Cisco Intrusion Prevention System Device Manager Configuration Guide for IPS 5.1

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-8674-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Intrusion Prevention System Device Manager Configuration Guide for IPS 5.1
Copyright © 2005-2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Revised: July 9, 2012, OL-8674-01

Contents

This document describes how to install, configure, and use Intrusion Prevention System Device Manager (IDM) for IPS 5.1. It includes a glossary that contains expanded acronyms and pertinent IPS terms. It is part of the documentation set for Cisco Intrusion Prevention System 5.1. Use this guide in conjunction with the documents listed in Related Documentation, page xxii. This preface contains the following topics:

Audience

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

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

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 more information on Cisco IPS, refer to the following documentation found at this URL:

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

- *Documentation Roadmap for Cisco Intrusion Prevention System*
- *Release Notes for Cisco Intrusion Prevention System*
- *Cisco Intrusion Prevention System Manager Express Configuration Guide*
- *Cisco Intrusion Prevention System Command Reference*
- *Cisco Intrusion Prevention System Sensor CLI Configuration Guide*
- *Cisco Intrusion Prevention System Appliance and Module Installation Guide*
- *Installling and Removing Interface Cards in Cisco IPS-4260 and IPS 4270-20*

- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500-X Series Appliances and the Cisco Intrusion Prevention System 4300 Series Appliances*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4500 Series Sensor Appliance*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Getting Started

Note *Installing and Using Cisco Intrusion Prevention System Device Manager Version 5.1* also applies to the IPS section of ASDM. The path in ASDM has two additional initial jumps, Configuration > Features before you reach the IPS section, for example, Configuration > Features > IPS > Network.

This chapter describes IDM and provides information for getting started using IDM. It contains the following sections:

Advisory

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 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.

Introducing IDM

IDM is a web-based, Java application that enables you to configure and manage your sensor. The web server for IDM resides on the sensor. You can access it through the Internet Explorer, Netscape, or Mozilla web browsers.

The IDM user interface consists of the File and Help menus, Configuration and Monitoring buttons whose menus open in the left-hand TOC pane, and the configuration pane on the right side of the page. The following four buttons appear next to the Configuration and Monitoring buttons:

- Back—Takes you to the pane you were previously on.
- Forward—Takes you forward to the next pane you have been on.
- Refresh—Loads the current configuration from the sensor.
- Help—Opens the online help in a new window.

To configure the sensor, choose **Configuration** and go through the menus in the left-hand pane. Choose **Monitoring** and go through the menus in the left-hand pane to configure monitoring**.**

New configurations do not take effect until you click **Apply** on the pane you are configuring. Click **Reset** to discard current changes and return settings to their previous state for that pane.

System Requirements

The following lists the system requirements for IDM:

- Windows 2000, Windows XP
  - Internet Explorer 6.0 with Java Plug-in 1.4.2 or 1.5 or Netscape 7.1 with Java Plug-in 1.4.2 or 1.5
  - Pentium III or equivalent running at 450 Mhz or higher
  - 256 MB minimum, 512 MB or more strongly recommended
  - 1024 x 768 resolution and 256 colors (minimum)
- Sun SPARC Solaris
  - Sun Solaris 2.8 or 2.9
  - Mozilla 1.7
  - 256 MB minimum, 512 MB or more strongly recommended
  - 1024 x 768 resolution and 256 colors (minimum)
- Linux
  - Red Hat Linux 9.0 or Red Hat Enterprise Linux WS, Version 3 running GNOME or KDE
  - Mozilla 1.7
  - 256 MB minimum, 512 MB or more strongly recommended
  - 1024 x 768 resolution and 256 colors (minimum)

Note Although other web browsers may work with IDM, we only support the listed browsers.

Increasing the Memory Size of the Java Plug-in

To correctly run IDM, your browser must have Java Plug-in 1.4.2 or 1.5 installed. By default the Java Plug-in allocates 64 MB of memory to IDM. IDM can run out of memory while in use, which can cause IDM to freeze or display blank screens. Running out of memory can also occur when you click **Refresh**. An `OutofMemoryError` message appears in the Java console whenever this occurs. You must change the memory settings of Java Plug-in before using IDM. The mandatory minimum memory size is 256 MB.

Note We recommend that you use Sun Microsystems Java. Using any other version of Java could cause problems with IDM.

This section contains the following topics:

Java Plug-In on Windows

To change the settings of Java Plug-in on Windows for Java Plug-in 1.4.2 and 1.5, follow these steps:

Step 1 Close all instances of Internet Explorer or Netscape.

Step 2 Choose **Start > Settings > Control Panel**.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click Java Plug-in.

The Java Plug-in Control Panel appears.

b. Click the **Advanced** tab.

c. Enter **`-Xms256m`** in the Java RunTime Parameters field.

d. Click **Apply** and exit the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click Java.

The Java Control Panel appears.

b. Click the **Java** tab.

c. Click **View** under Java Applet Runtime Settings.

The Java Runtime Settings Panel appears.

d. Enter **`-Xmxs256m`** in the Java Runtime Parameters field and then click **OK**.

e. Click **OK** and exit the Java Control Panel.

Java Plug-In on Linux and Solaris

To change the settings of Java Plug-in 1.4.2 or 1.5 on Linux and Solaris, follow these steps:

Step 1 Close all instances of Netscape or Mozilla.

Step 2 Bring up Java Plug-in Control Panel by launching the ControlPanel executable file.

Note In the Java 2 SDK, this file is located at <SDK installation directory>/jre/bin/ControlPanel. For example if your Java 2 SDK is installed at /usr/j2se, the full path is /usr/j2se/jre/bin/ControlPanel.

Note In a Java 2 Runtime Environment installation, the file is located at <JRE installation directory>/bin/ControlPanel.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click the **Advanced** tab.

b. Enter `-Xms256m` in the Java RunTime Parameters field.

c. Click **Apply** and close the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click the **Java** tab.

b. Click **View** under Java Applet Runtime Settings.

c. Enter `-Xms256m` in the Java Runtime Parameters field and then click **OK**.

d. Click **OK** and exit the Java Control Panel.

Initializing the Sensor

This section explains how to initialize the sensor, and contains the following topics:

Overview

After you have installed the sensor on your network, you must use the **setup** command to initialize it. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, Telnet server, web server port, access control lists, time settings, and assign and enable interfaces. After you have initialized the sensor, you can communicate with it over the network. You are then ready to configure intrusion prevention.

Initializing the Sensor

To initialize the sensor, follow these steps:

Step 1 Log in to the sensor using an account with administrator privileges:

- Log in to the appliance by using a serial connection or with a monitor and keyboard.

  Note You cannot use a monitor and keyboard with IDS-4215, IPS-4240, or IPS-4255.

- Session to IDSM-2:
  - For Catalyst software:

    ```
    console> enable
    console> (enable) session module_number
    ```

  - For Cisco IOS software:

    ```
    Router# session slot slot_number processor 1
    ```

- Session to NM-CIDS:

  ```
  router# service-module IDS-Sensor slot_number/port_number session
  ```

- Session to AIP-SSM:

  ```
  asa# session 1
  ```

  Note The default username and password are both **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.

Caution If you forget your password, you may have to reimage your sensor unless there is another user with Administrator privileges (see Chapter 13, "Upgrading, Downgrading, and Installing System Images"). The other Administrator can log in and assign a new password to the user who forgot the password. Or, if you have created the service account for support purposes, you can have TAC create a password. For more information, refer to Creating the Service Account.

After you change the password, the `sensor#` prompt appears.

Step 3 Enter the **setup** command.

The System Configuration Dialog is displayed.

Note The System Configuration Dialog is an interactive dialog. The default settings are displayed.

```
    --- 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 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
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


Current time: Wed May 5 10:25:35 2004
```

Step 4 Press the spacebar to get to the following question:

```
Continue with configuration dialog?[yes]:
```

Press the spacebar to show one page at a time. Press **Enter** to show one line at a time.

Step 5 Enter **yes** to continue.

Step 6 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 7 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 where X = 0-255, 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 where Y = 0-255.

Step 8 Specify the Telnet server status.

You can disable or enable Telnet services. The default is disabled.

Step 9 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 If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format `https://`*sensor_ip_ address*`:port` (for example, `https://10.1.9.201:1040`).

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 10 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.

The IP network interface is in the form of IP Address/Netmask: X.X.X.X/nn, where X.X.X.X specifies the network IP address as a 32-bit address written as 4 octets separated by periods where X = 0-255, nn specifies the number of bits in the netmask for that network.

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.

d. Press **Enter** at a blank permit line to proceed to the next step.

Step 11 Enter **`yes`** to modify the system clock settings.

a. Enter **`yes`** if you want to use NTP.

You will 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. For the procedure, refer to Configuring the Sensor to Use an NTP Server as its Time Source.

b. Enter **`yes`** to modify summertime settings.

Note Summertime is also known as DST. If your location does not use Summertime, go to Step n.

c. Choose recurring, date, or disable to specify how you want to configure summertime settings.

The default is recurring.

d. 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 april.

e. Specify the week you want to start summertime settings.

Valid entries are first, second, third, fourth, fifth, and last.

The default is first.

f. Specify the day you want to start summertime settings.

Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday.

The default is sunday.

g. 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 a.m. on the first Sunday in April, and a stop time of 2 a.m. on the fourth Sunday in October. The default summertime offset is 60 minutes.

h. 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 october.

i. Specify the week you want the summertime settings to end.

Valid entries are first, second, third, fourth, fifth, and last.

The default is last.

j. 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.

k. Specify the time you want summertime settings to end.

l. Specify the DST zone.

The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+:,_/-]+$.

m. 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 0.

n. Enter **yes** to modify the system time zone.

o. Specify the standard time zone name.

The zone name is a character string up to 24 characters long.

p. Specify the standard time offset.

The default is 0.

Specify the standard time zone offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian).

Step 12 Enter **yes** to modify the virtual sensor configuration (vs0).

The current interface configuration appears:

```
Current interface configuration
  Command control: GigabitEthernet0/1
  Unused:
    GigabitEthernet2/1
    GigabitEthernet2/0
  Promiscuous:
    GigabitEthernet0/0
  Inline:
    None
```

```
Inline VLAN Pair:
  None
```

Step 13 Enter **yes** to add a promiscuous or monitoring interface.

Step 14 Enter the interface you want to add, for example, **GigabitEthernet0/1**.

Step 15 Enter **yes** to add inline interface pairs (appears only if your platform supports inline interface pairs).

a. Enter the inline interface pair name.

b. Enter the inline interface pair description.

The default is `Created via setup by user <yourusername>`.

c. Enter the name of the first interface in the inline pair, **interface1**.

d. Enter the name of the second interface in the inline pair, **interface2**.

e. Repeat Steps a through d to add another inline interface pair, or press **Enter** for the next option.

Step 16 Enter **yes** to add inline VLAN pairs (appears only if your platform supports inline VLAN pairs).

A list of interfaces available for inline VLAN pairs appears:

```
Available Interfaces:
 [1] GigabitEthernet0/0
 [2] GigabitEthernet2/0
 [3] GigabitEthernet2/1
```

Step 17 Enter the number of the interface you want to subdivide into inline VLAN pairs.

The current inline VLAN pair configuration for that interface appears:

```
Inline Vlan Pairs for GigabitEthernet0/0
  None
```

a. Enter the subinterface number to add.

b. Enter the inline VLAN pair description.

c. Enter the first VLAN number (vlan1).

d. Enter the second VLAN number (vlan2).

e. Repeat Steps a through d to add another inline VLAN pair on this interface or press **Enter** for the next option.

Step 18 Enter **yes** to subdivide another interface. Enter **no** or press **Enter** to complete the addition of the inline VLAN pairs.

Your configuration appears with the following options:

```
[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 19 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 20 Enter **yes** to modify the system date and time.

Note This option is not available on modules or when NTP has been configured. The modules get their time from the router or switch in which they are installed, or from the configured NTP server.

a. Enter the local date (yyyy-mm-dd).

b. Enter the local time (hh:mm:ss).

Step 21 Reboot the sensor:

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 22 Enter **yes** to continue the reboot.

Step 23 Display the self-signed X.509 certificate (needed by TLS):

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 24 Write down the certificate fingerprints.

You need these to check the authenticity of the certificate when connecting to this sensor with a web browser.

Step 25 Apply the most recent service pack and signature update.

For information on how to obtain the most recent software, see Obtaining Cisco IPS Software, page 12-1. The Readme explains how to apply the most recent software update.

You are now ready to configure your sensor for intrusion prevention.

Verifying Initialization

To verify that you initialized your sensor, follow these steps:

Step 1 Log in to the sensor.

For the procedure, refer to Logging In to the Sensor.

Step 2 View your configuration:

```
sensor# show configuration
generating current config:
! ------------------------------
! Version 5.1(1)
! Current configuration last modified Wed Jun 29 19:18:14 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 0
physical-interface GigabitEthernet2/1
exit
exit
! ------------------------------
service authentication
```

```
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
access-list 171.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
bypass-mode auto
interface-notifications
missed-percentage-threshold 19
notification-interval 36
idle-interface-delay 33
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 2004 0
alert-severity low
status
enabled true
exit
alert-frequency
```

```
summary-mode fire-all
exit
exit
exit
signatures 3201 1
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3301 0
status
enabled true
exit
exit
signatures 3401 0
status
enabled true
retired false
exit
engine string-tcp
event-action produce-alert|request-block-host
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
trusted-certificates 10.89.149.227:443 certificate MIICJDCCAY0CCPy71vhtAwyNMA0GC
SqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTAlVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwE
AYDVQQLEwlTU00tSVBTMTAxFjAUBgNVBAMTDTEwLjg5LjE0OS4yMjcwHhcNMDUwNjE0MDUwODA3WhcNM
DcwNjE1MDUwODA3WjBXMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESM
BAGA1UECxMJU1NNLUlQUzEwMRYwFAYDVQQDEw0xMC44OS4xNDkuMjI3MIGfMA0GCSqGSIb3DQEBAQUAA
4GNADCBiQKBgQCoOobDuZOEPudw63Rlt8K1YsymzR/D9Rlcnad/U0gjAQGfcUh3sG3TXPQewon1fH0+A
nBw8Jxv/ovSB1HJ3ujh5k7BrrB2QMv73ESsBDdxLY6SoX/yYANMf4zPcPCAORJ6DMQHFj44A+3tMZWsC
yaod23S1oYOxx7v5puPDYn3IQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAHfPM7jawvdfXkYyazqvy3ZOK
kHVwHji12vBLo+biULJG95hbTFlqO+ba3R6nPD3tepgx5zTdOr2onnlFHWD95Ii+PKdUxj7vfDBG8atn
obsEBJ1lAQDiogskdCs4ax1tB4SbEU5y1tktKgcwWEdJpbbNJhzpoRsRICfM3HlOEwN
exit
! ------------------------------
service web-server
exit
sensor#
```

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
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
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 these to check the authenticity of the certificate when connecting to this sensor with a web browser.

Logging In to IDM

This section describes how to log in to IDM, and contains the following topics:

Overview

The number of concurrent CLI sessions is limited based on the platform. IDS-4210, IDS-4215, and NM-CIDS are limited to three concurrent CLI sessions. All other platforms allow ten concurrent sessions.

Prerequisites

IDM is part of the version 5.1 sensor. You must use the **setup** command to initialize the sensor so that it can communicate with IDM. For the procedure, see Initializing the Sensor, page 1-4.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

Logging In to IDM

To log in to IDM, follow these steps:

Step 1 Open a web browser and enter the sensor IP address:

https://*sensor_ip_address*

Note IDM is already installed on the sensor.

Note `https://10.1.9.201` is the default address, which you change to reflect your network environment when you initialize the sensor. When you change the web server port, you must specify the port in the URL address of your browser when you connect to IDM in the format `https://sensor_ip_ address:port` (for example, `https://10.1.9.201:1040`).

A Security Alert dialog box appears. For more information about security and IDM, see IDM and Certificates, page 1-15.

Step 2 Enter your username and password in the Enter Network Password dialog box and click **OK**.

Note The default username and password are both **cisco**. You were prompted to change the password during sensor initialization. For the procedure, see Initializing the Sensor, page 1-4.

The Cisco IDM 5.1 Information window opens and informs you that it is loading IDM. IDM appears in another browser window.

The Memory Warning dialog box displays the following message:

```
Your current Java memory heap size is less than 256 MB. You must increase the Java memory
heap size before launching IDM. Click Help for information on changing the Java memory
heap size.
```

Step 3 Click **Help** to see the procedure for changing the Java memory heap size.

Step 4 Follow the directions for changing the Java memory heap size.

Step 5 Close any browser windows you have open.

Step 6 Relaunch IDM by opening a browser window and typing the sensor IP address.

Step 7 Enter your username and password in the Password Needed - Networking dialog box and click **Yes**.

A Warning dialog box displays the following message:

```
There is no license key installed on the sensor. To install a new license, go to
Configuration > Licensing.
```

For the procedure for licensing the sensor, see Licensing the Sensor, page 1-19.

The Status dialog box displays the following message:

```
Please wait while the IDM is loading the current configuration from the Sensor.
```

The main window of IDM appears.

IDM and Cookies

IDM uses cookies to track sessions, which provide a consistent view. IDM uses only session cookies (temporary), not stored cookies. Because the cookies are not stored locally, there is no conflict with your browser cookie policy. The cookies are handled by the IDM Java applet rather than the browser.

IDM and Certificates

This section explains how certificates work with IDM, and contains the following topics:

Understanding Certificates

IPS 5.1 contains a web server that is running IDM and that the management stations, such as VMS, connect to. 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 IDM because it does not trust the CA.

Note 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 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 IDM, you receive the manual override dialog boxes. You must perform the certificate fingerprint validation again for Internet Explorer, Netscape, and Mozilla.

Validating the CA for Internet Explorer

To use Internet Explorer to validate the certificate fingerprint, follow these steps:

Step 1 Open a web browser and enter the sensor IP address to connect to IDM:

```
https://sensor_ ip_address
```

The Security Alert pane appears.

Step 2 Click **View Certificate**.

The Certificate Information pane appears.

Step 3 Click the **Details** tab.

Step 4 Scroll down the list to find **Thumbprint** and select it.

You can see the thumbprint in the text field.

Note Leave the Certificate pane open.

Step 5 Connect to the sensor in one of the following ways:

- Connect a terminal to the console port of the sensor.
- Use a keyboard and monitor directly connected to the sensor.
- Telnet to the sensor.
- Connect through SSH.

Step 6 Display the TLS fingerprint:

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 7 Compare the SHA1 fingerprint with the value displayed in the open Certificate thumbprint text field.

You have validated that the certificate that you are about to accept is authentic.

Caution If the fingerprints do not match, you need to determine why. Make sure you are connected to the correct IP address for the sensor. If you are connected to the correct IP address and the fingerprints do not match, this could indicate that your sensor may have been compromised.

Step 8 Click the **General** tab.

Step 9 Click **Install Certificate**.

The Certificate Import Wizard appears.

Step 10 Click **Next**.

The Certificate Store dialog box appears.

Step 11 Select **Place all certificates in the following store**, and then click **Browse**.

The Select Certificate Store dialog box appears.

Step 12 Click **Trusted Root Certification Authorities**, and then click **OK**.

Step 13 Click **Next**, and then click **Finish**.

The Security Warning dialog box appears.

Step 14 Click **Yes**, and then click **OK**.

Step 15 Click **OK** to close the Certificate dialog box.

Step 16 Click **Yes** to open IDM.

Validating the CA for Netscape

To use Netscape to validate the certificate fingerprint, follow these steps:

Step 1 Open a web browser and enter the sensor IP address to connect to IDM:

```
https://sensor_ip_address
```

The New Site Certificate pane appears.

Step 2 Click **Next**, and then click **More Info**.

The View A Certificate pane appears.

Step 3 Connect to the sensor in one of the following ways:

- Connect a terminal to the console port of the sensor.
- Use a keyboard and monitor directly connected to the sensor.
- Telnet to the sensor.
- Connect through SSH.

Step 4 Display the TLS fingerprint:

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 5 Compare the MD5 fingerprint with the value displayed in the View A Certificate pane.

You have validated that the certificate that you are about to accept is authentic.

Caution If the fingerprints do not match, you need to determine why. Make sure you are connected to the correct IP address for the sensor. If you are connected to the correct IP address and the fingerprints do not match, this could indicate that your sensor may have been compromised.

Step 6 Click **OK** to close the View A Certificate pane.

Step 7 Click **Next** and click the **Accept this certificate forever (until it expires)** radio button.

Step 8 Click **Next** twice, and then click **Finish**.

Validating the CA for Mozilla

To use Mozilla to validate the certificate fingerprint, follow these steps:

Step 1 Open a web browser and enter the sensor IP address to connect to IDM:

```
https://sensor_ip_address
```

The Website Certified by an Unknown Authority pane appears.

Step 2 Click **Examine Certificate**.

The Certificate Viewer pane appears.

Step 3 Connect to the sensor in one of the following ways:

- Connect a terminal to the console port of the sensor.
- Use a keyboard and monitor directly connected to the sensor.
- Telnet to the sensor.
- Connect through SSH.

Step 4 Display the TLS fingerprint:

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 5 Compare the MD5 fingerprint with the value displayed on the Certificate Viewer General tab.

You have validated that the certificate that you are about to accept is authentic.

Caution If the fingerprints do not match, you need to determine why. Make sure you are connected to the correct IP address for the sensor. If you are connected to the correct IP address and the fingerprints do not match, this could indicate that your sensor may have been compromised.

Step 6 Click **Close** to close the Certificate Viewer: pane.

Step 7 Select **Accept this certificate permanently** and then click **OK** to close the pane.

The login dialog box appears.

Step 8 Enter your username and password in the **Prompt** dialog box.

Step 9 Click **Yes** to accept the certificate.

Licensing the Sensor

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

Overview

Although the sensor functions without the license key, you must have a license key to obtain signature updates. 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. For more information, see Service Programs for IPS Products, page 1-20.

- Your IPS device serial number

  To find the IPS device serial number in IDM, choose **Configuration > Licensing**, or in the CLI use the **show version** command.

- 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. For the procedure, see Obtaining and Installing the License Key, page 1-22.

You can view the status of the license key on the Licensing pane in IDM. Whenever you start IDM, 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 IDM but you cannot download signature updates.

When you enter the CLI, you are informed of your license status, for example, you receive the following message if there is no license installed:

```
***LICENSE NOTICE***
There is no license key installed on the system.
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.
```

You will continue to see this message until you install a license key.

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:

- IDS-4215
- IPS-4240
- IPS-4255
- IDSM-2
- NM-CIDS

For ASA products, if you purchased one of the following ASA products that do not contain IPS, you must purchase a SMARTnet contract:

- ASA5510-K8
- ASA5510-DC-K8
- ASA5510-SEC-BUN-K9
- ASA5520-K8
- ASA5520-DC-K8
- ASA5520-BUN-K9
- ASA5540-K8
- ASA5540-DC-K8
- ASA5540-BUN-K9

Note SMARTnet provides operating system updates, access to Cisco.com, access to TAC, a nd hardware replacement NBD on site.

If you purchased one of the following ASA products that ships with the AIP-SSM installed or if you purchased AIP-SSM to add to your ASA product, you must purchase the Cisco Services for IPS service contract:

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9
- ASA5540-AIP20-K9
- ASA-SSM-AIP-10-K9
- ASA-SSM-AIP-20-K9

Note Cisco Services for IPS provides IPS signature updates, operating system updates, access to Cisco.com, access to TAC, a nd hardware replacement NBD on site.

For example, if you purchased an ASA-5510 and then later wanted to add IPS and purchased an ASA-SSM-AIP-10-K9, you must now purchase the Cisco Services for IPS service contract.

Once you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key. For the procedure, see Obtaining and Installing the License Key, page 1-22.

Caution If you ever have to RMA your product, the serial number will change. You must then get a new license key for the new serial number.

Supported User Role

You must be Administrator to view license information on the Licensing pane and to install the sensor license key.

Field Definitions

The following fields and buttons are found on the Licensing pane.

Field Descriptions:

- Current License—Provides the status of the current license:
  - License Status—Current license status of the sensor.
  - Expiration Date—Date when the license key expires (or has expired).

    If the key is invalid, no date is displayed.
  - Serial Number—Serial number of the sensor.
- Update License—Specifies from where to obtain the new license key:
  - Cisco Connection Online—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 containing the license key is.

Button Functions:

- Download—Lets you download a copy of your license to the computer that IDM 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.

  The Download button is disabled unless you have a valid license on the sensor.
- Browse Local—Invokes a file browser to find the license key.
- Update License—Delivers a new license key to the sensor based on the selected option.

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. For more information, see Service Programs for IPS Products, page 1-20.

To obtain and install the license key, follow these steps:

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

Step 2 Choose **Configuration > Licensing**.

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 3 Obtain a license key by doing one of the following:

- Choose **Cisco Connection Online** to obtain the license from Cisco.com.

  IDM 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 4.

- Choose **License File** to use a license file.

  To use this option, you must apply for a license key at www.cisco.com/go/license.

  The license key is sent to you in e-mail and you save it to a drive that IDM can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.

Step 4 Click **Update License**.

The Licensing dialog box appears.

Step 5 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 Go to www.cisco.com/go/license.

Step 8 Fill in the required fields.

Caution You must have the correct IPS device serial number because the license key only functions on the device with that number.

Your license key is sent to the e-mail address you specified.

Step 9 Save the license key to a hard-disk drive or a network drive that the client running IDM can access.

Step 10 Log in to IDM.

Step 11 Choose **Configuration > Licensing**.

Step 12 Under Update License, choose **Update From: License File**.

Step 13 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

The Select License File Path dialog box appears.

Step 14 Browse to the license file and click **Open**.

Step 15 Click **Update License**.

CHAPTER 2

Setting Up the Sensor

This chapter describes how to set up the sensor, and contains the following sections:

Understanding Setup

After you have installed the sensor on your network, you must use the **setup** command to initialize it. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, Telnet server, web server port, access control lists, time settings, and assign and enable interfaces. After you have initialized the sensor, you can communicate with it over the network. You are then ready to configure intrusion prevention.

Caution You must initialize the sensor before you can use Configuration > Sensor Setup in IDM to further configure the sensor. For the procedure, see Initializing the Sensor, page 1-4.

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

Configuring Network Settings

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

Overview

Use the Network pane to specify network and communication parameters for the sensor.

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

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure network settings.

Field Definitions

The following fields and buttons are found on the Network pane.

Field Descriptions:

- Hostname—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—IP address of the sensor.

  The default is 10.1.9.201.
- Network Mask—Mask corresponding to the IP address.

  The default is 255.255.255.0.
- Default Route—Default gateway address.

  The default is 10.1.9.1.
- 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.
- Web Server Settings—Sets the web server security level and port.
  - Enable TLS/SSL—Enables TLS and SSL in the web server.

    The default is enabled. We strongly recommend that you enable TLS and SSL.
  - Web server port—TCP port used by the web server.

The default is 443 for HTTPS. You receive an error message if you enter a value out of the range of 1 to 65535.

- Remote Access—Enables the sensor for remote access.
  - 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.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Network Settings

To configure network settings, follow these steps:

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

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

The Network pane appears.

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 change the amount of FTP timeout, enter the new amount in the FTP Timeout field.

Step 8 To enable or disable TLS/SSL, check or uncheck Enable TLS/SSL.

Note We strongly recommend that you enable TLS/SSL.

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

Step 9 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 IDM. Use the format `https://`*sensor_ip_address:port_number* (for example, `https://10.1.9.201:1040`).

Step 10 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.

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

Step 11 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.

Configuring Allowed Hosts

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

Overview

Use the Allowed Hosts pane to specify hosts or networks that have permission to access the sensor.

Note After you use the **setup** command to initialize the sensor, the allowed hosts parameter values appear on the Allowed Hosts pane. If you need to change these parameters, you can do so from the Allowed Hosts pane.

By default, there are no entries in the list, and therefore no hosts are permitted until you add them.

Note You must add the management host, such as ASDM, IDM, IDS MC and the monitoring host, such as IDS Security Monitor, to the allowed hosts list, otherwise they will not be able to 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure allowed hosts and networks.

Field Definitions

This section lists the field definitions for allowed hosts, and contains the following topics:

- Allowed Hosts Pane, page 2-5
- Add and Edit Allowed Host Dialog Boxes, page 2-5

Allowed Hosts Pane

The following fields are found on the Allowed Hosts pane:

Field Descriptions:

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

Button Functions:

- Add—Opens the Add Allowed Host dialog box.

  From this dialog box, you can add a host or network to the list of allowed hosts.
- Edit—Opens the Edit Allowed Host dialog box.

  From this dialog box, you can change the values associated with this host or network.
- Delete—Removes this host or network from the list of allowed hosts.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Allowed Host Dialog Boxes

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

Field Descriptions:

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

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Allowed Hosts

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

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

Step 2 Choose **Configuration > Sensor Setup > Allowed Hosts**.

The Allowed Hosts pane appears.

Step 3 Click **Add** to add a host or network to the list.

The Add Allowed Host dialog box appears.

You can add a maximum of 512 allowed hosts.

Step 4 Enter the IP address of the host or network in the IP Address field.

You receive an error message if the IP address is already included as part of an existing list entry.

Step 5 Enter the network mask of the host or network in the Network Mask field or select a network mask from the drop-down list.

IDM 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.

Step 6 Click **OK**.

The new host or network appears in the allowed hosts list on the Allowed Hosts pane.

Step 7 To edit an existing entry in the allowed hosts list, select it, and click **Edit**.

The Edit Allowed Host dialog box appears.

Step 8 Edit the IP address of the host or network in the IP Address field.

Step 9 Edit the network mask of the host or network in the Network Mask field.

Step 10 Click **OK**.

The edited host or network appears in the allowed hosts list on the Allowed Hosts pane.

Step 11 To delete a host or network from the list, select it, and click **Delete**.

The host no longer appears in the allowed hosts list on the Allowed Hosts pane.

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

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

Step 12 Click **Apply** to apply your changes and save the revised configuration.

Configuring 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.

SSH authenticates the hosts or networks using one or more of the following:

- Password
- User RSA public key

SSH protects against the following:

- IP spoofing—A remote host sends out packets pretending to come from another trusted host.

  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.

Note SSH never sends passwords in clear text.

This section contains the following topics:

Defining Authorized Keys

This section describes how to define public keys, and contains the following topics:

Overview

Use the Authorized Keys pane to define public keys for a client allowed to use RSA authentication to log in to the local SSH server. The Authorized Keys pane displays the public keys of all SSH clients allowed to access the sensor.

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 SSH 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 Keys pane.

You can view only your key and not the keys of other users.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

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.

Field Definitions

This section lists the field definitions for authorized keys, and contains the following topics:

- Authorized Keys Pane, page 2-8
- Add and Edit Authorized Key Dialog Boxes, page 2-9

Authorized Keys Pane

The following fields and buttons are found on the Authorized Keys pane.

Field Descriptions:

- ID—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—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]*$.

Button Functions:

- Add—Opens the Add Authorized Key dialog box. From this dialog box, you can add a new authorized key.
- Edit—Opens the Edit Authorized Key dialog box. From this dialog box, you can change the values associated with this authorized key.
- Delete—Removes this authorized key from the list.

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Authorized Key Dialog Boxes

The following fields and buttons are found in the Add and Edit Authorized Key dialog boxes.

Field Descriptions:

- ID—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—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]*$.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Defining Authorized Keys

To define public keys, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > SSH > Authorized Keys**.

The Authorized Keys pane appears.

Step 3 Click **Add** to add a public key to the list.

The Add Authorized Key dialog box appears.

You can add a maximum 50 SSH authorized keys.

Step 4 Enter a unique ID to identify the key in the **ID** field.

Step 5 Enter an integer in the Modulus Length field.

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 5 through 7.

Step 6 Enter an integer in the Public Exponent field.

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 7 Enter a value in the Public Modulus field.

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 Key dialog box, click **Cancel**.

Step 8 Click **OK**.

The new key appears in the authorized keys list on the Authorized Keys pane.

Step 9 To edit an existing entry in the authorized keys list, select it, and click **Edit**.

The Edit Authorized Key dialog box appears.

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.

Step 11 Click **OK**.

The edited key appears in the authorized keys list on the Authorized Keys pane.

Step 12 To delete a public key from the list, select it, and click **Delete**.

The key no longer appears in the authorized keys list on the Authorized Keys pane.

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

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

Defining Known Host Keys

This section describes how to define known host keys, and contains the following topics:

Overview

Use the Known Host 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 Keys pane. If you cannot obtain the public key in the correct format, click **Retrieve Host Key** in the Add Known Host Keys dialog box.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to add or edit known host keys.

Field Definitions

This section lists the field definitions for known host keys, and contains the following topics:

- Known Host Keys Pane, page 2-11
- Add and Edit Known Host Key Dialog Boxes, page 2-12

Known Host Keys Pane

The following fields and buttons are found on the Known Host Keys pane.

Field Descriptions:

- IP Address—IP address of the host you are adding keys for.
- Modulus Length—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]*$.

Button Functions:

- Add—Opens the Add Known Host Key dialog box. From this dialog box, you can add a new known host key.
- Edit—Opens the Edit Known Host Key dialog box. From this dialog box, you can change the values associated with this known host key.
- Delete—Removes this known host key from the list.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Known Host Key Dialog Boxes

The following fields and buttons are found in the Add and Edit Known Host Key dialog boxes.

Field Descriptions:

- IP Address—IP address of the host you are adding keys for.
- Modulus Length—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]*$.

Button Functions:

- Retrieve Host Key—IDM attempts to retrieve the known host key from the host specified by the IP address. If successful, IDM populates the Add Known Host Key pane with the key.

  Available only in the Add dialog box. You receive an error message if the IP address is invalid.
- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Defining Known Host Keys

To define known host keys, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > SSH > Known Host Keys**.

The Known Host Keys pane appears.

Step 3 Click **Add** to add a known host key to the list.

The Add Known Host Key dialog box appears.

Step 4 Enter the IP address of the host you are adding keys for in the IP Address field.

Step 5 Click **Retrieve Host Key**.

The Device Manager 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 6 Enter an integer in the Modulus Length field.

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 7 Enter an integer in the Public Exponent field.

The RSA algorithm uses the public exponent to encrypt data.

Step 8 Enter a value in the Public Modulus field.

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 Key dialog box, click **Cancel**.

Step 9 Click **OK**.

The new key appears in the known host keys list on the Known Host Keys pane.

Step 10 To edit an existing entry in the authorized keys list, select it, and click **Edit**.

The Edit Authorized Key dialog box appears.

Step 11 Edit the Modulus Length, Public Exponent, and Public Modulus fields.

Caution You cannot modify the **ID** field after you have created an entry.

Step 12 Click **OK**.

The edited key appears in the known host keys list on the Known Host Keys pane.

Step 13 To delete a public key from the list, select it, and click **Delete**.

The key no longer appears in the known host keys list on the Known Host Keys pane.

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

Step 14 Click **Apply** to apply your changes and save the revised configuration.

Displaying and Generating the Sensor SSH Host Key

This section describes how to display and generate the Sensor SSH host key, and contains the following topics:

Overview

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 SSH host key the first time it starts up. It is displayed on the Sensor Key pane. Click **Generate Key** to replace that key with a new key.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to generate sensor SSH host keys.

Field Definitions

The Sensor Key pane displays the sensor SSH host key. The Generate Key button generates a new sensor SSH host key.

Displaying and Generating the Sensor SSH Host Key

To display and generate sensor SSH host keys, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > SSH > Sensor Key**.

The Sensor Key pane appears.

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?
```

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.

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.

Configuring Certificates

For more information on the sensor and certificates, see IDM and Certificates, page 1-15. This section contains the following topics:

Adding Trusted Hosts

This section describes how to add trusted hosts and contains the following topics:

Overview

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.

The Trusted Hosts pane lists all trusted host certificates that you have added. You can add certificates by entering an IP address. IDM 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to add trusted hosts.

Field Definitions

This section lists field definitions for trusted hosts, and contains the following topics:

Trusted Hosts Pane

The following fields and buttons are found on the Trusted Hosts pane.

Field Descriptions:

- IP Address—IP address of the trusted host.
- MD5—Message Digest 5 encryption.

  MD5 is an algorithm used to compute the 128-bit hash of a message.
- SHA1—Secure Hash Algorithm.

  SHA1 is a cryptographic message digest algorithm.

Button Functions:

- Add—Opens the Add Trusted Host dialog box. From this dialog box, you can add a new trusted host.
- View—Opens the View Trusted Host dialog box. From this dialog box, you can view the certificate data associated with this trusted host.
- Delete—Removes this trusted host from the list.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add Trusted Host Dialog Box

The following fields and buttons are found on the Add Trusted Host dialog box.

Field Descriptions:

- IP Address—IP address of the trusted host.
- Port—(Optional) specifies the port number of where to obtain the host certificate.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Adding Trusted Hosts

To add trusted hosts, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Certificate > Trusted Hosts**.

The Trusted Hosts pane appears.

Step 3 Click **Add** to add a trusted host to the list.

The Add Trusted Host dialog box appears.

Step 4 Enter the IP address of the trusted host you are adding in the IP Address field.

Step 5 Enter a port number in the **Port** field if the sensor is using a port other than 443.

Step 6 Click **OK**.

IDM retrieves the certificate from the host whose IP address you entered in Step 3. The new trusted host appears in the trusted hosts list on the Trusted Hosts pane.

A dialog box informs you that IDM is communicating with the sensor:

```
Communicating with the sensor, please wait ...
```

A dialog box provides status about whether IDM was successful in adding a trusted host:

```
The new host was added successfully.
```

Step 7 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. See Step 7. If you find any discrepancies, delete the trusted host immediately. See Step 8.

Step 8 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 9 Click **OK**.

Step 10 To delete a trusted host from the list, select it, and click **Delete**.

The trusted host no longer appears in the trusted hosts list on the Trusted Hosts pane.

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

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

Displaying and Generating the Server Certificate

This section describes how to display and generate a server certificate, and contains the following topics:

Overview

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to generate server certificates.

Field Definitions

The Server Certificate pane displays the sensor server X.509 certificate. Clicking Generate Certificate generates a new sensor X.509 certificate.

Displaying and Generating the Server Certificate

To display and generate the sensor server X.509 certificate, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Certificate > Server Certificate**.

The Server Certificate pane appears.

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?
```

Caution 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.

Step 4 Click **OK** to continue.

A new server certificate is generated and the old server certificate is deleted.

Configuring Time

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

- Configuring Time on the Sensor, page 2-23
- Correcting Time on the Sensor, page 2-24

Overview

Use the Time pane to configure the 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's time source.

Time Sources and the Sensor

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. For more information, see Initializing the Sensor, page 1-4.

Here is a summary of ways to set the time on sensors:

- For appliances
  - Use the **clock set** command to set the time. This is the default.

    For the procedure, refer to Manually Setting the Clock.
  - Use NTP

    You can configure the appliance to get its time from an NTP time synchronization source. For the procedure, refer to Configuring a Cisco Router to be an NTP Server. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can set up NTP on the appliance during initialization or you can configure NTP through the CLI, IDM, or ASDM.

    Note We recommend that you use an NTP time synchronization source.
- For IDSM-2
  - The IDSM-2 can automatically synchronize its clock with the switch time. This is the default.

    Note The UTC time is synchronized between the switch and the IDSM-2. The time zone and summertime settings are not synchronized between the switch and the IDSM-2.

Caution Be sure to set the time zone and summertime settings on both the switch and IDSM-2 to ensure that the UTC time settings are correct. The local time of IDSM-2 could be incorrect if the time zone and/or summertime settings do not match between IDSM-2 and the switch.

- Use NTP

  You can configure IDSM-2 to get its time from an NTP time synchronization source. For the procedure, refer to Configuring a Cisco Router to be an NTP Server. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure IDSM-2 to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

  Note We recommend that you use an NTP time synchronization source.

- For NM-CIDS
  - NM-CIDS can automatically synchronize its clock with the clock in the router chassis in which it is installed (parent router). This is the default.

    Note The UTC time is synchronized between the parent router and NM-CIDS. The time zone and summertime settings are not synchronized between the parent router and NM-CIDS.

Caution Be sure to set the time zone and summertime settings on both the parent router and NM-CIDS to ensure that the UTC time settings are correct. The local time of NM-CIDS could be incorrect if the time zone and/or summertime settings do not match between NM-CIDS and the router.

  - Use NTP

    You can configure NM-CIDS to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. For the procedure, refer to Configuring a Cisco Router to be an NTP Server. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure NM-CIDS to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

- For AIP-SSM:
  - AIP-SSM can automatically synchronize its clock with the clock in the ASA in which it is installed. This is the default.

    Note The UTC time is synchronized between ASA and AIP-SSM. The time zone and summertime settings are not synchronized between ASA and AIP-SSM.

Caution Be sure to set the time zone and summertime settings on both ASA and AIP-SSM to ensure that the UTC time settings are correct. The local time of AIP-SSM could be incorrect if the time zone and/or summertime settings do not match between AIP-SSM and ASA.

– Use NTP

You can configure AIP-SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. For the procedure, refer to Configuring a Cisco Router to be an NTP Server. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure AIP-SSM to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

Note We recommend that you use an NTP time synchronization source.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure time settings.

Field Definitions

This section lists the field definitions for time, and contains the following topics:

- Time Pane, page 2-21
- Configure Summertime Dialog Box, page 2-22

Time Pane

The following fields and buttons are found on the Time pane.

Field Descriptions:

- Sensor Local Date—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—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—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—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—IP address of the NTP server if you use this to set time on the sensor.
  - Key—NTP MD5 key type.
  - Key ID—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.
- Summertime—Lets you enable and configure summertime settings.
  - Enable Summertime—Click to enable summertime mode.

    The default is disabled.

Button Functions:

- Configure Summertime—Click to open the Configure Summertime dialog box.

  You can only open the Configure Summertime box if you have Enable Summertime selected.
- Apply—Applies your changes and saves the revised configuration.

  Apply is enabled if any other settings on the Time pane are modified (such as NTP, summertime, and standard time zone settings). Apply corresponds to all other fields on the Time pane except the date and time.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.
- Apply Time to Sensor—Sets the date and time on the sensor.

  Apply Time to Sensor is only enabled when you change the date and time. If you want the modified date and time to be saved to the sensor, you must click **Apply Time to Sensor**.

Configure Summertime Dialog Box

The following fields and buttons are found on the Configure Summertime dialog box.

Field Descriptions:

- Summer Zone Name—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—The number of minutes to add during summertime.

  The default is 60. If you select a predefined time zone, this field is populated automatically.

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

- Start Time—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—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—Duration is in recurring mode.
  - Date—Duration is in nonrecurring mode.
  - Start—Start week, day, and month setting.
  - End—End week, day, and month setting.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Time on the Sensor

To configure time on the sensor, follow these steps:

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

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

The Time pane appears.

Step 3 Under Date, choose the current date from the drop down boxes.

Date indicates the date on the local host.

Step 4 Under 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 will have the wrong time stamp. You must clear the events. For more information, see Correcting Time on the Sensor, page 2-24.

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

Step 5 Under Standard Time Zone:

a. Select a time zone from the drop down box in the Zone Name field or enter one that you have created.

This is the time zone to be displayed when summertime hours are not in effect.

b. Enter the offset in minutes from UTC in the UTC Offset field.

If you select 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:

a. The IP address of the NTP server in the IP Address field

b. The key of the NTP server in the Key field

c. 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 7 Under Summertime, check the **Enable Summertime** check box to enable daylight saving time.

Step 8 Click **Configure Summertime**.

The Configure Summertime dialog box appears.

Step 9 Select the Summer Zone Name from the drop down box or enter one that you have created.

This is the name to be displayed when daylight saving time is in effect.

Step 10 Enter the number of minutes to add during summertime.

If you select a predefined summer zone name, this field is automatically populated.

Step 11 Enter the time to apply summertime settings in the Start Time field.

Step 12 Enter the time to remove summertime settings in the End Time field.

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—Select the Start and End times from the drop down boxes.

The default is the first Sunday in April and the last Sunday in October.

b. Date—Select the Start and End time from the drop down boxes.

The default is January 1 for the start and end time.

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 (Steps 1 and 2), you must also click **Apply Time to Sensor** to save the time and date settings on the sensor.

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. For more information on the **clear events** command refer to Clearing Events from Event Store.

Caution You cannot remove individual events.

Configuring Users

This section describes how to add and remove users on the system, and contains the following topics:

Overview

IDM permits multiple users 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.

There are four user roles:

- Viewers—Can view configuration and events, but cannot modify any configuration data except their user passwords.
- Operators—Can view everything and can modify the following options:
  - Signature tuning (priority, disable or enable)
  - Virtual sensor definition
  - Managed routers
  - Their user passwords
- Administrators—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 IDM. The service user logs in to a bash shell rather than the CLI.

Note 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.

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 new password if the Administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to add and edit users.

Field Definitions

This section lists the field definitions for users, and contains the following topics:

- Users Pane, page 2-27
- Add and Edit User Dialog Boxes, page 2-27

Users Pane

The following fields and buttons are found on the Users pane.

Field Descriptions:

- Username—The username.

  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.
- Role—The user role.

  The values are Administrator, Operator, Service, and Viewer. The default is Viewer.
- Status—Displays the current user account status, such as active, expired, or locked.

Button Functions:

- Add—Opens the Add User dialog box. From this dialog box, you can add a user to the list of users.
- Edit—Opens the Edit User dialog box. From this dialog box, you can edit a user in the list of users. Delete—Removes this user from the list of users.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit User Dialog Boxes

The following fields and buttons are found in the Add and Edit User dialog boxes.

Field Descriptions:

- Username—The username.

  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.
- User Role—The user role.

  Valid values are Administrator, Operator, Service, and Viewer. The default is Viewer.
- Password—The user password.

  The password must contain a minimum of eight characters. All characters except space are allowed.
- 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 user's password.

  Only available in the Edit dialog box.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Users

To configure users on the sensor, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Users**.

The Users pane appears.

Step 3 Click **Add** to add a user.

The Add User dialog box appears.

Step 4 Enter the user name in the Username field.

Step 5 Select one of the following user roles from the drop-down list in the User Role field:

- Administrator
- Operator
- Viewer
- Service

Step 6 Enter the new password for that user in the Password field.

Step 7 Confirm the new password for that user in the Confirm Password field.

Step 8 Click **OK**.

The new user appears in the users list on the Users pane.

Step 9 To edit a user, select the user in the users list, and click **Edit**.

The Edit User dialog box appears.

Step 10 Check the **Change the password to access the sensor** check box.

Step 11 Make any changes you need to in the User Role and Password fields.

Step 12 Click **OK**.

The edited user appears in the users list on the Users 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 on the User pane.

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

Step 14 Click **Apply** to apply your changes and save the revised configuration.

CHAPTER 3

Configuring Interfaces

This chapter describes the various interface modes and how to configure interfaces on the sensor. It contains the following sections:

Understanding Interfaces

The command and control interface is permanently mapped to a specific physical interface, which depends on the type of sensor you have. You can configure the sensing interfaces to operate in promiscuous mode, inline interface mode, or inline VLAN pair mode. For sensors that support inline interface mode, you can pair the sensing interfaces into logical interfaces called “inline pairs.” For sensors that support VLANS, you can pair the VLANs into inline VLAN pairs. You must enable the interfaces, interface pairs, or VLAN pairs before the sensor can monitor traffic.

Note On appliances, the sensing interfaces are disabled by default. On modules, the sensing interfaces are always enabled and cannot be disabled.

With the addition of the inline VLAN pair feature, each sensing interface operates in one of three possible modes at any time: promiscuous, inline interface, or inline VLAN pair. On sensors with multiple sensing interfaces, any combination of modes are allowed on the same sensor:

- A sensing interface is in inline interface mode if it is paired with another sensing interface in an inline interface pair and its subinterface type is set to none (the default).
- A sensing interface is in inline VLAN pair mode if its subinterface type is set to inline VLAN pair.
- A sensing interface is in promiscuous mode by default, that is, if it is not in either of the other modes.

The sensing interface does not have an IP address assigned to it and is therefore invisible to attackers. This lets the sensor monitor the data stream without letting attackers know they are being watched. Promiscuous mode is contrasted by inline interface mode where all packets entering or leaving the network must pass through the sensor. For more information, see Understanding Promiscuous Mode, page 3-2, Understanding Inline Interface Mode, page 3-3, and Understanding Inline VLAN Pair Mode, page 3-3.

The sensor only monitors traffic on interfaces, inline interface pairs, and inline VLAN pairs that are assigned to the default virtual sensor. For more information, see Assigning Interfaces to the Virtual Sensor, page 4-3.

To configure the sensor so that traffic continues to flow through inline pairs even when SensorApp is not running, you can enable bypass mode. Bypass mode minimizes dataflow interruptions during reconfiguration, service pack installation, or software failure.

The sensor detects the interfaces of modules that have been installed while the chassis was powered off. You can configure them the next time you start the sensor. If a module is removed, the sensor detects the absence of the interfaces the next time it is started. Your interface configuration is retained, but the sensor ignores it if the interfaces are not present.

The following interface configuration events are reported as status events:

- Link up or down
- Traffic started or stopped
- Bypass mode auto activated or deactivated
- Missed packet percentage threshold exceeded

Understanding Promiscuous Mode

In promiscuous mode, packets do not flow through the IPS. 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 IPS 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, for atomic attacks, however, 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).

Understanding Inline Interface Mode

Operating in inline interface 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 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 AIP-SSM to operate inline even though it has 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.

Understanding Inline VLAN Pair Mode

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 pairs are supported on all sensors that are compatible with IPS 5.1 except NM-CIDS, AIP-SSM-10, and AIP-SSM-20.

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 any packets received on the VLAN that are not assigned to an inline VLAN pair.

Interface Support

Table 3-1 describes the interface support for appliances and modules running IPS 5.1:

Table 3-1 Interface Support

Base Chassis	Added PCI Cards	Interfaces Supporting Inline	Possible Port Combinations	Interfaces Not Supporting Inline
IDS-4210	—	None	N/A	All
IDS-4215	—	None	N/A	All
IDS-4215	4FE	FastEthernet0/1 4FE FastEthernetS/0[1] FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3 0/1<->1/0 0/1<->1/1 0/1<->1/2 0/1<->1/3	FastEthernet0/0
IDS-4235	—	None	N/A	All
IDS-4235	4FE	4FE FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4235	TX (GE)	TX onboard + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 or GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	—	None	N/A	All
IDS-4250	4FE	4FE FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4250	TX (GE)	TX onboard + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 or GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	SX	None	N/A	All
IDS-4250	SX + SX	2 SX GigabitEthernet1/0 GigabitEthernet2/0	1/0<->2/0	GigabitEthernet0/0 GigabitEthernet0/1

Table 3-1 Interface Support (continued)

Base Chassis	Added PCI Cards	Interfaces Supporting Inline	Possible Port Combinations	Interfaces Not Supporting Inline
IDS-4250	XL	2 SX of the XL GigabitEthernet2/0 GigabitEthernet2/1	2/0<->2/1	GigabitEthernet0/0 GigabitEthernet0/1
IDSM-2	—	port 7 and 8 GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2
IPS-4240	—	4 onboard GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS-4255	—	4 onboard GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS-4260	—	4 onboard GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
NM-CIDS	—	None	N/A	All
AIP-SSM-10	—	GigabitEthernet0/1	By security context	GigabitEthernet0/0
AIP-SSM-20	—	GigabitEthernet0/1	By security context	GigabitEthernet0/0

1. The 4FE card can be installed in either slot 1 or 2. S indicates the slot number, which can be either 1 or 2.

Interface Configuration Restrictions

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
  - On modules (IDSM-2, NM-CIDS, AIP-SSM-10, and AIP-SSM-20) and IPS-4240, IPS-4255, and IPS-4260 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 fiber interfaces (1000-SX and XL on the IDS-4250), valid speed settings are 1000 Mbps and auto.

  - For Gigabit copper interfaces (1000-TX on the IDS-4235, IDS-4250, IPS-4240, IPS-4255, and IPS-4260), 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 officially supported. For more information, see Interface Support, page 3-4.
  - 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**.
- Inline VLAN Pairs
  - You cannot pair a VLAN with itself.
  - 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.
- 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.

    Note The exception to this restriction is the IDSM-2. The alternate TCP reset interface assignments for both sensing interfaces is System0/1 (protected).

Understanding Hardware Bypass

In addition to IPS 5.1 software bypass, IPS-4260 also supports hardware bypass.

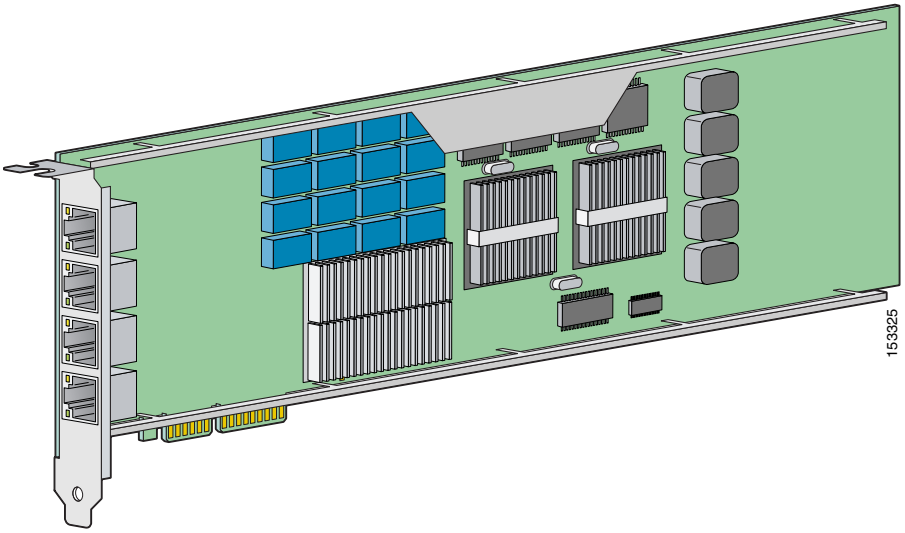
This section describes the 4GE bypass interface card and its configuration restrictions. For the procedure for installing and removing PCI cards, refer to Installing and Removing PCI Cards.

This section contains the following topics:

4GE Bypass Interface Card

IPS-4260 supports the 4-port GigabitEthernet card (part number IPS-4GE-BP-INT=) with hardware bypass. This 4GE bypass interface card supports hardware bypass only between ports 0 and 1 and between ports 2 and 3. Figure 3-1 shows the 4GE bypass interface card.

Figure 3-1 4GE Bypass Interface Card



Hardware bypass complements the existing software bypass feature in IPS 5.1. For more information on software bypass mode, see Configuring Bypass Mode, page 3-20. The following conditions apply to hardware bypass and software bypass on IPS-4260:

- When bypass is set to OFF, software bypass is not active.

  For each inline interface for which hardware bypass is available, the component interfaces are set to disable the fail-open capability. If SensorApp fails, the sensor is powered off, reset, or if the NIC interface drivers fail or are unloaded, the paired interfaces enter the fail-closed state (no traffic flows through inline interface or inline VLAN subinterfaces).

- When bypass is set to ON, software bypass is active.

  Software bypass forwards packets between the paired physical interfaces in each inline interface and between the paired VLANs in each inline VLAN subinterface. For each inline interface on which hardware bypass is available, the component interfaces are set to standby mode. If the sensor is

powered off, reset, or if the NIC interfaces fail or are unloaded, those paired interfaces enter fail-open state in hardware (traffic flows unimpeded through inline interface). Any other inline interfaces enter fail-closed state.

- When bypass is set to AUTO (traffic flows without inspection), software bypass is activated if sensorApp fails.

  For each inline interface on which hardware bypass is available, the component interfaces are set to standby mode. If the sensor is powered off, reset, or if the NIC interfaces fail or are unloaded, those paired interfaces enter fail-open state in hardware. Any other inline interfaces enter the fail-closed state.

Note To test fail-over, set the bypass mode to ON or AUTO, create one or more inline interfaces and power down the sensor and verify that traffic still flows through the inline path.

Hardware Bypass Configuration Restrictions

To use the hardware bypass feature on the 4GE bypass interface card, you must pair interfaces to support the hardware design of the card. If you create an inline interface that pairs a hardware-bypass-capable interface with an interface that violates one or more of the hardware-bypass configuration restrictions, hardware bypass is deactivated on the inline interface and you receive a warning message similar to the following:

