コンテンツセキュリティアプライアンスでのパケットキャプチャの設定

内容

はじめに

このドキュメントでは、CiscoセキュアWebアプライアンス(SWA)、Eメールセキュリティアプライアンス(ESA)、およびセキュリティ管理アプライアンス(SMA)でのパケットキャプチャについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Ciscoコンテンツセキュリティアプライアンスの管理

Cisco では次の前提を満たす推奨しています。

- インストールされている物理または仮想SWA/ESA/SMA。

- SWA/ESA/SMAグラフィカルユーザインターフェイス(GUI)への管理アクセス。
- SWA/ESA/SMAコマンドラインインターフェイス(CLI)への管理アクセス

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

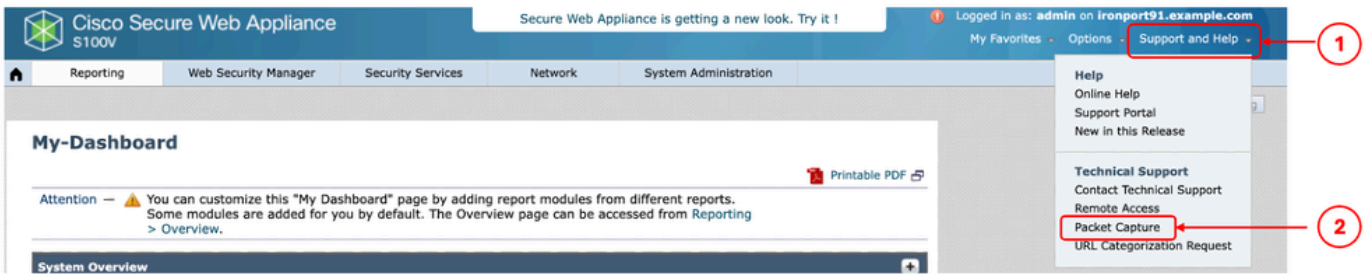
GUIからのパケットキャプチャの実行

GUIからパケットキャプチャを実行するには、次の手順を使用します。

ステップ 1：GUI にログインします。

ステップ 2：ページの右上で、Support and Helpの順に選択します。

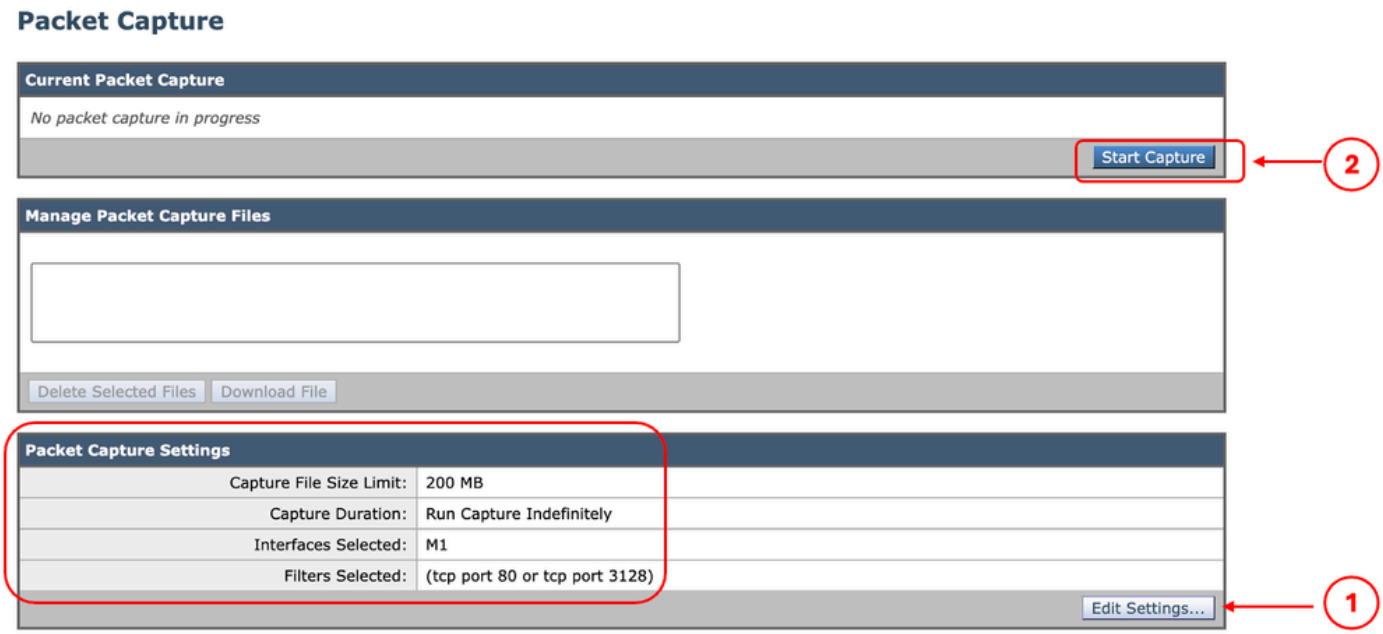
ステップ 3：Packet Captureを選択します。



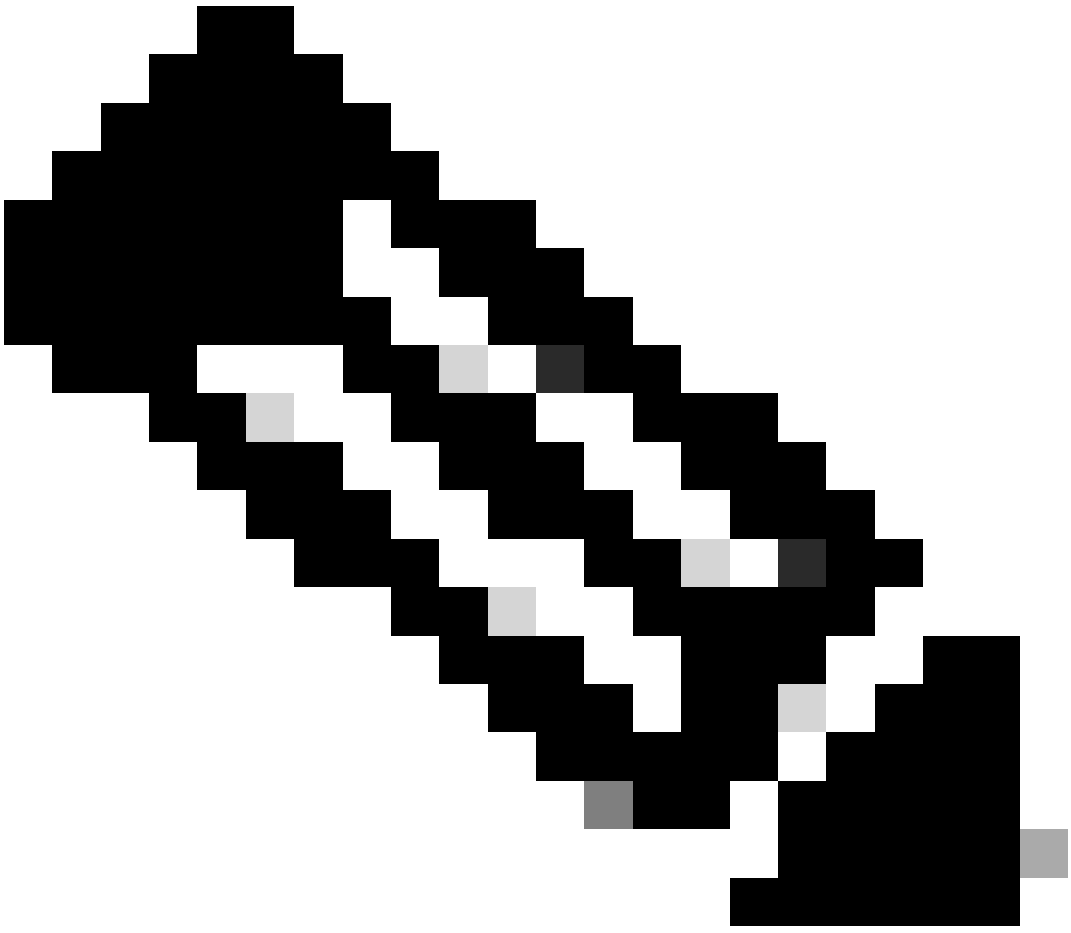
イメージ：パケットキャプチャ

ステップ4:（オプション）現在のフィルタを編集するには、Edit Settingsを選択します。（フィルタの詳細については、このドキュメントの「フィルタ」セクションを参照してください）

ステップ 5：キャプチャの開始.

