Configurer et capturer les paquets intégrés sur le logiciel

Table des matières

Introduction

Ce document décrit la fonctionnalité de capture de paquets intégrée (EPC) dans le logiciel Cisco IOS®.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- Cisco IOS version 12.4(20)T ou ultérieure
- Cisco IOS XE version 15.2(4)S - 3.7.0 ou ultérieure

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.

Informations générales

Lorsque cette option est activée, le routeur capture les paquets envoyés et reçus. Les paquets sont stockés dans une mémoire tampon dans la mémoire DRAM et ne sont pas conservés lors d'un rechargement. Une fois les données capturées, elles peuvent être examinées sous forme de résumé ou de vue détaillée sur le routeur.

En outre, les données peuvent être exportées sous la forme d'un fichier de capture de paquets (PCAP) pour permettre un examen plus approfondi. L'outil est configuré en mode d'exécution et est considéré comme un outil d'assistance temporaire. Par conséquent, la configuration de l'outil n'est pas stockée dans la configuration du routeur et ne reste pas en place après le rechargement du système.

L'outil Packet Capture Config Generator and Analyzer est disponible pour les clients Cisco afin de les aider à configurer, capturer et extraire les captures de paquets.

Exemple de configuration de Cisco IOS

Configuration EPC de base

1. Définissez un « tampon de capture », qui est un tampon temporaire dans lequel les paquets capturés sont stockés.
2. Différentes options peuvent être sélectionnées lorsque la mémoire tampon est définie, telles que la taille, la taille maximale de paquet et circulaire/linéaire :

```
monitor capture buffer BUF size 2048 max-size 1518 linear
```

3. Un filtre est applicable pour limiter la capture au trafic souhaité. Définissez une liste de contrôle d'accès (ACL) en mode de configuration et appliquez le filtre à la mémoire tampon :

```
ip access-list extended BUF-FILTER
    permit ip host 192.168.1.1 host 172.16.1.1
    permit ip host 172.16.1.1 host 192.168.1.1
```

```
monitor capture buffer BUF filter access-list BUF-FILTER
```

4. Définissez un point de capture qui définit l'emplacement où la capture a lieu.
5. Le point de capture définit également si la capture a lieu pour IPv4 ou IPv6 et dans quel

chemin de commutation (processus ou cef) :

```
monitor capture point ip cef POINT fastEthernet 0 both
```

6. Fixez la mémoire tampon au point de capture :

```
monitor capture point associate POINT BUF
```

7. Démarrez la capture :

```
monitor capture point start POINT
```

8. La capture est maintenant active. Permettre la collecte des données nécessaires.
9. Arrêtez la capture :

```
monitor capture point stop POINT
```

10. Examinez la mémoire tampon de l'unité :

```
show monitor capture buffer BUF dump
```

Remarque : cette sortie affiche uniquement le vidage hexadécimal des captures de paquets. Afin de les voir dans lisible par l'homme il y a deux façons.

Exportez la mémoire tampon du routeur pour une analyse plus approfondie :

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```

La méthode précédente n'est pas toujours pratique car elle nécessitait un accès T/FTP au routeur. Dans de telles situations, prenez une copie de l'hex dump et utilisez n'importe quel convertisseur hex-pcap en ligne afin de visualiser les fichiers.

11. Une fois que les données nécessaires ont été collectées, supprimez le « point de capture » et le « tampon de capture » :

```
no monitor capture point ip cef POINT fastEthernet 0 both
no monitor capture buffer BUF
```

Informations de configuration Cisco IOS supplémentaires

- Dans les versions antérieures à la version 15.0(1)M de Cisco IOS, la taille de la mémoire tampon était limitée à 512 Ko.
- Dans les versions antérieures à Cisco IOS version 15.0(1)M, la taille du paquet capturé était limitée à 1 024 octets.
- Le tampon de paquets est stocké dans la mémoire DRAM et ne persiste pas lors des rechargements.
- La configuration de capture n’est pas stockée dans la mémoire vive non volatile et ne persiste pas lors des rechargements.
- Le point de capture peut être défini pour capturer dans les chemins de commutation cef ou process.
- Le point de capture peut être défini pour capturer uniquement sur une interface ou globalement.
- Lorsque le tampon de capture est exporté au format PCAP, les informations L2 (telles que l'encapsulation Ethernet) ne sont pas conservées.
- Consultez Méthodes conseillées pour les commandes de recherche pour plus d'informations sur les commandes utilisées dans cette section.

