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 防火墙管理中心 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**部分而不是从**智能应用绕行设置**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。

防火墙管理中心	Firewall Threat Defense	大象流或 IAB 配置
防火墙管理中心 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。
防火墙管理中心 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。

配置大象流检测

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，从数据包流行末尾的 **更多** 下拉箭头中点击 **高级设置** 。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

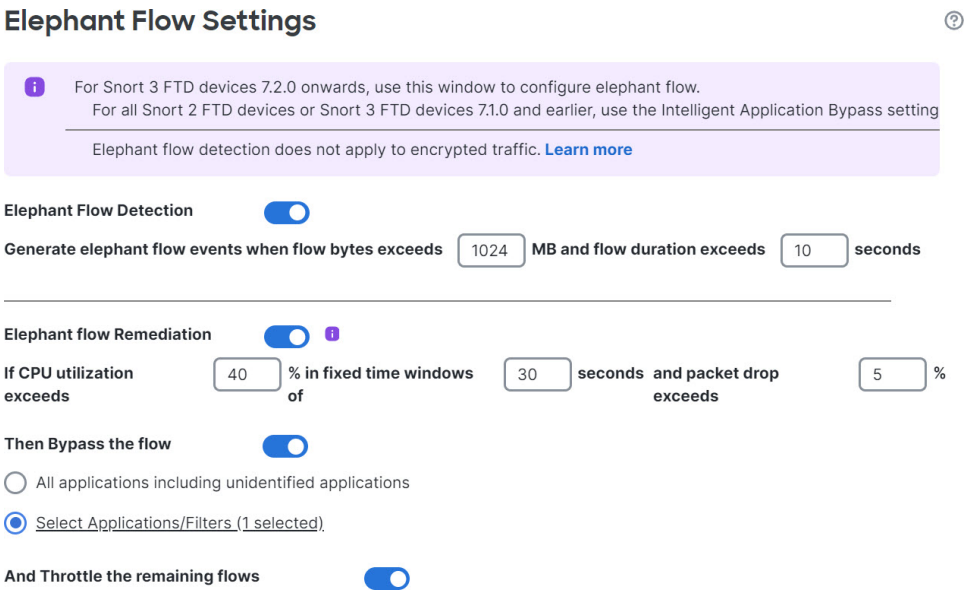


图 *2:* 配置大象流检测

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。

CPU利用率是根据流延迟计算的每个大象流。如果CPU使用率超出配置的阈值，并且也匹配其他配置（例如固定时间窗口和丢包），则会应用大象流补救操作。同样，丢包计算基于每个CPU丢弃的数据包。当丢包百分比超过特定CPU上的配置值后，系统将应用补救操作。例如，假设配置设置为默认值，即 CPU 使用率为 40%，固定时间窗口为 30 秒，丢包率为 5%。在特定 CPU 上，如果检测到的丢包数超过 5%，并且每个数据流的 CPU 使用率在 30 秒的固定时间范围内超过 40%，则会绕过或限制这些数据流。

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** - 选择此选项可选择要绕过其流量的应用或过滤器；请参阅《Cisco Secure Firewall Management Center 设备配置指南》的**访问控制规则**一章中的**配置应用条件和过滤器**主题。
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》。

步骤 6 在 **补救豁免规则** 部分，点击 **添加规则** 为必须豁免补救的流配置 L4 访问控制列表 (ACL) 规则。

步骤 7 在 **添加规则** 窗口中，使用 **网络** 选项卡添加网络详细信息，即源网络和目的网络。使用 **端口** 选项卡添加源端口和目的端口。

如果检测到象流并且它与定义的规则相匹配，则会在 **连接事件**的 **原因** 列标题中生成一个事件，其原因为 **象流豁免** 。

步骤 8 在 **补救豁免规则** 部分，可以查看免于执行补救操作的流。

步骤 9 点击**确定** 以保存大象流设置。

步骤 10 点击**保存**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。

配置大流设置后，监控连接事件以查看是否检测到、绕过或限制了任何流。您可以在连接事件的 **原因** 字段中查看此信息。出现大象流连接的三个原因是：

- 大象流
- 受限制的大象流
- 受信任的大象流

注意 仅启用大象流检测不会导致为大象流生成连接事件。如果由于其他原因已记录连接事件，并且流也是大象流，则 **原因** 字段包含此信息。但是，要确保记录所有大象流，必须在适用的访问控制规则中启用连接日志记录。