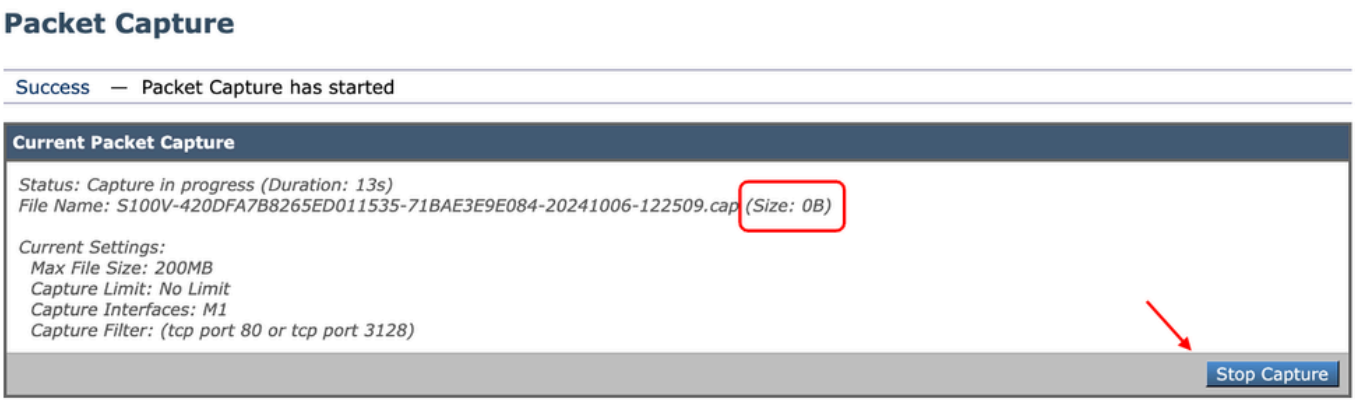


イメージ：パケットキャプチャのステータスとフィルタ



注：パケットキャプチャファイルのサイズ制限は200 MBです。ファイルサイズが200 MBに達すると、パケットキャプチャが停止します。

「現在のパケットキャプチャ」セクションには、ファイルサイズや適用されているフィルタなど、パケットキャプチャのステータスが表示されます。

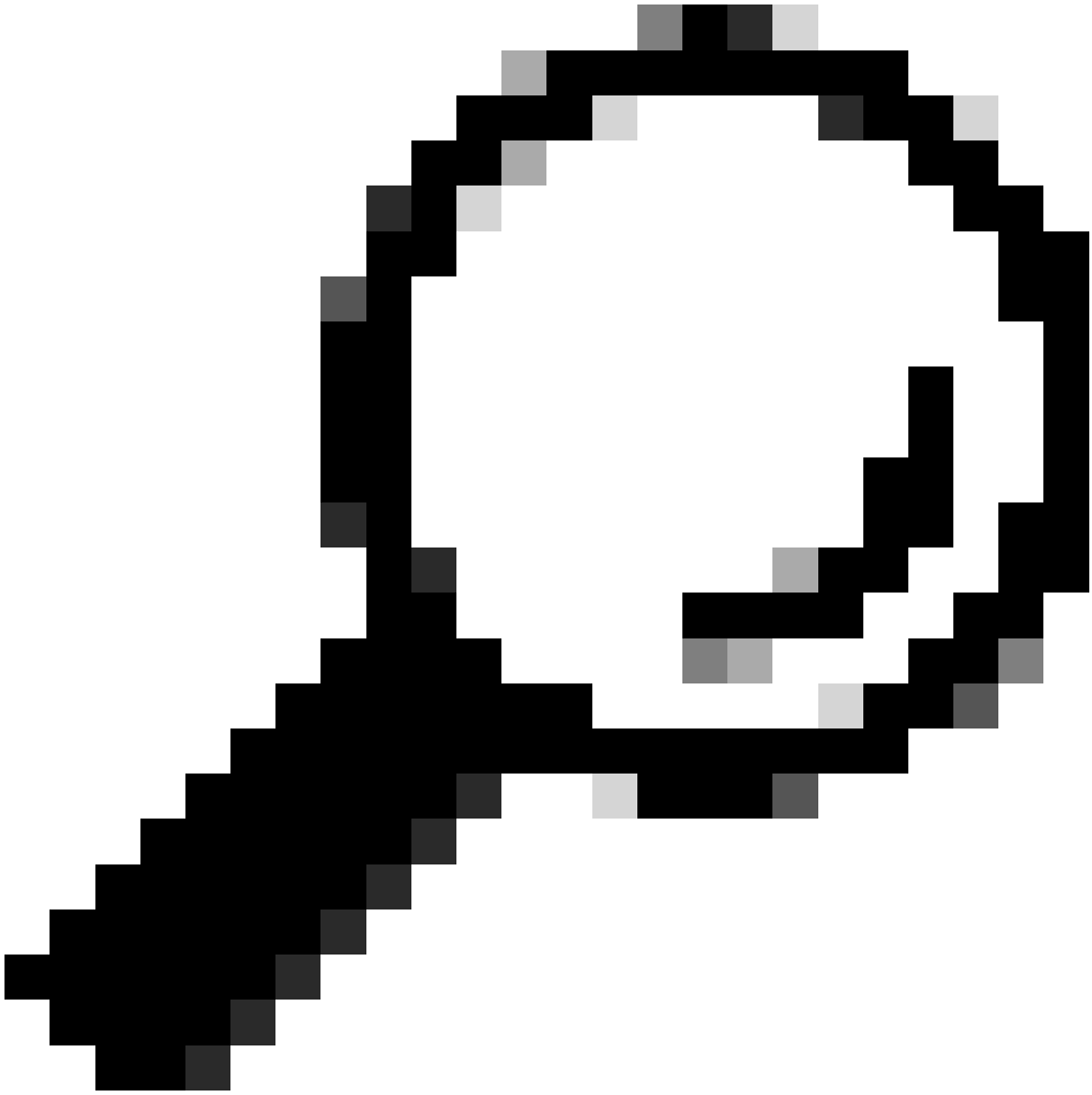


イメージ：パケットキャプチャステータス

手順 6：実行中のパケットキャプチャを停止するには、Stop Captureをクリックします。

手順 7：パケットキャプチャファイルをダウンロードするには、Manage Packet Capture Filesリストからファイルを選択して、Download Fileをクリックします。

イメージ：パケットキャプチャのダウンロード



ヒント：最新のファイルがリストの一番上に表示されます。

ステップ8: (オプション) パケットキャプチャファイルを削除するには、Manage Packet Capture Filesリストからファイルを選択して、Delete Selected Filesをクリックします。

CLIからのパケットキャプチャの実行

CLIからパケットキャプチャを開始する場合も、次の手順を使用できます。

ステップ 1 : CLIにログインします。

ステップ 2 : packetcapture と入力してEnter キーを押します。

ステップ3: (オプション) 現在のフィルタタイプSETUPを編集するには、次のコマンドを使用し

ます (フィルタの詳細については、このドキュメントの「フィルタ」の項を参照してください) 。

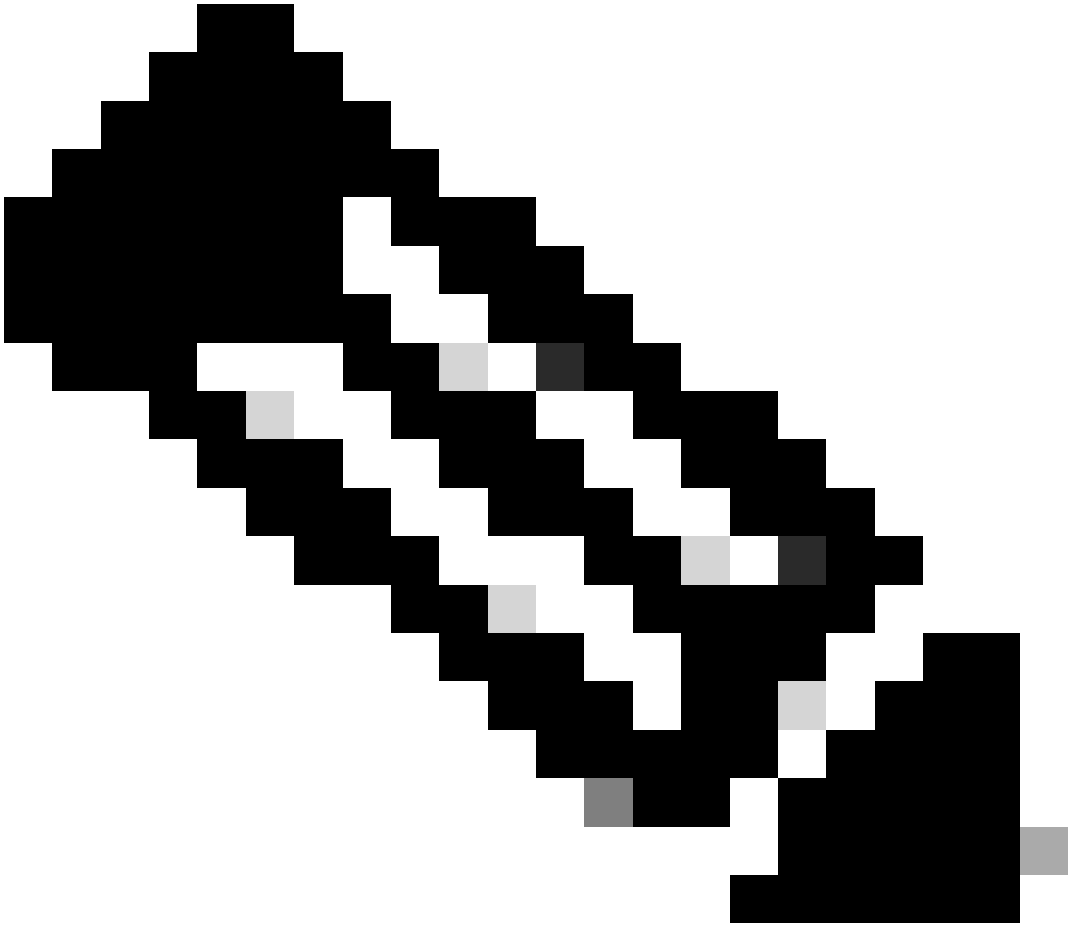
ステップ 4 : STARTを選択して、キャプチャを開始します。

```
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.
```

