

Konfigurieren der Paketerfassung auf der Content Security Appliance

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Paketerfassung über GUI durchführen](#)

[Paketerfassung über CLI durchführen](#)

[Filter](#)

[Nach Host-IP-Adresse filtern](#)

[Filtern nach Host-IP in der GUI](#)

[Nach Host-IP in CLI filtern](#)

[Nach Portnummer filtern](#)

[Nach Portnummer in GUI filtern](#)

[Nach Portnummer in CLI filtern](#)

[Filtern in SWA mit transparenter Bereitstellung](#)

[Filtern in SWA mit transparenter Bereitstellung in GUI](#)

[Filtern in SWA mit transparenter Bereitstellung in CLI](#)

[Häufigste Filter](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Paketerfassung auf Cisco Secure Web Appliance (SWA), Email Security Appliance (ESA) und Security Management Appliance (SMA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Administration der Cisco Content Security Appliance

Cisco empfiehlt Folgendes:

- Installierte physische oder virtuelle SWA/ESA/SMA.
- Administratorzugriff auf die grafische Benutzeroberfläche (GUI) von SWA/ESA/SMA.

- Administratorzugriff auf die SWA/ESA/SMA-CLI (Command Line Interface)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Paketerfassung über GUI durchführen

Führen Sie folgende Schritte aus, um die Paketerfassung über die GUI durchzuführen:

Schritt 1: Melden Sie sich bei der GUI an.

Schritt 2: Wählen Sie oben rechts auf der Seite Support und Hilfe aus.

Schritt 3: Wählen Sie Paketerfassung aus.

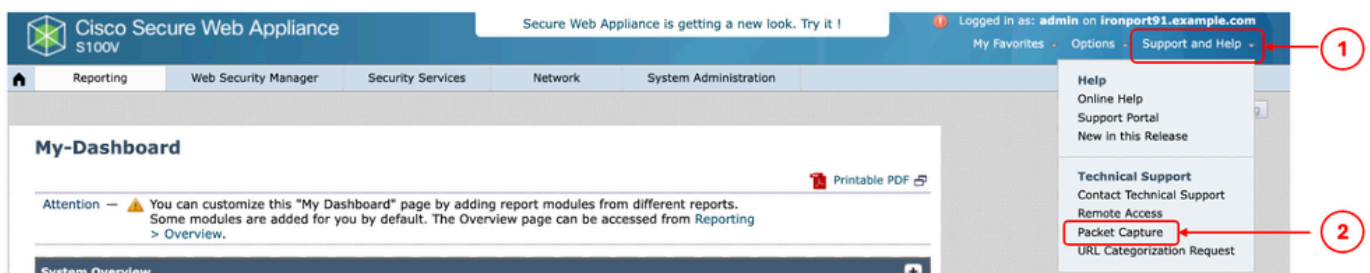


Image - Paketerfassung

Schritt 4. (Optional) Um den aktuellen Filter zu bearbeiten, wählen Sie Einstellungen bearbeiten. (Weitere Informationen zu den Filtern finden Sie im Abschnitt Filter dieses Dokuments.)

Schritt 5: Erfassung starten.

Packet Capture

Current Packet Capture

No packet capture in progress

[Start Capture](#) 2

Manage Packet Capture Files

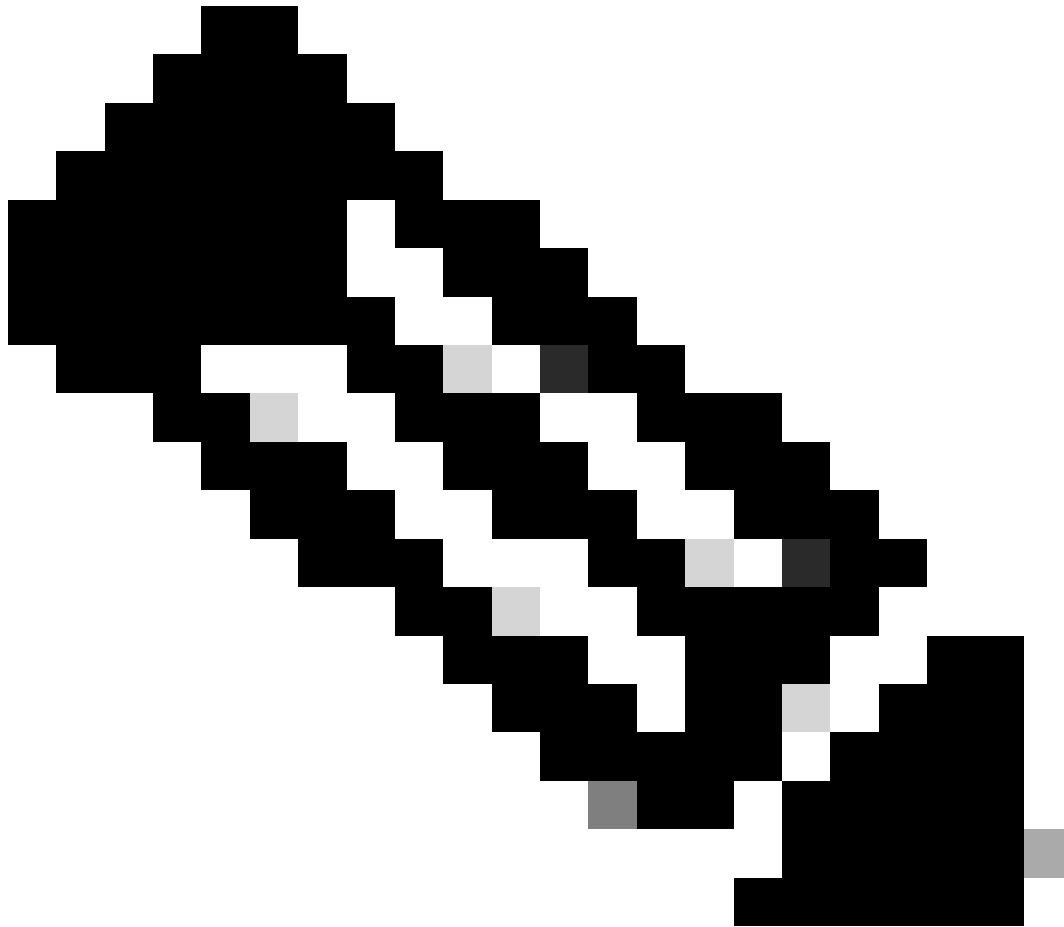
[Delete Selected Files](#) [Download File](#)

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

Image: Status und Filter der Paketerfassung



Hinweis: Die Größenbeschränkung der Paketerfassungsdatei beträgt 200 MB. Wenn die Dateigröße 200 MB erreicht hat, wird die Paketerfassung beendet.

Der Abschnitt Aktuelle Paketerfassung zeigt den Paketerfassungsstatus an, einschließlich der Dateigröße und der angewendeten Filter.

