Configurer la capture de paquets sur l'appliance de sécurité du contenu

Table des matières

Introduction

Ce document décrit la capture de paquets sur Cisco Secure Web Appliance (SWA), Email Security Appliance (ESA) et Security Management Appliance (SMA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration de Cisco Content Security Appliance.

Cisco recommande que vous ayez :

- SWA/ESA/SMA physique ou virtuel installé.
- Accès administratif à l'interface utilisateur graphique (GUI) SWA/ESA/SMA.

- Accès administratif à l'interface de ligne de commande (CLI) SWA/ESA/SMA

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Effectuer une capture de paquets depuis l'interface graphique

Pour capturer des paquets à partir de l'interface utilisateur graphique, procédez comme suit :

Étape 1. Connectez-vous à l'interface utilisateur graphique.

Étape 2. Dans la partie supérieure droite de la page, sélectionnez Support et aide.

Étape 3. Sélectionnez Packet Capture.

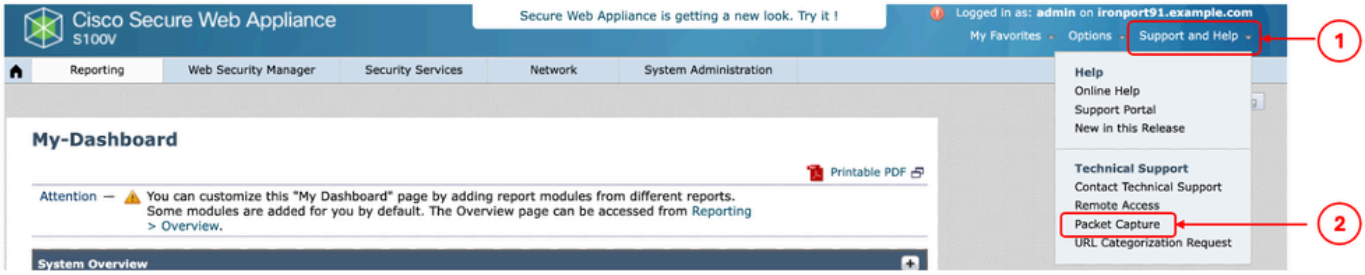


Image - Capture de paquets

Étape 4. (Facultatif) Pour modifier le filtre actuel, sélectionnez Modifier les paramètres. (Pour plus d'informations sur les filtres, consultez la section Filtres de ce document)

Étape 5. Démarrez la capture.

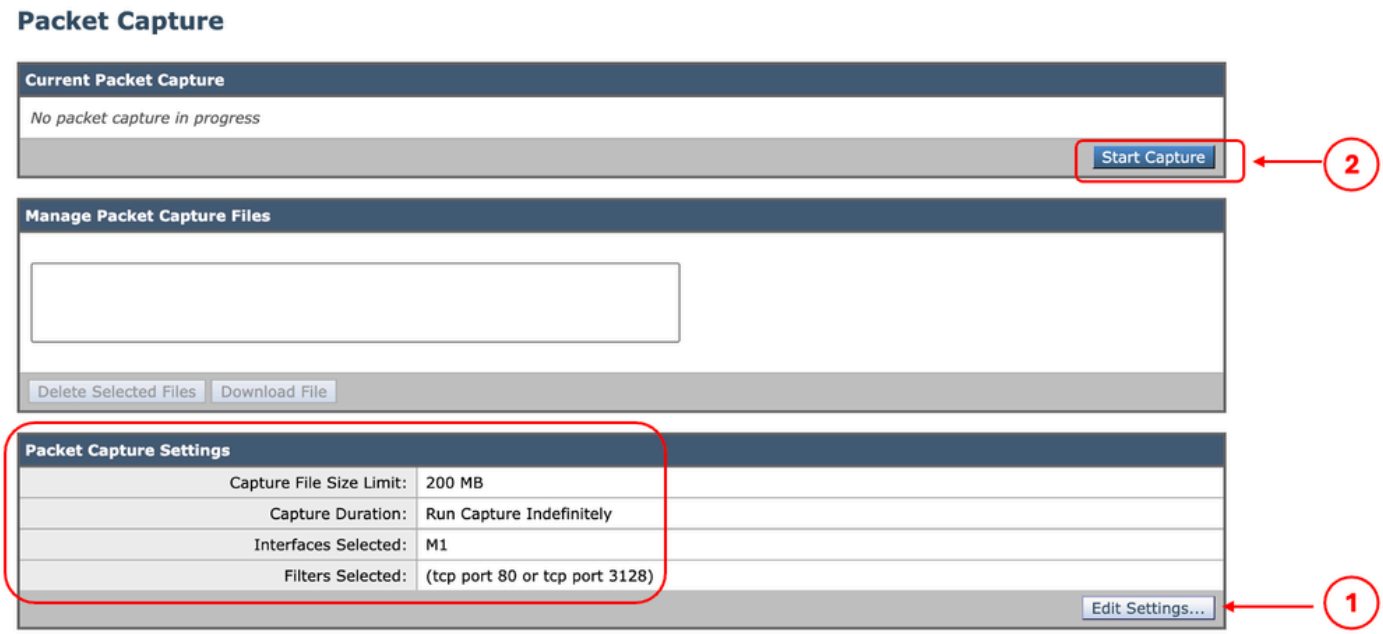
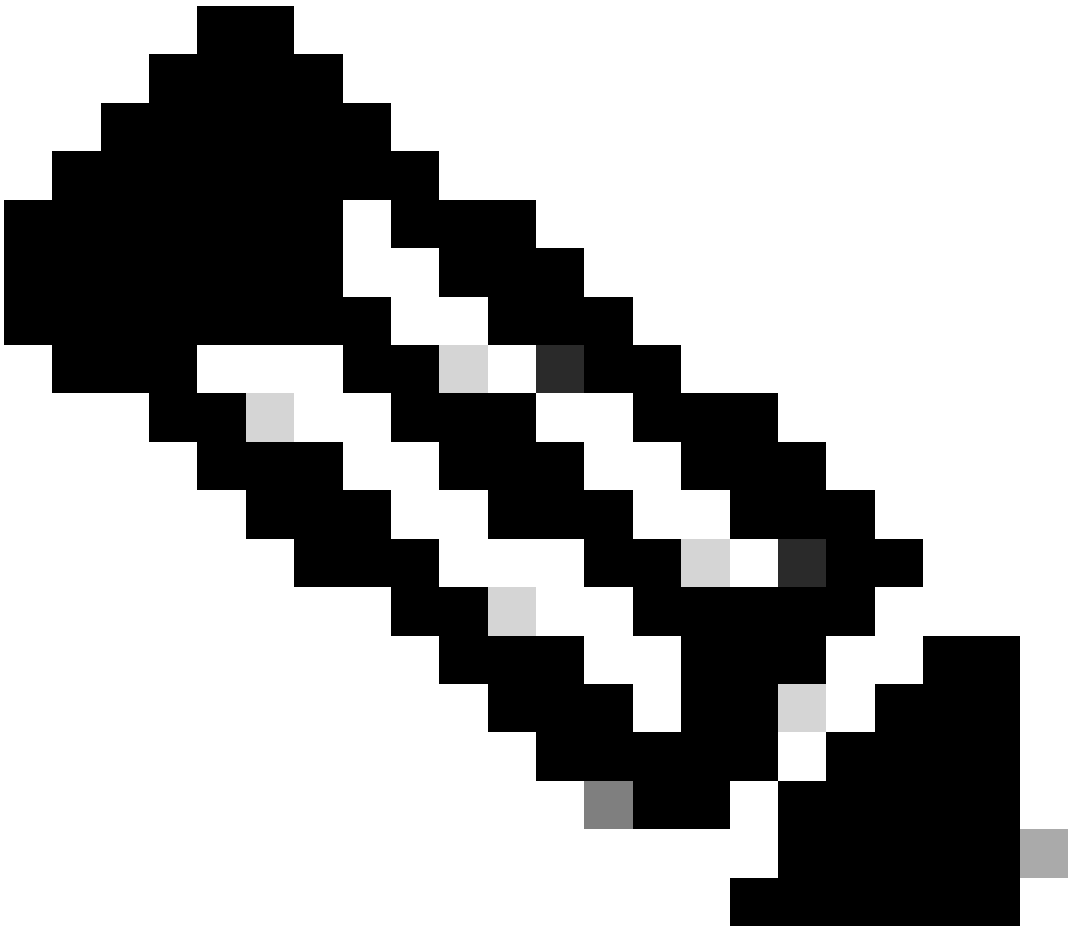


Image - Filtres et état de capture des paquets



Remarque : la taille maximale du fichier de capture de paquets est de 200 Mo. Lorsque la taille du fichier atteint 200 Mo, la capture de paquets s'arrête.

La section Capture de paquets en cours affiche l'état de la capture de paquets, y compris la taille du fichier et les filtres appliqués.

