CLIモードでのvManage/vSmart/vEdge TCPDUMPパケットキャプチャの設定

内容

はじめに

このドキュメントでは、CLIモードでvManage/vSmart/vEdge TCPDUMPパケットキャプチャを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

使用するコンポーネント

このドキュメントの情報は、Cisco vManageバージョン20.9.4に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリア（デフォルト）設定で作業を開始しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

Cisco SD-WANアーキテクチャでは、vManage、vSmart、およびvEdgeがそれぞれ管理、制御、およびデータ転送の中心的な役割を果たします。ネットワークの安定性とセキュリティを確保し

、ネットワーク障害をトラブルシューティングするために、ネットワークエンジニアは多くの場合、これらのデバイスを通過するトラフィックのパケットキャプチャと分析を行う必要があります。TCPDUMPは、インターフェイスを通過するデータパケットのキャプチャと分析に使用できる、軽量で強力なコマンドラインツールです。

CLIモードでTCPDUMPを設定して使用すると、ユーザは追加のツールや中間プロキシデバイスを必要とせずに、デバイス上のリアルタイムトラフィックを直接キャプチャできます。これは、ルーティングの異常、接続障害の制御、パケット損失、トラフィックパスの検証などの問題を特定する上で非常に重要です。Cisco SD-WANデバイス（vEdgeなど）はカスタマイズされたオペレーティングシステム（Viptela OSなど）を実行するため、TCPDUMPの使用は、一部の点では従来のLinux環境の使用とは少し異なる場合があります。そのため、基本的なコマンド構造と使用制限を理解することが特に重要です。

このセクションでは、ユーザが効果的なネットワークトラフィック分析と問題の診断を実行できるように、vManage、vSmart、およびvEdgeデバイスのCLIモードでTCPDUMPを設定および実行する方法について説明します。

TCPDUMP（コントローラ）キーポイントの説明

```
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 ]
```

- インターフェイスを指定してください（vpnだけを指定した出力は得られません）
- オプションを引用符で囲みます(" ")。中止するには、ctrl cを使用します
- IPをホスト名に変換しないようにするには-nを使用し、名前とポートを変換しないようにするには-nnを使用します。
- -vより詳細な情報（IPヘッダー情報、tos、ttl、オフセット、フラグ、プロトコル）が表示されます。
- -vvおよび-vvvは、特定のパケットタイプの詳細を示します
- Proto ex - udp、tcp icmp pim igmp vrrp esp arp
- !またはnot、&&または、| |またはorを否定し、( ) not(udpまたはicmp)を使用します。

TCPDUMP（続き）

- linux tcpdumpコマンドから調整されますが、使用可能なオプションの一部はサポートされません。バッファに保存されたパケットのスナップショットは、PCAPにエクスポートできません。
- -pフラグ（「no-promiscuous mode」を意味する）を指定して実行します。コントローラは、コントロールパケットやブロードキャストパケットなど、コントローラインターフェイス宛てのパケットのみをキャプチャします。データプレーントラフィックをキャプチャできません。

- -s 128で実行され、スナップショットの長さがバイト単位で表示されます。パケットの最初のxバイトがキャプチャされます。

tcpdump コマンドの使用

この節では、tcpdumpcommandコマンドの使用方法を説明する例を示します。

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

show interface descriptionコマンドの出力に、現在使用中のvpn/interfaceの名前と番号に関する正確な情報が示されます。

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

「options」キーワードを使用すると、パケットキャプチャフィルタリングに条件を追加できます。

```
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 ]
```