Packet Capture

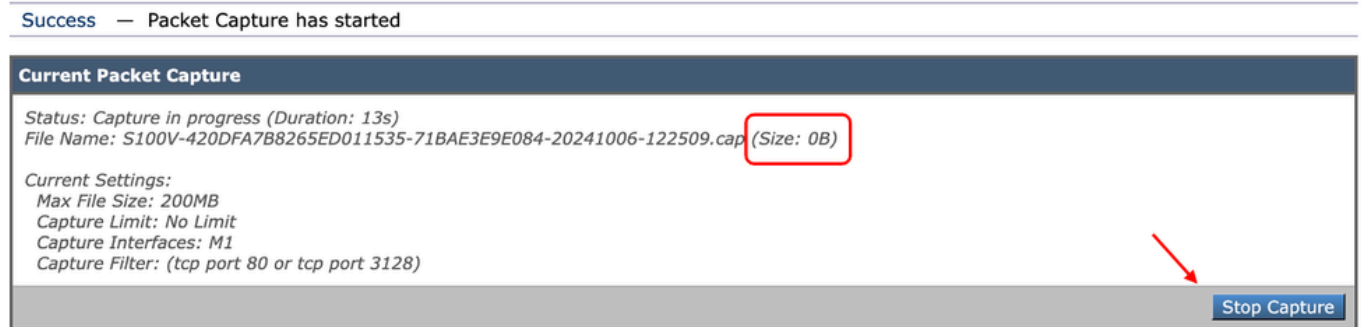


Image - Status der Paketerfassung

Schritt 6: Um die laufende Paketerfassung zu beenden, klicken Sie auf Stopp Capture (Erfassung beenden).

Schritt 7. Um die Paketerfassungsdatei herunterzuladen, wählen Sie die Datei aus der Liste Paketerfassungsdateien verwalten, und klicken Sie auf Datei herunterladen.

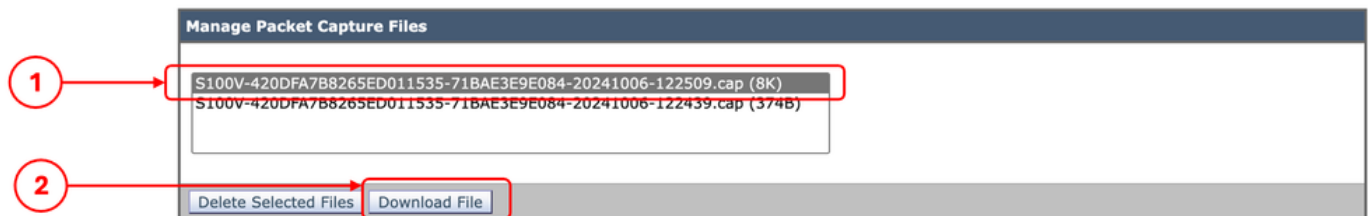
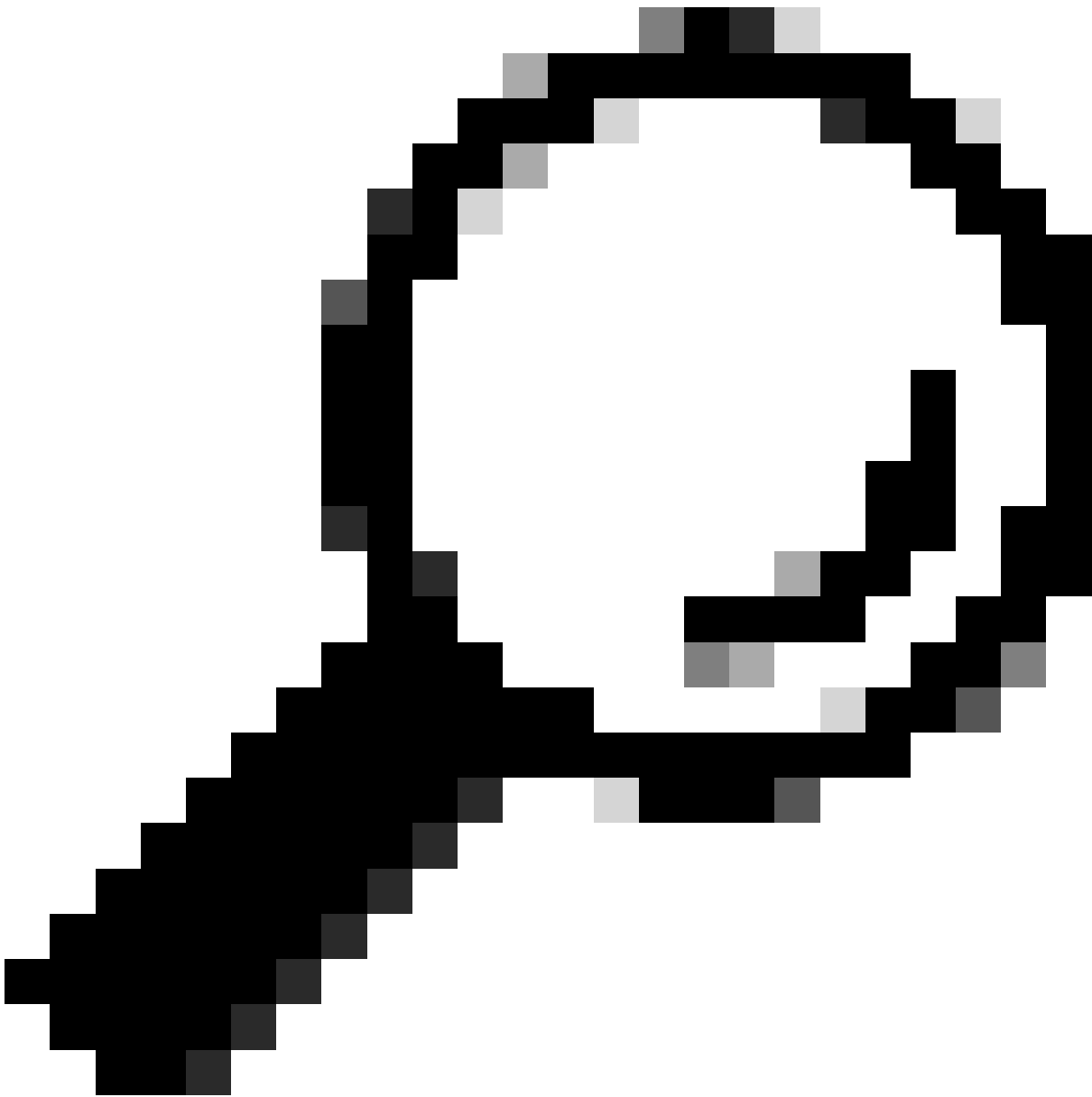


Image: Paketerfassung herunterladen



Tipp: Die neueste Datei befindet sich oben in der Liste.

Schritt 8. (Optional) Um eine beliebige Paketerfassungsdatei zu löschen, wählen Sie die Datei aus der Liste Paketerfassungsdateien verwalten und klicken Sie auf Ausgewählte Dateien löschen.

Paketerfassung über CLI durchführen

Sie können die Paketerfassung auch über die CLI starten, indem Sie folgende Schritte ausführen:

Schritt 1: Melden Sie sich bei der CLI an.

Schritt 2: Geben Sie PacketCapture ein, und drücken Sie die Eingabetaste.