ステップ5: (オプション) パケットキャプチャのステータスを表示するには、STATUSを選択します。

```
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)
```

手順 6 : パケットキャプチャを停止するには、STOPと入力してEnterキーを押します。



注：CLIから収集したパケットキャプチャファイルをダウンロードするには、GUIからダウンロードするか、File Transfer Protocol（FTP；ファイル転送プロトコル）を使用してアプライアンスに接続し、Capturesフォルダからダウンロードします。

フィルタ

ここでは、コンテンツセキュリティアプライアンスで使用できるフィルタに関するガイドを示します。

ホストIPアドレスによるフィルタリング

GUIでのホストIPによるフィルタリング

ホストIPアドレスでフィルタリングするには、GUIから次の2つのオプションを使用します。

- 定義済みフィルタ

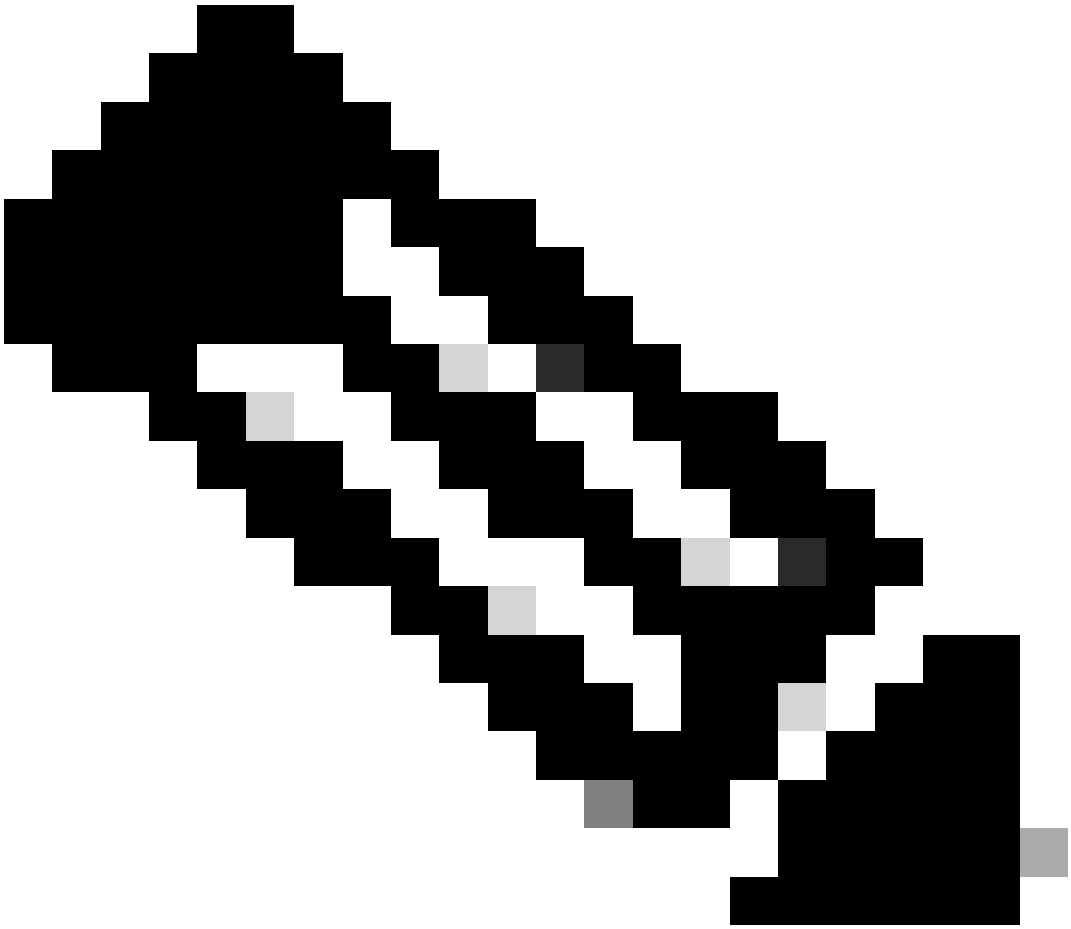
- カスタムフィルタ

GUIから事前定義済みフィルタを使用するには、次の手順を実行します。

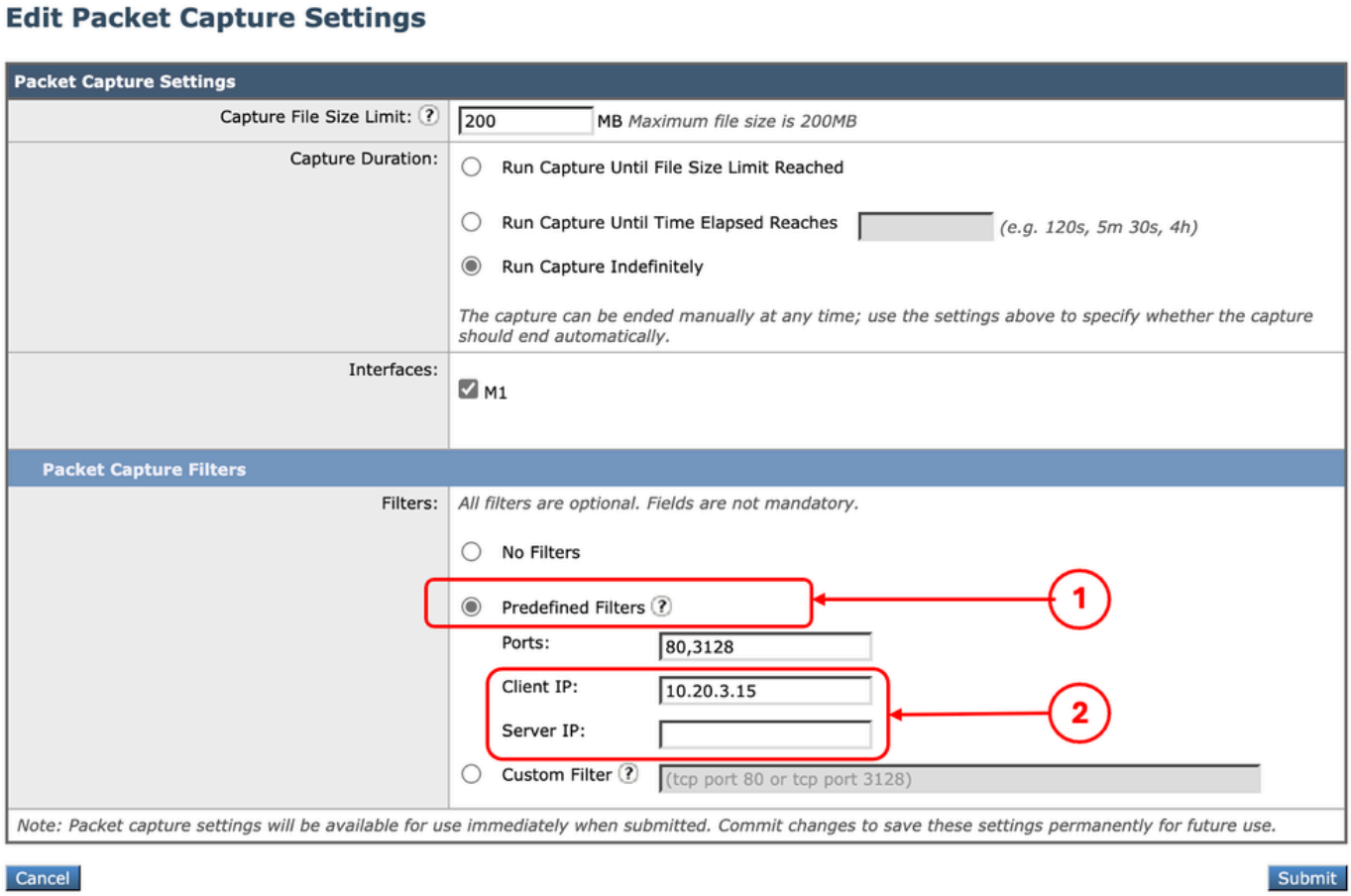
ステップ 1：Packet Captureページで、Edit Settingsを選択します。