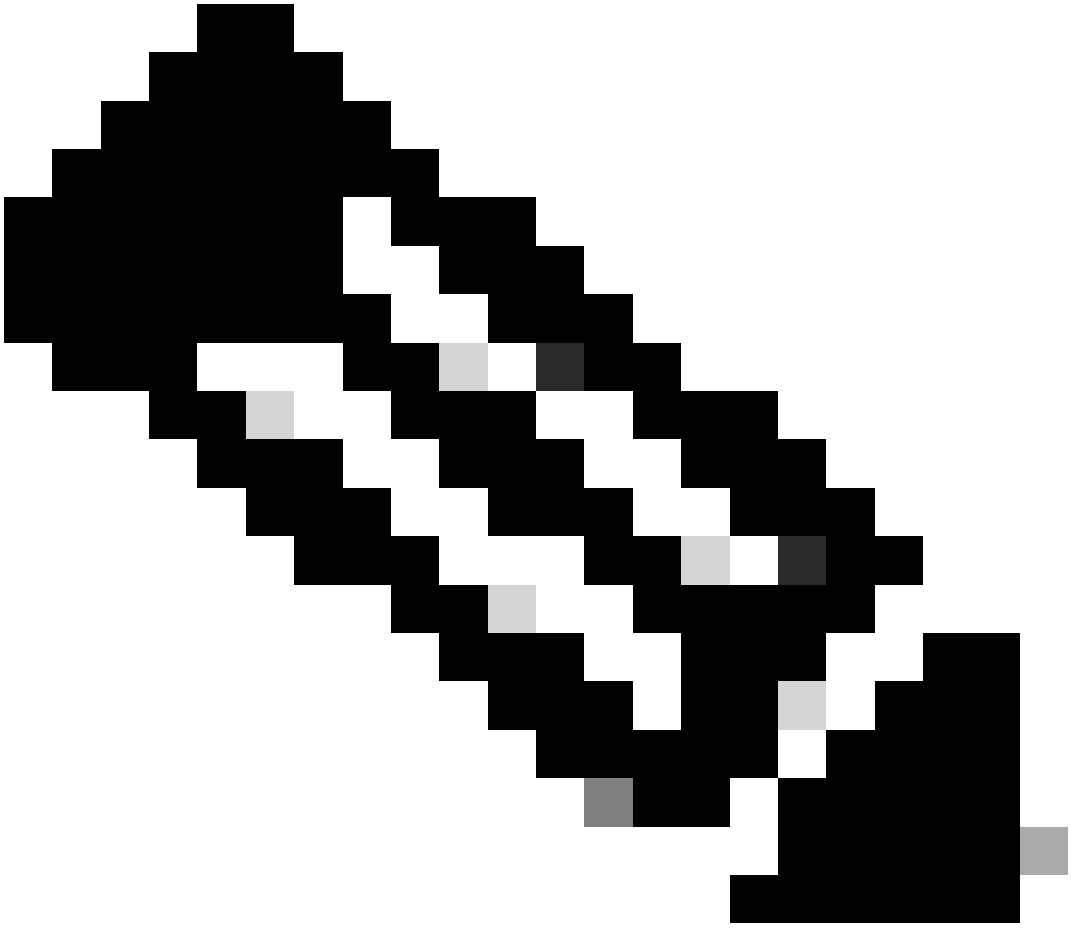
オプション「-c count」コマンドで特定のパッケージ数を指定できます。特定のパッケージの数を表示しない場合、無制限の連続キャプチャが実行されます。

```
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
```

オプションで、ホストアドレスとプロトコルタイプに関するフィルタ条件を追加することもできます。

```
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
```

