	Address With Localhost IP Address[1] RFC 1918 Address Src IP Eq Dst IP
Specify IP Header Length {Yes | No}	(Optional) Enables inspection of the IP header length: • IP Header Length—Specifies the length of the IP header to inspect.	0 to 16
Specify IP Identifier {Yes | No}	(Optional) Enables inspection of the IP identifier: • IP Identifier—Specifies the IP ID to inspect.	0 to 255
Specify IP Option Inspection {Yes | No}	(Optional) Enables inspection of the IP options: • IP Option Inspection—Specifies the value of the IP option: – IP Option—Specifies the IP OPTION code to match. – IP Option Abnormal Options—Specifies the list of options is malformed.	0 to 65535
Specify IP Payload Length {Yes | No}	(Optional) Enables inspection of the IP payload length: • IP Payload Length—Specifies the length of IP payload to inspect.	0 to 65535
Specify IP Type of Service {Yes | No}	(Optional) Specifies the IP type of service: • IP Type of Service—Specifies the IP type of service to inspect.	0 to 6 255
Specify IP Total Length {Yes | No}	(Optional) Enables inspection of the IP total length: • IP Total Length—Specifies the total length of IP packet to inspect.	0 to 65535

Table B-9 Atomic IP Engine Parameters (continued)

Parameter	Description	Value
Specify IP Time-to-Live {Yes | No}	(Optional) Enables inspection of IP time-to-live: • IP Time-to-Live—Specifies the value of the IP TTL to inspect.	0 to 255
Specify IP Version {Yes | No}	(Optional) Enables inspection of the IP version: • IP Version—Specifies which IP version to inspect.	0 to 16
Specify L4 Protocol {Yes | No}	(Optional) Enables inspection of the Layer 4 protocol: • L4 Protocol—Specifies which Layer 4 protocol to inspect.	ICMP Protocol TCP Protocol UDP Protocol Other IP Protocols
Specify ICMP Code {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMP code: • ICMP Code—Specifies the value of the ICMP header CODE.	0 to 65535
Specify ICMP ID {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMP ID: • ICMP ID—Specifies the value of the ICMP header IDENTIFIER.	0 to 65535
Specify ICMP Sequence {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMP sequence: • ICMP Sequence—Specifies the ICMP sequence to inspect.	0 to 65535
Specify ICMP Type {Yes | No}	(Optional) Enables inspection of the ICMP header type: • ICMP Type—Specifies the value of the ICMP header TYPE.	0 to 65535
Specify ICMP Total Length {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMP total header length: • ICMP Total Length—Specifies the value of the ICMP total length to inspect.	0 to 65535
Specify Other IP Protocol ID {Yes | No}	(Optional) Enables inspection of the other Layer 4 protocols: • Other IP Protocol ID—Specifies which single IP protocol ID or single range of IP protocol IDs for which to send alerts.	0 to 255

Table B-9 Atomic IP Engine Parameters (continued)

Parameter	Description	Value
Specify Destination Port {Yes | No}	(Optional) Enables the destination port for use: • Destination Port—Specifies the destination port of interest for this signature.	0 to 65535
Specify Source Port {Yes | No}	(Optional) Enables source port for use: • Source Port—Specifies the source port of interest for this signature.	0 to 65535
Specify TCP Mask {Yes | No}	(Optional) Enables the TCP mask for use: • TCP Mask—Specifies the mask used in TCP flags comparison: – URG bit – ACK bit – PSH bit – RST bit – SYN bit – FIN bit	URG ACK PSH RST SYN FIN
Specify TCP Flags {Yes | No}	(Optional) Enables TCP flags for use: • TCP Flags—Specifies the TCP flags to match when masked by mask: – URG bit – ACK bit – PSH bit – RST bit – SYN bit – FIN bit	URG ACK PSH RST SYN FIN
Specify TCP Reserved {Yes | No}	(Optional) Enables TCP reserved for use: • TCP Reserved—Specifies the value of TCP reserved.	0 to 63
Specify TCP Header Length {Yes | No}	(Optional) Enables inspection of the Layer 4 TCP header length: • TCP Header Length—Specifies the length of the TCP header used in inspection.	0 to 60

Table B-9 Atomic IP Engine Parameters (continued)

Parameter	Description	Value
Specify TCP Payload Length {Yes | No}	(Optional) Enables inspection of the Layer 4 TCP payload length: • TCP Payload Length—Specifies the length of the TCP payload.	0 to 65535
Specify TCP URG Pointer {Yes | No}	(Optional) Enables inspection of the L4 TCP URG pointer: • TCP URG Pointer—Specifies the value of the TCP URG flag to inspect.	0 to 65535
Specify TCP Window Size {Yes | No}	(Optional) Enables inspection of the Layer 4 TCP window size: • TCP Window Size—Specifies the window size of the TCP packet.	0 to 65535
Specify UDP Length {Yes | No}	(Optional) Enables inspection of the Layer 4 UDP length: • UDP Length—Fires an alert when the IP Data length is less than the UDP Header length.	0 to 65535
Specify UDP Valid Length {Yes | No}	(Optional) Enables inspection of the Layer 4 UDP valid length: • UDP Valid Length—Specifies UDP packet lengths that are considered valid and should not be inspected.	0 to 65535
Specify UDP Length Mismatch {Yes | No}	(Optional) Enables inspection of the Layer 4 UDP length mismatch: • UDP Length Mismatch—Fires an alert when the IP Data length is less than the UDP Header length.	0 to 65535

1. Use the following syntax: x.x.x.x-z.z.z.z, for example, 10.10.10.1-10.10.10.254.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Atomic IPv6 Engine

The Atomic IPv6 engine detects two IOS vulnerabilities that are stimulated by malformed IPv6 traffic. These vulnerabilities can lead to router crashes and other security issues. One IOS vulnerability deals with multiple first fragments, which cause a buffer overflow. The other one deals with malformed ICMPv6 Neighborhood Discovery options, which also cause a buffer overflow.

Note IPv6 increases the IP address size from 32 bits to 128 bits, which supports more levels of addressing hierarchy, a much greater number of addressable nodes, and autoconfiguration of addresses.

Atomic IPv6 Signatures

There are eight Atomic IPv6 signatures. The Atomic IPv6 inspects Neighborhood Discovery protocol of the following types:

- Type 133—Router Solicitation
- Type 134—Router Advertisement
- Type 135—Neighbor Solicitation
- Type 136—Neighbor Advertisement
- Type 137—Redirect

Note Hosts and routers use Neighborhood Discovery to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. Hosts also use Neighborhood Discovery to find neighboring routers that will forward packets on their behalf.

Each Neighborhood Discovery type can have one or more Neighborhood Discovery options. The Atomic IPv6 engine inspects the length of each option for compliance with the legal values stated in RFC 2461. Violations of the length of an option results in an alert corresponding to the option type where the malformed length was encountered (signatures 1601 to 1605).

Note The Atomic IPv6 signatures do not have any specific parameters to configure.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Fixed Engine

The Fixed engines combine multiple regular expression patterns in to a single pattern matching table that allows a single search through the data. It supports ICMP, TCP, and UDP protocols. After a minimum inspection depth is reached (1 to 100 bytes), inspection stops. There are three Fixed engines: Fixed ICMP, Fixed TCP, and Fixed UDP.

Note The Fixed TCP and Fixed UDP engines use the Service Ports parameter as exclusion ports. The Fixed ICMP engine uses the Service Ports parameter as excluded ICMP types.

Table B-10 lists the parameters specific to the Fixed ICMP engine.

Table B-10 Fixed ICMP Engine Parameters

Parameter	Description	Value
Direction	Specifies the direction of traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
Max Payload Inspect Length	Specifies the maximum inspection depth for the signature.	1 to 250
Regex String	Specifies the regular expression to search for in a single packet.	*string*
Specify Exact Match Offset {Yes | No}	(Optional) Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the Regex String must report for a match to be valid.	0 to 65535
Specify Minimum Match Length {Yes | No}	(Optional) Enables minimum match length: • Minimum Match Length—Specifies the minimum number of bytes the Regex String must match.	0 to 65535
Specify ICMP Type {Yes | No}	(Optional) Enables inspection of the Layer 4 ICMP header type: • ICMP Type—Specifies the value of the ICMP header TYPE.	0 to 65535
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

Table B-11 lists the parameters specific to the Fixed TCP engine.

Table B-11 Fixed TCP Engine Parameters

Parameter	Description	Value
Direction	Specifies the direction of traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
Max Payload Inspect Length	Specifies the maximum inspection depth for the signature.	1 to 250
Regex String	Specifies the regular expression to search for in a single packet.	*string*

Table B-11 Fixed TCP Engine Parameters (continued)

Parameter	Description	Value
Specify Exact Match Offset {Yes | No}	(Optional) Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the Regex String must report for a match to be valid.	0 to 65535
Specify Min Match Length {Yes | No}	(Optional) Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the Regex String must match.	0 to 65535
Exclude Service Ports {Yes | No}	Enables service ports for use: • Excluded Service Ports—Specifies a comma-separated list of ports or port ranges to exclude.	0 to 65535[1] a-b[,c-d]
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. The second number in the range must be greater than or equal to the first number.

Table B-12 lists the parameters specific to the Fixed UDP engine.

Table B-12 Fixed UDP Engine Parameters

Parameter	Description	Value
Direction	Specifies the direction of traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port	From Service To Service
Max Payload Inspect Length	Specifies the maximum inspection depth for the signature.	1 to 250
Regex String	Specifies the regular expression to search for in a single packet.	*string*
Specify Exact Match Offset {Yes | No}	(Optional) Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the Regex String must report for a match to be valid.	0 to 65535
Specify Min Match Length {Yes | No}	(Optional) Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the Regex String must match.	0 to 65535

Table B-12 Fixed UDP Engine Parameters (continued)

Parameter	Description	Value
Exclude Service Ports {Yes | No}	Enables service ports for use: • Excluded Service Ports—Specifies a comma-separated list of ports or port ranges to exclude.	0 to 65535[1] a-b[,c-d]
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. The second number in the range must be greater than or equal to the first number.

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Flood Engine

The Flood engines define signatures that watch for any host or network sending multiple packets to a single host or network. For example, you can create a signature that fires when 150 or more packets per second (of the specific type) are found going to the victim host. There are two Flood engines: Flood Host and Flood Net.

Table B-13 lists the parameters specific to the Flood Host engine.

Table B-13 Flood Host Engine Parameters

Parameter	Description	Value
Protocol	Specifies which kind of traffic to inspect.	ICMP UDP
Rate	Specifies the threshold number of packets per second.	0 to 65535[1]
ICMP Type	Specifies the value for the ICMP header type.	0 to 65535
Dst Ports	Specifies the destination ports when you choose UDP protocol.	0 to 65535[2] a-b[,c-d]
Src Ports	Specifies the source ports when you choose UDP protocol.	0 to 65535[2] a-b[,c-d]

1. An alert fires when the rate is greater than the packets per second.
2. The second number in the range must be greater than or equal to the first number.

Table B-14 lists the parameters specific to the Flood Net engine.

Table B-14 Flood Net Engine Parameters

Parameter	Description	Value
Gap	Specifies the gap of time allowed (in seconds) for a flood signature.	0 to 65535
Peaks	Specifies the number of allowed peaks of flood traffic.	0 to 65535
Protocol	Specifies which kind of traffic to inspect.	ICMP TCP UDP
Rate	Specifies the threshold number of packets per second.	0 to 65535[1]
Sampling Interval	Specifies the interval used for sampling traffic.	1 to 3600
ICMP Type	Specifies the value for the ICMP header type.	0 to 65535

1. An alert fires when the rate is greater than the packets per second.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Meta Engine

Caution A large number of Meta engine signatures could adversely affect overall sensor performance.

The Meta engine defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets. As signature events are generated, the Meta engine inspects them to determine if they match any or several Meta definitions. The Meta engine generates a signature event after all requirements for the event are met.

All signature events are handed off to the Meta engine by the Signature Event Action Processor. The Signature Event Action Processor hands off the event after processing the minimum hits option. Summarization and event action are processed after the Meta engine has processed the component events.

Table B-15 lists the parameters specific to the Meta engine.

Table B-15 Meta Engine Parameters

Parameter	Description	Value
Component List	Specifies the Meta engine component: • edit—Edits an existing entry. • insert—Inserts a new entry into the list: – begin—Places the entry at the beginning of the active list. – end—Places the entry at the end of the active list. – inactive—Places the entry into the inactive list. – before—Places the entry before the specified entry. – after—Places the entry after the specified entry. • move—Moves an entry in the list. • Component Count—Specifies the number of times component must fire before this component is satisfied • Component Sig ID—Specifies the signature ID of the signature to match this component on. • Component SubSig ID—Specifies the subsignature ID of the signature to match this component on. • Is Not Component—Specifies that the component is a NOT component.	*name1* Yes | No
Component List In Order	Specifies to fire the component list in order.	Yes | No
All Components Required	Specifies to use all components.	Yes | No
All NOT Components Required	Specifies to use all of the NOT components.	Yes | No
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)
Meta Reset Interval	Specifies the time in seconds to reset the Meta signature.	0 to 3600

Table B-15 Meta Engine Parameters (continued)

Parameter	Description	Value
Meta Key	Specifies the storage type for the Meta signature: • Attacker address • Attacker and victim addresses • Attacker and victim addresses and ports • Victim address	• Axxx • AxBx • AaBb • xxBx
Unique Victims	Specifies the number of unique victims ports required per Meta signature.	1 to 256

For More Information

- For an example of a custom Meta engine signature, see Example Meta Engine Signature, page 10-27.
- For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Multi String Engine

Caution The Multi String engine can have a significant impact on memory usage.

The Multi String engine lets you define signatures that inspect Layer 4 transport protocol (ICMP, TCP, and UDP) payloads using multiple string matches for one signature. You can specify a series of regular expression patterns that must be matched to fire the signature. For example, you can define a signature that looks for regex 1 followed by regex 2 on a UDP service. For UDP and TCP you can specify port numbers and direction. You can specify a single source port, a single destination port, or both ports. The string matching takes place in both directions.

Use the Multi String engine when you need to specify more than one Regex pattern. Otherwise, you can use the String ICMP, String TCP, or String UDP engine to specify a single Regex pattern for one of those protocols.

Table B-16 lists the parameters specific to the Multi String Engine.

Table B-16 Multi String Engine Parameters

Parameter	Description	Value
Inspect Length	Specifies the length of the stream or packet that must contain all offending strings for the signature to fire.	0 to 4294967295
Protocol	Specifies the Layer 4 protocol selection.	ICMP TCP UDP

Table B-16 Multi String Engine Parameters (continued)

Parameter	Description	Value
Regex Component	Specifies the list of Regex components: • Regex String—Specifies the string to search for. • Spacing Type—Specifies the type of spacing required from the match before or from the beginning of the stream/packet if it is the first entry in the list.	list (1 to 16 items) exact minimum
Port Selection	Specifies the type of TCP or UDP port to inspect: • Both Ports—Specifies both source and destination port. • Destination—Specifies a range of destination ports. • Source—Specifies a range of source ports.[1]	0 to 65535 [2]
Extra Spacing	Specifies the exact number of bytes that must be between this Regex string and the one before, or from the beginning of the stream/packet if it is the first entry in the list.	0 to 4294967296
Minimum Spacing	Specifies the minimum number of bytes that must be between this Regex string and the one before, or from the beginning of the stream/packet if it is the first entry in the list.	0 to 4294967296
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. Port matching is performed bidirectionally for both the client-to-server and server-to-client traffic flow directions. For example, if the source-ports value is 80, in a client-to-server traffic flow direction, inspection occurs if the client port is 80. In a server-to-client traffic flow direction, inspection occurs if the server port is port 80.
2. A valid value is a comma- separated list of integer ranges a-b[,c-d] within 0 to 65535. The second number in the range must be greater than or equal to the first number.

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Normalizer Engine

Note You cannot add custom signatures to the Normalizer engine. You can tune the existing ones.

The Normalizer engine deals with IP fragment reassembly and TCP stream reassembly. With the Normalizer engine you can set limits on system resource usage, for example, the maximum number of fragments the sensor tries to track at the same time. Sensors in promiscuous mode report alerts on violations. Sensors in inline mode perform the action specified in the event action parameter, such as Produce Alert, Deny Packet Inline, and Modify Packet Inline.

Caution For signature 3050 Half Open SYN Attack, if you choose Modify Packet Inline as the action, you can see as much as 20 to 30% performance degradation while the protection is active. The protection is only active during an actual SYN flood.

IP Fragmentation Normalization

Intentional or unintentional fragmentation of IP datagrams can hide exploits making them difficult or impossible to detect. Fragmentation can also be used to circumvent access control policies like those found on firewalls and routers. And different operating systems use different methods to queue and dispatch fragmented datagrams. If the sensor has to check for all possible ways that the end host can reassemble the datagrams, the sensor becomes vulnerable to DoS attacks. Reassembling all fragmented datagrams inline and only forwarding completed datagrams and refragmenting the datagram if necessary, prevents this. The IP Fragmentation Normalization unit performs this function.

TCP Normalization

Through intentional or natural TCP session segmentation, some classes of attacks can be hidden. To make sure policy enforcement can occur with no false positives and false negatives, the state of the two TCP endpoints must be tracked and only the data that is actually processed by the real host endpoints should be passed on. Overlaps in a TCP stream can occur, but are extremely rare except for TCP segment retransmits. Overwrites in the TCP session should not occur. If overwrites do occur, someone is intentionally trying to elude the security policy or the TCP stack implementation is broken. Maintaining full information about the state of both endpoints is not possible unless the sensor acts as a TCP proxy. Instead of the sensor acting as a TCP proxy, the segments are ordered properly and the Normalizer engine looks for any abnormal packets associated with evasion and attacks.

IPv6 Fragments

The Normalizer engine can reassemble IPv6 fragments and forward the reassembled buffer for inspection and actions by other engines and processors. The following differences exist between IPv4 and IPv6:

- Modify Packet Inline for Normalizer engine signatures has no effect on IPv6 datagrams.
- Signature 1206 (IP Fragment Too Small) does not fire for IPv6 datagrams. Signature 1741 in the Atomic IP Advanced engine fires for IPv6 fragments that are too small.
- Signature 1202 allows 48 additional bytes beyond the Maximum Datagram Size for IPv6 because of the longer IPv6 header fields.

TCP Normalizer Signature Warning

You receive the following warning if you disable a default-enabled TCP Normalizer signature or remove a default-enabled modify packet inline, deny packet inline, or deny connection inline action:

```
Use caution when disabling, retiring, or changing the event action settings of a <Sig ID>
TCP Normalizer signature for a sensor operating in IPS mode. The TCP Normalizer signature
default values are essential for proper operation of the sensor.
If the sensor is seeing duplicate packets, consider assigning the traffic to multiple
virtual sensors. If you are having problems with asymmetric or out-of-order TCP packets,
consider changing the normalizer mode from strict evasion protection to asymmetric mode
protection. Contact Cisco TAC if you require further assistance.
```

ASA IPS Modules and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the ASA 5500-X IPS SSP and ASA 5585-X IPS SSP, because the ASA itself handles the normalization. Packets on the ASA IPS modules go through a special path in the Normalizer that only reassembles fragments and puts packets in the right order for the TCP stream. The Normalizer does not do any of the normalization that is done on an inline IPS appliance, because that causes problems in the way the ASA handles the packets.

The following Normalizer engine signatures are not supported:

- 1300.0
- 1304.0
- 1305.0
- 1307.0
- 1308.0
- 1309.0
- 1311.0
- 1315.0
- 1316.0
- 1317.0
- 1330.0
- 1330.1
- 1330.2
- 1330.9
- 1330.10
- 1330.12
- 1330.14
- 1330.15
- 1330.16
- 1330.17
- 1330.18

Table B-17 lists the parameters that are specific to the Normalizer engine.

Table B-17 Normalizer Engine Parameters

Parameter	Description
Edit Defaults	Editable signatures.
Specify Fragment Reassembly Timeout	(Optional) Enables fragment reassembly timeout.
Specify Hijack Max Old Ack	(Optional) Enables hijack-max-old-ack.
Specify Max Datagram Size	(Optional) Enables maximum datagram size.
Specify Max Fragments	(Optional) Enables maximum fragments: • Max Fragments—Lets you specify the number of maximum fragments.

Table B-17 Normalizer Engine Parameters (continued)

Parameter	Description
Specify Max Fragments per Datagram	(Optional) Enables maximum fragments per datagram.
Specify Max Last Fragments	(Optional) Enables maximum last fragments.
Specify Max Partial Datagrams	(Optional) Enables maximum partial datagrams.
Specify Max Small Frags	(Optional) Enables maximum small fragments.
Specify Min Fragment Size	(Optional) Enables minimum fragment size.
Specify Service Ports	(Optional) Enables service ports.
Specify SYN Flood Max Embryonic	(Optional) Enables SYN flood maximum embryonic.
Specify TCP Closed Timeout	(Optional) Enables TCP closed timeout.
Specify TCP Embryonic Timeout	(Optional) Enables TCP embryonic timeout.
Specify TCP Idle Timeout	(Optional) Enables TCP idle timeout: • TCP Idle Timeout—Lets you specify the TCP idle timeout time.
Specify TCP Max MSS	(Optional) Enables TCP maximum mss.
Specify TCP Max Queue	(Optional) Enables TCP maximum queue.
Specify TCP Min MSS	(Optional) Enables TCP minimum mss.
Specify TCP Option Number	(Optional) Enables TCP option number.

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For the procedures for configuring signatures in the Normalizer engine, see Configuring IP Fragment Reassembly Signatures, page 10-51, and Configuring TCP Stream Reassembly Signatures, page 10-54.

Service Engines

This section describes the Service engines, and contains the following topics:

Understanding the Service Engines

The Service engines analyze Layer 5+ traffic between two hosts. These are one-to-one signatures that track persistent data. The engines analyze the Layer 5+ payload in a manner similar to the live service.

The Service engines have common characteristics but each engine has specific knowledge of the service that it is inspecting. The Service engines supplement the capabilities of the generic string engine specializing in algorithms where using the string engine is inadequate or undesirable.

Service DNS Engine

The Service DNS engine specializes in advanced DNS decode, which includes anti-evasive techniques, such as following multiple jumps. It has many parameters, such as lengths, opcodes, strings, and so forth. The Service DNS engine is a biprotocol inspector operating on both TCP and UDP port 53. It uses the stream for TCP and the quad for UDP.

Table B-18 lists the parameters specific to the Service DNS engine.

Table B-18 Service DNS Engine Parameters

Parameter	Description	Value
Protocol	Specifies the protocol of interest for this inspector.	TCP UDP
Specify Query Chaos String {Yes | No}	(Optional) Enables the DNS Query Class Chaos String: • Query Chaos String—Specifies the query chaos string to search on.	*query-chaos-string*
Specify Query Class {Yes | No}	(Optional) Enables the query class: • Query Class—Specifies the DNS Query Class 2 Byte Value.	0 to 65535
Specify Query Invalid Domain Name {Yes | No}	(Optional) Enables the query invalid domain name: • Query Invalid Domain Name—Specifies the DNS Query Length greater than 255.	Yes | No
Specify Query Jump Count Exceeded {Yes | No}	(Optional) Enables query jump count exceeded: • Query Jump Count Exceeded—DNS compression counter.	Yes | No

Table B-18 Service DNS Engine Parameters (continued)

Parameter	Description	Value
Specify Query Opcode {Yes | No}	(Optional) Enables query opcode: • Query Opcode—Specifies the DNS Query Opcode 1 byte Value.	0 to 65535
Specify Query Record Data Invalid {Yes | No}	(Optional) Enables query record data invalid: • Query Record Data Invalid—Specifies the DNS Record Data incomplete.	Yes | No
Specify Query Record Data Length {Yes | No}	(Optional) Enables the query record data length: • Query Record Data Length—Specifies the DNS Response Record Data Length.	0 to 65535
Specify Query Src Port 53 {Yes | No}	(Optional) Enables the query source port 53: • Query Src Port 53—Specifies the DNS packet source port 53.	Yes | No
Specify Query Stream Length {Yes | No}	(Optional) Enables the query stream length: • Query Record Data Length—Specifies the DNS Packet Length.	0 to 65535
Specify Query Type {Yes | No}	(Optional) Enables the query type: • Query Type—Specifies the DNS Query Type 2 Byte Value.	0 to 65535
Specify Query Value {Yes | No}	(Optional) Enables the query value: • Query Value—Specifies the Query 0 Response 1.	Yes | No

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Service FTP Engine

The Service FTP engine specializes in FTP port command decode, trapping invalid **port** commands and the PASV port spoof. It fills in the gaps when the String engine is not appropriate for detection. The parameters are Boolean and map to the various error trap conditions in the **port** command decode. The Service FTP engine runs on TCP ports 20 and 21. Port 20 is for data and the Service FTP engine does not do any inspection on this. It inspects the control transactions on port 21.

Table B-19 lists the parameters that are specific to the Service FTP engine.

Table B-19 Service FTP Engine Parameters

Parameter	Description	Value
Direction	Specifies the direction of traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
FTP Inspection Type	Specifies the type of inspection to perform: • Looks for an invalid address in the FTP port command. • Looks for an invalid port in the FTP port command. • Looks for the PASV port spoof.	Invalid Address in PORT Command Invalid Port in PORT Command PASV Port Spoof
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. The second number in the range must be greater than or equal to the first number.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Service Generic Engine

The Service Generic engine allows programmatic signatures to be issued in a config-file-only signature update. It has a simple machine and assembly language that is defined in the configuration file. It runs the machine code (distilled from the assembly language) through its virtual machine, which processes the instructions and pulls the important pieces of information out of the packet and runs them through the comparisons and operations specified in the machine code. It is intended as a rapid signature response engine to supplement the String and State engines.

New functionality adds the Regex parameter to the Service Generic engine and enhanced instructions. The Service Generic engine can analyze traffic based on the mini-programs that are written to parse the packets. These mini-programs are composed of commands, which dissect the packet and look for certain conditions.

Note You cannot use the Service Generic engine to create custom signatures.

Caution Due to the proprietary nature of this complex language, we do not recommend that you edit the Service Generic engine signature parameters other than severity and event action.

Table B-20 lists the parameters specific to the Service Generic engine.

Table B-20 Service Generic Engine Parameters

Parameter	Description	Value
Specify Dst Port {Yes | No}	(Optional) Enables the destination port: • Dst Port—Specifies the destination port of interest for this signature.	0 to 65535
Specify IP Protocol {Yes | No}	(Optional) Enables IP protocol: • IP Protocol—Specifies the IP protocol this inspector should examine.	0 to 255
Specify Payload Source {Yes | No}	(Optional) Enables payload source inspection: • Payload Source—Specifies the payload source inspection for the following types: – Inspects ICMP data – Inspects Layer 2 headers – Inspects Layer 3 headers – Inspects Layer 4 headers – Inspects TCP data – Inspects UDP data	ICMP Data 12 Header 13 Header 14 Header TCP Data UDP Data
Specify Src Port {Yes | No}	(Optional) Enables the source port: • Src Port—Specifies the source port of interest for this signature.	0 to 65535
Specify Regex String {Yes | No}	Specifies the regular expression to look for when the policy type is Regex: • Regex String—Specifies a regular expression to search for in a single TCP packet. • (Optional) Specify Min Match Length—Enables minimum match length for use: – Min Match Length—Specifies the minimum length of the Regex match required to constitute a match.	*string* 0 to 65535
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Service H225 Engine

The Service H225 engine analyzes H225.0 protocol, which consists of many subprotocols and is part of the H.323 suite. H.323 is a collection of protocols and other standards that together enable conferencing over packet-based networks.

H.225.0 call signaling and status messages are part of the H.323 call setup. Various H.323 entities in a network, such as the gatekeeper and endpoint terminals, run implementations of the H.225.0 protocol stack. The Service H225 engine analyzes H225.0 protocol for attacks on multiple H.323 gatekeepers, VoIP gateways, and endpoint terminals. It provides deep packet inspection for call signaling messages that are exchanged over TCP PDUs. The Service H225 engine analyzes the H.225.0 protocol for invalid H.255.0 messages, and misuse and overflow attacks on various protocol fields in these messages.

H.225.0 call signaling messages are based on Q.931 protocol. The calling endpoint sends a Q.931 setup message to the endpoint that it wants to call, the address of which it procures from the admissions procedure or some lookup means. The called endpoint either accepts the connection by transmitting a Q.931 connect message or rejects the connection. When the H.225.0 connection is established, either the caller or the called endpoint provides an H.245 address, which is used to establish the control protocol (H.245) channel.

Especially important is the SETUP call signaling message because this is the first message exchanged between H.323 entities as part of the call setup. The SETUP message uses many of the commonly found fields in the call signaling messages, and implementations that are exposed to probable attacks will mostly also fail the security checks for the SETUP messages. Therefore, it is highly important to check the H.225.0 SETUP message for validity and enforce checks on the perimeter of the network.

The Service H225 engine has built-in signatures for TPKT validation, Q.931 protocol validation, and ASN.1PER validations for the H225 SETUP message. ASN.1 is a notation for describing data structures. PER uses a different style of encoding. It specializes the encoding based on the data type to generate much more compact representations.

You can tune the Q.931 and TPKT length signatures and you can add and apply granular signatures on specific H.225 protocol fields and apply multiple pattern search signatures of a single field in Q.931 or H.225 protocol.

The Service H225 engine supports the following features:

- TPKT validation and length check
- Q.931 information element validation
- Regular expression signatures on text fields in Q.931 information elements
- Length checking on Q.931 information elements
- SETUP message validation
- ASN.1 PER encode error checks
- Configuration signatures for fields like ULR-ID, E-mail-ID, h323-id, and so forth for both regular expression and length.

There is a fixed number of TPKT and ASN.1 signatures. You cannot create custom signatures for these types. For TPKT signatures, you should only change the value-range for length signatures. You should not change any parameters for ASN.1. For Q.931 signatures, you can add new regular expression signatures for text fields. For SETUP signatures, you can add signatures for length and regular expression checks on various SETUP message fields.

Table B-21 lists parameters specific to the Service H225 engine.

Table B-21 Service H.225 Engine Parameters

Parameter	Description	Value
Message Type	Specifies the type of H225 message to which the signature applies: • SETUP • ASN.1-PER • Q.931 • TPKT	ASN.1-PER Q.931 SETUP TPKT
Policy Type	Specifies the type of H225 policy to which the signature applies: • Inspects field length. • Inspects presence. If certain fields are present in the message, an alert is sent. • Inspects regular expressions. • Inspects field validations. • Inspects values. **Note** Regex and presence are not valid for TPKT signatures.	Field Validation Length Check Presence Regex Value
Specify Field Name {Yes | No}	(Optional) Enables field name for use. Gives a dotted representation of the field name to which this signature applies. • Field Name—Specifies the field name to inspect. **Note** Only valid for SETUP and Q.931 message types.	1 to 512
Specify Invalid Packet Index {Yes | No}	(Optional) Enables invalid packet index for use for specific errors in ASN, TPKT, and other errors that have fixed mapping. • Invalid Packet Index—Specifies the inspection for invalid packet index.	0 to 255

Table B-21 Service H.225 Engine Parameters (continued)

Parameter	Description	Value
Value Range Regex String {Yes | No}	Specifies the regular expression to look for when the policy type is Regex: • Regex String—Specifies a regular expression to search for in a single TCP packet. • (Optional) Specify Min Match Length—Enables minimum match length for use: – Min Match Length—Specifies the minimum length of the Regex match required to constitute a match. **Note** This is never set for TPKT signatures.	*string* 0 to 65535
Specify Value Range {Yes | No}	Enables value range for use: • Value Range—Specifies the range of values. **Note** Valid for the length or value policy types (0x00 to 6535). Not valid for other policy types.	0 to 65535[1] a-b
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. The second number in the range must be greater than or equal to the first number.

