大象流检测

大象流非常大（以总字节数为单位），由 TCP（或其他协议）设置的连续流通过网络链路测量。默认情况下，大象流是速率大于每 10 秒 1GB 的流。它们可能会在 Snort 核心中造成性能威胁。大象流并不多，但它们可以在一段时间内占总带宽的不成比例。它们可能导致问题，例如CPU 占用、丢包等。

从 管理中心 7.2.0 开始（仅限 Snort 3 设备），您可以使用象流检测功能对象流进行监测和补救，这有助于减少系统压力并解决上述问题。

关于大象流检测和补救

您可以使用大象流检测功能来检测和补救大象流。可应用以下补救操作：

- **绕过大象流 (Bypass elephant flow)** - 您可以配置大象流以绕过 Snort 检测。如已配置，则 Snort 不会收到来自该流的任何数据包。
- **限制大象流 (Throttle elephant flow)** – 您可以对流应用速率限制并继续检查流。流速会以动态方式进行计算，流速会降低 10%。Snort 会将判定（流量减少 10% 的 QoS 流）发送到防火墙引擎。如果选择绕过所有应用，包括未识别的应用，您将无法为任何流配置限制操作（速率限制）。

注释 要使大象流检测正常工作，Snort 3 必须是检测引擎。

从智能应用绕行升级大象流

从 7.2.0 版开始，在 Snort 3 设备中已弃用智能应用绕行 (IAB)。

对于运行 7.2.0 或更高版本的设备，您必须在 AC 策略（高级设置选项卡）的**大象流设置 (Elephant Flow Settings)** 部分下配置象流设置。

在升级到 7.2.0（或更高版本）后，如果您使用的是 Snort 3 设备，则将从**大象流设置 (Elephant Flow Settings)** 部分而不是从**智能应用绕行设置 (Intelligent Application Bypass Settings)** 部分中挑选和部署大象流配置设置，这样，如果您没有迁移到大象流配置设置，那么您的设备在下次部署时将失去大象流配置。

下表显示了可应用于运行 Snort 3 或 Snort 2 引擎的版本 7.2.0 或更高版本以及版本 7.1.0 或更早版本的 IAB 或大象流配置。

管理中心	威胁防御	大象流或 IAB 配置
管理中心 7.0 或 7.1	Snort 2 设备	来自 IAB 的配置将适用。
	Snort 3 设备	来自 IAB 的配置将适用。
管理中心 7.2.0	Snort 2 设备	来自 IAB 的配置将适用。
	Snort 3 设备（7.1.0 及更早版本）	来自 IAB 的配置将适用。
	Snort 3 设备（7.2.0 及更高版本）	大象流中的配置将适用。

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.

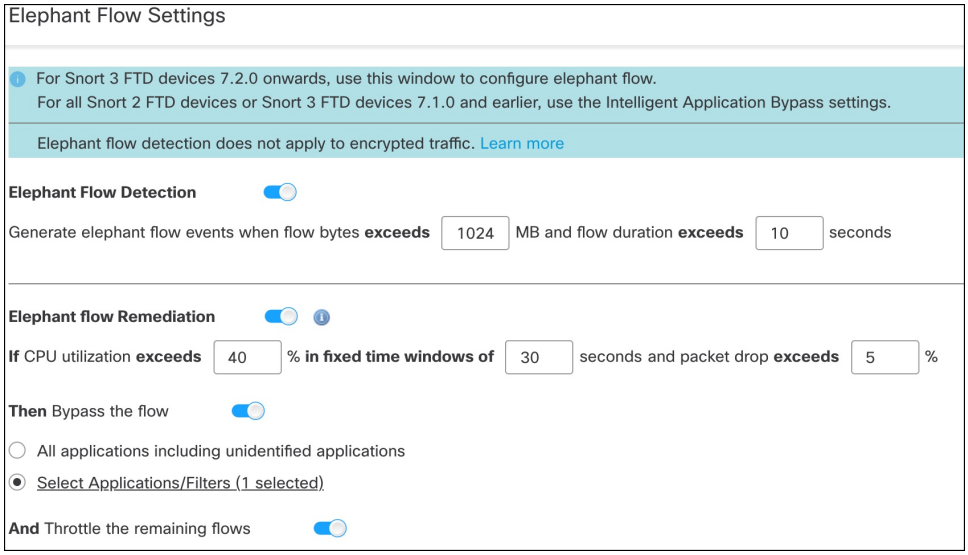
Attention Elephant flow detection is not applicable for prefiltered, trusted, or fast-forwarded flows, which do not process through Snort. As elephant flows are detected by Snort, elephant flow detection is not applicable for encrypted traffic.

Procedure

步骤 1 In the access control policy editor, click **Advanced**, then click **编辑**（ ） next to **Elephant Flow Settings**.

如果显示**视图**（ ），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

Figure 1: Configure Elephant Flow Detection



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

步骤 3 To remediate elephant flows, enable the **Elephant flow Remediation** toggle button.

步骤 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 %.

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

a. **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 配置应用条件和过滤器.

b. **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.

步骤 6 Click **OK** to save the elephant flow settings.

步骤 7 Click **Save** to save the policy.

What to do next

部署配置更改；请参阅 《Cisco Secure Firewall Management Center 管理指南》。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。