Configurer la capture de paquets vManage/vSmart/vEdge TCPDUMP en mode CLI

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

TCPDUMP(Controllers) Points clés Explication

TCPDUMP (suite)

Utiliser la commande TCPDUMP

Exemples TCPDUMP

Documents associés

Introduction

Ce document décrit comment configurer vManage/vSmart/vEdge TCPDUMP Packet Capture en mode CLI.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) de Cisco

Composants utilisés

Les informations contenues dans ce document sont basées sur la version 20.9.4 de Cisco vManage

The information in this document was created from the devices in a specific lab environment. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est actif, assurez-vous que vous comprenez l'impact potentiel de toute commande.

Informations générales

Dans l'architecture Cisco SD-WAN, vManage, vSmart et vEdge jouent respectivement les rôles principaux de gestion, de contrôle et de transfert de données. Pour assurer la stabilité et la sécurité du réseau et pour résoudre les problèmes de réseau, les ingénieurs réseau doivent souvent capturer et analyser les paquets sur le trafic traversant ces périphériques. TCPDUMP est un outil en ligne de commande léger et puissant qui peut être utilisé pour capturer et analyser des paquets de données passant par des interfaces.

En configurant et en utilisant TCPDUMP en mode CLI, les utilisateurs peuvent capturer directement le trafic en temps réel sur le périphérique sans avoir besoin d'outils supplémentaires ou de périphériques proxy intermédiaires. Cela est très important pour localiser des problèmes tels que des anomalies de routage, des échecs de connexion de contrôle, des pertes de paquets et la vérification des chemins de trafic. Puisque les périphériques Cisco SD-WAN (tels que vEdge) exécutent des systèmes d'exploitation personnalisés (tels que Viptela OS), l'utilisation de TCPDUMP peut différer légèrement de celle des environnements Linux traditionnels sous certains aspects. Par conséquent, la compréhension de sa structure de commande de base et de ses limitations d'utilisation est particulièrement cruciale.

Cette section explique comment configurer et exécuter TCPDUMP en mode CLI des périphériques vManage, vSmart et vEdge, afin d'aider les utilisateurs à effectuer une analyse efficace du trafic réseau et un diagnostic des problèmes.

TCPDUMP(Controllers) Points clés Explication

```
tcpdump [vpn x | interface x | vpn x interface x] options " "
Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUv] [ -B size ] [ -c count ]
               [ -E algo:secret ] [ -j tstamptype ] [ -M secret ]
               [ -T type ] [ -y datalinktype ] [ expression ]
```

- Spécifier une interface (impossible d'obtenir la sortie en spécifiant uniquement le VPN)
- Placez les options entre guillemets (« ») , utilisez ctrl c pour arrêter
- Utilisez -n pour empêcher la conversion d’ip en nom d’hôte et -nn pour empêcher le nom et le port ?
- -v affiche plus de détails (informations d'en-tête IP, tos, ttl, offset, indicateurs, protocole)
- -vv et -vvv affichent plus de détails sur certains types de paquets
- Proto ex - udp, tcp icmp pim igmp vrrp esp arp
- Négate ! ou non, && ou et, | | ou ou, utiliser avec ( ) non (udp ou icmp)

TCPDUMP (suite)

- Adapté de la commande tcpdump de linux mais ne prend pas en charge toutes les options disponibles. Les instantanés de paquets enregistrés dans une mémoire tampon ne peuvent pas être exportés vers un PCAP.
- S'exécute avec l'indicateur -p, ce qui signifie « mode sans proximité » : le contrôleur capture

uniquement les paquets destinés à l'interface du contrôleur, y compris les paquets de contrôle ou les paquets de diffusion. Impossible de capturer le trafic du plan de données.
- Exécuté avec -s 128, longueur de l'instantané en octets. Les x premiers octets du paquet sont capturés.

