Configurazione dell'acquisizione pacchetti su Content Security Appliance

Sommario

Introduzione

In questo documento viene descritta l'acquisizione di pacchetti su Cisco Secure Web Appliance (SWA), Email Security Appliance (ESA) e Security Management Appliance (SMA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione di Cisco Content Security Appliance.

Cisco raccomanda:

- SWA/ESA/SMA fisico o virtuale installato.
- Accesso amministrativo all'interfaccia grafica utente (GUI) SWA/ESA/SMA.

- Accesso amministrativo all'interfaccia CLI (Command Line Interface) SWA/ESA/SMA

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Acquisizione pacchetti dalla GUI

Per eseguire l'acquisizione dei pacchetti dalla GUI, attenersi alla seguente procedura:

Passaggio 1. Accedere alla GUI.

Passaggio 2. Nella parte superiore destra della pagina scegliere Supporto e Guida.

Passaggio 3. Selezionare Packet Capture.

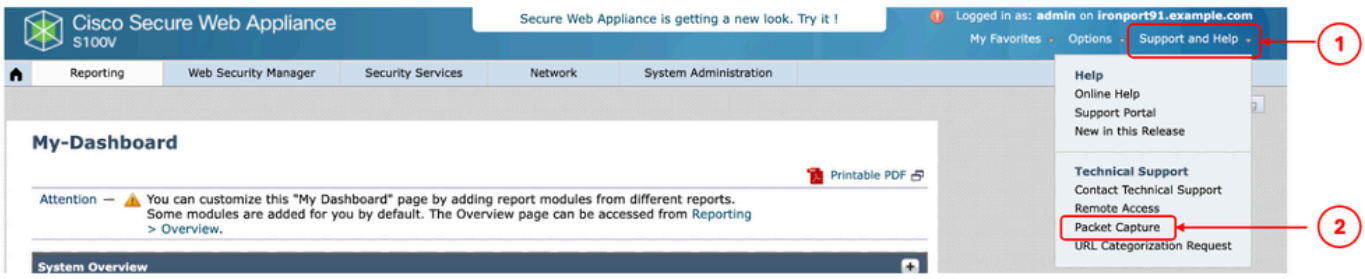


Immagine - Acquisizione pacchetto

Passaggio 4. (Facoltativo) Per modificare il filtro corrente, scegliere Modifica impostazioni. (Per ulteriori informazioni sui filtri, consultare la sezione Filtri in questo documento)

Passaggio 5. Avviare la cattura.

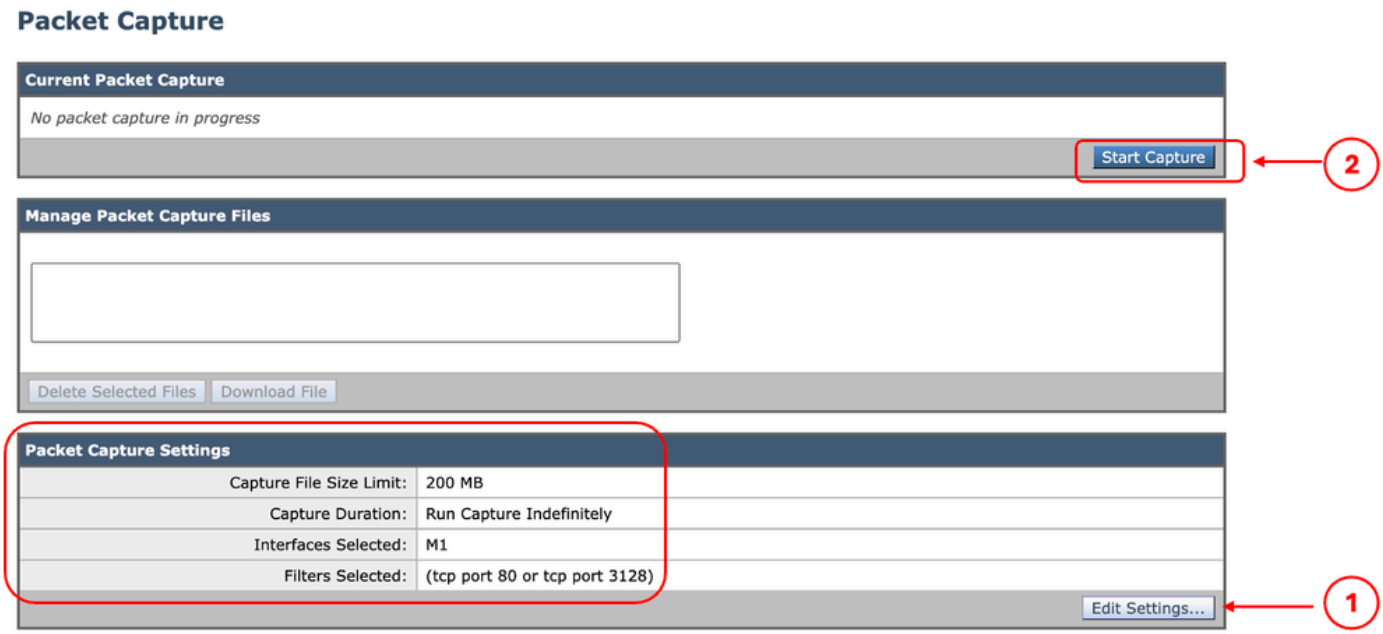
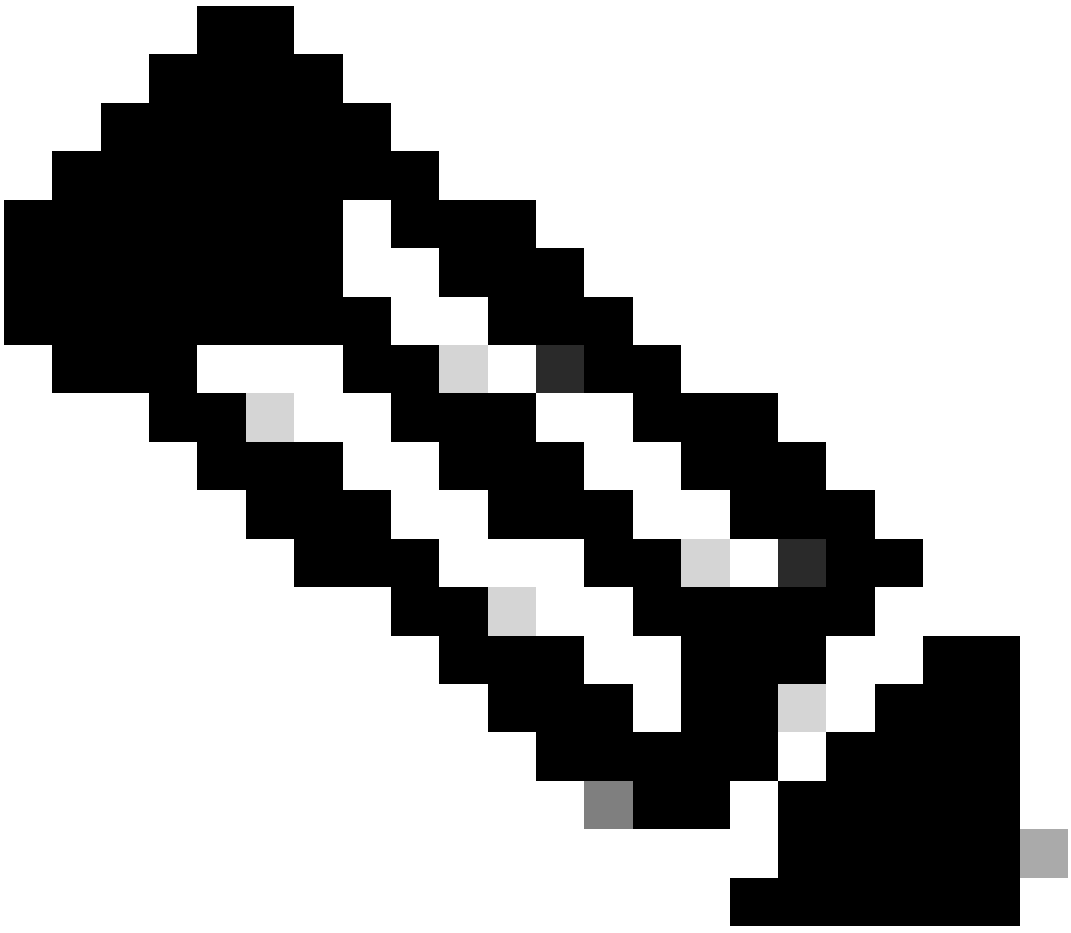


Immagine - Stato e filtri di acquisizione pacchetti



Nota: le dimensioni massime del file Packet Capture sono di 200 MB. Quando le dimensioni del file hanno raggiunto i 200 MB, l'acquisizione del pacchetto si interrompe.

La sezione Current Packet Capture mostra lo stato di Packet Capture, incluse le dimensioni del file e i filtri applicati.