```
Hardware bypass functionality is not available on Inline-interface pair0.
Physical-interface GigabitEthernet1/0 is capable of performing hardware bypass only when
paired with GigabitEthernet1/1, and both interfaces are enabled and configured with the
same speed and duplex settings.
```

The following configuration restrictions apply to hardware bypass:

- The 4-port bypass card is only supported on IPS-4260.
- Fail-open hardware bypass only works on inline interfaces (interface pairs), not on inline VLAN pairs.
- Fail-open hardware bypass is available on an inline interface if all the following conditions are met:
  - Both of the physical interfaces support hardware bypass.
  - Both of the physical interfaces are on the same interface card.
  - The two physical interfaces are associated in hardware as a bypass pair.
  - The speed and duplex settings are identical on the physical interfaces.
  - Both of the interfaces are administratively enabled.
- Autonegotiation must be set on MDI/X switch ports connected to IPS-4260.

  You must configure both the sensor ports and the switch ports for autonegotiation for hardware bypass to work. The switch ports must support MDI/X, which automatically reverses the transmit and receive lines if necessary to correct any cabling problems. The sensor is only guaranteed to operate correctly with the switch if both of them are configured for identical speed and duplex, which means that the sensor must be set for autonegotiation too.

Summary

This section describes the Summary pane, and contains the following topics:

Overview

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 pair mode, or inline VLAN pair mode, but you cannot configure an interface in a combination of these modes.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

Field Definitions

The following fields and buttons are found on the Summary pane.

Field Descriptions:

- Name—Name of the interface.

  The values are FastEthernet or GigabitEthernet for promiscuous interfaces. For inline interfaces, the name is whatever you assigned to the pair.
- Details—Tells you whether the interface is promiscuous or inline and whether there are VLAN pairs.
- Description—Your description of the interface.
- Assigned Virtual Sensor—Whether the interface or interface pair has been assigned to the virtual sensor, vs0.

Configuring Interfaces

Note For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see Interface Configuration Restrictions, page 3-5.

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

Overview

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 on the Interfaces pane.

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 the default virtual sensor, vs0, and enabled the interface or inline pair. If you need to change your interfaces settings, you can do so on the Interfaces pane.To assign the interface or inline pair to the virtual sensor, vs0, in the Edit Virtual Sensor dialog box, choose **Configuration > Analysis Engine > Virtual Sensor > Edit**.

TCP Reset Interfaces

This section explains the TCP reset interfaces and when to use them. It contains the following topics:

Understanding Alternate TCP Reset

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.

Note 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.

  Note Taps do not allow incoming traffic from the sensor.

  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.

Designating the 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.

  Note 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.

  Note Taps do not permit incoming traffic from the sensor.

  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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to edit the interfaces on the sensor.

Field Definitions

This section lists the field definitions for interfaces, and contains the following topics:

Interfaces Pane

The following fields and buttons are found on the Interfaces pane.

Field Descriptions:

- Interface Name—Name of the interface.

  The values are FastEthernet or GigabitEthernet for all interfaces.
- Enabled—Whether or not the interface is enabled.
- 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 parent chassis' backplane.
- 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).
- 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.
- Description—Lets you provide a description of the interface.

Button Functions:

- Select All—Lets you select all entries in the list.
- Edit—Opens the Edit Interface dialog box. From this dialog box, you can change some of the values associated with this interface.
- Enable—Enables this interface.
- Disable—Disables this interface.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Edit Interface Dialog Box

The following fields and buttons are found in the Edit Interface dialog box.

Field Descriptions:

- Interface Name—Name of the interface.

  The values are FastEthernet or GigabitEthernet for all interfaces.
- Description—Lets you provide a description of the interface.
- 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 parent chassis' backplane.
- Enabled—Whether or not the interface is enabled.
- 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).
- Use 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.
  - Select Interface—Sets the interface that will send the TCP reset.

    For more information on the alternate TCP reset interface, see TCP Reset Interfaces, page 3-10.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Interfaces

To enable or disable the interface or edit its settings, follow these steps:

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

Step 2 Choose **Configuration > Interface Configuration > Interfaces**.

The Interfaces pane appears.

Step 3 Select the row or double-click it and then click **Enable**.

The interface is enabled. To have the interface monitor traffic, it must also be assigned to a virtual sensor. For the procedure, see Assigning Interfaces to the Virtual Sensor, page 4-3.

Step 4 To edit some of the values associated with the interface, select the interface, and then click **Edit**.

The Edit Interface dialog box appears.

Step 5 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 **Use Alternative TCP Reset Interface** check box.

Step 6 Click **OK**.

The changes appear in the list on the Interfaces pane.

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

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Configuring Inline Interface Pairs

Note For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see Interface Configuration Restrictions, page 3-5.

This section describes how to set up inline interface pairs, and contains the following topics:

Overview

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

Note AIP-SSM does not need an inline pair for monitoring. You only need to add the physical interface to the virtual sensor.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure interface pairs.

Field Definitions

This sections lists field definitions for interface pairs, and contains the following topics:

- Interface Pairs Pane, page 3-15
- Add and Edit Interface Pair Dialog Boxes, page 3-16

Interface Pairs Pane

The following fields and buttons are found on the Interface Pairs pane.

Field Descriptions:

- Interface Pair Name—The name you give the interface pair.
- Paired Interfaces—The two interfaces that you have paired (for example, GigabitEthernet0/0<->GigabitEthernet0/1).
- Description—Lets you add a description of this interface pair.

Button Functions:

- Select All—Selects all interface pairs.
- Add—Opens the Add Interface Pair dialog box. From this dialog box, you can add an interface pair.
- Edit—Opens the Edit Interface Pair dialog box. From this dialog box, you can edit the values of the interface pair.
- Delete—Deletes the selected interface pair.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Interface Pair Dialog Boxes

The following fields and buttons are found in the Add and Edit Interface Pair dialog boxes.

Field Descriptions:

- Interface Pair Name—The name you give the interface pair.
- Select two interfaces—Select two interfaces from the list to pair (for example, GigabitEthernet0/0<->GigabitEthernet0/1).
- Description—Lets you add a description of this interface pair.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Inline Interface Pairs

To configure inline interface pairs, follow these steps:

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

Step 2 Choose **Configuration > Interface Configuration > Interface Pairs**.

The Interface Pairs pane appears.

Step 3 Click **Add** to add inline interface pairs.

The Add Interface Pair dialog box appears.

Step 4 Enter a name in the Interface Pair Name field.

The inline interface name is a name that you create.

Step 5 Select two interfaces to form a pair in the Select two interfaces field.

For example, GigabitEthernet0/0 and GigabitEthernet0/1.

Step 6 You can add a description of the inline interface pair in the Description field if you want to.

Step 7 Click **OK**.

The new inline interface pair appears in the list on the Interface Pairs pane.

Step 8 To edit an inline interface pair, select it, and click **Edit**.

The Edit Interface Pair dialog box appears.

Step 9 You can change the name, choose a new inline interface pair, or edit the description.

Step 10 Click **OK**.

The edited inline interface pair appears in the list on the Interface Pairs pane.

Step 11 To delete an inline interface pair, select it, and click **Delete**.

The inline interface pair no longer appears in the list on the Interface Pairs pane.

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

Step 12 Click **Apply** to apply your changes and save the revised configuration.

Configuring Inline VLAN Pairs

Note For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see Interface Configuration Restrictions, page 3-5.

This section describes how to configure inline VLAN pairs, and contains the following topics:

Overview

The VLAN Pairs pane displays the existing inline VLAN pairs for each physical interface. Click **Add** 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 the 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. 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 If your sensor does not support inline VLAN pairs, the VLAN Pairs pane is not displayed. AIP-SSM and NM-CIDS do not support inline VLAN pairs.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure inline VLAN pairs.

Field Definitions

This sections lists field definitions for inline VLAN pairs, and contains the following topics:

- VLAN Pairs Pane, page 3-18
- Add and Edit VLAN Pair Dialog Boxes, page 3-19

VLAN Pairs Pane

The following fields and buttons are found on the Interface Pairs pane.

Field Descriptions:

- Interface Name—Name of the inline VLAN pair.
- Subinterface (VLAN Pair)—Subinterface number of the inline VLAN pair.

  The value is 1 to 255.
- VLAN1—Displays the VLAN number for VLAN1.

  The value is 1 to 4095.
- VLAN2—Displays the VLAN number for VLAN2.

  The value is 1 to 4095.
- Description—Your description of the inline VLAN pair.

Button Functions:

- Select All—Selects all VLAN pairs.
- Add—Opens the Add VLAN Pair dialog box. From this dialog box, you can add a VLAN pair.
- Edit—Opens the Edit VLAN Pair dialog box.

  From this dialog box, you can edit the values of the VLAN pair.
- Delete—Deletes the selected VLAN pair.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit VLAN Pair Dialog Boxes

The following fields and buttons are found on the Add and Edit Inline VLAN Pair dialog boxes:

Field Descriptions:

Note You cannot pair a VLAN with itself.

- Interface Name—Lets you choose the available interface to make an inline VLAN pair.
- Subinterface Number—Lets you assign a subinterface number.
  You can assign a number from 1 to 255.
- VLAN 1—Lets you specify the first VLAN for this inline VLAN pair.
  You can assign any VLAN from 1 to 4095.
- VLAN 2—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 The subinterface number and the VLAN numbers should be unique to each physical interface.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Inline VLAN Pairs

To configure inline VLAN pairs, follow these steps:

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

Step 2 Choose **Configuration > Interface Configuration > VLAN Pairs**.
The VLAN Pairs pane appears.

Step 3 Click **Add** to add inline VLAN pairs.
The Add Inline VLAN Pair dialog box appears.

Step 4 Select an interface from the Interface Name list.

Step 5 Enter a subinterface number (1 to 255) for the inline VLAN pair in the Subinterface Number field.

Step 6 Specify the first VLAN (1 to 4095) for this inline VLAN pair in the VLAN 1 field.

Step 7 Specify the other VLAN (1 to 4095) for this inline VLAN pair in the VLAN 2 field.

Step 8 You can add a description of the inline VLAN pair in the Description field if you want to.

Step 9 Click **OK**.
The new inline VLAN pair appears in the list on the VLAN Pairs pane.

Step 10 To edit an inline VLAN pair, select it, and click **Edit**.

The Edit Inline VLAN Pair dialog box appears.

Step 11 You can change the subinterface number, the VLAN numbers, or edit the description.

Step 12 Click **OK**.

The edited VLAN pair appears in the list on the VLAN Pairs pane.

Step 13 To delete a VLAN pair, select it, and click **Delete**.

The VLAN pair no longer appears in the list on the VLAN Pairs pane.

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

Step 14 Click **Apply** to apply your changes and save the revised configuration.

Configuring Bypass Mode

Note For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see Interface Configuration Restrictions, page 3-5.

This section describes how to configure bypass mode, and contains the following topics:

Overview

You can use the bypass mode as a diagnostic tool and a failover protection mechanism. You can set the sensor in a mode where all the IPS processing subsystems are bypassed and traffic is permitted to flow between the inline pairs directly. The bypass mode ensures that packets continue to flow through the sensor when the sensor's processes are temporarily stopped for upgrades or when the sensor's monitoring processes fail. There are three modes: on, off, and automatic. By default, bypass mode is set to automatic.

Note Bypass mode was originally intended to only be applicable to inline-paired interfaces. Because of a defect, it does affect promiscuous mode. A future version may address this defect. We recommend you configure bypass mode to automatic or off for promiscuous mode and not use the on mode.

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.

Note Bypass mode only functions when the operating system is running. If the sensor is powered off or shut down, bypass mode does not work—traffic is not passed to the sensor.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure bypass mode on the sensor.

Field Definitions

The following fields and buttons are found on the Bypass pane.

Field Descriptions:

- Auto—Traffic flows through the sensor for inspection unless the sensor's monitoring process is down.

  If the sensor's monitoring process 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 sensor's monitoring process is down, traffic stops flowing. This means that inline traffic is always inspected.
- On—Traffic bypasses the SensorApp and is not inspected. This means that inline traffic is never inspected.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Traffic Flow Notifications

This section describes how to configure traffic flow notifications, and contains the following topics:

Overview

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

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure traffic flow notifications.

Field Definitions

The following fields and buttons are found on the Traffic Flow Notifications pane.

Field Descriptions:

- Missed Packets Threshold—The percentage of packets that must be missed during a specified time before a notification is sent.
- Notification Interval—The interval the sensor checks for the missed packets percentage.
- Interface Idle Threshold—The number of seconds an interface must be idle and not receiving packets before a notification is sent.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Traffic Flow Notifications

To configure traffic flow notification, follow these steps:

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

Step 2 Choose **Configuration > Interface Configuration > Traffic Flow Notifications**.

The Traffic Flow Notifications pane appears.

Step 3 Choose the percent of missed packets that has to occur before you want to receive notification and enter that amount in the Missed Packets Threshold field.

Step 4 Choose the amount of seconds that you want to check for the percentage of missed packets and enter that amount in the Notification Interval field.

Step 5 Choose the amount of seconds that you will allow an interface to be idle and not receiving packets before you want to be notified and enter that in the Interface Idle Threshold field.

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

Step 6 Click **Apply** to apply your changes and save the revised configuration.

CHAPTER 4

Analysis Engine

This chapter explains the function of Analysis Engine and how to assign interfaces to the virtual sensor. It contains the following sections:

Understanding Analysis Engine

Analysis Engine performs packet analysis and alert detection. It monitors traffic that flows through specified interfaces and interface pairs.

Configuring the Virtual Sensor

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

Overview

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 and from behind the firewall. IPS 5.1 only supports one virtual sensor, so a single sensor policy and configuration are applied to all monitored data streams.

Be aware of the following limitation when adding interfaces to the sensor—the same traffic flow cannot traverse the sensor twice either through the same interface in inline mode or through separate monitored interfaces. If packets from the same traffic flow traverse the sensor twice, the virtual sensor interprets the packets as duplicates, which results in false positive alerts.

You can configure NAT to change the IP address to handle this limitation. NAT causes the sensor to treat the before and after translation packets as separate flows. For example, if a firewall is using NAT from its internal to external networks, the sensor can monitor both of these networks without problem.

You can assign interfaces, interface pairs, and VLAN pairs to the virtual sensor and you can change the description of the virtual sensor, but you cannot add a virtual sensor or change the virtual sensor name.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the virtual sensor.

Field Definitions

This section lists the field definitions for the virtual sensor, and contains the following topics:

- Virtual Sensor Pane, page 4-2
- Edit Virtual Sensor Dialog Box, page 4-2

Virtual Sensor Pane

The following fields and buttons are found on the Virtual Sensor pane.

Field Descriptions:

- Name—The Name of the virtual sensor.

  There is only one virtual sensor in IPS 5.1 and it is named vs0.
- Assigned Interfaces (or Pairs)—The interfaces or interface pairs that belong to this virtual sensor.
- Description—The description of the virtual sensor.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Edit Virtual Sensor Dialog Box

The following fields and buttons are found in the Edit Virtual Sensor dialog box.

Field Descriptions:

- Virtual Sensor Name—The name of the virtual sensor.

  There is only one virtual sensor in IPS 5.1 and it is named vs0.
- Description—The description of the virtual sensor.

- Assign Interfaces—Lets you assign the interfaces to the virtual sensor.
  - Name—The list of available interfaces or interface pairs that you can assign to the virtual sensor.
  - Details—Lists the mode (inline or promiscuous) of the interface and the interfaces of the inline pairs.
  - Assigned—Whether the interfaces or interface pairs have been assigned to the virtual sensor.

Button Functions:

- Select All—Lets you select all of the interfaces in the list.
- Assign—Adds the selected interface or interface pair to the Assigned Interfaces (or Pairs) list.
- Remove—Removes the selected interface or interface pair from the Assigned Interfaces (or Pairs) list.

Assigning Interfaces to the Virtual Sensor

To assign or remove an interface, inline interface pair, or inline VLAN pair from the virtual sensor, follow these steps:

Note You must assign all interfaces to the virtual sensor and enable them before they can monitor traffic. For the procedures for enabling sensor interfaces, see Chapter 3, "Configuring Interfaces."

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Click **Configuration > Analysis Engine > Virtual Sensor**.

The Virtual Sensor pane appears.

Step 3 Click **Edit**.

The Edit Virtual Sensor dialog box appears.

Step 4 To assign an interface, inline interface pair, or inline VLAN pair to the virtual sensor, select it in the Available Interfaces (or Pairs) list, and click **Add**.

Step 5 To remove an interface, inline interface pair, or inline VLAN pair from the virtual sensor, select it from the Assigned Interfaces (or Pairs) list, and click **Remove**.

Step 6 To change the description from "default virtual sensor," enter a new description in the Description field.

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

Step 7 Click **OK**.

The interface appears in the list on the Virtual Sensor pane.

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

Step 8 Click **Apply** to apply your changes and save the revised configuration.

Configuring Global Variables

This section describes how to configure global variables, and contains the following topics:

Overview

You can configure global variables inside the analysis engine component. There is only one global variable: Maximum Open IP Log Files.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure global variables.

Field Definitions

The following fields and buttons are found on the Global Variables pane.

Field Descriptions:

- Maximum Open IP Log Files—Maximum number of concurrently open IP log files.

  The valid range is from 20 to 100. The default is 20.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

CHAPTER 5

Defining Signatures

This chapter explains how to configure signatures. It contains the following sections:

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 sensor's event store. 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.

IPS 5.1 contains over 1000 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.

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.

Configuring Signature Variables

This section describes how to create signature variables, and contains the following topics:

Overview

When you want to use the same value within multiple signatures, use a variable. When you change the value of a variable, the variables in all signatures are updated. 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 choose 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure signature variables.

Field Definitions

This section lists the field definitions for signature variables, and contains the following topics:

Signature Variables Pane

The following fields and buttons are found in the Signature Variables pane.

Field Descriptions:

- 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.

  To designate multiple port numbers for a single variable, place a comma between the entries. For example, 80, 3128, 8000, 8010, 8080, 8888, 24326.

Button Functions:

- Add—Opens the Add Signature Variable dialog box. From this dialog box, you can add a new variable and specify the values associated with that variable.
- Edit—Opens the Edit Signature Variable dialog box. From this dialog box, you can change the values associated with this variable.
- Delete—Removes the selected variable from the list of available variables.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Signature Variable Dialog Boxes

The following fields and buttons are found in the Add and Edit Signature Variable dialog boxes.

Field Descriptions:

- 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.

  To designate multiple port numbers for a single variable, place a comma between the entries. For example, 80, 3128, 8000, 8010, 8080, 8888, 24326.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Signature Variables

To configure signature variables, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Variables**.

The Signature Variables pane appears.

Step 3 Click **Add** to create a variable.

The Add Signature Variable dialog box appears.

Step 4 Type the name of the signature variable in the Name field.

Note A valid name can only contain numbers or letters. You can also use a hyphen (-) or underscore (_).

Step 5 Type the value into the Value field for the new signature variable.

Note You can use commas as delimiters. Make sure there are no trailing spaces after the comma. Otherwise, you receive a `Validation failed` error.

WEBPORTS 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.

Step 6 Click **OK**.

The new variable appears in the signature variables list in the Signature Variables pane.

Step 7 To edit an existing variable, select it in the signature variables list, and then click **Edit**.

The Edit Signature Variable dialog box appears for the variable that you chose.

Step 8 Make any necessary changes to the Value field.

Step 9 Click **OK**.

The edited variable appears in the signature variables list in the Signature Variables pane.

Step 10 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 in the Signature Variables pane.

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

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

Configuring Signatures

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

Overview

You can perform the following tasks in the Signature Configuration pane:

- Sort and view all signatures stored on the sensor.

  You can sort by attack type, protocol, service, operating system, action to be performed, engine, signature ID, or signature name.
- View the MySDN information about the selected signature.

  The MySDN pages list the key attributes, a description, any benign triggers, and any recommended filters for the selected signature.
- Edit (tune) an existing signature to change the value(s) associated with the parameter(s) for that signature.
- Create a signature, either by cloning an existing signature and using the parameters of that signature as a starting point for the new signature, or by adding a new signature from scratch.

  You can also use the Custom Signature Wizard to create a signature. The wizard guides you through the parameters that you must choose to configure a custom signature, including selection of the appropriate signature engine.
- Enable or disable an existing signature.
- Restore the factory defaults to the signature.
- Delete a custom signature.

  You cannot delete built-in signatures.
- Activate or retire an existing signature.
- Assign actions to a signature.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure signatures.

Field Definitions

This section lists the field definitions for configuring signatures, and contains the following topics:

Signature Configuration Pane

The following fields and buttons are found in the Signature Configuration pane.

Field Descriptions:

- Select By—Lets you sort the list of signatures by selecting an attribute to sort on, such as protocol, service, or action.
- Select Criteria—Lets you further sort within a category by selecting a specific class within that category.

  For example, if you choose to sort by protocol, you can choose L2/L3/L4 protocol and view only signatures that are related to L2/L3/L4 protocol.
- Sig ID—Identifies the unique numerical value assigned to this signature.

  This value lets the sensor identify a particular signature.
- SubSig ID—Identifies the unique numerical value assigned to this subsignature.

  A SubSig ID is used to identify a more granular version of a broad 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.
- Action—Identifies the actions the sensor will take when this signature fires.
- 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 RR 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 signature's severity level is high
- Severity Factor = 75 if signature's severity level is medium
- Severity Factor = 50 if signature's severity level is low
- Severity Factor = 25 if signature's severity level is informational

- 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.

Button Functions:

- Select All—Selects all signatures.
- MySDN Link—Opens the MySDN page for the selected signature.

  The MySDN pages lists the key attributes, a description, any benign triggers, and any recommended filters for the selected signature.
- Add—Opens the Add Signature dialog box. You can create a signature by selecting the appropriate parameters.
- Clone—Opens the Clone Signature dialog box. You can create a signature by changing the prepopulated values of the existing signature you chose to clone.
- Edit—Opens 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.
- Enable—Enables the selected signature.
- Disable—Disables the selected signature.
- Actions—Displays the Assign Actions dialog box.
- Restore Defaults—Returns all parameters to the default settings for the selected signature.
- Delete—Deletes the selected custom signature.

  You cannot delete built-in signatures.
- Activate—Activates the selected signature if the signature is retired.

  This process can take some time because the sensor has to add the signature back to the appropriate signature engine and reconstruct the signature engine.
- Retire—Retires the selected signature and removes it from the signature engine.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously saved value.

Add Signatures Dialog Box

The following fields and buttons are found in the Add Signature dialog box:

Field Descriptions:

- 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. A subsignature ID is used to identify 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.
- Sig Description—Lets you specify the following attributes that help you distinguish this signature from other signatures:
  - Signature Name—Name your signature. The default is MySig.
  - Alert Notes—Add alert notes in this field.
  - User Comments—Add your comments about this signature in this field.
  - Alarm Traits—Add the alarm trait in this field. The value is 0 to 65535. The default is 0.
  - Release—Add the software release in which the signature first appeared.
- Engine—Lets you choose the engine that parses and inspects the traffic specified by this signature.
  - AIC FTP—Inspects FTP traffic and lets you control the commands being issued.
  - AIC HTTP—Provides granular control over HTTP sessions to prevent abuse of the HTTP protocol.
  - Atomic ARP—Inspects Layer-2 ARP protocol. The Atomic ARP engine is different because most engines are based on Layer-3-IP.
  - Atomic IP—Inspects IP protocol packets and associated Layer-4 transport protocols.
  - Flood Host—Detects ICMP and UDP floods directed at hosts.
  - Flood Net—Detects ICMP and UDP floods directed at networks.
  - Meta—Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.
  - Multi String—Defines 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.
  - 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 DNS—Inspects DNS (TCP and UDP) traffic.
  - Service FTP—Inspects FTP traffic.

  - Service Generic—Decodes custom service and payload.
  - Service H225— Inspects VoIP traffic.
  - Service HTTP—Inspects HTTP traffic. The WEBPORTS variable defines inspection port for HTTP traffic.
  - Service IDENT—Inspects IDENT (client and server) traffic.
  - Service MSRPC—Inspects MSRPC traffic.
  - Service MSSQL—Inspects Microsoft SQL traffic.
  - Service NTP—Inspects NTP traffic.
  - Service RPC—Inspects RPC traffic.
  - Service SMB—Inspects SMB traffic.
  - Service SNMP—Inspects SNMP traffic.
  - Service SSH—Inspects SSH traffic.
  - State—Stateful searches of strings in protocols such as SMTP.
  - String ICMP—Searches on Regex strings based on ICMP protocol.
  - String TCP—Searches on Regex strings based on TCP protocol.
  - String UDP—Searches on Regex strings based on UDP protocol.
  - Sweep—Analyzes sweeps of ports, hosts, and services, from a single host (ICMP and TCP), from destination ports (TCP and UDP), and multiple ports with RPC requests between two nodes.
  - Sweep Other TCP—Analyzes TCP flag combinations from reconnaissance scans that are trying to get information about a single host. The signatures look for flags A, B, and C. When all three are seen, an alert is fired.
  - Traffic ICMP—Analyzes nonstandard protocols, such as TFN2K, LOKI, and DDOS. There are only two signatures with configurable parameters.
  - Trojan Bo2k—Analyzes traffic from the nonstandard protocol BO2K. There are no user-configurable parameters in this engine.
  - Trojan Tfn2k—Analyzes traffic from the nonstandard protocol TFN2K. There are no user-configurable parameters in this engine.
  - Trojan UDP—Analyzes traffic from the UDP protocol. There are no user-configurable parameters in this engine.

- Event Action—Lets you assign the actions the sensor takes when it responds to events.
  - 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 will still be 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 **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.

- 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 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 > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
- 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.

- 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 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.
- 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.
- Modify Packet Inline— Modifies packet data to remove ambiguity about what the end point might do with the packet.
- 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.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- 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. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note Request Rate Limit applies to a select set of signatures. For the list of signatures for which you can request a rate limit, see Understanding Rate Limiting, page 8-3.

- 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 Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
- 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.

- 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—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—The storage type used to count events for this signature. You can 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. You can choose Yes or No 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—The mode of alert summarization. You can choose Fire All, Fire Once, Global Summarize, or Summarize.
  - Summary Interval—The time in seconds used in each summary alert. The value is 1 to 65535. The default is 15.
  - Summary Key—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. You can 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.
  - Retired—Let you choose whether the signature is retired or not. The default is no.

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:

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

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.

Clone and Edit Signature Dialog Boxes

The following fields and buttons are found in the Clone and Edit Signature dialog boxes:

Field Descriptions:

- 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. A subsignature ID is used to identify 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.
- Sig Description—Lets you specify the following attributes that help you distinguish this signature from other signatures:
  - Signature Name—Name your signature. The default is MySig.
  - Alert Notes—Add alert notes in this field.
  - User Comments—Add your comments about this signature in this field.
  - Alarm Traits—Add the alarm trait in this field. The value is 0 to 65535. The default is 0.
  - Release—Add the software release in which the signature first appeared.
- Engine—Lets you choose the engine that parses and inspects the traffic specified by this signature.
  - AIC FTP—Inspects FTP traffic and lets you control the commands being issued.
  - AIC HTTP—Provides granular control over HTTP sessions to prevent abuse of the HTTP protocol.
  - Atomic ARP—Inspects Layer-2 ARP protocol. The Atomic ARP engine is different because most engines are based on Layer-3-IP.
  - Atomic IP—Inspects IP protocol packets and associated Layer-4 transport protocols.

- Flood Host—Detects ICMP and UDP floods directed at hosts.
- Flood Net—Detects ICMP and UDP floods directed at networks.
- Meta—Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.
- Multi String—Defines 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.
- 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 DNS—Inspects DNS (TCP and UDP) traffic.
- Service FTP—Inspects FTP traffic.
- Service Generic—Decodes custom service and payload.
- Service H225— Inspects VoIP traffic.
- Service HTTP—Inspects HTTP traffic. The WEBPORTS variable defines inspection port for HTTP traffic.
- Service IDENT—Inspects IDENT (client and server) traffic.
- Service MSRPC—Inspects MSRPC traffic.
- Service MSSQL—Inspects Microsoft SQL traffic.
- Service NTP—Inspects NTP traffic.
- Service RPC—Inspects RPC traffic.
- Service SMB—Inspects SMB traffic.
- Service SNMP—Inspects SNMP traffic.
- Service SSH—Inspects SSH traffic.
- State—Stateful searches of strings in protocols such as SMTP.
- String ICMP—Searches on Regex strings based on ICMP protocol.
- String TCP—Searches on Regex strings based on TCP protocol.
- String UDP—Searches on Regex strings based on UDP protocol.
- Sweep—Analyzes sweeps of ports, hosts, and services, from a single host (ICMP and TCP), from destination ports (TCP and UDP), and multiple ports with RPC requests between two nodes.
- Sweep Other TCP—Analyzes TCP flag combinations from reconnaissance scans that are trying to get information about a single host. The signatures look for flags A, B, and C. When all three are seen, an alert is fired.
- Traffic ICMP—Analyzes nonstandard protocols, such as TFN2K, LOKI, and DDOS. There are only two signatures with configurable parameters.
- Trojan Bo2k—Analyzes traffic from the nonstandard protocol BO2K. There are no user-configurable parameters in this engine.
- Trojan Tfn2k—Analyzes traffic from the nonstandard protocol TFN2K. There are no user-configurable parameters in this engine.
- Trojan UDP—Analyzes traffic from the UDP protocol. There are no user-configurable parameters in this engine.

- Event Action—Lets you assign the actions the sensor takes when it responds to events.
  - 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 will still be 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 **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.

  - 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 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 > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

  - Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
  - 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.

  - 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 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.
  - 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.
  - Modify Packet Inline— Modifies packet data to remove ambiguity about what the end point might do with the packet.
  - 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.

- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- 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. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note Request Rate Limit applies to a select set of signatures. For the list of signatures for which you can request a rate limit, see Understanding Rate Limiting, page 8-3.

- 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 Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
- 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.

• 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—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—The storage type used to count events for this signature. You can 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. You can choose Yes or No 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—The mode of alert summarization. You can choose Fire All, Fire Once, Global Summarize, or Summarize.
  - Summary Interval—The time in seconds used in each summary alert. The value is 1 to 65535. The default is 15.
  - Summary Key—The storage type used to summarize alerts. You can 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. You can 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.
  - Retired—Lets you choose whether the signature is retired or not. The default is no.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Assign Actions Dialog Box

The following fields and buttons are found in the Assign Actions dialog box.

An event action is the sensor's response to an event. Event actions are configurable on a per signature basis.

Field Descriptions:

- 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 will still be 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 **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.

- 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 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 > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
- 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.

- 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 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.
- 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.
- Modify Packet Inline— Modifies packet data to remove ambiguity about what the end point might do with the packet.
- 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.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- 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. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note Request Rate Limit applies to a select set of signatures. For the list of signatures for which you can request a rate limit, see Understanding Rate Limiting, page 8-3.

- 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 Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
- 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.

Button Functions:

- Select All—Lets you choose all event actions.
- Select None—Clears all event action selections.

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:

- droppedPacket
- deniedFlow

- tcpOneWayResetSent

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.

Adding Signatures

To add signatures, follow these steps:

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is currently using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

Step 3 To create a custom signature that is not based on an existing signature, follow these steps:

a. Click **Add** to open the Add Signature dialog box.

b. Specify a unique signature ID for the new signature in the Signature field.

c. Specify a unique subsignature ID for the new signature in the Subsignature field.

d. Click the green icon next to the Alert Severity field and choose the severity you want to associate with this signature.

e. Click the green icon next to the Signature Fidelity Rating field and specify a value between 1and 100 to represent the signature fidelity rating for this signature.

f. Complete the signature description fields and add any comments about this signature.

g. Select the engine the sensor will use to enforce this signature.

Note If you do not know which engine to choose, use the Custom Signature Wizard to help you create a custom signature. For more information, see Creating Custom Signatures, page 6-22.

h. Click the green icon next to the Event Actions field, and 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.

i. Under Event Counter, complete the Event Counter fields if you want events counted.

j. Under Alert Frequency, complete the Alert Frequency fields to specify how you want to receive alerts.

k. Under Status, choose **Yes** to enable the signature.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

l. Under Status, specify if this signature is retired. Click **No** to activate the signature. This places the signature in the engine.

Note A signature must be activated for the sensor to actively detect the attack specified by the signature.

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

m. Click **OK**.

The new signature appears in the list with the Type set to Custom.

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

Step 4 Click **Apply** to apply your changes and save the revised configuration.

Cloning Signatures

In the Signature Configuration 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.

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is currently using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

To clone signatures, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

Step 3 To locate a signature, choose a sorting option from the Select By list.

For example, if you are searching for a UDP Flood signature, choose L2/L3/L4 Protocol and then UDP Floods.

The Signature Configuration pane refreshes and displays only those signatures that match your sorting criteria.

Step 4 To create a signature by using an existing signature as the starting point, select the signature and follow these steps:

a. Click **Clone** to open the Clone Signature dialog box.

b. Specify a unique signature ID for the new signature in the Signature field.

c. Specify a unique subsignature ID for the new signature in the Subsignature field.

d. Review the parameter values and change the value of any parameter you want to be different for this new signature.

Tip To choose more than one event action, hold down the **Ctrl** key.

e. Under Status, choose **Yes** to enable the signature.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

f. Under Status, specify if this signature is retired. Click **No** to activate the signature. This places the signature in the engine.

Note A signature must be activated 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**.

g. Click **OK**.

The cloned signature now appears in the list with the Type set to Custom.

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

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Tuning Signatures

To tune signatures, follow these steps:

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is currently using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

Step 3 To locate a signature, choose a sorting option from the Select By list.

For example, if you are searching for a UDP Flood signature, choose L2/L3/L4 Protocol and then UDP Floods.

The Signature Configuration pane refreshes and displays only those signatures that match your sorting criteria.

Step 4 To tune an existing signature, select the signature, and follow these steps:

a. Click **Edit** to open the Edit Signature dialog box.

b. Review the parameter values and change the value of any parameter you want to tune.

Tip To choose more than one event action, hold down the **Ctrl** key.

c. Under Status, choose **Yes** to enable the signature.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

d. Under Status, specify if this signature is retired. Click **No** to activate the signature. This places the signature in the engine.

Note A signature must be activated 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**.

e. Click **OK**.

The edited signature now appears in the list with the Type set to Tuned.

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

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Enabling and Disabling Signatures

To enable signatures, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

Step 3 To locate a signature, choose a sorting option from the Select By list.

For example, if you are searching for a UDP Flood signature, choose L2/L3/L4 Protocol and then UDP Floods.

The Signature Configuration 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 value Yes in this column.

b. To enable a signature that is disabled, select the signature and click **Enable**.

c. To disable a signature that is enabled, select the signature and click **Disable**.

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

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Activating and Retiring Signatures

Caution Activating and retiring signatures can take a very long time, up to 30 minutes or longer.

To activate and retire signatures, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

Step 3 To locate a signature, choose a sorting option from the Select By list.

For example, if you are searching for a UDP Flood signature, choose L2/L3/L4 Protocol and then UDP Floods.

The Signature Configuration pane refreshes and displays only those signatures that match your sorting criteria.

Step 4 To activate a signature that is retired, select the signature, and then click **Activate**.

Step 5 To retire a signature that is activated, select the signature and then click **Retire**.

Note If you retire a signature, that signature is removed from the engine but remains in the signature configuration list. You can later activate the retired signature, but doing so requires the sensor to rebuild the signature list for that engine and could delay signature processing.

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

Step 6 Click **Apply** to apply your changes and save the revised configuration.

Assigning Actions to Signatures

To assign actions to signatures, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

Step 3 To locate a signature, choose a sorting option from the Select By list.

For example, if you are searching for a UDP Flood signature, choose L2/L3/L4 Protocol and then UDP Floods.

The Signature Configuration pane refreshes and displays only those signatures that match your sorting criteria.

Step 4 To assign actions to a signature or set of signatures, select the signature(s), and then click **Actions**.

The Assign Actions dialog box appears.

a. Select the actions you want to assign to the signature(s).

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.

- 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 will still be 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 **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.

- 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 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 > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
- 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.

- 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 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.
- 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.
- Modify Packet Inline— Modifies packet data to remove ambiguity about what the end point might do with the packet.
- 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.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action. For more information, see Chapter 8, “Configuring Attack Response Controller for Blocking and Rate Limiting.”
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action. For more information, see Chapter 8, “Configuring Attack Response Controller for Blocking and Rate Limiting.”

Note For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- 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. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note Request Rate Limit applies to a select set of signatures. For the list of signatures for which you can request a rate limit, see Understanding Rate Limiting, page 8-3.

- 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 Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
- 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 choose more than one action, hold down the **Ctrl** key.

b. If you want to assign all actions to the selected signatures, click **All**. Or, if you want to remove all actions from the selected signatures, choose **None**.

Tip To discard your changes and close the Assign Actions dialog box, click **Cancel**.

c. Click **OK** to save your changes and close the dialog box.

The new action now appears in the Action column.

Configuring the Miscellaneous Pane

This section describes how to configure the Miscellaneous pane, and contains the following topics:

Overview

In the Miscellaneous pane, you can perform the following tasks:

- Configure the application policy parameters

  You can configure the sensor to provide Layer 4 to Layer 7 packet inspection to prevent malicious attacks related to web services.

- 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.

- 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.

- 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the parameters in the Miscellaneous pane.

Field Definitions

The following fields and buttons are found in the Miscellaneous pane.

- Application Policy—Lets you configure application policy enforcement.
  - Enable HTTP —Enables protection for web services. Choose **Yes** 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.

Note We recommend that you not configure AIC web ports, but rather use the default web ports.

  - Enable FTP—Enables protection for web services. Choose **Yes** to require the sensor to inspect FTP traffic.

- Fragment Reassembly—Lets you configure 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 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—May only be seeing 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 IP logging when any of the following conditions are met:
  - Max IP Log Packets—Identifies the number of packets you want logged.
  - IP Log Time—Identifies the duration you want the sensor to log. A valid value is 1 to 60 seconds. The default is 30 seconds.
  - Max IP Log Bytes—Identifies the maximum number of bytes you want logged.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Application Policy

This section describes Application Policy (AIC) signatures and how to configure them. For more information on this signature engine, see AIC Engine, page B-8. This section contains the following topics:

Overview

AIC provides detailed analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It also allows administrative control over applications that attempt to tunnel over specified ports, such as instant messaging, and tunneling applications such as, gotomypc. Inspection and policy checks for P2P and instant messaging is 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.

The AIC engine runs 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.

Caution The AIC web ports are regular HTTP web ports. You can turn on AIC web ports to distinguish which ports should watch for regular HTTP traffic and which ports should watch for AIC enforcement. You might use AIC web ports, for example, if you have a proxy on port 82 and you need to monitor it. We recommend that you do not configure separate ports for AIC enforcement.

AIC has the following categories of signatures:

- HTTP request method
  - Define request method
  - Recognized request methods

  For a list of signature IDs and descriptions, see AIC Request Method Signatures, page 5-29.
- MIME type
  - Define content type
  - Recognized content type

  For a list of signature IDs and descriptions, see AIC MIME Define Content Type Signatures, page 5-30. For the procedure for creating a custom MIME signature, see Example Recognized Define Content Type (MIME) Signature, page 5-35.
- 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

  For a list of signature IDs and descriptions, see AIC Transfer Encoding Signatures, page 5-33.

- FTP commands

  Associates an action with an FTP command. For a list of signature IDs and descriptions, see AIC FTP Commands Signatures, page 5-33.

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 5-1 lists the predefined define request method signatures. Enable the signatures that have the predefined method you need. For the procedure for enabling signatures, see Enabling and Disabling Signatures, page 5-22.

Table 5-1 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

Table 5-1 Request Method Signatures (continued)

Signature ID	Define Request Method
12710	Define Request Method GETPROPERTIES
12711	Define Request Method STARTENV
12712	Define Request Method STOPREV

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 5-2 on page 5-30 lists the predefined define content type signatures. Enable the signatures that have the predefined content type you need. For the procedure for enabling signatures, see Enabling and Disabling Signatures, page 5-22. You can also create custom define content type signatures. For the procedure, see Example Recognized Define Content Type (MIME) Signature, page 5-35.

Table 5-2 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

Table 5-2 Define Content Type Signatures (continued)

Signature ID	Signature Description
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
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

Table 5-2 Define Content Type Signatures (continued)

Signature ID	Signature Description
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
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

Table 5-2 Define Content Type Signatures (continued)

Signature ID	Signature Description
12669 0 12669 1	Content Type image/x-bitmap Header Check Content Type image/x-bitmap Invalid Message Length
12673 0	Recognized content type

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 5-3 lists the predefined transfer encoding signatures. Enable the signatures that have the predefined transfer encoding method you need. For the procedure for enabling signatures, see Enabling and Disabling Signatures, page 5-22.

Table 5-3 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

AIC FTP Commands Signatures

Table 5-4 on page 5-33 lists the predefined FTP commands signatures. Enable the signatures that have the predefined FTP command you need. For the procedure for enabling signatures, see Enabling and Disabling Signatures, page 5-22.

Table 5-4 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

Table 5-4 FTP Commands Signatures (continued)

Signature ID	FTP Command
12906	Define FTP command cwd
12907	Define FTP command dele
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

Configuring Application Policy

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

To configure the application policy parameters, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Miscellaneous**.

The Miscellaneous pane appears.

Step 3 Under Application Policy, click the green icon next to Enable HTTP and choose Yes to enable inspection of HTTP traffic.

Step 4 Click the green icon next to Max HTTP Requests and specify the number of outstanding HTTP requests per connection that can be outstanding without having received a response from the server.

Step 5 (Optional) Click the green icon next to AIC Web Ports and specify the ports you want active.

Note We recommend that you not configure AIC web ports, but rather use the default web ports.

Step 6 Click the green icon next to Enable FTP and choose Yes 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 **Reset**.

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Example Recognized Define Content Type (MIME) Signature

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

The following example demonstrates how to tune a Recognized Content Type (MIME) signature.

To tune a MIME-type policy signature, for example Signature 12623 1 (Content Type image/tiff Invalid Message Length), follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

Step 3 In the Select By box, choose **Engine**.

Step 4 In the Select Engine box, choose AIC HTTP.

Step 5 Scroll down the list and select Sig ID 12623 1, and click **Edit**.

The Edit Signature dialog box appears.

Step 6 Under Status, click the green icon next to Enabled and choose **Yes**.

Step 7 Click the green icon next to Content Type Details and choose one of the options, for example, Length.

Step 8 In the Length field, make the length smaller by changing the default to 30,000.

Step 9 Click **OK**.

Step 10 Click **Apply** to save the changes or click **Reset** to discard them.

Configuring IP Fragment Reassembly

This section describes IP fragment reassembly, lists the IP fragment reassembly signatures with their configurable parameters, and describes how to configure them. For more information on this signature engine, see Normalizer Engine, page B-15.

This section contains the following topics:

Overview

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 reassemble 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.

You configure the IP fragment reassembly per signature.

IP Fragment Reassembly Signatures and Configurable Parameters

Table 5-5 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 5-5 IP Fragment Reassembly Signatures

IP Fragment Reassembly Signature	Parameter With Default Value
1200 IP Fragmentation Buffer Full	Specify Max Fragments 10000
1201 IP Fragment Overlap	None
1202 IP Fragment Overrun - Datagram Too Long	Specify Max Datagram Size 65536
1203 IP Fragment Overwrite - Data is Overwritten	None
1204 IP Fragment Missing Initial Fragment	None
1205 IP Fragment Too Many Datagrams	Specify Max Partial Datagrams 1000
1206 IP Fragment Too Small	Specify Max Small Frags 2 Specify Min Fragment Size 400
1207 IP Fragment Too Many Datagrams	Specify Max Fragments per Datagram 170
1208 IP Fragment Incomplete Datagram	Specify Fragment Reassembly Timeout 60
1220 Jolt2 Fragment Reassembly DoS attack	Specify Max Last Fragments 4
1225 Fragment Flags Invalid	None

Configuring IP Fragment Reassembly Signatures

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

To configure IP fragment reassembly parameters for a particular signature, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration.**

Step 3 In the Select By box, choose **Engine**.

Step 4 In the Select Engine box, choose **Normalizer**.

Step 5 Select the IP fragment reassembly signature you want to configure in the list, for example, Sig ID 1200 SubSig 0, and click **Edit**.

The Edit Signature dialog box appears.

Step 6 Change the default setting of any IP fragment reassembly parameters that can be configured for signature 1200. For example, click the green icon next to Max Fragments and 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, click **Reset**.

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Configuring the Method for IP Fragment Reassembly

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

Note You can configure this option if your sensor is operating in promiscuous mode. If your sensor is operating in line mode, the method is NT only.

To configure the method the sensor will use for IP fragment reassembly, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Miscellaneous**.

The Miscellaneous pane appears.

Step 3 Under Fragment Reassembly, click the green icon next to IP Reassembly Mode and choose the operating system you want to use to reassemble the fragments.

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

Step 4 Click **Apply** to apply your changes and save the revised configuration.

Configuring TCP Stream Reassembly

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. For more information on this signature engine, see Normalizer Engine, page B-15.

This section contains the following topics:

Overview

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.

TCP Stream Reassembly Signatures and Configurable Parameters

Table 5-6 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 5-6 TCP Stream Reassembly Signatures

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1300 TCP Segment Overwrite[1]	Fires when the data in an overlapping TCP segment (such as a retransmit) sends data that is different from the data already seen on this session	—	Deny Connection Inline Product Alert[2]
1301 TCP Inactive Timeout[3]	Fires when a TCP session has been idle for a TCP Idle Timeout.	TCP Idle Timeout 3600 (15-3600)	None[4]
1302 TCP Embryonic Timeout[5]	Fires when a TCP session has not completes the three-way handshake in TCP embryonic timeout seconds.	TCP Embryonic Timeout 15 (3-300)	None[6]

Table 5-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1303 TCP Closing Timeout[7]	Fires when a TCP session has not closed completely in TCP Closed Timeout seconds after the first FIN.	TCP Closed Timeout 5 (1-60)	None[8]
1304 TCP Max Segments Queued Per Session	Fires when the number of queued out of order segments for a session exceed TCP Max Queue. The segment containing the sequence furthermost from the expected sequence is dropped.	TCP Max Queue 32 (0-128)	Deny Packet Inline Product Alert[9]
1305 TCP Urgent Flag[10]	Fires when the TCP urgent flag is seen	None	Modify Packet Inline is disabled[11]
1306 0 TCP Option Other	Fires when a TCP option in the range of TCP Option Number is seen.	TCP Option Number 6-7,9-255 (Integer Range Allow Multiple 0-255 constraints)	Modify Packet Inline Produce Alert[12]
1306 1 TCP SACK Allowed Option	Fires when a TCP selective ACK allowed option is seen.	—	Modify Packet Inline disabled[13]
1306 2 TCP SACK Data Option	Fires when a TCP selective ACK data option is seen.	—	Modify Packet Inline disabled[14]
1306 3 TCP Timestamp Option	Fires when a TCP timestamp option is seen.	—	Modify Packet Inline disabled[15]
1306 4 TCP Window Scale Option	Fires when a TCP window scale option is seen.	—	Modify Packet Inline disabled[16]
1307 TCP Window Size Variation	Fires when the right edge of the recv window for TCP moves to the right (decreases).	—	Deny Connection Inline Produce Alert disabled[17]
1308 TTL Varies[18]	Fire when the TTL seen on one direction of a session is higher than the minimum that has been observed	—	Modify Packet Inline[19]
1309 TCP Reserved Bits Set	Fires when the reserved bits (including bits used for ECN) are set on the TCP header.	—	Modify Packet Inline Produce Alert disabled[20]

Table 5-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
1310 TCP Retransmit Protection[21]	Fires when the sensor detects that a retransmitted segment has different data than the original segment.	—	Deny Connection Inline Produce Alert[22]
1311 TCP Packet Exceeds MSS	Fires when a packet exceeds the MSS that was exchanged during the three-way handshake.	—	Deny Connection Inline Produce Alert[23]
1312 TCP Min MSS	Fires when the MSS value in a packet containing a SYN flag is less that TCP Min MSS.	TCP Min MSS 400 (0-16000)	Modify Packet Inline disabled[24]
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[25]
1314 TCP Data SYN	Fires when TCP payload is sent in the SYN packet.	—	Deny Packet Inline disabled[26]
1315 ACK Without TCP Stream	Fires when an ACK packet is sent that does not belong to a stream.	—	Produce Alert disabled[27]
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[28] 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

Table 5-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
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
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

Table 5-6 TCP Stream Reassembly Signatures (continued)

Signature ID and Name	Description	Parameter With Default Value and Range	Default Actions
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. IPS keeps the last 256 bytes in each direction of the TCP session.
2. 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.
3. 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.
4. Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
5. 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).
6. Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
7. 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).
8. Modify Packet Inline, Deny Connection Inline, and Deny Packet Inline have no effect on this signature.
9. Modify Packet Inline and Deny Packet Inline have no effect on this signature. Deny Connection Inline drops the current packet and the TCP session.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. This signature is not limited to the last 256 bytes like signature 1300.
22. 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.
23. 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.

24. 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.
25. 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.
26. 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.
27. 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.
28. 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 TCP Stream Reassembly Signatures

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

To configure TCP stream reassembly parameters for a particular signature, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration.**

Step 3 In the Select By box, choose **Engine**.

Step 4 In the Select Engine box, choose **Normalizer**.

Step 5 Select the TCP fragment reassembly signature you want to configure in the list, for example, Sig ID 1313 SubSig 0, and click **Edit**.

The Edit Signature dialog box appears.

Step 6 Change the default setting of any configurable IP fragment reassembly parameters for signature 1313. For example, click the green icon next to TCP Max MSS and change the setting from the default of 1460 to 1380.

Note Changing this parameter from the default of 1460 to 1380 helps prevent fragmentation of traffic going through a VPN tunnel.

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, click **Reset**.

Step 7 Click **Apply** to apply your changes and save the revised configuration.

Configuring the Mode for TCP Stream Reassembly

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

To configure the TCP stream reassembly mode, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Miscellaneous**.

The Miscellaneous pane appears.

Step 3 Under Stream Reassembly, click the green icon next to TCP Handshake Required and choose yes.

Selecting TCP Handshake Required specifies that the sensor should only track sessions for which the three-way handshake is completed.

Step 4 Click the green icon next to TCP Reassembly Mode and 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, click **Reset**.

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Configuring IP Logging

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.

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is currently using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

Note When the sensor meets any one of the IP logging conditions, it stops IP logging.

To configure the IP logging parameters, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Miscellaneous**.

The Miscellaneous pane appears.

Step 3 Under IP Log, click the green icon next to Max IP Log Packets and then specify the number of packets you want logged.

Step 4 Click the green icon next to IP Log Time and then specify the duration you want the sensor to log.

A valid value is 1 to 60 minutes. The default is 30 minutes.

Step 5 Click the green icon next to Max IP Log Bytes and then specify the maximum number of bytes you want logged.

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

Step 6 Click **Apply** to apply your changes and save the revised configuration.

Example MEG Signature

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 SEAP. SEAP 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. For more information about SEAP, see Signature Event Action Processor, page 7-4.

Caution A large number of Meta signatures could adversely affect overall sensor performance.

The following example demonstrates how to create a MEG signature based on the Meta engine.

For example, signature 64000 subsignature 0 will fire 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.

Tip The Meta engine is different from other engines in that it takes alerts as input where most engines take packets as input. For more information on the Meta engine, see Meta Engine, page B-13.

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is currently using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

To create a MEG signature based on the Meta engine, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Signature Configuration**.

The Signature Configuration pane appears.

Step 3 Click **Add** to open the Add Signature dialog box.

Step 4 Specify a unique signature ID for the new signature in the Signature field.

Step 5 Specify a unique subsignature ID for the new signature in the Subsignature field.

Step 6 Click the green icon next to the Alert Severity field and choose the severity you want to associate with this signature.

Step 7 Click the green icon next to the Signature Fidelity Rating field and specify a value between 1and 100 to represent the signature fidelity rating for this signature.

Step 8 Leave the default value for the Promiscuous Delta field.

Step 9 Complete the signature description fields and add any comments about this signature.

Step 10 Select Meta in the Engine field.

Step 11 Configure the Meta engine-specific parameters:

a. Click the green icon next to the Meta Reset Interval field and specify the time in seconds to reset the Meta signature.

The valid range is 0 to 3600 seconds. The default is 60 seconds.

b. Choose the storage type for the Meta signature from the Meta Key list:

- Attacker address
- Attacker and victim addresses
- Attacker and victim addresses and ports
- Victim address

c. Click the pencil icon next to Component List to insert the new MEG signature.

The Component List dialog box appears.

d. Click **Add** to insert the first MEG signature.

The Add List Entry dialog box appears.

e. Specify a name for the entry in the Entry Key field, for example, Entry1.

The default is MyEntry.

f. Under Component Group, specify the number of times this component must fire before it is satisfied in the Component Count field.

g. Under Component Group, specify the signature ID of the signature (2000 in this example) on which to match this component in the Component Sig ID field.

h. Under Component Group, specify the subsignature ID of the signature (0 in this example) on which to match this component in the Component SubSig ID field.

i. Click **OK**.

   You are returned to the Add List Entry dialog box.

j. Highlight your entry and click **Select** to move it to the Selected Entries list.

k. Click **OK**.

l. Click **Add** to insert the next MEG signature.

   The Add List Entry dialog box appears.

m. Specify a name for the entry in the Entry Key field, for example Entry2.

n. Under Component Group, specify the number of times this component must fire before it is satisfied in the Component Count field.

o. Under Component Group, specify the signature ID of the signature (3000 in this example) on which to match this component in the Component Sig ID field.

p. Under Component Group, specify the subsignature ID of the signature (0 in this example) on which to match this component in the Component SubSig ID field.

q. Click **OK**.

   You are returned to the Add List Entry dialog box.

r. Highlight your entry and click **Select** to move it to the Selected Entries list.

s. Highlight the new entry and click **Move Up** or **Move Down** to order the new entry.

Tip To return the entries to the Entry Key list, click **Reset Ordering**.

t. Click **OK**.

u. Click the green icon next to the Component List in Order field and choose Yes to have the component list fire in order.

Step 12 Click the green icon next to the Event Action field, and 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 to ensure that all of the actions stay selected.

Step 13 Under Event Counter, complete the Event Counter fields if you want events counted.

Step 14 Under Alert Frequency, complete the Alert Frequency fields to specify how you want to receive alerts.

Step 15 Under Status, choose **Yes** to enable the signature.

Note A signature must be enabled for the sensor to actively detect the attack specified by the signature.

Step 16 Under Status, specify if this signature is retired. Click **No** to activate the signature. This places the signature in the engine.

Note A signature must be activated for the sensor to actively detect the attack specified by the signature.

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.

CHAPTER 6

Creating Custom Signatures

This chapter explains how to use the Custom Signature wizard to create custom signatures. For more information on the individual signature engines, see Appendix B, "Signature Engines."

This chapter contains the following sections:

About Custom Signature Wizard

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.

The Custom Signature wizard in IPS 5.1 does not support creating custom signatures based on the following signature engines:

- AIC FTP
- AIC HTTP
- Atomic ARP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H224
- Service IDENT
- Service MSSQL

- Service NTP
- Service SMB
- Service SNMP
- Service SSH
- Sweep TCP Other

To create custom signatures based on these existing signature engines, clone an existing signature from the engine you want by choosing Configuration > Signature Configuration > Clone. For more information, see Cloning Signatures, page 5-19.

For more information on using the CLI to create custom signatures using these signature engines, refer to *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*.

This section contains the following topics:

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
- Service HTTP
- Service MSRPC
- Service RPC
- State (SMTP, ...)
- String ICMP
- String TCP
- String UDP
- Sweep

Step 2 Assign the signature identifiers:

- 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 or change it by clicking **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**.

Not Using a Signature Engine

The following sequence applies if you are not using a signature engine to create your custom signature:

Step 1 Click the **No** radio button in the Welcome window.

Step 2 Choose the protocol you want to use:

- IP—Go to Step 4.
- ICMP—Go to Step 3.
- UDP—Go to Step 3.
- TCP—Go to Step 3.

Step 3 For ICMP and UDP protocols, choose the traffic type and inspect data type. For TCP protocol, choose the traffic type.

Step 4 Assign the signature identifiers:

- Signature ID
- SubSignature ID
- Signature Name
- Alert Notes (optional)
- User Comments (optional)

Step 5 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 6 Assign the alert response:

- Signature Fidelity Rating
- Severity of the alert

Step 7 Assign the alert behavior.

You can accept the default alert behavior or change it by clicking **Advanced**, which opens the Advanced Alert Behavior wizard. With this wizard you can configure how you want to handle alerts for this signature.

Step 8 Click **Finish**.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to create custom signatures.

Field Definitions

The following section describes the Custom Signature wizard field definitions window by window. It contains the following topics:

Welcome Field Definitions

The following fields and buttons are found in the Welcome window of the Custom Signature wizard.

Field Descriptions:

- 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 the engine type from the 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Protocol Type Field Definitions

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

The following fields and buttons are found in the Protocol Type window of the Custom Signature wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Signature Identification Field Definitions

The following fields and buttons are found in the Signature Identification window of the Custom Signature wizard.

Field Descriptions:

- 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.

  A subsignature ID is used to identify 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Atomic IP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

  The default is Produce Alert.

Tip To choose 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 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 Total IP Length—(Optional) Lets you specify the total IP length.
- Specify IP Option Inspection Options—(Optional) Lets you specify the IP inspection options.

  Choose from the following:

  - IP Option—IP option code to match.
  - IP Option Abnormal Options—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 Addresses—Lets you specify the source or destination address.
  - 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.

- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Service HTTP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

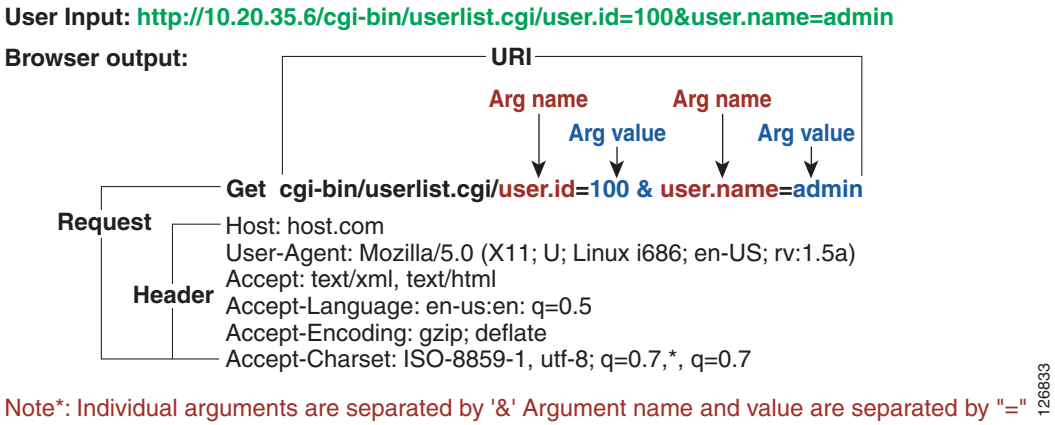
  The default is Produce Alert.

Tip To choose 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 source and destination addresses that are reported in the alert when this signature fires.

  The default is No.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.

- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Service MSRPC Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

  The default is Produce Alert.

Tip To choose 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Service RPC Engine Parameters Field Definitions

The following fields and buttons 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 choose 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 comma-separated list of ports or port ranges.
- Specify Port Map Program—Identifies the program number sent to the port mapper of interest for this signature.

  The valid range is 0 to 9999999999.
- Specify RPC Program—Identifies the RPC program number of interest for this signature.

  The valid range is 0 to 1000000.
- Specify Spool 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 alarm. 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

State Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

  The default is Produce Alert.

Tip To choose 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.
- 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 source and destination addresses that are reported in the alert when this signature fires.

  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.

  The valid range is 0 to 65535.

  If you choose No, you can set the minimum and maximum match offset.

  The valid range is 1 to 65535.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

String ICMP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

  The default is Produce Alert.

Tip To choose 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 source and destination addresses that are reported in the alert when this signature fires.

  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 No, you can set the minimum and maximum match offset.

  The valid range for the maximum match offset is 1 to 65535. The valid range for the minimum match offset is 0 to 65535.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

String TCP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

  The default is Produce Alert.

Tip To choose 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 No, you can set the minimum and maximum match offset.

  The valid range for the maximum match offset is 1 to 65535. The valid range for the minimum match offset is 0 to 65535.

- Swap Attacker Victim—Specifies whether to swap the source and destination addresses that are reported in the alert when this signature fires.

  The default is No.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

String UDP Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

  The default is Produce Alert.

Tip To choose 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.
- Specify Exact Match Offset—Identifies the exact stream offset in bytes in which the regular expression string must report the match.

  The valid range is 0 to 65535.

  If you choose No, you can set the minimum and maximum match offset.

  The valid range is 1 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 source and destination addresses that are reported in the alert when this signature fires.

  The default is No.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.

- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Sweep Engine Parameters Field Definitions

The following fields and buttons 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.

Field Descriptions:

- Event Action—Specifies the actions you want the sensor to perform if this signature is detected.

  The default is Produce Alert.

Tip To choose 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
- Swap Attacker Victim—Specifies whether to swap the source and destination addresses that are reported in the alert when this signature fires.

  The default is No.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

ICMP Traffic Type Field Definitions

The following fields and buttons are found in the ICMP Traffic Type window of the Custom Signature wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

UDP Traffic Type Field Definitions

The following fields and buttons are found in the UDP Traffic Type window of the Custom Signature wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

TCP Traffic Type Field Definitions

The following fields and buttons are found in the TCP Traffic Type window of the Custom Signature wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

UDP Sweep Type Field Definitions

The following fields and buttons are found in the UDP Sweep Type window of the Custom Signature wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

TCP Sweep Type Field Definitions

The following fields and buttons are found in the TCP Sweep Type window of the Custom Signature wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Service Type Field Definitions

The following fields and buttons are found in the Service Type window of the Custom Signature wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Inspect Data Field Definitions

The following fields and buttons are found in the Inspect Data window of the Custom Signature wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Alert Response Field Definitions

The following fields and buttons are found in the Alert Response window of the Custom Signature wizard.

Field Descriptions:

- Signature Fidelity Rating—A weight associated with how well this signature might perform in the absence of specific knowledge of the target.

  SFR 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 SFR than a signature that is written with generic rules.
- Severity of the Alert—The severity at which the alert is reported.

  You can choose from the following options:
  - High—The most serious security alert.
  - Medium—A moderate security alert.
  - Low—The least security alert.
  - Information—Denotes network activity, not a security alert.

Button Functions:

- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.

- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Alert Behavior Field Definitions

The following buttons are found in the Alert Behavior window of the Custom Signature wizard.

- Advanced—Opens the Advanced Alert Behavior window from which you can change the default alert behavior and configure how often the sensor sends alerts.
- Back—Returns you to the previous window in the Custom Signature wizard.
- Next—Advances you to the next window in the Custom Signature wizard.
- Finish—Completes the Custom Signature wizard and saves the signature you created.
- Cancel—Exits the Custom Signature wizard.
- Help—Displays the help topic for this feature.

Advanced Alert Behavior Wizard

The following section describes the field definitions for the Advanced Alert Behavior wizard. It contains the following topics:

Event Count and Interval Field Definitions

The following fields and buttons are found in the Event Count and Interval window of the Advanced Alert Behavior wizard.

Field Descriptions:

- 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, choose 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 each other.
- Event Interval (seconds)—Identifies the time interval during which the sensor counts events for rate-based counting.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.
- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Alert Summarization Field Definitions

The following fields and buttons are found in the Alert Summarization window of the Advanced Alert Behavior wizard.

Field Descriptions:

- 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.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.
- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Alert Dynamic Response Summary Field Definitions

The following fields and buttons are found in the Alert Dynamic Response Summary window of the Advanced Alert Behavior wizard.

Field Descriptions:

- 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, choose 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.

  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.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.
- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Alert Dynamic Response Fire All Field Definitions

The following fields and buttons are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you chose Alert Every Time the Signature Fires.

Field Descriptions:

- Use Dynamic Summarization—Lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.
- Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a summary alert for this signature.
- 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.
- 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.
- Specify Global Summary Threshold—Lets the sensor dynamically enter global summarization mode.

  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.
- Global Summary Threshold—Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.

- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Alert Dynamic Response Fire Once Field Definitions

The following fields and buttons are found in the Alert Dynamic Response window of the Advanced Alert Behavior wizard when you chose Alert the First Time the Signature Fires.

Field Descriptions:

- 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.
- 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.

  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.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.
- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Global Summarization Field Definitions

The following fields and buttons are found in the Global Summarization window of the Advanced Alert Behavior wizard.

Field Descriptions:

- Global Summary Interval (seconds)—Identifies the time interval during which the sensor counts events for summarization.

Button Functions:

- Back—Returns you to the previous window in the Alert Behavior wizard.
- Next—Advances you to the next window in the Alert Behavior wizard.
- Finish—Completes the Alert Behavior wizard and saves the signature you created.
- Cancel—Exits the Alert Behavior wizard.
- Help—Displays the help topic for this feature.

Creating Custom Signatures

This section provides examples of custom signatures. It contains the following topics:

Signature Engines Not Supported in the Custom Signature Wizard

The Custom Signature wizard in IPS 5.1 does not support creating custom signatures based on the following signature engines:

- AIC FTP
- AIC HTTP
- Atomic ARP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H224
- Service IDENT
- Service MSSQL
- Service NTP
- Service SMB
- Service SNMP
- Service SSH
- Sweep TCP Other

To create custom signatures based on these existing signature engines, clone an existing signature from the engine you want by choosing Configuration > Signature Configuration > Clone. For more information, see Cloning Signatures, page 5-19.

For more information on using the CLI to create custom signatures using these signature engines, refer to *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*.

Master Custom Signature Procedure

The Custom Signature wizard provides a step-by-step procedure for configuring custom signatures. For more information on the individual signature engines, see Appendix B, "Signature Engines."

To create custom signatures using the Custom Signature wizard, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Custom Signature Wizard**.

The Start window appears.

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.

Step 3 Click **Start the Wizard**.

The Welcome window appears.

Step 4 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 list, and then click **Next.** Go to Step 13.

If you do not know what engine you should use, click the **No** radio button, and then click **Next**.

The Protocol Type window appears.

Step 5 Choose the protocol that best matches the type of traffic you want this signature to inspect and then click **Next**:

- IP (If you choose IP, go to Step 13.)
- ICMP (If you choose ICMP, go to Step 6.)
- UDP (If you choose UDP, go to Step 7.)
- TCP (If you choose TCP, go to Step 9.)

Step 6 In the ICMP Traffic Type window, choose one of the following options, 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 12.
- Sweeps

  You are creating a signature to detect a sweep attack using the sweep engine for your new signature.

  Go to Step 13.

Step 7 In the UDP Traffic Type window, choose one of the following options, 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 12.
- Sweeps

  You are creating a signature to detect a sweep attack using the sweep engine for the signature.

Go to Step 8.

Step 8 In the UDP Sweep Type window, choose one of the following options, 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 13.

- 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 13.

Step 9 In the TCP Traffic Type window, choose one of the following options, 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 13.

- Single TCP Connection

  You are creating a signature to detect an attack in a single TCP connection.

  Go to Step 10.

- Multiple Connections

  You are creating a signature to inspect multiple connections for an attack.

