Packet Capture configureren op Content Security Applicatie

Inhoud

Inleiding

Dit document beschrijft pakketvastlegging op Cisco Secure Web Applicatie (SWA), E-mail security applicatie (ESA) en security beheer applicatie (SMA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Content Security Appliance-beheer.

Cisco raadt u aan het volgende te doen:

- Fysieke of virtuele SWA/ESA/SMA geïnstalleerd.
- Administratieve toegang tot de grafische gebruikersinterface (GUI) van SWA/ESA/SMA.

- Administratieve toegang tot de SWA/ESA/SMA Command Line Interface (CLI)

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

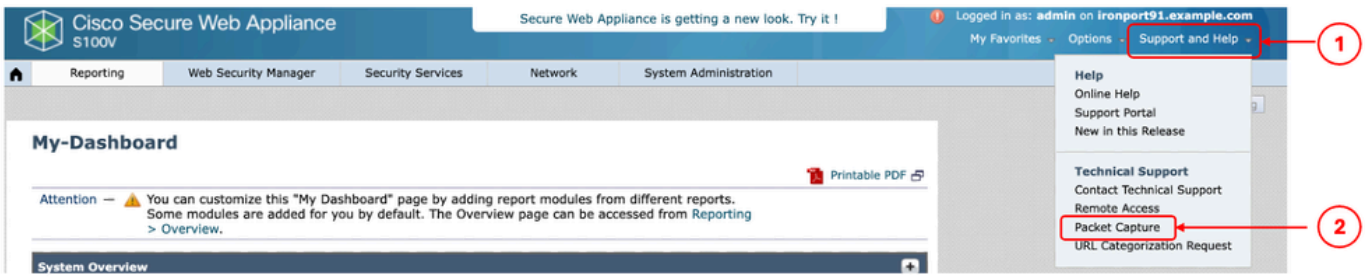
Packet Capture uitvoeren vanuit GUI

Om pakketopname van GUI uit te voeren, gebruikt u deze stappen:

Stap 1. Log in op de GUI.

Stap 2. Kies Ondersteuning en Help in de rechterbovenhoek van de pagina.

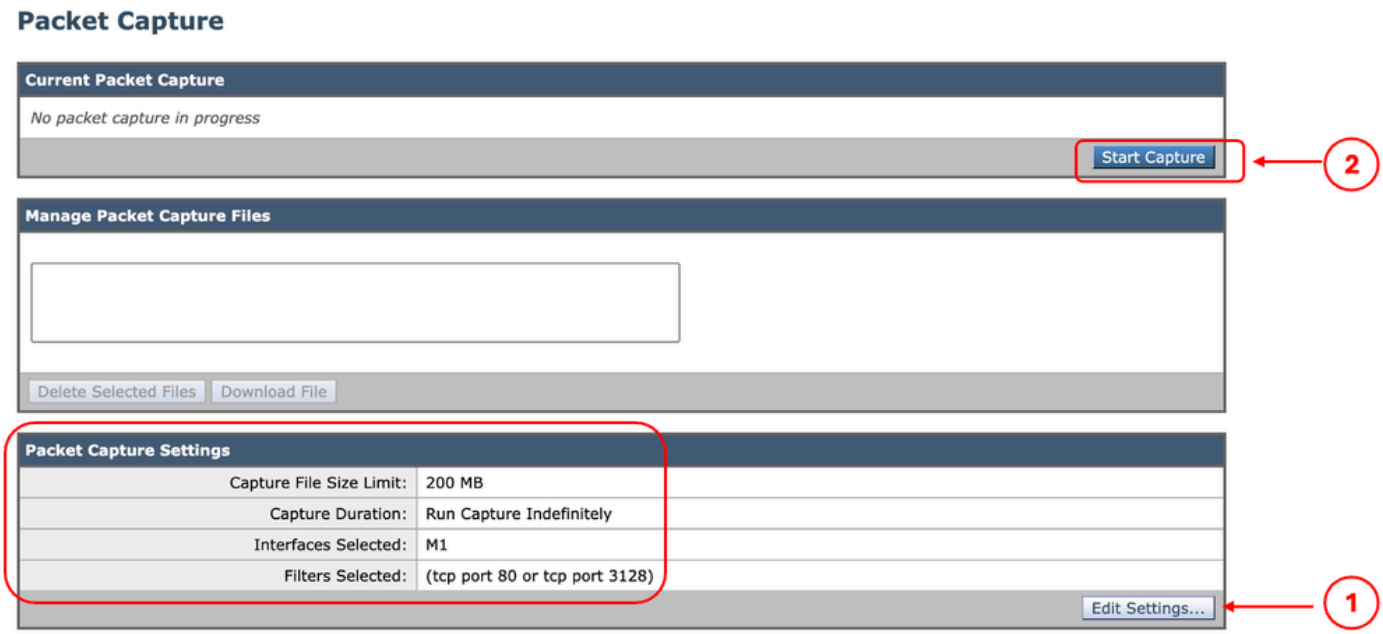
Stap 3. Selecteer Packet Capture.



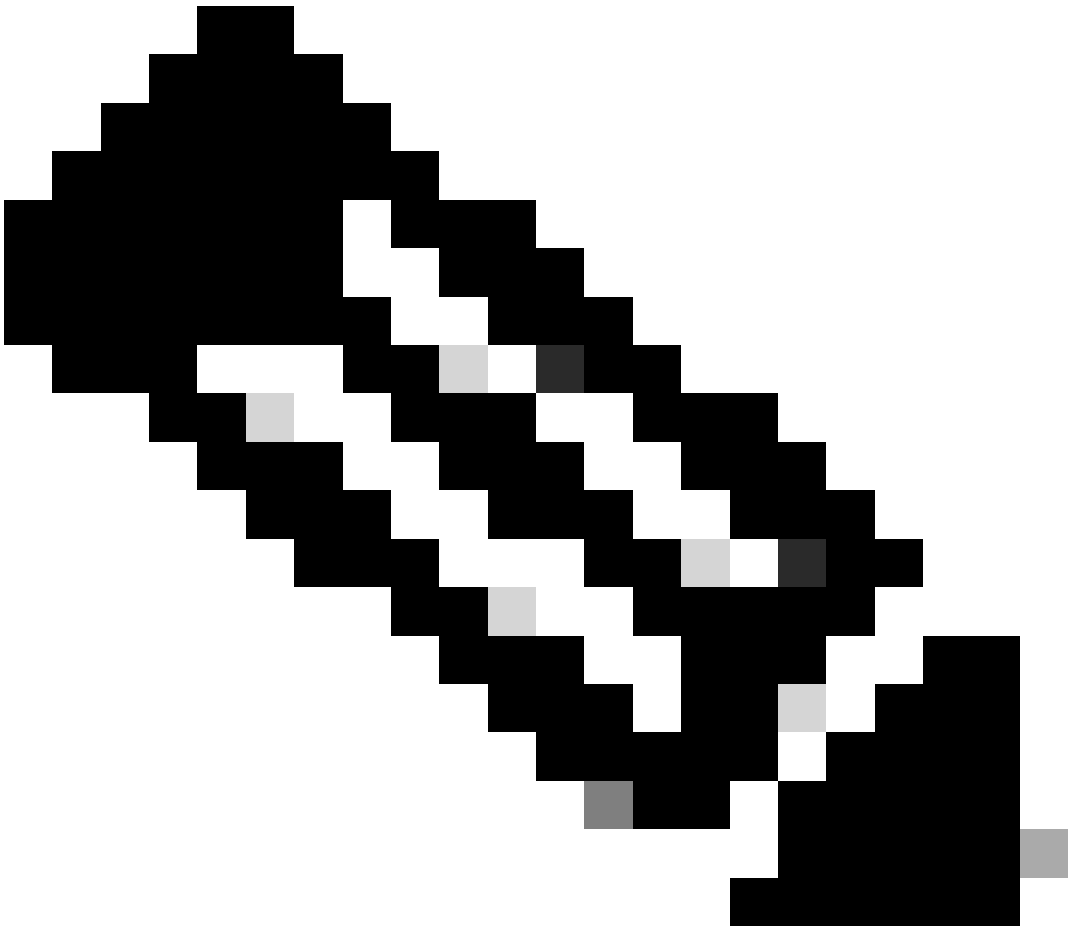
Afbeelding - PacketCapture

Stap 4. (Optioneel) Kies Instellingen bewerken als u het huidige filter wilt bewerken. (Kijk voor meer informatie over de filters in het gedeelte Filters in dit document)

Stap 5. Start de vastlegging.

