在内容安全设备上配置数据包捕获

目录

简介

本文档介绍思科安全网络设备(SWA)、邮件安全设备(ESA)和安全管理设备(SMA)上的数据包捕获。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科内容安全设备管理。

Cisco 建议您：

- 已安装物理或虚拟SWA/ESA/SMA。
- 对SWA/ESA/SMA图形用户界面(GUI)的管理访问。
- 对SWA/ESA/SMA命令行界面(CLI)的管理访问

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

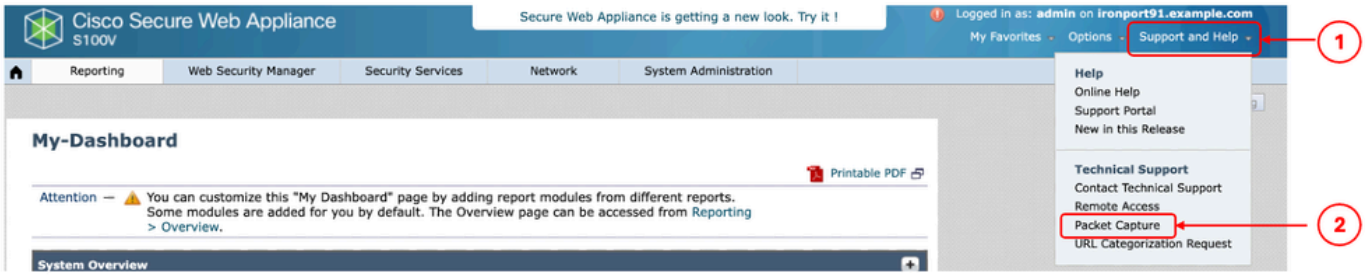
从GUI执行数据包捕获

要从GUI执行数据包捕获，请执行以下步骤：

步骤1:登录到GUI。

第二步：从页面右上方选择Support and Help。

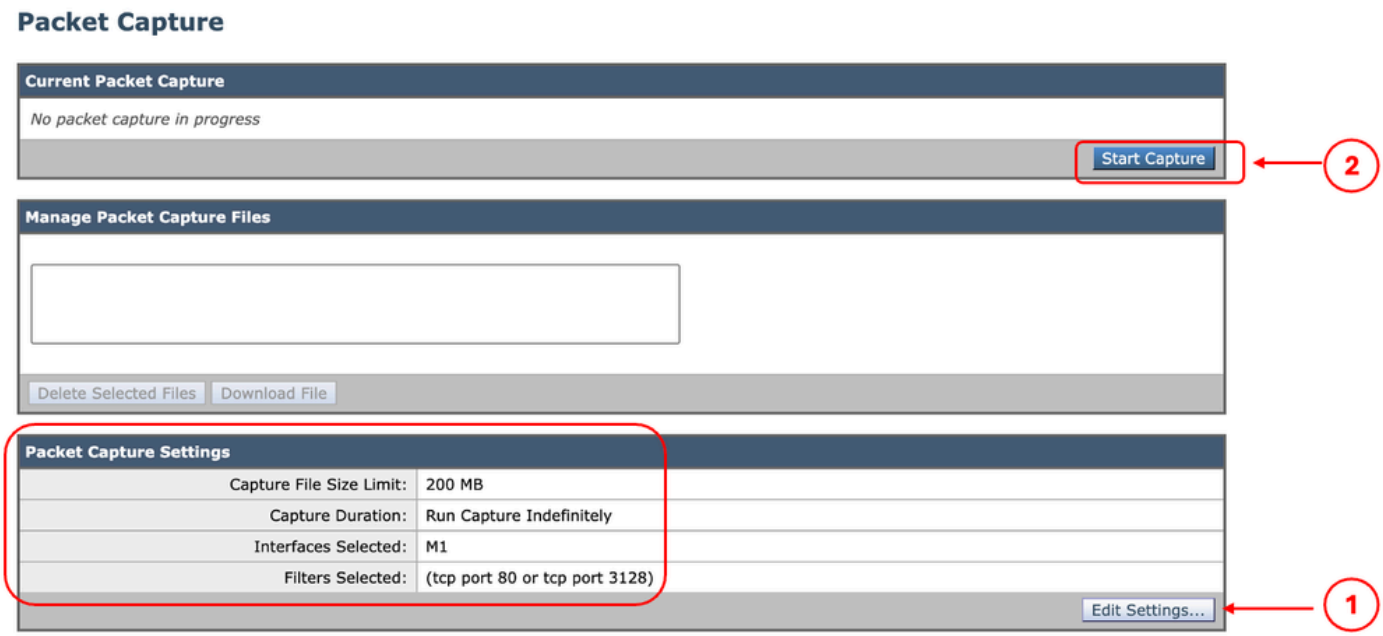
第三步：选择Packet Capture。

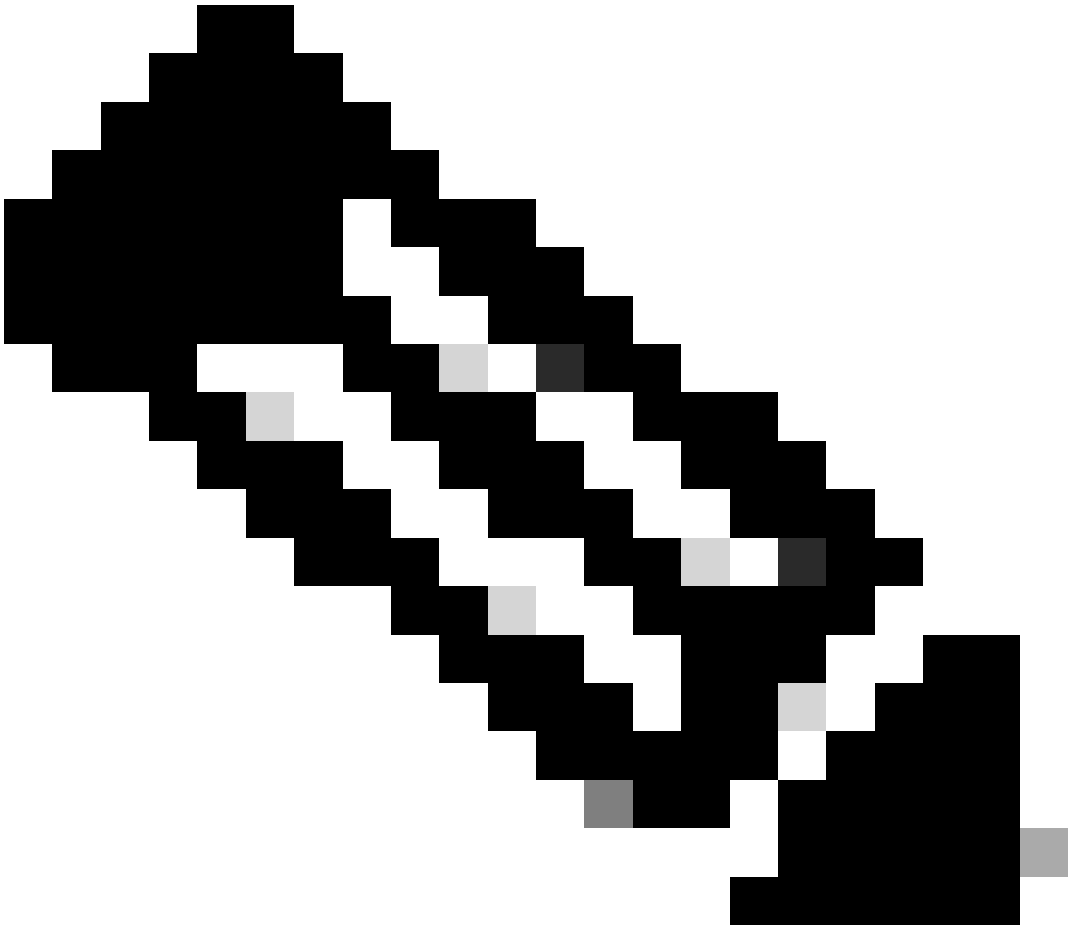


图像-数据包捕获

第4步（可选）要编辑当前过滤器，请选择Edit Settings。（有关过滤器的详细信息，请检查本文档中的过滤器部分）

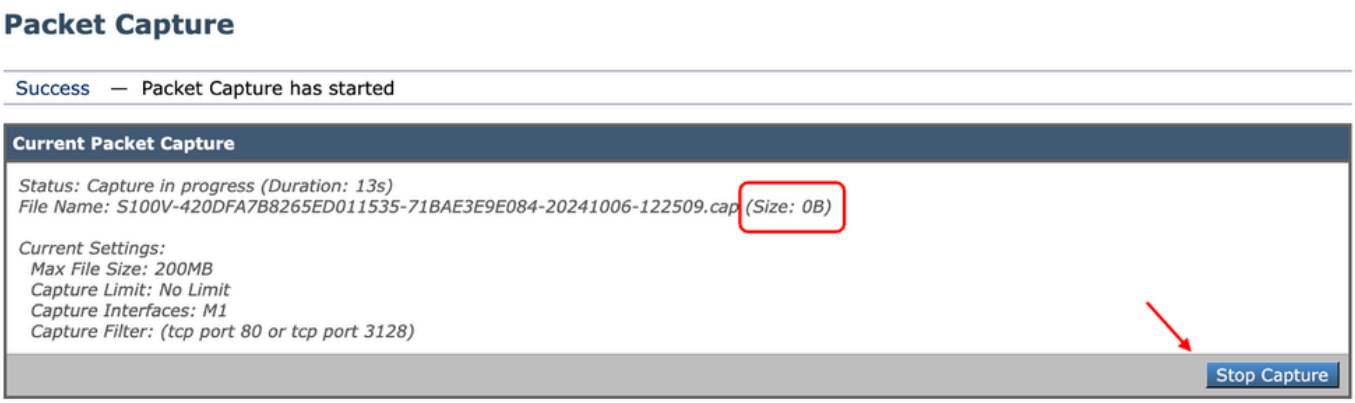
第五步：开始捕获。





注意：数据包捕获文件大小限制为200MB。当文件大小达到200MB时，数据包捕获停止。

Current Packet Capture（当前数据包捕获）部分显示数据包捕获状态，包括文件大小和应用过滤器。



映像-数据包捕获状态

第六步：要停止运行的数据包捕获，请点击Stop Capture。

步骤 7.要下载数据包捕获文件，请从Manage Packet Capture Files列表中选择文件，然后单击Download File。

映像-下载数据包捕获

提示：最新文件位于列表顶部。

