在CLI模式下配置vManage/vSmart/vEdge TCPDUMP資料包捕獲

目錄

簡介

本檔案介紹如何在CLI模式下設定vManage/vSmart/vEdge TCPDUMP封包擷取。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)

採用元件

本檔案中的資訊是根據Cisco vManage 20.9.4版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在Cisco SD-WAN架構中，vManage、vSmart和vEdge分別扮演管理、控制和資料轉發的核心角色。為了確保網路的穩定性和安全性以及排除網路故障，網路工程師通常需要對流經這些裝置的流量進行資料包捕獲和分析。TCPDUMP是一個輕量級且功能強大的命令列工具，可用於捕獲和分析通過介面的資料包。

通過在CLI模式下配置和使用TCPDUMP，使用者可直接捕獲裝置上的即時流量，而無需其他工具或中間代理裝置。這對於查詢路由異常、控制連線故障、資料包丟失以及驗證流量路徑等問題具有重要的意義。由於Cisco SD-WAN裝置（例如vEdge）運行自定義作業系統（例如Viptela OS），因此TCPDUMP的使用在某些方面與傳統Linux環境略有不同。因此，瞭解其基本命令結構和使用限制尤為重要。

本節介紹如何在vManage、vSmart和vEdge裝置的CLI模式下配置和運行TCPDUMP，以協助使用者執行有效的網路流量分析和問題診斷。

TCPDUMP(Controllers)要點說明

```
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 ]
```

- 指定介面（無法獲取僅指定vpn的輸出）
- 將選項置於引號之間(" ")，使用ctrl c停止
- 使用-n阻止ip轉換為主機名，使用-nn阻止名稱和埠？
- -v顯示更多詳細資訊（IP報頭資訊、tos、ttl、偏移、標誌、協定）
- -vv和-vv在某些數據包型別中顯示更多詳細資訊
- Proto ex - udp， tcp icmp pim igmp vrrp esp arp
- 反門!或否,&&或和, | |或或，與()一起使用，不(udp或icmp)

TCPDUMP（續）

- 從linux tcpdump命令改編，但不支援所有可用選項。儲存到緩衝區的資料包的快照，無法匯出到PCAP。
- 使用 — p標誌執行，表示「無混雜模式」 — 控制器僅捕獲發往控制器介面的資料包，包括控制資料包或廣播資料包。無法捕獲資料平面流量。
- 使用 — s 128執行，快照長度（位元組）。捕獲資料包的前x個位元組。

使用TCPDUMP命令

本節提供的範例將說明使用thetcpdumpcommand的方式。

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

show interface description 命令的輸出提供有關當前使用的vpn/interface名稱和編號的準確資訊。

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

您可以使用「options」關鍵字為封包擷取過濾新增更多條件。

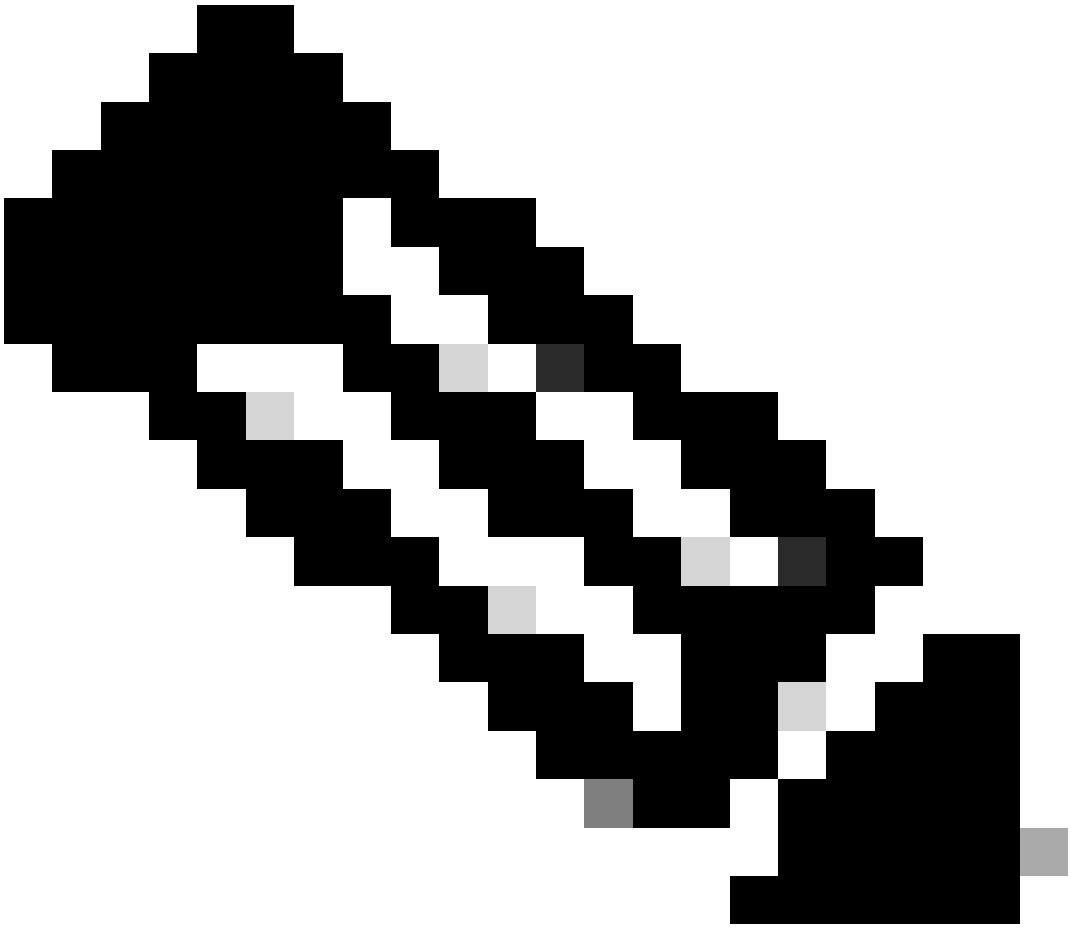
```
vmanage# tcpdump vpn 0 interface eth0 help

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 ]
```

