Managing Time-Based Actions

The IDM lets you manage time-based actions, such as configuring and viewing the list of denied attackers, configuring IP logging, setting up host and network blocks, and configuring and managing rate limiting. This section describes how to manage time-based actions, and contains the following topics:

Configuring and Monitoring Denied Attackers

This section describes how to monitor the denied attackers list, and contains the following topics:

Denied Attackers Pane

Note You must be administrator to monitor and clear the denied attackers list.

The Denied Attackers pane displays all IP addresses and the hit count for denied attackers. You can reset the hit count for all IP addresses or clear the list of denied attackers. You can also configure denied attackers to be monitored.

Note Resetting and clearing apply to all items in the table.

Denied Attackers Pane Field Definitions

The following fields are found in the Denied Attackers pane:

- Virtual Sensor—Indicates the virtual sensor that is denying the attacker.
- Attacker IP—Specifies the IP address of the attacker the sensor is denying.
- Victim IP—Specifies the IP address of the victim the sensor is denying.
- Port—Specifies the port of the host the sensor is denying.
- Protocol—Specifies the protocol that the attacker is using.
- Requested Percentage—Specifies the percentage of traffic that you configured to be denied by the sensor in inline mode.
- Actual Percentage—Specifies the percentage of traffic in inline mode that the sensor actually denies.

Note The sensor tries to deny exactly the percentage you requested, but because of percentage fractions, the sensor is sometimes below the requested threshold.

- Hit Count—Displays the hit count for that denied attacker.

Monitoring the Denied Attackers List and Adding Denied Attackers

To view the list of denied attackers, their hit counts, to add and delete denied attackers, and to clear the list of denied attackers and reset the hit count, follow these steps:

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

Step 2 Choose **Configuration > Sensor Management > Time-Based Actions > Denied Attackers**.

Step 3 To refresh the list, click **Refresh**.

Step 4 To clear the entire list of denied attackers, click **Clear List**.

Step 5 To have the hit count start over for all denied attackers, click **Reset All Hit Counts**.

Step 6 To add a denied attacker to the list to be monitored, click **Add**.

Step 7 In the Attacker IP field, enter the attacker IP address.

Note You can enter IPv4 and IPv6 IP addresses.

Step 8 Click the **Specify Victim Address or Port** check box, and enter the IP address and port number.

Step 9 Click the **Specify Virtual Sensor** check box and choose the virtual sensor from the drop-down list.

Tip To discard your changes and return to the Denied Attackers pane, click **Cancel**.

Step 10 Click **OK** to save your changes. The denied attacker appears in the Denied Attacker list.

Step 11 To delete a denied attacker from the list, select it, and then click **Delete**.

Configuring Host Blocks

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

Host Blocks Pane

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Note You must be administrator or operator to configure active host blocks.

Use the Host Blocks pane to configure and manage blocking of hosts. A host block denies traffic from a specific host permanently (until you remove the block) or for a specified amount of time. You can base the block on a connection by specifying the destination IP address and the destination protocol and port. A host block is defined by its source IP address. If you add a block with the same source IP address as an existing block, the new block overwrites the old block.

If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the host block remains in effect until the sensor is rebooted or the block is deleted.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Host Block Pane Field Definitions

The following fields are found in the Host Blocks pane:

- Source IP—Specifies the source IP address for the block.
- Destination IP—Specifies the destination IP address for the block.
- Destination Port—Specifies the destination port for the block.
- Protocol—Specifies the type of protocol (TCP, UDP, or ANY). The default is ANY.
- Minutes Remaining—Specifies the time remaining for the blocks in minutes.
- Timeout (minutes)—Specifies the original timeout value for the block in minutes. A valid value is between 1 to 70560 minutes (49 days).
- VLAN—Specifies the VLAN that carried the data that fired the signature.

Note Even though the VLAN ID is included in the block request, it is not passed to the security appliance. Sensors cannot block on FWSM 2.1 or greater when logged in to the admin context.

- Connection Block Enabled—Specifies whether or not to block the connection for the host.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Add Active Host Block Dialog Box Field Definitions

The following fields are found in the Add Active Host Block dialog box:

- Source IP—Specifies the source IP address for the block.
- Enable connection blocking—Specifies whether or not to block the connection for the host.
- Connection Blocking—Lets you configure parameters for connection blocking:
  - Destination IP—Specifies the destination IP address for the block.
  - Destination Port (optional)—Specifies the destination port for the block.
  - Protocol (optional)—Specifies the type of protocol (TCP, UDP, or ANY). The default is ANY.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

- VLAN (optional)—Specifies the VLAN that carried the data that fired the signature.