第8步（可选）要删除任何数据包捕获文件，请从Manage Packet Capture Files列表中选择文件，然后点击Delete Selected Files。

从CLI执行数据包捕获

您还可以从CLI使用以下步骤开始数据包捕获：

步骤1:登录到CLI。

第二步：键入packetcapture 并按Enter。

第3步（可选）要编辑当前过滤器类型SETUP。（有关过滤器的详细信息，请检查本文档中的过滤器部分。）

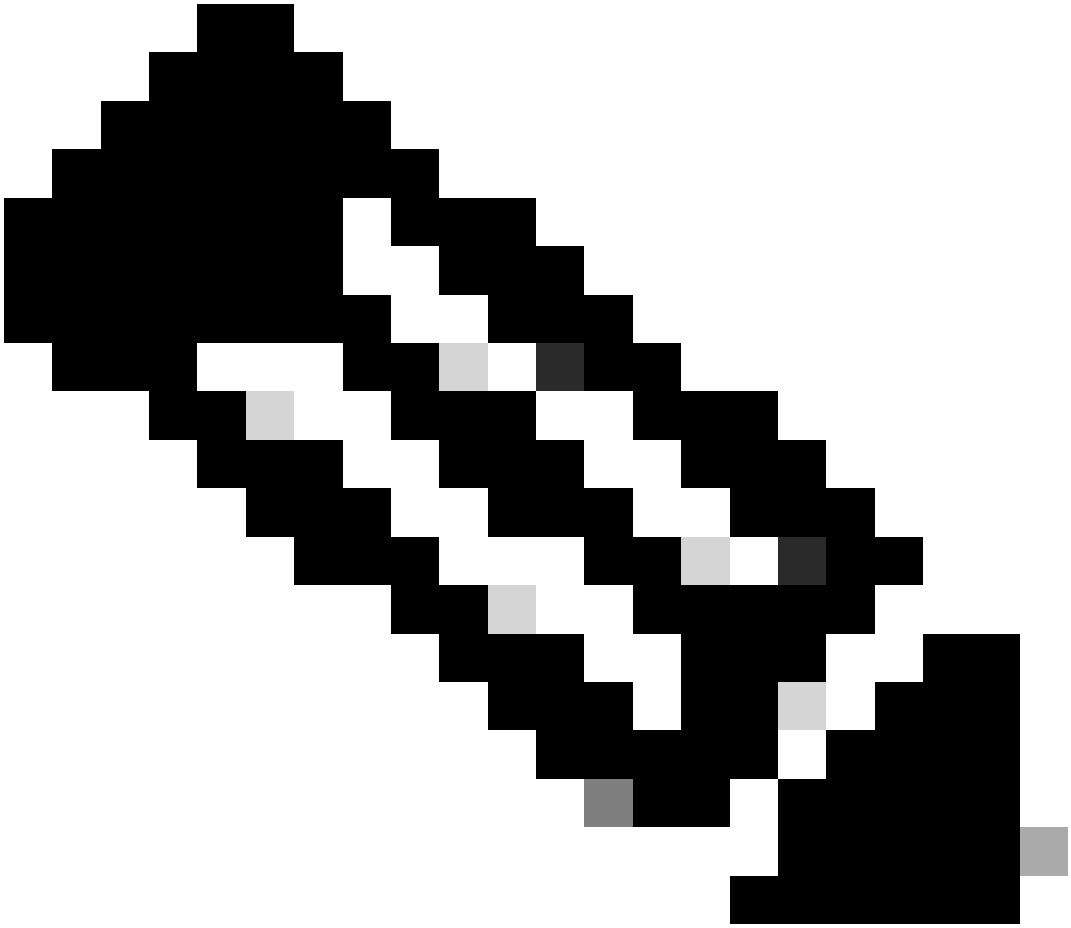
第四步： 选择START开始捕获。

```
SWA_CLI> packetcapture
Status: No capture running

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     (tcp port 80 or tcp port 3128)

Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
```

第5步（可选）您可以通过选择STATUS查看数据包捕获的状态：

```
Choose the operation you want to perform:
- STOP - Stop packet capture.
- STATUS - Display current capture status.
- SETUP - Change packet capture settings.
[]> STATUS

Status: Capture in progress
File Name: S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-130426.cap
File Size: 0K
Duration:  45s

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     (tcp port 80 or tcp port 3128)
```