有关详细信息，请参阅 Cisco Secure Firewall 大象流检测 。

大象流检测示例

关于大象流

大象流非常大（以总字节数为单位），由 TCP（或其他协议）设置的相对长运行的网络连接通过网络链路测量。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或问题。大象流很重要，因为它们可能会消耗过多的CPU资源，并影响检测资源的其他竞争流，并导致延迟增加或丢包等问题。

关于大象流检测和补救的优势

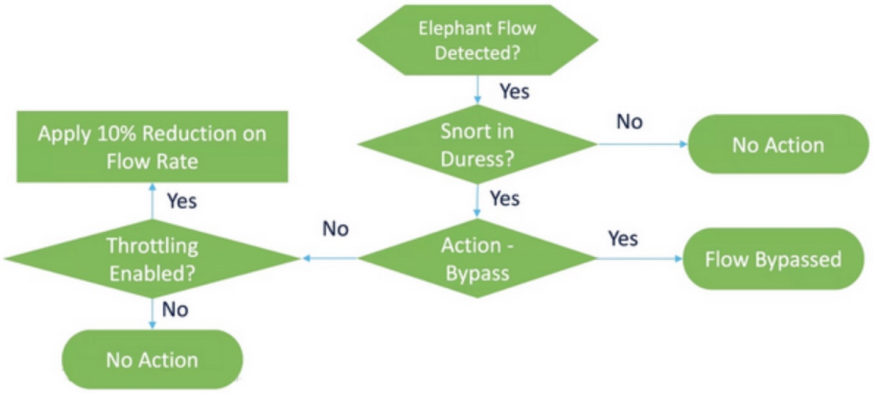
- 大象流配置允许自定义和绕过甚至限制大象流的选项。
- 您可以选择绕过或限制基于所选应用的流量，以提供可疑流量的Snort检查，同时绕过更受信任的流量。
- 大象流补救有助于根据您的特定要求确定优先级并为内部应用释放更多带宽。

大象流工作流程

当根据配置的参数检测到大量流时，您可以选择绕过或限制该流。当流量被绕过时，允许流量通过而不进行 Snort 检查。限制表示流量吞吐量降低。以 10% 的增量降低流量，直到 CPU 使用率降至配置的阈值以下。在识别大流并满足额外的CPU和时间窗口参数后，会发生绕行或限制。在识别大流之前，入侵策略会处理流，假设您已在“允许”规则中配置此流。这意味着不允许大量流在完全未经检查的情况下通过系统，因为大多数攻击都是在连接中很早就被检测到的。

要了解如何处理流，请参阅以下流程图。

图 *3:* 大象流工作流程



除非系统检测到Snort强制条件（性能问题），否则不会执行任何操作。系统不会仅仅因为流量大而限制或绕过流量。此外，限制和旁路的操作是相互排斥的。这意味着您可以绕过或限制流，但不能同时绕过或限制流。

如果您不想绕过导致威胁的所有大流，可以将绕过选项限制为仅适用于特定应用。您可以优先考虑您信任的应用的连接，而不会限制性能。您可以配置必须绕过的应用，但剩余流量（导致威胁）将受到限制。这可确保其他不受信任的应用流仍会收到完整的 Snort 检测，尽管其带宽已减少。

示例业务情景

在数据中心中，会发生多项活动，例如集群之间的数据复制、虚拟机集成和数据库备份。组织中的用户可能正在OTT上观看或下载视频。此类活动的带宽利用率可能会导致大量流量，降低网络速度并影响重要任务的性能。作为网络管理员（根据您的特定要求），您希望了解导致带宽问题的大型数据流并进行补救。

例如，让我们看看如何配置大流参数来绕过WebEx流量（您的组织用于实时视频会议）并限制其余应用或连接，包括视频、电影等。

前提条件

- 确保您运行的是管理中心 7.2.0 或更高版本，并且托管威胁防御也是 7.2.0 或更高版本。
- 仅启用大象流检测不会生成其他连接事件。大象流检测将大象流表示法添加到已记录到管理中心的匹配连接。**要记录这些事件，必须在访问控制策略中启用连接日志记录**。您可以对特定规则执行此操作，也可以添加记录所有连接（包括大流）的监控规则。

