تكوين التقاط حزمة vManage/vSmart/vEdge TCPDUMP في وضع CLI

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين التقاط حزم TCPDUMP/vManage/vEdge في وضع واجهة سطر الأوامر.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة المنطقة الواسعة المعرفة من برنامج Cisco (SD-WAN)

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى الإصدار 20.9.4 من Cisco vManage

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

في بنية شبكة SD-WAN من Cisco، تلعب تقنية vManage و vSmart و vEdge على التوالي الأدوار الأساسية للإدارة والتحكم وإعادة توجيه البيانات. لضمان استقرار الشبكة وأمانها واستكشاف أخطاء الشبكة وإصلاحها، يحتاج مهندسو الشبكة غالبا إلى إجراء التقاط الحزم

وتحليلها على حركة المرور المتدفقة عبر هذه الأجهزة. TCPDUMP هي أداة سطر أوامر مفتوحة المصدر تتيح للمستخدمين التقاط حزم البيانات التي تمر عبر الواجهات وتحليلها.

من خلال تكوين TCPDUMP واستخدامه في وضع واجهة سطر الأوامر، يمكن للمستخدمين التقاط حركة مرور البيانات في الوقت الفعلي على جهاز مباشرة دون الحاجة إلى أدوات إضافية أو أجهزة وكيل وسيطة. ويكون هذا ذا أهمية كبيرة لتحديد موقع المشاكل مثل حالات عدم التطابق في التوجيه، ومشاكل الاتصال بالتحكم، وفقدان الحزمة، والتحقق من مسارات حركة المرور. بما أن أجهزة SD-WAN من Cisco (مثل vEdge) تستخدم أنظمة تشغيل مخصصة (مثل نظام التشغيل Viptela OS)، فإن استخدام TCPDUMP وتفريغ يمكن أن يختلف قليلا عن ذلك في بيئات Linux التقليدية في بعض الجوانب. وبالتالي، فإن فهم بنيتها الأساسية وقواعد استخدامها هو أمر بالغ الأهمية بشكل خاص.

يوضح هذا القسم كيفية تكوين وتفريغ TCPDUMP وتشغيله في وضع واجهة سطر الأوامر (CLI) الخاص بأجهزة vManage و vSmart و vEdge، لمساعدة المستخدمين في إجراء تحليل فعال لحركة مرور البيانات على الشبكة وتشخيص المشكلة.

شرح النقاط الرئيسية ل TCPDUMP(وحدات التحكم)

```
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 ]
```

- حدد واجهة (لا يمكن الحصول على مخرجات تحدد VPN فقط)
- ضع الخيارات بين علامات الاقتباس (") ، أستخدم ctrl c للإيقاف
- أستخدم -n لمنع تحويل IP إلى اسم المضيف و-nn لمنع الاسم والمنفذ ؟
- -v يظهر المزيد من التفاصيل (معلومات رأس IP، TOS، TTL، إزاحة، علامات، بروتوكول)
- يعرض -vv و-vv المزيد من التفاصيل في أنواع معينة من الحزم
- بروتوكول EX - UDP و TCP ICMP IGMP vrrp ARP
- نفي ! أو ال، && أو و، | | أو أو، أستخدم مع (ال (UDP أو ICMP)

TCPDUMP (عبات)

- تم تعديله من أمر tcpdump لبيئة لينوكس ولكنه لا يدعم جميع الخيارات المتاحة. التقاطات للمزح المحفوظة في مخزن يتقؤم، لا يمكن تصديرها إلى PCAP.
- يتم التنفيذ باستخدام علامة -p، مما يعني "الوضع غير المختلطة" - حيث توقع وحدة التحكم فقط بالتقاط الحزم الموجهة لواجهة وحدة التحكم، بما في ذلك حزم التحكم أو وحدات PKTS للبث. يتعذر التقاط حركة مرور مستوى البيانات.
- تم التنفيذ باستخدام -s 128، لطول اللقطة بالبايت. يتم التقاط أول x بايت من الحزمة.

إستخدام الأمر tcpdump

يقدم هذه القسم أمثلة توضح كيفية إستخدام الأمرcppdumpcommand.

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

يزود الإنتاج من العرض قارن وصف أمر معلومات دقيقة حول ال vpn/قارن إسم ورقم أن يكون حاليا يستعمل.

