Configuring IP Logging

This chapter describes how to configure IP logging on the sensor. It contains the following sections:

Understanding IP Logging

You can manually configure the sensor to capture all IP traffic associated with a host you specify by IP address. You can specify how long you want the IP traffic to be logged, how many packets you want logged, and how many bytes you want logged. The sensor stops logging IP traffic at the first parameter you specify.

You can also have the sensor log IP packets every time a particular signature is fired. You can specify how long you want the sensor to log IP traffic and how many packets and bytes you want logged.

⚠
Caution   Enabling IP logging slows down system performance.

✎
Note   You cannot delete or manage IP log files. The **no iplog** command does not delete IP logs, it only stops more packets from being recorded for that IP log. IP logs are stored in a circular buffer that is never filled because new IP logs overwrite old ones.

You can copy the IP logs from the sensor and have them analyzed by a tool that can read packet files in a libpcap format, such as Wireshark or TCPDUMP.

✎
Note   Each alert references IP logs that are created because of that alert. If multiple alerts create IP logs for the same IP address, only one IP log is created for all the alerts. Each alert references the same IP log. However, the output of the IP log status only shows the event ID of the first alert triggering the IP log.

✎
Note On IPS sensors with multiple processors (for example, the IPS 4260 and IPS 4270-20), packets may be captured out of order in the IP logs and by the **packet** command. Because the packets are not processed using a single processor, the packets can become out of sync when received from multiple processors.

Configuring Automatic IP Logging

Use the **ip-log-packets** *number*, **ip-log-time** *number*, and **ip-log-bytes** *number* commands to configure automatic IP logging parameters on the sensor. To reset the parameters, use the **default** keyword.

✎
Note IP logging allows a maximum limit of 20 concurrent IP log files. Once the limit of 20 is reached, you receive the following message in main.log: `Cid/W errWarnIpLogProcessor::addIpLog: Ran out of file descriptors.`

The following options apply:

- **ip-log-packets**—Identifies the number of packets you want logged.

  The valid value is 0 to 65535. The default is 0.

- **ip-log-time**—Identifies the duration you want the sensor to log packets.

  The valid value is 0 to 65535 minutes. The default is 30 minutes.

- **ip-log-bytes** —Identifies the maximum number of bytes you want logged.

  The valid value is 0 to 2147483647. The default is 0.

✎
Note An automatic IP log continues capturing packets until one of these parameters is reached.

Automatic IP logging is configured on a per signature basis or as an event action override. The following actions trigger automatic IP logging:

- log-attacker-packets
- log-victim-packets
- log-pair-packets

To configure automatic IP logging parameters, follow these steps:

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

Step 2 Enter signature definition IP log configuration submode.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# ip-log
```

Step 3 Specify the number of packets you want the sensor to log.

```
sensor(config-sig-ip)# ip-log-packets 200
```

Step 4 Specify the duration you want the sensor to log packets.

```
sensor(config-sig-ip)# ip-log-time 60
```

Step 5   Specify the number of bytes you want logged.

```
sensor(config-sig-ip)# ip-log-bytes 5024
```

Step 6   Verify the settings.

```
sensor(config-sig-ip)# show settings
   ip-log
   -----------------------------------------------
      ip-log-packets: 200 default: 0
      ip-log-time: 60 default: 30
      ip-log-bytes: 5024 default: 0
   -----------------------------------------------
sensor(config-sig-ip)#
```

Step 7   Exit IP logging submode.

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

Step 8   Press **Enter** to apply the changes or type **no** to discard the changes.

For More Information

- To copy and view an IP log file, see Copying IP Log Files to Be Viewed, page 11-7.

- For more information, see Assigning Actions to Signatures, page 8-15 and Configuring Event Action Overrides, page 7-16.

Configuring Manual IP Logging for a Specific IP Address

Use the **iplog** *name ip_address* [**duration** *minutes*] [**packets** *numPackets*] [**bytes** *numBytes*] command to log IP packets manually on a virtual sensor for a specific IP address.

Note   The *minutes*, *numPackets*, and *numBytes* parameters are optional, you do not have to specify all three. However, if you include more than one parameter, the sensor continues logging only until the first threshold is reached. For example, if you set the duration to 5 minutes and the number of packets to 1000, the sensor stops logging after the 1000th packet is captured, even if only 2 minutes have passed.

The following options apply:

- *name*—Virtual sensor on which to begin and end logging.

- *ip_address*—Logs packets containing the specified source and/or destination IP address.

- *minutes*—Duration the logging should be active. The valid range is 1 to 60 minutes. The default is 10 minutes.

- *numPackets*—Maximum number of packets to log. The valid range is 0 to 4294967295. The default is 1000 packets.

- *numBytes*—Maximum number of bytes to log. The valid range is 0 to 4294967295. A value of 0 indicates unlimited bytes.

To manually log packets on a virtual sensor for a specific IP address, follow these steps:

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

Step 2   Start IP logging for a specific IP address.