  Go to Step 11.

Step 10 In the Service Type window, choose one of the following options, and then click **Next**:

- 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.

Go to Step 13.

Step 11 On the TCP Sweep Type window, choose one of the following options, 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 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.

Go to Step 13

Step 12 For a single packet, choose one of the following inspection options:

- 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.

Go to Step 13.

Step 13 To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:

a. Type a number in the Signature ID field.

Custom signatures are in the range of 60000 to 65000.

b. Type a number in the SubSignature ID field.

The default is 0.

You can assign a subsignature ID if you are grouping signatures together that are similar.

c. Type a name in the Signature Name field.

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 are reported to the event viewer when an alert is generated.

d. (Optional) Type text in the Alert Notes field

You can add text to be included in alarms associated with this signature. These notes are reported to the event viewer when an alert is generated.

e. (Optional) Type text in the User Comments field.

You can add any text that you find useful here. This field does not affect the signature or alert in any way.

Step 14 Assign values to the engine-specific parameters, and then click **Next**.

Tip A + icon indicates that more parameters are available for this signature. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to activate the parameter field and edit the value.

Step 15 Specify the following alert response options:

a. Specify a value in the Signature Fidelity Rating field.

The SFR is a valid value between 0 and 100 that indicates your confidence in the signature, with 100 being the most confident.

b. Choose the severity to be reported by the event viewer when the sensor sends an alert:

- High
- Informational
- Low
- Medium

Step 16 To change the default alert behavior, click **Advanced**.

The Advanced Alert Behavior wizard Event Count and Interval window appears.

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 17 Configure the event count, key, and interval:

a. Type a value for the event count in the Event Count field.

This is the minimum number of hits the sensor must receive before sending one alert for this signature.

b. 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 Use Event Interval and then specify the number of seconds that you want to use for your interval.

d. Click **Next** to continue.

The Alert Summarization window appears.

Step 18 To control the volume of alerts and configure how the sensor summarizes alerts, choose one of the following options:

- 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 19.

- 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 20.

- 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 21.

- 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 22.

Step 19 To configure the Alert Every Time the Signature Fires:

a. 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. Use Dynamic Summarization

Lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.

c. Summary Threshold

Identifies the minimum number of hits the sensor must receive before sending a summary alert for this signature.

d. 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.

e. Specify Global Summary Threshold

Lets the sensor dynamically enter global summarization mode.

f. Global Summary Threshold

Identifies the minimum number of hits the sensor must receive before sending a global summary alert.

Step 20 To configure Alert the First Time the Signature Fires:

a. 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. Use Dynamic Global Summarization

Lets the sensor dynamically enter global summarization mode.

c. Global Summary Threshold

Identifies 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.

d. Global Summary Interval (seconds)

Identifies the time interval during which the sensor counts events for summarization

Step 21 To configure Send Summary Alerts, choose one of the following options

a. Summary Interval (seconds)

Identifies the time interval during which the sensor counts events for summarization.

b. 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. Use Dynamic Global Summarization

Lets the sensor dynamically enter global summarization mode.

d. Global Summary Threshold

Identifies 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 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.

Step 22 To configure Global Summarization, specify the time interval during which the sensor should count events for summarization

Step 23 Click **Next** to continue.

Step 24 Click **Finish** to save your changes.

The Create Custom Signature dialog box appears.

Step 25 Click **Yes** to create the custom signature.

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

The signature you created is enabled and added to the list of signatures.

Example String TCP Signature

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.

Use the Custom Signature wizard to create a custom String TCP signature. For more information on the String engines, see Appendix B, "Signature Engines."

Note 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 IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Custom Signature Wizard**.

The Start window appears.

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.

Step 3 Click **Start the Wizard**.

The Welcome window appears.

Step 4 Click the **Yes** radio button, choose String TCP from the Select Engine list, and then click **Next.**

The Signature Identification window appears.

Step 5 To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:

a. Type a number in the Signature ID field.

Custom signatures range from 60000 to 65000.

b. Type a number in the SubSignature ID field.

The default is 0.

You can assign a subsignature ID if you are grouping signatures together that are similar.

c. Type a name in the Signature Name field.

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 are reported to the Event Viewer when an alert is generated.

d. (Optional) Type text in the Alert Notes field

You can add text to be included in alarms associated with this signature. These notes are reported to the event viewer when an alert is generated. The default is My Sig Info.

e. (Optional) Type text in the User Comments field.

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.

Click **Next**.

The Engine Specific Parameters window appears.

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

Step 6 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 choose more than one action, hold down the **Ctrl** key.

Step 7 Click the green icon next to Direction and 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 8 In the Regex String field specify the string this signature will be looking for in the TCP packet.

Step 9 In the Service Ports field, specify the port, for example, 23.

Service Ports is a comma-separated list of ports or port ranges where the target service resides.

Step 10 (Optional) You can configure the following optional parameters for this signature:

- Specify Exact Match Offset—Enables exact match offset, the exact stream offset the regular expression string must report for a match to be valid (0 to 65535).
- Specify Min Match Length—Enables minimum match length, 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.
- Swap Attacker Victim—Swaps the address (and ports) source and destination in the alert message.

Step 11 Click **Next**.

The Alert Response window appears.

Step 12 Change the following default alert response options if desired:

a. Specify a value in the Signature Fidelity Rating field.

The SFR 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. Choose the severity to be reported by the event viewer when the sensor sends an alert. The default is Medium.

- High
- Informational
- Low
- Medium

Step 13 Click **Next**.

The Alert Behavior window appears.

Step 14 To change the default alert behavior, click **Advanced**.

The Advanced Alert Behavior wizard Event Count and Interval window appears. To change the default alert behavior, follow Steps 15 though 21. Otherwise click **Finish** and your custom signature is created.

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 15 Configure the event count, key, and interval:

a. Type a value for the event count in the Event Count field.

This is the minimum number of hits the sensor must receive before sending one alert for this signature.

b. 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 Use Event Interval and then specify the number of seconds that you want to use for your interval.

d. Click **Next** to continue.

The Alert Summarization window appears.

Step 16 To control the volume of alerts and to configure how the sensor summarizes alerts, choose one of the following options and then click **Next**:

- 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 17a.

- 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 17b.

- 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 17c.

- 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 17d.

The Alert Dynamic Response window appears.

Step 17 Configure the alert dynamic response:

a. To configure the Alert Every Time the Signature Fires, choose one of the following options:

- 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.

- Use Dynamic Summarization

  Lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.

- Summary Threshold

  Identifies the minimum number of hits the sensor must receive before sending a summary alert for this signature.

- 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.

- Specify Global Summary Threshold

  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.

b. To configure Alert the First Time the Signature Fires, choose one of the following options:

- 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.

- 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. 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

c. To configure Send Summary Alerts, choose one of the following options

- 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, choose 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. 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.

d. To configure Global Summarization, specify the time interval during which the sensor should count events for summarization

Step 18 Click **Finish** to save your changes.

The Alert Behavior window appears.

Step 19 Click **Finish**.

The Create Custom Signature dialog box appears and asks if you want to create and apply this custom signature to the sensor.

Step 20 Click **Yes** to create the custom signature.

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

The signature you created is enabled and added to the list of signatures.

Example Service HTTP Signature

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 today's networks. In addition, it requires the most amount of preprocessing time and has the most number of signatures requiring inspection making it critical to the system's overall performance.

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 to web services 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.

Use the Custom Signature wizard to create a custom Service HTTP signature. For more information on the Service HTTP engine, see Service HTTP Engine, page B-23.

To create a custom Service HTTP signature, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Signature Definition > Custom Signature Wizard**.

The Start window appears.

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.

Step 3 Click **Start the Wizard**.

The Welcome window appears.

Step 4 Click the **Yes** radio button, choose Service HTTP from the Select Engine list, and then click **Next.**

The Signature Identification window appears.

Step 5 To specify the attributes that uniquely identify this signature, complete the following required values, and then click **Next**:

a. Type a number in the Signature ID field.

Custom signatures range from 60000 to 65000.

b. Type a number in the SubSignature ID field.

The default is 0.

You can assign a subsignature ID if you are grouping signatures together that are similar.

c. Type a name in the Signature Name field.

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 are reported to the event viewer when an alert is generated.

d. (Optional) Type text in the Alert Notes field

You can add text to be included in alarms associated with this signature. These notes are reported to the event viewer when an alert is generated. The default is My Sig Info.

e. (Optional) Type text in the User Comments field.

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.

Click **Next**.

The Engine Specific Parameters window appears.

Tip A + icon indicates that more options are available for this parameter. Click the + icon to expand the section and view the remaining parameters.

Tip A green icon indicates that the parameter is using the default value. Click the green icon to change it to red, which activates the parameter field so you can edit the value.

Step 6 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 choose more than one action, hold down the **Ctrl** key.

Step 7 Click the green icon next to De Obfuscate and choose Yes to configure the signature to apply anti-evasive deobfuscation before searching.

Step 8 (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 9 Under Regex, configure the regex parameters:

a. Choose Yes for Specify URI Regex.

b. Specify the URI Regex in the URI Regex field, 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 10 In the Service Ports field, specify the port, for example, use the web ports variable, $WEBPORTS.

Service Ports is a comma-separated list of ports or port ranges where the target service resides.

Step 11 (Optional) From the Swap Attacker Victim drop-down list, choose **Yes** to swap the attacker and victim addresses and ports (destination and source) in the alert message and for any actions taken.

Step 12 Click **Next**.

The Alert Response window appears.

Step 13 (Optional) Change the following default alert response options:

a. Specify a value in the Signature Fidelity Rating field.

The SFR 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. Choose the severity to be reported by the event viewer when the sensor sends an alert. The default is Medium.
   - High
   - Informational
   - Low
   - Medium

Step 14 Click **Next**.

The Alert Behavior window appears.

Step 15 To change the default alert behavior, click **Advanced**.

The Advanced Alert Behavior wizard Event Count and Interval window appears. To change the default alert behavior, follow Steps 15 though 21. Otherwise click **Finish** and your custom signature is created.

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. Type a value for the event count in the Event Count field.

   This is the minimum number of hits the sensor must receive before sending one alert for this signature.

b. 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 Use Event Interval and then specify 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 to configure how the sensor summarizes alerts, choose one of the following options and then click **Next**:

- 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 17a.

- 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 17b.

- 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 17c.

- 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 17d.

The Alert Dynamic Response window appears.

Step 18 Configure the alert dynamic response:

a. To configure the Alert Every Time the Signature Fires, choose one of the following options:

- 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.

- Use Dynamic Summarization

  Lets the sensor dynamically adjust the volume of alerts it sends based on the summary parameters you configure.

- Summary Threshold

  Identifies the minimum number of hits the sensor must receive before sending a summary alert for this signature.

- 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.

- Specify Global Summary Threshold

  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.

b. To configure Alert the First Time the Signature Fires, choose one of the following options:

- 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.

- 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. 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

c. To configure Send Summary Alerts, choose one of the following options

- 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, choose 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. 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.

d. To configure Global Summarization, specify the time interval during which the sensor should count events for summarization

Step 19 Click **Finish** to save your changes.

The Alert Behavior window appears.

Step 20 Click **Finish**.

The Create Custom Signature dialog box appears and asks if you want to create and apply this custom signature to the sensor.

Step 21 Click **Yes** to create the custom signature.

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

The signature you created is enabled and added to the list of signatures.

CHAPTER 7

Configuring Event Action Rules

This chapter explains how to configure event action rules. It contains the following sections:

Understanding Event Action Rules

Event action rules are a group of settings you configure for the event action processing component of the sensor. These rules dictate the actions the sensor performs when an event occurs.

The event action processing component is responsible for the following functions:

- Calculating the risk rating
- Adding event action overrides
- Filtering event action
- Executing the resulting event action
- Summarizing and aggregating events
- Maintaining a list of denied attackers

This section contains the following topics:

Calculating the Risk Rating

An 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 (ASR and SFR) and on a per-server basis (TVR).

RRs let you prioritize alerts that need your attention. These RR factors take into consideration the severity of the attack if it succeeds, the fidelity of the signature, and the overall value of the target host to you. The RR is reported in the evIdsAlert.

The following values are used to calculate the RR for a particular event:

- Attack Severity Rating (ASR)—A weight associated with the severity of a successful exploit of the vulnerability.

  The ASR is derived from the alert severity parameter of the signature.

- Signature Fidelity Rating (SFR)—A weight associated with how well this signature might perform in the absence of specific knowledge of the target.

  SFR 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 SFR than a signature that is written with generic rules.

- Target Value Rating (TVR)—A weight associated with the perceived value of the target.

  TVR is a user-configurable value 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 TVR to the company web server that is higher than the TVR you assign to a desktop node. In this example, attacks against the company web server have a higher RR than attacks against the desktop node.

Note RR is a product of ASR, SFR, and TVR with an optional PD (promiscuous delta) subtracted in promiscuous mode only.

Event Overrides

You can add an event action override to change the actions associated with an event based on the RR 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 RR range. If a signature event occurs and the RR 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 an RR of 85 or more to generate an SNMP trap, you can set the RR 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.

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 and Aggregation

This section explains how event actions are summarized and aggregated. It contains the following topics:

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 non-alert 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 choose one of the other alert-generating actions and do not have it filtered out, the alert is created even if you do not choose Produce 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—Fire All mode fires an alert each time the signature is triggered. If the threshold is set for summarization, the following happens: 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 of that signature.
- Summary—Summary mode 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—Global Summarization mode fires an alert for every summary interval. Signatures can be preconfigured for global summarization.
- Fire Once—Fire Once mode fires an alert for each address set. You can upgrade this mode to Global Summarization mode.

Signature Event Action Processor

SEAP coordinates the data flow from the signature event in the alarm channel to processing through the SEAO, the SEAF, and the SEAH. It consists of the following components:

- Alarm channel

  The unit that represents the area to communicate signature events from the Sensor App inspection path to signature event handling.
- Signature event action override (SEAO)

  Adds actions based on the RR value. SEAO applies to all signatures that fall into the range of the configured RR threshold. Each SEAO is independent and has a separate configuration value for each action type. For more information, see Calculating the Risk Rating, page 7-2.
- Signature event action filter (SEAF)

  Subtracts actions based on the signature event's signature ID, addresses, and RR. The input to the SEAF is the signature event with actions possibly added by the SEAO.

  Note The SEAF can only subtract actions, it cannot add new actions.

  The following parameters apply to the SEAF:

  - Signature ID
  - Subsignature ID
  - Attacker address
  - Attacker port
  - Victim address
  - Victim port
  - RR threshold range
  - Actions to subtract
  - Sequence identifier (optional)

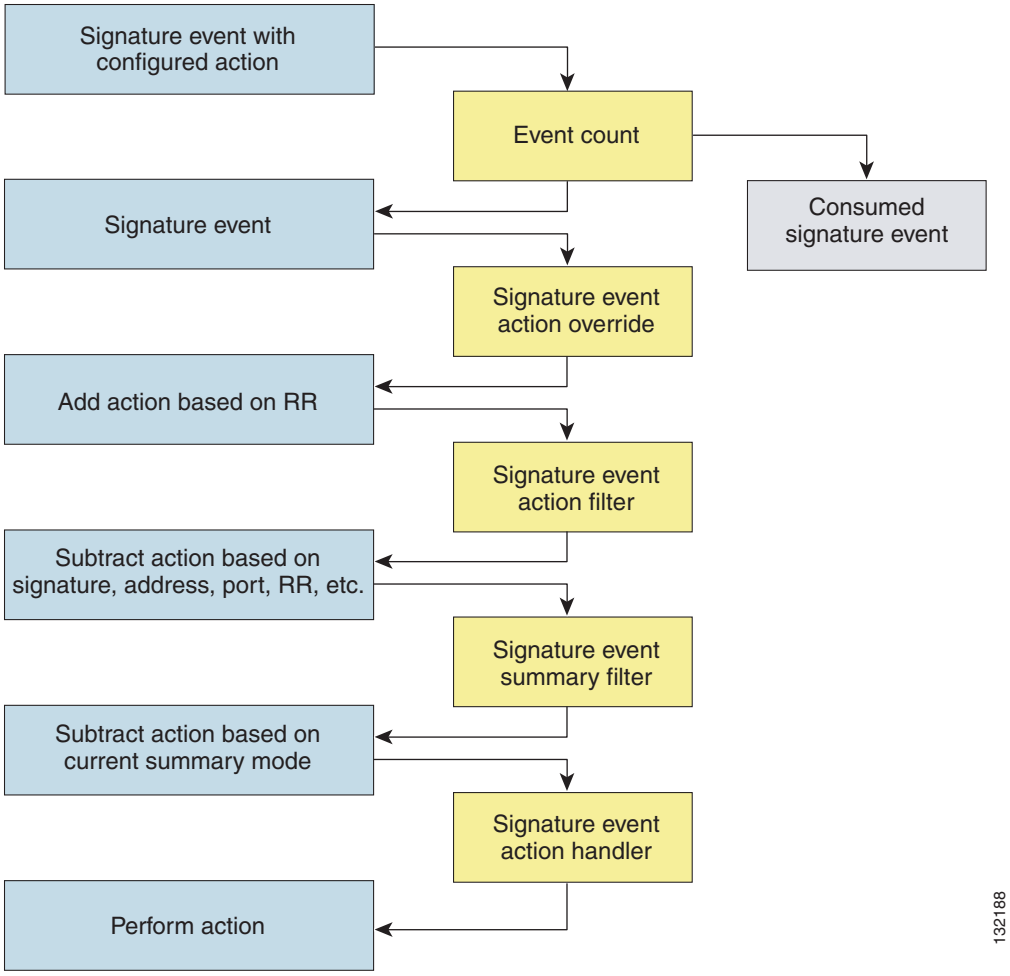
  - Stop-or-continue bit
  - Enable action filter line bit

- Signature event action handler (SEAH)

  Performs the requested actions. The output from the SEAH is the actions being performed and possibly an <evIdsAlert> written to the Event Store.

Figure 7-1 illustrates the logical flow of the signature event through the SEAP 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 SEAP.

Figure 7-1 Signature Event Through SEAP



Event Actions

Table 7-1 describes the event actions.

Table 7-1 Event Actions

Event Action Name	Description
Deny Attacker Inline	(Inline mode only) Does not transmit this packet and future packets originating from the attacker address for a specified period of time.[1] **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 **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network.For the procedure, see Monitoring the Denied Attackers List, page 11-2.
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 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. **Note** For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.
Deny Connection Inline	(Inline mode only) Does not transmit this packet and future packets on the TCP flow.
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.
Log Attacker Packets	Starts IP logging packets containing the attacker address. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Log Pair Packets	Starts IP logging packets containing the attacker-victim address pair. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Log Victim Packets	Starts IP logging packets containing the victim address.
Modify Packet Inline	Modifies packet data to remove ambiguity about what the end point might do with the packet. **Note** Modify Packet Inline is not an option for Add Event Action Filter or Add Event Action Override.

Table 7-1 Event Actions (continued)

Event Action Name	Description
Produce Alert	Writes the event to the Event Store as an alert. **Note** The Produce Alert action is not automatic when you enable alerts for a signature. To have an alert created in the Event Store, you must choose Produce Alert. If you add a second action, you must include Produce 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.
Produce Verbose Alert	Includes an encoded dump of the offending packet in the alert. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Request Block Connection	Sends a request to ARC to block this connection. **Note** You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
Request Block Host	Sends a request to ARC to block this attacker host. **Note** You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting." **Note** For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.
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. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting." **Note** Request Rate Limit applies to a select set of signatures. See Understanding Rate Limiting, page 8-3, for the list of signatures for which you can request a rate limit.
Request SNMP Trap	Sends a request to NotificationApp to perform SNMP notification. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
Reset TCP Connection	Sends TCP resets to hijack and terminate the TCP flow. **Note** Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

1. 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 will still be denied.

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:

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

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.

Event Action Rule Example

The following example demonstrates how the individual components of your event action rules work together.

Risk Rating Ranges for Example 1

- Produce Alert—1-100
- Produce Verbose Alert—90-100
- Request SNMP Trap—50-100
- Log Pair Packets—90-100
- Log Victim Packets—90-100
- Log Attacker Packets—90-100
- Reset TCP Connection—90-100
- Request Block Connection—70-89
- Request Block Host—90-100
- Deny Attacker Inline—0-0
- Deny Connection Inline—90-100
- Deny Packet Inline—90-100

Event Action Filters for Example 1

1. SigID=2004, Attacker Address=*, Victim Address=20.1.1.1, Actions to Remove=ALL, Risk Rating Range=1-100, StopOnMatch=True
2. SigID=2004, Attacker Address=30.1.1.1, Victim Address=*, Actions to Remove=ALL, Risk Rating Range=1-100, StopOnMatch=True
3. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=None, Risk Rating Range=95-100, StopOnMatch=True
4. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=denyAttackerInline, requestBlockHost, requestBlockConnection, Risk Rating Range=56-94, StopOnMatch=True
5. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=denyAttackerInline, requestBlockHost, produceAlert, resetTcpConnection, logAttackerPackets, Risk Rating Range=1-55, StopOnMatch=True

Results for Example 1

When SIG 2004 is detected:

- If the attacker address is 30.1.1.1 or the victim address is 20.1.1.1, the event is consumed (ALL actions are subtracted).

If the attacker address is not 30.1.1.1 and the victim address is not 20.1.1.1:

- If the RR is 50, Produce Alert and Request SNMP Trap are added by the event action override component, but Produce Alert is subtracted by the event action filter. However, the event action policy forces the alert action because Request SNMP Trap is dependent on the evIdsAlert.
- If the RR is 89, Request SNMP Trap and Request Block Connection are added by the event action override component. However, Request Block Connection is subtracted by the event action filter.
- If the RR is 96, all actions except Deny Attacker Inline and Request Block Connection are added by the event action override component, and none are removed by the event action filter. The third filter line with the filter action NONE is optional, but is presented as a clearer way to define this type of filter.

Configuring Event Variables

This section describes how to configure event variables, and contains the following topics:

Overview

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 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 choose 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.

When configuring IP 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
- 10.1.1.1-10.2.255.255, 10.89.10.10-10.89.10.23

Timesaver For example, 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 engineering group's IP address space. You could then use this variable to configure a filter that would ignore all Windows-based attacks for this group.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure event variables.

Field Definitions

This section lists the field definitions for event variables, and contains the following topics:

- Event Variables Pane, page 7-10
- Add and Edit Event Variable Dialog Boxes, page 7-11

Event Variables Pane

The following fields and buttons are found in the Event Variables pane.

Field Descriptions:

- 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.

Button Functions:

- Add—Opens the Add Variable dialog box. From this dialog box, you can add a variable and specify the values associated with that variable.
- Edit—Opens the Edit Variable dialog box. From this dialog box, you can change the values associated with this variable.
- Delete—Removes the selected variable from the list of available variables.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Event Variable Dialog Boxes

The following fields and buttons are found in the Add and Edit Event Variable dialog boxes.

Field Descriptions:

- 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.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Event Variables

To configure event variables, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Event Action Rules > Event Variables**.

The Event Variables pane appears.

Step 3 Click **Add** to create a variable.

The Add Variable dialog box appears.

Step 4 Type a name for this variable in the Name field.

Note A valid name can only contain numbers or letters. You can also use a hyphen (-) or an underscore (_).

Step 5 Type the values for this variable in the Value field.

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.

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

Step 6 Click **OK**.

The new variable appears in the list in the Event Variables pane.

Step 7 To edit an existing variable, select it in the list, and then click **Edit**.

The Edit Event Variable dialog box appears.

Step 8 Make your changes to the value in the Value field.

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

Step 9 Click **OK**.

The edited event variable now appears in the list in the Event Variables pane.

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

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Configuring Target Value Ratings

This section describes how to configure target value ratings, and contains the following topics:

Overview

You can assign a TVR to your network assets. The TVR is one of the factors used to calculate the RR value for each alert. You can assign different TVRs to different targets. Events with a higher RR trigger more severe signature event actions.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure target value ratings.

Field Definitions

This section lists the field definitions for TVR, and contains the following topics:

- Target Value Rating Pane, page 7-13
- Add and Edit Target Value Rating Dialog Boxes, page 7-13

Target Value Rating Pane

The following fields and buttons are found in the Target Value Rating pane.

Field Descriptions:

- 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 TVR.

Button Functions:

- Select All—Selects all configured targets.
- Add—Opens the Add Target Value Rating dialog box. From this dialog box, you add the IP address(es) of the network asset and assign a TVR to the asset.
- Edit—Opens the Edit Target Value Rating dialog box. From this dialog box, you can change the IP address(es) of the network asset.
- Delete—Removes the selected TVR from the list of available ratings.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Target Value Rating Dialog Boxes

The following fields and buttons are found in the Add and Edit Target Value Rating dialog boxes.

Field Descriptions:

- 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(es)—Identifies the IP address of the network asset you want to prioritize with a TVR.

Button Functions:

- OK—Accepts your changes and closes the dialog box.

- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Target Value Ratings

To configure TVR, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Event Action Rules > Target Value Rating**.

The Target Value Rating pane appears.

Step 3 Click **Add** to create a TVR.

The Add Target Value Rating dialog box appears.

Step 4 To assign a TVR to a new group of assets, follow these steps:

a. Click **Add**. to add a new group of network assets.

b. Choose a rating from the Target Value Rating list box.

The values are High, Low, Medium, Mission Critical, or No Value.

c. Type the IP address of the network asset in the Target IP Address(es) field.

To enter a range of IP addresses, type 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 5 Click **OK**.

The new TVR for the new asset appears in the list in the Target Value Rating pane.

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

The Edit Target Value Rating dialog box appears.

Step 7 Make your changes to the values in the Target IP Address(es) field.

Tip To discard your changes and close the Edit Target Value Rating dialog box, click **Cancel**.

Step 8 Click **OK**.

The edited network asset now appears in the list in the Target Value Rating pane.

Step 9 To delete a network asset, select in the list, and then click **Delete**.

The network asset no longer appears in the list in the Target Value Rating pane.

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

Step 10 Click **Apply** to apply your changes and save the revised configuration.

Configuring Event Action Overrides

This section describes how to configure event action overrides, and contains the following topics:

Overview

You can add an event action override to change the actions associated with an event based on specific details about that event.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure event action overrides.

Field Definitions

This section lists the field definitions for the event action overrides, and contains the following topics:

Event Action Overrides Pane

The following fields and buttons are found in the Event Action Overrides pane.

Field Descriptions:

- Use Event Action Overrides—If selected, lets you use any event action override that is enabled.
- Event Action—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.

- Risk Rating—Indicates the RR range between 0 and 100 that should be used to trigger this event action override.

  If an event occurs with a RR that falls within the minimum-maximum range you configure here, the event action is added to this event.

Button Functions:

- Select All—Selects all event action overrides listed in the table.
- Add—Opens the Add Event Action Override dialog box. From this dialog box, you can add an event action override and specify the values associated with that override.
- Edit—Opens the Edit Event Action Override dialog box. From this dialog box, you can change the values associated with this event action override.
- Enable—Enables the selected event action override. You must check the Use Event Action Overrides check box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set here.
- Disable—Disables the selected event action override.
- Delete—Removes the selected event action override from the list of available overrides.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Event Action Overrides Dialog Boxes

The following fields and buttons are found in the Add and Edit Event Action Overrides dialog boxes.

Field Descriptions:

- Event Action—Specifies the event action that will be added to an event if the conditions of this event action override are satisfied.
  - 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 will still be 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 **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.

  - 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 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 > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
- 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.

- 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 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 the 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 the Event Store, even if Produce Alert is not selected.
- Modify Packet Inline— Modifies packet data to remove ambiguity about what the end point might do with the packet.

Note Modify Packet Inline is not an option for Add Event Action Filter or Add Event Action Override.

- Produce Alert—Writes the event to the 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 the Event Store, even if Produce Alert is not selected.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action. For more information, see Chapter 8, “Configuring Attack Response Controller for Blocking and Rate Limiting.”
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action. For more information, see Chapter 8, “Configuring Attack Response Controller for Blocking and Rate Limiting.”

Note For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- 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. For more information, see Chapter 8, “Configuring Attack Response Controller for Blocking and Rate Limiting.”

  - 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 Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
  - 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.
- Enabled—Check the Yes check box to enable the override, check the No check box to disable the override.
- Risk Rating—Indicates the RR range between 0 and 100 that should be used to trigger this event action override.

  If an event occurs with an RR that falls within the minimum-maximum range you configure here, the event action is added to this event.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

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:

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

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.

Configuring Event Action Overrides

To configure event action overrides, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Event Action Rules > Event Action Overrides**.

The Event Action Overrides pane appears.

Step 3 Click **Add** to create a event action override.

The Add Event Action Override dialog box appears.

Step 4 From the Event Action list, choose the event action this event action override will correspond to.

Step 5 Under Enabled, check the Yes check box.

Step 6 Under Risk Rating assign an RR range to this network asset in the Minimum and Maximum fields.

All values should be between 0 and 100 and the value in the Minimum field must be less than or equal to the value in the Maximum field.

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 in the Event Action Overrides pane.

Step 8 Check the Use Event Action Overrides check box.

Note You must check the Use Event Action Overrides check box in the Event Action Overrides pane 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**.

The Edit Event Action Override dialog box appears.

Step 10 Under Enabled, check the Yes check box.

Step 11 Under Risk Rating assign an RR range to this network asset in the Minimum and Maximum fields.

All values should be between 0 and 100 and the value in the Minimum field must be less than or equal to the value in the Maximum field.

Tip To discard your changes and close the Edit Event Action Override dialog box, click **Cancel**.

Step 12 Click **OK**.

The edited event action override now appears in the list in the Event Action Overrides pane.

Step 13 Check the Use Event Action Overrides check box.

Note You must check the Use Event Action Overrides check box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set.

Step 14 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 in the Event Action Overrides pane.

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.

Step 15 To enable or disable an event action override, select it in the list, and then click **Enable** or **Disable**.

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

Step 16 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:

Overview

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 in the Event Variables pane to group addresses for your filters.

Note 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure Event Action Filters.

Field Definitions

This section lists the field definitions for event action filters, and contains the following topics:

Event Action Filters Pane

The following fields and buttons are found in the Event Action Filters pane.

Field Descriptions:

- Use Event Action Filters—Enables the event action filter component.

  You must check this check box to use any filter that is enabled.
- 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.
- Active—Indicates whether the filter has been put into the filter list and will take effect on filtering events.
- 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.

  A subSig ID is used to identify a more granular version of a broad signature. You can also enter a range of subSig IDs.
- Attacker (address/port)—Identifies the IP address and/or port of the host that sent the offending packet.

  You can also enter a range of addresses.
- Attacker (address/port)—Identifies the IP address and/or port used by the attacker host.

  This is the port from where the offending packet originated. You can also enter a range of ports.
- Risk Rating—Indicates the RR range between 0 and 100 that should be used to trigger this Event Action Filter.

  If an event occurs with an RR 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.
- Deny Pct—Indicates the percentage of packets to deny for deny attacker features.
- 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—Identifies the user comments associated with this filter.

Button Functions:

- Select All—Selects all event action filters listed.
- Add—Opens the Add Event Action Filter dialog box. From this dialog box, you can add an event action filter and specify the values associated with that filter.
- Insert Before—Lets you add an event action filter above the one you have selected. Opens the Add Event Action Filter dialog box.
- Insert After—Lets you add an event action filter after the one you have selected. Opens the Add Event Action Filter dialog box.
- Move Up—Moves the selected filter up one row in the list and changes the processing order of the filters.
- Move Down—Moves the selected filter down one row in the list and changes the processing order of the filters.
- Edit—Opens the Edit Event Action Filter dialog box. From this dialog box, you can change the values associated with this filter.
- Active—Lets you add a filter to the filter list so that it takes effect on filtering events.
- Inactive—Lets you take a filter out of the list so that it does not take effect on filtering events.
- Enable—Enables the selected event action filter.

  You must check the Use Event Action Filters check box on the Event Action Filters pane or none of the event action filters will be enabled regardless of the value you set here.
- Disable—Disables the selected event action filter.
- Delete—Removes this event action filter from the list of available filters.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Event Action Filters Dialog Boxes

The following fields and buttons are found in the Add and Edit Event Action Filters dialog boxes.

Field Descriptions:

- 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.
- Active—Lets you add the filter to the filter list so that it takes effect on filtering events.
- Enabled—Indicates whether or not this filter is enabled.
- 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.

  A subSig ID is used to identify a more granular version of a broad signature. You can also enter a range of subSig IDs.
- Attacker Address—Identifies the IP address of the host that sent the offending packet.

  You can also enter a range of addresses.

- 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.
- Victim Address—Identifies the IP address of the host being attacked (the recipient of the offending packet).

  You can also enter a range of addresses.
- Victim Port—Identifies the port through which the offending packet was received.

  You can also enter a range of ports.
- Risk Rating—Indicates the RR range between 0 and 100 that should be used to trigger this event action filter.

  If an event occurs with an RR 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.
  - 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 will still be 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 **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.
  - 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 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 > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.
  - Deny Connection Inline—(Inline only) Terminates the current packet and future packets on this TCP flow.
  - 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.

- 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 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 the 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 the Event Store, even if Produce Alert is not selected.
- Modify Packet Inline— Modifies packet data to remove ambiguity about what the end point might do with the packet.

Note Modify Packet Inline is not an option for Add Event Action Filter or Add Event Action Override.

- Produce Alert—Writes the event to the 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 the Event Store, even if Produce Alert is not selected.
- Request Block Connection—Sends a request to ARC to block this connection. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- Request Block Host—Sends a request to ARC to block this attacker host. You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."

Note For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.

- 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. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- 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 Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
- 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.

- 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—Identifies the user comments associated with this filter.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Event Action Filters

To configure event action filters, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Event Action Rules > Event Action Filters**.

The Event Action Filters pane appears.

Step 3 To create an event action filter, do one of the following:

- To add a new event action filter, click **Add**.
- Or, to add a filter above or below the current filter, right-click a filter and then choose Insert Before or Insert After.

The Add Event Action Filter dialog box appears.

Step 4 Type the signature IDs of all signatures to which this filter should be applied in the Signature ID field.

You can use a list (2001, 2004), or a range (2001–2004) or one of the SIG variables if you defined them in the Event Variables pane. Preface the variable with $.

Step 5 Type the subsignature IDs of the subsignatures to which this filter should be applied in the SubSignature ID field.

Step 6 Type the IP address of the source host in the Attacker Address field.

You can use one of the variables if you defined them in the Event Variables pane. Preface the variable with $. You can also enter a range of addresses (0.0.0.0-255.255.255.255).

Step 7 Type the port number used by the attacker to send the offending packet in the Attacker Port field.

Step 8 Type the IP address of the recipient host in the Victim Address field.

You can use one of the variables if you defined them in the Event Variables pane. Preface the variable with $. You can also enter a range of addresses (0.0.0.0-255.255.255.255).

Step 9 Type the port number used by the victim host to receive the offending packet in the Victim Port field.

Step 10 Assign an RR range to this filter in the Risk Rating field.

If the RR for an event falls within the range you specify, the event is processed against the criteria of this filter.

Step 11 Select the actions you want this filter to remove from the event from the Actions to Subtract list.

Tip To choose more than one event action in the list, hold down the **Ctrl** key.

Step 12 Type the percentage of packets to deny for deny attacker features in the Deny Percentage field. The default is 100 percent.

Step 13 Next to Stop on Match, check one of the following check boxes:

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 14 Next to Enabled, choose Yes to enable this filter.

Note You must also check the Use Event Action Filters check box in the Event Action Filters pane or none of the event action filters will be enabled regardless of whether you check the Yes check box in the Add Event Action Filter dialog box.

Step 15 Next to Active, choose Yes to add this filter to the list so that it takes effect on filtering events.

Step 16 Type any comments that you want to store with this filter in the Comments field, 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 17 Click **OK**.

The new event action filter now appears in the list in the Event Action Filters pane.

Step 18 Check the Use Event Action Overrides check box.

Note You must check the Use Event Action Overrides box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set in the Add Event Action Filter dialog box.

Step 19 To edit an existing event action filter, select it in the list, and then click **Edit**.

The Edit Event Action Filter dialog box appears.

Step 20 Change any values in the fields that you need to.

See Steps 3 through 14 for information on completing the fields.

Tip To discard your changes and close the Edit Event Action Filter dialog box, click **Cancel**.

Step 21 Click **OK**.

The edited event action filter now appears in the list in the Event Action Filter pane.

Step 22 Check the Use Event Action Overrides check box.

Note You must check the Use Event Action Overrides box in the Event Action Overrides pane or none of the event action overrides will be enabled regardless of the value you set in the Edit Event Action Filter dialog box.

Step 23 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 in the Event Action Filters pane.

Step 24 To enable or disable an event action filter, select it in the list, and then click **Enable** or **Disable**.

Step 25 To move an event action filter up or down in the list, select it, and then click **Move Up** or **Move Down**.

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

Step 26 Click **Apply** to apply your changes and save the revised configuration.

Configuring the General Settings

This section describes how to configure the general settings, and contains the following topics:

Overview

You can configure the general settings that apply 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 turn off the Summarizer or Meta Event Generator except for troubleshooting purposes. If you turn off the Summarizer, every signature is set to Fire All with no summarization. If you turn off the Meta Event Generator, all Meta engine signatures are disabled.

You can configure how long you want to deny attackers, the maximum number of denied attackers, and how long you want blocks to last.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the general settings for event action rules.

Field Definitions

The following fields and buttons are found in the General Settings pane.

Field Descriptions:

- 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 will be disabled.
- Deny Attacker Duration—Number of seconds to deny the attacker inline.

  The valid range is 0 to 518400. The default is 3600.
- Block Attack Duration—Number of minutes to block a host or connection.

  The valid range is 0 to 10000000. The default is 30.
- Maximum Denied Attackers—Limits the number of denied attackers possible in the system at any one time.

  The valid range is 0 to 10000000. The default is 10000.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Event Action Rules General Settings

Caution The Summarizer and Meta Event Generator 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 IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration >Event Action Rules > General Settings**.

The General Settings pane appears.

Step 3 Check the Use Summarizer check box to enable the summarizer feature.

Caution Only disable the Summarizer for troubleshooting purposes. Otherwise, make sure the Summarizer is enabled so that all signatures you configure for summarization will actually summarize.

Step 4 Check the Use Meta Event Generator check box to enable the meta event generator.

Caution Only disable the Meta Event Generator for troubleshooting purposes. Otherwise, make sure the Meta Event Generator is enabled so that all Meta engine signatures are functional.

Step 5 Type the number of seconds you want to deny the attacker inline in the Deny Attacker Duration field.

Step 6 Type the number of minutes you want to block a host or connection in the Block Action Duration field.

Step 7 Type the maximum number of denied attackers you want at any one time in the Maximum Denied Attackers field.

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

Step 8 Click **Apply** to apply your changes and save the revised configuration.

Monitoring Events

This section describes how to monitor events, and contains the following topics:

Overview

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. You can access these events by clicking View.

When you click **View**, IDM 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, IDM limits the number of events you can view at one time (the maximum number of rows per page is 500). You can click **Back** and **Next** to view more events.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

Field Definitions

This section lists the field definitions configuring events and viewing events. It contains the following topics:

Events Pane

The following fields and buttons are found in the Events pane.

Field Descriptions:

- Show alert events—Lets you configure the level of alert you want to view:
  - Informational
  - Low
  - Medium
  - High

  The default is all levels enabled.
- Show error events—Lets you configure the type of errors you want to view:
  - Warning
  - Error
  - Fatal

  The default is all levels enabled.
- Show Network Access Controller events—Shows ARC (formally known as Network Access Controller) events.

  The default is disabled.
- 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.

Button Functions:

- View—Causes the Event Viewer to appear.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Event Viewer Page

The following fields and buttons are found on the Event Viewer page.

- #—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.
- Event ID—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.

Button Functions

- Details—Displays the details of the selected event in a separate dialog box.

  Displays the application, attacker, target, and signature details.
- Refresh—Lets you refresh the Event Viewer with new events.
- Back—Displays the previous page in the Event Viewer.
- Next—Displays the next page in the Event Viewer.
- Close—Closes the open dialog box.
- Help—Displays the help topic for this feature.

Configuring Event Display

To configure how you want events to be displayed, follow these steps:

Step 1 Log in to IDM.

Step 2 Choose **Monitoring > Events**.

The Events pane appears.

Step 3 Under Events, choose the levels of alerts you want to be displayed.

Step 4 Under Events, choose the types of errors you want to be displayed.

Step 5 Check the **Show Network Access Controller events** check box if you want ARC (formerly known as Network Access Controller) events to be displayed.

Step 6 Check the **Show status events** check box if you want status events to be displayed.

Step 7 Choose the number of rows per page you want displayed.

The default is 100. The values are 100, 200, 300, 400, or 500.

Step 8 If you want to set a time for events to be displayed, choose one of the following:

- Show all events currently stored on the sensor
- Show past events

  Type in the hours and minutes you want to go back to view past events.
- Show events from the following time range

  Select a start and end time.

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

Step 9 Click **View** to display the events you configured.

The Event Viewer appears.

Step 10 To sort up and down in a column, click the right-hand side to see the up and down arrow.

Step 11 Click **Next** or **Back** to page by one hundred.

Step 12 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.

CHAPTER 8

Configuring Attack Response Controller for Blocking and Rate Limiting

This chapter provides information for setting up Attack Response Controller (ARC) to perform blocking and rate limiting on the sensor.

Note ARC was formerly known as Network Access Controller. The name has been changed for IPS 5.1, although IDM still contains the term Network Access Controller.

This chapter contains the following sections:

Understanding Blocking

ARC, the blocking application on the sensor, starts and stops blocks on routers, switches, PIX. Firewalls, FWSM, and ASA. 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. ARC monitors the time for the block and removes the block after the time has expired.

Caution If FWSM is configured in multi-mode, blocking is not supported for the admin context. Blocking is only supported in single mode and in multi-mode customer context.

Note ARC was designed to complete the action response for a new block in no more than 4 to 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 firewall, ASA, or FWSM 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, ARC may not apply blocks in a timely manner or may not be able to apply blocks at all.

For firewalls, such as ASA, PIX Firewall 7.0, and FWSM 2.1 or greater, configured in multi-mode, IPS 5.1 does not include VLAN information in the block request. Therefore you must make sure the IP addresses being blocked are correct for each firewall. For example, the sensor is monitoring packets on a firewall customer context that is configured for VLAN A, but is blocking on a different firewall 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.

  Note Connection blocks are not supported on firewalls. Firewalls only support host blocks with additional connection information.

- 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.

Caution Do not confuse blocking with the sensor's ability 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 choose Request Block Host or Request Block Connection as the event action for particular signatures, and add them to any event action overrides you have configured, so that SensorApp sends a block request to ARC when the signature is triggered. Once ARC receives the block request from SensorApp, it updates the device configurations to block the host or connection. For the procedure to add the Request Block Host or Request Block Connection event actions to the signature, see Assigning Actions to Signatures, page 5-23. Or for the procedure for configuring overrides that add the Request Block Host or Request Block Connection event actions to alarms of specific risk ratings, see Configuring Event Action Overrides, page 7-15.

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 PIX Firewall, FWSM, and ASA 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. For more information, see How the Sensor Manages Devices, page 8-22.

You need the following information for 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 a PIX Firewall, FWSM, or ASA 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 check the status of ARC, enter **show statistics network-access** at the `sensor#`. The output shows the devices you are managing, any active blocks and rate limits, and the status of all devices. Or in IDM, choose **Monitoring > Statistics** to see the status of ARC.

Note ARC is formerly known as Network Access Controller. Although the name has been changed, IDM and the CLI contain references to Network Access Controller, **nac**, and **network-access**.

Understanding Rate Limiting

Rate limiting lets sensors restrict the rate of specified traffic classes on network devices. Rate limit responses are supported for the Host Flood and Net Flood engines, and the TCP half-open SYN signature. ARC can configure rate limits on network devices running Cisco IOS version 12.3 or later. For configuring rate limiting on routers, see Configuring Blocking and Rate Limiting Devices, page 8-18. Master blocking sensors can also forward rate limit requests to blocking forwarding sensors. See Configuring the Master Blocking Sensor for more information.

Tip To check the status of ARC, enter **show statistics network-access** at the `sensor#`. The output shows the devices you are managing, any active blocks and rate limits, and the status of all devices. Or in IDM, choose **Monitoring > Statistics** to see the status of ARC.

To add a rate limit, you specify a combination of protocol, destination IP address, and data value to match one of the signatures that are allowed to generate rate limit events. For the procedure, see Managing Active Rate Limits, page 8-11. You must also set the action to Request Rate Limit and set the percentage for these signatures.

Table 8-1 lists the supported signatures and parameters.

Table 8-1 Rate Limit 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

Before Configuring ARC

Before you configure 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.

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. For the procedure, see Configuring the Master Blocking Sensor, page 8-31.

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 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.

- 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

By default, ARC supports up to 250 devices in any combination. The following devices are supported for blocking by ARC:

Note ARC was designed to complete the action response for a new block in no more than 4 to 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 firewall, ASA, or FWSM 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.

Caution If the recommended limits are exceeded, ARC may not apply blocks in a timely manner or may not be able to apply blocks at all.

- 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 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

Configuring Blocking Properties

This section describes how to configure blocking properties, and contains the following topics:

Overview

Use the Blocking Properties pane to configure the basic settings required to enable blocking and rate limiting.

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 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. For more information, see Configuring Event Action Filters, page 7-20.

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 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 ARC could be making a change at the same time on the same device. This could cause the device or ARC to fail.

Note 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to add or edit blocking properties.

Field Definitions

This section lists the field definitions for blocking properties, and contains the following topics:

Blocking Properties Pane

The following fields and buttons are found in the Blocking Properties pane.

Field Descriptions:

- Enable blocking— 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 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 the sensor IP address to be blocked—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 ARC first connects.

  If enabled, NVRAM is written each time the ACLs are updated. The default is disabled.

  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 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—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 Firewall 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 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 firewall 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 firewalls, 250 routers, 250 Catalyst Software switches, and 100 master blocking sensors.

- Maximum Rate Limit Entries—Maximum number of rate limit entries.

  The maximum rate limit should be equal or less then 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. For more information, see Configuring Event Action Filters, page 7-25.

  - IP Address—IP address to never block.
  - Mask—Mask corresponding to the IP address never to block.

Button Functions:

- Add—Opens the Add Never Block Address dialog box. From this dialog box, you can add a host or network to the list of hosts and networks never to be blocked.
- Edit—Opens the Edit Never Block dialog box. From this dialog box, you can change the host or network that is never to be blocked.
- Delete—Removes this host or network from the list of hosts and networks never to be blocked.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Never Block Address Dialog Boxes

The following fields and buttons are found in the Add and Edit Never Block Address dialog boxes.

Field Descriptions:

- IP Address—IP address to never block.
- Mask—Mask corresponding to the IP address never to block.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Blocking Properties

To configure blocking properties, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Blocking > Blocking Properties**.

The Blocking Properties pane appears.

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. For the procedures, see Configuring Router Blocking or Rate Limiting Device Interfaces, page 8-22, and Configuring Cat 6K Blocking Device Interfaces, page 8-27.

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 choose 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 ARC first connects.

Step 7 Check the Enable ACL logging check box if you want ARC to append the log parameter to block entries in the ACL or VACL.

Step 8 Enter how many blocks are to be maintained simultaneously (1 to 65535) in the Maximum Block Entries field.

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 or less then the maximum blocking entries. If you configure more rate limit entries than block entries, you receive an error.

Step 11 Click **Add** to add a host or network to the list of addresses never to be blocked.

The Add Never Block Address dialog box appears.

Step 12 Enter the IP address of the host or network in the IP Address field.

Step 13 Enter the network mask of the host or network in the Network Mask field or choose a network mask from the list.

Tip To discard your changes and close the Add Never Block Address dialog box, click **Cancel**.

Step 14 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 15 To edit an existing entry in the never block addresses list, select it, and click **Edit**.

The Edit Never Block Address dialog box appears.

Step 16 Edit the IP address of the host or network in the IP Address field.

Step 17 Edit the network mask of the host or network in the Network Mask field.

Tip To discard your changes and close the Edit Never Block Address dialog box, click **Cancel**.

Step 18 Click **OK**.

The edited host or network appears in the Never Block Addresses list in the Allowed Hosts pane.

Step 19 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 20 Click **Apply** to apply your changes and save the revised configuration.

Managing Active Rate Limits

This section describes how to manage active rate limits, and contains the following sections:

Overview

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.

Caution Although the pane displays source address, source port, and destination port, those fields are not supported in this version.

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure rate limits.

Field Definitions

This section lists the field definitions for rate limits, and contains the following topics:

- Rate Limits Pane, page 8-12
- Add Rate Limit Dialog Box, page 8-13

Rate Limits Pane

The following fields and buttons are found in the Rate Limits pane.

Field Descriptions:

- Protocol—Protocol of the traffic that is rate limited.
- Rate—Percent of maximum bandwidth that is allowed for the rate-limited traffic.

  Matching traffic that exceeds this rate will be dropped.
- Source IP—(Optional) Source host IP address of the rate-limited traffic.
- Source Port—(Optional) Source host port of the rate-limited traffic.
- Destination IP—Destination Host IP address of the rate-limited traffic.
- Destination Port—(Optional) Destination host port of the rate-limited traffic.

- Data—(Optional) 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—Remaining minutes that this rate limit is in effect.
- Timeout (minutes)—Total number of minutes for this rate limit.

Button Functions:

- Add—Opens the Add Rate Limit dialog box. From this dialog box, you can configure the options for rate limiting.
- Delete—Deletes this entry from the table.
- Refresh—Refreshes the contents of the table.

Add Rate Limit Dialog Box

The following fields and buttons are found in the Add Rate Limit dialog box.

Field Descriptions:

- Protocol—Protocol of the traffic that is rate-limited (ICMP, TCP, or UDP).
- Rate—Percentage of the maximum bandwidth allowed for the rate-limited traffic.
- Source IP—(Optional) Source host IP address of the rate-limited traffic.
- Source Port—(Optional) Source host port of the rate-limited traffic.
- Destination IP—(Optional) Destination host IP address of the rate-limited traffic.
- Destination Port—(Optional) Destination host port of the rate-limited traffic.
- Use Additional Data—(Optional) 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—Timeout not enabled.
  - Enable Timeout—Lets you specify the timeout in minutes (1 to 70560).

Button Functions:

- Apply—Applies your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring and Managing Rate Limits

For more information on rate limiting, see Understanding Rate Limiting, page 8-3.

To configure and manage rate limiting, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Monitoring > Rate Limits**.

The Rate Limits pane appears.

Step 3 Click **Add** to add a rate limit.

The Add Rate Limit dialog box appears.

Step 4 Choose the protocol (ICMP, TCP, or UDP) of the traffic you want rate limited from the Protocol list.

Step 5 Enter the rate limit (1 to 100) in the Rate field.

Step 6 (Optional) Enter the destination IP address in the Destination IP field.

Step 7 Check the Use Additional Data check box if you want to configure the rate limit to use additional data.

Step 8 Choose the additional data (echo-reply, echo-request, or halfOpenSyn) from the Select Data list.

Step 9 Check the Enable Timeout check box if you want to configure a timeout in minutes.

Step 10 Enter the amount of time in minutes (1 to 70560) in the Timeout field.

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

Step 11 Check the No Timeout check box if you do not want to configure the rate limit for a specified amount of time.

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, choose 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.

Configuring Device Login Profiles

This section describes how to configure device login profiles, and contains the following topics:

Overview

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to add or edit device login profiles.

Field Definitions

This section lists the field definitions for device login profiles, and contains the following topics:

- Device Login Profile Pane, page 8-15
- Add and Edit Device Login Profile Dialog Boxes, page 8-16

Device Login Profile Pane

The following fields and buttons are found in the Device Login Profile pane.

Field Descriptions:

- Profile Name—Name of the profile.
- Username—Username used to log in to the blocking device (optional).
- Login Password—Login password used to log in to the blocking device (optional).

  Found only in the Add Device Login Profile dialog box.

  Note If a password exists, it is displayed with a fixed number of asterisks.

- Enable Password—Enable password used on the blocking device (optional).

  Found only in the Add Device Login Profile dialog box.

  Note If a password exists, it is displayed with a fixed number of asterisks.

Button Functions:

- Add—Opens the Add Device Login Profile dialog box. From this dialog box, you can add a device login profile.
- Edit—Opens the Edit Device Login Profile box. From this dialog box, you can change the values associated with this device login profile.
- Delete—Removes this device login profile from the list of device login profiles. You receive an error message if you try to delete a profile that is being used.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Device Login Profile Dialog Boxes

The following fields and buttons are found in the Add and Edit Device Login Profile dialog boxes.

Field Descriptions:

- Profile Name—Name of the profile.
- Username—Username used to log in to the blocking device (optional).
- Login Password—Login password used to log in to the blocking device (optional).

  Found only in the Add Device Login Profile dialog box.

  Note If a password exists, it is displayed with a fixed number of asterisks.

- Enable Password—Enable password used on the blocking device (optional).

  Found only in the Add Device Login Profile dialog box.

  Note If a password exists, it is displayed with a fixed number of asterisks.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Device Login Profiles

To configure device login profiles, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Blocking > Device Login Profiles**.

The Device Login Profiles pane appears.

Step 3 Click **Add** to add a profile.

The Add Device Login Profile dialog box appears.

Step 4 Enter the profile name in the Profile Name field.

Step 5 Enter the username used to log in to the blocking device in the Username field.

Step 6 Enter the login password in the New Password field and retype it in the Confirm New Password field.

Step 7 Enter the enable password in the New Password field and retype it in the Confirm New Password field.

Tip To discard your changes and close the Add Device Login Profile dialog box, click **Cancel**.

Step 8 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 9 To edit an existing entry in the device login profile list, select it, and click **Edit**.

The Edit Device Login Profile dialog box appears.

Step 10 Edit the username used to log in to the blocking device in the Username field.

Step 11 Check the Change the login password check box to change the login password.

Step 12 Enter the new login password in the New Password field and reenter it in the Confirm New Password field.

Step 13 Check the Change the enable password check box to change the enable password.

Step 14 Enter the new enable password in the New Password field and reenter it in the Confirm New Password field.

Tip To discard your changes and close the Edit Device Login Profile dialog box, click **Cancel**.

Step 15 Click **OK**.

The edited device login profile appears in the list in the Device Login Profile pane.

Step 16 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 17 Click **Apply** to apply your changes and save the revised configuration.

Configuring Blocking and Rate Limiting Devices

This section describes how to configure blocking and rate limiting devices, and contains the following topics:

Overview

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 PIX Firewall or ASA. The router, switch, or firewall 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. For the procedure for setting up a master blocking sensor, see Configuring the Master Blocking Sensor, page 8-31.

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure blocking devices.

Field Definitions

This section lists the field definitions for blocking devices, and contains the following topics:

- Blocking Devices Pane, page 8-19
- Add and Edit Blocking Devices Dialog Boxes, page 8-19

Blocking Devices Pane

The following fields and buttons are found in the Blocking Devices pane.

Field Descriptions:

- IP Address—IP address of the blocking device.
- Sensor's NAT Address—(Optional) NAT address of the sensor.
- Device Login Profile—Device login profile used to log in to the blocking device.
- Device Type—Type of device (Cisco Router, Cat 6K, PIX/ASA).

  The default is Cisco Router.
- Response Capabilities—Indicates whether the device uses blocking or rate limiting or both.
- Communication—Indicates the communication mechanism used to log in to the blocking device (SSH 3DES, SSH DES, Telnet).

  The default is SSH 3DES.

Button Functions:

- Add—Opens the Add Blocking Device dialog box. From this dialog box, you can add a blocking device.

  You receive an error message if the IP address already exists.
- Edit—Opens the Edit Blocking Device box. From this dialog box, you can change the values associated with this blocking device.
- Delete—Removes this blocking device from the list of blocking devices. You receive an error message if you try to delete a blocking device that is being used.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Blocking Devices Dialog Boxes

The following fields and buttons are found in the Add and Edit Blocking Device dialog boxes.

Field Descriptions:

- IP Address—IP address of the blocking device.
- Sensor's NAT Address—(Optional) NAT address of the sensor.
- Device Login Profile—Device login profile used to log in to the blocking device.

- Device Type—Type of device (Cisco Router, Cat 6K, PIX/ASA).

  The default is Cisco Router.
- Response Capabilities—Indicates whether the device uses blocking or rate limiting or both.
- Communication—Indicates the communication mechanism used to log in to the blocking device (SSH 3DES, SSH DES, Telnet).

  The default is SSH 3DES.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Blocking and Rate Limiting Devices

To configure blocking and rate limiting devices, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Blocking > Blocking Devices**.

The Blocking Devices pane appears.

Step 3 Click **Add** to add a blocking device.

You receive an error message if you have not configured the device login profile. For the procedure, see Configuring Device Login Profiles, page 8-14.

The Add Blocking Device dialog box appears.

Step 4 Enter the IP address of the blocking device in the IP Address field.

Step 5 (Optional) Enter the sensor's NAT address in the Sensor's NAT Address field.

Step 6 Choose the device login profile from the Device Login Profile drop-down list.

Step 7 Choose the device type from the Device Type drop-down list.

Step 8 Choose whether the device will perform blocking, rate limiting, or both by checking the Block and/or Rate Limit check boxes.

Note You must choose 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. For more information, see Assigning Actions to Signatures, page 5-23.

Step 9 Choose the communication type from the Communication drop-down list.

If you choose SSH 3DES or SSH DES, go to Step11.

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

Step 10 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 11 If you choose SSH 3DES or SSH DES, you must add the device to the known hosts list:

Note If you choose SSH 3DES or SSH DES, the blocking device must have a feature set or license that supports the desired 3DES/DES encryption.

Note You can also add the device to the known hosts list in the Configuration > SSH > Known Host Keys > Add Known Host Key dialog box. For the procedure, see Defining Known Host Keys, page 2-10.

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 12 To edit an existing entry in the blocking devices list, select it, and click **Edit**.

The Edit Blocking Device dialog box appears.

Step 13 Edit the sensor's NAT address if desired.

Step 14 Change the device login profile if desired.

Step 15 Change the device type if desired.

Step 16 Change whether the device will perform blocking or rate limiting if desired.

Step 17 Change the communication type if desired.

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

Step 18 Click **OK**.

The edited blocking device appears in the list in the Blocking Device pane.

Step 19 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 20 Click **Apply** to apply your changes and save the revised configuration.

Configuring Router Blocking or Rate Limiting Device Interfaces

This section describes how to configure the router blocking or rate limiting interfaces, and contains the following topics:

How the Sensor Manages Devices

ARC uses ACLs on Cisco routers and switches to manage those devices. These ACLs are built as follows:

Note ACLs do not apply to rate limiting devices.

1. A **permit** line with the sensor's 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 ARC reads the lines in the ACL and copies these lines to the beginning of the ACL.

3. Any active blocks
4. Either:
   - Post-Block ACL (if specified)

     This ACL must already exist on the device.

     Note 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.

– **permit ip any any** (not used if a Post-Block ACL is specified)

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. ARC then reverses the process on the next cycle.

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.

Note The ACLs that ARC creates are not removed from the managed device after you configure ARC to no longer manage that device. You must remove the ACLs manually on any device that ARC formerly managed.

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 device configuration.
3. Reenable blocking on the sensor.

When blocking is reenabled, the sensor reads the new device configuration. For the procedure, see Configuring Blocking Properties, page 8-6.

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 the procedure, see Configuring the Master Blocking Sensor, page 8-31.

Understanding Service Policies for Rate Limiting

IPS 5.1 does not support service policies that you define and apply in connection with rate limiting. They are not compatible with sensor rate limits. 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.

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.

Overview

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.

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.

Note Pre-Block and Post-Block ACLS do not apply to rate limiting.

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the router blocking device interfaces.

Field Definitions

This section lists the field definitions for router interfaces, and contains the following topics:

Router Blocking Device Interfaces Pane

The following fields and buttons are found in the Router Blocking Device Interfaces pane.

Field Descriptions:

- Router Blocking Device—IP address of the router blocking or rate limiting device.
- Blocking Interface—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—Direction to apply the blocking ACL.

  A valid value is In or Out.
- Pre-Block ACL—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—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.

Button Functions:

- Add—Opens the Add Router Blocking Device Interface dialog box. From this dialog box, you can add a router blocking or rate limiting device interface.

  You receive an error message if there are no router blocking devices.
- Edit—Opens the Edit Router Blocking Device Interface box. From this dialog box, you can change the values associated with this router blocking or rate limiting device interface.
- Delete—Removes this router blocking device interface from the list of router blocking device interfaces.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Router Blocking Device Interface Dialog Boxes

The following fields and buttons are found in the Add and Edit Router Blocking Device Interface dialog boxes.

Field Descriptions:

- Router Blocking Device—IP address of the router blocking or rate limiting device.
- Blocking Interface—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—Direction to apply the blocking ACL.

  A valid value is In or Out.
- Pre-Block ACL—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—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.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

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 IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Blocking > Router Blocking Device Interfaces**.

The Router Blocking Device Interfaces pane appears.

Step 3 Click **Add** to add a router blocking or rate limiting device interface.

The Add Router Blocking Device Interface dialog box appears.

Step 4 Choose the IP address of the router blocking or rate limiting device from the drop-down list.

Step 5 Enter the blocking or rate limiting interface name in the Blocking Interface field.

Step 6 Choose the direction (in or out) from the Direction drop-down list.

Step 7 (Optional) Enter the name of the Pre-Block ACL in the Pre-Block ACL field.

Note This step does not apply to rate limiting devices.

Step 8 (Optional) Enter the name of the Post-Block ACL in the Post-Block ACL field.

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 9 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 10 To edit an existing entry in the router blocking device interfaces list, select it, and click **Edit**.

The Edit Router Blocking Device dialog box appears.

Step 11 Edit the blocking or rate limiting interface name.

Step 12 Change the direction.

Step 13 (Optional) Edit the Pre-Block ACL name.

Step 14 (Optional) Edit the Post-Block ACL name.

Tip To discard your changes and close the Edit Router Blocking Device Interface dialog box, click **Cancel**.

Step 15 Click **OK**.

The edited router blocking or rate limiting device interface appears in the list in the Router Blocking Device Interfaces pane.

Step 16 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 17 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 switch interfaces,and contains the following topics:

Overview

You specify the VLAN ID and VACLs on the blocking Catalyst 6500 series switch on the Cat 6K Blocking Device Interfaces pane.

You can configure 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.

Note IDSM-2 inserts **permit ip any any capture** 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's 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the Catalyst 6500 series switches blocking device interfaces.

Field Definitions

This section lists the field definitions for the Catalyst 6500 series switch interfaces, and contains the following topics:

- Cat 6K Blocking Device Interfaces Pane, page 8-29
- Add and Edit Cat 6K Blocking Device Interface Dialog Boxes, page 8-29

Cat 6K Blocking Device Interfaces Pane

The following fields and buttons are found in the Cat 6K Blocking Device Interfaces pane.

Field Descriptions:

- Cat 6K Blocking Device—IP address of the Catalyst 6500 series switch blocking device.
- VLAN ID—VLAN ID to be used on the Catalyst 6500 series switch blocking device.

  The value is 1 to 4094.
- Pre-Block VACL—VACL to apply before the blocking VACL.

  The value is 0 to 64 characters.
- Post-Block VACL—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.

Button Functions:

- Add—Opens the Add Cat 6K Blocking Device Interface dialog box. From this dialog box, you can add a Catalyst 6500 series switch blocking device interface.

  You receive an error if there are no Catalyst 6500 series switches.
- Edit—Opens the Edit Cat 6K Blocking Device Interface box. From this dialog box, you can change the values associated with this Catalyst 6500 series switch blocking device interface.
- Delete—Removes this switch interface from the list of switch blocking device interfaces.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Cat 6K Blocking Device Interface Dialog Boxes

The following fields and buttons are found in the Add and Edit Cat 6K Blocking Device Interface dialog boxes.

Field Descriptions:

- Cat 6K Blocking Device—IP address of the Catalyst 6500 series switch blocking device.
- VLAN ID—VLAN ID to be used on the Catalyst 6500 series switch blocking device.

  The value is 1 to 4094.
- Pre-Block VACL—VACL to apply before the blocking VACL.

  The value is 0 to 64 characters.
- Post-Block VACL—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.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Cat 6K Blocking Device Interfaces

To configure Catalyst 6500 series switch blocking device interfaces, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Blocking > Cat 6K Blocking Device Interfaces**.

The Cat 6K Blocking Device Interfaces pane appears.

Step 3 Click **Add** to add a Catalyst 6500 series switch blocking device interface.

The Add Cat 6K Blocking Device Interface dialog box appears.

Step 4 Choose the IP address of the Catalyst 6500 series switch from the drop-down list.

Step 5 Enter the VLAN ID in the VLAN ID field.

Step 6 (Optional) Enter the name of the Pre-Block VACL in the Pre-Block VACL field.

Step 7 (Optional) Enter the name of the Post-Block VACL in the Post-Block VACL field.

Tip To discard your changes and close the Add Cat 6K Blocking Device Interface dialog box, click **Cancel**.

Step 8 Click **OK**.

You receive an error message if issued if the IP address/VLAN combination already exists.

The new interface appears in the list in the Cat 6K Blocking Device Interfaces pane.

Step 9 To edit an existing entry in the Catalyst 6500 series switch blocking device interfaces list, select it, and click **Edit**.

The Edit Cat 6K Blocking Device Interface dialog box appears.

Step 10 Edit the VLAN ID.

Step 11 Edit the Pre-Block VACL name.

Step 12 Edit the Post-Block VACL name.

Tip To discard your changes and close the Edit Cat 6K Blocking Device Interface dialog box, click **Cancel**.

Step 13 Click **OK**.

The edited Catalyst 6500 series switch blocking device interface appears in the list in the Cat 6K Blocking Device Interfaces pane.

Step 14 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 15 Click **Apply** to apply your changes and save the revised configuration.

Configuring the Master Blocking Sensor

This section describes how to configure the sensor to be a master blocking sensor, and contains the following topics:

Note A master blocking sensor can also operate as a master rate limiting sensor.

Overview

You specify the master blocking sensor that is used to control the blocking devices in the Master Blocking Sensor pane.

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.

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 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.

Master blocking sensors can also forward rate limits.

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure the master blocking sensor.

Field Definitions

This section lists the field definitions for the master blocking sensor, and contains the following topics:

- Master Blocking Sensor Pane, page 8-32
- Add and Edit Master Blocking Sensor Dialog Boxes, page 8-33

Master Blocking Sensor Pane

The following fields and buttons are found in the Master Blocking Sensor pane.

Field Descriptions:

- IP Address—IP address of the master blocking sensor.
- Port—Port on which to connect to the master blocking sensor.

  The default is 443.

- Username—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—Whether or not TLS is being used.

Button Functions:

- Add—Opens the Add Master Blocking Sensor dialog box. From this dialog box, you can add an master blocking sensor.
- Edit—Opens the Edit Master Blocking Sensor box. From this dialog box, you can change the values associated with this master blocking sensor.
- Delete—Removes this master blocking sensor from the list of master blocking sensors.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Master Blocking Sensor Dialog Boxes

The following fields and buttons are found in the Add and Edit Master Blocking Sensor dialog boxes.

Field Descriptions:

- IP Address—IP address of the master blocking sensor.

  You receive a warning if the IP address already exists.
- Port—(Optional) Port on which to connect on the master blocking sensor.

  The default is 443.
- Username—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.
- Change the password—Whether or not to change the password.
- New Password—Login password used to log in to the master blocking sensor.
- Confirm Password—Confirm the login password.
- Use TLS—Whether or not to use TLS.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring the Master Blocking Sensor

To configure the master blocking sensor, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Configuration > Blocking > Master Blocking Sensor**.

The Master Blocking Sensor pane appears.

Step 3 Click **Add** to add an master blocking sensor.

The Add Master Blocking Sensor dialog box appears.

Step 4 Enter the IP address of the master blocking sensor in the IP Address field.

Step 5 (Optional) Enter the port number in the Port field.

The default is 443.

Step 6 Enter the username in the Username field.

Step 7 Enter the password for the user in the Password field.

Step 8 Retype the password in the Confirm New Password field.

Step 9 Check the TLS check box.

Tip To discard your changes and close the Add Master Blocking Sensor dialog box, click **Cancel**.

Step 10 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 11 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 configure the blocking forwarding sensor to accept the X.509 certificate by choosing Configuration > Certificates > Trusted Hosts > Add Trusted Host. For the procedure, see Adding Trusted Hosts, page 2-15.

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
```

