

在內容安全裝置上配置資料包捕獲

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[從GUI執行資料包捕獲](#)

[從CLI執行資料包捕獲](#)

[篩選條件](#)

[按主機IP地址過濾](#)

[在GUI中按主機IP過濾](#)

[在CLI中按主機IP過濾](#)

[依連線埠號碼篩選](#)

[在GUI中按埠號過濾](#)

[在CLI中按埠號過濾](#)

[在具有透明部署的SWA中過濾](#)

[在SWA中使用透明部署在GUI中過濾](#)

[在SWA中使用透明部署在CLI中過濾](#)

[最常見的過濾器](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹思科安全網路裝置(SWA)、電子郵件安全裝置(ESA)和安全管理裝置(SMA)上的封包擷取。

必要條件

需求

思科建議您瞭解以下主題：

- 思科內容安全裝置管理。

思科建議您：

- 已安裝物理或虛擬SWA/ESA/SMA。
- 對SWA/ESA/SMA圖形使用者介面(GUI)的管理訪問。
- 對SWA/ESA/SMA命令列介面(CLI)的管理訪問

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

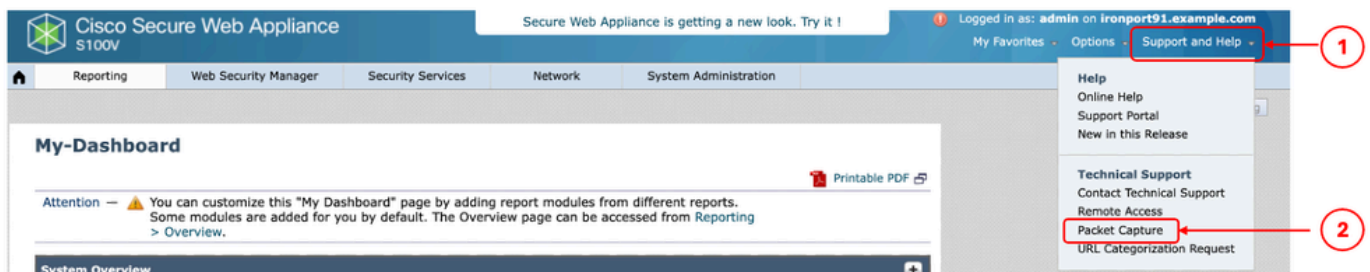
從GUI執行資料包捕獲

要從GUI執行資料包捕獲，請執行以下步驟：

步驟 1. 登入GUI。

步驟 2. 從頁右上方選擇支援和幫助。

步驟 3. 選擇Packet Capture。

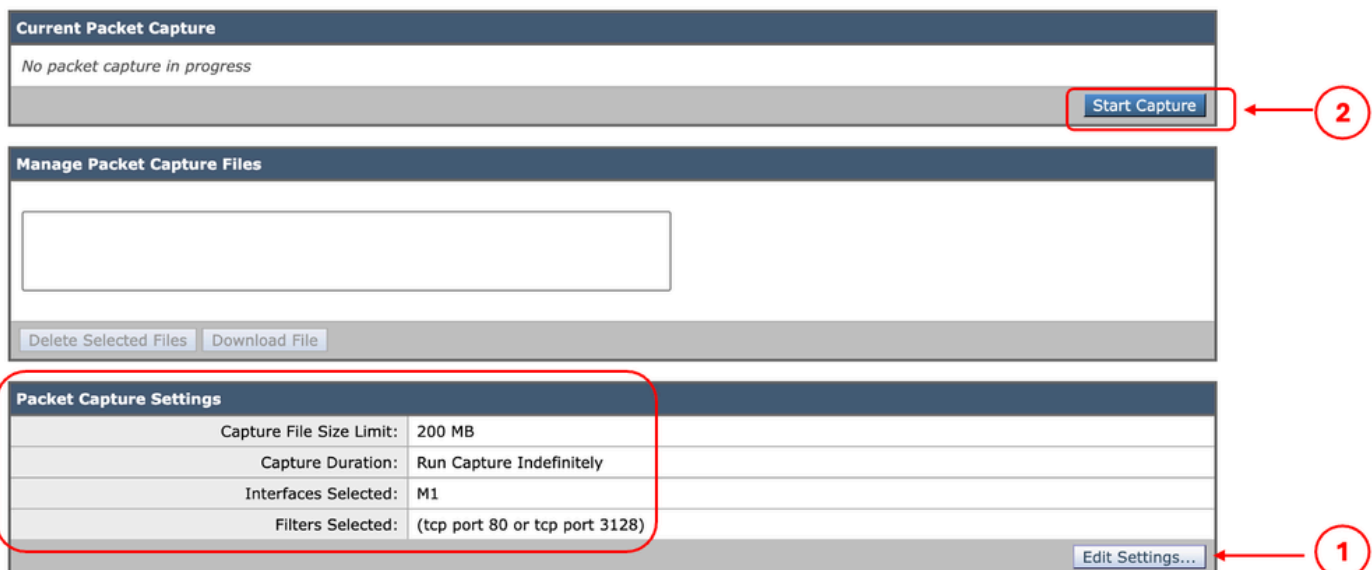