```
sensor# iplog vs0 10.16.0.0 duration 5
Logging started for virtual sensor vs0, IP address 10.16.0.0, Log ID 1
Warning: IP Logging will affect system performance.
sensor#
```

The example shows the sensor logging all IP packets for 5 minutes to and from the IP address 10.16.0.0.

> **Note**   Make note of the Log ID for future reference.

Step 3   Monitor the IP log status with the **iplog-status** command.

```
sensor# iplog-status
Log ID:            1
IP Address 1:      10.16.0.0
Virtual Sensor:    vs0
Status:            added
Event ID:          0
Bytes Captured:    0
Packets Captured:  0
sensor#
```

> **Note**   Each alert references IP logs that are created because of that alert. If multiple alerts create IP logs for the same IP address, only one IP log is created for all the alerts. Each alert references the same IP log. However, the output of the IP log status only shows the event ID of the first alert triggering the IP log.

For More Information

- To stop logging IP packets for a specific IP address, see Stopping Active IP Logs, page 11-6.
- To log IP packets as an event associated with a signature, see Configuring Automatic IP Logging, page 11-2.
- To copy and view an IP log file, see Copying IP Log Files to Be Viewed, page 11-7.

Displaying the Contents of IP Logs

Use the **iplog-status** [**log-id** *log_id*] [**brief**] [**reverse**] [| {**begin** *regular_expression* | **exclude** *regular_expression* | **include** *regular_expression* }] command to display the description of the available IP log contents.

When the log is created, the status reads added. If and when the first entry is inserted in the log, the status changes to started. When the log is completed, because it reaches the packet count limit, for example, the status changes to completed.

The following options apply:

- *log_id*—(Optional) The log ID of the file for which you want to see the status.
- **brief**—(Optional) Displays a summary of IP log status information for each log.
- **reverse**—(Optional) Displays the list in reverse chronological order (newest log first).
- |—(Optional) Indicates that an output processing specification follows.
- *regular_expression*—Any regular expression found in the IP log status output.
- **begin**—Searches the output of the **more** command and displays the output from the first instance of a specified string.
- **exclude**—Filters the IP log status output so that it excludes lines that contain a particular regular expression.
- **include**—Filters the IP log status output so that it includes lines that contain a particular regular expression.

To view the contents of IP logs, follow these steps:

Step 1   Log in to the CLI.

Step 2   Display the status of all IP logs.

```
sensor# iplog-status
Log ID:               2425
IP Address 1:         10.1.1.2
Virtual Sensor:       vs0
Status:               started
Start Time:           2003/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured:     1039438


Log ID:               2342
IP Address 1:         10.2.3.1
IP Address 2:         10.2.3.4
Virtual Sensor:       vs0
Status:               completed
Event ID:             209348
Start Time:           2003/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:             2003/07/30 18:34:18 2002/07/30 12:34:18 CST
sensor#
```

Step 3   Display a brief list of all IP logs.