Note You are prompted to accept the certificate based on the certificate's fingerprint. Sensors provide only self-signed certificates (instead of certificates signed by a recognized certificate authority). You can verify the master blocking sensor host sensor's certificate by logging in to the host sensor and entering the **show tls fingerprint** command to see that the host certificate's fingerprints match.

Step 12 To edit an existing entry in the master blocking sensor list, select it, and click **Edit**.

The Edit Master Blocking Sensor dialog box appears.

Step 13 (Optional) Edit the port.

Step 14 Edit the username.

Step 15 Check the Change the password check box if you want to change the password for this user.

a. Enter the new password in the New Password field.

b. Confirm the new password in the Confirm New Password field.

Step 16 Check or uncheck the TLS check box.

Tip To discard your changes and close the Edit Master Blocking Sensor dialog box, click **Cancel**.

Step 17 Click **OK**.

The edited master blocking sensor appears in the list in the Master Blocking Sensor pane.

Step 18 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 19 Click **Apply** to apply your changes and save the revised configuration.

Managing Active Host Blocks

This section describes how to manage active host blocks, and contains the following topics:

Overview

Use the Active Host Blocks pane to configure and manage blocking of hosts.

An active 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.

An active 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure active host blocks.

Field Definitions

This section lists the field definitions for active host blocks, and contains the following topics:

- Active Host Blocks Pane, page 8-36
- Add Active Host Block Dialog Box, page 8-37

Active Host Blocks Pane

The following fields and buttons are found in the Active Host Blocks pane.

Field Descriptions:

- Source IP—Source IP address for the block.
- Destination IP—Destination IP address for the block.
- Destination Port—Destination port for the block.
- Protocol—Type of protocol (TCP, UDP, or ANY).

  The default is ANY.
- Minutes Remaining—Time remaining for the blocks in minutes.
- Timeout (minutes)—Original timeout value for the block in minutes.

  A valid value is between 1 to 70560 minutes (49 days).
- VLAN— Indicates the VLAN that carried the data that fired the signature.

Caution Even though the VLAN ID is included in the block request, it is not passed to the firewall. Sensors cannot block on FWSM 2.1 or greater when logged in to the admin context.

- Connection Block Enabled—Whether or not to block the connection for the host.

Button Functions:

- Add—Opens the Add Active Host Block dialog box. From this dialog box, you can add a manual block for a host.
- Delete—Removes this manual block from the list of active host blocks.
- Refresh—Refreshes the contents of the table.

Add Active Host Block Dialog Box

The following fields and buttons are found in the Add Active Host Block dialog box.

Field Descriptions:

- Source IP—Source IP address for the block.
- Enable connection blocking—Whether or not to block the connection for the host.
- Connection Blocking—Lets you configure parameters for connection blocking:
  - Destination IP—Destination IP address for the block.
  - Destination Port—(Optional) Destination port for the block.
  - Protocol—(Optional) Type of protocol (TCP, UDP, or ANY).

    The default is ANY.
- VLAN—(Optional) Indicates the VLAN that carried the data that fired the signature.

Caution Even though the VLAN ID is included in the block request, it is not passed to the firewall. 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—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.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring and Managing Active Host Blocks

To configure and manage active host blocks, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Monitoring > Active Host Blocks**.

The Active Host Blocks pane appears.

Step 3 Click **Add** to add an active host block.

The Add Active Host Block dialog box appears.

Step 4 Enter the source IP address of the host you want blocked.

Step 5 Check the Enable Connection Blocking check box if you want the block to be connection-based.

Note A connection block blocks traffic from a given source IP address to a given destination IP address and destination port.

a. Enter the destination IP address in the Destination IP field.

b. (Optional) Enter the destination port in the Destination Port field.

c. Choose the protocol from the Protocol drop-down list.

Step 6 (Optional) Enter the VLAN for the connection block in the VLAN field.

Step 7 Check the Enable Timeout check box if you want to configure the block for a specified amount of time.

Step 8 Enter the amount of time in minutes in the Timeout field.

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

Step 9 Check the No Timeout check box if you do not want to configure the block for a specified amount of time.

Step 10 Click **Apply**.

You receive an error message if a block is configured for that IP address.

The new active host block appears in the list in the Active Host Blocks pane.

Step 11 Click **Refresh** to refresh the contents of the active host blocks list.

Step 12 To delete a block, choose an active host block in the list, and click **Delete**.

The Delete Active Host Block dialog box asks if you are sure you want to delete this block.

Tip To discard your changes and close the Delete Active Host Block dialog box, click **Cancel**.

Step 13 Click **Yes** to delete the block.

Managing Network Blocks

This section describes how to manage network blocks, and contains the following topics:

Overview

Use the Network Blocks pane to configure and managing 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure network blocks.

Field Definitions

This section lists the field definitions for network blocks, and contains the following topics:

Network Blocks Pane

The following fields and buttons are found in the Network Blocks pane.

Field Descriptions:

- IP Address—IP address for the block.
- Mask—Network mask for the block.
- Minutes Remaining—Time remaining for the blocks in minutes.

- Timeout (minutes)—Original timeout value for the block in minutes.

  A valid value is between 1 and 70560 minutes (49 days).

Button Functions:

- Add—Opens the Add Network Block dialog box. From this dialog box, you can add a block for a network.
- Delete—Removes this network block from the list of blocks.
- Refresh—Refreshes the contents of the table.

Add Network Block Dialog Box

The following fields and buttons are found in the Add Network Block dialog box.

Field Descriptions:

- Source IP—IP address for the block.
- Netmask—Network mask for the block.
- Enable Timeout—Indicates a timeout value for the block in minutes.
- Timeout—Indicates 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.

Button Functions:

- Apply—Sends this block to the sensor immediately.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring and Managing Network Blocks

To configure and manage network blocks, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Monitoring > Features > IPS >Network Blocks**.

The Network Blocks pane appears.

Step 3 Click **Add** to add a network block.

The Add Network Block dialog box appears.

Step 4 Enter the source IP address of the network you want blocked.

Step 5 Choose the netmask from the Netmask drop-down list.

Step 6 Check the Enable Timeout check box if you want to configure the block for a specified amount of time.

Step 7 Enter the amount of time in minutes in the Timeout field.

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

Step 8 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 9 Click **Refresh** to refresh the contents of the network blocks list.

Step 10 Choose 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 11 Click **Yes** to delete the block.

CHAPTER 9

Configuring SNMP

Note To have the sensor send SNMP traps, you must also choose Request SNMP Trap as the event action when you configure signatures. For more information, see Assigning Actions to Signatures, page 5-23.

This chapter describes how to configure the sensor to use SNMP and SNMP traps. This chapter 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.

Configuring SNMP

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

Overview

Use the SNMP General Configuration pane to configure the sensor to use SNMP.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure the sensor to use SNMP.

Field Definitions

The following fields and buttons are found in the SNMP General Configuration pane.

Field Descriptions:

- Enable SNMP Gets/Sets—If checked, allows SNMP gets and sets.
- SNMP Agent Parameters—Configures the parameters for SNMP agent.
  - Read-Only Community String—Identifies the community string for read-only access.
  - Read-Write Community String—Identifies the community string for read and write access.
  - Sensor Contact—Identifies the contact person, contact point, or both for the sensor.
  - Sensor Location—Identifies the location of the sensor.

- Sensor Agent Port—Identifies the IP port of the sensor.

  The default is 161.
- Sensor Agent Protocol—Identifies the IP protocol of the sensor.