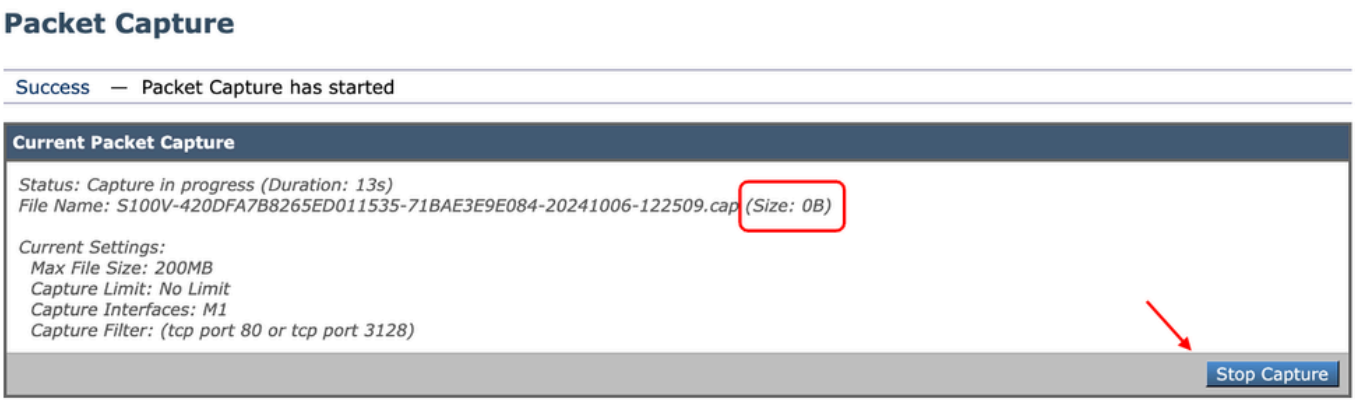
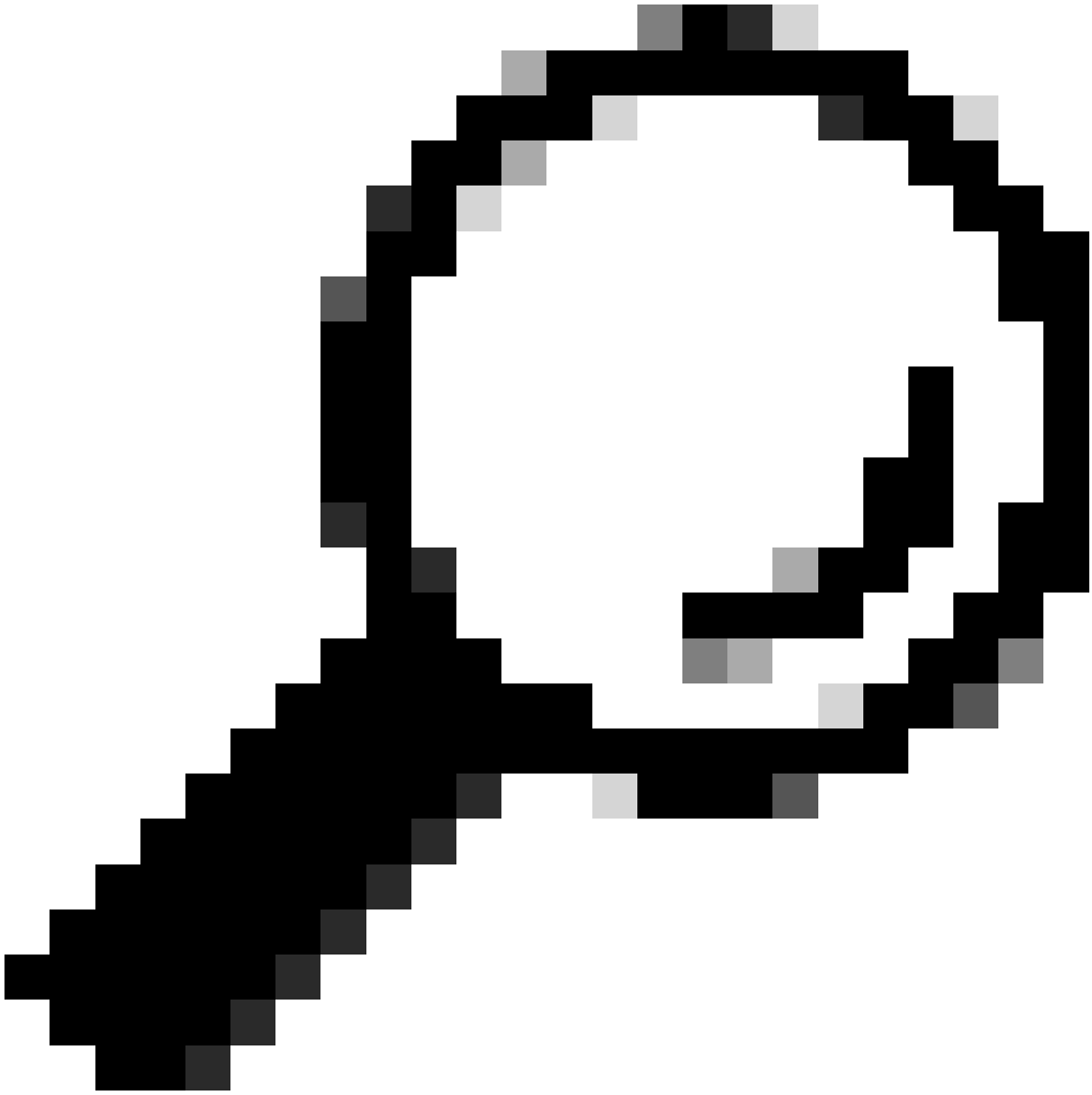


Immagine - Stato acquisizione pacchetto

Passaggio 6. Per interrompere l'acquisizione dei pacchetti in esecuzione, fare clic su Stop Capture.

Passaggio 7. Per scaricare il file Packet Capture, sceglierlo dall'elenco Gestisci file di Packet Capture e fare clic su Scarica file.

Immagine - Scarica Packet Capture



Suggerimento: l'ultimo file si trova in cima all'elenco.

Passaggio 8. (Facoltativo) Per eliminare un file di acquisizione pacchetti, scegliere il file dall'elenco Gestisci file di acquisizione pacchetti e fare clic su Elimina file selezionati.

Acquisizione pacchetti dalla CLI

È possibile avviare l'acquisizione del pacchetto dalla CLI anche attenendosi alla seguente procedura:

Passaggio 1. Accedere alla CLI.

Passaggio 2. Digitare packetcapture e premere Invio.

Passaggio 3. (Facoltativo) Per modificare il tipo di filtro corrente SETUP. (Per ulteriori informazioni sui filtri, consultare la sezione Filtri in questo documento.)

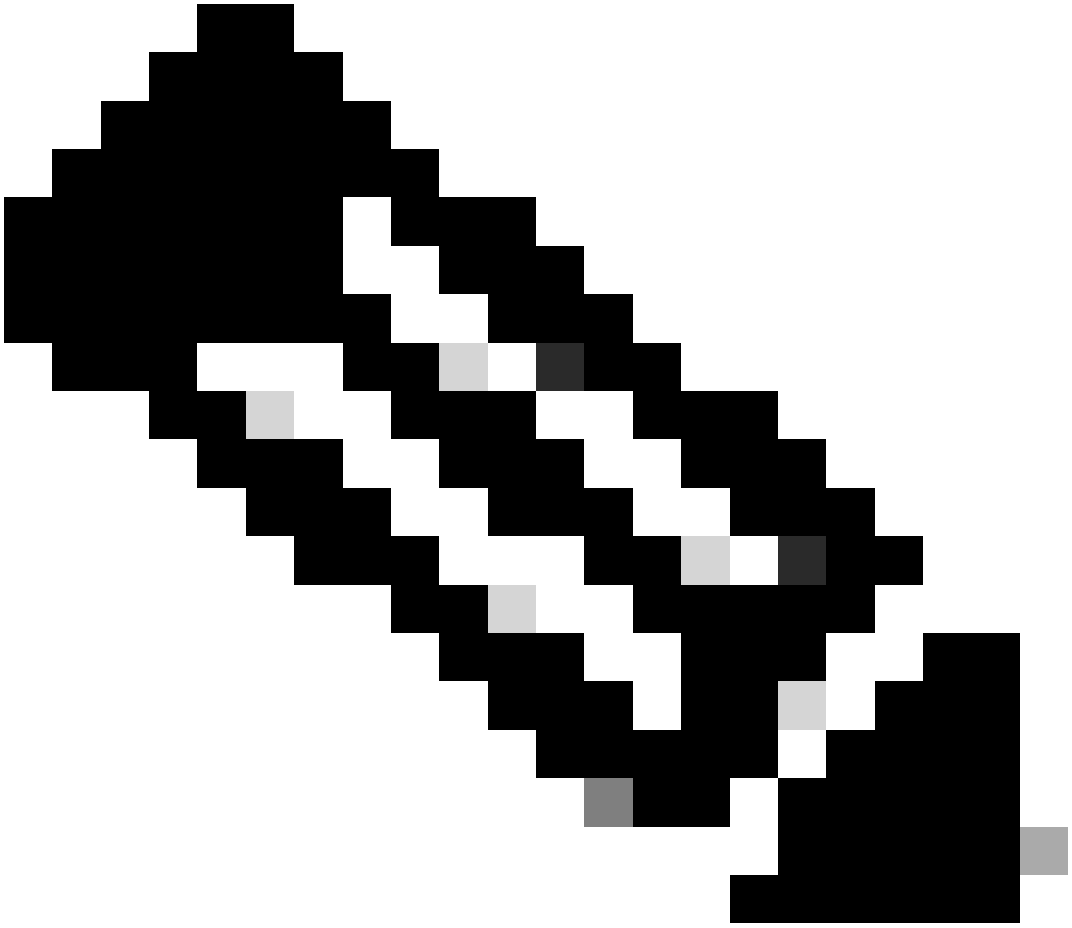
Passaggio 4. Scegliere START per avviare l'acquisizione.

```
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.
```