Note Even though the VLAN ID is included in the block request, it is not passed to the security appliance. Sensors cannot block on FWSM 2.1 or later when logged in to the admin context.

- Enable Timeout—Lets you set a timeout value for the block in minutes.
- Timeout—Specifies the number of minutes for the block to last. A valid value is between 1 and 70560 minutes (49 days).
- No Timeout—Lets you choose to have no timeout for the block.

Configuring and Managing Host Blocks

To add, delete, and manage host blocks, follow these steps:

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

Step 2 Choose **Configuration > Sensor Management > Time-Based Actions > Host Blocks**, and then click **Add** to add a host block.

Step 3 In the Source IP field, enter the source IP address of the host you want blocked.

Step 4 To make the block connection-based, check the **Enable Connection Blocking** check box:

Note A connection block blocks traffic from a given source IP address to a given destination IP address and destination port.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

a. In the Destination IP field, enter the destination IP address.

b. (Optional) In the Destination Port field, enter the destination port.

c. (Optional) From the Protocol drop-down list, choose the protocol.

Step 5 (Optional) In the VLAN field, enter the VLAN for the connection block.

Step 6 Configure the timeout:

- To configure the block for a specified amount of time, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes.
- T o not configure the block for a specified amount of time, click the **No Timeout** radio button.

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

Step 7 Click **Apply**. The new host block appears in the list in the Host Blocks pane.

Step 8 Click **Refresh** to refresh the contents of the host blocks list.

Step 9 To delete a block, select a host block in the list, and click **Delete**. The Delete Host Block dialog box asks if you are sure you want to delete this block.

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

Step 10 Click **Yes** to delete the block. The host block no longer appears in the list in the Host Blocks pane.

Configuring Network Blocks

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

Network Blocks Pane

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Note You must be administrator or operator to configure network blocks.

Use the Network Blocks pane to configure and manage blocking of networks. A network block denies traffic from a specific network permanently (until you remove the block) or for a specified amount of time. A network block is defined by its source IP address and netmask. The netmask defines the blocked subnet. A host subnet mask is accepted also.

If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the block remains in effect until the sensor is rebooted or the block is deleted.

Note Connection blocks and network blocks are not supported on adaptive security appliances. Adaptive security appliances only support host blocks with additional connection information.

Network Blocks Pane Field Definitions

The following fields are found in the Network Blocks pane:

- IP Address—Specifies the IP address for the block.
- Mask—Specifies the network mask for the block.
- Minutes Remaining—Specifies the time remaining for the blocks in minutes.
- Timeout (minutes)—Specifies the original timeout value for the block in minutes. A valid value is between 1 and 70560 minutes (49 days).

Add Network Block Dialog Box Field Definitions

The following fields are found in the Add Network Block dialog box:

- Source IP—Specifies the IP address for the block.
- Netmask—Specifies the network mask for the block.
- Enable Timeout—Specifies the timeout value for the block in minutes.
- Timeout—Specifies the duration of the block in minutes. A valid value is between 1 and 70560 minutes (49 days).
- No Timeout—Lets you choose to have no timeout for the block.

Configuring and Managing Network Blocks

To add, delete, and manage network blocks, follow these steps:

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

Step 2 Choose **Configuration > Sensor Management > Time-Based Actions > Network Blocks**, and then click **Add** to add a network block.

Step 3 In the Source IP field, enter the source IP address of the network you want blocked.

Step 4 From the Netmask drop-down list, choose the netmask.

Step 5 Configure the timeout:

- To configure the block for a specified amount of time, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes.
- To not configure the block for a specified amount of time, click the **No Timeout** radio button.

Tip To undo your changes and close the Add Network Block dialog box, click **Cancel**.

Step 6 Click **Apply**. You receive an error message if a block has already been added. The new network block appears in the list in the Network Blocks pane.

Step 7 Click **Refresh** to refresh the contents of the network blocks list.

Step 8 Select a network block in the list and click **Delete** to delete that block. The Delete Network Block dialog box asks if you are sure you want to delete this block.

Step 9 Click **Yes** to delete the block. The network block no longer appears in the list in the Network Blocks pane.

Configuring Rate Limits

This section describes how to configure and manage rate limits, and contains the following topics:

Rate Limits Pane

Note You must be administrator to add rate limits.