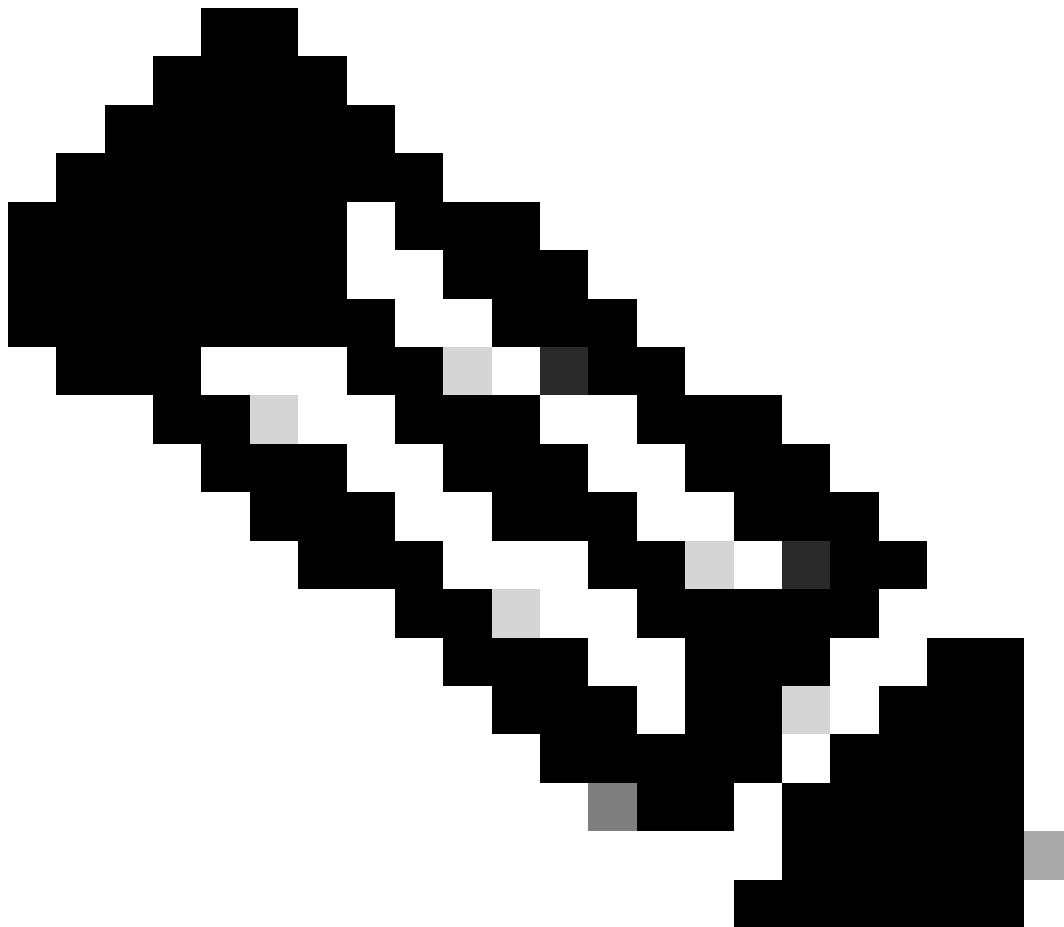
映像-資料包捕獲

步驟4.（可選）要編輯當前過濾器，請選擇Edit Settings。（有關過濾器的詳細資訊，請查閱本文檔中的「過濾器」部分）

步驟 5. 開始捕獲。

Packet Capture





注意：資料包捕獲檔案大小限制為200MB。當檔案大小達到200MB時，資料包捕獲停止。

「當前資料包捕獲」部分顯示資料包捕獲狀態，包括檔案大小和應用的過濾器。

Packet Capture

Success — Packet Capture has started

Current Packet Capture

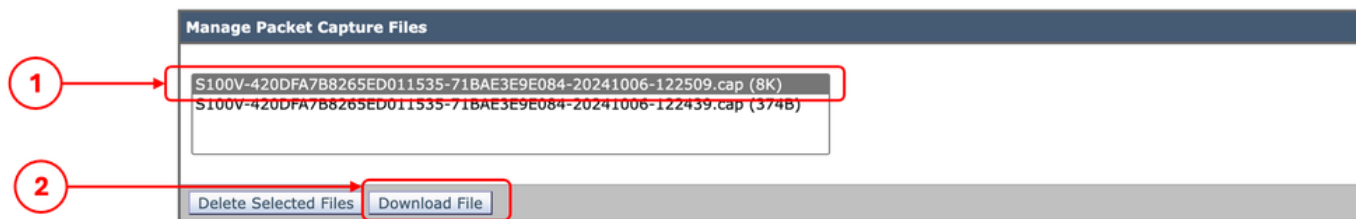
Status: Capture in progress (Duration: 13s)
File Name: S100V-420DFA7B8265ED011535-71BAE3E9E084-20241006-122509.cap (Size: 0B)

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

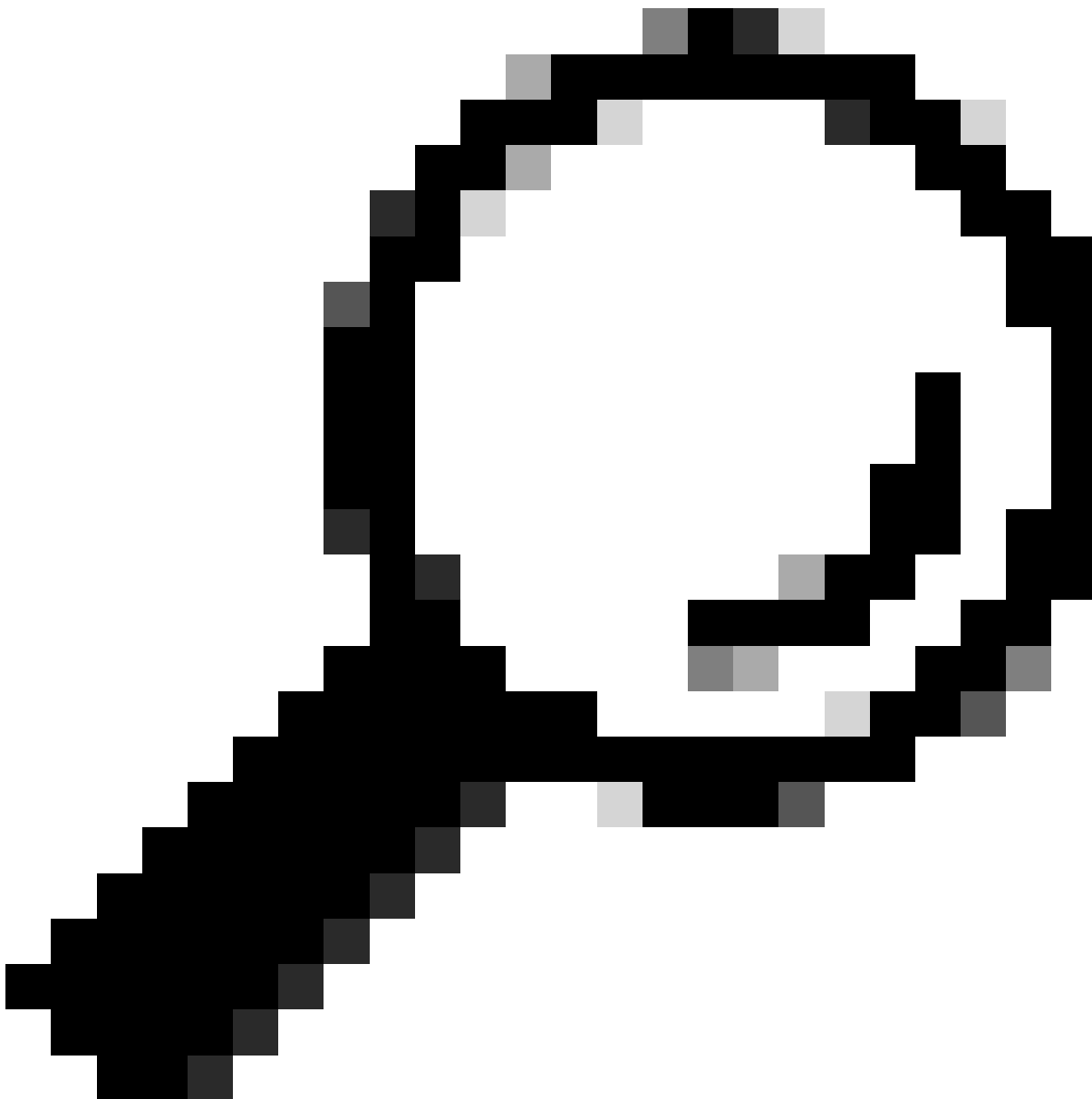
Stop Capture

步驟 6.要停止運行的資料包捕獲，請點選停止捕獲。

步驟 7.要下載資料包捕獲檔案，請從Manage Packet Capture Files清單中選擇檔案，然後按一下 Download File。



映像-下載資料包捕獲



提示：最新檔案位於清單頂端。

步驟8. (可選) 要刪除任何資料包捕獲檔案，請從Manage Packet Capture Files清單中選擇該檔案並點選Delete Selected Files。