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Service HTTP Engine

The Service HTTP engine is a service-specific string-based pattern-matching inspection engine. The HTTP protocol is one of the most commonly used in networks of today. In addition, it requires the most amount of preprocessing time and has the most number of signatures requiring inspection making it critical to the overall performance of the system.

The Service HTTP engine uses a Regex library that can combine multiple patterns into a single pattern-matching table allowing a single search through the data. This engine searches traffic directed only to web services, or HTTP requests. You cannot inspect return traffic with this engine. You can specify separate web ports of interest in each signature in this engine.

HTTP deobfuscation is the process of decoding an HTTP message by normalizing encoded characters to ASCII equivalent characters. It is also known as ASCII normalization.

Before an HTTP packet can be inspected, the data must be deobfuscated or normalized to the same representation that the target system sees when it processes the data. It is ideal to have a customized decoding technique for each host target type, which involves knowing what operating system and web server version is running on the target. The Service HTTP engine has default deobfuscation behavior for the Microsoft IIS web server.

Table B-22 lists the parameters specific the Service HTTP engine.

Table B-22 Service HTTP Engine Parameters

Parameter	Description	Value
De Obfuscate	Applies anti-evasive deobfuscation before searching.	Yes | No
Max Field Sizes	Enables maximum field sizes grouping.	—
Specify Max Arg Field Length {Yes | No}	(Optional) Enables maximum argument field length: • Max Arg Field Length—Specifies the maximum length of the arguments field.	0 to 65535
Specify Max Header Field Length {Yes | No}	(Optional) Enables maximum header field length: • Max Header Field Length—Specifies the maximum length of the header field.	0 to 65535
Specify Max Request Field Length {Yes | No}	(Optional) Enables maximum request field length: • Max Request Field Length—Specifies the maximum length of the request field.	0 to 65535
Specify Max URI Field Length {Yes | No}	(Optional) Enables the maximum URI field length: • Max URI Field Length—Specifies the maximum length of the URI field.	0 to 65535
Regex	Enables regular expression grouping.	—
Specify Arg Name Regex {Yes | No}	(Optional) Enables searching the Arguments field for a specific regular expression: • Arg Name Regex—Specifies the regular expression to search for in the HTTP Arguments field (after the ? and in the Entity body as defined by Content-Length).	—
Specify Header Regex {Yes | No}	(Optional) Enables searching the Header field for a specific regular expression: • Header Regex—Specifies the regular expression to search in the HTTP Header field. **Note** The Header is defined after the first CRLF and continues until CRLFCRLF.	—

Table B-22 Service HTTP Engine Parameters (continued)

Parameter	Description	Value
Specify Request Regex {Yes | No}	(Optional) Enables searching the Request field for a specific regular expression: • Request Regex—Specifies the regular expression to search in both HTTP URI and HTTP Argument fields. • Specify Min Request Match Length—Enables setting a minimum request match length: – Min Request Match Length—Specifies the minimum request match length.	0 to 65535
Specify URI Regex {Yes | No}	(Optional) Specifies the regular expression to search in HTTP URI field. **Note** The URI field is defined to be after the HTTP method (GET, for example) and before the first CRLF. **Note** The regular expression is protected, which means you cannot change the value.	[/\\][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][.]jpeg
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. The second number in the range must be greater than or equal to the first number.

For More Information

- For an example Service HTTP custom signature, see Example Service HTTP Engine Signature, page 11-17.
- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Service IDENT Engine

The Service IDENT engine inspects TCP port 113 traffic. It has basic decode and provides parameters to specify length overflows. For example, when a user or program at computer A makes an IDENT request of computer B, it may only ask for the identity of users of connections between A and B. The IDENT server on B listens for connections on TCP port 113. The client at A establishes a connection, then specifies which connection it wants identification for by sending the numbers of the ports on A and B that the connection is using. The server at B determines what user is using that connection, and replies to A with a string that names that user. The Service IDENT engine inspects the TCP port 113 for IDENT abuse.

Table B-23 lists the parameters specific to the Service IDENT engine.

Table B-23 Service IDENT Engine Parameters

Parameter	Description	Value
Inspection Type	Specifies the type of inspection to perform.	Has Newline Has Bad Port Payload Size
Has Newline	Inspects payload for a nonterminating new line character.	—
Has Bad Port	Inspects payload for a bad port.	—
Payload Size	Inspects for payload length longer than this: • Max Bytes—Specifies the maximum bytes for the payload length.	0 to 65535
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]
Direction	Specifies the direction of the traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service

1. The second number in the range must be greater than or equal to the first number.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Service MSRPC Engine

The Service MSRPC engine processes MSRPC packets. MSRPC allows for cooperative processing between multiple computers and their application software in a networked environment. It is a transaction-based protocol, implying that there is a sequence of communications that establishes the channel and passes processing requests and replies.

MSRPC is an ISO Layer 5-6 protocol and is layered on top of other transport protocols such as UDP, TCP, and SMB. The MSRPC engine contains facilities to allow for fragmentation and reassembly of the MSRPC PDUs.

This communication channel is the source of recent Windows NT, Windows 2000, and Window XP security vulnerabilities. The Service MSRPC engine only decodes the DCE and RPC protocol for the most common transaction types.

Table B-24 lists the parameters specific to the Service MSRPC engine.

Table B-24 Service MSRPC Engine Parameters

Parameter	Description	Value
Protocol	Enables the protocol of interest for this inspector: • Type—Specifies UDP or TCP.	TCP UDP
Specify Flags {Yes | No}	Enables the flags to set: • MSRPC TCP Flags—Specifies MSRPC TCP flags. • MSRPC TCP Flags Mask—Specifies the MSRPC TCP flags mask.	Concurrent Execution Did Not Execute First Fragment Last Fragment Maybe Semantics Object UUID Pending Cancel Reserved
Specify Operation {Yes | No}	(Optional) Enables using MSRPC operation: • Operation—Specifies the MSRPC operation requested. **Note** Required for SMB_COM_TRANSACTION commands. Exact match.	0 to 65535
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

Table B-24 Service MSRPC Engine Parameters (continued)

Parameter	Description	Value
Specify Regex String {Yes | No}	(Optional) Enables using a regular expression string: • Specify Exact Match Offset—Enables the exact match offset: – Exact Match Offset—Specifies the exact stream offset the regular expression string must report for a match to be valid. • Specify Min Match Length—Enables the minimum match length: – Min Match Length—Specifies the minimum number of bytes the regular expression string must match. • Specify Min Match Offset—Enables the minimum match length: – Min Match Offset—Specifies the minimum stream offset the regular expression string must report for a match to be valid. • Specify Max Match Offset—Enables the maximum match offset: – Max Match Offset—Specifies the maximum stream offset the regular expression string must report for a match to be valid.	0 to 65535
Specify UUID {Yes | No}	(Optional) Enables UUID: • UUID—Specifies the MSRPC UUID field.	000001a000000000c00 0000000000046

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Service MSSQL Engine

The Service MSSQL engine inspects the protocol used by the Microsoft SQL server. There is one MSSQL signature. It fires an alert when it detects an attempt to log in to an MSSQL server with the default sa account. You can add custom signatures based on MSSQL protocol values, such as login username and whether a password was used.

Table B-25 lists the parameters specific to the Service MSSQL engine.

Table B-25 Service MSSQL Engine Parameters

Parameter	Description	Value
Password Present	Specifies whether or not a password was used in an MS SQL login.	Yes | No
Specify SQL Username	(Optional) Enables using an SQL username: • SQL Username—Specifies the username (exact match) of user logging in to MS SQL service.	sa

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Service NTP Engine

The Service NTP engine inspects NTP protocol. There is one NTP signature, the NTP readvar overflow signature, which fires an alert if a readvar command is seen with NTP data that is too large for the NTP service to capture. You can tune this signature and create custom signatures based on NTP protocol values, such as mode and size of control packets.

Table B-26 lists the parameters specific to the Service NTP engine.

Table B-26 Service NTP Engine Parameters

Parameter	Description	Value
Inspection Type	Specifies the type of inspection to perform.	Inspect NTP Packets Is Invalid Data Packet Is Non NTP Traffic
Inspect NTP Packets	Enables inspection of NTP packets: • Control Opcode—Specifies the opcode number of an NTP control packet according to RFC1305, Appendix B. • Max Control Data Size—Specifies the maximum allowed amount of data sent in a control packet. • Operation Mode—Specifies the mode of operation of the NTP packet per RFC 1305.	0 to 65535
Is Invalid Data Packet	Enables inspection of invalid NTP data packets and checks the structure of the NTP data packet to make sure it is the correct size.	—
Is Non NTP Traffic	Enables the inspection of nonNTP packets on an NTP port.	—

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Service P2P

P2P networks use nodes that can simultaneously function as both client and server for the purpose of file sharing. P2P networks often contain copyrighted material and their use on a corporate network can violate company policy. The Service P2P engine monitors such networks and provides optimized TCP and UDP P2P protocol identification. The Service P2P engine has the following characteristics:

- Listens on all TCP and UDP ports.
- Increased performance through the use of hard-coded signatures rather than regular expressions.
- Ignores traffic once P2P protocol is identified or after seeing 10 packets without a P2P protocol being identified.

Note Because the P2P signatures are hard coded, the only parameters that you can edit are the Master engine parameters.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Service RPC Engine

The Service RPC engine specializes in RPC protocol and has full decode as an anti-evasive strategy. It can handle fragmented messages (one message in several packets) and batch messages (several messages in a single packet).

The RPC portmapper operates on port 111. Regular RPC messages can be on any port greater than 550. RPC sweeps are like TCP port sweeps, except that they only count unique ports when a valid RPC message is sent. RPC also runs on UDP.

Table B-27 lists the parameters specific to the Service RPC engine.

Table B-27 Service RPC Engine Parameters

Parameter	Description	Value
Direction	Specifies the direction of traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
Protocol	Specifies the protocol of interest.	TC UDP
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]

Table B-27 Service RPC Engine Parameters (continued)

Parameter	Description	Value
Specify Regex String {Yes | No}	(Optional) Enables using a regular expression string: • Specify Exact Match Offset—Enables the exact match offset: – Exact Match Offset—Specifies the exact stream offset the regular expression string must report for a match to be valid. • Specify Min Match Length—Enables the minimum match length: – Min Match Length—Specifies the minimum number of bytes the regular expression string must match.	0 to 65535
Specify Spoof Src {Yes | No}	(Optional) Enables the spoof source address: • Is Spoof Src—Fires an alert when the source address is 127.0.0.1.	Yes | No
Specify Port Map Program {Yes | No}	(Optional) Enables the portmapper program: • Port Map Program—Specifies the program number sent to the portmapper for this signature.	0 to 9999999999
Specify RPC Max Length {Yes | No}	(Optional) Enables RPC maximum length: • RPC Max Length—Specifies the maximum allowed length of the entire RPC message. **Note** Lengths longer than what you specify fire an alert.	0 to 65535
Specify RPC Procedure {Yes | No}	(Optional) Enables RPC procedure: • RPC Procedure—Specifies the RPC procedure number for this signature.	0 to 1000000
Specify RPC Program {Yes | No}	(Optional) Enables RPC program: • RPC Program—Specifies the RPC program number for this signature.	0 to 1000000
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. The second number in the range must be greater than or equal to the first number.

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Service SMB Advanced Engine

Note The SMB engine has been replaced by the SMB Advanced engine. Even though the SMB engine is still visible in IDM, IME, and the CLI, its signatures have been obsoleted; that is, the new signatures have the obsoletes parameter set with the IDs of their corresponding old signatures. Use the new SMB Advanced engine to rewrite any custom signature that were in the SMB engine.

The Service SMB Advanced engine processes Microsoft SMB and Microsoft RPC over SMB packets. The Service SMB Advanced engine uses the same decoding method for connection-oriented MSRPC as the MSRPC engine with the requirement that the MSRPC packet must be over the SMB protocol. The Service SMB Advanced engine supports MSRPC over SMB on TCP ports 139 and 445. It uses a copy of the connection-oriented DCS/RPC code from the MSRPC engine.

Table B-28 lists the parameters specific to the Service SMB Advanced engine.

Table B-28 Service SMB Advanced Engine Parameters

Parameter	Description	Value
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535 a-b[,c-d] [1]
Specify SMB Command {Yes | No}	(Optional) Enables SMB commands: • SMB Command—Specifies the SMB command value. **Note** Exact match required; defines the SMB packet type.[2]	0 to 255
Specify Direction {Yes | No}	(Optional) Enables traffic direction: • Direction—Specifies the direction of traffic: – From Service—Traffic from service port destined to client port. – To Service—Traffic from client port destined to service port.	From Service To Service
Specify MSRPC over SMB Operation {Yes | No}	(Optional) Enables MSRPC over SMB: • MSRPC over SMB Operation—Specifies MSRPC over SMB. **Note** Required for SMB_COM_TRANSACTION commands, exact match required.	0 to 65535
Specify Regex String {Yes | No}	(Optional) Enables searching for Regex strings: • Regex String—Specifies a regular expression to search for in a single TCP packet.	*string*

Table B-28 Service SMB Advanced Engine Parameters (continued)

Parameter	Description	Value
Specify Exact Match Offset {Yes | No}	(Optional) Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the Regex string must report for a match to be valid.	0 to 65535
Specify Min Match Length {Yes | No}	(Optional) Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the Regex string must match.	0 to 65535
Specify Regex Payload Source {Yes | No}	(Optional) Enables payload source inspection: • Payload Source—Specifies the kind of payload source inspection.[3]	Resource SMB Data TCP Data
Specify Scan Interval {Yes | No}	(Optional) Enables scan interval: • Scan Interval—Specifies the interval in seconds used to calculate alert rates.	1 to 131071
Specify TCP Flags {Yes | No}	(Optional) Enables TCP flags: • MSRPC TCP Flags—Specifies the MSRPC TCP flags. • MSRPC TCP Flags Mask—Specifies the MSRPC flags mask.	Concurrent Execution Did Not Execute First Fragment Last Fragment Maybe Semantics Object UUID Pending Cancel Reserved
Specify MSRPC over SMB PDU Type {Yes | No}	(Optional) Enables MSRPC PDU type over the SMB packet: • MSRPC over SMB PDU Type—Specifies the PDU type of MSRPC over the SMB packet.	0 = Request 2 = Response 11 = Bind 12 = Bind Ack
Specify MSRPC over SMB UUID {Yes | No}	(Optional) Enables MSRPC over UUID: • MSRPC over SMB UUID—Specifies the MSRPC UUID.	32-character string composed of hexadecimal characters 0-9, a-f, A-F.
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	True | False (default)

1. The second number in the range must be greater than or equal to the first number.
2. Currently supporting 37 (0x25) SMB_COM_TRANSACTION command \x26amp; 162 (0xA2) SMB_COM_NT_CREATE_ANDX command.
3. TCP_Data performs Regex over entire packet, SMB_Data performs Regex on SMB payload only, Resource_DATA performs Regex on SMB_Resource.

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

Service SNMP Engine

The Service SNMP engine inspects all SNMP packets destined for port 161. You can tune SNMP signatures and create custom SNMP signatures based on specific community names and object identifiers.

Instead of using string comparison or regular expression operations to match the community name and object identifier, all comparisons are made using the integers to speed up the protocol decode and reduce storage requirements.

Table B-29 lists the parameters specific to the Service SNMP engine.

Table B-29 Service SNMP Engine Parameters

Parameter	Description	Value
Inspection Type	Enables the SNMP inspection type.	Brute Force Inspection (default) Invalid Packet Inspection Non-SNMP Traffic Inspection SNMP Inspection
Brute Force Inspection	Enables brute force inspection: • Bruce Force Count—Specifies the number of unique SNMP community names that constitute a brute force attempt.	0 to 65535
Invalid Packet Inspection	Inspects for SNMP protocol violations.	—
Non-SNMP Traffic Inspection	Inspects for non-SNMP traffic destined for UDP port 161.	—
SNMP Inspection {Yes | No}	Enables inspection of SNMP traffic: • Specify Object ID—Enables inspection of the SNMP Object identifier: – Object ID—Specifies to search for the SNMP object identifier. • Specify Community Name—Enables inspection of the SNMP community name: – Community Name—Specifies to search for the SNMP community name (SNMP password).	*object-id* *community-name*

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Service SSH Engine

The Service SSH engine specializes in port 22 SSH traffic. Because all but the setup of an SSH session is encrypted, the Service SSH engine only looks at the fields in the setup. There are two default signatures for SSH. You can tune these signatures, but you cannot create custom signatures.

Table B-30 lists the parameters specific to the Service SSH engine.

Table B-30 Service SSH Engine Parameters

Parameter	Description	Value
Length Type	Inspects for one of the following SSH length types: • Key Length—Enables inspection of the length of the SSH key: – Length—Specifies that keys larger than this fire the RSAREF overflow. • User Length—Enables user length SSH inspection: – Length—Specifies that keys larger than this fire the RSAREF overflow.	0 to 65535
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]
Specify Packet Depth {Yes | No}	(Optional) Enables packet depth: • Packet Depth—Specifies the number of packets to watch before determining the session key was missed.	0 to 65535

1. The second number in the range must be greater than or equal to the first number.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Service TNS Engine

The Service TNS engine inspects TNS protocol. TNS provides database applications with a single common interface to all industry-standard network protocols. With TNS, applications can connect to other database applications across networks with different protocols. The default TNS listener port is TCP 1521. TNS also supports REDIRECT frames that redirect the client to another host and/or another TCP port. To support REDIRECT packets, the TNS engine listens on all TCP ports and has a quick TNS frame header validation routine to ignore non-TNS streams.

Table B-31 lists the parameters specific to the Service TNS engine

Table B-31 Service TNS Engine Parameters

Parameter	Description	Value
Direction	Specifies the direction of traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
Specify Regex String {Yes | No}	(Optional) Enables using a regular expression string: • Regex String—Specifies the regular expression to search for.	*string*
Specify Exact Match Offset {Yes | No}	Enables the exact match offset: • Exact Match Offset—Specifies the exact stream offset the Regex String must report for a match to be valid.	0 to 65535
Specify Max Match Offset {Yes | No}	Enables maximum match offset: • Max Match Offset—Specifies the maximum stream offset the Regex String must report for a match to be valid.	0 to 65535
Specify Min Match Offset {Yes | No}	Enables minimum match offset: • Min Match Offset—Specifies the minimum stream offset the Regex String must report for a match to be valid.	0 to 65535
Specify Min Match Length {Yes | No}	Enables the minimum match length: – Min Match Length—Specifies the minimum number of bytes the Regex String must match.	0 to 65535
Specify Regex Payload Source {Yes | No}	Enables the inspection of TCP or TNS protocol: • Payload Source—Specifies which protocol to inspect: – TCP Data—Performs Regex over the data portion of the TCP packet. – TNS Data—Performs Regex only over the TNS data (with all white space removed).	TCP Data TNS Data
Type Frame Type	Specifies the TNS frame value type: • 1—Connect • 2—Accept • 4—Refuse • 5—Redirect • 6—Data • 11—Resend • 12—Marker	1 2 4 5 6 11 12

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.

State Engine

The State engine provides state-based regular expression-based pattern inspection of TCP streams. A state engine is a device that stores the state of an event and at a given time can operate on input to transition from one state to another and/or cause an action or output to take place. State machines are used to describe a specific event that causes an output or alarm. There are three state machines in the State engine: SMTP, Cisco Login, and LPR Format String.

Table B-32 lists the parameters specific to the State engine.

Table B-32 State Engine Parameters

Parameter	Description	Value
State Machine	Specifies the state machine grouping.	Cisco Login LPR Format String SMPT
Cisco Login	Specifies the state machine for Cisco login: • State Name—Name of the state required before the signature fires an alert: – Cisco device state – Control-C state – Password prompt state – Start state	Cisco Device Control C Pass Prompt Start
LPR Format String	Specifies the state machine to inspect for the LPR format string vulnerability: • State Name—Name of the state required before the signature fires an alert: – Abort state to end LPR Format String inspection – Format character state – State state	Abort Format Char Start

Table B-32 State Engine Parameters (continued)

Parameter	Description	Value
SMPT	Specifies the state machine for the SMTP protocol: • State Name—Name of the state required before the signature fires an alert: – Abort state to end LPR Format String inspection – Mail body state – Mail header state – SMTP commands state – Start state	Abort Mail Body Mail Header SMPT Commands Start
Specify Min Match Length {Yes | No}	(Optional) Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the regular expression string must match.	0 to 65535
Regex String	Specifies the regular expression to search for. **Note** This parameter is protected; you cannot edit it.	*string*
Direction	Specifies the direction of the traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)
Specify Exact Match Offset {Yes | No}	(Optional) Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the regular expression string must report for a match to be valid.	0 to 65535
Specify Max Match Offset {Yes | No}	(Optional) Enables maximum match offset: • Max Match Offset—Specifies the maximum stream offset the regular expression string must report for a match to be valid.	0 to 65535
Specify Min Match Offset {Yes | No}	(Optional) Enables minimum match offset: • Min Match Offset—Specifies the minimum stream offset the regular expression string must report for a match to be valid.	0 to 65535

1. The second number in the range must be greater than or equal to the first number.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

String Engines

The String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP protocols. The String engine uses a regular expression engine that can combine multiple patterns into a single pattern-matching table allowing for a single search through the data. There are three String engines: String ICMP, String TCP, and String UDP.

Table B-33 lists the parameters specific to the String ICMP engine.

Table B-33 String ICMP Engine Parameters

Parameter	Description	Value
Direction	Specifies the direction of the traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
ICMP Type	Specifies the value of the ICMP header TYPE.	0 to 18[1] a-b[,c-d]
Regex String	The Regex pattern to use in the search.	string
Specify Exact Match Offset {Yes | No}	(Optional) Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the regular expression string must report for a match to be valid.	0 to 65535
Specify Min Match Length {Yes | No}	(Optional) Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the regular expression string must match.	0 to 65535
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. The second number in the range must be greater than or equal to the first number.

Table B-34 lists the parameters specific to the String TCP engine.

Table B-34 String TCP Engine

Parameter	Description	Value
Direction	Specifies the direction of the traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
Regex String	The Regex pattern to use in the search.	*string*
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]

Table B-34 String TCP Engine (continued)

Parameter	Description	Value
Specify Exact Match Offset {Yes | No}	(Optional) Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the regular expression string must report for a match to be valid.	0 to 65535
Specify Min Match Length {Yes | No}	(Optional) Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the regular expression string must match.	0 to 65535
Strip Telnet Options	Strips the Telnet option characters from the data before the pattern is searched.[2]	Yes | No
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

1. The second number in the range must be greater than or equal to the first number.
2. This parameter is primarily used as an IPS anti-evasion tool.

Table B-35 lists the parameters specific to the String UDP engine.

Table B-35 String UDP Engine

Parameter	Description	Value
Direction	Specifies the direction of the traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	• From Service • To Service
Regex String	The Regex pattern to use in the search.	*string*
Service Ports	Specifies a comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]
Specify Exact Match Offset {Yes | No}	(Optional) Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset the regular expression string must report for a match to be valid.	0 to 65535
Specify Min Match Length {Yes | No}	(Optional) Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the regular expression string must match.	0 to 65535
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No

1. The second number in the range must be greater than or equal to the first number.

For More Information

- For an example custom String engine signature, see Example String TCP Engine Signature, page 11-22.
- For more information on the parameters common to all signature engines, see Master Engine, page B-4.

String XL Engines

Note The IPS 4345, IPS 4360, IPS 4510, IPS 4520, IPS 4520-XL, ASA 5525-X IPS SSP, ASA 5545-X IPS SSP, ASA 5555-X IPS SSP, and ASA 5585-X IPS SSP support the String XL engines and the Regex accelerator card.

The String XL engines do the same thing as the other String engines—provide a matching capability of one string per signature—but they use a different Regex syntax.The String TCP XL engine is stream-based and uses cross-packet inspection (XPI). The packets must be in order. UDP and ICMP are both stateless, thus the String UDP XL and String ICMP XL signature engines require no session state to be allocated and so each packet is a separate search.

The Regex accelerator card is used for both the standard String engines and the String XL engines. Most standard String engine signatures can be compiled and analyzed by the Regex accelerator card without modification. However, there are special circumstances in which the standard String engine signatures cannot be compiled for the Regex accelerator card. In these situations a new signature is written in a String XL engine using the specific parameters in the String XL engine that do compile on the Regex accelerator card. The new signature in the String XL engine obsoletes the original signature in the standard String engine.

Although you can use regular expression syntax or raw expression syntax, raw expression syntax is for expert users only. When configuring String XL signatures, the Regex String parameter is required unless you are using raw expression syntax.

Note Raw Regex is regular expression syntax used for raw mode processing. It is expert mode only and targeted for use by the Cisco IPS signature development team or only those who are under supervision by the Cisco IPS signature development team. You can configure a String XL signature in either regular Regex or raw Regex.

Table B-36 lists the parameters specific to the String XL engines (TCP, ICMP, and UDP).

Table B-36 String XL Engine Parameters

Parameter	Description	Value
Direction	(Required) Direction of the traffic to inspect: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	From Service To Service
Dot All	If set to Yes, matches [\x00-\xFF] including \n; if set to No, matches anything in the range [\x00-\xFF] except \n.	Yes | No (default)
End Optional	Specifies that at the end of a packet, if all other conditions are satisfied but the end is not seen, a match is reported if the minimum is exceeded.	Yes | No (default)
ICMP Type	Specifies the ICMP message type. Required if the signature engine is String ICMP.	0 to 18[1] a-b[,c-d]
No Case	Specifies to treat all alphabetic characters in the expression as case insensitive.	Yes | No (default)
Raw Regex	If set to Yes, Min Match Length, Max Match Length, Min Whole Length, Max Whole Length, Dot All, UTF8, No Case, Stingy, and End Optional are not used to reformat the regular expression string. **Note** Raw Regex lets you enter a regular expression string in Raw syntax without being translated.	Yes | No (default)
Regex String	(Required) Specifies the Regex pattern to use in the search. **Note** This parameter is required unless Max Stream Length is set. Do not set the Regex String if Max Stream Length is set.	string
Service Ports	(Required) Specifies a comma-separated list of ports or port ranges where the target service resides. **Note** This parameter is required for the String XL TCP and String XL UDP signature engines. It cannot be used for the String XL ICMP signature engine.	0 to 65535[1] a-b[,c-d]

Table B-36 String XL Engine Parameters (continued) (continued)

Parameter	Description	Value
Specify Exact Match Offset {Yes | No}	Enables exact match offset: • Exact Match Offset—Specifies the exact stream offset in bytes the regular expression string must report for a match to be valid.	0 to 65535
Specify Maximum Match Offset {Yes | No}	Enables maximum match offset: • Maximum Match Offset—Specifies the maximum stream offset in bytes the regular expression string must report for a match to be valid.	0 to 65535
Specify Min Match Offset {Yes | No}	Enables minimum match offset: • Min Match Offset—Specifies the minimum stream offset in bytes the regular expression string must report for a match to be valid.	0 to 65535
Specify Max Match Length {Yes | No}	Enables maximum match length: • Max Match Length—Specifies the maximum number of bytes the regular expression string must match for the pattern to be considered a hit.	0 to 65535
Specify Min Match Length {Yes | No}	Enables minimum match length: • Min Match Length—Specifies the minimum number of bytes the regular expression string must match for the pattern to be considered a hit.	0 to 65535
Specify Max Stream Length {Yes | No}	Enables maximum stream length: • Max Stream Length—Limits the search to the first configured number of bytes. The length of the stream is checked again this value. If the stream contains more bytes than this value, an alert is triggered. **Note** When you specify this parameter, you cannot configure Raw Regex or Regex String.	Yes | No 0 to 65535
Specify Max Whole Length {Yes | No}	Enables maximum whole length: • Max Whole Length—Specifies the maximum length for the pattern that will not be fragmented.	Yes | No 0 to 65535
Specify Min Whole Length {Yes | No}	Enables minimum whole length: • Min Whole Length—Specifies the minimum length for the pattern that will not be fragmented.	Yes | No 0 to 65535

Table B-36 String XL Engine Parameters (continued) (continued)

Parameter	Description	Value
Stingy	Specifies to stop looking for larger matches after the first completed match. **Note** Stingy can only be used with Min Match Length; otherwise, it is ignored.	True | False (default)
Strip Telnet Options	Strips the Telnet option characters from the data before the pattern is searched.[2]	True | False (default)
Swap Attacker Victim	True if address (and ports) source and destination are swapped in the alert message. False for no swap (default).	Yes | No (default)
UTF8	Treats all legal UTF-8 byte sequences in the expression as a single character.	True | False (default)

1. The second number in the range must be greater than or equal to the first number.
2. This parameter is primarily used as an IPS anti-evasion tool.

Unsupported String XL Parameters

Although you see the End Optional and Specify Max Stream Length parameters in the String XL engine, they are disabled. You receive an error message if you try to configure them. For example, here is the error message you receive after you create a signature using Specify Max Stream Length and then try to save it:

```
Apply Changes?[yes]: yes
Error: string-xl-tcp 60003.0 : Maximum Stream Length is currently not supported.
Please don't use this option.

The configuration changes failed validation, no changes were applied.
Would you like to return to edit mode to correct the errors? [yes]:
```

For More Information

- For more information on the parameters common to all signature engines, see Master Engine, page B-4.
- For a list of the signature regular expression syntax, see Regular Expression Syntax, page B-9.
- For example String XL TCP engine signatures, see Example String XL TCP Match Offset Signature, page 10-32 and Example String XL TCP Engine Minimum Match Length Signature, page 10-35.

Sweep Engines

This section describes the Sweep engines, and contains the following topics:

Sweep Engine

The Sweep engine analyzes traffic between two hosts or from one host to many hosts. You can tune the existing signatures or create custom signatures. The Sweep engine has protocol-specific parameters for ICMP, UDP, and TCP.

The alert conditions of the Sweep engine ultimately depend on the count of the unique parameter. The unique parameter is the threshold number of distinct hosts or ports depending on the type of sweep. The unique parameter triggers the alert when more than the unique number of ports or hosts is seen on the address set within the time period. The processing of unique port and host tracking is called counting.

Caution Event action filters based on source and destination IP addresses do not function for the Sweep engine, because they do not filter as regular signatures. To filter source and destination IP addresses in sweep alerts, use the source and destination IP address filter parameters in the Sweep engine signatures.

A unique parameter must be specified for all signatures in the Sweep engine. A limit of 2 through 40 (inclusive) is enforced on the sweeps. 2 is the absolute minimum for a sweep, otherwise, it is not a sweep (of one host or port). 40 is a practical maximum that must be enforced so that the sweep does not consume excess memory. More realistic values for unique range between 5 and 15.