Schritt 3. (Optional) Bearbeiten Sie den aktuellen Filtertyp SETUP. (Weitere Informationen zu den

Filtern finden Sie im Abschnitt Filter dieses Dokuments.)

Schritt 4: Wählen Sie START, um die Erfassung zu 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.

Schritt 5: (Optional) Sie können den Status der Paketerfassung anzeigen, indem Sie STATUS auswählen:

```
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)
```

Schritt 6: Um die Paketerfassung zu stoppen, geben Sie STOP ein, und drücken Sie die Eingabetaste:



Hinweis: Um die über die CLI gesammelten Packet Capture-Dateien herunterzuladen, können Sie sie über die Benutzeroberfläche herunterladen oder über File Transfer Protocol (FTP) eine Verbindung zur Appliance herstellen und sie aus dem Ordner Captures herunterladen.

Filter

Hier finden Sie einige Leitfäden zu den Filtern, die Sie in den Content Security Appliances verwenden können.

Nach Host-IP-Adresse filtern

Filtern nach Host-IP in der GUI

Um nach der IP-Adresse des Hosts zu filtern, gibt es in der GUI zwei Optionen:

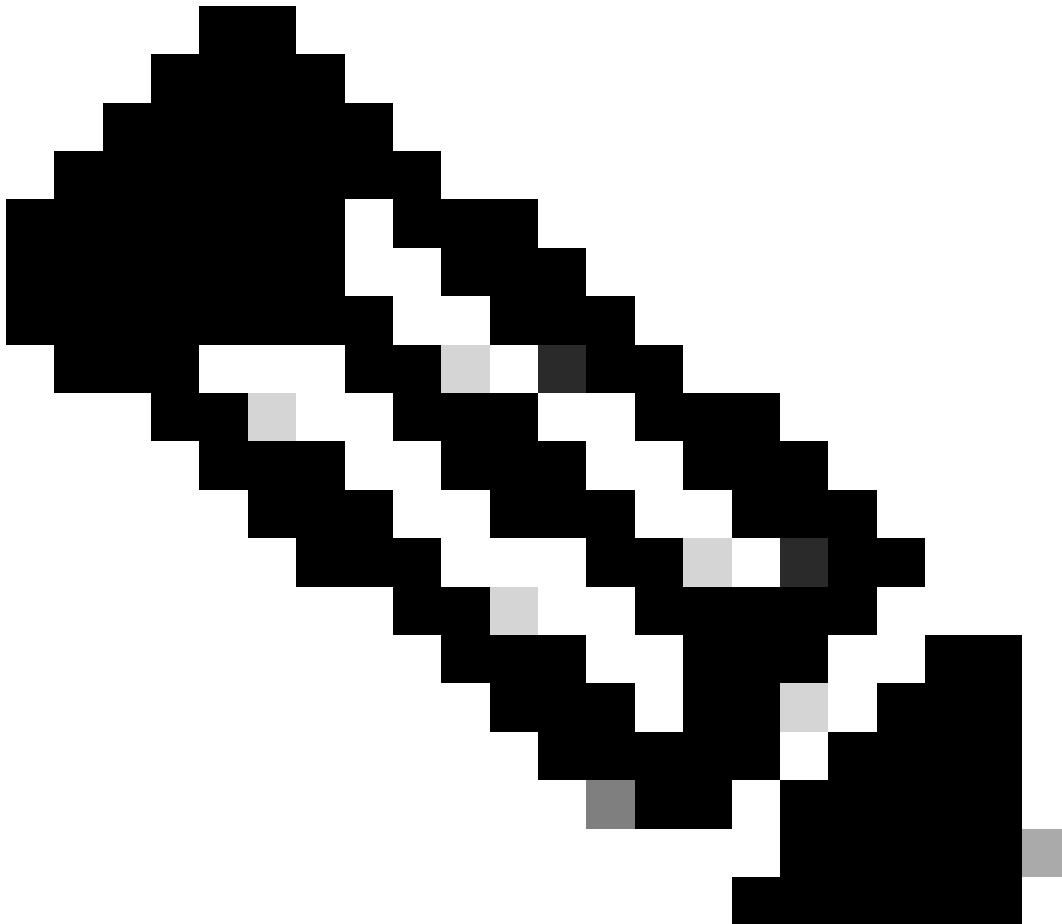
- Vordefinierte Filter
- Benutzerdefinierte Filter

So verwenden Sie vordefinierte Filter aus der GUI:

Schritt 1: Wählen Sie auf der Seite Paketerfassung die Option Einstellungen bearbeiten aus.

Schritt 2: Wählen Sie unter Paketerfassungsfiler die Option Vordefinierte Filter aus.

Schritt 3: Sie können die IP-Adresse im Abschnitt Client IP oder Server IP eingeben.



Hinweis: Die Auswahl zwischen Client-IP und Server-IP ist nicht auf die Quell- oder Zieladresse beschränkt. Dieser Filter erfasst alle Pakete mit der IP-Adresse, die als Quelle oder Ziel definiert ist.

