Configurar a captura de pacotes no dispositivo de segurança de conteúdo

Contents

Introdução

Este documento descreve a captura de pacotes no Cisco Secure Web Appliance (SWA), Email Security Appliance (ESA) e Security Management Appliance (SMA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração do Cisco Content Security Appliance.

A Cisco recomenda que você:

- SWA/ESA/SMA físico ou virtual instalado.
- Acesso administrativo à interface gráfica do usuário (GUI) SWA/ESA/SMA.

- Acesso administrativo à interface de linha de comando (CLI) SWA/ESA/SMA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Executar Captura de Pacotes a partir da GUI

Para executar a captura de pacotes da GUI, use estas etapas:

Etapa 1. Faça login na GUI.

Etapa 2. No canto superior direito da página, selecione Support and Help.

Etapa 3. Selecione Captura de pacotes.

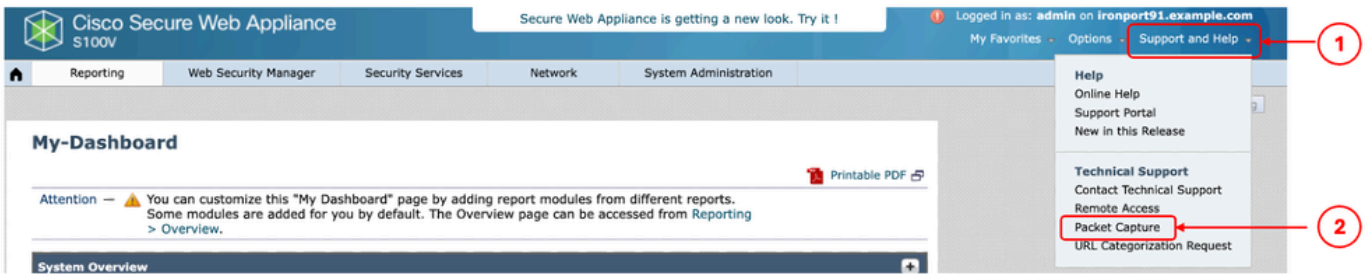


Imagem - Captura de pacotes

Etapa 4. (Opcional) Para editar o filtro atual, escolha Editar configurações. (Para obter mais informações sobre os filtros, consulte a seção Filtros neste documento)

Etapa 5. Inicie a captura.

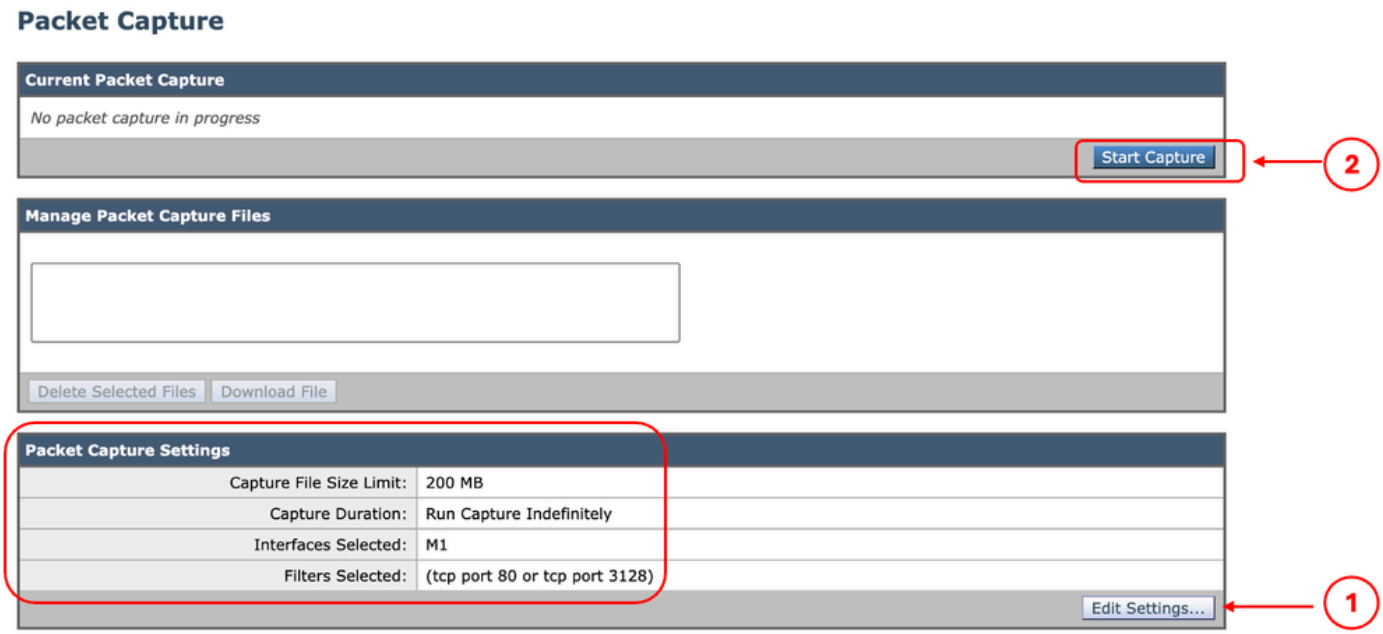
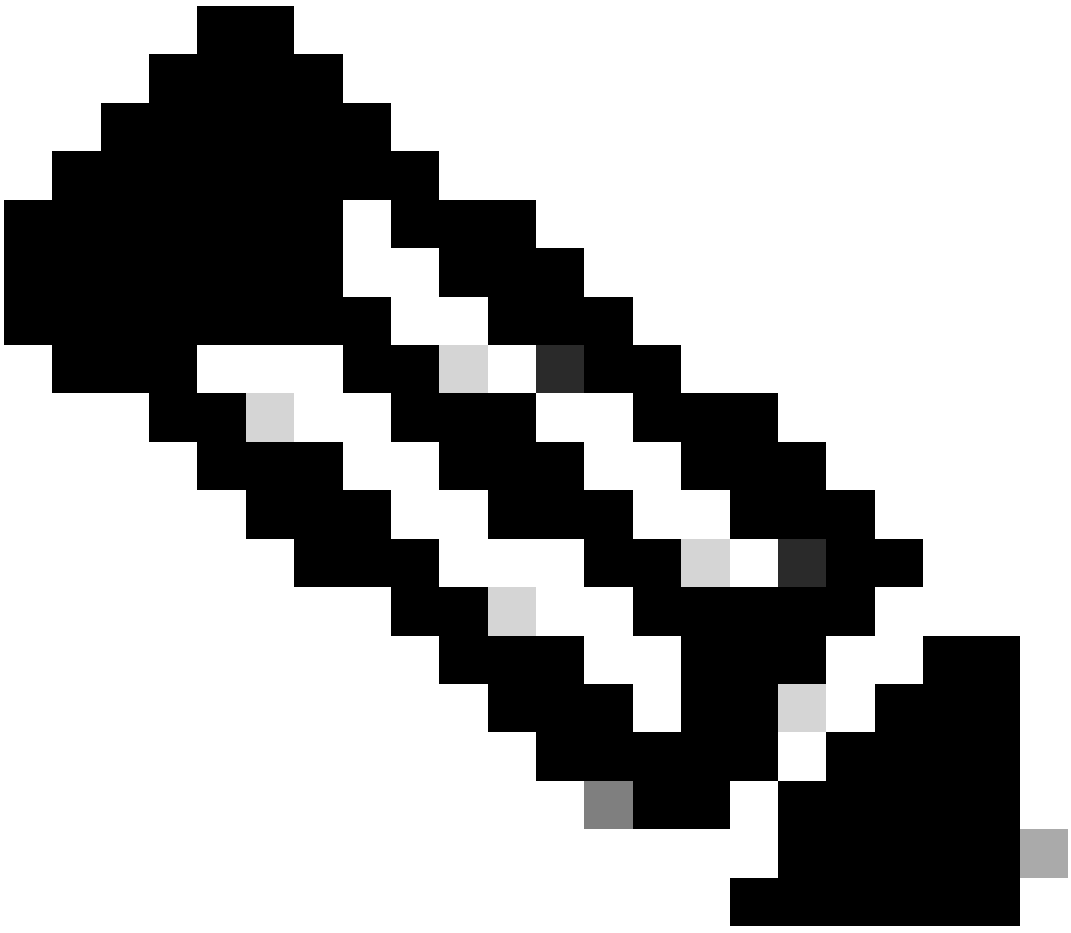


Imagem - Status e filtros da captura de pacotes



Observação: o limite de tamanho do arquivo de Captura de Pacotes é de 200 MB. Quando o tamanho do arquivo atingiu 200 MB, a Captura de Pacotes é interrompida.

A seção Captura de pacote atual mostra o status da Captura de pacote, incluindo o tamanho do arquivo e os filtros aplicados.