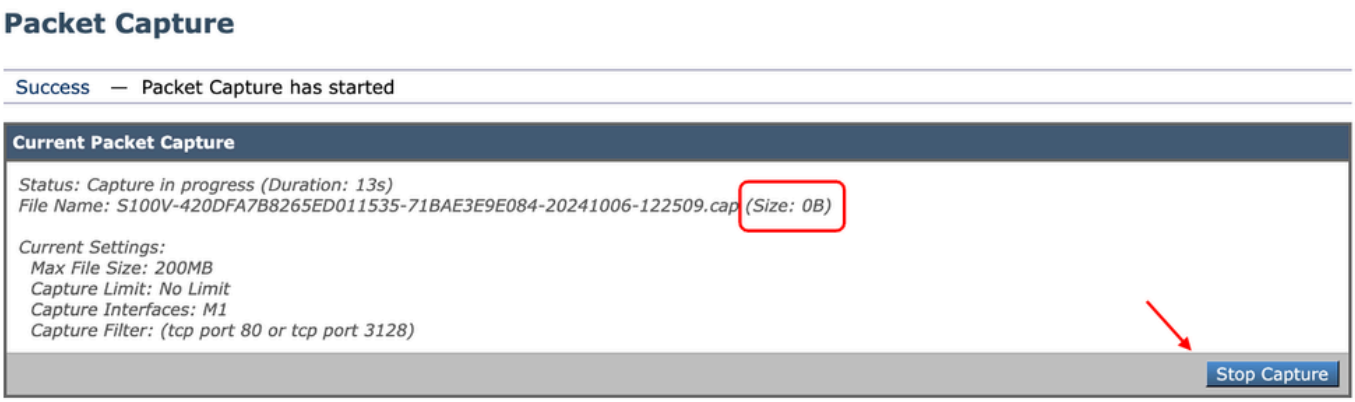
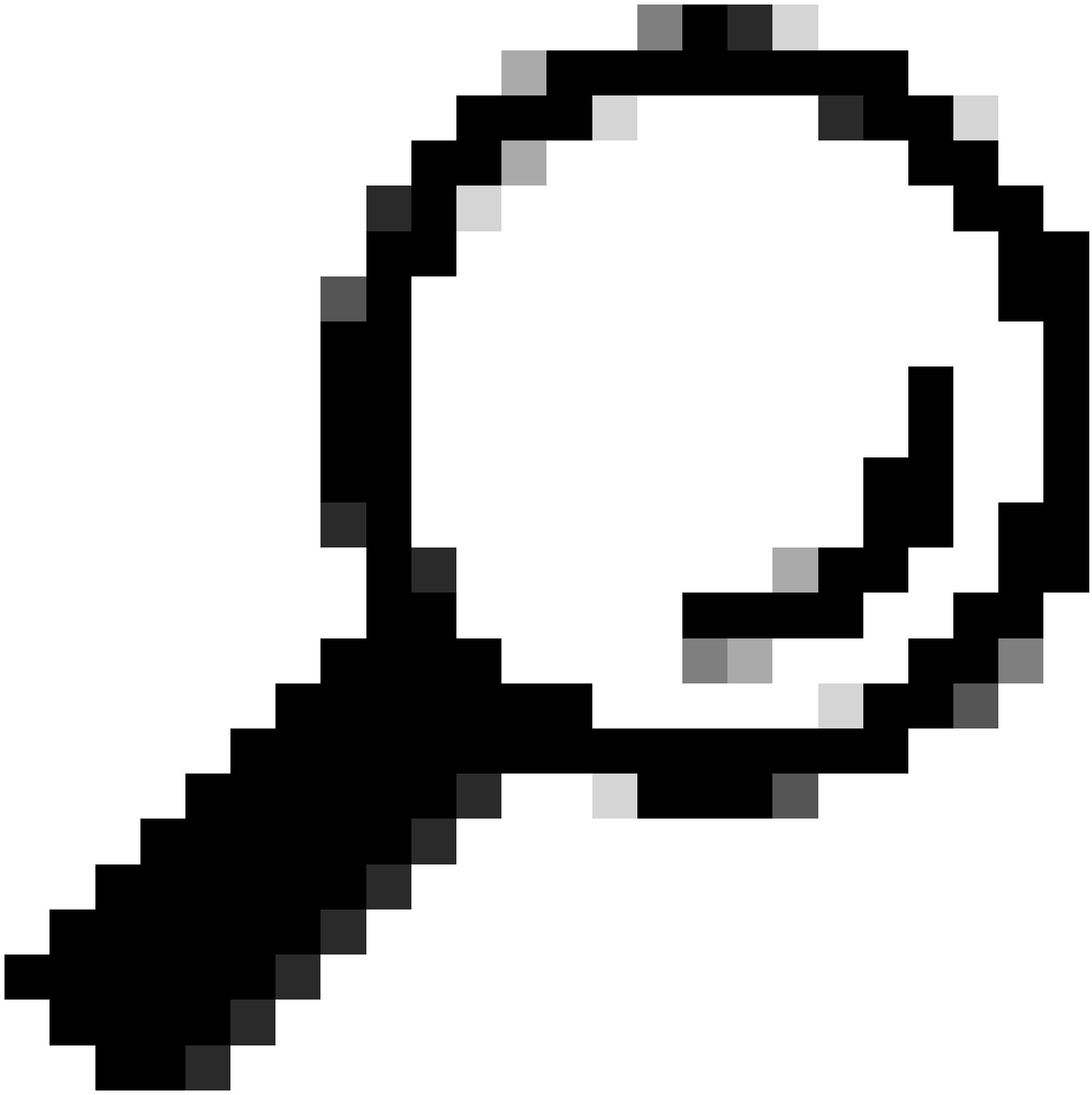


Image - État de capture des paquets

Étape 6. Pour arrêter la capture de paquets en cours d'exécution, cliquez sur Arrêter la capture.

Étape 7. Pour télécharger le fichier de capture de paquets, choisissez le fichier dans la liste Manage Packet Capture Files et cliquez sur Download File.

Image - Télécharger la capture de paquets



Conseil : le dernier fichier se trouve en haut de la liste.

Étape 8. (Facultatif) Pour supprimer un fichier de capture de paquets, sélectionnez-le dans la liste Gérer les fichiers de capture de paquets et cliquez sur Supprimer les fichiers sélectionnés.

Capture de paquets à partir de CLI

Vous pouvez également démarrer la capture de paquets à partir de l'interface de ligne de commande en procédant comme suit :

Étape 1. Connectez-vous à la CLI.

Étape 2. Tapez packet capture et appuyez sur Entrée.

Étape 3. (Facultatif) Pour modifier le type de filtre actuel, SETUP. (Pour plus d'informations sur les filtres, consultez la section Filtres de ce document.)

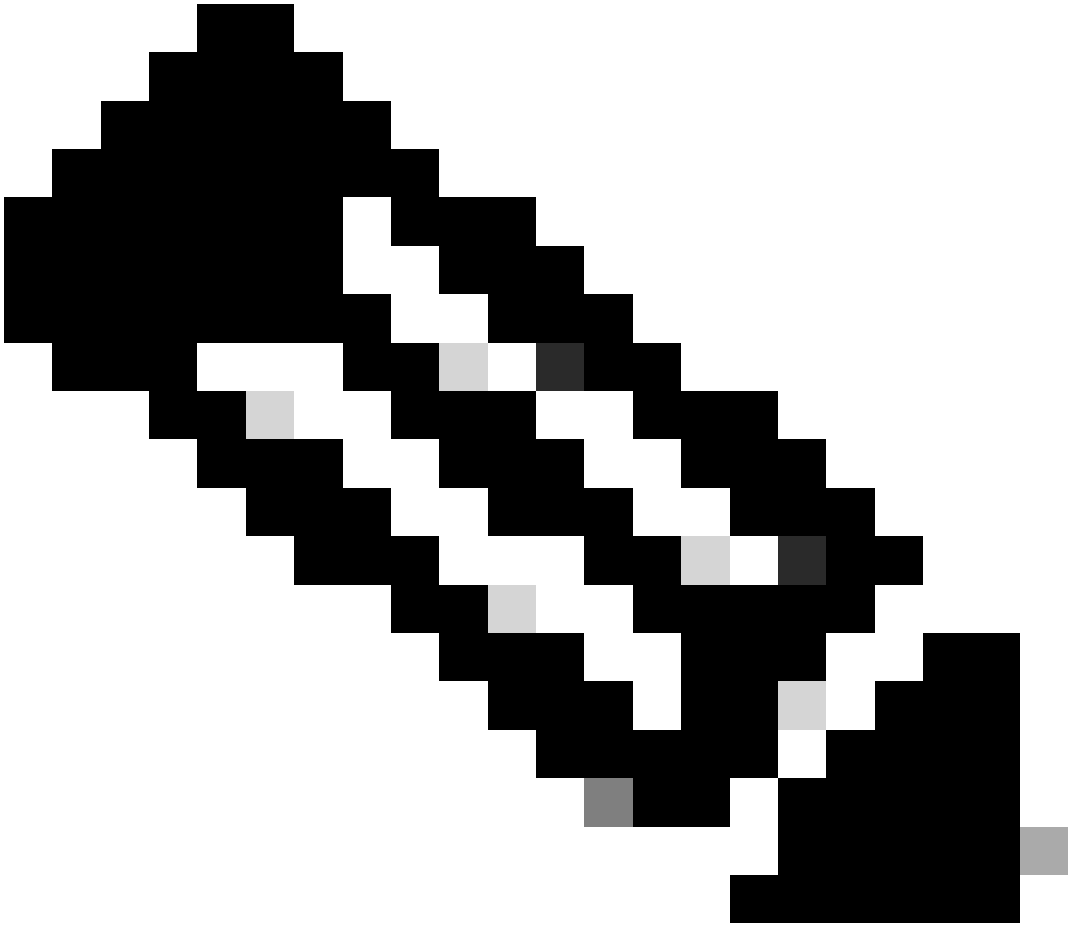
Étape 4. Sélectionnez START pour démarrer la capture.

```
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.
```