TCP sweeps must have a TCP flag and mask specified to determine which sweep inspector slot in which to count the distinct connections. ICMP sweeps must have an ICMP type specified to discriminate among the various types of ICMP packets.

Data Node

When an activity related to Sweep engine signatures is seen, the IPS uses a data node to determine when it should stop monitoring for a particular host. The data node contains various persistent counters and variables needed for cross-packet reassembly of streams and for tracking the inspection state on a per-stream/per-source/per-destination basis The data node containing the sweep determines when the sweep should expire. The data node stops a sweep when the data node has not seen any traffic for *x* number of seconds (depending on the protocol).

There are several adaptive timeouts for the data nodes. The data node expires after 30 seconds of idle time on the address set after all of the contained objects have been removed. Each contained object has various timeouts, for example, TCP Stream has a one-hour timeout for established connections. Most other objects have a much shorter expiration time, such as 5 or 60 seconds.

Table B-37 lists the parameters specific to the Sweep engine.

Table B-37 Sweep Engine Parameters

Parameter	Description	Value
Destination Address Filter	Specifies the destination IP address to exclude from the sweep counting algorithm.	<A.B.C.D>-<A.B.C.D> [,<A.B.C.D>-<A.B.C.D>]
Source Address Filter	Specifies the source IP address to exclude from the sweep counting algorithm.	<A.B.C.D>-<A.B.C.D> [,<A.B.C.D>-<A.B.C.D>]

Table B-37 Sweep Engine Parameters (continued)

Parameter	Description	Value
Protocol	Specifies the protocol of interest for this inspector.	ICMP UDP TCP
Specify ICMP Type {Yes | No}	(Optional) Enables the ICMP header type: • ICMP Type—Specifies the value of the ICMP header TYPE.	0 to 255
Specify Port Range {Yes | No}	(Optional) Enables using a port range for inspection: • Port Range—Specifies the UDP port range used in inspection.	0 to 65535 a-b[,c-d]
Fragment Status	Specifies whether fragments are wanted or not: • Any fragment status • Do not inspect fragments • Inspect fragments	Any No Fragment Want Fragment
Inverted Sweep	Uses source port instead of destination port for unique counting.	True | False
Mask	Specifies the mask used in TCP flags comparison: • URG bit • ACK bit • PSH bit • RST bit • SYN bit • FIN bit	URG ACK PSH RST SYN FIN
Storage Key	Specifies the type of address key used to store persistent data: • Attacker address • Attacker and victim addresses • Attacker address and victim port	Axxx AxBx Axxb
Suppress Reverse	Does not fire when a sweep has fired in the reverse direction on this address set.	Yes | No
Swap Attacker Victim	Swaps the attacker and victim addresses and ports (source and destination) in the alert message and in any actions taken.	Yes | No (default)

Table B-37 Sweep Engine Parameters (continued)

Parameter	Description	Value
TCP Flags	Specifies the TCP flags to match when masked by mask: • URG bit • ACK bit • PSH bit • RST bit • SYN bit • FIN bit	URG ACK PSH RST SYN FIN
Unique	Specifies the threshold number of unique port connections between the two hosts.	0 to 65535

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Sweep Other TCP Engine

The Sweep Other TCP engine analyzes traffic between two hosts looking for abnormal packets typically used to fingerprint a victim. You can tune the existing signatures or create custom signatures.

TCP sweeps must have a TCP flag and mask specified. You can specify multiple entries in the set of TCP flags. And you can specify an optional port range to filter out certain packets.

Table B-38 lists the parameters specific to the Sweep Other TCP engine.

Table B-38 Sweep Other TCP Engine Parameters

Parameter	Description	Value
Specify Port Range {Yes | No}	(Optional) Enables using a port range for inspection: • Port Range—Specifies the UDP port range used in inspection.	0 to 65535 a-b[,c-d]
Set TCP Flags	Lets you set TCP flags to match. • TCP Flags—Specifies the TCP flags used in this inspection: – URG bit – ACK bit – PSH bit – RST bit – SYN bit – FIN bit	URG ACK PSH RST SYN FIN

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Traffic Anomaly Engine

Note Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

Note You can edit or tune anomaly detection signatures but you cannot create custom anomaly detection signatures.

The Traffic Anomaly engine contains nine anomaly detection signatures covering the three protocols (TCP, UDP, and other). Each signature has two subsignatures, one for the scanner and the other for the worm-infected host (or a scanner under worm attack). When anomaly detection discovers an anomaly, it triggers an alert for these signatures. All anomaly detection signatures are enabled by default and the alert severity for each one is set to high.

When a scanner is detected but no histogram anomaly occurred, the scanner signature fires for that attacker (scanner) IP address. If the histogram signature is triggered, the attacker addresses that are doing the scanning each trigger the worm signature (instead of the scanner signature). The alert details state which threshold is being used for the worm detection now that the histogram has been triggered. From that point on, all scanners are detected as worm-infected hosts.

The following anomaly detection event actions are possible:

- Product Alert—Writes the event to the Event Store.
- Deny Attacker Inline—Does not transmit this packet and future packets originating from the attacker address for a specified period of time.
- Log Attacker Packets—Starts IP logging for packets that contain the attacker address.
- Log Attacker/Victim Pair Packets—Starts IP logging for packets that contain the attacker and victim address pair.

  Note For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > *sensor_name* > Policies > Event Action Rules > rules0 > General Settings**.

- Deny Attacker Service Pair Inline—Blocks the source IP address and the destination port.
- Request SNMP Trap—Sends a request to NotificationApp to perform SNMP notification.
- Request Block Host—Sends a request to ARC to block this host (the attacker).

Table B-39 lists the anomaly detection worm signatures.

Table B-39 Anomaly Detection Worm Signatures

Signature ID	Subsignature ID	Name	Description
13000	0	Internal TCP Scanner	Identified a single scanner over a TCP protocol in the internal zone.
13000	1	Internal TCP Scanner	Identified a worm attack over a TCP protocol in the internal zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.
13001	0	Internal UDP Scanner	Identified a single scanner over a UDP protocol in the internal zone.
13001	1	Internal UDP Scanner	Identified a worm attack over a UDP protocol in the internal zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13002	0	Internal Other Scanner	Identified a single scanner over an Other protocol in the internal zone.
13002	1	Internal Other Scanner	Identified a worm attack over an Other protocol in the internal zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.
13003	0	External TCP Scanner	Identified a single scanner over a TCP protocol in the external zone.
13003	1	External TCP Scanner	Identified a worm attack over a TCP protocol in the external zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.
13004	0	External UDP Scanner	Identified a single scanner over a UDP protocol in the external zone.
13004	1	External UDP Scanner	Identified a worm attack over a UDP protocol in the external zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13005	0	External Other Scanner	Identified a single scanner over an Other protocol in the external zone.
13005	1	External Other Scanner	Identified a worm attack over an Other protocol in the external zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.
13006	0	Illegal TCP Scanner	Identified a single scanner over a TCP protocol in the illegal zone.
13006	1	Illegal TCP Scanner	Identified a worm attack over a TCP protocol in the illegal zone; the TCP histogram threshold was crossed and a scanner over a TCP protocol was identified.

Table B-39 Anomaly Detection Worm Signatures (continued)

Signature ID	Subsignature ID	Name	Description
13007	0	Illegal UDP Scanner	Identified a single scanner over a UDP protocol in the illegal zone.
13007	1	Illegal UDP Scanner	Identified a worm attack over a UDP protocol in the illegal zone; the UDP histogram threshold was crossed and a scanner over a UDP protocol was identified.
13008	0	Illegal Other Scanner	Identified a single scanner over an Other protocol in the illegal zone.
13008	1	Illegal Other Scanner	Identified a worm attack over an Other protocol in the illegal zone; the Other histogram threshold was crossed and a scanner over an Other protocol was identified.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Traffic ICMP Engine

The Traffic ICMP engine analyzes nonstandard protocols, such as TFN2K, LOKI, and DDoS. There are only two signatures (based on the LOKI protocol) with user-configurable parameters.

TFN2K is the newer version of the TFN. It is a DDoS agent that is used to control coordinated attacks by infected computers (zombies) to target a single computer (or domain) with bogus traffic floods from hundreds or thousands of unknown attacking hosts. TFN2K sends randomized packet header information, but it has two discriminators that can be used to define signatures. One is whether the L3 checksum is incorrect and the other is whether the character 64 'A' is found at the end of the payload. TFN2K can run on any port and can communicate with ICMP, TCP, UDP, or a combination of these protocols.

LOKI is a type of back door Trojan. When the computer is infected, the malicious code creates an ICMP Tunnel that can be used to send small payload in ICMP replies (which may go straight through a firewall if it is not configured to block ICMP.) The LOKI signatures look for an imbalance of ICMP echo requests to replies and simple ICMP code and payload discriminators.

The DDoS category (excluding TFN2K) targets ICMP-based DDoS agents. The main tools used here are TFN and Stacheldraht. They are similar in operation to TFN2K, but rely on ICMP only and have fixed commands: integers and strings.

Table B-40 lists the parameters specific to the Traffic ICMP engine.

Table B-40 Traffic ICMP Engine Parameters

Parameter	Description	Value
Parameter Tunable Sig	Specifies the whether this signature has configurable parameters.	Yes | No
Inspection Type	Specifies the type of inspection to perform: • Inspects for original LOKI traffic • Inspects for modified LOKI traffic	is Loki Is Mod Loki
Reply Ratio	Specifies the imbalance of replies to requests. The alert fires when there are this many more replies than requests.	0 to 65535
Want Request	Requires an ECHO REQUEST be seen before firing the alert.	True | False

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Trojan Engines

The Trojan engines analyze nonstandard protocols, such as BO2K and TFN2K. There are three Trojan engines: Trojan BO2K, TrojanTFN2K, and Trojan UDP.

BO was the original Windows back door Trojan that ran over UDP only. It was soon superseded by BO2K. BO2K supported UDP and TCP both with basic XOR encryption. They have plain BO headers that have certain cross-packet characteristics.

BO2K also has a stealthy TCP module that was designed to encrypt the BO header and make the cross-packet patterns nearly unrecognizable. The UDP modes of BO and BO2K are handled by the Trojan UDP engine. The TCP modes are handled by the Trojan BO2K engine.

Note There are no specific parameters to the Trojan engines, except for Swap Attacker Victim in the Trojan UDP engine.

For More Information

For more information on the parameters common to all signature engines, see Master Engine, page B-4.

Troubleshooting

This appendix contains troubleshooting tips and procedures for sensors and software. It contains the following sections:

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve our customers' effectiveness in network risk management and device troubleshooting.

BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The service has provision to filter bugs based on credentials to provide external and internal bug views for the search input.

Check out Bug Search Tools & Resources on Cisco.com. For more details on the tool overview and FAQs, check out the help page, located at this URL: http://www.cisco.com/web/applicat/cbsshelp/help.html.

Preventive Maintenance

This section describes how to perform preventive maintenance for your sensor, and contains the following topics:

Understanding Preventive Maintenance

The following actions will help you maintain your sensor:

- Back up a good configuration. If your current configuration becomes unusable, you can replace it with the backup version.
- Save your backup configuration to a remote system.
- Always back up your configuration before you do a manual upgrade. If you have auto upgrades configured, make sure you do periodic backups.
- Create a service account. A service account is needed for special debug situations directed by TAC.

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. Analyze your situation to decide if you want a service account existing on the system.

For More Information

- For the procedure for backing up a configuration file, see Creating and Using a Backup Configuration File, page C-2.
- For the procedure for using a remote server to copy and restore the a configuration file, see Backing Up and Restoring the Configuration File Using a Remote Server, page C-3.
- For more information about the service account, see Creating the Service Account, page C-5.

Creating and Using a Backup Configuration File

To protect your configuration, you can back up the current configuration and then display it to confirm that is the configuration you want to save. If you need to restore this configuration, you can merge the backup configuration file with the current configuration or overwrite the current configuration file with the backup configuration file.

To back up your current configuration, follow these steps:

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

Step 2 Save the current configuration. The current configuration is saved in a backup file.

```
sensor# copy current-config backup-config
```

Step 3 Display the backup configuration file. The backup configuration file is displayed.

```
sensor# more backup-config
```

Step 4 You can either merge the backup configuration with the current configuration, or you can overwrite the current configuration:

- Merge the backup configuration into the current configuration.

  ```
  sensor# copy backup-config current-config
  ```

- Overwrite the current configuration with the backup configuration.

  ```
  sensor# copy /erase backup-config current-config
  ```

Backing Up and Restoring the Configuration File Using a Remote Server

Note We recommend copying the current configuration file to a remote server before upgrading.

Use the **copy** [**/erase**] *source_url destination_url keyword* command to copy the configuration file to a remote server. You can then restore the current configuration from the remote server. You are prompted to back up the current configuration first.

The following options apply:

- **/erase**—Erases the destination file before copying.

  This keyword only applies to the current-config; the backup-config is always overwritten. If this keyword is specified for destination current-config, the source configuration is applied to the system default configuration. If it is not specified for the destination current-config, the source configuration is merged with the current-config.

- *source_url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination_url*—The location of the destination file to be copied. It can be a URL or a keyword.
- **current-config**—The current running configuration. The configuration becomes persistent as the commands are entered.
- **backup-config**—The storage location for the configuration backup.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

  - ftp:—Source or destination URL for an FTP network server. The syntax for this prefix is:

    ftp://[[username@]location][/relativeDirectory]/filename

    ftp://[[username@]location][//absoluteDirectory]/filename

Note You are prompted for a password.

– scp:—Source or destination URL for the SCP network server. The syntax for this prefix is:

scp://[[username@]location][/relativeDirectory]/filename

scp://[[username@]location][//absoluteDirectory]/filename

Note You are prompted for a password. You must add the remote host to the SSH known hosts list.

– http:—Source URL for the web server. The syntax for this prefix is:

http://[[username@]location][/directory]/filename

Note The directory specification should be an absolute path to the desired file.

– https:—Source URL for the web server. The syntax for this prefix is:

https://[[username@]location][/directory]/filename

Note The directory specification should be an absolute path to the desired file. The remote host must be a TLS trusted host.

Caution Copying a configuration file from another sensor may result in errors if the sensing interfaces and virtual sensors are not configured the same.

Backing Up the Current Configuration to a Remote Server

To back up your current configuration to a remote server, follow these steps:

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

Step 2 Back up the current configuration to the remote server.

```
sensor# copy current-config scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

Step 3 Enter **yes** to copy the current configuration to a backup configuration.

```
cfg            100% |***********************************************| 36124       00:00
```

Restoring the Current Configuration From a Backup File

To restore your current configuration from a backup file, follow these steps:

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

Step 2 Back up the current configuration to the remote server.

```
sensor# copy scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

Step 3 Enter **yes** to copy the current configuration to a backup configuration.

```
cfg            100% |***********************************************| 36124       00:00

Warning: Replacing existing network-settings may leave the box in an unstable state.
Would you like to replace existing network settings
(host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:
sensor#
```

Step 4 Enter **no** to retain the currently configured hostname, IP address, subnet mask, management interface, and access list. We recommend you retain this information to preserve access to your sensor after the rest of the configuration has been restored.

For More Information

For a list of supported HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 27-3.

Creating the Service Account

You can create a service account for TAC to use during troubleshooting. Although more than one user can have access to the sensor, only one user can have service privileges on a sensor. The service account is for support purposes only.

The root user password is synchronized to the service account password when the service account is created. To gain root access you must log in with the service account and switch to user root with the **su - root** command.

Caution Do not make modifications to the sensor through the service account except under the direction of TAC. If you use the service account to configure the sensor, your configuration is not supported by TAC. Adding services to the operating system through the service account affects proper performance and functioning of the other IPS services. TAC does not support a sensor on which additional services have been added.

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

Note For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.

To create the service account, follow these steps:

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

Step 2 Enter configuration mode.

```
sensor# configure terminal
```

Step 3 Specify the parameters for the service account. The username follows the pattern ^[A-Za-z0-9()+:,_/-]+$, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and _, and can contain 1 to 64 characters.

```
sensor(config)# user username privilege service
```

Step 4 Specify a password when prompted. A valid password is 8 to 32 characters long. All characters except space are allowed. If a service account already exists for this sensor, the following error is displayed and no service account is created.

```
Error: Only one service account may exist
```

Step 5 Exit configuration mode.

```
sensor(config)# exit
sensor#
```

When you use the service account to log in to the CLI, you receive this warning.

```
************************ WARNING ******************************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. This account is intended to be
used for support and troubleshooting purposes only. Unauthorized modifications are not
supported and will require this device to be reimaged to guarantee proper operation.
*******************************************************************************************
```

Disaster Recovery

Follow these recommendations so that you are ready in case of a disaster:

- If you are using the CLI, IDM, or IME for configuration, copy the current configuration from the sensor to an FTP or SCP server any time a change has been made.
- You should note the specific software version for that configuration. You can apply the copied configuration only to a sensor of the same version.
- You also need the list of user IDs that have been used on that sensor. The list of user IDs and passwords are not saved in the configuration.

When a disaster happens and you need to recover the sensor, try the following:

1. Reimage the sensor.

2. Log in to the sensor with the default user ID and password—**cisco**.

Note You are prompted to change the **cisco** password.

3. Initialize the sensor.
4. Upgrade the sensor to the IPS software version it had when the configuration was last saved and copied.

Warning **Trying to copy the saved configuration without getting the sensor back to the same IPS software version it had before the disaster can cause configuration errors.**

5. Copy the last saved configuration to the sensor.
6. Update clients to use the new key and certificate of the sensor. Reimaging changes the sensor SSH keys and HTTPS certificate, so you must add the hosts back to the SSN known hosts list.
7. Create previous users.

For More Information

- For the procedure for backing up a configuration file, see Creating and Using a Backup Configuration File, page C-2.
- For the procedure for obtaining a list of the current users on the sensor, see Configuring Authentication, page 6-17.
- For the procedures for reimage a sensor, see Chapter 27, "Upgrading, Downgrading, and Installing System Images."
- For the procedure for using the **setup** command to initialize the sensor, see Chapter 25, "Initializing the Sensor."
- For more information on obtaining IPS software and how to install it, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for using a remote server to copy and restore the a configuration file, see Backing Up and Restoring the Configuration File Using a Remote Server, page C-3.
- For the procedure for adding hosts to the SSH known hosts list, see Defining Known Host RSA1 Keys, page 15-9.
- For the procedure for adding users, see Configuring Authentication, page 6-17.

Password Recovery

For most IPS platforms, you can now recover the password on the sensor rather than using the service account or reimaging the sensor. This section describes how to recover the password for the various IPS platforms. It contains the following topics:

Understanding Password Recovery

Note Administrators may need to disable the password recovery feature for security reasons.

Password recovery implementations vary according to IPS platform requirements. Password recovery is implemented only for the cisco administrative account and is enabled by default. The IPS administrator can then recover user passwords for other accounts using the CLI. The cisco user password reverts to **cisco** and must be changed after the next login.

Table C-1 lists the password recovery methods according to platform.

Table C-1 Password Recovery Methods According to Platform

Platform	Description	Recovery Method
4300 series sensors 4500 series sensors	Standalone IPS appliances	GRUB prompt or ROMMON
ASA 5500-X IPS SSP ASA 5585-X IPS SSP	ASA 5500 series adaptive security appliance IPS modules	Adaptive security appliance CLI command

Recovering the Appliance Password

This section describes the two ways to recover the password for appliances. It contains the following topics:

Using the GRUB Menu

Note You must have a terminal server or direct serial connection to the appliance to use the GRUB menu to recover the password.

For the IPS 4355, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL appliances, the password recovery is found in the GRUB menu, which appears during bootup. When the GRUB menu appears, press any key to pause the boot process.

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance to see the GRUB menu.

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
-----------------------------------------
0: Cisco IPS
1: Cisco IPS Recovery
2: Cisco IPS Clear Password (cisco)
```

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

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    Commands before booting, or 'c' for a command-line.

    Highlighted entry is 0:
```

Step 2 Press any key to pause the boot process.

Step 3 Choose **`2: Cisco IPS Clear Password (cisco)`**. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

Using ROMMON

For the IPS 4345 IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL, you can use the ROMMON to recover the password. To access the ROMMON CLI, reboot the sensor from a terminal server or direct connection and interrupt the boot process.

Note After recovering the password, you must reset the confreg to **0**, otherwise, when you try to upgrade the sensor, the upgrade fails because when the sensor reboots, it goes to password recovery (**confreg 0x7**) rather than to the upgrade option.

To recover the password using the ROMMON CLI, follow these steps:

Step 1 Reboot the appliance.

Step 2 To interrupt the boot process, press **ESC** or **Control-R** (terminal server) or send a **BREAK** command (direct connection). The boot code either pauses for 10 seconds or displays something similar to one of the following:

- `Evaluating boot options`
- `Use BREAK or ESC to interrupt boot`

Step 3 Enter the following commands to reset the password:

```
confreg 0x7
boot
```

Sample ROMMON session:

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS-4360-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
```

```
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

Step 4 Enter the following command to reset the confreg value to 0:

```
confreg 0
```

Recovering the and ASA 5500-X IPS SSP Password

You can reset the password to the default (**cisco**) for the ASA 5500-X IPS SSP using the CLI or the ASDM. Resetting the password causes it to reboot. IPS services are not available during a reboot.

Note To reset the password, you must have ASA 8.6.1 or later.

Use the **sw-module module ips password-reset** command to reset the password to the default **cisco**. If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

To reset the password on the ASA 5500-X IPS SSP, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command:

```
asa# sw-module module ips password-reset
Reset the password on module ips? [confirm]
```

Step 2 Press **Enter** to confirm.

```
Password-Reset issued for module ips.
```

Step 3 Verify the status of the module. Once the status reads `Up`, you can session to the ASA 5500-X IPS SSP.

```
asa# show module ips
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
ips ASA 5555-X IPS Security Services Processor   ASA5555-IPS        FCH151070GR

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
ips 503d.e59c.7c4c to 503d.e59c.7c4c  N/A          N/A          7.2.(1)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- -------------------------
ips IPS                            Up               7.2.(1)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
ips Up                 Up

Mod License Name   License Status  Time Remaining
--- -------------- --------------- ---------------
ips IPS Module     Enabled         210 days
```

Step 4 Session to the ASA 5500-X IPS SSP.

```
asa# session ips
```

```
Opening command session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-^X'.
```

Step 5 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
Password: cisco

You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
```

Step 6 Enter your new password twice.

```
New password: new password
Retype new password: new password

***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on this IPS platform. The system will continue to
operate with the currently installed signature set. A valid license must be obtained in
order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a
new license or install a license.

asa-ssp#
```

Using the ASDM

To reset the password in the ASDM, follow these steps:

Step 1 From the ASDM menu bar, choose **Tools > IPS Password Reset**.

Note This option does not appear in the menu if there is no IPS present.

Step 2 In the IPS Password Reset confirmation dialog box, click **OK** to reset the password to the default (**cisco**). A dialog box displays the success or failure of the password reset. If the reset fails, make sure you have the correct ASA and IPS software versions.

Step 3 Click **Close** to close the dialog box. The sensor reboots.

Recovering the ASA 5585-X IPS SSP Password

Note To reset the password, you must have ASA 8.2.(4.4) or later or ASA 8.4.2 or later. The ASA 5585-X IPS SSP is not supported in ASA 8.3(*x*).

You can reset the password to the default (**cisco**) for the ASA 5585-X IPS SSP using the CLI or the ASDM. Resetting the password causes it to reboot. IPS services are not available during a reboot.

Use the **hw-module module** *slot_number* **password-reset** command to reset the password to the default **cisco**. If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

To reset the password on the ASA 5585-X IPS SSP, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command:

```
asa# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm]
```

Step 2 Press **Enter** to confirm.

```
Password-Reset issued for slot 1.
```

Step 3 Verify the status of the module. Once the status reads `Up`, you can session to the ASA 5585-X IPS SSP.

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5585-X IPS Security Services Processor-4 ASA5585-SSP-IPS40  JAF1436ABSG

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 5475.d029.8c74 to 5475.d029.8c7f  0.1          2.0(12)3     7.2.(1)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- -------------------------
  1 IPS                            Up               7.2.(1)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

Step 4 Session to the ASA 5585-X IPS SSP.

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 5 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
Password: cisco

You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
```

Step 6 Enter your new password twice.

```
New password: new password
Retype new password: new password

***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on this IPS platform. The system will continue to
operate with the currently installed signature set. A valid license must be obtained in
order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a
new license or install a license.
ips_ssp#
```

Using the ASDM

To reset the password in the ASDM, follow these steps:

Step 1 From the ASDM menu bar, choose **Tools > IPS Password Reset**.

Note This option does not appear in the menu if there is no IPS present.

Step 2 In the IPS Password Reset confirmation dialog box, click **OK** to reset the password to the default (**cisco**). A dialog box displays the success or failure of the password reset. If the reset fails, make sure you have the correct ASA and IPS software versions.

Step 3 Click **Close** to close the dialog box. The sensor reboots.

Disabling Password Recovery

Caution If you try to recover the password on a sensor on which password recovery is disabled, the process proceeds with no errors or warnings; however, the password is not reset. If you cannot log in to the sensor because you have forgotten the password, and password recovery is set to disabled, you must reimage your sensor.

Password recovery is enabled by default. You can disable password recovery through the CLI or IME.

Disabling Password Recovery Using the CLI

To disable password recovery in the CLI, follow these steps:

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

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Enter host mode.

```
sensor(config)# service host
```

Step 4 Disable password recovery.

```
sensor(config-hos)# password-recovery disallowed
```

Disabling Password Recovery Using the IME

To disable password recovery in the IME, follow these steps:

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

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Network**.

Step 3 To disable password recovery, uncheck the **Allow Password Recovery** check box.

Verifying the State of Password Recovery

Use the **show settings | include password** command to verify whether password recovery is enabled.

To verify whether password recovery is enabled, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

Step 3 Verify the state of password recovery by using the **include** keyword to show settings in a filtered output.

```
sensor(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
sensor(config-hos)#
```

Troubleshooting Password Recovery

When you troubleshoot password recovery, pay attention to the following:

- You cannot determine whether password recovery has been disabled in the sensor configuration from the ROMMON prompt, GRUB menu, switch CLI, or router CLI. If you attempt password recovery, it always appears to succeed. If it has been disabled, the password is not reset to **cisco**. The only option is to reimage the sensor.
- You can disable password recovery in the host configuration. For the platforms that use external mechanisms, such as ROMMON, although you can run commands to clear the password, if password recovery is disabled in the IPS, the IPS detects that password recovery is not allowed and rejects the external request.
- To check the state of password recovery, use the **show settings | include password** command.

Time Sources and the Sensor

This section describes how to maintain accurate time on the sensor, and contains the following topics:

Time Sources and the Sensor

Note We recommend that you use an NTP server to regulate time on your sensor. You can use authenticated or unauthenticated NTP. For authenticated NTP, you must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server. You can set up NTP during initialization or you can configure NTP through the CLI, IDM, IME, or ASDM.

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings. This section provides a summary of the various ways to set the time on sensors.

The IPS Standalone Appliances

- Use the **clock set** command to set the time. This is the default.
- Configure the appliance to get its time from an NTP time synchronization source.

Note The currently supported Cisco IPS appliances are the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL.

The ASA IPS Modules

- The ASA 5500-X IPS SSP and ASA 5585-X IPS SSP automatically synchronize their clocks with the clock in the adaptive security appliance in which they are installed. This is the default.
- Configure them to get their time from an NTP time synchronization source, such as a Cisco router other than the parent router.

For More Information

For the procedure for configuring NTP, see Configuring NTP, page 6-13.

Synchronizing IPS Module Clocks with Parent Device Clocks

The ASAIPS modules (ASA 5500-X IPS SSP ASA 5585-X IPS SSP) synchronize their clocks to the parent chassis clock (adaptive security appliance) each time the IPS boots up and any time the parent chassis clock is set. The IPS clock and parent chassis clock tend to drift apart over time. The difference can be as much as several seconds per day. To avoid this problem, make sure that both the IPS clock and the parent clock are synchronized to an external NTP server. If only the IPS clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs.

Verifying the Sensor is Synchronized with the NTP Server

In IPS, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the **show statistics host** command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.

To verify the NTP configuration, follow these steps:

Step 1 Log in to the sensor.

Step 2 Generate the host statistics.

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
          2 10373  9014   yes   yes  none    reject   reachable  1
        status = Not Synchronized
     ...
```

Step 3 Generate the hosts statistics again after a few minutes.

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
        *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
         LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f624   yes   yes   ok   sys.peer   reachable  2
          2 10373  9024   yes   yes  none    reject   reachable  2
        status = Synchronized
```

Step 4 If the status continues to read `Not Synchronized`, check with the NTP server administrator to make sure the NTP server is configured correctly.

Correcting Time on the Sensor

If you set the time incorrectly, your stored events will have the incorrect time because they are stamped with the time the event was created. The Event Store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command.

Note You cannot remove individual events.

For More Information

For the procedure for clearing events, see Clearing Events, page C-100.

Advantages and Restrictions of Virtualization

To avoid configuration problems on your sensor, make sure you understand the advantages and restrictions of virtualization on your sensor.

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:

- ASA 5500-X IPS SSP
- ASA 5585-X IPS SSP
- IPS 4345
- IPS 4345-DC
- IPS 4360
- IPS 4510
- IPS 4520

Supported MIBs

Note To receive sensor health information through SNMP traps, you must have the sensor health metrics enabled. Choose **Configuration > *sensor_name* > Sensor Management > Sensor Health** to enable sensor health metrics.

To avoid problems with configuring SNMP, be aware of the MIBs that are supported on the sensor.

The following private MIBs are supported on the sensor:

- CISCO-CIDS-MIB

  The CISCO-CIDS-MIB has been updated to include SNMP health data.
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

You can obtain these private Cisco MIBs under the heading SNMP v2 MIBs at this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Note MIB II is available on the sensor, but we do not support it. We know that some elements are not correct (for example, the packet counts from the IF MIB on the sensing interfaces). While you can use elements from MIB II, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

Note CISCO-PROCESS-MIB is available on the sensor, but we do not support it. We know that some elements are not available. While you can use elements from CISCO-PROCESS-MIB, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

When to Disable Anomaly Detection

If you have anomaly detection enabled and you have your sensor configured to see only one direction of traffic, you should disable anomaly detection. Otherwise, you will receive many alerts, because anomaly detection sees asymmetric traffic as having incomplete connections, that is, like worm scanners, and fires alerts.

To disable anomaly detection, follow these steps:

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

Step 2 Enter analysis engine submode.

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

Step 3 Enter the virtual sensor name that contains the anomaly detection policy you want to disable.

```
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)#
```

Step 4 Disable anomaly detection operational mode.