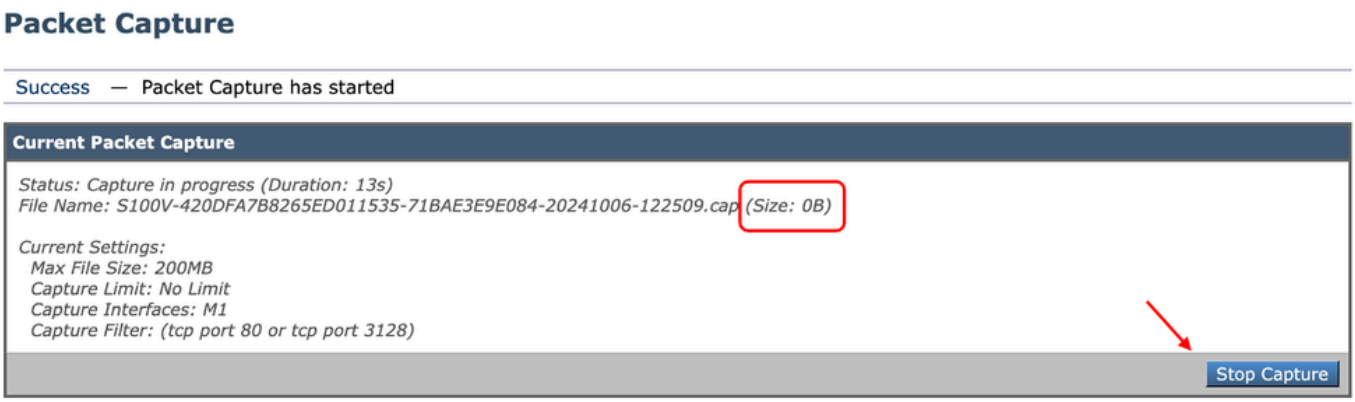
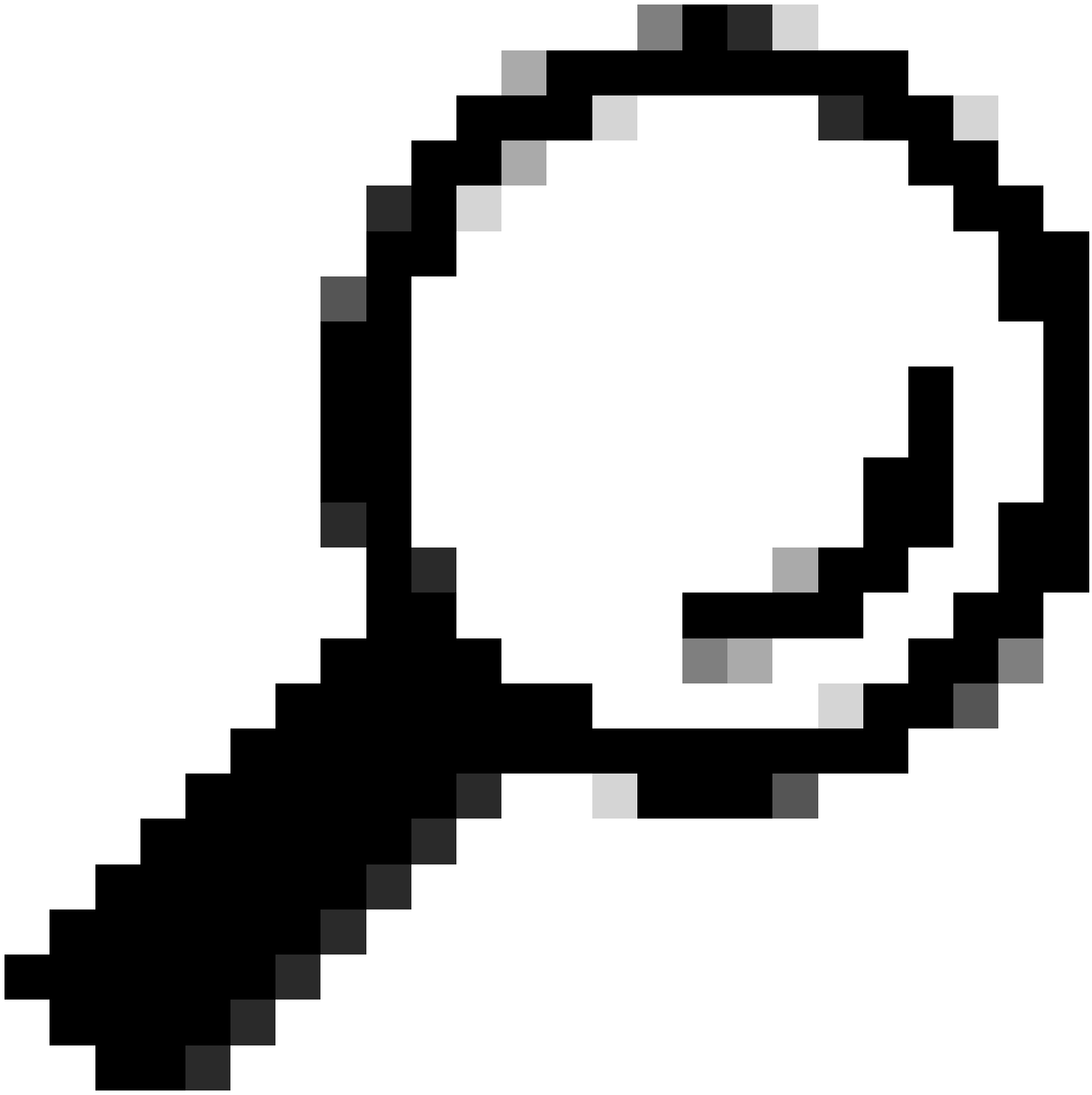


Imagem - Status de captura de pacote

Etapa 6. Para interromper a execução da captura de pacotes, clique em Stop Capture.

Passo 7. Para baixar o arquivo de Captura de Pacotes, escolha o arquivo na lista Gerenciar Arquivos de Captura de Pacotes e clique em Baixar Arquivo.

Imagem - Captura de pacote de download



Dica: o arquivo mais recente está localizado no topo da lista.

Etapa 8. (Opcional) Para excluir qualquer arquivo de Captura de Pacotes, escolha o arquivo na lista Gerenciar Arquivos de Captura de Pacotes e clique em Excluir Arquivos Selecionados.

Executar captura de pacotes a partir do CLI

Você também pode iniciar a Captura de pacotes a partir do CLI usando estas etapas:

Etapa 1. Faça login na CLI.

Etapa 2. Digite packetcapture e pressione Enter.

Etapa 3. (Opcional) Para editar o tipo de filtro atual SETUP. (Para obter mais informações sobre

os filtros, consulte a seção Filtros neste documento.)

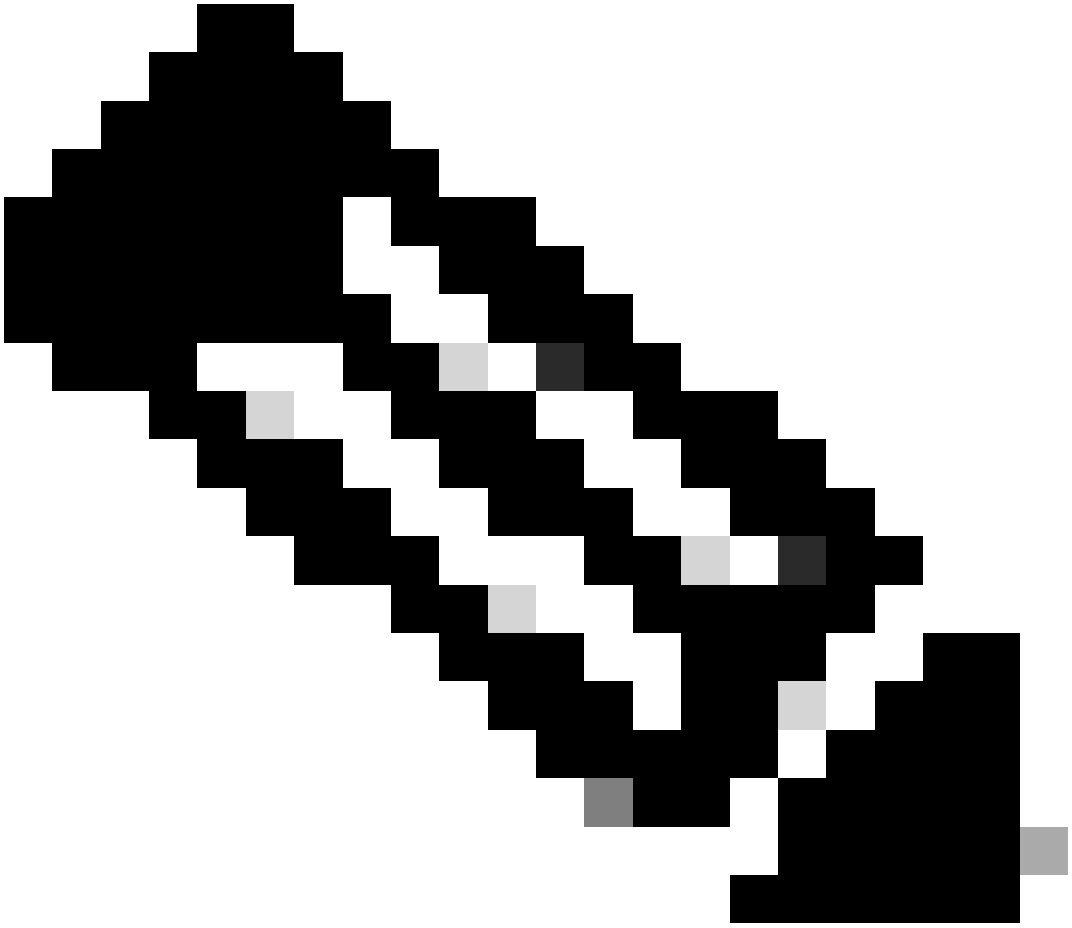
Etapa 4. Escolha START para iniciar a captura.

```
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.
```

Etapa 5. (Opcional) Você pode exibir o status da Captura de Pacotes escolhendo STATUS:

```
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)
```

Etapa 6. Para interromper a Captura de Pacotes, digite STOP e pressione Enter:



Observação: para baixar os arquivos de Captura de Pacotes coletados da CLI, você pode baixá-los da GUI ou conectar-se ao dispositivo via FTP e baixá-los da pasta Capturas.

