# 使用案例 - 配置大象流检测结果



## 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。

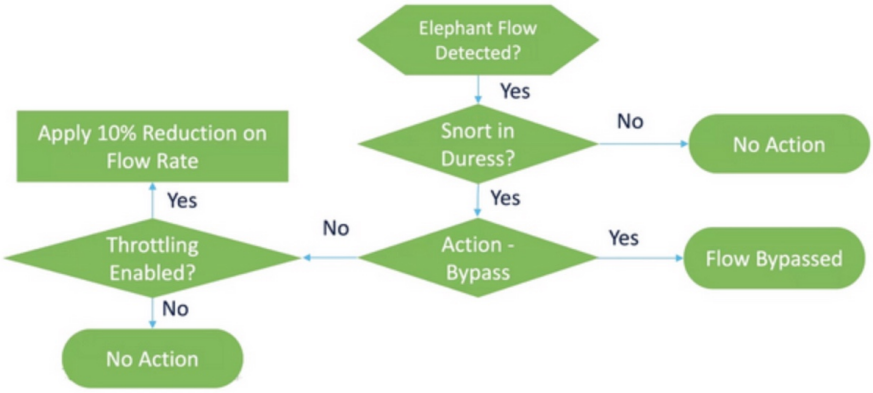
## 大象流工作流程

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 *1:* 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

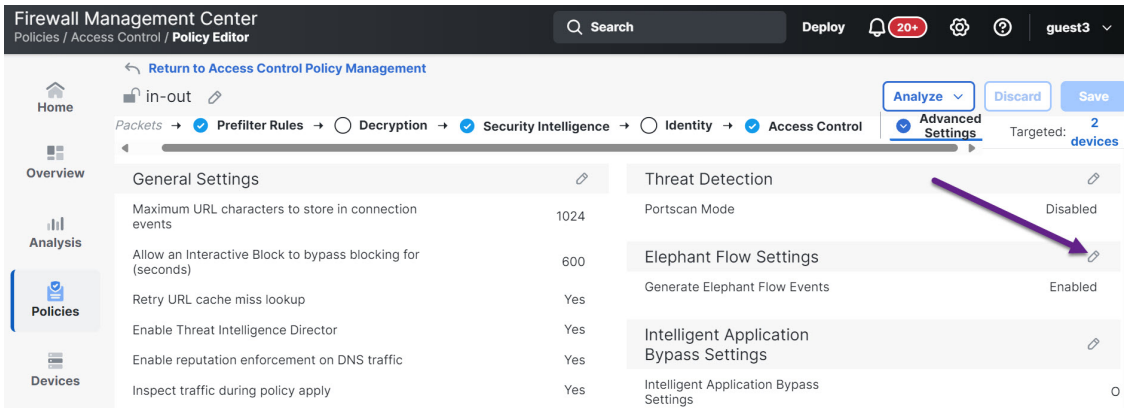
过程

**步骤 1** 依次选择**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** (✎)。

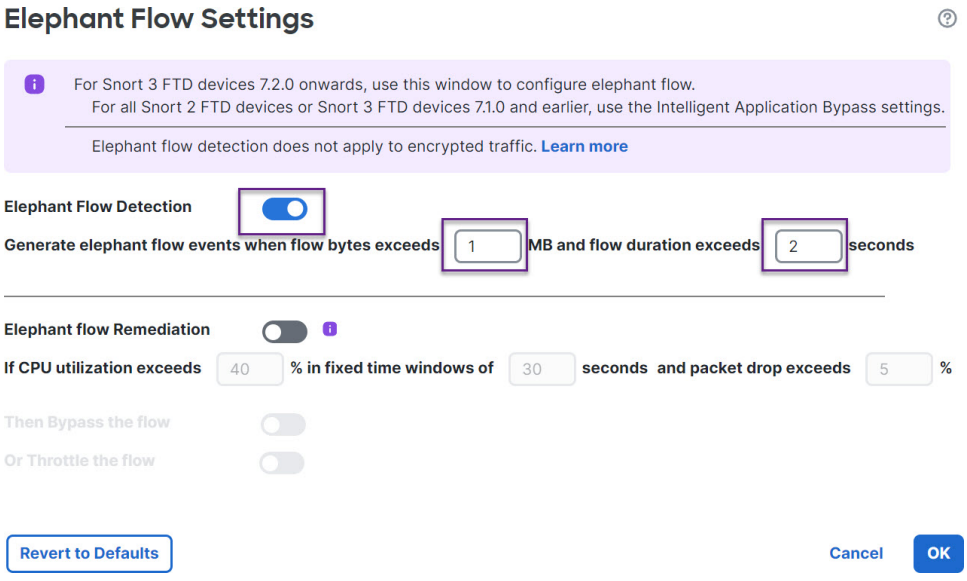
**步骤 3** 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