從CLI執行資料包捕獲

您也可以從CLI使用以下步驟開始資料包捕獲：

步驟 1. 登入到CLI。

步驟 2. 鍵入packetcapture，然後按Enter。

步驟3. (可選) 要編輯當前過濾器型別SETUP。(有關過濾器的詳細資訊，請查閱本文檔中的「過濾器」部分。)

步驟 4. 選擇START開始捕獲。

```
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.
```

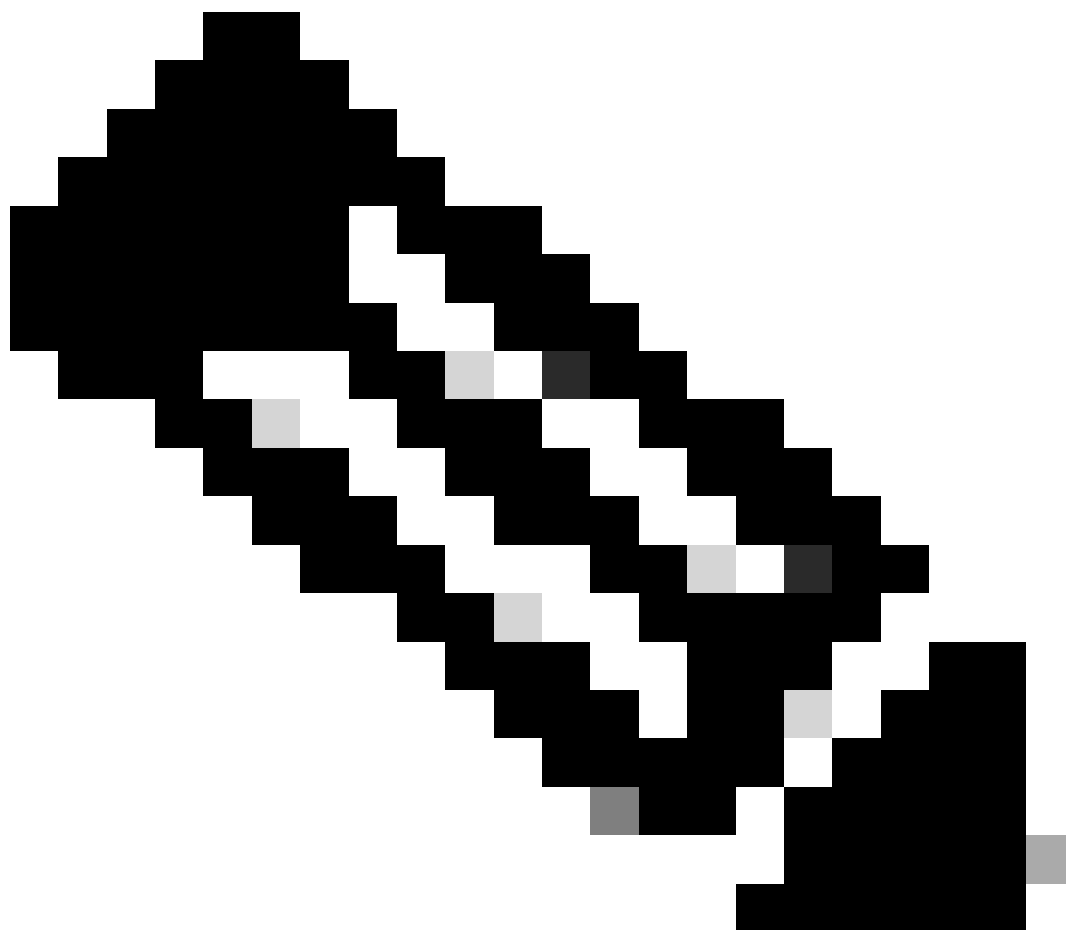
步驟5. (可選) 您可以透過選擇STATUS檢視資料包捕獲的狀態：

```
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)
```

