Capture incluse de paquet pour l'exemple de Cisco IOS et de configuration IOS-XE

Contenu

Introduction

Ce document décrit la caractéristique incluse de la capture de paquet (CPE) en logiciel de Cisco IOS®.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour 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 ultérieures
- Release 15.2(4)S de Cisco IOS XE - 3.7.0 ou plus tard

Les informations dans ce document ont été créées des périphériques dans un environnement de travaux pratiques. 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.

Informations générales

Une fois activé, le routeur capture les paquets envoyés et reçus. Les paquets sont enregistrés dans une mémoire tampon dans la mémoire vive dynamique et ne sont ainsi pas persistants par une recharge. Une fois que les données sont capturées, elles peuvent être examinées dans une vue récapitulative ou détaillée sur le routeur. En outre, les données peuvent être exportées comme fichier de la capture de paquet (PCAP) pour tenir compte davantage de d'examen. L'outil est configuré dans le mode d'exécution et est considéré un outil d'aide temporaire. En conséquence, la configuration d'outil n'est pas enregistrée dans la configuration de routeur et ne restera pas en place après un rechargement du système.

L'outil de générateur et d'analyseur de config de capture de paquet est disponible pour que les clients de Cisco facilitent la configuration, la capture, et l'extraction des captures de paquet.

Exemple de configuration Cisco IOS

Configuration de base CPE

1. Définissez une « mémoire tampon de capture », qui est une mémoire tampon provisoire que les paquets capturés sont enregistrés en dedans. Il y a de diverses options qui peuvent être sélectionnées quand la mémoire tampon est définie ; comme la taille, la longueur de paquet de maxium, et circulaire/Linéaire :

   ```
   monitor capture buffer BUF size 2048 max-size 1518 linear
   ```
2. Un filtre peut également être appliqué pour limiter la capture au trafic désiré. Définissez une liste de contrôle d'accès (ACL) dans le mode de config 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 192.168.1.1monitor capture buffer BUF filter access-list
   BUF-FILTER
   ```
3. Définissez un « point de capture », qui définit l'emplacement où la capture se produit. Le point de capture définit également si la capture se produit pour l'ipv4 ou l'IPv6 et dans quel chemin de commutation (processus contre le cef) :

   ```
   monitor capture point ip cef POINT fastEthernet 0 both
   ```
4. Reliez la mémoire tampon au point de capture :

   ```
   monitor capture point associate POINT BUF
   ```
5. Commencez la capture :

   ```
   monitor capture point start POINT
   ```
6. La capture est maintenant en activité. Permettez la collecte des données nécessaires.

7. Arrêtez la capture :

   ```
   monitor capture point stop POINT
   ```
8. Examinez la mémoire tampon sur l'unité :

   `show monitor capture buffer BUF dump`Remarque: Cette sortie affiche seulement le vidage hexadécimal des captures de paquets. Afin de voir ils dans lisible pour l'homme là sont deux

manières.Exportez la mémoire tampon du routeur pour l'analyse approfondie :

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```
Conseil : La demande d'amélioration CSCuw77601 a été classée afin d'ajouter a messagerie-à l'option sous l'exportation ainsi vous pouvez envoyer la mémoire tampon diretly à un email-id.Cependant la méthode précédente n'est pas toujours pratique en tant qu'elle a exigé l'accès T/FTP au routeur. Dans de telles situations, vous pouvez prendre une copie du vidage hexadécimal et utiliser n'importe quel convertisseur en ligne d'hexa-pcap afin de visualiser les fichiers.

9. Une fois que les données nécessaires ont été collectées, supprimez le « point de capture » et « capturez la mémoire tampon » : `no monitor capture point ip cef POINT fastEthernet 0 both`
`no monitor capture buffer BUF`

Remarques :

- Dans les versions plus tôt que la Cisco IOS version 15.0(1)M, la taille de mémoire tampon a été limitée à 512K.
- Dans les versions plus tôt que la Cisco IOS version 15.0(1)M, la longueur de paquet saisie a été limitée à 1024 octets.
- Le tampon de paquets est enregistré dans la mémoire vive dynamique et ne persistera pas par des recharges.
- La configuration de capture n'est pas enregistrée dans NVRAM et ne persistera pas par des recharges.
- Le point de capture peut être défini pour le capturer dans les chemins de commutation de cef ou de processus.
- Le point de capture peut être défini pour le capturer seulement sur une interface ou globalement.
- Quand la mémoire tampon de capture est exportée dans le format PCAP, les informations L2 (telles que l'encapsulation Ethernet) ne sont pas préservées.
- SeeBest pratique pour rechercher des commandes afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Exemple de configuration de Cisco IOS XE

La caractéristique incluse de saisie de paquet a été introduite dans la version 3.7 de Cisco IOS XE - 15.2(4)S. La configuration de la capture est différente que le Cisco IOS car elle ajoute plus de caractéristiques.

Configuration de base CPE

1. Définissez l'emplacement où la capture se produira :

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```
2. Associez un filtre. Le filtre peut être en ligne spécifié, ou un ACL ou un class-map peut être mis en référence :

```
monitor capture CAP match ipv4 protocol tcp any any
```
3. Commencez la capture :

```
monitor capture CAP start
```

4. La capture est maintenant en activité. Permettez-lui pour 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 dans le format PCAP pour l'analyse approfondie :

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

9. Une fois que les données nécessaires ont été collectées, retirez la capture :

```
no monitor capture CAP
```

Remarques :

- La capture peut être effectuée sur des interfaces physiques, des sous-interfaces, et des interfaces de tunnel.
- Le Reconnaissance d'application fondée sur le réseau (NBAR) a basé des filtres, cette utilisation la commande de **match protocol** sous le class-map, ne sont pas actuellement pris en charge.
- Voir les pratiques recommandées pour rechercher des commandes afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Vérifiez

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

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour la CPE qui fonctionne sur le Cisco IOS XE, cette commande de débogage peut être utilisée pour s'assurer que la CPE est installée correctement :

```
no monitor capture CAP
```

Informations connexes

- Capture incluse de paquet - Cisco IOS XE
- Capture incluse de paquet - Cisco IOS
- Support et documentation techniques - Cisco Systems