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



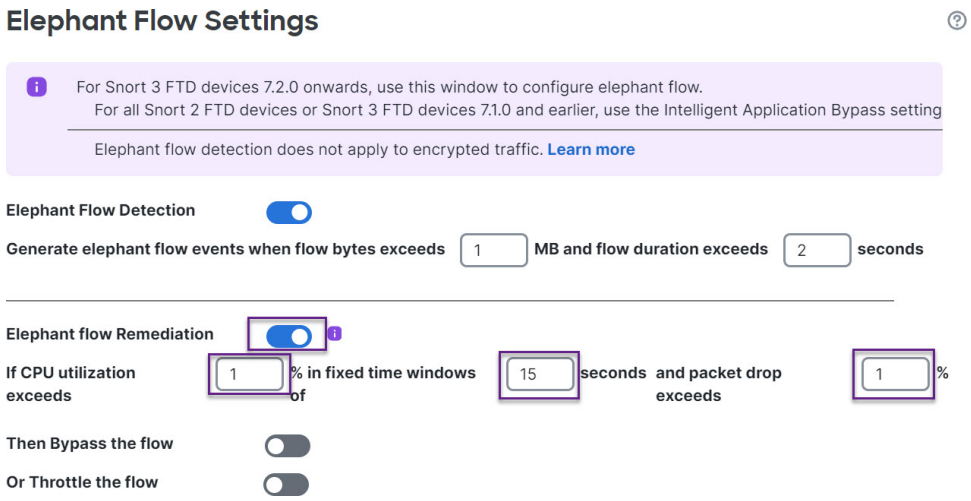

**步骤 5** 默认情况下，**大象流检测 (Elephant Flow Detection)** 切换按钮处于启用状态。默认设置仅启用检测，不配置默认操作。检测设置允许您调整流字节和持续时间，以便可以识别系统中的大象流。

作为测试设置，配置流字节和持续时间参数，如下图所示。

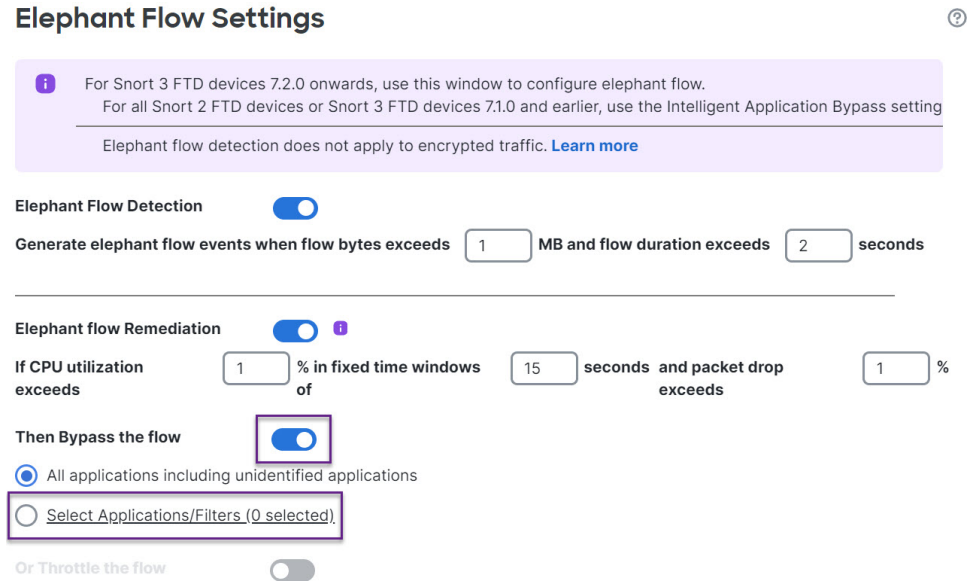


**步骤 6** 启用 **大象流补救** 切换按钮。当检测到大象流时，您可以选择绕过或限制该流。绕过流意味着允许流量通过而无需 Snort 检查。限制表示流量吞吐量降低。