أستكشاف أخطاء إتصالات مستوى البيانات وكشف إعادة التوجيه ثنائي الإتجاه ل vEdge وإصلاحها

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات مستوى التحكم
التحقق من الخصائص المحلية لعنصر التحكم
فحص اتصالات التحكم
بروتوكول إدارة التراكب
التحقق من الإعلان عن وحدات التحكم في الوصول إلى الإنترنت (OMP) من خلال vEdges
التحقق من أن vSmart يستلم ويعلن عن وحدات التحكم في الوصول إلى النقل (TLOCs)
اكتشاف إعادة التوجيه ثنائي الاتجاه
أمر جلسة bfd لعرض المفهوم
الأمر لنفق عرض تايئاصحإ
قائمة الوصول
ترجمة عنوان الشبكة
كيفية استخدام أدوات stun-client لاكتشاف خرائط NAT لمواءمة التصفية.
أنواع NAT المدعومة لأنفاق مستوى البيانات "الإرسال" المستخدمة في CLI
جدران الحماية
الأمان
مشاكل ISP مع حركة مرور البيانات التي تم وضع علامة DSCP عليها
Debug BFD
إستخدام تتبع الحزمة لالتقاط حزم BFD (20.5 والإصدارات الأحدث)
معلومات ذات صلة

المقدمة

يصف هذا المستند مشاكل اتصال مستوى بيانات vEdge بعد اتصال مستوى تحكم ولكن لا يوجد اتصال مستوى بيانات بين المواقع.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة **Cisco Software Defined Wide Area Network (SDWAN)** الحل.

المكونات المستخدمة

هذه الوثيقة ليست مقيدة بإصدارات برامج ومكونات مادية معينة. يركز هذه المستند على أنظمة vEdge الأساسية.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.
لموجهات Cisco Edge (موجهات Cisco IOS® XE في وضع وحدة التحكم)، يرجى القراءة .

معلومات مستوى التحكم

التحقق من الخصائص المحلية لعنصر التحكم

للتحقق من حالة Wide Area Network (WAN) الواجهات على vEdge، أستخدم الأمر show control local-properties wan-interface-list.

في هذا الإخراج، يمكن رؤية RFC 4787 Network Address Translation (NAT) Type.

عندما يكون vEdge خلف جهاز NAT (جدار الحماية، الموجه، وما إلى ذلك)، وعنوان IPv4 العام والخاص، يتم إستخدام User Datagram Protocol (UDP) منافذ المصدر العامة والخاصة لإنشاء أنفاق مستوى البيانات.

يمكن أيضا العثور على حالة واجهة النفق ولون الحد الأقصى لعدد إتصالات التحكم التي تم تكوينها.

```
vEdge1# show control local-properties wan-interface-list

 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Requires minimum two vbonds to learn the NAT type

           PUBLIC          PUBLIC PRIVATE         PRIVATE          PRIVATE                          MAX
INTERFACE  IPv4            PORT   IPv4            IPv6             PORT    VS/VM COLOR        STATE CNTL

-------------------------------------------------------------------------------------------------------
ge0/0      203.0.113.225   4501   10.19.145.2     ::               12386    1/1  gold           up    2
ge0/1      10.20.67.10     12426  10.20.67.10     ::               12426    0/0  mpls           up    2
```

باستخدام هذه البيانات، يمكنك تحديد معلومات معينة حول كيفية إنشاء أنفاق البيانات وما المنافذ التي يمكنك توقعها (من منظور الموجهات) للاستخدام عند تكوين أنفاق البيانات.

فحص إتصالات التحكم

من المهم التأكد من أن اللون الذي ال يشكل أنفاق مستوى البيانات لديه اتصال تحكم تم إنشاؤه مع وحدات التحكم في التغشية.

والإ، فلن يقوم vEdge بإرسال **Transport Locator (TLOC)** المعلومات إلى برنامج vSmart عبر **Overlay Management Protocol (OMP)**.

يمكنك التحقق مما إذا كان قيد التشغيل باستخدام **show control connections** الأمر، والبحث عن **connect** الحالة.

```
vEdge1# show control connections
                                                                                PEER
PEER    PEER PEER            SITE       DOMAIN PEER                            PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                      PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vsmart  dtls 10.1.0.3         3          1      203.0.113.13                   12446 203.0.113.1
vbond   dtls -                0          0      203.0.113.12                   12346 203.0.113.1
vmanage dtls 10.1.0.1         1          0      203.0.113.14                   12646 203.0.113.1
```

إذا حاولت الواجهة (التي ال تشكل أنفاق بيانات) االتصال، فقم بحلها من خالل بدء انجح االتصاالت التحكم عبر هذا اللون.

أو، قم بتعيين **max-control-connections 0** الواجهة المحددة تحت قسم واجهة النفق.

```
vpn 0
 interface ge0/1
  ip address 10.20.67.10/24
  tunnel-interface
   encapsulation ipsec
   color mpls restrict
   max-control-connections 0
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
  !
  no shutdown
 !
```

ملاحظة: في بعض الأحيان، يمكنك إستخدام الأمر **no control-connections** لتحقيق نفس الهدف. ومع ذلك، ال يوقف هذا الأمر بإنشاء الحد الأقصى لعدد إتصالات التحكم. تم إهمال هذا الأمر من الإصدار 15.4 والي تم إستخدامه على البرامج الأحدث.

بروتوكول إدارة التراكب

التحقق من الإعلان عن وحدات التحكم في الوصول إلى الإنترنت (OMP) من خالل

vEdges

ال يمكن إرسال قوائم التحكم في الوصول إلى البنية الأساسية (OMP) لأن الواجهة تحاول تكوين إتصالات التحكم عبر هذا اللون ولا يمكنها الوصول إلى وحدات التحكم.

تحقق مما إذا كان اللون (الذي تقوم أنفاق البيانات به) يرسل وحدة التحكم في الوصول إلى النقل (TLOC) لهذا اللون المعين إلى vSmart.

أستخدم الأمر للتحقق **show omp tlocs advertised** من قوائم التحكم في الوصول (TLOCs) التي يتم إرسالها إلى أقران بروتوكول OMP.