步驟 6.要停止資料包捕獲，請鍵入STOP並按Enter：



注意：要下載從CLI收集的資料包捕獲檔案，可以從GUI下載這些檔案，也可以透過檔案傳輸協定(FTP)連線到裝置，然後從Captures資料夾下載這些檔案。

篩選條件

以下是一些有關可在內容安全裝置中使用的過濾器的指南。

按主機IP地址過濾

在GUI中按主機IP過濾

要按主機IP地址過濾，在GUI中有兩個選項：

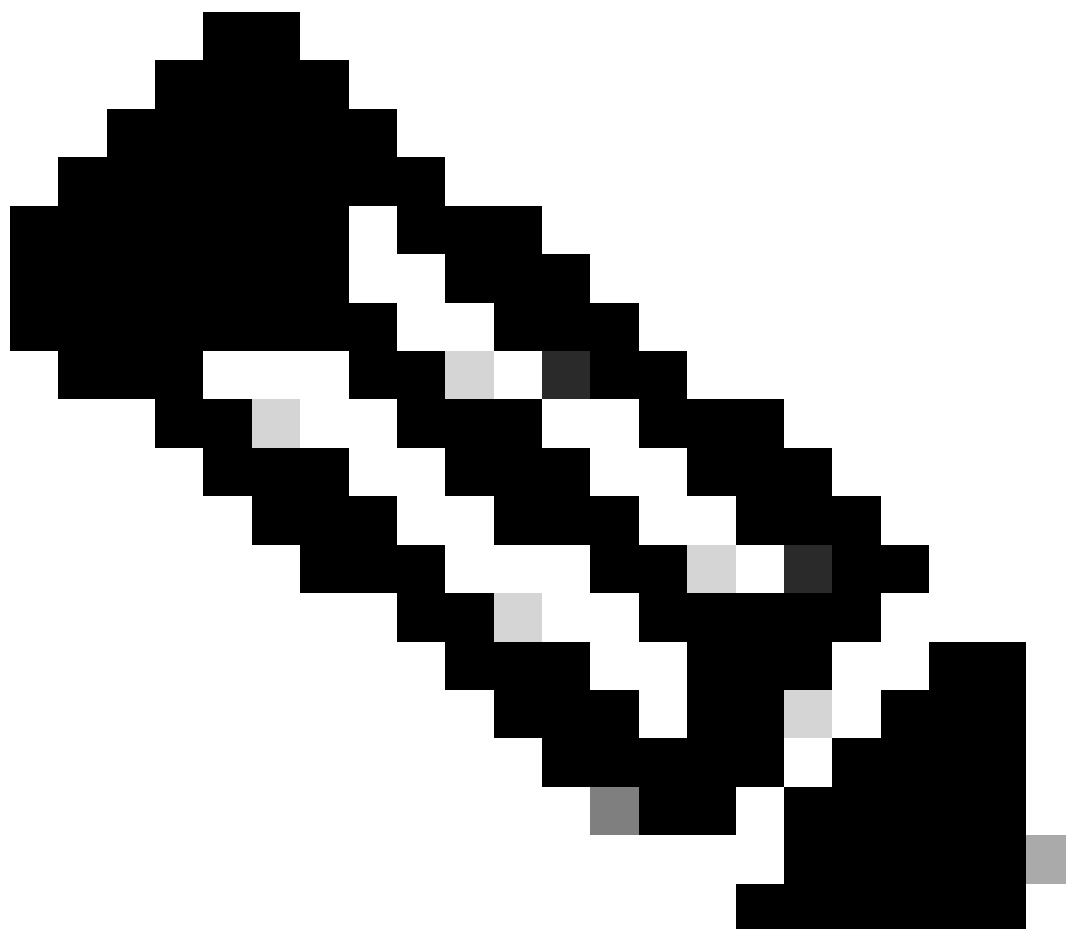
- 預先定義的篩選
- 自訂篩選條件

要從GUI使用預定義過濾器：

步驟 1.在「資料包捕獲」頁中，選擇編輯設定。

步驟 2.在Packet Capture Filters中選擇Predefined Filters。

步驟 3.可以在客戶端IP或伺服器IP部分輸入IP地址。



注意：選擇客戶端IP或伺服器IP並不侷限於源地址或目標地址。此過濾器捕獲所有IP地址定義為源或目標的資料包。

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 ? 1 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)"/> 2
<small>Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.</small>	