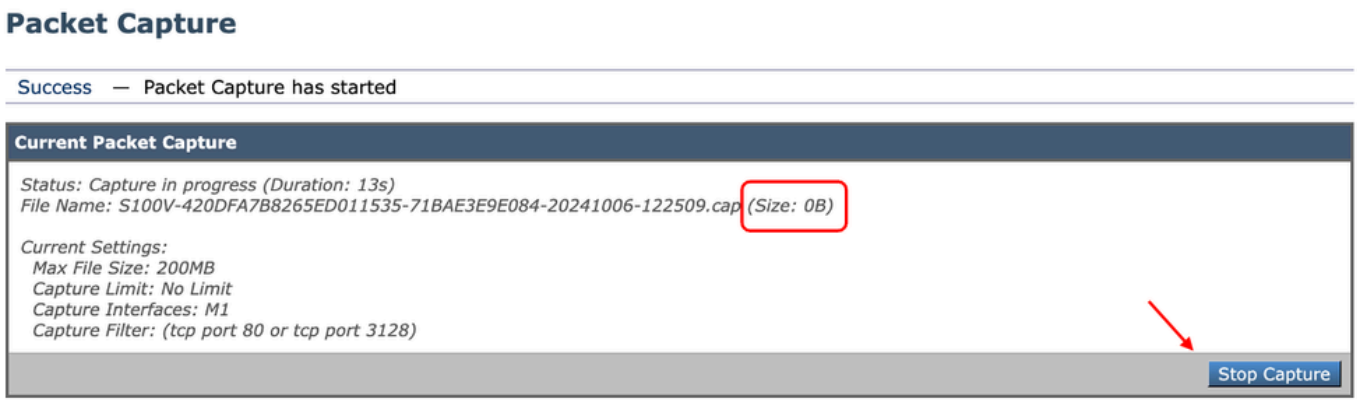


Afbeelding - Status en filters van pakketvastlegging



Opmerking: de maximale pakketgrootte van een bestand is 200 MB. Wanneer de bestandsgrootte 200 MB bereikte, stopt de Packet Capture.

De sectie Huidige pakketvastlegging toont de status van pakketvastlegging, inclusief de bestandsgrootte en toegepaste filters.

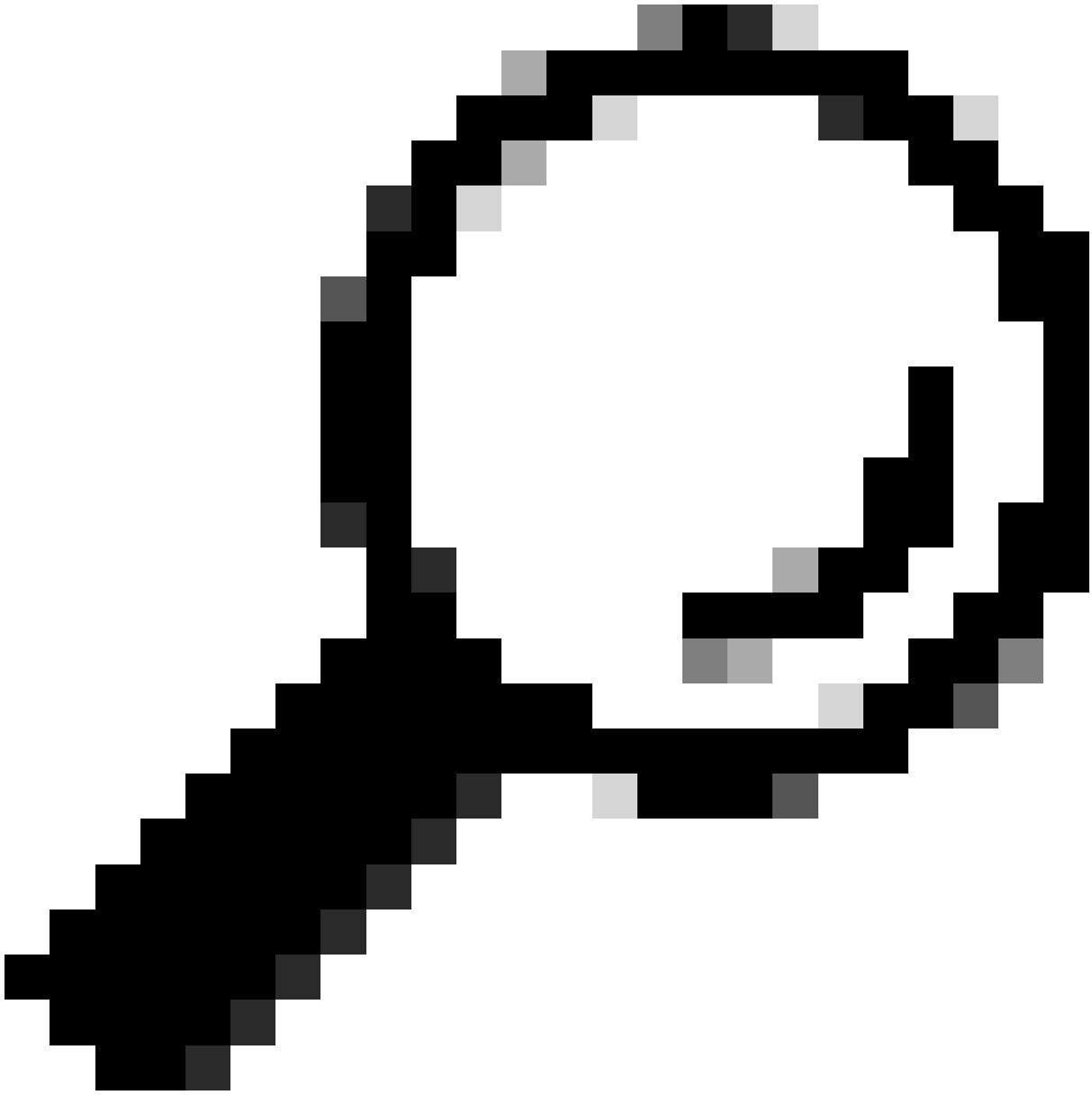


Afbeelding - Packet Capture Status

Stap 6. Om de lopende pakketopname te stoppen, klik op Stop Capture.

Stap 7. Als u het Packet Capture-bestand wilt downloaden, kiest u het bestand in de lijst Manager Packet Capture Files en klikt u op Download File.

Afbeelding - Packet Capture downloaden



Tip: Het laatste bestand bevindt zich boven aan de lijst.

Stap 8. (optioneel) Als u een Packet Capture-bestand wilt verwijderen, kiest u het bestand uit de lijst Manager Packet Capture Files en klikt u op Geselecteerde bestanden verwijderen.

Packet Capture vanaf CLI uitvoeren

U kunt de Packet Capture ook starten vanaf CLI met de volgende stappen:

Stap 1. Log in op de CLI.

Stap 2. Typ pakketopname en druk op ENTER.

Stap 3. (optioneel) U kunt het huidige filtertype SETUP bewerken. (Controleer het gedeelte Filters

in dit document voor meer informatie over de filters.)

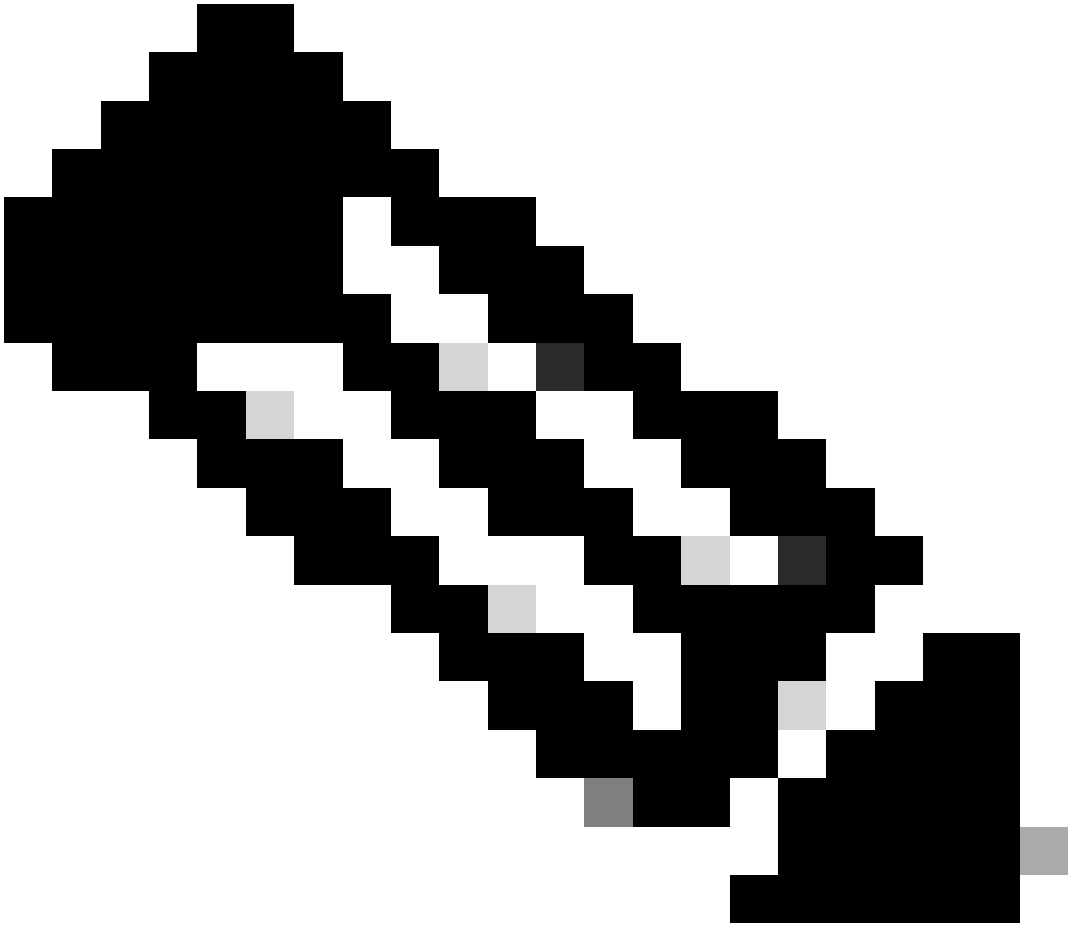
Stap 4. Kies START om de opname te starten.

```
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.
```

Stap 5. (optioneel) U kunt de status van Packet Capture bekijken door STATUS te kiezen:

```
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)
```

Stap 6. Om de Packet Capture te stoppen, typt u STOP en drukt u op ENTER:



Opmerking: om de Packet Capture-bestanden te downloaden die van CLI zijn verzameld, kunt u ze downloaden van GUI of verbinding maken met het apparaat via File Transfer Protocol (FTP) en ze downloaden van de Capture map.

