

# Configuración de la captura de paquetes en el dispositivo de seguridad de contenido

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Realizar captura de paquetes desde la GUI](#)

[Realizar captura de paquetes desde CLI](#)

[Filtros](#)

[Filtrar por dirección IP de host](#)

[Filtrar por IP de host en la GUI](#)

[Filtrar por IP de host en CLI](#)

[Filtrar por número de puerto](#)

[Filtrar por número de puerto en la GUI](#)

[Filtrar por número de puerto en CLI](#)

[Filtro en SWA con implementación transparente](#)

[Filtro en SWA con implementación transparente en GUI](#)

[Filtro en SWA con implementación transparente en CLI](#)

[Filtros más comunes](#)

[Troubleshoot](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe la captura de paquetes en Cisco Secure Web Appliance (SWA), Email Security Appliance (ESA) y Security Management Appliance (SMA).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de Cisco Content Security Appliance.

Cisco recomienda que tenga:

- SWA/ESA/SMA físico o virtual instalado.
- Acceso administrativo a la interfaz gráfica de usuario (GUI) SWA/ESA/SMA.

- Acceso administrativo a la interfaz de línea de comandos (CLI) SWA/ESA/SMA

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Realizar captura de paquetes desde la GUI

Para realizar la captura de paquetes desde la GUI, siga estos pasos:

Paso 1. Inicie sesión en la GUI.

Paso 2. En la parte superior derecha de la página, seleccione Soporte y Ayuda.

Paso 3. Seleccione Captura de paquetes.

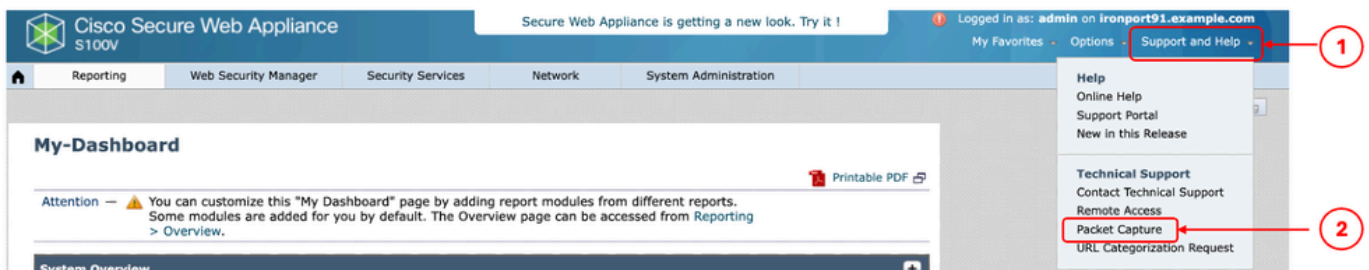


Imagen - Captura de paquetes

Paso 4. (Opcional) Para editar el filtro actual, seleccione Editar configuración. (Para obtener más información sobre los filtros, consulte la sección Filtros de este documento)

Paso 5. Inicie la captura.

## Packet Capture

**Current Packet Capture**

No packet capture in progress

[Start Capture](#) 2

**Manage Packet Capture Files**

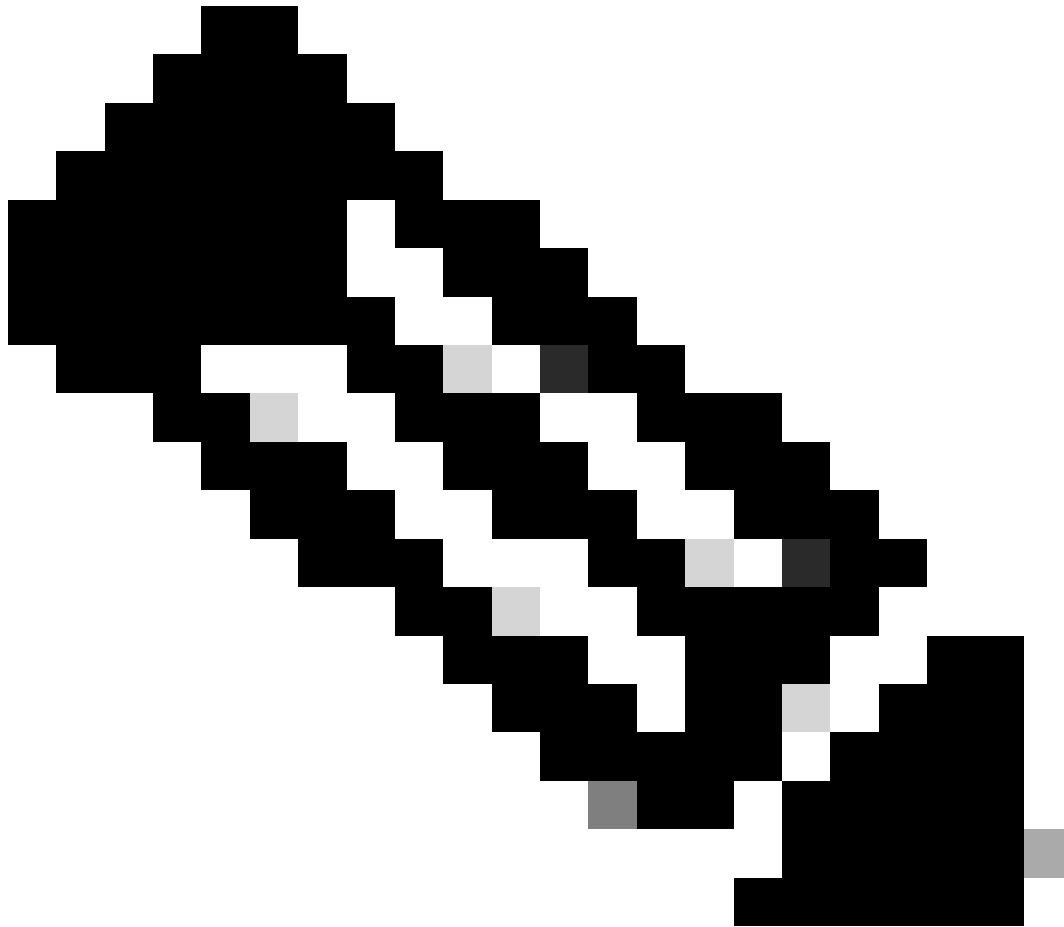
[Delete Selected Files](#) [Download File](#)

**Packet Capture Settings**

Capture File Size Limit:	200 MB
Capture Duration:	Run Capture Indefinitely
Interfaces Selected:	M1
Filters Selected:	(tcp port 80 or tcp port 3128)

[Edit Settings...](#) 1

Imagen: estado y filtros de captura de paquetes



Nota: El límite de tamaño del archivo de captura de paquetes es de 200 MB. Cuando el tamaño del archivo alcanza los 200 MB, la captura de paquetes se detiene.