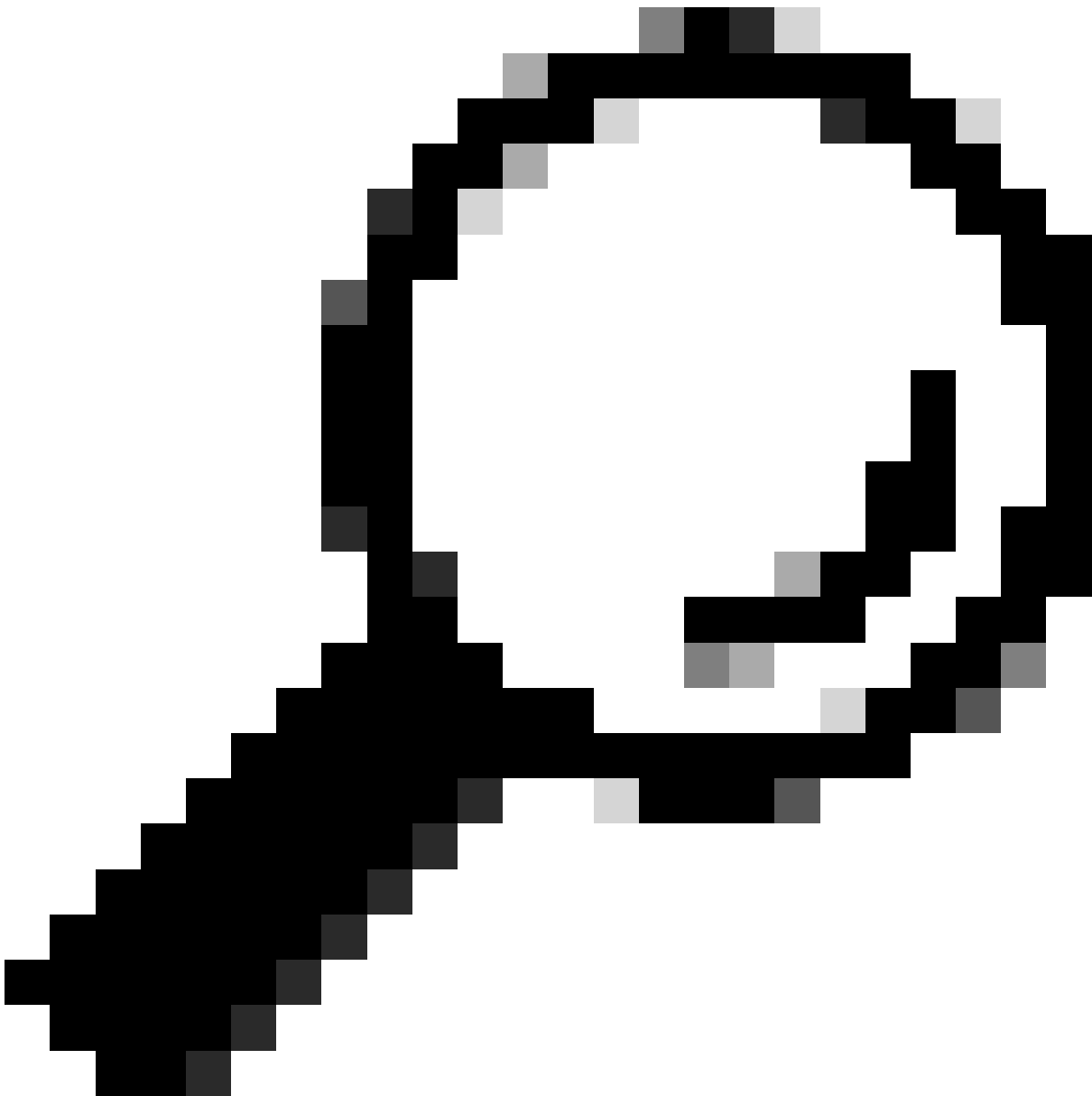
Edit Packet Capture Settings

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>	

Bild: Filtern nach Host-IP von vordefinierten GUI-Filtern

Schritt 4: Senden Sie die Änderungen.

Schritt 5: Erfassung starten.



Tipp: Es ist nicht erforderlich, Änderungen zu bestätigen. Der neu hinzugefügte Filter wird auf die aktuelle Erfassung angewendet. Wenn Sie die Änderungen bestätigen, können Sie den Filter für die zukünftige Verwendung speichern.

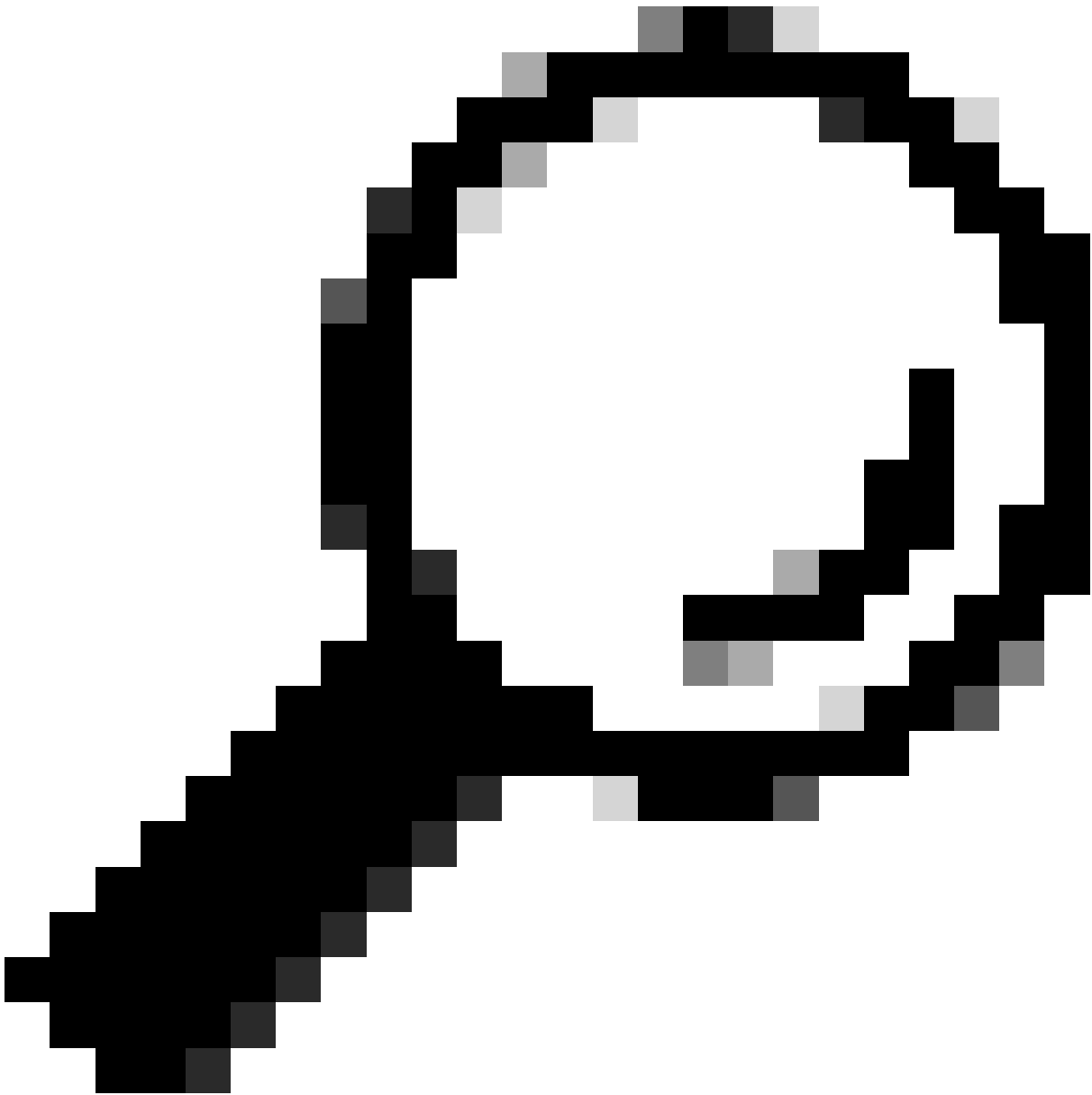
So verwenden Sie benutzerdefinierte Filter und vordefinierte Filter aus der GUI:

Schritt 1: Wählen Sie auf der Seite Paketerfassung die Option Einstellungen bearbeiten aus.

Schritt 2: Wählen Sie aus den Paketerfassungsfiltren die Option Benutzerdefinierter Filter aus.

Schritt 3: Verwenden Sie die Host-Syntax gefolgt von der IP-Adresse.

In diesem Beispiel wird der gesamte Datenverkehr mit der Quell- oder Ziel-IP-Adresse 10.20.3.15 gefiltert.



Tipp: Um nach mehr als einer IP-Adresse zu filtern, können Sie logische Operanden wie oder und und verwenden (nur Kleinbuchstaben).