Passaggio 5. (Facoltativo) È possibile visualizzare lo stato di Packet Capture scegliendo 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)
```

Passaggio 6. Per interrompere l'acquisizione del pacchetto, digitare STOP e premere Invio:



Nota: per scaricare i file Packet Capture raccolti dalla CLI, è possibile scaricarli dalla GUI o collegarsi all'accessorio tramite il protocollo FTP (File Transfer Protocol) e scaricarli dalla cartella Capture.

Filtri

Di seguito sono riportate alcune guide relative ai filtri che è possibile utilizzare nelle appliance di protezione dei contenuti.

Filtra per indirizzo IP host

Filtra per IP host nella GUI

Per filtrare in base all'indirizzo IP dell'host, dalla GUI sono disponibili due opzioni:

- Filtri predefiniti

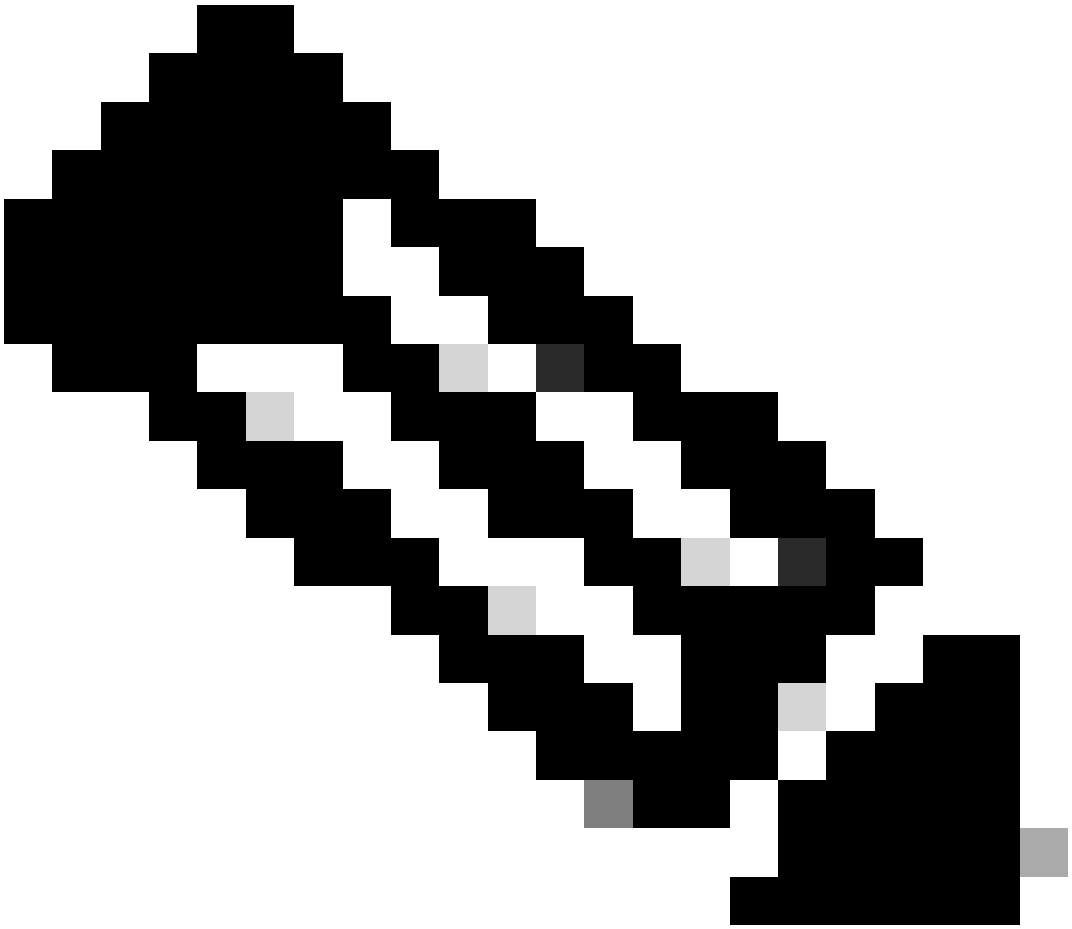
- Filtri personalizzati

Per utilizzare i filtri predefiniti dalla GUI:

Passaggio 1. Nella pagina Packet Capture, scegliere Modifica impostazioni.

Passaggio 2. Da Filtri di acquisizione pacchetti, selezionare Filtri predefiniti.

Passaggio 3. È possibile immettere l'indirizzo IP nella sezione IP client o IP server.



Nota: la scelta tra IP client o IP server non è limitata all'indirizzo di origine o di destinazione. Questo filtro acquisisce tutti i pacchetti con l'indirizzo IP definito come origine o destinazione.

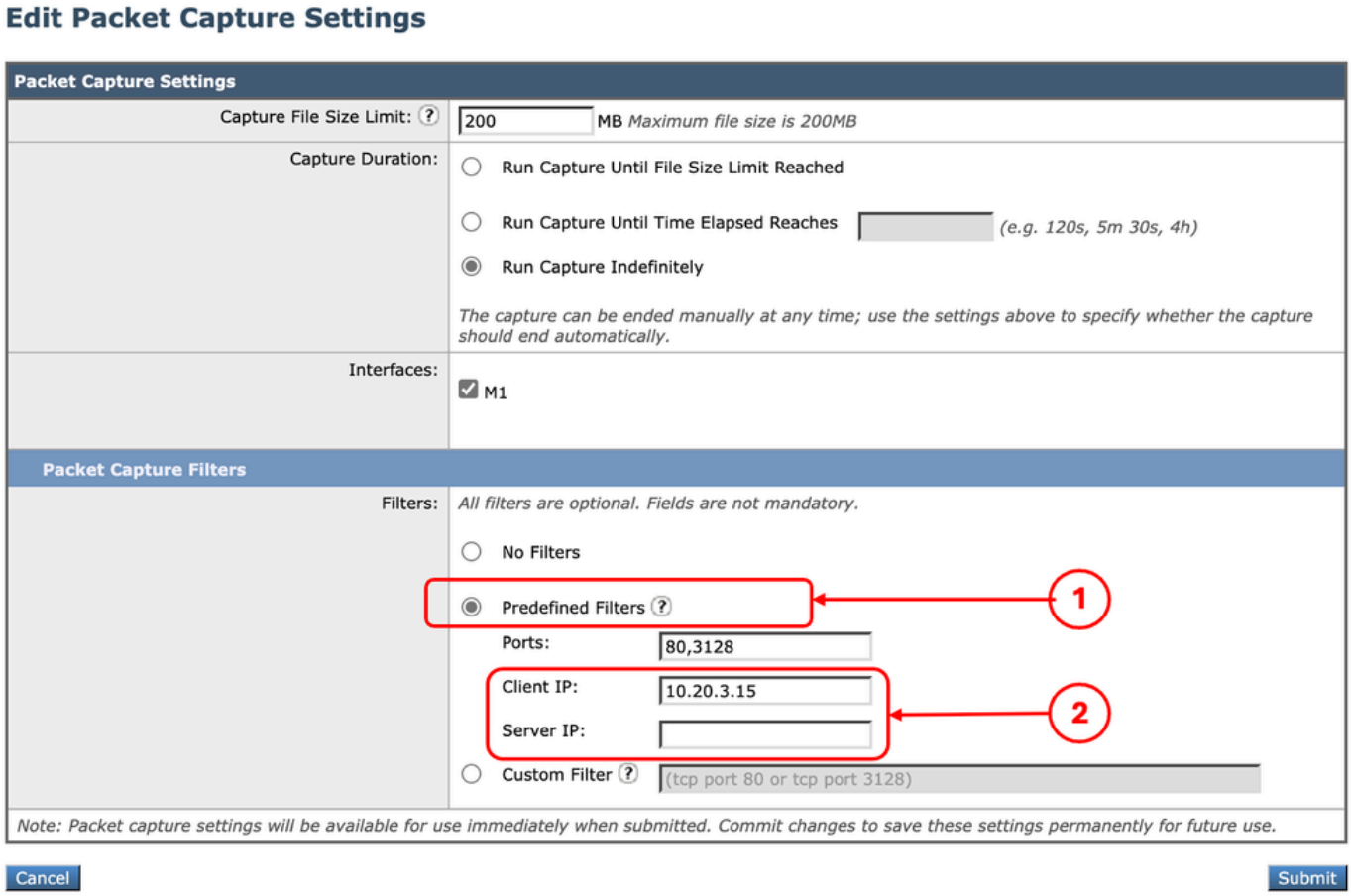
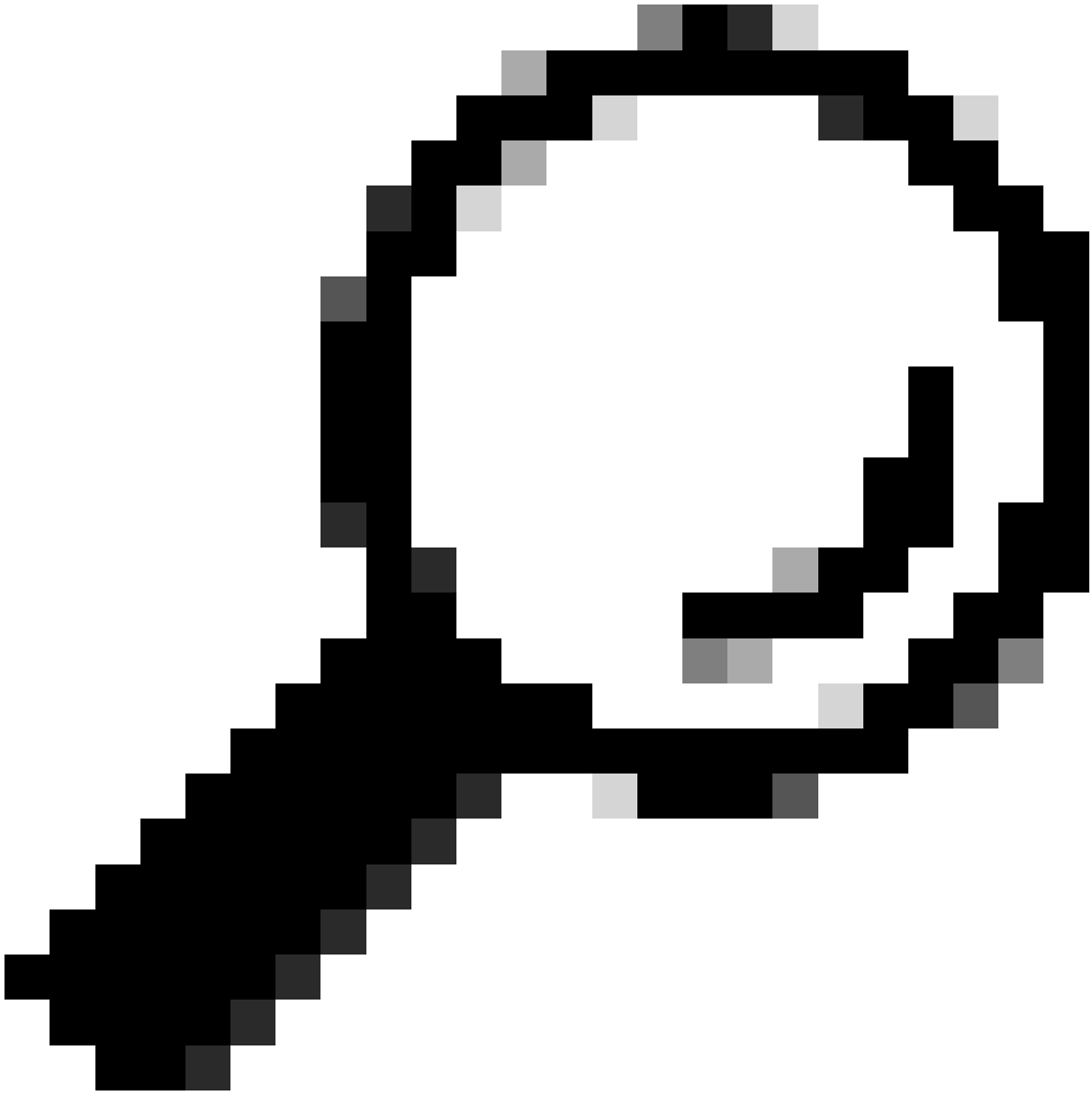


Image- Filtra per IP host da filtri predefiniti della GUI

Passaggio 4. Inviare le modifiche.

Passaggio 5. Avviare la cattura.



Suggerimento: non è necessario eseguire il commit delle modifiche, poiché il filtro appena aggiunto viene applicato all'acquisizione corrente. L'esecuzione del commit delle modifiche consente di salvare il filtro per utilizzarlo in futuro.

Per utilizzare filtri personalizzati e filtri predefiniti dalla GUI:

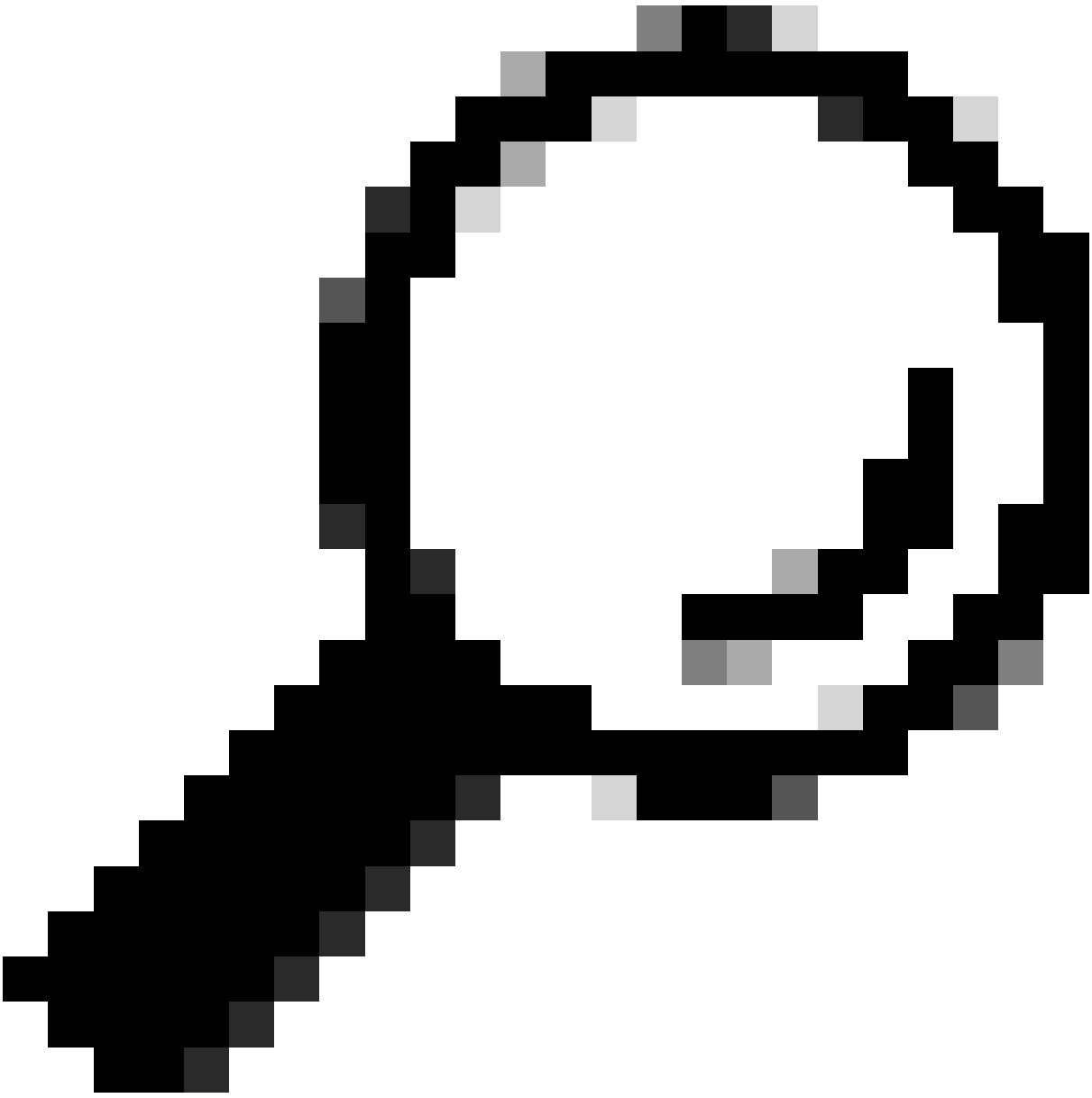
Passaggio 1. Nella pagina Packet Capture, scegliere Modifica impostazioni.

Passaggio 2. In Filtri di acquisizione pacchetti selezionare Filtro personalizzato.

Passaggio 3. Utilizzare la sintassi host seguita dall'indirizzo IP.

Di seguito è riportato un esempio per filtrare tutto il traffico con l'indirizzo IP di origine o di destinazione 10.20.3.15