مثال: الألوان **mpls** و **gold**. لم يتم إرسال أي TLOC إلى vSmart لأجهزة MPLS الملونة.

```
vEdge1# show omp tlocs advertised
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Stg -> staged
Inv -> invalid
```

```
ADDRESS                                                                    PSEUDO                    P
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        P
-----------------------------------------------------------------------------------------------------------
ipv4     10.1.0.5         gold             ipsec  0.0.0.0          C,Red,R   1       203.0.113.225    4
         10.1.0.2         mpls             ipsec  10.1.0.3          C,I,R     1       10.20.67.20
         10.1.0.2         blue             ipsec  10.1.0.3          C,I,R     1       198.51.100.187
         10.1.0.30         mpls             ipsec  10.1.0.3          C,I,R     1       10.20.67.30
         10.1.0.30         gold             ipsec  10.1.0.3          C,I,R     1       192.0.2.129
         10.1.0.4         mpls             ipsec  10.1.0.3          C,I,R     1       10.20.67.40
         10.1.0.4         gold             ipsec  10.1.0.3          C,I,R     1       203.0.113.226
```

مثال: الألوان **mpls** و **gold**. يتم إرسال TLOC لكل من الألوان.

```
vEdge2# show omp tlocs advertised
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Stg -> staged
Inv -> invalid
```

```
ADDRESS                                                                                  PSEUDO                    PU
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP         PO
-----------------------------------------------------------------------------------------------------------------------
ipv4     10.1.0.5         gold             ipsec  10.1.0.3          C,I,R     1       203.0.113.225    4
         10.1.0.2         mpls             ipsec  0.0.0.0          C,Red,R   1       10.20.67.20      1
         10.1.0.2         blue             ipsec  0.0.0.0          C,Red,R   1       198.51.100.187   1
         10.1.0.30         mpls             ipsec  10.1.0.3          C,I,R     1       10.20.67.30
         10.1.0.30         gold             ipsec  10.1.0.3          C,I,R     1       192.0.2.129
         10.1.0.4         mpls             ipsec  10.1.0.3          C,I,R     1       10.20.67.40
         10.1.0.4         gold             ipsec  10.1.0.3          C,I,R     1       203.0.113.226
```

✎ ملاحظة: بالنسبة لأي معلومات مستوى تحكم تم إنشاؤها محليا، يتم تعيين الحقل**FROM PEER**" على 0.0.0.0. عند البحث عن المعلومات التي تم إنشاؤها محليا، تأكد من المطابقة استنادا إلى هذه القيمة.

التحقق من أن vSmart يستلم ويعلن عن وحدات التحكم في الوصول إلى النقل (TLOCs)

يتم الآن الإعلان عن قوائم التحكم في الوصول إلى النقل (TLOC) لشركة vSmart. تأكد من أنه يتلقى عناوين TLOC من النظير الصحيح وأعلن عنها إلى vEdge الآخر.

مثال: يستلم vSmart قوائم التحكم في الوصول إلى النقل من 10.1.0.2 vEdge1.

<#root>

```
vSmart1# show omp tlocs received

C   -> chosen
I   -> installed

Red -> redistributed
Rej -> rejected
L   -> looped

R   -> resolved

S   -> stale
Ext -> extranet
Stg -> staged
Inv -> invalid
```

```
ADDRESS                                                                                  PSEUDO                    PU
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP         PO
-----------------------------------------------------------------------------------------------------------------------
ipv4     10.1.0.5         gold             ipsec  10.1.0.5          C,I,R     1       203.0.113.225   450

         10.1.0.2         mpls             ipsec  10.1.0.2          C,I,R     1       10.20.67.20      12


         10.1.0.2         blue             ipsec  10.1.0.2          C,I,R     1       198.51.100.187   12


         10.1.0.30        mpls             ipsec  10.1.0.30         C,I,R     1       10.20.67.30
         10.1.0.30        gold             ipsec  10.1.0.30         C,I,R     1       192.0.2.129
```

```
        10.1.0.4        mpls            ipsec  10.1.0.4        C,I,R     1       10.20.67.40      1
        10.1.0.4        gold            ipsec  10.1.0.4        C,I,R     1       203.0.113.226    1
```

إذا لم ترى TLOCs أو ترى أي رموز أخرى هنا، تحقق من هذه:

<#root>

```
vSmart-vIPtela-MEX# show omp tlocs received

C   -> chosen

I   -> installed

Red -> redistributed

Rej -> rejected

L   -> looped

R   -> resolved

S   -> stale
Ext -> extranet
Stg -> staged

Inv -> invalid
```

```
ADDRESS                                                                  PSEUDO                  P
FAMILY   TLOC IP         COLOR           ENCAP  FROM PEER       STATUS    KEY     PUBLIC IP       P
-----------------------------------------------------------------------------------------------------
ipv4     10.1.0.5        gold            ipsec  10.1.0.5        C,I,R     1       203.0.113.225    4

         10.1.0.2        mpls            ipsec  10.1.0.2        C,I,R     1       10.20.67.20      12


         10.1.0.2        blue            ipsec  10.1.0.2        Rej,R,Inv 1       198.51.100.187   12


         10.1.0.30        mpls            ipsec  10.1.0.30        C,I,R     1       10.20.67.30
         10.1.0.30        gold            ipsec  10.1.0.30        C,I,R     1       192.0.2.129
         10.1.0.4        mpls            ipsec  10.1.0.4        C,I,R     1       10.20.67.40      1
         10.1.0.4        gold            ipsec  10.1.0.4        C,I,R     1       203.0.113.226    1
```

تحقق من عدم وجود نهج يقوم بحظر TLOCs.

show run policy control-policy - ابحث عن أي قائمة تلوc ترفض أدوات التحكم في الوصول (TLOCs) الخاصة بك **advertised** كما هو **received** في تقنية vSmart.

<#root>

```
vSmart1(config-policy)# sh config
policy
 lists
```

```
  tloc-list SITE20

   tloc 10.1.0.2 color blue encap ipsec

  !
 !
 control-policy SDWAN

  sequence 10
   match tloc
    tloc-list SITE20
   !
   action reject ---->

here we are rejecting the TLOC 10.1.0.2,blue,ipsec
   !
  !
  default-action accept
 !
apply-policy
 site-list SITE20

  control-policy SDWAN in ----->

the policy is applied to control traffic coming IN the vSmart, it will filter the tlocs before adding i
```

✎ ملاحظة: إذا كان أحد أدوات التحكم في الوصول إلى البنية الأساسية (TLOC) **Rejected** أو **Invalid**الـ يتم الإعلان عنه للحواف الظاهرية الأخرى.

تأكد من أن السياسة ال تقوم بتصفية TLOC عند الإعلان عنه من vSmart. يمكنك أن ترى أن TLOC تم إستلامه على vSmart، ولكن ال يمكنك رؤيته على vEdge الأخرى.

مثال 1: vSmart مع TLOC في C،I،R.

