Vastleggen van vManage/vSmart/vEdge TCPDUMP-pakketten configureren in CLI-modus

Inhoud

Inleiding

In dit document wordt beschreven hoe u vManage/vSmart/vEdge TCPDUMP Packet Capture in CLI-modus kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco vManage versie 20.9.4

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een uitgeklaarde (standaard) configuratie. Als uw netwerk live is, moet u ervoor zorgen dat u de potentiële impact van een opdracht begrijpt.

Achtergrondinformatie

In de Cisco SD-WAN-architectuur spelen vManage, vSmart en vEdge respectievelijk de kernrollen van beheer, controle en gegevensdoorgifte. Om de stabiliteit en veiligheid van het netwerk te

garanderen en netwerkfouten op te lossen, moeten netwerkingenieurs vaak pakketregistratie en analyse uitvoeren op het verkeer dat door deze apparaten stroomt. TCPDUMP is een lichtgewicht en krachtige opdrachtregeltool die kan worden gebruikt om gegevenspakketten die door interfaces gaan, vast te leggen en te analyseren.

Door TCPDUMP in de CLI-modus te configureren en te gebruiken, kunnen gebruikers direct realtime verkeer op het apparaat vastleggen zonder dat extra hulpmiddelen of tussenliggende proxyapparaten nodig zijn. Dit is van groot belang voor het lokaliseren van problemen zoals routeringsanomalieën, verbindingsfouten in de besturing, pakketverlies en verificatie van verkeerspaden. Aangezien Cisco SD-WAN-apparaten (zoals vEdge) aangepaste besturingssystemen (zoals Viptela OS) uitvoeren, kan het gebruik van TCPDUMP in sommige opzichten enigszins afwijken van dat in traditionele Linux-omgevingen. Daarom is het begrijpen van de basiscommandostructuur en gebruiksbeperkingen bijzonder cruciaal.

In dit gedeelte wordt uitgelegd hoe u TCPDUMP configureert en uitvoert in de CLI-modus van vManage-, vSmart- en vEdge-apparaten, om gebruikers te helpen bij het uitvoeren van een effectieve analyse van het netwerkverkeer en probleemdiagnose.

TCPDUMP(controllers) Belangrijkste punten Toelichting

```
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 ]
```

- Geef een interface op (kan geen uitvoer krijgen die alleen vpn specificeert)
- Zet opties tussen aanhalingstekens ("") , gebruik ctrl c om te stoppen
- Gebruik –n om te voorkomen dat ip naar hostname wordt geconverteerd en –nn om naam en poort te voorkomen?
- -v toont meer details (IP-header informatie, tos, ttl, offset, vlaggen, protocol)
- -VV en –VVV tonen meer details in bepaalde pakkettypen
- Proto ex – udp, tcp icmp pim igmp vrrp esp arp
- Negeren of niet, &&of en, | | of, gebruiken met ( ) niet (udp of icmp)

TCPDUMP (vervolg)

- Aangepast van linux tcpdump commando, maar ondersteunt niet alle beschikbare opties. Momentopnamen van pakketten die in een buffer zijn opgeslagen, kunnen niet naar een PCAP worden geëxporteerd.
- Voert uit met -p-vlag, wat 'niet-promiscue modus' betekent - controller neemt alleen pakketten op die zijn bestemd voor de controller-interface, inclusief besturingspakketten of uitzendpunten. Het verkeer van het gegevensvliegtuig kan niet worden vastgelegd.
- Uitgevoerd met –s 128, lengte van momentopnamen in bytes. De eerste x bytes van het

pakket worden vastgelegd.

De opdracht TCPDUMP gebruiken

Deze sectie geeft voorbeelden die de manier illustreren waarop de opdracht cpdumpcommand wordt gebruikt.

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

De uitvoer van de opdracht show interface description geeft nauwkeurige informatie over de naam en het nummer van de VPN/interface die momenteel in gebruik is.