配置大象流参数

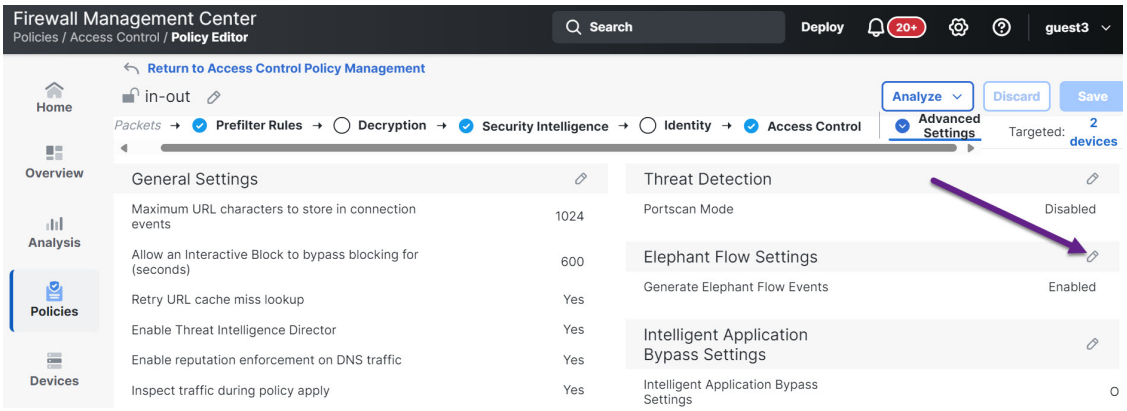
过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎)。

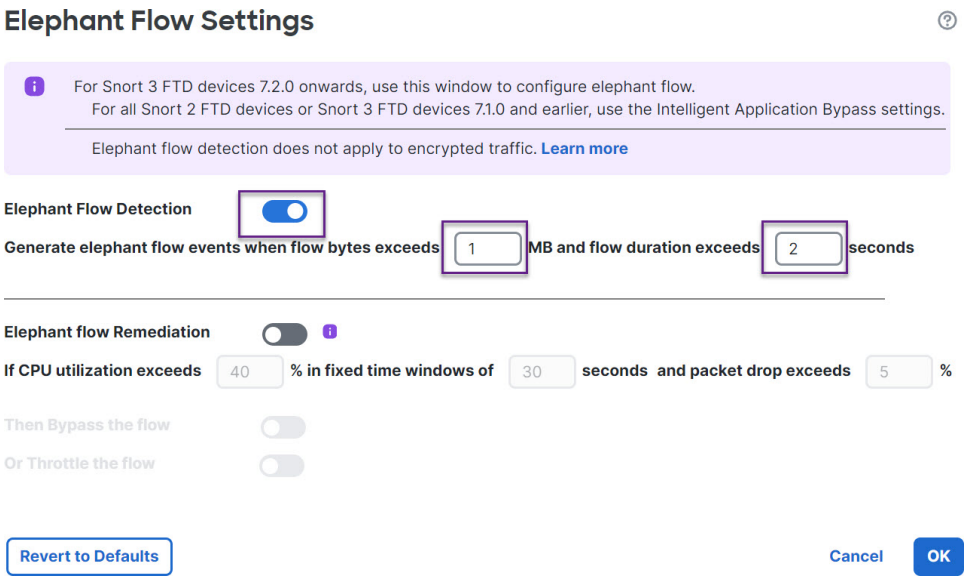
步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 4 点击**大象流设置 (Elephant Flow Settings)** 旁边的 **编辑** (✎)。