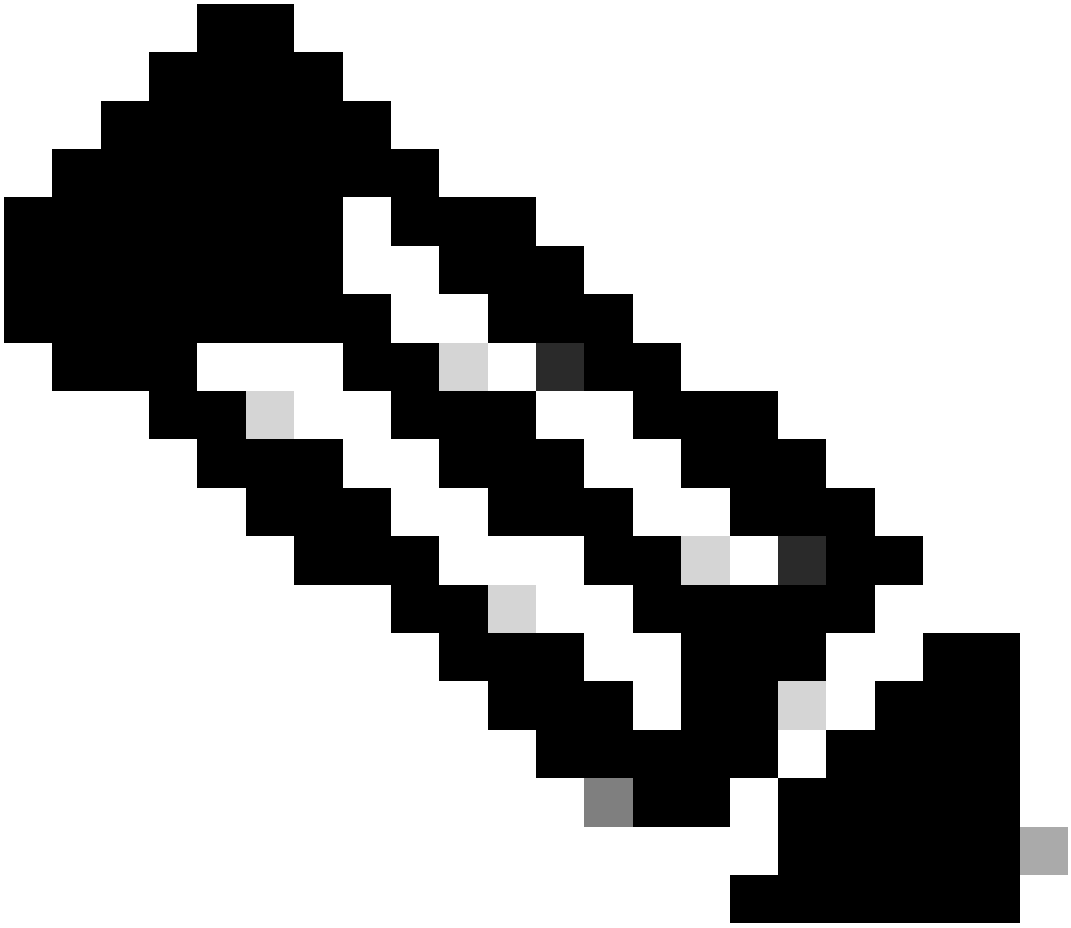


注:Cisco IOS XE SD-WANソフトウェアでは、TCPDUMPの代わりにEmbedded Packet Capture(EPC)を使用できます。

TCPDUMPの例

一般的なUDPパケットのリスニング：

tcpdump vpn 0オプション「 – vvv -nnn udp」



注：これは他のプロトコル（icmp、arpなど）にも適用できます。

ICMPおよびUDPを使用した特定のポートのリスニング：
tcpdump vpn 0 interface ge0/4 options "icmp or udp"

特定のポート番号でリッスンする（TLSポートでリッスンする）：
tcpdump vpn 0 interface ge0/4 options "-vvvv -nn port 23456"

特定のポート番号でリッスンする（DTLSポートでリッスンする）：
tcpdump vpn 0 interface ge0/4 options "-vvvv -nn port 12346"

特定のホストのリスニング（そのホストとの間）：-eはリンクレベルのヘッダを出力します。
tcpdump vpn 0 interface ge0/4 options "host 64.100.103.2 -vvv -nn -e"

ICMPを使用した特定のホストのリスニングのみ

tcpdump vpn 0 interface ge0/4 options “host 64.100.103.2 && icmp”

送信元/宛先によるフィルタリング
tcpdump vpn 0 interface ge0/4 options “src 64.100.103.2 && dst 64.100.100.75”

GREカプセル化トラフィックのフィルタリング
tcpdump vpn 0 interface ge0/4 options "-v -n proto 47 "

関連資料

- SD-WAN制御接続のトラブルシューティング
- Cisco SD-WAN：一般的な問題
- TCPDUMPのマニュアルページ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。