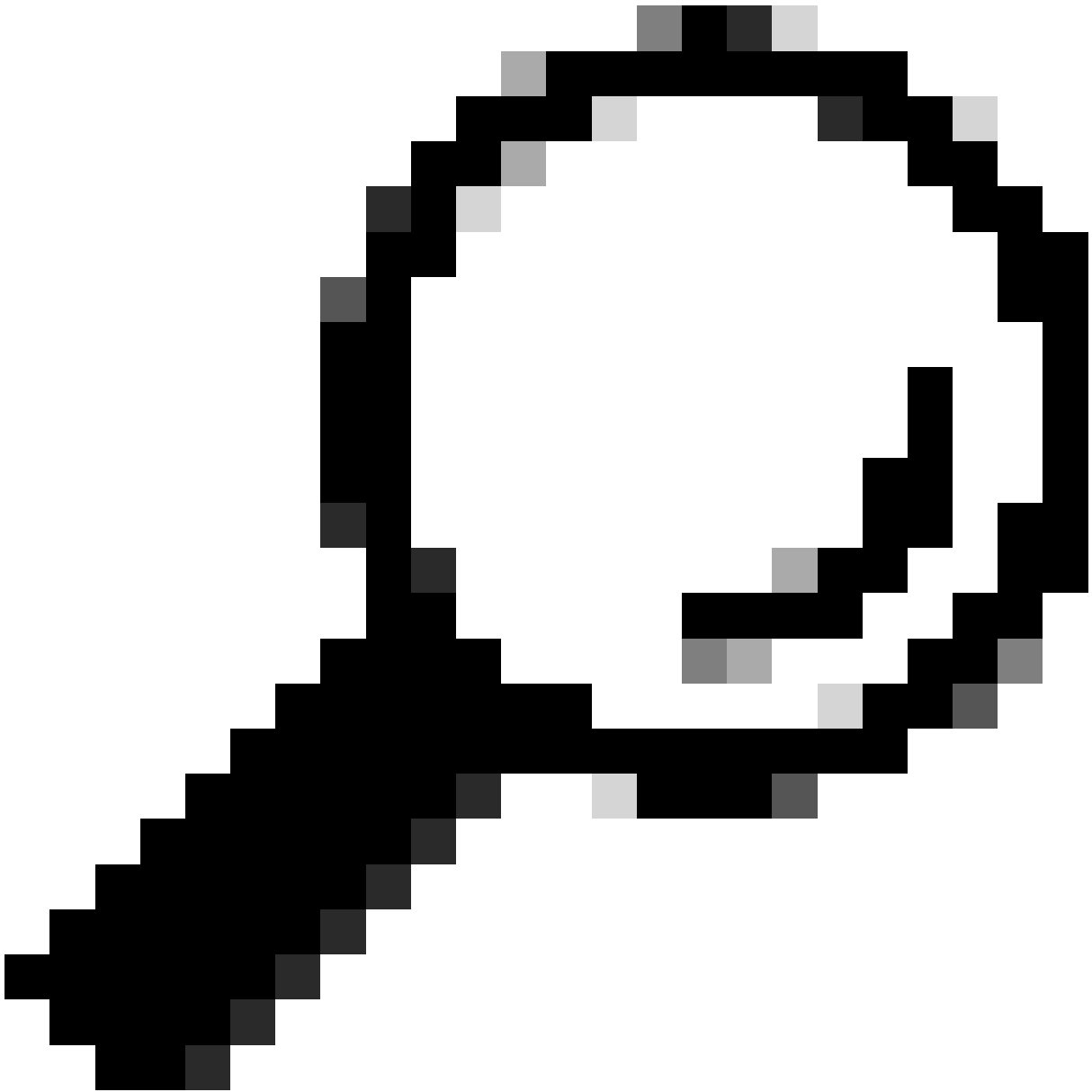
Cancel

Submit

影象-透過GUI預定義過濾器按主機IP過濾

步驟 4.提交變更。

步驟 5.開始捕獲。



提示：不需要提交更改，新增加的過濾器應用於當前捕獲。提交變更有助於儲存篩選器以供未來使用。

要在GUI中使用自定義過濾器和預定義過濾器，請執行以下操作：

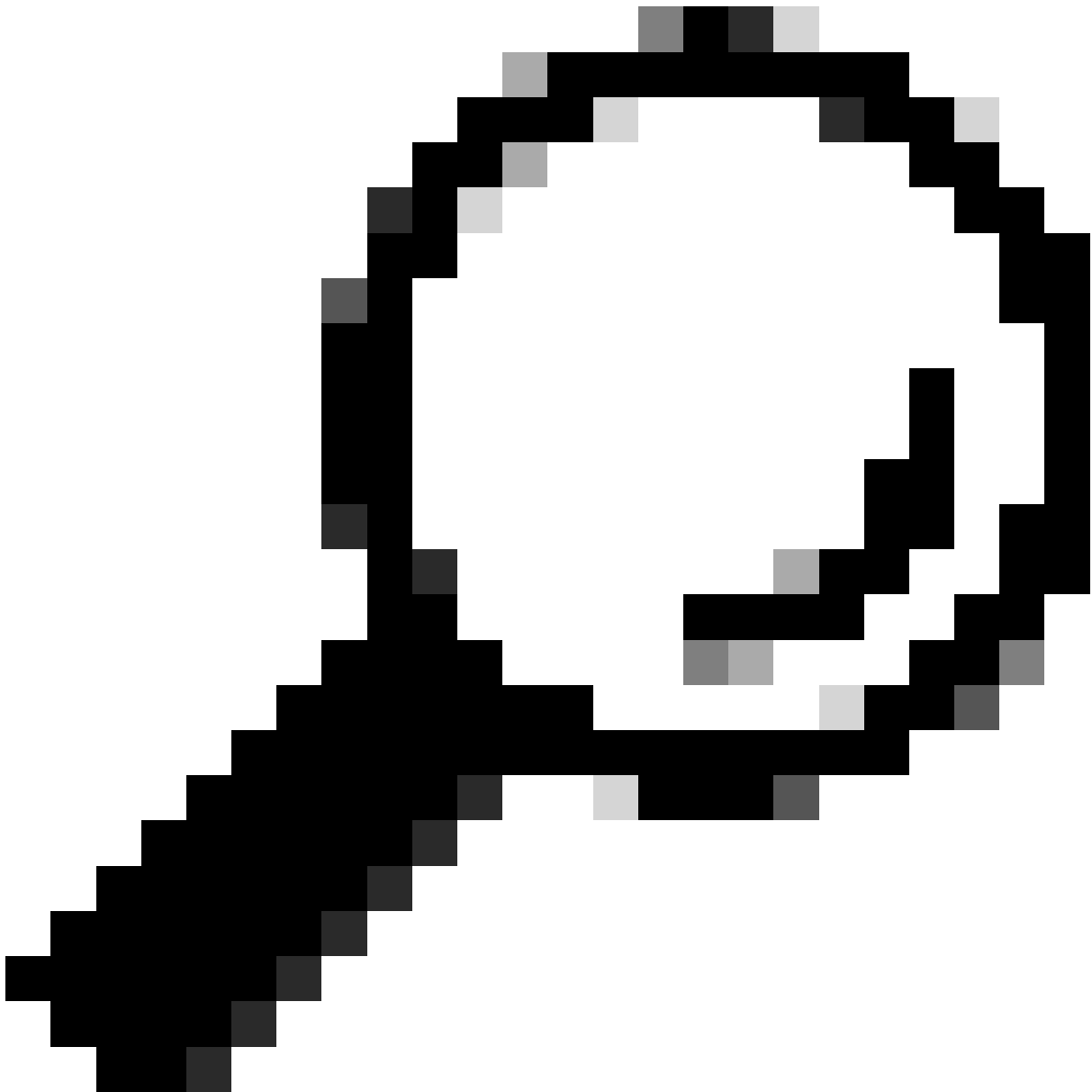
步驟 1.在資料包捕獲頁面中，選擇編輯設定。

步驟 2.從資料包捕獲過濾器中選擇自定義過濾器。

步驟 3.請使用後跟IP地址的host 語法。

以下是過濾來源或目的地IP位址為10.20.3.15的所有流量的範例

```
host 10.20.3.15
```



提示：要按多個IP地址過濾，您可以使用邏輯運算元，例如或和和（僅小寫字母）。

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.

步驟 4.提交變更。

步驟 5.開始捕獲

在CLI中按主機IP過濾

從CLI按主機IP地址過濾：

步驟 1.登入到CLI。

步驟 2.鍵入packetcapture，然後按Enter。

步驟 3. 要編輯當前過濾器，請鍵入SETUP。

步驟 4.回答問題，直到您到達輸入用於捕獲的過濾器

步驟 5. 您可以使用與GUI中的自定義過濾器相同的過濾器字串。

以下是過濾來源或目的地IP位址為10.20.3.15或10.0.0.60的所有流量的範例

```
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
```

