Procédures de capture de paquet sur le périphérique de Cisco FirePOWER

Contenu

Introduction

Ce document décrit comment employer la commande de **tcpdump** afin de capturer les paquets qui sont vus par une interface réseau de votre périphérique de FirePOWER. Il utilise la syntaxe du filtre de paquet de Berkeley (BPF).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du périphérique de Cisco FirePOWER et des modèles de périphérique virtuel.

Composants utilisés

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

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.

> **Avertissement** : Si vous exécutez la commande de **`tcpdump`** sur un système de production, il peut affecter des performances du réseau.

Étapes pour capturer des paquets

Ouvrez une session au CLI de votre périphérique de FirePOWER.

Dans les versions 6.1 et ultérieures, écrivez le capture-**trafic**. Exemple :

```
> 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, écrivez le capture-**trafic de support de système**. Exemple :

```
> system support capture-traffic

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

Après que vous fassiez une sélection, vous serez incité pour des options :

```
> system support capture-traffic

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

Afin de capturer des données suffisantes des paquets, il est nécessaire d'employer `- l'` option `s` afin de placer le snaplength correctement. Le snaplength devrait être placé à une valeur qui apparie la valeur configurée de Maximum Transmission Unit (MTU) de la configuration réglée d'interface, qui se transfère sur 1518.

> **Avertissement** : Puisque capturer le trafic à l'écran peut dégrader la représentation du système et du réseau, Cisco recommande que vous utilisiez `- l'` option de `<filename> W` avec la commande de `tcpdump`. Il capture les paquets à un fichier. Si vous exécutez la commande sans `- l'` option `W`, appuient sur la combinaison de touches **CTRL-C** afin de quitter.

Exemple `- de l'` option de `<filename> W` :

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

> **Attention** : N'utilisez aucun élément de chemin quand vous spécifiez le nom du fichier de capture de paquet (pcap). Vous devez spécifier seulement le nom du fichier de pcap à créer dans l'appliance.

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

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

Supplémentaire, 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 paquet à 5000 paquets avec une source ou une adresse IP de destination de 192.0.2.1, vous pourriez utiliser ces options :

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

Quand vous capturez le trafic qui est le RÉSEAU LOCAL virtuel (VLAN) étiqueté, vous devez spécifier le VLAN avec la syntaxe BPF. Autrement, le pcap ne contient pas les paquets balisés l'uns des VLAN. Par exemple, cet exemple limite la capture au trafic qui est VLAN étiqueté de 192.0.2.1 :

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

Si vous êtes incertain si le trafic est VLAN étiqueté, cette syntaxe pourrait être utilisée afin de capturer le trafic de 192.0.2.1 qui est et n'est pas VLAN étiqueté :

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

> **Note**: Dans l'exemple précédent, les parenthèses sont nécessaires de sorte que « `ou` » s'applique non seulement au « `VLAN` ». Les apostrophes sont nécessaires alors afin d'empêcher n'importe quelle erreur d'interprétation possible des parenthèses par le shell.

La spécification d'une balise VLAN capture tout le trafic VLAN qui apparie le reste de votre BPF. Cependant, si vous voulez capturer une balise de la particularité VLAN, vous pouvez spécifier que la balise VLAN vous voudrait capturer comme ainsi :

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

Après que vous spécifiiez les options désirées et les appuyiez sur **entriez**, le tcpdump commence à capturer le trafic.

> **Conseil** : Si `- l'` option `c` n'a pas été utilisée, appuie sur la combinaison de touches **CTRL-C** afin d'arrêter la capture.

Une fois que vous arrêtez la capture, vous recevrez la confirmation. Exemple :

```
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.
```

Copiez un fichier de Pcap

Afin de copier un pcap classez d'une appliance de FirePOWER à un autre système qui reçoit les connexions SSH d'arrivée, utilisent cette commande :

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

Après que vous appuyiez sur **entrez**, vous sera incité pour le mot de passe au système distant. Le fichier sera copié à travers le réseau.

> **Note**: Dans cet exemple, l'**adresse Internet** se rapporte au nom ou à l'adresse IP du serveur distant de cible, le **nom d'utilisateur** spécifie le nom d'utilisateur sur le serveur distant, le **destination_directory** spécifie le chemin de destination sur le serveur distant, et le **pcap_file** spécifie le fichier local de pcap pour le transfert.