  The default is UDP.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring SNMP

Note To have the sensor send SNMP traps, you must also choose Request SNMP Trap as the event action when you configure signatures. For more information, see Assigning Actions to Signatures, page 5-23.

To set the general SNMP parameters, follow these steps:

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

Step 2 Choose **Configuration > SNMP > SNMP General Configuration**.

The SNMP General Configuration pane appears.

Step 3 Check the Enable SNMP Gets/Sets check box to enable SNMP so that the SNMP management workstation can issue requests to the sensor SNMP agent.

Step 4 Configure the SNMP agent parameters:

These are the values that the SNMP management workstation can request from the sensor SNMP agent.

a. Assign the read-only community string in the Read-Only Community String field.

The read-only community string helps to identify the sensor SNMP agent.

b. Assign the read-write community string in the Read-Write Community String field.

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. Enter the sensor contact user ID in the Sensor Contact field.

d. Enter the location of the sensor in the Sensor Location field.

e. Enter the port of the sensor SNMP agent in the Sensor Agent Port field.

The default SNMP port number is 161.

f. Choose the protocol the sensor SNMP agent will use from the Sensor Agent Protocol list.

g. 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 SNMP Traps

This section describes how to configure SNMP traps, and contains the following topics:

Overview

Use the SNMP 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure SNMP traps on the sensor.

Field Definitions

This section lists the field definitions for SNMP traps, and contains the following topics:

SNMP Traps Configuration Pane

The following fields and buttons are found in the SNMP Traps Configuration pane.

Field Descriptions:

- Enable SNMP Traps—If checked, indicates the remote server will use a pull update.
- Select 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.
- Default Trap Community String—The community string used for the traps if no specific string has been set for the trap.
- Specify SNMP trap destinations—Identifies the destination for the trap.

  You must specify the following information about the destination:
  - IP Address—The IP address of the trap destination.
  - UDP Port—The UDP port of the trap destination.
  - Trap Community String—The trap community string.

Button Functions:

- Add—Opens the Add SNMP Trap Destination dialog box. From this dialog box you can add a new destination for SNMP traps.
- Edit—Opens the Edit SNMP Trap Destination dialog box. From this dialog box you can change the parameters that define the chosen destination.
- Delete—Deletes the chosen destination.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit SNMP Trap Destination Dialog Boxes

The following fields and buttons are found in the Add and Edit SNMP Trap Destination dialog boxes.

Field Descriptions:

- IP Address—The IP address of the trap destination.
- UDP Port—The UDP port of the trap destination.

  The default is port 162.
- Trap Community String—The trap community string.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring SNMP Traps

Note To have the sensor send SNMP traps, you must also choose Request SNMP Trap as the event action when you configure signatures. For more information, see Assigning Actions to Signatures, page 5-23.

To configure SNMP traps, follow these steps:

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

Step 2 Choose **Configuration > SNMP > SNMP Traps Configuration**.

The SNMP Traps Configuration pane appears.

Step 3 Check the Enable SNMP Traps check box to enable SNMP traps.

Step 4 Set the parameters for the SNMP trap:

a. Choose 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. Choose whether you want detailed SNMP traps by checking the Enable detailed traps for alerts check box.

c. Enter the community string to be included in the detailed traps in the Default Trap Community String field.

Step 5 Set the parameters for the SNMP trap destinations so the sensor knows which management workstations to send them to:

a. Click **Add**.

The Add SNMP Trap Destination dialog box appears.

b. Enter the IP address of the SNMP management station in the IP Address field.

c. Enter the UDP port of the SNMP management station in the UDP Port field.

d. Enter the trap Community string in the Trap Community String field.

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.

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 SNMP Traps Configuration pane.

Step 7 To edit an SNMP trap destination, select it, and click **Edit**.

The Edit SNMP Trap Destination dialog box appears.

Step 8 Edit the UDP Port and Trap Community String fields.

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 SNMP 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 SNMP 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

The following private MIBs are supported on the sensor:

- CISCO-CIDS-MIB
- 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.

CHAPTER 10

Maintaining the Sensor

This chapter describes how to maintain the sensor by automatically updating the sensor with the latest software, or updating it immediately, restoring the factory defaults, and shutting down the sensor. You can also generate information for troubleshooting purposes and to use if you need to contact TAC.

This chapter contains the following sections:

Updating the Sensor Automatically

This section describes how to configure the sensor for automatic updates, and contains the following topics:

Overview

You can configure automatic service pack and signature updates, so that when service pack or signature updates are loaded on a central FTP or SCP server, they are downloaded and applied to your sensor.

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.

Note The sensor cannot automatically download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP or SCP server, and then configure the sensor to download them from the FTP or SCP server.

Caution After you download an update from Cisco.com, you must take steps to ensure the integrity of the downloaded file while it resides on your FTP or SCP server.

UNIX-Style Directory Listings

To configure Auto 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 Auto 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.

Supported User Role

You must be Administrator view the Auto Update pane and to configure automatic updates.

Field Definitions

The following fields and buttons are found in the Auto Update pane.

Field Descriptions:

- Enable Auto Update—Lets the sensor install updates stored on a remote server.

  If Enable Auto Update is not selected, all fields are disabled and cleared. You cannot toggle this on or off without losing all other settings.
- Remote Server Settings—Lets you specify the following options:
  - IP Address—Identifies the IP address of the remote server.
  - File Copy Protocol—Specifies whether to use FTP or SCP.
  - Directory—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.
  - Confirm Password—Confirms the password by forcing you to retype the remote server password.
- Schedule—Lets you specify the following 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.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Auto Update

To configure automatic updates, follow these steps:

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

Step 2 Choose **Configuration > Auto Update**.

The Auto Update pane appears.

Step 3 Check the **Enable Auto Update** check box to enable automatic updates.

Step 4 Enter the IP address of the remote server where you have downloaded and stored updates in the IP Address field.

Step 5 Choose either FTP or SCP from the File Copy Protocol list to identify the protocol used to connect to the remote server.

Step 6 Enter the path to the directory on the remote server where the updates are located in the Directory field.

A valid value for the path is 1 to 128 characters.

Step 7 Enter the username to use when logging in to the remote server in the Username field.

A valid value for the username is 1 to 2047 characters.

Step 8 Enter the username password on the remote server in the Password field.

A valid value for the password is 1 to 2047 characters.

Step 9 Repeat the password in the Confirm Password field.

Step 10 For hourly updates, select Hourly, and follow these steps:

a. Enter the time you want the updates to start in the Start Time field.

The valid value is hh:mm:ss.

b. Enter the hour interval at which you want every update to occur in the Every_hours field.

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.

Step 11 For weekly updates, select Daily, and follow these steps:

a. Enter the time you want the updates to start in the Start Time field.

The valid value is hh:mm:ss.

b. Choose the day(s) you want the sensor to check for and download available updates in the Days field.

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

Step 12 Click **Apply** to save your changes.

Restoring the Defaults

This section describes how to restore factory defaults to the sensor, and contains the following topics:

Overview

You can restore the default configuration 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.**

Supported User Role

You must be Administrator to view the Restore Defaults pane and to restore the sensor defaults.

Field Definitions

The following buttons are found in the Restore Defaults pane.

Button Functions:

- Restore Defaults—Opens the Restore Defaults dialog box. From this dialog box, you can begin the restore defaults process. This process returns the sensor configuration to the default settings and immediately terminates connection to the sensor.
- OK—Starts the restore defaults process.
- Cancel—Closes the Restore Defaults dialog box and returns you to the Restore Defaults pane without performing the restore defaults process.

Restoring the Defaults

To restore the default configuration, follow these steps:

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

Step 2 Choose **Configuration >Restore Defaults**.

The Restore Defaults pane appears.

Step 3 Click **Restore Configuration Defaults** to restore the default configuration.

The Restore Defaults dialog box appears.

Step 4 Click **Yes** to begin the restore defaults process.

Note Restoring defaults resets the IP address, netmask, default gateway, and access list. The password, and time will not be reset. Manual and automatic blocks also remain in effect.

Rebooting the Sensor

This section describes how to reboot the sensor from IDM, and contains the following topics:

Overview

You can shut down and restart the sensor from the Reboot Sensor pane.

Supported User Role

You must be Administrator to see the Reboot Sensor pane and to reboot the sensor.

Field Definitions

The following buttons are found in the Reboot Sensor pane.

Button Functions:

- Reboot Sensor—Opens the Reboot Sensor dialog box. From this dialog box, you can begin the process that shuts down and restarts the sensor.
- OK—Shuts down and restarts the sensor, causing you to immediately lose connection with the sensor. You can log back in after the senor restarts.
- Cancel—Closes the Reboot Sensor dialog box and returns you to the Reboot Sensor pane without shutting down the sensor.

Rebooting the Sensor

To reboot the sensor, follow these steps:

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

Step 2 Choose **Configuration > Reboot Sensor**.

The Reboot Sensor pane appears.

Step 3 Click **Reboot Sensor**.

The Reboot Sensor dialog box appears.

Step 4 Click **OK** to shut down and restart the sensor.

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

This section describes how to shut down the sensor from IDM, and contains the following topics:

Overview

You can shut down the IPS applications and then put the sensor in a state in which it is safe to power it off.

Supported User Role

You must be Administrator to view the Shut Down Sensor pane and to shut down the sensor.

Field Definitions

The following fields and buttons are found in the Shut Down Sensor pane.

Button Functions:

- Shut Down Sensor—Opens the Shut Down Sensor dialog box. From this dialog box you can begin the process that shuts down the sensor.
- OK—Shuts down the sensor and immediately closes any open connections to the sensor.
- Cancel—Closes the Shut Down Sensor dialog box without beginning the shutdown process.

Shutting Down the Sensor

To shut down the sensor, follow these steps:

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

Step 2 Choose **Configuration > Shut Down Sensor.**

The Shut Down Sensor pane appears.

Step 3 Click **Shut Down Sensor**.

The Shut Down Sensor dialog box appears.

Step 4 Click **OK** to shut down the sensor.

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.

Updating the Sensor

This section describes how to update the sensor with the most current software, and contains the following topics:

Overview

From the Update Sensor pane, you can immediately apply service pack and signature updates.

Note The sensor cannot download service pack and signature updates from Cisco.com. 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.

Supported User Role

You must be Administrator to view the Update Sensor pane and to update the sensor with service packs and signature updates.

Field Definitions

The following fields and buttons are found in the Update Sensor pane.

Field Descriptions:

- 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/S, 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.

Button Functions:

- Update Sensor—Opens the Update Sensor dialog box. From this dialog box, you can initiate an instant update.
- OK—Immediately updates the sensor, according to the parameters you have set in the Update Sensor pane.
- Cancel—Closes the Update Sensor dialog box without performing any updates.

Updating the Sensor

To immediately apply a service pack and signature update, follow these steps:

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

Step 2 Choose **Configuration > Update Sensor**.

The Update Sensor pane appears.

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. Enter the URL where the update can be found in the URL field.

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.

  The syntax for this prefix is the following:

  `https://location/directory/filename`

Note Before using the HTTPS protocol, use the **tls trusted-host** command to set up a TLS trusted host.

- 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`

Note You must have already downloaded the update from Cisco.com and put it on the FTP server.

c. Enter the username for an account on the remote server in the Username field.

d. Enter the password associated with this account on the remote server in the Password field.

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.

Tip To discard your changes and close the Update Sensor dialog box, click **Cancel**.

Note The IDM and CLI connection are lost during the following updates: service pack, minor, major, and engineering patch. If you are applying one of these updates, the installer automatically 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.

Generating a Diagnostics Report

This section describes how to generate a diagnostics report, and contains the following topics:

Overview

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.

Note Generating a diagnostics report can take a few minutes.

You can view the report in the Diagnostics Report pane or you can click **Save** and save it to the hard-disk drive.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to run diagnostics.

Field Definitions

The following button is found in the Diagnostics Report pane.

Button Functions:

- 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

To run diagnostics, follow these steps:

Caution After you start the diagnostics process, do not click any other options in IDM or leave the Diagnostics pane. This process must be completed before you can perform any other tasks for the sensor.

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

Step 2 Choose **Monitoring > Support Information > Diagnostics Report**.

The Diagnostics pane appears.

Step 3 Click **Generate New 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.

Note 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

This section describes how to view sensor statistics, and contains the following topics:

Overview

The Statistics pane shows statistics for the following categories:

- Analysis Engine
- Event Server
- Event Store
- Host
- Interface Configuration
- Logger
- Attack Response Controller (formerly known as Network Access Controller)
- Notification
- Transaction Server
- Transaction Source
- Virtual Sensor
- Web Server

Supported User Role

Administrators, Operators, and Viewers can view system statistics.

Field Definitions

The following button is found in the Statistics pane.

Button Functions:

- Refresh—Displays the most recent information about the sensor applications, including the Web Server, Transaction Source, Transaction Server, Network Access Controller (known as Attack Response Controller in IPS 5.1 but still listed as Network Access Controller in the statistics), Logger, Host, Event Store, Event Server, Analysis Engine, Interface Configuration, and Authentication.

Viewing Statistics

To show statistics for your sensor, follow these steps:

Step 1 Choose **Monitoring > Support Information > Statistics**.

The Statistics page appears.

Step 2 To update statistics as they change, click **Refresh**.

Viewing System Information

This section describes how to view system information, and contains the following topics:

Overview

The System Information pane displays following information:

- TAC contact information
- How long the sensor has been running
- Type of sensor
- Software version
- Status of applications
- Upgrades installed

- PEP information
- Memory usage
- Disk usage

Supported User Role

You must be Administrator or Operator to view system information. Viewers can see all of the system information except for how long the sensor has been running and the disk usage.

Field Definitions

The following button is found in the System Information pane.

Button Functions:

- 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 Choose **Monitoring > Support Information > System Information**.

The System Information pane displays information about the system.

Step 2 Click **Refresh**.

The pane refreshes and displays new information.

CHAPTER 11

Monitoring the Sensor

This chapter describes how to monitor and clear the denied attackers list, how to monitor and configure active host blocks and network blocks, how to configure and manage rate limits, and how to configure and download IP logs. This chapter contains the following sections:

Denied Attackers

This section describes how to configure the denied attackers list, and contains the following topics:

Overview

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to monitor and clear the denied attackers list.

Field Definitions

The following fields and buttons are found in the Denied Attackers pane.

Field Descriptions:

- Attacker IP—IP address of the attacker the sensor is denying.
- Victim IP—IP address of the victim the sensor is denying.
- Port—Port of the host the sensor is denying.
- Protocol—Protocol that the attacker is using.
- Percentage—Percentage of traffic that has been denied by the sensor in inline mode.
- Hit Count—Displays the hit count for that denied attacker.
- Virtual Sensor—Name of the virtual sensor. Currently IPS 5.1 only supports one virtual sensor, vs0.

Button Functions:

- Reset All Hit Counts—Clears the hit count for the denied attackers.
- Clear List—Clears the list of the denied attackers.
- Refresh—Refreshes the contents of the pane.

Monitoring the Denied Attackers List

To view the list of denied attackers and their hit counts, follow these steps:

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

Step 2 Choose **Monitoring > Denied Attackers**.

The Denied Attackers pane appears.

Step 3 Click **Refresh** to refresh the list.

Step 4 Click **Reset All Hit Counts** to have the hit count start over.

Step 5 Click **Clear List** to clear the entire list of denied attackers.

Configuring and Managing Active Host Blocks

This section describes how to manage active host blocks, and contains the following topics:

Overview

Use the Active Host Blocks pane to configure and manage blocking of hosts.

An active 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.

An active 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure active host blocks.

Field Definitions

This section lists the field definitions for active host blocks, and contains the following topics:

- Active Host Blocks Pane, page 11-3
- Add Active Host Block Dialog Box, page 11-4

Active Host Blocks Pane

The following fields and buttons are found in the Active Host Blocks pane.

Field Descriptions:

- Source IP—Source IP address for the block.
- Destination IP—Destination IP address for the block.
- Destination Port—Destination port for the block.
- Protocol—Type of protocol (TCP, UDP, or ANY).

  The default is ANY.
- Minutes Remaining—Time remaining for the blocks in minutes.
- Timeout (minutes)—Original timeout value for the block in minutes.

  A valid value is between 1 to 70560 minutes (49 days).

- VLAN— Indicates the VLAN that carried the data that fired the signature.

Caution Even though the VLAN ID is included in the block request, it is not passed to the firewall. Sensors cannot block on FWSM 2.1 or greater when logged in to the admin context.

- Connection Block Enabled—Whether or not to block the connection for the host.

Button Functions:

- Add—Opens the Add Active Host Block dialog box.

  From this dialog box, you can add a manual block for a host.
- Delete—Removes this manual block from the list of active host blocks.
- Refresh—Refreshes the contents of the table.

Add Active Host Block Dialog Box

The following fields and buttons are found in the Add Active Host Block dialog box.

Field Descriptions:

- Source IP—Source IP address for the block.
- Enable connection blocking—Whether or not to block the connection for the host.
- Connection Blocking—Lets you configure parameters for connection blocking:
  - Destination IP—Destination IP address for the block.
  - Destination Port—(Optional) Destination port for the block.
  - Protocol—(Optional) Type of protocol (TCP, UDP, or ANY).

    The default is ANY.
- VLAN—(Optional) Indicates the VLAN that carried the data that fired the signature.

Caution Even though the VLAN ID is included in the block request, it is not passed to the firewall. Sensors cannot block on FWSM 2.1 or later when logged in to the admin context.

  This field is optional.
- Enable Timeout—Lets you set a timeout value for the block in minutes.
- Timeout—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.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring and Managing Active Host Blocks

To configure and manage active host blocks, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Monitoring > Active Host Blocks**.

The Active Host Blocks pane appears.

Step 3 Click **Add** to add an active host block.

The Add Active Host Block dialog box appears.

Step 4 Enter the source IP address of the host you want blocked.

Step 5 Check the Enable Connection Blocking check box if you want the block to be connection-based.

Note A connection block blocks traffic from a given source IP address to a given destination IP address and destination port.

a. Enter the destination IP address in the Destination IP field.

b. (Optional) Enter the destination port in the Destination Port field.

c. Choose the protocol from the Protocol list.

Step 6 (Optional) Enter the VLAN for the connection block in the VLAN field.

Step 7 Check the Enable Timeout check box if you want to configure the block for a specified amount of time.

Step 8 Enter the amount of time in minutes in the Timeout field.

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

Step 9 Check the No Timeout check box if you do not want to configure the block for a specified amount of time.

Step 10 Click **Apply**.

You receive an error message if a block is configured for that IP address.

The new active host block appears in the list in the Active Host Blocks pane.

Step 11 Click **Refresh** to refresh the contents of the active host blocks list.

Step 12 To delete a block, select an active host block in the list, and click **Delete**.

The Delete Active Host Block dialog box asks if you are sure you want to delete this block.

Tip To discard your changes and close the Delete Active Host Block dialog box, click **Cancel**.

Step 13 Click **Yes** to delete the block.

Configuring and Managing Network Blocks

This section describes how to manage network blocks, and contains the following topics:

Overview

Use the Network Blocks pane to configure and managing 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure network blocks.

Field Definitions

This section lists the field definitions for network blocks, and contains the following topics:

Network Blocks Pane

The following fields and buttons are found in the Network Blocks pane.

Field Descriptions:

- IP Address—IP address for the block.
- Mask—Network mask for the block.

- Minutes Remaining—Time remaining for the blocks in minutes.
- Timeout (minutes)—Original timeout value for the block in minutes.

  A valid value is between 1 and 70560 minutes (49 days).

Button Functions:

- Add—Opens the Add Network Block dialog box.

  From this dialog box, you can add a block for a network.
- Delete—Removes this network block from the list of blocks.
- Refresh—Refreshes the contents of the table.

Add Network Block Dialog Box

The following fields and buttons are found in the Add Network Block dialog box.

Field Descriptions:

- Source IP—IP address for the block.
- Netmask—Network mask for the block.
- Enable Timeout—Indicates a timeout value for the block in minutes.
- Timeout—Indicates 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.

Button Functions:

- Apply—Sends this block to the sensor immediately.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring and Managing Network Blocks

To configure and manage network blocks, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Monitoring > Network Blocks**.

The Network Blocks pane appears.

Step 3 Click **Add** to add a network block.

The Add Network Block dialog box appears.

Step 4 Enter the source IP address of the network you want blocked.

Step 5 Choose the netmask from the Netmask list.

Step 6 Check the Enable Timeout check box if you want to configure the block for a specified amount of time.

Step 7 Enter the amount of time in minutes in the Timeout field.

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

Step 8 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 9 Click **Refresh** to refresh the contents of the network blocks list.

Step 10 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 11 Click **Yes** to delete the block.

Configuring and Managing Rate Limits

This section describes rate limiting and how to configure it. It contains the following sections:

Overview

Rate limiting lets sensors restrict the rate of specified traffic classes on network devices. Rate limit responses are supported for the Host Flood and Net Flood engines, and the TCP half-open SYN signature. ARC can configure rate limits on network devices running Cisco IOS version 12.3 or later. For configuring rate limiting on routers, see Configuring Router Blocking or Rate Limiting Device Interfaces, page 8-22. Master blocking sensors can also forward rate limit requests to blocking forwarding sensors. For more information, see Configuring the Master Blocking Sensor, page 8-31.

You can view the active rate limit list in the ARC statistics. For more information, see Viewing Statistics, page 10-12.

To add a rate limit, you specify a combination of protocol, destination IP address, and data value to match one of the signatures that are allowed to generate rate limit events. For the procedure, see Configuring and Managing Rate Limits, page 11-10. You must also set the action to Request Rate Limit and set the percentage for these signatures.

Table 11-1 lists the supported signatures and parameters.

Table 11-1 Rate Limit 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

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator or Operator to configure rate limits.

Field Definitions

This section lists the field definitions for rate limits, and contains the following topics:

- Rate Limits Pane, page 11-9
- Add Rate Limit Dialog Box, page 11-10

Rate Limits Pane

The following fields and buttons are found in the Rate Limits pane.

Field Descriptions:

- Protocol—Protocol of the traffic that is rate limited.
- Rate—Percent of maximum bandwidth that is allowed for the rate-limited traffic.

  Matching traffic that exceeds this rate will be dropped.
- Source IP—(Optional) Source host IP address of the rate-limited traffic.
- Source Port—(Optional) Source host port of the rate-limited traffic.
- Destination IP—Destination Host IP address of the rate-limited traffic.
- Destination Port—(Optional) Destination host port of the rate-limited traffic.

- Data—(Optional) 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—Remaining minutes that this rate limit is in effect.
- Timeout (minutes)—Total number of minutes for this rate limit.

Button Functions:

- Add—Opens the Add Rate Limit dialog box.

  From this dialog box, you can configure the options for rate limiting.
- Delete—Deletes this entry from the table.
- Refresh—Refreshes the contents of the table.

Add Rate Limit Dialog Box

The following fields and buttons are found in the Add Rate Limit dialog box.

Field Descriptions:

- Protocol—Protocol of the traffic that is rate-limited (ICMP, TCP, or UDP).
- Rate—Percentage of the maximum bandwidth allowed for the rate-limited traffic.
- Source IP—(Optional) Source host IP address of the rate-limited traffic.
- Source Port—(Optional) Source host port of the rate-limited traffic.
- Destination IP—(Optional) Destination host IP address of the rate-limited traffic.
- Destination Port—(Optional) Destination host port of the rate-limited traffic.
- Use Additional Data—(Optional) 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—Timeout not enabled.
  - Enable Timeout—Lets you specify the timeout in minutes (1 to 70560).

Button Functions:

- Apply—Applies your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring and Managing Rate Limits

To configure and manage rate limiting, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Monitoring > Rate Limits**.

The Rate Limits pane appears.

Step 3 Click **Add** to add a rate limit.

The Add Rate Limit dialog box appears.

Step 4 Choose the protocol (ICMP, TCP, or UDP) of the traffic you want rate limited from the Protocol list.

Step 5 Enter the rate limit (1 to 100) in the Rate field.

Step 6 (Optional) Enter the destination IP address in the Destination IP field.

Step 7 Check the Use Additional Data check box if you want to configure the rate limit to use additional data.

Step 8 Choose the additional data (echo-reply, echo-request, or halfOpenSyn) from the Select Data list.

Step 9 Check the Enable Timeout check box if you want to configure a timeout in minutes.

Step 10 Enter the amount of time in minutes (1 to 70560) in the Timeout field.

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

Step 11 Check the **No Timeout** check box if you do not want to configure the rate limit for a specified amount of time.

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.

Configuring IP Logging

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.

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.

Caution Turning on IP logging slows system performance.

This section contains the following topics:

Overview

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 choose 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator

You must be Administrator or Operator to configure IP logging.

Field Definitions

This section lists the field definitions for IP logging, and contains the following topics:

IP Logging Pane

The following fields and buttons are found in the IP Logging pane.

Field Descriptions:

- Log ID—ID of the IP log.
- IP Address—IP address of the host for which the log is being captured.
- Status—Status of the IP log.

  Valid values are added, started, or completed.
- Event Alert—Event alert, if any, that triggered the IP log.
- Start Time—Timestamp of the first captured packet.
- Current End Time—Timestamp of the last captured packet.

  There is no timestamp if the capture is not complete.
- Packets Captured—Current count of the packets captured.
- Bytes Captured—Current count of the bytes captured.

Button Functions:

- Add—Opens the Add IP Logging dialog box. From this dialog box, you can add an IP log.
- Edit—Opens the Edit IP Logging box. From this dialog box, you can change the values associated with this IP log.
- Download—Applies your changes and saves the revised configuration.
- Stop—Stops capturing for an IP log that is started.
- Refresh—Refreshes the contents of the table.

Add and Edit IP Logging Dialog Boxes

The following fields and buttons are found in the Add and Edit IP Logging dialog boxes.

Field Descriptions:

- IP Address—IP address of the host for which the log is being captured.
- Maximum Values—Lets you set the values for IP logging.
  - Duration—Maximum duration to capture packets.

    Note For the Edit IP Logging dialog box, the Duration field is the time that is extended once you apply the edit to IP logging.

    The range is 1 to 60 minutes. The default is 10 minutes.
  - Packets—(Optional) Maximum number of packets to capture.

    The range is 1 to 4294967295 packets.
  - Bytes—(Optional) Maximum number of bytes to capture.

    The range is 0 to 4294967295 bytes.

Button Functions:

- Apply—Accepts your changes and closes the dialog box.

- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring IP Logging

To log IP traffic for a particular host, follow these steps:

Step 1 Log in to IDM using an account with administrator or operator privileges.

Step 2 Choose **Monitoring > IP Logging**.

The IP Logging pane appears.

Step 3 Click **Add** to add IP logging.

The Add IP Logging dialog box appears.

Step 4 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.

Step 5 Enter how many minutes you want IP logs to be captured in the Duration field.

Step 6 (Optional) Enter how many packets you want to be captured in the Packets field.

Step 7 (Optional) Enter how many bytes you want to be captured in the Bytes field.

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 edit an existing log entry in the list, select it, and click **Edit**.

The Edit IP Logging dialog box appears.

Step 10 Edit the duration you want packets to be captured.

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

The edited IP log appears in the list in the IP Logging pane.

Step 12 To stop IP logging, select the log ID for the log you want to stop and click **Stop**.

The Stop IP Logging dialog box appears.

Step 13 Click **OK** to stop IP logging for that log.

Step 14 To download an IP log, select the log ID, and click **Download**.

The Save As dialog box appears.

Step 15 Save the log to your local machine. You can view it with Wireshark.

CHAPTER 12

Obtaining Software

This chapter provides information on obtaining Cisco IPS software for the sensor. It contains the following sections:

Caution The BIOS on Cisco IDS/IPS sensors is specific to Cisco IDS/IPS sensors and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on Cisco IDS/IPS sensors voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 12-1.

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.

Note You must be logged in to Cisco.com to download software.

Signature updates are posted to Cisco.com approximately every week, more often if needed. Service packs are posted to Cisco.com as needed. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.

Note You must have an active IPS maintenance contract and a Cisco.com password to download software. You must have a license to apply signature updates.

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 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.

- Fill out the form and click **Submit**.

  The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.

- 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.

The File Download dialog box appears.

Step 11 Open the file or save it to your computer.

Step 12 Follow the instructions in the Readme to install the update.

Note Major and minor updates, service packs, recovery files, signature and signature engine updates are the same for all sensors. System image files are unique per platform.

IPS Software Versioning

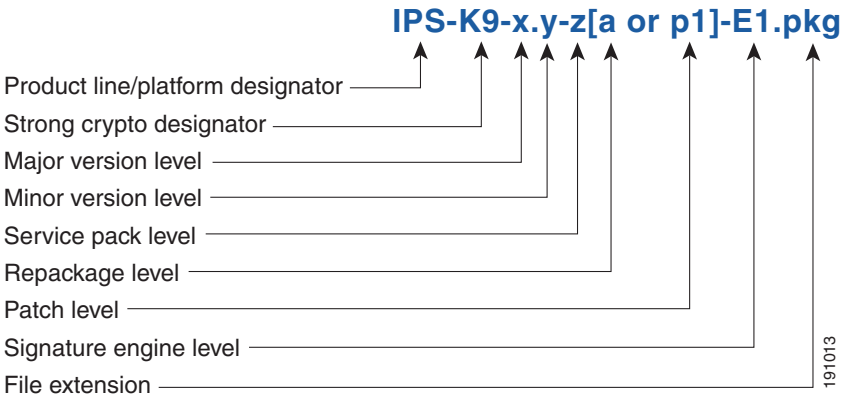
When you download IPS software images from Cisco.com, you should understand the versioning scheme so that you know which files are base files, which are cumulative, and which are incremental.

This section describes the various IPS software files, gives software release examples, and contains the following topics:

Major and Minor Updates, Service Packs, and Patch Releases

Figure 12-1 illustrates what each part of the IPS software file represents for major and minor updates, service packs, and patch releases.

Figure 12-1 IPS Software File Name for Major and Minor Updates, Service Packs, and Patch Releases



Major Update

Contains new functionality or an architectural change in the product. For example, the IPS 5.0 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 5.0(1) requires 4.*x*. With each major update there are corresponding system and recovery packages.

Note The 5.0(1) major update is only used to upgrade 4.*x* sensors to 5.0(1). If you are reinstalling 5.0(1) on a sensor that already has 5.0(1) installed, use the system image or recovery procedures rather than the major update.

Minor Update

Incremental to the major version. Minor updates are also base versions for service packs. The first minor update for 5.0 is 5.1(1). 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 Packs

Cumulative following a base version release (minor or major). Service packs are used for the release of defect fixes with no new enhancements. Service packs contain all service pack fixes since the last base version (minor or major) and the new 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 6.0(3) is released, and E3 is the latest engine level, the service pack is released as 6.0(3)E3.

Patch Release

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.

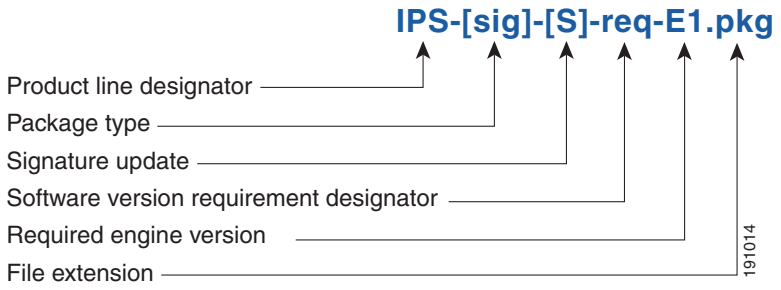
Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 5.0(1p1) requires 5.0(1).

Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 5.0(1p1) to 5.0(1p2) without first uninstalling 5.0(1p1).

Signature/Virus Updates and Signature Engine Updates

Figure 12-2 illustrates what each part of the IPS software file represents for signature/virus updates.

Figure 12-2 IPS Software File Name for Signature/Virus Updates,



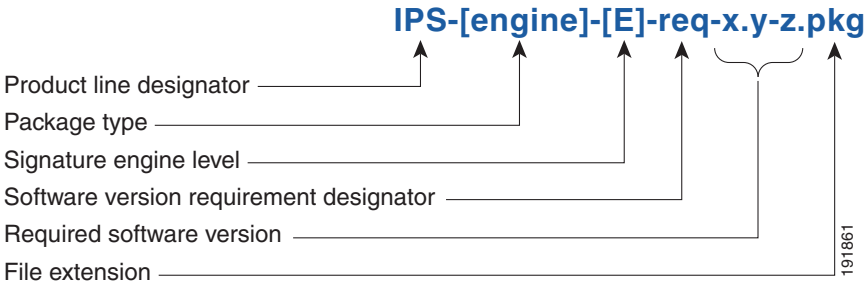
Signature/Virus Updates

Executable 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 virus component for the signature updates is packaged with the signature update. Virus updates are generated by Trend Microsystems for use by the Cisco Intrusion Containment System (Cisco ICS). Once created for use by Cisco ICS, they are later be incorporated into standard Cisco signature updates.

Figure 12-3 illustrates what each part of the IPS software file represents for signature engine updates.

Figure 12-3 IPS Software File Name for Signature Engine Updates



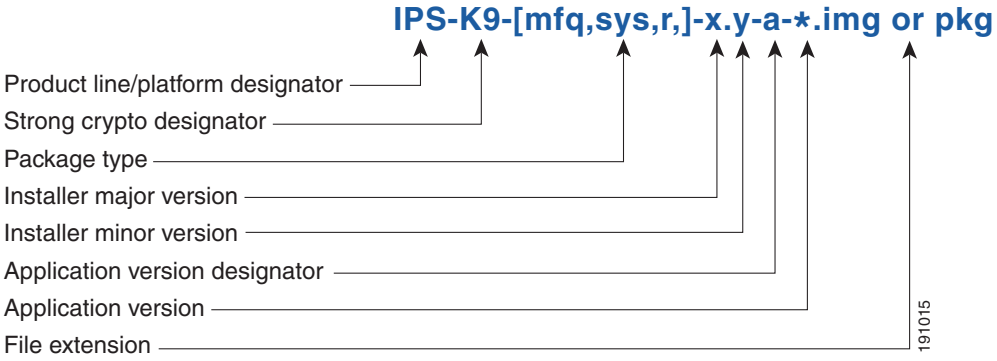
Signature Engine Updates

Executable files containing binary code to support new signature updates. Signature engine files require a specific service pack, which is also identified by the *req* designator.

Recovery, Manufacturing, and System Images

Figure 12-4 illustrates what each part of the IPS software file represents for recovery and system image filenames.

Figure 12-4 IPS Software File Name for Recovery and System Image Filenames



Recovery and system images contain separate versions for the installer and the underlying application. The installer version contains a major and minor version field.

Installer Major Version

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.

Installer Minor Version

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.

IPS 5.1 Software Release Examples

Table 12-1 lists platform-independent IDS 5.1(5)E1 software release examples. Refer to the Readmes that accompany the software files for detailed instructions on how to install the files. For instructions on how to access these files on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Table 12-1 Platform-Independent Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Signature update[1]	Weekly	sig	S700	IPS-sig-S700-req-E1.pkg
Signature engine update[2]	As needed	engine	E1	IPS-engine-E1-req-5.1-3.pkg
Service packs[3]	Semi-annually or as needed	—	5.1(3)	IPS-K9-5.1-3-E1.pkg
Minor version update[4]	Annually	—	5.1(1)	IPS-K9-5.1-1-E1.pkg
Major version update[5]	Annually	—	5.0(1)	IPS-K9-6.0-1-E1.pkg
Patch release[6]	As needed	patch	5.0(1p1)	IPS-K9-patch-5.1-1pl-E1.pkg
Recovery package[7]	Annually or as needed	r	1.1-5.0(1)	IPS-K9-r-1.1-a-5.1-1-E1.pkg

1. Signature updates include the latest cumulative IPS signatures.
2. Signature engine updates add new engines or engine parameters that are used by new signatures in later signature updates.
3. Service packs include defect fixes.
4. Minor versions include new minor version features and/or minor version functionality.
5. Major versions include new major version functionality or new architecture.
6. Patch releases are for interim fixes.
7. 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 5.0(1), but the recovery partition image will be r 1.2.

Table 12-2 describes platform-dependent software release examples.

Table 12-2 Platform-Dependent Release Examples

Release	Target Frequency	Identifier	Supported Platform	Example Filename
System image[1]	Annually	sys	Separate file for each sensor platform	IPS-4240-K9-sys-1.1-a-5.1-1-E1.img
Maintenance partition image[2]	Annually	mp	IDSM-2	c5svc-mp.2-1-2.bin.gz
Bootloader	As needed	bl	NM-CIDS AIM-IPS NME-IPS	servicesengine-boot-1.0-4.bin

1. The system image includes the combined recovery and application image used to reimage an entire sensor.
2. The maintenance partition image includes the full image for the IDSM-2 maintenance partition. The file is installed from but does not affect the IDSM-2 application partition.

Table 12-3 describes the platform identifiers used in platform-specific names.

Note IDS-4235 and IDS-4250 do not use platform-specific image files.

Table 12-3 Platform Identifiers

Sensor	Identifier
IDS-4215	IDS-4215-
IPS-4240	IPS-4240-
IPS-4255	IPS-4255-
IPS-4260	IPS-4260-
IDS module for Catalyst 6K	WS-SVC-IDSM2-
IDS network module	IPS-NM-CIDS-
AIP-SSM	IPS-SSM-

Upgrading Cisco IPS Software to 5.*x*

Note You cannot upgrade the IDSM (WS-X6381) to Cisco IDS 5.*x*. You must replace your IDSM (WS-X6381) with IDSM-2 (WS-SVC-IDSM2-K9), which supports version 5.*x*.

Pay attention to the following when upgrading to IPS 5.x:

- The minimum required version for upgrading to 5.1 is 5.0. The minimum required version for upgrading to 5.0 is 4.1(1). The upgrades from Cisco 5.0 to 5.1 and Cisco 4.1 to 5.0 are available as a downloads from Cisco.com. For the procedure for accessing Downloads on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.
- After downloading the 5.1 upgrade file, refer to the accompanying Readme for the procedure for installing the 5.1 upgrade file using the **upgrade** command. Fro more information, see Upgrading the Sensor, page 13-2.
- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- If you configured Auto Update for your sensor, copy the 5.1 upgrade file to the directory on the server that your sensor polls for updates. See Configuring Automatic Upgrades, page 13-6.
- If you install an upgrade on your sensor and the sensor is unusable after it reboots, you must reimage your sensor. Upgrading a sensor from any Cisco IDS version before 4.1 also requires you to use the **recover** command or the recovery/upgrade CD.

You can reimage your sensor in the following ways:

- For IDS appliances with a CD-ROM drive, use the recovery/upgrade CD.

  For the procedure, see Using the Recovery/Upgrade CD, page 13-22.
- For all sensors, use the **recover** command.

  For the procedure, see Recovering the Application Partition, page 13-9.
- For the IDS-4215, IPS-4240, IPS 4255, and IPS-4260 use the ROMMON to restore the system image.

  For the procedures, see Installing the IDS-4215 System Image, page 13-14, Installing the IPS-4240 and IPS-4255 System Image, page 13-17, and Installing the IPS-4260 System Image, page 13-20.
- For NM-CIDS, use the bootloader.

  For the procedure, see Installing the NM-CIDS System Image, page 13-23.
- For IDSM-2, reimage the application partition from the maintenance partition.

  For the procedure, see Installing the IDSM-2 System Image, page 13-25.
- For AIP-SSM, reimage from ASA using the **hw-module module 1 recover configure/boot** command.

  For the procedure, see Installing the AIP-SSM System Image, page 13-36.

Caution When you install the system image for your sensor, all accounts are removed and the default account and password are reset to cisco.

Obtaining a License Key From Cisco.com

This section describes how to obtain a license key from Cisco.com and how to install it using the CLI or IDM. It contains the following topics:

Overview

Although the sensor functions without the license key, you must have a license key to obtain signature updates. 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. For more information, see Service Programs for IPS Products, page 12-9.

- Your IPS device serial number

  To find the IPS device serial number in IDM, click **Configuration > Licensing**, or in the CLI use the **show version** command.

- Valid Cisco.com username and password

Note You can install the first few signature updates for 5.*x* without a license. This gives you time to get your sensor licensed. If you are unable to get your sensor licensed because of confusion with your contract, you can obtain a 60-day trail 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. For the procedure, see Obtaining and Installing the License, page 12-11.

Whenever you start IDM, a dialog box informs you 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 IDM but you cannot download signature updates.

When you enter the CLI, you receive the following message if there is no license installed:

```
***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.
```

You will continue to see this message until you have installed a license.

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:

- IDS-4215
- IPS-4240
- IPS-4255
- IDSM-2
- NM-CIDS

For ASA products, if you purchased one of the following ASA products that do not contain IPS, you must purchase a SMARTnet contract:

- ASA5510-K8
- ASA5510-DC-K8
- ASA5510-SEC-BUN-K9
- ASA5520-K8
- ASA5520-DC-K8
- ASA5520-BUN-K9
- ASA5540-K8
- ASA5540-DC-K8
- ASA5540-BUN-K9

Note SMARTnet provides operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

If you purchased one of the following ASA products that ships with the AIP-SSM installed or if you purchased AIP-SSM to add to your ASA product, you must purchase the Cisco Services for IPS service contract:

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9
- ASA5540-AIP20-K9
- ASA-SSM-AIP-10-K9
- ASA-SSM-AIP-20-K9

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 purchased an ASA-5510 and then later wanted to add IPS and purchased an ASA-SSM-AIP-10-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. For the procedure, see Obtaining and Installing the License, page 12-11.

Caution If you ever send your product for RMA, the serial number will change. You must then get a new license key for the new serial number.

Obtaining and Installing the License

This section describes how to obtain and install the license using IDM or the CLI. It contains the following topics:

- Using IDM, page 12-11
- Using the CLI, page 12-12

Using IDM

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. For more information, see Service Programs for IPS Products, page 12-9.

To obtain and install the sensor license, follow these steps:

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

Step 2 Choose **Configuration > Licensing**. The Licensing pane appears. Information about the current license state is displayed. If you have already installed your license, you can click **Download** to update it if needed.

Step 3 Choose the method to deliver the license:

a. Select **Cisco Connection Online** to obtain the license from Cisco.com.

IDM 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 4.

b. Select **License File** to use a license file.

To use this option, you must apply for a license at www.cisco.com/go/license.

The license is sent to you in e-mail and you save it to a drive that is accessible by IDM. This option is useful if your computer does not have access to Cisco.com.

Go to Step 7.

Step 4 Click **Update License**. The Licensing dialog box appears.

Step 5 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 has been updated.

Step 6 Click **OK**.

Step 7 Go to www.cisco.com/go/license.

Step 8 Fill in the required fields.

Caution You must have the correct IPS device serial number because the license key only functions on the device with that number.

Your Cisco IPS Signature Subscription Service license key is sent by e-mail to the e-mail address you specified.

Step 9 Save the license file to a hard-disk drive or a network drive that is accessible by the client running IDM.

Step 10 Log in to IDM.

Step 11 Choose **Configuration > Licensing**.

Step 12 Under Update License, choose **Update From: License File**.

Step 13 In the **Local File Path** field, specify the path to the license file or click **Browse Local** to browse to the file. The Select License File Path dialog box appears.

Step 14 Browse to the license file and click **Open**.

Step 15 Click **Update License**.

Using the CLI

Use the **copy** *source_url license_file_name* **license-key** command to copy the license file to your sensor.

The following options apply:

- *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.
- **license-key**—The subscription license file.
- *license_file_name*—The name of the license file you receive.

Note You cannot install an older license key over a newer license key.

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
- 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
- http:—Source URL for the web server. The syntax for this prefix is:

  http:[[/[username@]location]/directory]/filename
- https:—Source URL for the web server. The syntax for this prefix is:

  https:[[/[username@]location]/directory]/filename

  Note If you use FTP or SCP, you are prompted for a password.

Note If you use SCP, the remote host must be on the SSH known hosts list. For the procedure, see Defining Known Host Keys, page 2-10.

Note If you use HTTPS, the remote host must be a TLS trusted host. For the procedure, see Adding Trusted Hosts, page 2-15.

To install the license key, follow these steps:

Step 1 Apply for the license key at www.cisco.com/go/license.

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. For more information, see Service Programs for IPS Products, page 12-9.

Step 2 Fill in the required fields.

Note You must have the correct IPS device serial number because the license key only functions on the device with that number.

Your Cisco IPS Signature Subscription Service license key is sent by e-mail to the e-mail address you specified.

Step 3 Save the license key to a system that has a web server, FTP server, or SCP server.

Step 4 Log in to the CLI using an account with administrator privileges.

Step 5 Copy the license key to the sensor:

```
sensor# copy scp://user@10.89.147.3://tftpboot/dev.lic license-key
Password: *******
```

Step 6 Verify the sensor is licensed:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R0JS
Licensed, expires: 19-Dec-2005 UTC
Sensor up-time is 2 days.
Using 706699264 out of 3974291456 bytes of available memory (17% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.5M out of 166.8M bytes of available disk space (23% usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_15_03.00   (QATest)    2005-02-15T12:59:35-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600
```

```
Upgrade History:

    IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149


sensor#
```

Step 7 Copy your license key from a sensor to a server to keep a backup copy of the license:

```
sensor# copy license-key scp://user@10.89.147.3://tftpboot/dev.lic
Password: *******
sensor#
```

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

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.

CHAPTER 13

Upgrading, Downgrading, and Installing System Images

This chapter describes how to upgrade, downgrade, and install system images. It contains the following sections:

Caution The BIOS on Cisco IDS/IPS sensors is specific to Cisco IDS/IPS sensors and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on Cisco IDS/IPS sensors voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 12-1.

Overview

Note After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.

You can upgrade and downgrade the software on the sensor. Upgrading applies a service pack, signature update, minor version, major version, or recovery partition file. Downgrading removes the last applied upgrade from the sensor.

Caution You cannot use the **downgrade** command to go from 5.*x* to 4.*x*. To revert to 4.*x*, you must reimage 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 the recovery /upgrade CD, ROMMON, the bootloader/helper 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. For the procedure, see Initializing the Sensor, page 1-4.

After you reimage and initialize your sensor, upgrade your sensor with the most recent service pack, signature update, minor version, major version, and recovery partition file. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Upgrading the Sensor

This section explains how to use the **upgrade** command to upgrade the software on the sensor. It contains the following topics:

Overview

You can upgrade the sensor with the following files, all of which have the extension .pkg:

Note Upgrading the sensor changes the software version of the sensor.

Cisco IPS 5.1(1) through 5.1(4):

- Signature updates, for example, IPS-sig-S150-minreq-5.1-1.pkg
- Major updates, for example, IPS-K9-maj-6.0-1-pkg
- Minor updates, for example, IPS-K9-min-5.1-1.pkg
- Service packs, for example, IPS-K9-sp-5.1-2.pkg
- Recovery packages, for example, IPS-K9-r-1.1-a-5.1-1.pkg

Cisco IPS 5.1(5)E1 and later:

- Signature updates, for example, IPS-sig-S700-req-E1.pkg
- Signature engine updates, for example, IPS-engine-E1-req-5.1-3.pkg
- Major updates, for example, IPS-K9-5.1-1-E1.pkg
- Minor updates, for example, IPS-K9-5.1-1-E1.pkg
- Service packs, for example, IPS-K9-5.1-3-E1.pkg
- Patch releases, for example, IPS-K9-patch-5.1-1pl-E1.pkg
- Recovery packages, for example, IPS-K9-r-1.1-a-5.1-1-E1.pkg

Upgrade Command and Options

Use the **auto-upgrade-option enabled** command in the service host submode to configure automatic upgrades.

The following options apply:

- **default**— Sets the value back to the system default setting.
- **directory**— Directory where upgrade files are located on the file server.

  A leading '/' indicates an absolute path.
- **file-copy-protocol**— File copy protocol used to download files from the file server. The valid values are **ftp** or **scp**.

  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. For the procedure, see Defining Known Host Keys, page 2-10.
- **ip-address**— IP address of the file server.
- **password**— User password for authentication on the file server.
- **schedule-option**—Schedules when automatic upgrades occur. Calendar scheduling starts upgrades at specific times on specific days. Periodic scheduling starts upgrades at specific periodic intervals.
  - **calendar-schedule**—Configure the days of the week and times of day that automatic upgrades will be performed.

    days-of-week—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—Times of day at which auto-upgrades will begin. You can select multiple times. The valid value is *hh:mm[:ss]*.
  - **periodic-schedule**—Configure the time that the first automatic upgrade should occur, and how long to wait between automatic upgrades.

    interval—The number of hours to wait between automatic upgrades. Valid values are 0 to 8760.

    start-time—The time of day to start the first automatic upgrade. The valid value is *hh:mm[:ss]*.
- **user-name**—Username for authentication on the file server.

Using the Upgrade Command

To upgrade the sensor, follow these steps:

Step 1 Download the major update file (for example, IPS-K9-6.0-2-E1.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Note You must log in to Cisco.com using an account with cryptographic privileges to download the file. Do not change the file name. You must preserve the original file name for the sensor to accept the update.

For the procedure for locating software on Cisco.com and using an account with cryptographic privileges, see Obtaining Cisco IPS Software, page 12-1.

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# configure terminal
sensor(config)# upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-6.0-2-E1.pkg
```

Step 5 Enter the password when prompted:

```
Enter password: ********
Re-enter password: ********
```

Step 6 Type **yes** to complete the upgrade.

Note Major and minor updates and service packs may force a restart of the IPS processes or even force a reboot of the sensor to complete installation.