Filters

Hier zijn enkele gidsen over de filters die u kunt gebruiken in de Content Security applicaties.

Filteren op IP-adres van host

Filteren op host IP in de GUI

Om door gastheer IP adres, van GUI te filteren, zijn er twee opties:

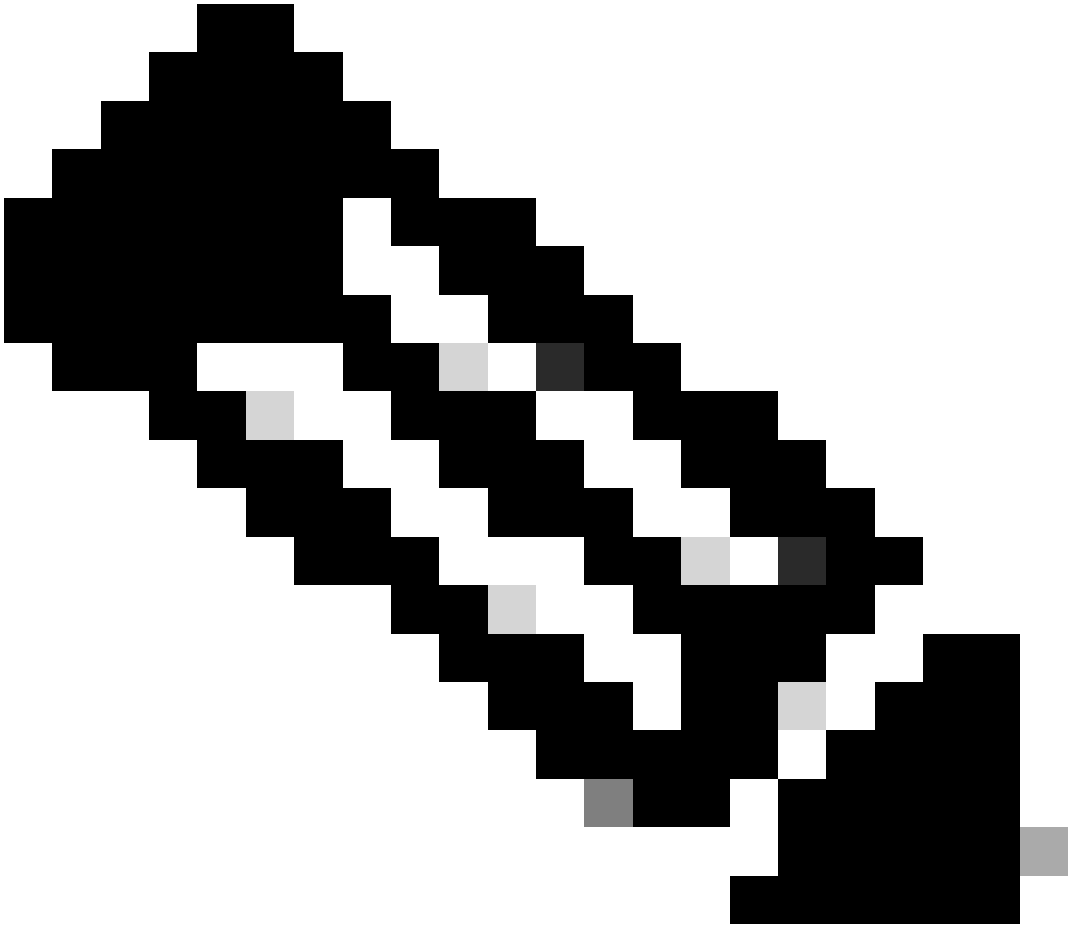
- Voorgedefinieerde filters
- Aangepaste filters

U kunt als volgt vooraf gedefinieerde filters gebruiken vanuit de GUI:

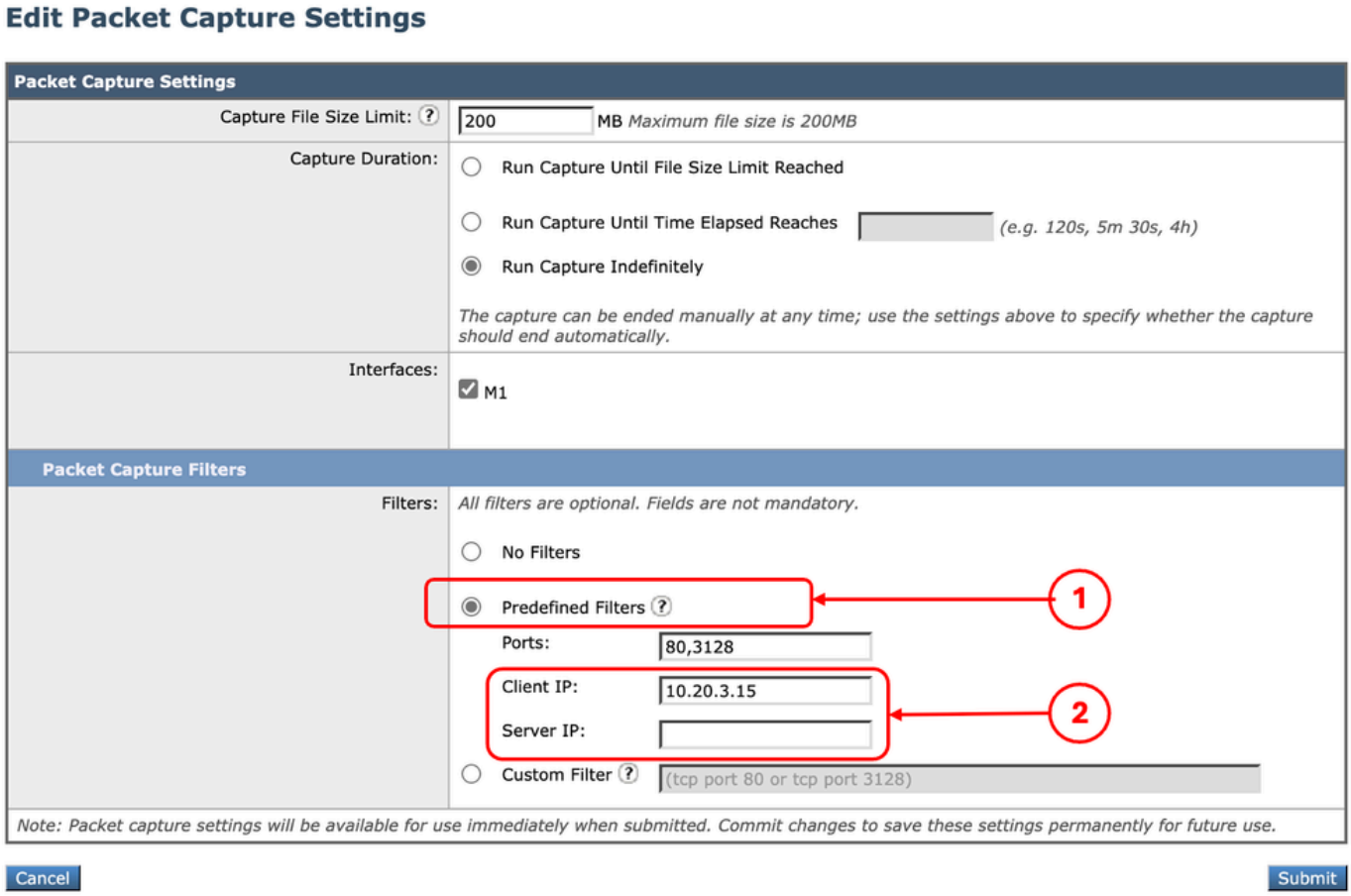
Stap 1. Kies Instellingen bewerken op de pagina Packet Capture.

Stap 2. Selecteer vanuit Packet Capture Filters voorgedefinieerde filters.

Stap 3. U kunt het IP-adres invoeren in het gedeelte IP van de client of IP van de server.



