在CLI模式下配置vManage/vSmart/vEdge TCPDUMP数据包捕获

目录

简介

本文档介绍如何在CLI模式下配置vManage/vSmart/vEdge TCPDUMP数据包捕获。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科软件定义的广域网(SD-WAN)

使用的组件

本文档中的信息基于Cisco vManage 20.9.4版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备都以清除（默认）配置启动。如果您的网络处于活动状态，请确保您了解任何命令的潜在影响。

背景信息

在思科SD-WAN架构中，vManage、vSmart和vEdge分别扮演管理、控制和数据转发等核心角色。为了确保网络的稳定性和安全性，以及排除网络故障，网络工程师通常需要对流经这些设备的流量执行数据包捕获和分析。TCPDUMP是一个轻量级且功能强大的命令行工具，可用于捕获和分析通过接口的数据包。

通过在CLI模式下配置并使用TCPDUMP，用户可直接捕获设备上的实时流量，而无需其他工具或中间代理设备。这对于定位路由异常、控制连接故障、丢包和验证流量路径等问题具有重要意义。由于Cisco SD-WAN设备（如vEdge）运行自定义操作系统（如Viptela OS），因此TCPDUMP的使用在某些方面可能略不同于传统Linux环境。因此，了解其基本命令结构和使用限制尤为重要。

本节介绍如何在vManage、vSmart和vEdge设备的CLI模式下配置和运行TCPDUMP，以协助用户进行有效的网络流量分析和问题诊断。

TCPDUMP（控制器）要点说明

```
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 ]
```

- 指定接口（无法获取仅指定vpn的输出）
- 将选项置于引号之间(" ")，使用ctrl c停止
- 使用-n阻止将ip转换为主机名，使用-nn阻止名称和端口？
- -v显示更多详细信息（IP报头信息、tos、ttl、偏移、标志、协议）
- -vv和-vvv在某些数据包类型中显示更多详细信息
- Proto ex - udp、tcp icmp pim igmp vrrp esp arp
- 反门!或否,&&或和, | |或或，与()一起使用(udp或icmp)

TCPDUMP（续）

- 从linux tcpdump命令改编，但不支持所有可用选项。保存到缓冲区的数据包的快照，无法导出到PCAP。
- 使用 — p标志执行，表示“无混杂模式” — 控制器仅捕获发往控制器接口的数据包，包括控制数据包或广播数据包。无法捕获数据平面流量。
- 使用 — s 128执行，快照长度（以字节为单位）。捕获数据包的前x个字节。

使用TCPDUMP命令

本部分提供了说明如何使用tcpdumpcommand的示例。

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

show interface description命令的输出提供有关当前使用的vpn/interface名称和编号的精确信息。

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

您可以通过“options”关键字为数据包捕获过滤添加更多条件。

```
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 ]
```

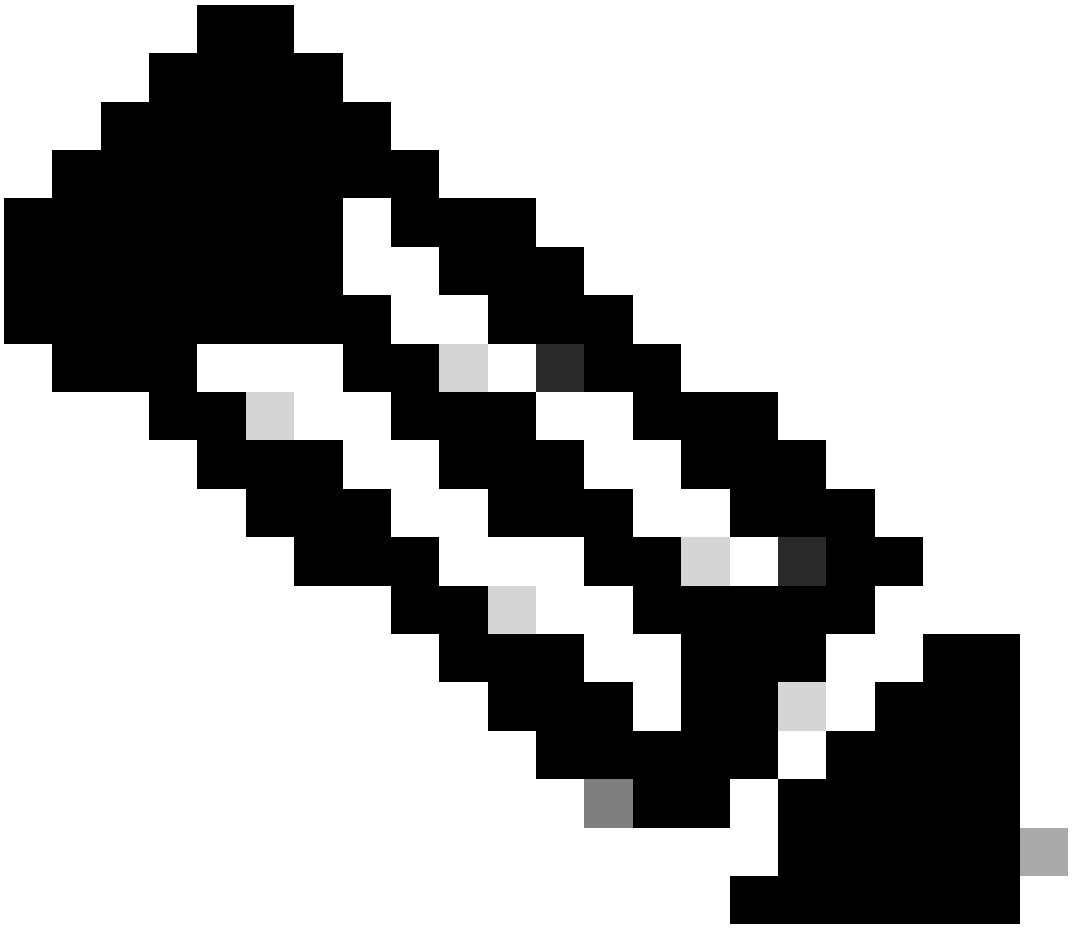
您可以通过选项“ — c count”命令指示特定包计数。如果没有指定特定的软件包计数，则无限制地运行连续捕获。

```
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
```