ステップ 2：Packet Capture Filtersから、Predefined Filtersを選択します。

ステップ 3：IPアドレスは、Client IPまたはServer IPセクションで入力できます。



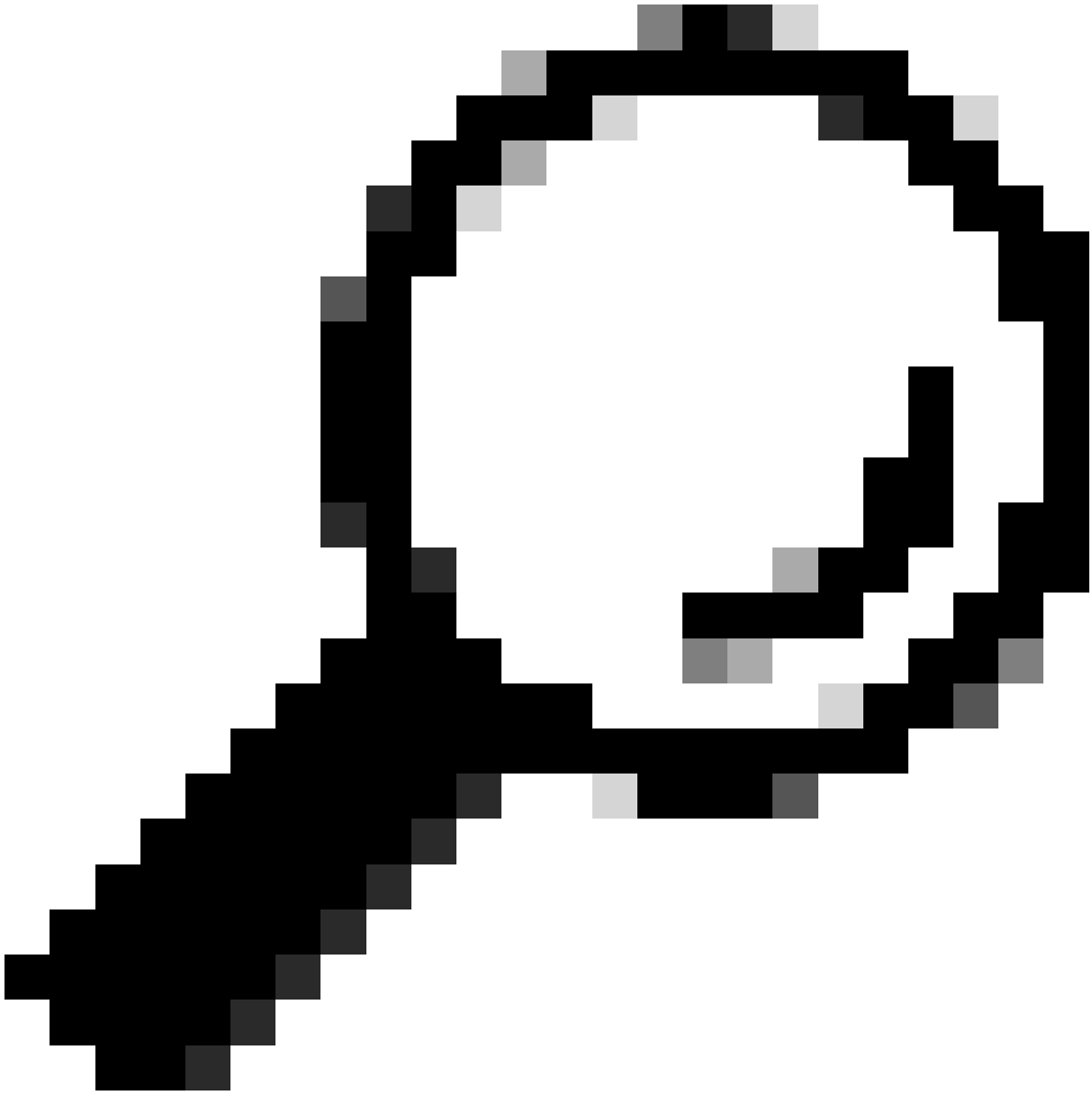
注：クライアントIPまたはサーバIPの選択は、送信元アドレスまたは宛先アドレスに限定されません。このフィルタは、送信元または宛先として定義されたIPアドレスを持つすべてのパケットをキャプチャします。



イメージ – GUIの事前定義済みフィルタからのホストIPによるフィルタリング

ステップ 4：変更を送信します。

ステップ 5：キャプチャの開始.



ヒント：現在のキャプチャに適用されている新しく追加されたフィルタである変更をコミットする必要はありません。変更をコミットすると、将来の使用に備えてフィルタを保存できます。

GUIからカスタムフィルタおよび定義済みフィルタを使用するには、次の手順を実行します。

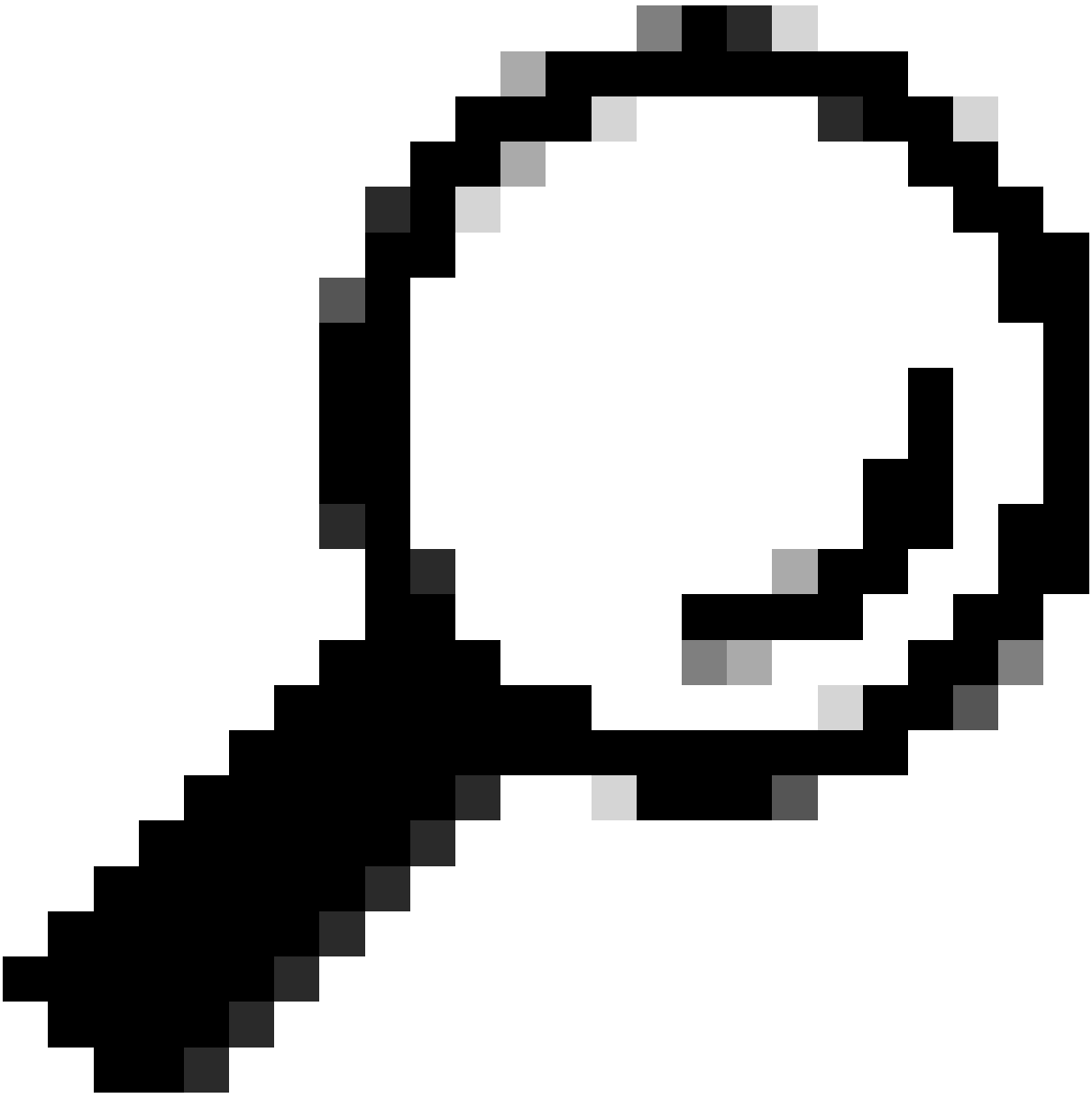
ステップ 1：Packet Captureページで、Edit Settingsを選択します。