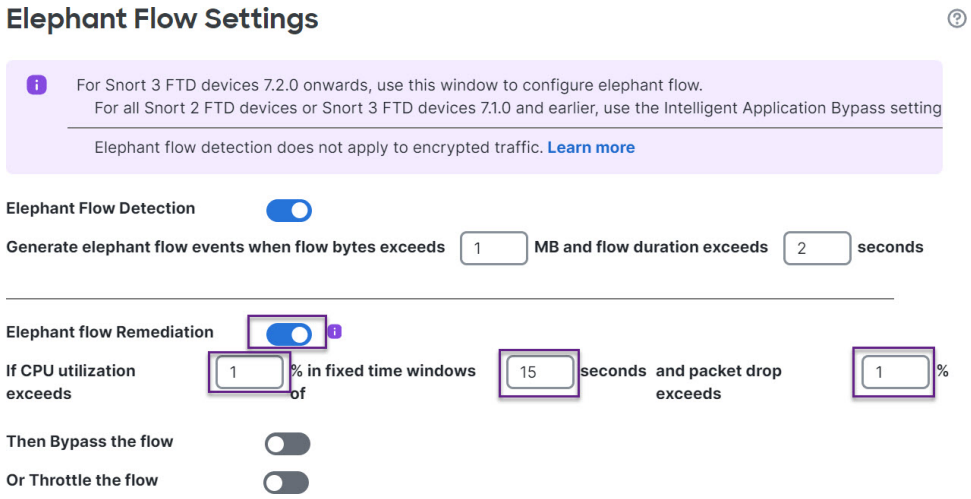
步骤 5 默认情况下，**大象流检测 (Elephant Flow Detection)** 切换按钮处于启用状态。默认设置仅启用检测，不配置默认操作。检测设置允许您调整流字节和持续时间，以便可以识别系统中的大象流。

作为测试设置，配置流字节和持续时间参数，如下图所示。

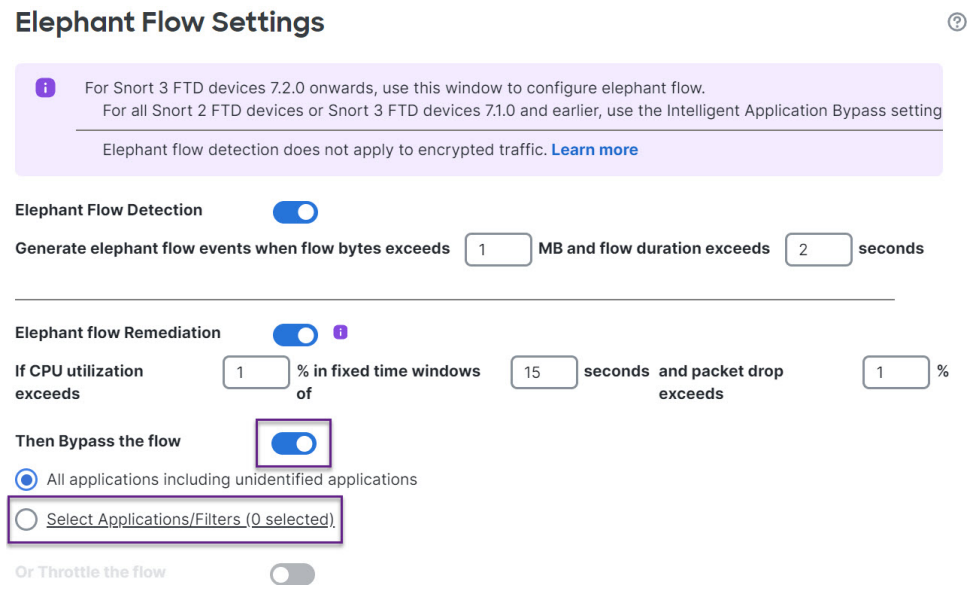


步骤 6 启用**大象流补救**切换按钮。当检测到大象流时，您可以选择绕过或限制该流。绕过流意味着允许流量通过而无需 Snort 检查。限制表示流量吞吐量降低。此速率降低以 10% 为增量，直到 CPU 使用率降至低于配置的阈值。

