Configuración de la captura de paquetes TCPDUMP de vManage/vSmart/vEdge en modo CLI

Contenido

Introducción

Este documento describe cómo configurar vManage/vSmart/vEdge TCPDUMP Packet Capture en el modo CLI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software de Cisco (SD-WAN)

Componentes Utilizados

La información de este documento se basa en la versión 20.9.4 de Cisco vManage

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos utilizados en este documento comenzaron con una configuración desactivada (predeterminada). Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando.

Antecedentes

En la arquitectura SD-WAN de Cisco, vManage, vSmart y vEdge desempeñan respectivamente las funciones principales de gestión, control y reenvío de datos. Para garantizar la estabilidad y la seguridad de la red, así como para solucionar los fallos de red, los ingenieros de redes a menudo necesitan llevar a cabo la captura y el análisis de paquetes en el tráfico que fluye a través de estos dispositivos. TCPDUMP es una herramienta de línea de comandos ligera y potente que se puede utilizar para capturar y analizar los paquetes de datos que pasan a través de las interfaces.

Al configurar y utilizar TCPDUMP en modo CLI, los usuarios pueden capturar directamente el tráfico en tiempo real en el dispositivo sin necesidad de herramientas adicionales o dispositivos proxy intermedios. Esto es de gran importancia para la localización de problemas como anomalías de routing, fallos de conexión de control, pérdida de paquetes y verificación de rutas de tráfico. Dado que los dispositivos SD-WAN de Cisco (como vEdge) ejecutan sistemas operativos personalizados (como Viptela OS), el uso de TCPDUMP puede diferir ligeramente del de los entornos Linux tradicionales en algunos aspectos. Por lo tanto, comprender su estructura de comandos básica y sus limitaciones de uso es especialmente crucial.

En esta sección se explica cómo configurar y ejecutar TCPDUMP en el modo CLI de los dispositivos vManage, vSmart y vEdge para ayudar a los usuarios a realizar un análisis eficaz del tráfico de red y un diagnóstico de problemas.

Explicación de los puntos clave de TCPDUMP(controladores)

```
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 ]
```

- Especifique una interfaz (no se puede obtener salida especificando vpn solamente)
- Coloque las opciones entre comillas ("") , utilice ctrl c para detener
- Use -n para evitar la conversión de ip a nombre de host y -nn para evitar la conversión de nombre y puerto ?
- -v muestra más detalles (información de encabezado IP, tos, ttl, desplazamiento, indicadores, protocolo)
- -vv y -vvv muestran más detalles en ciertos tipos de paquetes
- Proto ex - udp, tcp icmp pim igmp vrrp esp arp
- ¡Negar! o no, && o y, | | o o, utilizar con ( ) no (udp o icmp)

TCPDUMP (cont.)

- Adaptado desde el comando tcpdump de linux pero no soporta todas las opciones disponibles. Instantáneas de paquetes guardados en un búfer, no se pueden exportar a una PCAP.
- Se ejecuta con el indicador -p, que significa ‘modo no promiscuo’ - el controlador solo

captura paquetes destinados a la interfaz del controlador, incluyendo paquetes de control o paquetes de broadcast. No se puede capturar el tráfico del plano de datos.
- Ejecutado con -s 128, longitud de instantánea en bytes. Se capturan los primeros x bytes del paquete.

Utilice el comando TCPDUMP

Esta sección proporciona ejemplos que ilustran la forma en que se utiliza el comando tetcpdump.

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

El resultado del comando show interface description proporciona información precisa sobre el nombre y el número de vpn/interface que se está utilizando actualmente.