ステップ 2：Packet Capture Filtersで、Custom Filterを選択します。

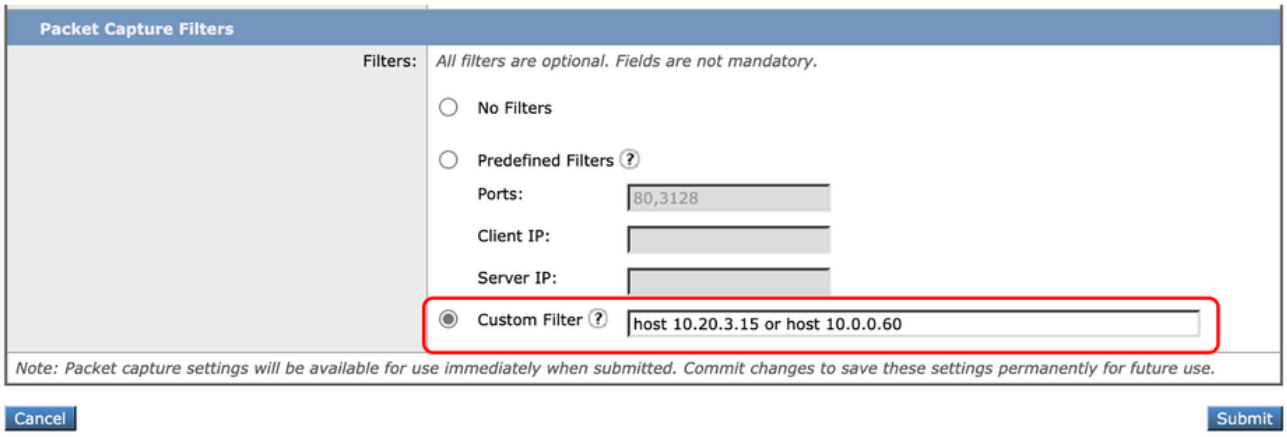
ステップ 3：host構文に続けてIPアドレスを指定します。

次に、送信元または宛先IPアドレスが10.20.3.15であるすべてのトラフィックをフィルタリングする例を示します

```
host 10.20.3.15
```



ヒント：複数のIPアドレスでフィルタリングするには、or（小文字のみ）やand（小文字のみ）などの論理オペランドを使用できます。



イメージ – 2つのIPアドレスのカスタムフィルタ

ステップ 4：変更を送信します。

ステップ 5：キャプチャの開始

CLIでのホストIPによるフィルタリング

CLIからホストIPアドレスでフィルタリングするには、次のコマンドを実行します。

ステップ 1：CLIにログインします。

ステップ 2：packetcapture と入力してEnterキーを押します。

ステップ 3： 現在のフィルタを編集するには、SETUPと入力します。

ステップ 4：Enter the filter to use the captureに達するまで質問に答えます。

ステップ 5： GUIのカスタムフィルタと同じフィルタ文字列を使用できます。

次に、送信元または宛先IPアドレスが10.20.3.15または10.0.0.60のすべてのトラフィックをフィルタリングする例を示します

```
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
```

ポート番号によるフィルタ

GUIでのポート番号によるフィルタリング

ポート番号でフィルタリングするには、GUIから次の2つのオプションを使用します。

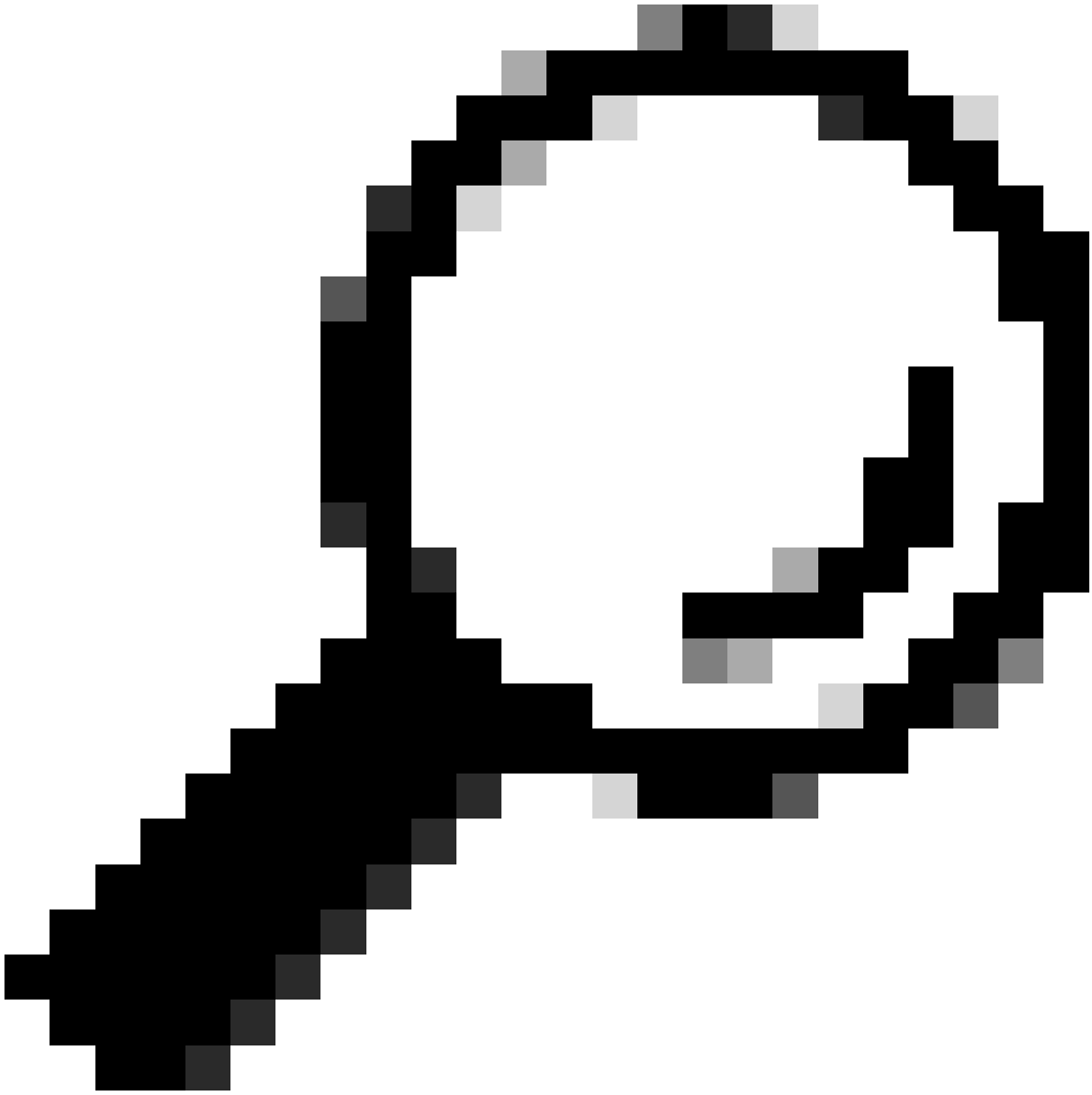
- 定義済みフィルタ
- カスタムフィルタ

GUIから事前定義済みフィルタを使用するには、次の手順に従います。

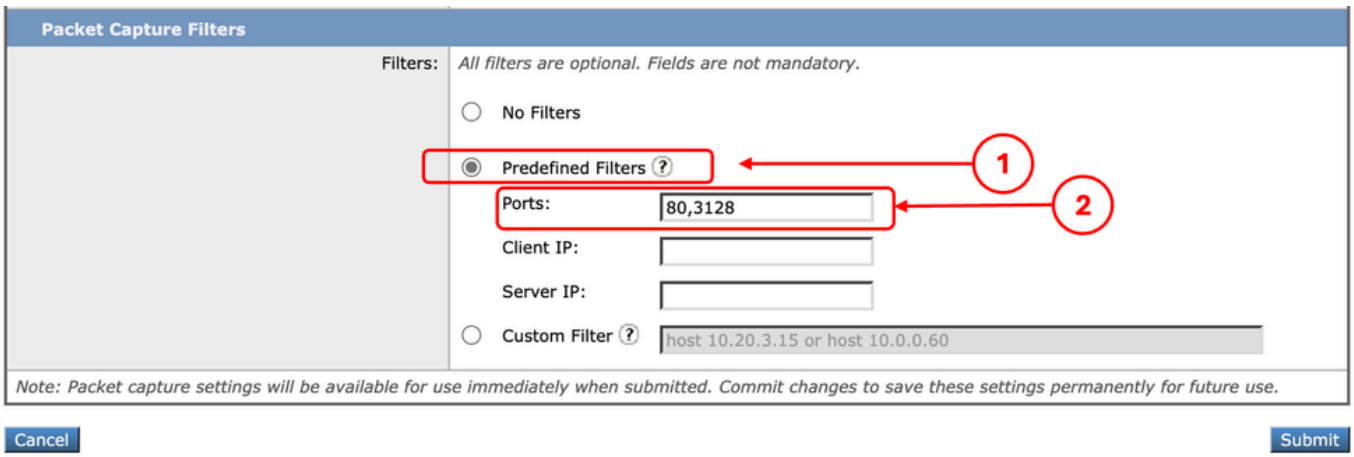
ステップ 1：Packet Captureページで、Edit Settingsを選択します。