```
sensor# iplog-status brief
Log ID   VS    IP Address1    Status      Event ID   Start Date
2425     vs0   10.1.1.2       started     N/A        2003/07/30
2342     vs0   10.2.3.1       completed   209348     2003/07/30
sensor#
```

Stopping Active IP Logs

Use the **no iplog** [**log-id** *log_id* | **name** *name*] command to stop logging for the logs that are in the started state and to remove logs that are in the added state.

Note   Using the **no iplog** command on an added state IP log stops the IP log. The added state means that the IP log is still empty (no packets). Stopping it when there are no packets means you are stopping an empty IP log. An empty log is removed when it is stopped.

Note   The **no iplog** command does not remove or delete the IP log. It only signals to the sensor to stop capturing additional packets on that IP log.

The following options apply:

- *log_id*—Log ID of the logging session to stop. Use the **iplog-status** command to find the log ID.
- *name*—Virtual sensor on which to begin or end logging.

To disable one or all IP logging sessions, follow these steps:

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

Step 2   To stop a particular IP logging session:

a.   Find the log ID of the session you want to stop.

```
sensor# iplog-status
Log ID:          1
IP Address 1:    10.16.0.0
Virtual Sensor:  vs0
Status:          added
Event ID:        0
Bytes Captured:  0
Packets Captured: 0
sensor#
```

Note   Each alert references IP logs that are created because of that alert. If multiple alerts create IP logs for the same IP address, only one IP log is created for all the alerts. Each alert references the same IP log. However, the output of the IP log status only shows the event ID of the first alert triggering the IP log.

b.   Stop the IP log session.

```
sensor# no iplog log-id 137857512
```

Step 3   To stop all IP logging sessions on a virtual sensor:

```
sensor# no iplog name vs0
```

Step 4   Verify that IP logging has been stopped.

```
sensor# iplog-status
Log ID:          1
IP Address 1:    10.16.0.0
Virtual Sensor:  vs0
Status:          completed
```

```
Event ID:          0
Bytes Captured:    0
Packets Captured:  0
sensor#
```

When the logs are stopped, the status shows them as completed.

Copying IP Log Files to Be Viewed

Use the **copy iplog** *log_id destination_url* command to copy IP log files to an FTP or SCP server so that you can view them with a sniffing tool such as Ethereal or TCPDump.

The following options apply:

- *log_id*—The log ID of the logging session. You can retrieve the log ID using the **iplog-status** command.

- *destination_url*—The location of the destination file to be copied. It can be a URL or a keyword.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- ftp:—Destination URL for an FTP network server. The syntax for this prefix is:

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp:—Destination URL for the SCP network server. The syntax for this prefix is:

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

When you use FTP or SCP protocol, you are prompted for a password.

To copy IP log files to an FTP or SCP server, follow these steps:

Step 1   Log in to the CLI.

Step 2   Monitor the IP log status with the **iplog-status** command until you see that the status reads completed for the log ID of the log file that you want to copy.

```
sensor# iplog-status
Log ID:            2425
IP Address:        10.1.1.2
Virtual Sensor:    vs0
Status:            started
Start Time:        2003/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured:  1039438

Log ID:            2342
IP Address:        10.2.3.1
Virtual Sensor:    vs0
Status:            completed
Event ID:          209348
Start Time:        2003/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:          2003/07/30 18:34:18 2002/07/30 12:34:18 CST
sensor#
```

Step 3   Copy the IP log to your FTP or SCP server.

```
sensor# copy iplog 2342 ftp://root@10.16.0.0/user/iplog1
Password: ******** Connected to 10.16.0.0 (10.16.0.0). 220 linux.machine.com FTP server
(Version wu-2.6.0(1) Mon Feb 28 10:30 :36 EST 2000) ready. ftp> user (username) root 331
Password required for root. Password:230 User root logged in. ftp> 200 Type set to I. ftp>
put iplog.8518.tmp iplog1 local: iplog.8518.tmp remote: iplog1 227 Entering Passive Mode
(2,4,6,8,179,125) 150 Opening BINARY mode data connection for iplog1. 226 Transfer
complete. 30650 bytes sent in 0.00246 secs (1.2e+04 Kbytes/sec) ftp>
```

Step 4   Open the IP log using a sniffer program such as Wireshark or TCPDUMP.

For more information on Wireshark, go to http://www.wireshark.org. For more information on
TCPDUMP, go to http://www.tcpdump.org/.