Filtros

Aqui estão alguns guias sobre os filtros que você pode usar nos dispositivos de segurança de conteúdo.

Filtrar por endereço IP do host

Filtrar por IP do host na GUI

Para filtrar por endereço IP do host, na GUI, há duas opções:

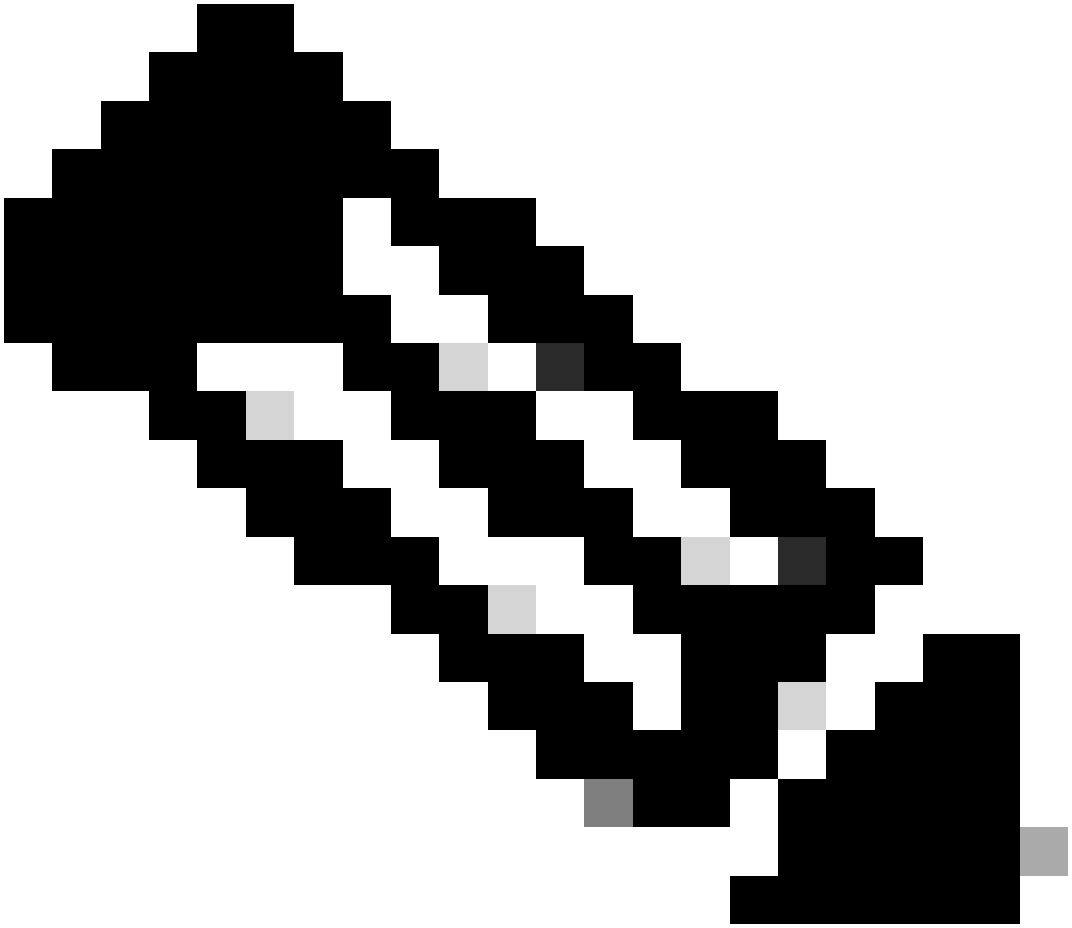
- Filtros predefinidos
- Filtros personalizados

Para usar filtros predefinidos na GUI:

Etapa 1. Na página Captura de pacotes, escolha Editar configurações.

Etapa 2. Em Packet Capture Filters, selecione Predefined Filters.

Etapa 3. Você pode inserir o endereço IP na seção IP do cliente ou IP do servidor.



Observação: escolher entre IP do cliente ou IP do servidor não está limitado ao endereço origem ou ao endereço destino. Esse filtro captura todos os pacotes com o endereço IP definido como origem ou destino.

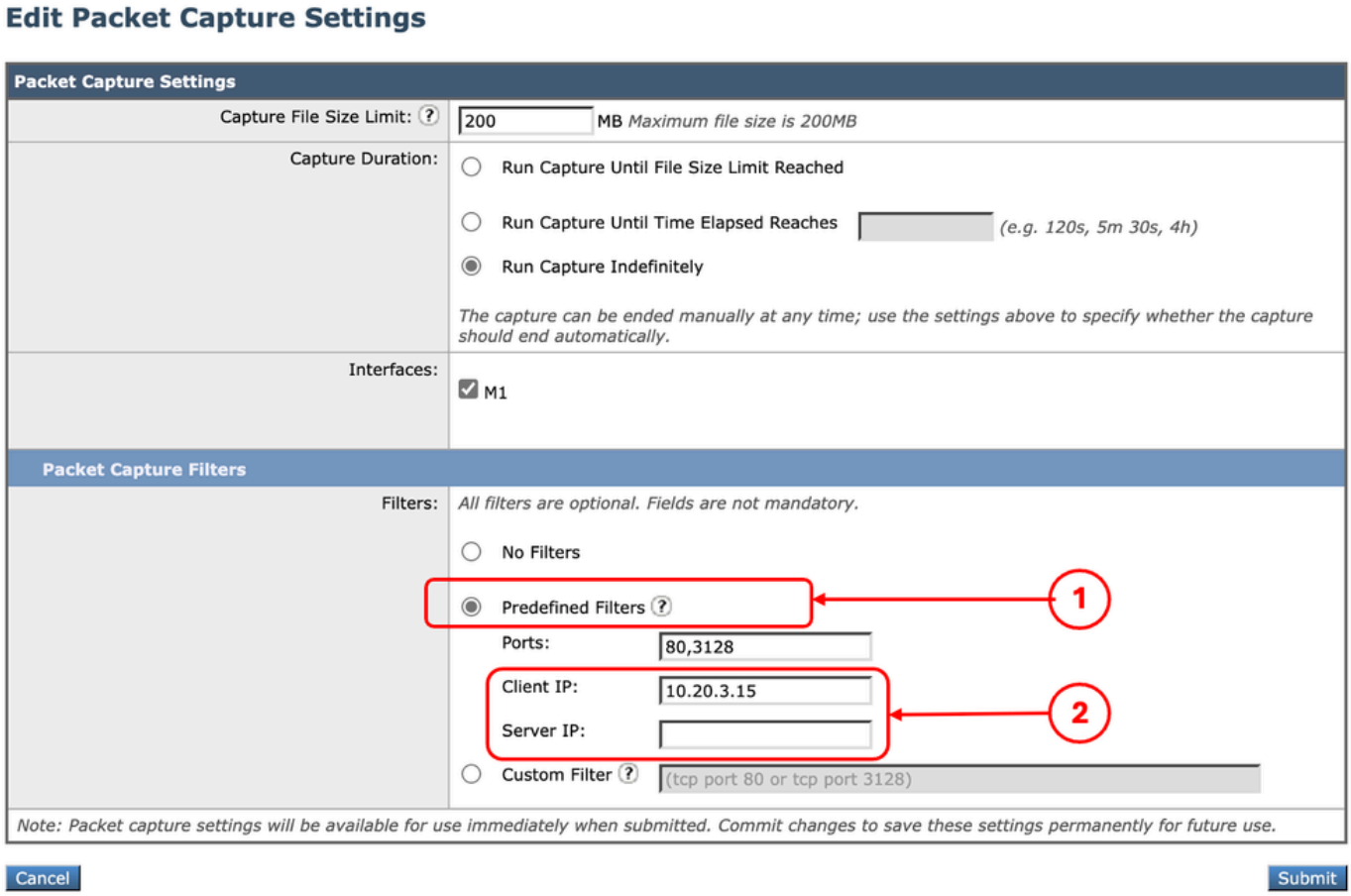
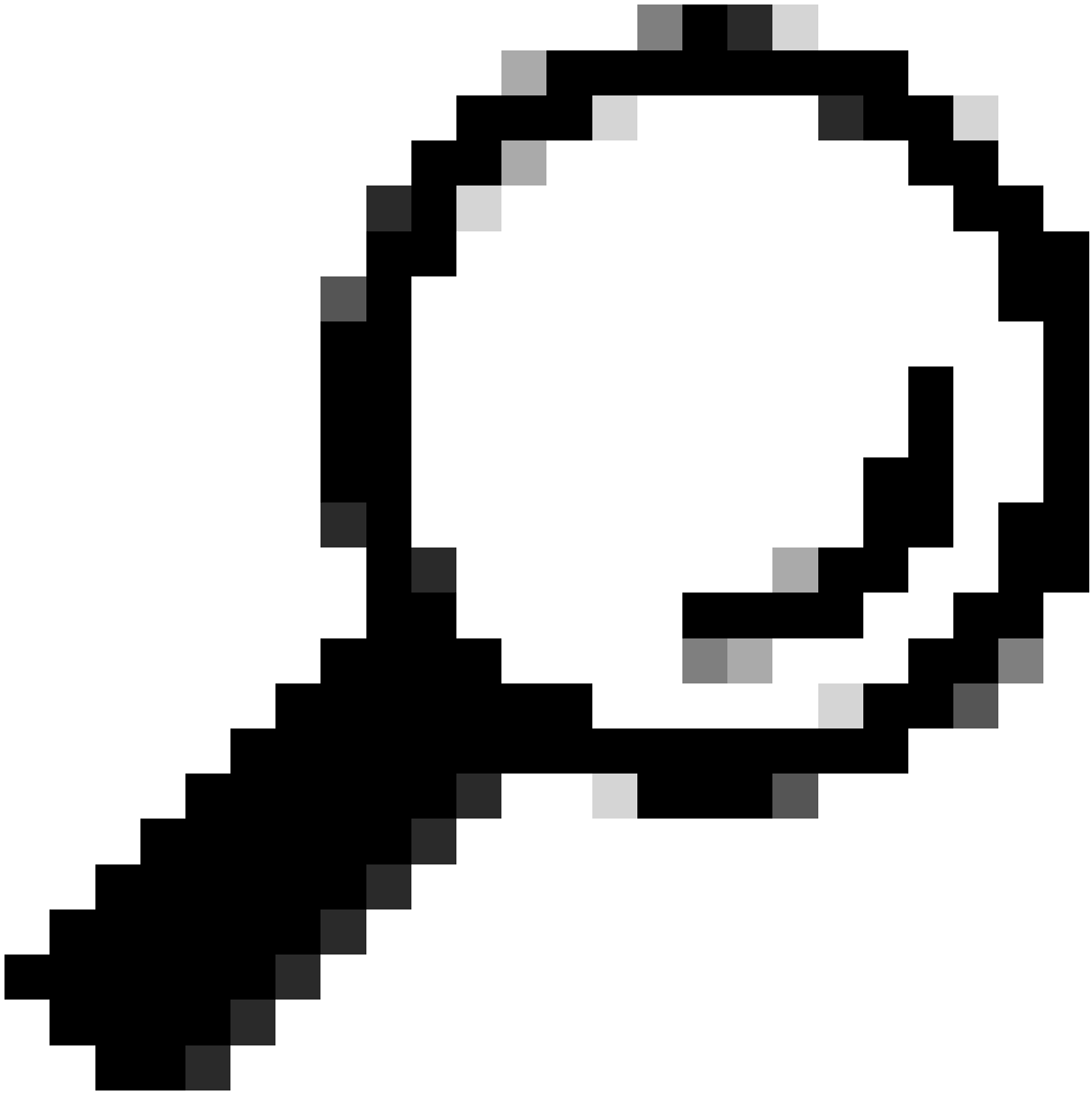