Utiliser la commande TCPDUMP

Cette section fournit des exemples illustrant la manière dont la commande cpdumpest utilisée.

```
vmanage# tcpdump ?
Possible completions:
interface  Interface on which tcpdump listens
vpn        VPN ID
```

Le résultat de la commande show interface description fournit des informations précises sur le nom et le numéro de vpn/interface qui est actuellement utilisé.

```
vmanage# tcpdump vpn 0 interface eth0 ?
Possible completions:
help       tcpdump help
options    tcpdump options or expression
|          Output modifiers
<cr>
```

Vous pouvez ajouter d'autres conditions pour le filtrage de capture de paquets via le mot clé "options".

```
vmanage# tcpdump vpn 0 interface eth0 help

Tcpdump options:
help              Show usage
vpn               VPN or namespace
interface         Interface name
options           Tcpdump options like -v, -vvv, t,-A etc or expressions like port 25 and not host 10.0

e.g., tcpdump vpn 1 interface ge0/4 options "icmp or udp"

Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUv] [ -B size ] [ -c count ] [ -E algo:secret ] [ -j tstamptype ]
               [ -T type ] [ -y datalinktype ] [ expression ]
```

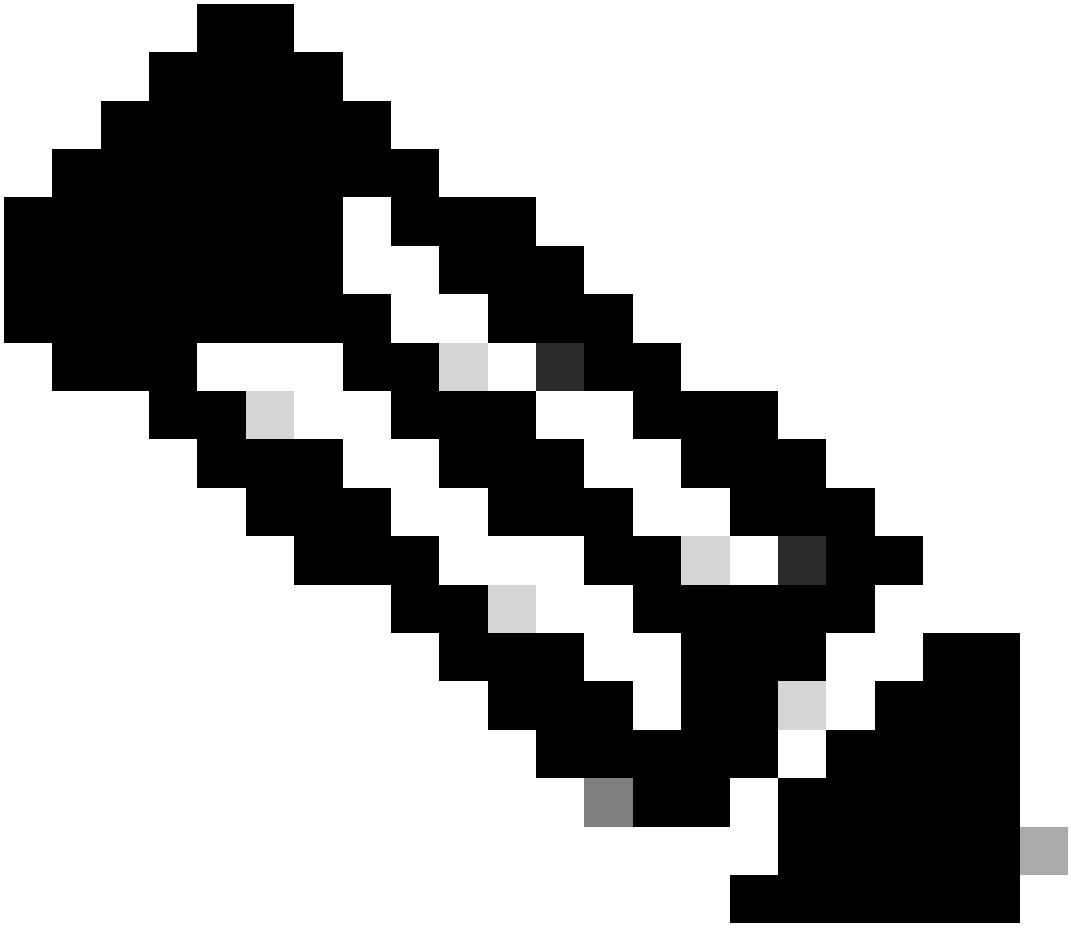
Vous pouvez indiquer le nombre spécifique de paquets par la commande options "-c count". Si vous n'indiquez pas de nombre de packages spécifique, une capture continue est exécutée sans limite.

```
vmanage# tcpdump vpn 0 interface eth0 options "-c 10 "
```

```
tcpdump -p -i eth0 -s 128 -c 10 in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes
04:56:55.797308 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 237
04:56:55.797371 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 205
04:56:55.797554 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.797580 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.808036 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 173
04:56:55.917567 ARP, Request who-has 50.128.76.31 (Broadcast) tell 50.128.76.1, length 46
04:56:55.979071 IP 50.128.76.22.12346 > 50.128.76.25.12346: UDP, length 182
04:56:55.979621 IP 50.128.76.25.12346 > 50.128.76.22.12346: UDP, length 146
04:56:56.014054 IP 50.128.76.22.12746 > softbank219168102002.bbtec.net.12366: UDP, length 237
04:56:56.135636 IP 50.128.76.32.12426 > 50.128.76.22.12546: UDP, length 140
10 packets captured
1296 packets received by filter
0 packets dropped by kernel
```