```
host 10.20.3.15
```



Suggerimento: per filtrare in base a più indirizzi IP è possibile utilizzare operandi logici come o e e (solo lettere minuscole).

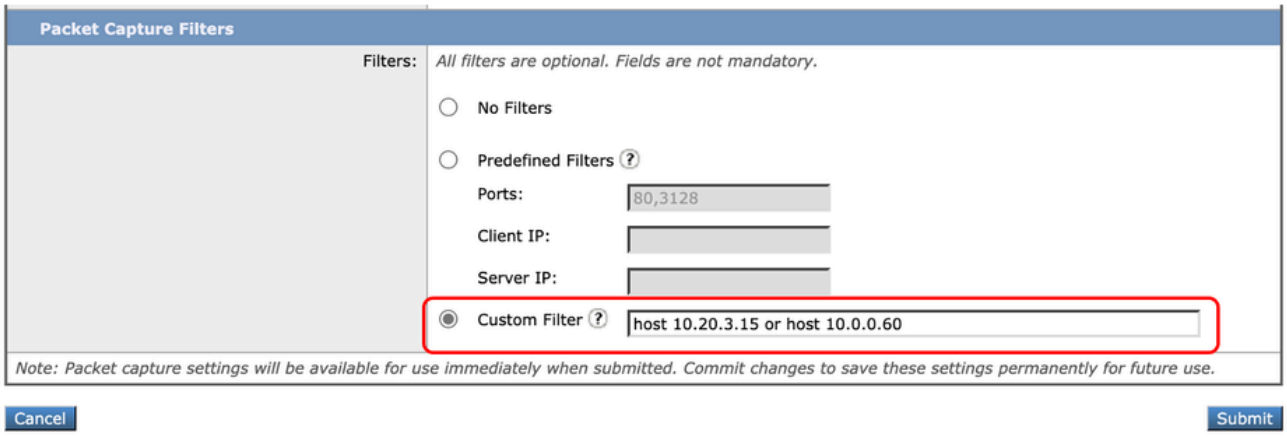


Immagine - Filtro personalizzato per due indirizzi IP

Passaggio 4. Inviare le modifiche.

Passaggio 5. Avvia l'acquisizione

Filtra per IP host nella CLI

Per filtrare dalla CLI in base all'indirizzo IP dell'host:

Passaggio 1. Accedere alla CLI.

Passaggio 2. Digitare packetcapture e premere Invio.

Passaggio 3. Per modificare il tipo di filtro corrente, digitare SETUP.

Passaggio 4. Rispondere alle domande fino a immettere il filtro da utilizzare per l'acquisizione

Passaggio 5. È possibile utilizzare la stessa stringa Filter del filtro personalizzato nell'interfaccia utente.

Di seguito è riportato un esempio di filtro di tutto il traffico con indirizzo IP di origine o destinazione 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
```

