Konfigurieren von vManage/vSmart/vEdge TCPDUMP Packet Capture im CLI-Modus

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie vManage/vSmart/vEdge TCPDUMP Packet Capture im CLI-Modus konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Software-defined Wide Area Network (SD-WAN)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco vManage, Version 20.9.4.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit der gelöschten (Standard-)Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

In der Cisco SD-WAN-Architektur übernehmen vManage, vSmart und vEdge die zentralen Funktionen für Management, Kontrolle und Datenweiterleitung. Um die Stabilität und Sicherheit

des Netzwerks zu gewährleisten und Netzwerkfehler zu beheben, müssen Netzwerktechniker häufig eine Paketerfassung und -analyse für den Datenverkehr durchführen, der durch diese Geräte fließt. TCPDUMP ist ein leichtes und leistungsstarkes Befehlszeilentool, mit dem über Schnittstellen übertragene Datenpakete erfasst und analysiert werden können.

Durch die Konfiguration und Verwendung von TCPDUMP im CLI-Modus können Benutzer den Echtzeitverkehr auf dem Gerät direkt erfassen, ohne zusätzliche Tools oder zwischengeschaltete Proxygeräte zu benötigen. Dies ist von großer Bedeutung für die Lokalisierung von Problemen, wie z. B. Routing-Anomalien, Verbindungsausfälle bei der Steuerung, Paketverluste und die Überprüfung von Datenverkehrspfaden. Da auf Cisco SD-WAN-Geräten (wie vEdge) benutzerdefinierte Betriebssysteme (wie Viptela OS) ausgeführt werden, kann sich die Verwendung von TCPDUMP in einigen Aspekten leicht von der in herkömmlichen Linux-Umgebungen unterscheiden. Daher ist es besonders wichtig, die grundlegende Befehlsstruktur und die Nutzungsbeschränkungen zu verstehen.

In diesem Abschnitt wird erläutert, wie TCPDUMP im CLI-Modus von vManage-, vSmart- und vEdge-Geräten konfiguriert und ausgeführt wird, um Benutzern bei der Durchführung einer effektiven Analyse des Netzwerkverkehrs und der Problemdiagnose zu helfen.

TCPDUMP (Controller) Erläuterung der Schlüsselpunkte

```
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 ]
```

- Geben Sie eine Schnittstelle an (die Ausgabe kann nicht nur mit VPN abgerufen werden).
- Setzen Sie Optionen in Anführungszeichen (""), verwenden Sie Strg c zu stoppen
- Verwenden Sie -n, um die Konvertierung von IP in Hostname zu verhindern, und -nn, um Name und Port zu verhindern.
- -v zeigt mehr Details an (IP-Header-Informationen, tos, ttl, offset, flags, protocol)
- -vv und -vvv zeigen mehr Details in bestimmten Pakettypen
- Proto ex - udp, tcp icmp pim igmp vrrp esp arp
- Negieren! oder nicht, && oder und, | | oder oder mit ( ) nicht (udp oder icmp) verwenden.

TCPDUMP (Fortsetzung)

- Übernommen aus Linux tcpdump-Befehl, aber nicht alle verfügbaren Optionen unterstützt. Snapshots von Paketen, die in einem Puffer gespeichert sind, können nicht in ein PCAP exportiert werden.
- Ausführung mit -p-Flag, d. h. "no-promiscuous mode" (Kein Promiscuous-Modus): Der Controller erfasst nur Pakete, die für die Controller-Schnittstelle bestimmt sind, einschließlich Steuerungspakete oder Broadcast-Pakete. Datenverkehr auf Datenebene kann nicht erfasst

werden.
- Mit -s 128 ausgeführt, Snapshot-Länge in Byte. Die ersten x Byte des Pakets werden erfasst.

Verwenden des Befehls TCPDUMP

In diesem Abschnitt finden Sie Beispiele, die die Verwendung des Befehls "cpdump" veranschaulichen.

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

Die Ausgabe des Befehls show interface description liefert präzise Informationen zum aktuell verwendeten VPN/Schnittstellennamen und der Schnittstellennummer.