Imagem - Filtrar por IP do host a partir de filtros predefinidos da GUI

Etapa 4. Envie as alterações.

Etapa 5. Inicie a captura.



Dica: não é necessário confirmar as alterações, o filtro recém-adicionado aplicado à captura atual. A confirmação das alterações ajuda a salvar o filtro para uso futuro.

Para usar Filtros personalizados e Filtros predefinidos da GUI:

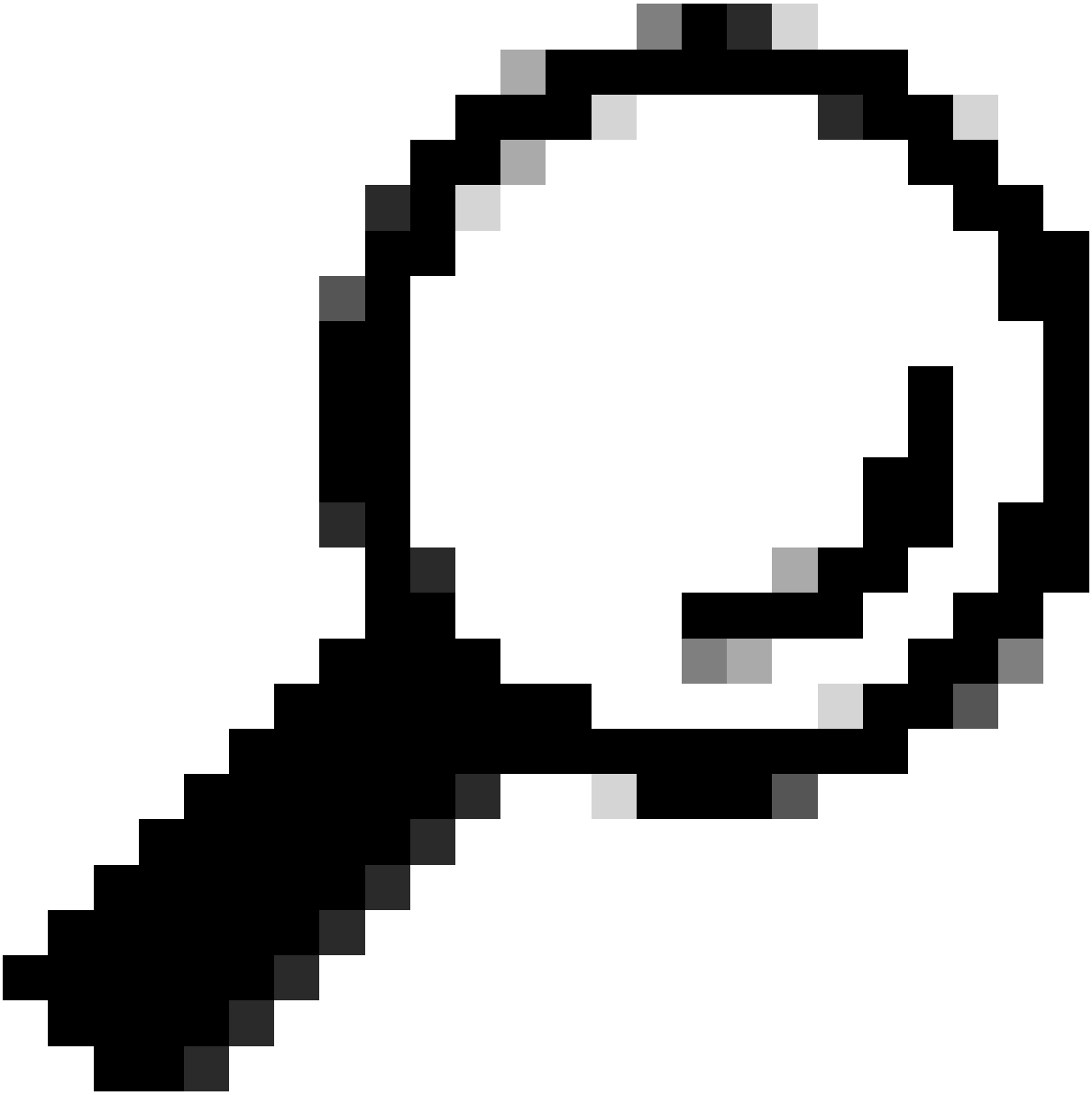
Etapa 1. Na página Captura de pacotes, escolha Editar configurações.

Etapa 2. Em Packet Capture Filters, selecione Custom Filter.

Etapa 3. Use a sintaxe do host seguida pelo endereço IP.

Aqui está um exemplo para filtrar todo o tráfego com o endereço IP origem ou destino 10.20.3.15

```
host 10.20.3.15
```



Dica: para filtrar por mais de um endereço IP, você pode usar operandos lógicos como or e and (somente letras minúsculas).

