

CISCO Elephant Flow Detection User Guide

[Home](#) » [Cisco](#) » **CISCO Elephant Flow Detection User Guide** 

Contents

- [1 CISCO Elephant Flow Detection User Guide](#)
- [2 About Elephant Flow Detection and Remediation](#)
- [3 Elephant Flow Upgrade from Intelligent Application Bypass](#)
- [4 Configure Elephant Flow](#)
- [5 Documents / Resources](#)

CISCO Elephant Flow Detection User Guide



Elephant flows are extremely large (in total bytes), continuous flows set up by a TCP (or other protocols) flow measured over a network link. By default, elephant flows are those larger than 1 GB/10 seconds. They can cause performance duress in Snort cores. Elephant flows are not numerous, but they can occupy a disproportionate share of the total bandwidth over a period of time. They can lead to problems, such as high CPU utilization, packet drops, and so on.

From management center 7.2.0 onwards (Snort 3 devices only), you can use the elephant flow feature to detect and remediate elephant flows, which helps to reduce system stress and resolve the mentioned issues.

- About Elephant Flow Detection and Remediation, on page 1
- Elephant Flow Upgrade from Intelligent Application Bypass, on page 1
- Configure Elephant Flow, on page 2

About Elephant Flow Detection and Remediation

You can use the elephant flow detection feature to detect and remediate elephant flows. The following remediation actions can be applied:

- Bypass elephant flow—You can configure elephant flow to bypass Snort inspection. If this is configured, Snort does not receive any packet from that flow.
- Throttle elephant flow—You can apply rate-limit to the flow and continue to inspect flows. The flow rate is calculated dynamically and 10% of the flow rate is reduced. Snort sends the verdict (QoS flow with 10% less flow rate) to the firewall engine. If you choose to bypass all applications including unidentified applications, you cannot configure the throttle action (rate-limit) for any flow.

Note For the elephant flow detection to work, Snort 3 must be the detection engine.

Elephant Flow Upgrade from Intelligent Application Bypass

Intelligent Application Bypass (IAB) is deprecated from version 7.2.0 onwards for Snort 3 devices. For devices running 7.2.0 or later, you must configure elephant flow settings under the Elephant Flow Settings section in the AC policy (Advanced settings tab).


Post-upgrade to 7.2.0 (or later), if you are using a Snort 3 device, the elephant flow configuration settings will be picked and deployed from the Elephant Flow Settings section and not from the Intelligent Application Bypass Settings section, so if you have not migrated to Elephant Flow configuration settings, your device will lose the elephant flow configuration upon the next deployment.

The following table shows the IAB or elephant flow configurations that can be applied to version 7.2.0 or later and to version 7.1.0 or earlier that are running Snort 3 or Snort 2 engines.

Management Center	Threat Defense	Elephant Flow or IAB Configuration
Management Center 7.0 or 7.1	Snort 2 device	Configuration from IAB is applicable.
	Snort 3 device	Configuration from IAB is applicable.
Management Center 7.2.0	Snort 2 device	Configuration from IAB is applicable.
	Snort 3 device (7.1.0 and earlier)	Configuration from IAB is applicable.
	Snort 3 device (7.2.0 and later)	Configuration from Elephant Flow is applicable.

Configure Elephant Flow

You can configure elephant flow to take actions on elephant flows, which helps resolve issues, such as system duress, high CPU utilization, packet drops, and so on.

 **Attention :** Elephant flow detection is not applicable for prefiltered, trusted, or fast-forwarded flows, which do not process through Snort. As elephant flows are detected by Snort, elephant flow detection is not applicable for encrypted traffic.

Procedure

Step 1

In the access control policy editor, click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line. Then, click **Edit** (✎) next to **Elephant Flow Settings**.

If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Figure 1: Configure Elephant Flow Detection

The screenshot shows the 'Elephant Flow Settings' window. At the top, there is a light blue banner with two lines of text: 'For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.' and 'For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass settings.' Below this is another light blue banner stating 'Elephant flow detection does not apply to encrypted traffic. [Learn more](#)'. The main settings area has a section titled 'Elephant Flow Detection' with a toggle switch that is turned on. Below this, it says 'Generate elephant flow events when flow bytes exceeds 1024 MB and flow duration exceeds 10 seconds'. The next section is 'Elephant flow Remediation' with a toggle switch that is also turned on. Below this, it says 'If CPU utilization exceeds 40 % in fixed time windows of 30 seconds and packet drop exceeds 5 %'. There is a section 'Then Bypass the flow' with a toggle switch that is turned on. Below this, there are two radio button options: 'All applications including unidentified applications' and 'Select Applications/Filters (1 selected)'. The last section is 'And Throttle the remaining flows' with a toggle switch that is turned on.