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# operational-mode inactive
sensor(config-ana-vir-ano)#
```

Step 5 Exit analysis engine submode.

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

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

For More Information

For more information about Worms, see Worms, page 13-2.

The Analysis Engine is Not Responding

Error Message `Output from show statistics analysis-engine`
`Error: getAnalysisEngineStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.`

Error Message `Output from show statistics anomaly-detection`
`Error: getAnomalyDetectionStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.`

Error Message `Output from show statistics denied-attackers`
`Error: getDeniedAttackersStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.`

Possible Cause These error messages appear when you run the **show tech support** command and the Analysis Engine is not running.

Recommended Action Verify the Analysis Engine is running and monitor it to see if the issue is resolved.

To verify the Analysis Engine is running and to monitor the issue, follow these steps:

Step 1 Log in to the sensor.

Step 2 Verify that the Analysis Engine is not running, Check to see if the Analysis Engine reads `Not Running`.

```
sensor# show version

-----
MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500 Not
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
```

Step 3 Enter **`show tech-support`** and save the output.

Step 4 Reboot the sensor.

Step 5 Enter **`show version`** after the sensor has stabilized to see if the issue is resolved.

Step 6 If the Analysis Engine still reads `Not Running`, contact TAC with the original **show tech support** command output.

Troubleshooting RADIUS Authentication

Symptom Attempt limit configured on the IPS sensor may not be enforced for a RADIUS user.

Conditions Applicable for RADIUS users only. The RADIUS user must have logged in to the sensor at least once after RADIUS authentication is enabled or after the sensor is reset or rebooted.

Workaround Log in to the sensor with the correct credentials and from that time on the attempt limit is enforced for that RADIUS user.

For More Information

For detailed information about RADIUS authentication, see Configuring Authentication, page 6-17.

Troubleshooting Global Correlation

Make sure you observe the following when configuring global correlation:

- Because global correlation updates occur through the sensor management interface, firewalls must allow port 443/80 traffic.
- You must have an HTTP proxy server or a DNS server configured to allow global correlation features to function.
- If you have an HTTP proxy server configured, the proxy must allow port 443/80 traffic from IPS systems.
- You must have a valid IPS license to allow global correlation features to function.
- Global correlation features only contain external IP addresses, so if you position a sensor in an internal lab, you may never receive global correlation information.
- Make sure your sensor supports the global correlation features.
- Make sure your IPS version supports the global correlation features.

For More Information

For more information on global correlation features and how to configure them, see Chapter 14, “Configuring Global Correlation.”

Troubleshooting External Product Interfaces

This section lists issues that can occur with external product interfaces and provides troubleshooting tips. It contains the following topics:

External Product Interfaces Issues

When the external product interface receives host posture and quarantine events, the following issues can arise:

- The sensor can store only a certain number of host records:
  - If the number of records exceeds 10,000, subsequent records are dropped.
  - If the 10,000 limit is reached and then it drops to below 9900, new records are no longer dropped.
- Hosts can change an IP address or appear to use another host IP address, for example, because of DHCP lease expiration or movement in a wireless network. In the case of an IP address conflict, the sensor presumes the most recent host posture event to be the most accurate.
- A network can include overlapping IP address ranges in different VLANs, but host postures do not include VLAN ID information. You can configure the sensor to ignore specified address ranges.
- A host can be unreachable from the CSA MC because it is behind a firewall. You can exclude unreachable hosts.
- The CSA MC event server allows up to ten open subscriptions by default. You can change this value. You must have an administrative account and password to open subscriptions.
- CSA data is not virtualized; it is treated globally by the sensor.
- Host posture OS and IP addresses are integrated into passive OS fingerprinting storage. You can view them as imported OS profiles.
- You cannot see the quarantined hosts.
- The sensor must recognize each CSA MC host X.509 certificate. You must add them as a trusted host.
- You can configure a maximum of two external product devices.

For More Information

- For more information on external product interfaces, see Chapter 19, "Configuring External Product Interfaces."
- For more information on working with OS maps and identifications, see Adding, Editing, Deleting, and Moving Configured OS Maps, page 12-27 and Configuring OS Identifications, page 21-17.
- For the procedure for adding trusted hosts, see Adding Trusted Hosts, page 15-13.

External Product Interfaces Troubleshooting Tips

To troubleshoot external product interfaces, check the following:

- Make sure the interface is active by checking the output from the **show statistics external-product-interface** command in the CLI, or choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Statistics** in the IME and check the Interface state line in the response.
- Make sure you have added the CSA MC IP address to the trusted hosts. If you forgot to add it, add it, wait a few minutes and then check again.
- Confirm subscription login information by opening and closing a subscription on the CSA MC using the browser.

- Check the Event Store for the CSA MC subscription errors.

For More Information

- For the procedure for adding trusted hosts, see Adding Trusted Hosts, page 15-13.
- For the procedure for displaying events, see Displaying Events, page C-97.

Troubleshooting the Appliance

Tip Before troubleshooting the appliance, check the Caveats section of the Readme for the software version you have installed on your sensor to see if you are dealing with a known issue.

This section contains information to troubleshoot the appliance. It contains the following topics:

Troubleshooting Loose Connections

Perform the following actions to troubleshoot loose connections on sensors:

- Make sure all power cords are securely connected.
- Make sure all cables are properly aligned and securely connected for all external and internal components.
- Remove and check all data and power cables for damage. Make sure no cables have bent pins or damaged connectors.
- Make sure each device is properly seated.
- If a device has latches, make sure they are completely closed and locked.
- Check any interlock or interconnect indicators that indicate a component is not connected properly.
- If problems continue, remove and reinstall each device, checking the connectors and sockets for bent pins or other damage.

The Analysis Engine is Busy

After you reimage a sensor, the Analysis Engine is busy rebuilding Regex tables and does not respond to new configurations. You can check whether the Analysis Engine is busy by using the **show statistics virtual-sensor** command. You receive the following error message if the Analysis Engine is busy:

```
sensor# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy rebuilding regex tables. This
may take a while.
sensor#
```

When the Analysis Engine is busy rebuilding Regex tables, you receive an error message if you try to update a configuration, for example, enabling or retiring a signature:

```
sensor# configure terminal
sensor(config)# service sig sig0
sensor(config-sig)# sig 2000 0
sensor(config-sig-sig)# status enabled
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# retired false
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
Error: editConfigDeltaSignatureDefinition : Analysis Engine is busy rebuilding regex
tables. This may take a while.
The configuration changes failed validation, no changes were applied.
Would you like to return to edit mode to correct the errors? [yes]: no
No changes were made to the configuration.
sensor(config)#
```

If you try to get the virtual sensor statistics immediately after you boot a sensor, you receive an error message. Although the sensor has rebuilt the cache files, the virtual sensor is not finished initializing.

```
sensor# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy.
sensor#
```

When you receive the errors that the Analysis Engine is busy, wait a while before trying to make configuration changes. Use the **show statistics virtual-sensor** command to find out when the Analysis Engine is available again.

Communication Problems

This section helps you troubleshoot communication problems with the 4200 series sensor. It contains the following topics:

Cannot Access the Sensor CLI Through Telnet or SSH

If you cannot access the sensor CLI through Telnet (if you already have it enabled) or SSH, follow these steps:

Step 1 Log in to the sensor CLI through a console, terminal, or module session.

Step 2 Make sure that the sensor management interface is enabled. The management interface is the interface in the list with the status line `Media Type = TX`. If the Link Status is `Down`, go to Step 3. If the Link Status is `Up`, go to Step 5.

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 944333
   Total Bytes Received = 83118358
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 397633
   Total Bytes Transmitted = 435730956
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 3 Make sure the sensor IP address is unique. If the management interface detects that another device on the network has the same IP address, it does not come up.

```
sensor# setup
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

Step 4 Make sure the management port is connected to an active network connection. If the management port is not connected to an active network connection, the management interface does not come up.

Step 5 Make sure the IP address of the workstation that is trying to connect to the sensor is permitted in the sensor access list. If the workstation network address is permitted in the sensor access list, go to Step 6.

```
sensor# setup
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

Step 6 Add a permit entry for the workstation network address, save the configuration, and try to connect again.

Step 7 Make sure the network configuration allows the workstation to connect to the sensor. If the sensor is protected behind a firewall and the workstation is in front of the firewall, make sure the firewall is configured to allow the workstation to access the sensor. Or if the workstation is behind a firewall that is performing network address translation on the workstation IP address, and the sensor is in front of the firewall, make sure that the sensor access list contains a permit entry for the workstation translated address.

For More Information

- For the procedures for changing the IP address, changing the access list, and enabling and disabling Telnet, see Configuring Network Settings, page 6-1.
- For the various ways to open a CLI session directly on the sensor, see Chapter 24, "Logging In to the Sensor."

Correcting a Misconfigured Access List

To correct a misconfigured access list, follow these steps:

Step 1 Log in to the CLI.

Step 2 View your configuration to see the access list.

```
sensor# show configuration | include access-list
access-list 10.0.0.0/8
access-list 64.0.0.0/8
sensor#
```

Step 3 Verify that the client IP address is listed in the allowed networks. If it is not, add it.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# access-list 171.69.70.0/24
```

Step 4 Verify the settings.

```
sensor(config-hos-net)# show settings
   network-settings
   ----------------------------------------------
      host-ip: 192.168.1.2/24,192.168.1.1 default: 10.1.9.201/24,10.1.9.1
      host-name: sensor-238 default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 3)
      ---------------------------------------------
         network-address: 10.0.0.0/8
         ---------------------------------------------
         network-address: 64.0.0.0/8
         ---------------------------------------------
         network-address: 171.69.70.0/24
         ---------------------------------------------
      ---------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ----------------------------------------------
sensor(config-hos-net)#
```

Duplicate IP Address Shuts Interface Down

If you have two newly imaged sensors with the same IP address that come up on the same network at the same time, the interface shuts down. Linux prevents the command and control interface from activating if it detects an address conflict with another host.

To verify that the sensor in question does not have an IP address conflict with another host on the network, follow these steps:

Step 1 Log in to the CLI.

Step 2 Determine whether the interface is up. If the output says the command and control interface link status is down, there is a hardware issue or an IP address conflict.

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1822323
   Total Bytes Received = 131098876
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 219260
   Total Bytes Transmitted = 103668610
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 3 Make sure the sensor cabling is correct.

Step 4 Make sure the IP address is correct.

For More Information

- To make sure the sensor cabling is correct, refer to your sensor chapter in *Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 7.2*.
- For the procedure for making sure the IP address is correct, see Configuring Network Settings, page 6-1.

The SensorApp and Alerting

This section helps you troubleshoot issues with the SensorApp and alerting. It contains the following topics:

The SensorApp Not Running

The sensing process, SensorApp, should always be running. If it is not, you do not receive any alerts. The SensorApp is part of the Analysis Engine, so you must make sure the Analysis Engine is running.

To make sure the Analysis Engine is running, follow these steps:

Step 1 Log in to the CLI.

Step 2 Determine the status of the Analysis Engine service and whether you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0        2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
No license present
Sensor up-time is 3 days.
Using 14470M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.1M out of 376.1M bytes of available disk space (24%
 usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
```

```
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

  IPS-K9-7.2-1-E4   11:17:07 UTC Thu Jan 10 2013

Recovery Partition Version 1.1 - 7.2(1)E4

Host Certificate Valid from: 17-Apr-2013 to 18-Apr-2015
sensor#
```

Step 3 If the Analysis Engine is not running, look for any errors connected to it.

```
sensor# show events error fatal past 13:00:00 | include AnalysisEngine
evError: eventId=1077219258696330005 severity=warning

originator:
hostId: sensor
appName: sensorApp
appInstanceId: 1045
time: 2004/02/19 19:34:20 2004/02/19 19:34:20 UTC
errorMessage: name=errUnclassified Generating new Analysis Engine configuration file.
```

Note The date and time of the last restart is listed. In this example, the last restart was on 2-19-2004 at 7:34.

Step 4 If you do not have the latest software updates, download them from Cisco.com. Read the Readme that accompanies the software upgrade for any known DDTS for the SensorApp or the Analysis Engine.

Step 5 If the Analysis Engine is still not running, enter **show tech-support** and save the output.

Step 6 Reboot the sensor.

Step 7 Enter **show version** after the sensor has stabilized to see if the issue is resolved.

Step 8 If the Analysis Engine still reads `Not Running`, contact TAC with the original **show tech support** command output.

For More Information

- For more information on IPS system architecture, see Appendix A, "System Architecture."
- For the procedure for obtaining the latest Cisco IPS software, see Obtaining Cisco IPS Software, page 26-1.

Physical Connectivity, SPAN, or VACL Port Issue

If the sensor is not connected properly, you do not receive any alerts.

To make sure the sensor is connected properly, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the interfaces are up and that the packet count is increasing.

```
sensor# show interfaces
```

```
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1830137
   Total Bytes Received = 131624465
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 220052
   Total Bytes Transmitted = 103796666
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 3 If the Link Status is down, make sure the sensing port is connected properly:

- Make sure the sensing port is connected properly on the appliance.
- Make sure the sensing port is connected to the correct SPAN or VACL capture port on IDSM2.

Step 4 Verify the interface configuration:

- Make sure you have the interfaces configured properly.
- Verify the SPAN and VACL capture port configuration on the Cisco switch.

  Refer to your switch documentation for the procedure.

Step 5 Verify again that the interfaces are up and that the packet count is increasing.

```
sensor# show interfaces
```

For More Information

- For the procedure for properly installing the sensing interface on your sensor, refer to your sensor chapter in *Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 7.2*.
- For the procedures for configuring interfaces on your sensor, see Chapter 7, "Configuring Interfaces."

Unable to See Alerts

If you are not seeing alerts, try the following:

- Make sure the signature is enabled
- Make sure the signature is not retired
- Make sure that you have Produce Alert configured as an action

Note If you choose Produce Alert, but come back later and add another event action and do not add Produce Alert to the new configuration, alerts are not sent to the Event Store. Every time you configure a signature, the new configuration overwrites the old one, so make sure you have configured all the event actions you want for each signature.

- Make sure the sensor is seeing packets
- Make sure that alerts are being generated
- Make sure the sensing interface is in a virtual sensor

To make sure you can see alerts, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the signature is enabled.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# show settings
   status
   ----------------------------------------------
      enabled: true <defaulted>
      retired: false <defaulted>
   ----------------------------------------------
sensor(config-sig-sig-sta)#
```

Step 3 Make sure you have Produce Alert configured.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine ?
normalizer     Signature engine
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert
sensor(config-sig-sig-nor)# show settings
   normalizer
   ----------------------------------------------
      event-action: produce-alert default: produce-alert|deny-connection-inline
      edit-default-sigs-only
      ----------------------------------------------
```

```
sensor#
```

Step 4 Make sure the sensor is seeing packets.

```
sensor# show interfaces FastEthernet0/1
MAC statistics from interface FastEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 267581
   Total Bytes Received = 24886471
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 57301
   Total Bytes Transmitted = 3441000
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 1
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 5 Check for alerts.

```
sensor# show statistics virtual-sensor
SigEvent Preliminary Stage Statistics
    Number of Alerts received = 0
    Number of Alerts Consumed by AlertInterval = 0
    Number of Alerts Consumed by Event Count = 0
    Number of FireOnce First Alerts = 0
    Number of FireOnce Intermediate Alerts = 0
    Number of Summary First Alerts  = 0
    Number of Summary Intermediate Alerts  = 0
    Number of Regular Summary Final Alerts  = 0
    Number of Global Summary Final Alerts  = 0
    Number of Alerts Output for further processing = 0alertDetails: Traffic Source: int0 ;
```

Sensor Not Seeing Packets

If the sensor is not seeing any packets on the network, you could have the interfaces set up incorrectly.

If the sensor is not seeing packets, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the interfaces are up and receiving packets.

```
sensor# show interfaces GigabitEthernet0/1
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
```

```
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Down
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 3 If the interfaces are not up, do the following:

- Check the cabling.
- Enable the interface.

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/1
   -----------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      alt-tcp-reset-interface
      ------------------------------------------------
         none
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   -----------------------------------------------
sensor(config-int-phy)#
```

Step 4 Check to see that the interface is up and receiving packets.

```
sensor# show interfaces
MAC statistics from interface GigabitEthernet0/1
   Media Type = TX
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 3
   Total Bytes Received = 900
   Total Multicast Packets Received = 3
```

```
Total Broadcast Packets Received = 0
Total Jumbo Packets Received = 0
Total Undersize Packets Received = 0
Total Receive Errors = 0
Total Receive FIFO Overruns = 0
Total Packets Transmitted = 0
Total Bytes Transmitted = 0
Total Multicast Packets Transmitted = 0
Total Broadcast Packets Transmitted = 0
Total Jumbo Packets Transmitted = 0
Total Undersize Packets Transmitted = 0
Total Transmit Errors = 0
Total Transmit FIFO Overruns = 0 ...
```

For More Information

For the procedure for installing the sensor properly, refer to your sensor chapter in *Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 7.2*.

Cleaning Up a Corrupted SensorApp Configuration

If the SensorApp configuration has become corrupted and the SensorApp cannot run, you must delete it entirely and restart the SensorApp.

To delete the SensorApp configuration, follow these steps:

Step 1 Log in to the service account.

Step 2 Su to root.

Step 3 Stop the IPS applications.

```
/etc/init.d/cids stop
```

Step 4 Replace the virtual sensor file.

```
cp /usr/cids/idsRoot/etc/defVirtualSensorConfig.xml
/usr/cids/idsRoot/etc/VS-Config/virtualSensor.xml
```

Step 5 Remove the cache files.

```
rm /usr/cids/idsRoot/var/virtualSensor/*.pmz
```

Step 6 Exit the service account.

Step 7 Log in to the sensor CLI.

Step 8 Start the IPS services.

```
sensor# cids start
```

Step 9 Log in to an account with administrator privileges.

Step 10 Reboot the sensor.

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? [yes]:yes
Request Succeeded.
sensor#
```

For More Information

For more information on IPS system architecture, see Appendix A, "System Architecture."

Blocking

This section provides troubleshooting help for blocking and the ARC service. It contains the following topics.

Troubleshooting Blocking

After you have configured the ARC, you can verify if it is running properly by using the **show version** command. To verify that the ARC is connecting to the network devices, use the **show statistics network-access** command.

Note The ARC was formerly known as Network Access Controller. Although the name has been changed since IPS 5.1, it still appears in IDM, IME, and the CLI as Network Access Controller, **nac**, and **network-access**.

To troubleshoot the ARC, follow these steps:

1. Verify that the ARC is running.
2. Verify that the ARC is connecting to the network devices.
3. Verify that the Event Action is set to Block Host for specific signatures.
4. Verify that the master blocking sensor is properly configured.

For More Information

- For the procedure to verify that the ARC is running, see Verifying the ARC is Running, page C-37.
- For the procedure to verify that the ARC is connecting, see Verifying ARC Connections are Active, page C-38.
- For the procedure to verify that the Event Action is set to Block Host, see Blocking Not Occurring for a Signature, page C-42.
- For the procedure to verify that the master blocking sensor is properly configured, see Verifying the Master Blocking Sensor Configuration, page C-43.
- For a discussion of ARC architecture, see Attack Response Controller, page A-12.

Verifying the ARC is Running

To verify that the ARC is running, use the **show version** command. If the MainApp is not running, the ARC cannot run. The ARC is part of the MainApp.

To verify that the ARC is running, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify that the MainApp is running.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0        2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
No license present
Sensor up-time is 3 days.
Using 14470M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.1M out of 376.1M bytes of available disk space (24%
 usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

  IPS-K9-7.2-1-E4   11:17:07 UTC Thu Jan 10 2013

Recovery Partition Version 1.1 - 7.2(1)E4
```

```
Host Certificate Valid from: 17-Apr-2013 to 18-Apr-2015
sensor#
```

Step 3 If the MainApp displays `Not Running`, the ARC has failed. Contact TAC.

For More Information

For more information on IPS system architecture, see Appendix A, "System Architecture."

Verifying ARC Connections are Active

If the State is not `Active` in the ARC statistics, there is a problem.

To verify that the State is Active in the statistics, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify that the ARC is connecting. Check the State section of the output to verify that all devices are connecting.

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.89.147.54
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.89.147.54
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
sensor#
```

Step 3 If the ARC is not connecting, look for recurring errors.

```
sensor# show events error hh:mm:ss month day year | include : nac
```

Example

```
sensor# show events error 00:00:00 Apr 01 2011 | include : nac
```

Step 4 Make sure you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

Host:
```

```
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0        2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
No license present
Sensor up-time is 3 days.
Using 14470M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.1M out of 376.1M bytes of available disk space (24%
 usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

  IPS-K9-7.2-1-E4   11:17:07 UTC Thu Jan 10 2013

Recovery Partition Version 1.1 - 7.2(1)E4

Host Certificate Valid from: 17-Apr-2013 to 18-Apr-2015
sensor#
```

Note If you do not have the latest software updates, download them from Cisco.com. Read the Readme that accompanies the software upgrade for any known DDTS for the ARC.

Step 5 Make sure the configuration settings for each device are correct (the username, password, and IP address).

Step 6 Make sure the interface and directions for each network device are correct.

Step 7 If the network device is using SSH-3DES, make sure that you have enabled SSH connections to the device.

Step 8 Verify that each interface and direction on each controlled device is correct.

For More Information

- For the procedure for obtaining the latest Cisco IPS software, see Obtaining Cisco IPS Software, page 26-1.
- For more information about configuring devices, see Device Access Issues, page C-40.
- For the procedure for verifying the interfaces and directions for each network device, see Verifying the Interfaces and Directions on the Network Device, page C-41.
- For the procedure for enabling SSH, see Enabling SSH Connections to the Network Device, page C-42.

Device Access Issues

The ARC may not be able to access the devices it is managing. Make sure the you have the correct IP address and username and password for the managed devices and the correct interface and direction configured.

Note SSH devices must support SSH 1.5. The sensor does not support SSH 2.0.

To troubleshoot device access issues, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify the IP address for the managed devices.

```
sensor# configure terminal
sensor (config)# service network-access
sensor(config-net)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   ------------------------------------------------
      profile-name: r7200
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ------------------------------------------------
   ------------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ------------------------------------------------
      ip-address: 10.89.147.54
      ------------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
```

```
            profile-name: r7200
            block-interfaces (min: 0, max: 100, current: 1)
            ----------------------------------------------
               interface-name: fa0/0
               direction: in
               ---------------------------------------------
                  pre-acl-name: <defaulted>
                  post-acl-name: <defaulted>
               ---------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      firewall-devices (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
sensor(config-net)#
```

Step 3 Manually connect to the device to make sure you have used the correct username, password, and enable password, and to ensure that the device is reachable from the sensor:

a. Log in to the service account.

b. Telnet or SSH to the network device to verify the configuration.

c. Make sure you can reach the device.

d. Verify the username and password.

Step 4 Verify that each interface and direction on each network device is correct.

For More Information

For the procedure for verifying the interfaces and directions for each network device, see Verifying the Interfaces and Directions on the Network Device, page C-41.

Verifying the Interfaces and Directions on the Network Device

To verify that each interface and direction on each controlled device is correct, you can send a manual block to a bogus host and then check to see if deny entries exist for the blocked addresses in the ACL of the router.

Note To perform a manual block, choose **Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Host Blocks**.

To initiate a manual block to a bogus host, follow these steps:

Step 1 Enter ARC general submode.

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
```

Step 2 Start the manual block of the bogus host IP address.

```
sensor(config-net-gen)# block-hosts 10.16.0.0
```

Step 3 Exit general submode.

```
sensor(config-net-gen)# exit
```

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

Step 4 Press **Enter** to apply the changes or type **no** to discard them.

Step 5 Telnet to the router and verify that a deny entry for the blocked address exists in the router ACL. Refer to the router documentation for the procedure.

Step 6 Remove the manual block by repeating Steps 1 through 4 except in Step 2 place **no** in front of the command.

```
sensor(config-net-gen)# no block-hosts 10.16.0.0
```

Enabling SSH Connections to the Network Device

If you are using SSH-3DES as the communication protocol for the network device, you must make sure you have enabled it on the device.

To enable SSH-3DES connections to the network device, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter configuration mode.

```
sensor# configure terminal
```

Step 3 Enable SSH-3DES.

```
sensor(config)# ssh-3des host blocking_device_ip_address
```

Step 4 Type **yes** when prompted to accept the device.

Blocking Not Occurring for a Signature

If blocking is not occurring for a specific signature, check that the event action is set to block the host.

To make sure blocking is occurring for a specific signature, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter signature definition submode.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)#
```

Step 3 Make sure the event action is set to block the host.

Note If you want to receive alerts, you must always add **produce-alert** any time you configure the event actions.

```
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert|request-block-host
sensor(config-sig-sig-nor)# show settings
```

```
   normalizer
   ----------------------------------------------
      event-action: produce-alert|request-block-host default: produce-alert|deny
-connection-inline
      edit-default-sigs-only
      ---------------------------------------------
         default-signatures-only
         ----------------------------------------------
            specify-service-ports
            ---------------------------------------------
               no
               ---------------------------------------------
               ---------------------------------------------
            ---------------------------------------------
            specify-tcp-max-mss
            ---------------------------------------------
               no
               ---------------------------------------------
               ---------------------------------------------
            ---------------------------------------------
            specify-tcp-min-mss
            ---------------------------------------------
               no
               ---------------------------------------------
               ---------------------------------------------
--MORE--
```

Step 4 Exit signature definition submode.

```
sensor(config-sig-sig-nor)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Step 5 Press **Enter** to apply the changes or type **no** to discard them.

Verifying the Master Blocking Sensor Configuration

To verify that a master blocking sensor is set up properly or to troubleshoot a master blocking sensor that is not set up properly, you can use the **show statistics network-access** command. Make sure that the forwarding sensor is set up as TLS trusted host if the remote master blocking sensor is using TLS for web access.

To verify a master blocking sensor configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 View the ARC statistics and verify that the master blocking sensor entries are in the statistics.

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
```

```
      Host
         IP = 122.122.122.44
         ShunMinutes = 60
         MinutesRemaining = 59
```

Step 3 If the master blocking sensor does not show up in the statistics, you need to add it.

Step 4 Initiate a manual block to a bogus host IP address to make sure the master blocking sensor is initiating blocks.

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
sensor(config-net-gen)# block-hosts 10.16.0.0
```

Step 5 Exit network access general submode.

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

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

Step 7 Verify that the block shows up in the ARC statistics.

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes =
```

Step 8 Log in to the CLI of the master blocking sensor host, and using the **show statistics network-access** command, verify that the block also shows up in the master blocking sensor ARC statistics.

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes = 60
         MinutesRemaining = 59
```

Step 9 If the remote master blocking sensor is using TLS for web access, make sure the forwarding sensor is configured as a TLS host.

```
sensor# configure terminal
sensor(config)# tls trust ip master_blocking_sensor_ip_address
```

For More Information

For the procedure to configure the sensor to be a master blocking sensor, see Configuring the Master Blocking Sensor, page 16-23.

Logging

This section describes debug logging, and contains the following topics:

Understanding Debug Logging

TAC may suggest that you turn on debug logging for troubleshooting purposes. Logger controls what log messages are generated by each application by controlling the logging severity for different logging zones. By default, debug logging is not turned on.

If you enable individual zone control, each zone uses the level of logging that it is configured for. Otherwise, the same logging level is used for all zones.

Enabling Debug Logging

Caution Enabling debug logging seriously affects performance and should only be done when instructed by TAC.

To enable debug logging, follow these steps:

Step 1 Log in to the service account.

Step 2 Edit the log.conf file to increase the size of the log to accommodate the additional log statements.

```
vi /usr/cids/idsRoot/etc/log.conf
```

Step 3 Change `fileMaxSizeInK=500` to `fileMaxSizeInK=5000`.

Step 4 Locate the zone and CID section of the file and set the severity to debug.

```
severity=debug
```

Step 5 Save the file, exit the vi editor, and exit the service account.

Step 6 Log in to the CLI as administrator.

Step 7 Enter master control submode.

```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# master-control
```

Step 8 Enable debug logging for all zones.

```
sensor(config-log-mas)# enable-debug true
sensor(config-log-mas)# show settings
   master-control
```

```
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: false <defaulted>
   ----------------------------------------------
sensor(config-log-mas)#
```

Step 9 Turn on individual zone control.

```
sensor(config-log-mas)# individual-zone-control true
sensor(config-log-mas)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
sensor(config-log-mas)#
```

Step 10 Exit master zone control.

```
sensor(config-log-mas)# exit
```

Step 11 View the zone names.

```
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: false <defaulted>
      individual-zone-control: true default: false
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: warning <defaulted>
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
```

```
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ----------------------------------------------
sensor(config-log)#
```

Step 12 Change the severity level (debug, timing, warning, or error) for a particular zone.

```
sensor(config-log)# zone-control IdsEventStore severity error
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
```

```
   ----------------------------------------------
sensor(config-log)#
```

Step 13 Turn on debugging for a particular zone.

```
sensor(config-log)# zone-control nac severity debug
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: debug default: warning
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ----------------------------------------------
sensor(config-log)#
```

Step 14 Exit the logger submode.

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

Step 15 Press **Enter** to apply changes or type `no` to discard them:

For More Information

For a list of what each zone name refers to, see Zone Names, page C-49.

Zone Names

Table C-2 lists the debug logger zone names:

Table C-2 Debug Logger Zone Names

Zone Name	Description
AD	Anomaly Detection zone
AuthenticationApp	Authentication zone
Cid	General logging zone
Cli	CLI zone
IdapiCtlTrans	All control transactions zone
IdsEventStore	Event Store zone
MpInstaller	IDSM-2 master partition installer zone
cmgr	Card Manager service zone
cplane	Control Plane zone
csi	CIDS Servlet Interface[1]
ctlTransSource	Outbound control transactions zone
intfc	Interface zone
nac	ARC zone
rep	Reputation zone
sched	Automatic update scheduler zone
sensorApp	AnalysisEngine zone
tls	SSL and TLS zone

1. The CIDS servlet interface is the interface layer between the CIDS web server and the servlets.

For More Information

To learn more about the IPS Logger service, see Logger, page A-19.

Directing cidLog Messages to SysLog

It might be useful to direct cidLog messages to syslog.

To direct cidLog messages to syslog, follow these steps:

Step 1 Go to the idsRoot/etc/log.conf file.

Step 2 Make the following changes:

a. Set [logApp] `enabled=false`

Comment out the `enabled=true` because `enabled=false` is the default.

b. Set [drain/main] `type=syslog`

The following example shows the logging configuration file:

```
timemode=local
;timemode=utc

[logApp]
;enabled=true
;-------- FIFO parameters --------
fifoName=logAppFifo
fifoSizeInK=240
;-------- logApp zone and drain parameters --------
zoneAndDrainName=logApp
fileName=main.log
fileMaxSizeInK=500

[zone/Cid]
severity=warning
drain=main

[zone/IdsEventStore]
severity=debug
drain=main

[drain/main]
type=syslog
```

The syslog output is sent to the syslog facility local6 with the following correspondence to syslog message priorities:

```
LOG_DEBUG,        //   debug
LOG_INFO,             //    timing
LOG_WARNING,   //    warning
LOG_ERR,             //    error
LOG_CRIT             //     fatal
```

Note Make sure that your /etc/syslog.conf has that facility enabled at the proper priority.

Caution The syslog is much slower than logApp (about 50 messages per second as opposed to 1000 or so). We recommend that you enable debug severity on one zone at a time.