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

Sie können weitere Bedingungen für die Paketerfassungsfilterung mit dem Schlüsselwort "options" hinzufügen.

```
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 ]
```

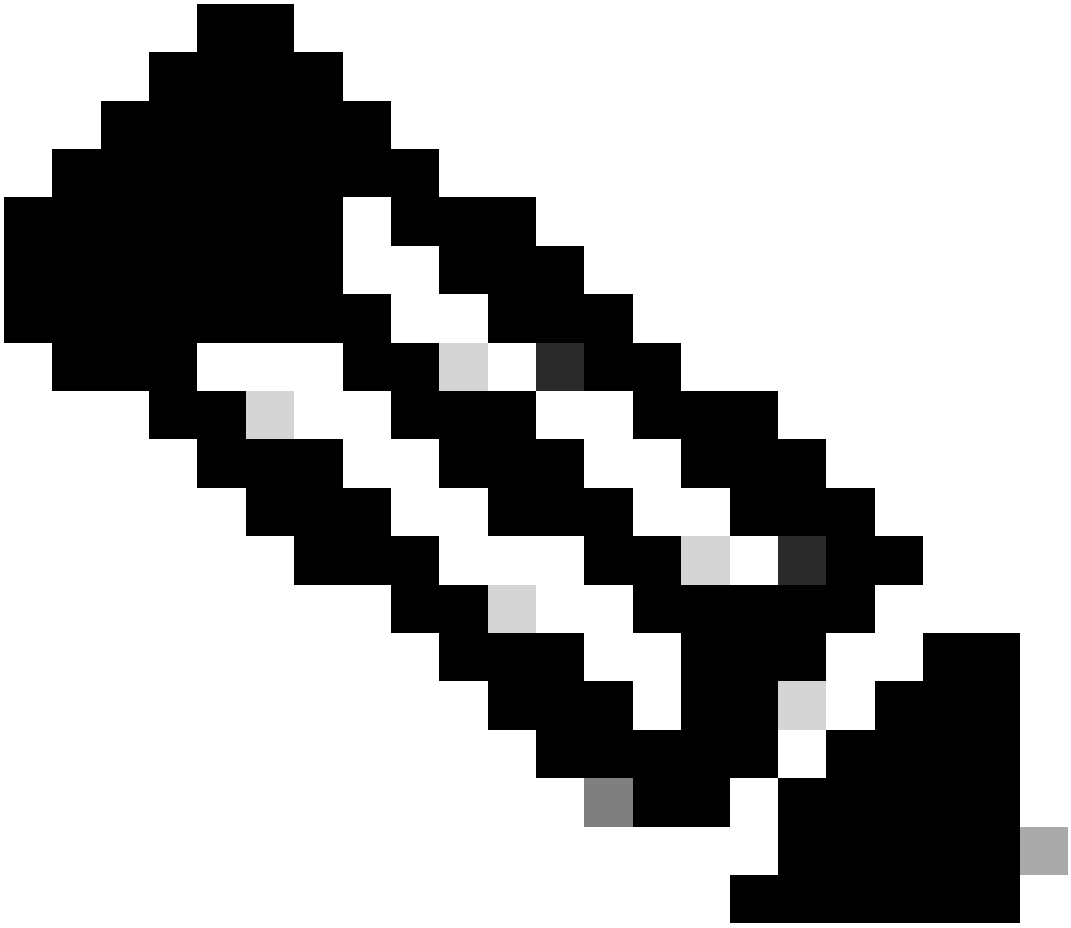
Sie können die Anzahl der Pakete durch den Befehl "-c count" angeben. Wenn Sie keine bestimmte Paketanzahl angeben, wird eine kontinuierliche Erfassung ohne Limit ausgeführt.

```
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
```

Sie können in den Optionen auch Filterbedingungen für die Hostadresse und den Protokolltyp hinzufügen.

```
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
```