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

U kunt meer voorwaarden toevoegen voor het filteren van pakketopnames via het trefwoord "opties".

```
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 ]
```

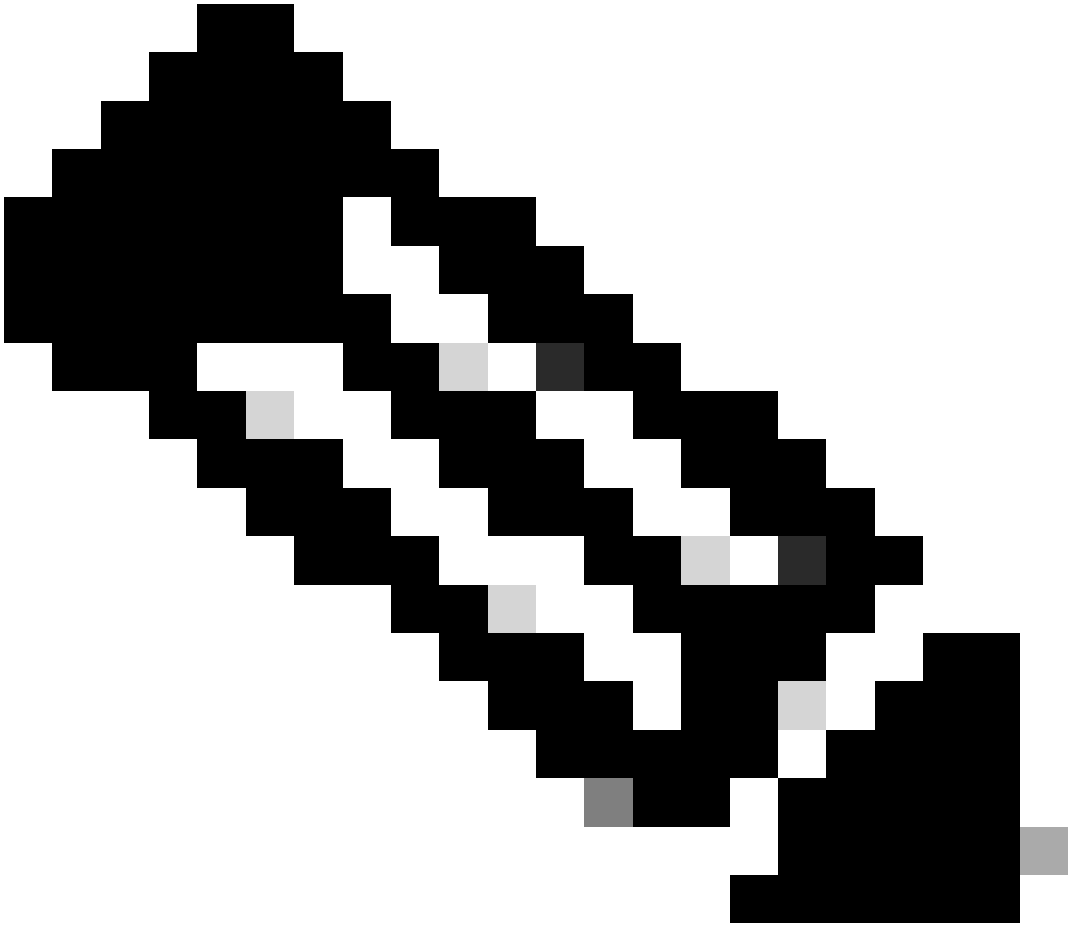
U kunt het specifieke aantal pakketten aangeven met de optie "-account". Als u geen specifiek aantal pakketten aangeeft, wordt een continue opname zonder limiet uitgevoerd.

```
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
```

U kunt ook filtervoorwaarden toevoegen over het hostadres en protocoltype in de opties.

```
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
```