Filtra per numero di porta

Filtra per numero di porta nella GUI

Per filtrare in base ai numeri di porta, dalla GUI sono disponibili due opzioni:

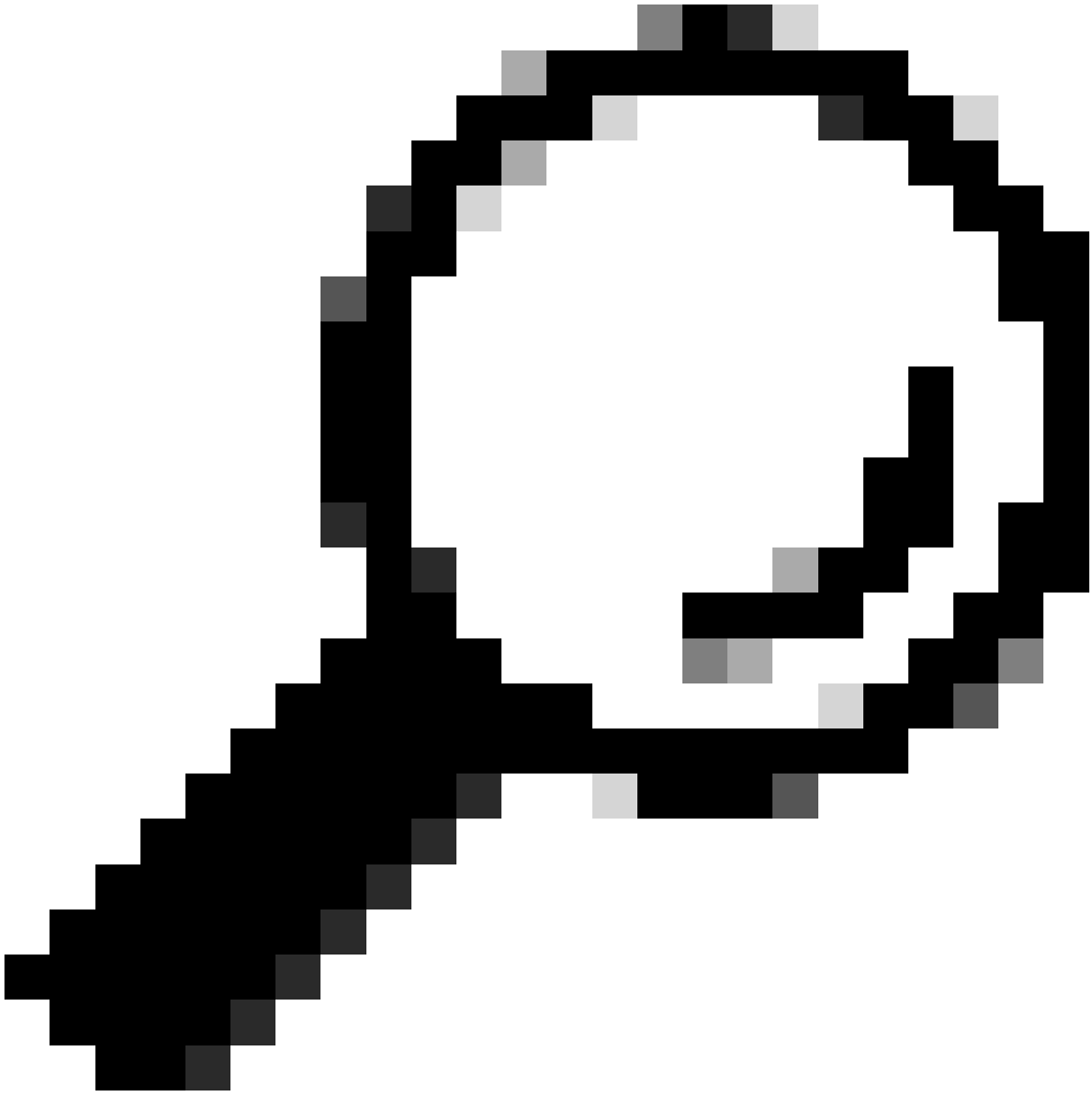
- Filtri predefiniti
- Filtri personalizzati

Per utilizzare i filtri predefiniti dalla GUI:

Passaggio 1. Nella pagina Packet Capture, scegliere Modifica impostazioni.

Passaggio 2. In Filtri di acquisizione pacchetti selezionare Filtri predefiniti.

Passaggio 3. Nella sezione Porte digitare i numeri di porta che si desidera filtrare.



Suggerimento: è possibile aggiungere più numeri di porta separandoli con la virgola " , ".