<#root>

```
vSmart1# show omp tlocs

C   -> chosen
I   -> installed

Red -> redistributed
Rej -> rejected
L   -> looped

R   -> resolved

S   -> stale
Ext -> extranet
Stg -> staged
Inv -> invalid


ADDRESS                                                                    PSEUDO                    P
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        P
-----------------------------------------------------------------------------------------------------------
ipv4     10.1.0.5         mpls             ipsec  10.1.0.5         C,I,R     1       10.20.67.10      1
         10.1.0.5         gold             ipsec  10.1.0.5         C,I,R     1       203.0.113.225    4
```

```
 10.1.0.2         mpls             ipsec  10.1.0.2         C,I,R     1       10.20.67.20      12386   10
         10.1.0.2         blue             ipsec  10.1.0.2         C,I,R     1       198.51.100.187   12


         10.1.0.30         mpls             ipsec  10.1.0.30         C,I,R     1       10.20.67.30
         10.1.0.30         gold             ipsec  10.1.0.30         C,I,R     1       192.0.2.129
         10.1.0.4         mpls             ipsec  10.1.0.4         C,I,R     1       10.20.67.40      1
         10.1.0.4         gold             ipsec  10.1.0.4         C,I,R     1       203.0.113.226    1
```

مثال 2: ال يقوم vEdge1 برؤية TLOC من اللون الأزرق الذي يأتي من vEdge2. إنه ال يرى سوى MPLS TLOC.

<#root>

```
vEdge1# show omp tlocs
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Stg -> staged
Inv -> invalid


ADDRESS                                                                    PSEUDO                    P
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        P
-----------------------------------------------------------------------------------------------------------
ipv4     10.1.0.5         mpls             ipsec  0.0.0.0          C,Red,R   1       10.20.67.10      1
         10.1.0.5         gold             ipsec  0.0.0.0          C,Red,R   1       203.0.113.225    4

         10.1.0.2         mpls             ipsec  10.1.0.3          C,I,R     1       10.20.67.20      1


         10.1.0.30         mpls             ipsec  10.1.0.3          C,I,R     1       10.20.67.30
         10.1.0.30         gold             ipsec  10.1.0.3          C,I,R     1       192.0.2.129
         10.1.0.4         mpls             ipsec  10.1.0.3          C,I,R     1       10.20.67.40      1
         10.1.0.4         gold             ipsec  10.1.0.3          C,I,R     1       203.0.113.226    1
```

عندما تقوم بالتحقق من النهج، يمكنك ملاحظة سبب عدم ظهور TLOC على vEdge1.

<#root>

```
vSmart1# show running-config policy
policy
 lists
  tloc-list SITE20

   tloc 10.1.0.2 color blue encap ipsec

  !
  site-list SITE10
   site-id 10
  !
```

```
 !
 control-policy SDWAN
  sequence 10
   match tloc

    tloc-list SITE20

   !
   action reject
   !
  !
  default-action accept
 !
apply-policy
 site-list SITE10

  control-policy SDWAN out


 !
!
```

اكتشاف إعادة التوجيه ثنائي الإتجاه

يفهم العرض bfd جلسة أمر

هذه هي الأشياء الأساسية التي يتعين علينا أن نبحث عنها في الناتج:

<#root>

```
vEdge-2# show bfd sessions
                                        SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID  STATE        COLOR            COLOR            SOURCE IP
-----------------------------------------------------------------------------------------------------------

10.1.0.5         10       down         blue             gold             10.19.146.2


10.1.0.30         30       up           blue             gold             10.19.146.2
10.1.0.4         40       up           blue             gold             10.19.146.2

10.1.0.4         40       up           mpls             mpls             10.20.67.10
```

- **SYSTEM IP**: نظام النظراء-ip
- **SOURCE and REMOTE TLOC COLOR**: هذا مفيد أن يعرف ما TLOC يتوقع أن يستلم ويرسل.
- **SOURCE IP**: وه **private** مصدر ip. إن يكون أنت وراء NAT، هذا معلومة عرض هنا (وه يستطيع كنت رأيت مع الإستعمالمن **show control local-properties**
  < trong=""><>).
  - **DST PUBLIC IP**: إنه الوجهة التي يستخدمها VEdge لتكوين **Data Plane** النفق، سواء كان وراء NAT أم ال. (مثال: الحواف المتصلة مباشرة بالإنترنت، أو **Multi-Protocol Label Switching**

(MPLS) الرواطب)

- **DST PUBLIC PORT** منفذ NAT-ed عام يستخدمه vEdge لتكوين **Data Plane** النفق إلى vEdge البعيد.
- **TRANSITIONS**: عدد مرات تغيير جلسة عمل BFD حالتها، من **NA** إلى **UP** والعكس.

إحصائيات عرض النفق للأمر

يمكن أن **show tunnel statistics** يعرض المعلومات حول أنفاق مستوى البيانات. يمكنك تحديد ما إذا كنت ترسل أو تستلم حزم لنفق IPSec معين بين vEdges.

يمكن أن يساعدك ذلك على فهم ما إذا كانت الحزم تصل إلى كل نهاية، وعزل مشاكل الاتصال بين العقد.

في المثال، عندما توقف بتشغيل الأمر عدة مرات، يمكنك ملاحظة زيادة أو ال زيادة في **tx-pkts** أو **rx-pkts**.

تلميح: إذا كان العداد الخاص بك لزيادة tx-pkts، فإنك تنقل البيانات إلى النظير. إذا لم يتزايد RX-PKTS، فهذا يعني أنه ال يتم تلقي البيانات من النظير. في هذه الحدث، تحقق من الطرف الآخر وتأكد من زيادة tx-pkts.

<#root>

```
vEdge2# show tunnel statistics

TUNNEL                                    SOURCE  DEST                                                        T
PROTOCOL  SOURCE IP      DEST IP          PORT    PORT   SYSTEM IP    LOCAL COLOR      REMOTE COLOR     M
-----------------------------------------------------------------------------------------------------------

ipsec     172.16.16.147  10.88.244.181    12386   12406  10.1.0.5     public-internet  default          1


ipsec     172.16.16.147  10.152.201.104   12386   63364  10.1.0.0  public-internet  default          1441
ipsec     172.16.16.147  10.152.204.31    12386   58851  10.1.0.7     public-internet  public-internet  1
ipsec     172.24.90.129  10.88.244.181    12426   12406  10.1.0.5     biz-internet     default          1
ipsec     172.24.90.129  10.152.201.104   12426   63364  10.1.0.0  biz-internet     default          1441
ipsec     172.24.90.129  10.152.204.31    12426   58851  10.1.0.7     biz-internet     public-internet  1

TUNNEL                                    SOURCE  DEST                                                        T
PROTOCOL  SOURCE IP      DEST IP          PORT    PORT   SYSTEM IP    LOCAL COLOR      REMOTE COLOR     M
-----------------------------------------------------------------------------------------------------------

ipsec     172.16.16.147  10.88.244.181    12386   12406  10.1.0.5     public-internet  default          1


ipsec     172.16.16.147  10.152.201.104   12386   63364  10.1.0.0  public-internet  default          1441
ipsec     172.16.16.147  10.152.204.31    12386   58851  10.1.0.7     public-internet  public-internet  1
ipsec     172.24.90.129  10.88.244.181    12426   12406  10.1.0.5     biz-internet     default          1
ipsec     172.24.90.129  10.152.201.104   12426   63364  10.1.0.0  biz-internet     default          1441
ipsec     172.24.90.129  10.152.204.31    12426   58851  10.1.0.7     biz-internet     public-internet  1
```