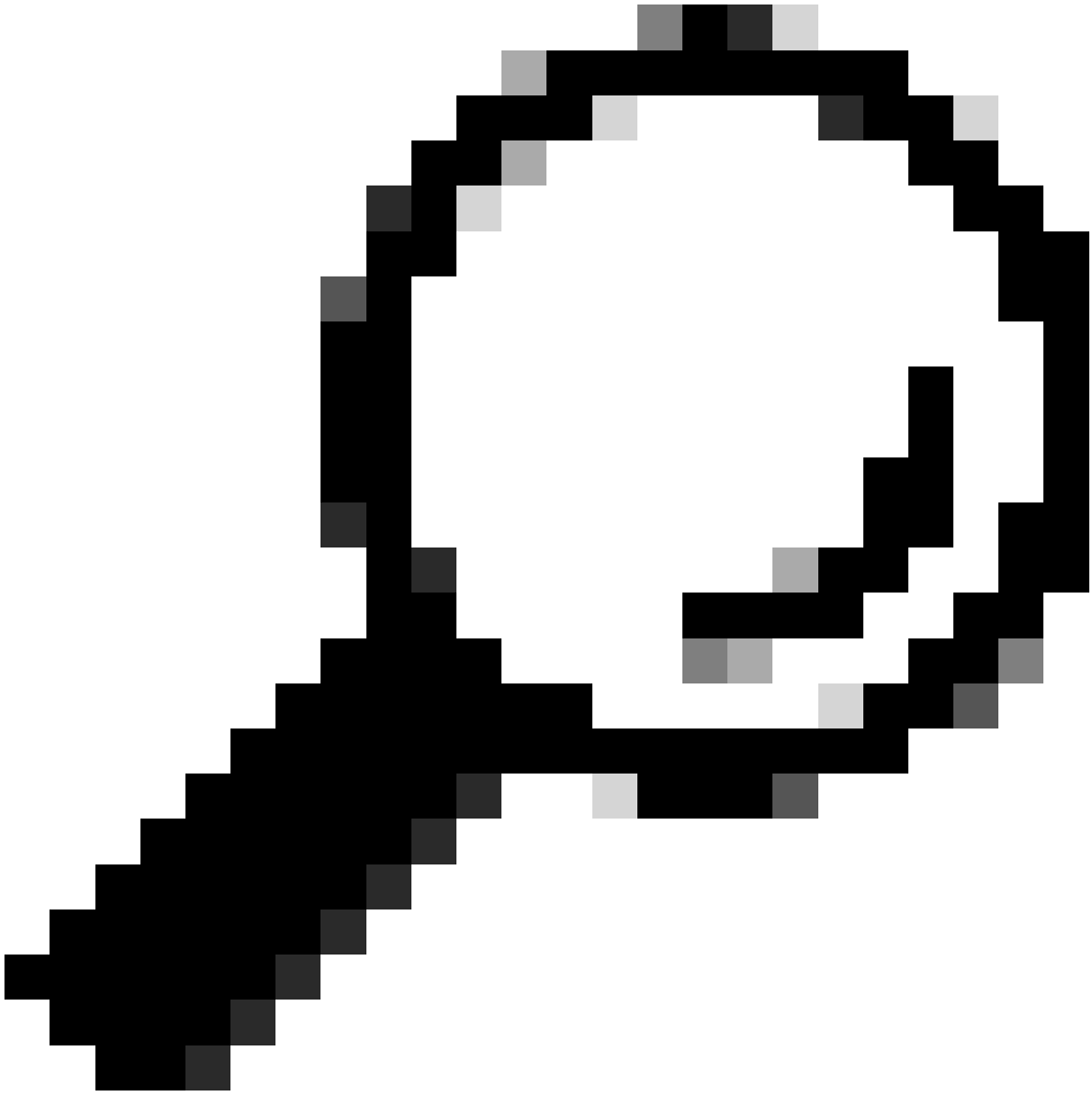
Opmerking: kiezen tussen client-IP of server-IP is niet beperkt tot bronadres of doeladres. Deze filter neemt alle pakketten op met het IP-adres dat als bron of bestemming is gedefinieerd.



Afbeelding - Filteren op host IP via GUI voorgedefinieerde filters

Stap 4. Leg de wijzigingen voor.

Stap 5. Start de vastlegging.



Tip: Er is geen noodzaak om Wijzigingen vast te leggen, het nieuw toegevoegde filter is op de huidige opname toegepast. Door de wijzigingen aan te brengen, kunt u het filter later opslaan.

U kunt als volgt aangepaste filters en vooraf gedefinieerde filters gebruiken vanuit de GUI:

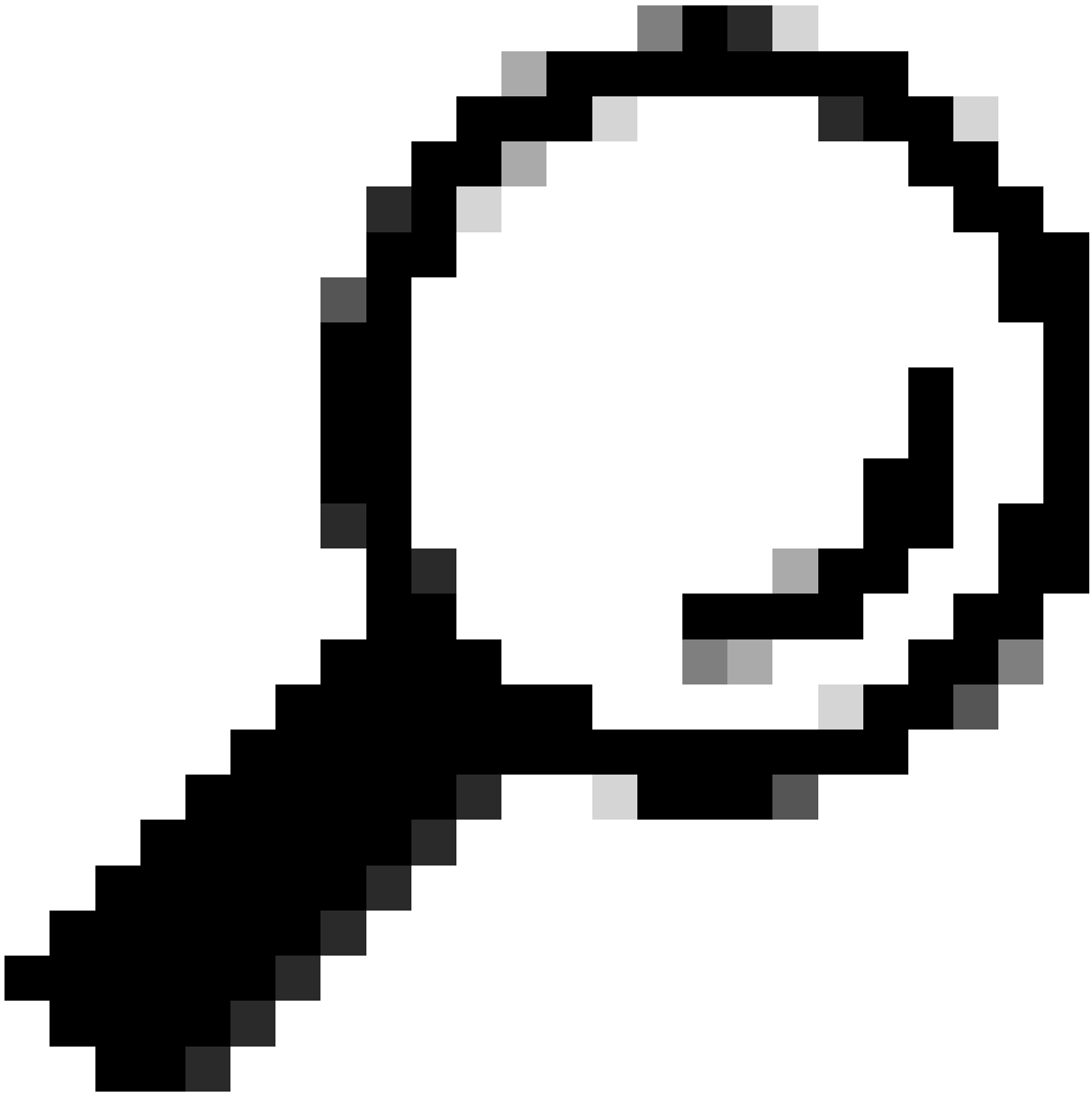
Stap 1. Kies Instellingen bewerken op de pagina Packet Capture.

Stap 2. Selecteer vanuit Packet Capture Filters Aangepaste filter.

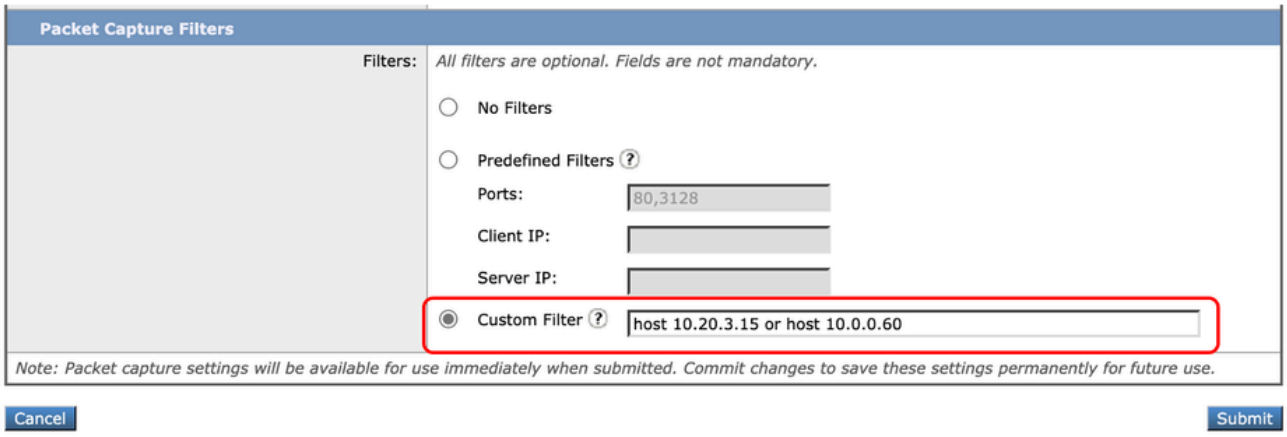
Stap 3. Gebruik de host-syntaxis gevolgd door het IP-adres.