La sección Captura de paquetes actual muestra el estado de la captura de paquetes, incluido el tamaño del archivo y los filtros aplicados.

## Packet Capture

Success — Packet Capture has started

---

**Current Packet Capture**

Status: Capture in progress (Duration: 13s)  
File Name: S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-122509.cap (Size: 0B)

Current Settings:  
Max File Size: 200MB  
Capture Limit: No Limit  
Capture Interfaces: M1  
Capture Filter: (tcp port 80 or tcp port 3128)

Stop Capture

Imagen - Estado de captura de paquetes

Paso 6. Para detener la captura de paquetes en ejecución, haga clic en Detener captura.

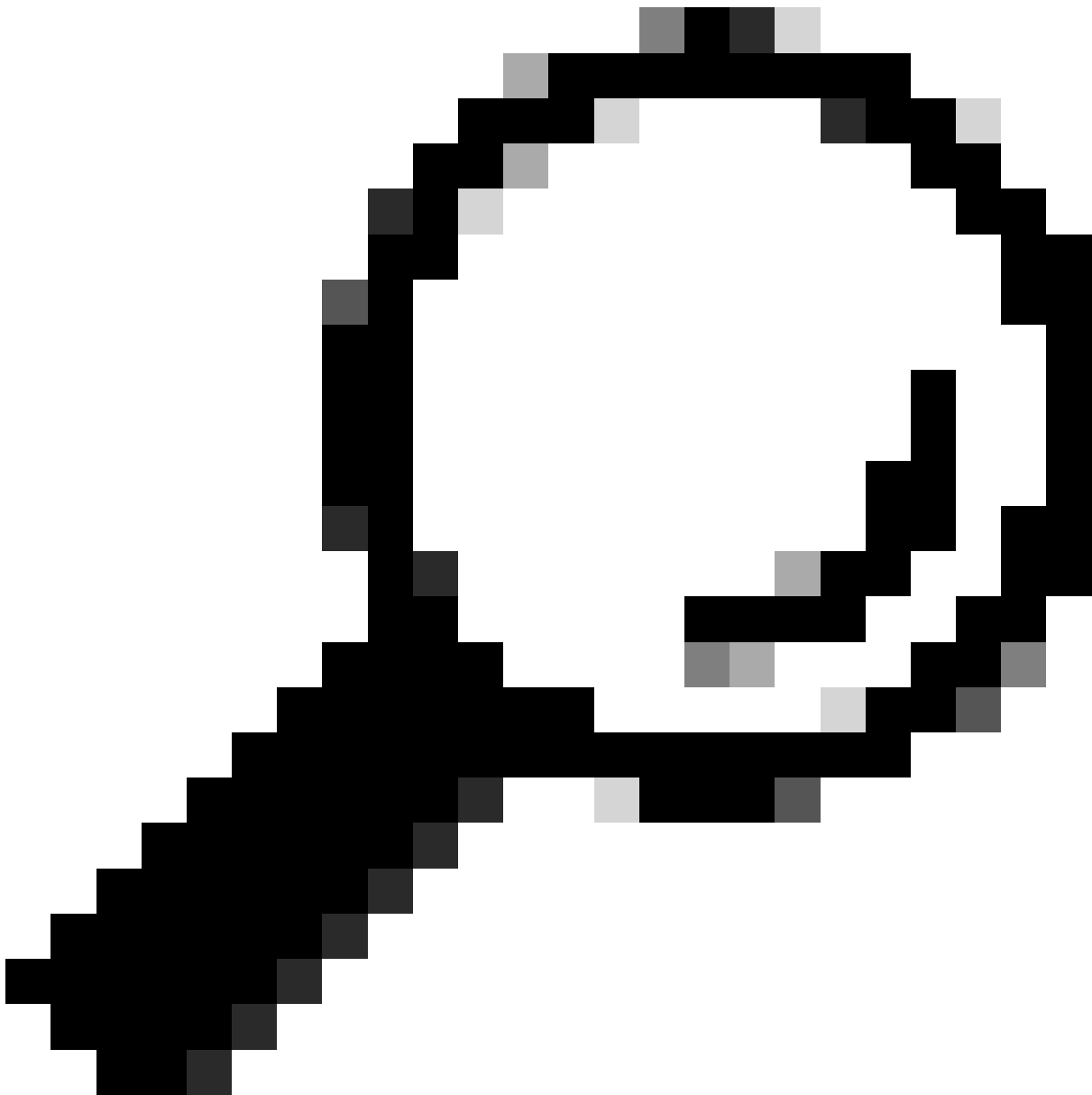
Paso 7. Para descargar el archivo de captura de paquetes, elija el archivo en la lista Administrar archivos de captura de paquetes y haga clic en Descargar archivo.

**Manage Packet Capture Files**

S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-122509.cap (8K)
S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-122439.cap (374B)

Delete Selected Files Download File

Imagen- Descargar captura de paquetes



Sugerencia: el archivo más reciente se encuentra en la parte superior de la lista.

---

Paso 8. (Opcional) Para eliminar cualquier archivo de captura de paquetes, elija el archivo en la lista Administrar archivos de captura de paquetes y haga clic en Eliminar archivos seleccionados.

## Realizar captura de paquetes desde CLI

También puede iniciar la captura de paquetes desde la CLI mediante estos pasos:

Paso 1. Inicie sesión en la CLI.

Paso 2. Escriba `packetcapture` y presione Enter.

Paso 3. (Opcional) Para editar el tipo de filtro actual SETUP. (Para obtener más información sobre

los filtros, consulte la sección Filtros de este documento.)

Paso 4. Elija START para iniciar la 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.

Paso 5. (Opcional) Puede ver el estado de la captura de paquetes seleccionando STATUS (ESTADO):

```
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)
```

Paso 6. Para detener la captura de paquetes, escriba STOP y pulse Intro:



Nota: para descargar los archivos de captura de paquetes recopilados de CLI, puede descargarlos de la GUI o conectarse al dispositivo mediante el protocolo de transferencia de archivos (FTP) y descargarlos de la carpeta Capturas.

---

## Filtros

A continuación, encontrará algunas guías sobre los filtros que puede utilizar en los dispositivos de seguridad de contenido.