第六步：要停止数据包捕获，请键入STOP并按Enter：



注意：要下载从CLI收集的数据包捕获文件，可以从GUI下载这些文件或通过文件传输协议(FTP)连接到设备，然后从Captures文件夹下载这些文件。

过滤器

以下是有关可在内容安全设备中使用的过滤器的一些指南。

按主机IP地址过滤

在GUI中按主机IP过滤

要按主机IP地址过滤，从GUI中有两个选项：

- 预定义过滤器

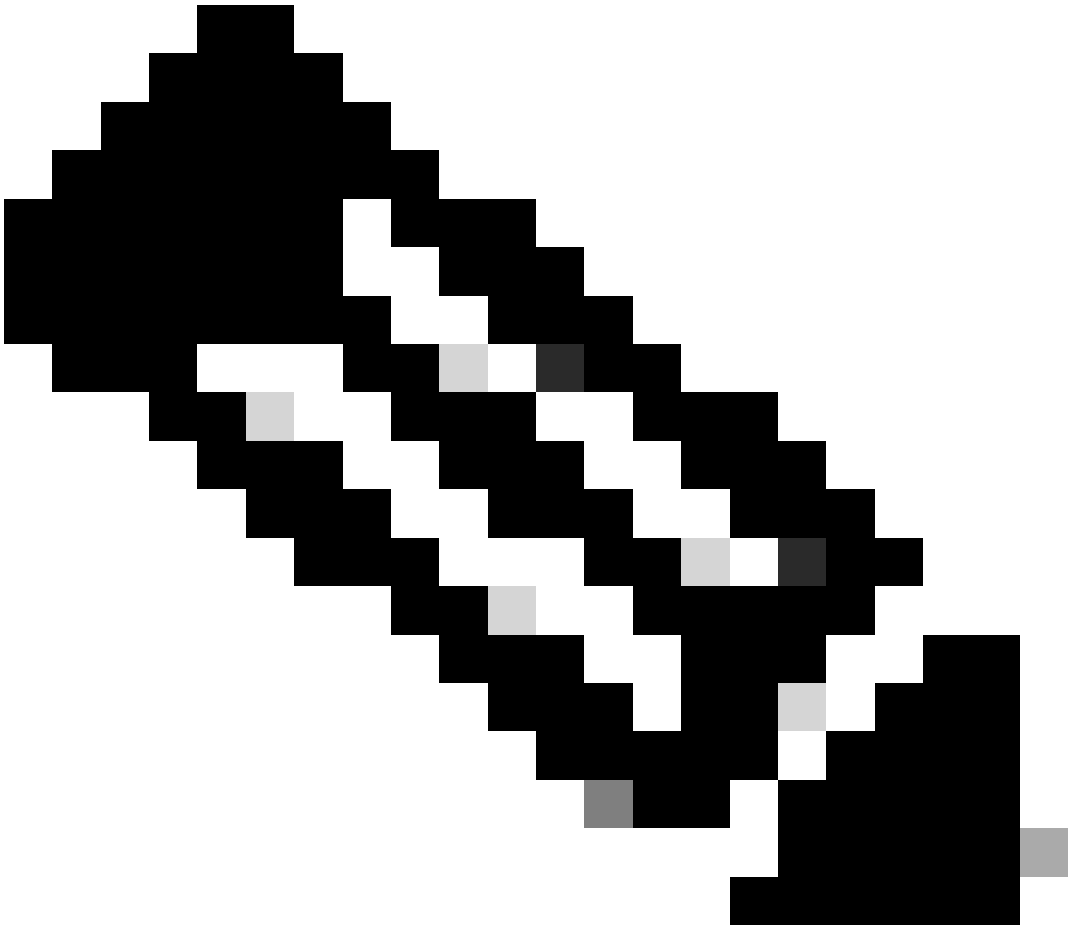
- 自定义过滤器

要从GUI使用预定义过滤器，请执行以下操作：

步骤1:在Packet Capture页面中，选择Edit Settings。

第二步：从Packet Capture Filters中选择Predefined Filters。

第三步：可以在客户端IP或服务器IP部分输入IP地址。



注意：在客户端IP或服务器IP之间进行选择并不限于源地址或目标地址。此过滤器可捕获IP地址定义为源或目标的所有数据包。

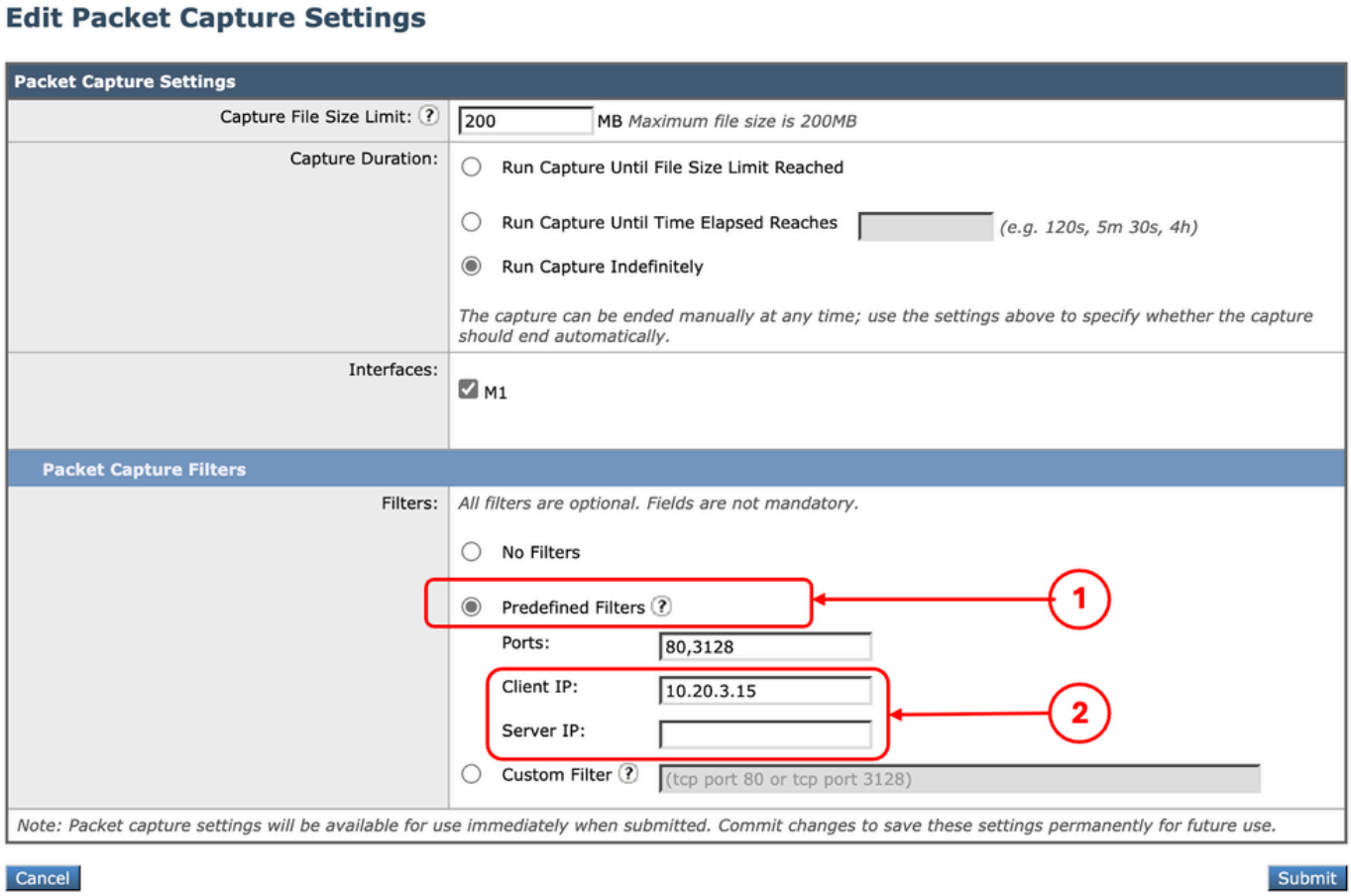
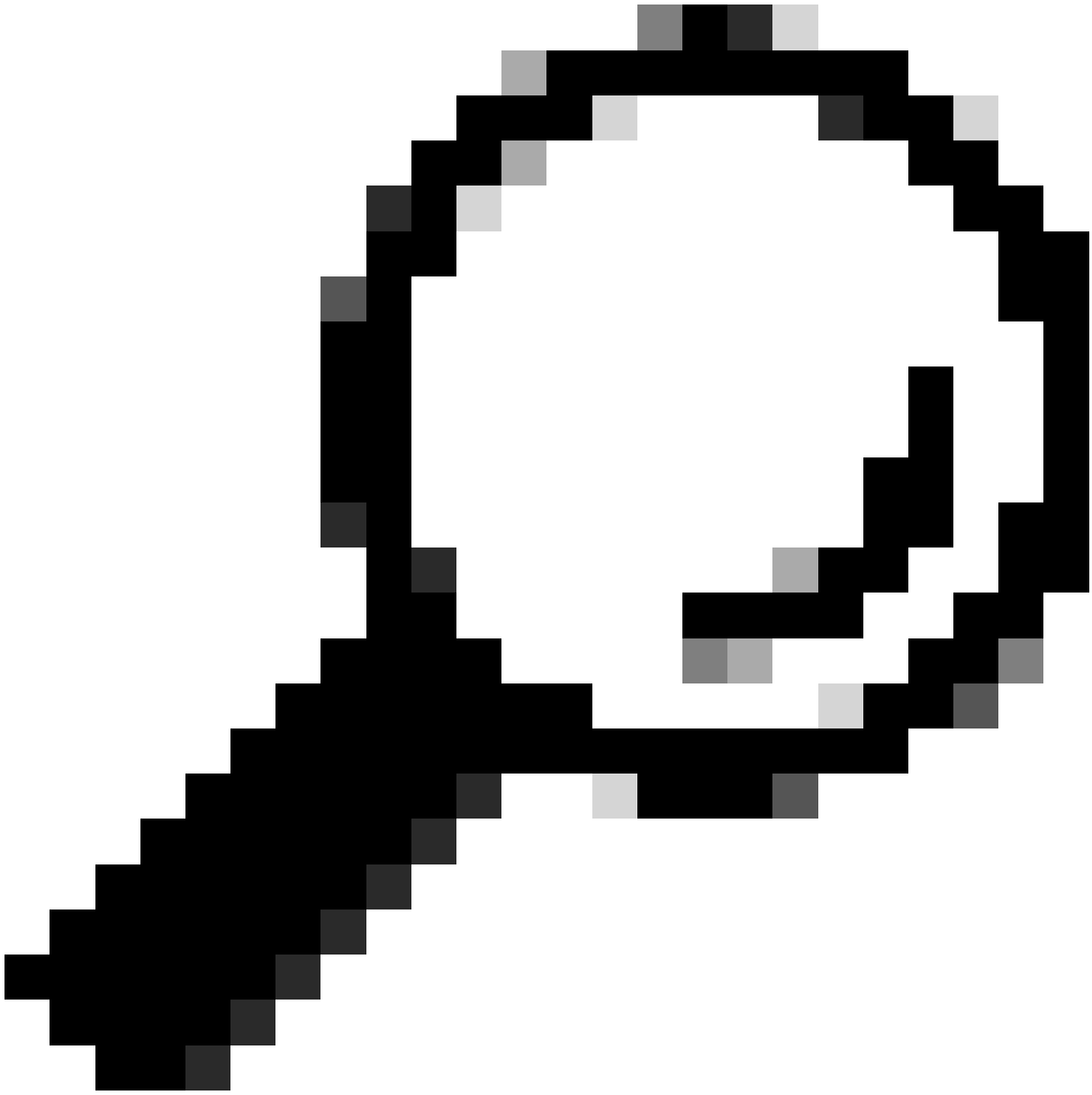