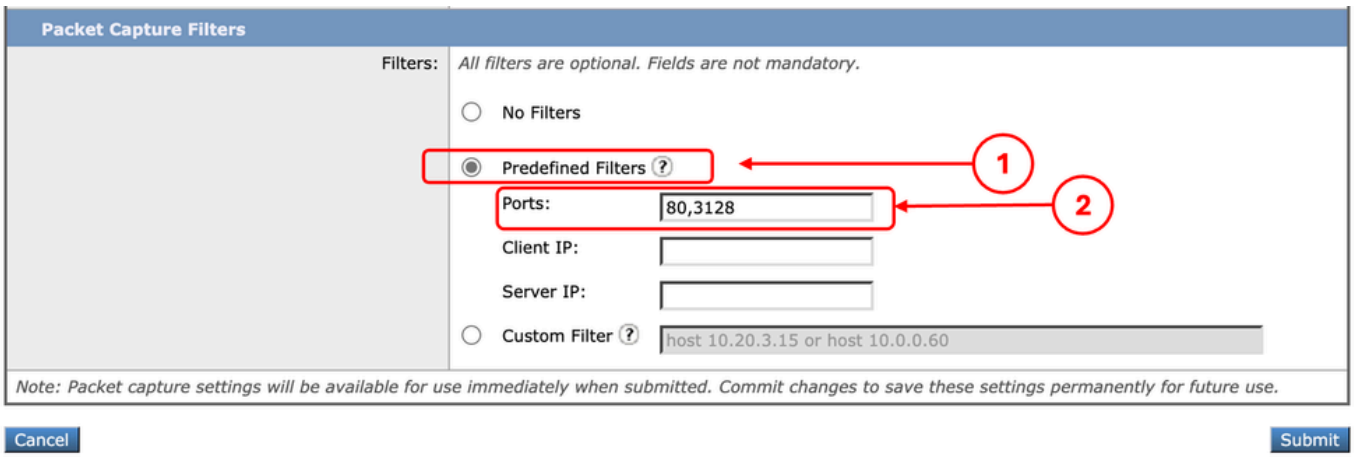
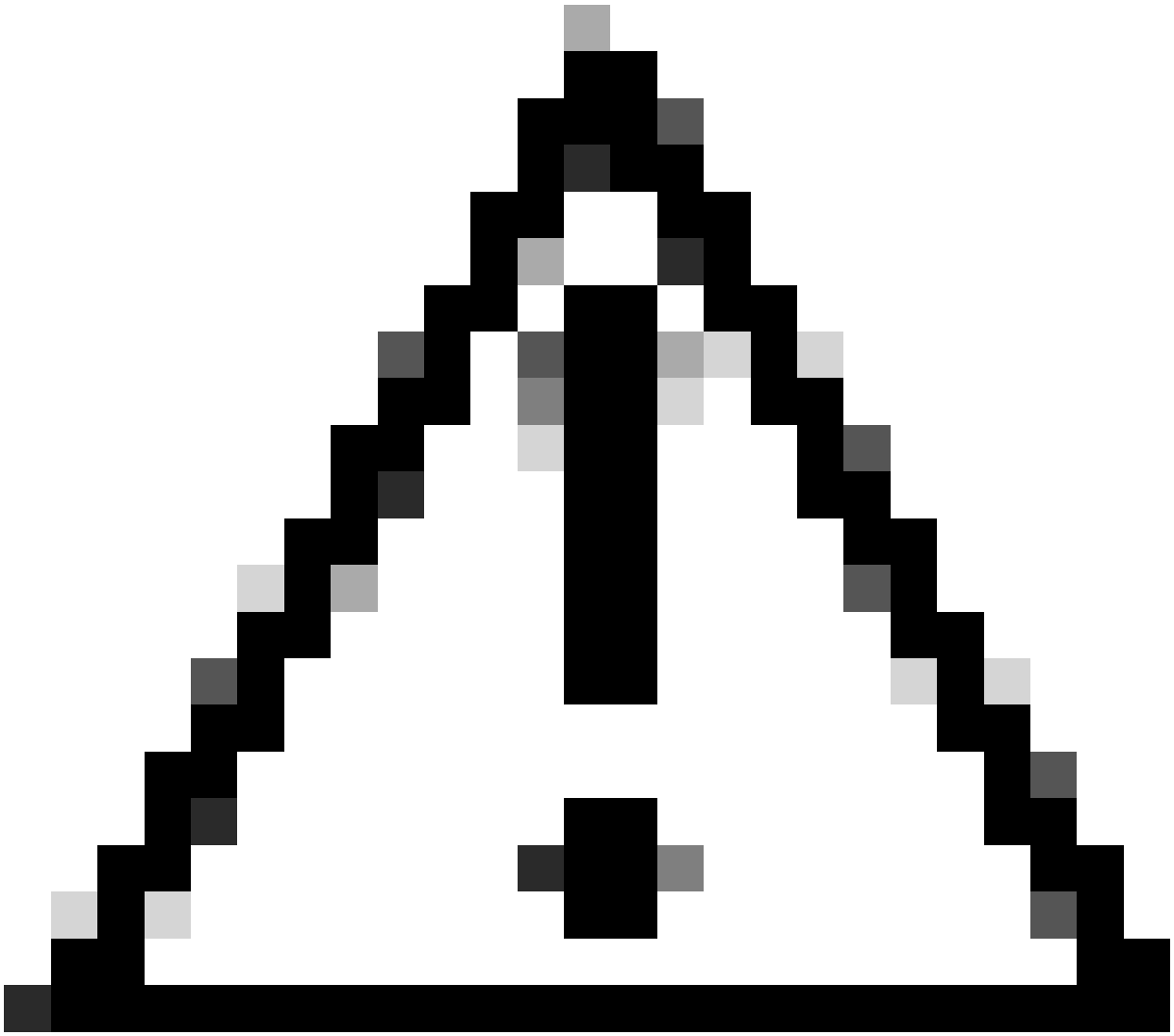


Immagine - Filtra per numero di porta

Passaggio 4. Inviare le modifiche.

Passaggio 5. Avviare la cattura.



Attenzione: questo approccio acquisisce solo il traffico TCP con i numeri di porta definiti. Per acquisire il traffico UDP, utilizzare il filtro personalizzato.

Per utilizzare filtri personalizzati dalla GUI:

Passaggio 1. Nella pagina Packet Capture, scegliere Modifica impostazioni.

Passaggio 2. In Filtri di acquisizione pacchetti selezionare Filtro personalizzato.

Passaggio 3. Utilizzare la sintassi port seguita dal numero di porta.

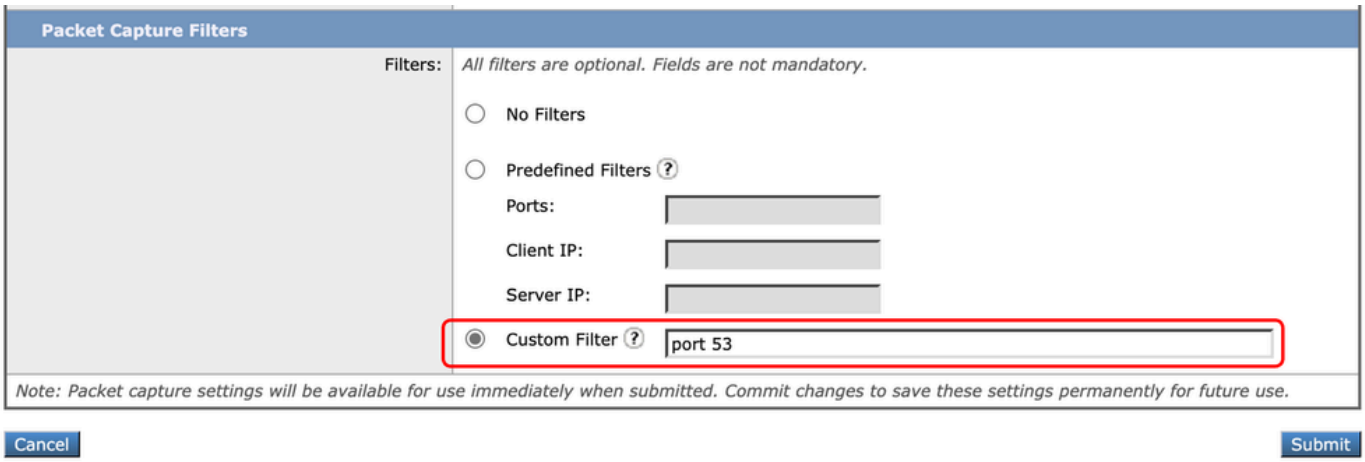
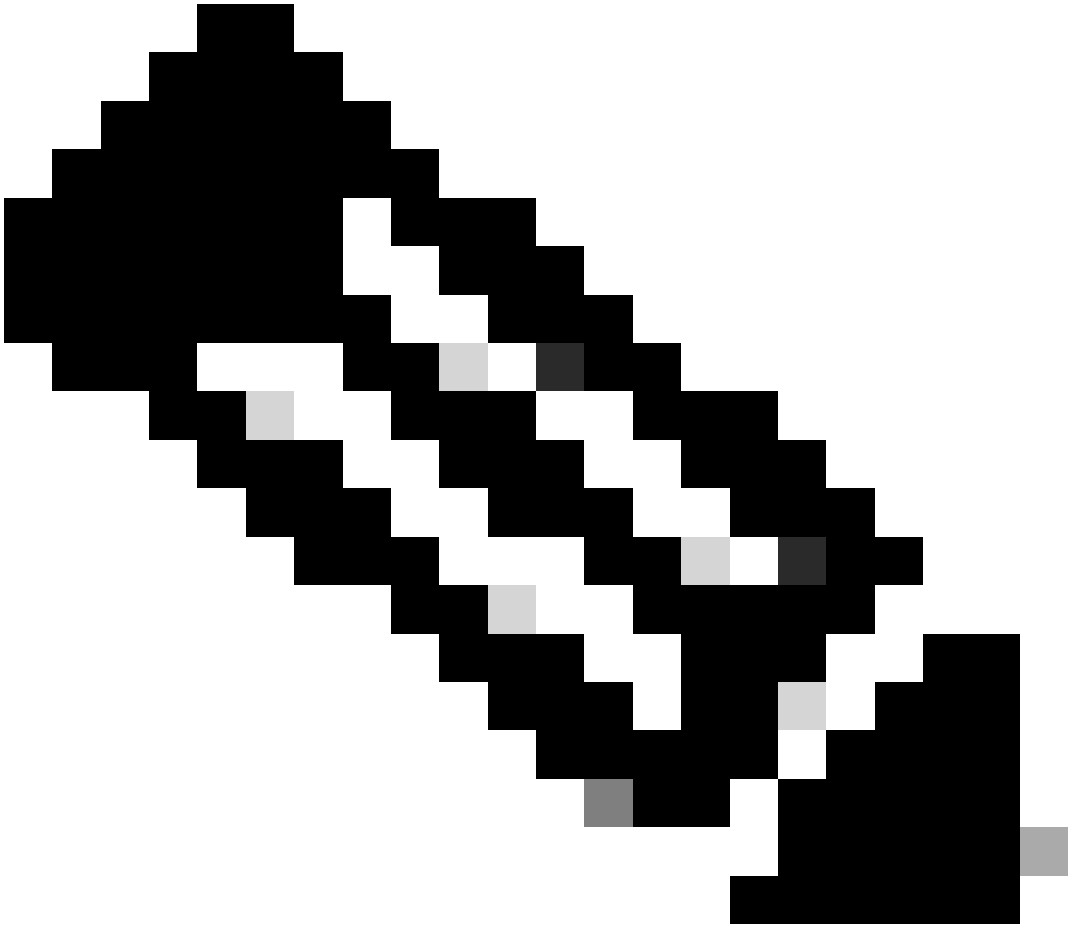


Immagine - Filtro personalizzato in base al numero di porta



Nota: se si usa solo la porta, questo filtro copre entrambe le porte TCP e UDP.

Passaggio 4. Inviare le modifiche.

Passaggio 5. Avviare la cattura.