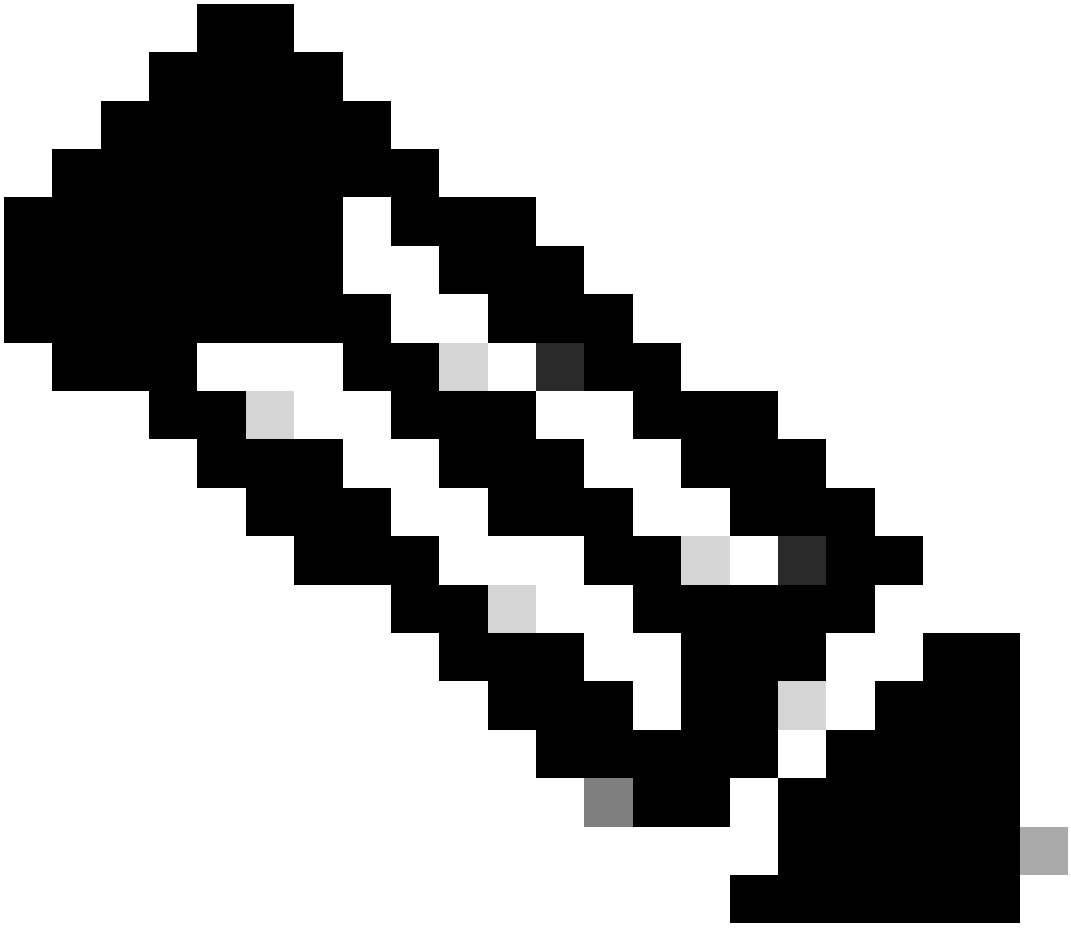


Opmerking: In Cisco IOS XE SD-WAN-software kunt u Embedded Packet Capture (EPC) gebruiken in plaats van TCPDUMP.

TCPDUMP-voorbeelden

Algemeen UDP-pakket beluisteren:

tcpdump VPN 0-opties "-vvv -nnn UDP"



Opmerking: Dit kan ook worden toegepast voor andere protocollen... bijv.: icmp, arp, etc

---

Luisteren naar een specifieke poort met ICMP en UDP:
TCPDUMP VPN 0-interface GE0/4-opties "ICMP of UDP"

Luisteren op een specifiek poortnummer (Luisteren op TLS-poort):
TCPDUMP VPN 0 interface GE0/4 opties "-VVV –NN poort 23456"

Luisteren op een specifiek poortnummer (Luisteren op DTLS-poort):
TCPDUMP VPN 0 interface GE0/4 opties "-VVV –NN poort 12346"

Luisteren naar een specifieke host (van/naar die host): -e drukt koptekst op linkniveau af
TCPDUMP VPN 0-interface GE0/4-opties "Host 64.100.103.2 –VVV –NN –E"

Luisteren naar een specifieke host met alleen ICMP

TCPDUMP VPN 0-interface GE0/4-opties "Host 64.100.103.2 && ICMP"

Filteren op bron en/of bestemming
TCPDUMP VPN 0-interface GE0/4-opties "SRC 64.100.103.2 & DST 64.100.100.75"

Filter op GRE-ingekapseld verkeer
TCPDUMP VPN 0-interface GE0/4-opties "-V –N PROTO 47 "

Gerelateerde documenten

- Problemen oplossen met SD-WAN-besturingsverbindingen
- Cisco SD-WAN: de gebruikelijke verdachten
- TCPDUMP-MANPAGINA

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.