Use Case - Configure Elephant Flow Detection Outcomes

About Elephant Flows

Elephant flows are extremely large (in total bytes), relative long-running network connections set up by a TCP (or other protocols) flow measured over a network link. By default, elephant flows are flows or connections that are larger than 1 GB per 10 seconds. They can cause performance duress or issues in Snort cores. Elephant flows are important because they can potentially consume an excessive amount of CPU resources and impact other competing flows for detection resources and cause issues, such as increased latency or packet drops.

## Benefits of Elephant Flow Detection and Remediation

- Elephant flow configuration allows customization and the option to bypass or even throttle elephant flows.

- You can choose to bypass or throttle flows that are based on your chosen applications to provide Snort inspection of suspect traffic, while bypassing more trusted traffic.

- Elephant flow remediation helps prioritize and free up more bandwidth for your internal applications, depending on your specific requirements.

Elephant Flow Workflow

When an elephant flow is detected based on your configured parameters, you can choose to bypass or throttle the flow. When a flow is bypassed, the traffic is allowed to pass without Snort inspection. Throttling indicates that the flow throughput is reduced. The reduction on flow rate is done in 10 percent increments until the CPU utilization reduces to below the configured threshold. Bypassing or throttling happens after identifying the elephant flow and meeting the additional CPU and time window parameters. Prior to identification of the elephant flow, your intrusion policy processes the flow, assuming that you have configured this in an Allow rule. This means that elephant flows are not allowed to pass through the system completely uninspected because most of the attacks are detected very early in a connection.

To understand how flows are handled, see the following flow diagram.

Figure 1: Elephant Flow Workflow
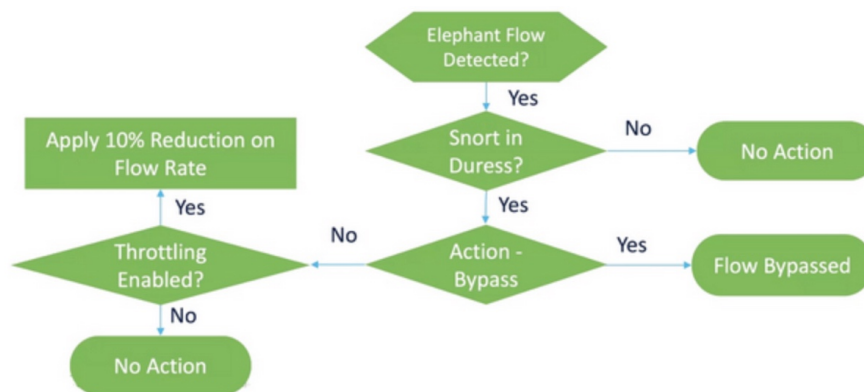
No action is taken unless the system detects a Snort duress condition (performance issue). The system does not throttle or bypass a flow just because it is large. Also, the actions of throttle and bypass are mutually exclusive. This means that you can either bypass or throttle a flow, but not both.

If you do not want to bypass all the elephant flows causing duress, you can limit the bypass option to specific applications only. You can prioritize connectivity for the applications that you trust, without throttling performance. You can configure the applications that must be bypassed, but the remaining flows (causing duress) are throttled. This ensures that the other nontrusted application flows still receive full Snort inspection although their bandwidth is reduced.

Sample Business Scenario

In a data center, several activities are happening, such as replication of data between clusters, virtual machine integration, and database backup. Users in an organization could be watching videos on an OTT or downloading them. Bandwidth utilization for such activities might result in elephant flows, slow down the network, and impact the performance of important tasks. As a network administrator (and depending on your specific requirements), you want visibility into such large flows that are causing bandwidth issues and remediate them.

As an example, let us see how you can configure elephant flow parameters to bypass Snort inspection for WebEx traffic (which your organization uses for real-time video conferencing) and throttle the remaining applications or connections, including videos, movies, and so on.

Prerequisites

- Ensure that you are running management center 7.2.0 or later and that the managed threat defense is also 7.2.0 or later.

