



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，第 1 页](#)
- [从智能应用绕行升级大象流，第 1 页](#)
- [配置大象流，第 2 页](#)

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。

配置大象流

您可以配置大象流以便对大象流执行操作，这有助于解决系统强制、高 CPU 使用率、丢包等问题。



注意 大象流检测不适用于不通过 Snort 处理的预过滤流、受信任流或快速转发流。由于大象流由 Snort 检测，因此大象流检测不适用于加密流量。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**，然后点击 **大象流设置** 旁边的 **编辑** (✎)。

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。

图 1: 配置大象流检测

步骤 2 默认情况下，大象流检测 (**Elephant Flow Detection**) 切换按钮处于启用状态。您可以配置流字节和流持续时间的值。当它们超过配置的值时，就会生成大象流事件。

步骤 3 要补救大象流，请启用 **大象流补救** 切换按钮。

步骤 4 要设置大象流补救标准，请配置 CPU 利用率 %、固定时间窗口的持续时间和丢包百分比的值。

步骤 5 当大象流补救符合配置的条件时，您可以对其执行以下操作：

1. **绕过流 (Bypass the flow)** - 启用此按钮可绕过所选应用或过滤器的 Snort 检查。选项包括：

- **包括未识别应用在内的所有应用 (All applications including unidentified applications)** - 选择此选项可绕过所有应用流量。如果配置此选项，则无法为任何流配置限制操作（速率限制）。
- **选择应用/过滤器 (Select Applications/Filters)** - 选择此选项可选择要绕过其流量的应用或过滤器；请参阅[配置应用条件和过滤器](#)。

2. **限制流 (Throttle the flow)** - 启用此按钮可对流应用速率限制并继续检查流。请注意，您可以选择应用或过滤器来绕过 Snort 检查，同时限制剩余流量。

注释 当系统摆脱压力时，即 Snort 数据包丢弃的百分比小于配置的阈值时，会自动从已限制的大象流中删除限制。因此，速率限制也会被删除。

您还可以使用以下威胁防御命令从已限制的流量中手动删除限制：

- **clear efd-throttle <5-tuple/all> bypass** - 此命令从已限制的大象流中删除限制并绕过 Snort 检查。
- **clear efd-throttle <5-tuple/all>** - 此命令从已限制的大象流中删除限制，Snort 检测将继续。使用此命令后，系统将跳过大象流补救。

有关这些命令的详细信息，请参阅《[Cisco Secure Firewall Threat Defense 命令参考](#)》。

注意 思科 Firepower 2100 系列设备不支持对大象流执行操作（绕过和限制流）。

步骤 6 点击**确定 (OK)** 以保存大象流设置。

步骤 7 点击**保存 (Save)** 保存策略。

下一步做什么

部署配置更改；请参阅[部署配置更改](#)。

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。