Step 7 Verify your new sensor version:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.0(2)E1

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S280.0                  2007-04-11
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS-4260
Serial Number:          AZBW5470042
No license present
Sensor up-time is 2 days.
Using 1897000960 out of 3569864704 bytes of available memory (53% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 43.8M out of 166.8M bytes of available disk space (28%
 usage)
boot is using 37.9M out of 69.5M bytes of available disk space (57% usage)


MainApp          2007_MAR_29_14_06   (Release)   2007-03-29T14:44:36-0600   Running
AnalysisEngine   2007_MAR_29_14_06   (Release)   2007-03-29T14:44:36-0600   Running
CLI              2007_MAR_29_14_06   (Release)   2007-03-29T14:44:36-0600
```

```
Upgrade History:

  IPS-K9-6.0-2-E1   14:06:00 UTC Thu Mar 29 2007

Recovery Partition Version 1.1 6.0(2)E1

sensor#
```

Upgrading the Recovery Partition

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.

Note Recovery partition images are generated for major and minor software releases and only in rare situations for service packs or signature updates.

Note To upgrade the recovery partition the sensor must already be running version 5.0(1) or later.

To upgrade the recovery partition on your sensor, follow these steps:

Step 1 Download the recovery partition image file (IPS-K9-r-1.1-a-5.0-1-E1.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

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-K9-r-1.1-a-5.0-1-E1.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-5.0-1-E1.pkg
```

Step 5 Type 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 the procedure, see Using the Recover Command, page 13-10.

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:

Overview

You can configure the sensor to look for new upgrade files in your upgrade directory automatically.

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 the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Auto-upgrade Command and Options

Use the **auto-upgrade-option enabled** command in the service host submode to configure automatic upgrades.

The following options apply:

- **default**— Sets the value back to the system default setting.
- **directory**— Directory where upgrade files are located on the file server.

  A leading '/' indicates an absolute path.
- **file-copy-protocol**— File copy protocol used to download files from the file server. The valid values are **ftp** or **scp**.

  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. For the procedure, see Defining Known Host Keys, page 2-10.
- **ip-address**— IP address of the file server.

- **password**— User password for authentication on the file server.
- **schedule-option**—Schedules when automatic upgrades occur. Calendar scheduling starts upgrades at specific times on specific days. Periodic scheduling starts upgrades at specific periodic intervals.
  - **calendar-schedule**—Configure the days of the week and times of day that automatic upgrades will be performed.

    days-of-week—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—Times of day at which auto-upgrades will begin. You can select multiple times. The valid value is *hh:mm[:ss]*.
  - **periodic-schedule**—Configure the time that the first automatic upgrade should occur, and how long to wait between automatic upgrades.

    interval—The number of hours to wait between automatic upgrades. Valid values are 0 to 8760.

    start-time—The time of day to start the first automatic upgrade. The valid value is *hh:mm[:ss]*.
- **user-name**—Username for authentication on the file server.

Using the auto-upgrade Command

To schedule automatic upgrades, follow these steps:

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

Step 2 Configure the sensor to automatically look for new upgrades in your upgrade directory.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# auto-upgrade-option enabled
```

Step 3 Specify the scheduling:

a. For calendar scheduling, which 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, which 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 4 Specify the IP address of the file server:

```
sensor(config-hos-ena-per)# exit
sensor(config-hos-ena)# ip-address 10.1.1.1
```

Step 5 Specify the directory where the upgrade files are located on the file server:

```
sensor(config-hos-ena)# directory /tftpboot/update/5.1_dummy_updates
```

Step 6 Specify the username for authentication on the file server:

```
sensor(config-hos-ena)# user-name tester
```

Step 7 Specify the password of the user:

```
sensor(config-hos-ena)# password
Enter password[]: ******
Re-enter password: ******
```

Step 8 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. For the procedure, see Defining Known Host Keys, page 2-10.

Step 9 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/5.0_dummy_updates
      user-name: tester
      password: <hidden>
      file-copy-protocol: ftp default: scp
   ----------------------------------------------
sensor(config-hos-ena)#
```

Step 10 Exit auto upgrade submode:

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

Step 11 Press **Enter** to apply the changes or type **no** to discard them.

UNIX-Style Directory Listings

To configure Auto 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 Auto 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.

Downgrading the Sensor

Use the **downgrade** command to remove the last applied upgrade from the sensor.

Caution You cannot use the **downgrade** command to go from 5.*x* to 4.*x*. To revert to 4.*x*, you must reimage the sensor.

To remove the last applied upgrade 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 reboot the system and downgrade to
IPS-K9-sp.5.0-2.pkg. Configuration changes made since the last upgrade will be lost and
the system may be rebooted.
Continue with downgrade?:
```

Step 4 Type **yes** to continue with the downgrade.

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

This section explains how to recover the application partition, and contains the following topics:

Overview

You can recover the application partition image for the appliance 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 appliance.

Note 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. For the procedure for upgrading the recovery partition to the most recent version, see Using the Recover Command, page 13-10.

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 If the appliance supports it, you can also use the recovery/upgrade CD to reinstall both the recovery and application partitions. For the procedure, see Using the Recovery/Upgrade CD, page 13-22.

Note When you reconnect to the sensor after recovery, you must log in with the default username and password `cisco`.

Using the Recover Command

To recover the application partition image, follow these steps:

Step 1 Download the recovery partition image file (IPS-K9-r-1.1-a-5.0-1-E1.pkg) to the tftp root directory of a TFTP server that is accessible from your sensor.

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of 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 5.0(0.27)S91(0.27). All configuration changes except for network settings will be
reset to default.
Continue with recovery? []:
```

Step 5 Type **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 appliance with the **setup** command. For the procedure, see Initializing the Sensor, page 1-4.

Note 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.

If you cannot access the CLI to execute the **recover application-partition** command, you can reboot the sensor and select the option from the boot menu during the bootup process. This lets you boot to the recovery partition and reimage the application partition. Executing the **recovery** command in this way requires console or keyboard and monitor access to the sensor, which is possible on the appliances and NM-CIDS, but not on IDSM-2 or AIP-SSM.

Installing System Images

This section contains the procedures for installing system images on the appliances and modules. It contains the following topics:

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. For the procedure see Recovering the Application Partition, page 13-9.

Understanding 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 the procedure for using a terminal server, see Connecting an Appliance to a Terminal Server, page 13-12.

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 IDS-4215, IPS-4240, and IPS-4255:
  - For RJ-45 connections, connect a 180 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.
- For all other appliances, connect the M.A.S.H. adapter (part number 29-4077-01) to COM1 on the appliance and:
  - For RJ-45 connections, connect a 180 rollover cable from the M.A.S.H. adapter to a port on the terminal server.
  - For hydra cable assemblies, connect a straight-through patch cable from the M.A.S.H. adapter to a port on the terminal server.

Step 2 Configure the line and port on the terminal server as follows:

a. 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
```

b. If you are configuring a terminal server for an IDS-4215, IPS-4240, or IPS-4255, go to Step 3.

Otherwise, for all other supported appliances, to direct all output to the terminal server, log in to the CLI and enter the following commands:

```
sensor# configure terminal
sensor(config)# display-serial
```

Output is directed to the serial port. Use the **no display-serial** command to redirect output to the keyboard and monitor.

Note You can set up a terminal server and use the **display-serial** command to direct all output from the appliance to the serial port. This option lets you view system messages on a console connected to the serial port, even during the boot process. When you use this option, all output is directed to the serial port and any local keyboard and monitor connection is disabled. However, BIOS and POST messages are still displayed on the local keyboard and monitor. For the procedure, refer to Directing Output to a Serial Connection.

Note There are no keyboard or monitor ports on an IDS-4215, IPS-4240, or IPS-4255; therefore, the **display-serial** and **no display-serial** commands do not apply to those platforms.

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 IDS-4215 System Image

You can install the IDS-4215 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

Caution Before installing the system image, you must first upgrade the IDS-4215 BIOS to version 5.1.7 and the ROMMON to version 1.4 using the upgrade utility file IDS-4215-bios-5.1.7-rom-1.4.bin. For the procedure, see Upgrading the IDS-4215 BIOS and ROMMON, page 13-16.

To install the IDS-4215 system image, follow these steps:

Step 1 Download the IDS-4215 system image file (IPS-4215-K9-sys-1.1-a-5.1-5-E1.img) to the tftp root directory of a TFTP server that is accessible from your IDS-4215. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1. Make sure you can access the TFTP server location from the network connected to your IDS-4215 Ethernet port.

Step 2 Boot IDS-4215.

Step 3 Press **Ctrl-R** at the following prompt while the system is booting:

```
Evaluating Run Options...
```

Note You have five seconds to press **Ctrl-R**.

The console display resembles the following:

```
CISCO SYSTEMS IDS-4215
Embedded BIOS Version 5.1.7 02/23/04 15:50:39.31
Compiled by dnshep
Evaluating Run Options...
Cisco ROMMON (1.4) #3: Mon Feb 23 15:52:45 MST 2004
Platform IDS-4215

Image Download Memory Sizing
Available Image Download Space: 510MB

0: i8255X @ PCI(bus:0 dev:13 irq:11)
1: i8255X @ PCI(bus:0 dev:14 irq:11)

Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.0001.0001
Use ? for help.
rommon>
```

Step 4 Verify that IDS-4215 is running BIOS version 5.1.7 or later and ROMMON version 1.4 or later.

Note If IDS-4215 does not have the correct BIOS and ROMMON versions, you must upgrade the BIOS and ROMMON before reimaging. For the procedure, see Upgrading the IDS-4215 BIOS and ROMMON, page 13-16.

The current versions are shown in the console display information identified in Step 3.

Step 5 If necessary, change the port used for the TFTP download:

```
rommon> interface port_number
```

The port in use is listed just before the rommon prompt. In the example, port 1 is being used as noted by the text, `Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.0001.0001`.

Note The default port used for TFTP downloads is port 1, which corresponds with the command and control interface of IDS-4215.

Note Ports 0 (monitoring interface) and 1 (command and control interface) are labeled on the back of the chassis.

Step 6 Specify an IP address for the local port on IDS-4215:

```
rommon> address ip_address
```

Note Use the same IP address that is assigned to IDS-4215.

Step 7 Specify the TFTP server IP address:

```
rommon> server ip_address
```

Step 8 Specify the gateway IP address:

```
rommon> gateway ip_address
```

Step 9 Verify that you have access to the TFTP server by pinging it from the local Ethernet port:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 10 Specify the path and filename on the TFTP file server from which you are downloading the image:

```
rommon> file path/filename
```

UNIX example:

```
rommon> file /system_images/IPS-4215-K9-sys-1.1-a-5.1-5-E1.img
```

Note The path is relative to the UNIX TFTP server's default tftpboot directory. Images located in the default tftpboot directory do not have any directory names or slashes in the file location.

Windows example:

```
rommon> file C:\tftp_directory\IPS-4215-K9-sys-1.1-a-5.1-5-E1.img
```

Step 11 Download and install the system image:

```
rommon> tftp
```

Note IDS-4215 reboots several times during the reimaging process. Do not remove power from IDS-4215 during the update process or the upgrade can become corrupted.

Upgrading the IDS-4215 BIOS and ROMMON

The BIOS/ROMMON upgrade utility (IDS-4215-bios-5.1.7-rom-1.4.bin) upgrades the BIOS of IDS-4215 to version 5.1.7 and the ROMMON to version 1.4.

To upgrade the BIOS and ROMMON on IDS-4215, follow these steps:

Step 1 Download the BIOS ROMMON upgrade utility (IDS-4215-bios-5.1.7-rom-1.4.bin) to the TFTP root directory of a TFTP server that is accessible from IDS-4215. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of IDS-4215.

Step 2 Boot IDS-4215. While rebooting, IDS-4215 runs the BIOS POST. After the completion of POST, the console displays the message: `Evaluating Run Options ...`for about 5 seconds.

Step 3 Press **Ctrl-R** while this message is displayed to display the ROMMON menu.

The console display resembles the following:

```
CISCO SYSTEMS IDS-4215
Embedded BIOS Version 5.1.3 05/12/03 10:18:14.84
Compiled by ciscouser
Evaluating Run Options ...
Cisco ROMMON (1.2) #0: Mon May 12 10:21:46 MDT 2003
Platform IDS-4215
0: i8255X @ PCI(bus:0 dev:13 irq:11)
1: i8255X @ PCI(bus:0 dev:14 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.c0ff.ee01
Use ? for help.
rommon>
```

Step 4 If necessary, change the port number used for the TFTP download:

```
rommon> interface port_number
```

The port in use is listed just before the rommon prompt. Port 1 (default port) is being used as indicated by the text, `Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.c0ff.ee01.`

Note Ports 0 (monitoring port) and 1 (command and control port) are labeled on the back of the chassis.

Step 5 Specify an IP address for the local port on IDS-4215:

```
rommon> address ip_address
```

Note Use the same IP address that is assigned to IDS-4215.

Step 6 Specify the TFTP server IP address:

```
rommon> server ip_address
```

Step 7 Specify the gateway IP address:

```
rommon> gateway ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from the local Ethernet port:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 Specify the filename on the TFTP file server from which you are downloading the image:

```
rommon> file filename
```

Example:

```
rommon> file IDS-4215-bios-5.1.7-rom-1.4.bin
```

Note The syntax of the file location depends on the type of TFTP server used. Contact your system or network administrator for the appropriate syntax if the above format does not work.

Step 10 Download and run the update utility:

```
rommon> tftp
```

Step 11 Type **y** at the upgrade prompt and the update is executed.

IDS-4215 reboots when the update is complete.

Caution Do not remove power to IDS-4215 during the update process, otherwise the upgrade can get corrupted. If this occurs, IDS-4215 will be unusable and require an RMA.

Installing the IPS-4240 and IPS-4255 System Image

You can install the IPS-4240 and IPS-4255 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

Note This procedure is for IPS-4240, but is also applicable to IPS-4255. The system image for IPS-4255 has "4255" in the filename.

To install the IPS-4240 and IPS-4255 system image, follow these steps:

Step 1 Download the IPS-4240 system image file (IPS-4240-K9-sys-1.1-a-5.1-5-E1.img) to the tftp root directory of a TFTP server that is accessible from your IPS-4240. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS-4240.

Step 2 Boot IPS-4240. The console display resembles the following:

```
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-4240-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
```

The output on the configured system resembles the following:

```
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 IPS-4240
- Server—TFTP server IP address where the application image is stored
- Gateway—Gateway IP address used by IPS-4240
- Port—Ethernet interface used for IPS-4240 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 Management0/0, which corresponds to the MGMT interface of IPS-4240.

```
rommon> PORT=interface_name
```

Step 6 If necessary, assign an IP address for the local port on IPS-4240:

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to IPS-4240.

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-4240-K9-sys-1.1-a-5.1-5-E1.img
```

Note The path is relative to the UNIX TFTP server's 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=C:\system_images\IPS-4240-K9-sys-1.1-a-5.1-5-E1.img
```

Step 11 Type **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 type 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 IPS-4240 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on IPS-4240. Be sure to use the IPS-4240 image.

Installing the IPS-4260 System Image

You can install the IPS-4260 system image by using the ROMMON on the appliance to TFTP the system image onto the flash device.

To install the IPS-4260 system image, follow these steps:

Step 1 Download the IPS-4260 system image file (IPS-4260-K9-sys-1.1-a-5.1-5-E1.img) to the tftp root directory of a TFTP server that is accessible from your IPS-4260. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1. Make sure you can access the TFTP server location from the network connected to your IPS-4260 Ethernet port.

Step 2 Boot IPS-4260.

Step 3 Press **Ctrl-R** at the following prompt while the system is booting:

```
Evaluating Run Options...
```

Note You have five seconds to press **Ctrl-R**.

The console display resembles the following:

```
Assuming IPS-4260-K9 Platform
 2 Ethernet Interfaces detected

Cisco Systems ROMMON Version (1.0(11)1c) #26: Mon Mar 13 18:05:54 CST 2006

Platform IPS-4260-K9
Management0/0
Link is UP
MAC Address: 0004.23cc.6047


Use ? for help.
rommon #0>
```

Step 4 If necessary, change the port used for the TFTP download:

```
rommon #1> interface name
```

The port in use is listed just after the platform identification. In the example, port Management0/0 is being used.

Note The default port used for TFTP downloads is Management0/0, which corresponds with the command and control (MGMT) interface of the IPS-4260.

Note Ports Management0/0 (MGMT) and GigabitEthernet0/1 (GE 0/1) are labeled on the back of the chassis.

Step 5 Specify an IP address for the local port on IPS-4260:

```
rommon> address ip_address
```

Note Use the same IP address that is assigned to IPS-4260.

Step 6 Specify the TFTP server IP address:

```
rommon> server ip_address
```

Step 7 Specify the gateway IP address:

```
rommon> gateway ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from the local Ethernet port:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 Specify the path and filename on the TFTP file server from which you are downloading the image:

```
rommon> file path/filename
```

UNIX example:

```
rommon> file /system_images/IPS-4260-K9-sys-1.1-a-5.1-5-E1.img
```

Note The path is relative to the UNIX TFTP server's default tftpboot directory. Images located in the default tftpboot directory do not have any directory names or slashes in the file location.

Windows example:

```
rommon> file <tftpboot_directory>IPS-4260-K9-sys-1.1-a-5.1-5-E1.img
```

Step 10 Download and install the system image:

```
rommon> tftp
```

Note IPS-4260 reboots once during the reimaging process. Do not remove power from IPS-4260 during the update process or the upgrade can become corrupted.

Using the Recovery/Upgrade CD

You can use the recovery/upgrade CD on appliances that have a CD-ROM, such as the IDS-4210, IDS-4235, and IDS-4250. The recovery/upgrade CD reimages both the recovery and application partitions.

Caution You are installing a new software image. All configuration data is overwritten.

After you install the system image with the recovery/upgrade CD, you must use the **setup** command to initialize the appliance. You will need your configuration information. You can obtain this information by generating a diagnostics report through IDM.

Signature updates occur approximately every week or more often if needed. The most recent signature update will not be on the recovery/upgrade CD that shipped with your appliance. Download the most recent signature update and apply it after you have recovered the system image.

To recover the system image with the recovery/upgrade CD, follow these steps:

Step 1 Obtain your configuration information from IDM:

a. To access IDM, point your browser to the appliance you are upgrading.
b. Select **Monitoring > Diagnostics**. The Diagnostics panel appears.
c. Click **Run Diagnostics**. Running the diagnostics may take a while.
d. Click **View Results**. The results are displayed in a report.
e. To save the diagnostics report, select **Menu > Save As** in your browser.

Step 2 Insert the recovery/upgrade CD into the CD-ROM drive.

Step 3 Power off the appliance and then power it back on. The boot menu appears, which lists important notices and boot options.

Step 4 Type **k** if you are installing from a keyboard, or type **s** if you are installing from a serial connection.

Note A blue screen is displayed for several minutes without any status messages while the files are being copied from the CD to your appliance.

Step 5 Log in to the appliance by using a serial connection or with a monitor and keyboard.

Note The default username and password are both cisco.

Step 6 You are prompted to change the default password.

Note Passwords must be at least eight characters long and be strong, that is, not be a dictionary word.

After you change the password, the `sensor#` prompt appears.

Step 7 Type the **setup** command to initialize the appliance. For the procedure, see Initializing the Sensor, page 1-4.

Step 8 Install the most recent service pack and signature update. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Installing the NM-CIDS System Image

This section describes how to install the NM-CIDS system image, and contains the following topics:

Overview

You can reimage the NM-CIDS using the system image file (IPS-NM-CIDS-K9-sys-1.1-a-5.1-1.pkg). If NM-CIDS is already running version 5.0, the bootloader has been upgraded. If NM-CIDS is not running 5.0, you must upgrade the bootloader before installing the 5.1 image. For the procedure to upgrade the bootloader, refer to Installing the NM-CIDS System Image.

Installing the NM-CIDS System Image

Note The bootloader has a timeout of 10 minutes, which means reimages over slow WAN links will fail. To avoid this situation, download the bootloader file to a local TFTP server and have the NM-CIDS reimage from the local TFTP server.

To reimage NM-CIDS, follow these steps:

Step 1 Download the NM-CIDS system image file (IPS-NM-CIDS-K9-sys-1.1-a-5.1-5-E1.img) to the TFTP root directory of a TFTP server that is accessible from your NM-CIDS. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Note Make sure you can access the TFTP server location from the network connected to the NM-CIDS Ethernet port.

Step 2 Log in to the router.

Step 3 Enter enable mode:

```
router# enable
router(enable)#
```

Step 4 Session to NM-CIDS:

```
router(enable)# service-module IDS-Sensor slot_number/0 session
```

Note Use the **show configuration | include interface IDS-Sensor** command to determine the NM-CIDS slot number.

Step 5 Suspend the session by pressing **Shift-Ctrl-6 X**. You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 6 Reset NM-CIDS:

```
router(enable)# service-module IDS-Sensor slot_number/0 reset
```

You are prompted to confirm the **reset** command.

Step 7 Press **Enter** to confirm.

Step 8 Press **Enter** to resume the suspended session. After displaying its version, the bootloader displays this prompt for 15 seconds:

```
Please enter '***' to change boot configuration:
```

Step 9 Enter ******* during the 15-second delay. The bootloader prompt appears.

Step 10 Display the bootloader configuration:

```
ServicesEngine boot-loader> show config
```

Caution If the bootloader version is not 1.0.17-1, you must upgrade it before installing 5.1. For the procedure, refer to Installing the NM-CIDS System Image.

Step 11 Configure the bootloader parameters:

```
ServicesEngine boot-loader> config
```

Step 12 You are prompted for each value line by line.

a. Specify the IP address—The external fast Ethernet port on NM-CIDS. This must be a real IP address on your network.

b. Specify the subnet mask—The external fast Ethernet port on NM-CIDS. This must be a real IP address on your network.

c. Specify the TFTP server IP address—The IP address of the TFTP server from which to download the NM-CIDS system image.

d. Specify the gateway IP address—The IP address of the default gateway for hosts on your subnet.

e. Specify the default helper file—The name of the helper image to boot. The NM-CIDS helper file is boot helper IPS-NM-CIDS-K9-sys-1.1-a-5.1-1.img.

f. Specify the Ethernet interface—The Ethernet interface is always set to **external**.

g. Specify the default boot device—The default boot device is always set to **disk**.

h. Specify the default bootloader—The default bootloader is always set to **primary**.

If you made any changes, the bootloader stores them permanently. The bootloader command prompt appears.

Caution The next step erases all data from the NM-CIDS hard-disk drive.

Step 13 Boot the system image:

```
ServicesEngine boot-loader> boot helper IPS-NM-CIDS-K9-sys-1.1-a-5.1-5-E1.img
```

The bootloader displays a spinning line while loading the system image from the TFTP server. When the system image is loaded, it is booted. The system image installs IPS 5.1(1) on NM-CIDS. When the installation is complete, NM-CIDS reboots. The system is restored to default settings. The user account and password are set to `cisco`. You must initialize NM-CIDS with the **setup** command. For the procedure, see Initializing the Sensor, page 1-4.

Installing the IDSM-2 System Image

If the IDSM-2 application partition becomes unusable, you can reimage it from the maintenance partition. After you reimage the application partition of IDSM-2, you must initialize IDSM-2 using the **setup** command. For the procedure, see Initializing the Sensor, page 1-4. When there is a new maintenance partition image file, you can reimage the maintenance partition from the application partition.

This section describes how to reimage the application partition and maintenance partition for Catalyst software and Cisco IOS software. It contains the following topics:

Installing the System Image

This section describes how to install the IDSM-2 system image, and contains the following topics:

Catalyst Software

To install the system image, follow these steps:

Step 1 Download the IDSM-2 system image file (WS-SVC-IDSM2-K9-sys-1.1-a-5.1-5-E1.bin.gz) to the FTP root directory of a FTP server that is accessible from your IDSM-2. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Step 2 Log in to the switch CLI.

Step 3 Boot IDSM-2 to the maintenance partition:

```
cat6k> (enable) reset module_number cf:1
```

Step 4 Log in to the maintenance partition CLI:

```
login: guest
Password: cisco
```

Note You must configure the maintenance partition on IDSM-2. For the procedure, see Configuring the Maintenance Partition, page 13-28.

Step 5 Install the system image:

```
guest@hostname.localdomain# upgrade ftp://user@ftp server IP/directory
path/WS-SVC-IDSM2-K9-sys-1.1-a-5.1-5-E1.bin.gz
```

Step 6 Specify the FTP server password. After the application partition file has been downloaded, you are asked if you want to proceed:

```
Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing
it [y|n]:
```

Step 7 Type **y** to continue. When the application partition file has been installed, you are returned to the maintenance partition CLI.

Step 8 Exit the maintenance partition CLI and return to the switch CLI.

Step 9 Reboot IDSM-2 to the application partition:

```
cat6k> (enable) reset module_number hdd:1
```

Step 10 When IDSM-2 has rebooted, check the software version. For the procedure, refer to Verifying IDSM-2 Installation.

Step 11 Log in to the application partition CLI and initialize IDSM-2. For the procedure, see Initializing the Sensor, page 1-4.

Cisco IOS Software

To install the system image, follow these steps:

Step 1 Download the IDSM-2 system image file (WS-SVC-IDSM2-K9-sys-1.1-a-5.1-5-E1.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM-2.

Step 2 Log in to the switch CLI.

Step 3 Boot IDSM-2 to the maintenance partition.

```
router# hw-module module module_number reset cf:1
```

Step 4 Session to the maintenance partition CLI.

```
router# session slot slot_number processor 1
```

Step 5 Log in to the maintenance partition CLI.

```
login: guest
Password: cisco
```

Step 6 Configure the maintenance partition interface IP address.

```
guest@localhost.localdomain# ip address ip_address netmask
```

Note Choose an address that is appropriate for the VLAN on which the IDSM-2 management interface is located based on the switch configuration.

Step 7 Configure the maintenance partition default gateway address.

```
guest@localhost.localdomain# ip gateway gateway_address
```

Step 8 Install the system image.

```
guest@hostname.localdomain# upgrade
ftp://user@ftp_server_ip_address/directory_path/WS-SVC-IDSM2-K9-sys-1.1-a-5.1-5-E1.bin.gz
–install
```

Step 9 Specify the FTP server password. After the application partition file has been downloaded, you are asked if you want to proceed:

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

Step 10 Enter **y** to continue. When the application partition file has been installed, you are returned to the maintenance partition CLI.

Step 11 Exit the maintenance partition CLI and return to the switch CLI.

Step 12 Reboot IDSM-2 to the application partition.

```
router# hw-module module module_number reset hdd:1
```

Step 13 Verify that IDSM-2 is online and that the software version is correct and that the status is `ok`.

```
router# show module module_number
```

Step 14 Session to the IDSM-2 application partition CLI.

```
router# session slot slot_number processor 1
```

Step 15 Initialize IDSM-2 using the **setup** command. For the procedure, see Initializing the Sensor, page 1-4.

Configuring the Maintenance Partition

This section describes how to configure the maintenance partition on IDSM-2, and contains the following topics:

- Catalyst Software, page 13-28
- Cisco IOS Software, page 13-32

Catalyst Software

To configure the IDSM-2 maintenance partition, follow these steps:

Step 1 Log in to the switch CLI.

Step 2 Enter privileged mode:

```
cat6k# enable
cat6k(enable)#
```

Step 3 Session to IDSM-2:

```
cat6k# session 9
Trying IDS-9...
Connected to IDS-9.
Escape character is '^]'.

Cisco Maintenance image
```

Note You cannot Telnet or SSH to the IDSM-2 maintenance partition.You must session to it from the switch CLI.

Step 4 Log in as user **guest** and password **cisco**.

Note You can change the guest password, but we do not recommend it. If you forget the maintenance partition guest password, and you cannot log in to the IDSM-2 application partition for some reason, you will have to RMA IDSM-2.

```
login: guest
Password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

Step 5 View the IDSM-2 maintenance partition host configuration:

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 6 Clear the IDSM-2 maintenance partition host configuration (ip address, gateway, hostname):

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

Step 7 Configure the maintenance partition host configuration:

a. Specify the IP address:

```
guest@localhost.localdomain# ip address ip_address netmask
```

b. Specify the default gateway:

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c. Specify the hostname:

```
guest@localhost.localdomain# ip host hostname
```

Step 8 View the maintenance partition host configuration:

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 9 Verify the image installed on the application partition:

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
Hard disk(hdd)          1                       5.0(1)
guest@idsm2.localdomain#
```

Step 10 Verify the maintenance partition version (including the BIOS version):

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
```

```
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

Step 11 Upgrade the application partition:

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'SIZE WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
(unknown size)
/tmp/upgrade.gz           [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

Step 12 Type **y** to proceed with the upgrade.

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

Step 13 Display the upgrade log:

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
```

```
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

Step 14 Clear the upgrade log:

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

Step 15 Display the upgrade log:

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

Step 16 Ping another computer:

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

Step 17 Reset IDSM-2:

Note You cannot specify a partition when issuing the **reset** command from the maintenance partition. IDSM-2 boots to whichever partition is specified in the boot device variable. If the boot device variable is blank, IDSM-2 boots to the application partition.

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
2005 Mar 11 21:55:46 CST -06:00 %SYS-4-MOD_SHUTDOWNSTART:Module 9 shutdown in progress. Do
not remove module until shutdown completes

Broadcast message from root Fri Mar 11 21:55:47 2005...

The system is going down for system halt NOW !!
cat6k> (enable)
```

Cisco IOS Software

To configure the IDSM-2 maintenance partition, follow these steps:

Step 1 Log in to the switch CLI.

Step 2 Session to IDSM-2:

```
switch# session slot 11 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.111 ... Open

Cisco Maintenance image
```

Note You cannot Telnet or SSH to the IDSM-2 maintenance partition.You must session to it from the switch CLI.

Step 3 Log in as user **guest** and password **cisco**.

Note You can change the guest password, but we do not recommend it. If you forget the maintenance partition guest password, and you cannot log in to the IDSM-2 application partition for some reason, you will have to RMA IDSM-2.

```
login: guest
password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

Step 4 View the maintenance partition host configuration:

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 5 Clear the maintenance partition host configuration (ip address, gateway, hostname):

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

Step 6 Configure the maintenance partition host configuration:

a. Specify the IP address:

```
guest@localhost.localdomain# ip address ip_address netmask
```

b. Specify the default gateway:

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c. Specify the hostname:

```
guest@localhost.localdomain# ip host hostname
```

Step 7 View the maintenance partition host configuration:

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 8 Verify the image installed on the application partition:

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
Hard disk(hdd)          1                       5.0(1)
guest@idsm2.localdomain#
```

Step 9 Verify the maintenance partition version (including the BIOS version):

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

Step 10 Upgrade the application partition:

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'SIZE WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
(unknown size)
/tmp/upgrade.gz           [|]   28616K
```

```
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

Step 11 Type **y** to proceed with the upgrade.

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

Step 12 Display the upgrade log:

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

Step 13 Clear the upgrade log:

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

Step 14 Display the upgrade log:

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

Step 15 Ping another computer:

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

Step 16 Reset IDSM-2:

Note You cannot specify a partition when issuing the **reset** command from the maintenance partition. IDSM-2 boots to whichever partition is specified in the boot device variable. If the boot device variable is blank, IDSM-2 boots to the application partition.

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
Broadcast message from root Fri Mar 11 22:04:53 2005...

The system is going down for system halt NOW !!

[Connection to 127.0.0.111 closed by foreign host]
switch#
```

Upgrading the Maintenance Partition

This section describes how to upgrade the maintenance partition, and contains the following topics:

- Catalyst Software, page 13-35
- Cisco IOS Software, page 13-36

Catalyst Software

To upgrade the maintenance partition, follow these steps:

Step 1 Download the IDSM-2 maintenance partition file (c6svc-mp.2-1-1.bin.gz) to the FTP root directory of a FTP server that is accessible from your IDSM-2.

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Step 2 Log in to the IDSM-2 CLI.

Step 3 Enter configuration mode:

```
idsm2# configure terminal
```

Step 4 Upgrade the maintenance partition:

```
idsm2# upgrade ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-1.bin.gz
```

You are asked whether you want continue.

Step 5 Type **y** to continue.

The maintenance partition file is upgraded.

Cisco IOS Software

To upgrade the maintenance partition, follow these steps:

Step 1 Download the IDSM-2 maintenance partition file (c6svc-mp.2-1-1.bin.gz) to the FTP root directory of a FTP server that is accessible from your IDSM-2. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Step 2 Log in to the switch CLI.

Step 3 Session in to the application partition CLI:

```
switch# session slot slot_number processor 1
```

Step 4 Enter configuration mode:

```
idsm2# configure terminal
```

Step 5 Upgrade the maintenance partition:

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-1.bin.gz
```

Step 6 Specify the FTP server password:

```
Password: ********
```

You are prompted to continue:

```
Continue with upgrade?:
```

Step 7 Type **yes** to continue.

Installing the AIP-SSM System Image

You can reimage the AIP-SSM in one of the following ways:

- From ASA using the **hw-module module 1 recover configure/boot** command. See the following procedure.
- Recovering the application image from the sensor's CLI using the **recover application-partition** command. For the procedure, see Recovering the Application Partition, page 13-9.

- Upgrading the recovery image from the sensor's CLI using the **upgrade** command. For the procedure, see Upgrading the Recovery Partition, page 13-5.

To install the AIP-SSM system image, follow these steps:

Step 1 Download the AIP-SSM system image file (IPS-SSM-K9-sys-1.1-a-5.1-5-E1.img) to the TFTP root directory of a TFTP server that is accessible from your AIP-SSM. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Note Make sure you can access the TFTP server location from the network connected to the AIP-SSM Ethernet port.

Step 2 Log in to the ASA.

Step 3 Enter enable mode:

```
asa> enable
```

Step 4 Configure the recovery settings for AIP-SSM:

```
asa# 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 system image:

```
Image URL [tftp://0.0.0.0/]:
```

Example:

```
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-5-E1.img
```

Step 6 Specify the command and control interface of AIP-SSM:

```
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 AIP-SSM:

```
Gateway IP Address [0.0.0.0]:
```

Example:

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

Step 9 Execute the recovery:

```
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 reimaging is complete.

```
asa# show module 1

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5540 Adaptive Security Appliance         ASA5540            P2B00000019
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         P1D000004F4

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7b1c to 000b.fcf8.7b20  0.2          1.0(7)2      7.0(0)82
  1 000b.fcf8.011e to 000b.fcf8.011e  0.1          1.0(7)2      5.0(0.22)S129.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa#
```

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 11 Session to AIP-SSM and initialize AIP-SSM with the **setup** command. For the procedure, see Initializing the Sensor, page 1-4.

APPENDIX A

System Architecture

This appendix describes the system architecture of IPS 5.1. It contains the following sections:

System Overview

You can install Cisco IPS software on two platforms: the appliances and the modules (for a list of current appliances and modules, refer to Supported Sensors.

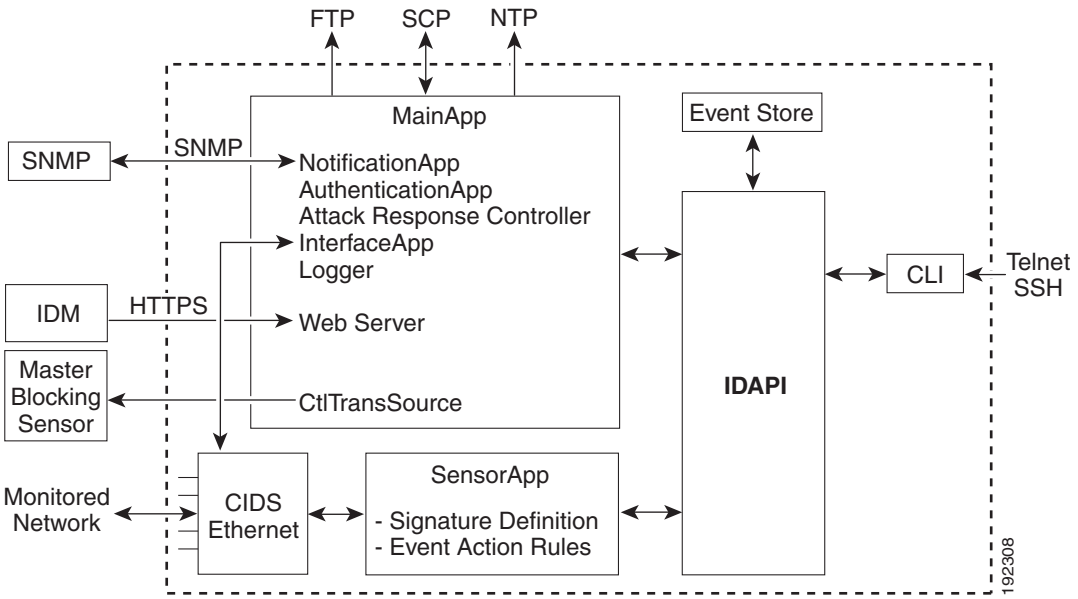
This section contains the following topics:

System Design

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.

Figure A-1 System Design



IPS software includes the following applications:

Note Each application has its own configuration file in XML format.

- 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 Attack Response Controller's (formerly known as Network Access Controller) master blocking sensor capability.
  - Event Store—An indexed store used to store IPS events (error, status, and alert system messages) that is accessible through the CLI, IDM, ASDM, or RDEP.
  - InterfaceApp—Handles bypass and physical settings and defines paired interfaces. Physical settings are speed, duplex, and administrative state.
  - LogApp—Writes all the application's log messages to the log file and the application's error messages to 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. 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. NotificationApp uses the public domain SNMP agent. SNMP GETs provide information about the general health of the sensor.
  - Web Server (HTTP RDEP2 server)—Provides a web interface and communication with other IPS devices through RDEP2 using several servlets to provide IPS services.

  - AuthenticationApp—Verifies that users are authorized to perform CLI, IDM, ASDM, or RDEP actions.
- SensorApp (Analysis Engine)—Performs packet capture and analysis.
- 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 IPS applications communicate with each other through a common API called IDAPI. Remote applications (other sensors, management applications, and third-party software) communicate with sensors through RDEP2 and SDEE protocols.

The sensor has the following partitions:

- Application partition—A full IPS system image.
- Maintenance partition—A special purpose IPS image used to reimage the application partition of the IDSM-2. When you reimage the maintenance partition, all configuration settings are lost.
- 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.

IPS 5.1 New Features

Cisco IPS 5.1 contains the following new features:

- Support for the Incident Control System (ICS).

  The ICS service augments Cisco's current IPS Signature Service by providing for the delivery of a more rapid and focused response to breaking threats.
- Inline VLAN (on a stick)

  The sensor can perform inline sensing between one or more VLAN pairs on a single sensor interface. Cisco Catalyst line cards that connect directly to the switch backplane and appliances that connect to an external port of the switch can use this feature.
- 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 rate limit 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.
- New Event Actions

  Two new deny attacker event actions have been added in the 5.1 release: Deny Attacker Service Pair Inline and Deny Attacker Victim Pair Inline. A new Request Rate Limit event action with a parameter that lets you specify a percentage of traffic from a denied attacker has been added to support rate limiting.
- GRE/IPV4-in-IPV4 Tunneling

  IPS 5.1 sensors can now monitor GRE and IPV4-inIPV4 encapsulated traffic.

User Interaction

You interact with IPS 5.1 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 IPS 5.1 through the CLI, IDM, IDS MC, ASDM or through another application using RDEP2/IDCONF.

- Tune

  You make minor modifications to the configuration, primarily to the 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 IPS 5.1 through the CLI, IDM, IDS MC, ASDM or through another application using RDEP2/IDCONF.

- Update

  You can schedule automatic updates or apply updates immediately to the applications and signature data files. You can update IPS 5.1 through the CLI, IDM, IDS MC, ASDM or through another application using RDEP2/IDCONF

- Retrieve information

  You can retrieve data (status messages, errors, and alarms) from the system through the CLI, IDM, IDS MC, ASDM or another application using RDEP or RDEP2.

Security Features

IPS 5.1 has the following security features:

- Network access is restricted to hosts who are specifically allowed access.
- All remote hosts who attempt to connect through 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 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

MainApp now includes all IPS components except SensorApp and the CLI. This section describes MainApp, and contains the following topics:

MainApp Responsibilities

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 Event Store
- Install and uninstall software upgrades
- Shut down or reboot the operating system

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 (for example, IDS-4240, WS-SVC-IDSM2)
- Version of sensor build on the other partition

MainApp also gathers the host statistics.

The following applications are now part of MainApp and are responsible for event storage, management, actions, and communication: Event Store, NotificationApp, CtlTransSource, ARC (formerly known as Network Access Controller), and LogApp.

These applications contain the following new features:

- SNMP support through NotificationApp

  Support for SNMP is one of the most significant changes for the management interface of the system. Through SNMP you can obtain standard health and welfare information about the system. Signatures have a new action of SNMP notification that causes an SNMP trap to be sent when the signatures fires.

  SNMP version 2 is the only version of SNMP supported.

- Event storage and retrieval

  The oldest entries expire in Event Store when there is no more room for new entries. RDEP provides different queries for retrieving just audit data vs. IPS alert data. All RDEP and RDEP2 SDEE queries are supported. All events are stored in SDEE CIDEE format.

- New "health" control transaction

  A new health and welfare type of control transaction is defined in the IDCONF specification. This control transaction reports the status and welfare of the system.

Event Store

This section describes Event Store, and contains the following topics:

About Event Store

Each IPS event is stored in 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. SensorApp is the only application that writes alert events into Event Store. All applications write log, status, and error events into 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 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 SensorApp. The sensor detects intrusion events.
- Error events—Caused by hardware or software malfunctions.
- Status events—Reports of a change in the application's status, 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 application's status 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 an application instance's configuration data
- Request for an application instance's diagnostic data
- Request to reset an application instance's diagnostic data
- 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 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, IDM, and ASDM.

SensorApp and ARC log response actions (TCP resets, IP logging start and stop, blocking start and stop, trigger packet) as status messages.

NotificationApp

NotificationApp allows the sensor to send alerts and system error messages as SNMP traps. It subscribes to events in Event Store and translates them into SNMP MIBs and sends them to destinations through a public-domain SNMP agent. NotificationApp supports sending sets and gets. The SNMP GETs provide information about basic sensor health.

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

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

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). NotificationApp sends the following information from the evError event:

- Originator information
- Event ID
- Event severity
- Time (UTC and local time)
- Error message

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 port
- IP nodes keyed on both IP address
- 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 IDS and IPS platforms support PEP.

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

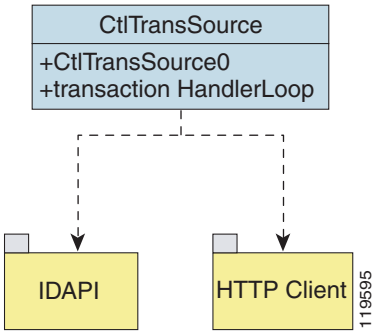
CtlTransSource is an application that forwards locally initiated remote control transactions to their remote destinations using the RDEP and HTTP protocols. CtlTransSource initiates either TLS or non-TLS connections and communicates remote control transactions to HTTP servers over these connections.

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 CtlTransSource. The transactionHandlerLoop method is a loop that waits on remote control transactions that are directed to CtlTransSource.

Figure A-2 shows the transactionHandlerLoop method in the CtlTransSource.

Figure A-2 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 an RDEP control transaction message. The transactionHandlerLoop uses the HttpClient classes to issue the RDEP control transaction request to the HTTP server on the remote node. The remote HTTP server handles the remote control transaction and returns the appropriate RDEP 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 RDEP response or a failure response as the control transaction's response to the remote control transaction's initiator. 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 CtlTransSource's designated username and password to authenticate the requestor's identity. 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 ARC, which is the IPS application that starts and stops blocking on routers, switches, and firewalls. A *block* is an entry in a device's configuration or ACL to block incoming and outgoing traffic for a specific host IP address or network address. ARC also controls rate limiting on routers running Cisco IOS 12.3.

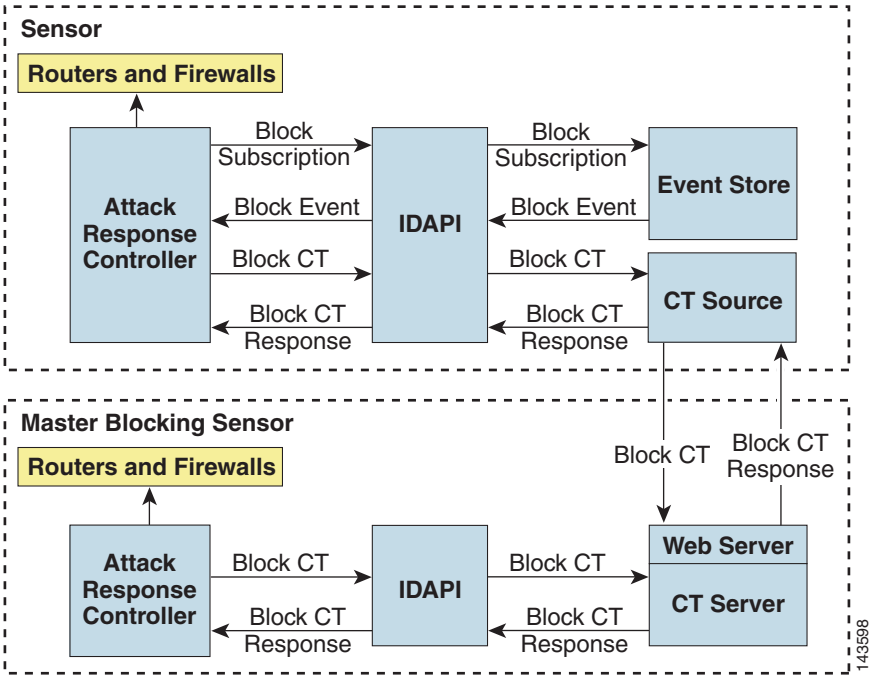
This section contains the following topics:

About ARC

ARC's main responsibility 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 ARC. ARC on the master blocking sensor then interacts with the devices it is managing to enable the block.

Figure A-3 illustrates ARC.

Figure A-3 ARC



Note An ARC instance can control 0, 1, or many network devices. 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.

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, or ASDM
- A block configured permanently against a host or network address

When you configure ARC to block a device, it initiates either a Telnet or SSH connection with the device. ARC maintains the connection with each device. After the block is initiated, 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

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, 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 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 ARC controls. The firewall device types use a different API to perform blocks and 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.

  For more information, see ACLs and VACLs, page A-15.

- Forwarding blocks to a list of remote sensors

  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. For more information on master blocking sensor, see Configuring the Master Blocking Sensor, page 8-31.

- 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.

  Note Cisco firewalls do not block based on interface or direction, so this configuration is never specified for them.

  ARC can simultaneously control up to 250 interfaces.

- Blocking hosts or networks for a specified time

  ARC can block a host or network for a specified number of minutes or indefinitely. ARC determines when a block has expired and unblocks the host or network at that time.

- Logging important events

  ARC writes a confirmation event when block or unblock actions are completed successfully or if any errors occur. 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

  ARC reapplies blocks that have not expired when a shutdown or restart occurs. ARC removes blocks that have expired while it was shut down.

  Note ARC can only maintain the blocking state successfully if no one changes the system time while the application is shut down.

For more information, see Maintaining State Across Restarts, page A-15.

- Maintaining blocking state across network device restarts

  ARC reapplies blocks and removes expired blocks as needed whenever a network device is shut down and restarted. ARC is not affected by simultaneous or overlapping shutdowns and restarts of ARC.

- Authentication and authorization

  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

  ARC supports host blocks and network blocks. Host blocks are connection based or unconditional. Network blocks are always unconditional.

  For more information, see Connection-Based and Unconditional Blocking, page A-16.

- NAT addressing

  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

  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 ARC through the CLI or any IPS manager. When ARC is reenabled, it completely reinitializes itself, including rereading the current configuration for each controlled network device.

  Note We recommend that you disable ARC from blocking when you are configuring any network device, including firewalls.

- Maintains up to 250 active blocks at any given time

  ARC can maintain up to 250 active blocks at a time. Although 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

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 500 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 ARC controls, you can configure 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. 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.

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. For more information, see Blocking with Cisco Firewalls, page A-17.

Maintaining State Across Restarts

When the sensor shuts down, ARC writes all blocks and rate limits (with starting timestamps) to a local file (nac.shun.txt) that is maintained by ARC. When 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 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 ARC is not running.

Caution Do not make manual changes to the nac.shun.txt file.

The following scenarios demonstrate how ARC maintains state across restarts.

Scenario 1

There are two blocks in effect when ARC stops and one of them expires before ARC restarts. When 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 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

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, ARC checks for the connectionShun attribute on the host block. If connectionShun is set to true, 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, 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

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*]

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 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.

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, 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. 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 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*

LogApp

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, ASDM, and RDEP clients.

The IPS applications use LogApp to log messages. LogApp sends log messages at any of five levels of severity: debug, timing, warning, error, and fatal. LogApp 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), LogApp converts the message to an evError event (with the corresponding error severity) and inserts it in Event Store.

Note For the procedure for displaying tech support information, see Generating a Diagnostics Report, page 10-10. For the procedure for displaying events, see Configuring Event Display, page 7-31.

LogApp receives all syslog messages, except cron messages, that are at the level of informational and above (*.info;cron.none), and inserts them into Event Store as <evErrors> with the error severity set to Warning. LogApp and application logging are controlled through the service logger commands.

LogApp 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. For more information, see Enabling Debug Logging, page C-24.

AuthenticationApp

This section describes AuthenticationApp, and contains the following topics:

- AuthenticationApp Responsibilities, page A-19
- Authenticating Users, page A-19
- Configuring Authentication on the Sensor, page A-20
- Managing TLS and SSH Trust Relationships, page A-20

AuthenticationApp Responsibilities

AuthenticationApp has the following responsibilities:

- To authenticate a user's identity
- To administer the user's accounts, privileges, keys, and certificates
- To configure which authentication methods are used by 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 IDM or 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 account's password.

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 account's authentication token 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. For more information, see User Roles, page A-27.

Configuring Authentication on the Sensor

When a user tries to access the sensor through a service such as Web Server or the CLI, the user's identity must be authenticated and the user's privileges must be established. The service that is providing access to the user initiates an execAuthenticateUser control transaction request to AuthenticationApp to authenticate the user's identity. The control transaction request typically includes the username and a password, or the user's identity can be authenticated using an SSH authorized key.