- Only enabling elephant flow detection does not generate additional connection events. Elephant flow detection adds the Elephant Flow notation to matching connections that are already being logged to the management center. **To log these events, you must enable connection logging in your access control policy.** You can do that for specific rules or add a Monitor rule that logs all connections, including elephant flows.

Configure Elephant Flow Parameters

Procedure

Step 1   Choose **Policies** > **Security policies** > **Access Control**.

Step 2   Click **Edit** (✎) next to the access control policy that you want to edit.

Step 3   Choose **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 4   Click **Edit** (✎) next to **Elephant Flow Settings**.
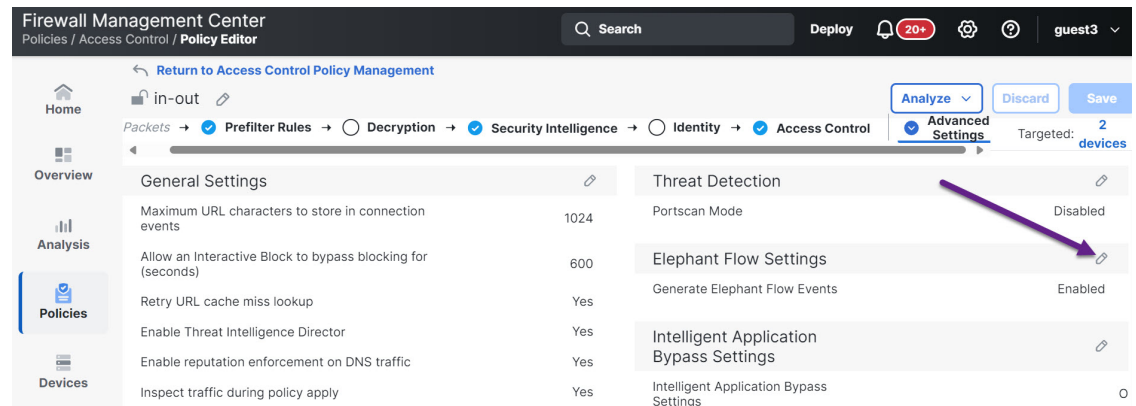
Step 5   The **Elephant Flow Detection** toggle button is enabled by default. The default setting enables detection only and no default action is configured. The detection settings allow you to adjust the flow bytes and duration so that you can identify the elephant flows in your system.

As a test setting, configure the flow bytes and duration parameters, as shown in the following figure.

Elephant Flow Settings ?

> ⓘ For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
> For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass settings.
>
> Elephant flow detection does not apply to encrypted traffic. **Learn more**

Elephant Flow Detection 🔵

Generate elephant flow events when flow bytes exceeds `1` MB and flow duration exceeds `2` seconds

Elephant flow Remediation ⚪ ⓘ

If CPU utilization exceeds `40` % in fixed time windows of `30` seconds and packet drop exceeds `5` %

Then Bypass the flow ⚪

Or Throttle the flow ⚪

[Revert to Defaults]   Cancel   [**OK**]

Step 6   Enable the **Elephant Flow Remediation** toggle button. When an elephant flow is detected, you can choose to bypass or throttle the flow. Bypassing a flow means that the traffic is allowed to pass without Snort inspection. Throttling indicates that the flow throughput is reduced. This rate reduction is done in 10 percent increments until the CPU utilization reduces to lesser than the configured threshold.

As a test setting, configure the elephant flow remediation parameters as shown in the following figure.

Elephant Flow Settings ?

> ⓘ For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
> For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass setting
>
> Elephant flow detection does not apply to encrypted traffic. **Learn more**

Elephant Flow Detection 🔵

Generate elephant flow events when flow bytes exceeds `1` MB and flow duration exceeds `2` seconds

Elephant flow Remediation 🔵 ⓘ

If CPU utilization exceeds `1` % in fixed time windows of `15` seconds and packet drop exceeds `1` %

Then Bypass the flow ⚪

Or Throttle the flow ⚪

Step 7   Enable the **Bypass the flow** toggle button and click the **Select Applications/Filters** radio button.