### Filtrar por dirección IP de host

#### Filtrar por IP de host en la GUI

Para filtrar por dirección IP de host, en la GUI, hay dos opciones:

- Filtros predefinidos

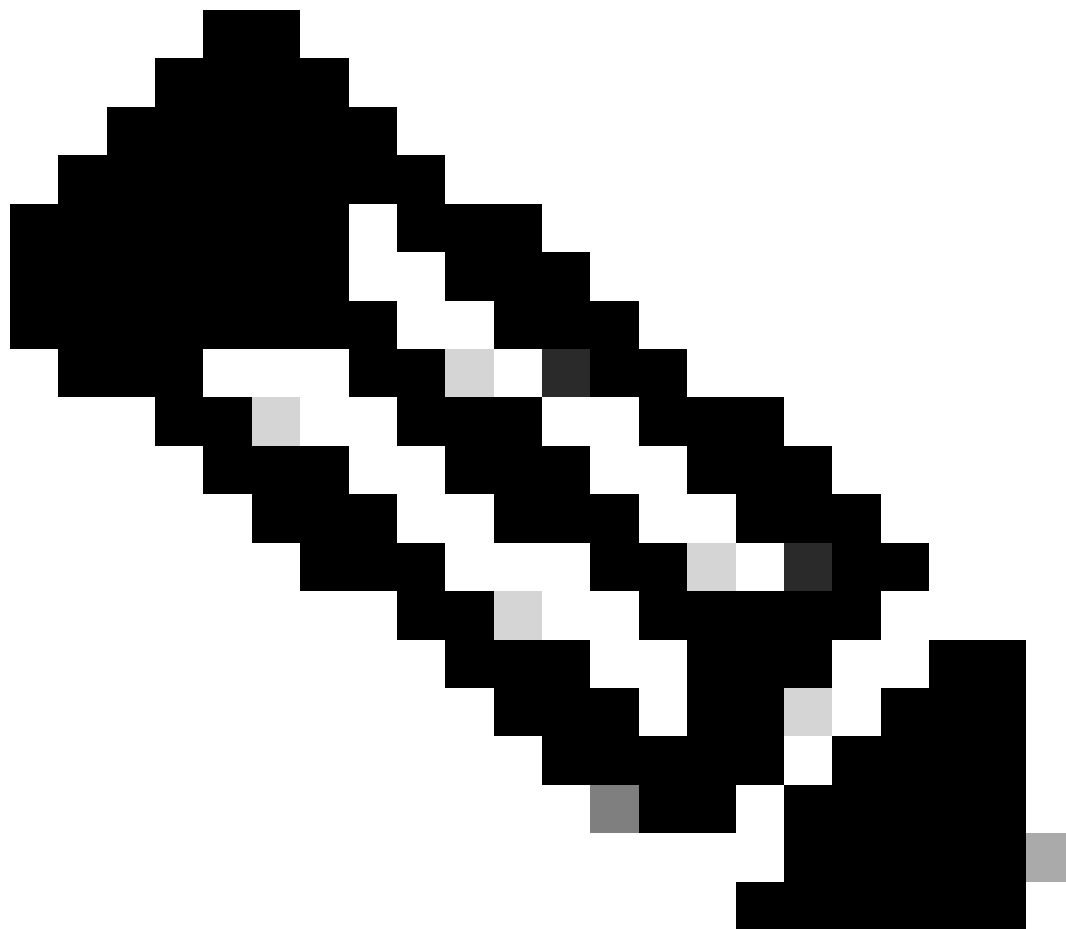
- Filtros personalizados

Para utilizar Filtros predefinidos desde la GUI:

Paso 1. En la página Captura de paquetes, seleccione Editar configuración.

Paso 2. En Filtros de captura de paquetes, seleccione Filtros predefinidos.

Paso 3. Puede ingresar la dirección IP en la sección IP del cliente o IP del servidor.



Nota: Elegir entre IP de cliente o IP de servidor no está limitado a Dirección de origen o Dirección de destino. Este filtro captura todos los paquetes con la dirección IP definida como origen o destino.