此速率降低以 10% 为增量，直到 CPU 使用率降至低于配置的阈值。

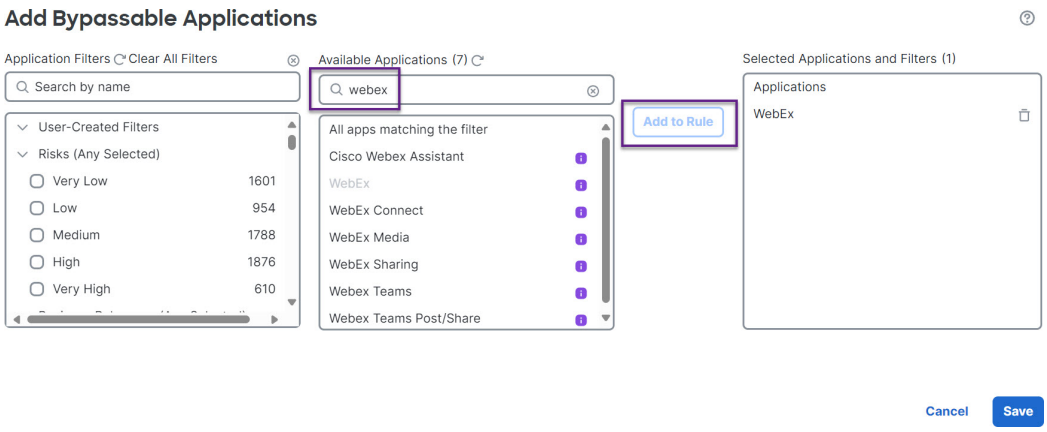
作为测试设置，配置大象流补救参数，如下图所示。




**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**。

**步骤 11** 点击**保存**。

### 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

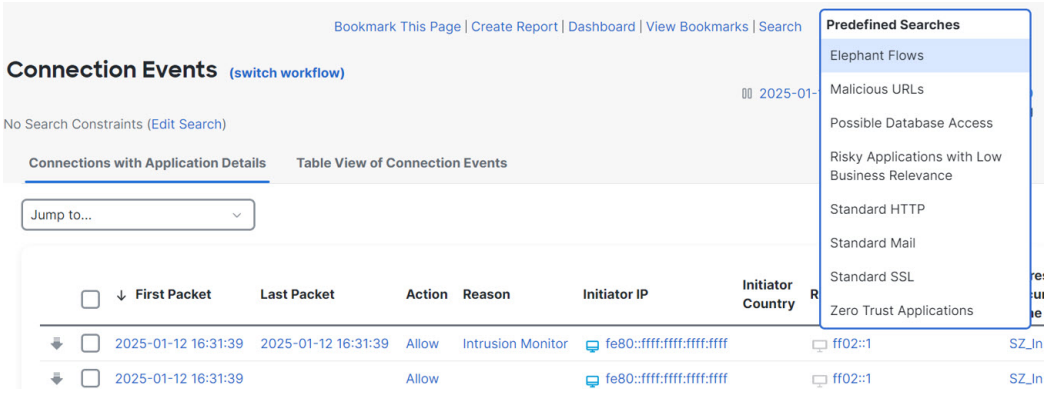
配置大流设置后，监控连接事件以查看是否检测到、绕过或限制了任何流。您可以在连接事件的 **原因** 字段中查看此信息。大象流连接的三种类型为：