ステップ 2：Packet Capture Filtersから、Predefined Filtersを選択します。

ステップ 3： Portsセクションで、フィルタリングするポート番号を入力します。



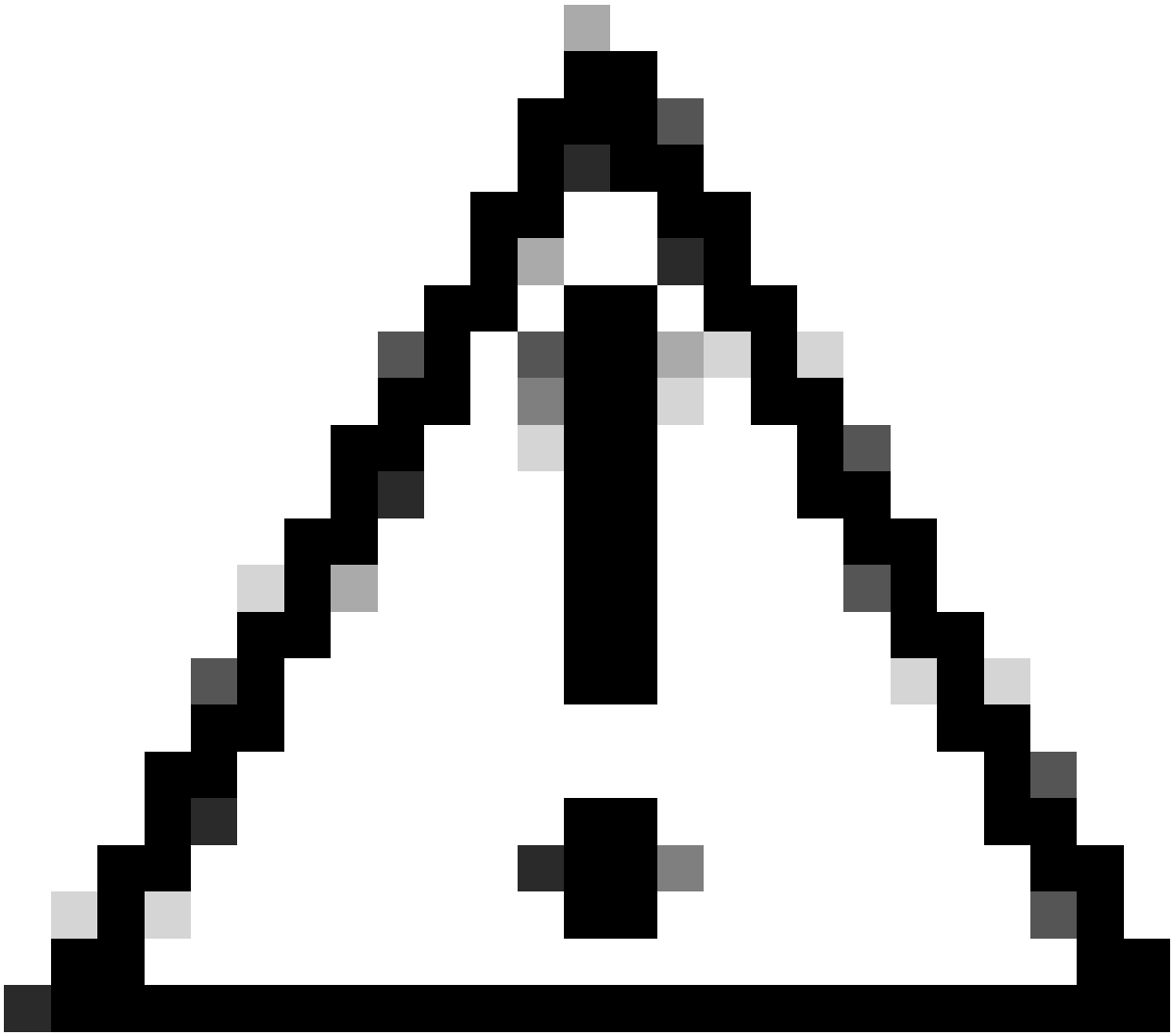
ヒント：複数のポート番号をカンマ「，」で区切って追加できます。



イメージ – ポート番号によるフィルタリング

ステップ 4：変更を送信します。

ステップ 5：キャプチャの開始.



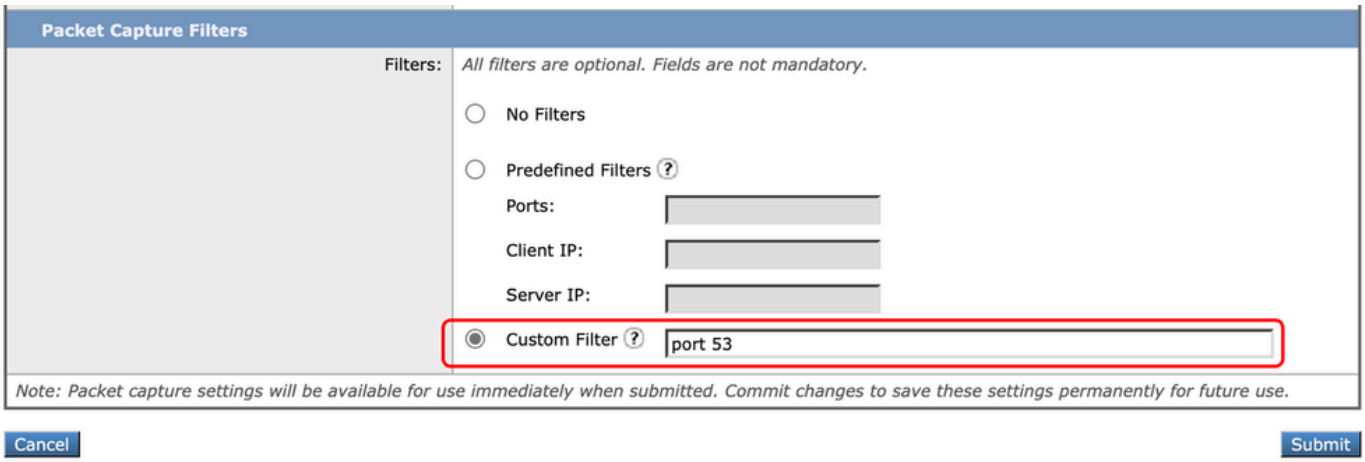
注意：このアプローチでは、定義されたポート番号を持つTCPトラフィックだけがキャプチャされます。UDPトラフィックをキャプチャするには、カスタムフィルタを使用します。

GUIからカスタムフィルタを使用するには、次の手順を実行します。

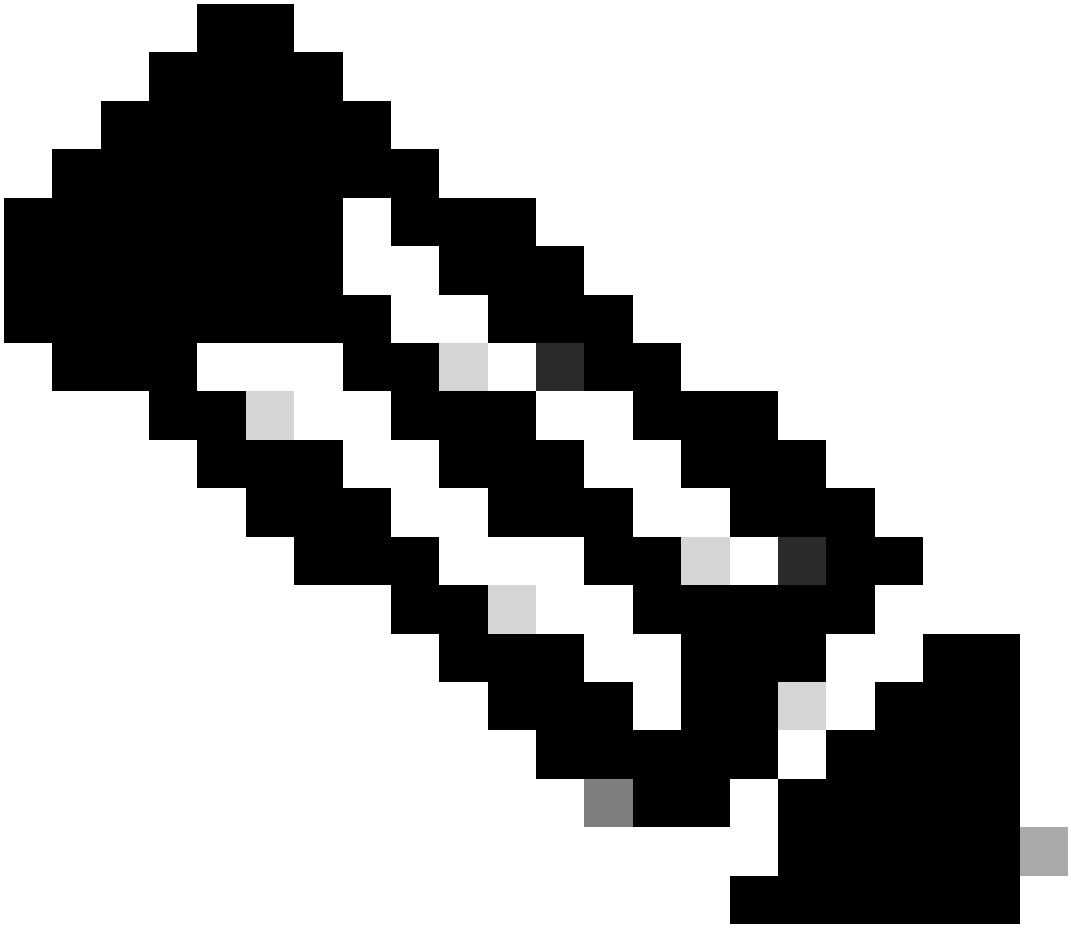
ステップ 1：Packet Captureページで、Edit Settingsを選択します。

ステップ 2：Packet Capture Filtersで、Custom Filterを選択します。

ステップ 3：port構文に続けてポート番号を指定します。



イメージ – ポート番号によるカスタムフィルタ



注：portだけを使用する場合、このフィルタはTCPポートとUDPポートの両方を対象とします。

ステップ 4：変更を送信します。

ステップ 5：キャプチャの開始.