---



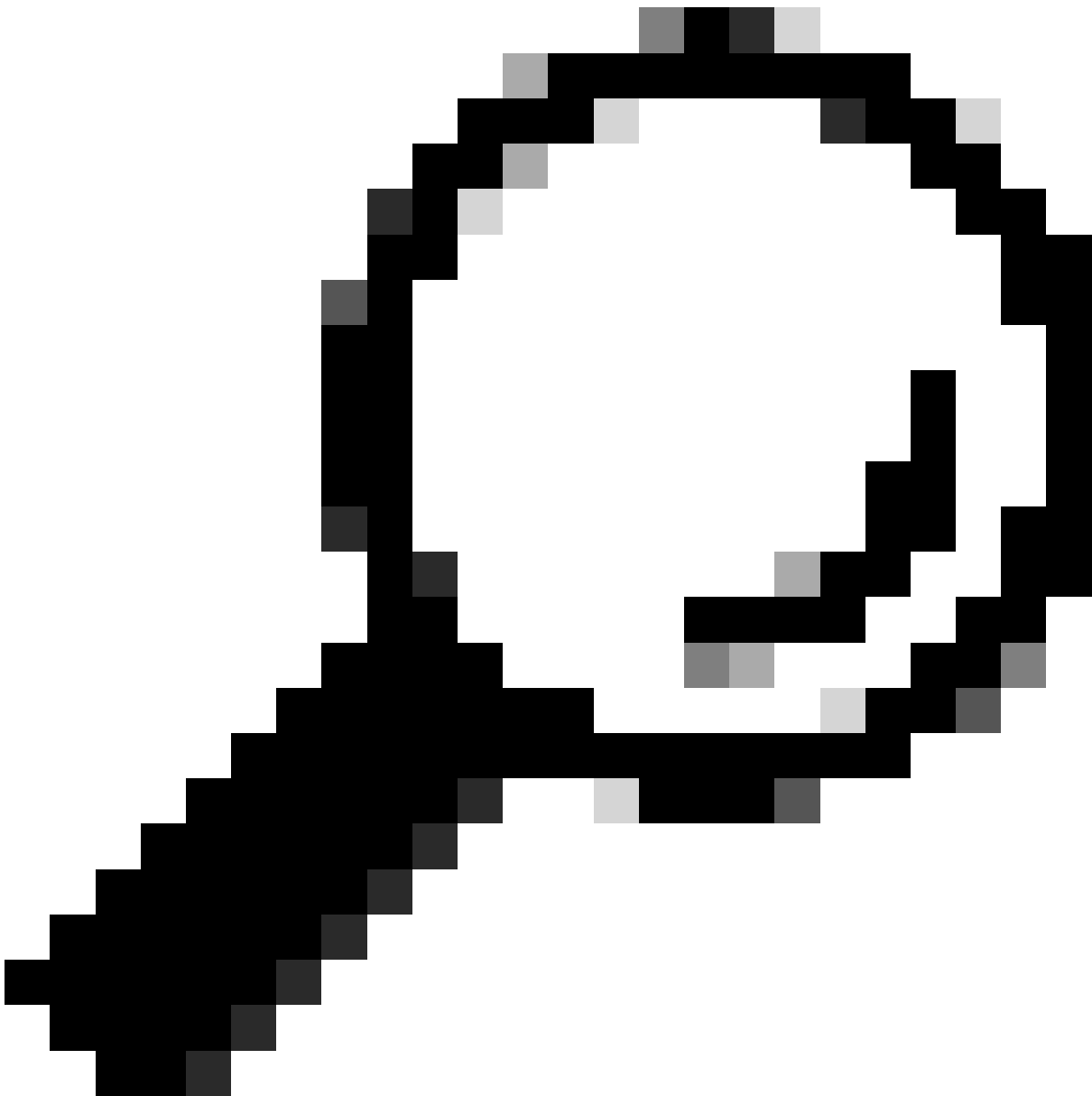
## Edit Packet Capture Settings

Packet Capture Settings	
Capture File Size Limit: ?	<input type="text" value="200"/> MB <small>Maximum file size is 200MB</small>
Capture Duration:	<input type="radio"/> Run Capture Until File Size Limit Reached <input type="radio"/> Run Capture Until Time Elapsed Reaches <input type="text"/> (e.g. 120s, 5m 30s, 4h) <input checked="" type="radio"/> Run Capture Indefinitely  <small>The capture can be ended manually at any time; use the settings above to specify whether the capture should end automatically.</small>
Interfaces:	<input checked="" type="checkbox"/> M1
Packet Capture Filters	
Filters:	<small>All filters are optional. Fields are not mandatory.</small> <input type="radio"/> No Filters <input checked="" type="radio"/> Predefined Filters ? <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">1</span> Ports: <input type="text" value="80,3128"/> Client IP: <input type="text" value="10.20.3.15"/> Server IP: <input type="text"/> <input type="radio"/> Custom Filter ? <input type="text" value="(tcp port 80 or tcp port 3128)"/> <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">2</span>
<small>Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.</small>	

Imagen: Filtrar por IP de host desde filtros predefinidos de GUI

Paso 4. Envíe los cambios.

Paso 5. Inicie la captura.



Sugerencia: No es necesario registrar cambios, el filtro recién agregado que se aplica a la captura actual. La realización de los cambios ayuda a guardar el filtro para su uso futuro.

---

Para utilizar Filtros personalizados y Filtros predefinidos desde la GUI:

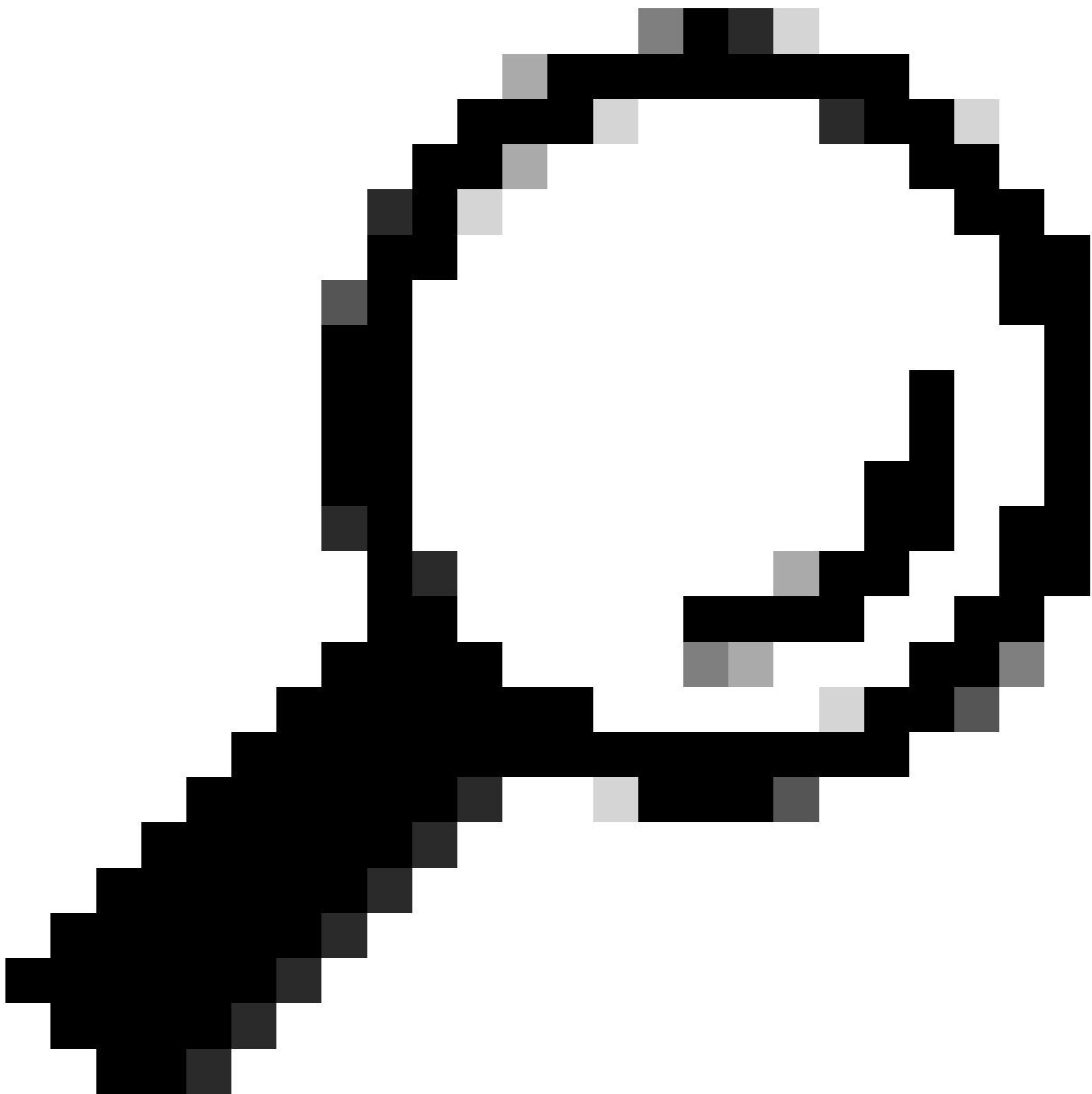
Paso 1. En la página Captura de paquetes, elija Editar configuración.