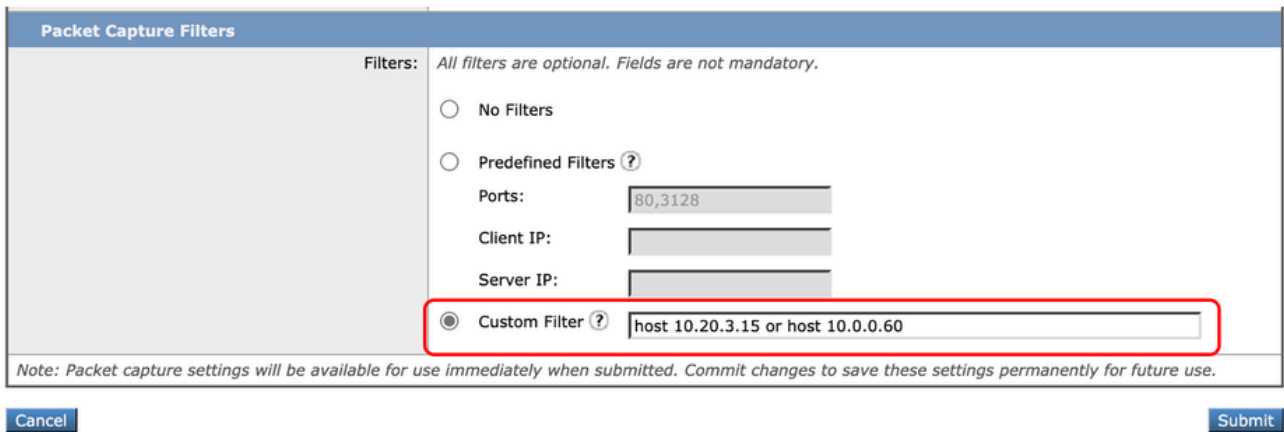


Bild - Benutzerdefinierter Filter für zwei IP-Adressen

Schritt 4: Senden Sie die Änderungen.

Schritt 5: Erfassung starten

Nach Host-IP in CLI filtern

So filtern Sie anhand der Host-IP-Adresse in der CLI:

Schritt 1: Melden Sie sich bei der CLI an.

Schritt 2: Geben Sie PacketCapture ein, und drücken Sie die Eingabetaste.

Schritt 3: Um den aktuellen Filter zu bearbeiten, geben Sie SETUP ein.

Schritt 4: Beantworten Sie die Fragen, bis Sie erreicht haben Geben Sie den Filter ein, der für die Erfassung verwendet werden soll.

Schritt 5: Sie können die gleiche Filterzeichenfolge wie der benutzerdefinierte Filter in der GUI verwenden.

Hier ist ein Beispiel für das Filtern des gesamten Datenverkehrs mit der Quell- oder Ziel-IP-Adresse 10.20.3.15 oder 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

Nach Portnummer filtern

Nach Portnummer in GUI filtern

Für die Filterung nach Portnummer(n) stehen in der GUI zwei Optionen zur Verfügung:

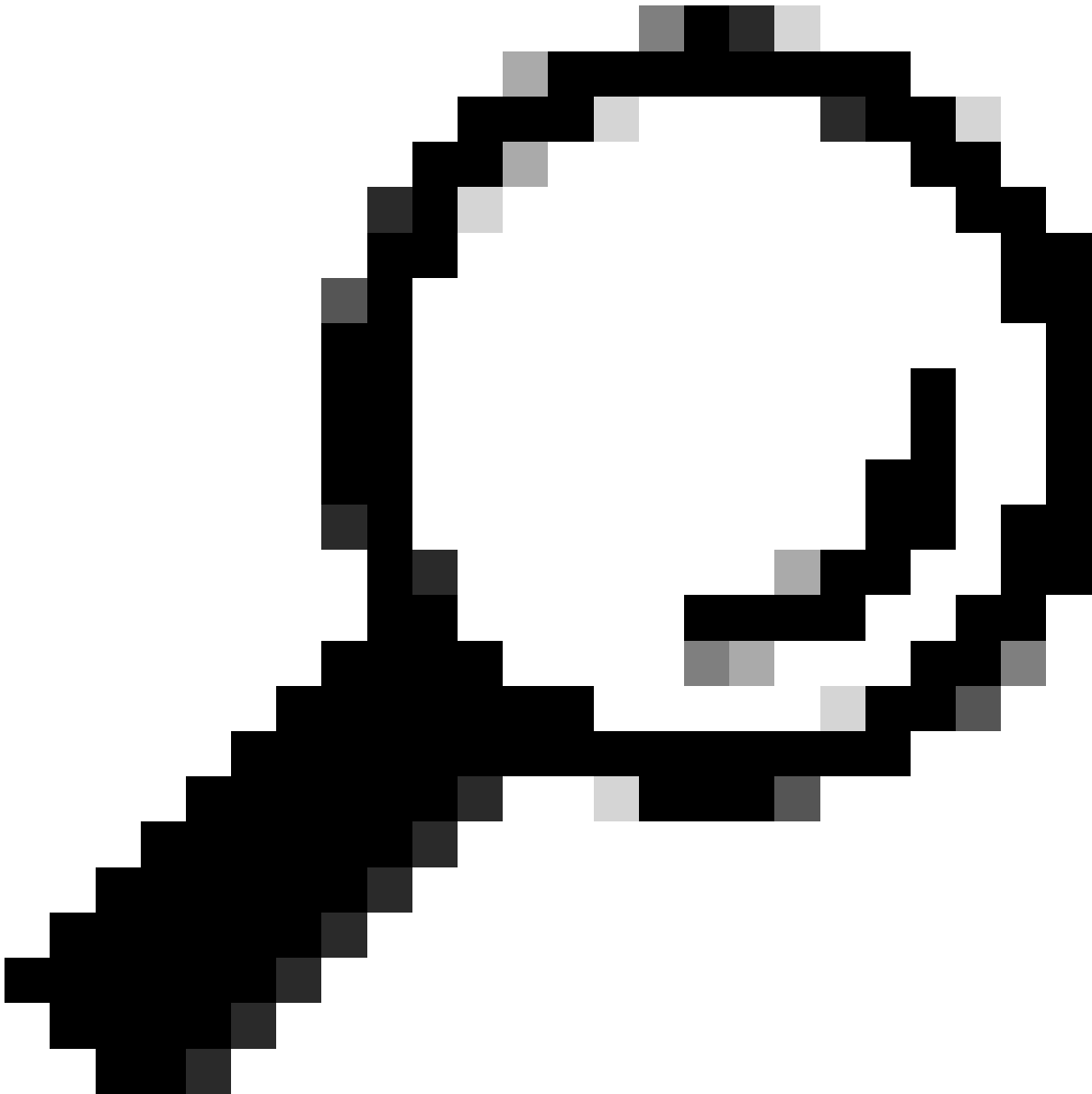
- Vordefinierte Filter
- Benutzerdefinierte Filter

So verwenden Sie vordefinierte Filter aus der GUI:

Schritt 1: Wählen Sie auf der Seite Paketerfassung die Option Einstellungen bearbeiten aus.

Schritt 2: Wählen Sie unter Paketerfassungsfiler die Option Vordefinierte Filter aus.

Schritt 3: Geben Sie im Abschnitt Ports die Portnummern ein, die Sie filtern möchten.



Tipp: Sie können mehrere Portnummern hinzufügen, indem Sie sie durch Kommas ", " voneinander trennen.

Packet Capture Filters

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

No Filters

Predefined Filters ?