还可以在选项中添加有关主机地址和协议类型的过滤条件。

```
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
```

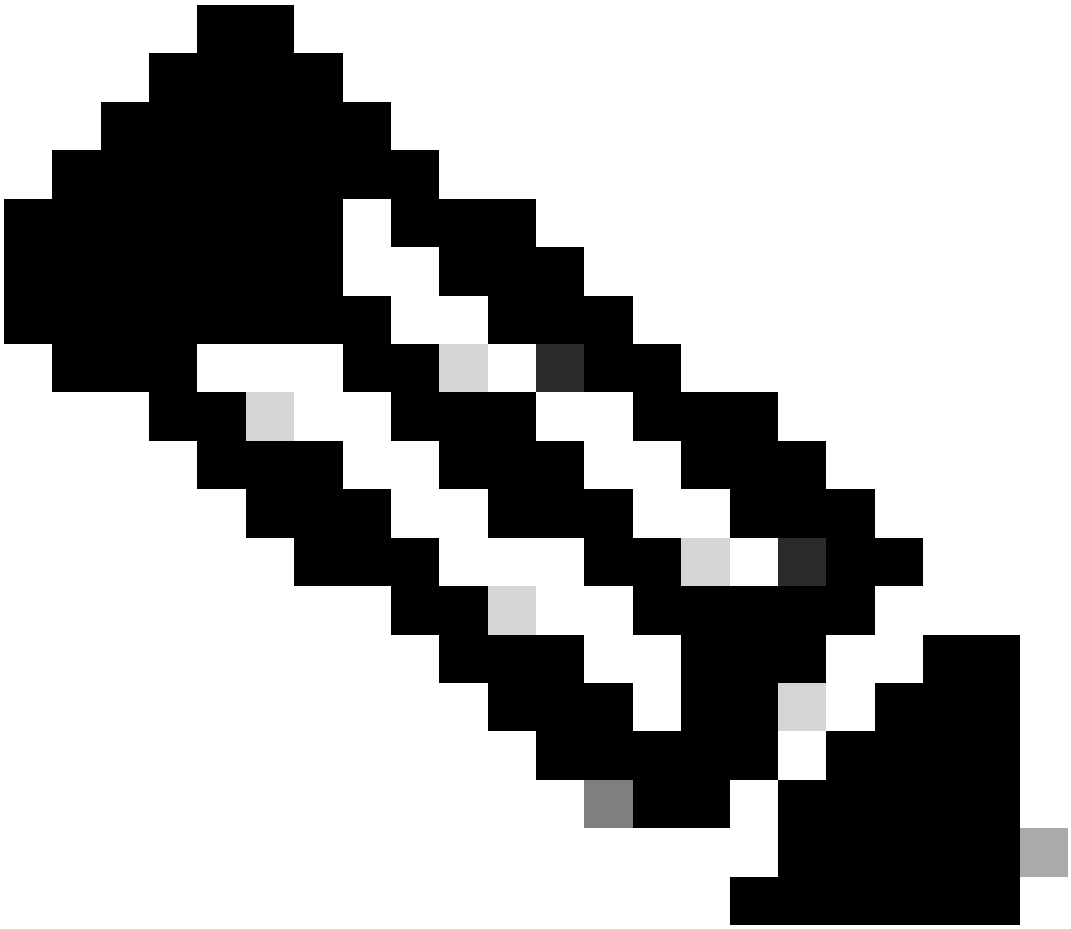


注意：在Cisco IOS XE SD-WAN软件上，您可以使用嵌入式数据包捕获(EPC)而非TCPDUMP。

TCPDUMP示例

侦听常规UDP数据包：

tcpdump vpn 0选项"-vvv -nnn udp"



注意：这也适用于其他协议，例如：icmp、arp等

使用ICMP和UDP侦听特定端口：
tcpdump vpn 0 interface ge0/4 options "icmp or udp"

在特定端口号侦听（在TLS端口侦听）：
tcpdump vpn 0 interface ge0/4 options "-vvv -nn port 23456"

侦听特定端口号（侦听DTLS端口）：
tcpdump vpn 0 interface ge0/4 options "-vvv -nn port 12346"

侦听特定主机（至/自该主机）：-e打印链路级报头
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 -vvv -nn -e"

仅使用ICMP侦听特定主机
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 && icmp"

按源和/或目标过滤
tcpdump vpn 0 interface ge0/4 options "src 64.100.103.2 && dst 64.100.100.75"

过滤GRE封装的流量
tcpdump vpn 0 interface ge0/4 options "-v -n proto 47 "

相关文档

- 排除SD-WAN控制连接故障
- 思科SD-WAN:通常的嫌犯
- TCPDUMP手册页

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。