Paso 2. En Filtros de captura de paquetes, seleccione Filtro personalizado.

Paso 3. Utilice la sintaxis host seguida de la dirección IP.

Este es un ejemplo para filtrar todo el tráfico con la dirección IP de origen o destino 10.20.3.15

```
host 10.20.3.15
```



Sugerencia: para filtrar por más de una dirección IP, puede utilizar operandos lógicos como o y y (sólo letras minúsculas).

---

**Packet Capture Filters**

Filters: *All filters are optional. Fields are not mandatory.*

No Filters

Predefined Filters ?

Ports:

Client IP:

Server IP:

Custom Filter ?

Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.

Imagen: filtro personalizado para dos direcciones IP

Paso 4. Envíe los cambios.

Paso 5. Inicie la captura

Filtrar por IP de host en CLI

Para filtrar por la dirección IP del host desde la CLI:

Paso 1. Inicie sesión en la CLI.

Paso 2. Escriba packetcapture y presione Enter.

Paso 3. Para editar el filtro actual, escriba SETUP.

Paso 4. Responda a las preguntas hasta que llegue a Introduzca el filtro que se utilizará para la captura

Paso 5. Puede utilizar la misma cadena de filtro que el filtro personalizado en la GUI.

Este es un ejemplo de filtrado de todo el tráfico con la dirección IP de origen o destino 10.20.3.15 o 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 puerto

### Filtrar por número de puerto en la GUI

Para filtrar por número(s) de puerto, en la GUI hay dos opciones:

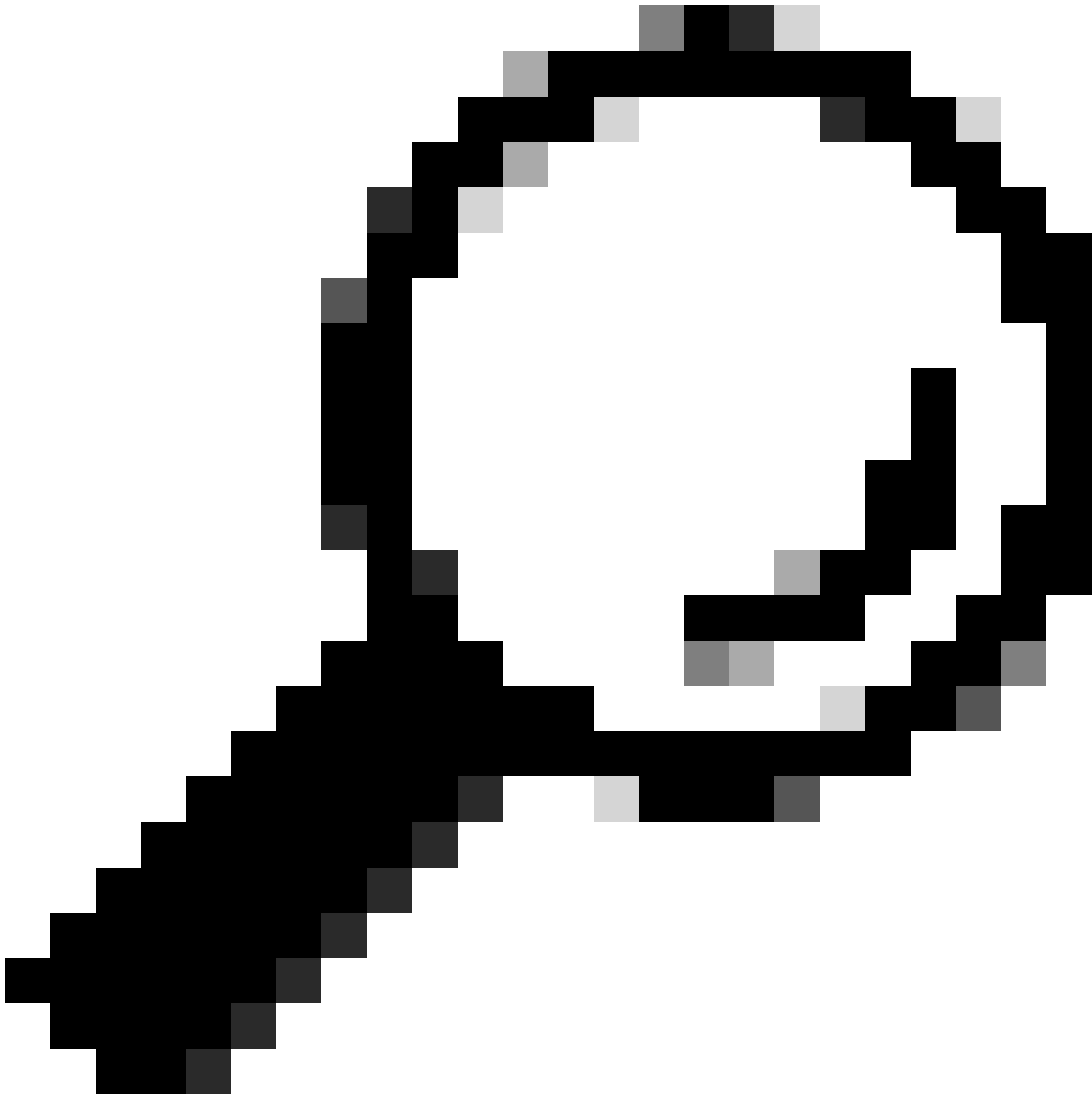
- Filtros predefinidos
- Filtros personalizados

Para utilizar filtros predefinidos desde la GUI:

Paso 1. En la página Captura de paquetes, elija Editar configuración.

Paso 2. En Filtros de captura de paquetes, seleccione Filtros predefinidos.

Paso 3. En la sección Puertos, escriba los números de puerto que desea filtrar.



Sugerencia: puede agregar varios números de puerto separándolos con una coma ", ".