AuthenticationApp responds to the execAuthenticateUser control transaction request by attempting to authenticate the user's identity. AuthenticationApp returns a control transaction response that contains the user's authentication status and privileges. If the user's identity cannot be authenticated, AuthenticationApp returns an unauthenticated status and anonymous user privileges in the control transaction response. The control transaction response also indicates if the account's password has expired. User interface applications that authenticate users by initiating an execAuthenticateUser control transaction prompt the user to change the password.

AuthenticationApp uses the underlying operating system to confirm a user's identity. All the IPS applications send control transactions to 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 imposter 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 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 server's key fingerprints 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 imposter.

You can use the **show ssh server-key** and **show tls fingerprint** to display the sensor's key fingerprints. By recording the output of these commands when directly connected to the sensor console, you can reliably use this information to confirm the sensor's identity 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 Internet Explorer's user interface, 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 browser's list of trusted CAs 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 sensor's command and control interface. Consequently, if you change the command and control IP address of the sensor, the server's X.509 certificate 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 AuthenticationApp, you can operate sensors at a high level of security.

Web Server

Web Server provides RDEP2 support, which enables the sensor to report security events, receive IDIOM transactions, and serve IP logs.

Web Server supports HTTP 1.0 and 1.1. Communications with 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.

SensorApp

This section describes SensorApp, and contains the following topics:

- SEAP, page A-24
- New Features, page A-25

Responsibilities and Components

SensorApp performs packet capture and analysis. Policy violations are detected through signatures in SensorApp and the information about the violations is forwarded to 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.

SensorApp supports the following processors:

- Time Processor (TP)

  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 (DFP)

  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 (SEAP)

  This processor processes event actions. 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

  Event actions can be associated with an event RR threshold that must be surpassed for the actions to take place.

- Statistics Processor (SP)

  This processor keeps track of system statistics such as packet counts and packet arrival rates.

- Layer 2 Processor (L2P)

  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 (DBP)

  This processor maintains the signature state and flow databases.

- Fragment Reassembly Processor (FRP)

  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 (SRP)

  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 SRP 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 (SAP)

  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 (SDP)

  A process found only on dual CPU systems.

Some of the processors call inspectors to perform signature analysis. All inspectors can call the alarm channel to produce alerts as needed.

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.

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 SEAP.

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

  TP --> L2P --> DFP --> FRP --> SP --> DBP --> SAP --> SRP --> EAP

- Dual processor execution

  Execution Thread 1 TP --> L2P --> DFP --> FRP --> SP --> DBP --> SAP --> SDP --> | Execution Thread 2 DBP --> SRP --> EAP

SEAP

SEAP coordinates the data flow from the signature event in the alarm channel to processing through the SEAO, the SEAF, and the SEAH. It consists of the following components:

- Alarm channel

  The unit that represents the area to communicate signature events from the Sensor App inspection path to signature event handling.

- Signature event action override (SEAO)

  Adds actions based on the RR value. SEAO applies to all signatures that fall into the range of the configured RR threshold. Each SEAO is independent and has a separate configuration value for each action type. For more information, see Calculating the Risk Rating, page 7-2.

- Signature event action filter (SEAF)

  Subtracts actions based on the signature event's signature ID, addresses, and RR. The input to the SEAF is the signature event with actions possibly added by the SEAO.

  Note The SEAF can only subtract actions, it cannot add new actions.

  The following parameters apply to the SEAF:

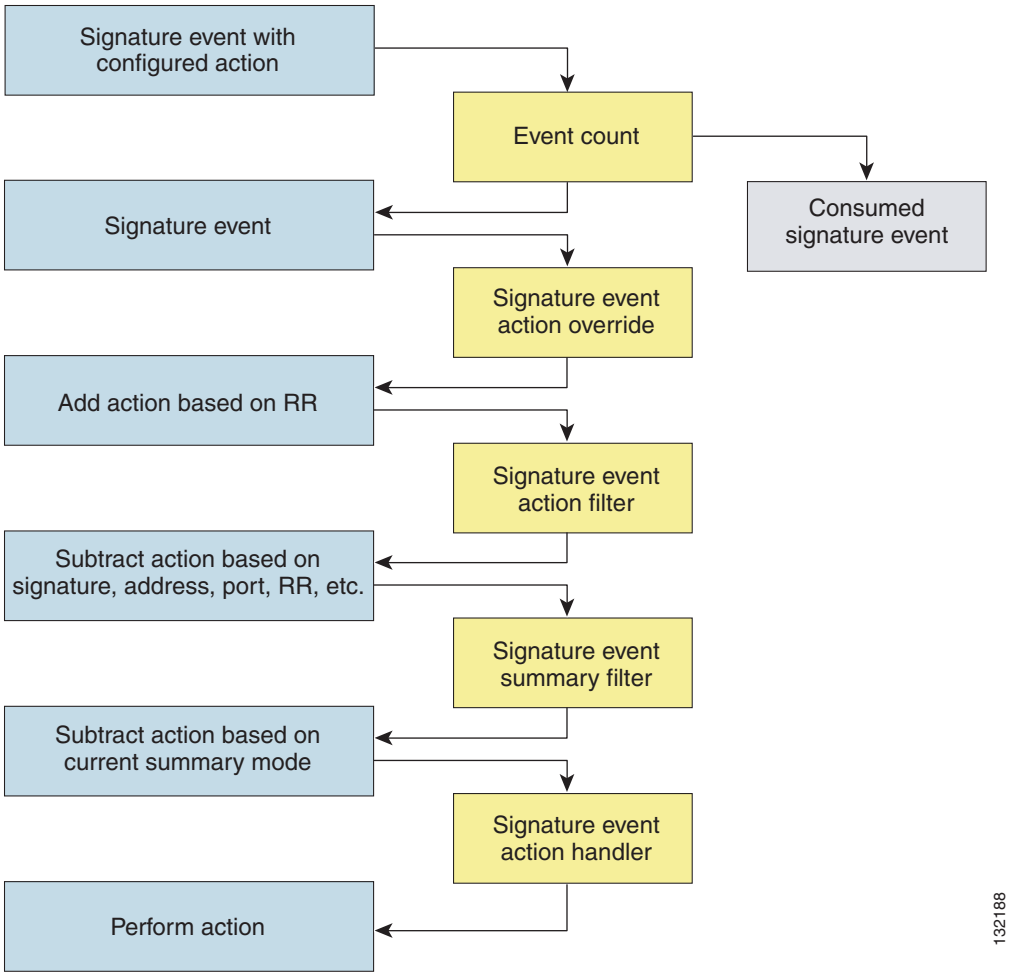
  - Signature ID
  - Subsignature ID
  - Attacker address
  - Attacker port
  - Victim address
  - Victim port
  - RR threshold range
  - Actions to subtract
  - Sequence identifier (optional)
  - Stop-or-continue bit
  - Enable action filter line bit

- Signature event action handler (SEAH)

  Performs the requested actions. The output from the SEAH is the actions being performed and possibly an <evIdsAlert> written to Event Store.

Figure A-4 on page A-25 illustrates the logical flow of the signature event through the SEAP 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 SEAP.

Figure A-4 Signature Event Through SEAP



New Features

SensorApp contains the following new 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, 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.

- Enhanced configuration

- Backup for dataflow in inline operations
- Hold down timer

  When SensorApp first starts, it may need to build state information for any flows that currently exist. The hold-down timer prevents SensorApp from denying packets while building this state information. During the hold-down timer, SensorApp still enforces policy whenever there is enough information.
- 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 RR

  The event RR 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

  Event RR helps reduce false positives from the system and gives you more control over what causes an alarm.

- Event action filters and processing

  4.*x* event filters filtered all actions. 5.*x* event filters handle events separately. Sending the alarm is now also considered an action and you can filter or configure it like the other actions.

- Driver support for concurrent SensorApp and TCPdump capture

  The drivers for the data interfaces support concurrent use of the interfaces by SensorApp and TCPdump or other libpcap-based reader

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.

This section contains the following topics:

User Roles

The CLI for IPS 5.1 permits multiple users 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 CLI supports four user roles: Administrator, Operator, Viewer, and Service. The privilege levels for each role are different; therefore, the menus and available commands vary for each role.

- **Administrators**—This user role has the highest level of privileges. Administrators have unrestricted view access and can perform the following functions:
  - Add users and assign passwords
  - Enable and disable control of physical interfaces and virtual sensors
  - Assign physical sensing interfaces to a virtual sensor
  - Modify the list of hosts allowed to connect to the sensor as a configuring or viewing agent
  - Modify sensor address configuration
  - Tune signatures
  - Assign configuration to a virtual sensor
  - Manage routers
- **Operators**—This user role has the second highest level of privileges. Operators have unrestricted view access and can perform the following functions:
  - Modify their passwords
  - Tune signatures
  - Manage routers
  - Assign configuration to a virtual sensor

- **Viewers**—This user role has the lowest level of privileges. Viewers can view configuration and event data and can modify their passwords.

Tip Monitoring applications only require viewer access to the sensor. You can use the CLI to set up a user account with viewer privileges and then configure the event viewer to use this account to connect to the sensor.

- **Service**—This user 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 device 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.

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 available for TAC to use for troubleshooting your sensor. For the procedure to create the service account, see Creating the Service Account.

Only one service account is allowed per sensor and only one account is allowed a service role. When the service account's password is set or reset, the root account's password 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 root account's password 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 IPS 5.1 incorporates several troubleshooting features that are available through the CLI or IDM. The service account is not necessary for most troubleshooting situations. You may need to create the service account at the TAC's direction 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.

CLI Behavior

Follow these tips when using the IPS CLI:

Prompts

- You cannot change the prompt displayed for the CLI commands.
- User interactive prompts occur when the system displays a question and waits for user input. The default input is displayed inside brackets [ ]. To accept the default input, press **Enter**.

Help

- To display the help for a command, type **?** after the command.

  The following example demonstrates the ? function:

  ```
  sensor# configure ?
  terminal     Configure from the terminal
  sensor# configure
  ```

  Note When the prompt returns from displaying help, the command previously entered is displayed without the ?.

- You can type **?** after an incomplete token to view the valid tokens that complete the command. If there is a trailing space between the token and the ?, you receive an ambiguous command error:

  ```
  sensor# show c ?
  % Ambiguous command : "show c"
  ```

  If you enter the token without the space, a selection of available tokens for the completion (with no help description) appears:

  ```
  sensor# show c?
  clock configuration
  sensor# show c
  ```

- Only commands available in the current mode are displayed by help.

Tab Completion

- Only commands available in the current mode are displayed by tab complete and help.
- If you are unsure of the complete syntax for a command, you can type a portion of the command and press **Tab** to complete the command.
- If multiple commands match for tab completion, nothing is displayed.

Recall

- To recall the commands entered in a mode, use the Up Arrow or Down Arrow keys or press **Ctrl-P** or **Ctrl-N**.

  Note Help and tab complete requests are not reported in the recall list.

- A blank prompt indicates the end of the recall list.

Case Sensitivity

- The CLI is not case sensitive, but it does echo back the text in the same case you typed it. For example, if you type:

  ```
  sensor# CONF
  ```

  and press **Tab**, the sensor displays:

  ```
  sensor# CONFigure
  ```

Display Options

- `–More–` is an interactive prompt that indicates that the terminal output exceeds the allotted display space. To display the remaining output, press the **spacebar** to display the next page of output or press **Enter** to display the output one line at a time.
- To clear the current line contents and return to a blank command line, press **Ctrl-C**.

Communications

This section describes the communications protocols used by IPS 5.1. It contains the following topics:

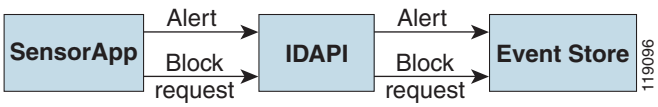
IDAPI

IPS applications use an interprocess communication API called IDAPI to handle internal communications. IDAPI reads and writes event data and provides a mechanism for control transactions. IDAPI is the interface through which all the applications communicate.

SensorApp captures and analyzes the network traffic on its interfaces. When a signature is matched, SensorApp generates an alert, which is stored in Event Store. If the signature is configured to perform the blocking response action, SensorApp generates a block event, which is also stored in Event Store.

Figure A-5 illustrates the IDAPI interface.

Figure A-5 IDAPI



Each application registers to the IDAPI to send and receive events and control transactions. 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 Event Store when received.
  - Reads IPS events from Event Store.
  - Writes IPS events to Event Store.

IDAPI provides the necessary synchronization mechanisms to guarantee atomic data accesses.

RDEP2

External communications use RDEP2. RDEP2 is an application-level communications protocol used to exchange IPS event, IP log, configuration, and control messages between IPS clients and IPS servers. RDEP2 communications consist of request and response messages. RDEP2 clients initiate request messages to RDEP2 servers. RDEP2 servers respond to request messages with response messages.

RDEP2 defines three classes of request/response messages: event, IP log, and transaction messages. Event messages include IPS alert, status, and error messages. Clients use IP log requests to retrieve IP log data from servers. Transaction messages are used to configure and control IPS servers.

RDEP2 uses the industry standards HTTP, TLS and SSL and XML to provide a standardized interface between RDEP2 agents. The RDEP2 protocol is a subset of the HTTP 1.1 protocol. All RDEP2 messages are legal HTTP 1.1 messages. RDEP2 uses HTTP's message formats and message exchange protocol to exchange messages between RDEP2 agents.

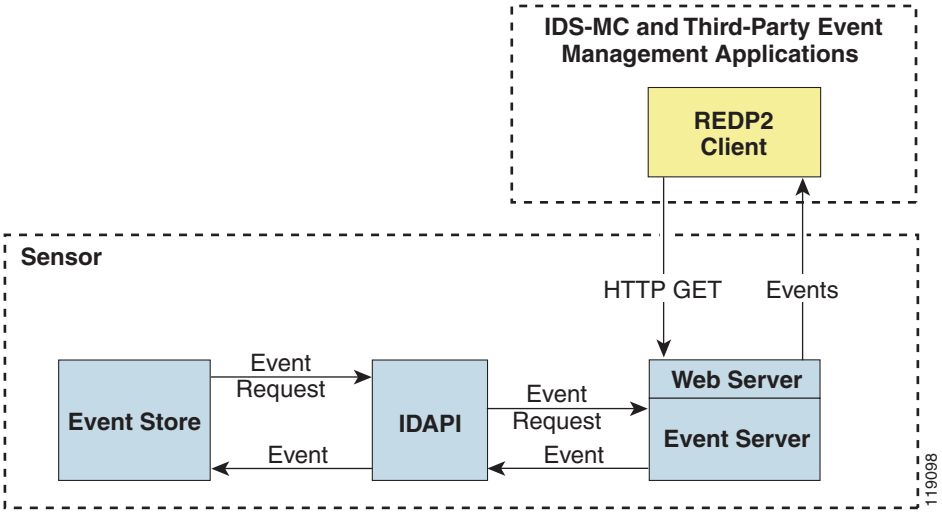
You use the IPS manager to specify which hosts are allowed to access the sensor through the network. Sensors accept connections from 1 to 10 RDEP2 clients simultaneously. Clients selectively retrieve data by time range, type of event (alert, error, or status message) and level (alert = high, medium, low, or informational; error = high, medium, low). Events are retrieved by a query (a single bulk get) or subscription (a real-time persistent connection) or both. Communications are secured by TLS or SSL.

Note For retrieving events, the sensor is backwards-compatible to RDEP even though the new standard for retrieval is RDEP2. We recommend you use RDEP2 to retrieve events and send configuration changes for IPS 5.1.

Remote applications retrieve events from the sensor through RDEP2. The remote client sends an RDEP2 event request to the sensor's Web Server, which passes it to the Event Server. The Event Server queries Event Store through IDAPI and then returns the result.

Figure A-6 shows remote applications retrieving events from the sensor through RDEP2.

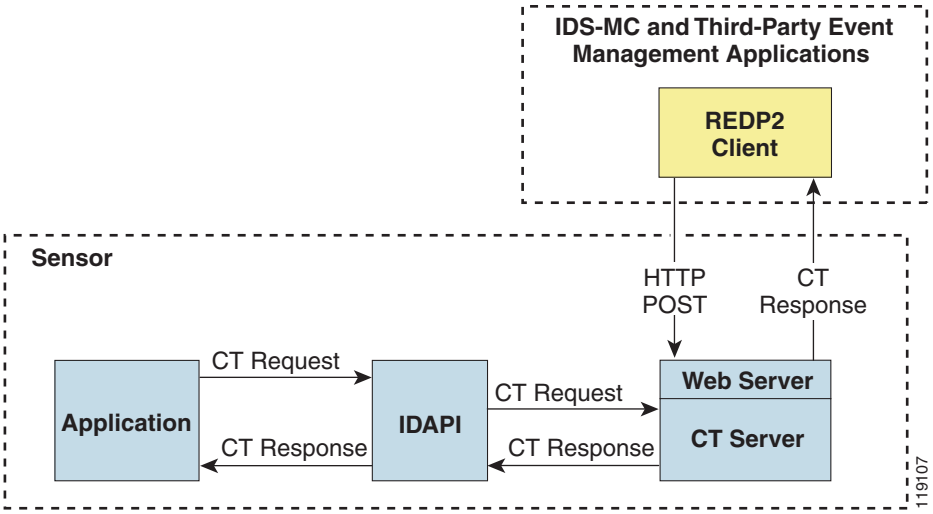
Figure A-6 Retrieving Events Through RDEP2



Remote applications send commands to the sensor through RDEP2. The remote client sends an RDEP2 control transaction to the sensor's Web Server, which passes it to the Control Transaction Server. The Control Transaction Server passes the control transaction through IDAPI to the appropriate application, waits for the application's response, and then returns the result.

Figure A-7 shows remote applications sending commands to the sensor through RDEP2.

Figure A-7 Sending Commands Through RDEP2



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 using the RDEP2 protocol 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

IPS 5.1 manages its configuration using XML documents. IDCONF specifies the XML schema including IPS 5.1 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 exchanged over RDEP2 and 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

IPS produces various types of events including intrusion alerts and status events. IPS communicates events to clients such as management applications using the proprietary RDEP2. We have also developed an IPS-industry leading protocol, SDEE, which is a product-independent standard for communicating security device events. SDEE is an enhancement to the current version of RDEP2 that 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.

IPS includes Web Server, which processes HTTP or HTTPS requests. 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 client's identity and determine the client's privilege level.

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 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 IPS-specific security device events as well as the IPS extensions to SDEE evIdsAlert elements.

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 may be 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>
…
```

IPS 5.1 File Structure

IPS 5.1 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 iplog 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/falcondump—Contains the application for getting packet dumps on the sensing ports of the IDS-4250-XL and IDSM-2.
- /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 IPS 5.1 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.
CLI	Accepts command line input and modifies the local configuration using IDAPI.
Event Server[1]	Accepts RDEP2 request for events from remote clients.
MainApp	Reads the configuration and starts applications, handles starting and stopping of applications and node reboots, handles software upgrades.
InterfaceApp	Handles bypass and physical settings and defines paired interfaces. Physical settings are speed, duplex, and administrative state.
LogApp	Writes all the application's log messages to the log file and the application's error messages to Event Store.
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 a 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.
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.
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.
Control Transaction Server[2]	Accepts control transactions from a remote RDEP2 client, initiates a local control transaction, and returns the response to the remote client.
Control Transaction Source[3]	Waits for control transactions directed to remote applications, forwards the control transactions to the remote node using RDEP2, and returns the response to the initiator.
IDM	The Java applet that provides an HTML IPS management interface.
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 web server servlet.
3. This is a remote control transaction proxy.

APPENDIX **B**

Signature Engines

This appendix describes the IPS signature engines. It contains the following sections:

About 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 5.1 engines support a standardized Regex.

IPS 5.1 contains the following signature engines:

- 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. 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.

For more information on configuring the AIC engine signatures, see Configuring Application Policy, page 5-27.

- Atomic—The Atomic engines are now combined into two 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.
  - 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 ARP—Inspects Layer-2 ARP protocol. The Atomic ARP engine is different because most engines are based on Layer-3-IP.
- 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.

  Note The Multi String engine is new for IPS 5.1.

- 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. Service engine has the following protocol types:
  - DNS—Inspects DNS (TCP and UDP) traffic.
  - FTP—Inspects FTP traffic.
  - GENERIC—Decodes custom service and payload.
  - 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.
  - IDENT—Inspects IDENT (client and server) traffic.
  - MSRPC—Inspects MSRPC traffic.
  - MSSQL—Inspects Microsoft SQL traffic.

  - NTP—Inspects NTP traffic.
  - RPC—Inspects RPC traffic.
  - SMB—Inspects SMB traffic.
  - SNMP—Inspects SNMP traffic.
  - SSH—Inspects SSH traffic.
- State—Stateful searches of strings in protocols such as SMTP.

  The state engine now 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.
- 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.
- 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

The following parameters are part of the Master engine and apply to all signatures.

Table B-1 lists the general master engine parameters.

Table B-1 Master Engine General Parameters

Parameter	Description	Value
alert-severity	Severity of the alert: • Dangerous alert • Medium-level alert • Low-level alert • Informational alert	high medium low informational
engine	Specifies the engine the signature belongs to.	—
event-counter	Grouping for event count settings.	—
event-count	Number of times an event must occur before an alert is generated.	1 to 65535
event-count-key	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	Enables alert interval.	yes | no
alert-interval	Time in seconds before the event count is reset.	2 to 1000
promisc-delta	Delta value used to determine seriousness of the alert.	0 to 30
sig-fidelity-rating	Rating of the fidelity of this signature.	0 to 100
sig-description	Grouping for your description of the signature.	—
sig-name	Name of the signature.	*sig-name*
sig-string-info	Additional information about this signature that will be included in the alert message.	*sig-string-info*
sig-comment	Comments about this signature.	sig-comment
alert-traits	Traits you want to document about this signature.	0 to 65335
release	The release in which the signature was most recently updated.	*release*
status	Whether the signature is enabled or disabled, active or retired.	enabled retired

Caution We do not recommend that you change the promisc-delta setting for a signature.

Promiscuous delta lowers the RR 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 and they never reach the target host, so it does not matter if the target was vulnerable. The attack was not allowed on the network and so we do not subtract from the risk rating value.

Signatures that are not service, OS, or application-specific have 0 for the promiscuously 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.

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
alert-frequency	Summary options for grouping alerts.	—
summary-mode	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.	—
specify-summary-threshold	(Optional) Enables summary threshold.	yes | no
summary-threshold	Threshold number of alerts to send signature into summary mode.	0 to 65535
specify-global-summary-threshold	Enable global summary threshold.	yes | no
global-summary-threshold	Threshold number of events to take alerts into global summary.	1 to 65535
summary-interval	Time in seconds used in each summary alert.	1 to 1000
summary-key	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

Most of the following event actions belong to each signature engine unless they are not appropriate for that particular engine.

Table B-3 describes the event actions.

Table B-3 Event Actions

Event Action Name	Description
Deny Attacker Inline	(Inline mode only) Does not transmit this packet and future packets originating from the attacker address for a specified period of time.[1] **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 **Monitoring > Denied Attackers > Clear List**, which permits the addresses back on the network. For the procedure, see Monitoring the Denied Attackers List, page 11-2.
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 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. **Note** For deny actions, to set the specified period of time and maximum number of denied attackers, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.
Deny Connection Inline	(Inline mode only) Does not transmit this packet and future packets on the TCP flow.
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
Log Attacker Packets	Starts IP logging packets containing the attacker address. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Log Pair Packets	Starts IP logging packets containing the attacker-victim address pair. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Log Victim Packets	Starts IP logging packets containing the victim address.
Modify Packet Inline	Modifies packet data to remove ambiguity about what the end point might do with the packet. **Note** Modify Packet Inline is not an option for Add Event Action Filter or Add Event Action Override.

Table B-3 Event Actions (continued)

Event Action Name	Description
Produce Alert	Writes the event to the Event Store as an alert. **Note** The Produce Alert action is not automatic when you enable alerts for a signature. To have an alert create in the Event Store, you must select Produce Alert. If you add a second action, you must include Produce 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.
Produce Verbose Alert	Includes an encoded dump of the offending packet in the alert. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected.
Request Block Connection	Sends a request to ARC to block this connection. **Note** You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting."
Request Block Host	Sends a request to ARC to block this attacker host. **Note** You must have blocking devices configured to implement this action. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting." **Note** For block actions, to set the duration of the block, choose **Configuration > Event Action Rules > General Settings**. For the procedure, see Configuring the General Settings, page 7-27.
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. For more information, see Chapter 8, "Configuring Attack Response Controller for Blocking and Rate Limiting." **Note** Request Rate Limit applies to a select set of signatures. For the list of signatures for which you can request a rate limit, see Understanding Rate Limiting, page 8-3.
Request SNMP Trap	Sends a request to NotificationApp to perform SNMP notification. **Note** This action causes an alert to be written to the Event Store, even if Produce Alert is not selected. You must have SNMP configured on the sensor to implement this action. For more information, see Chapter 9, "Configuring SNMP."
Reset TCP Connection	Sends TCP resets to hijack and terminate the TCP flow. **Note** Reset TCP Connection only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

1. 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 will still be denied.

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:

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

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.

AIC Engine

The AIC engine inspects HTTP web traffic and enforces FTP commands. This section describes the AIC engine and its parameters, and contains the following topics:

- Overview, page B-8
- AIC Engine Parameters, page B-9

Overview

The AIC engine defines signatures for deep inspection of web traffic. It also defines signatures that authorize and enforce FTP commands.

There are two AIC engines: AIC HTTP and AIC FTP.

The AIC engine has 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

AIC Engine Parameters

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.

The AIC engine runs 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.

Caution The AIC web ports are regular HTTP web ports. You can turn on AIC web ports to distinguish which ports should watch for regular HTTP traffic and which ports should watch for AIC enforcement. You might use AIC web ports, for example, if you have a proxy on port 82 and you need to monitor it. We recommend that you do not configure separate ports for AIC enforcement.

For the procedures for configuring AIC engine signatures, see Configuring Application Policy, page 5-27. For an example of a custom AIC signature, see Example Recognized Define Content Type (MIME) Signature, page 5-35.

Table B-4 lists the parameters that are specific to the AIC HTTP engine.

Table B-4 AIC HTTP Engine Parameters

Parameter	Description
signature-type	Specifies the type of AIC signature.
content-types	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.

Table B-4 AIC HTTP Engine Parameters (continued)

Parameter	Description
define-web-traffic-policy	Specifies the action to take when noncompliant HTTP traffic is seen. The **alarm-on-non-http-traffic [true | false]** command enables the signature. This signature is disabled by default.
max-outstanding-requests-overrun	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	AIC signature that allows actions to be associated with HTTP request methods: • define-request-method, such as get, put, and so forth. • recognized-request-methods lists methods recognized by the sensor.
transfer-encodings	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-error specifies actions to be taken when a chunked encoding error is seen.

Table B-5 lists the parameters that are specific to the AIC FTP engine.

Table B-5 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.

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, page B-11
- Atomic IP Engine, page B-11

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-6 lists the parameters that are specific to the Atomic ARP engine.

Table B-6 Atomic ARP Engine Parameters

Parameter	Description
specify-mac-flip	Fires an alert when the MAC address changes more than this many times for this IP address.
specify-type-of-arp-sig	Specifies the type of ARP signatures you want to fire on: • Source Broadcast (default)—Fires an alarm for this signature when it sees an ARP source address of 255.255.255.255. • Destination Broadcast—Fires an alarm for this signature when it sees an ARP destination address of 255.255.255.255. • Same Source and Destination—Fires an alarm for this signature when it sees an ARP destination address with the same source and destination MAC address • Source Multicast—Fires an alarm for this signature when it sees an ARP source MAC address of 01:00:5e:(00-7f).
specify-request-inbalance	Fires an alert when there are this many more requests than replies on the IP address.
specify-arp-operation	The ARP operation code for this signature.

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.

Note 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-7 lists the parameters that are specific to the Atomic IP engine.

Table B-7 Atomic IP Engine Parameters

Parameter	Description
fragment-status	Specifies whether or not fragments are wanted.
specify-ip-payload-length	Specifies IP datagram payload length.
specify-ip-header-length	Specifies IP datagram header length.
specify-ip-addr-options	Specifies IP addresses.
specify-ip-id	Specifies IP identifier.
specify-ip-total-length	Specifies IP datagram total length.

Table B-7 Atomic IP Engine Parameters (continued)

Parameter	Description
specify-ip-option-inspection	Specifies IP options inspection.
specify-l4-protocol	Specifies Layer 4 protocol.
specify-ip-tos	Specifies type of server.
specify-ip-ttl	Specifies time to live.
specify-ip-version	Specifies IP protocol version.

Flood Engine

The Flood engine defines 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 types of Flood engines: Flood Host and Flood Net.

Table B-8 lists the parameters specific to the Flood Host engine.

Table B-8 Flood Host Engine Parameters

Parameter	Description	Value
protocol	Which kind of traffic to inspect.	ICMP UDP
rate	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[3] 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.
3. The second number in the range must be greater than or equal to the first number.

Table B-9 lists the parameters specific to the Flood Net engine.

Table B-9 Flood Net Engine Parameters

Parameter	Description	Value
gap	Gap of time allowed (in seconds) for a flood signature.	0 to 65535
peaks	Number of allowed peaks of flood traffic.	0 to 65535
protocol	Which kind of traffic to inspect.	ICMP TCP UDP
rate	Threshold number of packets per second.	0 to 65535[1]

Table B-9 Flood Net Engine Parameters (continued)

Parameter	Description	Value
sampling-interval	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.

Meta Engine

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 SEAP. SEAP 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. For more information about SEAP, see Signature Event Action Processor, page 7-4.

Caution A large number of Meta signatures could adversely affect overall sensor performance.

Table B-10 lists the parameters specific to the Meta engine.

Table B-10 Meta Engine Parameters

Parameter	Description	Value
meta-reset-interval	Time in seconds to reset the META signature.	0 to 3600
component-list	List of Meta components: • 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	*name1*
meta-key	Storage type for the Meta signature: • Attacker address • Attacker and victim addresses • Attacker and victim addresses and ports • Victim address	AaBb AxBx Axxx xxBx

Table B-10 Meta Engine Parameters (continued)

Parameter	Description	Value
unique-victim-ports	Number of unique victims ports required per Meta signature.	1 to 256
component-list-in-order	Whether to fire the component list in order.	true | false

For an example of a custom Meta engine signature, see Example MEG Signature, page 5-46.

Multi String Engine

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-11 lists the parameters specific to the Multi String Engine.

Table B-11 Multi String Engine Parameters

Parameter	Description	Value
inspect-length	Length of stream or packet that must contain all offending strings for the signature to fire.	0 to 4294967295
protocol	Layer 4 protocol selection.	icmp tcp udp
regex-component	List of regex components: • regex-string—The string to search for. • spacing-type—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	Type of TCP or UDP port to inspect: • both-ports—Specifies both source and destination port. • dest-ports—Specifies a range of destination ports. • source-ports—Specifies a range of source ports.[1]	0 to 65535 [2]

Table B-11 Multi String Engine Parameters (continued)

Parameter	Description	Value
exact-spacing	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
min-spacing	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.	true | false (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.

Caution The Multi String engine can have a significant impact on memory usage.

Normalizer Engine

The Normalizer engine deals with IP fragmentation and TCP normalization. This section describes the Normalizer engine, and contains the following topics:

- Overview, page B-15
- Normalizer Engine Parameters, page B-16

Overview

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.

Note You cannot add custom signatures to the Normalizer engine. You can tune the existing ones.

- 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 will reassemble the datagrams, the sensor becomes vulnerable to denial of service attacks.

Reassembling all fragmented datagrams inline and only forwarding completed datagrams, 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 will be ordered properly and the normalizer will look for any abnormal packets associated with evasion and attacks.

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.

For the procedures for configuring signatures in the Normalizer engine, see Configuring IP Fragment Reassembly, page 5-36, and Configuring TCP Stream Reassembly, page 5-39.

Normalizer Engine Parameters

Table B-12 lists the parameters that are specific to the Normalizer engine.

Table B-12 Normalizer Engine Parameters

Parameter	Description
edit-default-sigs-only	Editable signatures.
specify-fragment-reassembly-timeout	(Optional) Enables fragment reassembly timeout.
specify-hijack-max-old-ack	(Optional) Enables hijack-max-old-ack.
specify-max-dgram-size	(Optional) Enables maximum datagram size.
specify-max-fragments	(Optional) Enables maximum fragments.
specify-max-fragments-per-dgram	(Optional) Enables maximum fragments per datagram.
specify-max-last-fragments	(Optional) Enables maximum last fragments.
specify-max-partial-dgrams	(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.
specify-tcp-max-mss	(Optional) Enables TCP maximum mss.
specify-tcp-max-queue	(Optional) Enables TCP maximum queue.

Table B-12 Normalizer Engine Parameters (continued)

Parameter	Description
specify-tcp-min-mss	(Optional) Enables TCP minimum mss.
specify-tcp-option-number	(Optional) Enables TCP option number.

Service Engines

The Service engines analyze L5+ traffic between two hosts. These are one-to-one signatures that track persistent data. The engines analyze the L5+ 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.

This section contains the following topics:

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-13 lists the parameters specific to the Service DNS engine.

Table B-13 Service DNS Engine Parameters

Parameter	Description	Value
protocol	Protocol of interest for this inspector.	TCP UDP
specify-query-chaos-string	(Optional) Enables the DNS Query Class Chaos String.	*query-chaos-string*
specify-query-class	(Optional) Enables the query class: • query-class—DNS Query Class 2 Byte Value	0 to 65535
specify-query-invalid-domain-name	(Optional) Enables query invalid domain name: • query-invalid-domain-name—DNS Query Length greater than 255	true | false
specify-query-jump-count-exceeded	(Optional) Enables query jump count exceeded: • query-jump-count-exceeded—DNS compression counter	true | false
specify-query-opcode	(Optional) Enables query opcode: • query-opcode—DNS Query Opcode 1 byte Value	0 to 65535
specify-query-record-data-invalid	(Optional) Enables query record data invalid: • query-record-data-invalid—DNS Record Data incomplete	true | false
specify-query-record-data-len	(Optional) Enables the query record data length: • query-record-data-len—DNS Response Record Data Length	0 to 65535
specify-query-src-port-53	(Optional) Enables the query source port 53: • query-src-port-53—DNS packet source port 53	true | false
specify-query-stream-len	(Optional) Enables the query stream length: • query-stream-len—DNS Packet Length	0 to 65535
specify-query-type	(Optional) Enables the query type: • query-type—DNS Query Type 2 Byte Value	0 to 65535
specify-query-value	(Optional) Enables the query value: • query-value—Query 0 Response 1	true | false

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-14 lists the parameters that are specific to the Service FTP engine.

Table B-14 Service FTP Engine Parameters

Parameter	Description	Value
direction	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	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	bad-port-cmd-address bad-port-cmd-port pasv
service-ports	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.	true | false (default)

1. The second number in the range must be greater than or equal to the first number.

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.

Note You cannot use the Service Generic engine to create custom signatures.

Caution Only advanced users should tune Service Generic engine signatures.

Table B-15 lists the parameters specific to the Service Generic engine.

Table B-15 Service Generic Engine Parameters

Parameter	Description	Value
specify-dst-port	(Optional) Enables the destination port: • dst-port—Destination port of interest for this signature	0 to 65535
specify-ip-protocol	(Optional) Enables IP protocol: • ip-protocol—The IP protocol this inspector should examine	0 to 255
specify-payload-source	(Optional) Enables payload source inspection: • payload-source—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 l2-header l3-header l4-header tcp-data udp-data
specify-src-port	(Optional) Enables the source port: • src-port—Source port of interest for this signature	0 to 65535

Service H225 Engine

This section describes the Service H225 engine, and contains the following topics:

- Overview, page B-20
- Service H255 Engine Parameters, page B-22

Overview

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.

Service H255 Engine Parameters

Table B-16 lists parameters specific to the Service H225 engine.

Table B-16 Service H.225 Engine Parameters

Parameter	Description	Value
message-type	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	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. Regex and presence are not valid for TPKT signatures.	length presence regex validate value
specify-field-name	(Optional) Enables field name for use. Only valid for SETUP and Q.931 message types. Gives a dotted representation of the field name that this signature applies to. • field-name—Field name to inspect.	1 to 512
specify-invalid-packet-index	(Optional) Enables invalid packet index for use for specific errors in ASN, TPKT, and other errors that have fixed mapping. • invalid-packet-index—Inspection for invalid packet index.	0 to 255
specify-regex-string	The regular expression to look for when the policy type is regex. This is never set for TPKT signatures: • A regular expression to search for in a single TCP packet • (Optional) Enables min match length for use. The minimum length of the Regex match required to constitute a match. This is never set for TPKT signatures.	regex-string specify-min-match-length
specify-value-range	Valid for the length or value policy types (0x00 to 6535). Not valid for other policy types. • value-range—Range of values.	0 to 65535[1] a-b

1. The second number in the range must be greater than or equal to the first number.

Service HTTP Engine

This section describes the Service HTTP engine, and contains the following topics:

Overview

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 today's networks. In addition, it requires the most amount of preprocessing time and has the most number of signatures requiring inspection making it critical to the system's overall performance.

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 to web services 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.

Service HTTP Engine Parameters

For an example Service HTTP custom signature, see Example Service HTTP Signature, page 6-33.

Table B-17 lists the parameters specific the Service HTTP engine.

Table B-17 Service HTTP Engine Parameters

Parameter	Description	Value
de-obfuscate	Applies anti-evasive deobfuscation before searching.	true | false
max-field-sizes	Maximum field sizes grouping.	—
specify-max-arg-field-length	(Optional) Enables maximum argument field length: • max-arg-field-length—Maximum length of the arguments field.	0 to 65535
specify-max-header-field-length	(Optional) Enables maximum header field length: • max-header-field-length—Maximum length of the header field.	0 to 65535
specify-max-request-length	(Optional) Enables maximum request field length: • max-request-length—Maximum length of the request field.	0 to 65535

Table B-17 Service HTTP Engine Parameters (continued)

Parameter	Description	Value
specify-max-uri-field-length	(Optional) Enables the maximum URI field length: • max-uri-field-length—Maximum length of the URI field.	0 to 65535
regex	Regular expression grouping.	—
specify-arg-name-regex	(Optional) Enables searching the Arguments field for a specific regular expression: • arg-name-regex—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	(Optional) Enables searching the Header field for a specific regular expression: • header-regex—Regular Expression to search in the HTTP Header field. The Header is defined after the first CRLF and continues until CRLFCRLF.	—
specify-request-regex	(Optional) Enables searching the Request field for a specific regular expression: • request-regex—Regular expression to search in both HTTP URI and HTTP Argument fields. • specify-min-request-match-length—Enables setting a minimum request match length.	0 to 65535
specify-uri-regex	(Optional) Regular expression to search in HTTP URI field. The URI field is defined to be after the HTTP method (GET, for example) and before the first CRLF. 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][a-zA-Z][.]jpeg
service-ports	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.	true | false (default)

1. The second number in the range must be greater than or equal to the first number.

Service IDENT Engine

The Service IDENT engine inspects TCP port 113 traffic. It has basic decode and provides parameters to specify length overflows.

Table B-18 lists the parameters specific to the Service IDENT engine.

Table B-18 Service IDENT Engine Parameters

Parameter	Description	Value
inspection-type	Type of inspection to perform.	—
has-bad-port	Inspects payload for a bad port.	true | false
has-newline	Inspects payload for a nonterminating new line character.	true | false
size	Inspects for payload length longer than this.	0 to 65535
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]
direction	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.

Service MSRPC Engine

This section describes the Service MSRPC engine, and contains the following topics:

- Overview, page B-25
- Service MSRPC Engine Parameters, page B-26

Overview

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 establish the channel and pass 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.

Service MSRPC Engine Parameters

Table B-19 lists the parameters specific to the Service MSRPC engine.

Table B-19 Service MSRPC Engine Parameters

Parameter	Description	Value
protocol	Protocol of interest for this inspector.	tcp udp
specify-operation	(Optional) Enables using MSRPC operation: • operation—MSRPC operation requested. Required for SMB_COM_TRANSACTION commands. Exact match.	0 to 65535
specify-regex-string	(Optional) Enables using a regular expression string: • specify-exact-match-offset—Enables the exact match offset: – exact-match-offset—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—Minimum number of bytes the regular expression string must match.	0 to 65535
specify-uuid	(Optional) Enables UUID: • uuid—MSRPC UUID field.	000001a0000 00000c00000 0000000046

Service MSSQL Engine

The Service MSSQL engine inspects the protocol used by Microsoft's SQL server (MSSQL).

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-20 lists the parameters specific to the Service MSSQL engine.

Table B-20 Service MSSQL Engine Parameters

Parameter	Description	Value
password-present	Whether or not a password was used in an MS SQL login.	true | false
specify-sql-username	(Optional) Enables using an SQL username: • sql-username—Username (exact match) of user logging in to MS SQL service.	sa

Service NTP Engine

The Service NTP engine inspects NTP protocol. There is one NTP signature, the NTPd 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-21 lists the parameters specific to the Service NTP engine.

Table B-21 Service NTP Engine Parameters

Parameter	Description	Value
inspection-type	Type of inspection to perform.	
inspect-ntp-packets	Inspects NTP packets: • control-opcode—Opcode number of an NTP control packet according to RFC1305, Appendix B. • max-control-data-size—Maximum allowed amount of data sent in a control packet. • mode —Mode of operation of the NTP packet per RFC 1305.	0 to 65535
is-invalid-data-packet	Looks for invalid NTP data packets. Checks the structure of the NTP data packet to make sure it is the correct size.	true | false
is-non-ntp-traffic	Checks for nonNTP packets on an NTP port.	true | false

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-22 lists the parameters specific to the Service RPC engine.

Table B-22 Service RPC Engine Parameters

Parameter	Description	Value
direction	Direction of traffic: • Traffic from service port destined to client port. • Traffic from client port destined to service port.	from-service to-service
protocol	Protocol of interest.	tcp udp
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535[1] a-b[,c-d]

Table B-22 Service RPC Engine Parameters (continued)

Parameter	Description	Value
specify-is-spoof-src	(Optional) Enables the spoof source address: • is-spoof-src—Fires an alert when the source address is 127.0.0.1.	true | false
specify-port-map-program	(Optional) Enables the portmapper program: • port-map-program—The program number sent to the portmapper for this signature.	0 to 9999999999
specify-rpc-max-length	(Optional) Enables RPC maximum length: • rpc-max-length—Maximum allowed length of the entire RPC message. Lengths longer than what you specify fire an alert.	0 to 65535
specify-rpc-procedure	(Optional) Enables RPC procedure: • rpc-procedure—RPC procedure number for this signature.	0 to 1000000
specify-rpc-program	(Optional) Enables RPC program: • rpc-program—RPC program number for this signature.	0 to 1000000

1. The second number in the range must be greater than or equal to the first number.

Service SMB Engine

The Service SMB engine inspects SMB packets. You can tune SMB signatures and create custom SMB signatures based on SMB control transaction exchanges and SMB NT_Create_AndX exchanges.

Table B-23 lists the parameters specific to the Service SMB engine.

Table B-23 Service SMB Engine Parameters

Parameter	Description	Value
service-ports	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 a-b[,c-d] [1]
specify-allocation-hint	(Optional) Enables MSRPC allocation hint: • allocation-hint—MSRPC Allocation Hint, which is used in SMB_COM_TRANSACTION command parsing.[2]	0 to 42949677295
specify-byte-count	(Optional) Enables byte count: • byte-count—Byte count from SMB_COM_TRANSACTION structure.[3]	0 to 65535
specify-command	(Optional) Enables SMB commands: • command—SMB command value.[4]	0 to 255

Table B-23 Service SMB Engine Parameters (continued)

Parameter	Description	Value
specify-direction	(Optional) Enables traffic direction: • direction—Lets you specify 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-file-id	(Optional) Enables using a transaction file ID: • file-id—Transaction File ID.[5] **Note** This parameter may limit a signature to a specific exploit instance and its use should be carefully considered.	0 to 65535
specify-function	(Optional) Enables named pipe function: • function—Named Pipe function.[6]	0 to 65535
specify-hit-count	(Optional) Enables hit counting: • hit-count—The threshold number of occurrences in scan-interval to fire alerts.[7]	0 to 65535
specify-operation	(Optional) Enables MSRPC operation: • operation—MSRPC operation requested. Required for SMB_COM_TRANSACTION commands. An exact match is required.	0 to 65535
specify-resource	(Optional) Enables resource: • resource—Specifies that pipe or the SMB filename is used to qualify the alert. In ASCII format. An exact match is required.	*resource*
specify-scan-interval	(Optional) Enables scan interval: • scan-interval—The interval in seconds used to calculate alert rates.[8]	0 to 131071
specify-set-count	(Optional) Enables counting setup words: • set-count—Number of Setup words.[9]	0 to 255
specify-type	(Optional) Enables searching for the Type field of an MSRPC packet: • type —Type Field of MSRPC packet. 0 = Request; 2 = Response; 11 = Bind; 12 = Bind Ack	0 to 255

Table B-23 Service SMB Engine Parameters (continued)

Parameter	Description	Value
specify-word-count	(Optional) Enables word counting for command parameters: • word-count—Word count for the SMB_COM_TRANSACTION command parameters.[10]	0 to 255
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. An exact match is optional.
3. An exact match is optional.
4. An exact match is required. Currently supporting the 37 (0x25) SMB_COM_TRANSACTION command \x26amp and the 162 (0xA2) SMB_COM_NT_CREATE_ANDX command.
5. An exact match is optional.
6. An exact match is required. Required for SMB_COM_TRANSACTION commands.
7. Valid for signatures 3302 and 6255 only.
8. Valid for signatures 3302 and 6255 only.
9. An exact match is required. Usually two are required for SMB_COM_TRANSACTION commands.
10. An exact match is required. Only 16 word transactions are decoded.

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-24 lists the parameters specific to the Service SNMP engine.

Table B-24 Service SNMP Engine Parameters

Parameter	Description	Value
inspection-type	Type of inspection to perform.	—
brute-force-inspection	Inspects for brute force attempts: • brute-force-count—The number of unique SNMP community names that constitute a brute force attempt.	0 to 65535
invalid-packet-inspection	Inspects for SNMP protocol violations.	—

Table B-24 Service SNMP Engine Parameters (continued)

Parameter	Description	Value
non-snmp-traffic-inspection	Inspects for non-SNMP traffic destined for UDP port 161.	—
snmp-inspection	Inspects SNMP traffic: • specify-community-name [yes | no]: – community-name—Searches for the SNMP community name, that is, the SNMP password. • specify-object-id [yes | no]: – object-id—Searches for the SNMP object identifier.	*community-name* *object-id*

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 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-25 lists the parameters specific to the Service SSH engine.

Table B-25 Service SSH Engine Parameters

Parameter	Description	Value
length-type	Inspects for one of the following SSH length types: • key-length—Length of the SSH key to inspect for: – length—Keys larger than this fire the RSAREF overflow. • user-length—User length SSH inspection: – length—Keys larger than this fire the RSAREF overflow.	0 to 65535
service-ports	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	(Optional) Enables packet depth: • packet-depth—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.

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 something 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-26 lists the parameters specific to the State engine.

Table B-26 State Engine Parameters

Parameter	Description	Value
state-machine	State machine grouping.	—
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
smtp	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 smtp-commands start
direction	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	A comma-separated list of ports or port ranges where the target service resides.	0 to 65535 a-b[,c-d] [1]
specify-exact-match-offset	(Optional) Enables exact match offset: • exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid.	0 to 65535

Table B-26 State Engine Parameters (continued)

Parameter	Description	Value
specify-min-match-length	(Optional) Enables minimum match length: • min-match-length—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.	true | false (default)

1. The second number in the range must be greater than or equal to the first number.

String Engines

This section describes the String engine, and contains the following topics:

Overview

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.

String ICMP Engine Parameters

For an example custom String engine signature, see Example String TCP Signature, page 6-28.

Table B-27 lists the parameters specific to the String ICMP engine.

Table B-27 String ICMP Engine Parameters

Parameter	Description	Value
direction	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	ICMP header TYPE value.	0 to 18[1] a-b[,c-d]

Table B-27 String ICMP Engine Parameters (continued)

Parameter	Description	Value
specify-exact-match-offset	(Optional) Enables exact match offset: • exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid.	0 to 65535
specify-min-match-length	(Optional) Enables minimum match length: • min-match-length—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.	true | false (default)

1. The second number in the range must be greater than or equal to the first number.

String TCP Engine Parameters

For an example custom String engine signature, see Example String TCP Signature, page 6-28.

Table B-28 lists the parameters specific to the String TCP engine.

Table B-28 String TCP Engine

Parameter	Description	Value
direction	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	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	(Optional) Enables exact match offset: • exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid.	0 to 65535
specify-min-match-length	(Optional) Enables minimum match length: • min-match-length—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]	true | false
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. This parameter is primarily used as an IPS anti-evasion tool.

String UDP Engine Parameters

For an example custom String engine signature, see Example String TCP Signature, page 6-28.

Table B-29 lists the parameters specific to the String UDP engine.

Table B-29 String UDP Engine

Parameter	Description	Value
direction	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	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	(Optional) Enables exact match offset: • exact-match-offset—The exact stream offset the regular expression string must report for a match to be valid.	0 to 65535
specify-min-match-length	(Optional) Enables minimum match length: • min-match-length—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.	true | false (default)

1. The second number in the range must be greater than or equal to the first number.

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.

You can configure source and destination address filters, which means the sweep signature will exclude these addresses from the sweep-counting algorithm.

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. The ICMP sweeps must have an ICMP type specified to discriminate among the various types of ICMP packets.

DataNode

When an activity related to Sweep engine signatures is seen, the IPS uses a DataNode to determine when it should stop monitoring for a particular host. The DataNode 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 DataNode containing the sweep determines when the sweep should expire. The DataNode stops a sweep when the DataNode has not seen any traffic for *x* number of seconds (depending on the protocol).

There are several adaptive timeouts for the DataNodes. The DataNode 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-30 lists the parameters specific to the Sweep engine.

Table B-30 Sweep Engine Parameters

Parameter	Description	Value
dst-addr-filter	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>]
src-addr-filter	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>]
protocol	Protocol of interest for this inspector.	icmp udp tcp
specify-icmp-type	(Optional) Enables the ICMP header type: • icmp-type—ICMP header TYPE value.	0 to 255
specify-port-range	(Optional) Enables using a port range for inspection: • port-range—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-fragments want-fragments
inverted-sweep	Uses source port instead of destination port for unique counting.	true | false

Table B-30 Sweep Engine Parameters (continued)

Parameter	Description	Value
mask	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	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.	true | false
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)
tcp-flags	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	Threshold number of unique port connections between the two hosts.	0 to 65535

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.

Tribe Flood Net 2000 (TFN2K) is the newer version of the TFN. It is a Distributed Denial Of Service (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 (Tribe Flood Net) and Stacheldraht. They are similar in operation to TFN2K, but rely on ICMP only and have fixed commands: integers and strings.

Table B-31 lists the parameters specific to the Traffic ICMP engine.

Table B-31 TRAFFIC.ICMP Engine Parameters

Parameter	Description	Value
parameter-tunable-sig	Whether this signature has configurable parameters.	yes | no
inspection-type	Type of inspection to perform: • Inspects for original LOKI traffic. • Inspects for modified LOKI traffic.	is-loki is-mod-loki
reply-ratio	Inbalance 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

Trojan Engines

The Trojan engines analyze nonstandard protocols, such as BO2K andTFN2K. There are three Trojan engines: Trojan BO2K, Trojan TFN2K, and Trojan UDP.

BackOrifice (BO) was the original Windows back door Trojan that ran over UDP only. It was soon superseded by BackOrifice 2000 (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.

APPENDIX C

Troubleshooting

This appendix contains troubleshooting tips and procedures for sensors and software. It contains the following sections:

Caution The BIOS on Cisco IDS/IPS sensors is specific to Cisco IDS/IPS sensors and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on Cisco IDS/IPS sensors voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 12-1.

Bug Toolkit

For the most complete and up-to-date list of caveats, use the Bug Toolkit to refer to the caveat release note. You can use the Bug Toolkit to search for known bugs based on software version, feature set, and keywords. The resulting matrix shows when each bug was integrated, or fixed if applicable. It also lets you save the results of a search in Bug Groups, and also create persistent Alert Agents that can feed those groups with new defect alerts.

Note You must be logged in to Cisco.com to access the Bug Toolkit.

If you are a registered Cisco.com user, you can view the Bug Toolkit at this URL:

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

To become a registered cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

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.

  For the procedure, refer to Creating and Using a Backup Configuration File.
- Save your backup configuration to a remote system.

  For the procedure, refer to Copying and Restoring the Configuration File Using a Remote Server.
- 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 password recovery and other special debug situations directed by TAC.

  For the procedure, refer to Creating the Service Account.

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 new password if the Administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

Note You cannot use the service account for password recovery on AIP-SSM, because you cannot get shell access to AIP-SSM. You must use ROMMON to get shell access to AIP-SSM.

Disaster Recovery

This section provides recommendations and steps to take if you need to recover your sensor after a disaster.

Follow these recommendations so that you are ready in case of a disaster:

- If you are using the CLI or IDM for configuration, copy the current configuration from the sensor to an FTP or SCP server any time a change has been made.

  For the procedure, refer to Creating and Using a Backup Configuration File.

  Note You should note the specific software version for that configuration. You can apply the copied configuration only to a sensor of the same version.

Note 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. For the procedure for obtaining a list of the current users on the sensor, refer to Viewing User Status.

- If you are using IDS MC, the current configuration is saved in the IDS MC database and a separate copy is not needed.

Note The list of user IDs is not saved in the IDS MC database. You must make a note of the user IDs.

Note You should note the specific software version for that configuration. You can push the copied configuration only to a sensor of the same version.

When a disaster happens and you need to recover the sensor, try the following:

1. Reimage the sensor.

   For the procedures for appliances and modules, see Chapter 13, "Upgrading, Downgrading, and Installing System Images."

2. Log in to the sensor with the default user ID and password—cisco.

   Note You are prompted to change the cisco password.

3. Run the **setup** command.

   For the procedure, see Initializing the Sensor, page 1-4.

4. Upgrade the sensor to the IPS software version it had when the configuration was last saved and copied.

   For more information on obtaining IPS software versions and how to install them, see Obtaining Cisco IPS Software, page 12-1.

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.

   For the procedure, refer to Creating and Using a Backup Configuration File.

6. Update clients to use the new key and certificate of the sensor.

   Reimaging changes the sensor's SSH keys and HTTPS certificate. For the procedure, see Defining Known Host Keys, page 2-10.

7. Create previous users.

   For the procedure, see Configuring Users, page 2-25.

Password Recovery

The following password recovery options exist:

- If another administrator account exists, the other administrator can change the password.
- If a service account exists, you can log in to the service account and switch to user root using the command **su - root**. Use the **password** command to change the CLI administrator account's password. For example, if the administrator username is "adminu," the command is **password adminu**. You are prompted to enter the new password twice. For more information, refer to Creating the Service Account.

You can reimage the sensor using either the recovery partition or a system image file. For more information, see Chapter 13, "Upgrading, Downgrading, and Installing System Images."

PIX 7.1 Devices and Normalizer Inline Mode

For IPS 5.0 and 5.1, normalizer inline mode may deny packets and/or connections if a PIX 7.1 device is in the traffic flow and the PIX device has been configured for the MSS workaround.

Certain web applications on port 80 cause the PIX device to require the MSS workaround. If that workaround is active, the IPS must have a complimentary workaround.

Problem There is an incompatibility with PIX and IPS when the PIX MSS workaround has been applied. The **show stat vi** command shows many deny packet or deny connection actions along with many 13*xx* signature firings.

Solution Disable or remove all actions from the following normalizer signatures: 1306 and 1311.

Troubleshooting the 4200 Series Appliance

This section contains information to troubleshoot the 4200 series 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 the following topics:

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

Note For the procedure for enabling and disabling Telnet on the sensor, refer to Enabling and Disabling Telnet.

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.

For the various ways to open a CLI session directly on the sensor, refer to Logging In to the Sensor.

Step 2 Make sure that the sensor's management interface is enabled:

```
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#
```

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.

Step 3 Make sure the sensor's IP address is unique.