TCP Reset Not Occurring for a Signature

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

If you do not have the event action set to reset, the TCP reset does not occur for a specific signature.

Note TCP Resets are not supported over MPLS links or the following tunnels: GRE, IPv4 in IPv4, IPv6 in IPv4, or IPv4 in IPv6.

To troubleshoot a reset not occurring for a specific signature, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the event action is set to TCP reset.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1000 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# event-action reset-tcp-connection|produc-alert
sensor(config-sig-sig-ato)# show settings
   atomic-ip
   ----------------------------------------------
      event-action: produce-alert|reset-tcp-connection default: produce-alert
      fragment-status: any <defaulted>
      specify-l4-protocol
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-payload-length
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-header-length
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-tos
      ----------------------------------------------
--MORE--
```

Step 3 Exit signature definition submode.

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

Step 4 Press **Enter** to apply the changes or type **no** to discard them.

Step 5 Make sure the correct alarms are being generated.

```
sensor# show events alert
evAlert: eventId=1047575239898467370 severity=medium
originator:
hostId: sj_4250_40
appName: sensorApp
appInstanceId: 1004
signature: sigId=20000 sigName=STRING.TCP subSigId=0 version=Unknown
addr: locality=OUT 172.16.171.19
port: 32771
victim:
addr: locality=OUT 172.16.171.13 port: 23
actions:
tcpResetSent: true
```

Step 6 Make sure the switch is allowing incoming TCP reset packet from the sensor. Refer to your switch documentation for more information.

Step 7 Make sure the resets are being sent.

```
root# ./tcpdump -i eth0 src host 172.16.171.19
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0
13:58:03.823929 172.16.171.19.32770 > 172.16.171.13.telnet: R 79:79(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
```

Software Upgrades

This section helps in troubleshooting software upgrades. It contains the following topics:

Upgrading

When you upgrade an IPS sensor, you may receive an error that the Analysis Engine is not running:

```
sensor# upgrade scp://user@10.1.1.1/upgrades/IPS-K9-7.2.-1-E4.pkg
Password: ********
Warning: Executing this command will apply a major version upgrade to the application
partition. The system may be rebooted to complete the upgrade.
Continue with upgrade?: yes
Error: AnalysisEngine is not running. Please reset box and attempt upgrade again.
```

If you receive this error, you must get the Analysis Engine running before trying to upgrade again. This error is often caused by a defect in the currently running version. Try rebooting the sensor, and after reboot, run the **setup** command and remove the interfaces from the virtual sensor vs0. When it is not monitoring traffic, Analysis Engine usually stays up and running. You can upgrade at this time. After the upgrade, add the interfaces back to the virtual sensor vs0 using the **setup** command.

Or you can use the system image file to reimage the sensor directly to the version you want. You can reimage a sensor and avoid the error because the reimage process does not check to see if the Analysis Engine is running.

Caution Reimaging using the system image file restores all configuration defaults.

For More Information

- For more information on running the **setup** command, see Chapter 25, "Initializing the Sensor."
- For more information on reimaging your sensor, see Chapter 27, "Upgrading, Downgrading, and Installing System Images."

Which Updates to Apply and Their Prerequisites

You must have the correct service pack and minor and major version of the software. If you are having trouble with applying new software, make sure that you are applying the proper updates with the proper prerequisites:

- Signature updates require the minimum version and engine version listed in the filename.
- Engine updates require the major or minor version in the engine update filename. Service packs require the correct minor version.
- Minor versions require the correct major version.
- Major versions require the previous major version.

For More Information

To understand how to interpret the IPS software filenames, see IPS Software Versioning, page 26-3.

Issues With Automatic Update

The following list provides suggestions for troubleshooting automatic updates:

- Run TCPDUMP:
  - Create a service account. **Su** to root and run TCPDUMP on the command and control interface to capture packets between the sensor and the FTP server.
  - Use the **upgrade** command to manually upgrade the sensor.
  - Look at the TCPDUMP output for errors coming back from the FTP server.
- Make sure the sensor is in the correct directory. The directory must be specified correctly. This has caused issues with Windows FTP servers. Sometimes an extra "/" or even two "/" are needed in front of the directory name. To verify this, use the same FTP commands you see in the TCPDUMP output through your own FTP connection.
- You must use the Windows FTP server setup option to emulate UNIX file structure and not MS-DOS file structure.
- If you are using SCP, make sure you have added the SSH host key to the known hosts list.

Try the manual **upgrade** command before attempting the automatic update. If it works with the **upgrade** command and does not work with the automatic update, try the following:

- Determine which IPS software version your sensor has.
- Make sure the passwords are configured for automatic update. Make sure they match the same passwords used for manual update.
- Make sure that the filenames in the FTP server are exactly what you see on Downloads on Cisco.com. This includes capitalization. Some Windows FTP servers allow access to the file with the incorrect capitalization but the sensor ultimately rejects the file because the name has changed.
- If necessary, run TCPDUMP on automatic update. You can compare the successful manual update with the unsuccessful automatic update and troubleshoot from there.

For More Information

- For the procedure for creating the service account, see Creating the Service Account, page C-5.
- For the procedure for reimaging your sensor, see Chapter 27, "Upgrading, Downgrading, and Installing System Images."
- For the procedure for adding hosts to the SSH known hosts list, see Defining Known Host RSA1 Keys, page 15-9.
- For the procedure for determining the software version, see Displaying Version Information, page C-80.

Updating a Sensor with the Update Stored on the Sensor

You can store the update package in the /var directory on the sensor and update the sensor from there if you need to.

To update the sensor with an update stored on the sensor, follow these steps:

Step 1 Log in to the service account.

Step 2 Obtain the update package file from Cisco.com.

Step 3 FTP or SCP the update file to the sensor /usr/cids/idsRoot/var directory.

Step 4 Set the file permissions:.

```
chmod 644 ips_package_file_name
```

Step 5 Exit the service account.

Step 6 Log in to the sensor using an account with administrator privileges.

Step 7 Store the sensor host key.

```
sensor# configure terminal
sensor(config)# service ssh
sensor(config-ssh)# rsa1-keys sensor_ip_address
```

Step 8 Upgrade the sensor.

```
sensor(config)# upgrade scp://service@sensor_ip_address/upgrade/ips_package_file_name
Enter password: *****
Re-enter password: *****
```

For More Information

For the procedure for obtaining Cisco IPS software, see Obtaining Cisco IPS Software, page 26-1.

Troubleshooting the IDM

Tip Before troubleshooting the IDM, check the Caveats section of the Readme for the software version you have installed on your sensor to see if you are dealing with a known issue.

Note These procedures also apply to the IPS section of the ASDM.

Note The IDM is part of the IME configuration, so these troubleshooting procedures also apply to the IME.

Note After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.

This section contains troubleshooting procedures for the IDM. It contains the following topics:

Cannot Launch the IDM - Loading Java Applet Failed

Symptom The browser displays `Loading Cisco IDM. Please wait ...` At the bottom left corner of the window, `Loading Java Applet Failed` is displayed.

Possible Cause This condition can occur if multiple Java Plug-ins are installed on the machine on which you are launching the IDM.

Recommended Action Clear the Java cache and remove temp files and clear history in the browser you are using. The result is that neither of these plug-ins will be used by default and each applet should use the correct plug-in.

To clear the cache, follow these steps:

Step 1 Close all browser windows.

Step 2 If you have Java Plug-in 1.3.*x* installed:

a. Click **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.3.x**.

b. Click the **Advanced** tab.

c. Under Java Runtime Environment, select **JRE 1.3.x** from the drop-down menu.
d. Click the **Cache** tab.
e. Click **Clear**.

Step 3 If you have Java Plug-in 1.4.*x* installed:

a. Click **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.4.x**.
b. Click the **Advanced** tab.
c. Under Java Runtime Environment, select **JRE 1.3.x** from the drop-down menu.
d. Click the **Cache** tab.
e. Click the **Browser** tab.
f. Deselect all browser check boxes.
g. Click **Clear Cache**.

Step 4 Delete the temp files and clear the history in the browser.

Cannot Launch the IDM-the Analysis Engine Busy

Error Message `Error connecting to sensor. Failed to load sensor-errNotAvailable-Analysis Engine is busy. Exiting IDM.`

Possible Cause This condition can occur if the Analysis Engine in the sensor is busy getting ready to perform a task and so does not respond to the IDM.

Recommended Action Wait for a while and try again to connect.

The IDM, Remote Manager, or Sensing Interfaces Cannot Access Sensor

If the IDM, a remote manager, or sensing interfaces cannot access the sensor, but you can access the sensor CLI using SSH or Telnet (if enabled), follow these steps:

Step 1 Make sure the network configuration allows access to the web server port that is configured on the sensor:

```
sensor# setup


    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
```

```
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
```

Step 2 If network devices, such as routers, switches, or firewalls, are between the sensor and the workstation, make sure these devices are configured to allow the workstation to access the sensor web server port. All remote management communication is performed by the sensor web server.

For More Information

For the procedure for enabling and disabling Telnet on the sensor, and configuring the web server, see Configuring Network Settings, page 6-1.

Signatures Not Producing Alerts

Caution You cannot add other actions each time you configure the event actions. You are actually replacing the list of event actions every time you configure it, so make sure you choose Produce Alert every time you configure event actions.

If you are not seeing any alerts when signatures are firing, make sure that you have configured Produce Alert as an event action. For example, if you choose Produce Alert, but later add another event action and do not add Produce Alert to the new configuration, alerts are not sent to the Event Store. To make sure you are getting alerts, check the statistics for the virtual sensor and the Event Store.

For More Information

- For more information about event actions, see Event Actions, page 12-7.
- For the procedure for configuring event actions, see Assigning Actions to Signatures, page 10-23.
- For the procedure for obtaining statistics about virtual sensor and Event Store, see Viewing Statistics, page 21-22.

Troubleshooting the IME

Tip Before troubleshooting the IME, check the Caveats section of the Readme for the software version you have installed on your sensor to see if you are dealing with a known issue.

This section describes troubleshooting tools for the IME, and contains the following sections:

Time Synchronization on the IME and the Sensor

Symptom The IME displays `No Data Available` on the Events dashboard. A historical query does not return any events; however, events are coming in to the IME and they appear in the real-time event viewer.

Possible Cause The time is not synchronized between the sensor and the IME local server. The IME dashboards use a time relative to the IME local time. If these times are not synchronized, the query does not return any results. When you add a sensor to the IME, it checks for the time synchronization and warns you to correct it if is in wrong. The IME also displays a clock warning in Home > Devices > Device List to warn you about problems with synchronization.

Recommended Action Change the time settings on the sensor or the IME local server. In most cases, the time change is required for the sensor because it is configured with the incorrect or default time.

For More Information

- For more information on time and the sensor, see Time Sources and the Sensor, page C-15.
- For the procedure for changing the time on the sensor, see Correcting Time on the Sensor, page C-17.

Not Supported Error Message

Symptom The IME displays `Not Supported` in the device list table and in some gadgets, and no data is included.

Possible Cause Click **Details** to see an explanation for this message. The IME needs IPS 6.1 or later to obtain certain information. The IME still operates with event monitoring and reporting for IPS 5.0 and later and specific IOS IPS versions, but some functions, such as health information and integrated configuration, are not available.

Recommended Action Upgrade to IPS 6.1 or later.

Troubleshooting the ASA 5500-X IPS SSP

Tip Before troubleshooting the ASA 5500-X IPS SSP, check the Caveats section of the Readme for the software version installed on your sensor to see if you are dealing with a known issue.

This section contains troubleshooting information specific to the ASA 5500-X IPS SSP, and contains the following topics:

Failover Scenarios

The following failover scenarios apply to the ASA 5500-X series in the event of configuration changes, signature/signature engine updates, service packs, and SensorApp crashes on theASA 5500-X IPS SSP.

Single ASA in Fail-Open Mode

- If the ASA is configured in fail-open mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP experiences a configuration change or signature/signature engine update, traffic is passed through the ASA without being inspected.
- If the ASA is configured in fail-open mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is passed through the ASA without being inspected.

Single ASA in Fail-Close Mode

- If the ASA is configured in fail-close mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the ASA.
- If the ASA is configured in fail-close mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is stopped from passing through the ASA.

Two ASAs in Fail-Open Mode

- If the ASAs are configured in fail-open mode and if the ASA 5500-X IPS SSP on the active ASA experiences a configuration change or a signature/signature engine update, traffic is still passed through the active ASA without being inspected. Failover is not triggered.
- If the ASAs are configured in fail-open mode, and if the ASA 5500-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5500-X IPS SSP that was previously the standby ASA 5500-X IPS SSP.

Two ASAs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the ASA 5500-X IPS SSP on the active ASA experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the active ASA. No failover is triggered.
- If the ASAs are configured in fail-close mode, and if the ASA 5500-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5500-X IPS SSP that was previously the standby for the ASA 5500-X IPS SSP.

Configuration Examples

Use the following configuration for the primary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Use the following configuration for the secondary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Health and Status Information

To see the general health of the ASA 5500-X IPS SSP, use the **show module ips details** command.

```
asa# show module ips details
Getting details from the Service Module, please wait...

Card Type:          IPS 5555 Intrusion Prevention System
Model:              IPS5555
Hardware version:   N/A
Serial Number:      FCH1504V0CW
Firmware version:   N/A
Software version:   7.2.(1)E4
MAC Address Range:  503d.e59c.7ca0 to 503d.e59c.7ca0
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2.(1)E4
Data Plane Status:  Up
Status:             Up
License:            IPS Module  Enabled  perpetual
Mgmt IP addr:       192.168.1.2
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.168.1.1
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

The output shows that the ASA 5500-X IPS SSP is up. If the status reads `Down`, you can reset it using the **sw-module module 1 reset** command.

If you have problems with reimaging the ASA 5500-X IPS SSP, use the **debug module-boot** command to see the output as it boots. Make sure you have the correct IP address for the TFTP server and you have the correct file on the TFTP server. Then use the **sw-module module ips recover** command again to reimage the module.

```
asa-ips# sw-module module ips recover configure image
disk0:/IPS-SSP_5555-K9-sys-1.1-a-7.2.-1-E4.aip
Image URL [tftp://192.0.2.1/IPS-5545-K9-sys-1.1-a-7.2.-1-E4.aip]:
Port IP Address [192.0.2.226]:
VLAN ID [0]:
Gateway IP Address [192.0.2.254]:

asa-ips# debug module-boot
debug module-boot  enabled at level 1
asa-ips# sw-module module ips reload

Reload module ips? [confirm]
Reload issued for module ips.
asa-ips# Mod-ips 228> ***
Mod-ips 229> *** EVENT: The module is reloading.
Mod-ips 230> *** TIME: 08:07:36 CST Jan 17 2012
Mod-ips 231> ***
Mod-ips 232> Mod-ips 233> The system is going down NOW!
Mod-ips 234> Sending SIGTERM to all processes
Mod-ips 235> Sending SIGKILL to all processes
Mod-ips 236> Requesting system reboot
Mod-ips 237> e1000 0000:00:07.0: PCI INT A disabled
Mod-ips 238> e1000 0000:00:06.0: PCI INT A disabled
Mod-ips 239> e1000 0000:00:05.0: PCI INT A disabled
Mod-ips 240> Restarting system.
Mod-ips 241> machine restart
Mod-ips 242> IVSHMEM: addr = 4093640704 size = 67108864
Mod-ips 243>   Booting 'Cisco IPS'
Mod-ips 244> root (hd0,0)
Mod-ips 245>  Filesystem type is ext2fs, partition type 0x83
Mod-ips 246> kernel /ips-2.6.ld ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
init
Mod-ips 247> fs=runtime-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepag
Mod-ips 248> es=3223
Mod-ips 249>    [Linux-bzImage, setup=0x2c00, size=0x2bad80]
Mod-ips 250> Linux version 2.6.29.1 (ipsbuild@seti-teambuilder-a) (gcc version 4.3.2
(crosstool
Mod-ips 251> -NG-1.4.1) ) #56 SMP Tue Dec 6 00:46:11 CST 2011
Mod-ips 252> Command line: ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
initfs=runti
Mod-ips 253> me-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepages=3223
Mod-ips 254> KERNEL supported cpus:
Mod-ips 255>   Intel GenuineIntel
Mod-ips 256>   AMD AuthenticAMD
Mod-ips 257>   Centaur CentaurHauls
Mod-ips 258> BIOS-provided physical RAM map:
Mod-ips 259>  BIOS-e820: 0000000000000000 - 000000000009f400 (usable)
Mod-ips 260>  BIOS-e820: 000000000009f400 - 00000000000a0000 (reserved)
Mod-ips 261>  BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
Mod-ips 262>  BIOS-e820: 0000000000100000 - 00000000dfffd000 (usable)
Mod-ips 263>  BIOS-e820: 00000000dfffd000 - 00000000e0000000 (reserved)
Mod-ips 264>  BIOS-e820: 00000000fffbc000 - 0000000100000000 (reserved)
Mod-ips 265>  BIOS-e820: 0000000100000000 - 0000000201400000 (usable)
```

```
Mod-ips 266> DMI 2.4 present.
Mod-ips 267> last_pfn = 0x201400 max_arch_pfn = 0x100000000
Mod-ips 268> last_pfn = 0xdfffd max_arch_pfn = 0x100000000
Mod-ips 269> init_memory_mapping: 0000000000000000-00000000dfffd000
Mod-ips 270> last_map_addr: dfffd000 end: dfffd000
Mod-ips 271> init_memory_mapping: 0000000100000000-0000000201400000
Mod-ips 272> last_map_addr: 201400000 end: 201400000
Mod-ips 273> ACPI: RSDP 000F88D0, 0014 (r0 BOCHS )
Mod-ips 274> ACPI: RSDT DFFFDD00, 0034 (r1 BOCHS  BXPCRSDT        1 BXPC        1)
Mod-ips 275> ACPI: FACP DFFFFD90, 0074 (r1 BOCHS  BXPCFACP        1 BXPC        1)
Mod-ips 276> FADT: X_PM1a_EVT_BLK.bit_width (16) does not match PM1_EVT_LEN (4)
Mod-ips 277> ACPI: DSDT DFFFDF10, 1E22 (r1   BXPC   BXDSDT        1 INTL 20090123)
Mod-ips 278> ACPI: FACS DFFFFD40, 0040
Mod-ips 279> ACPI: SSDT DFFFDE90, 0079 (r1 BOCHS  BXPCSSDT        1 BXPC        1)
Mod-ips 280> ACPI: APIC DFFFDD80, 0090 (r1 BOCHS  BXPCAPIC        1 BXPC        1)
Mod-ips 281> ACPI: HPET DFFFDD40, 0038 (r1 BOCHS  BXPCHPET        1 BXPC        1)
Mod-ips 282> No NUMA configuration found
Mod-ips 283> Faking a node at 0000000000000000-0000000201400000
Mod-ips 284> Bootmem setup node 0 0000000000000000-0000000201400000
Mod-ips 285>   NODE_DATA [0000000000011000 - 000000000001ffff]
Mod-ips 286>   bootmap [0000000000020000 -  000000000006027f] pages 41
Mod-ips 287> (6 early reservations) ==> bootmem [0000000000 - 0201400000]
Mod-ips 288>   #0 [0000000000 - 0000001000]   BIOS data page ==> [0000000000 - 0000001000]
Mod-ips 289>   #1 [0000006000 - 0000008000]       TRAMPOLINE ==> [0000006000 - 0000008000]
Mod-ips 290>   #2 [0000200000 - 0000d55754]    TEXT DATA BSS ==> [0000200000 - 0000d55754]
Mod-ips 291>   #3 [000009f400 - 0000100000]    BIOS reserved ==> [000009f400 - 0000100000]
Mod-ips 292>   #4 [0000008000 - 000000c000]          PGTABLE ==> [0000008000 - 000000c000]
Mod-ips 293>   #5 [000000c000 - 0000011000]          PGTABLE ==> [000000c000 - 0000011000]
Mod-ips 294> found SMP MP-table at [ffff8800000f8920] 000f8920
Mod-ips 295> Zone PFN ranges:
Mod-ips 296>   DMA      0x00000000 -> 0x00001000
Mod-ips 297>   DMA32    0x00001000 -> 0x00100000
Mod-ips 298>   Normal   0x00100000 -> 0x00201400
Mod-ips 299> Movable zone start PFN for each node
Mod-ips 300> early_node_map[3] active PFN ranges
Mod-ips 301>     0: 0x00000000 -> 0x0000009f
Mod-ips 302>     0: 0x00000100 -> 0x000dfffd
Mod-ips 303>     0: 0x00100000 -> 0x00201400
Mod-ips 304> ACPI: PM-Timer IO Port: 0xb008
Mod-ips 305> ACPI: LAPIC (acpi_id[0x00] lapic_id[0x00] enabled)
Mod-ips 306> ACPI: LAPIC (acpi_id[0x01] lapic_id[0x01] enabled)
Mod-ips 307> ACPI: LAPIC (acpi_id[0x02] lapic_id[0x02] enabled)
Mod-ips 308> ACPI: LAPIC (acpi_id[0x03] lapic_id[0x03] enabled)
Mod-ips 309> ACPI: LAPIC (acpi_id[0x04] lapic_id[0x04] enabled)
Mod-ips 310> ACPI: LAPIC (acpi_id[0x05] lapic_id[0x05] enabled)
Mod-ips 311> ACPI: IOAPIC (id[0x06] address[0xfec00000] gsi_base[0])
Mod-ips 312> IOAPIC[0]: apic_id 6, version 0, address 0xfec00000, GSI 0-23
Mod-ips 313> ACPI: INT_SRC_OVR (bus 0 bus_irq 5 global_irq 5 high level)
Mod-ips 314> ACPI: INT_SRC_OVR (bus 0 bus_irq 9 global_irq 9 high level)
Mod-ips 315> ACPI: INT_SRC_OVR (bus 0 bus_irq 10 global_irq 10 high level)
Mod-ips 316> ACPI: INT_SRC_OVR (bus 0 bus_irq 11 global_irq 11 high level)
Mod-ips 317> Using ACPI (MADT) for SMP configuration information
Mod-ips 318> ACPI: HPET id: 0x8086a201 base: 0xfed00000
Mod-ips 319> SMP: Allowing 6 CPUs, 0 hotplug CPUs
Mod-ips 320> Allocating PCI resources starting at e2000000 (gap: e0000000:1ffbc000)
Mod-ips 321> NR_CPUS:32 nr_cpumask_bits:32 nr_cpu_ids:6 nr_node_ids:1
Mod-ips 322> PERCPU: Allocating 49152 bytes of per cpu data
Mod-ips 323> Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 1939347
Mod-ips 324> Policy zone: Normal
Mod-ips 325> Kernel command line: ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
initf
Mod-ips 326> s=runtime-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepages=3
Mod-ips 327> 223
```

```
Mod-ips 328> hugetlb_lowmem_setup: Allocated 2097152 huge pages (size=0x200000) from
lowmem are
Mod-ips 329> a at 0xffff88002ee00000 phys addr 0x000000002ee00000
Mod-ips 330> Initializing CPU#0
Mod-ips 331> PID hash table entries: 4096 (order: 12, 32768 bytes)
Mod-ips 332> Fast TSC calibration using PIT
Mod-ips 333> Detected 2792.965 MHz processor.
Mod-ips 334> Console: colour VGA+ 80x25
Mod-ips 335> console [ttyS0] enabled
Mod-ips 336> Checking aperture...
Mod-ips 337> No AGP bridge found
Mod-ips 338> PCI-DMA: Using software bounce buffering for IO (SWIOTLB)
Mod-ips 339> Placing 64MB software IO TLB between ffff880020000000 - ffff880024000000
Mod-ips 340> software IO TLB at phys 0x20000000 - 0x24000000
Mod-ips 341> Memory: 7693472k/8409088k available (3164k kernel code, 524688k absent,
190928k re
Mod-ips 342> served, 1511k data, 1032k init)
Mod-ips 343> Calibrating delay loop (skipped), value calculated using timer frequency..
5585.93
Mod-ips 344>  BogoMIPS (lpj=2792965)
Mod-ips 345> Dentry cache hash table entries: 1048576 (order: 11, 8388608 bytes)
Mod-ips 346> Inode-cache hash table entries: 524288 (order: 10, 4194304 bytes)
Mod-ips 347> Mount-cache hash table entries: 256
Mod-ips 348> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 349> CPU: L2 cache: 4096K
Mod-ips 350> CPU 0/0x0 -> Node 0
Mod-ips 351> Freeing SMP alternatives: 29k freed
Mod-ips 352> ACPI: Core revision 20081204
Mod-ips 353> Setting APIC routing to flat
Mod-ips 354> ..TIMER: vector=0x30 apic1=0 pin1=0 apic2=-1 pin2=-1
Mod-ips 355> CPU0: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 356> Booting processor 1 APIC 0x1 ip 0x6000
Mod-ips 357> Initializing CPU#1
Mod-ips 358> Calibrating delay using timer specific routine.. 5585.16 BogoMIPS
(lpj=2792581)
Mod-ips 359> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 360> CPU: L2 cache: 4096K
Mod-ips 361> CPU 1/0x1 -> Node 0
Mod-ips 362> CPU1: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 363> checking TSC synchronization [CPU#0 -> CPU#1]:
Mod-ips 364> Measured 1453783140569731 cycles TSC warp between CPUs, turning off TSC
clock.
Mod-ips 365> Marking TSC unstable due to check_tsc_sync_source failed
Mod-ips 366> Booting processor 2 APIC 0x2 ip 0x6000
Mod-ips 367> Initializing CPU#2
Mod-ips 368> Calibrating delay using timer specific routine.. 5580.51 BogoMIPS
(lpj=2790259)
Mod-ips 369> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 370> CPU: L2 cache: 4096K
Mod-ips 371> CPU 2/0x2 -> Node 0
Mod-ips 372> CPU2: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 373> Booting processor 3 APIC 0x3 ip 0x6000
Mod-ips 374> Initializing CPU#3
Mod-ips 375> Calibrating delay using timer specific routine.. 5585.18 BogoMIPS
(lpj=2792594)
Mod-ips 376> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 377> CPU: L2 cache: 4096K
Mod-ips 378> CPU 3/0x3 -> Node 0
Mod-ips 379> CPU3: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 380> Booting processor 4 APIC 0x4 ip 0x6000
Mod-ips 381> Initializing CPU#4
Mod-ips 382> Calibrating delay using timer specific routine.. 5585.15 BogoMIPS
(lpj=2792579)
Mod-ips 383> CPU: L1 I cache: 32K, L1 D cache: 32K
```

```
Mod-ips 384> CPU: L2 cache: 4096K
Mod-ips 385> CPU 4/0x4 -> Node 0
Mod-ips 386> CPU4: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 387> Booting processor 5 APIC 0x5 ip 0x6000
Mod-ips 388> Initializing CPU#5
Mod-ips 389> Calibrating delay using timer specific routine.. 5585.21 BogoMIPS
(lpj=2792609)
Mod-ips 390> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 391> CPU: L2 cache: 4096K
Mod-ips 392> CPU 5/0x5 -> Node 0
Mod-ips 393> CPU5: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 394> Brought up 6 CPUs
Mod-ips 395> Total of 6 processors activated (33507.17 BogoMIPS).
Mod-ips 396> net_namespace: 1312 bytes
Mod-ips 397> Booting paravirtualized kernel on bare hardware
Mod-ips 398> NET: Registered protocol family 16
Mod-ips 399> ACPI: bus type pci registered
Mod-ips 400> dca service started, version 1.8
Mod-ips 401> PCI: Using configuration type 1 for base access
Mod-ips 402> mtrr: your CPUs had inconsistent variable MTRR settings
Mod-ips 403> mtrr: your CPUs had inconsistent MTRRdefType settings
Mod-ips 404> mtrr: probably your BIOS does not setup all CPUs.
Mod-ips 405> mtrr: corrected configuration.
Mod-ips 406> bio: create slab <bio-0> at 0
Mod-ips 407> ACPI: Interpreter enabled
Mod-ips 408> ACPI: (supports S0 S5)
Mod-ips 409> ACPI: Using IOAPIC for interrupt routing
Mod-ips 410> ACPI: No dock devices found.
Mod-ips 411> ACPI: PCI Root Bridge [PCI0] (0000:00)
Mod-ips 412> pci 0000:00:01.3: quirk: region b000-b03f claimed by PIIX4 ACPI
Mod-ips 413> pci 0000:00:01.3: quirk: region b100-b10f claimed by PIIX4 SMB
Mod-ips 414> IVSHMEM: addr = 4093640704 size = 67108864
Mod-ips 415> ACPI: PCI Interrupt Link [LNKA] (IRQs 5 *10 11)
Mod-ips 416> ACPI: PCI Interrupt Link [LNKB] (IRQs 5 *10 11)
Mod-ips 417> ACPI: PCI Interrupt Link [LNKC] (IRQs 5 10 *11)
Mod-ips 418> ACPI: PCI Interrupt Link [LNKD] (IRQs 5 10 *11)
Mod-ips 419> SCSI subsystem initialized
Mod-ips 420> usbcore: registered new interface driver usbfs
Mod-ips 421> usbcore: registered new interface driver hub
Mod-ips 422> usbcore: registered new device driver usb
Mod-ips 423> PCI: Using ACPI for IRQ routing
Mod-ips 424> pnp: PnP ACPI init
Mod-ips 425> ACPI: bus type pnp registered
Mod-ips 426> pnp: PnP ACPI: found 9 devices
Mod-ips 427> ACPI: ACPI bus type pnp unregistered
Mod-ips 428> NET: Registered protocol family 2
Mod-ips 429> IP route cache hash table entries: 262144 (order: 9, 2097152 bytes)
Mod-ips 430> TCP established hash table entries: 524288 (order: 11, 8388608 bytes)
Mod-ips 431> TCP bind hash table entries: 65536 (order: 8, 1048576 bytes)
Mod-ips 432> TCP: Hash tables configured (established 524288 bind 65536)
Mod-ips 433> TCP reno registered
Mod-ips 434> NET: Registered protocol family 1
Mod-ips 435> Adding htlb page ffff88002ee00000 phys 000000002ee00000 page ffffe20000a41000
Mod-ips 436> HugeTLB registered 2 MB page size, pre-allocated 3223 pages
Mod-ips 437> report_hugepages: Using 1 pages from low memory at ffff88002ee00000 HugeTLB
FS
Mod-ips 438> msgmni has been set to 15026
Mod-ips 439> alg: No test for stdrng (krng)
Mod-ips 440> io scheduler noop registered
Mod-ips 441> io scheduler anticipatory registered
Mod-ips 442> io scheduler deadline registered
Mod-ips 443> io scheduler cfq registered (default)
Mod-ips 444> pci 0000:00:00.0: Limiting direct PCI/PCI transfers
Mod-ips 445> pci 0000:00:01.0: PIIX3: Enabling Passive Release
```

```
Mod-ips 446> pci 0000:00:01.0: Activating ISA DMA hang workarounds
Mod-ips 447> pci_hotplug: PCI Hot Plug PCI Core version: 0.5
Mod-ips 448> pciehp: PCI Express Hot Plug Controller Driver version: 0.4
Mod-ips 449> acpiphp: ACPI Hot Plug PCI Controller Driver version: 0.5
Mod-ips 450> acpiphp_glue: can't get bus number, assuming 0
Mod-ips 451> decode_hpp: Could not get hotplug parameters. Use defaults
Mod-ips 452> acpiphp: Slot [1] registered
Mod-ips 453> acpiphp: Slot [2] registered
Mod-ips 454> acpiphp: Slot [3] registered
Mod-ips 455> acpiphp: Slot [4] registered
Mod-ips 456> acpiphp: Slot [5] registered
Mod-ips 457> acpiphp: Slot [6] registered
Mod-ips 458> acpiphp: Slot [7] registered
Mod-ips 459> acpiphp: Slot [8] registered
Mod-ips 460> acpiphp: Slot [9] registered
Mod-ips 461> acpiphp: Slot [10] registered
Mod-ips 462> acpiphp: Slot [11] registered
Mod-ips 463> acpiphp: Slot [12] registered
Mod-ips 464> acpiphp: Slot [13] registered
Mod-ips 465> acpiphp: Slot [14] registered
Mod-ips 466> acpiphp: Slot [15] registered
Mod-ips 467> acpiphp: Slot [16] registered
Mod-ips 468> acpiphp: Slot [17] registered
Mod-ips 469> acpiphp: Slot [18] registered
Mod-ips 470> acpiphp: Slot [19] registered
Mod-ips 471> acpiphp: Slot [20] registered
Mod-ips 472> acpiphp: Slot [21] registered
Mod-ips 473> acpiphp: Slot [22] registered
Mod-ips 474> acpiphp: Slot [23] registered
Mod-ips 475> acpiphp: Slot [24] registered
Mod-ips 476> acpiphp: Slot [25] registered
Mod-ips 477> acpiphp: Slot [26] registered
Mod-ips 478> acpiphp: Slot [27] registered
Mod-ips 479> acpiphp: Slot [28] registered
Mod-ips 480> acpiphp: Slot [29] registered
Mod-ips 481> acpiphp: Slot [30] registered
Mod-ips 482> acpiphp: Slot [31] registered
Mod-ips 483> shpchp: Standard Hot Plug PCI Controller Driver version: 0.4
Mod-ips 484> fakephp: Fake PCI Hot Plug Controller Driver
Mod-ips 485> fakephp: pci_hp_register failed with error -16
Mod-ips 486> fakephp: pci_hp_register failed with error -16
Mod-ips 487> fakephp: pci_hp_register failed with error -16
Mod-ips 488> fakephp: pci_hp_register failed with error -16
Mod-ips 489> fakephp: pci_hp_register failed with error -16
Mod-ips 490> fakephp: pci_hp_register failed with error -16
Mod-ips 491> fakephp: pci_hp_register failed with error -16
Mod-ips 492> processor ACPI_CPU:00: registered as cooling_device0
Mod-ips 493> processor ACPI_CPU:01: registered as cooling_device1
Mod-ips 494> processor ACPI_CPU:02: registered as cooling_device2
Mod-ips 495> processor ACPI_CPU:03: registered as cooling_device3
Mod-ips 496> processor ACPI_CPU:04: registered as cooling_device4
Mod-ips 497> processor ACPI_CPU:05: registered as cooling_device5
Mod-ips 498> hpet_acpi_add: no address or irqs in _CRS
Mod-ips 499> Non-volatile memory driver v1.3
Mod-ips 500> Linux agpgart interface v0.103
Mod-ips 501> ipmi message handler version 39.2
Mod-ips 502> ipmi device interface
Mod-ips 503> IPMI System Interface driver.
Mod-ips 504> ipmi_si: Unable to find any System Interface(s)
Mod-ips 505> IPMI SMB Interface driver
Mod-ips 506> IPMI Watchdog: driver initialized
Mod-ips 507> Copyright (C) 2004 MontaVista Software - IPMI Powerdown via sys_reboot.
Mod-ips 508> Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled
Mod-ips 509> ?serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
```

```
Mod-ips 510> serial8250: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
Mod-ips 511> 00:06: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
Mod-ips 512> 00:07: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
Mod-ips 513> brd: module loaded
Mod-ips 514> loop: module loaded
Mod-ips 515> lpc: version 0.1 (Nov 10 2011)
Mod-ips 516> tun: Universal TUN/TAP device driver, 1.6
Mod-ips 517> tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
Mod-ips 518> Uniform Multi-Platform E-IDE driver
Mod-ips 519> piix 0000:00:01.1: IDE controller (0x8086:0x7010 rev 0x00)
Mod-ips 520> piix 0000:00:01.1: not 100native mode: will probe irqs later
Mod-ips 521>     ide0: BM-DMA at 0xc000-0xc007
Mod-ips 522>     ide1: BM-DMA at 0xc008-0xc00f
Mod-ips 523> hda: QEMU HARDDISK, ATA DISK drive
Mod-ips 524> Clocksource tsc unstable (delta = 2851415955127 ns)
Mod-ips 525> hda: MWDMA2 mode selected
Mod-ips 526> hdc: QEMU DVD-ROM, ATAPI CD/DVD-ROM drive
Mod-ips 527> hdc: MWDMA2 mode selected
Mod-ips 528> ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
Mod-ips 529> ide1 at 0x170-0x177,0x376 on irq 15
Mod-ips 530> ide_generic: please use "probe_mask=0x3f" module parameter for probing all
legacy
Mod-ips 531> ISA IDE ports
Mod-ips 532> ide-gd driver 1.18
Mod-ips 533> hda: max request size: 512KiB
Mod-ips 534> hda: 7815168 sectors (4001 MB) w/256KiB Cache, CHS=7753/255/63
Mod-ips 535> hda: cache flushes supported
Mod-ips 536>  hda: hda1 hda2 hda3 hda4
Mod-ips 537> Driver 'sd' needs updating - please use bus_type methods
Mod-ips 538> Driver 'sr' needs updating - please use bus_type methods
Mod-ips 539> ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI) Driver
Mod-ips 540> ohci_hcd: USB 1.1 'Open' Host Controller (OHCI) Driver
Mod-ips 541> uhci_hcd: USB Universal Host Controller Interface driver
Mod-ips 542> Initializing USB Mass Storage driver...
Mod-ips 543> usbcore: registered new interface driver usb-storage
Mod-ips 544> USB Mass Storage support registered.
Mod-ips 545> PNP: PS/2 Controller [PNP0303:KBD,PNP0f13:MOU] at 0x60,0x64 irq 1,12
Mod-ips 546> serio: i8042 KBD port at 0x60,0x64 irq 1
Mod-ips 547> serio: i8042 AUX port at 0x60,0x64 irq 12
Mod-ips 548> mice: PS/2 mouse device common for all mice
Mod-ips 549> rtc_cmos 00:01: rtc core: registered rtc_cmos as rtc0
Mod-ips 550> rtc0: alarms up to one day, 114 bytes nvram
Mod-ips 551> input: AT Translated Set 2 keyboard as /class/input/input0
Mod-ips 552> i2c /dev entries driver
Mod-ips 553> piix4_smbus 0000:00:01.3: SMBus Host Controller at 0xb100, revision 0
Mod-ips 554> device-mapper: ioctl: 4.14.0-ioctl (2008-04-23) initialised:
dm-devel@redhat.com
Mod-ips 555> cpuidle: using governor ladder
Mod-ips 556> usbcore: registered new interface driver usbhid
Mod-ips 557> usbhid: v2.6:USB HID core driver
Mod-ips 558> TCP cubic registered
Mod-ips 559> IPv6: Loaded, but is disabled by default. IPv6 may be enabled on individual
interf
Mod-ips 560> aces.
Mod-ips 561> NET: Registered protocol family 10
Mod-ips 562> NET: Registered protocol family 17
Mod-ips 563> NET: Registered protocol family 5
Mod-ips 564> rtc_cmos 00:01: setting system clock to 2012-01-17 14:06:34 UTC (1326809194)
Mod-ips 565> Freeing unused kernel memory: 1032k freed
Mod-ips 566> Write protecting the kernel read-only data: 4272k
Mod-ips 567> Loader init started...
Mod-ips 568> kjournald starting.  Commit interval 5 seconds
Mod-ips 569> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 570> input: ImExPS/2 Generic Explorer Mouse as /class/input/input1
```

```
Mod-ips 571> 51216 blocks
Mod-ips 572> Checking rootrw fs: corrected filesystem
Mod-ips 573> kjournald starting.  Commit interval 5 seconds
Mod-ips 574> EXT3 FS on hda2, internal journal
Mod-ips 575> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 576> mkdir: cannot create directory '/lib/modules': File exists
Mod-ips 577> init started: BusyBox v1.13.1 (2011-11-01 07:21:34 CDT)
Mod-ips 578> starting pid 678, tty '': '/etc/init.d/rc.init'
Mod-ips 579> Checking system fs: no errors
Mod-ips 580> kjournald starting.  Commit interval 5 seconds
Mod-ips 581> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 582> /etc/init.d/rc.init: line 102: /proc/sys/vm/bdflush: No such file or
directory
Mod-ips 583> starting pid 728, tty '': '/etc/init.d/rcS'
Mod-ips 584> Initializing random number generator... done.
Mod-ips 585> Starting network... ifconfig lo 127.0.0.1 netmask 255.255.255.255 up
Mod-ips 586> starting inetd
Mod-ips 587> done
Mod-ips 588> Starting sshd:
Mod-ips 589> Starting nscd:
Mod-ips 590> Set Irq Affinity ... cpus:
Mod-ips 591> Checking kernel allocated memory: EXT3 FS on hda1, internal journal
Mod-ips 592> [  OK  ]
Mod-ips 593> Unloading REGEX-CP drivers ...
Mod-ips 594> Loading REGEX-CP drivers ...
Mod-ips 595> ACPI: PCI Interrupt Link [LNKD] enabled at IRQ 11
Mod-ips 596> cpp_user_kvm 0000:00:04.0: PCI INT A -> Link[LNKD] -> GSI 11 (level, high) ->
IRQ
Mod-ips 597> 11
Mod-ips 598> Detected cpp_user_kvm device with 33554432 bytes of shared memory
Mod-ips 599> Device 0: model=LCPX8640, cpc=T2005, cpe0=None, cpe1=None
Mod-ips 600> Load cidmodcap:
Mod-ips 601> Create node:
Mod-ips 602> ln: /etc/modprobe.conf: File exists
Mod-ips 603> Shutting down network... ifconfig lo down
Mod-ips 604> ifconfig lo down
Mod-ips 605> done
Mod-ips 606> Load ihm:
Mod-ips 607> Create node:
Mod-ips 608> Load kvm_ivshmem: IVSHMEM: writing 0x0 to 0xc86cf8
Mod-ips 609> IVSHMEM: IntrMask write(w) val = 0xffff
Mod-ips 610> Create node:
Mod-ips 611> Create node:
Mod-ips 612> Create node:
Mod-ips 613> Set Irq Affinity ... cpus: 6
Mod-ips 614> Starting network... ifconfig lo 127.0.0.1 netmask 255.255.255.255 up
Mod-ips 615> done
Mod-ips 616> Creating boot.info[  OK  ]
Mod-ips 617> Checking for system modifications since last boot[  OK  ]
Mod-ips 618> Checking model identification[  OK  ]
Mod-ips 619> Model: ASA-5555
Mod-ips 620> Model=ASA-5555
Mod-ips 621> Unable to set speed and duplex for user mode interfaces
Mod-ips 622> interface type 0x8086:0x100e at pci address 0:6.0(0) is currently named eth1
Mod-ips 623> Renaming eth1 --> ma0_0
Mod-ips 624> interface type 0x8086:0x100e at pci address 0:7.0(0) is currently named po0_0
Mod-ips 625> interface type 0x8086:0x100e at pci address 0:5.0(0) is currently named eth0
Mod-ips 626> Renaming eth0 --> sy0_0
Mod-ips 627> Initializing access list
Mod-ips 628> MGMT_INTFC_CIDS_NAME Management0/0
Mod-ips 629> MGMT_INTFC_OS_NAME ma0_0
Mod-ips 630> SYSTEM_PCI_IDS 0x0030,0x0028
Mod-ips 631> Load rebootkom:
Mod-ips 632> root: Starting SSM controlplane
```

```
Mod-ips 633> Starting CIDS:
Mod-ips 634> starting pid 1718, tty '/dev/ttyS0': '/sbin/getty -L ttyS0 9600 vt100'
```