Étape 5. (Facultatif) Vous pouvez afficher l'état de la capture de paquets en sélectionnant 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)
```

Étape 6. Pour arrêter la capture de paquets, tapez STOP et appuyez sur Entrée :



Remarque : pour télécharger les fichiers de capture de paquets collectés à partir de l'interface de ligne de commande, vous pouvez les télécharger à partir de l'interface utilisateur graphique ou vous connecter à l'appliance via le protocole FTP (File Transfer Protocol) et les télécharger à partir du dossier Captures.

Filtres

Voici quelques guides sur les filtres que vous pouvez utiliser dans les appliances de sécurité du contenu.

Filtrer par adresse IP hôte

Filtrer par adresse IP hôte dans l’interface utilisateur graphique

Pour filtrer par adresse IP d'hôte, deux options sont disponibles depuis l'interface utilisateur graphique :

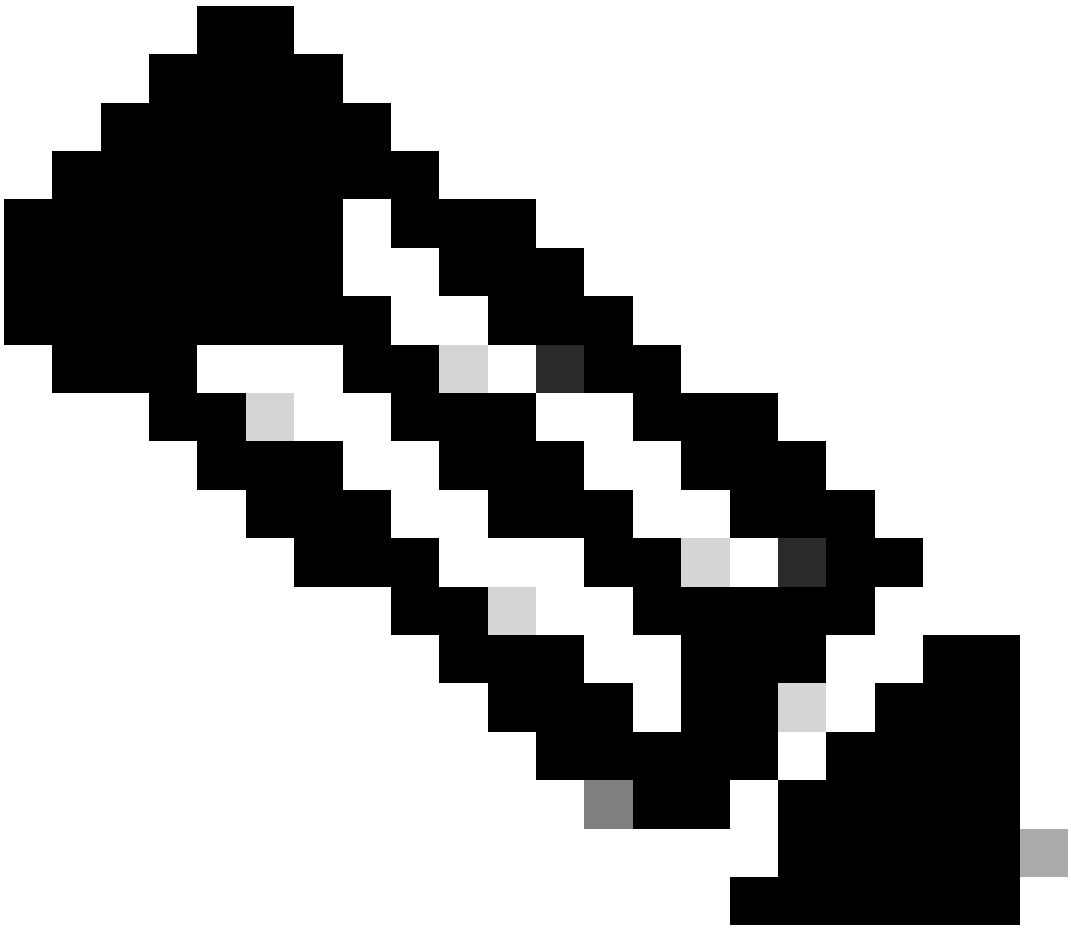
- Filtres prédéfinis
- Filtres personnalisés

Pour utiliser des filtres prédéfinis à partir de l'interface utilisateur graphique :

Étape 1. Dans la page Capture de paquets, sélectionnez Modifier les paramètres.

Étape 2. Dans Packet Capture Filters, sélectionnez Predefined Filters.

Étape 3. Vous pouvez entrer l'adresse IP dans la section Client IP ou Server IP.



Remarque : le choix entre l'adresse IP du client ou l'adresse IP du serveur ne se limite pas à l'adresse source ou de destination. Ce filtre capture tous les paquets dont l'adresse IP est définie comme source ou destination.

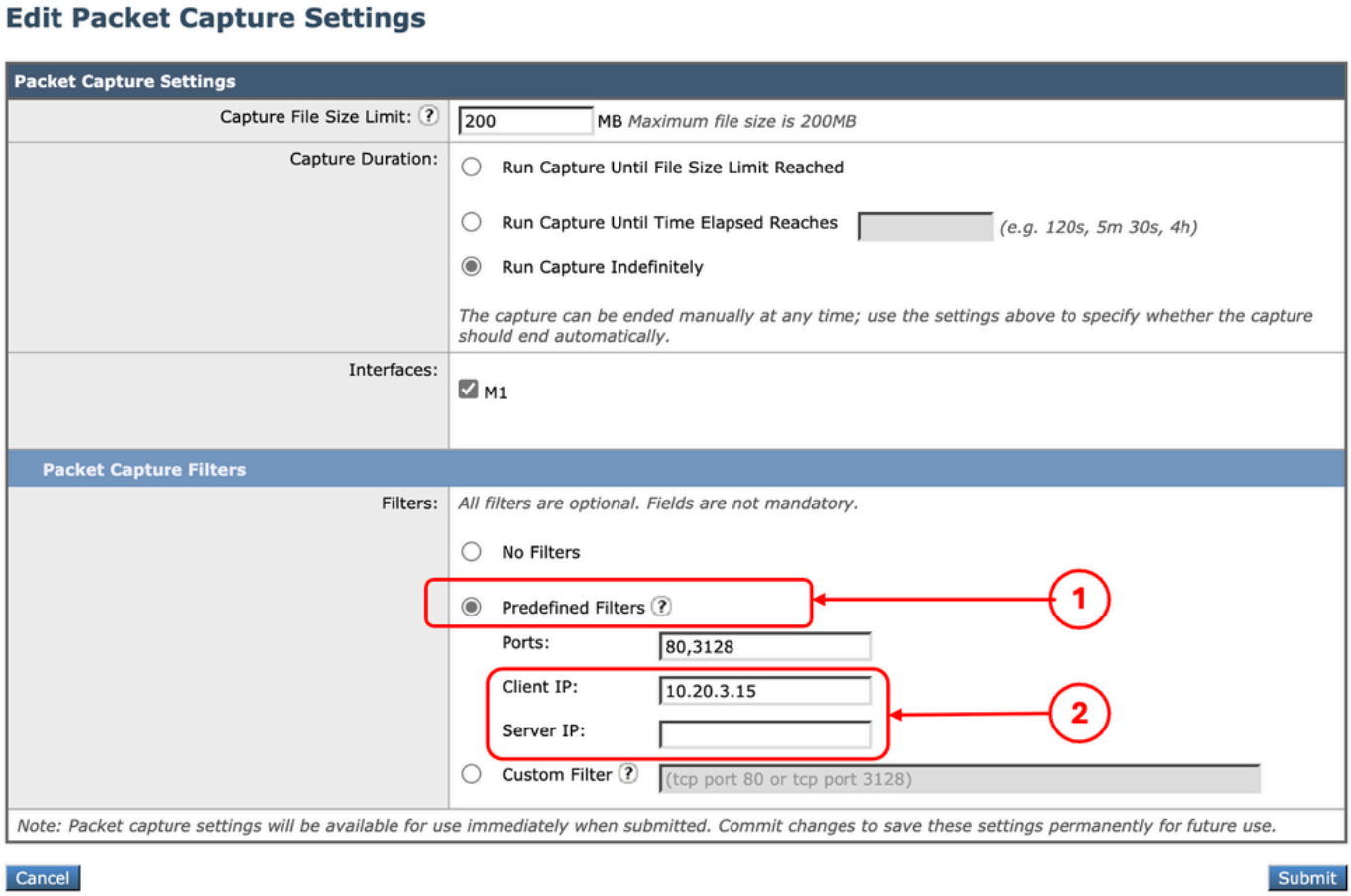
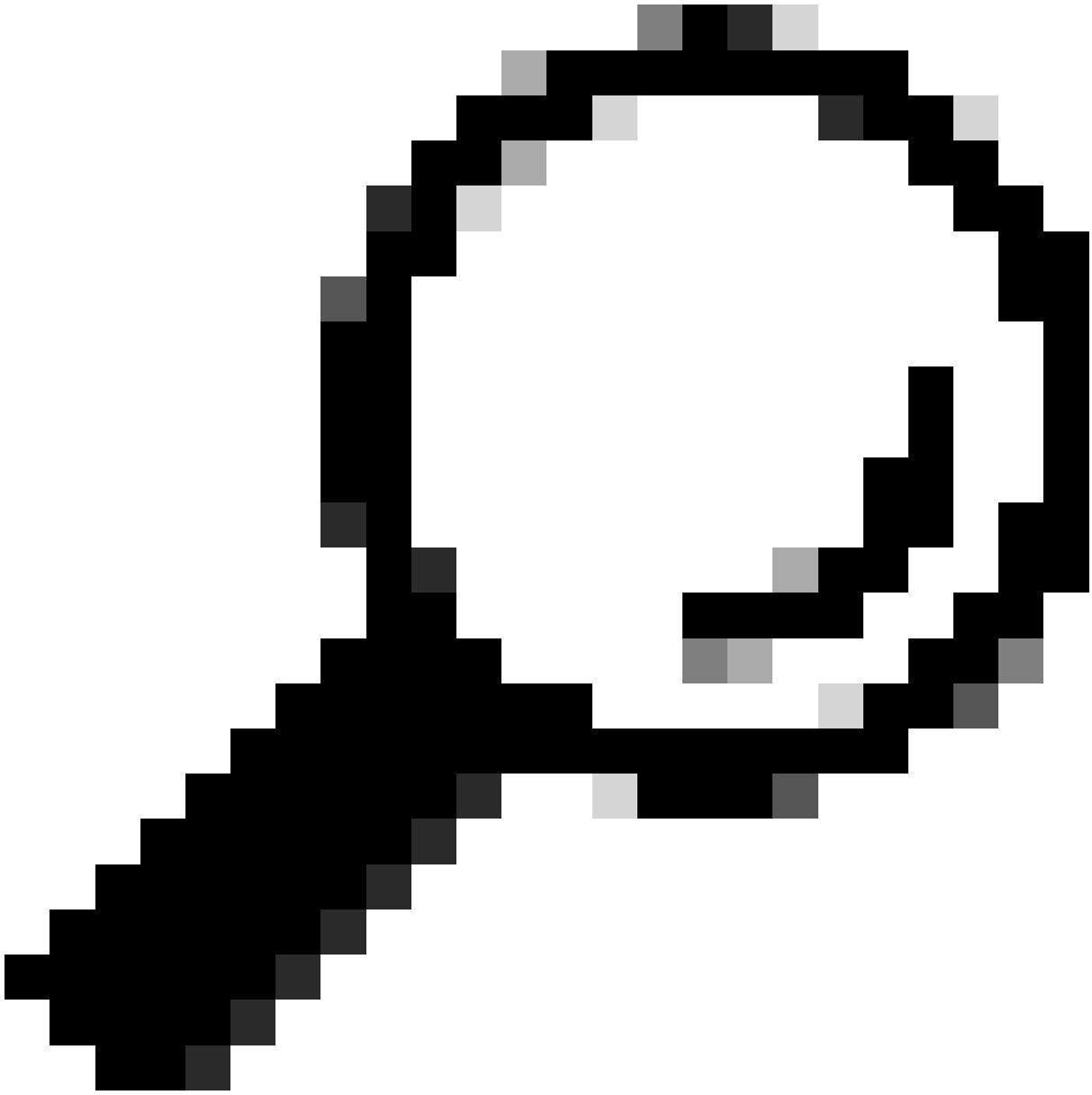


Image - Filtrer par IP hôte à partir des filtres prédéfinis de l'interface graphique

Étape 4. Envoyez les modifications.

Étape 5. Démarrez la capture.



Conseil : il n'est pas nécessaire de valider les modifications, le filtre nouvellement ajouté est appliqué à la capture actuelle. La validation des modifications permet d'enregistrer le filtre pour une utilisation ultérieure.

Pour utiliser les filtres personnalisés et les filtres prédéfinis depuis l'interface utilisateur graphique :

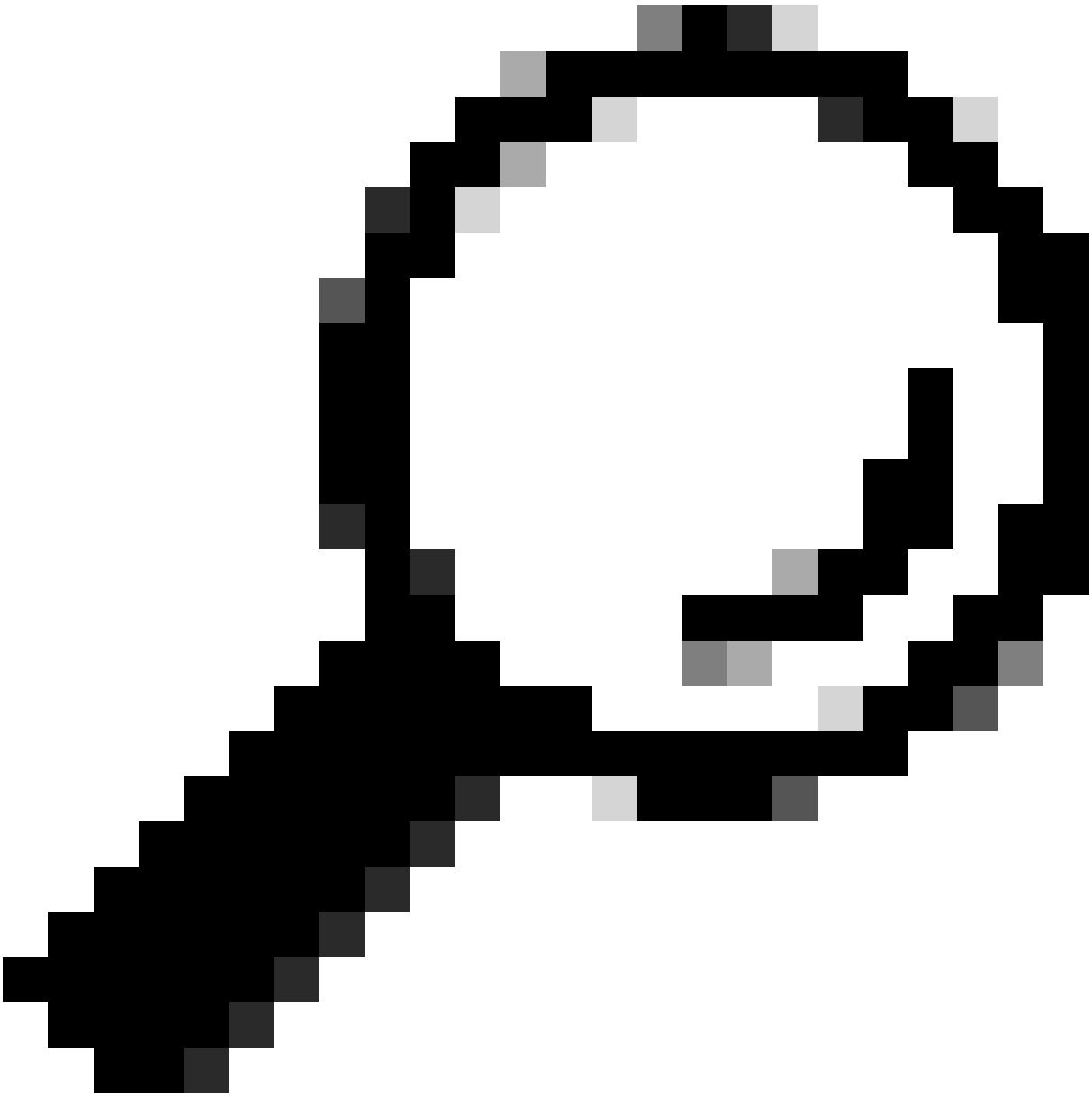
Étape 1. Dans la page Capture de paquets, sélectionnez Modifier les paramètres.

Étape 2. Dans Packet Capture Filters, sélectionnez Custom Filter.

Étape 3. Utilisez la syntaxe host suivie de l'adresse IP.

Voici un exemple pour filtrer tout le trafic avec l'adresse IP source ou de destination 10.20.3.15