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

Puede agregar más condiciones para el filtrado de captura de paquetes mediante la palabra clave "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 ]
```

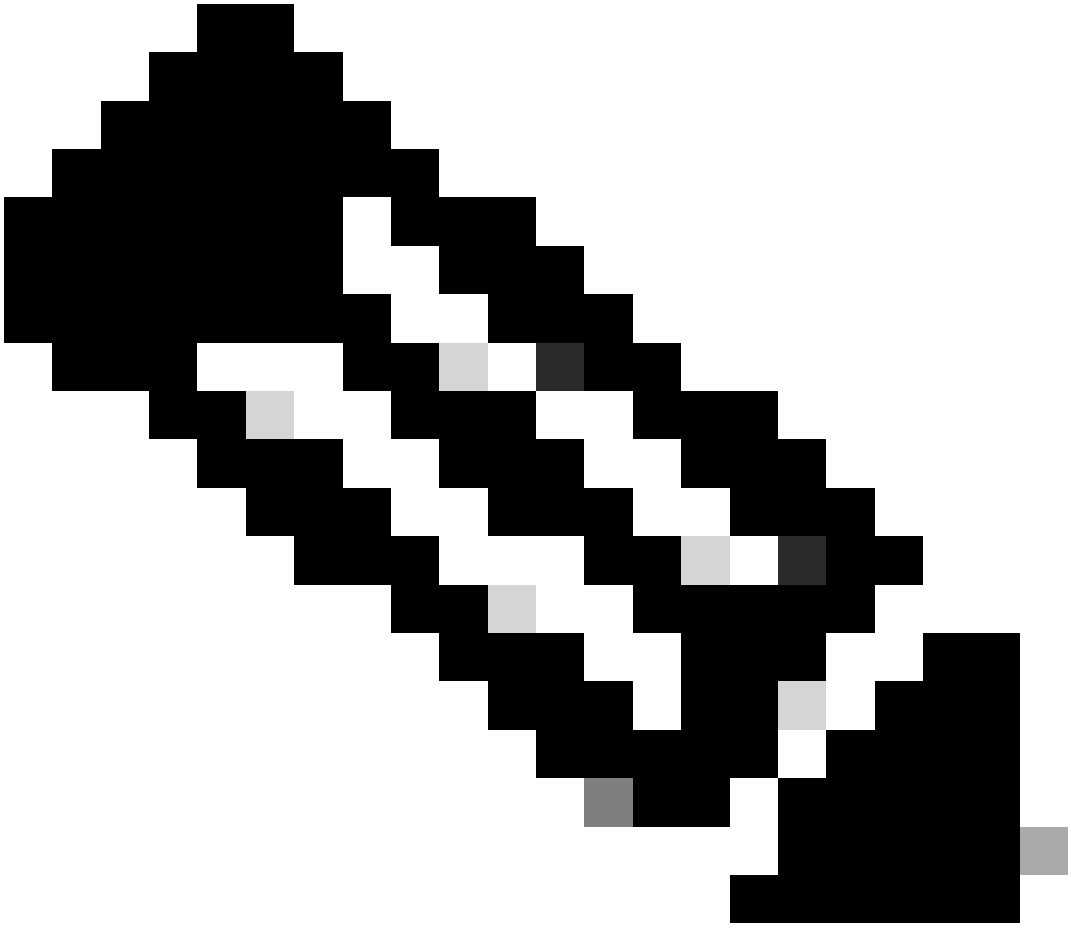
Puede indicar el recuento de paquetes específico mediante el comando options "-c count". Si no indica un recuento de paquetes específico, se ejecuta una captura continua sin límite.

```
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
```

También puede agregar condiciones de filtro sobre la dirección de host y el tipo de protocolo en las opciones.

