Foire aux questions d'appareils de sécurité du contenu : Comment effectuez-vous une capture de paquet sur une appliance de sécurité du contenu de Cisco ?

Contenu

Introduction

Ce document décrit comment effectuer des captures de paquet sur les appliances de sécurité du contenu de Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité du courrier électronique de Cisco (ESA)
- Appliance de sécurité Web de Cisco (WSA)
- Appliance de Gestion de sécurité Cisco (SMA)
- AsyncOS

Composants utilisés

Les informations dans ce document sont de base sur toutes les versions d'AsyncOS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Comment effectuez-vous une capture de paquet sur une appliance de sécurité du contenu de Cisco ?

Terminez-vous ces étapes afin d'effectuer une capture de paquet (commande de **tcpdump**) avec le GUI :

1. Naviguez **pour aider et capture de support > de paquet** sur le GUI.
2. Éditez les configurations de capture de paquet au besoin, comme l'interface réseau sur laquelle la capture de paquet s'exécute. Vous pouvez utiliser un des filtres de prédéfinis, ou vous pouvez créer un filtre personnalisé avec l'utilisation de n'importe quelle syntaxe qui est prise en charge par la commande de **tcpdump d'**Unix.
3. **Capture de début de** clic afin de commencer la capture.
4. **Capture d'arrêt de** clic afin de finir la capture.
5. Téléchargez la capture de paquet.

Terminez-vous ces étapes afin d'effectuer une capture de paquet (commande de **tcpdump**) avec le CLI :

1. Sélectionnez cette commande dans le CLI :

```
wsa.run> 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)
```

2. Choisissez l'exécution que vous voulez exécuter :

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. Écrivez la taille maximale permise pour le fichier de capture (dans le Mo) :

```
[200]> 200

Do you want to stop the capture when the file size is reached? (If not, a new
 file will be started and the older capture data will be discarded.)

[N]> n

The following interfaces are configured:

1. Management

2. T1

3. T2
```

4. Écrivez le nom ou le nombre d'un ou plusieurs interfaces desquelles pour capturer des paquets, séparés par des virgules :

```
[1]> 1
```

5. Entrez dans le filtre que vous voulez utiliser pour la capture. Introduisez le mot **ESPACE LIBRE** afin d'effacer le filtre et capturer tous les paquets sur les interfaces sélectionnées.

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80


Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```

6. Choisissez l'exécution de **début** afin de commencer la capture :

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> start


Status: Capture in progress (Duration: 0s)

File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)
```

```
 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```

7. Choisissez l'exécution d'**arrêt** afin de finir la capture :

```
- STOP - Stop packet capture.

- STATUS - Display current capture status.

- SETUP - Change packet capture settings.

[]> stop


Status: No capture running (Capture stopped by user)


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```