Globally Limiting Intrusion Event Logging

You can use thresholds to limit the number of times the system logs and displays intrusion events. This chapter covers the following sections:

Limiting Intrusion Event Logging

Thresholds, which you configure as part of your intrusion policy, cause the system to generate events based on how many times traffic matching a rule originates from or is targeted to a specific address or address range within a specified time period. This can prevent you from being overwhelmed with a large number of events. This feature requires a Protection license.

You can set event notification thresholds in two ways:

- You can set a global threshold across all traffic to limit how often events from a specific source or destination are logged and displayed per specified time period. For more information, see Understanding Thresholding, on page 1 and Configuring Global Thresholds, on page 3.
- You can set thresholds per shared object rule, standard text rule, or preprocessor rule in your intrusion policy configuration, as described in Configuring Event Thresholding.

Understanding Thresholding

License: Protection

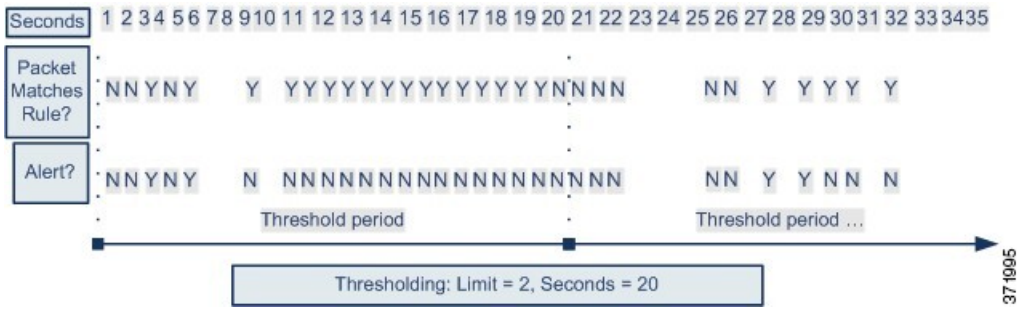
By default, every intrusion policy contains a global rule threshold. The default threshold limits event generation for each rule to one event every 60 seconds on traffic going to the same destination. This global threshold applies by default to all intrusion rules and preprocessor rules. Note that you can disable the threshold in the Advanced Settings page in an intrusion policy.

You can also override this threshold by setting individual thresholds on specific rules. For example, you might set a global limit threshold of five events every 60 seconds, but then set a specific threshold of ten events for every 60 seconds for SID 1315. All other rules generate no more than five events in each 60-second period, but the system generates up to ten events for each 60-second period for SID 1315.

For more information on setting rule-based thresholds, see Configuring Event Thresholding.

The following diagram shows an example where an attack is in progress for a specific rule. A global limit threshold limits event generation for each rule to two events every 20 seconds.

Note that the period starts at one second and ends at 21 seconds. After the period ends, note that the cycle starts again and the next two rule matches generate events, then the system does not generate any more events during that period.



Understanding Thresholding Options

License: Protection

Thresholding allows you to limit intrusion event generation by generating only a specific number of events in a time period, or by generating one event for a set of events. When you configure global thresholding, you must first specify the thresholding type, as described in the following table.

Table 1: Thresholding Options

Option	Description
Limit	Logs and displays events for the specified number of packets (specified by the count argument) that trigger the rule during the specified time period. For example, if you set the type to **Limit**, the **Count** to 10 , and the **Seconds** to 60 , and 14 packets trigger the rule, the system stops logging events for the rule after displaying the first 10 that occur within the same minute.
Threshold	Logs and displays a single event when the specified number of packets (specified by the count argument) trigger the rule during the specified time period. Note that the counter for the time restarts after you hit the threshold count of events and the system logs that event. For example, you set the type to **Threshold**, **Count** to 10 , and **Seconds** to 60 , and the rule triggers 10 times by second 33. The system generates one event, then resets the Seconds and Count counters to 0 . The rule then triggers another 10 times in the next 25 seconds. Because the counters reset to 0 at second 33, the system logs another event.
Both	Logs and displays an event once per specified time period, after the specified number (count) of packets trigger the rule. For example, if you set the type to **Both**, **Count** to 2 , and **Seconds** to 10 , the following event counts result: • If the rule is triggered once in 10 seconds, the system does not generate any events (the threshold is not met) • If the rule is triggered twice in 10 seconds, the system generates one event (the threshold is met when the rule triggers the second time) • If the rule is triggered four times in 10 seconds, the system generates one event (the threshold is met when the rule triggered the second time and following events are ignored)

Next, specify the tracking, which determines whether the event instance count is calculated per source or destination IP address. Finally, specify the number of instances and time period that define the threshold.