```
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
```

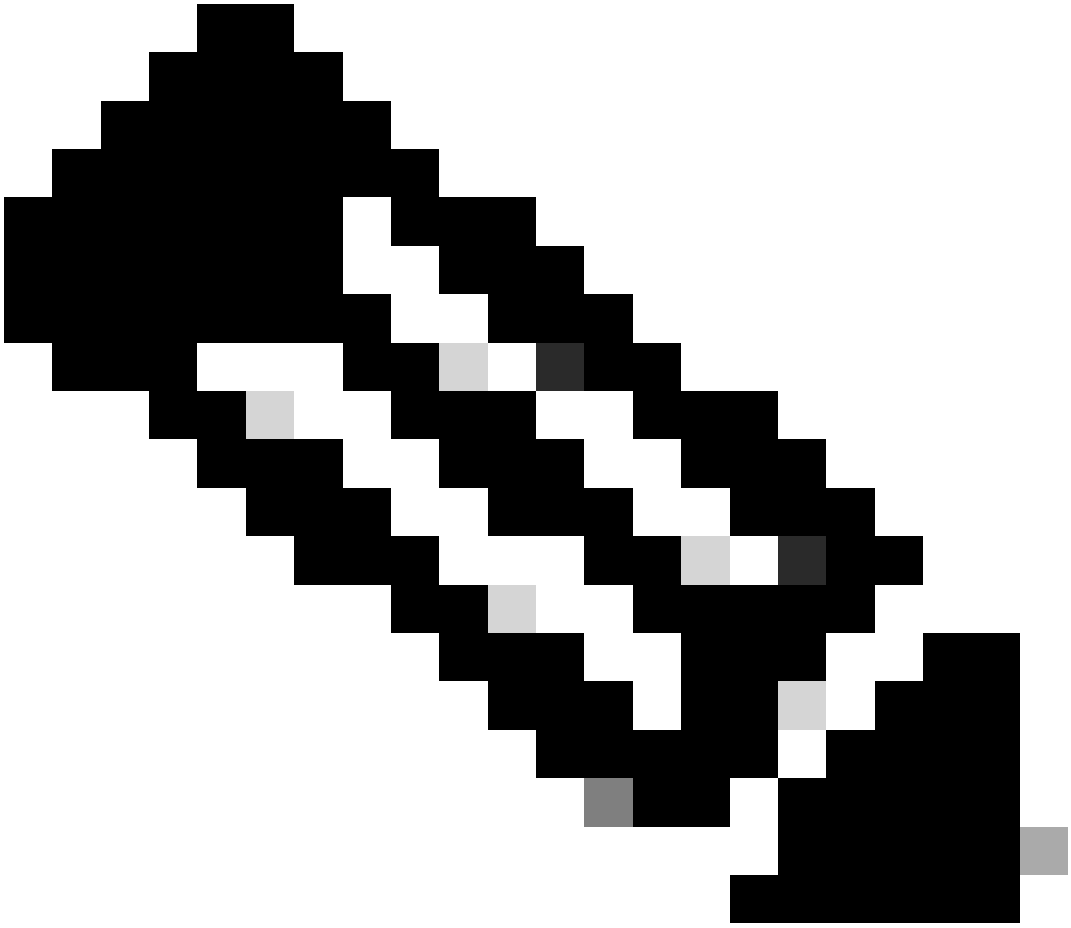


Nota: En el software Cisco IOS XE SD-WAN, puede utilizar la captura de paquetes integrada (EPC) en lugar de TCPDUMP.

Ejemplos de TCPDUMP

Escuchando paquete UDP general:

tcpdump vpn 0 options "-vvv -nnn udp"



Nota: Esto también se puede aplicar a otros protocolos, por ejemplo: icmp, arp, etc

---

Escucha de un puerto específico con ICMP y UDP:
tcpdump vpn 0 interface ge0/4 options "icmp or udp"

Escuchar en un número de puerto específico(Escuchar en puerto TLS):
tcpdump vpn 0 interface ge0/4 options "-vvv -nn port 23456"

Escuchar en un número de puerto específico(Escuchar en puerto DTLS):
tcpdump vpn 0 interface ge0/4 options "-vvv -nn port 12346"

Recepción de un host específico (hacia/desde ese host): -e imprime el encabezado de nivel de vínculo
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 -vv -nn -e"

Escucha de un host específico sólo con ICMP
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 && icmp"

Filtrado por Origen y/o Destino
tcpdump vpn 0 interface ge0/4 options "src 64.100.103.2 && dst 64.100.100.75"

Filtrar por tráfico GRE encapsulado
tcpdump vpn 0 interface ge0/4 options "-v -n proto 47 "

Documentos Relacionados

- Solucionar problemas de conexiones de control SD-WAN
- SD-WAN de Cisco: Los sospechosos habituales
- PÁGINA DE COMANDO MAN TCPDUMP

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).