أمر آخر مفيد هو **show tunnel statistics bfd** أن يستطيع كنت استعملت أن يفحص الرقم من BFD ربط يرسل ويستلم ضمن بيانات مستوى نفق خاص:

<#root>

```
vEdge1# show tunnel statistics bfd

                                                                                                               BFD   BFD
                                                                    BFD       BFD                              PMTU  PMT
TUNNEL                                      SOURCE    DEST    ECHO TX   ECHO RX   BFD ECHO     BFD ECHO     TX    RX
PROTOCOL  SOURCE IP      DEST IP           PORT      PORT    PKTS      PKTS      TX OCTETS    RX OCTETS    PKTS  PKT
---------------------------------------------------------------------------------------------------------------------------
ipsec     192.168.109.4  192.168.109.5  4500      4500    0         0         0            0            0     0
ipsec     192.168.109.4  192.168.109.5  12346     12366   1112255   1112253   186302716    186302381    487   487
ipsec     192.168.109.4  192.168.109.7  12346     12346   1112254   1112252   186302552    186302210    487   487
ipsec     192.168.109.4  192.168.110.5  12346     12366   1112255   1112253   186302716    186302381    487   487
```

قائمة الوصول

قائمة الوصول هي خطوة مفيدة وضرورية بعد أن تنظر إلى **show bfd sessions** المخرجات.

الآن بعد أن أصبحت بروتوكولات IP والمنافذ الخاصة والعامة معروفة، يمكنك إنشاء **Access Control List (ACL)** لمطابقة SRC_Port و DST_Port و SRC_IP و DST_IP.

يمكن أن يساعد ذلك في التحقق من رسائل BFD المرسلة والمستلمة.

هنا، يمكنك العثور على مثال لتكوين قائمة التحكم في الوصول (ACL):

<#root>

```
policy
 access-list checkbfd-out
  sequence 10
   match
    source-ip        192.168.0.92/32
    destination-ip   198.51.100.187/32
    source-port      12426
    destination-port 12426
   !
   action accept
    count bfd-out-to-dc1-from-br1
   !
  !
  default-action accept
 !
 access-list checkbfd-in
  sequence 20
   match
    source-ip        198.51.100.187/32
    destination-ip   192.168.0.92/32
    source-port      12426
    destination-port 12426
   !
```

```
   action accept
    count bfd-in-from-dc1-to-br1
   !
  !
  default-action accept
 !
vpn 0
 interface ge0/0
   access-list checkbfd-in in
   access-list checkbfd-out out
  !
 !
!
```

في المثال، تستخدم قائمة التحكم في الوصول (ACL) هذه تسلسلين. يتطابق التسلسل 10 مع رسائل BFD التي يتم إرسالها من هذا vEdge إلى النظير. التسلسل 20 يفعل العكس.

وهو يطابق ضد المصدر (**Private**) ميناء وغاية (**Public**) ميناء. إن يستعمل ال vEdge NAT، تضمن أن يفحص يمين مصدر وغاية ميناء.

للتحقق من نتائج كل عداد تسلسل، قم بإصدار **show policy access-list counters**

<#root>

```
vEdge1# show policy access-list-counters

NAME      COUNTER NAME               PACKETS  BYTES
-----------------------------------------------------
checkbfd  bfd-out-to-dc1-from-br1    10       2048
          bfd-in-from-dc1-to-br1        0        0
```

ترجمة عنوان الشبكة

كيفية إستخدام أدوات stun-client لاكتشاف خارئط NAT وعوامل التصفية.

إن كنت قد قمت بكل الخطوات وأنت خلف NAT، فإن الخطوة التالية هي تحديد **UDP NAT Traversal (RFC 4787) Map and Filter** السلوك.

تستخدم هذه الأداة لاكتشاف عنوان IP الخارجي المحلي vEdge عندما يكون vEdge هذا موجودا خلف جهاز nat.

يحصل هذا أمر ميناء خطط للجهاز ويكشف إختيارات خاصة حول ال NAT بين الأداة محلي وخادم (خادم عام: مثال: خادم جوجل الصعق).

ملاحظة: لمزيد من المعلومات التفصيلية، يرجى زيارة الموقع:

<#root>

```
vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 12386 --verbosity 2 stun
```

```
stunclient --mode full --localaddr 192.168.12.100 stun.l.google.com in VPN 0
Binding test: success
Local address: 192.168.12.100:12386
Mapped address: 203.0.113.225:4501
Behavior test: success
```

```
Nat behavior: Address Dependent Mapping
```

```
Filtering test: success
```

```
Nat filtering: Address and Port Dependent Filtering
```

في الإصدارات الأحدث من البرنامج، يمكن أن تختلف الصياغة قليلا:

<#root>

```
vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 --localport 12386 --verb
```

في هذا المثال، تم إجراء اختبار كشف NAT كامل باستخدام منفذ مصدر UDP 12386 إلى خادم Google STUN.

يمكن إخراج هذا الأمر سلوك NAT وعوامل تشويش NAT استنادا إلى RFC 4787.

ملاحظة: عند استخدام الأمر **tools stun**، تذكر السماح بحركة مرور STUN في واجهة النفق، وإلا فإنها لا تعمل. أستخدم **allow-service stun** للسماح بتمرير بيانات الصوت.

<#root>

```
vEdge1# show running-config vpn 0 interface ge0/0
vpn 0
 interface ge0/0
  ip address 10.19.145.2/30
  !
  tunnel-interface
   encapsulation ipsec
   color gold
   max-control-connections 1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   no allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf

   allow-service stun

  !
```

```
  no shutdown
 !
!
```

يوضح هذا التعيين بين مصطلحات STUN (NAT كامل المخروط) و RFC 4787 (سلوك NAT ل UDP).