```
host 10.20.3.15
```



Conseil : pour filtrer par plusieurs adresses IP, vous pouvez utiliser des opérandes logiques tels que ou et et (lettres minuscules uniquement).

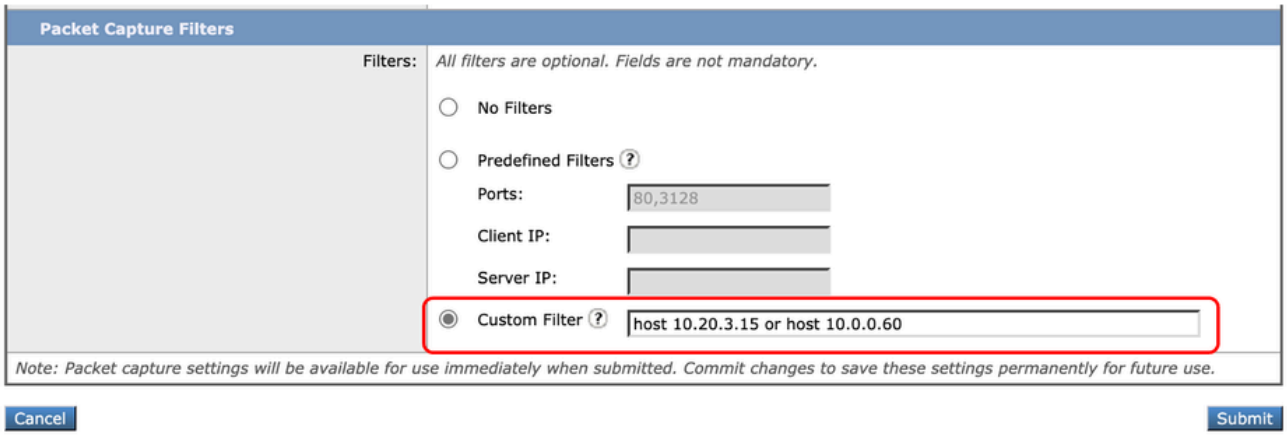


Image - Filtre personnalisé pour deux adresses IP

Étape 4. Envoyez les modifications.

Étape 5. Démarrer la capture

Filtrer par IP hôte dans CLI

Pour filtrer par l'adresse IP de l'hôte à partir de la CLI :

Étape 1. Connectez-vous à la CLI.

Étape 2. Tapez packet capture et appuyez sur Entrée.

Étape 3. Pour modifier le filtre actuel, tapez SETUP.

Étape 4. Répondez aux questions jusqu'à ce que vous atteigniez Entrez le filtre à utiliser pour la capture

Étape 5. Vous pouvez utiliser la même chaîne de filtre que le filtre personnalisé dans l'interface utilisateur graphique.

Voici un exemple de filtrage de tout le trafic avec l'adresse IP source ou de destination 10.20.3.15 ou 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
```