Image - Filter by Host IP from GUI Predefined Filters

第四步：提交更改。

第五步：开始捕获。



提示：无需提交更改(Commit Changes)，新添加的过滤器应用于当前捕获。提交更改有助于保存过滤器以供将来使用。

要在GUI中使用自定义过滤器和预定义过滤器，请执行以下操作：

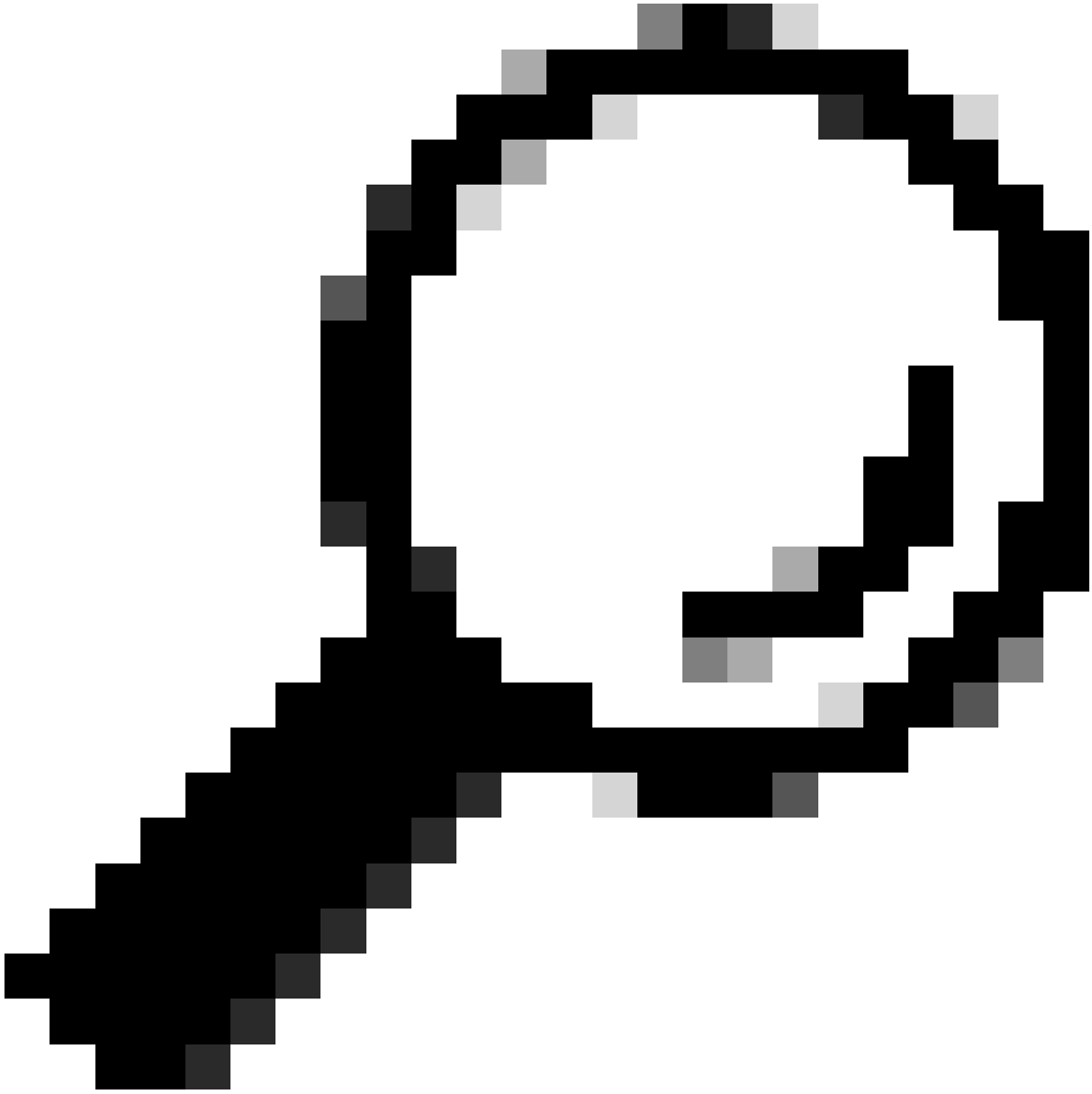
步骤1:在Packet Capture页面中，选择Edit Settings。

第二步：从Packet Capture Filters中选择Custom Filter。

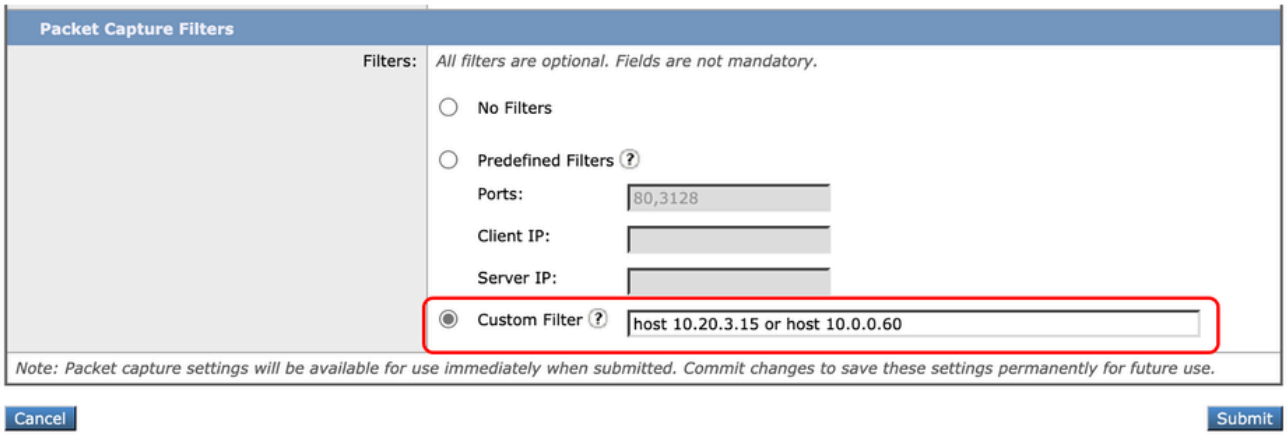
第三步：请使用后跟IP地址的host 语法。

以下是过滤源IP地址或目标IP地址为10.20.3.15的所有流量的示例

```
host 10.20.3.15
```



提示：要按多个IP地址过滤，您可以使用逻辑操作数，例如或和和（仅小写字母）。



图像-用于两个IP地址的自定义过滤器

第四步：提交更改。

第五步：开始捕获

在CLI中按主机IP过滤

要从CLI按主机IP地址过滤，请执行以下操作：

步骤1:登录到CLI。

第二步：键入packetcapture并按Enter。

第三步： 要编辑当前过滤器，请键入SETUP。

第四步：回答问题，直到您达到Enter the filter to be used for the capture

第五步： 可以使用与GUI中的自定义过滤器相同的过滤器字符串。

以下示例使用源或目标IP地址10.20.3.15或10.0.0.60过滤所有流量

```
SWA_CLI> packetcapture

Status: No capture running (Capture stopped by user)
File Name: S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-130426.cap
File Size: 4K
Duration:  2m 2s

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     (tcp port 80 or tcp port 3128)

Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> SETUP

Enter maximum allowable size for the capture file (in MB)
[200]>

Do you want to stop the capture when the file size is reached? (If not, a new file will be started and
[N]> y

The following interfaces are configured:
1. Management
Enter the name or number of one or more interfaces to capture packets from, separated by commas:
[1]>

Enter the filter to be used for the capture.
Enter the word "CLEAR" to clear the filter and capture all packets on the selected interfaces.
[(tcp port 80 or tcp port 3128)]> host 10.20.3.15 or host 10.0.0.60
```