The ASA 5500-X IPS SSP and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the ASA 5500-X IPS SSP, because the ASA itself handles the normalization. Packets on the ASA IPS modules go through a special path in the Normalizer that only reassembles fragments and puts packets in the right order for the TCP stream. The Normalizer does not do any of the normalization that is done on an inline IPS appliance, because that causes problems in the way the ASA handles the packets.

The following Normalizer engine signatures are not supported:

- 1300.0
- 1304.0
- 1305.0
- 1307.0
- 1308.0
- 1309.0
- 1311.0
- 1315.0
- 1316.0
- 1317.0
- 1330.0
- 1330.1
- 1330.2
- 1330.9
- 1330.10
- 1330.12
- 1330.14
- 1330.15
- 1330.16
- 1330.17
- 1330.18

The ASA 5500-X IPS SSP and Memory Usage

For the ASA 5500-X IPS SSP, the memory usage is 93%. The default health thresholds for the sensor are 80% for yellow and 91% for red, so the sensor health will be shown as red on these platforms even for normal operating conditions. You can tune the threshold percentage for memory usage so that it reads more accurately for these platforms by configuring the Memory Usage option in the sensor health metrics.

Note Make sure you have the Memory Usage option in the sensor health metrics enabled.

Table C-3 lists the Yellow Threshold and the Red Threshold health values.

Table C-3 ASA 5500-X IPS SSP Memory Usage Values

Platform	Yellow	Red	Memory Used
ASA 5512-X IPS SSP	85%	91%	28%
ASA 5515-X IPS SSP	88%	92%	14%
ASA 5525-X IPS SSP	88%	92%	14%
ASA 5545-X IPS SSP	93%	96%	13%
ASA 5555-X IPS SSP	95%	98%	17%

The ASA 5500-X IPS SSP and Jumbo Packets

The jumbo packet count in the **show interface** command output from the lines `Total Jumbo Packets Received` and `Total Jumbo Packets Transmitted` for ASA IPS modules may be larger than expected due to some packets that were almost jumbo size on the wire being counted as jumbo size by the IPS. This miscount is a result of header bytes added to the packet by the ASA before the packet is transmitted to the IPS. For IPv4, 58 bytes of header data are added. For IPv6, 78 bytes of header data are added. The ASA removes the added IPS header before the packet leaves the ASA.

Reloading IPS Messages

The following messages generated during some IPS signature and global correlation updates for IPS 7.1 and later on the ASA 5500-X IPS SSP can cause confusion since the IPS is not reloading:

```
ASA5585-SSP-IPS20 Module in slot 1, application up "IPS", version "7.1(1)E4" Normal
Operation
ASA5585-SSP-IPS20 Module in slot 1, application reloading "IPS", version "7.1(1)E4" Config
Change
```

These messages are generated during some, but not all, of the global correlation updates that are attempted every five minutes. This is expected behavior. There is a global correlation check every five minutes, but there may not be an update available, thus the message appears every hour or so. When a global correlation update actually takes place, a message is sent from the IPS to the ASA indicating that a configuration change is taking place.

Troubleshooting the ASA 5585-X IPS SSP

Tip Before troubleshooting the ASA 5585-X IPS SSP, check the Caveats section of the Readme for the software version installed on your sensor to see if you are dealing with a known issue.

This section contains troubleshooting information specific to the ASA 5585-X IPS SSP, and contains the following topics:

Failover Scenarios

The following failover scenarios apply to the ASA 5585-X in the event of configuration changes, signature/signature engine updates, service packs, and SensorApp crashes on the ASA 5585-X IPS SSP.

Single ASA 5585-X in Fail-Open Mode

- If the ASA is configured in fail-open mode for the ASA 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a configuration change or signature/signature engine update, traffic is passed through the ASA without being inspected.
- If the ASA is configured in fail-open mode for the ASA 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is passed through the ASA without being inspected.

Single ASA 5585-X in Fail-Close Mode

- If the ASA is configured in fail-close mode for the ASA 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the ASA.
- If the ASA is configured in fail-close mode for the ASA 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is stopped from passing through the ASA.

Two ASA 5585-Xs in Fail-Open Mode

- If the ASAs are configured in fail-open mode and if the ASA 5585-X IPS SSP on the active ASA experiences a configuration change or a signature/signature engine update, traffic is still passed through the active ASA without being inspected. Failover is not triggered.
- If the ASAs are configured in fail-open mode, and if the ASA 5585-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5585-X IPS SSP that was previously the standby ASA 5585-X IPS SSP.

Two ASA 5585-Xs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the ASA 5585-X IPS SSP on the active ASA experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the active ASA. No failover is triggered.
- If the ASAs are configured in fail-close mode, and if the ASA 5585-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5585-X IPS SSP that was previously the standby for the ASA 5585-X IPS SSP.

Configuration Examples

Use the following configuration for the primary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Use the following configuration for the secondary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Traffic Flow Stopped on IPS Switchports

Problem Traffic on any port located on the ASA 5585-X IPS SSP (1/x) no longer passes through the adaptive security appliance when the ASA 5585-X IPS SSP is reset or shut down. This affects all traffic through these ports regardless of whether or not the traffic would have been monitored by the IPS. The link on the ports will link down when the ASA 5585-X IPS SSP is reset or shut down.

Possible Cause Using the ports located on the ASA 5585-X IPS SSP (1/x), and resetting or shutting it down via any mechanism.

Solution Use the ports on the adaptive security appliance (0/x) instead because those ports do not lose their link when the ASA 5585-X IPS SSP is reset or shut down.

Health and Status Information

To see the general health of the ASA 5585-X IPS SSP, use the **show module 1 details** command.

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(1)3
Software version:   7.2.(1)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2.(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
```

```
Mgmt TLS enabled    true
asa
```

The output shows that the ASA 5585-X IPS SSP is up. If the status reads `Down`, you can reset it using the **hw-module module 1 reset** command.

```
asa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2.(1)E4
Data plane Status:  Not Applicable
Status:             Shutting Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2.(1)E4
Data plane Status:  Not Applicable
Status:             Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2.(1)E4
Data plane Status:  Not Applicable
Status:             Init
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
```

```
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Reload
App. Status Desc:   Starting up
App. version:       7.2.(1)E4
Data plane Status:  Down
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2.(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

If you have problems with reimaging the ASA 5585-X IPS SSP, use the **debug module-boot** command to see the output as it boots. Make sure you have the correct IP address for the TFTP server and you have the correct file on the TFTP server. Then use the **hw-module module 1 recover** command again to reimage the module.

```
ips-ssp# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.10.10.10//IPS-SSP_20-K9-sys-1.1-a-7.2.-1-E4.img
Port IP Address [0.0.0.0]: 10.10.10.11
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.10.10.254

asa(config)# debug module-boot
debug module-boot enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered. This may erase all configuration and all data on
that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10
PST 2010
Slot-1 141> Platform ASA5585-SSP-IPS20
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
Slot-1 144> MAC Address: 000b.fcf8.0176
```

```
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=192.0.2.3
Slot-1 147>   SERVER=192.0.2.15
Slot-1 148>   GATEWAY=192.0.2.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSP-K9-sys-1.1-a-7.2.-1.1.img
Slot-1 152>   CONFIG=
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSP_10-K9-sys-1.1-a-7.2.-0.1.img@192.0.2.15 via 192.0.2.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2010
Slot-1 161> Platform ASA5585-SSP-IPS20
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=192.0.2.3
Slot-1 167>   SERVER=192.0.2.15
Slot-1 168>   GATEWAY=192.0.2.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSP_10-K9-sys-1.1-a-7.2.-0.1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSP_10-K9-sys-1.1-a-7.2.-0.1.img@192.0.2.15 via 192.0.2.254
```

The ASA 5585-X IPS SSP and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the ASA 5585-X IPS SSP, because the ASA itself handles the normalization. Packets on the ASA IPS modules go through a special path in the Normalizer that only reassembles fragments and puts packets in the right order for the TCP stream. The Normalizer does not do any of the normalization that is done on an inline IPS appliance, because that causes problems in the way the ASA handles the packets.

The following Normalizer engine signatures are not supported:

- 1300.0
- 1304.0
- 1305.0
- 1307.0
- 1308.0
- 1309.0
- 1311.0
- 1315.0
- 1316.0
- 1317.0
- 1330.0

- 1330.1
- 1330.2
- 1330.9
- 1330.10
- 1330.12
- 1330.14
- 1330.15
- 1330.16
- 1330.17
- 1330.18

The ASA 5585-X IPS SSP and Jumbo Packets

The jumbo packet count in the **show interface** command output from the lines `Total Jumbo Packets Received` and `Total Jumbo Packets Transmitted` for ASA IPS modules may be larger than expected due to some packets that were almost jumbo size on the wire being counted as jumbo size by the IPS. This miscount is a result of header bytes added to the packet by the ASA before the packet is transmitted to the IPS. For IPv4, 58 bytes of header data are added. For IPv6, 78 bytes of header data are added. The ASA removes the added IPS header before the packet leaves the ASA.

Reloading IPS Messages

The following messages generated during some IPS signature and global correlation updates for IPS 7.1 and later on the ASA 5585-X IPS SSP can cause confusion since the IPS is not reloading:

```
ASA5585-SSP-IPS20 Module in slot 1, application up "IPS", version "7.1(1)E4" Normal
Operation
ASA5585-SSP-IPS20 Module in slot 1, application reloading "IPS", version "7.1(1)E4" Config
Change
```

These messages are generated during some, but not all, of the global correlation updates that are attempted every five minutes. This is expected behavior. There is a global correlation check every five minutes, but there may not be an update available, thus the message appears every hour or so. When a global correlation update actually takes place, a message is sent from the IPS to the ASA indicating that a configuration change is taking place.

Gathering Information

This section describes how to gather troubleshooting information about your sensor, and contains the following topics:

Understanding Information Gathering

You can use the following CLI commands and scripts to gather information and diagnose the state of the sensor when problems occur. You can use the **show tech-support** command to gather all the information of the sensor, or you can use the other individual commands listed in this section for specific information.

Health and Network Security Information

Caution When the sensor is first starting, it is normal for certain health metric statuses to be red until the sensor is fully up and running.

Note The ASA 5500-X IPS SSP and the ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

Use the **show health** command in privileged EXEC mode to display the overall health status information of the sensor. The health status categories are rated by red and green with red being critical.

To display the overall health status of the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Show the health and security status of the sensor.

```
sensor# show health
Overall Health Status                                    Red
Health Status for Failed Applications                    Green
Health Status for Signature Updates                      Green
Health Status for License Key Expiration                 Red
Health Status for Running in Bypass Mode                 Green
Health Status for Interfaces Being Down                  Red
Health Status for the Inspection Load                    Green
Health Status for the Time Since Last Event Retrieval    Green
Health Status for the Number of Missed Packets           Green
Health Status for the Memory Usage                       Not Enabled
Health Status for Global Correlation                     Red
Health Status for Network Participation                  Not Enabled

Security Status for Virtual Sensor vs0   Green
sensor#
```

Tech Support Information

This section describes the **show tech-support** command, and contains the following topics:

Understanding the show tech-support Command

Note The /var/log/messages file is now persistent across reboots and the information is displayed in the output of the **show tech-support** command.

The **show tech-support** command captures all status and configuration information on the sensor and includes the current configuration, version information, and cidDump information. The output can be large, over 1 MB. You can transfer the output to a remote system.

To get the same information from IME, choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > System Information**.

Note Always run the **show tech-support** command before contacting TAC.

For More Information

For the procedure for copying the output to a remote system, see Displaying Tech Support Information, page C-77.

Displaying Tech Support Information

Note The **show tech-support** command now displays historical interface data for each interface for the past 72 hours.

Use the **show tech-support** [**page**] [**destination-url** *destination_url*] command to display system information on the screen or have it sent to a specific URL. You can use the information as a troubleshooting tool with the TAC.

The following parameters are optional:

- **page**—Displays the output, one page of information at a time. Press **Enter** to display the next line of output or use the spacebar to display the next page of information.
- **destination-url**—Indicates the information should be formatted as HTML and sent to the destination that follows this command. If you use this keyword, the output is not displayed on the screen.
- *destination_url*—Indicates the information should be formatted as HTML.The URL specifies where the information should be sent. If you do not use this keyword, the information is displayed on the screen.

- You can specify the following destination types:
  - **ftp:**—Destination URL for FTP network server. The syntax for this prefix is:
    `ftp://[[username@location]/relativeDirectory]/filename` or
    `ftp://[[username@location]//absoluteDirectory]/filename`
  - **scp:**—Destination URL for the SCP network server. The syntax for this prefix is:
    `scp://[[username@]location]/relativeDirectory]/filename` or
    `scp://[[username@]location]//absoluteDirectory]/filename`

Varlog Files

The /var/log/messages file has the latest logs. A new softlink called varlog has been created under the /usr/cids/idsRoot/log folder that points to the /var/log/messages file. Old logs are stored in varlog.1 and varlog.2 files. The maximum size of these varlog files is 200 KB. Once they cross the size limit the content is rotated. The content of varlog, varlog.1, and varlog.2 is displayed in the output of the **show tech-support** command.

Displaying Tech Support Information

To display tech support information, follow these steps:

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

Step 2 View the output on the screen. The system information appears on the screen, one page at a time. Press the spacebar to view the next page or press **Ctrl-C** to return to the prompt

```
sensor# show tech-support page
```

Step 3 To send the output (in HTML format) to a file:

a. Enter the following command, followed by a valid destination. The `password:` prompt appears.

```
sensor# show tech-support destination-url destination_url
```

Example

To send the tech support output to the file `/absolute/reports/sensor1Report.html`:

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

b. Enter the password for this user account. The `Generating report:` message is displayed.

Tech Support Command Output

The following is an example of the **show tech-support** command output:

Note This output example shows the first part of the command and lists the information for the interfaces, authentication, and the Analysis Engine.

```
sensor# show tech-support page
System Status Report
This Report was generated on Mon Apr 22 18:31:33 2013.
Output from show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4
```

```
Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0            2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
Licensed, expires:      18-Sep-2013 UTC
Sensor up-time is 9:46.
Using 14389M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.3M out of 376.1M bytes of available disk space (24% usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

  IPS-K9-7.2-1-E4   11:17:07 UTC Thu Jan 10 2013

Recovery Partition Version 1.1 - 7.2(1)E4

Host Certificate Valid from: 17-Apr-2013 to 18-Apr-2015


Output from show interfaces
Interface Statistics
   Total Packets Received = 92475
   Total Bytes Received = 8216738
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
   Interface function = Sensing interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Inline Mode = Paired with interface GigabitEthernet0/1
   Pair Status = Up
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Up
   Admin Enabled Status = Enabled
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Missed Packet Percentage = 0
   Total Packets Received = 90664
   Total Bytes Received = 7789276
   Total Multicast Packets Received = 70475
   Total Broadcast Packets Received = 2190
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 1301
   Total Bytes Transmitted = 298432
```

```
   Total Multicast Packets Transmitted = 1258
   Total Broadcast Packets Transmitted = 16
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description =
--MORE--
```

Version Information

This section describes the **show version** command, and contains the following topics:

- Understanding the show version Command, page C-80
- Displaying Version Information, page C-80

Understanding the show version Command

The **show version** command shows the basic sensor information and can indicate where a failure is occurring. It gives the following information:

- Which applications are running
- Versions of the applications
- Disk and memory usage
- Upgrade history of the applications

Note To get the same information from IME, choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Diagnostics Report**.

Displaying Version Information

Use the **show version** command to display version information for all installed operating system packages, signature packages, and IPS processes running on the system. To view the configuration for the entire system, use the **more current-config** command.

Note The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS version you have installed.

Note For the IPS 4500 series sensors, the **show version** command output contains an extra application called the SwitchApp.

To display the version and configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 View version information.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0        2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
No license present
Sensor up-time is 3 days.
Using 14470M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.1M out of 376.1M bytes of available disk space (24%
 usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

  IPS-K9-7.2-1-E4   11:17:07 UTC Thu Jan 10 2013

Recovery Partition Version 1.1 - 7.2(1)E4

Host Certificate Valid from: 17-Apr-2013 to 18-Apr-2015
sensor#
```

Note If the `--MORE--` prompt is displayed, press the spacebar to see more information or **Ctrl-C** to cancel the output and get back to the CLI prompt.

Step 3 View configuration information.

Note You can use the **more current-config** or **show configuration** commands.