Ports:

Client IP:

Server IP:

Custom Filter ?

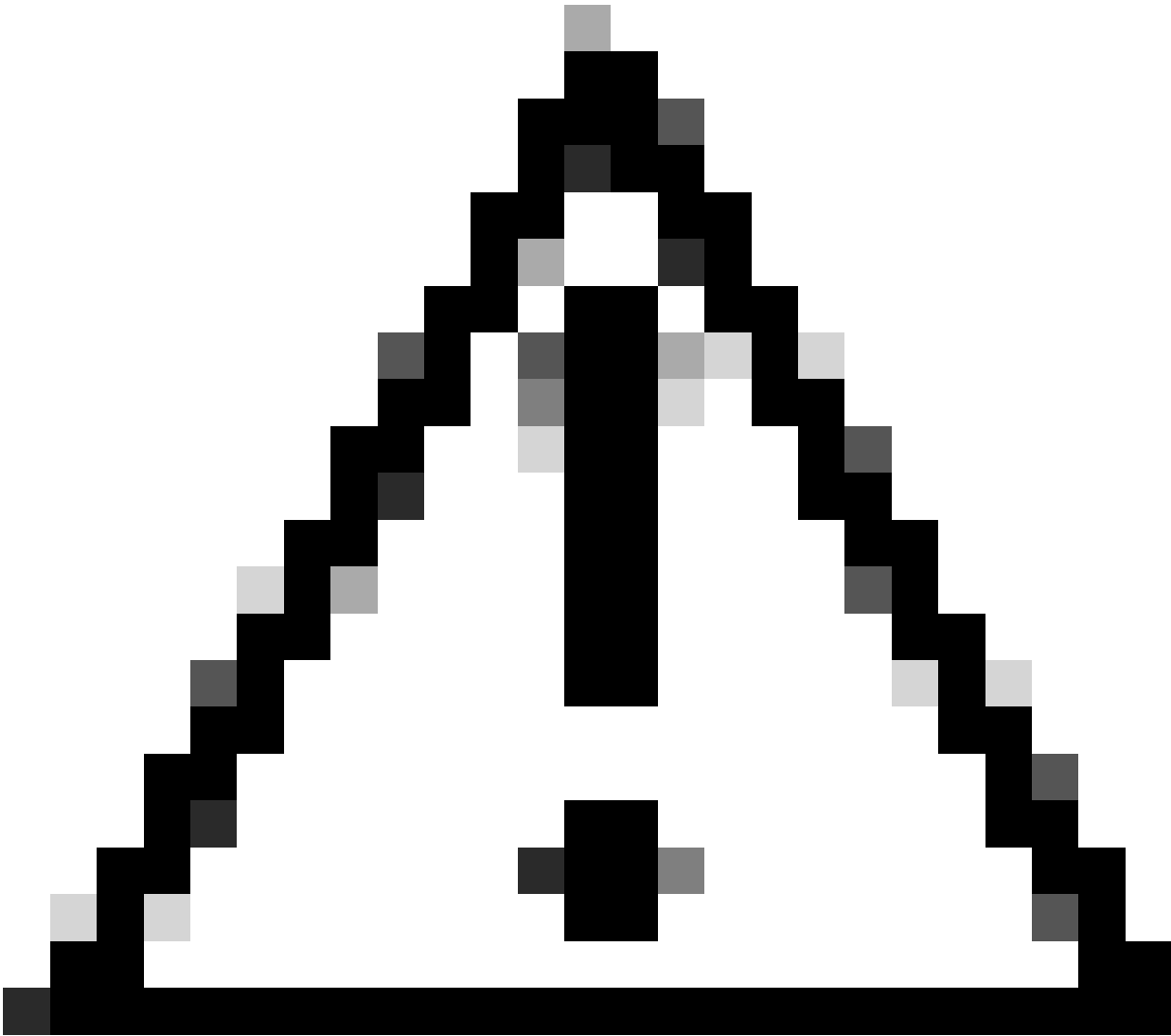
Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.

Cancel

Submit

Schritt 4: Senden Sie die Änderungen.

Schritt 5: Erfassung starten.



Vorsicht: Bei diesem Ansatz wird nur TCP-Datenverkehr mit den definierten Portnummern erfasst. Um den UDP-Datenverkehr zu erfassen, verwenden Sie den benutzerdefinierten Filter.

So verwenden Sie benutzerdefinierte Filter aus der GUI:

Schritt 1: Wählen Sie auf der Seite Paketerfassung die Option Einstellungen bearbeiten aus.

Schritt 2: Wählen Sie aus den Paketerfassungsfiltern die Option Benutzerdefinierter Filter aus.

Schritt 3: Verwenden Sie die Portsyntax gefolgt von der Portnummer.

Packet Capture Filters

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

No Filters

Predefined Filters ?

Ports:

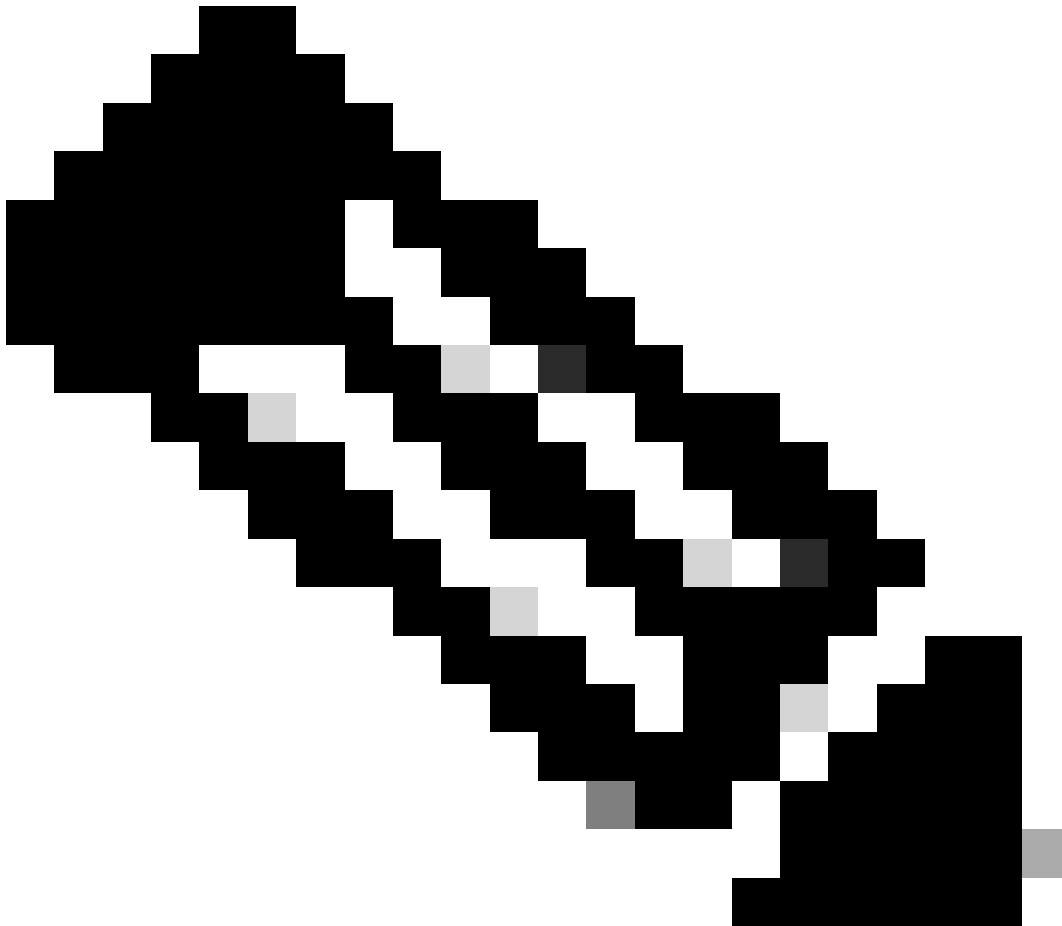
Client IP:

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.