Use the Rate Limits pane to configure and manage rate limiting. A rate limit restricts the amount of a specified type of traffic that is allowed on a network device interface to a percentage of maximum bandwidth capacity. Traffic that exceeds this percentage is dropped by the network device. A rate limit

can restrict traffic to a specified target host, or to all traffic that crosses the configured interface/directions. You can use rate limits permanently or for a specified amount of time. A rate limit is identified by a protocol, an optional destination address, and an optional data value.

Because the rate limit is specified as a percent, it may translate to different actual limits on interfaces with different bandwidth capacities. A rate limit percent value must be an integer between 1 and 100 inclusive.

Rate Limits Pane Field Definitions

The following fields are found in the Rate Limits pane:

- Protocol—Specifies the protocol of the traffic that is rate limited.
- Rate—Specifies the percent of maximum bandwidth that is allowed for the rate-limited traffic. Matching traffic that exceeds this rate will be dropped.
- Source IP—Specifies the source host IP address of the rate-limited traffic.
- Source Port—Specifies the source host port of the rate-limited traffic.
- Destination IP—Specifies the destination host IP address of the rate-limited traffic.
- Destination Port—Specifies the destination host port of the rate-limited traffic.
- Data—Specifies the additional identifying information needed to more precisely qualify traffic for a given protocol. For example, echo-request narrows the ICMP protocol traffic to rate-limit pings.
- Minutes Remaining—Specifies the remaining minutes that this rate limit is in effect.
- Timeout (minutes)—Specifies the total number of minutes for this rate limit.

Add Rate Limit Dialog Box Field Definitions

The following fields are found in the Add Rate Limit dialog box:

- Protocol—Specifies the protocol of the traffic that is rate-limited (ICMP, TCP, or UDP).
- Rate (1-100)—Specifies the percentage of the maximum bandwidth allowed for the rate-limited traffic.
- Source IP (optional)—Specifies the source host IP address of the rate-limited traffic.
- Source Port (optional)—Specifies the source host port of the rate-limited traffic.
- Destination IP (optional)—Specifies the destination host IP address of the rate-limited traffic.
- Destination Port (optional)—Specifies the destination host port of the rate-limited traffic.
- Use Additional Data—Lets you choose whether to specify more data, such as echo-reply, echo-request, or halfOpenSyn.
- Timeout—Lets you choose whether to enable timeout:
  - No Timeout—Specifies that timeout not enabled.
  - Enable Timeout—Lets you specify the timeout in minutes (1 to 70560).

Configuring and Managing Rate Limiting

To add, delete, and manage rate limiting, follow these steps:

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

Step 2 Choose **Configuration > Sensor Management > Time-Based Actions > Rate Limits**, and then click **Add** to add a rate limit.

Step 3 From the Protocol drop-down list, choose the protocol (ICMP, TCP, or UDP) of the traffic you want rate limited.

Step 4 In the Rate field, enter the rate limit (1 to 100) percent.

Step 5 (Optional) In the Source IP field, enter the source IP address.

Step 6 (Optional) In the Source Port field, enter the source port.

Step 7 (Optional) In the Destination IP field, enter the destination IP address.

Step 8 (Optional) In the Destination Port field, enter the destination port.

Step 9 (Optional) To configure the rate limit to use additional data, check the **Use Additional Data** check box.

Step 10 From the Select Data drop-down list, choose the additional data (echo-reply, echo-request, or halfOpenSyn).

Step 11 Configure the timeout:

- If you do not want to configure the rate limit for a specified amount of time, click the **No Timeout** radio button.
- If you want to configure a timeout in minutes, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes (1 to 70560).

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

Step 12 Click **Apply**. The new rate limit appears in the list in the Rate Limits pane.

Step 13 Click **Refresh** to refresh the contents of the Rate Limits list.

Step 14 To delete a rate limit, select a rate limit from the list, and click **Delete**. The Delete Rate Limit dialog box asks if you are sure you want to delete this rate limit.

Tip To close the Delete Rate Limit dialog box, click **No**.

Step 15 Click **Yes** to delete the rate limit. The rate limit no longer appears in the rate limits list.

Configuring IP Logging

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

Understanding IP Logging

Caution Turning on IP logging slows system performance.

The simplest IP logging consists of an IP address. You can configure the sensor to capture all IP traffic associated with a host you specify by IP address. The sensor begins collecting as soon as it sees the first IP packet with this IP address and continues collecting depending on the parameters that you have set. You can specify in minutes how long you want the IP traffic to be logged at the IP address, and/or how many packets you want logged, and/or how many bytes you want logged. The sensor stops logging IP traffic at the first parameter you specify.