Hier is een voorbeeld om al het verkeer met bron of bestemming IP adres 10.20.3.15 te filteren

```
host 10.20.3.15
```



Tip: om met meer dan één IP-adres te filteren kunt u logische operands gebruiken zoals of en en (alleen kleine letters).



Afbeelding - Aangepaste filter voor twee IP-adressen

Stap 4. Leg de wijzigingen voor.

Stap 5. Start de vastlegging

Filteren op host IP in CLI

U kunt als volgt filteren op het IP-adres van de host uit CLI:

Stap 1. Log in op de CLI.

Stap 2. Typ pakketopname en druk op ENTER.

Stap 3. U bewerkt het huidige filtertype SETUP.

Stap 4. Beantwoord de vragen tot u de filter voor de opname invoert.

Stap 5. U kunt dezelfde filtertekenreeks gebruiken als het aangepaste filter in de GUI.

Hier is een voorbeeld van het filteren van al het verkeer met het IP-adres van de bron of bestemming 10.20.3.15 of 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
```

Filteren op poortnummer

Filteren op poortnummer in GUI

U kunt uit de GUI naar poortnummer(s) filteren met twee opties:

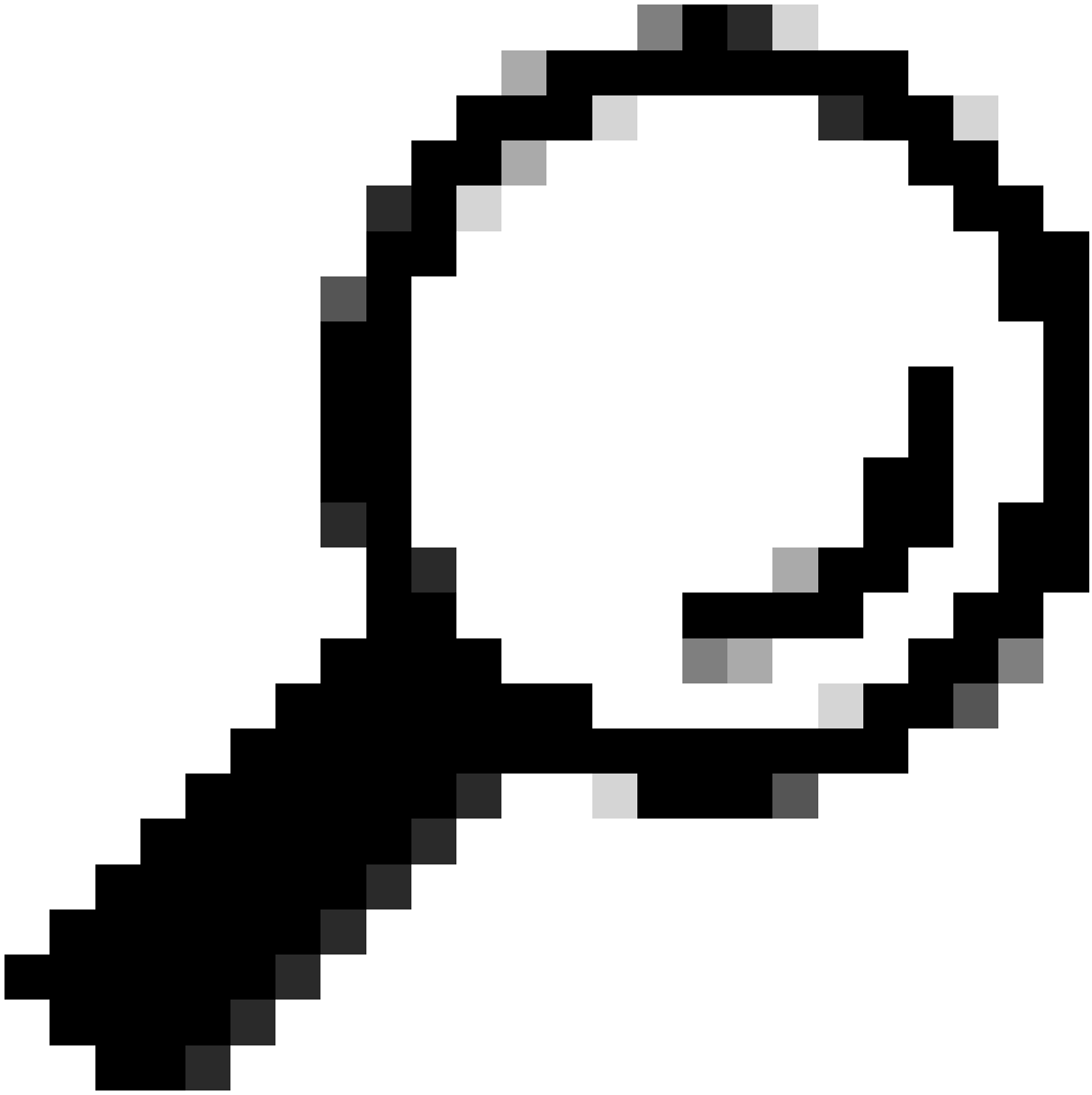
- Voorgedefinieerde filters
- Aangepaste filters

U kunt als volgt voorgedefinieerde filters gebruiken vanuit GUI:

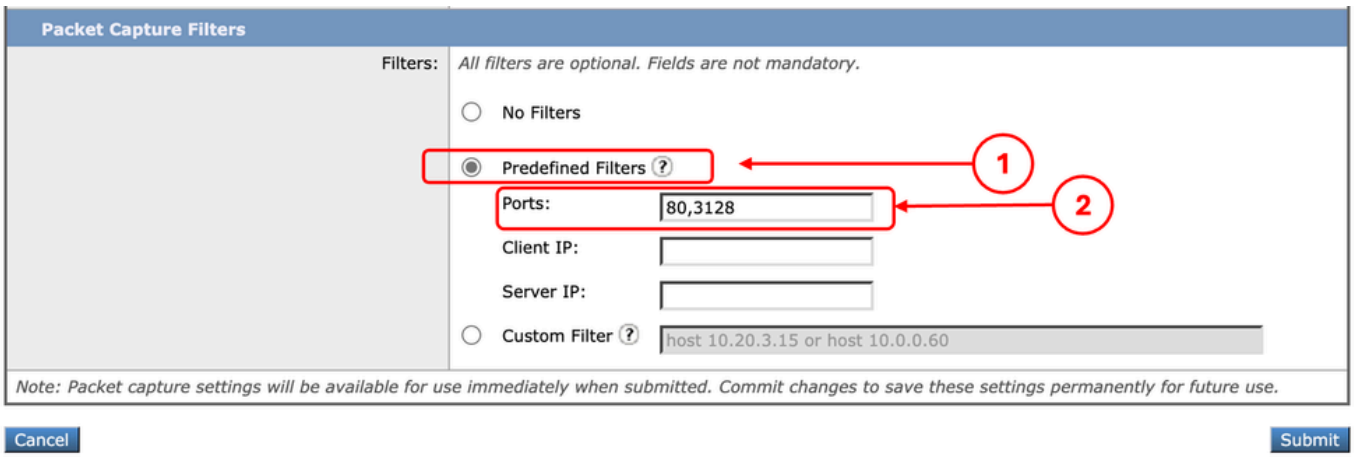
Stap 1. Kies Instellingen bewerken op de pagina Packet Capture.

Stap 2. Selecteer vanuit Packet Capture Filters voorgedefinieerde filters.

Stap 3. Typ in het gedeelte Poorten de poortnummers die u wilt filteren.