Filtrer par numéro de port

Filtrer par numéro de port dans l'interface utilisateur

Pour filtrer par numéro(s) de port, l'interface utilisateur graphique propose deux options :

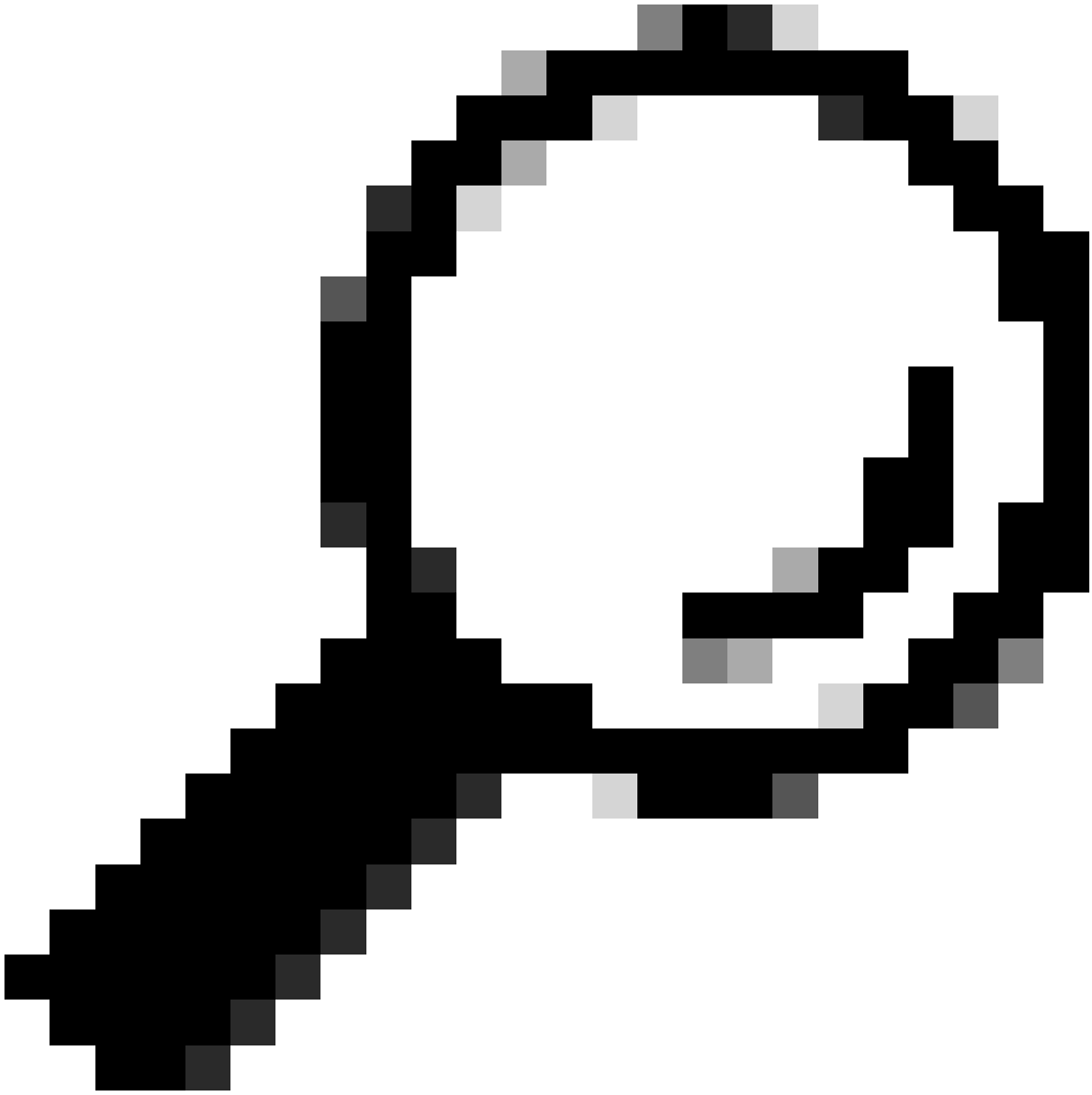
- Filtres prédéfinis
- Filtres personnalisés

Pour utiliser des filtres prédéfinis depuis l'interface utilisateur graphique :

Étape 1. Dans la page Capture de paquets, sélectionnez Modifier les paramètres.

Étape 2. Dans Packet Capture Filters, sélectionnez Predefined Filters.

Étape 3. Dans la section Ports, tapez les numéros de port que vous souhaitez filtrer.



Conseil : vous pouvez ajouter plusieurs numéros de port en les séparant par une virgule " , ".