按端口号过滤

在GUI中按端口号过滤

要按端口号过滤，在GUI中有两个选项：

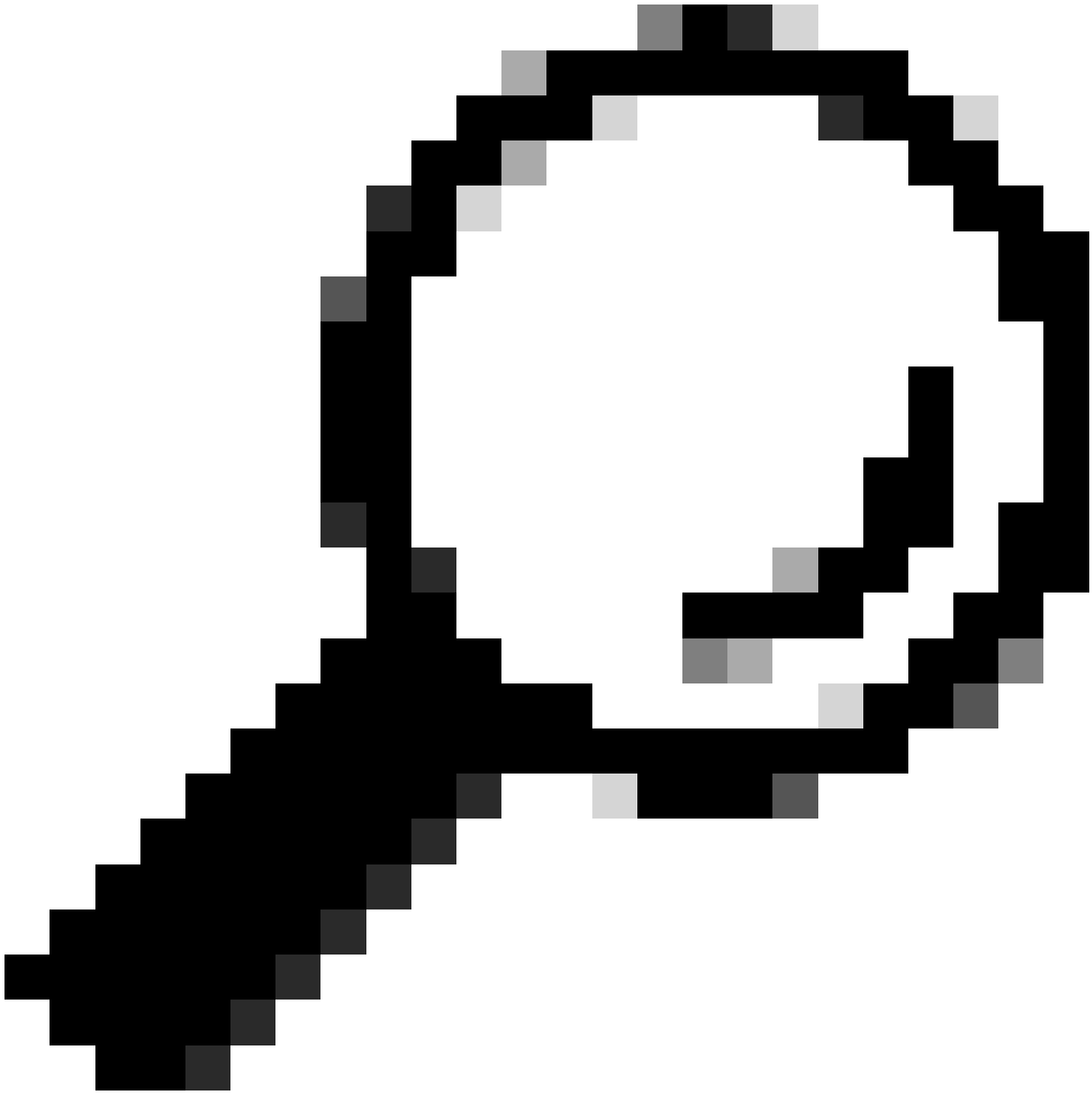
- 预定义过滤器
- 自定义过滤器

要从GUI使用预定义过滤器，请执行以下操作：

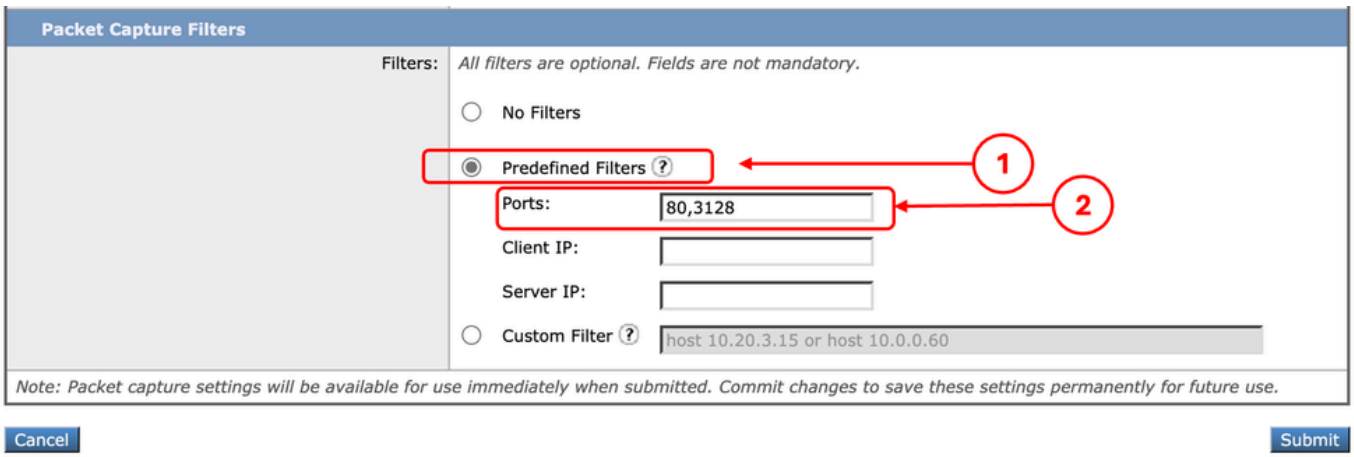
步骤1:在Packet Capture页面中，选择Edit Settings。

第二步：从Packet Capture Filters中选择Predefined Filters。

第三步： 在端口部分，键入要过滤的端口号。



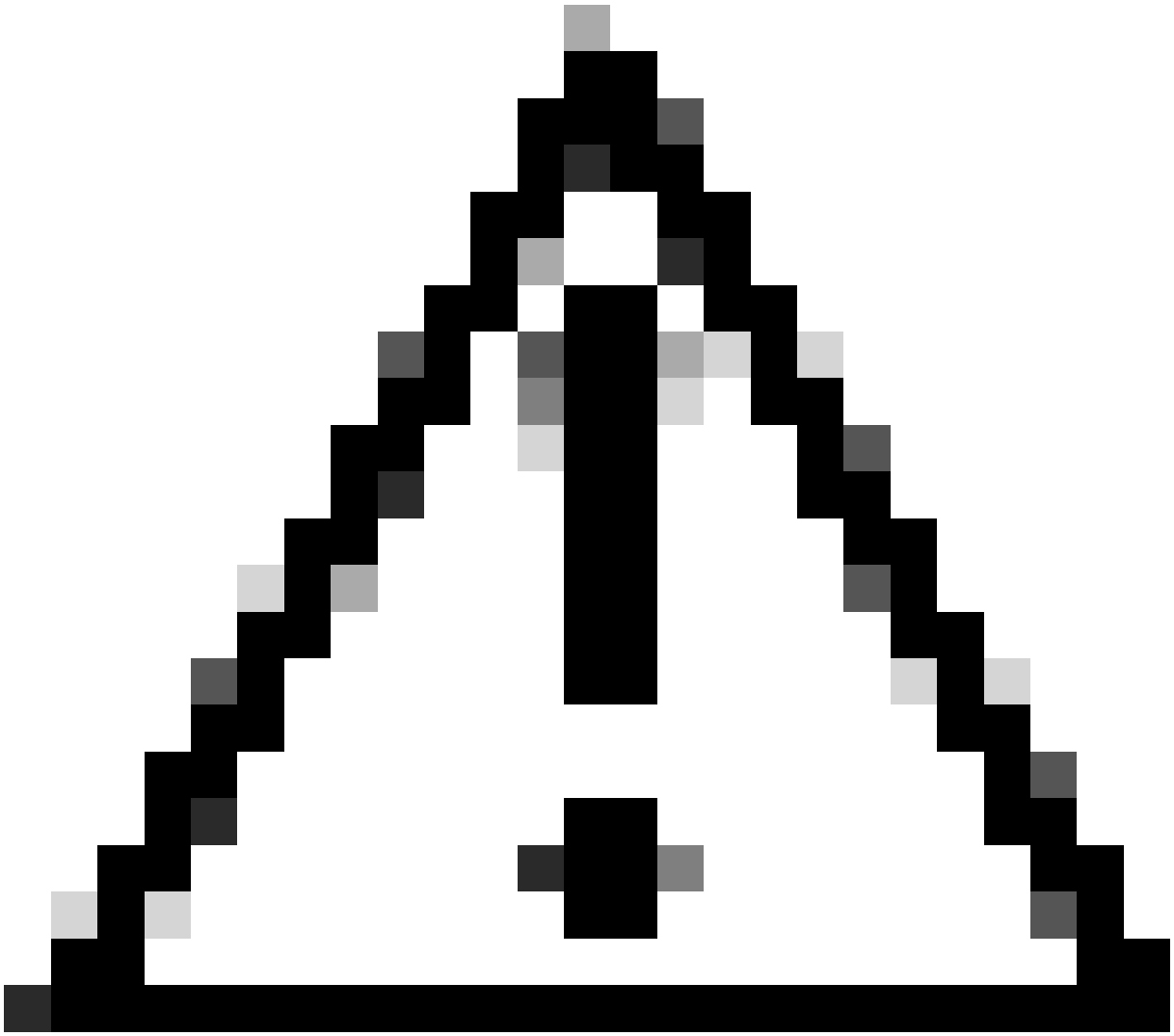
提示：您可以添加多个端口号，用逗号“ ”、“ ”隔开。



图像-按端口号过滤

第四步：提交更改。

第五步：开始捕获。



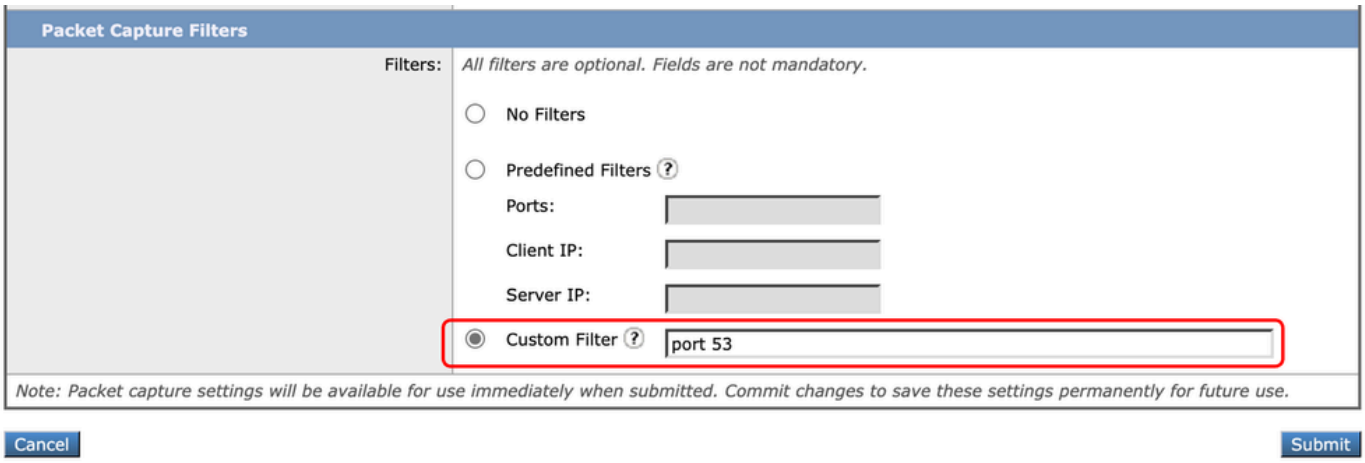
注意：此方法仅捕获具有定义端口号的TCP流量。若要捕获UDP流量，请使用自定义过滤器。

要从GUI使用自定义过滤器，请执行以下操作：

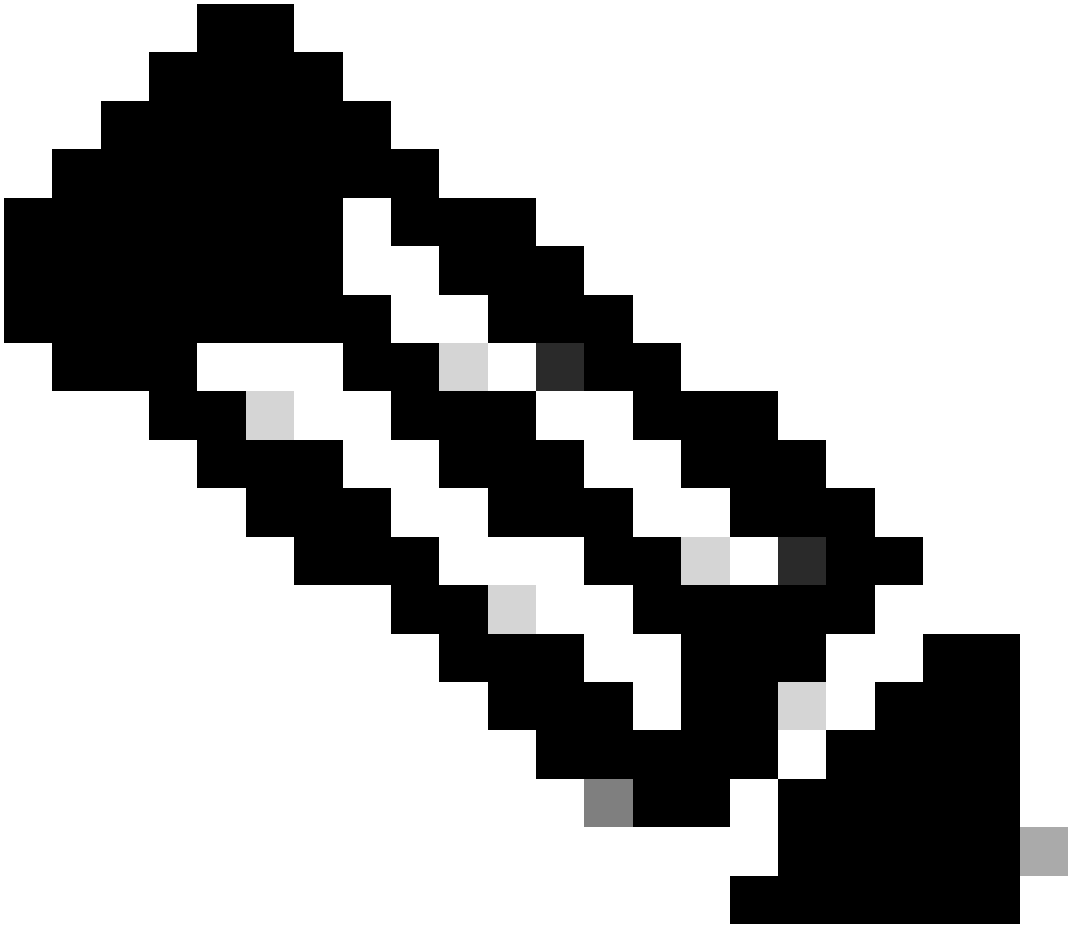
步骤1:在Packet Capture页面中，选择Edit Settings。

第二步：从Packet Capture Filters中选择Custom Filter。

第三步：使用后跟端口号的port语法。



图像-按端口号自定义过滤



注意：如果仅使用port，则此过滤器将同时涵盖TCP和UDP端口。

第四步：提交更改。

第五步：开始捕获。

在CLI中按端口号过滤

要从CLI按端口号过滤，请执行以下操作：

步骤1:登录到CLI。

第二步：键入packetcapture并按Enter。

第三步： 要编辑当前过滤器，请键入SETUP。

第四步：回答问题，直到您达到Enter the filter to be used for the capture

第五步： 可以使用与GUI中的自定义过滤器相同的过滤器字符串。

以下示例为TCP和UDP端口过滤源或目标端口号为53的所有流量：

```
SWA_CLI> packetcapture
Status: No capture running

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     (tcp port 80 or tcp port 3128)

Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> SETUP

Enter maximum allowable size for the capture file (in MB)
[200]>

Do you want to stop the capture when the file size is reached? (If not, a new file will be started and
[N]>

The following interfaces are configured:
1. Management
Enter the name or number of one or more interfaces to capture packets from, separated by commas:
[1]>

Enter the filter to be used for the capture.
Enter the word "CLEAR" to clear the filter and capture all packets on the selected interfaces.
[(tcp port 80 or tcp port 3128)]> port 53
```

使用透明部署的SWA中的过滤器

在透明部署的SWA中，虽然网络缓存通信协议(WCCP)连接通过通用路由封装(GRE)隧道，但传入或传出SWA的数据包中的源和目标IP地址是路由器IP地址和SWA IP地址。