- 大象流
- 受限制的大象流
- 受信任的大象流

### 过程

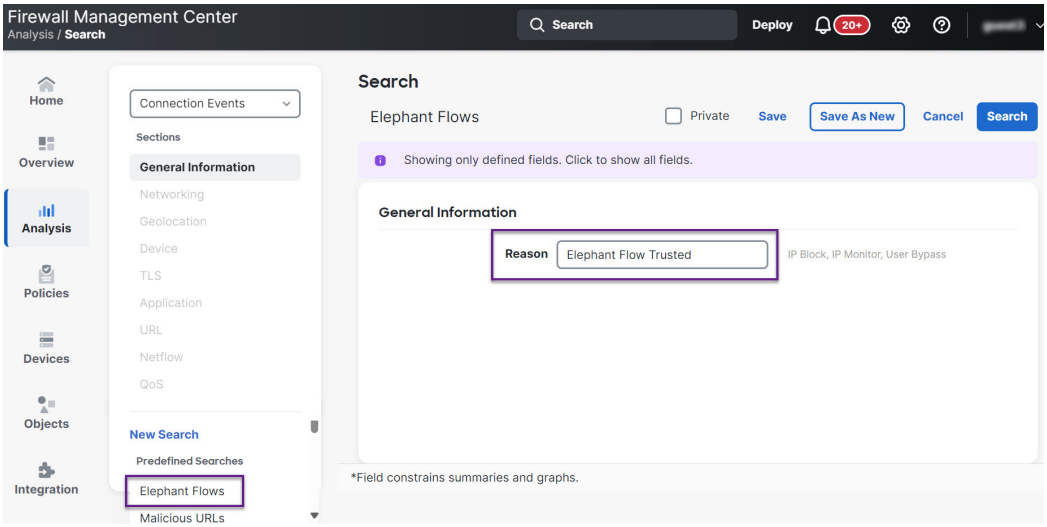
**步骤 1** 选择**分析** > **连接** > **事件**。您还可以在 **统一事件** 查看器中查看事件。

**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。

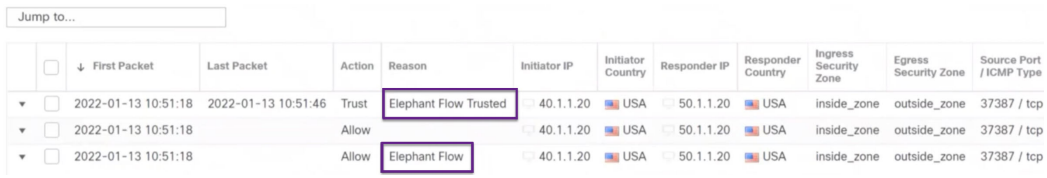



**提示**

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** 依次选择**策略** > **访问控制**。

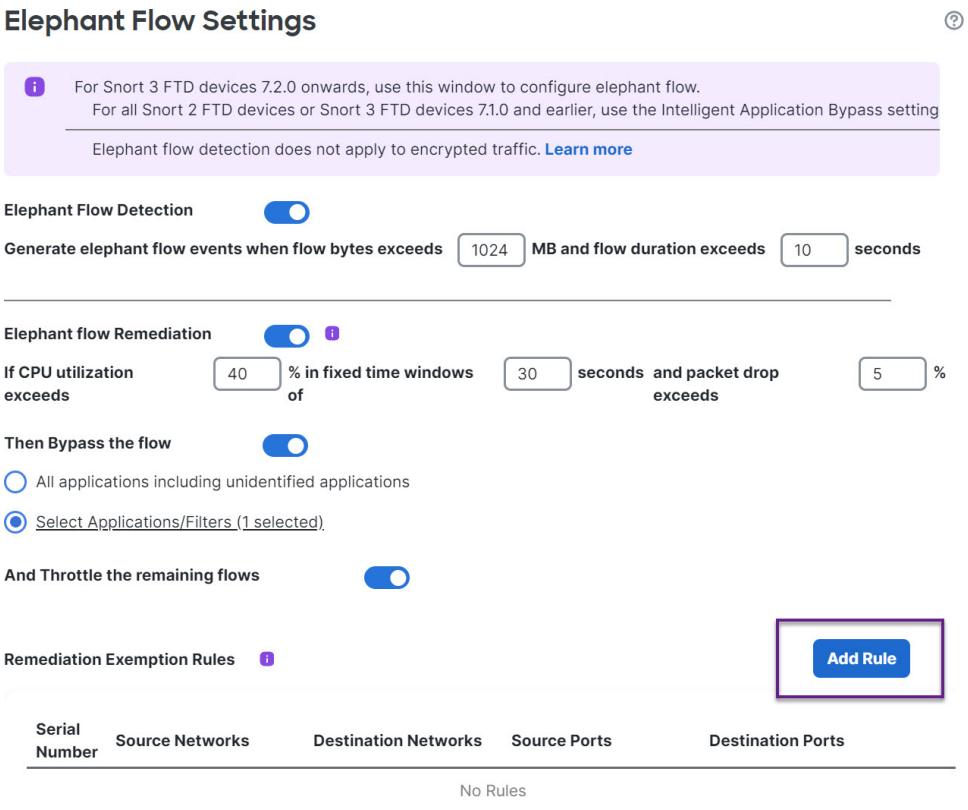
**步骤 2** 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

