Configurazione dell'acquisizione pacchetti vManage/vSmart/vEdge TCP-DUMP in modalità CLI

Sommario

Introduzione

In questo documento viene descritto come configurare vManage/vSmart/vEdge TCP DUMP Packet Capture in modalità CLI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco

Componenti usati

Le informazioni di questo documento si basano su Cisco vManage versione 20.9.4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nell'architettura Cisco SD-WAN, vManage, vSmart e vEdge svolgono rispettivamente il ruolo principale di gestione, controllo e inoltro dei dati. Per garantire la stabilità e la sicurezza della rete e per risolvere i problemi di rete, i tecnici della rete spesso devono eseguire l'acquisizione e l'analisi dei pacchetti sul traffico che attraversa questi dispositivi. TCPDUMP è uno strumento da riga di comando leggero e potente che può essere utilizzato per acquisire e analizzare i pacchetti di dati che passano attraverso le interfacce.

Configurando e utilizzando TCP DUMP in modalità CLI, gli utenti possono acquisire direttamente il traffico in tempo reale sul dispositivo senza la necessità di strumenti aggiuntivi o dispositivi proxy intermedi. Questa funzione è molto importante per individuare problemi quali anomalie di routing, errori di connessione di controllo, perdita di pacchetti e verifica dei percorsi del traffico. Poiché i dispositivi Cisco SD-WAN (ad esempio vEdge) eseguono sistemi operativi personalizzati (ad esempio Viptela OS), l'utilizzo di TCP DUMP può differire leggermente da quello negli ambienti Linux tradizionali per alcuni aspetti. Pertanto, è particolarmente importante comprendere la struttura dei comandi di base e i limiti di utilizzo.

Questa sezione spiega come configurare ed eseguire TCP DUMP nella modalità CLI dei dispositivi vManage, vSmart e vEdge, in modo da assistere gli utenti nell'esecuzione efficace dell'analisi del traffico di rete e della diagnosi dei problemi.

Spiegazione dei punti chiave di TCPDUMP(Controller)

```
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 ]
```

- Specificare un'interfaccia (impossibile ottenere l'output specificando solo vpn)
- Inserire le opzioni tra virgolette (""), utilizzare ctrl c per interrompere
- Utilizzare -n per impedire la conversione di ip in nome host e -nn per impedire la conversione di nome e porta?
- -v mostra maggiori dettagli (informazioni intestazione IP, tos, ttl, offset, flag, protocollo)
- -vv e -vv mostrano più dettagli in alcuni tipi di pacchetti
- Proto ex - udp, tcp icmp pim igmp vrp esp arp
- Negate! o no, && o e, | | oppure o, utilizzare con ( ) not (udp o icmp)

TCPDUMP (continua)

- Adattato dal comando linux tcpdump, ma non supporta tutte le opzioni disponibili. Le istantanee dei pacchetti salvati in un buffer non possono essere esportate in PCAP.
- Esegue con il flag -p, che significa "modalità non promiscua" - il controller acquisisce solo i pacchetti destinati all'interfaccia del controller, inclusi i pacchetti di controllo o i pacchetti broadcast. Impossibile acquisire il traffico del piano dati.

- Eseguito con -s 128, lunghezza dello snapshot in byte. Vengono acquisiti i primi x byte del pacchetto.

Utilizzare il comando TCP DUMP

In questa sezione vengono forniti esempi che illustrano il modo in cui viene utilizzato il comando cpdumpcommand.

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

L'output del comando show interface description fornisce informazioni precise sul nome della vpn/interfaccia e sul numero attualmente in uso.