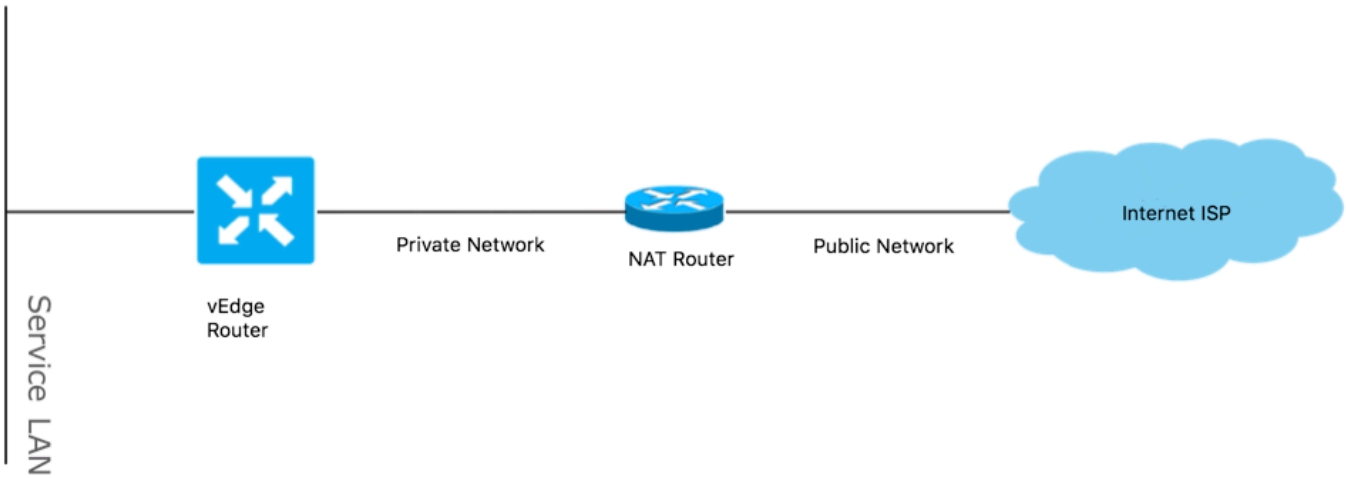
NAT Traversal Mapping Between used Viptela Terminologies		
STUN RFC 3489 Terminology	**RFC 4787 Terminology**	
	Mapping Behavior	**Filtering Behavior**
Full-cone NAT	Endpoint-Independent Mapping	Endpoint-Independent Filtering
Restricted Cone NAT	Endpoint-Independent Mapping	Address-Dependent Filtering
Port-Restricted Cone NAT	Endpoint-Independent Mapping	Address and Port-Dependent Filtering
Symmetric NAT	Address-and(or) Port-Dependent Mapping	Address-Dependent Filtering
		Address and Port-Dependent Filtering

أنواع NAT المدعومة لأنفاق مستوى البيانات "الإرسال" المستخدمة في CLI

في معظم الحالات، يمكن ربط أنواع الدعامة مثل biz-internet أو الدعامة-internet مباشرة بالإنترنت.

في حالات أخرى، هناك جهاز nat خلف واجهة vEdge WAN ومزود خدمة الإنترنت الفعلي.

بهذه الطريقة، يمكن أن يكون ل VEdge عنوان IP خاص ويمكن أن يكون الجهاز الآخر (الموجه، وجدار الحماية، وما إلى ذلك) هو الجهاز الذي يحمل عنواني IP الدعامة.



إن يتلقى أنت غير صحيح nat نوع، بعد ذلك وه أمكن كنت أحد أكثر الأسباب شيوعا أن ال يسمح تشكيل مستوى أنفاق. هذه هي أنواع NAT المدعومة.

NAT Traversal Support		
Source	**Destination**	**Supported (YES/NO)**
Full-Cone NAT	Full-cone NAT	Yes
Full-Cone NAT	Restricted Cone NAT	Yes
Full-Cone NAT	Port-Restricted Cone NAT	Yes
Full-Cone NAT	Symmetric NAT	Yes
Restricted Cone NAT	Full-cone NAT	Yes
Restricted Cone NAT	Restricted Cone NAT	Yes
Restricted Cone NAT	Port-Restricted Cone NAT	Yes
Restricted Cone NAT	Symmetric NAT	Yes
Port-Restricted Cone NAT	Full-cone NAT	Yes
Port-Restricted Cone NAT	Restricted Cone NAT	Yes
Port-Restricted Cone NAT	Port-Restricted Cone NAT	Yes
Port-Restricted Cone NAT	Symmetric NAT	**No**
Symmetric NAT	Full-cone NAT	Yes
Symmetric NAT	Restricted Cone NAT	yes
Symmetric NAT	Port-Restricted Cone NAT	**No**
Symmetric NAT	Symmetric NAT	**No**

جدران الحماية

إن يفحص أنت ال nat بالفعل وليس في ال غير مدعوم مصدر وغاية نوع، وه يمكن أن جدار حماية يمنع الميناء يستعمل أن يشكل **Data Plane** الأنفاق.

تأكد من فتح هذه المنافذ في جدار الحماية لاتصالات مستوى البيانات: **vEdge to vEdge Data Plane**:

UDP 12346 إلى 13156

لاتصالات التحكم من vEdge إلى وحدات التحكم:

UDP 12346 إلى 13156

بروتوكول TCP من 23456 إلى 24156

تأكد من فتح هذه المنافذ لتحقيق اتصال ناجح لأنفاق مستوى البيانات.

عندما تحقق من منافذ المصدر والوجهة المستخدمة لأنفاق مستوى البيانات، يمكنك إستخدام **show tunnel statistics** أو **show bfd sessions | tab** لكن ليس **show bfd sessions**.

وه ال يبدي أي مصدر ميناء، فقط غاية ميناء بما أن أنت يستطيع رأيت:

<#root>

```
vEdge1# show bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID  STATE       COLOR            COLOR           SOURCE IP
-----------------------------------------------------------------------------------------------------
192.168.30.105   50       up          biz-internet     biz-internet    192.168.109.181
192.168.30.105   50       up          private1         private1        192.168.110.181

vEdge1# show bfd sessions | tab
```

```
                                          SRC    DST                    SITE
SRC IP          DST IP          PROTO     PORT   PORT   SYSTEM IP       ID    LOCAL COLOR   COLOR
-------------------------------------------------------------------------------------------------
192.168.109.181 192.168.109.182 ipsec     12346  12346  192.168.30.105  50    biz-internet  biz-internet
192.168.110.181 192.168.110.182 ipsec     12346  12346  192.168.30.105  50    private1      private1
```

ملاحظة: يمكن العثور على مزيد من المعلومات حول منافذ جدار حماية SD-WAN المستخدمة هنا.

الأمان

إذا لاحظت أن عداد قائمة التحكم في الوصول (ACL) يزيد الوارد والصادر، فتحقق من العديد من التكرارات **show system statistics diff** and ensure there are no drops.

<#root>

```
vEdge1# show policy access-list-counters

NAME      COUNTER NAME               PACKETS  BYTES
-----------------------------------------------------

checkbfd  bfd-out-to-dc1-from-br1    55       9405



   bfd-in-from-dc1-to-br1     54      8478
```

في هذا الناتج، **rx_replay_integrity_drops** زيادة مع كل تكرار لـ **show system statistics diff** command.