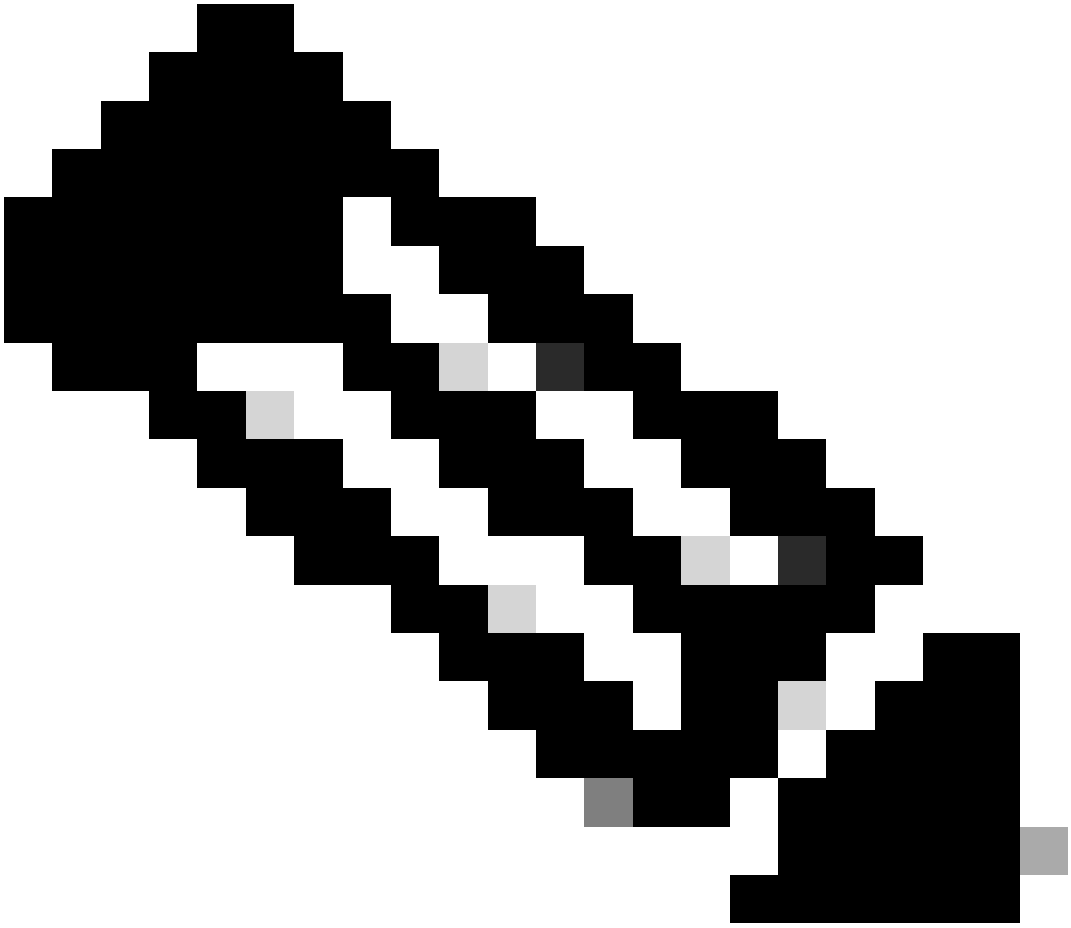


Anmerkung: Auf der Cisco IOS XE SD-WAN-Software können Sie statt TCPDUMP Embedded Packet Capture (EPC) verwenden.

Beispiele für TCPDUMP

Überwachendes allgemeines UDP-Paket:

tcpdump vpn 0, Optionen "-vv -nn udp"



Anmerkung: Dies kann auch auf andere Protokolle angewendet werden. Beispiel: icmp, arp usw.

Zuhören eines bestimmten Ports mit ICMP und UDP:
tcpdump vpn 0 interface ge0/4 options "icmp oder udp"

Zuhören zu einer bestimmten Portnummer(Zuhören zu einem TLS-Port):
tcpdump vpn 0 interface ge0/4 options "-vvv -nn port 23456"

Zuhören zu einer bestimmten Portnummer(Zuhören zu einem DTLS-Port):
tcpdump vpn 0 interface ge0/4 options "-vvv -nn port 12346"

Zuhören für einen bestimmten Host (zu/von diesem Host): -e druckt Header auf Verbindungsebene
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 -vvv -nn -e"

Zuhören nur für einen bestimmten Host mit ICMP
tcpdump vpn 0 interface ge0/4, Optionen "host 64.100.103.2 && icmp"

Filterung nach Quelle und/oder Ziel
tcpdump vpn 0 interface ge0/4 options "src 64.100.103.2 && dst 64.100.100.75"

Filtern nach GRE-gekapseltem Datenverkehr
tcpdump vpn 0 interface ge0/4 options "-v -n proto 47 "

Verwandte Dokumente

- Fehlerbehebung bei SD-WAN-Steuerverbindungen
- Cisco SD-WAN: Die üblichen Verdächtigen
- TCPDUMP MAN-SEITE

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.