# Utiliser les procédures de capture de paquets sur un périphérique Firepower

## Table des matières



## Introduction

Ce document décrit comment utiliser la commande **tcpdump** afin de capturer des paquets qui sont vus par une interface réseau de votre périphérique Firepower.

## Conditions préalables

### Exigences

Cisco vous recommande de connaître les modèles de périphériques Cisco Firepower et de périphériques virtuels.

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. Il utilise la syntaxe BPF (Berkeley Packet Filter).

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 lâ€™incidence possible des commandes.

---

> **Avertissement** : si vous exécutez la commande **tcpdump** sur un système de production, cela peut avoir un impact sur les performances du réseau.

---

## Étapes de capture des paquets

Connectez-vous à l'interface CLI de votre périphérique Firepower.

Dans les versions 6.1 et ultérieures, entrez **capture-traffic**. Exemple :

<#root>

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

Dans les versions 6.0.x.x et antérieures, entrez **system support capture-traffic**. Exemple :

<#root>

```
> system support capture-traffic
```

```
Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

Après avoir effectué une sélection, vous êtes invité à saisir les options suivantes :

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

Afin de capturer suffisamment de données à partir des paquets, il est nécessaire d'utiliser l'option -s afin de définir correctement la longueur d'accrochage. La longueur d'accrochage peut être définie sur une valeur qui correspond à la valeur MTU (unité de transmission maximale) configurée de la configuration de l'ensemble d'interfaces, qui est par défaut de 1518.

---

> **Avertissement** : lorsque vous capturez du trafic à l'écran, il peut dégrader les performances du système et du réseau. Cisco recommande d'utiliser l'option -w <filename> avec la commande tcpdump. Il capture les paquets dans un fichier. Si vous exécutez la commande sans l'option -w , appuyez sur la combinaison de touches **Ctrl-C** afin de quitter.

---

Exemple de l'option -w <filename> :

<#root>

```
-w capture.pcap -s 1518
```

---

> **Attention** : n'utilisez aucun élément de chemin lorsque vous spécifiez le nom de fichier de capture de paquets (pcap). Vous ne devez spécifier que le nom du fichier pcap à créer dans l'appliance.

---

S'il est souhaitable de capturer un nombre limité de paquets, vous pouvez utiliser l'indicateur -c <packets> afin de spécifier le nombre de paquets à capturer. Par exemple, afin de capturer exactement 5000 paquets :

<#root>

```
-w capture.pcap -s 1518 -c 5000
```

En outre, un filtre BPF peut être ajouté à la fin de la commande afin de limiter quels paquets sont capturés. Par exemple, afin de limiter la capture de paquets à 5 000 paquets avec une adresse IP source ou de destination de 192.0.2.1, vous pouvez utiliser ces options :

<#root>

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

Lorsque vous capturez du trafic étiqueté VLAN (Virtual LAN), vous devez spécifier le VLAN avec la syntaxe BPF. Sinon, le pcap ne contient aucun des paquets étiquetés VLAN. Par exemple, cet exemple limite la capture au trafic étiqueté VLAN depuis 192.0.2.1 :

<#root>

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

Si vous ne savez pas si le trafic est étiqueté VLAN, cette syntaxe peut être utilisée afin de capturer le trafic de 192.0.2.1 qui est et n'est pas étiqueté VLAN :

<#root>

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

---

> **Remarque** : dans l'exemple précédent, les parenthèses sont nécessaires pour que 'or' ne s'applique pas uniquement à 'vlan'. Les guillemets simples sont alors nécessaires afin d'éviter toute mauvaise interprétation possible des parenthèses par le shell.

---

La spécification d'une étiquette VLAN capture tout le trafic VLAN qui correspond au reste de votre BPF. Toutefois, si vous souhaitez capturer une balise VLAN spécifique, vous pouvez spécifier la balise VLAN que vous souhaitez capturer de la manière suivante :

<#root>

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

Après avoir spécifié les options souhaitées et appuyé sur **Entrée**, tcpdump commence à capturer le trafic.

---

> **Conseil** : si l'option -c n'a pas été utilisée, appuyez sur la combinaison de touches **Ctrl-C** afin d'arrêter la capture.

---

Une fois la capture arrêtée, vous recevez une confirmation. Exemple :

<#root>

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

**-w capture.pcap -s 1518 -c 5000 host 192.0.2.1**

```
Cleaning up.
Done.
```

# Copier un fichier Pcap

Afin de copier un fichier pcap d'une appliance FirePOWER vers un autre système qui accepte les connexions SSH entrantes, utilisez cette commande :

<#root>

**> system file secure-copy hostname username destination_directory pcap_file**

Après avoir appuyé sur **Entrée**, vous êtes invité à saisir le mot de passe pour le système distant. Le fichier peut être copié sur le réseau.

---

**Remarque** : dans cet exemple, le nom d'hôte fait référence au nom ou à l'adresse IP de l'hôte distant cible, le nom d'utilisateur indique le nom de l'utilisateur sur l'hôte distant, le répertoire de destination indique le chemin de destination sur l'hôte distant et le fichier pcap indique le fichier pcap local à transférer.

---

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.