Log files are in one of three states:

- Added—When IP logging is added
- Started—When the sensor sees the first packet, the log file is opened and placed into the Started state.
- Completed—When the IP logging limit is reached.

The number of files in all three states is limited to 20. The IP logs are stored in a circular buffer that is never filled because new IP logs overwrite the old ones. Once the limit of 20 is reached, you receive the following message in main.log: `Cid/W errWarnIpLogProcessor::addIpLog: Ran out of file descriptors.`

Note Logs remain on the sensor until the sensor reclaims them. You cannot manage IP log files on the sensor.

You can copy IP log files to an FTP or SCP server so that you can view them with a sniffing tool such as WireShark or TCPDUMP. The files are stored in PCAP binary form with the pcap file extension.

IP Logging Pane

Note You must be administrator to configure IP logging.

The IP Logging pane displays all IP logs that are available for downloading on the system. IP logs are generated in two ways:

- When you add IP logs in the Add IP Logging dialog box
- When you select one of the following as the event action for a signature:
  - Log Attacker Packets
  - Log Pair Packets
  - Log Victim Packets

When the sensor detects an attack based on this signature, it creates an IP log. The event alert that triggered the IP log appears in the IP logging table.

Caution You must have packet logging enabled on the Packet Logging pane (**Configuration > Sensor Management > Packet Logging**) to configure IP logging.

IP Logging Pane Field Definitions

The following fields are found in the IP Logging pane:

- Log ID—Specifies the ID of the IP log.
- Virtual Sensor—Specifies the virtual sensor with which the IP log is associated.
- IP Address—Specifies the IP address of the host for which the log is being captured.
- Status—Specifies the status of the IP log. Valid values are added, started, or completed.
- Start Time—Specifies the timestamp of the first captured packet.
- Current End Time—Specifies the timestamp of the last captured packet. There is no timestamp if the capture is not complete.
- Alert ID—Specifies the ID of the event alert, if any, that triggered the IP log.
- Packets Captured—Specifies the current count of the packets captured.
- Bytes Captured—Specifies the current count of the bytes captured.

Add and Edit IP Logging Dialog Boxes Field Definitions

The following fields are found on the Add and Edit IP Logging dialog boxes:

- Virtual Sensor—Specifies the virtual sensor from which you want to capture IP logs.
- IP Address—Specifies the IP address of the host for which the log is being captured.

Note You can enter IPv4 and IPv6 IP addresses.

Note If IP logging is already enabled for a particular IP address and virtual sensor, that IP log is overwritten with the new IP log.

- Maximum Values—Lets you set the values for IP logging:
  - Duration—Specifies the maximum duration to capture packets. The range is 1 to 60 minutes. The default is 10 minutes.
  - Packets (optional)—Specifies the maximum number of packets to capture. The range is 0 to 4294967295 packets.
  - Bytes (optional)—Specifies the maximum number of bytes to capture. The range is 0 to 4294967295 bytes.

Configuring IP Logging

To log IP traffic for a particular host, follow these steps:

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

Step 2 Choose **Configuration > Sensor Management > Time-Based Actions > IP Logging**, and then click **Add**.

Step 3 From the Virtual Sensor drop-down list, choose for which virtual sensor you want to turn on IP logging.

Step 4 In the IP Address field, enter the IP address of the host from which you want IP logs to be captured. You receive an error message if a capture is being added that exists and is in the Added or Started state.

Note You can enter IPv4 and IPv6 IP addresses.

Note If IP logging is already enabled for a particular IP address and virtual sensor, that IP log is overwritten with the new IP log.

Step 5 In the Duration field, enter how many minutes you want IP logs to be captured. The range is 1 to 60 minutes. The default is 10 minutes.

Step 6 (Optional) In the Packets field, enter how many packets you want to be captured. The range is 0 to 4294967295 packets.

Step 7 (Optional) in the Bytes field, enter how many bytes you want to be captured. The range is 0 to 4294967295 packets.

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

Step 8 Click **Apply** to apply your changes and save the revised configuration. The IP log with a log ID appears in the list in the IP Logging pane.

Step 9 To stop IP logging, select the log ID for the log you want to stop, and click **Stop**.

Step 10 Click **OK** to stop IP logging for that log.

Step 11 To download an IP log, select the log ID, and click **Download**.

Step 12 Save the log to your local machine. You can view it with WireShark.