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

يمكنك إضافة المزيد من الشروط لتصفية التقاط الحزم من خلال الكلمة الأساسية خيارات".

```
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 ]
```

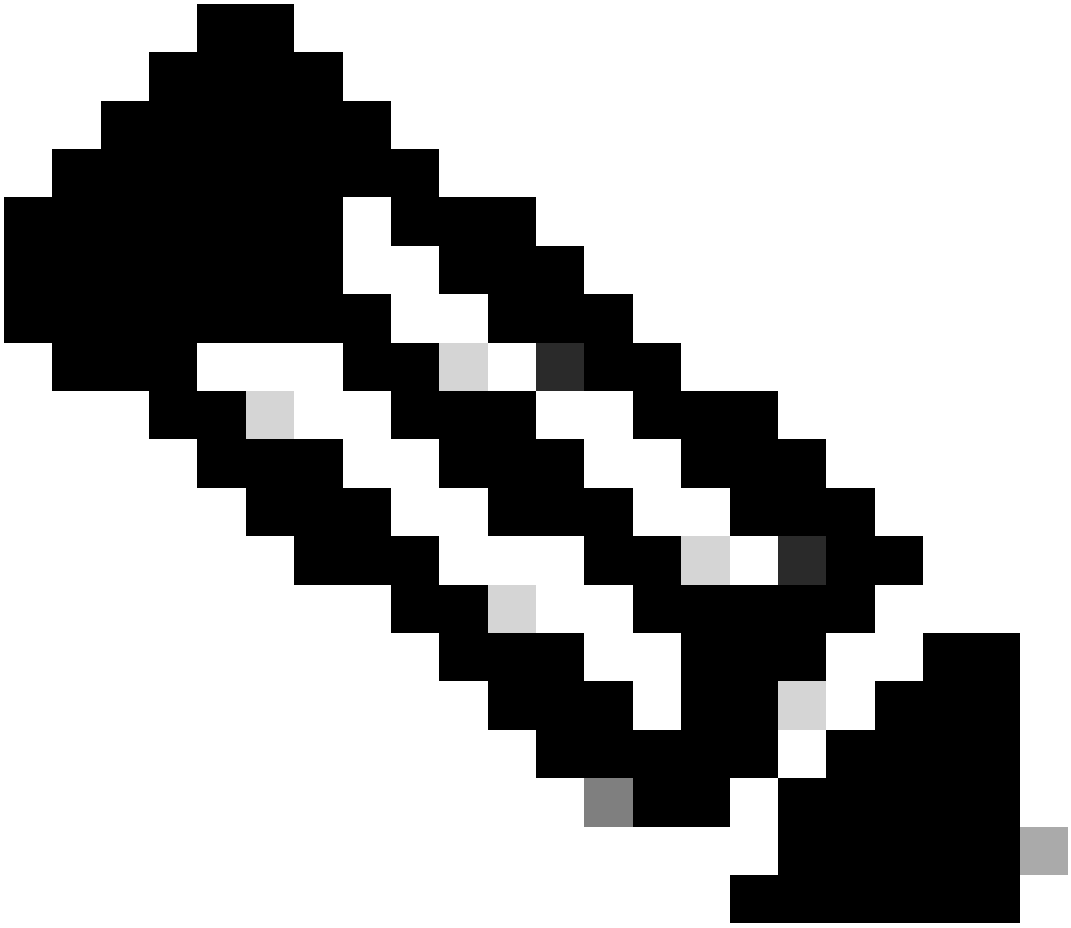
يمكنك الإشارة إلى عدد الحزم المحدد بواسطة الأمر خيارات عدد-c". إذا لم تقم بتحديد عدد حزم معين، سيتم تشغيل التقاط مستمر بدون حدود.

```
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
```

يمكنك أيضا إضافة شروط مرشح حول عنوان المضيف ونوع البروتوكول في الخيارات.

```
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
```