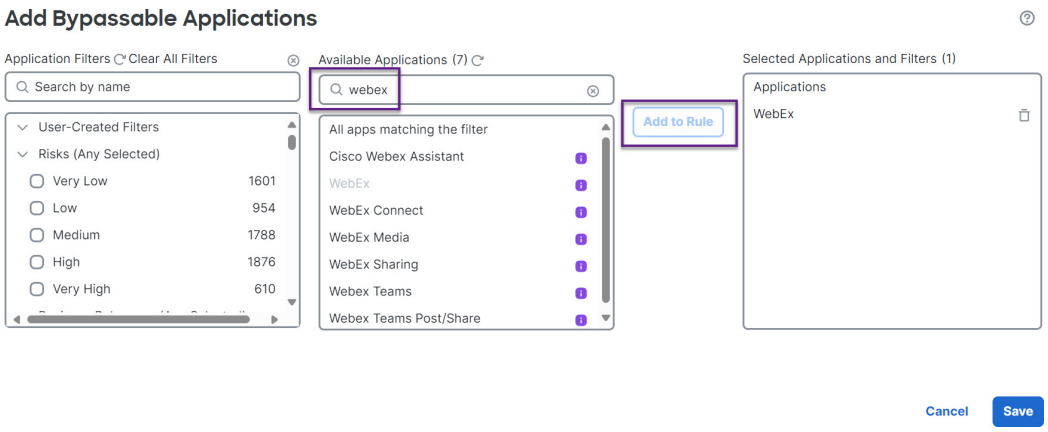
作为测试设置，配置大象流补救参数，如下图所示。



步骤 7 启用 **绕过流** 切换按钮，然后点击 **选择应用/过滤器** 单选按钮。



步骤 8 在 **应用过滤器** 下，搜索并选择 **WebEx** 应用，将其添加到规则中，然后点击 **保存**。这意味着 WebEx 连接是受信任的和优先的，如果这些 WebEx 连接被检测为大象流，则将根据配置的参数跳过 Snort 检查。



步骤 9 启用 **限制** 切换按钮以限制剩余流量（导致强制）。这可确保所有其他流量以 10% 的增量减慢，直到满足 Snort 强制条件。

步骤 10 点击**确定 (OK)**。

步骤 11 点击**保存 (Save)**。

下一步做什么

部署配置更改。请参阅部署配置更改。

查看大象流的事件

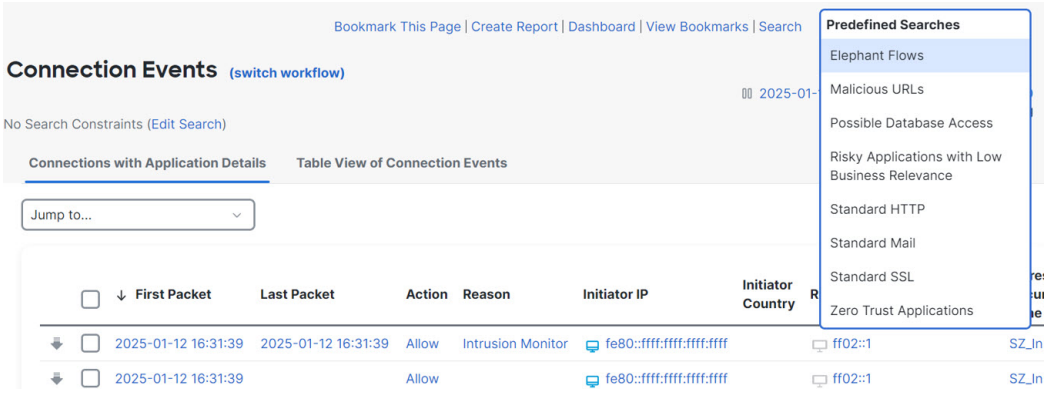
配置大流设置后，监控连接事件以查看是否检测到、绕过或限制了任何流。您可以在连接事件的 **原因** 字段中查看此信息。大象流连接的三种类型为：

- 大象流
- 受限制的大象流
- 受信任的大象流

过程

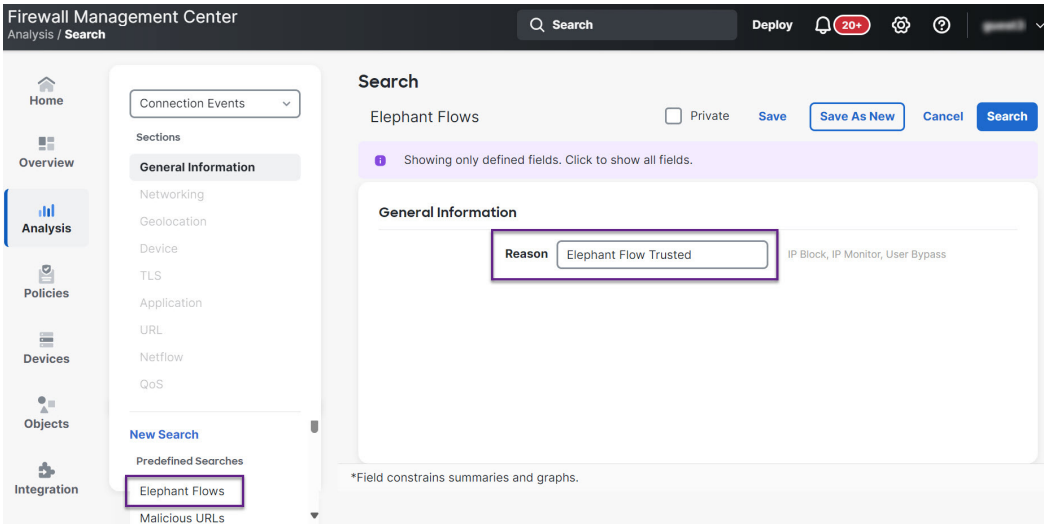
步骤 1 选择**事件和日志** > **+ 显示更多** > **连接** > **事件**。您还可以在 **统一事件** 查看器中查看事件。