依連線埠號碼篩選

在GUI中按埠號過濾

要按埠號過濾，GUI中有兩個選項：

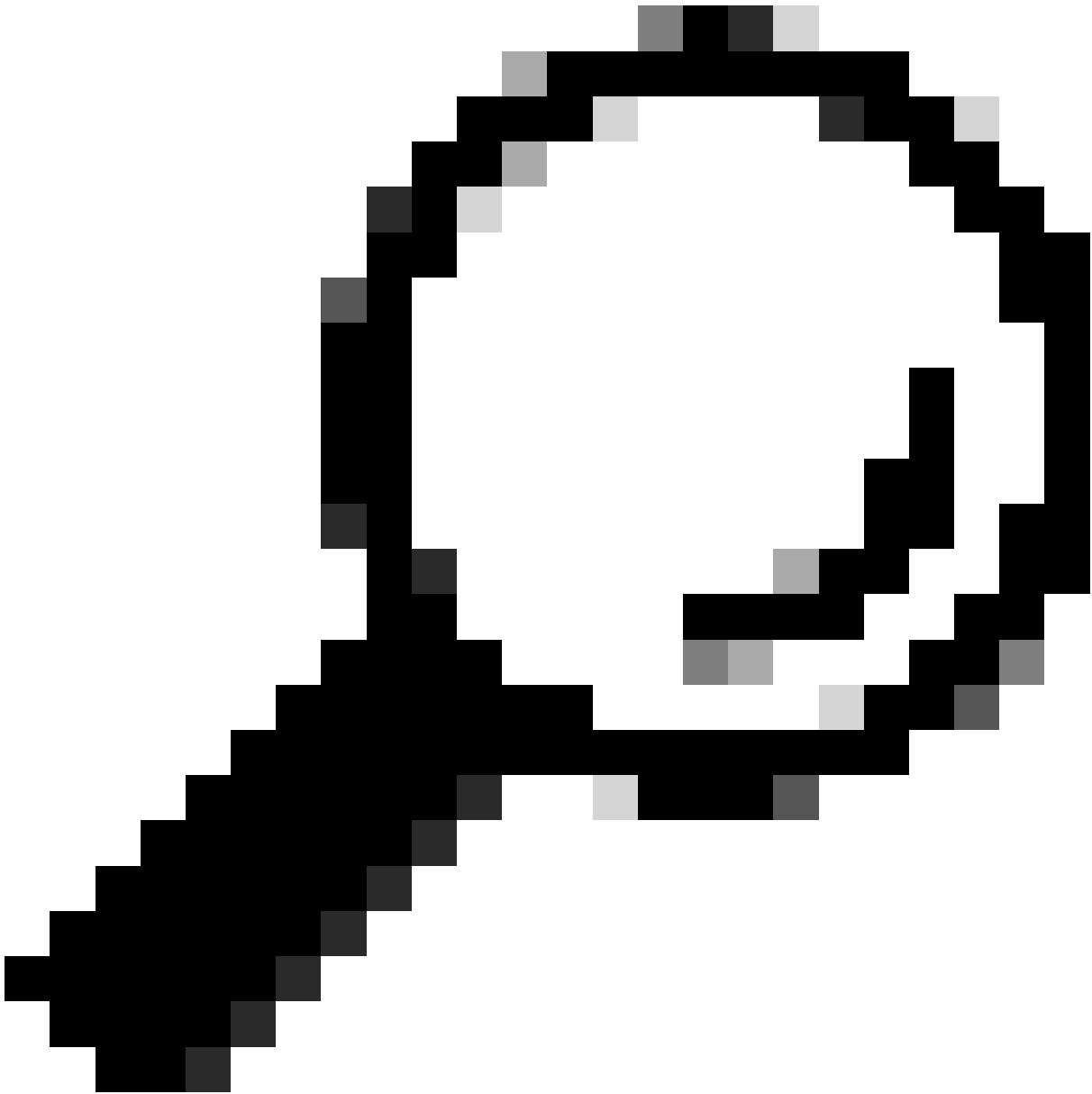
- 預先定義的篩選
- 自訂篩選條件

要從GUI使用預定義過濾器，請執行以下操作：

步驟 1. 在資料包捕獲頁面中，選擇編輯設定。

步驟 2. 從資料包捕獲過濾器中選擇預定義過濾器。

步驟 3. 在埠部分中，鍵入您要過濾的埠號。



提示：可以透過使用逗號「 , 」分隔多個埠號來增加多個埠號。

Packet Capture Filters

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

No Filters

Predefined Filters ?

Ports:

Client IP:

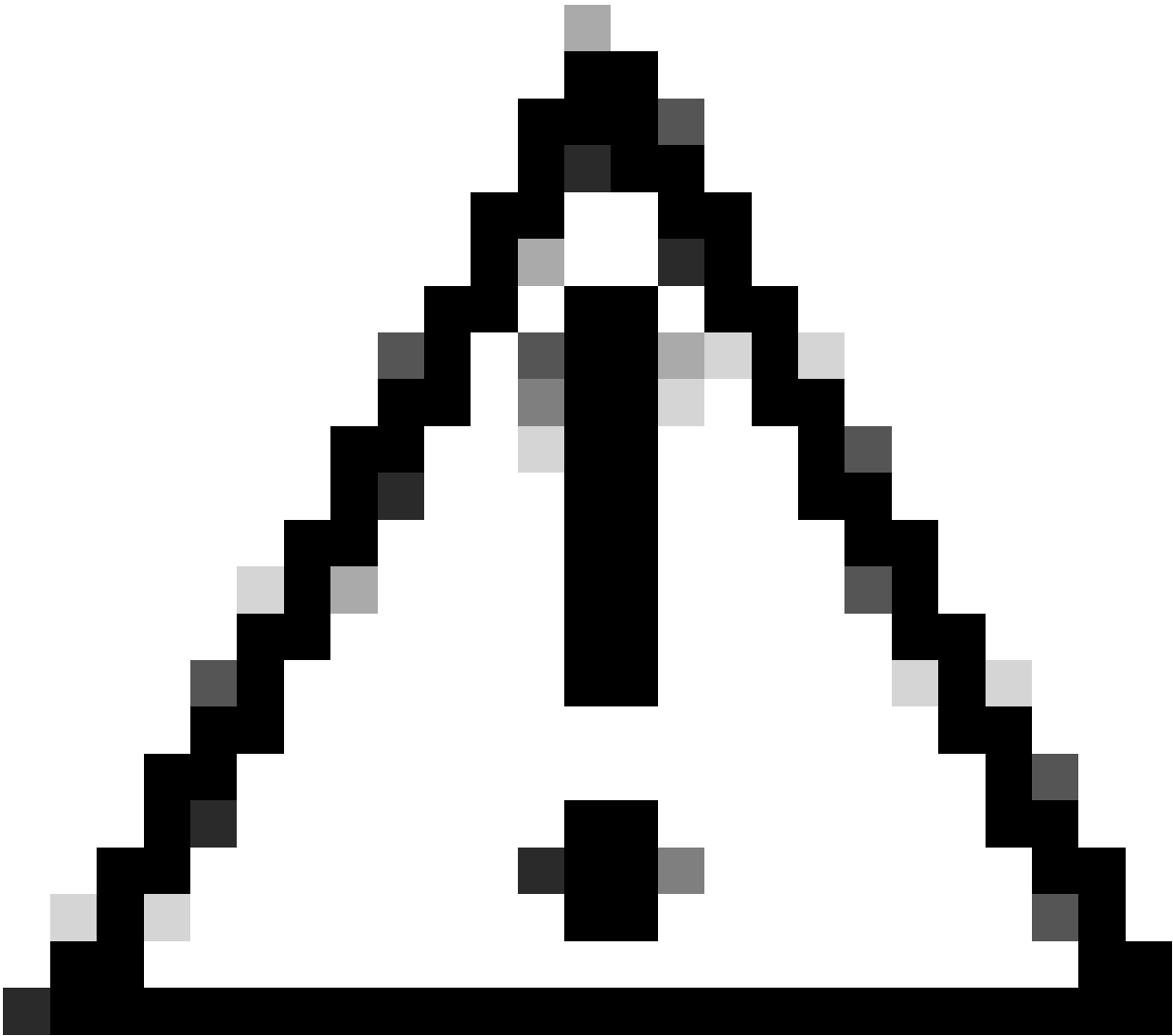
Server IP:

Custom Filter ?

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

步驟 4.提交變更。

步驟 5.開始捕獲。



注意：此方法僅捕獲具有定義埠號的TCP流量。要捕獲UDP資料流，請使用自定義過濾器。

要從GUI使用自定義過濾器，請執行以下操作：

步驟 1.在資料包捕獲頁面中，選擇編輯設定。

步驟 2.從資料包捕獲過濾器中選擇自定義過濾器。

步驟 3.請使用後跟埠號的port語法。

Packet Capture Filters

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

No Filters

Predefined Filters ?