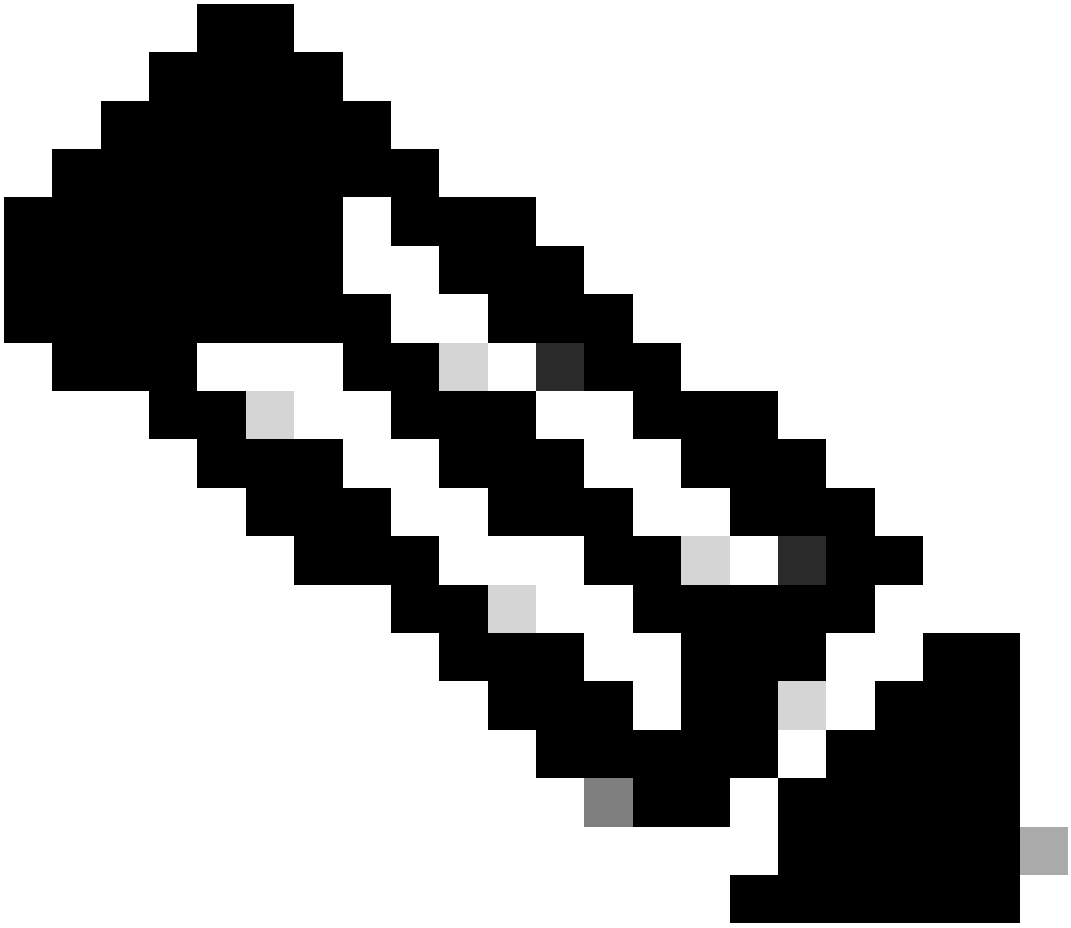


ملاحظة: في برنامج Cisco IOS XE SD-WAN، يمكنك إستخدام التقاط الحزم المضمن (EPC) بدلا من TCPDUMP.

أمثلة TCPDUMP

حزمة UDP العامة للإصغاء:

TCPDUMP vpn 0 options "-vvv -nnn udp"



ملاحظة: يمكن تطبيق هذه الإجراءات على البروتوكولات الأخرى أيضا... على سبيل المثال.: ICMP و ARP، إلخ

الاستماع لمنفذ محدد باستخدام ICMP و UDP:
خيارات Tcpdump VPN 0 interface ge0/4 "ICMP أو UDP"

الاستماع على رقم منفذ محدد (الاستماع على منفذ TLS):
بطاقة TCPDUMP vpn 0 interface ge0/4 options "-vvv -nn ميناء 23456"

الإصغاء على رقم منفذ محدد (الإصغاء على منفذ DTLS):
بطاقة TCPDUMP vpn 0 interface ge0/4 options "-vvv -nn ميناء 12346"

الاستماع لمضيف معين (إلى/من ذلك المضيف): -e طباعة رأس مستوى الارتباط
Tcpdump vpn 0 interface ge0/4 خيارات "المضيف 64.100.103.2 -vvv -nn -e"

الاستماع إلى مضيف معين باستخدام ICMP فقط
خيارات واجهة Tcpdump vpn 0 ge0/4 "المضيف 64.100.103.2 & icmp"

التصفية حسب المصدر و/أو الوجهة
خيارات Tcpdump vpn 0 interface ge0/4 "src 64.100.103.2 & dst 64.100.100.75"

التصفية على حركة مرور GRE المغلفة
خيارات Tcpdump VPN 0 interface ge0/4 "-v -n proto 47 "

المستندات ذات الصلة

- أستكشاف أخطاء إتصالات التحكم في SD-WAN وإصلاحها
- تقنية SD-WAN من Cisco: المشتبه بهم المعتادين
- صفحة رجل Tcpdump

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).