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

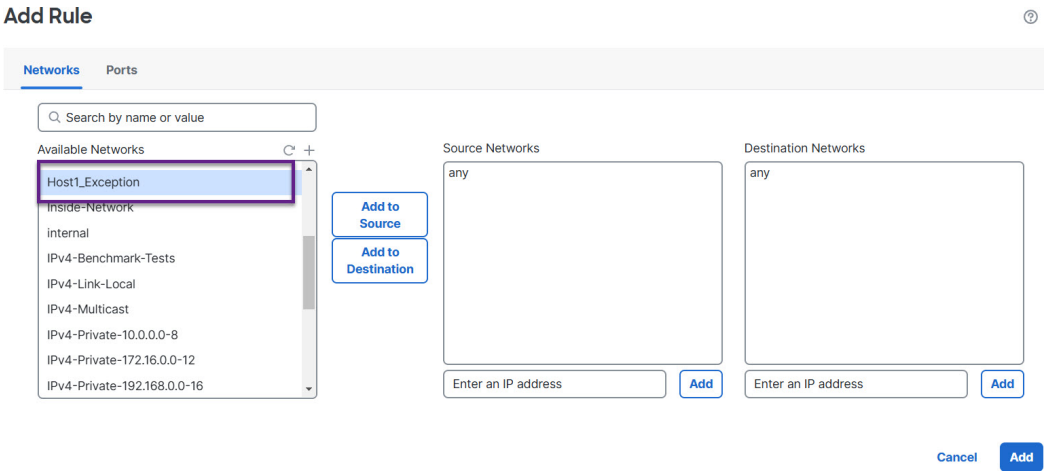
**步骤 4** 点击**大象流设置 (Elephant Flow Settings)** 旁边的 **编辑** (✎)。