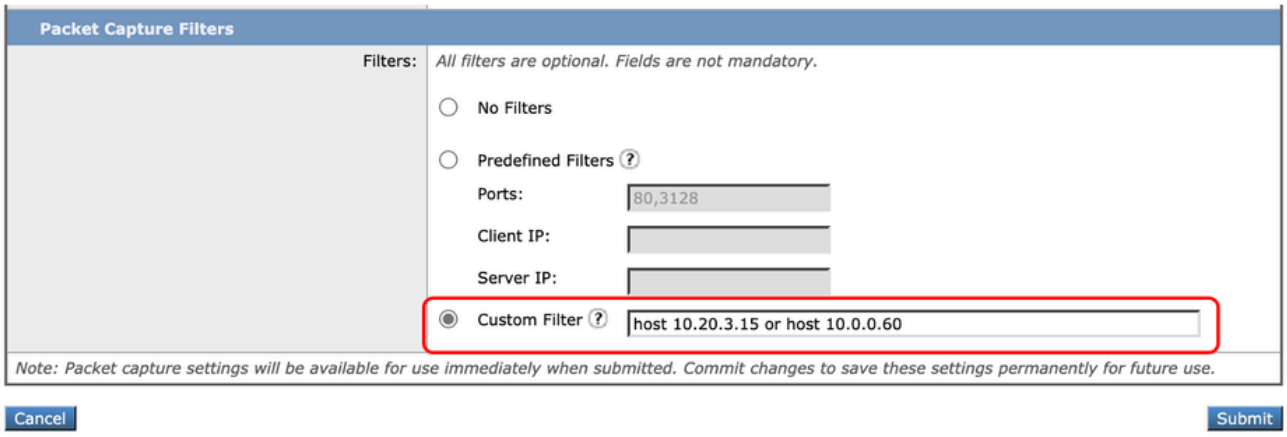


Imagem - Filtro Personalizado para dois endereços IP

Etapa 4. Envie as alterações.

Etapa 5. Iniciar a captura

Filtrar por IP do host na CLI

Para filtrar pelo endereço IP do host da CLI:

Etapa 1. Faça login na CLI.

Etapa 2. Digite packetcapture e pressione Enter.

Etapa 3. Para editar o tipo de filtro atual, digite SETUP.

Etapa 4. Responda às perguntas até chegar Inserir o filtro a ser usado para a captura

Etapa 5. Você pode usar a mesma sequência de caracteres de filtro que o filtro personalizado na GUI.

Este é um exemplo de filtragem de todo o tráfego com o endereço IP origem ou destino 10.20.3.15 ou 10.0.0.60

```
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
```

Filtrar por número de porta

Filtrar por número de porta na GUI

Para filtrar por número(s) de porta, na GUI, há duas opções:

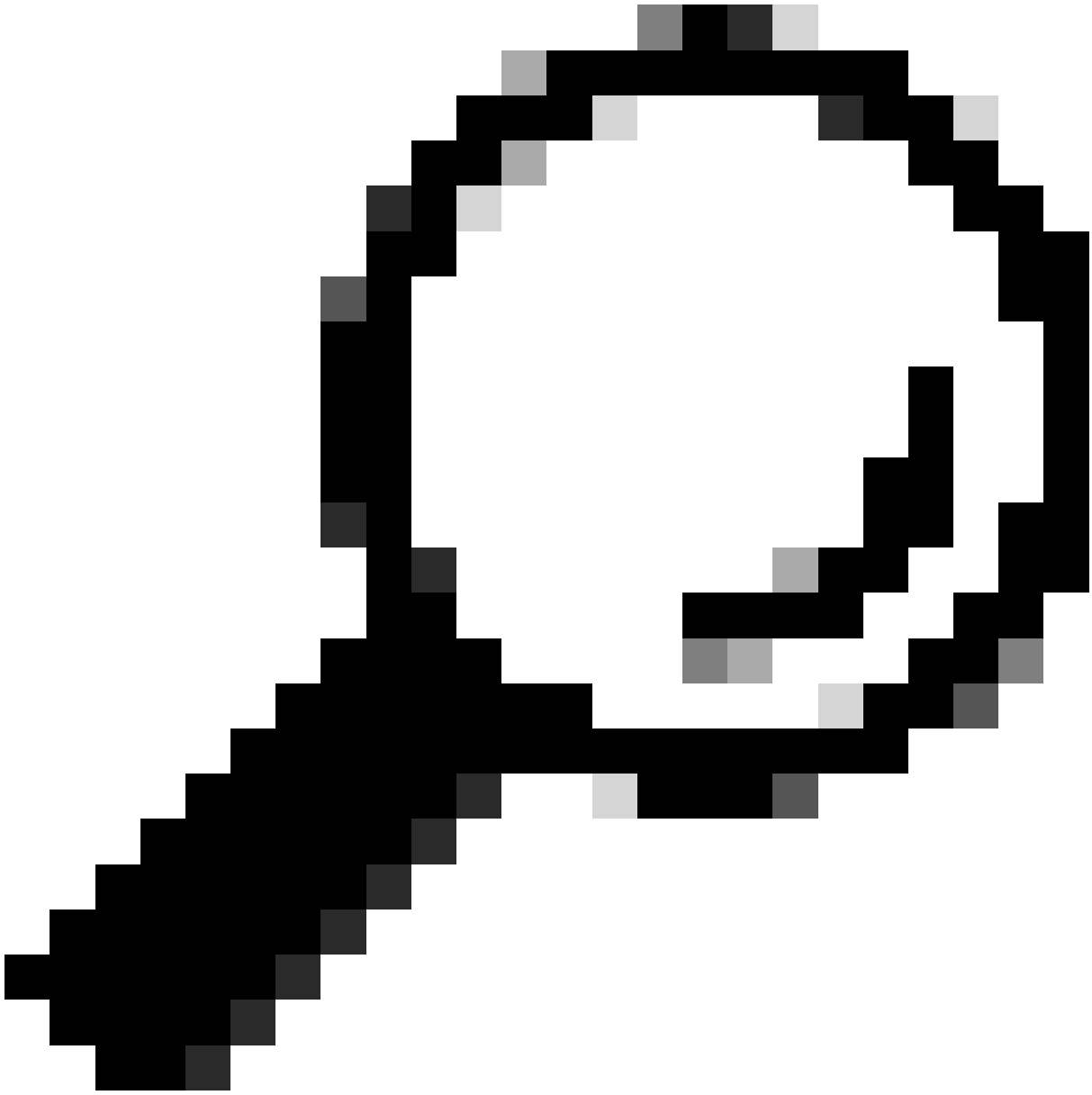
- Filtros predefinidos
- Filtros personalizados

Para usar filtros predefinidos da GUI:

Etapa 1. Na página Captura de pacotes, escolha Editar configurações.

Etapa 2. Em Packet Capture Filters, selecione Predefined Filters.

Etapa 3. Na seção Portas, digite os números de porta que deseja filtrar.



Dica: você pode adicionar vários números de porta separando-os com vírgula " , ".