CLIでのポート番号によるフィルタリング

CLIからポート番号でフィルタリングするには、次の手順を実行します。

ステップ 1：CLIにログインします。

ステップ 2：packetcapture と入力してEnterキーを押します。

ステップ 3： 現在のフィルタを編集するには、SETUPと入力します。

ステップ 4：Enter the filter to use the captureに達するまで質問に答えます。

ステップ 5： GUIのカスタムフィルタと同じフィルタ文字列を使用できます。

次に、TCPポートとUDPポートの両方について、送信元または宛先ポート番号が53であるすべてのトラフィックをフィルタリングする例を示します。

```
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
```

透過型導入を使用したSWAでのフィルタ

透過型導入のSWAでは、Web Cache Communication Protocol(WCCP)接続はGeneric Routing Encapsulation(GRE)トンネルを介しますが、SWAで発着信するパケットの送信元IPアドレスと宛

先IPアドレスは、ルータIPアドレスとSWA IPアドレスです。

GUIからIPアドレスまたはポート番号を使用してパケットキャプチャを収集するには、次の2つのオプションがあります。

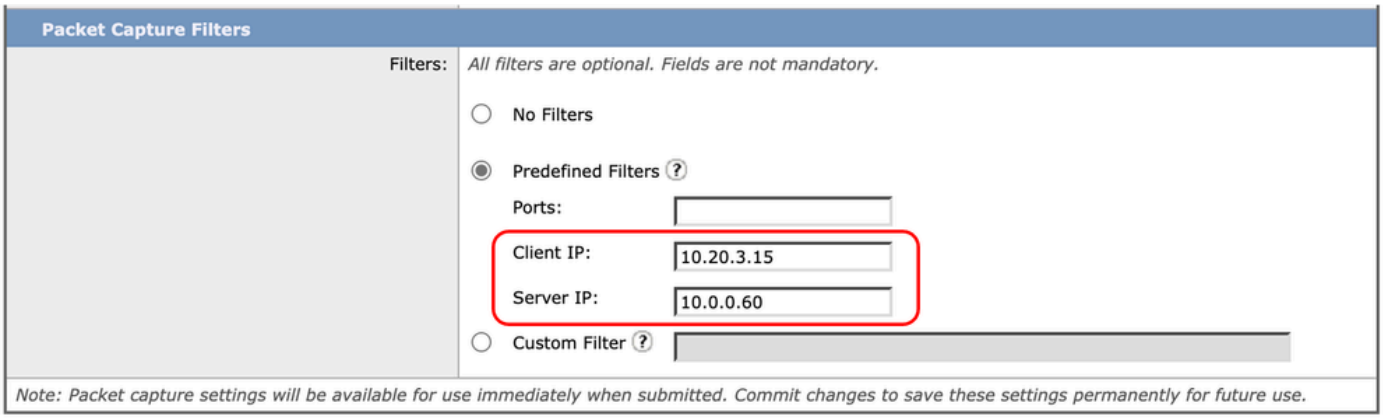
- 定義済みフィルタ
- カスタムフィルタ

GUIでの透過型導入を使用したSWAでのフィルタ

ステップ 1：Packet Captureページで、Edit Settingsを選択します。

ステップ 2：Packet Capture Filtersから、Predefined Filtersを選択します。

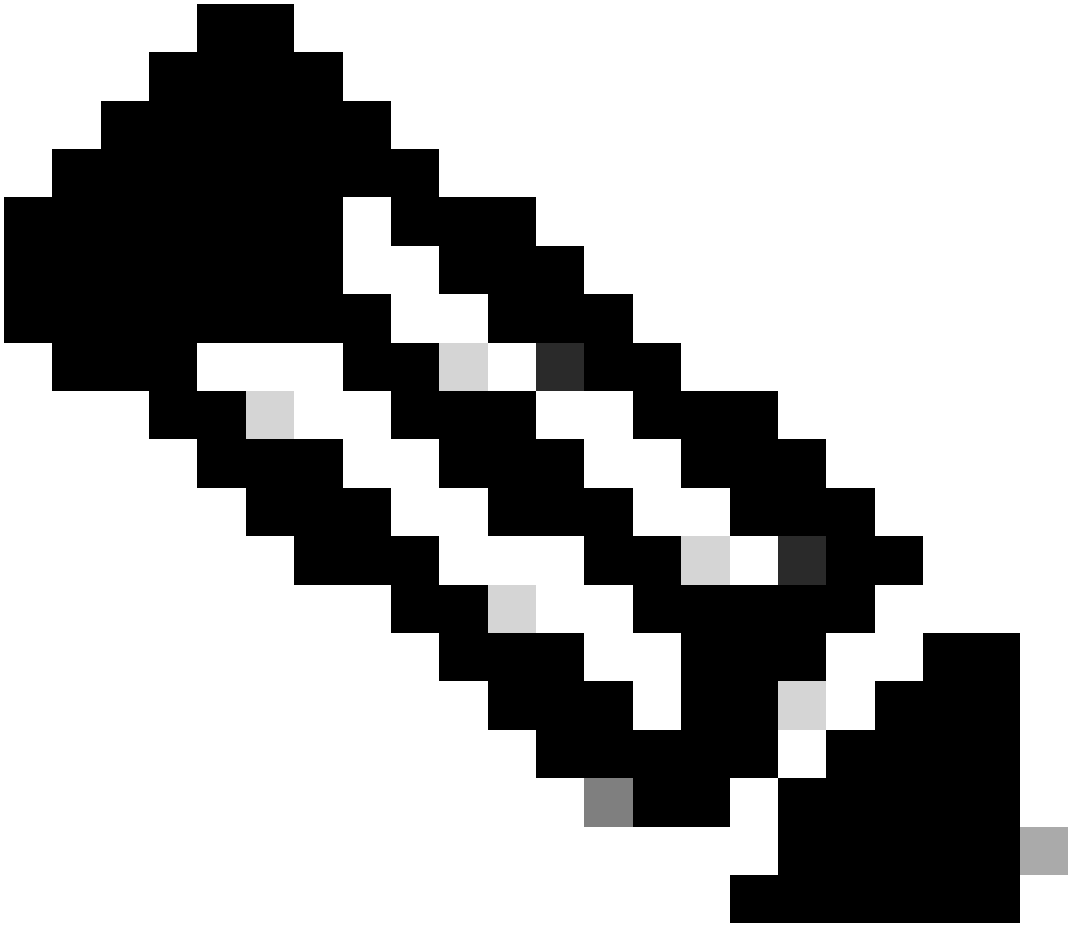
ステップ 3：IPアドレスは、Client IPまたはServer IPセクションで入力できます。



イメージ：事前定義フィルタでのIPアドレスの設定

ステップ 4：変更を送信します。

ステップ 5：キャプチャの開始.



注：フィルタを送信した後で、SWAによって「Filter Selected」セクションに条件が追加されたことが分かります。

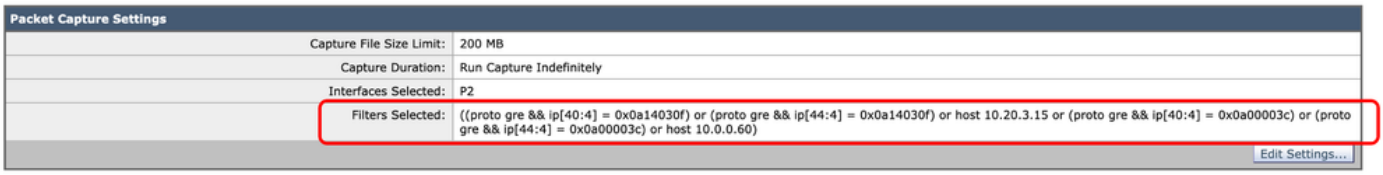


図 – GREトンネル内でパケットを収集するためにSWAによって追加される追加フィルタ

GUIからカスタムフィルタを使用するには、次の手順を実行します。

ステップ 1：Packet Captureページで、Edit Settingsを選択します。

ステップ 2：Packet Capture Filtersから、Custom Filterを選択します。

ステップ 3：最初にこの文字列を追加し、次に、この文字列の後にまたはを追加して、実装する予定のフィルタを追加します。

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

たとえば、10.20.3.15に等しいホストIPまたは8080に等しいポート番号でフィルタリングする場合は、次の文字列を使用できます。

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

ステップ 4：変更を送信します。

ステップ 5：キャプチャの開始.