Ports:

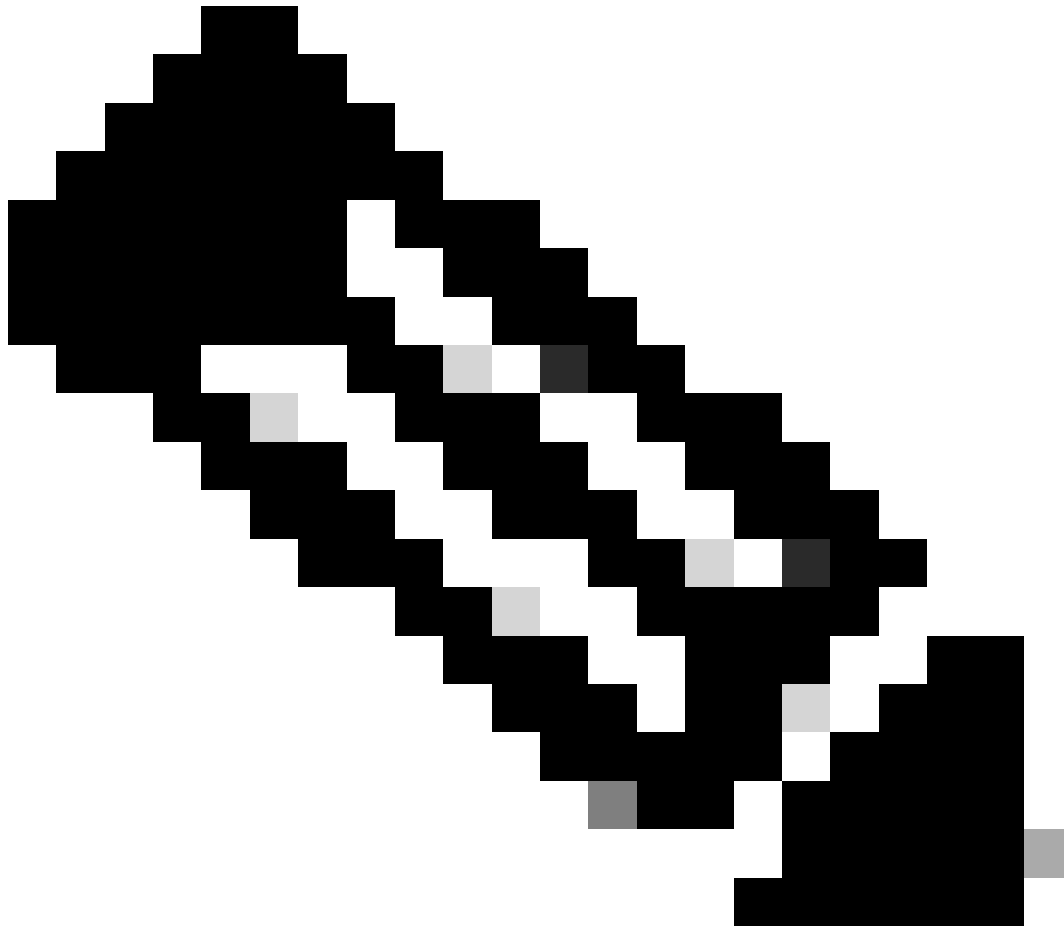
Client IP:

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.

影像-依連線埠號碼自訂濾鏡



注意：如果僅使用port，則此過濾器包括TCP和UDP埠。

步驟 4.提交變更。

步驟 5.開始捕獲。

在CLI中按埠號過濾

要在CLI中按埠號過濾，請執行以下操作：

步驟 1.登入到CLI。

步驟 2.鍵入packetcapture，然後按Enter。

步驟 3. 要編輯當前過濾器，請鍵入SETUP。

步驟 4.回答問題，直到您到達輸入用於捕獲的過濾器

步驟 5. 您可以使用與GUI中的自定義過濾器相同的過濾器字串。

以下示例為TCP和UDP埠過濾源或目標埠號為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
```

在具有透明部署的SWA中過濾

在使用透明部署的SWA中，Web快取通訊協定(WCCP)連線透過通用路由封裝(GRE)隧道，傳入或傳出SWA的資料包中的源和目標IP地址是路由器IP地址和SWA IP地址。

要從GUI使用IP地址或埠號收集資料包捕獲，有兩個選項：

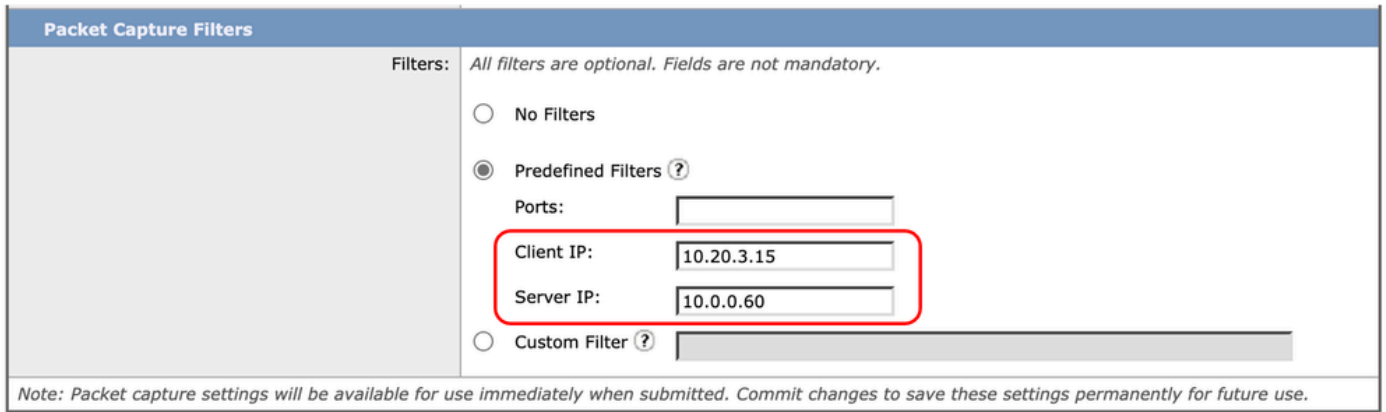
- 預先定義的篩選
- 自訂篩選條件

在SWA中使用透明部署在GUI中過濾

步驟 1.在「資料包捕獲」頁中，選擇編輯設定。

步驟 2.在Packet Capture Filters中選擇Predefined Filters。

步驟 3.可以在客戶端IP或伺服器IP部分輸入IP地址。



Packet Capture Filters

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

No Filters

Predefined Filters ?

Ports:

Client IP:

Server IP:

Custom Filter ?

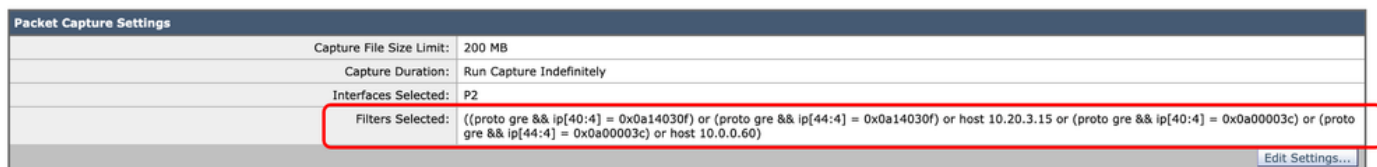
Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.

圖-在預定義過濾器中配置IP地址

步驟 4.提交變更。

步驟 5.開始捕獲。

備註：您可以在提交過濾條件後看到，SWA在「已選取的過濾條件」部分中增加了額外的條件。



映像- SWA為收集GRE隧道內的資料包而增加的額外過濾器

要從GUI使用自定義過濾器，請執行以下操作：

步驟 1.在「資料包捕獲」頁中，選擇編輯設定。

步驟 2.在資料包捕獲過濾器中，選擇自定義過濾器

步驟 3.首先增加此字串，然後增加計畫在此字串後實施的過濾器(或位於其後)：

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

例如，如果計畫按主機IP等於10.20.3.15或埠號等於8080進行過濾，則可以使用以下字串：

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

步驟 4.提交變更。

步驟 5.開始捕獲。

在SWA中使用透明部署在CLI中過濾

要從CLI過濾透明代理部署，請執行以下操作：

步驟 1.登入到CLI。

步驟 2.鍵入packetcapture，然後按Enter。

步驟 3. 要編輯當前過濾器，請鍵入SETUP。

步驟 4.回答問題，直到您到達輸入用於捕獲的過濾器

步驟 5. 您可以使用與GUI中的自定義過濾器相同的過濾器字串。

以下範例顯示依照主機IP等於10.20.3.15或連線埠編號等於8080進行過濾：