Bild - Benutzerdefinierter Filter nach Portnummer



Hinweis: Wenn Sie nur Port verwenden, deckt dieser Filter TCP- und UDP-Ports ab.

Schritt 4: Senden Sie die Änderungen.

Schritt 5: Erfassung starten.

Nach Portnummer in CLI filtern

So filtern Sie anhand der Portnummer der CLI:

Schritt 1: Melden Sie sich bei der CLI an.

Schritt 2: Geben Sie PacketCapture ein, und drücken Sie die Eingabetaste.

Schritt 3: Um den aktuellen Filter zu bearbeiten, geben Sie SETUP ein.

Schritt 4: Beantworten Sie die Fragen, bis Sie erreicht haben Geben Sie den Filter ein, der für die Erfassung verwendet werden soll.

Schritt 5: Sie können die gleiche Filterzeichenfolge wie der benutzerdefinierte Filter in der GUI verwenden.

Das folgende Beispiel zeigt eine Filterung des gesamten Datenverkehrs mit Quell- oder Ziel-Port-Nummer 53 für TCP- und UDP-Ports:

```
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
```

## Filtern in SWA mit transparenter Bereitstellung

In SWA mit transparenter Bereitstellung, während die Verbindung mit dem Web Cache Communication Protocol (WCCP) über Generic Routing Encapsulation (GRE) Tunnel erfolgt, sind die Quell- und Ziel-IP-Adressen in den Paketen, die an SWA gesendet oder von SWA gesendet werden, die Router-IP-Adresse und die SWA-IP-Adresse.

Um die Paketerfassung mit der IP-Adresse oder Portnummer von der GUI abrufen zu können, gibt es zwei Optionen:

- Vordefinierte Filter
- Benutzerdefinierte Filter

Filtern in SWA mit transparenter Bereitstellung in GUI

Schritt 1: Wählen Sie auf der Seite Paketerfassung die Option Einstellungen bearbeiten aus.

Schritt 2: Wählen Sie unter Paketerfassungsfiler die Option Vordefinierte Filter aus.

Schritt 3: Sie können die IP-Adresse im Abschnitt Client IP oder Server IP eingeben.

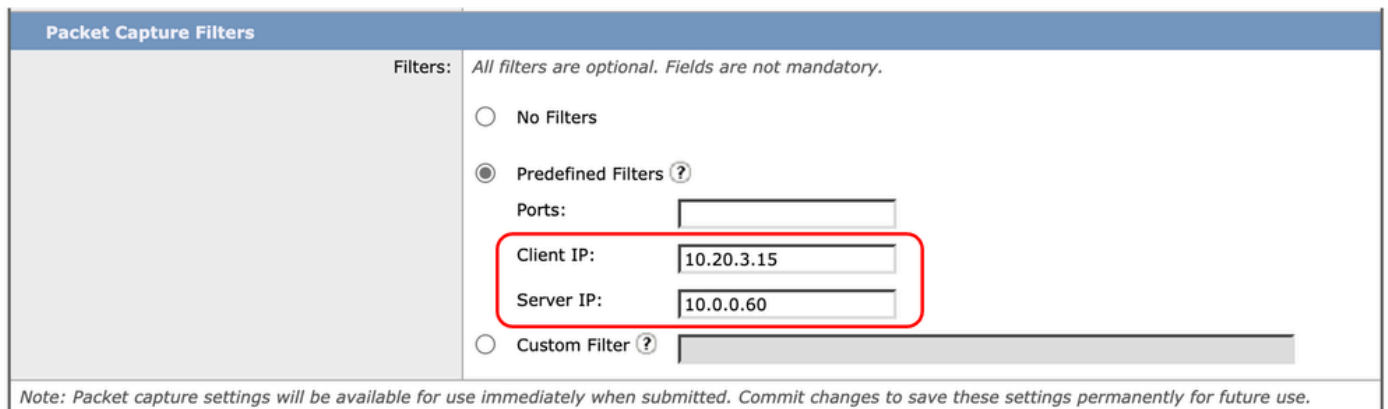


Bild - Konfigurieren der IP-Adresse in vordefinierten Filtern

Schritt 4: Senden Sie die Änderungen.

Schritt 5: Erfassung starten.



Hinweis: Nach dem Absenden des Filters hat SWA im Abschnitt "Filter Selected" (Ausgewählte Filter) zusätzliche Bedingungen hinzugefügt.

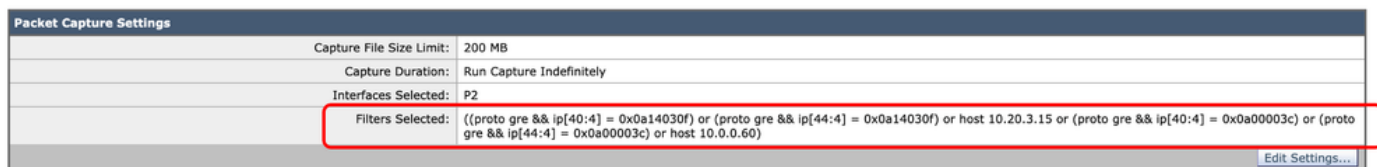


Bild - Zusätzliche Filter von SWA zum Sammeln von Paketen im GRE-Tunnel hinzugefügt

So verwenden Sie benutzerdefinierte Filter aus der GUI:

Schritt 1: Wählen Sie auf der Seite Paketerfassung die Option Einstellungen bearbeiten aus.

Schritt 2: Wählen Sie unter Paketerfassungsfiler die Option Benutzerdefinierter Filter aus.

Schritt 3: Fügen Sie zuerst diese Zeichenfolge hinzu, und dann den Filter, den Sie durch Hinzufügen oder nach dieser Zeichenfolge implementieren möchten:

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

Wenn Sie z. B. eine Filterung nach der Host-IP-Adresse 10.20.3.15 oder der Portnummer 8080 planen, können Sie folgende Zeichenfolge verwenden:

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

Schritt 4: Senden Sie die Änderungen.

Schritt 5: Erfassung starten.

Filtern in SWA mit transparenter Bereitstellung in CLI

So filtern Sie in transparenter Proxybereitstellung aus CLI:

Schritt 1: Melden Sie sich bei der CLI an.

Schritt 2: Geben Sie PacketCapture ein, und drücken Sie die Eingabetaste.