<#root>

```
vEdge1#show system statistics diff

 rx_pkts : 5741427
 ip_fwd : 5952166
 ip_fwd_arp : 3
 ip_fwd_to_egress : 2965437
 ip_fwd_null_mcast_group : 26
 ip_fwd_null_nhop : 86846
 ip_fwd_to_cpu : 1413393
 ip_fwd_from_cpu_non_local : 15
 ip_fwd_rx_ipsec : 1586149
 ip_fwd_mcast_pkts : 26
 rx_bcast : 23957
 rx_mcast : 304
 rx_mcast_link_local : 240
 rx_implicit_acl_drops : 12832
 rx_ipsec_decap : 21
 rx_spi_ipsec_drops : 16
```

```
rx_replay_integrity_drops : 1586035


 port_disabled_rx : 2
 rx_invalid_qtags : 212700
 rx_non_ip_drops : 1038073
 pko_wred_drops : 3
 bfd_tx_record_changed : 23
 rx_arp_non_local_drops : 19893
 rx_arp_reqs : 294
 rx_arp_replies : 34330
 arp_add_fail : 263
 tx_pkts : 4565384
 tx_mcast : 34406
 port_disabled_tx : 3
 tx_ipsec_pkts : 1553753
 tx_ipsec_encap : 1553753
 tx_pre_ipsec_pkts : 1553753
 tx_pre_ipsec_encap : 1553753
 tx_arp_replies : 377
 tx_arp_reqs : 34337
 tx_arp_req_fail : 2
 bfd_tx_pkts : 1553675
 bfd_rx_pkts : 21
 bfd_tx_octets : 264373160
 bfd_rx_octets : 3600
 bfd_pmtu_tx_pkts : 78
 bfd_pmtu_tx_octets : 53052
 rx_icmp_echo_requests : 48
 rx_icmp_network_unreach : 75465
 rx_icmp_other_types : 47
 tx_icmp_echo_requests : 49655
 tx_icmp_echo_replies : 48
 tx_icmp_network_unreach : 86849
 tx_icmp_other_types : 7
vEdge1# show system statistics diff

 rx_pkts : 151
 ip_fwd : 157
 ip_fwd_to_egress : 75
 ip_fwd_null_nhop : 3
 ip_fwd_to_cpu : 43
 ip_fwd_rx_ipsec : 41
 rx_bcast : 1


rx_replay_integrity_drops : 41


 rx_invalid_qtags : 7
 rx_non_ip_drops : 21
 rx_arp_non_local_drops : 2
 tx_pkts : 114
 tx_ipsec_pkts : 40
 tx_ipsec_encap : 40
 tx_pre_ipsec_pkts : 40
 tx_pre_ipsec_encap : 40
 tx_arp_reqs : 1
 bfd_tx_pkts : 40
 bfd_tx_octets : 6800
 tx_icmp_echo_requests : 1
vEdge1# show system statistics diff
```

```
 rx_pkts : 126
 ip_fwd : 125
 ip_fwd_to_egress : 58
 ip_fwd_null_nhop : 3
 ip_fwd_to_cpu : 33
 ip_fwd_rx_ipsec : 36
 rx_bcast : 1
 rx_implicit_acl_drops : 1


rx_replay_integrity_drops : 35


 rx_invalid_qtags : 6
 rx_non_ip_drops : 22
 rx_arp_replies : 1
 tx_pkts : 97
 tx_mcast : 1
 tx_ipsec_pkts : 31
 tx_ipsec_encap : 31
 tx_pre_ipsec_pkts : 31
 tx_pre_ipsec_encap : 31
 bfd_tx_pkts : 32
 bfd_tx_octets : 5442
 rx_icmp_network_unreach : 3
 tx_icmp_echo_requests : 1
 tx_icmp_network_unreach : 3
vEdge1# show system statistics diff

 rx_pkts : 82
 ip_fwd : 89
 ip_fwd_to_egress : 45
 ip_fwd_null_nhop : 3
 ip_fwd_to_cpu : 24
 ip_fwd_rx_ipsec : 22
 rx_bcast : 1
 rx_implicit_acl_drops : 1


rx_replay_integrity_drops : 24


 rx_invalid_qtags : 2
 rx_non_ip_drops : 14
 rx_arp_replies : 1
 tx_pkts : 62
 tx_mcast : 1
 tx_ipsec_pkts : 24
 tx_ipsec_encap : 24
 tx_pre_ipsec_pkts : 24
 tx_pre_ipsec_encap : 24
 tx_arp_reqs : 1
 bfd_tx_pkts : 23
 bfd_tx_octets : 3908
 rx_icmp_network_unreach : 3
 tx_icmp_echo_requests : 1
 tx_icmp_network_unreach : 3
vEdge1# show system statistics diff

 rx_pkts : 80
 ip_fwd : 84
 ip_fwd_to_egress : 39
 ip_fwd_to_cpu : 20
```

```
 ip_fwd_rx_ipsec : 24


rx_replay_integrity_drops : 22


 rx_invalid_qtags : 3
 rx_non_ip_drops : 12
 tx_pkts : 66
 tx_ipsec_pkts : 21
 tx_ipsec_encap : 21
 tx_pre_ipsec_pkts : 21
 tx_pre_ipsec_encap : 21
 bfd_tx_pkts : 21
 bfd_tx_octets : 3571
```

أولا، قم بتنفيذ **request security ipsec-rekey** a على vEdge. بعد ذلك، مر بعدة تكرارات **show system statistics** وانظر إذا كنت لا تزال ترى **rx_replay_integrity_drops**.

إذا قمت بذلك، فتحقق من تكوين الأمان الخاص بك.

<#root>

```
vEdge1# show running-config security
security
 ipsec
 authentication-type sha1-hmac ah-sha1-hmac
 !
!
```

مشاكل ISP مع حركة مرور البيانات التي تم وضع علامة DSCP عليها

بشكل افتراضي، تنتقل جميع حركات مرور بيانات التحكم والإدارة من موجه vEdge إلى وحدات التحكم عبر إتصالات DTLS أو TLS وتم وضع علامة عليها بقيمة DSCP من CS6 (48 رقما عشريا).

لحركة مرور أنفاق مكان البيانات، تستخدم موجهات vEdge تضمين IPsec أو GRE لإرسال حركة مرور البيانات إلى بعضها البعض.

لاكتشاف فشل مستوى البيانات وقياس الأداء، تقوم الموجهات بشكل دوري بإرسال حزم BFD بعضها البعض.

يتم أيضا تمييز حزم BFD هذه بقيمة DSCP من CS6 (48 رقما عشريا).