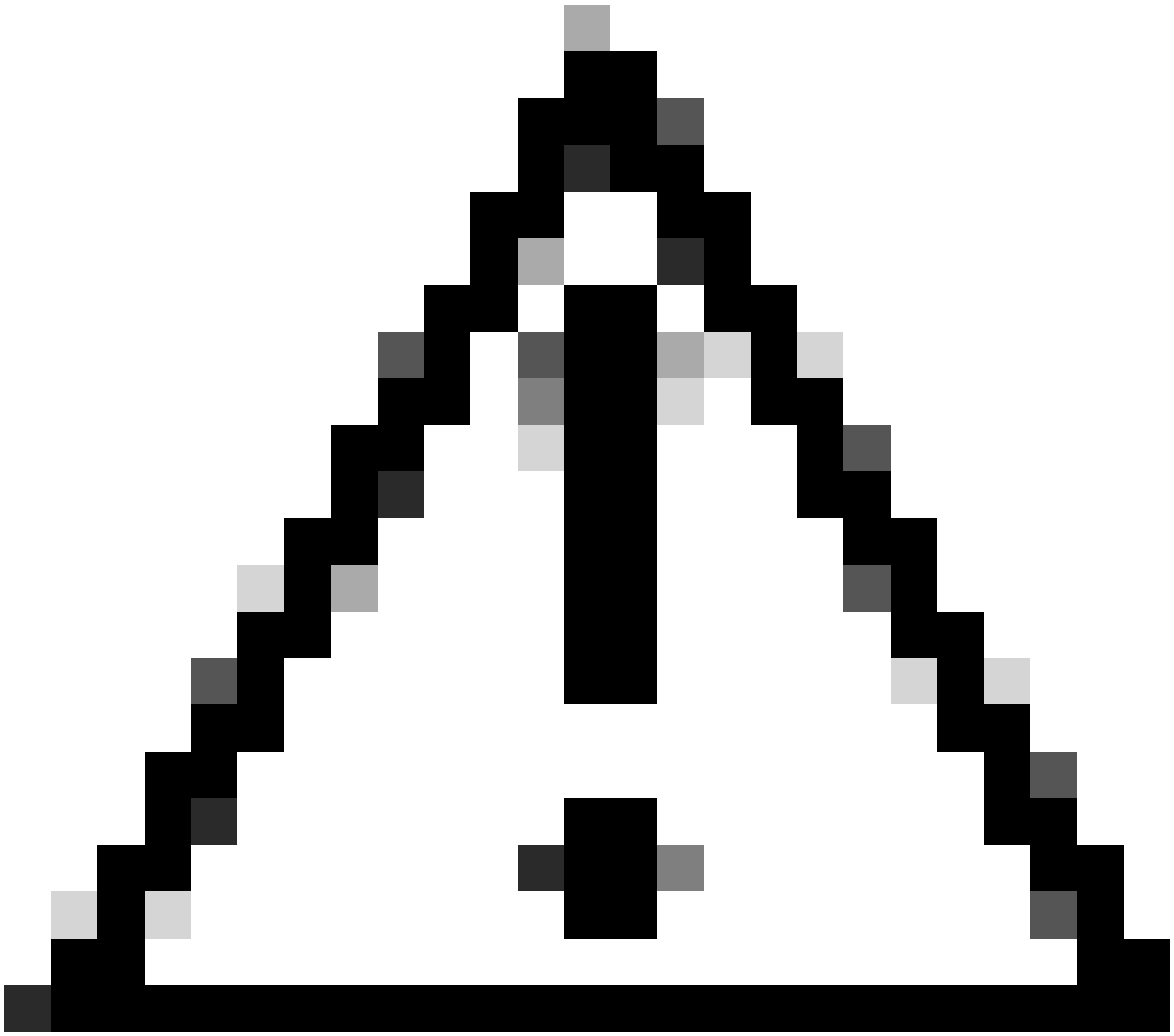
Tip: u kunt meerdere poortnummers toevoegen door deze te scheiden met een komma ", ".



Afbeelding - Filteren op poortnummer

Stap 4. Leg de wijzigingen voor.

Stap 5. Start de vastlegging.



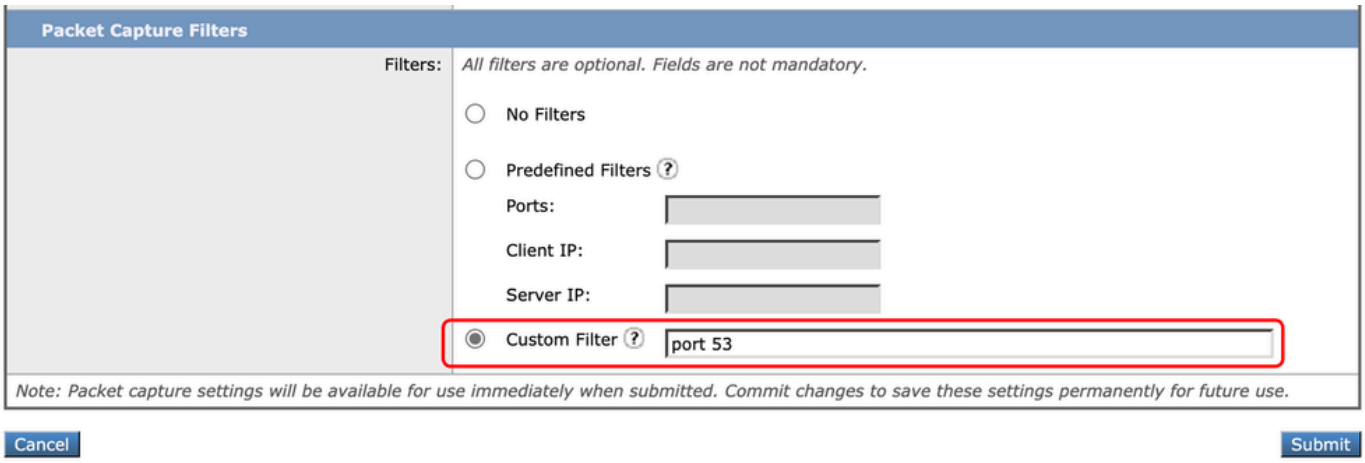
Waarschuwing: deze benadering neemt alleen TCP-verkeer met de gedefinieerde poortnummers op. Gebruik Aangepaste filter om het UDP-verkeer op te nemen.

U kunt als volgt aangepaste filters gebruiken vanuit de GUI:

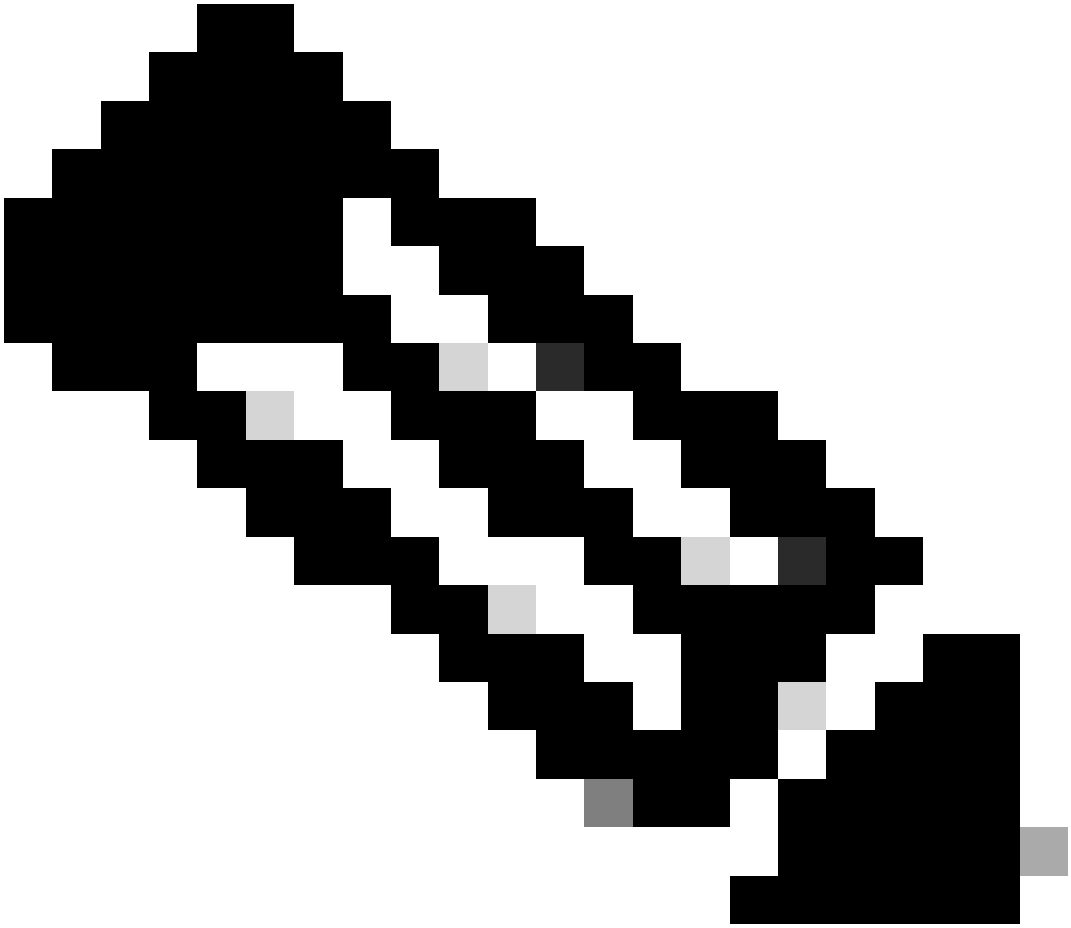
Stap 1. Kies Instellingen bewerken op de pagina Packet Capture.

Stap 2. Selecteer vanuit Packet Capture Filters Aangepaste filter.

Stap 3. Gebruik de poortsyntaxis gevolgd door het poortnummer.



Afbeelding - Aangepaste filter op poortnummer



Opmerking: als u alleen poort gebruikt, dekt dit filter zowel TCP- als UDP-poorten.

Stap 4. Leg de wijzigingen voor.

Stap 5. Start de vastlegging.

Filteren op poortnummer in CLI

U kunt als volgt filteren op het poortnummer van CLI:

Stap 1. Log in op de CLI.

Stap 2. Typ pakketopname en druk op ENTER.

Stap 3. U bewerkt het huidige filtertype SETUP.

Stap 4. Beantwoord de vragen tot u de filter voor de opname invoert.

Stap 5. U kunt dezelfde filtertekenreeks gebruiken als het aangepaste filter in de GUI.

Hier is een voorbeeld van het filteren van al het verkeer met bron- of bestemmingshaven nummer 53, voor zowel TCP- als UDP-poorten:

```
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
```

Filter in SWA met transparante implementatie

In SWA met Transparent plaatsing, terwijl de connectiviteit van de Communicatie van het Geheime voorgeheugen van het Web Protocol (WCCP) via de Generic Routing Encapsulation

(GRE) tunnels is, zijn de bron en bestemmingsIP adressen in de pakketten die aan of uitgaand van SWA komen het router IP adres en het adres van SWA IP.

Om Packet Capture met IP-adres of poortnummer te kunnen ophalen uit GUI, zijn er twee opties:

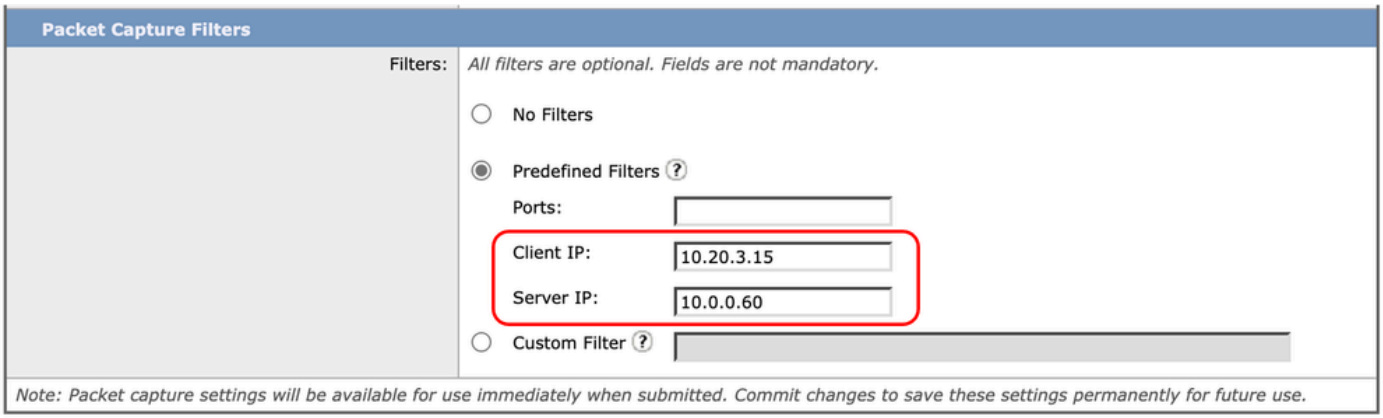
- Voorgedefinieerde filters
- Aangepaste filters

Filter in SWA met Transparante implementatie in GUI

Stap 1. Kies Instellingen bewerken op de pagina Packet Capture.

Stap 2. Selecteer vanuit Packet Capture Filters voorgedefinieerde filters.

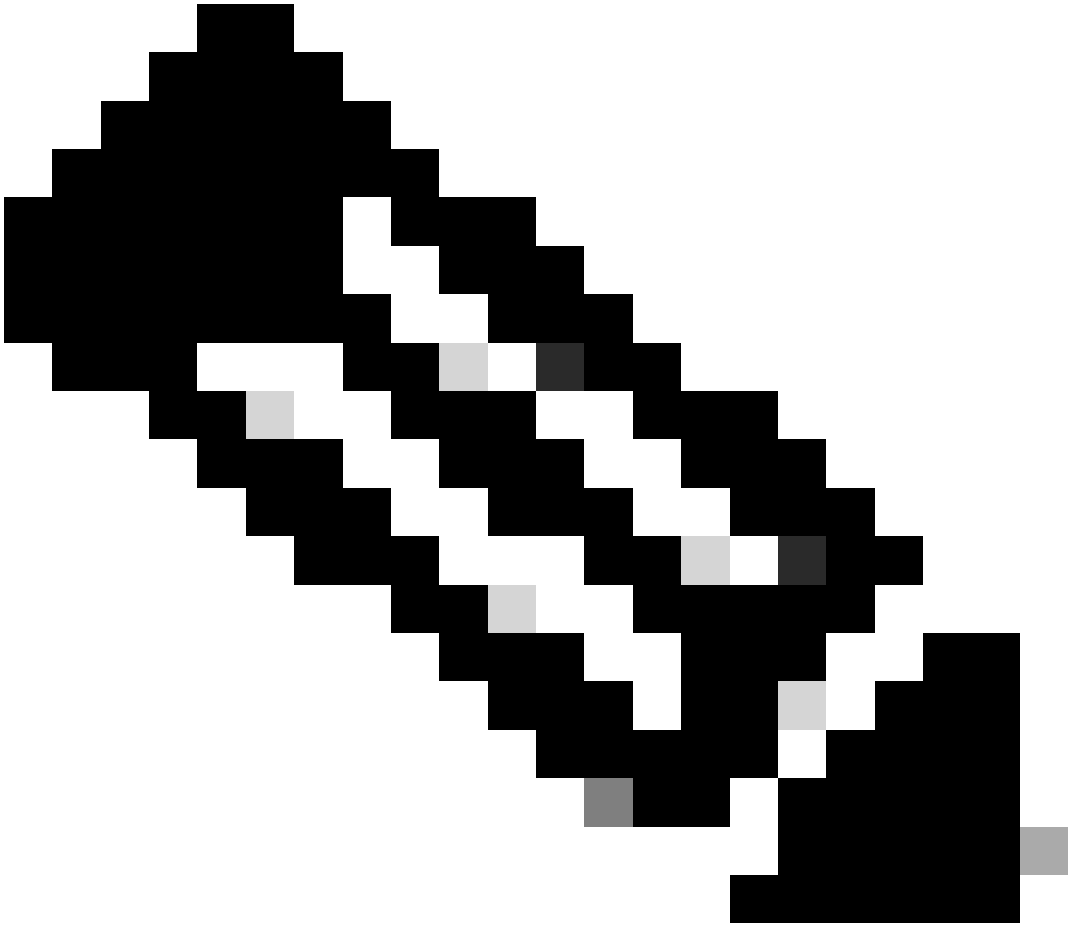
Stap 3. U kunt het IP-adres invoeren in het gedeelte IP van de client of IP van de server.



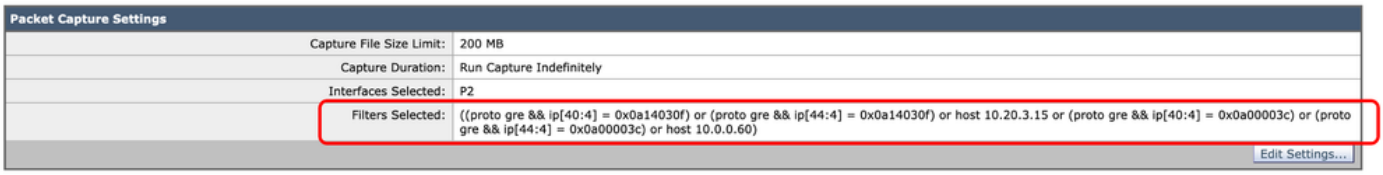
Afbeelding - IP-adres configureren in filters vooraf definiëren

Stap 4. Leg de wijzigingen voor.

Stap 5. Start de vastlegging.



Opmerking: na het indienen van het filter kunt u zien dat SWA extra voorwaarden heeft toegevoegd in het gedeelte Filter Selected.



Afbeelding - Extra Filters Toegevoegd door SWA om pakketten binnen GRE Tunnel te verzamelen

U kunt als volgt aangepaste filters gebruiken vanuit de GUI:

Stap 1. Kies Instellingen bewerken op de pagina Packet Capture.

Stap 2. Selecteer vanuit Packet Capture Filters Aangepaste filter

Stap 3. Voeg eerst deze string toe, gevolgd door het filter dat u wilt implementeren door het toevoegen of na deze string:

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

Als u bijvoorbeeld van plan bent te filteren op de IP-host gelijk aan 10.20.3.15 of op het poortnummer gelijk aan 8080, kunt u deze tekenreeks gebruiken:

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

Stap 4. Leg de wijzigingen voor.

Stap 5. Start de vastlegging.

Filter in SWA met Transparante implementatie in CLI

U kunt als volgt de implementatie van een transparante proxy filteren op CLI:

Stap 1. Log in op de CLI.

Stap 2. Typ pakketopname en druk op ENTER.

Stap 3. U bewerkt het huidige filtertype SETUP.

Stap 4. Beantwoord de vragen tot u de filter voor de opname invoert.

Stap 5. U kunt dezelfde filtertekenreeks gebruiken als het aangepaste filter in de GUI.

Hier is een voorbeeld om door de host IP gelijk aan 10.20.3.15 of het poortnummer gelijk aan 8080 te filteren:

```
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]>
```

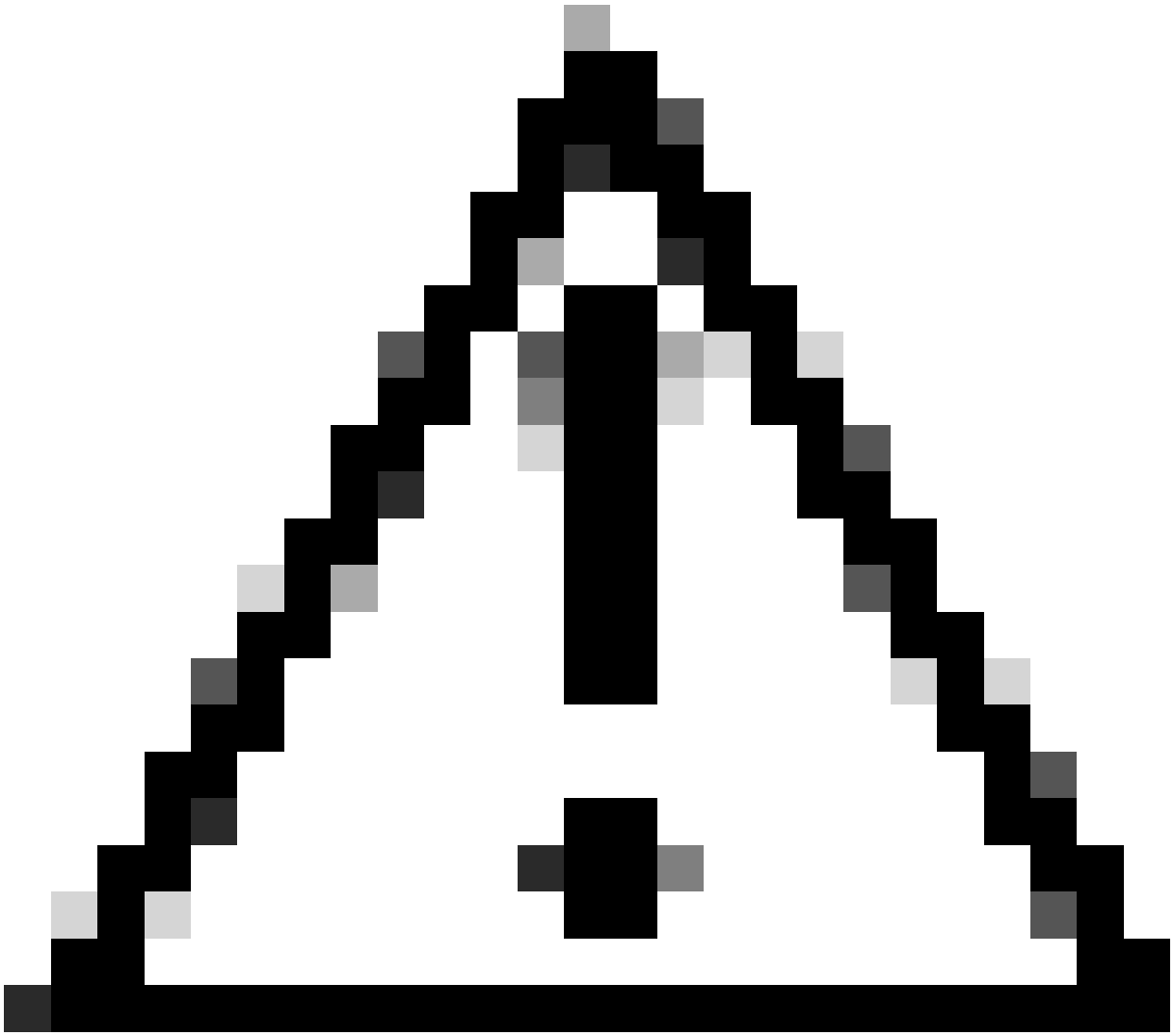
```
The following interfaces are configured:
1. Management
Enter the name or number of one or more interfaces to capture packets from, separated by commas:
[1]>

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
```

Populairste filters

Hier is een tabel met de meest voorkomende filters:

Beschrijving	filteren
Filter op IP-bronadres gelijk aan 10.20.3.15	src-host 10.20.3.15
Filter op bestemming IP-adres gelijk aan 10.20.3.15	dst host 10.20.3.15
Filter op IP-bronadres gelijk aan 10.20.3.15 en IP-adres van bestemming gelijk aan 10.0.0.60	(src-host 10.20.3.15) en (dst-host 10.0.0.60)
Filter op bron of bestemming IP-adres gelijk aan 10.20.3.15	host 10.20.3.15
Filter op bron of bestemming IP-adres gelijk aan 10.20.3.15 of gelijk aan 10.0.0.60	host 10.20.3.15 of host 10.0.0.60
Filter op TCP-poortnummer gelijk aan 8080	TCP-poort 8080
Filter op UDP-poortnummer gelijk aan 53	UDP-poort 53
Filter op poortnummer gelijk aan 514 (TCP of UDP)	poort 514
Alleen UDP-pakketten filteren	udp
Alleen ICMP-pakketten filteren	icmp

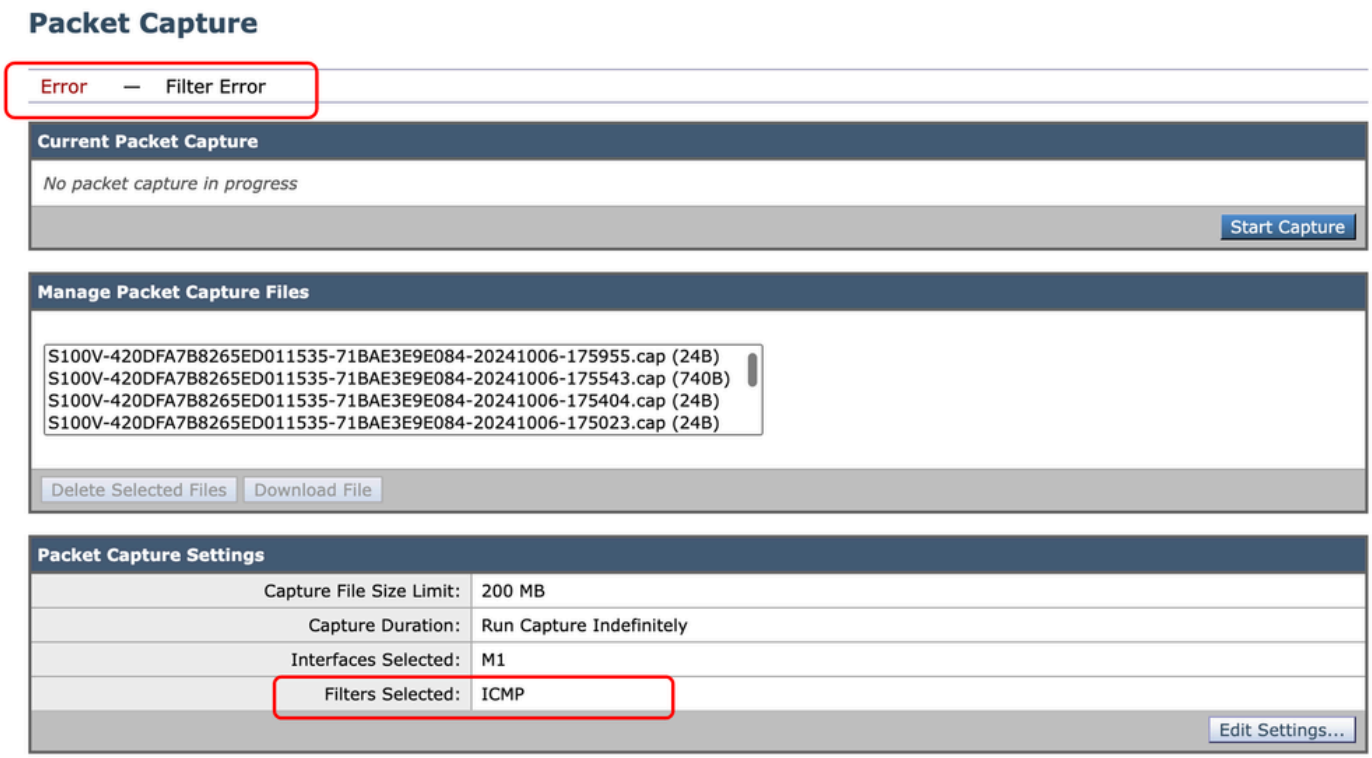
Hoofdfilter te gebruiken voor elke opname in transparante implementatie	(proto gre & ip[40:4] = 0x0a14030f) of (proto gre & ip[44:4] = 0x0a14030f) of (proto gre & ip[40:4] = 0x0a00003c) of (proto gre & ip[44:4] = 0x0a00003c)



Waarschuwing: alle filters zijn hoofdlettergevoelig.

Problemen oplossen

"Filterfout" is een van de meest voorkomende fouten tijdens het uitvoeren van de pakketopname.



Afbeelding - Filterfout

Deze fout is gewoonlijk verwant aan verkeerde filterimplementatie. In het bovenstaande voorbeeld bevat het ICMP-filter hoofdletters. Dat is de reden dat u Filter fout ontvangt. Om dit probleem op te lossen, moet u het filter bewerken en de ICMP vervangen door de ICMP.

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Applicatie - GD (Algemene implementatie) - Classify End-U...

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.