Filtra per numero di porta nella CLI

Per filtrare in base al numero di porta dalla CLI:

Passaggio 1. Accedere alla CLI.

Passaggio 2. Digitare packetcapture e premere Invio.

Passaggio 3. Per modificare il tipo di filtro corrente, digitare SETUP.

Passaggio 4. Rispondere alle domande fino a immettere il filtro da utilizzare per l'acquisizione

Passaggio 5. È possibile utilizzare la stessa stringa Filter del filtro personalizzato nell'interfaccia utente.

Di seguito è riportato un esempio di filtro di tutto il traffico con il numero di porta di origine o di destinazione 53, sia per le porte TCP che per le porte 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
```

Filtra in SWA con distribuzione trasparente

In un'appliance SWA con distribuzione trasparente, mentre la connettività WCCP (Web Cache

Communication Protocol) avviene tramite i tunnel GRE (Generic Routing Encapsulation), gli indirizzi IP di origine e di destinazione nei pacchetti in arrivo o in uscita dall'appliance SWA sono l'indirizzo IP del router e l'indirizzo IP dell'appliance SWA.

Per poter raccogliere l'acquisizione del pacchetto con indirizzo IP o numero di porta dalla GUI, sono disponibili due opzioni:

- Filtri predefiniti
- Filtri personalizzati

Filtraggio in SWA con distribuzione trasparente nella GUI

Passaggio 1. Nella pagina Packet Capture, scegliere Modifica impostazioni.

Passaggio 2. Da Filtri di acquisizione pacchetti, selezionare Filtri predefiniti.

Passaggio 3. È possibile immettere l'indirizzo IP nella sezione IP client o IP server.

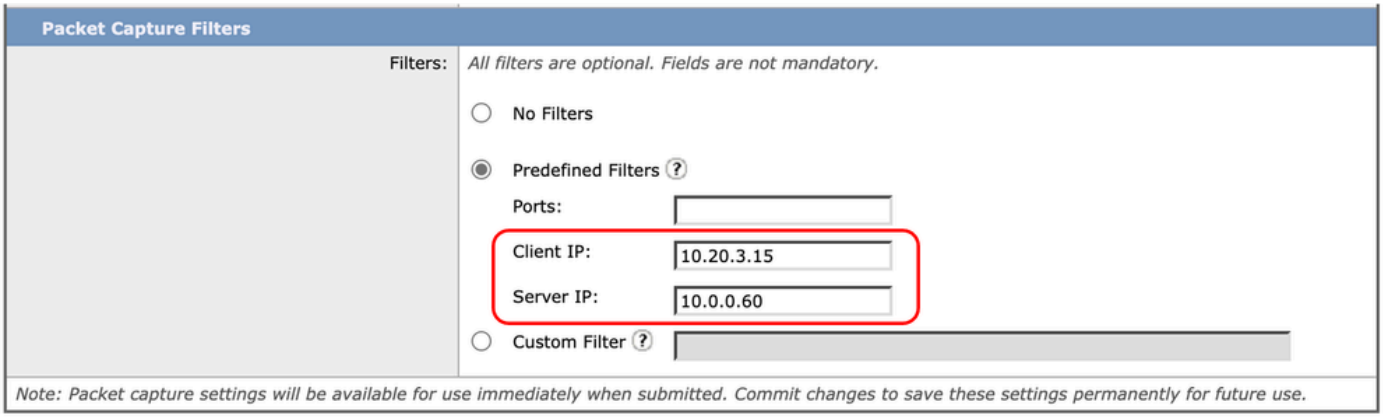
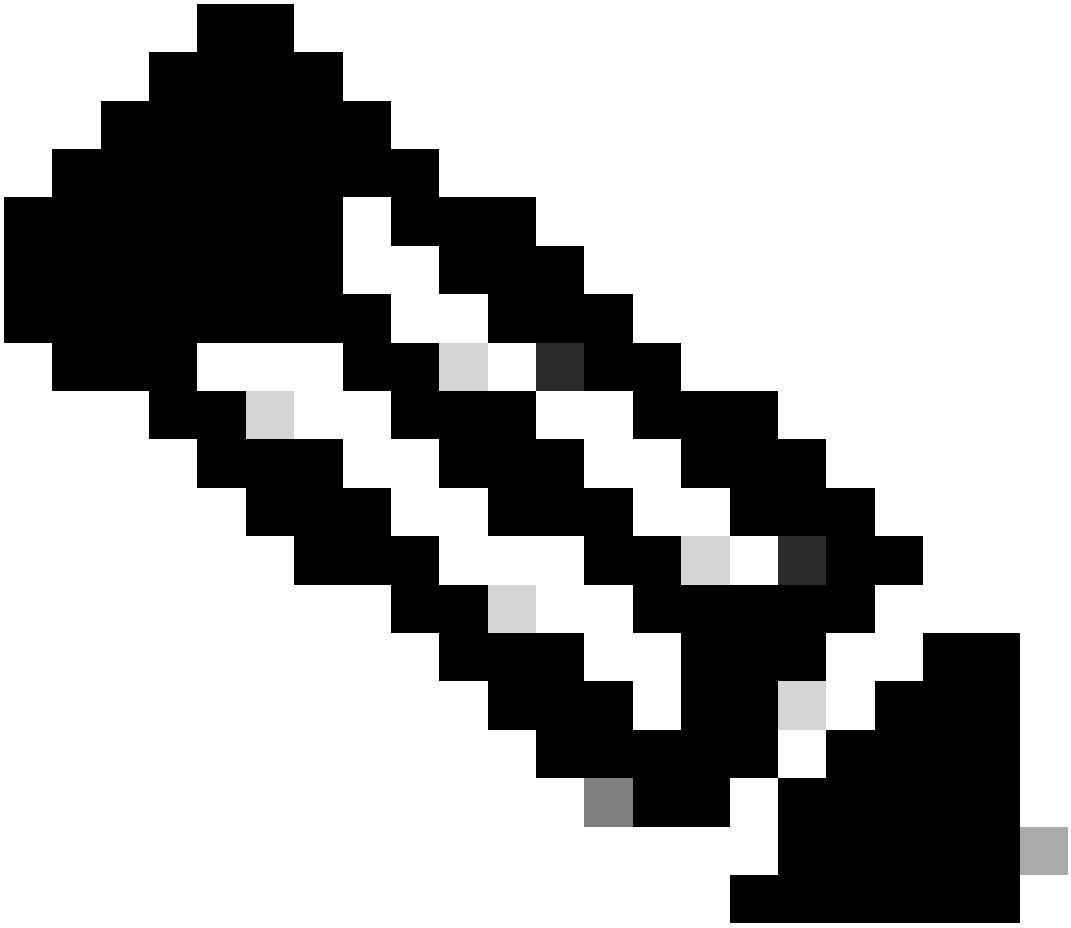


Immagine - Configurazione dell'indirizzo IP nei filtri predefiniti

Passaggio 4. Inviare le modifiche.

Passaggio 5. Avviare la cattura.



Nota: dopo aver sottomesso il filtro, SWA ha aggiunto altre condizioni nella sezione Filtro selezionato.

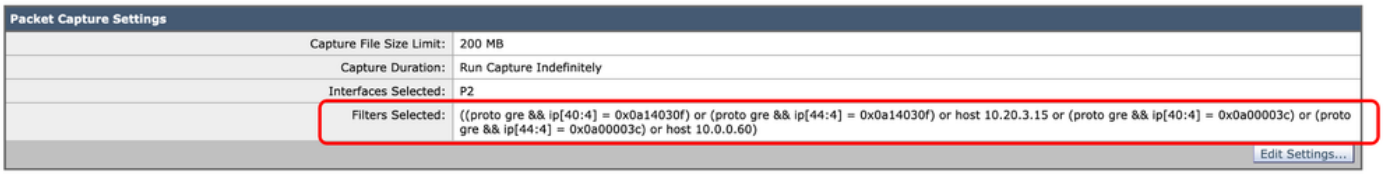


Immagine - Filtri aggiuntivi aggiunti da SWA per raccogliere pacchetti all'interno del tunnel GRE

Per utilizzare filtri personalizzati dalla GUI:

Passaggio 1. Nella pagina Packet Capture, scegliere Modifica impostazioni.

Passaggio 2. Da Filtri di acquisizione pacchetti, selezionare Filtro personalizzato

Passaggio 3. Aggiungere prima questa stringa, quindi il filtro che si desidera implementare aggiungendo o dopo questa stringa:

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

Ad esempio, se si intende filtrare in base all'indirizzo IP dell'host uguale a 10.20.3.15 o al numero di porta uguale a 8080, è possibile utilizzare la seguente stringa:

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

Passaggio 4. Inviare le modifiche.

Passaggio 5. Avviare la cattura.

Filtra in SWA con distribuzione trasparente nella CLI

Per filtrare la distribuzione proxy trasparente dalla CLI:

Passaggio 1. Accedere alla CLI.

Passaggio 2. Digitare packetcapture e premere Invio.

Passaggio 3. Per modificare il tipo di filtro corrente, digitare SETUP.

Passaggio 4. Rispondere alle domande fino a immettere il filtro da utilizzare per l'acquisizione

Passaggio 5. È possibile utilizzare la stessa stringa Filter del filtro personalizzato nell'interfaccia utente.

Di seguito è riportato un esempio di filtro in base all'indirizzo IP dell'host uguale a 10.20.3.15 o al numero di porta uguale 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
```