Vous pouvez également ajouter des conditions de filtre relatives à l'adresse hôte et au type de protocole dans les options.

```
vmanage# tcpdump vpn 0 interface eth0 options "-n host 50.128.76.27 and icmp"
tcpdump -p -i eth0 -s 128 -n host 50.128.76.27 and icmp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes
05:21:31.855189 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 34351, seq 29515, length 28
05:21:34.832871 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 44520, seq 29516, length 28
05:21:34.859655 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 44520, seq 29516, length 28
05:21:37.837244 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 39089, seq 29517, length 28
05:21:37.866201 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 39089, seq 29517, length 28
05:21:40.842214 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 24601, seq 29518, length 28
05:21:40.870203 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 24601, seq 29518, length 28
05:21:43.847548 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 42968, seq 29519, length 28
05:21:43.873016 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 42968, seq 29519, length 28
05:21:46.852305 IP 50.128.76.22 > 50.128.76.27: ICMP echo request, id 23619, seq 29520, length 28
05:21:46.880557 IP 50.128.76.27 > 50.128.76.22: ICMP echo reply, id 23619, seq 29520, length 28
^C                                                                                <<<< Ctrl + c can inter
11 packets captured
11 packets received by filter
0 packets dropped by kernel
```

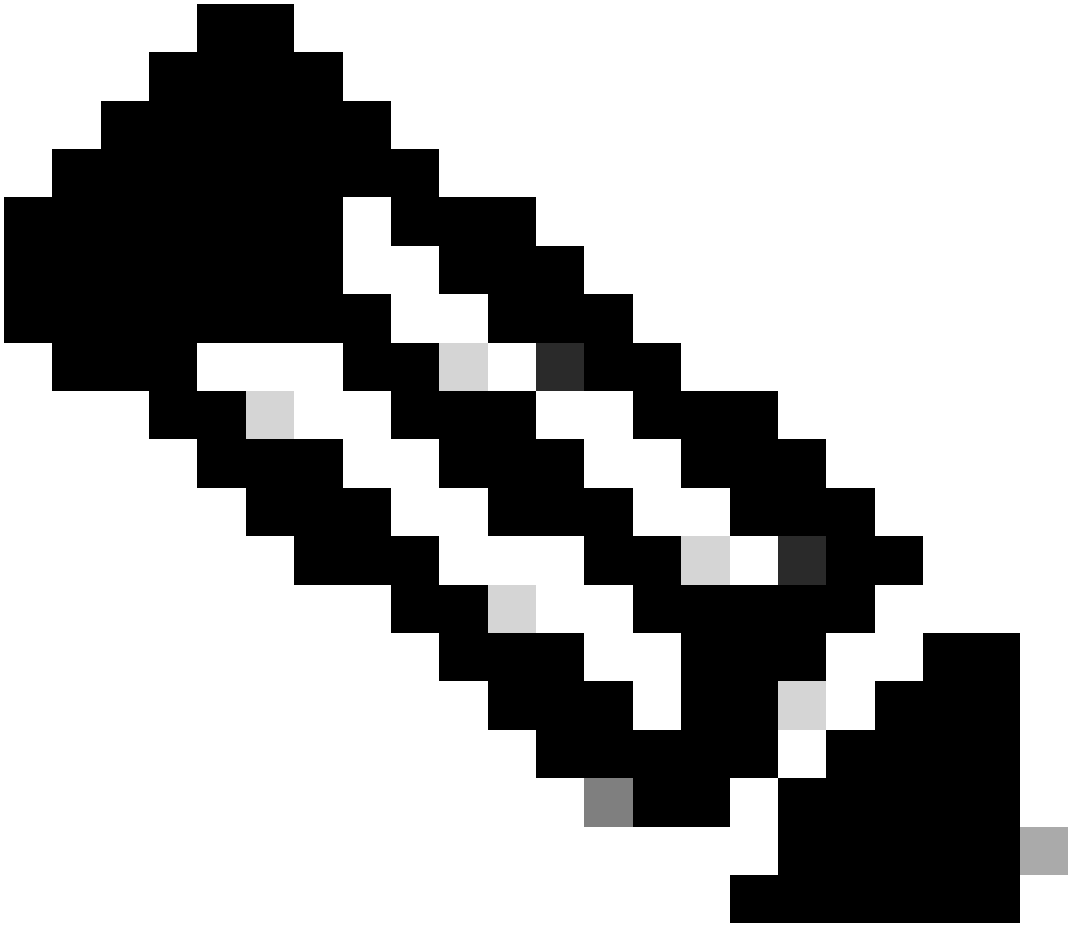


Remarque : Sur le logiciel Cisco IOS XE SD-WAN, vous pouvez utiliser Embedded Packet Capture (EPC) au lieu de TCPDUMP.

Exemples TCPDUMP

Écoute du paquet UDP général :

tcpdump vpn 0 options "-vvv -nnn udp"



Remarque : Cela peut également être appliqué à d'autres protocoles... par exemple : icmp, arp, etc.

Écoute d’un port spécifique avec ICMP et UDP :
tcpdump vpn 0 interface ge0/4 options "icmp ou udp"

Écoute sur un numéro de port spécifique (écoute sur le port TLS) :
tcpdump vpn 0 interface ge0/4 options «-vvv -nn port 23456 »

Écoute sur un numéro de port spécifique (écoute sur le port DTLS) :
tcpdump vpn 0 interface ge0/4 options «-vvv -nn port 12346 »

Écoute d’un hôte spécifique (vers/depuis cet hôte) : -e imprime l'en-tête de niveau liaison
tcpdump vpn 0 interface ge0/4 options « host 64.100.103.2 -vv -nn -e »

Écoute d’un hôte spécifique avec ICMP uniquement
tcpdump vpn 0 interface ge0/4 options « host 64.100.103.2 && icmp »

Filtrage par source et/ou destination
tcpdump vpn 0 interface ge0/4 options « src 64.100.103.2 && dst 64.100.100.75 »

Filtrer sur le trafic encapsulé GRE
tcpdump vpn 0 interface ge0/4 options « -v -n proto 47 »

Documents associés

- Dépannage des connexions de contrôle SD-WAN
- SD-WAN Cisco : Les suspects habituels
- PAGE DE MANUEL TCPDUMP

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.