**Packet Capture Filters**

Filters: *All filters are optional. Fields are not mandatory.*

No Filters

**Predefined Filters ?** ← 1

Ports:  ← 2

Client IP:

Server IP:

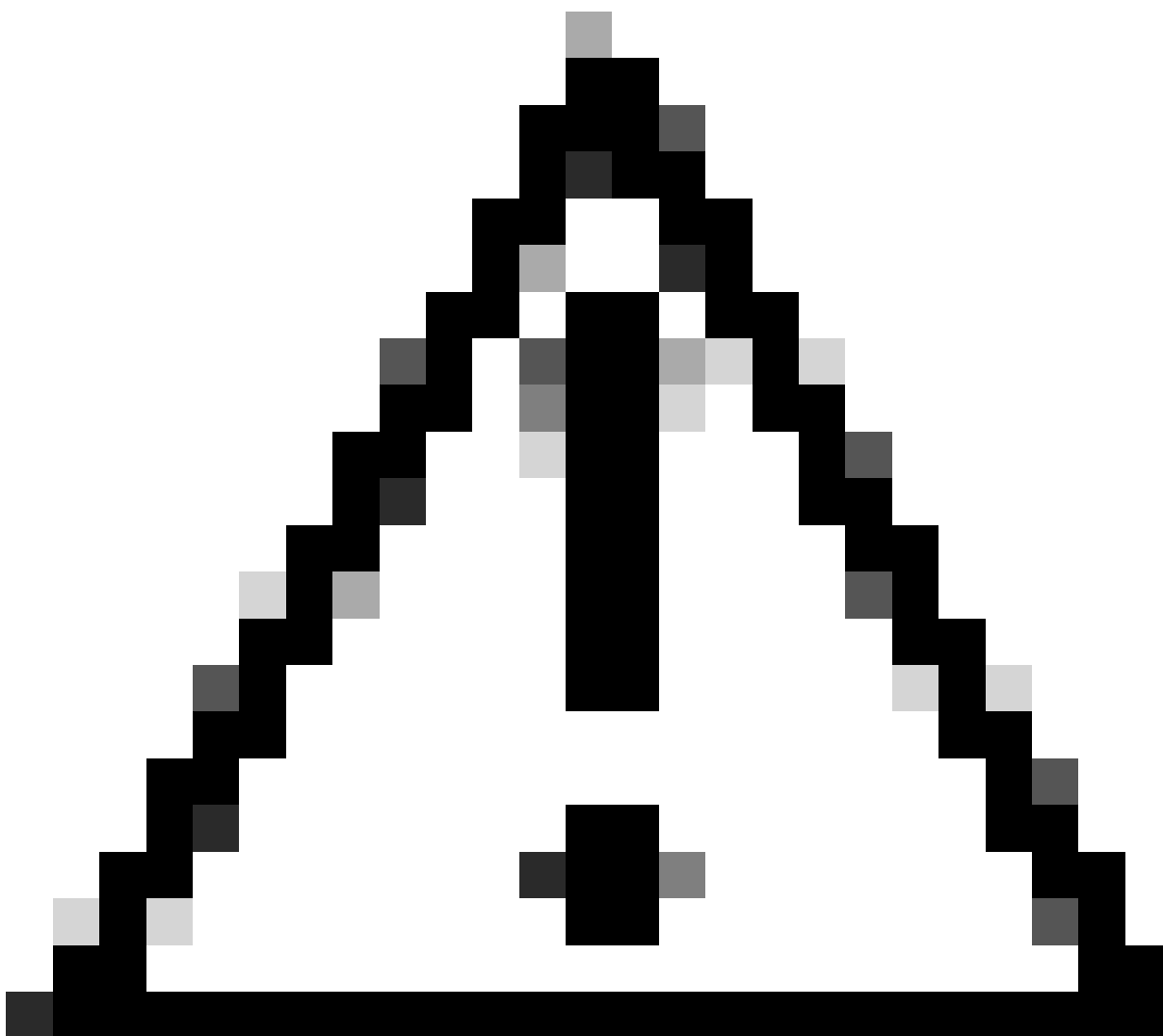
Custom Filter ?

Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.

Paso 4. Envíe los cambios.

Paso 5. Inicie la captura.

---



Precaución: este enfoque captura solamente el tráfico TCP con los números de puerto definidos. Para capturar el tráfico UDP, utilice el filtro personalizado.

---

Para utilizar filtros personalizados desde la GUI:

Paso 1. En la página Captura de paquetes, elija Editar configuración.

Paso 2. En Filtros de captura de paquetes, seleccione Filtro personalizado.

Paso 3. Utilice la sintaxis port seguida del número de puerto.

**Packet Capture Filters**

Filters: *All filters are optional. Fields are not mandatory.*

No Filters

Predefined Filters ?

Ports:

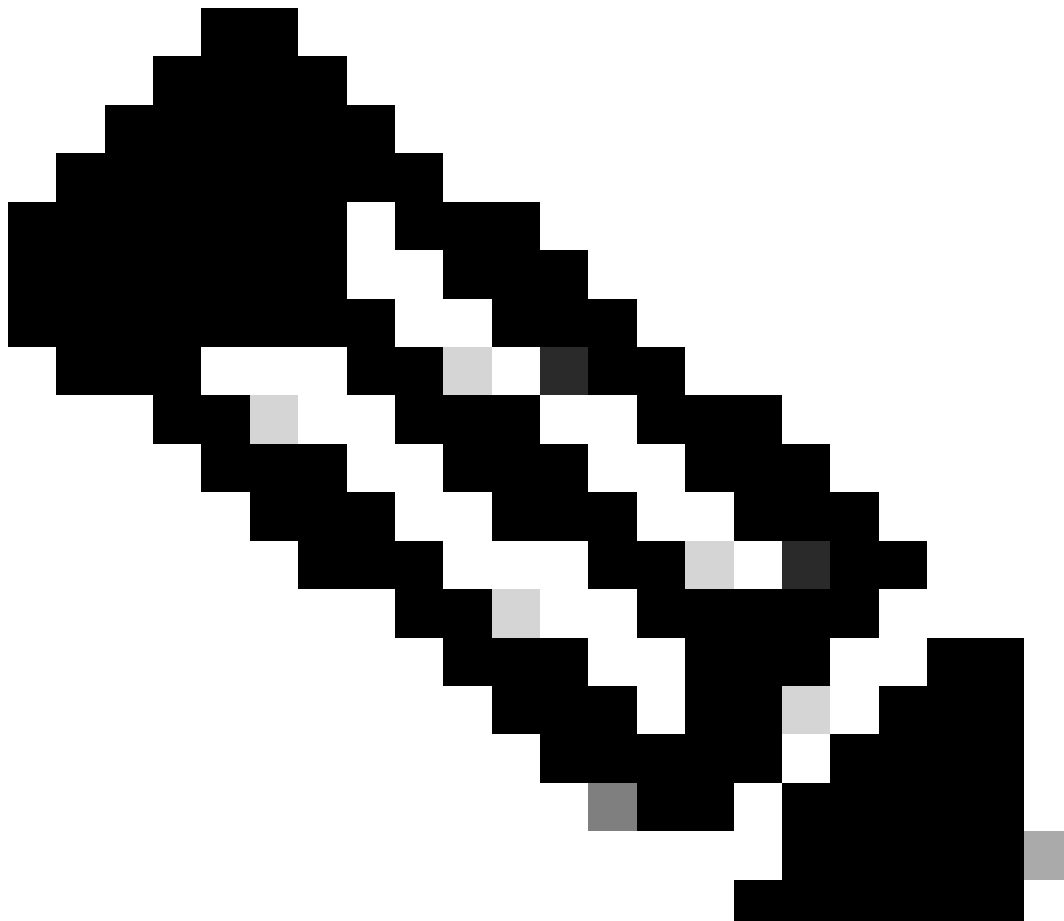
Client IP:

Server IP:

Custom Filter ?

Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.

Imagen - Filtro personalizado por número de puerto



Nota: Si sólo utiliza port, este filtro cubre los puertos TCP y UDP.

Paso 4. Envíe los cambios.



Paso 5. Inicie la captura.

Filtrar por número de puerto en CLI

Para filtrar por el número de puerto desde CLI:

Paso 1. Inicie sesión en la CLI.

Paso 2. Escriba packetcapture y presione Enter.

Paso 3. Para editar el filtro actual, escriba SETUP.

Paso 4. Responda a las preguntas hasta que llegue a Introduzca el filtro que se utilizará para la captura

Paso 5. Puede utilizar la misma cadena de filtro que el filtro personalizado en la GUI.

Este es un ejemplo de filtrado de todo el tráfico con el número de puerto de origen o de destino 53, para los puertos TCP y 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
```

## Filtro en SWA con implementación transparente

En SWA con implementación transparente, mientras que la conectividad del protocolo de

comunicación de caché web (WCCP) se realiza a través de los túneles de encapsulación de routing genérico (GRE), las direcciones IP de origen y destino de los paquetes que entran o salen de SWA son la dirección IP del router y la dirección IP de SWA.

Para poder recopilar la captura de paquetes con la dirección IP o el número de puerto de la GUI, existen dos opciones:

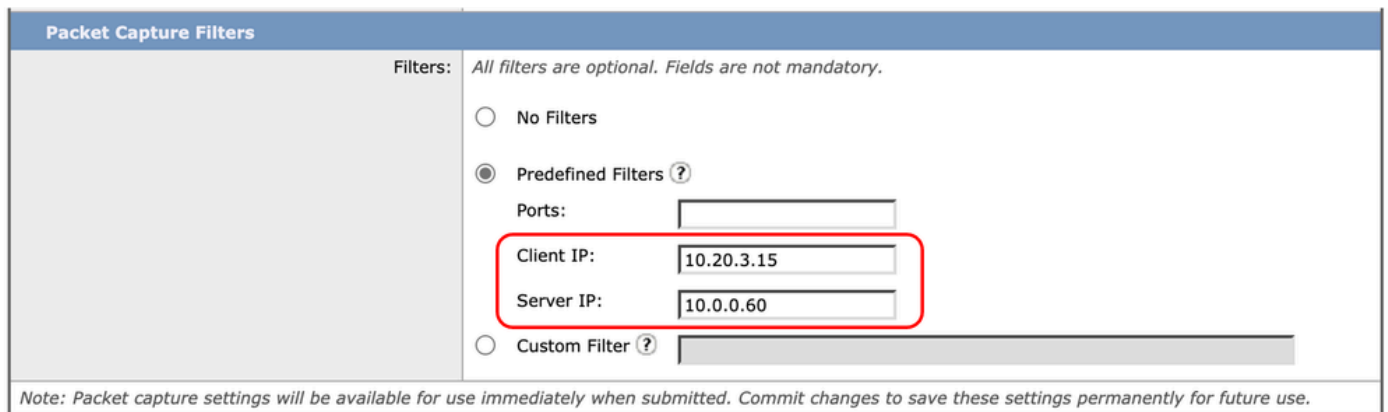
- Filtros predefinidos
- Filtros personalizados

Filtro en SWA con implementación transparente en GUI

Paso 1. En la página Captura de paquetes, seleccione Editar configuración.

Paso 2. En Filtros de captura de paquetes, seleccione Filtros predefinidos.

Paso 3. Puede ingresar la dirección IP en la sección IP del cliente o IP del servidor.



Packet Capture Filters

Filters: All filters are optional. Fields are not mandatory.

No Filters

Predefined Filters ?

Ports:

Client IP:

Server IP:

Custom Filter ?

Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.

Imagen - Configuración de la dirección IP en filtros predefinidos

Paso 4. Envíe los cambios.

Paso 5. Inicie la captura.



Nota: Puede ver que, después de enviar el filtro, SWA ha añadido condiciones adicionales en la sección Filtro seleccionado.

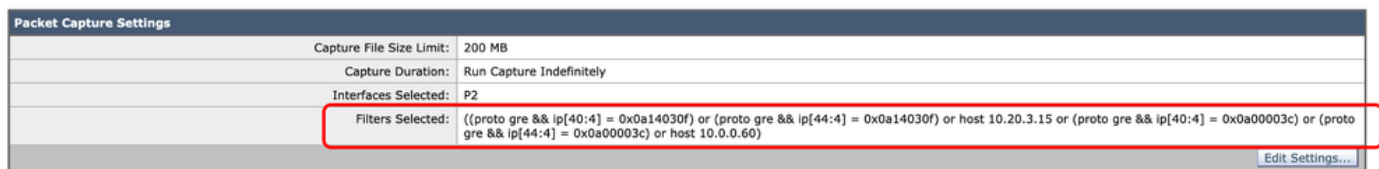


Imagen: filtros adicionales agregados por SWA para recopilar paquetes dentro del túnel GRE

Para utilizar filtros personalizados desde la GUI:

Paso 1. En la página Captura de paquetes, seleccione Editar configuración.

Paso 2. En Filtros de captura de paquetes, seleccione Filtro personalizado

Paso 3. Agregue primero esta cadena y, a continuación, el filtro que planea implementar agregando o después de esta cadena:

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

Por ejemplo, si planea filtrar por la IP del host igual a 10.20.3.15 o el número de puerto igual a 8080, puede utilizar esta cadena:

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

Paso 4. Envíe los cambios.

Paso 5. Inicie la captura.

Filtro en SWA con implementación transparente en CLI

Para filtrar la implementación de proxy transparente desde CLI:

Paso 1. Inicie sesión en la CLI.

Paso 2. Escriba packetcapture y presione Enter.

Paso 3. Para editar el filtro actual, escriba SETUP.

Paso 4. Responda a las preguntas hasta que llegue a Introduzca el filtro que se utilizará para la captura

Paso 5. Puede utilizar la misma cadena de filtro que el filtro personalizado en la GUI.

Este es un ejemplo para filtrar por la IP del host igual a 10.20.3.15 o el número de puerto 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.

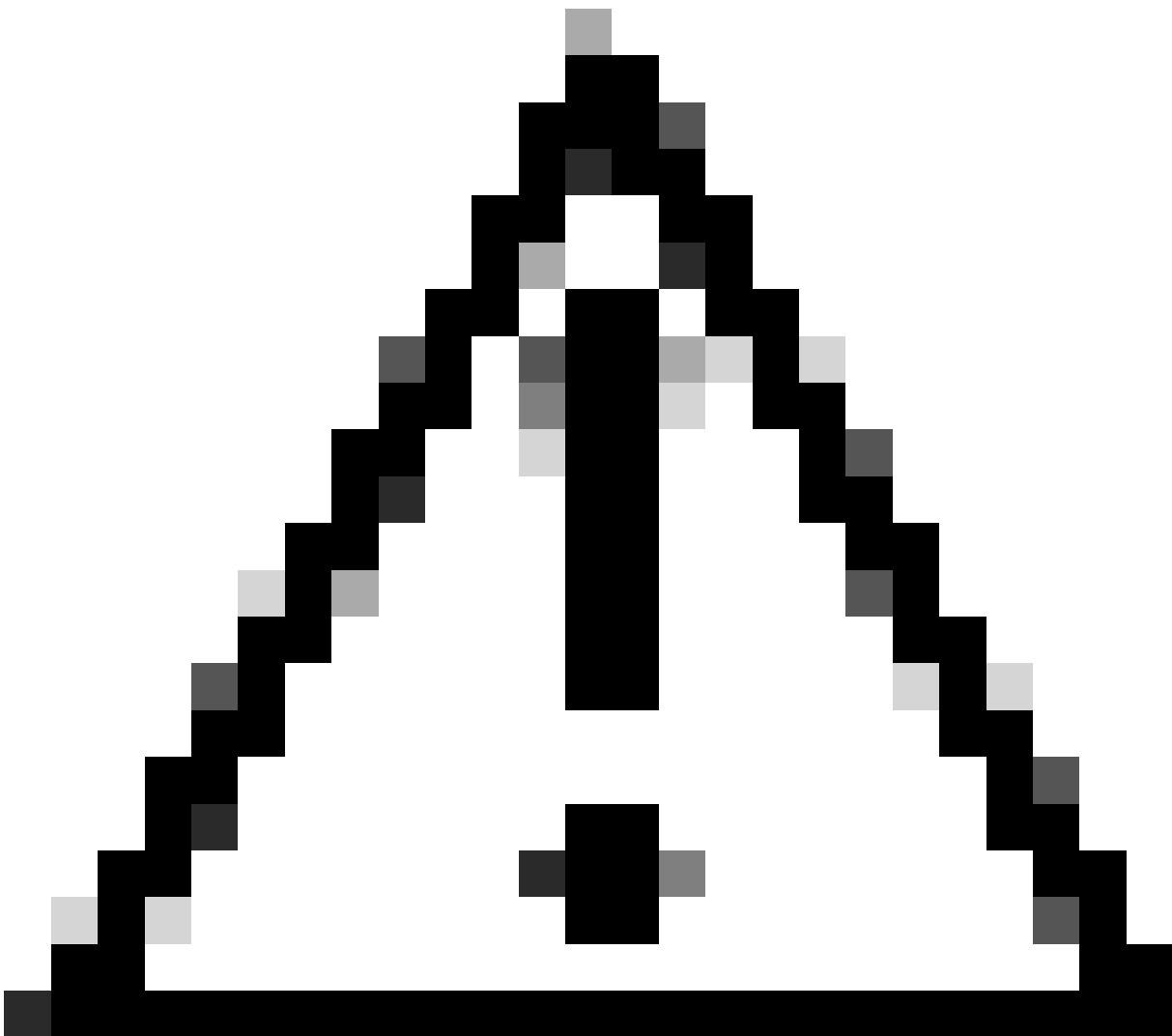
[(tcp port 80 or tcp port 3128)]> (proto gre && ip[40:4] = 0x0a14030f) or (proto gre && ip[44:4] = 0x0a

## Filtros más comunes

A continuación se muestra una tabla que enumera los filtros más comunes:

Descripción	Filtro
Filtrar por dirección IP de origen igual a 10.20.3.15	src host 10.20.3.15
Filtrar por dirección IP de destino igual a 10.20.3.15	dst host 10.20.3.15
Filtrar por dirección IP de origen igual a 10.20.3.15 y dirección IP de destino igual a 10.0.0.60	(src host 10.20.3.15) y (dst host 10.0.0.60)
Filtrar por dirección IP de origen o destino igual a 10.20.3.15	host 10.20.3.15
Filtrar por dirección IP de origen o destino igual a 10.20.3.15 o igual a 10.0.0.60	host 10.20.3.15 o host 10.0.0.60
Filtrar por número de puerto TCP igual a 8080	tcp port 8080
Filtrar por número de puerto UDP igual a 53	udp port 53
Filtrar por número de puerto igual a 514 (TCP o UDP)	port 514

Filtrar sólo paquetes UDP	udp
Filtrar sólo paquetes ICMP	icmp
Filtro principal que se utilizará para cada captura en la implementación transparente	(proto gre && ip[40:4] = 0x0a14030f) o (proto gre && ip[44:4] = 0x0a14030f) o (proto gre && ip[40:4] = 0x0a00003c) o (proto gre && ip[44:4] = 0x0a00003c)



Precaución: todos los filtros distinguen entre mayúsculas y minúsculas.

## Troubleshoot

"Error de filtro" es uno de los errores más comunes al realizar la captura de paquetes.

## Packet Capture

Error — Filter Error

---

### Current Packet Capture

No packet capture in progress

Start Capture

---

### Manage Packet Capture Files

- S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-175955.cap (24B)
- S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-175543.cap (740B)
- S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-175404.cap (24B)
- S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-175023.cap (24B)

Delete Selected Files Download File

---

### Packet Capture Settings

Capture File Size Limit:	200 MB
Capture Duration:	Run Capture Indefinitely
Interfaces Selected:	M1
Filters Selected:	ICMP

Edit Settings...

Imagen - Error de filtro

Este error suele estar relacionado con una implementación incorrecta del filtro. En el ejemplo anterior, el filtro ICMP tiene caracteres en mayúsculas. Esta es la razón por la que recibe el mensaje de error de filtro. Para solucionar este problema, debe editar el filtro y reemplazar el ICMP por icmp.

## Información Relacionada

- [Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - GD\(General Deployment\) - Classify End-U...](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).