من منظور ISP، يتم ملاحظة إذا النوع من حركة المرور على أنه حركة مرور UDP مع DSCP ذات قيمة CS6 وذلك لأن موجهات vEdge ووحدات التحكم في SD-WAN تنسخ بروتوكول DSCP

الذي يقوم بعلامات إلى رأس IP الخارجي بشكل افتراضي.

فيما يلي كيف يمكن أن يبدو الأمر إذا كانت tcpdump تعمل على موجه ISP العابرة:

<#root>

```
14:27:15.993766 IP (tos 0xc0, ttl 64, id 44063, offset 0, flags [DF], proto UDP (17), length 168)
    192.168.109.5.12366 > 192.168.20.2.12346: [udp sum ok] UDP, length 140
14:27:16.014900 IP (tos 0xc0, ttl 63, id 587, offset 0, flags [DF], proto UDP (17), length 139)
    192.168.20.2.12346 > 192.168.109.5.12366: [udp sum ok] UDP, length 111
14:27:16.534117 IP (tos 0xc0, ttl 63, id 0, offset 0, flags [DF], proto UDP (17), length 157)
    192.168.109.5.12366 > 192.168.110.6.12346: [no cksum] UDP, length 129
14:27:16.534289 IP (tos 0xc0, ttl 62, id 0, offset 0, flags [DF], proto UDP (17), length 150)
    192.168.110.6.12346 > 192.168.109.5.12366: [no cksum] UDP, length 122
```

كما يمكن رؤيته هنا، يتم وضع علامة على جميع الحزم ب TOS Byte 0xc0 المعروف أيضا باسم حقل DS (الذي يساوي الرقم العشري 192، أو 1100000 بالقيم الثنائية.

أول 6 وحدات بت عالية الترتيب تتوافق مع قيمة وحدات بت DSCP 48 في الرقم العشري أو CS6).

أول 2 ربط في الإنتاج يرادف إلى نفق مستوى تحكم و 2 أن يبقى، إلى مستوى معطيات نفق حركة مرور.

استنادا إلى طول الحزمة وعلامة TOS، فإنها يمكن أن تستنتج بثقة عالية أنها كانت حزم BFD (أتجاهات Rx و TX). يتم وضع علامة CS6 على هذه الحزم أيضا.

وفي بعض الأحيان يقوم بعض مزودي الخدمة (وخاصة مزودي خدمة VPN/MPLS L3 VPN/MPLS L2 VPN) بالحفاظ على مستويات مختلفة من مستوى الخدمة (SLA) ويمكنهم معالجة فئة مختلفة من حركة المرور استنادا إلى علامات DSCP بشكل مختلف.

على سبيل المثال، إذا كانت لديك خدمة فائقة لتحديد أولوية حركة مرور الصوت وإرسال الإشارات عبر بروتوكول DSCP EF و CS6.

بما أن أولوية حركة مرور يكون بشكل دائم تقريبا حددت، حتى إذا لم يتم تجاوز النطاق الترددي الإجمالي لارتباط ما، لهذا النوع من حركة مرور فقدان الحزمة يمكن رؤيتها، وبالتالي يمكن أن تكون جلسات BFD رفرفة أيضا.

وقد لوحظ في بعض الحالات أنه إذا تم تجويع قائمة انتظار الأولوية المخصصة على موجه مزود الخدمة، فلن ترى أي حالات سقوط لحركة المرور العادية (على سبيل المثال، عند تشغيل إختبار الاتصال البسيط من موجه vEdge).

وذلك لأنه يتم وضع علامة على حركة المرور هذه بقيمة DSCP الافتراضية 0 كما يمكن رؤيتها هنا (بايت TOS):

<#root>

```
15:49:22.268044 IP (tos 0x0, ttl 62, id 0, offset 0, flags [DF], proto UDP (17), length 142)
    192.168.110.5.12366 > 192.168.109.7.12346: [no cksum] UDP, length 114
```

```
15:49:22.272919 IP (tos 0x0, ttl 62, id 0, offset 0, flags [DF], proto UDP (17), length 142)
    192.168.110.5.12366 > 192.168.109.7.12346: [no cksum] UDP, length 114
15:49:22.277660 IP (tos 0x0, ttl 62, id 0, offset 0, flags [DF], proto UDP (17), length 142)
    192.168.110.5.12366 > 192.168.109.7.12346: [no cksum] UDP, length 114
15:49:22.314821 IP (tos 0x0, ttl 62, id 0, offset 0, flags [DF], proto UDP (17), length 142)
    192.168.110.5.12366 > 192.168.109.7.12346: [no cksum] UDP, length 114
```

ولكن في نفس الوقت، فإن جلسات BFD الخاصة بك ترفرف:

<#root>

```
show bfd history
                                                        DST PUBLIC       DST PUBLIC
SYSTEM IP        SITE ID  COLOR            STATE        IP               PORT        ENCAP  TIME
-------------------------------------------------------------------------------------------------------
192.168.30.4     13       public-internet  up           192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.4     13       public-internet  up           192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.4     13       public-internet  down         192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.4     13       public-internet  down         192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.4     13       public-internet  up           192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.4     13       public-internet  up           192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.4     13       public-internet  down         192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.4     13       public-internet  down         192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.4     13       public-internet  up           192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.6     13       public-internet  up           192.168.109.4    12346       ipsec  2019-05-01T03
192.168.30.6     13       public-internet  down         192.168.109.4    12346       ipsec  2019-05-01T03
```

وهنا يأتي التنقيط مفيد in order to تحريت:

<#root>

```
vedge2# tools nping vpn 0 options "--tos 0x0c --icmp --icmp-type echo --delay 200ms -c 100 -q" 192.168.1
Nping in VPN 0

Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2019-05-07 15:58 CEST
Max rtt: 200.305ms | Min rtt: 0.024ms | Avg rtt: 151.524ms
Raw packets sent: 100 (2.800KB) | Rcvd: 99 (4.554KB) | Lost: 1 (1.00%)
Nping done: 1 IP address pinged in 19.83 seconds
```

Debug BFD

إذا كان مطلوبا تحقيق أعمق، فقم بتشغيل تصحيح أخطاء BFD على موجه vEdge.