您可以通過選項「 — c count」命令指示特定的包計數。如果沒有指定特定的軟體包計數，則無限制地運行連續捕獲。

```
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
```

您還可以在選項中新增有關主機地址和協定型別的過濾條件。

```
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
```



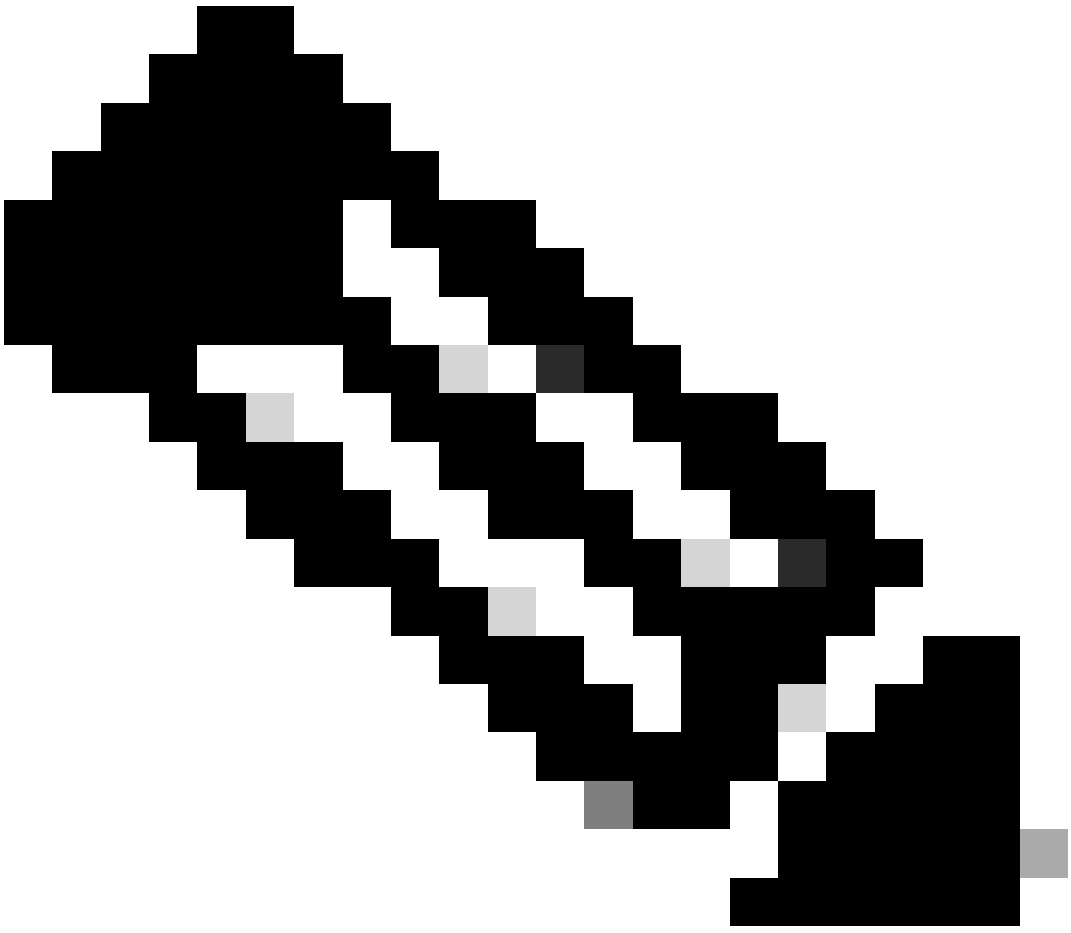
附註：在Cisco IOS XE SD-WAN軟體中，可以使用Embedded Packet Capture(EPC)而不

是TCPDUMP。

TCPDUMP示例

偵聽常規UDP資料包：

tcpdump vpn 0選項"-vvv -nnn udp"



附註：這也適用於其他協定，例如：icmp、arp等

使用ICMP和UDP偵聽特定埠：
tcpdump vpn 0 interface ge0/4 options "icmp or udp"

偵聽特定埠號（在TLS埠上偵聽）：
tcpdump vpn 0 interface ge0/4選項"-vvv -nn port 23456"

偵聽特定埠號（偵聽DTLS埠）：
tcpdump vpn 0 interface ge0/4選項"-vvv -nn port 12346"

偵聽特定主機（到該主機/從該主機）：-e列印鏈路級報頭
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 -vvv -nn -e"

僅使用ICMP偵聽特定主機
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 && icmp"

按源和/或目標篩選
tcpdump vpn 0 interface ge0/4 options "src 64.100.103.2 && dst 64.100.100.75"

篩選GRE封裝流量
tcpdump vpn 0 interface ge0/4選項"-v -n proto 47 "

相關檔案

- 排除SD-WAN控制連線故障
- Cisco SD-WAN:通常的疑犯
- TCPDUMP手冊頁

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。