Schritt 3: Um den aktuellen Filter zu bearbeiten, geben Sie SETUP ein.

Schritt 4: Beantworten Sie die Fragen, bis Sie erreicht haben Geben Sie den Filter ein, der für die Erfassung verwendet werden soll.

Schritt 5: Sie können die gleiche Filterzeichenfolge wie der benutzerdefinierte Filter in der GUI verwenden.

Im folgenden Beispiel wird nach der Host-IP-Adresse 10.20.3.15 oder der Portnummer 8080 gefiltert:

```
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.

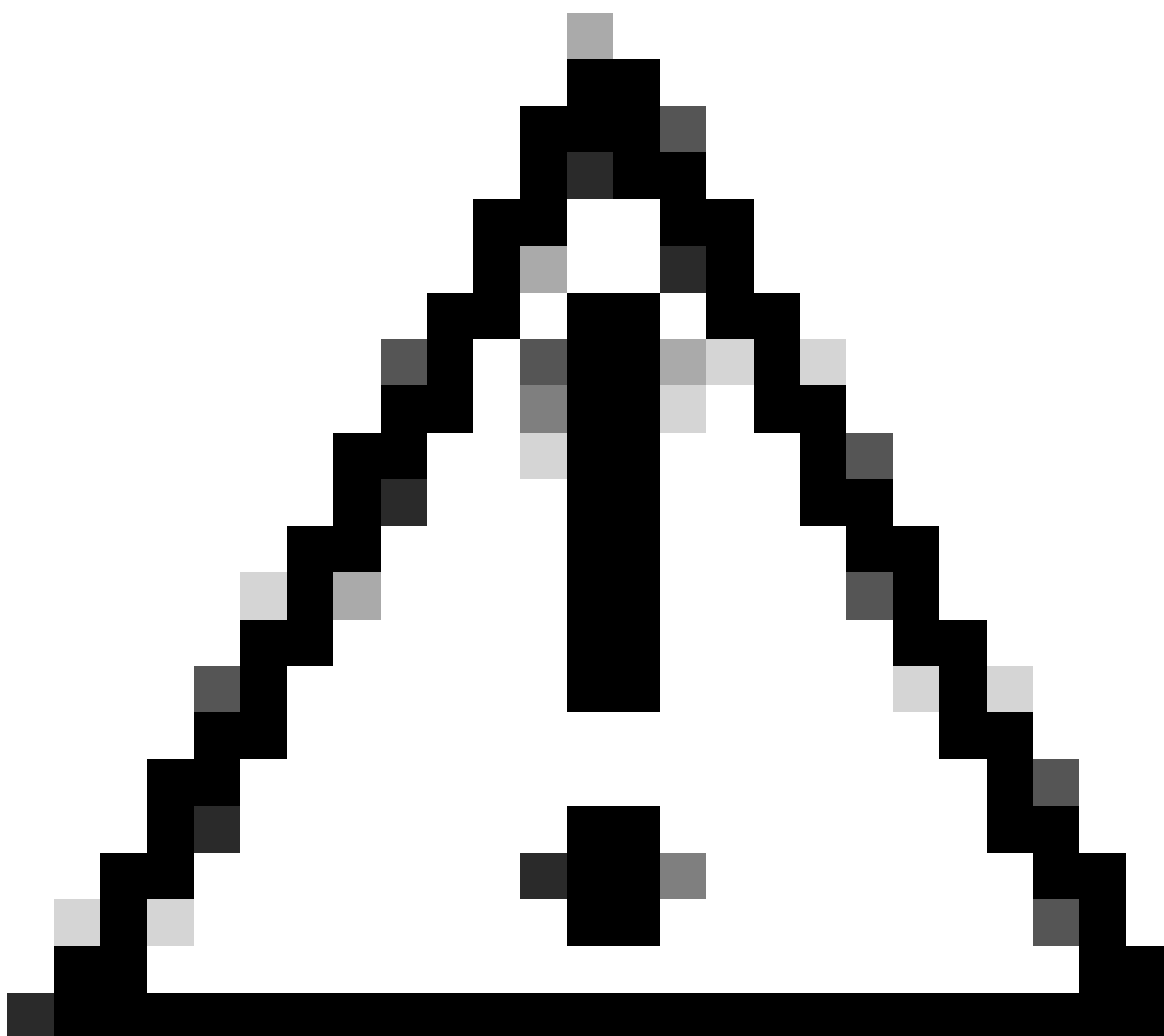
[(tcp port 80 or tcp port 3128)]> (proto gre && ip[40:4] = 0x0a14030f) or (proto gre && ip[44:4] = 0x0a

## Häufigste Filter

In der folgenden Tabelle sind die gängigsten Filter aufgeführt:

| Beschreibung                                                                     | Filter                                           |
|----------------------------------------------------------------------------------|--------------------------------------------------|
| Nach Quell-IP-Adresse filtern entspricht 10.20.3.15                              | src Host 10.20.3.15                              |
| Nach Ziel-IP-Adresse filtern entspricht 10.20.3.15                               | dst host 10,20.3,15                              |
| Nach Quell-IP-Adresse 10.20.3.15 und Ziel-IP-Adresse 10.0.0.60 filtern           | (Quellhost 10.20.3.15) und (Quellhost 10.0.0.60) |
| Nach Quell- oder Ziel-IP-Adresse filtern ist gleich 10.20.3.15                   | Host 10.20.3.15                                  |
| Filtern nach Quell- oder Ziel-IP-Adresse gleich 10.20.3.15 oder gleich 10.0.0.60 | Host 10.20.3.15 oder Host 10.0.0.60              |
| Nach TCP-Portnummer filtern entspricht 8080                                      | TCP-Port 8080                                    |
| Nach UDP-Portnummer filtern entspricht 53                                        | UDP-Port 53                                      |
| Nach Port-Nummer filtern, die 514 entspricht (TCP oder UDP)                      | Port 514                                         |
| Nur UDP-Pakete filtern                                                           | udp                                              |

|                                                                |                                                                                                                                                                    |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nur ICMP-Pakete filtern                                        | icmp                                                                                                                                                               |
| Hauptfilter für jede Erfassung in transparenter Bereitstellung | (proto gre && ip[40:4] = 0x0a14030f) oder (proto gre && ip[44:4] = 0x0a14030f) oder (proto gre && ip[40:4] = 0x0a00003c) oder (proto gre && ip[44:4] = 0x0a00003c) |



Achtung: Bei allen Filtern wird die Groß- und Kleinschreibung berücksichtigt.

## Fehlerbehebung

"Filter Error" (Filterfehler) ist einer der häufigsten Fehler bei der Paketerfassung.

## 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...

Bild - Filterfehler

Dieser Fehler ist normalerweise auf eine falsche Filterimplementierung zurückzuführen. Im vorherigen Beispiel enthält der ICMP-Filter Großbuchstaben. Aus diesem Grund erhalten Sie Filterfehler. Um dieses Problem zu beheben, müssen Sie den Filter bearbeiten und den ICMP durch icmp ersetzen.

## Zugehörige Informationen

- [Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - GD\(Allgemeine Bereitstellung\) - Endbenutzerklassifizierung...](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.