步骤 2 在 **连接事件** 页面中，从 **预定义搜索** 下拉列表中选择 **大象流** 以显示象形流事件。

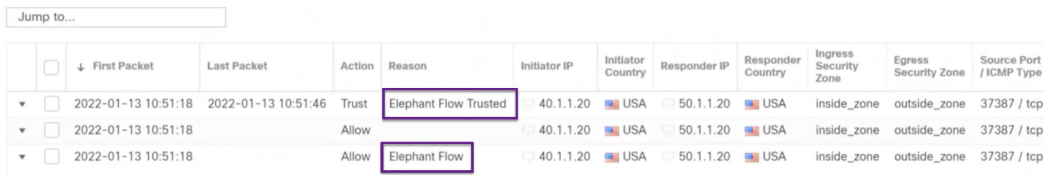


提示

要查看 **受信任的大象流** 或 **受限制的大象流** 事件类型，请点击页面左上角的 **编辑搜索** 链接，然后在 **原因** 字段中，选择左侧面板中的 **大象流** 。根据要搜索的内容，输入 **受信任的大象流** 或 **受限制的大象流**。



步骤 3 查看在流中检测到的大象流，并且 **原因** 字段显示 **大象流**。在流结束时，它被绕过，并且 **原因** 字段显示 **受信任的大象流**。



配置大象流补救豁免

您可以为必须豁免补救的流配置 L4 访问控制列表 (ACL) 规则。如果检测到大型流，并且该流与为必须豁免补救操作的流定义的规则匹配。

开始之前

您必须运行管理中心 7.4.0 或更高版本，并且托管威胁防御也必须是 7.4.0 或更高版本。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

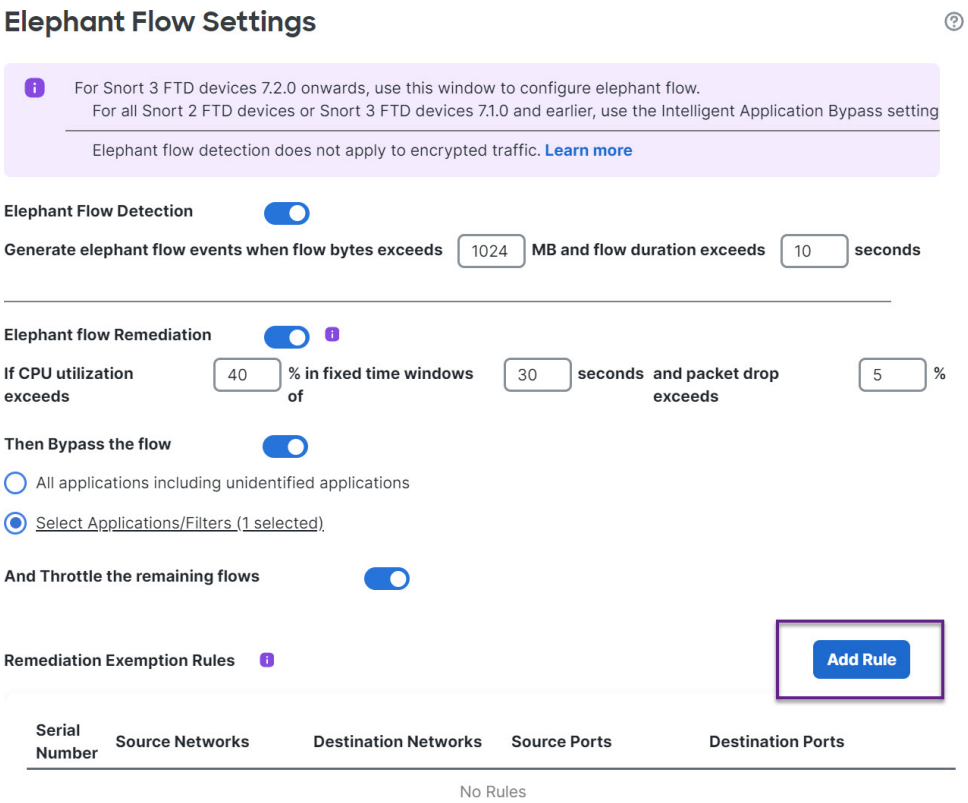
步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