```
sensor# more current-config
! ------------------------------
! Current configuration last modified Fri Apr 19 19:01:05 2013
! ------------------------------
! Version 7.2(1)
! Host:
!     Realm Keys          key1.0
```

```
! Signature Definition:
!     Signature Update    S697.0   2013-02-15
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
inline-interfaces pair0
interface1 GigabitEthernet0/0
interface2 GigabitEthernet0/1
exit
bypass-mode auto
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.106.133.159/23,10.106.132.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
websession-inactivity-timeout 3600
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
```

```
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
logical-interface pair0
exit
exitsensor#
```

Statistics Information

This section describes the **show statistics** command, and contains the following topics:

- Understanding the show statistics Command, page C-83
- Displaying Statistics, page C-84

Understanding the show statistics Command

The **show statistics** command provides a snapshot of the state of the sensor services. The following services provide statistics:

- AnalysisEngine
- Authentication
- Denied Attackers
- Event Server
- Event Store
- Host
- Logger
- Attack Response (formerly known as Network Access)
- Notification
- SDEE Server
- Transaction Server
- Transaction Source
- Virtual Sensor
- Web Server

Note To get the same information from IME, choose **Configuration** > ***sensor_name*** > **Sensor Monitoring** > **Support Information** >**Statistics**.

Displaying Statistics

Use the **show statistics [analysis-engine | anomaly-detection | authentication | denied-attackers | event-server | event-store | external-product-interface | global-correlation | host | logger | network-access | notification | os-identification | sdee-server | transaction-server | virtual-sensor | web-server**] [**clear**] command to display statistics for each sensor application.

Use the **show statistics** {**anomaly-detection | denied-attackers | os-identification | virtual-sensor**} [***name*** **| clear**] command to display statistics for these components for all virtual sensors. If you provide the virtual sensor name, the statistics for that virtual sensor only are displayed.

Note The **clear** option is not available for the analysis engine, anomaly detection, host, network access, or OS identification applications.

For the IPS 4510 and IPS 4520, at the end of the command output, there are extra details for the Ethernet controller statistics, such as the total number of packets received at the Ethernet controller, the total number of packets dropped at the Ethernet controller under high load conditions, and the total packets transmitted including the customer traffic packets and the internal keepalive packet count.

Note The Ethernet controller statistics are polled at an interval of 5 seconds from the hardware side. The keepalives are sent or updated at an interval of 10 ms. Because of this, there may be a disparity in the actual count reflected in the total packets transmitted. At times, it is even possible that the total packets transmitted may be less that the keepalive packets transmitted.

To display statistics for the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the statistics for the Analysis Engine.

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 431157
   Processing Load Percentage
         Thread    5 sec   1 min   5 min
         0         1       1       1
         1         1       1       1
         2         1       1       1
         3         1       1       1
         4         1       1       1
         5         1       1       1
         6         1       1       1
         Average   1       1       1

   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics
      Total number of packets processed since reset = 0
      Total number of IP packets processed since reset = 0
   Transmitter Statistics
      Total number of packets transmitted = 133698
      Total number of packets denied = 203
      Total number of packets reset = 3
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
```

```
TCP Stream Reassembly Unit Statistics
   TCP streams currently in the embryonic state = 0
   TCP streams currently in the established state = 0
   TCP streams currently in the closing state = 0
   TCP streams currently in the system = 0
   TCP Packets currently queued for reassembly = 0
The Signature Database Statistics.
   Total nodes active = 0
   TCP nodes keyed on both IP addresses and both ports = 0
   UDP nodes keyed on both IP addresses and both ports = 0
   IP nodes keyed on both IP addresses = 0
Statistics for Signature Events
   Number of SigEvents since reset = 0
Statistics for Actions executed on a SigEvent
   Number of Alerts written to the IdsEventStore = 0
Inspection Stats
      Inspector            active   call   create   delete   loadPct
      AtomicAdvanced       0        2312   4        4        33
      Fixed                0        1659   1606     1606     1
      MSRPC_TCP            0        20     4        4        0
      MSRPC_UDP            0        1808   1575     1575     0
      MultiString          0        145    10       10       2
      ServiceDnsUdp        0        1841   3        3        0
      ServiceGeneric       0        2016   14       14       1
      ServiceHttp          0        2      2        2        51
      ServiceNtp           0        3682   3176     3176     0
      ServiceP2PTCP        0        21     9        9        0
      ServiceRpcUDP        0        1841   3        3        0
      ServiceRpcTCP        0        130    9        9        0
      ServiceSMBAdvanced   0        139    3        3        0
      ServiceSnmp          0        1841   3        3        0
      ServiceTNS           0        18     14       14       0
      String               0        225    16       16       0
      SweepUDP             0        1808   1555     1555     6
      SweepTCP             0        576    17       17       0
      SweepOtherTcp        0        288    6        6        0
      TrojanBO2K           0        261    11       11       0
      TrojanUdp            0        1808   1555     1555     0

GlobalCorrelationStats
   SwVersion = 7.1(4.70)E4
   SigVersion = 645.0
   DatabaseRecordCount = 0
   DatabaseVersion = 0
   RuleVersion = 0
   ReputationFilterVersion = 0
   AlertsWithHit = 0
   AlertsWithMiss = 0
   AlertsWithModifiedRiskRating = 0
   AlertsWithGlobalCorrelationDenyAttacker = 0
   AlertsWithGlobalCorrelationDenyPacket = 0
   AlertsWithGlobalCorrelationOtherAction = 0
   AlertsWithAuditRepDenies = 0
   ReputationForcedAlerts = 0
   EventStoreInsertTotal = 0
   EventStoreInsertWithHit = 0
   EventStoreInsertWithMiss = 0
   EventStoreDenyFromGlobalCorrelation = 0
   EventStoreDenyFromOverride = 0
   EventStoreDenyFromOverlap = 0
   EventStoreDenyFromOther = 0
   ReputationFilterDataSize = 0
   ReputationFilterPacketsInput = 0
   ReputationFilterRuleMatch = 0
```

```
      DenyFilterHitsNormal = 0
      DenyFilterHitsGlobalCorrelation = 0
      SimulatedReputationFilterPacketsInput = 0
      SimulatedReputationFilterRuleMatch = 0
      SimulatedDenyFilterInsert = 0
      SimulatedDenyFilterPacketsInput = 0
      SimulatedDenyFilterRuleMatch = 0
      TcpDeniesDueToGlobalCorrelation = 0
      TcpDeniesDueToOverride = 0
      TcpDeniesDueToOverlap = 0
      TcpDeniesDueToOther = 0
      SimulatedTcpDeniesDueToGlobalCorrelation = 0
      SimulatedTcpDeniesDueToOverride = 0
      SimulatedTcpDeniesDueToOverlap = 0
      SimulatedTcpDeniesDueToOther = 0
      LateStageDenyDueToGlobalCorrelation = 0
      LateStageDenyDueToOverride = 0
      LateStageDenyDueToOverlap = 0
      LateStageDenyDueToOther = 0
      SimulatedLateStageDenyDueToGlobalCorrelation = 0
      SimulatedLateStageDenyDueToOverride = 0
      SimulatedLateStageDenyDueToOverlap = 0
      SimulatedLateStageDenyDueToOther = 0
      AlertHistogram
      RiskHistogramEarlyStage
      RiskHistogramLateStage
      ConfigAggressiveMode = 0
      ConfigAuditMode = 0
   RegexAccelerationStats
      Status = Enabled
      DriverVersion = 6.2.1
      Devices = 1
      Agents = 12
      Flows = 7
      Channels = 0
      SubmittedJobs = 4968
      CompletedJobs = 4968
      SubmittedBytes = 72258005
      CompletedBytes = 168
      TCPFlowsWithoutLCB = 0
      UDPFlowsWithoutLCB = 0
      TCPMissedPacketsDueToUpdate = 0
      UDPMissedPacketsDueToUpdate = 0
      MemorySize = 1073741824
      HostDirectMemSize = 0
   MaliciousSiteDenyHitCounts
   MaliciousSiteDenyHitCountsAUDIT
Ethernet Controller Statistics
   Total Packets Received = 0
   Total Received Packets Dropped = 0
   Total Packets Transmitted = 13643"
sensor#
```

Step 3 Display the statistics for anomaly detection.

```
sensor# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
```

```
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
sensor#
```

Step 4 Display the statistics for authentication.

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 128
   failedAuthenticationAttempts = 0
sensor#
```

Step 5 Display the statistics for the denied attackers in the system.

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


sensor#
```

Step 6 Display the statistics for the Event Server.

```
sensor# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
sensor#
```

Step 7 Display the statistics for the Event Store.

```
sensor# show statistics event-store
EEvent store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of filtered events not written to the event store = 850763
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Status events = 4257
      Shun request events = 0
      Error events, warning = 669
      Error events, error = 8
      Error events, fatal = 0
      Alert events, informational = 0
      Alert events, low = 0
      Alert events, medium = 0
      Alert events, high = 0
      Alert events, threat rating 0-20 = 0
      Alert events, threat rating 21-40 = 0
      Alert events, threat rating 41-60 = 0
      Alert events, threat rating 61-80 = 0
      Alert events, threat rating 81-100 = 0
   Cumulative number of each type of event
      Status events = 4257
      Shun request events = 0
      Error events, warning = 669
      Error events, error = 8
      Error events, fatal = 0
      Alert events, informational = 0
      Alert events, low = 0
      Alert events, medium = 0
      Alert events, high = 0
      Alert events, threat rating 0-20 = 0
      Alert events, threat rating 21-40 = 0
      Alert events, threat rating 41-60 = 0
      Alert events, threat rating 61-80 = 0
      Alert events, threat rating 81-100 = 0
sensor#
```

Step 8 Display the statistics for global correlation.

```
sensor# show statistics global-correlation
Network Participation:
   Counters:
      Total Connection Attempts = 0
      Total Connection Failures = 0
      Connection Failures Since Last Success = 0
   Connection History:
Updates:
   Status Of Last Update Attempt = Disabled
   Time Since Last Successful Update = never
   Counters:
      Update Failures Since Last Success = 0
      Total Update Attempts = 0
      Total Update Failures = 0
   Update Interval In Seconds = 300
   Update Server = update-manifests.ironport.com
   Update Server Address = Unknown
   Current Versions:
Warnings:
```

```
   Unlicensed = Global correlation inspection and reputation filtering have been
 disabled because the sensor is unlicensed.
   Action Required = Obtain a new license from http://www.cisco.com/go/license.
sensor#
```

Step 9 Display the statistics for the host.

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 25-Jan-2012 02:59:18
   Command Control Port Device = Management0/0
Network Statistics
    = ma0_0     Link encap:Ethernet  HWaddr 00:04:23:D5:A1:8D
    =           inet addr:10.89.130.98  Bcast:10.89.131.255  Mask:255.255.254.0
    =           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    =           RX packets:1688325 errors:0 dropped:0 overruns:0 frame:0
    =           TX packets:38546 errors:0 dropped:0 overruns:0 carrier:0
    =           collisions:0 txqueuelen:1000
    =           RX bytes:133194316 (127.0 MiB)  TX bytes:5515034 (5.2 MiB)
    =           Base address:0xcc80 Memory:fcee0000-fcf00000
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 1889357824
   freeBytes = 2210988032
   totalBytes = 4100345856
CPU Statistics
   Note: CPU Usage statistics are not a good indication of the sensor processin load. The
Inspection Load Percentage in the output of 'show inspection-load' should be used instead.
   Usage over last 5 seconds = 0
   Usage over last minute = 2
   Usage over last 5 minutes = 2
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 1889357824
   Memory free (bytes) = 2210988032
Auto Update Statistics
   lastDirectoryReadAttempt = N/A
   lastDownloadAttempt = N/A
   lastInstallAttempt = N/A
   nextAttempt = N/A
Auxilliary Processors Installed
sensor#
```

Step 10 Display the statistics for the logging application.

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
```

```
sensor#
```

Step 11 Display the statistics for the ARC.

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.4
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.5
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 192.0.2.6
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
      Type = CAT6000_VACL
      IP = 192.0.2.1
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = 502
         InterfacePreBlock = Pre_Acl_Test
      BlockInterface
         InterfaceName = 507
         InterfacePostBlock = Post_Acl_Test
State
   BlockEnable = true
   NetDevice
      IP = 192.0.2.3
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 192.0.2.7
      AclSupport = Does not use ACLs
      Version = 7.0
```

```
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 102.0.2.8
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 192.0.2.9
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 192.0.2.10
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 203.0.113.1
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.2
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 203.0.113.9
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

Step 12 Display the statistics for the notification application.

```
sensor# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
sensor#
```

Step 13 Display the statistics for OS identification.

```
sensor# show statistics os-identification
Statistics for Virtual Sensor vs0
   OS Identification
      Configured
      Imported
      Learned
sensor#
```

Step 14 Display the statistics for the SDEE server.

```
sensor# show statistics sdee-server
General
```

```
   Open Subscriptions = 1
   Blocked Subscriptions = 1
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
   sub-4-d074914f
      State = Read Pending
      Last Read Time = 23:54:16 UTC Wed Nov 30 2011
      Last Read Time (nanoseconds) = 1322697256078549000
sensor#
```

Step 15 Display the statistics for the transaction server.

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
sensor#
```

Step 16 Display the statistics for a virtual sensor.

```
sensor# show statistics virtual-sensor vs0
Statistics for Virtual Sensor vs0
      Name of current Signature-Defintion instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1151770
         MemoryAlloPercent = 23
         MemoryUsedPercent = 22
         MemoryMaxCapacity = 3500000
         MemoryMaxHighUsed = 4193330
         MemoryCurrentAllo = 805452
         MemoryCurrentUsed = 789047
         Processing Load Percentage = 1
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total IPv4 packets processed since reset = 0
         Total IPv6 packets processed since reset = 0
         Total IPv6 AH packets processed since reset = 0
         Total IPv6 ESP packets processed since reset = 0
         Total IPv6 Fragment packets processed since reset = 0
         Total IPv6 Routing Header packets processed since reset = 0
         Total IPv6 ICMP packets processed since reset = 0
         Total packets that were not IP processed since reset = 0
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 0
         Total packets that were not TCP, UDP, or ICMP processed since reset = 0
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total GRE Packets processed since reset = 0
         Total GRE Fragment Packets processed since reset = 0
         Total GRE Packets skipped since reset = 0
         Total GRE Packets with Bad Header skipped since reset = 0
         Total IpIp Packets with Bad Header skipped since reset = 0
         Total Encapsulated Tunnel Packets with Bad Header skipped since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total cross queue TCP packets processed since reset = 0
         Total cross queue UDP packets processed since reset = 0
         Packets dropped due to regex resources unavailable since reset = 0
         Total number of bytes processed since reset = 0
```

```
   The rate of packets per second since reset = 0
   The rate of bytes per second since reset = 0
   The average bytes per packet since reset = 0
Denied Address Information
   Number of Active Denied Attackers = 0
   Number of Denied Attackers Inserted = 0
   Number of Denied Attacker Victim Pairs Inserted = 0
   Number of Denied Attacker Service Pairs Inserted = 0
   Number of Denied Attackers Total Hits = 0
   Number of times max-denied-attackers limited creation of new entry = 0
   Number of exec Clear commands during uptime = 0
Denied Attackers and hit count for each.
Denied Attackers with percent denied and hit count for each.


The Signature Database Statistics.
   The Number of each type of node active in the system
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The number of each type of node inserted since reset
      Total nodes inserted = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The rate of nodes per second for each time since reset
      Nodes per second = 0
      TCP nodes keyed on both IP addresses and both ports per second = 0
      UDP nodes keyed on both IP addresses and both ports per second = 0
      IP nodes keyed on both IP addresses per second = 0
   The number of root nodes forced to expire because of memory constraints
      TCP nodes keyed on both IP addresses and both ports = 0
   Packets dropped because they would exceed Database insertion rate limits = 0
Fragment Reassembly Unit Statistics for this Virtual Sensor
   Number of fragments currently in FRU = 0
   Number of datagrams currently in FRU = 0
   Number of fragments received since reset = 0
   Number of fragments forwarded since reset = 0
   Number of fragments dropped since last reset = 0
   Number of fragments modified since last reset = 0
   Number of complete datagrams reassembled since last reset = 0
   Fragments hitting too many fragments condition since last reset = 0
   Number of overlapping fragments since last reset = 0
   Number of Datagrams too big since last reset = 0
   Number of overwriting fragments since last reset = 0
   Number of Inital fragment missing since last reset = 0
   Fragments hitting the max partial dgrams limit since last reset = 0
   Fragments too small since last reset = 0
   Too many fragments per dgram limit since last reset = 0
   Number of datagram reassembly timeout since last reset = 0
   Too many fragments claiming to be the last since last reset = 0
   Fragments with bad fragment flags since last reset = 0
TCP Normalizer stage statistics
   Packets Input = 0
   Packets Modified = 0
   Dropped packets from queue = 0
   Dropped packets due to deny-connection = 0
   Duplicate Packets = 0
   Current Streams = 0
   Current Streams Closed = 0
   Current Streams Closing = 0
   Current Streams Embryonic = 0
   Current Streams Established = 0
```

```
            Current Streams Denied = 0
            Total SendAck Limited Packets = 0
            Total SendAck Limited Streams = 0
            Total SendAck Packets Sent = 0
         Statistics for the TCP Stream Reassembly Unit
            Current Statistics for the TCP Stream Reassembly Unit
               TCP streams currently in the embryonic state = 0
               TCP streams currently in the established state = 0
               TCP streams currently in the closing state = 0
               TCP streams currently in the system = 0
               TCP Packets currently queued for reassembly = 0
            Cumulative Statistics for the TCP Stream Reassembly Unit since reset
               TCP streams that have been tracked since last reset = 0
               TCP streams that had a gap in the sequence jumped = 0
               TCP streams that was abandoned due to a gap in the sequence = 0
               TCP packets that arrived out of sequence order for their stream = 0
               TCP packets that arrived out of state order for their stream = 0
               The rate of TCP connections tracked per second since reset = 0
         SigEvent Preliminary Stage Statistics
            Number of Alerts received = 0
            Number of Alerts Consumed by AlertInterval = 0
            Number of Alerts Consumed by Event Count = 0
            Number of FireOnce First Alerts = 0
            Number of FireOnce Intermediate Alerts = 0
            Number of Summary First Alerts  = 0
            Number of Summary Intermediate Alerts  = 0
            Number of Regular Summary Final Alerts  = 0
            Number of Global Summary Final Alerts  = 0
            Number of Active SigEventDataNodes  = 0
            Number of Alerts Output for further processing = 0
--MORE--
```

Step 17 Display the statistics for the web server.

```
sensor# show statistics web-server
listener-443
   session-11
      remote host = 64.101.182.167
      session is persistent = no
      number of requests serviced on current connection = 1
      last status code = 200
      last request method = GET
      last request URI = cgi-bin/sdee-server
      last protocol version = HTTP/1.1
      session state = processingGetServlet
   number of server session requests handled = 957134
   number of server session requests rejected = 0
   total HTTP requests handled = 365871
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 12
   number of busy allocated session objects = 1
summarized log messages
   number of TCP socket failure messages logged = 0
   number of TLS socket failure messages logged = 0
   number of TLS protocol failure messages logged = 0
   number of TLS connection failure messages logged = 595015
   number of TLS crypto warning messages logged = 0
   number of TLS expired certificate warning messages logged = 0
   number of receipt of TLS fatal alert message messages logged = 594969
crypto library version = 6.2.1.0
sensor#
```

Step 18 Clear the statistics for an application, for example, the logging application. The statistics are retrieved and cleared.

```
sensor# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

Step 19 Verify that the statistics have been cleared. The statistics now all begin from 0.

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 0
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   TOTAL = 0
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 0
   TOTAL = 0
sensor#
```

Interfaces Information

This section describes the **show interfaces** command, and contains the following topics:

- Understanding the show interfaces Command, page C-95
- Interfaces Command Output, page C-96

Understanding the show interfaces Command

The **show interfaces** command is useful for gathering information on the sensing and command and control interfaces. You can learn the following information from the **show interfaces** command:

- Whether the interface is up or down
- Whether or not packets are being seen, and on which interfaces

- Whether or not packets are being dropped by SensorApp
- Whether or not there are errors being reported by the interfaces that can result in packet drops

The **show interfaces** command displays statistics for all system interfaces. Or you can use the individual commands to display statistics for the command and control interface (**show interfaces** *command_control_interface_name*), the sensing interface (**show interfaces** *interface_name*).

Interfaces Command Output

The following example shows the output from the **show interfaces** command:

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2211296
   Total Bytes Received = 157577635
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239723
   Total Bytes Transmitted = 107213390
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Events Information

This section describes the **show events** command, and contains the following topics:

Sensor Events

You can use the **show events** command to view the alerts generated by SensorApp and errors generated by an application. There are five types of events:

- evAlert—Intrusion detection alerts
- evError—Application errors
- evStatus—Status changes, such as an IP log being created
- evLogTransaction—Record of control transactions processed by each sensor application
- evShunRqst—Block requests

Events remain in the Event Store until they are overwritten by newer events.

Understanding the show events Command

The **show events** command is useful for troubleshooting event capture issues in which you are not seeing events in Event Viewer or Security Monitor. You can use the **show events** command to determine which events are being generated on the sensor to make sure events are being generated and that the fault lies with the monitoring side.

You can clear all events from Event Store by using the **clear events** command.

Here are the parameters for the **show events** command:

```
sensor# show events
<cr>
alert          Display local system alerts.
error          Display error events.
hh:mm[:ss]     Display start time.
log            Display log events.
nac            Display NAC shun events.
past           Display events starting in the past specified time.
status         Display status events.
|              Output modifiers.
```

Displaying Events

Note The Event Store has a fixed size of 30 MB for all platforms.

Note Events are displayed as a live feed. To cancel the request, press **Ctrl-C.**

Use the **show events** [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] command to display events from Event Store. Events are displayed beginning at the start time. If you do not specify a start time, events are displayed beginning at the current time. If you do not specify an event type, all events are displayed.

The following options apply:

- **alert**—Displays alerts. Provides notification of some suspicious activity that may indicate an attack is in process or has been attempted. Alert events are generated by the Analysis Engine whenever a signature is triggered by network activity. If no level is selected (informational, low, medium, or high), all alert events are displayed.
- **include-traits**—Displays alerts that have the specified traits.
- **exclude-traits**—Does not display alerts that have the specified traits.
- **traits**—Specifies the trait bit position in decimal (0 to 15).
- **min-threat-rating**—Displays events with a threat rating above or equal to this value. The default is 0. The valid range is 0 to 100.
- **max-threat-rating**—Displays events with a threat rating below or equal to this value. The default is 100. The valid range is 0 to 100.
- **error**—Displays error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.
- **NAC**—Displays the ARC (block) requests.

  Note The ARC is formerly known as NAC. This name change has not been completely implemented throughout the IDM, the IME, and the CLI .

- **status**—Displays status events.
- **past**—Displays events starting in the past for the specified hours, minutes, and seconds.
- *hh:mm:ss*—Specifies the hours, minutes, and seconds in the past to begin the display.

Note The **show events** command continues to display events until a specified event is available. To exit, press **Ctrl-C**.

Displaying Events

To display events from the Event Store, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display all events starting now. The feed continues showing all events until you press **Ctrl-C**.

```
sensor# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

```
evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

Step 3 Display the block requests beginning at 10:00 a.m. on February 9, 2011.

```
sensor# show events NAC 10:00:00 Feb 9 2011
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2011/02/09 10:33:31 2011/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

Step 4 Display errors with the warning level starting at 10:00 a.m. on February 9, 2011.

```
sensor# show events error warning 10:00:00 Feb 9 2011
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2011/01/07 04:49:25 2011/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

Step 5 Display alerts from the past 45 seconds.

```
sensor# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2011/03/02 14:15:59 2011/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp
```

```
evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

Step 6 Display events that began 30 seconds in the past.

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

Clearing Events

Use the **clear events** command to clear the Event Store.

To clear events from the Event Store, follow these steps:

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

Step 2 Clear the Event Store.

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

Step 3 Enter **yes** to clear the events.

cidDump Script

If you do not have access to the IDM, the IME, or the CLI, you can run the underlying script cidDump from the service account by logging in as root and running /usr/cids/idsRoot/bin/cidDump. The path of the cidDump file is /usr/cids/idsRoot/htdocs/private/cidDump.html. cidDump is a script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.

To run the cidDump script, follow these steps:

Step 1 Log in to the sensor service account.

Step 2 `Su` to `root` using the service account password.

Step 3 Enter the following command.

```
/usr/cids/idsRoot/bin/cidDump
```

Step 4 Enter the following command to compress the resulting /usr/cids/idsRoot/log/cidDump.html file.

```
gzip /usr/cids/idsRoot/log/cidDump.html
```

Step 5 Send the resulting HTML file to TAC or the IPS developers in case of a problem.

For More Information

For the procedure for putting a file on the Cisco FTP site, see Uploading and Accessing Files on the Cisco FTP Site, page C-101.

Uploading and Accessing Files on the Cisco FTP Site

You can upload large files, for example, cidDump.html, the **show tech-support** command output, and cores, to the ftp-sj server.

To upload and access files on the Cisco FTP site, follow these steps:

Step 1 Log in to ftp-sj.cisco.com as anonymous.

Step 2 Change to the /incoming directory.

Step 3 Use the **put** command to upload the files. Make sure to use the binary transfer type.

Step 4 To access uploaded files, log in to an ECS-supported host.

Step 5 Change to the /auto/ftp/incoming directory.

Revised: February 18, 2014

Numerals

3DES Triple Data Encryption Standard. A stronger version of DES, which is the default encryption method for SSH version 1.5. Used when establishing an SSH session with the sensor. It can be used when the sensor is managing a device.

802.x A set of IEEE standards for the definition of LAN protocols.

A

AAA authentication, authorization, and accounting. Pronounced “triple a.” The primary and recommended method for access control in Cisco devices.

ACE Access Control Entry. An entry in the ACL that describes what action should be taken for a specified address or protocol. The sensor adds/removes ACE to block hosts.

ACK acknowledgment. Notification sent from one network device to another to acknowledge that some event occurred (for example, the receipt of a message).

ACL Access Control List. A list of ACEs that control the flow of data through a router. There are two ACLs per router interface for inbound data and outbound data. Only one ACL per direction can be active at a time. ACLs are identified by number or by name. ACLs can be standard, enhanced, or extended. You can configure the sensor to manage ACLs.

ACS server Cisco Access Control Server. A RADIUS security server that is the centralized control point for managing network users, network administrators, and network infrastructure resources.

action The response of the sensor to an event. An action only happens if the event is not filtered. Examples include TCP reset, block host, block connection, IP logging, and capturing the alert trigger packet.

active ACL The ACL created and maintained by ARC and applied to the router block interfaces.

adaptive security appliance ASA. Combines firewall, VPN concentrator, and intrusion prevention software functionality into one software image. You can configure the adaptive security appliance in single mode or multi-mode.

AIC engine Application Inspection and Control engine. Provides deep analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications that try to tunnel over specified ports, such as instant messaging, and tunneling applications, such as gotomypc. It can also inspect FTP traffic and control the commands being issued.

ASA 5500-X IPS SSP Intrusion Prevention System Security Services Processor. The IPS is running as a service and ASA controls sending and receiving traffic to and from the IPS. The IPS services processor monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the ASA 5500-X IPS SSP detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager. See also adaptive security appliance.

ASA 5585-X IPS SSP Intrusion Prevention System Security Services Processor. The IPS plug-in module in the Cisco ASA 5585-X adaptive security appliance. The ASA 5585-X IPS SSP is an IPS services processor that monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the ASA 5585-X IPS SSP detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager. See also adaptive security appliance.

Alarm Channel The IPS software module that processes all signature events generated by the inspectors. Its primary function is to generate alerts for each event it receives.

alert Specifically, an IPS event type; it is written to the Event Store as an evidsAlert. In general, an alert is an IPS message that indicates a network exploit in progress or a potential security problem occurrence. Also known as an alarm.

Analysis Engine The IPS software module that handles sensor configuration. It maps the interfaces and also the signature and alarm channel policy to the configured interfaces. It performs packet analysis and alert detection. The Analysis Engine functionality is provided by the SensorApp process.

anomaly detection AD. The sensor component that creates a baseline of normal network traffic and then uses this baseline to detect worm-infected hosts.

API Application Programming Interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. Computer application programs run a set of standard software interrupts, calls, and data formats to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create links that an application needs to communicate with the operating system or with the network.

application Any program (process) designed to run in the Cisco IPS environment.

application image Full IPS image stored on a permanent storage device used for operating the sensor.

application instance A specific application running on a specific piece of hardware in the IPS environment. An application instance is addressable by its name and the IP address of its host computer.

application partition The bootable disk or compact-flash partition that contains the IPS software image.

ARC Attack Response Controller. Formerly known as Network Access Controller (NAC). A component of the IPS. A software module that provides block and unblock functionality where applicable.

architecture The overall structure of a computer or communication system. The architecture influences the capabilities and limitations of the system.

ARP Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.

ASDM Adaptive Security Device Manager. A web-based application that lets you configure and manage your adaptive security device.

ASN.1 Abstract Syntax Notation 1. Standard for data presentation.

aspect version Version information associated with a group of IDIOM default configuration settings. For example, Cisco Systems publishes the standard set of attack signatures as a collection of default settings with the S aspect. The S-aspect version number is displayed after the S in the signature update package file name. Other aspects include the Virus signature definitions in the V-aspect and IDIOM signing keys in the key-aspect.

atomic attack Represents exploits contained within a single packet. For example, the "ping of death" attack is a single, abnormally large ICMP packet.

Atomic engine There are two Atomic engines: Atomic IP inspects IP protocol packets and associated Layer-4 transport protocols, and Atomic ARP inspects Layer-2 ARP protocol.

attack An assault on system security that derives from an intelligent threat, that is, an intelligent act that is a deliberate attempt (especially in the sense of method or technique) to evade security services and violate the security policy of a system.

attack relevance rating ARR. A weight associated with the relevancy of the targeted OS. The attack relevance rating is a derived value (relevant, unknown, or not relevant), which is determined at alert time. The relevant OSes are configured per signature.

attack severity rating ASR. A weight associated with the severity of a successful exploit of the vulnerability. The attack severity rating is derived from the alert severity parameter (informational, low, medium, or high) of the signature. The attack severity rating is configured per signature and indicates how dangerous the event detected is.

authentication Process of verifying that a user has permission to use the system, usually by means of a password key or certificate.

AuthenticationApp A component of the IPS. Authorizes and authenticates users based on IP address, password, and digital certificates.

autostate In normal autostate mode, the Layer 3 interfaces remain up if at least one port in the VLAN remains up. If you have appliances, such as load balancers or firewall servers that are connected to the ports in the VLAN, you can configure these ports to be excluded from the autostate feature to make sure that the forwarding SVI does not go down if these ports become inactive.

AV Anti-Virus.

B

backplane The physical connection between an interface processor or card and the data buses and the power distribution buses inside a chassis.

base version A software release that must be installed before a follow-up release, such as a service pack or signature update, can be installed. Major and minor updates are base version releases.

benign trigger A situation in which a signature is fired correctly, but the source of the traffic is nonmalicious.

BIOS Basic Input/Output System. The program that starts the sensor and communicates between the devices in the sensor and the system.

blackhole Routing term for an area of the internetwork where packets enter, but do not emerge, due to adverse conditions or poor system configuration within a portion of the network.

block The ability of the sensor to direct a network device to deny entry to all packets from a specified network host or network.

block interface The interface on the network device that the sensor manages.

BO BackOrifice. The original Windows back door Trojan that ran over UDP only.

BO2K BackOrifice 2000. A Windows back door Trojan that runs over TCP and UDP.

bootloader A small set of system software that runs when the system first powers up. It loads the operating system (from the disk, network, external compact flash, or external USB flash), which loads and runs the IPS application. For the AIM IPS, it boots the module from the network and assists in software installation and upgrades, disaster recovery, and other operations when the module cannot access its software.

Botnets A collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software. The term Botnet is used to refer to a collection of compromised computers (called Zombie computers) running software, usually installed through worms, Trojan horses, or back doors, under a common command-and-control infrastructure.

Bpdu Bridge Protocol Data Unit. Spanning-Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.

bypass mode Mode that lets packets continue to flow through the sensor even if the sensor fails. Bypass mode is only applicable to inline-paired interfaces.

C

CA certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. Sensors use self-signed certificates.

CA certificate Certificate for one CA issued by another CA.

CEF Cisco Express Forwarding. CEF is advanced, Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.

certificate Digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

cidDump A script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.

CIDEE Cisco Intrusion Detection Event Exchange. Specifies the extensions to SDEE that are used by Cisco IPS systems. The CIDEE standard specifies all possible extensions that may be supported by Cisco IPS systems.

CIDS header The header that is attached to each packet in the IPS system. It contains packet classification, packet length, checksum results, timestamp, and the receive interface.

cipher key The secret binary data used to convert between clear text and cipher text. When the same cipher key is used for both encryption and decryption, it is called symmetric. When it is used for either encryption or decryption (but not both), it is called asymmetric.

Cisco IOS Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of Internet works while supporting a wide variety of protocols, media, services, and platforms.

CLI command-line interface. A shell provided with the sensor used for configuring and controlling the sensor applications.

CollaborationApp A component of the IPS. Shares information with other devices through a global correlation database to improve the combined efficacy of all the devices.

command and control interface The interface on the sensor that communicates with the IPS manager and other network devices. This interface has an assigned IP address.

community In SNMP, a logical group of managed devices and NMSs in the same administrative domain.

composite attack Spans multiple packets in a single session. Examples include most conversation attacks such as FTP, Telnet, and most Regex-based attacks.

connection block ARC blocks traffic from a given source IP address to a given destination IP address and destination port.

console A terminal or laptop computer used to monitor and control the sensor.

console port An RJ45 or DB9 serial port on the sensor that is used to connect to a console device.

control interface When ARC opens a Telnet or SSH session with a network device, it uses one of the routing interfaces of the device as the remote IP address. This is the control interface.

control transaction CT. An IPS message containing a command addressed to a specific application instance. Control transactions can be sent between a management application and an IPS sensor, or between applications on the same IPS sensor. Example control transactions include *start*, *stop*, *getConfig*.

