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.