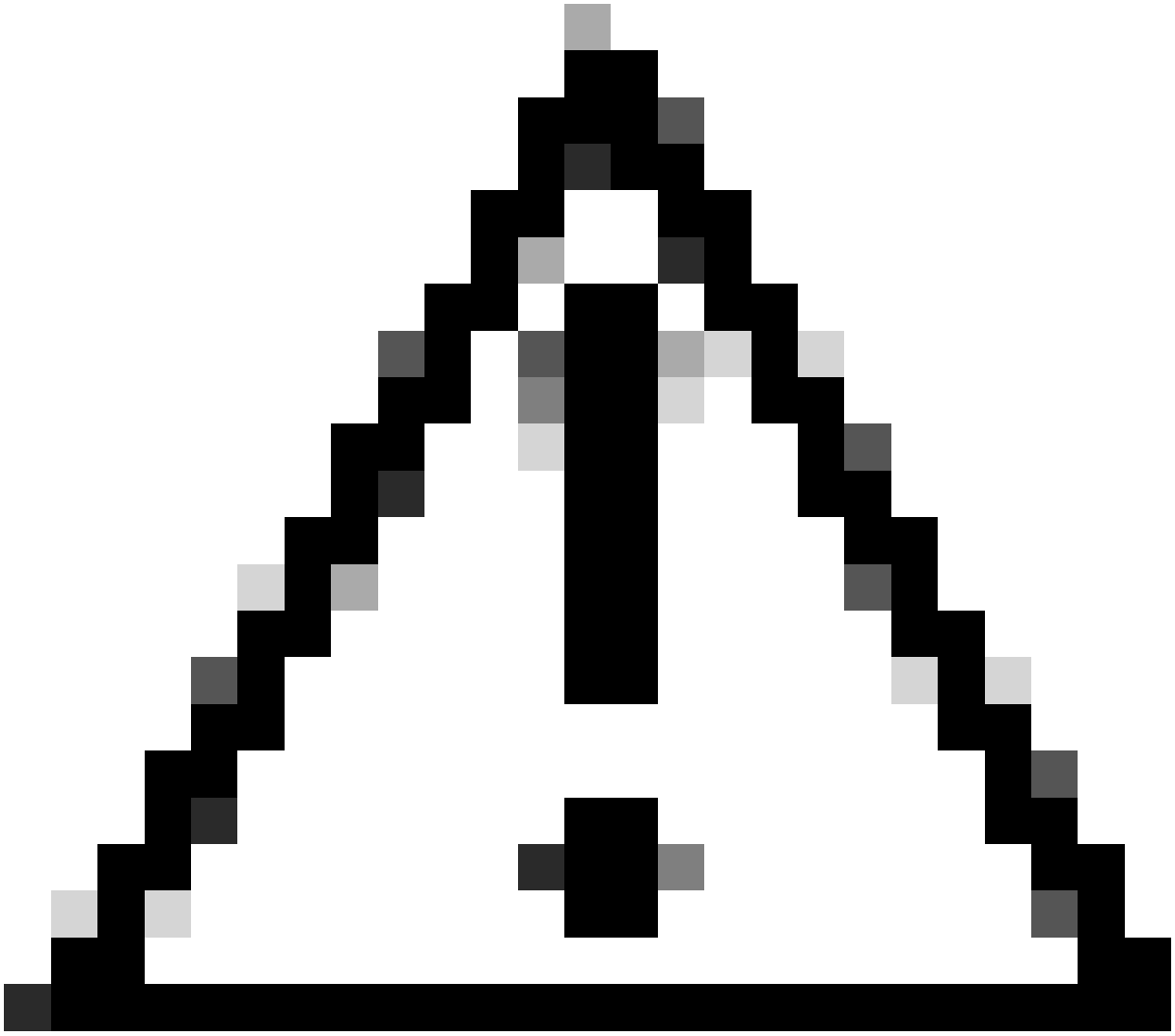
```
[N]>

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
```

Filtri più comuni

Di seguito è riportata una tabella in cui sono elencati i filtri più comuni:

Descrizione	Filtro
Filtra per indirizzo IP di origine uguale a 10.20.3.15	host src 10.20.3.15
Filtra per indirizzo IP di destinazione uguale a 10.20.3.15	host dst 10.20.3.15
Filtra per indirizzo IP di origine uguale a 10.20.3.15 e indirizzo IP di destinazione uguale a 10.0.0.60	(host src 10.20.3.15) e (host dst 10.0.0.60)
Filtra per indirizzo IP di origine o di destinazione uguale a 10.20.3.15	host 10.20.3.15
Filtra per indirizzo IP di origine o destinazione uguale a 10.20.3.15 o uguale a 10.0.0.60	host 10.20.3.15 o host 10.0.0.60
Filtra per numero di porta TCP uguale a 8080	porta tcp 8080
Filtra per UDP Numero porta uguale a 53	porta udp 53
Filtra per numero di porta uguale a 514 (TCP o UDP)	porta 514

Filtra solo pacchetti UDP	udp
Filtra solo pacchetti ICMP	icmp
Filtro principale da utilizzare per ogni acquisizione nella distribuzione trasparente	(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)



Attenzione: tutti i filtri distinguono tra maiuscole e minuscole.

Risoluzione dei problemi

"Errore filtro" è uno degli errori più comuni durante l'acquisizione del pacchetto.

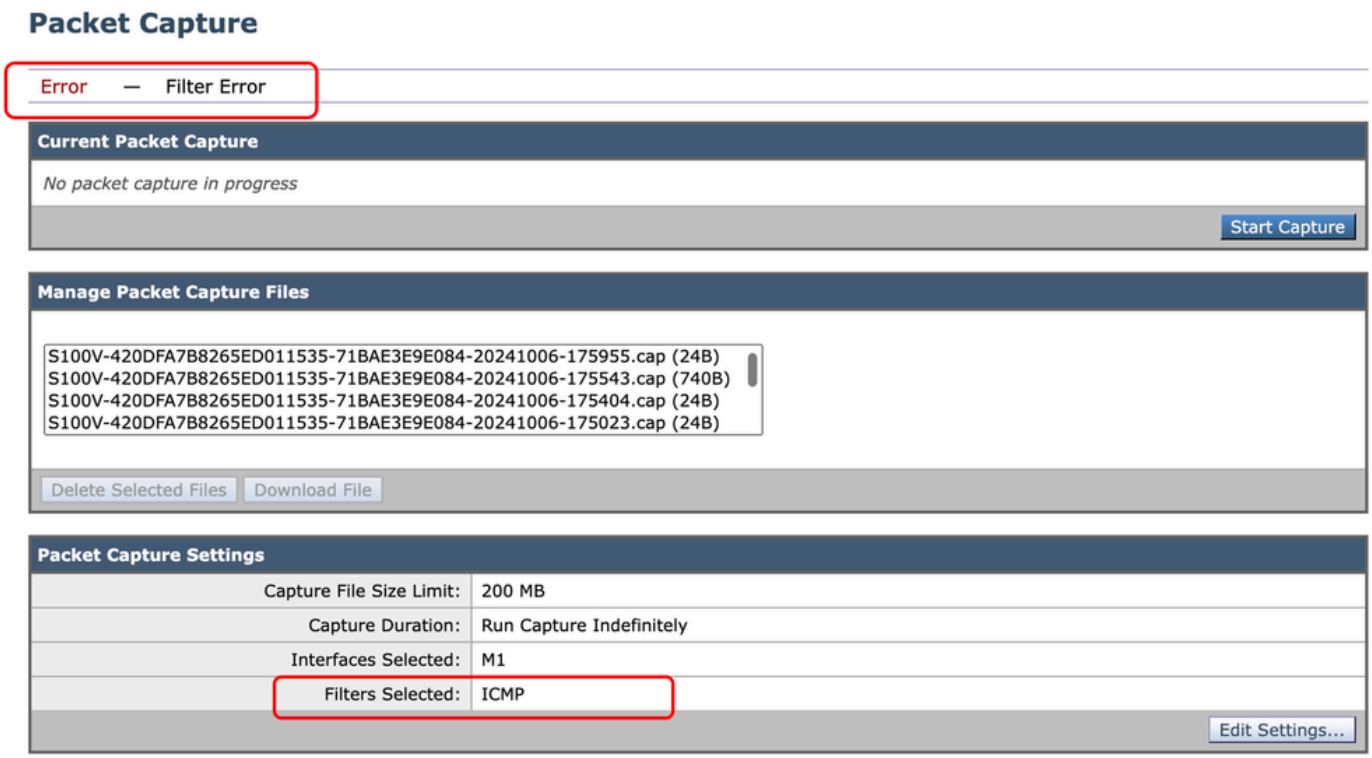


Immagine - Errore filtro

Questo errore è in genere correlato a un'implementazione errata del filtro. Nell'esempio precedente, il filtro ICMP è composto da caratteri maiuscoli. Questo è il motivo per cui si riceve l'errore di filtro. Per risolvere il problema, è necessario modificare il filtro e sostituire l'ICMP con icmp.

Informazioni correlate

- Guida per l'utente di AsyncOS 15.0 for Cisco Secure Web Appliance - GD (General Deployment) - Classify End-U...

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).