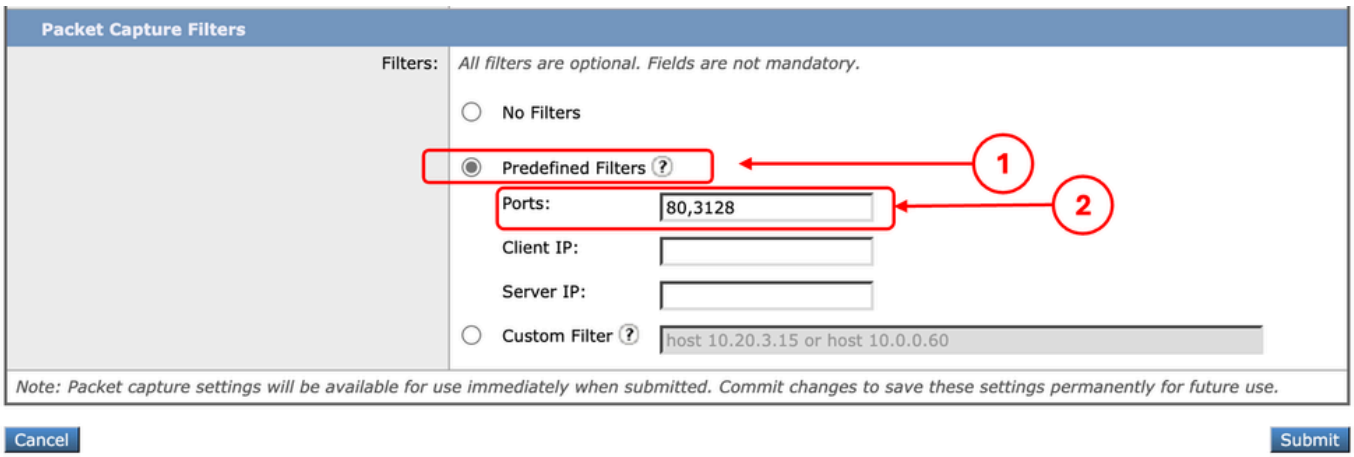
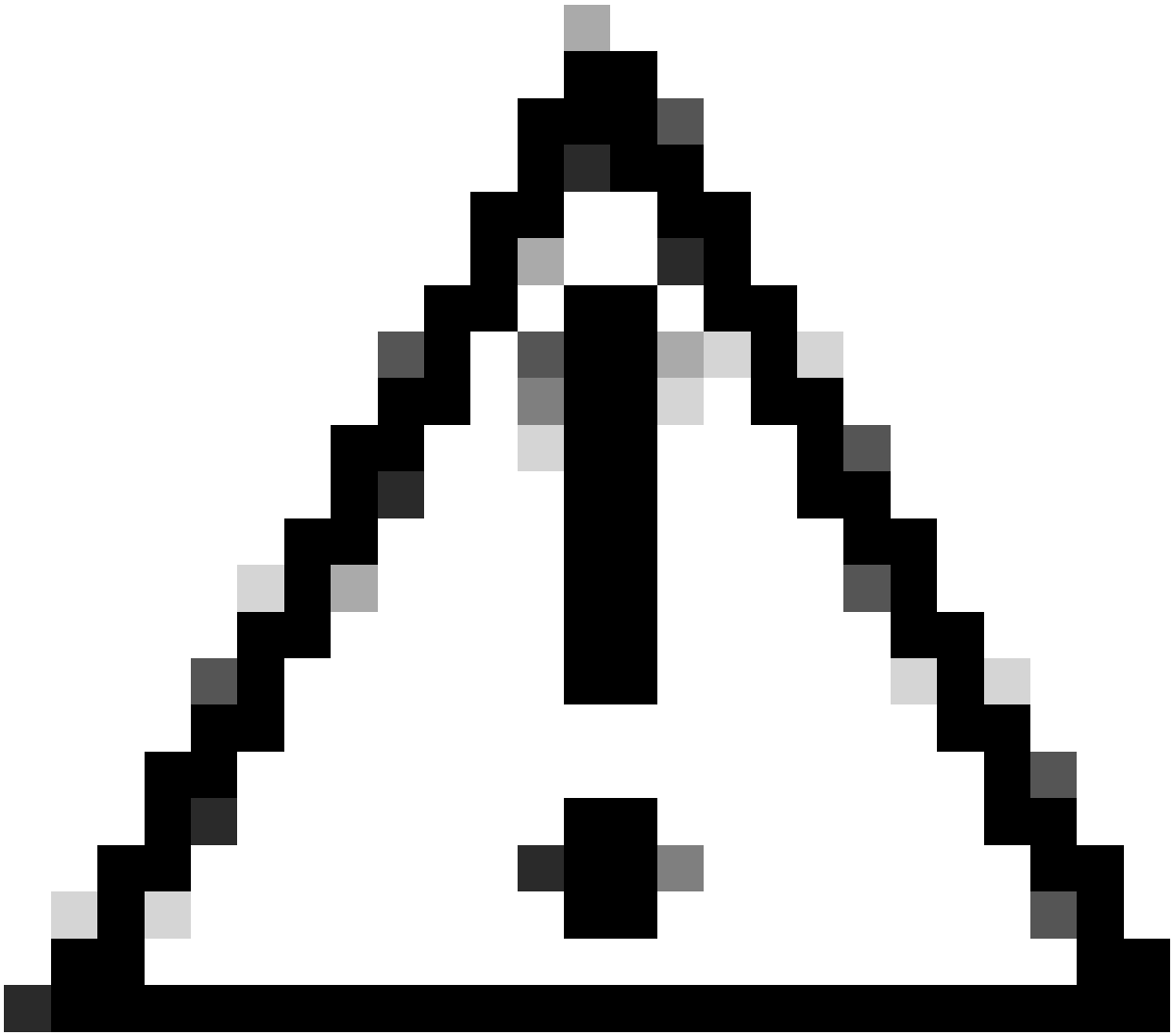


Imagem - Filtrar por número de porta

Etapa 4. Envie as alterações.

Etapa 5. Inicie a captura.



Cuidado: essa abordagem captura somente o tráfego TCP com os números de porta definidos. Para capturar o tráfego UDP, use o Filtro personalizado.

Para usar Filtros personalizados da GUI:

Etapa 1. Na página Captura de pacotes, escolha Editar configurações.

Etapa 2. Em Packet Capture Filters, selecione Custom Filter.

Etapa 3. Use a sintaxe de porta seguida pelo número da porta.

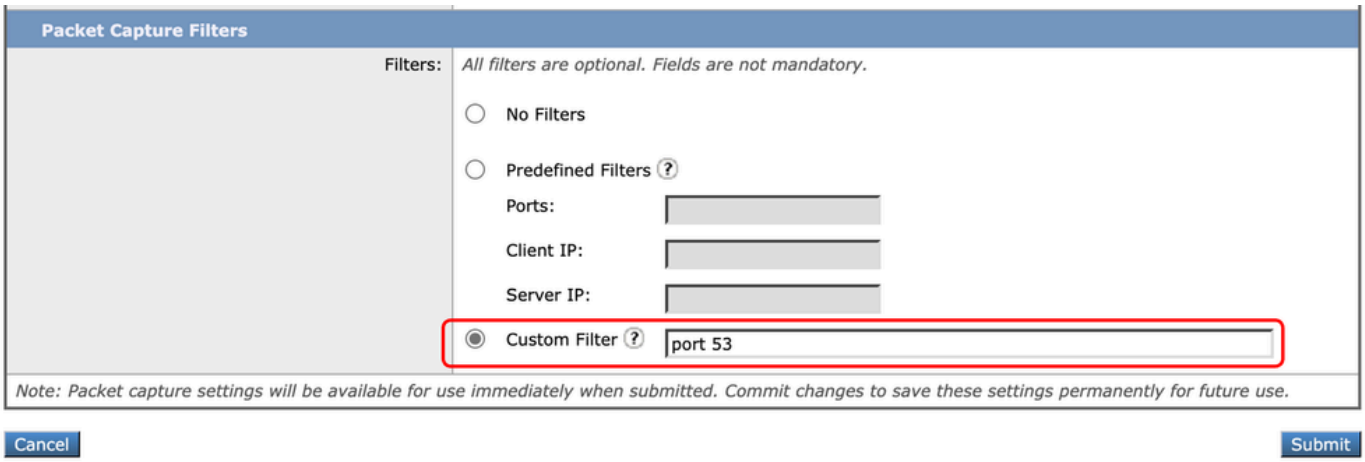
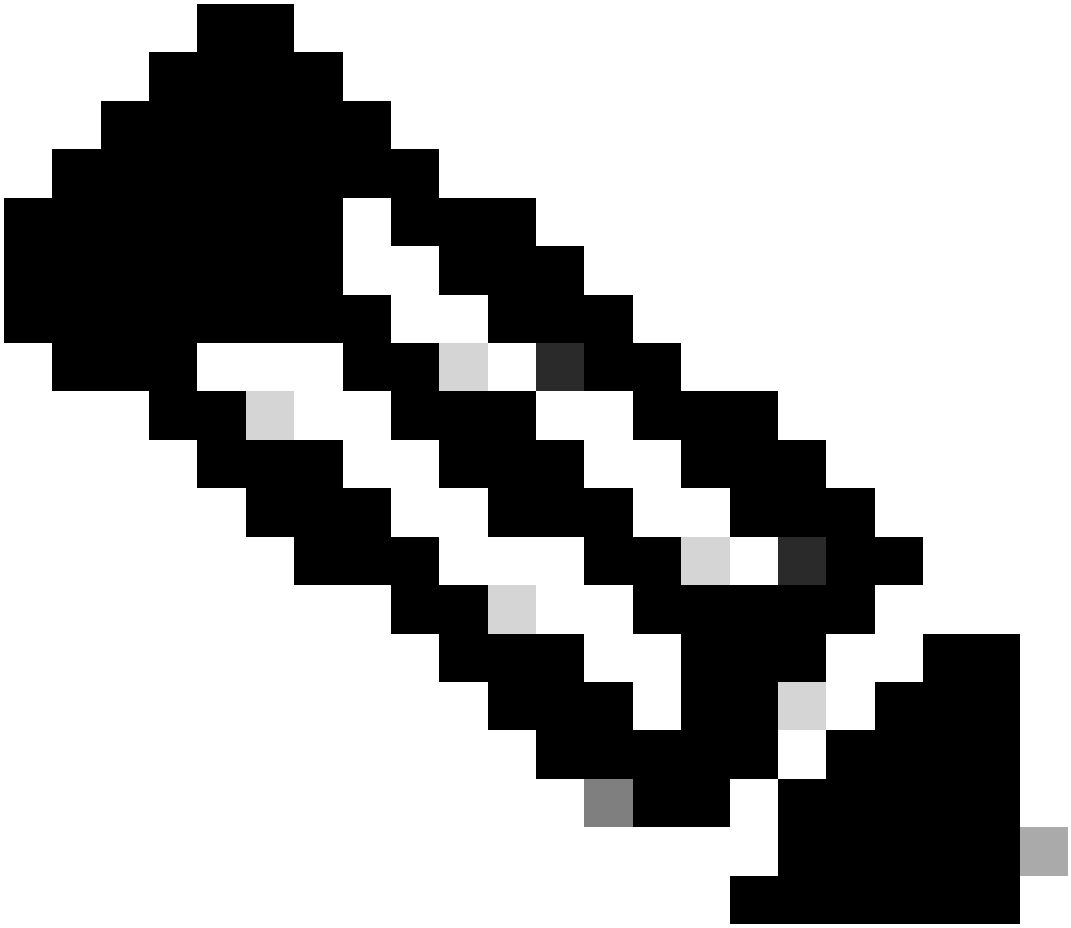


Imagem - Filtro personalizado por número de porta



Observação: se você usar apenas porta, esse filtro cobrirá as portas TCP e UDP.