```
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 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

If the management interface detects that another device on the network has the same IP address, it will not come up.

For more information, refer to Changing the IP Address, Netmask, and Gateway.

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 will 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's access list:

```
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 10.89.130.108/23,10.89.130.1
```

```
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

If the workstation's network address is permitted in the sensor's access list, go to Step 6.

Step 6 Add a permit entry for the workstation's network address, save the configuration, and try to connect again.

For more information, refer to Changing the Access List.

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's IP address, and the sensor is in front of the firewall, make sure that the sensor's access list contains a permit entry for the workstation's translated address.

For more information, refer to Changing the Access List.

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: 10.89.149.238/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
      host-name: qsensor-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:

```
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#
```

If the output says the command and control interface link status is down, there is a hardware issue or an IP address conflict.

Step 3 Make sure the sensor's cabling is correct. Refer to the chapter for your sensor in *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*.

Step 4 Run the **setup** command to make sure the IP address is correct. For the procedure, see Initializing the Sensor, page 1-4.

SensorApp and Alerting

This section helps you troubleshoot issues with SensorApp and alerting. It contains the following topics:

SensorApp Not Running

The sensing process, SensorApp, should always be running. If it is not, you do not receive any alerts. SensorApp is part of Analysis Engine, so you must make sure the Analysis Engine is running.

To make sure Analysis Engine is running, follow these steps:

Step 1 Log in to the CLI.

Step 2 Determine the status of the Analysis Engine service:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: ASA-SSM-20
Serial Number: 021
No license present
Sensor up-time is 19 days.
Using 505495552 out of 1984704512 bytes of available memory (25% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 37.7M out of 166.6M bytes of available disk space (24% usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)
```

```
MainApp          2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Running
AnalysisEngine   2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Not Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149

sensor#
```

Step 3 If 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 Make sure you have the latest software updates:

```
sensor# show version
Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149
```

If you do not have the latest software updates, download them from Cisco.com. For the procedure, see Obtaining Cisco IPS Software, page 12-1.

Step 5 Read the Readme that accompanies the software upgrade for any known DDTS for SensorApp or Analysis Engine.

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:

a. Make sure the sensing port is connected properly on the appliance.

Refer to the chapter for your sensor in *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*.

b. Make sure the sensing port is connected to the correct SPAN or VACL capture port on IDSM-2.

For more information, refer to Configuring IDSM-2.

Step 4 Verify the interface configuration:

a. Make sure you have the interfaces configured properly.

For the procedure, see Configuring Interfaces, page 3-10.

b. 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
```

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 be 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.

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:

a. Check the cabling.

For information on installing your sensor properly, refer to the chapter on your sensor in *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*.

b. 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 ...
```

Cleaning Up a Corrupted SensorApp Configuration

If the SensorApp configuration has become corrupted and SensorApp cannot run, you must delete it entirely and restart 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#
```

Bad Memory on IDS-4250-XL

Some IDS-4250-XLs were shipped with faulty DIMMs on the XL cards. The faulty DIMMs cause the sensor to hang or SensorApp to stop functioning and generate a core file.

For the procedure for checking IDS-4250-XL for faulty memory, refer to Partner Field Notice 52563.

Sensor Sending False Positive Alerts

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 and from behind the firewall. IPS 5.1 only supports one virtual sensor, so a single sensor policy and configuration are applied to all monitored data streams.

Symptom Sensor sending false positive alerts.

Possible Cause The same traffic flow cannot traverse the sensor twice either through the same interface in inline mode or through separate monitored interfaces. If packets from the same traffic flow traverse the sensor twice, the virtual sensor interprets the packets as duplicates, which results in false positive alerts.

Solution You can configure NAT to change the IP address to handle this limitation. NAT causes the sensor to treat the before and after translation packets as separate flows. For example, if a firewall is using NAT from its internal to external networks, the sensor can monitor both of these networks without problem.

Blocking

This section provides troubleshooting help for blocking and the ARC service. It contains the following topics:

Troubleshooting Blocking

After you have configured ARC, you can verify if it is running properly by using the **show version** command. To verify that ARC is connecting to the network devices, use the **show statistics network-access** command.

Note ARC was formerly known as Network Access Controller. Although the name has been changed for IPS 5.1, it still appears in IDM and the CLI as Network Access Controller, **nac**, and **network-access**.

To troubleshoot ARC, follow these steps:

1. Verify that ARC is running. For the procedure, see Verifying ARC is Running, page C-17.
2. Verify that ARC is connecting to the network devices. For the procedure, see Verifying ARC Connections are Active, page C-18.
3. Verify that the Event Action is set to Block Host for specific signatures. For the procedure, see Blocking Not Occurring for a Signature, page C-22.
4. Verify that the master blocking sensor is properly configured. For the procedure, see Verifying the Master Blocking Sensor Configuration, page C-23.

Note For a discussion of ARC architecture, see Attack Response Controller, page A-11.

Verifying ARC is Running

To verify that ARC is running, use the **show version** command. If MainApp is not running, ARC cannot run. ARC is part of MainApp.

Step 1 Log in to the CLI.

Step 2 Verify that MainApp is running:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1.1)S152.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
Sensor up-time is 3 days.
Using 734863360 out of 3974291456 bytes of available memory (18% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 35.6M out of 166.8M bytes of available disk space (23% usage)
boot is using 40.5M out of 68.6M bytes of available disk space (62% usage)


MainApp          2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Not Running
AnalysisEngine   2005_Mar_18_12.53   (Release)   2005-03-18T13:03:21-0600   Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-sp-5.0-1.1-   12:53:00 UTC Fri Mar 18 2005

Recovery Partition Version 1.1 - 5.0(1.1)

sensor#
```

Step 3 If MainApp displays `Not Running`, ARC has failed. Contact the TAC.

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 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 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 2005 | include : nac
```

Step 4 Make sure you have the latest software updates:

```
sensor# show version
Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149
```

If you do not have the latest software updates, download them from Cisco.com. For the procedure, see Obtaining Cisco IPS Software, page 12-1.

Step 5 Read the Readme that accompanies the software upgrade for any known DDTS for ARC.

Step 6 Make sure the configuration settings for each device are correct (the username, password, and IP address). For the procedure, see Device Access Issues, page C-19.

Step 7 Make sure the interface and directions for each network device are correct. For the procedure, see Verifying the Interfaces and Directions on the Network Device, page C-20.

Step 8 If the network device is using SSH-DES or SSH-3DES, make sure that you have enabled SSH connections to the device. For the procedure, see Enabling SSH Connections to the Network Device, page C-21.

Step 9 Verify that each interface and direction on each controlled device is correct. For the procedure, see Verifying the Interfaces and Directions on the Network Device, page C-20.

Device Access Issues

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/direction on each network device is correct. For the procedure, see Verifying the Interfaces and Directions on the Network Device, page C-20.

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 router's ACL.

Note You can also perform a manual block from IDM by clicking **Monitoring > Active 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's 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-DES or SSH-3DES as the communication protocol for the network device, you must make sure you have enabled it on the device.

To enable SSH 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:

```
sensor(config)# ssh host blocking_device_ip_ address
```

Step 4 Enter **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 sensor's master blocking sensor configuration, follow these steps:

Step 1 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 2 If the master blocking sensor does not show up in the statistics, you need to add it.

For the procedure, see Configuring the Master Blocking Sensor, page 8-31.

Step 3 Initiate a manual block to a bogus host IP address to make sure the master blocking sensor is initialing blocks:

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
sensor(config-net-gen)# block-hosts 10.16.0.0
```

Step 4 Exit network access general submode:

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

Step 5 Press **Enter** to apply the changes or type **no** to discard them.

Step 6 Verify that the block shows up in the ARC's statistics:

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes =
```

Step 7 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's 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 8 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
```

Logging

TAC may suggest that you turn on debug logging for troubleshooting purposes. LogApp 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.

This section contains the following topics:

- Enabling Debug Logging, page C-24
- Zone Names, page C-28
- Directing cidLog Messages to SysLog, page C-29

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 To 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 To 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)#
```

For a list of what each zone name refers to, see Zone Names, page C-28.

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:

Zone Names

Table C-1 lists the debug logger zone names.

Table C-1 Debug Logger Zone Names

Zone Name	Description
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[1]
cplane	Control Plane zone[2]
csi	CIDS Servlet Interface[3]
ctlTransSource	Outbound control transactions zone
intfc	Interface zone
nac	ARC zone
sensorApp	AnalysisEngine zone
tls	SSL and TLS zone

1. The Card Manager service is used on AIP-SSM to exchange control and state information between modules in the chassis.
2. The Control Plane is the transport communications layer used by Card Manager on AIP-SSM.
3. The CIDS servlet interface is the interface layer between the CIDS web server and the servlets.

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.

Verifying the Sensor is Synchronized with the NTP Server

In IPS 5.1, 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.

TCP Reset Not Occurring for a Signature

If you do not have the event action set to reset, the TCP reset does not occur for a specific signature.

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 the procedure.

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:

IDS-4235 and IDS-4250 Hang During A Software Upgrade

If the BIOS of IDS-4235 and IDS-4250 is at A03, you must upgrade it to A04 before applying the most recent IPS software, otherwise, the appliances hang during the software upgrade process. For the procedure for upgrading the BIOS, refer to Upgrading the BIOS. For the procedure for applying the latest IPS software, see Obtaining Cisco IPS Software, page 12-1.

Issues With Automatic Update

The following list provides suggestions for troubleshooting automatic update:

- 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. For the procedure, refer to Creating the Service Account.
  - Use the **upgrade** command to manually upgrade the sensor. For the procedure, see Chapter 13, "Upgrading, Downgrading, and Installing System Images."
  - 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.
- Make sure you have not modified the FTP server to use custom prompts.

  If you modify the FTP prompts to give security warnings, for example, this causes a problem, because the sensor is expecting a hard-coded list of responses.

  Note Not modifying the prompt only applies to versions before 4.1(4).
- 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. For the procedure, see Defining Known Host Keys, page 2-10.

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 (For the procedure, see Version Information, page C-49).

  Version 4.0(1) has a known problem with automatic update. Upgrade manually to 4.1(1) before trying to configure and use automatic update.
- Make sure the passwords 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.

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.

For the procedure, see Obtaining Cisco IPS Software, page 12-1.

Step 3 FTP or SCP the update file to the sensor's /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's 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: *****
```

Troubleshooting IDM

Note These procedures also apply to the IPS section of ASDM.

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 IDM. This section contains the following topics:

Increasing the Memory Size of the Java Plug-In

To correctly run IDM, your browser must have Java Plug-in 1.4.2 or 1.5 installed. By default the Java Plug-in allocates 64 MB of memory to IDM. IDM can run out of memory while in use, which can cause IDM to freeze or display blank screens. Running out of memory can also occur when you click **Refresh**. An `OutofMemoryError` message appears in the Java console whenever this occurs. You must change the memory settings of Java Plug-in before using IDM. The mandatory minimum memory size is 256 MB.

Note We recommend that you use Sun Microsystems Java. Using any other version of Java could cause problems with IDM.

This section contains the following topics:

Java Plug-In on Windows

To change the settings of Java Plug-in on Windows for Java Plug-in 1.4.2 and 1.5, follow these steps:

Step 1 Close all instances of Internet Explorer or Netscape.

Step 2 Choose **Start > Settings > Control Panel**.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Choose **Java Plug-in**.

The Java Plug-in Control Panel appears.

b. Click the **Advanced** tab.

c. In the Java RunTime Parameters field, enter **`-Xms256m`**.

d. Click **Apply** and exit the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Choose **Java**.

The Java Control Panel appears.

b. Click the **Java** tab.

c. Click **View** under Java Applet Runtime Settings.

The Java Runtime Settings window appears.

d. In the Java Runtime Parameters field, enter `-Xms256m`, and then click **OK**.

e. Click **OK** and exit the Java Control Panel.

Java Plug-In on Linux and Solaris

To change the settings of Java Plug-in 1.4.2 or 1.5 on Linux and Solaris, follow these steps:

Step 1 Close all instances of Netscape or Mozilla.

Step 2 Bring up Java Plug-in Control Panel by launching the ControlPanel executable file.

Note In the Java 2 SDK, this file is located at <SDK installation directory>/jre/bin/ControlPanel. For example if your Java 2 SDK is installed at /usr/j2se, the full path is /usr/j2se/jre/bin/ControlPanel.

Note In a Java 2 Runtime Environment installation, the file is located at <JRE installation directory>/bin/ControlPanel.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click the **Advanced** tab.

b. In the Java RunTime Parameters field, enter `-Xms256m`.

c. Click **Apply** and close the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click the **Java** tab.

b. Click **View** under Java Applet Runtime Settings.

c. In the Java Runtime Parameters field, enter `-Xms256m`, and then click **OK**.

d. Click **OK** and exit the Java Control Panel.

Cannot Launch 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 (1.4.*x* and/or 1.3.*x*) 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. Choose **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. Choose **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 IDM -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 IDM.

Recommended Action Wait for a while and try again to connect.

IDM, Remote Manager, or Sensing Interfaces Cannot Access the Sensor

Note For the procedure for enabling and disabling Telnet on the sensor, refer to Enabling and Disabling Telnet.

If 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 10.89.130.108/23,10.89.130.1
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
```

For more information, refer to Changing Web Server Settings.

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's web server port.

All remote management communication is performed by the sensor's web server. For more information, refer to Changing Web Server Settings.

Signatures Not Producing Alerts

If you are not seeing any alerts when signatures are firing, make sure that you have configured Produce Alert as an event action.

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.

For example, if you choose Produce Alert, but later add another event action and do not add Produce Alert to the new configuration, alerts will not be sent to the Event Store. To make sure you are getting alerts, use statistics for the virtual sensor and event store.

Troubleshooting IDSM-2

IDSM-2 has the same software architecture as the 4200 series sensors. You can use the same troubleshooting tools as outlined in Troubleshooting the 4200 Series Appliance, page C-4.

This section pertains specifically to troubleshooting IDSM-2. It contains the following topics:

Diagnosing IDSM-2 Problems

Use the following list to diagnose IDSM-2 problems:

- The ribbon cable between IDSM-2 and the motherboard is loose.

  During physical handling of the module, the connector can come loose from the base card, and cause the daughter card and the base card to lose contact with each other. A loose ribbon cable connector causes an on-line diagnostic error on ports 7 and 8. The module cannot operate when this condition exists.

  For more information, refer to Partner Field Notice 52816.

- Some IDSM-2s were shipped with faulty DIMMs.

  For the procedure for checking IDSM-s for faulty memory, refer to Partner Field 52563.

- The hard-disk drive fails to read or write.

  When the hard-disk drive has been in constant use for extended periods of time (for more than 2 weeks), multiple symptoms, such as the following, can occur:

  – An inability to log in

  - I/O errors to the console when doing read/write operations (the **ls** command)
  - Commands do not execute properly (cannot find the path to the executable)

  The switch reports that the module is ok, but if you log in to the Service account and try to execute commands, you see that the problem exists. The 4.1(4) service pack alleviates this problem, but if you reimage IDSM-2 with the 4.1(4) application partition image, you must apply the 4.1(4b) patch. For more information, refer to CSCef12198.

- SensorApp either crashes or takes 99% of the CPU when IP logging is enabled for stream-based signatures (1300 series). For the workaround, refer to CSCed32093.
- IDSM-2 appears to lock up and remote access is prohibited (SSH, Telnet, IDM, Event Server, Control Transaction Server, and IP log Server).

  This defect is related to using SWAP. IDSM-2 responds to pings. Apply the 4.1(4) service pack to resolve this issue. For more information, refer to CSCed54146.
- Shortly after you upgrade IDSM-2 or you tune a signature with VMS, IDSM-2 becomes unresponsive and often produces a SensorApp core file. Apply the 4.1(4b) patch to fix this issue.
- Confirm that IDSM-2 has the supported configurations.

  For the list of supported configurations, refer to Supported IDSM-2 Configurations.

If you have confirmed that IDSM-2 does not suffer from any of the problems listed above and yet it appears unresponsive, for example, you cannot log in through SSH or Telnet, nor can you session to the switch, determine if IDSM-2 responds to pings and if you can log in through the service account. If you can log in, obtain a cidDump and any core files and contact TAC.

Switch Commands for Troubleshooting

The following switch commands help you troubleshoot IDSM-2:

- **show module** (Cisco Catalyst Software and Cisco IOS Software)
- **show version** (Cisco Catalyst Software and Cisco IOS Software)
- **show port** (Cisco Catalyst Software)
- **show trunk** (Cisco Catalyst Software)
- **show span** (Cisco Catalyst Software)
- **show security acl** (Cisco Catalyst Software)
- **show intrusion-detection module** (Cisco IOS Software)
- **show monitor** (Cisco IOS Software)
- **show vlan access-map** (Cisco IOS Software)
- **show vlan filter** (Cisco IOS Software)

Status LED Off

If the status indicator is off on IDSM-2, you need to turn power on to IDSM-2.

To determine status of IDSM-2, follow these steps:

Step 1 Log in to the console.

Step 2 Verify that IDSM-2 is online:

For Catalyst Software:

```
console> enable

Enter password:
console> (enable) show module
Mod Slot Ports Module-Type                Model                Sub Status
--- ---- ----- ------------------------- -------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE     yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC          no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45       no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX       no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC       no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2         yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                         Hw     Fw          Sw
--- -------------------------------------- ------ ---------- ----------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1      8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)     8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)     8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)  5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
console> (enable)
```

For Cisco IOS software:

```
router#show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ------------------------------------- ------------------ -----------
  1   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD0401012S
  2   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  5    8  Intrusion Detection System             WS-SVC-IDSM-2      SAD0751059U
  6   16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
  7    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
```

```
 11    8  Intrusion Detection System            WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System            WS-SVC-IDSM-2      SAD072405D8

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1   4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4   5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0   7.2(1)       8.5(0.46)ROC Ok
  5  0003.fead.651a to 0003.fead.6521   4.0   7.2(1)       5.0(1.1)     Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0   7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0   8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3   Unknown      Unknown      PwrDown
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102 7.2(0.67)    5.0(1.1)     Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0   7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model               Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  5 IDS 2 accelerator board     WS-SVC-IDSUPG      07E91E508A    2.0    Ok
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1   1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX   2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .             2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976    2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  5 Pass
  6 Pass
  7 Pass
  9 Unknown
 11 Pass
 13 Pass
router#
```

Note It is normal for the status to read `other` when IDSM-2 is first installed. After IDSM-2 completes the diagnostics routines and comes online, the status reads `ok`. Allow up to 5 minutes for IDSM-2 to come online.

Step 3 If the status does not read `ok`, turn the module on:

```
router# set module power up module_number
```

Status LED On But IDSM-2 Does Not Come Online

If the status indicator is on, but IDSM-2 does not come online, try the following troubleshooting tips:

- Reset IDSM-2.
- Make sure IDSM-2 is installed properly in the switch.
- If the hard-disk drive status has failed, reimage the application partition.

To enable IDSM-2, follow these steps:

Step 1 Log in to the console.

Step 2 Make sure IDSM-2 is enabled:

```
router# show module
```

Step 3 If the status does not read `ok`, enable IDSM-2:

```
router# set module enable module_number
```

Step 4 If IDSM-2 still does not come online, reset it:

```
router# reset module_number
```

Wait for about 5 minutes for IDSM-2 to come online.

Step 5 If IDSM-2 still does not come online, make sure the hardware and operating system are ok:

```
router# show test module_number
```

Step 6 If the `port` status reads `fail`, make sure IDSM-2 is firmly connected in the switch.

Step 7 If the `hdd` status reads `fail`, you must reimage the application partition.

For the procedure, see Chapter 13, "Upgrading, Downgrading, and Installing System Images."

Cannot Communicate With IDSM-2 Command and Control Port

If you cannot communicate with the IDSM-2 command and control port, the command and control port may not be in the correct VLAN.

To communicate with the command and control port of IDSM-2, follow these steps:

Step 1 Log in to the console.

Step 2 Make sure you can ping the command port from any other system.

Step 3 Make sure the IP address, mask, and gateway settings are correct:

```
router# show configuration
```

Step 4 Make sure the command and control port is in the correct VLAN:

For Catalyst software:

```
console> (enable) show port 6/8
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 6/8                       connected  trunk        full        1000 IDS


Port  Status      ErrDisable Reason    Port ErrDisableTimeout  Action on Timeout
----  ----------  -------------------  ----------------------  -----------------
 6/8  connected                      -  Enable                  No Change
```

```
Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 6/8           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 6/8           0          0          0          0         0         0         -

Port  Last-Time-Cleared
----- --------------------------
 6/8  Wed Mar 2 2005, 15:29:49

Idle Detection
--------------
   --
console> (enable)
```

For Cisco IOS software:

```
router# show intrusion-detection module 5 management-port state
Intrusion-detection module 5 management-port:

Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1
Vlans allowed and active in management domain: 1
Vlans in spanning tree forwarding state and not pruned:
   1
Access Vlan = 1


router#
```

Step 5 If the command and control port is not in the correct VLAN, put it in the correct VLAN. For the procedure, refer to Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM-2.

Using the TCP Reset Interface

IDSM-2 has a TCP reset interface—port 1. IDSM-2 has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.

If you have TCP reset problems with IDSM-2, try the following:

- If the sensing ports are access ports (a single VLAN), you must configure the TCP reset port to be in the same VLAN.
- If the sensing ports are dot1q trunk ports (multi-VLAN), the sensing ports and TCP reset port all must have the same native VLAN, and the TCP reset port must trunk all the VLANs being trunked by both the sensing ports.

Connecting a Serial Cable to IDSM-2

You can connect a serial cable directly to the serial console port on IDSM-2. This lets you bypass the switch and module network interfaces.

To connect a serial cable to IDSM-2, follow these steps:

Step 1 Locate the two RJ-45 ports on IDSM-2.

You can find them approximately in the center of the mother board. If you are facing the module faceplate, the RJ-45 port on the right is the serial console port.

Step 2 Connect a straight-through cable to the right port on IDSM-2, and then connect the other end of the cable to a terminal server port.

Step 3 Configure the terminal server port to be 19200 baud, 8 bits, no parity.

You can now log directly in to IDSM-2.

Note Connecting a serial cable to IDSM-2 works only if there is no module located above IDSM-2 in the switch chassis, because the cable has to come out through the front of the chassis.

Troubleshooting AIP-SSM

AIP-SSM has the same software architecture as the 4200 series sensors. You can use the same troubleshooting tools as outlined in Troubleshooting the 4200 Series Appliance, page C-4.

The following section contains commands that are specific to troubleshooting AIP-SSM.

To see the general health of AIP-SSM, use the **show module 1 details** command:

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   0.2
Serial Number:      P2B000005D0
Firmware version:   1.0(10)0
Software version:   5.1(0.1)S153.0
Status:             Up
Mgmt IP addr:       10.89.149.219
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

The output shows that AIP-SSM is up. If the status reads `Down`, you can reset AIP-SSM 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(config)# show module

Mod Card Type                                    Model              Serial No.
```

```
--- ------------------------------------------ ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Shutting Down
**************************************************
asa(config)# show module

Mod Card Type                                     Model              Serial No.
--- ------------------------------------------ ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa(config)#
```

If you have problems with recovering AIP-SSM, use the **debug module-boot** command to see the output as AIP-SSM 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 recover AIP-SSM:

```
asa(config)# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-0.1.i$
Port IP Address [0.0.0.0]: 10.89.150.227
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.89.149.254
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 2005
Slot-1 141> Platform ASA-SSM-10
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=10.89.150.227
Slot-1 147>   SERVER=10.89.146.1
Slot-1 148>   GATEWAY=10.89.149.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.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-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
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 2005
Slot-1 161> Platform ASA-SSM-10
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=10.89.150.227
Slot-1 167>   SERVER=10.89.146.1
Slot-1 168>   GATEWAY=10.89.149.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.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-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
```

Gathering Information

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 sensor's information, or you can use the other individual commands listed in this section for specific information.

This section contains the following topics:

Tech Support Information

The **show tech-support** command is useful for capturing all the sensor's status and configuration information.

This section describes the **show tech-support** command, and contains the following topics:

Overview

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. For the procedure for copying the output to a remote system, see Displaying Tech Support Information, page C-47.

Note You can get the same information from IDM by choosing Monitoring > Support Information > System Information.

Note Always run the **show tech-support** command before contacting TAC.

Displaying Tech Support Information

Use the **show tech-support** [**page**] [**password**] [**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 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.
- **password**—Leaves passwords and other security information in the output.
- **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.

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:

```
sensor# show tech-support page
```

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.

Step 3 To send the output (in HTML format) to a file, follow these steps:

a. Enter the following command, followed by a valid destination:

```
sensor# show tech-support destination-url destination-url
```

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`.

For 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
```

The `password:` prompt appears.

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, ARC, and cidDump services.

```
sensor# show tech-support page

System Status Report
This Report was generated on Fri Feb 21 03:33:52 2003.
Output from 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 = 2208534
   Total Bytes Received = 157390286
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239437
   Total Bytes Transmitted = 107163351
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0

Output from show statistics networkAccess
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = true
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
State
   BlockEnable = true

Output from cidDump

cidDiag
CID Diagnostics Report Fri Feb 21 03:33:54 UTC 2003
5.0(1)
<defaultVersions>
<defaultVersion aspect="S">
<version>149.0</version>
<date>2005-03-04</date>
</defaultVersion>
</defaultVersions>
1.1 - 5.0(1)S149
Linux version 2.4.26-IDS-smp-bigphys (csailer@mcq) (gcc version 2.96 20000731 (R
ed Hat Linux 7.3 2.96-112)) #2 SMP Fri Mar 4 04:11:31 CST 2005
 03:33:54 up 21 days, 23:15,  3 users,  load average: 0.96, 0.86, 0.78
--MORE--
```

Version Information

The **show version** command is useful for establishing the general health of the sensor. This section describes the **show version** command, and contains the following topics:

- Overview, page C-49
- Displaying Version Information, page C-50

Overview

The **show version** command shows the general health of the sensor 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 You can get the same information from IDM or ASDM by choosing 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.

To display the version and configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 View version information:

```
sensor# show version
```

The following examples show sample version output for the appliance and the NM-CIDS.

Sample version output for the appliance:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(0.29)S135.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
Sensor up-time is 5 days.
Using 722145280 out of 3974291456 bytes of available memory (18% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.3M out of 166.8M bytes of available disk space (23% usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600


Upgrade History:

  IDS-K9-maj-5.0-0.29-S91-0.29-.pkg   03:00:00 UTC Mon Feb 16 2004

Recovery Partition Version 1.1 - 5.0(0.29)S91(0.29)

sensor#
```

Sample version output for NM-CIDS:

```
nm-cids# show version
Application Partition:
Cisco Intrusion Prevention System, Version 5.0(0.27)S129.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: NM-CIDS
```

```
Serial Number: JAD06490681
No license present
Sensor up-time is 1 day.
Using 485675008 out of 509448192 bytes of available memory (95% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 31.1M out of 166.8M bytes of available disk space (20% usage)
boot is using 39.5M out of 68.6M bytes of available disk space (61% usage)
application-log is using 529.6M out of 2.8G bytes of available disk space (20% usage)


MainApp          2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600   Running
AnalysisEngine   2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600   Running
CLI              2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600


Upgrade History:

  IDS-K9-maj-5.0-0.27-S91-0.27-.pkg   03:00:00 UTC Thu Feb 05 2004

Recovery Partition Version 1.1 - 5.0(0.27)S91(0.27)

nm-cids#
```

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
! ------------------------------
! Version 5.0(0.26)
! Current configuration last modified Wed Feb 16 03:20:54 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on banner login.
exit
time-zone-settings
--MORE--
```

Statistics Information

The **show statistics** command is useful for examining the state of the sensor's services. This section describes the **show statistics** command, and contains the following topics:

Overview

The **show statistics** command provides a snapshot of the state of the sensor's services. The following services provide statistics:

- AnalysisEngine
- Authentication
- Denied Attackers
- Event Server
- Event Store
- Host
- Logger
- Network Access
- Notification
- SDEE Server
- Transaction Server
- Transaction Source
- Virtual Sensor
- Web Server

Note You can get the same information from IDM by clicking **Monitoring > Support Information > Statistics**.

Displaying Statistics

Use the **show statistics virtual-sensor** [**clear**] command to display the statistics for the virtual sensor. Use the **show statistics** [**analysis-engine** | **authentication** | **denied-attackers** | **event-server** | **event-store** | **host** | **logger** | **network-access** | **notification** | **sdee-server** | **transaction-server** | **transaction-source** | **web-server**] [**clear**] command to generate statistics for each sensor application.

Note The **clear** option is not available for the analysis engine, host, or network access applications.

To display statistics for the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the statistics for the virtual sensor:

```
sensor# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = fe0_1
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1675
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 241
         Total IP packets processed since reset = 12
         Total packets that were not IP processed since reset = 229
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 12
         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 packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total number of bytes processed since reset = 22513
         The rate of packets per second since reset = 0
         The rate of bytes per second since reset = 13
         The average bytes per packet since reset = 93
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers 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.
      The Signature Database Statistics.
         The Number of each type of node active in the system (can not be reset)
            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 = 28
            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 = 6
         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
      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 Initial 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
   Current Streams = 0
   Current Streams Closed = 0
   Current Streams Closing = 0
   Current Streams Embryonic = 0
   Current Streams Established = 0
   Current Streams Denied = 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 = 491
   Number of Alerts Consumed by AlertInterval = 0
   Number of Alerts Consumed by Event Count = 0
   Number of FireOnce First Alerts = 6
   Number of FireOnce Intermediate Alerts = 480
   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 = 491
SigEvent Action Override Stage Statistics
   Number of Alerts received to Action Override Processor = 0
   Number of Alerts where an override was applied = 0
   Actions Added
      deny-attacker-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
```

```
            reset-tcp-connection = 0
         SigEvent Action Filter Stage Statistics
            Number of Alerts received to Action Filter Processor = 0
            Number of Alerts where an action was filtered = 0
            Number of Filter Line matches = 0
            Actions Filtered
               deny-attacker-inline = 0
               deny-connection-inline = 0
               deny-packet-inline = 0
               modify-packet-inline = 0
               log-attacker-packets = 0
               log-pair-packets = 0
               log-victim-packets = 0
               produce-alert = 0
               produce-verbose-alert = 0
               request-block-connection = 0
               request-block-host = 0
               request-snmp-trap = 0
               reset-tcp-connection = 0
         SigEvent Action Handling Stage Statistics.
            Number of Alerts received to Action Handling Processor = 491
            Number of Alerts where produceAlert was forced = 0
            Number of Alerts where produceAlert was off = 0
            Actions Performed
               deny-attacker-inline = 0
               deny-connection-inline = 0
               deny-packet-inline = 0
               modify-packet-inline = 0
               log-attacker-packets = 0
               log-pair-packets = 0
               log-victim-packets = 0
               produce-alert = 11
               produce-verbose-alert = 0
               request-block-connection = 0
               request-block-host = 5
               request-snmp-trap = 0
               reset-tcp-connection = 0
            Deny Actions Requested in Promiscuous Mode
               deny-packet not performed = 0
               deny-connection not performed = 0
               deny-attacker not performed = 0
               modify-packet not performed = 0
            Number of Alerts where deny-connection was forced for deny-packet action = 0
            Number of Alerts where deny-packet was forced for non-TCP deny-connection action
= 0
         Per-Signature SigEvent count since reset
            Sig 2004 = 5
            Sig 2156 = 486
sensor#
```

Step 3 Display the statistics for AnalysisEngine:

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1999
   Measure of the level of current resource utilization = 0
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 13
   Receiver Statistics
      Total number of packets processed since reset = 290
      Total number of IP packets processed since reset = 12
   Transmitter Statistics
```

```
      Total number of packets transmitted = 290
      Total number of packets denied = 0
      Total number of packets reset = 0
   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 = 491
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 11
sensor#
```

Step 4 Display the statistics for authentication:

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 2
   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.
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 Event Store:

```
sensor# show statistics event-store
Event 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 queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
      Alert events, low = 1
```

```
      Alert events, medium = 60
      Alert events, high = 0
sensor#
```

Step 8 Display the statistics for the host:

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05  Thu Feb 10 2005
   Command Control Port Device = FastEthernet0/0
Network Statistics
   fe0_0     Link encap:Ethernet  HWaddr 00:0B:46:53:06:AA
             inet addr:10.89.149.185  Bcast:10.89.149.255  Mask:255.255.255.128
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
             TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:57547021 (54.8 MiB)  TX bytes:63832557 (60.8 MiB)
             Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 500592640
   freeBytes = 8855552
   totalBytes = 509448192
Swap Usage
   Used Bytes = 77824
   Free Bytes = 600649728

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
Auto Update Statistics
   lastDirectoryReadAttempt = N/A
   lastDownloadAttempt = N/A
   lastInstallAttempt = N/A
   nextAttempt = N/A
sensor#
```

Step 9 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 10 Display the statistics for 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 = 10.89.150.219
      NATAddr = 0.0.0.0
      Communications = ssh-des
   NetDevice
      Type = PIX
      IP = 10.89.150.250
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 10.89.150.158
      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 = 10.89.150.138
      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 = 10.89.150.171
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 10.89.150.219
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
```

```
   NetDevice
      IP = 10.89.150.250
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 10.89.150.158
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 10.89.150.138
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 22.33.4.5
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 21.21.12.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 122.122.33.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 111.22.0.0
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

Step 11 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 12 Display the statistics for the SDEE server:

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
sensor#
```

Step 13 Display the statistics for the transaction server:

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
```

```
   failedControlTransactions = 0
sensor#
```

Step 14 Display the statistics for the transaction source:

```
sensor# show statistics transaction-source
General
   totalControlTransactions = 0
   failedControlTransactions = 0
sensor#
```

Step 15 Display the statistics for Web Server:

```
sensor# show statistics web-server
listener-443
   number of server session requests handled = 61
   number of server session requests rejected = 0
   total HTTP requests handled = 35
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 10
   number of busy allocated session objects = 0
crypto library version = 6.0.3
sensor#
```

Step 16 To clear the statistics for an application, for example, the logging application:

```
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
```

The statistics were retrieved and cleared.

Step 17 Verify that the statistics have been cleared:

```
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#
```

The statistics all begin from 0.

Interfaces Information

The **show interfaces** command is useful for gathering information on the sensing and command and control interfaces. This section describes the **show interfaces** command and contains the following topics:

- Overview, page C-61
- Interfaces Command Output, page C-61

Overview

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

You can use the **show events** command to view the alerts generated by SensorApp and errors generated by an application.

This section contains these topics:

Sensor Events

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.

Overview

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

Use the **show events** [{[**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***]] | **error** [warning] [error] [fatal] | **log** | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] command to display events from the 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.

Note Events are displayed as a live feed until you cancel the request by pressing **Ctrl-C**.

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.

  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**—Trait bit position in decimal (0 to 15).
- **error**—Displays error events. Error events are generated by services when error conditions are encountered.
- **log**—Displays log events. Log events are generated when a transaction is received and responded to by an application. Contains information about the request, response, and success or failure of the transaction.
- **NAC**—Displays ARC (block) requests.
- **status**—Displays status events.
- **past**—Displays events starting in the past for the specified hours, minutes, and seconds.
- *hh:mm:ss*—Hours, minutes, and seconds in the past to begin the display.

Note The **show events** command waits until a specified event is available. It continues to wait and display events until you exit by pressing **Ctrl-C.**

To display events from the Event Store, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display all events starting now:

```
sensor# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2003/01/07 04:41:45 2003/01/07 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: 2003/01/07 04:41:45 2003/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

The feed continues showing all events until you press **Ctrl-C**.

Step 3 Display the block requests beginning at 10:00 a.m. on February 9, 2005:

```
sensor# show events NAC 10:00:00 Feb 9 2005
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2005/02/09 10:33:31 2004/08/09 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. February 9 2005:

```
sensor# show events error warning 10:00:00 Feb 9 2005
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2003/01/07 04:49:25 2003/01/07 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: 2005/03/02 14:15:59 2005/03/02 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: 2003/01/08 02:41:00 2003/01/08 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: 2003/01/08 02:41:00 2003/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

Clearing Events

Use the **clear events** command to clear Event Store.

To clear events from Event Store, follow these steps:

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

Step 2 Clear 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 IDM 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 cidDump file's path 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/cidDum
```

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 the procedure, see Uploading and Accessing Files on the Cisco FTP Site, page C-67.

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.

GLOSSARY

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.

A

aaa authentication, authorization, and accounting. The primary and recommended method for access control in Cisco devices.

AAA authentication, authorization, and accounting. Pronounced “triple a.”

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 acknowledgement. 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.

action The sensor’s response 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.

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.

AIP-SSM Advanced Inspection and Prevention Security Services Module. The IPS plug-in module in the Cisco ASA 5500 series adaptive security appliance. See ASA.

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.

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 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.

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.

ASA Adaptive Security Appliance. The ASA combines firewall, VPN concentrator, and intrusion prevention software functionality into one software image. You can configure ASA in single mode or multi-mode.

ASDM Adaptive Security Device Manager. A web-based application that lets you configure and manage your ASA.

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.

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. It verifies that users have the correct permissions to perform CLI, IDM, or RDEP actions.

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 version upgrades 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.

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.

BO2K BackOrifice 2000. A windows back door Trojan that runs over TCP and UDP.

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.

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 internetworks 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.

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 device's routing interfaces as the remote IP address. This is the control interface.

control transaction An IPS message containing a command addressed to a specific application instance. Example control transactions include *start*, *stop*, *getConfig*.

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.

D

Database Processor See DBP.

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.

DBP Database Processor. Maintains the signature state and flow databases.

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.

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 See DFP.

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.

DFP Deny Filters Processor. Handles the deny attacker functions. It maintains a list of denied source IP addresses.

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.

E

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 Server One of the components of the IPS.

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.

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.

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 See FRP.

FRP Fragment Reassembly Processor. 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.

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

Gigabit Ethernet Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.

GMT Greenwich Mean Time. Time zone at zero degrees longitude. Now called Coordinated Universal Time (UTC).

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 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.

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 Netscape or Internet Explorer web browsers.

IDMEF Intrusion Detection Message Exchange Format. The IETF Intrusion Detection Working Group draft standard.

IDSM-2 Intrusion Detection System Module. A switching module that performs intrusion detection in the Catalyst 6500 series switch.

IDS MC Management Center for IDS Sensors. A web-based IDS manager that can manage configurations for up to 300 sensors.

inline mode All packets entering or leaving the network must pass through the sensor.

interface group Refers to the logical grouping of sensing interfaces. Multiple sensing interfaces can be assigned to a logical interface group. Signature parameters are tuned on a per-logical interface group basis.

intrusion detection system 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).

L

L2P Layer 2 Processor. Processes layer 2-related events. It also identifies malformed packets and removes them from the processing path.

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 See L2P.

Logger A component of the IPS.

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.

maintenance partition image A full IPS image used to reimage the maintenance partition of the IDSM-2.

major update A base version that contains major new functionality or a major architectural change in the product.

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.

MEG Mega Event Generator. Signature based on the Meta engine. The Meta engine takes alerts as input rather than packets.

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. AIP SSM, IDSM-2, and NM-CIDS are IPS modules.

monitoring interface See sensing interface.

MSFC, MSFC2 Multilayer Switch Feature Card. An optional card on a Catalyst 6000 supervisor engine that performs L3 routing for the switch.

MSRPC Microsoft Remote Procedure Call.

N

NAC Network Access Controller. See ARC.

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.

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.

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.

NM-CIDS A network module that integrates IPS functionality into the branch office router.

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, an IDSM-2, 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.

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.

P

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.

PASC 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 (Entering Passive Mode) command by opening an unauthorized connection.

passive fingerprinting Act of determining the OS or services available on a system from passive observation of network interactions.

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.

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. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

PIX Firewall Private Internet Exchange Firewall. A Cisco network security device that can be programmed to block/enable addresses and ports between networks.

PKI Public Key Infrastructure. Authentication of HTTP clients using the clients' X.509 certificates.

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 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.

R

rack mounting Refers to mounting a sensor in an equipment rack.

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 signalling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.

RDEP2 Remote Data Exchange Protocol version 2. The published specification for remote data exchange over the command and control network using HTTP and TLS.

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 partition image An IPS image 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.

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.

RR Risk Rating. An RR is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.

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 acknowledgement 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

SAP Signature Analysis Processor. Dispatches packets to the inspectors that are not stream-based and that are configured for interest in the packet in process.

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 is an enhancement to RDEP. It adds extensibility features that are needed for communicating events generated by various types of security devices.

SDP Slave Dispatch Processor.

SEAF signature event action filter. Subtracts actions based on the signature event's signature ID, addresses, and RR. The input to the SEAF is the signature event with actions possibly added by the SEAO.

SEAH signature event action handler. Performs the requested actions. The output from SEAH is the actions being performed and possibly an <evIdsAlert> written to the Event Store.

SEAO signature event action override. Adds actions based on the RR value. SEAO applies to all signatures that fall into the range of the configured RR threshold. Each SEAO is independent and has a separate configuration value for each action type.

SEAP Signature Event Action Processor. Processes event actions. Event actions can be associated with an event risk rating (RR) threshold that must be surpassed for the actions to take place.

Secure Shell Protocol Protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.

Security Monitor Monitoring Center for Security. Provides event collection, viewing, and reporting capability for network devices. Used with the IDS MC.

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 SL. NTP, RPC, SMB, SNMP, and SSH.

service pack Used for the release of bug fixes with no new enhancements. Service packs are cumulative following a base version release (minor or major).

session command Command used on routers and switches to provide either Telnet or console access to a module in the router or switch.

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 See SAP.

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 event action filter See SEAF.

signature event action handler See SEAH.

signature event action override See SEAO.

signature event action processor See SEAP.

signature update Executable image that updates the IPS signature analysis engine (SensorApp) and the NSDB. Applying an IPS signature update is like updating virus definitions on a virus scanning program. Signature updates are released independently and have their own versioning scheme.

Slave Dispatch Processor See SDP.

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.

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.

software bypass Passes traffic through the IPS system without inspection.

source address Address of a network device that is sending data.

SP Statistics Processor. Keeps track of system statistics such as packet counts and packet arrival rates.

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

SRP Stream Reassembly 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.

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 See SP.

Stream Reassembly Processor See SRP.

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.

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.

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, go to http://www.tcpdump.org/.

TCP reset interface The interface on the IDS-4250-XL and IDSM-2 that can send TCP resets. On most sensors the TCP resets are sent out on the same sensing interface on which the packets are monitored, but on the IDS-4250-XL and IDSM-2 the sensing interfaces cannot be used for sending TCP resets. On the IDS-4250-XL the TCP reset interface is the onboard 10/100/100 TX interface, which is normally used on the IDS-4250-TX appliance when the XL card is not present. On the IDSM-2 the TCP reset interface is designated as port 1 with Catalyst software, and is not visible to the user in Cisco IOS software. The TCP reset action is only appropriate as an action selection on those signatures that are associated with a TCP-based service.

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.

TFN2K Tribe Flood Network 2000. A common type of Denial of Service (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).

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 See TP.

TLS Transport Layer Security. The protocol used over stream transports to negotiate the identity of peers and establish encrypted communications.

topology Physical arrangement of network nodes and media within an enterprise networking structure.

TP Time 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.

TPKT RFC 1006-defined method of demarking messages in a packet.

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.

Transaction Server A component of the IPS.

Transaction Source A component of the IPS.

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.

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.

UPS Uninterruptable Power Source.

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

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.

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. IPS 5.x supports only one virtual sensor.

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.

virus update A signature update specifically addressing viruses.

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.

VMS CiscoWorks VPN/Security Management Solution. A suite of network security applications that combines web-based tools for configuring, monitoring, and troubleshooting enterprise VPN, firewalls, network intrusion detection systems and host-based intrusion prevention systems.

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.

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.

Web Server A component of the IPS.

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, go to 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.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W