Control Transaction Server A component of the IPS. Accepts control transactions from a remote client, initiates a local control transaction, and returns the response to the remote client.

Control Transaction Source A component of the IPS. Waits for control transactions directed to remote applications, forwards the control transactions to the remote node, and returns the response to the initiator.

cookie A piece of information sent by a web server to a web browser that the browser is expected to save and send back to the web server whenever the browser makes additional requests of the web server.

CSM Cisco Security Manager, the provisioning component of the Cisco Self-Defending Networks solution. CS-Manager is fully integrated with CS-MARS.

cut-through architecture Cut-through architecture is one method of design for packet-switching systems. When a packet arrives at a switch, the switch starts forwarding the packet almost immediately, reading only the first few bytes in the packet to learn the destination address. This technique improves performance

CVE Common Vulnerabilities and Exposures. A list of standardized names for vulnerabilities and other information security exposures maintained at http://cve.mitre.org/.

D

darknets A virtual private network where users connect only to people they trust. In its most general meaning, a darknet can be any type of closed, private group of people communicating, but the name is most often used specifically for file-sharing networks. Darknet can be used to refer collectively to all covert communication networks.

Database Processor A processor in the IPS. Maintains the signature state and flow databases.

datagram Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms cell, frame, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

DCE data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.

DCOM Distributed Component Object Model. Protocol that enables software components to communicate directly over a network. Developed by Microsoft and previously called Network OLE, DCOM is designed for use across multiple network transports, including such Internet protocols as HTTP.

DDoS Distributed Denial of Service. An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Deny Filters Processor A processor in the IPS. Handles the deny attacker functions. It maintains a list of denied source IP addresses.

DES Data Encryption Standard. A strong encryption method where the strength lies in a 56-bit key rather than an algorithm.

destination address Address of a network device that is receiving data.

DIMM Dual In-line Memory Modules.

DMZ demilitarized zone. A separate network located in the neutral zone between a private (inside) network and a public (outside) network.

DNS Domain Name System. An Internet-wide hostname to IP address mapping. DNS enables you to convert human-readable names into the IP addresses needed for network packets.

DoS Denial of Service. An attack whose goal is just to disrupt the operation of a specific system or network.

DRAM dynamic random-access memory. RAM that stores information in capacitors that must be refreshed periodically. Delays can occur because DRAMs are inaccessible to the processor when refreshing their contents. However, DRAMs are less complex and have greater capacity than SRAMs.

DTE Data Terminal Equipment. Refers to the role of a device on an RS-232C connection. A DTE writes data to the transmit line and reads data from the receive line.

DTP Dynamic Trunking Protocol. A Cisco proprietary protocol in the VLAN group used for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (ISL or 802.1q) to be used.

E

ECLB Ether Channel Load Balancing. Lets a Catalyst switch split traffic flows over different physical paths.

egress Traffic leaving the network.

encryption Application of a specific algorithm to data to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information.

engine A component of the sensor designed to support many signatures in a certain category. Each engine has parameters that can be used to create signatures or tune existing signatures.

enterprise network Large and diverse network connecting most major points in a company or other organization. Differs from a WAN in that it is privately owned and maintained.

escaped expression Used in regular expression. A character can be represented as its hexadecimal value, for example, \x61 equals ‘a,’ so \x61 is an escaped expression representing the character ‘a.’

ESD electrostatic discharge. Electrostatic discharge is the rapid movement of a charge from one object to another object, which produces several thousand volts of electrical charge that can cause severe damage to electronic components or entire circuit card assemblies.

event An IPS message that contains an alert, a block request, a status message, or an error message.

Event Store One of the components of the IPS. A fixed-size, indexed store used to store IPS events.

evIdsAlert The XML entity written to the Event Store that represents an alert.

F

fail closed Blocks traffic on the device after a hardware failure.

fail open Lets traffic pass through the device after a hardware failure.

false negative A signature is not fired when offending traffic is detected.

false positive Normal traffic or a benign action causes a signature to fire.

Fast Ethernet Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase 10 times that of the 10BaseT Ethernet specification while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification.

Fast flux Fast flux is a DNS technique used by Botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. It can also refer to the combination of peer-to-peer networking, distributed command and control, web-based load balancing and proxy redirection used to make malware networks more resistant to discovery and counter-measures. The Storm Worm is one of the recent malware variants to make use of this technique.

firewall Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

Flood engine Detects ICMP and UDP floods directed at hosts and networks.

flooding Traffic passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.

forwarding Process of sending a frame toward its ultimate destination by way of an internetworking device.

fragment Piece of a larger packet that has been broken down to smaller units.

fragmentation Process of breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Fragment Reassembly Processor A processor in the IPS. Reassembles fragmented IP datagrams. It is also responsible for normalization of IP fragments when the sensor is in inline mode.

FTP File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

FTP server File Transfer Protocol server. A server that uses the FTP protocol for transferring files between network nodes.

full duplex Capability for simultaneous data transmission between a sending station and a receiving station.

FQDN Fully Qualified Domain Name.A domain name that specifies its exact location in the tree hierarchy of the DNS. It specifies all domain levels, including the top-level domain, relative to the root domain. A fully qualified domain name is distinguished by this absoluteness in the name space.

FWSM Firewall Security Module. A module that can be installed in a Catalyst 6500 series switch. It uses the **shun** command to block. You can configure the FWSM in either single mode or multi-mode.

G

GBIC GigaBit Interface Converter. Often refers to a fiber optic transceiver that adapts optical cabling to fiber interfaces. Fiber-ready switches and NICs generally provide GBIC and/or SFP slots. For more information, refer to the *Catalyst Switch Cable, Connector, and AC Power Cord Guide.*

Gigabit Ethernet Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.

global correlation The IPS sensor shares information with other devices through a global correlation database to improve the combined efficacy of all devices.

global correlation client The software component of CollaborationApp that obtains and installs updates to the local global correlation databases.

global correlation database The collective information obtained from and shared with collaborative devices such as IPS sensors.

GMT Greenwich Mean Time. Time zone at zero degrees longitude. Now called Coordinated Universal Time (UTC).

GRUB Grand Unified Bootloader. Boot loader is the first software program that runs when a computer starts. It is responsible for loading and transferring control to the operating system kernel software. The kernel, in turn, initializes the rest of the operating system.

H

H.225.0 An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.

H.245 An ITU standard that governs H.245 endpoint control.

H.323 Allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.

half duplex Capability for data transmission in only one direction at a time between a sending station and a receiving station. BSC is an example of a half-duplex protocol.

handshake Sequence of messages exchanged between two or more network devices to ensure transmission synchronization.

hardware bypass A specialized interface card that pairs physical interfaces so that when a software error is detected, a bypass mechanism is engaged that directly connects the physical interfaces and allows traffic to flow through the pair. Hardware bypass passes traffic at the network interface, does not pass it to the IPS system.

host block ARC blocks all traffic from a given IP address.

HTTP Hypertext Transfer Protocol. The stateless request/response media transfer protocol used in the IPS architecture for remote data exchange.

HTTPS An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

I

ICMP Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

ICMP flood Denial of Service attack that sends a host more ICMP echo request ("ping") packets than the protocol implementation can handle.

IDAPI Intrusion Detection Application Programming Interface. Provides a simple interface between IPS architecture applications. IDAPI reads and writes event data and provides a mechanism for control transactions.

IDCONF Intrusion Detection Configuration. A data format standard that defines operational messages that are used to configure intrusion detection and prevention systems.

IDENT Ident protocol, specified in RFC 1413, is an Internet protocol that helps identify the user of a particular TCP connection.

IDIOM Intrusion Detection Interchange and Operations Messages. A data format standard that defines the event messages that are reported by intrusion detection systems and the operational messages that are used to configure and control intrusion detection systems.

IDM IPS Device Manager. A web-based application that lets you configure and manage your sensor. The web server for IDM resides on the sensor. You can access it through Internet Explorer or Firefox web browsers.

IDMEF Intrusion Detection Message Exchange Format. The IETF Intrusion Detection Working Group draft standard.

IME IPS Manager Express. A network management application that provides system health monitoring, events monitoring, reporting, and configuration for up to ten sensors.

inline mode All packets entering or leaving the network must pass through the sensor.

inline interface A pair of physical interfaces configured so that the sensor forwards all traffic received on one interface out to the other interface in the pair.

InterfaceApp A component of the IPS. Handles bypass and physical settings and defines paired interfaces. Physical settings are speed, duplex, and administrative state.

intrusion detection system IDS. A security service that monitors and analyzes system events to find and provide real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

IP address 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

IPS Intrusion Prevention System. A system that alerts the user to the presence of an intrusion on the network through network traffic analysis techniques.

IPS data or message Describes the messages transferred over the command and control interface between IPS applications.

iplog A log of the binary packets to and from a designated address. Iplogs are created when the log Event Action is selected for a signature. Iplogs are stored in a libpcap format, which can be read by WireShark and TCPDUMP.

IP spoofing IP spoofing attack occurs when an attacker outside your network pretends to be a trusted user either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you want to provide access to specified resources on your network. Should an attacker get access to your IPSec security parameters, that attacker can masquerade as the remote user authorized to connect to the corporate network.

IPv6 IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

ISL Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.

J

Java Web Start Java Web Start provides a platform-independent, secure, and robust deployment technology. It enables developers to deploy full-featured applications to you by making the applications available on a standard web server. With any web browser, you can launch the applications and be confident you always have the most-recent version.

JNLP Java Network Launching Protocol. Defined in an XML file format specifying how Java Web Start applications are launched. JNLP consists of a set of rules defining how exactly the launching mechanism should be implemented.

K

KB Knowledge Base. The sets of thresholds learned by Anomaly Detection and used for worm virus detection.

Knowledge Base See KB.

L

LACP Link Aggregation Control Protocol. LACP aids in the automatic creation of Ether Channel links by exchanging LACP packets between LAN ports. This protocol is defined in IEEE 802.3ad.

LAN Local Area Network. Refers to the Layer 2 network domain local to a given host. Packets exchanged between two hosts on the same LAN do not require Layer 3 routing.

Layer 2 Processor A processor in the IPS. Processes layer 2-related events. It also identifies malformed packets and removes them from the processing path.

Logger A component of the IPS. Writes all the log messages of the application to the log file and the error messages of the application to the Event Store.

logging Gathers actions that have occurred in a log file. Logging of security information is performed on two levels: logging of events (such as IPS commands, errors, and alerts), and logging of individual IP session information.

LOKI Remote access, back door Trojan, ICMP tunneling software. When the computer is infected, the malicious code creates an ICMP tunnel that can be used to send small payload ICMP replies.

M

MainApp The main application in the IPS. The first application to start on the sensor after the operating system has booted. Reads the configuration and starts applications, handles starting and stopping of applications and node reboots, handles software upgrades.

major update A base version that contains major new functionality or a major architectural change in the product.

Malware Malicious software that is installed on an unknowing host.

manufacturing image Full IPS system image used by manufacturing to image sensors.

master blocking sensor A remote sensor that controls one or more devices. Blocking forwarding sensors send blocking requests to the master blocking sensor and the master blocking sensor executes the blocking requests.

MD5 Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

Meta engine Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.

MIB Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MIME Multipurpose Internet Mail Extension. Standard for transmitting nontext data (or data that cannot be represented in plain ASCII code) in Internet mail, such as binary, foreign language text (such as Russian or Chinese), audio, or video data. MIME is defined in RFC 2045.

minor update A minor version that contains minor enhancements to the product line. Minor updates are incremental to the major version, and are also base versions for service packs.

module A removable card in a switch, router, or security appliance chassis. The ASA 5585-X IPS SSP is a module.

monitoring interface See sensing interface.

MPF Modular Policy Framework. A means of configuring security appliance features in a manner similar to Cisco IOS software Modular QoS CLI.

MSRPC Microsoft Remote Procedure Call. MSRPC is the Microsoft implementation of the DCE RPC mechanism. Microsoft added support for Unicode strings, implicit handles, inheritance of interfaces (which are extensively used in DCOM), and complex calculations in the variable-length string and structure paradigms already present in DCE/RPC.

MySDN My Self-Defending Network. A part of the signature definition section of IDM and IME. It provides detailed information about signatures.

N

NAC Network Access Controller. See ARC.

NAS-ID Network Access ID. An identifier that clients send to servers to communicate the type of service they are attempting to authenticate.

NAT Native Address Translation. A network device can present an IP address to the outside networks that is different from the actual IP address of a host.

NBD Next Business Day. The arrival of replacement hardware according to Cisco service contracts.

Neighborhood Discovery Protocol for IPv6. IPv6 nodes on the same link use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors.

Network Access ID See NAS-ID.

network device A device that controls IP traffic on a network and can block an attacking host. An example of a network device is a Cisco router or PIX Firewall.

network participation Networks contributing learned information to the global correlation database.

network participation client The software component of CollaborationApp that sends data to the SensorBase Network.

never block address Hosts and networks you have identified that should never be blocked.

never shun address See never block address.

NIC Network Interface Card. Board that provides network communication capabilities to and from a computer system.

NMS network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

node A physical communicating element on the command and control network. For example, an appliance or a router.

Normalizer engine Configures how the IP and TCP normalizer functions and provides configuration for signature events related to the IP and TCP normalizer.

NOS network operating system. Generic term used to refer to distributed file systems. Examples include LAN Manager, NetWare, NFS, and VINES.

NotificationApp A component of the IPS. Sends SNMP traps when triggered by alert, status, and error events. NotificationApp uses the public domain SNMP agent. SNMP GETs provide information about the general health of the sensor.

NTP Network Timing Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NTP server Network Timing Protocol server. A server that uses NTP. NTP is a protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NVRAM Non-Volatile Read/Write Memory. RAM that retains its contents when a unit is powered off.

O

OIR online insertion and removal. Feature that permits you to add, replace, or remove cards without interrupting the system power, entering console commands, or causing other software or interfaces to shutdown.

OPS Outbreak Prevention Service.

P

P2P Peer-to-Peer. P2P networks use nodes that can simultaneously function as both client and server for the purpose of file sharing.

packet Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data. The terms datagram, frame, message, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

PAgP Port Aggregation Control Protocol. PAgP aids in the automatic creation of EtherChannel links by exchanging PAgP packets between LAN ports. It is a Cisco-proprietary protocol.

PAM Software module that provides AAA functionality to applications.

PAP Password Authentication Protocol. Most commonly used RADIUS messaging protocol.

passive fingerprinting Act of determining the OS or services available on a system from passive observation of network interactions.

Passive OS Fingerprinting The sensor determines host operating systems by inspecting characteristics of the packets exchanged on the network.

PASV Port Spoof An attempt to open connections through a firewall to a protected FTP server to a non-FTP port. This happens when the firewall incorrectly interprets an FTP 227 **passive** command by opening an unauthorized connection.

PAT Port Address Translation. A more restricted translation scheme than NAT in which a single IP address and different ports are used to represent the hosts of a network.

patch release Release that addresses defects identified in the update (minor, major, or service pack) binaries after a software release (service pack, minor, or major update) has been released.

PAWS Protection Against Wrapped Sequence. Protection against wrapped sequence numbers in high performance TCP networks. See RFC 1323.

PCI Peripheral Component Interface. The most common peripheral expansion bus used on Intel-based computers.

PDU protocol data unit. OSI term for packet. See also BPDU and packet.

PEP Cisco Product Evolution Program. PEP is the UDI information that consists of the PID, the VID, and the SN of your sensor. PEP provides hardware version and serial number visibility through electronic query, product labels, and shipping items.

PER packed encoding rules. Instead of using a generic style of encoding that encodes all types in a uniform way, PER specializes the encoding based on the date type to generate much more compact representations.

PFC Policy Feature Card. An optional card on a Catalyst 6000 supervisor engine that supports VACL packet filtering.

PID Product Identifier. The orderable product identifier that is one of the three parts of the UDI. The UDI is part of the PEP policy.

ping packet internet groper. Often used in IP networks to test the reachability of a network device. It works by sending ICMP echo request packets to the target host and listening for echo response replies.

PKI Public Key Infrastructure. Authentication of HTTP clients using the clients X.509 certificates.

Pluggable Authentication Modules See PAM.

POST Power-On Self Test. Set of hardware diagnostics that runs on a hardware device when that device is powered up.

Post-ACL Designates an ACL from which ARC should read the ACL entries, and where it places entries after all deny entries for the addresses being blocked.

Pre-ACL Designates an ACL from which ARC should read the ACL entries, and where it places entries before any deny entries for the addresses being blocked.

promiscuous delta PD. A weight in the range of 0 to 30 configured per signature. This weight can be subtracted from the overall risk rating in promiscuous mode.

promiscuous mode A passive interface for monitoring packets of the network segment. The sensing interface does not have an IP address assigned to it and is therefore invisible to attackers.

Q

Q.931 ITU-T specification for signaling to establish, maintain, and clear ISDN network connections.

QoS quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

R

rack mounting Refers to mounting a sensor in an equipment rack.

RADIUS Remote Authentication Dial In User Service. A networking protocol that provides centralized AAA functionality for systems to connect and use a network service.

RAM random-access memory. Volatile memory that can be read and written by a microprocessor.

RAS Registration, Admission, and Status Protocol. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signaling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.

RBCP Router Blade Control Protocol. RBCP is based on SCP, but modified specifically for the router application. It is designed to run over Ethernet interfaces and uses 802.2 SNAP encapsulation for messages.

reassembly The putting back together of an IP datagram at the destination after it has been fragmented either at the source or at an intermediate node.

recovery package An IPS package file that includes the full application image and installer used for recovery on sensors.

Regex See regular expression.

regular expression A mechanism by which you can define how to search for a specified sequence of characters in a data stream or file. Regular expressions are a powerful and flexible notation almost like a mini-programming language that allow you to describe text. In the context of pattern matching, regular expressions allow a succinct description of any arbitrary pattern.

Remote Authentication Dial In User Service See RADIUS.

repackage release A release that addresses defects in the packaging or the installer.

reputation Similar to human social interaction, reputation is an opinion toward a device on the Internet. It enables the installed base of IPS sensors in the field to collaborate using the existing network infrastructure. A network device with reputation is most probably malicious or infected.

risk rating RR. A risk rating is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network. The risk of the attack accounts for the severity, fidelity, relevance, and asset value of the attack, but not any response or mitigation actions. This risk is higher when more damage could be inflicted on your network.

RMA Return Materials Authorization. The Cisco program for returning faulty hardware and obtaining a replacement.

ROMMON Read-Only-Memory Monitor. ROMMON lets you TFTP system images onto the sensor for recovery purposes.

round-trip time See RTT.

RPC remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

RSM Router Switch Module. A router module that is installed in a Catalyst 5000 switch. It functions exactly like a standalone router.

RTP Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.

RTT round-trip time. A measure of the time delay imposed by a network on a host from the sending of a packet until acknowledgment of the receipt.

RU rack unit. A rack is measured in rack units. An RU is equal to 44 mm or 1.75 inches.

S

SCP Switch Configuration Protocol. Cisco control protocol that runs directly over the Ethernet.

SCEP Simple Certificate Enrollment Protocol. The Cisco Systems PKI communication protocol that leverages existing technology by using PKCS#7 and PKCS#10. SCEP is the evolution of the enrollment protocol.

SDEE Security Device Event Exchange. A product-independent standard for communicating security device events. It adds extensibility features that are needed for communicating events generated by various types of security devices.

SDEE Server Accepts requests for events from remote clients.

Secure Shell Protocol Protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.

security context You can partition a single adaptive security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management.

sensing interface The interface on the sensor that monitors the desired network segment. The sensing interface is in promiscuous mode; it has no IP address and is not visible on the monitored segment.

sensor The sensor is the intrusion detection engine. It analyzes network traffic searching for signs of unauthorized activity.

SensorApp A component of the IPS. Performs packet capture and analysis. SensorApp analyzes network traffic for malicious content. Packets flow through a pipeline of processors fed by a producer designed to collect packets from the network interfaces on the sensor. SensorApp is the standalone executable that runs Analysis Engine.

Service engine Deals with specific protocols, such as DNS, FTP, H255, HTTP, IDENT, MS RPC, MS SQL, NTP, P2P, RPC, SMB, SNMP, SSH, and TNS.

service pack Used for the release of defect fixes and for the support of new signature engines. Service packs contain all of the defect fixes since the last base version (minor or major) and any new defects fixes.

session command Command used on routers and switches to provide either Telnet or console access to a module in the router or switch.

SFP Small Form-factor Pluggable. Often refers to a fiber optic transceiver that adapts optical cabling to fiber interfaces. See GBIC for more information.

shared secret A piece of data known only to the parties involved in a secure communication. The shared secret can be a password, a passphrase, a big number, or an array of randomly chosen bytes.

shun command Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection. It is used by ARC when blocking with a PIX Firewall.

Signature Analysis Processor A processor in the IPS. Dispatches packets to the inspectors that are not stream-based and that are configured for interest in the packet in process.

signature A signature distills network information and compares it against a rule set that indicates typical intrusion activity.

signature engine A component of the sensor that supports many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges or sets of values.

signature engine update Executable file with its own versioning scheme that contains binary code to support new signature updates.

Signature Event Action Filter Subtracts actions based on the signature event signature ID, addresses, and risk rating. The input to the Signature Event Action Filter is the signature event with actions possibly added by the Signature Event Action Override.

Signature Event Action Handler Performs the requested actions. The output from Signature Event Action Handler is the actions being performed and possibly an evIdsAlert written to the Event Store.

Signature Event Action Override Adds actions based on the risk rating value. Signature Event Action Override applies to all signatures that fall into the range of the configured risk rating threshold. Each Signature Event Action Override is independent and has a separate configuration value for each action type.

Signature Event Action Processor Processes event actions. Event actions can be associated with an event risk rating threshold that must be surpassed for the actions to take place.

signature fidelity rating SFR. A weight associated with how well a signature might perform in the absence of specific knowledge of the target. The signature fidelity rating is configured per signature and indicates how accurately the signature detects the event or condition it describes.

signature update Executable file that contains a set of rules designed to recognize malicious network activities, such as worms, DDOS, viruses, and so forth. Signature updates are released independently, are dependent on a required signature engine version, and have their own versioning scheme.

Slave Dispatch Processor A processor in the IPS. Process found on dual CPU systems.

SMB Server Message Block. File-system protocol used in LAN manager and similar NOSs to package data and exchange information with other systems.

SMTP Simple Mail Transfer Protocol. Internet protocol providing e-mail services.

SN Serial Number. Part of the UDI. The SN is the serial number of your Cisco product.

SNAP Subnetwork Access Protocol. Internet protocol that operates between a network entity in the subnetwork and a network entity in the end system. SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks. The SNAP entity in the end system makes use of the services of the subnetwork and performs three key functions: data transfer, connection management, and QoS selection.

sniffing interface See sensing interface.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP2 SNMP Version 2. Version 2 of the network management protocol. SNMP2 supports centralized and distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security.

SNMPv3 SNMP Version 3. Version 3 of the network management protocol. SNMPv3 adds security and remote configuration enhancements to SNMP, such as encryption of packets, message integrity, and authentication.

software bypass Passes traffic through the IPS system without inspection.

source address Address of a network device that is sending data.

SPAN Switched Port Analyzer. Feature of the Catalyst 5000 switch that extends the monitoring abilities of existing network analyzers into a switched Ethernet environment. SPAN mirrors the traffic at one switched segment onto a predefined SPAN port. A network analyzer attached to the SPAN port can monitor traffic from any other Catalyst switched port.

spanning tree Loop-free subset of a network topology.

SQL Structured Query Language. International standard language for defining and accessing relational databases.

SRAM Type of RAM that retains its contents for as long as power is supplied. SRAM does not require constant refreshing, like DRAM.

SSH Secure Shell. A utility that uses strong authentication and secure communications to log in to another computer over a network.

SSL Secure Socket Layer. Encryption technology for the Internet used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

Stacheldraht A DDoS tool that relies on the ICMP protocol.

State engine Stateful searches of HTTP strings.

Statistics Processor A processor in the IPS. Keeps track of system statistics such as packet counts and packet arrival rates.

STP Spanning Tree Protocol. A network protocol that ensures a loop-free topology for any bridged Ethernet local area network. STP prevents bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails without the danger of bridge loops or the need for manual enabling/disabling of these backup links.

Stream Reassembly Processor A processor in the IPS. Reorders TCP streams to ensure the arrival order of the packets at the various stream-based inspectors. It is also responsible for normalization of the TCP stream. The normalizer engine lets you enable or disable alert and deny actions.

String engine A signature engine that provides regular expression-based pattern inspection and alert functionality for multiple transport protocols, including TCP, UDP, and ICMP.

subsignature A more granular representation of a general signature. It typically further defines a broad scope signature.

surface mounting Refers to attaching rubber feet to the bottom of a sensor when it is installed on a flat surface. The rubber feet allow proper airflow around the sensor and they also absorb vibration so that the hard-disk drive is less impacted.

switch Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data link layer of the OSI model.

SwitchApp A component of the IPS. The IPS 4500 series sensors. have a built in switch that provides external monitoring interfaces. The SwitchApp enables the InterfaceApp and sensor initialization scripts to communicate with and control the switch.

SYN flood Denial of Service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

system image The full IPS application and recovery image used for reimaging an entire sensor.

T

TAC A Cisco Technical Assistance Center. There are four TACs worldwide.

TACACS+ Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

target value rating TVR. A weight associated with the perceived value of the target. Target value rating is a user-configurable value (zero, low, medium, high, or mission critical) that identifies the importance of a network asset (through its IP address).

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TCPDUMP The TCPDUMP utility is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can use different options for viewing summary and detail information for each packet. For more information, see http://www.tcpdump.org/.

Telnet Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

terminal server A router with multiple, low speed, asynchronous ports that are connected to other serial devices. Terminal servers can be used to remotely manage network equipment, including sensors.

TFN Tribe Flood Network. A common type of DoS attack that can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.

TFN2K Tribe Flood Network 2000. A common type of DoS attack that can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.

TFTP Trivial File Transfer Protocol. Simplified version of FTP that lets files be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

threat rating TR. A threat rating is a value between 0 and 100 that represents a numerical decrease of the risk rating of an attack based on the response action that depicts the threat of an alert on the monitored network.

three-way handshake Process whereby two protocol entities synchronize during connection establishment.

threshold A value, either upper- or lower-bound that defines the maximum/minimum allowable condition before an alarm is sent.

Time Processor A processor in the IPS. Processes events stored in a time-slice calendar. Its primary task is to make stale database entries expire and to calculate time-dependent statistics.

TLS Transport Layer Security. The protocol used over stream transports to negotiate the identity of peers and establish encrypted communications.

TNS Transparent Network Substrate. Provides database applications with a single common interface to all industry-standard network protocols. With TNS, database applications can connect to other database applications across networks with different protocols.

topology Physical arrangement of network nodes and media within an enterprise networking structure.

TPKT Transport Packet. RFC 1006-defined method of demarking messages in a packet. The protocol uses ISO transport services on top of TCP.

traceroute Program available on many systems that traces the path a packet takes to a destination. It is used mostly to debug routing problems between hosts. A traceroute protocol is also defined in RFC 1393.

traffic analysis Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence.

Traffic ICMP engine Analyzes traffic from nonstandard protocols, such as TFN2K, LOKI, and DDOS.

trap Message sent by an SNMP agent to an NMS, a console, or a terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

Trojan engine Analyzes traffic from nonstandard protocols, such as BO2K and TFN2K.

trunk Physical and logical connection between two switches across which network traffic travels. A backbone is composed of a number of trunks.

trusted certificate Certificate upon which a certificate user relies as being valid without the need for validation testing; especially a public-key certificate that is used to provide the first public key in a certification path.

trusted key Public key upon which a user relies; especially a public key that can be used as the first public key in a certification path.

tune Adjusting signature parameters to modify an existing signature.

U

UDI Unique Device Identifier. Provides a unique identity for every Cisco product. The UDI is composed of the PID, VID, and SN. The UDI is stored in the Cisco IPS ID PROM.

UDLD UniDirectional Link Detection. Cisco proprietary protocol that allows devices connected through fiber-optic or copper Ethernet cables connected to LAN ports to monitor the physical configuration of the cables and detect when a unidirectional link exists. When a unidirectional link is detected, UDLD shuts down the affected LAN port and sends an alert, since unidirectional links can cause a variety of problems, such as, spanning tree topology loops.

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

unblock To direct a router to remove a previously applied block.

UniDirectional Link Detection See UDLD.

unvirtualized sensing interface An unvirtualized sensing interface has not been divided into subinterfaces and the entire interfaces can be associated with at most one virtual sensor.

UPS Uninterruptable Power Source.

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

UTF-8 8-bit Unicode Transformation Format. A variable-length character encoding for Unicode. UTF-8 can represent every character in the Unicode character set and is backwards-compatible with ASCII.

V

VACL VLAN ACL. An ACL that filters all packets (both within a VLAN and between VLANs) that pass through a switch. Also known as security ACLs.

VID Version identifier. Part of the UDI.

VIP Versatile Interface Processor. Interface card used in Cisco 7000 and Cisco 7500 series routers. The VIP provides multilayer switching and runs Cisco IOS. The most recent version of the VIP is VIP2.

virtual sensor A logical grouping of sensing interfaces and the configuration policy for the signature engines and alarm filters to apply to them. In other words, multiple virtual sensors running on the same appliance, each configured with different signature behavior and traffic feeds.

virtualized sensing interface A virtualized interface has been divided into subinterfaces each of which consists of a group of VLANs. You can associate a virtual sensor with one or more subinterfaces so that different intrusion prevention policies can be assigned to those subinterfaces. You can virtualize both physical and inline interfaces.

virus Hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—that is, inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

VLAN Virtual Local Area Network. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VTP VLAN Trunking Protocol. Cisco Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis.

VoIP Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

VPN Virtual Private Network(ing). Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VTP VLAN Trunking Protocol. A Cisco Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis.

vulnerability One or more attributes of a computer or a network that permit a subject to initiate patterns of misuse on that computer or network.

W

WAN wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.

watch list rating WLR. A weight associated with the CSA MC watch list in the range of 0 to 100 (CSA MC only uses the range 0 to 35).

Web Server A component of the IPS. Waits for remote HTTP client requests and calls the appropriate servlet application.

WHOIS A TCP-based query/response protocol used for querying an official database to determine the owner of a domain name or an IP address.

Wireshark Wireshark is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. For more information, see http://www.wireshark.org.

worm A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and can consume computer resources destructively.

X

X.509 Standard that defines information contained in a certificate.

XML eXtensible Markup Language. Textual file format used for data interchange between heterogeneous hosts.

XPI Cross Packet Inspection. Technology used by TCP that allows searches across packets to achieve packet and payload reassembly.

Z

zone A set of destination IP addresses sorted into an internal, illegal, or external zone used by Anomaly Detection.

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z