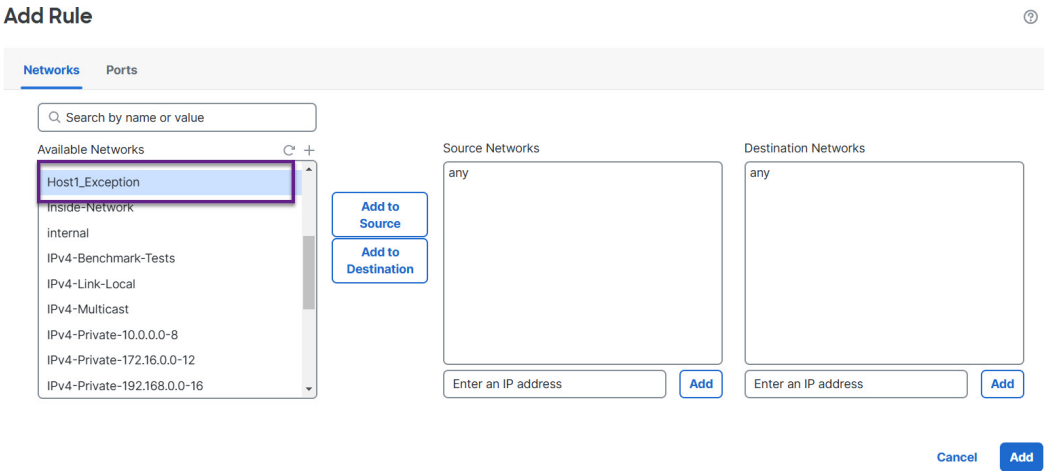
步骤 4 点击**大象流设置 (Elephant Flow Settings)** 旁边的 **编辑** (✎)。

步骤 5 确保您已配置大象流检测和补救参数。请参阅配置大象流参数，第 6 页。

步骤 6 点击 **补救豁免规则**旁边的 **添加规则** 按钮。



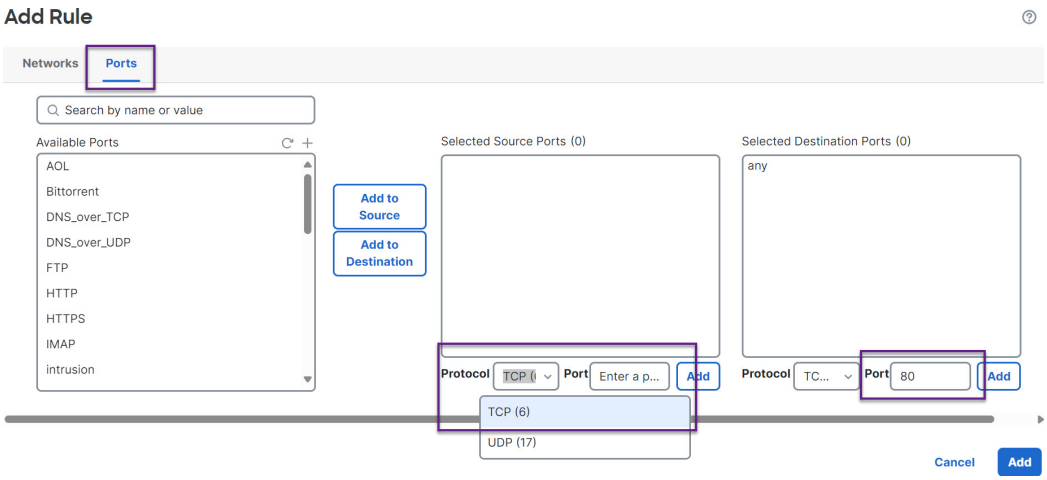
步骤 7 从 **可用网络**列表中，选择要免于执行大象流补救的已配置主机。在本示例中，我们创建了一个名为“Host1_Exception”的主机。