```
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.

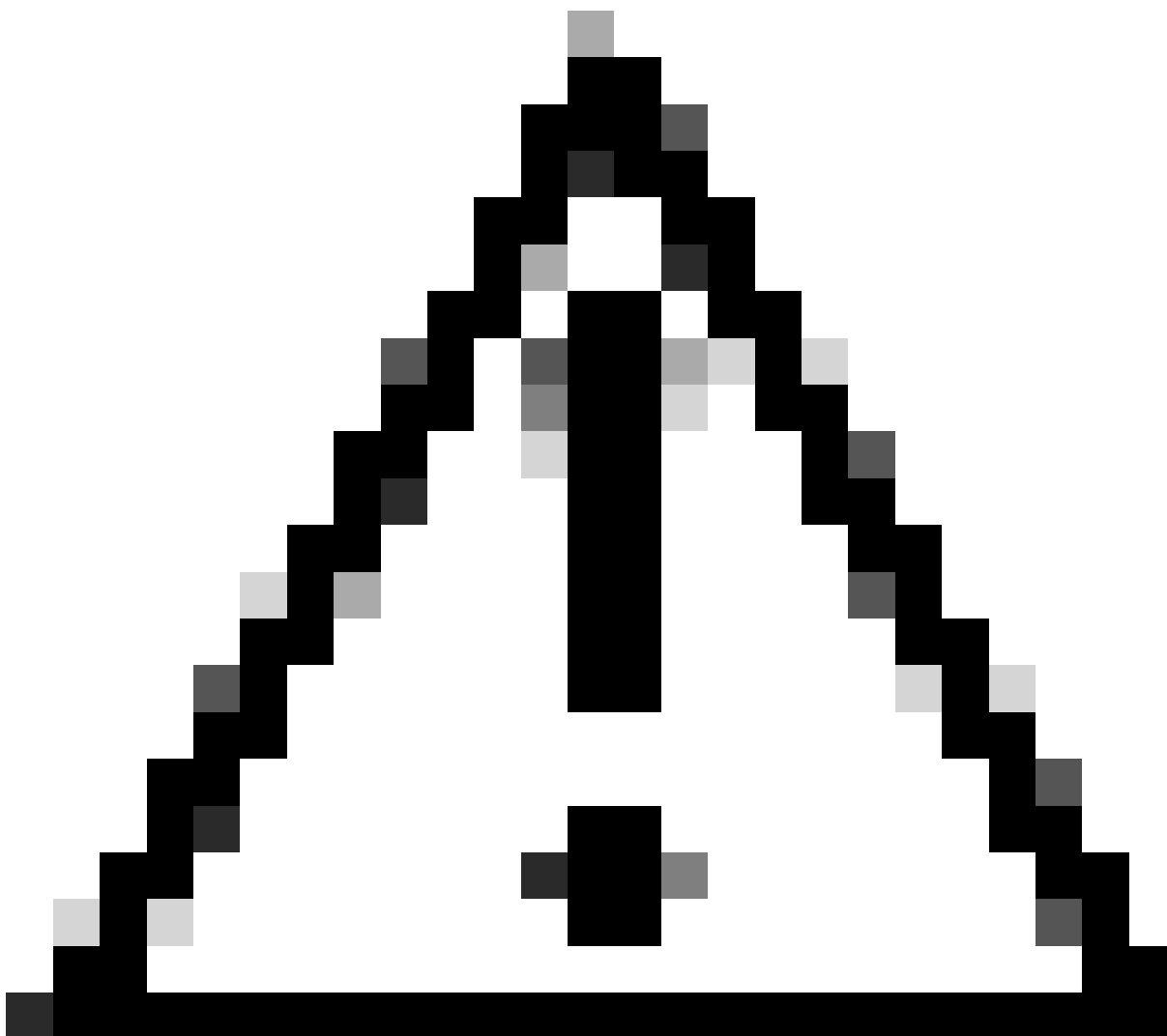
Enter the word "CLEAR" to clear the filter and capture all packets on the selected interfaces.

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

最常見的過濾器

以下表格列出最常見的篩選條件：

說明	篩選
按源IP地址等於10.20.3.15過濾	src host 10.20.3.15
按目標IP地址等於10.20.3.15過濾	dst主機10.20.3.15
按源IP地址等於10.20.3.15和目標IP地址等於10.0.0.60進行過濾	(src host 10.20.3.15)和(dst host 10.0.0.60)
按源或目標IP地址等於10.20.3.15過濾	主機10.20.3.15
按源或目標IP地址等於10.20.3.15或等於10.0.0.60過濾	host 10.20.3.15或host 10.0.0.60
按TCP埠號等於8080進行過濾	tcp埠8080
按UDP埠號等於53過濾	udp埠53
按等於514的埠號過濾 (TCP或UDP)	埠514
僅過濾UDP資料包	udp
僅過濾ICMP資料包	icmp
用於透明部署中每次捕獲的主過濾器	(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：所有篩選器都區分大小寫。

疑難排解

「過濾器錯誤」是執行資料包捕獲時最常見的錯誤之一。

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...

影象-過濾器錯誤

此錯誤通常與錯誤的過濾器實現有關。在前面的示例中，ICMP過濾器使用大寫字元。這就是您收到 Filter Error 的原因。要解決此問題，需要編輯過濾器並使用 icmp 替換 ICMP。

相關資訊

- [Cisco Secure Web Appliance - GD \(常規部署\) 的 AsyncOS 15.0 使用手冊-分類終端.....](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。