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

È possibile aggiungere altre condizioni per il filtro dell'acquisizione dei pacchetti tramite la parola chiave "options" (opzioni).

```
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 ]
```

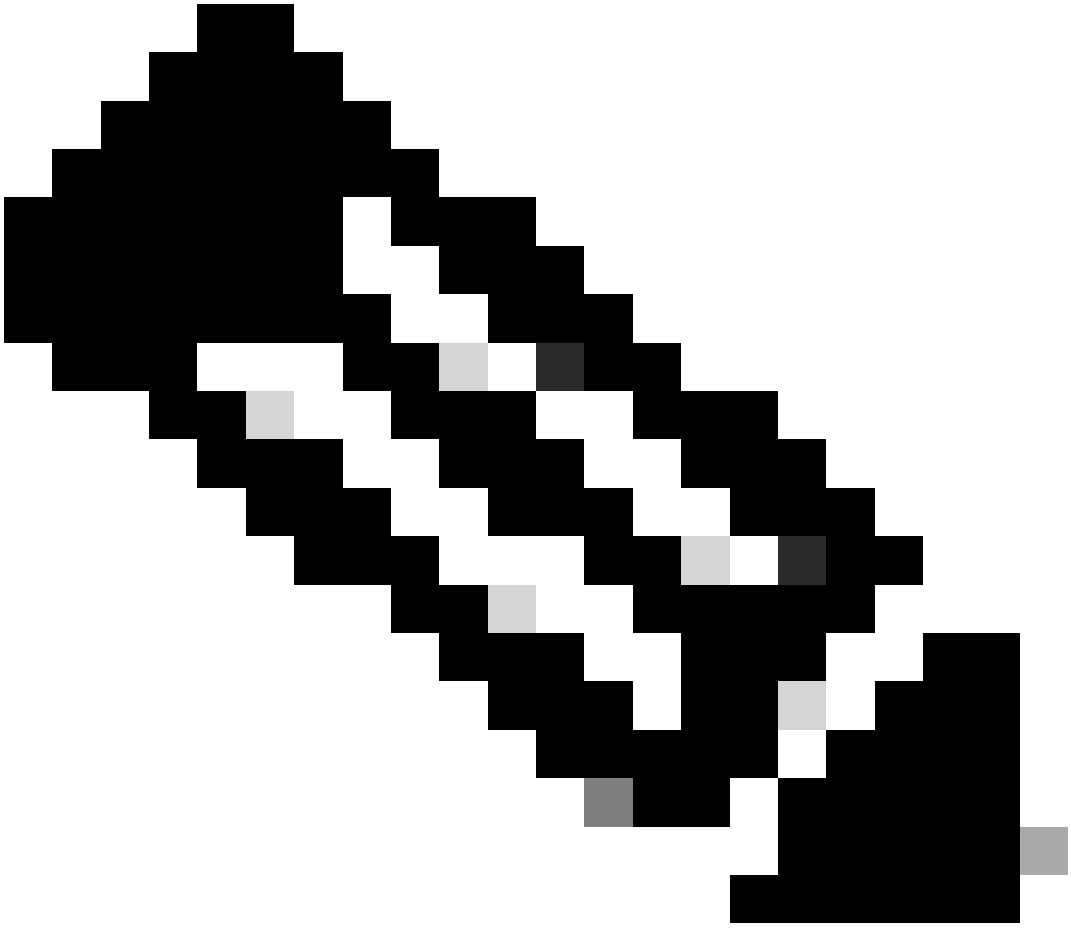
È possibile indicare il numero di pacchetti specifico mediante il comando delle opzioni "-c count". Se non si indica un numero specifico di pacchetti, viene eseguita un'acquisizione continua senza limiti.

```
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
```

È inoltre possibile aggiungere condizioni di filtro relative all'indirizzo host e al tipo di protocollo nelle opzioni.

```
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
```