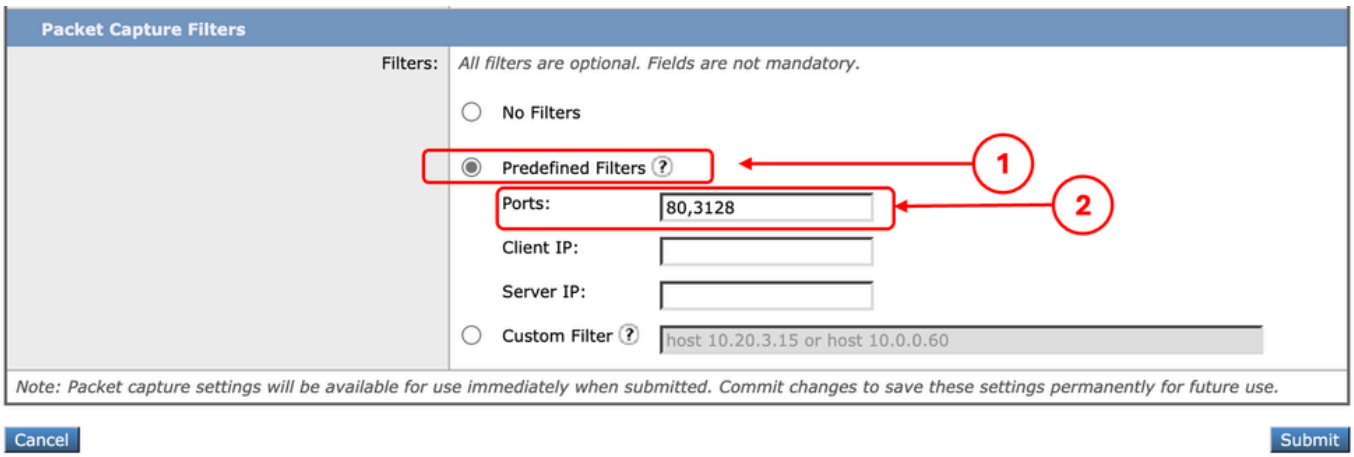
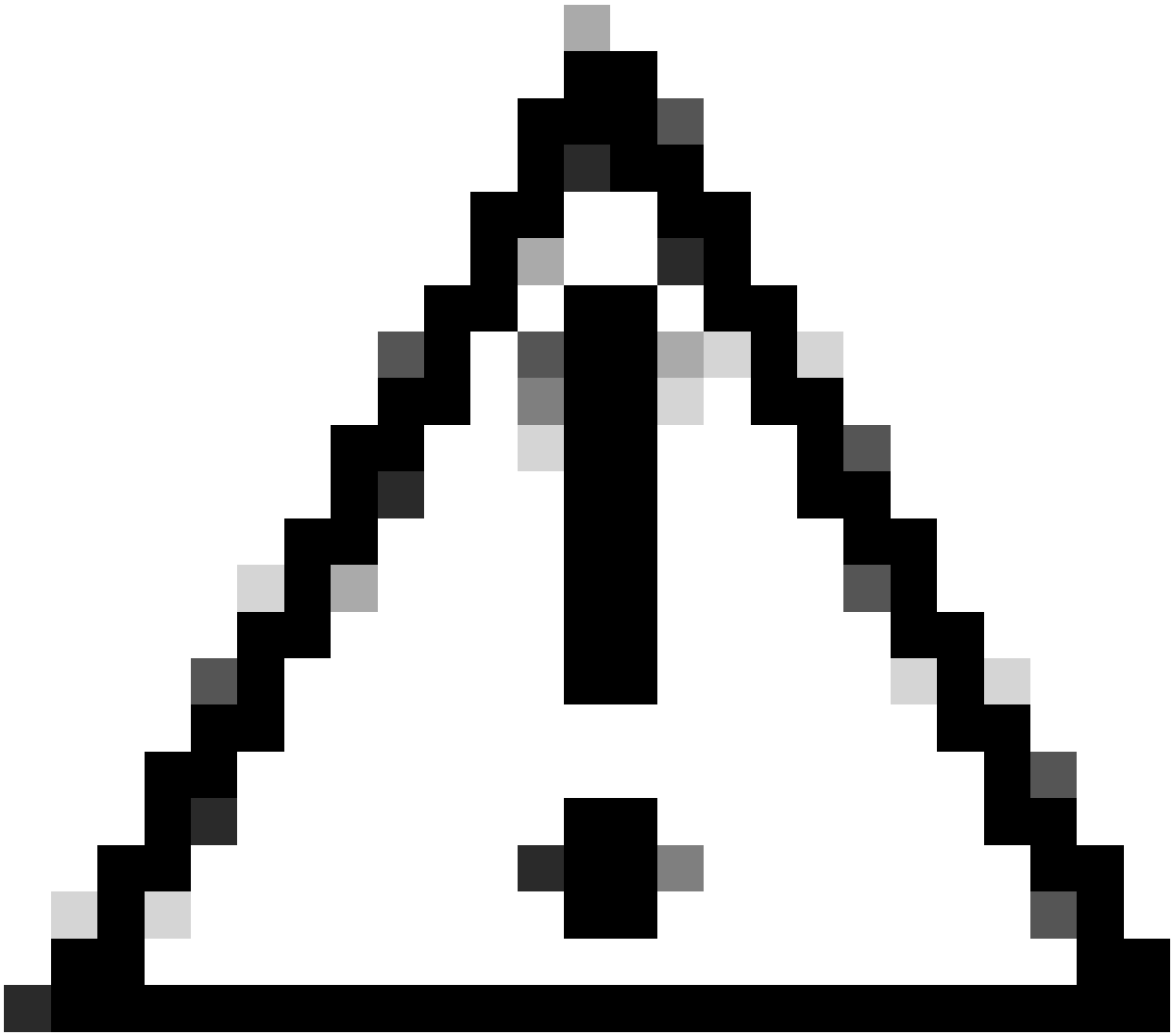


Image - Filtrer par numéro de port

Étape 4. Envoyez les modifications.

Étape 5. Démarrez la capture.



Attention : cette approche capture uniquement le trafic TCP avec les numéros de port définis. Pour capturer le trafic UDP, utilisez le filtre personnalisé.

Pour utiliser les filtres personnalisés depuis l'interface utilisateur graphique :

Étape 1. Dans la page Capture de paquets, sélectionnez Modifier les paramètres.

Étape 2. Dans Packet Capture Filters, sélectionnez Custom Filter.

Étape 3. Utilisez la syntaxe de port suivie du numéro de port.

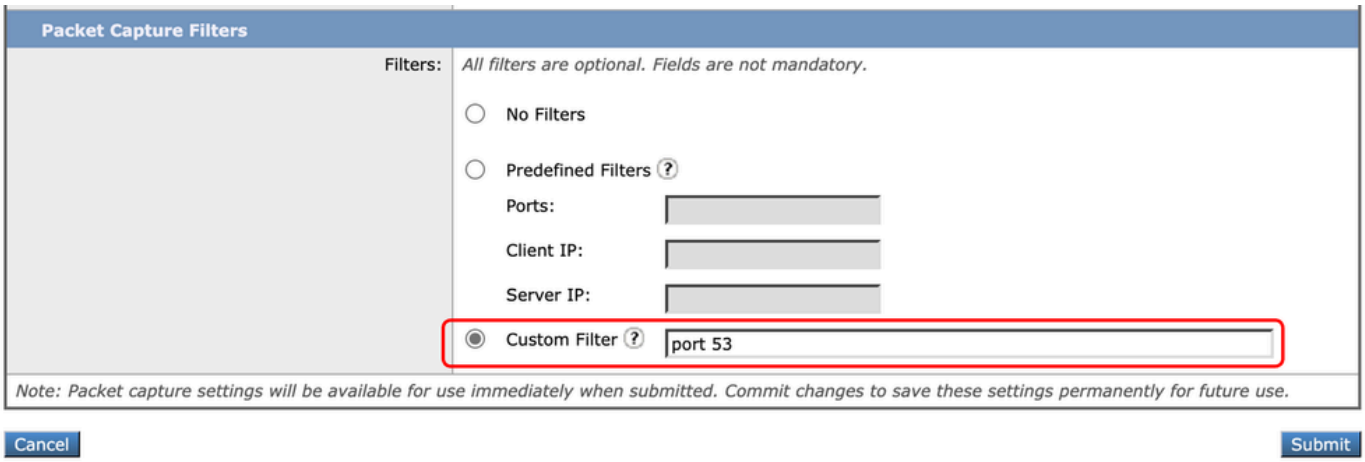
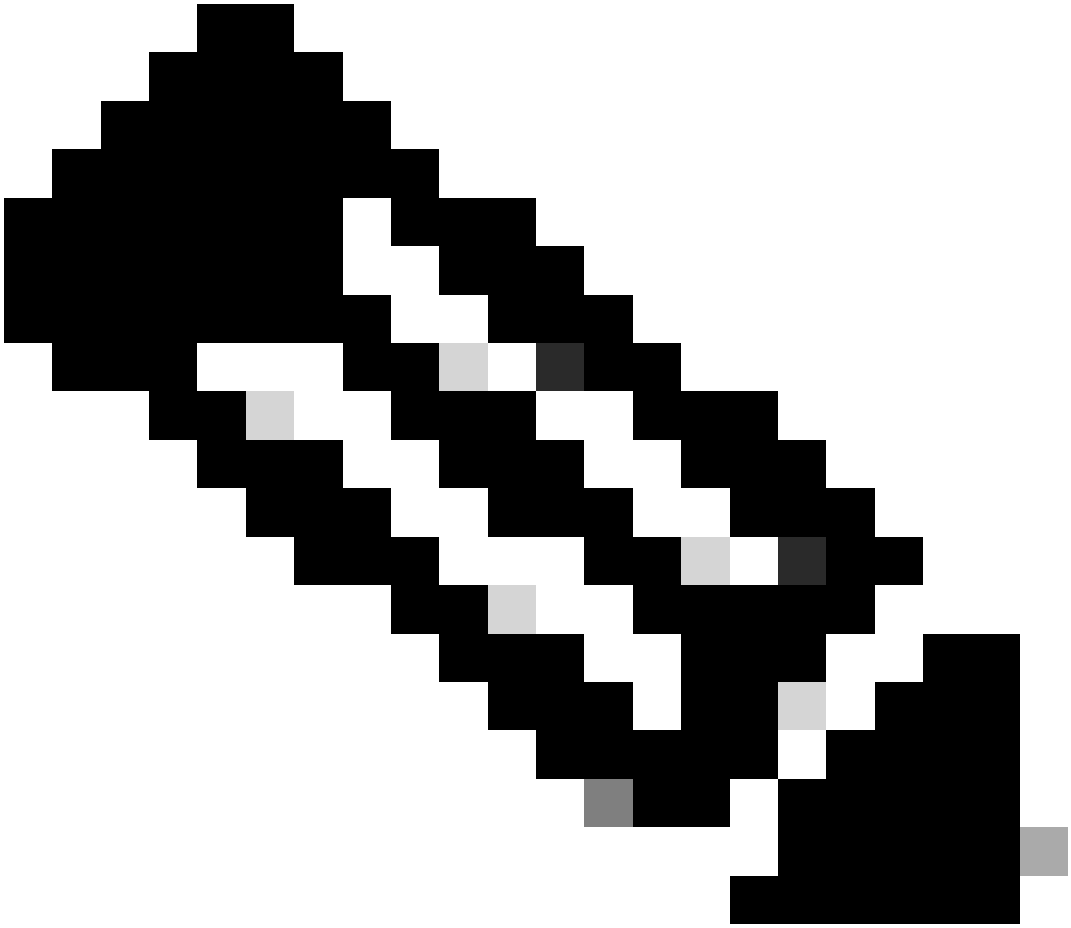


Image - Filtrage personnalisé par numéro de port



Remarque : si vous utilisez uniquement le port, ce filtre couvre à la fois les ports TCP et UDP.

Étape 4. Envoyez les modifications.

Étape 5. Démarrez la capture.

Filtrer par numéro de port dans CLI

Pour filtrer par numéro de port à partir de l'interface CLI :

Étape 1. Connectez-vous à la CLI.