CLIでの透過型導入を使用したSWAでのフィルタ

CLIからトランスペアレントプロキシ導入でフィルタリングするには、次の手順を実行します。

ステップ 1：CLIにログインします。

ステップ 2：packetcapture と入力してEnter キーを押します。

ステップ 3： 現在のフィルタを編集するには、SETUPと入力します。

ステップ 4：Enter the filter to use the captureに達するまで質問に答えます。

ステップ 5： GUIのカスタムフィルタと同じフィルタ文字列を使用できます。

ホストIPが10.20.3.15、またはポート番号が8080の場合のフィルタリング例を次に示します。

```
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:
```

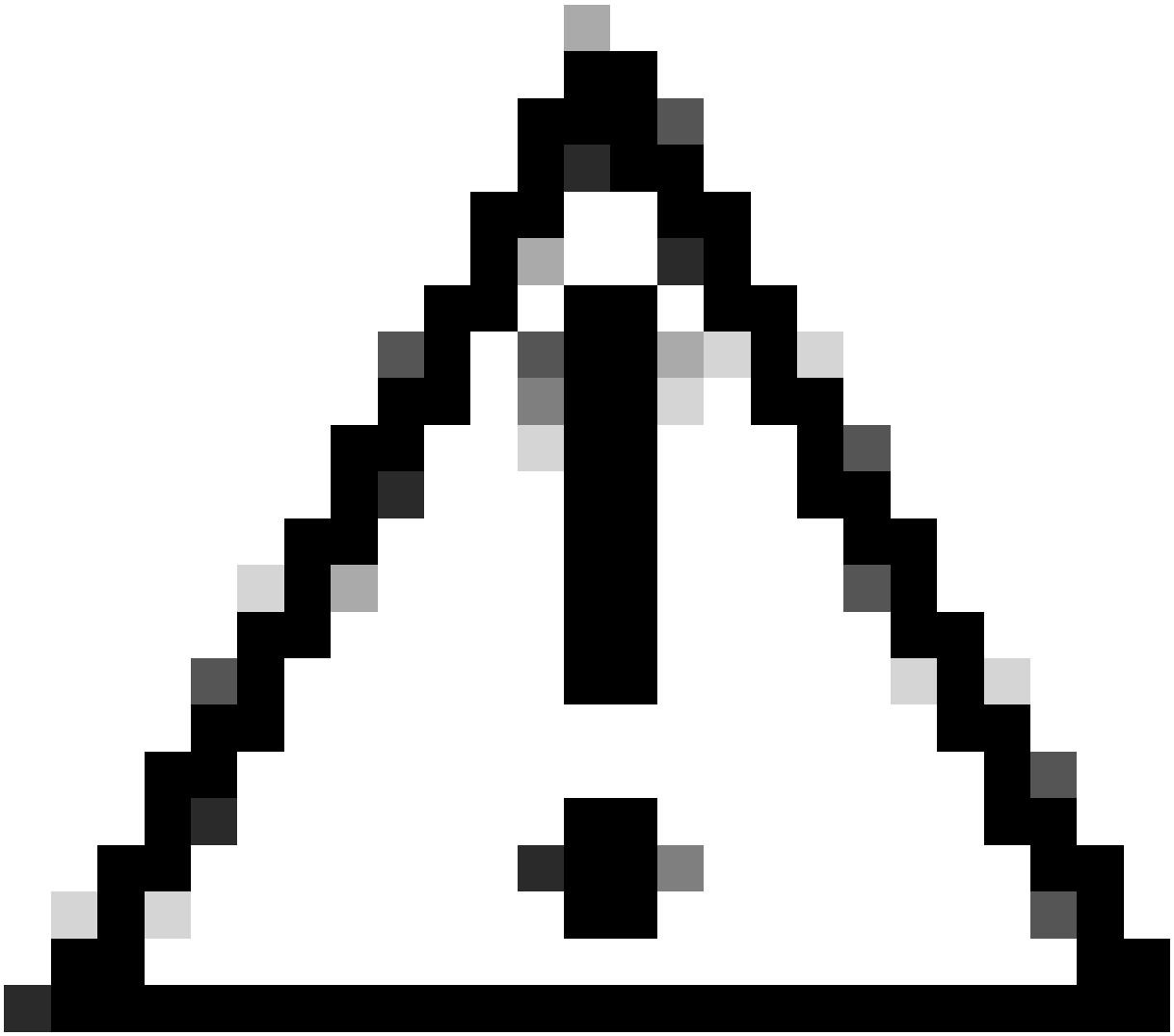
```
1. Management
Enter the name or number of one or more interfaces to capture packets from, separated by commas:
[1]>

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
```

最も一般的なフィルタ

次の表に、一般的なフィルタを示します。

説明	フィルタ
送信元IPアドレス10.20.3.15でフィルタリング	送信元ホスト10.20.3.15
10.20.3.15に等しい宛先IPアドレスでフィルタリング	dstホスト10.20.3.15
送信元IPアドレスが10.20.3.15、宛先IPアドレスが10.0.0.60のフィルタ	(src host 10.20.3.15)および(dst host 10.0.0.60)
送信元または宛先IPアドレスが10.20.3.15のフィルタ	ホスト10.20.3.15
送信元または宛先IPアドレスが10.20.3.15または10.0.0.60のフィルタ	host 10.20.3.15またはhost 10.0.0.60
TCPポート番号8080でフィルタリング	TCP ポート 8080
UDPポート番号53でフィルタリング	UDP ポート 53
514（TCPまたはUDP）に等しいポート番号でフィルタ	port 514
UDPパケットのみのフィルタ	udp
ICMPパケットのみをフィルタリングする	icmp

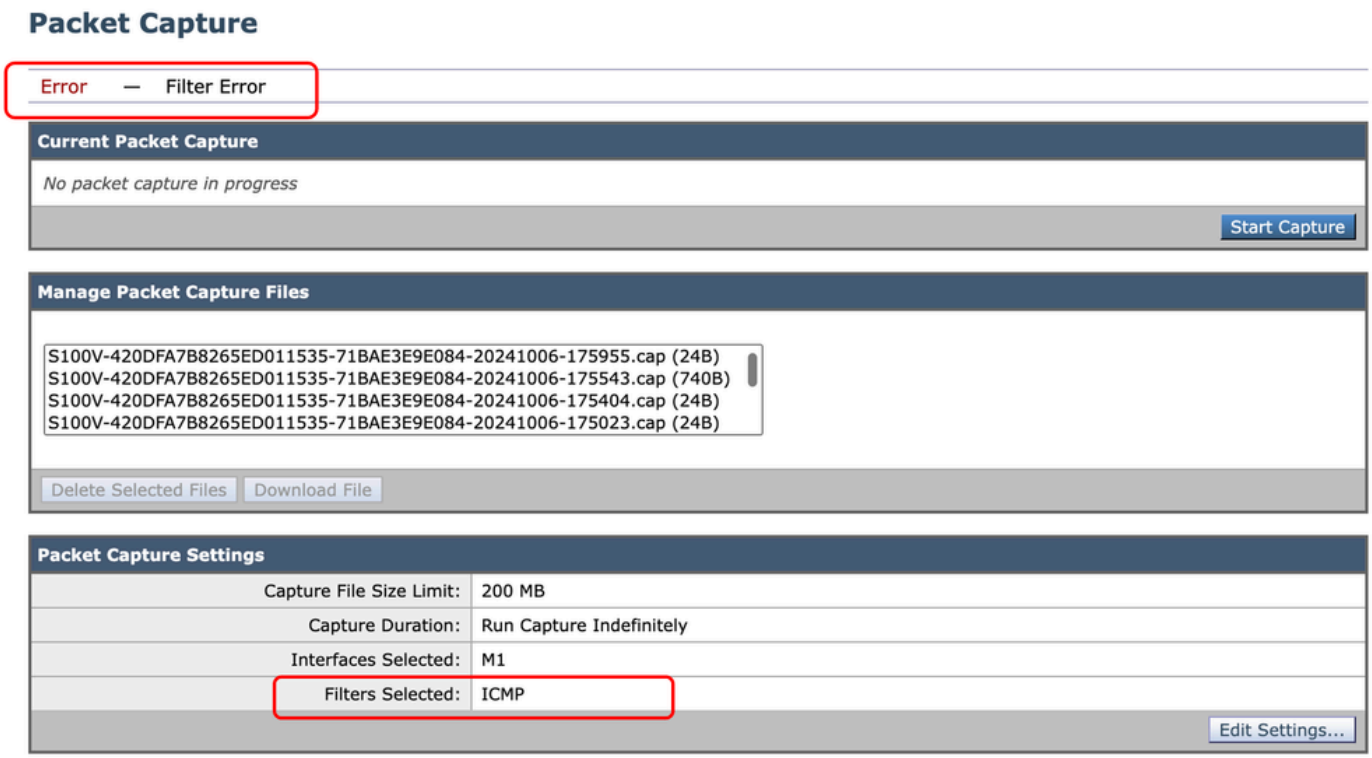
透過型展開のすべてのキャプチャに使用するメインフィルター	(proto gre && ip[40:4] = 0x0a14030f)または (proto gre && ip[44:4] = 0x0a14030f)または (proto gre && ip[40:4] = 0x0a00003c)または (proto gre && ip[44:4] = 0x0a00003c)



注意：すべてのフィルタで大文字と小文字が区別されます。

トラブルシュート

「フィルタエラー」は、パケットキャプチャの実行中に最もよく発生するエラーの1つです。



イメージ – フィルタエラー

このエラーは通常、誤ったフィルタの実装に関連しています。前記の例では、ICMPフィルタが大文字で設定されています。これがFilter Errorを受信する理由です。この問題を解決するには、フィルタを編集して、ICMPをicmpに置き換える必要があります。

関連情報

- AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド – GD(General Deployment) – エンドユーザライセンスの分類…

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。