要从GUI使用IP地址或端口号收集数据包捕获，有两个选项：

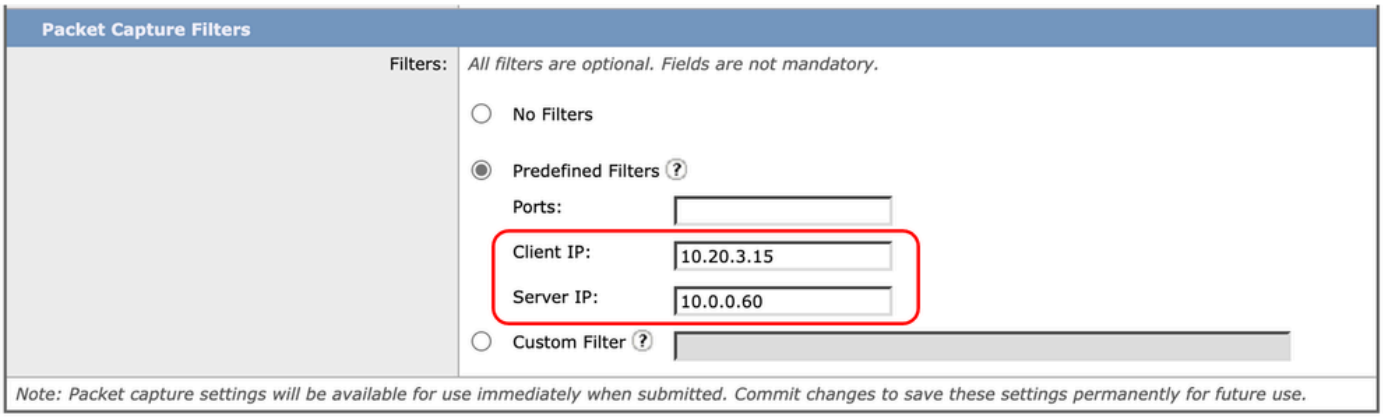
- 预定义过滤器
- 自定义过滤器

在SWA中过滤，在GUI中透明部署

步骤1:在Packet Capture页面中，选择Edit Settings。

第二步：从Packet Capture Filters中选择Predefined Filters。

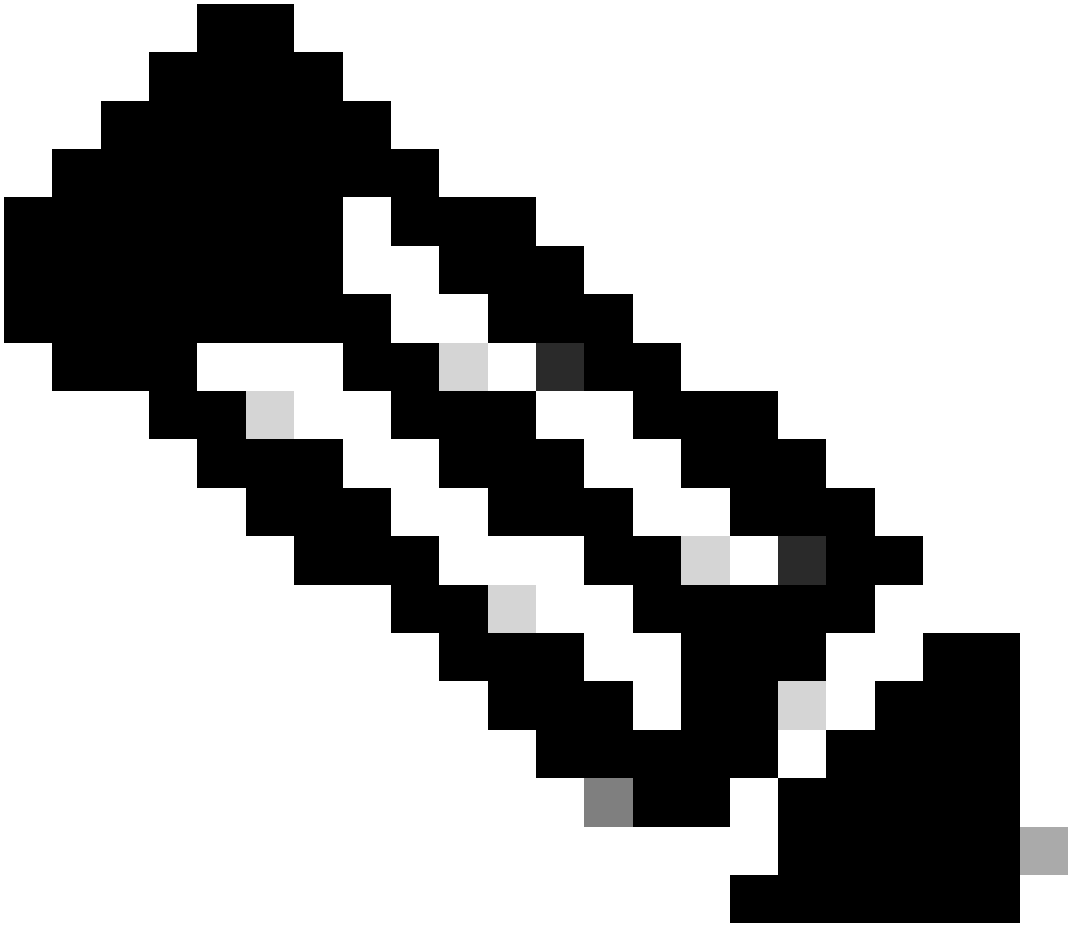
第三步：可以在客户端IP或服务器IP部分输入IP地址。



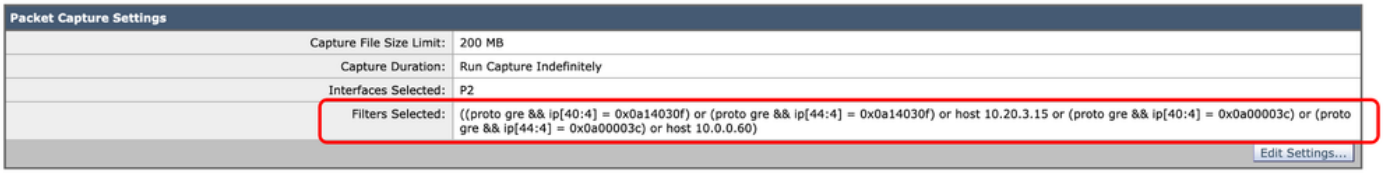
图像-在预定义过滤器中配置IP地址

第四步：提交更改。

第五步：开始捕获。



注意：在提交过滤器后，您可以看到SWA在Filter Selected部分添加了额外的条件。



映像- SWA添加的额外过滤器，用于收集GRE隧道内的数据包

要从GUI使用自定义过滤器，请执行以下操作：

步骤1:在Packet Capture页面中，选择Edit Settings。

第二步：从数据包捕获过滤器中，选择自定义过滤器

第三步：请先添加此字符串，然后再通过添加或在此字符串之后添加计划实施的过滤器：

```
(proto gre && ip[40:4] = 0x0a14030f) or (proto gre && ip[44:4] = 0x0a14030f) or (proto gre && ip[40:4] =
```

例如，如果计划按主机IP等于10.20.3.15或端口号等于8080进行过滤，则可以使用此字符串：

```
(proto gre && ip[40:4] = 0x0a14030f) or (proto gre && ip[44:4] = 0x0a14030f) or (proto gre && ip[40:4] =
```