Etapa 4. Envie as alterações.

Etapa 5. Inicie a captura.

Filtrar por número de porta no CLI

Para filtrar pelo número da porta do CLI:

Etapa 1. Faça login na CLI.

Etapa 2. Digite packetcapture e pressione Enter.

Etapa 3. Para editar o tipo de filtro atual, digite SETUP.

Etapa 4. Responda às perguntas até chegar Inserir o filtro a ser usado para a captura

Etapa 5. Você pode usar a mesma sequência de caracteres de filtro que o filtro personalizado na GUI.

Aqui está um exemplo de filtragem de todo o tráfego com a porta origem ou destino número 53, para portas TCP e UDP:

```
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
```

Filtrar no SWA com implantação transparente

Em SWA com implantação transparente, enquanto a conectividade do protocolo de comunicação

de cache da Web (WCCP) é por meio de túneis Generic Routing Encapsulation (GRE), os endereços IP origem e destino nos pacotes que chegam ou saem do SWA são o endereço IP do roteador e o endereço IP do SWA.

Para poder coletar a Captura de Pacotes com Endereço IP ou Número da Porta da GUI, há duas opções:

- Filtros predefinidos
- Filtros personalizados

Filtrar no SWA com implantação transparente na GUI

Etapa 1. Na página Captura de pacotes, escolha Editar configurações.

Etapa 2. Em Packet Capture Filters, selecione Predefined Filters.

Etapa 3. Você pode inserir o endereço IP na seção IP do cliente ou IP do servidor.

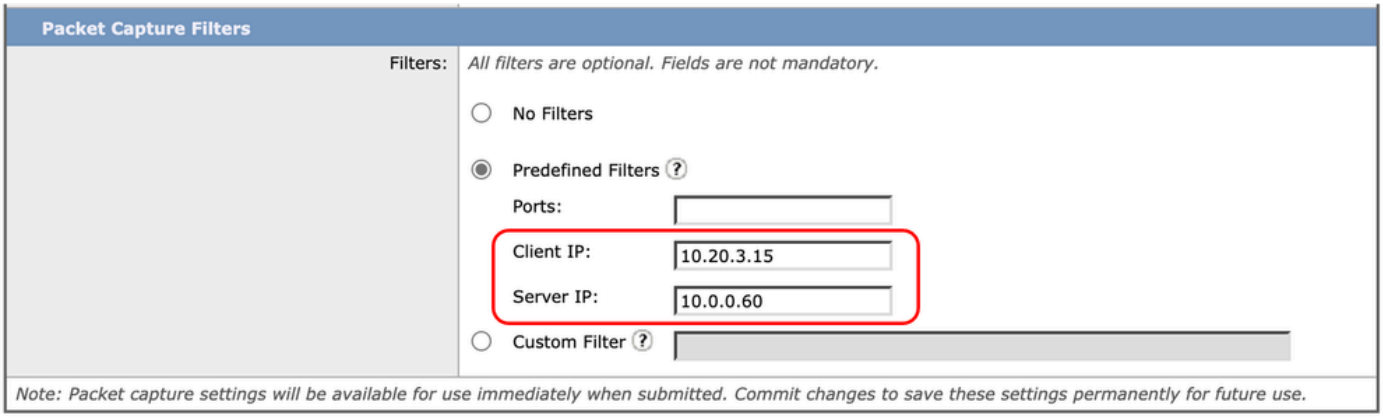
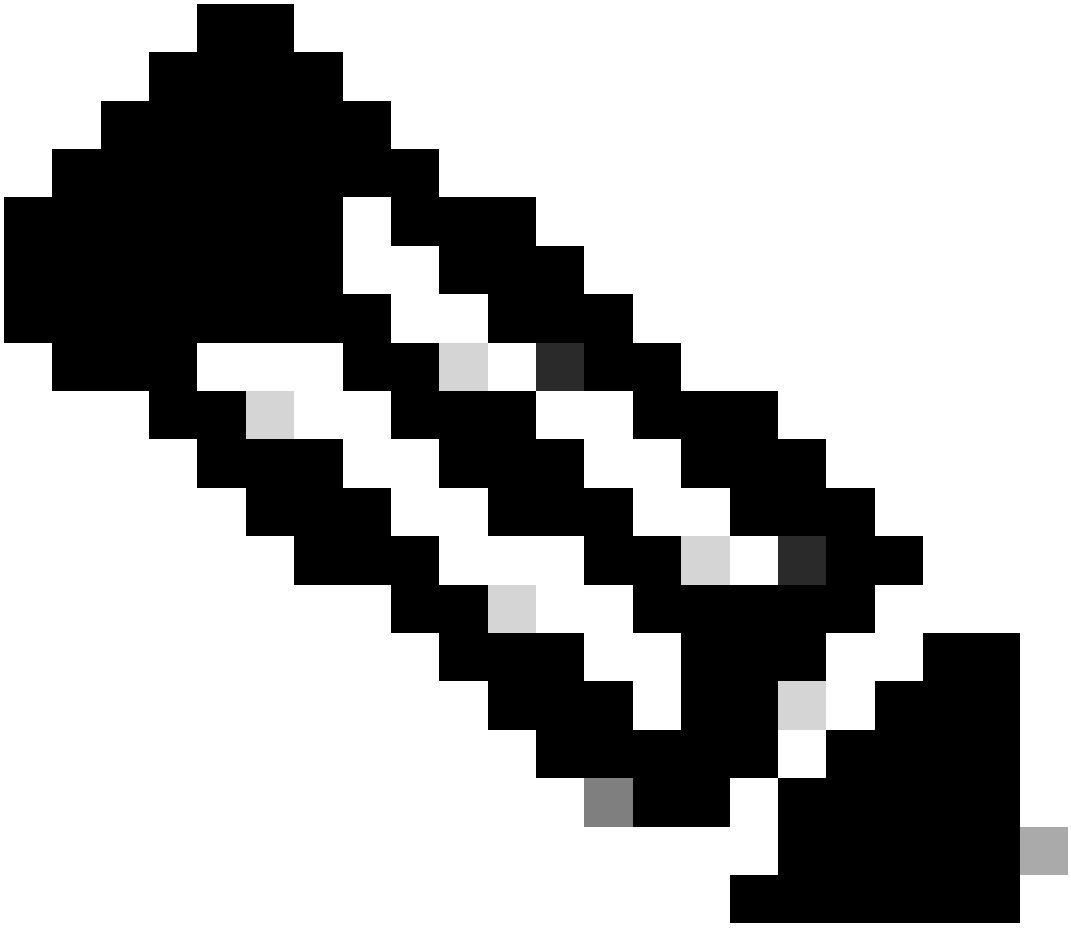


Imagem - Configurando o endereço IP em filtros predefinidos

Etapa 4. Envie as alterações.

Etapa 5. Inicie a captura.



Observação: você pode ver após enviar o filtro, o SWA adicionou condições extras na seção Filtro selecionado.

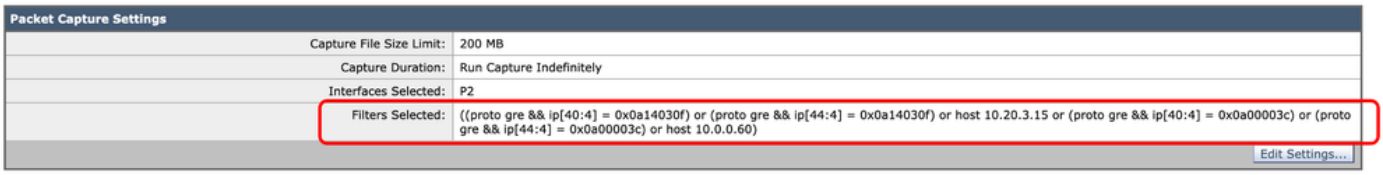


Imagem - Filtros extras adicionados pelo SWA para coletar pacotes dentro do túnel GRE

Para usar Filtros personalizados da GUI:

Etapa 1. Na página Captura de pacotes, escolha Editar configurações.

Etapa 2. Em Packet Capture Filters, selecione Custom Filter

Etapa 3. Adicione essa sequência de caracteres primeiro e, em seguida, o filtro que você planeja implementar adicionando ou depois dessa sequência de caracteres:

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

Por exemplo, se estiver planejando filtrar pelo IP do host igual a 10.20.3.15 ou pelo número da porta igual a 8080, você poderá usar esta string:

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

Etapa 4. Envie as alterações.

Etapa 5. Inicie a captura.

Filtrar no SWA com implantação transparente no CLI

Para filtrar a implantação de proxy transparente da CLI:

Etapa 1. Faça login na CLI.

Etapa 2. Digite packetcapture e pressione Enter.

Etapa 3. Para editar o tipo de filtro atual, digite SETUP.

Etapa 4. Responda às perguntas até chegar Inserir o filtro a ser usado para a captura

Etapa 5. Você pode usar a mesma sequência de caracteres de filtro que o filtro personalizado na GUI.