Step 2 The Elephant Flow Detection toggle button is enabled by default. You can configure the values for flow bytes and flow duration. When they exceed your configured values, elephant flow events are generated.

Step 3 To remediate elephant flows, enable the Elephant Flow Remediation toggle button.

Step 4 To set the criteria for remediation of the elephant flow, configure the values for CPU utilization %, duration of fixed time windows, and packet drop %.

Step 5 You can perform the following actions for elephant flow remediation when it meets the configured criteria:

- Bypass the flow—Enable this button to bypass Snort inspection for selected applications or filters. Choose from:
 - All applications including unidentified applications—Select this option to bypass all the application traffic. If you configure this option, you cannot configure the throttle action (rate-limit) for any flow.
 - Select Applications/Filters—Select this option to select the applications or filters whose traffic you want to bypass; see [Configuring Application Conditions and Filters](#).
- Throttle the flow—Enable this button to apply rate-limit to the flow and continue to inspect flows. Note that you can select the applications or filters to bypass Snort inspection and throttle the remaining flows.

Note

Automatic removal of throttle from a throttled elephant flow occurs when the system is out of duress, that is, the percentage of Snort packet drops is lesser than your configured threshold. Consequently, rate limiting is also removed.

You can also manually remove throttling from a throttled elephant flow, using the following threat defense commands:

- clear efd-throttle <5-tuple/all> bypass—This command removes throttling from the throttled elephant flow and bypasses Snort inspection.
 - clear efd-throttle <5-tuple/all>—This command removes throttling from the throttled elephant flow and Snort inspection continues. Elephant flow remediation is skipped after using this command.
- For more information about these commands, see the Cisco Secure Firewall Threat Defense Command Reference.

Attention

Taking action on elephant flows (bypass and throttle the flow) is not supported on Cisco Firepower 2100 series devices.

Step 6 In the Remediation Exemption Rule section, click Add Rule to configure L4 access control list (ACL) rules for flows that must be exempted from remediation.

Step 7 In the Add Rule window, use the Networks tab to add the network details, that is the source network and the destination network. Use the Ports tab to add the source port and the destination port.

If an elephant flow is detected and it matches the rules that are defined, an event is generated with the reason as Elephant Flow Exempted in the Reason column header of Connection Events.

Step 8 In the Remediation Exemption Rule section, you can view the flows that are exempt from the remediation action.

Step 9 Click OK to save the elephant flow settings.


Step 10 Click Save to save the policy.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

After configuring your elephant flow settings, monitor your connection events to see if any flows are detected, bypassed, or throttled. You can view this in the Reason field of your connection event. The three reasons for elephant flow connections are:


- Elephant Flow
- Elephant Flow Throttled
- Elephant Flow Trusted

 **Attention** Enabling elephant flow detection alone does not cause generation of connection events for elephant flows. If a connection event is already logged for another reason and the flow is also an elephant flow, then the Reason field contains this information. However, to ensure that you are logging all elephant flows, you must enable connection logging in the applicable access control rules.

Refer to Cisco Secure Firewall Elephant Flow Detection for more information.

Read More About This Manual & Download PDF:

Documents / Resources

 <p>Elephant Flow Detection</p> <p>Elephant Flow Detection is a new feature in Cisco Secure Firewall Threat Defense that allows you to detect and remediate elephant flows. This document provides information about the features and configuration of Elephant Flow Detection.</p> <p>About Elephant Flow Detection and Remediation</p> <p>Elephant Flow Detection is a new feature in Cisco Secure Firewall Threat Defense that allows you to detect and remediate elephant flows. This document provides information about the features and configuration of Elephant Flow Detection.</p> <p>Elephant Flow Upgrade from Intelligent Application Response</p> <p>Elephant Flow Upgrade from Intelligent Application Response is a new feature in Cisco Secure Firewall Threat Defense that allows you to upgrade from Intelligent Application Response to Elephant Flow Detection. This document provides information about the features and configuration of Elephant Flow Upgrade from Intelligent Application Response.</p>	<p>CISCO Elephant Flow Detection [pdf] User Guide</p> <p>7.4, Elephant Flow Detection, Detection</p>
--	--