Configuration de base de l'exportation du trafic IP

L'exportation de trafic IP est une méthode différente pour exporter des paquets IP reçus sur plusieurs interfaces WAN ou LAN simultanées.

1. En mode de configuration, définissez un profil d'exportation de trafic IP.

```
Device(config)# ip traffic-export profile mypcap mode capture
```

2. Configurez le trafic bidirectionnel dans le profil.

```
Device(config-rite)# bidirectional
```

3. Quitter

4. Spécifiez l'interface pour le trafic exporté.

```
Device(config-if)# interface GigabitEthernet 0/1
```

5. Activez l'exportation du trafic IP sur l'interface.

```
Device(config-if)# ip traffic-export apply mypcap size 10000000
```

6. Quitter

7. Démarrez la capture. La capture est maintenant active. Permettre la collecte des données nécessaires.

```
Device# traffic-export interface GigabitEthernet 0/1 start
```

8. Arrêtez la capture.

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```

9. Exportez la capture vers un serveur TFTP externe.

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```

10. Une fois les données nécessaires collectées, supprimez le profil.

```
Device(config)# no ip traffic-export profile mypcap
```

Inconvénients d'exportation du trafic IP

L'exportation de trafic IP présente les inconvénients suivants par rapport à la méthode EPC :

- L’interface vers laquelle le trafic capturé est exporté doit être une interface Ethernet.
- Pas de prise en charge IPv6.
- Aucune information de couche 2, uniquement les informations de couche 3 et supérieure.

Exemple de configuration de Cisco IOS-XE

La fonctionnalité Embedded Packet Capture a été introduite dans Cisco IOS XE version 3.7 - 15.2(4)S. La configuration de la capture est différente de celle de Cisco IOS, car elle ajoute davantage de fonctionnalités.

Configuration EPC de base

1. Définissez l'emplacement de la capture :

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. Associez un filtre. Le filtre est soit spécifié en ligne, soit une liste de contrôle d'accès ou un mappage de classe peut être référencé :

```
monitor capture CAP match ipv4 protocol tcp any any limit pps 1000000
```

3. Démarrez la capture :

```
monitor capture CAP start
```

4. La capture est maintenant active. Laisser le client collecter les données nécessaires.

5. Arrêtez la capture :

```
monitor capture CAP stop
```

6. Examinez la capture dans une vue récapitulative :

```
show monitor capture CAP buffer brief
```

7. Examinez la capture dans une vue détaillée :

```
show monitor capture CAP buffer detailed
```

8. En outre, exportez la capture au format PCAP pour une analyse plus approfondie :

```
monitor capture CAP export tftp://10.0.0.1/CAP.pcap
```

9. Une fois les données nécessaires collectées, supprimez la capture :

```
no monitor capture CAP
```

Additional Information

- La capture est effectuée sur les interfaces physiques, les sous-interfaces et les interfaces de tunnel.
- Filtres basés sur la reconnaissance d'applications réseau (NBAR) (qui utilisent le **match protocol** sous la class-map) ne sont actuellement pas prises en charge.
- Pour plus d'informations sur les commandes utilisées dans cette section, consultez Meilleures pratiques pour les commandes de recherche.

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Pour EPC qui s'exécute sur Cisco IOS-XE®, cette commande de débogage est utilisée pour s'assurer que EPC est correctement configuré :

```
debug epc provision
debug epc capture-point
```

Informations connexes

- Capture de paquets intégrée - Cisco IOS-XE
- Capture de paquets intégrée - Cisco IOS
- Assistance technique et téléchargements Cisco

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.