Étape 2. Tapez packet capture et appuyez sur Entrée.

Étape 3. Pour modifier le filtre actuel, tapez SETUP.

Étape 4. Répondez aux questions jusqu'à ce que vous atteigniez Entrez le filtre à utiliser pour la capture

Étape 5. Vous pouvez utiliser la même chaîne de filtre que le filtre personnalisé dans l'interface utilisateur graphique.

Voici un exemple de filtrage de tout le trafic avec le numéro de port source ou de destination 53, pour les ports TCP et 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
```

Filtrer dans SWA avec déploiement transparent

Dans SWA avec déploiement transparent, alors que la connectivité du protocole WCCP (Web Cache Communication Protocol) se fait via des tunnels GRE (Generic Routing Encapsulation), les adresses IP source et de destination dans les paquets entrant ou sortant de SWA sont l'adresse IP du routeur et l'adresse IP SWA.

Pour pouvoir collecter la capture de paquets avec l'adresse IP ou le numéro de port à partir de l'interface graphique, deux options sont possibles :

- Filtres prédéfinis
- Filtres personnalisés

Filtrer dans SWA avec déploiement transparent dans l'interface utilisateur graphique

Étape 1. Dans la page Capture de paquets, sélectionnez Modifier les paramètres.

Étape 2. Dans Packet Capture Filters, sélectionnez Predefined Filters.

Étape 3. Vous pouvez entrer l'adresse IP dans la section Client IP ou Server IP.

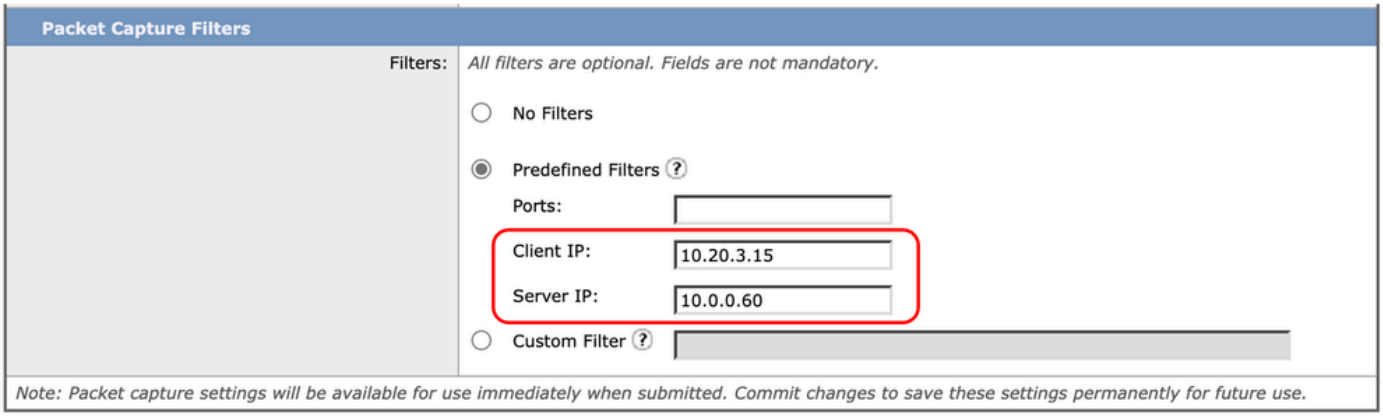
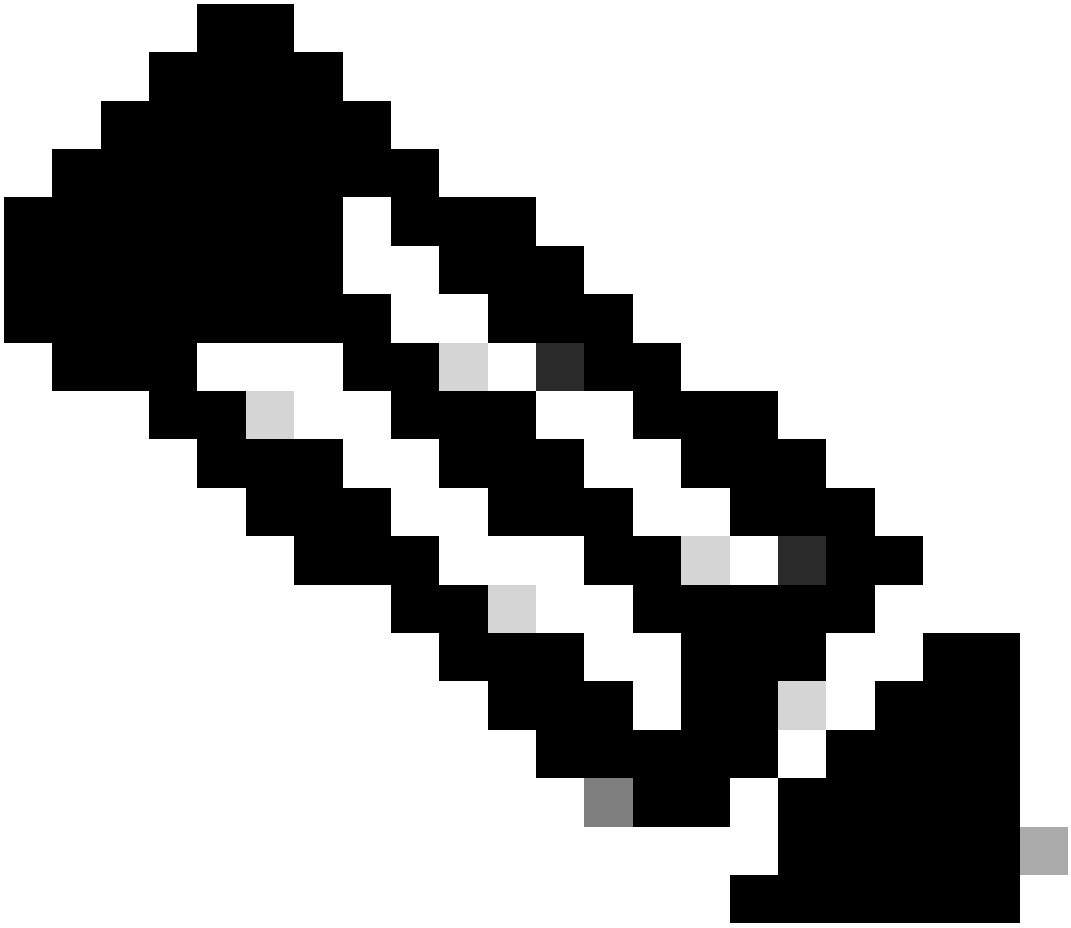


Image : configuration de l'adresse IP dans les filtres prédéfinis

Étape 4. Envoyez les modifications.

Étape 5. Démarrez la capture.



Remarque : vous pouvez voir qu'après l'envoi du filtre, SWA a ajouté des conditions supplémentaires dans la section Filtre sélectionné.

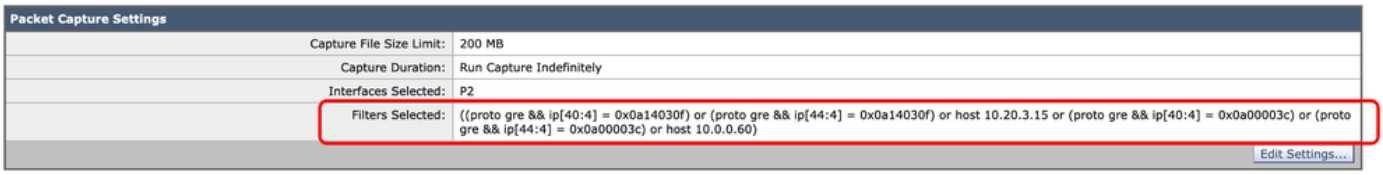


Image - Filtres supplémentaires ajoutés par SWA pour collecter les paquets dans le tunnel GRE

Pour utiliser les filtres personnalisés depuis l'interface utilisateur graphique :

Étape 1. Dans la page Capture de paquets, sélectionnez Modifier les paramètres.

Étape 2. Dans Packet Capture Filters, sélectionnez Custom Filter

Étape 3. Ajoutez d'abord cette chaîne, puis le filtre que vous prévoyez d'implémenter en ajoutant ou après cette chaîne :

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

Par exemple, si vous prévoyez de filtrer par l'adresse IP de l'hôte égale à 10.20.3.15 ou le numéro de port égal à 8080, vous pouvez utiliser cette chaîne :

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

Étape 4. Envoyez les modifications.

Étape 5. Démarrez la capture.

Filtrer dans SWA avec déploiement transparent dans CLI

Pour filtrer dans un déploiement de proxy transparent à partir de la CLI :

Étape 1. Connectez-vous à la CLI.

Étape 2. Tapez packet capture et appuyez sur Entrée.

Étape 3. Pour modifier le filtre actuel, tapez SETUP.

Étape 4. Répondez aux questions jusqu'à ce que vous atteigniez Entrez le filtre à utiliser pour la capture

Étape 5. Vous pouvez utiliser la même chaîne de filtre que le filtre personnalisé dans l'interface utilisateur graphique.

Voici un exemple pour filtrer par l'adresse IP de l'hôte égale à 10.20.3.15 ou le numéro de port égal à 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]>
```