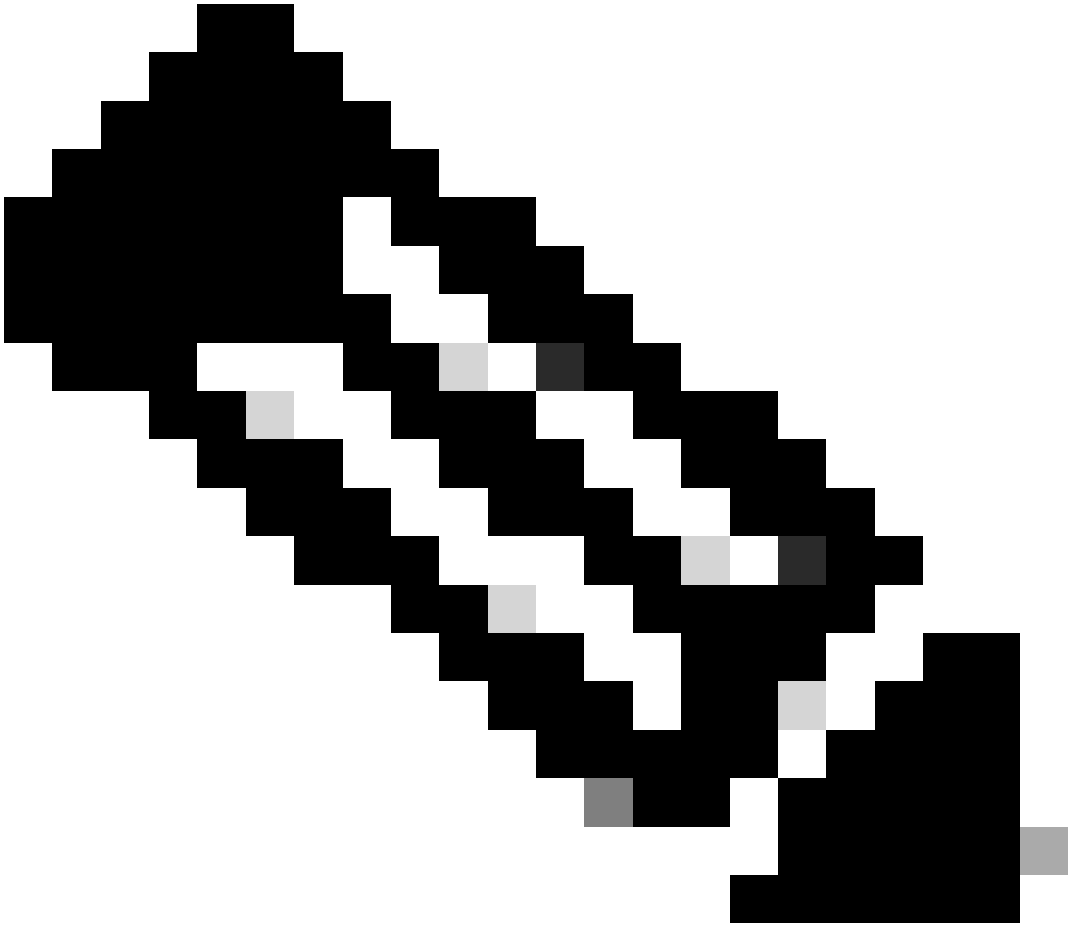


Nota: Sul software Cisco IOS XE SD-WAN, è possibile usare Embedded Packet Capture (EPC) anziché TCP DUMP.

Esempi di TCP-DUMP

Pacchetto UDP generale in ascolto:

tcpdump vpn 0 opzioni "-vv -nnn udp"



Nota: Questa procedura può essere applicata anche ad altri protocolli, ad esempio: icmp, arp, ecc.

In ascolto di una porta specifica con ICMP e UDP:
tcpdump vpn 0 interface ge0/4 options "icmp or udp" (opzioni tcpdump vpn 0 interface ge0/4 "icmp o udp")

In ascolto su un numero di porta specifico (in ascolto sulla porta TLS):
tcpdump vpn 0 interface ge0/4 options "-vv -nn port 23456"

In ascolto su un numero di porta specifico (in ascolto sulla porta DTLS):
tcpdump vpn 0 interface ge0/4 options "-vv -nn port 12346"

In ascolto di un host specifico (verso/da tale host): -e stampa l'intestazione a livello di collegamento

tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 -vv -nn -e"

In ascolto di un host specifico solo con ICMP
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 && icmp"

Filtraggio per origine e/o destinazione
tcpdump vpn 0 interface ge0/4 options "src 64.100.103.2 && dst 64.100.100.75"

Filtra in base al traffico incapsulato dal GRE
tcpdump vpn 0 interface ge0/4 options "-v -n proto 47 "

Documenti correlati

- Risoluzione dei problemi relativi alle connessioni di controllo SD-WAN
- Cisco SD-WAN: I soliti sospetti
- PAGINA MAN TCP DUMP

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).