第四步：提交更改。

第五步：开始捕获。

在SWA中过滤，在CLI中透明部署

要从CLI过滤透明代理部署，请执行以下操作：

步骤1:登录到CLI。

第二步：键入packetcapture 并按Enter。

第三步： 要编辑当前过滤器，请键入SETUP。

第四步：回答问题，直到您达到Enter the filter to be used for the capture

第五步： 可以使用与GUI中的自定义过滤器相同的过滤器字符串。

以下示例按主机IP等于10.20.3.15或端口号等于8080进行过滤：

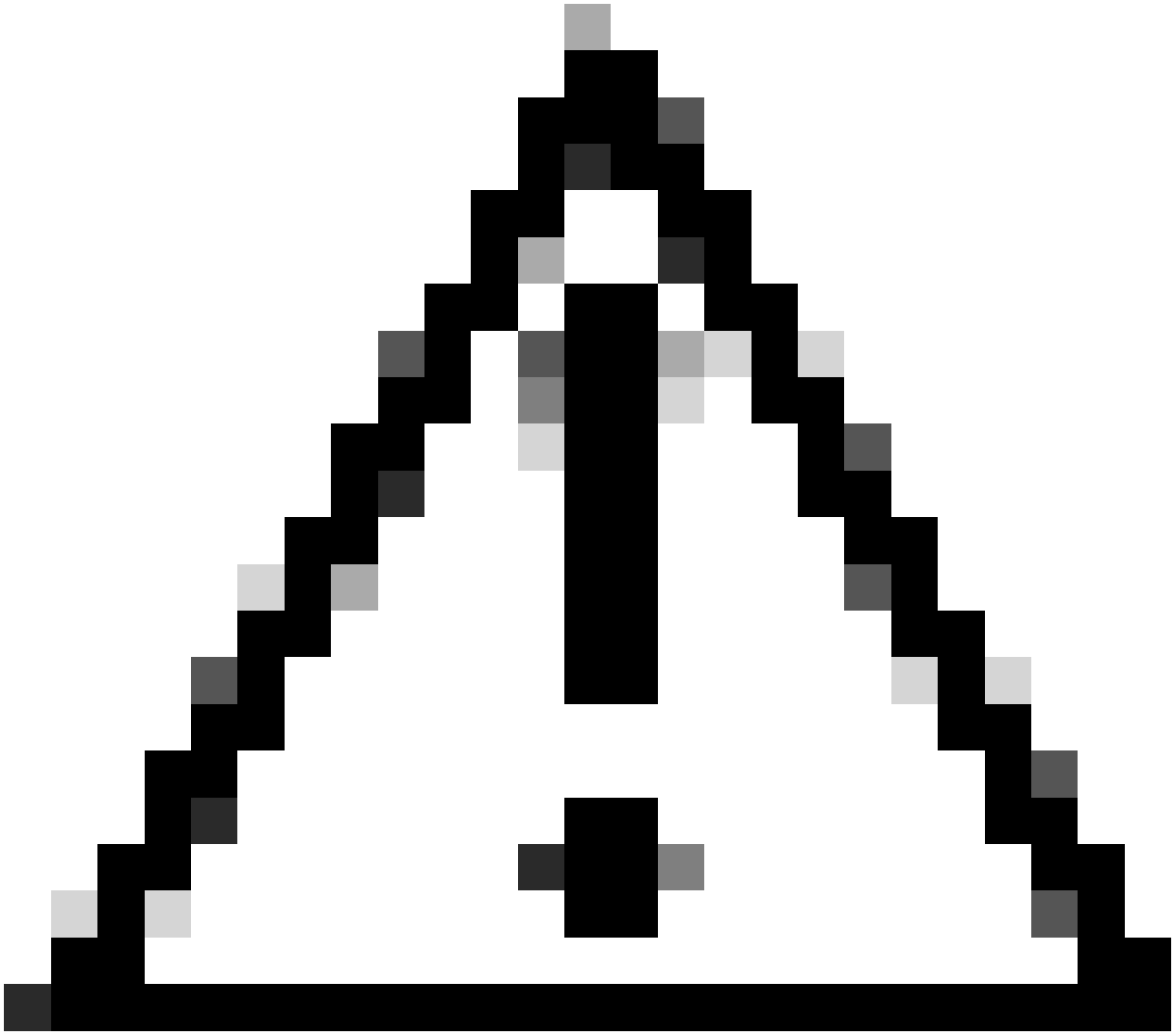
```
SWA_CLI> packetcapture
Status: No capture running

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     (tcp port 80 or tcp port 3128)

Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> SETUP

Enter maximum allowable size for the capture file (in MB)
[200]>

Do you want to stop the capture when the file size is reached? (If not, a new file will be started and
[N]>

The following interfaces are configured:
1. Management
Enter the name or number of one or more interfaces to capture packets from, separated by commas:
[1]>
```

```
Enter the filter to be used for the capture.
Enter the word "CLEAR" to clear the filter and capture all packets on the selected interfaces.
[(tcp port 80 or tcp port 3128)]> (proto gre && ip[40:4] = 0x0a14030f) or (proto gre && ip[44:4] = 0x0a
```

最常见的过滤器

下表列出了最常见的过滤器：

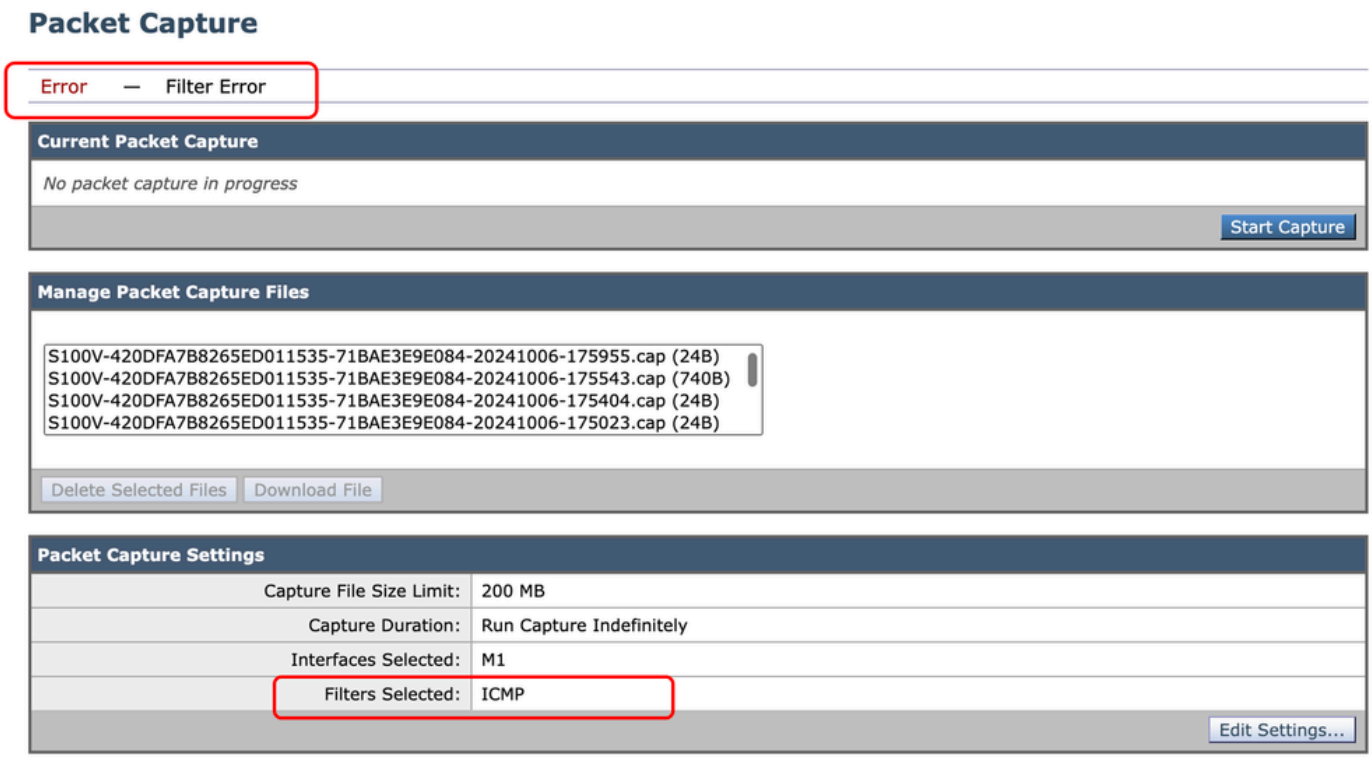
描述	过滤器
按源IP地址等于10.20.3.15过滤	src host 10.20.3.15
按目标IP地址等于10.20.3.15过滤	dst host 10.20.3.15
按源IP地址等于10.20.3.15且目标IP地址等于10.0.0.60进行过滤	(src host 10.20.3.15)和(dst host 10.0.0.60)
按源或目标IP地址等于10.20.3.15过滤	host 10.20.3.15
按源或目标IP地址等于10.20.3.15或等于10.0.0.60过滤	host 10.20.3.15或host 10.0.0.60
按TCP端口号等于8080过滤	tcp端口8080
按UDP端口号等于53过滤	udp端口53
按等于514（TCP或UDP）的端口号过滤	端口 514
仅过滤UDP数据包	udp
仅过滤ICMP数据包	icmp
用于透明部署中每个捕获的主过滤器	(proto gre && ip[40:4] = 0x0a14030f)或(proto gre && ip[44:4] = 0x0a14030f)或(proto gre && ip[40:4] = 0x0a00003c)或(proto gre && ip[44:4] = 0x0a00003c)



注意：所有过滤器都区分大小写。

故障排除

“过滤器错误”是执行数据包捕获时最常见的错误之一。



图像-过滤器错误

此错误通常与错误的过滤器实施有关。在上面的示例中，ICMP过滤器使用大写字符。这就是您收到过滤器错误的原因。要解决此问题，需要编辑过滤器并用icmp替换ICMP。

相关信息

- 思科安全网络设备AsyncOS 15.0用户指南- GD（通用部署）-最终用户分类……

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。