Elephant Flow Settings

> For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
> For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass setting
> Elephant flow detection does not apply to encrypted traffic. **Learn more**

Elephant Flow Detection

Generate elephant flow events when flow bytes exceeds   `1`   MB and flow duration exceeds   `2`   seconds

Elephant flow Remediation

If CPU utilization exceeds   `1`   % in fixed time windows of   `15`   seconds and packet drop exceeds   `1`   %

Then Bypass the flow

- ⦿ All applications including unidentified applications
- ○ Select Applications/Filters (0 selected)

Or Throttle the flow

Step 8   Under **Application Filters**, search for and select the **WebEx** application, add it to the rule, and click **Save**. This means that WebEx connections are trusted and prioritized and will skip Snort inspection if these WebEx connections are detected as elephant flows, based on the configured parameters.

Add Bypassable Applications

Application Filters ⟳ Clear All Filters	Available Applications (7) ⟳		Selected Applications and Filters (1)
🔍 Search by name	🔍 webex ⊗		Applications
∨ User-Created Filters	All apps matching the filter	**Add to Rule**	WebEx 🗑
∨ Risks (Any Selected)	Cisco Webex Assistant ⓘ		
☐ Very Low 1601	WebEx ⓘ		
☐ Low 954	WebEx Connect ⓘ		
☐ Medium 1788	WebEx Media ⓘ		
☐ High 1876	WebEx Sharing ⓘ		
☐ Very High 610	Webex Teams ⓘ		
	Webex Teams Post/Share ⓘ		

Cancel   **Save**

Step 9   Enable the **Throttle** toggle button to throttle the remaining flows (causing duress). This ensures that all the other flows are slowed down in 10 percent increments until the Snort duress condition is met.

Step 10   Click **OK**.

Step 11   Click **Save**.

What to do next

Deploy configuration changes. See Deploy Configuration Changes.

View Events for Elephant Flows

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

- Elephant Flow
- Elephant Flow Throttled
- Elephant Flow Trusted

Procedure

Step 1 Choose **Events & Logs** > **+ Show more** > **Connection** > **Events**. You can also view the events from the **Unified Events** viewer.

Step 2 In the **Connection Events** page, from the **Predefined Search** drop-down list, choose **Elephant Flows** to display elephant flow events.

Tip

To see **Elephant Flow Trusted** or **Elephant Flow Throttled** event types, click the **Edit Search** link on the top-left corner of the page and in the **Reason** field, choose **Elephant Flows** in the left panel. Enter **Elephant Flow Trusted** or **Elephant Flow Throttled**, depending on what you want to search.

Step 3   View the elephant flow that was detected mid-flow and the **Reason** field shows **Elephant Flow**. At the end of the flow, it was bypassed and the **Reason** field shows **Elephant Flow Trusted**.

Configure Elephant Flow Remediation Exemption

You can configure L4 access control list (ACL) rules for flows that must be exempted from remediation. If a flow is detected as an elephant flow and it matches the rules that are defined, that flow is exempted from the remediation action.

Before you begin

You must be running management center 7.4.0 or later and the managed threat defense must also be 7.4.0 or later.

Procedure

Step 1   Choose **Policies** > **Security policies** > **Access Control**.

Step 2   Click **Edit** (✎) next to the access control policy you want to edit.

Step 3   Choose **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 4   Click **Edit** (✎) next to **Elephant Flow Settings**.

Step 5   Ensure that you have configured the elephant flow detection and remediation parameters. See Configure Elephant Flow Parameters, on page 3.

Step 6   Click the **Add Rule** button next to **Remediation Exemption Rules**.

