Procédures de capture de paquet sur des appliances de puissance de feu de Sourcefire, et appliances virtuelles NGIPS

Contenu

Introduction

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

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance sur le périphérique de puissance de feu de Sourcefire et les modèles de périphérique virtuel.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliances de gamme 7000 de puissance de feu de Sourcefire, appliances de gamme 8000, et appliances virtuelles NGIPS
- Version de logiciel 5.0 de Sourcefire ou plus tard

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.

Configurations matérielles requises

Cette instruction s'applique sur des appliances de gamme 7000 de puissance de feu de Sourcefire, des appliances de gamme 8000, et des appliances virtuelles NGIPS.

Logiciels nécessaires

Cette instruction s'applique sur les versions de logiciel 5.0 ou plus grand.

Étapes pour capturer des paquets

Dans le CLI, écrivez le capture-**trafic d'assistance technique**. Exemple :

```
> system support capture-traffic

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

Après avoir fait une sélection, vous serez incité pour des options :

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

Afin de capturer des données suffisantes des paquets, il est nécessaire d'utiliser - l'option s 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 vous recommande pour utiliser - 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 **CTRL +** combinaison de touches **c** à quitter.

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

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

> **Attention** : N'utilisez aucun élément de chemin en spécifiant le nom du fichier de 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 pour spécifier le nombre de paquets pour capturer. Par exemple, pour capturer exactement 5000 paquets :

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

Supplémentaire, un filtre BPF peut être ajouté à la fin de la commande de limiter quels paquets sont capturés. Par exemple, pour limiter la capture de paquet à 5000 paquets avec une source ou une adresse IP de destination de 192.0.2.1, vous pourriez employer les options suivantes :

```
-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 utilisant la syntaxe BPF. Autrement, le pcap ne contient pas les paquets balisés l'uns des VLAN. Par exemple, ce qui suit limiterait 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, la syntaxe suivante pourrait être utilisée pour 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)'
```

> Remarque: Dans l'exemple précédent, la parenthèse sont nécessaire de sorte que « ou » s'applique non seulement au « VLAN ». Les apostrophes sont nécessaires alors pour empêcher n'importe quelle erreur d'interprétation possible de la parenthèse par le shell.

Spécifiant une balise VLAN capture tout le trafic VLAN appariant 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 avoir spécifié les options désirées et les avoir appuyé sur entrez, tcpdump commence capturant le trafic.

> **Conseil** : Si - l'option c n'a pas été utilisée, appuie sur **CTRL +** combinaison de touches **c** pour 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 puissance de feu à un autre système qui reçoit les connexions SSH d'arrivée, utilisent la commande suivante :

```
> 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.

Remarque: 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.