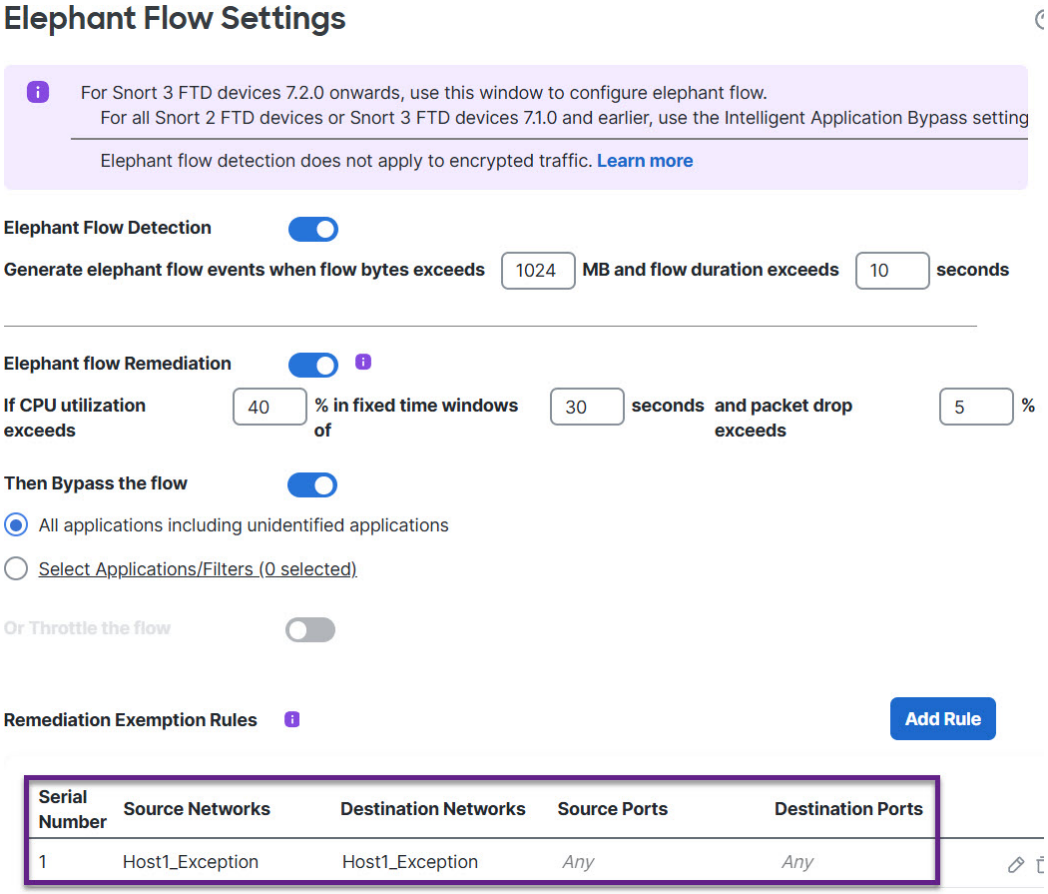
步骤 8 点击 **添加到源** 或 **添加到目标** （根据需要），将此主机添加到源或目标。

步骤 9 点击**端口**选项卡。

步骤 10 对于源端口，选择 **协议** 作为 TCP 并输入 **80** 作为目的端口，然后点击 **添加**。



步骤 11 点击**确定 (OK)**。



步骤 12 点击保存 **(Save)**。

下一步做什么

部署配置更改。请参阅部署配置更改。

查看大象流补救豁免事件

过程

步骤 1 选择事件和日志 > + 显示更多 > 连接 > 事件。您还可以在 统一事件 查看器中查看事件。

步骤 2 查看免于补救的大象流。 理由 字段显示 免于补救的大象流。


Jump to...

	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

其他参考资料

有关详细的概念信息，请参阅本指南中的“Snort 3 大象流检测”一章或以下链接中的内容：

- 大象流检测

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。

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。

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。