**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 3 页。

**步骤 6** 点击 **补救豁免规则**旁边的 **添加规则** 按钮。



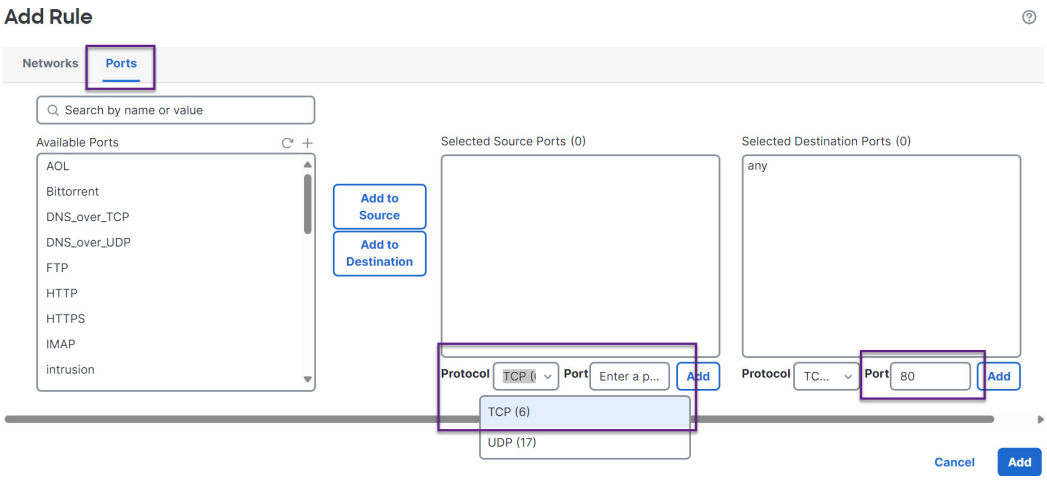

**步骤 7** 从 **可用网络**列表中，选择要免于执行大象流补救的已配置主机。在本示例中，我们创建了一个名为“Host1_Exception”的主机。



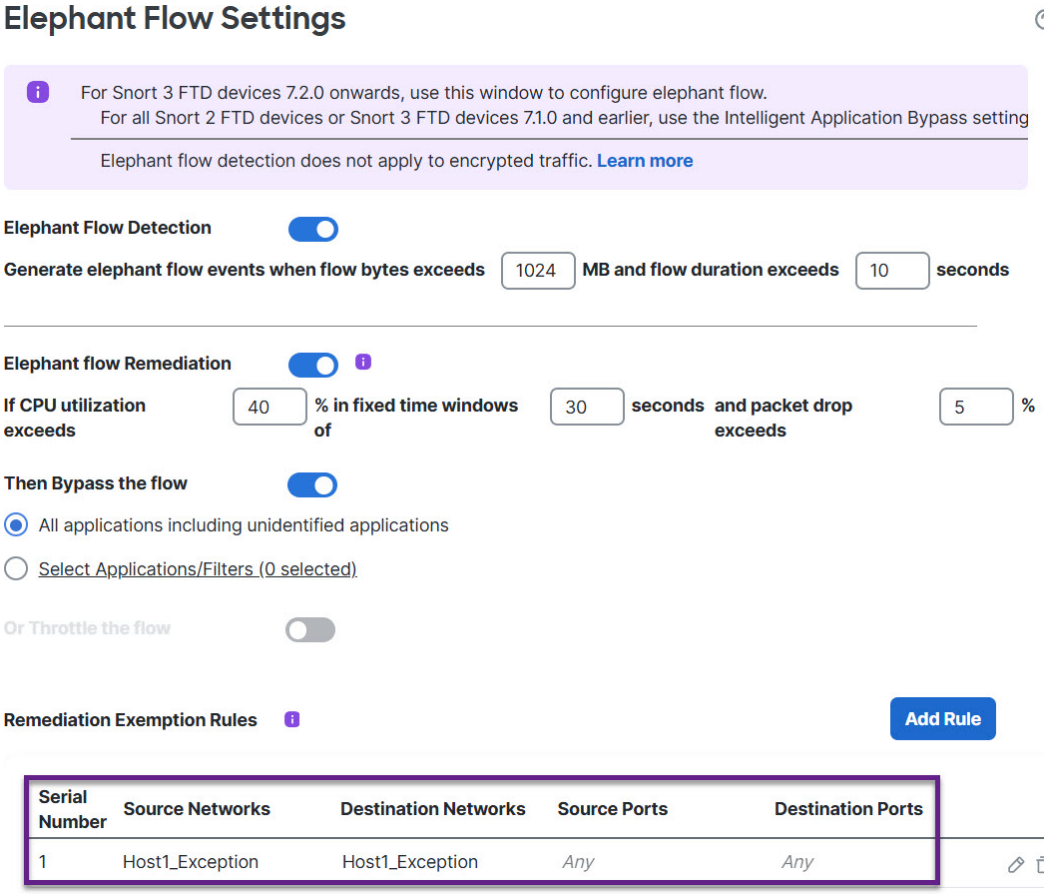

**步骤 8** 点击 **添加到源** 或 **添加到目标** （根据需要），将此主机添加到源或目标。

**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**。




步骤 12 点击保存。

### 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 选择分析 > 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。