Aqui está um exemplo para filtrar pelo IP do host igual a 10.20.3.15 ou pelo número de porta igual a 8080:

```
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
```

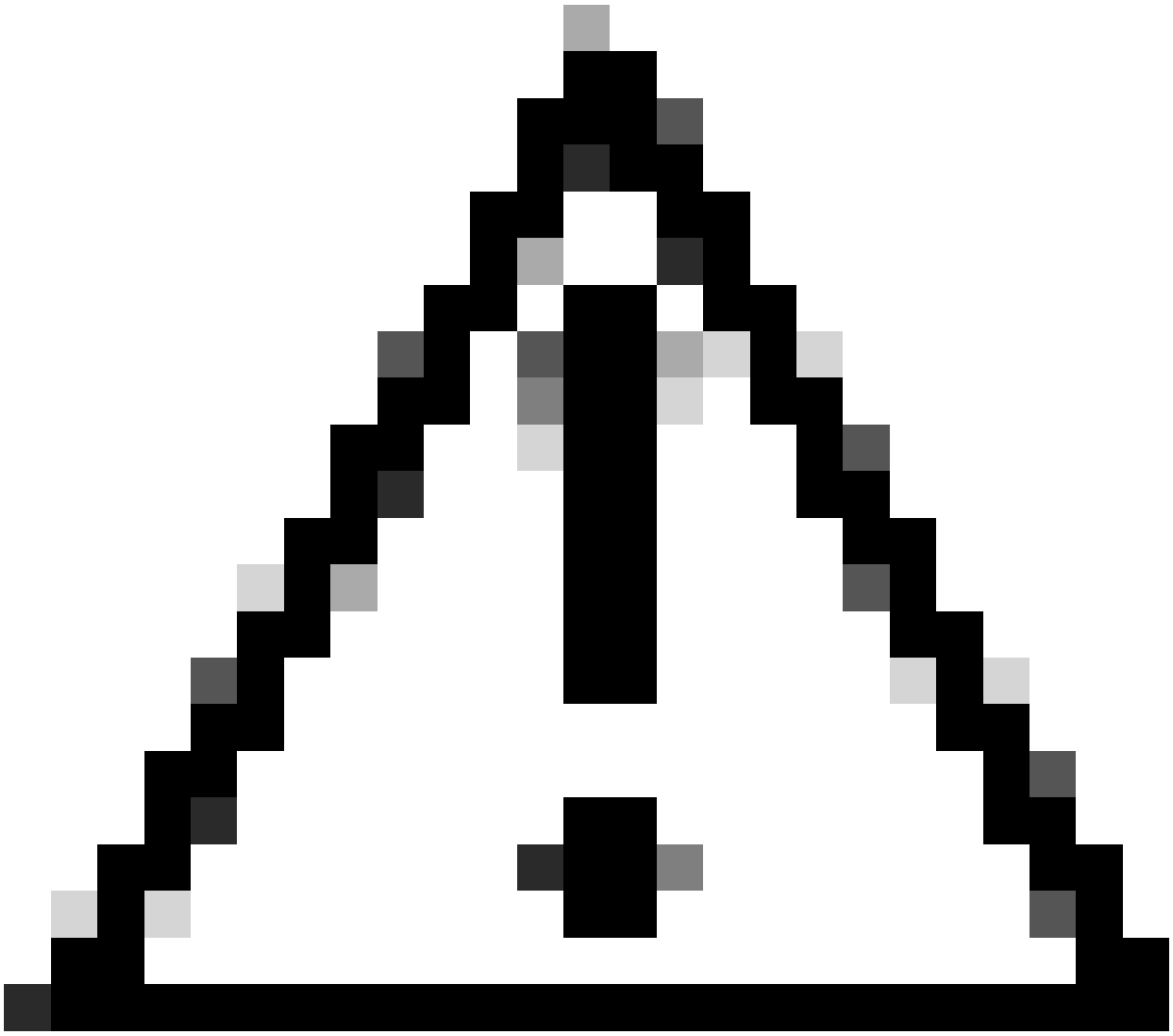
```
[N]>

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
```

Filtros mais comuns

Esta é uma tabela que lista os filtros mais comuns:

Descrição	Filtrar
Filtrar por endereço IP origem igual a 10.20.3.15	src host 10.20.3.15
Filtrar por endereço IP destino igual a 10.20.3.15	dst host 10.20.3.15
Filtrar por endereço IP origem igual a 10.20.3.15 e endereço IP destino igual a 10.0.0.60	(host src 10.20.3.15) e (host dst 10.0.0.60)
Filtrar por endereço IP origem ou destino igual a 10.20.3.15	host 10.20.3.15
Filtrar por endereço IP origem ou destino igual a 10.20.3.15 ou igual a 10.0.0.60	host 10.20.3.15 ou host 10.0.0.60
Filtrar por número de porta TCP igual a 8080	porta TCP 8080
Filtrar por número de porta UDP igual a 53	porta udp 53
Filtrar por número de porta igual a 514 (TCP ou UDP)	porta 514
Filtrar somente pacotes UDP	udp

Filtrar somente pacotes ICMP	icmp
Filtro principal a ser usado para cada captura na implantação transparente	(proto gre && ip[40:4] = 0x0a14030f) ou (proto gre && ip[44:4] = 0x0a14030f) ou (proto gre && ip[40:4] = 0x0a00003c) ou (proto gre && ip[44:4] = 0x0a00003c)



Cuidado: todos os filtros diferenciam maiúsculas de minúsculas.

Troubleshooting

"Erro de filtro" é um dos erros mais comuns ao executar a captura de pacotes.

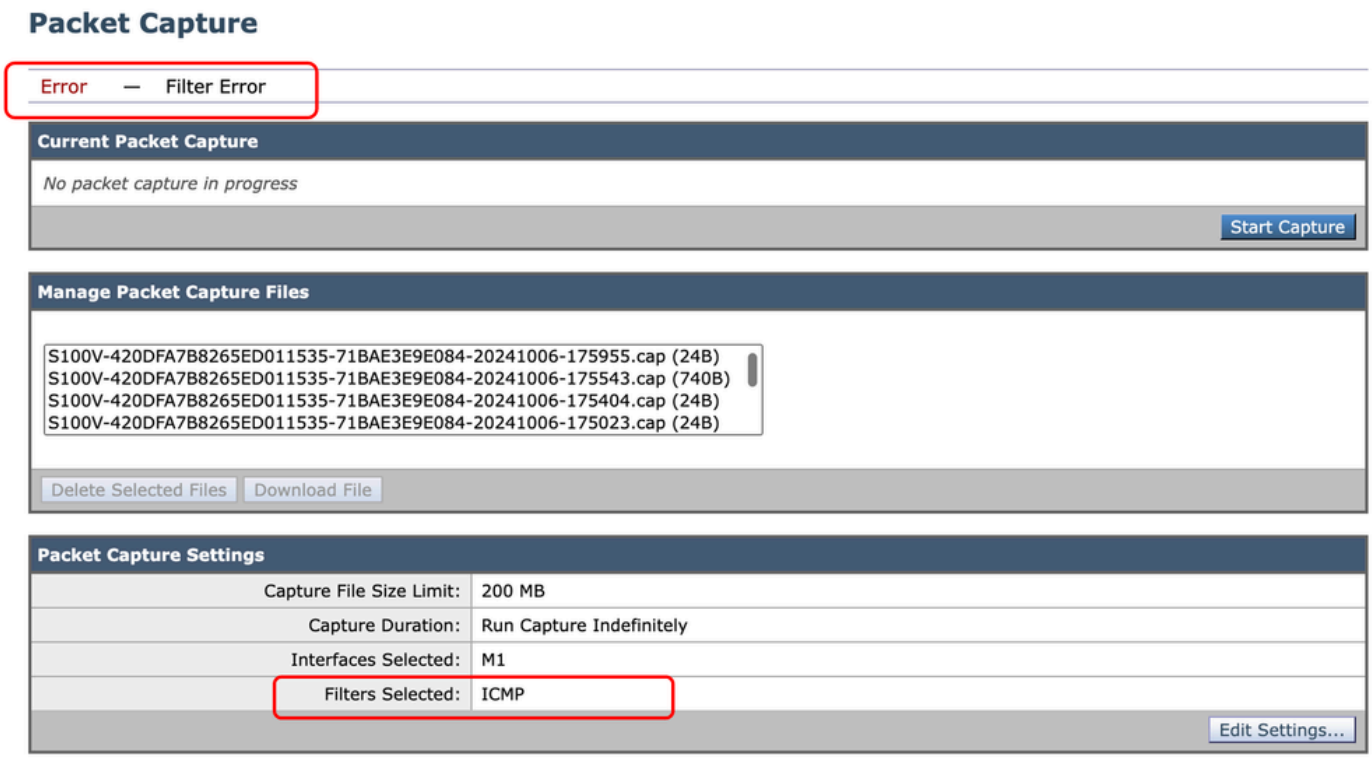


Imagem - Erro de filtro

Esse erro geralmente está relacionado à implementação incorreta do filtro. No exemplo anterior, o filtro ICMP tem caracteres maiúsculos. É por isso que você está recebendo Filter Error. Para corrigir esse problema, você precisa editar o filtro e substituir o ICMP por icmp.

Informações Relacionadas

- Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - GD (General Deployment) - Classify End-U...

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.