Elephant Flow Settings

ⓘ   For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
    For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass setting
    Elephant flow detection does not apply to encrypted traffic. **Learn more**

Elephant Flow Detection ⬤

Generate elephant flow events when flow bytes exceeds   `1024`   MB and flow duration exceeds   `10`   seconds

---

Elephant flow Remediation ⬤ ⓘ

If CPU utilization exceeds   `40`   % in fixed time windows of   `30`   seconds and packet drop exceeds   `5`   %

Then Bypass the flow ⬤

◯ All applications including unidentified applications

◉ Select Applications/Filters (1 selected)

And Throttle the remaining flows ⬤

Remediation Exemption Rules ⓘ   **Add Rule**

Serial Number	Source Networks	Destination Networks	Source Ports	Destination Ports

No Rules

Step 7   From the list of **Available Networks**, choose the configured host to exempt from elephant flow remediation. For the purposes of this example, we have created a host called "Host1_Exception."

Add Rule

Networks   Ports

🔍 Search by name or value

Available Networks	⟳ +
Host1_Exception	
Inside-Network	
internal	
IPv4-Benchmark-Tests	
IPv4-Link-Local	
IPv4-Multicast	
IPv4-Private-10.0.0.0-8	
IPv4-Private-172.16.0.0-12	
IPv4-Private-192.168.0.0-16	

Add to Source

Add to Destination

Source Networks: any

Enter an IP address   **Add**

Destination Networks: any

Enter an IP address   **Add**

Cancel   **Add**

Step 8   Click **Add to Source** or **Add to Destination** (as required) to add this host to the source or destination.

Step 9   Click the **Ports** tab.

Step 10   For the source port, choose **Protocol** as TCP and enter **80** as the destination port, and click **Add**.

Step 11 Click **OK**.

Elephant Flow Settings

For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass setting
Elephant flow detection does not apply to encrypted traffic. **Learn more**

Elephant Flow Detection

Generate elephant flow events when flow bytes exceeds [1024] **MB and flow duration exceeds** [10] **seconds**

Elephant flow Remediation

If CPU utilization exceeds [40] **% in fixed time windows of** [30] **seconds and packet drop exceeds** [5] **%**

Then Bypass the flow

◉ All applications including unidentified applications

○ Select Applications/Filters (0 selected)

Or Throttle the flow

Remediation Exemption Rules **Add Rule**

Serial Number	Source Networks	Destination Networks	Source Ports	Destination Ports	
1	Host1_Exception	Host1_Exception	Any	Any	

Step 12 Click **Save**.

What to do next

Deploy configuration changes. See Deploy Configuration Changes.

View Events for Elephant Flow Remediation Exemption

Procedure

Step 1   Choose **Events & Logs** > **+ Show more** > **Connection** > **Events**. You can also view the events from the **Unified Events** viewer.

Step 2   View the elephant flows that were exempted from remediation. The **Reason** field shows **Elephant Flow Exempted**.

		↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol
▾	☐	2022-12-19 11:23:58	2022-12-19 11:24:30	Allow	Elephant Flow Exempted	172.16.77.1		172.16.4.6		inside-zone56	outside-zone56	37780 / tcp	443 (https) / tcp	HTTP
▾	☐	2022-12-19 11:23:58		Allow		172.16.77.1		172.16.4.6		inside-zone56	outside-zone56	37780 / tcp	443 (https) / tcp	HTTP
▾	☐	2022-12-19 11:23:58		Allow	Elephant Flow Exempted	172.16.77.1		172.16.4.6		inside-zone56	outside-zone56	37780 / tcp	443 (https) / tcp	HTTP
▾	☐	2022-12-19 11:23:44	2022-12-19 11:23:50	Allow	Elephant Flow Exempted	172.16.77.1		172.16.4.5		inside-zone56	outside-zone56	50056 / tcp	80 (http) / tcp	HTTP
▾	☐	2022-12-19 11:23:44		Allow	Elephant Flow Exempted	172.16.77.1		172.16.4.5		inside-zone56	outside-zone56	50056 / tcp	80 (http) / tcp	HTTP

Additional References

For detailed conceptual information, see the Elephant Flow Detection for Snort 3 chapter in this guide or the content in the following link:

- Elephant Flow Detection