Table 2: Thresholding Instance/Time Options

Option	Description
Count	The number of event instances per specified time period per tracking IP address or address range required to meet the threshold.
Seconds	The number of seconds that elapse before the count resets. If you set the threshold type to **Limit**, the tracking to **Source**, **Count** to 10, and **Seconds** to 10, the system logs and displays the first 10 events that occur in 10 seconds from a given source port. If only seven events occur in the first 10 seconds, the system logs and displays those, if 40 events occur in the first 10 seconds, the system logs and displays 10, then begins counting again when the 10-second time period elapses.

Configuring Global Thresholds

License: Protection

You can set a global threshold to manage the number of events generated by each rule over a period of time. When you set a global threshold, that threshold applies for each rule that does not have an overriding specific threshold. For more information on configuring thresholds, see Understanding Thresholding, on page 1.

A global threshold is configured on your system by default. The default values are as follows:

- **Type** — Limit
- **Track By** — Destination
- **Count** — 1
- **Seconds** — 60

To configure global thresholding:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**.

The Intrusion Policy page appears.

Step 2 Click the edit icon ( ) next to the policy you want to edit.

If you have unsaved changes in another policy, click **OK** to discard those changes and continue. See Resolving Conflicts and Committing Policy Changes for information on saving unsaved changes in another policy.

The Policy Information page appears.

Step 3 Click **Advanced Settings** in the navigation panel on the left.

The Advanced Settings page appears.

Step 4 You have two choices, depending on whether **Global Rule Thresholding** under **Intrusion Rule Thresholds** is enabled:

- If the configuration is enabled, click **Edit**.

- If the configuration is disabled, click **Enabled**, then click **Edit**.

The Global Rule Thresholding page appears. A message at the bottom of the page identifies the intrusion policy layer that contains the configuration. See Using Layers in a Network Analysis or Intrusion Policy Layers for more information.

Step 5 From the **Type** radio buttons, select the type of threshold that will apply over the time specified by the seconds argument. See the Table 1: Thresholding Options , on page 2 table for more information:

- Select **Limit** to log and display an event for each packet that triggers the rule until the limit specified by the count argument is exceeded.
- Select **Threshold** to log and display a single event for each packet that triggers the rule and represents either the instance that matches the threshold set by the count argument or is a multiple of the threshold.
- Select **Both** to log and display a single event after the number of packets specified by the count argument trigger the rule.

Step 6 Select the tracking method from the **Track By** radio buttons:

- Select **Source** to identify rule matches in traffic coming from a particular source IP address or addresses.
- Select **Destination** to identify rule matches in traffic going to a particular destination IP address.

Step 7 In the **Count** field:

- For a **Limit** threshold, specify the number of event instances per specified time period per tracking IP address required to meet the threshold.
- For a **Threshold** threshold, specify the number of rule matches you want to use as your threshold.

Step 8 In the **Seconds** field:

- For a **Limit** threshold, specify the number of seconds that make up the time period when attacks are tracked.
- For a **Threshold** threshold, specify the number of seconds that elapse before the count resets. Note that the count resets if the number of rule matches indicated by the **Count** field occur before the number of seconds indicated elapse.

Step 9 Save your policy, continue editing, discard your changes, or exit while leaving your changes in the system cache. See Resolving Conflicts and Committing Policy Changes for more information.

Disabling the Global Threshold

License: Protection

By default, a global limit threshold limits the number of events on traffic going to a destination to one event per 60 seconds. You can disable global thresholding in the highest policy layer if you want to threshold events for specific rules and not apply thresholding to every rule by default.

To disable global thresholding:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**.

The Intrusion Policy page appears.

Step 2 Click the edit icon ( ) next to the policy you want to edit.

If you have unsaved changes in another policy, click **OK** to discard those changes and continue. See Resolving Conflicts and Committing Policy Changes for information on saving unsaved changes in another policy.

The Policy Information page appears.

Step 3 Click **Settings** in the navigation panel on the left.

The Settings page appears.

Step 4 Under **Intrusion Rule Thresholds**, disable **Global Rule Thresholding**.

Step 5 Save your policy, continue editing, discard your changes, or exit while leaving your changes in the system cache. See Resolving Conflicts and Committing Policy Changes for more information.

What to do next