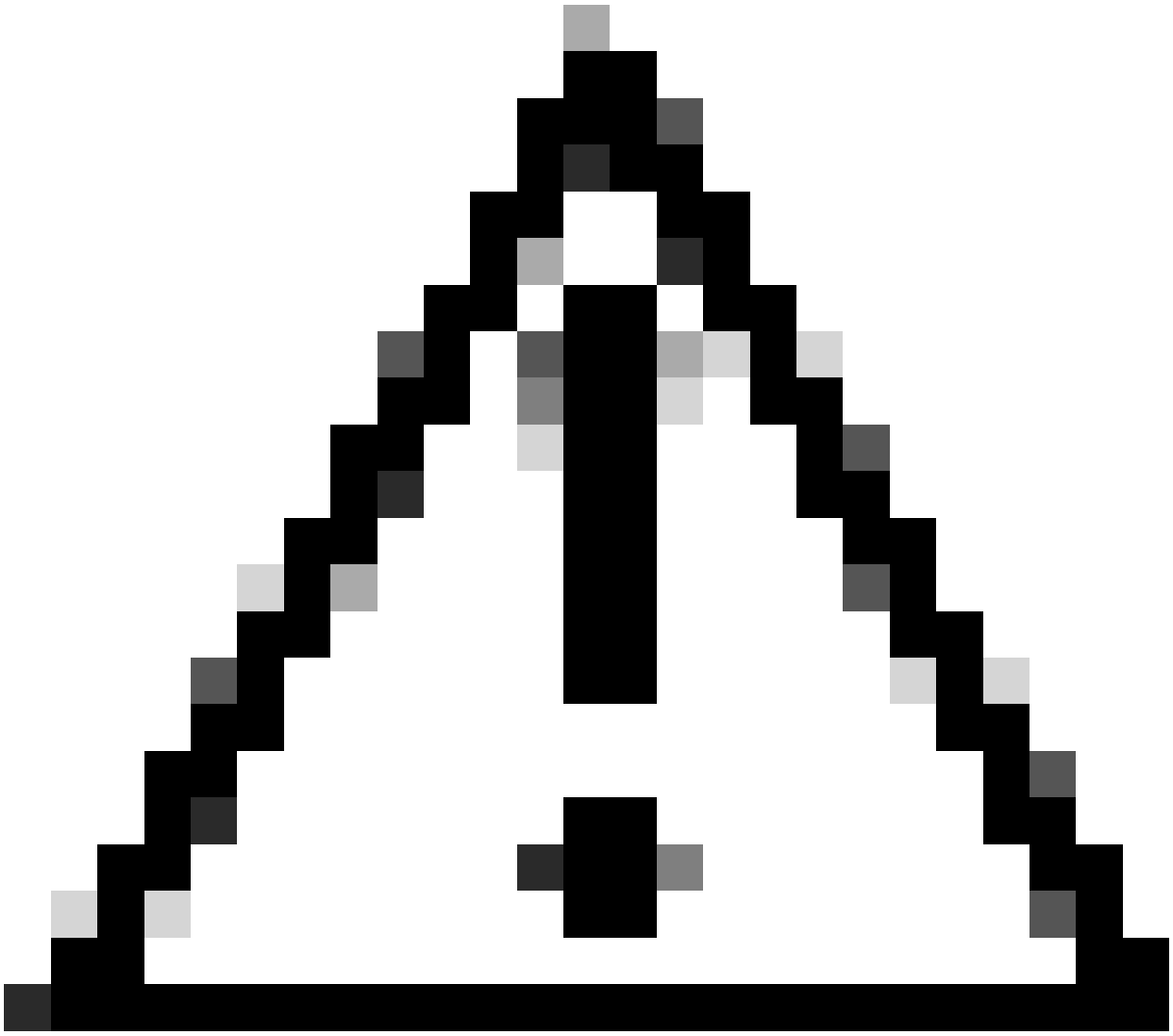
```
Do you want to stop the capture when the file size is reached? (If not, a new file will be started and
[N]>

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
```

Filtres les plus courants

Voici un tableau qui répertorie les filtres les plus courants :

Description	Filtre
Filtrer par adresse IP source égale à 10.20.3.15	hôte src 10.20.3.15
Filtrer par adresse IP de destination égale à 10.20.3.15	dst host 10.20.3.15
Filtrer par adresse IP source égale à 10.20.3.15 et adresse IP de destination égale à 10.0.0.60	(hôte src 10.20.3.15) et (hôte dst 10.0.0.60)
Filtrer par adresse IP source ou de destination égale à 10.20.3.15	hôte 10.20.3.15
Filtrer par adresse IP source ou de destination égale à 10.20.3.15 ou égale à 10.0.0.60	hôte 10.20.3.15 ou hôte 10.0.0.60
Filtrer par numéro de port TCP égal à 8080	port TCP 8080
Filtrer par numéro de port UDP égal à 53	port udp 53
Filtrer par numéro de port égal à 514 (TCP ou UDP)	port 514
Filtrer uniquement les paquets UDP	upp

Filtrer uniquement les paquets ICMP	icmp
Filtre principal à utiliser pour chaque capture dans un déploiement transparent	(proto gre && ip[40:4] = 0x0a14030f) ou (proto gre && ip[44:4] = 0x0a14030f) ou (proto gre && ip[40:4] = 0x0a00003c) ou (proto gre && ip[44:4] = 0x0a00003c)



Attention : tous les filtres sont sensibles à la casse.

Dépannage

« Erreur de filtre » est l'une des erreurs les plus courantes lors de la capture de paquets.

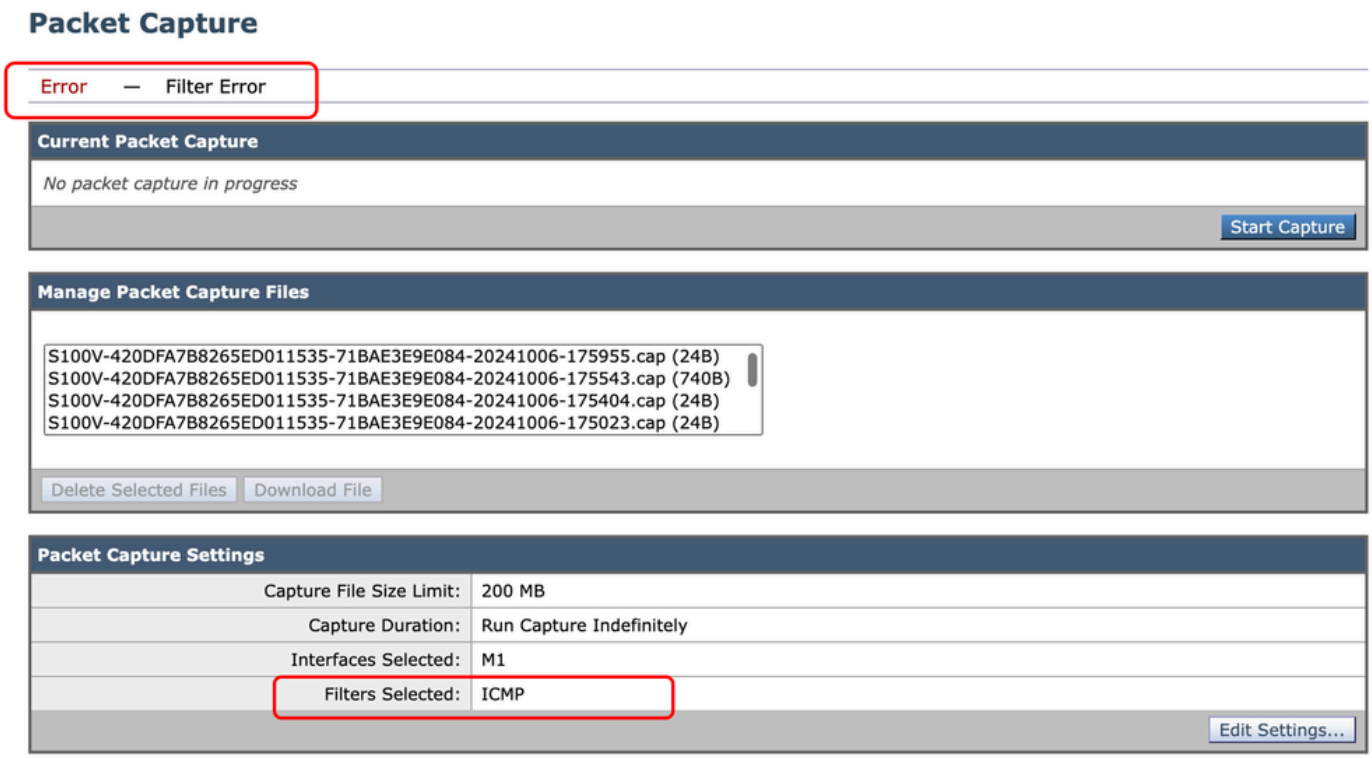


Image - Erreur de filtre

Cette erreur est généralement liée à une implémentation de filtre incorrecte. Dans l'exemple précédent, le filtre ICMP est en majuscules. C'est la raison pour laquelle vous recevez une erreur de filtre. Pour résoudre ce problème, vous devez modifier le filtre et remplacer l'ICMP par icmp.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - GD(General Deployment) - Classify End-U...

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.