يعد مدير حركة مرور إعادة التوجيه (FTM) مسؤولا عن عمليات BFD على موجهات vEdge وبالتالي فأنت بحاجة إلى **debug ftm bfd.**

يتم تخزين جميع مخرجات تصحيح الأخطاء في **/var/log/tmplog/vdebug** ملف وإذا كنت تريد أن تكون

لديك هذه الرسائل على وحدة التحكم (مثل terminal monitor سلوك Cisco IOS)، فيمكنك إستخدام **monitor start /var/log/tmplog/vdebug.**

لإيقاف التسجيل، يمكنك إستخدام **monitor stop /var/log/tmplog/vdebug**

انه كيف ينظر الإنتاج لجلسة عمل BFD أن يذهب إلى أسفل بسبب المهلة (TLOC بعيد مع عنوان IP 192.168.110.6 لم يعد يمكن الوصول إليه):

<#root>

```
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1008]: BFD-session TNL 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_proc_tunnel_public_tloc_msg[252]: tun_rec_index
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_increment_wanif_bfd_flap[2427]: BFD-session TNL
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1119]: BFD-session TNL 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1140]: Attempting to add TLOC : from_tt
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]: (32771:
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]: (32770:
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD session c
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]: (32771:3277
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD session c
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]: (32770:3277
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session TNL 192.
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32771:32772) src 192.168.11
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session TNL 192.
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32770:32772) src 192.168.10
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1008]: BFD-session TNL 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_proc_tunnel_public_tloc_msg[252]: tun_rec_index
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_increment_wanif_bfd_flap[2427]: BFD-session TNL
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1119]: BFD-session TNL 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1140]: Attempting to add TLOC : from_tt
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]: (32771:
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]: (32770:
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD session c
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]: (32771:3277
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD session c
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]: (32770:3277
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session TNL 192.
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32771:32772) src 192.168.11
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session TNL 192.
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32770:32772) src 192.168.10
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_send_bfd_msg[499]: Sending BFD notification Down
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1140]: Attempting to add TLOC : from_tt
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]: (32771:
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]: (32770:
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1285]: UPDATE local tloc
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD session c
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]: (32771:3277
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD session c
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]: (32770:3277
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session TNL 192.
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32771:32772) src 192.168.11
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session TNL 192.
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32770:32772) src 192.168.10
log:local7.info: May  7 16:23:09 vedge2 FTMD[674]: %Viptela-vedge2-ftmd-6-INFO-1400002: Notification: 5/
log:local7.info: May  7 16:23:09 vedge2 FTMD[674]: %Viptela-vedge2-ftmd-6-INFO-1400002: Notification: 5/
```

تصحيح أخطاء آخر ذو قيمة للتمكين وه تصحيح أخطاء **Tunnel Traffic Manager (TTM)** الألحداث **debug ttm events**.

فيما يلي كيف يبدو **BFD DOWN** الحدث من منظور TTM:

<#root>

```
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM Msg LINK_E
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[413]:     Remote-TLOC: 192.16
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM Msg LINK_E
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[413]:     Remote-TLOC: 192.16
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM Msg BFD, C
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[402]:     TLOC: 192.168.30.6
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_af_tloc_db_bfd_status[234]:   BFD message: I SAY
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Sent TTM Msg TLOC_ADD,
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[213]:     TLOC: 192.168.30.6
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[217]:       Attributes: GROUP
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[220]:         Preference: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[223]:         Weight: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[226]:         Gen-ID: 2147483
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[229]:         Version: 2
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[232]:         Site-ID: 13
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[235]:         Carrier: 4
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[241]:         Restrict: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[249]:         Group: Count: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[262]:         Groups: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[269]:         TLOCv4-Public:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[273]:         TLOCv4-Private:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[277]:         TLOCv6-Public:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[281]:         TLOCv6-Private:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[285]:         TLOC-Encap: ips
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[295]:           Authenticatio
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[312]:           SPI 334, Flag
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[317]:           Number of pro
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[328]:           Number of enc
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:           Encrypt type|
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:           Encrypt type|
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[339]:           Number of int
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[344]:           integrity typ
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[349]:       #Paths: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Sent TTM Msg TLOC_ADD,
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[213]:     TLOC: 192.168.30.6
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[217]:       Attributes: GROUP
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[220]:         Preference: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[223]:         Weight: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[226]:         Gen-ID: 2147483
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[229]:         Version: 2
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[232]:         Site-ID: 13
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[235]:         Carrier: 4
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[241]:         Restrict: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[249]:         Group: Count: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[262]:         Groups: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[269]:         TLOCv4-Public:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[273]:         TLOCv4-Private:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[277]:         TLOCv6-Public:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[281]:         TLOCv6-Private:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[285]:         TLOC-Encap: ips
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[295]:           Authenticatio
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[312]:           SPI 334, Flag
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[317]:           Number of pro
```

```
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[328]:           Number of enc
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:           Encrypt type|
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:           Encrypt type|
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[339]:           Number of int
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[344]:           integrity typ
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[349]:       #Paths: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Sent TTM Msg TLOC_ADD,
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[213]:     TLOC: 192.168.30.6
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[217]:       Attributes: GROUP
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[220]:         Preference: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[223]:         Weight: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[226]:         Gen-ID: 2147483
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[229]:         Version: 2
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[232]:         Site-ID: 13
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[235]:         Carrier: 4
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[241]:         Restrict: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[249]:         Group: Count: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[262]:         Groups: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[269]:         TLOCv4-Public:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[273]:         TLOCv4-Private:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[277]:         TLOCv6-Public:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[281]:         TLOCv6-Private:
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[285]:         TLOC-Encap: ips
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[295]:           Authenticatio
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[312]:           SPI 334, Flag
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[317]:           Number of pro
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[328]:           Number of enc
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:           Encrypt type|
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:           Encrypt type|
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[339]:           Number of int
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[344]:           integrity typ
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[349]:       #Paths: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Sent TTM Msg DATA_DEVIC
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[431]:     Device: 192.168.30.
log:local7.info: May  7 16:58:19 vedge2 FTMD[674]: %Viptela-vedge2-ftmd-6-INFO-1400002: Notification: 5/
log:local7.info: May  7 16:58:20 vedge2 FTMD[674]: %Viptela-vedge2-ftmd-6-INFO-1400002: Notification: 5/
```

إستخدام تتبع الحزمة لالتقاط حزم BFD (20.5 والإصدارات الأحدث)

أداة مفيدة أخرى تم تقديمها في 20.5.1 والبرامج الأحدث هي تتبع الحزم ل vEdges.
لأن جلسة عمل BFD تستخدم نفس المنافذ القياسية، بشكل عام 12346، فإنه من السهل التصفية استنادا إلى عنوان IP النظير.

على سبيل المثال:

<#root>

```
vedge# show bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID  STATE       COLOR            COLOR           SOURCE IP
-------------------------------------------------------------------------------------------------
10.4.4.1         101      up          default          default         192.168.16.29
```

```
10.4.4.2        102      up          default          default          192.168.16.29
```

سيتم تكوين تتبع الحزمة:

vedge# debug packet-trace condition ingress-if ge0/0 vpn 0 source-ip 192.168.29.39
بدء حالة تتبع الحزم ل vedge#debug
vEdge# debug حالة تتبع الحزم

يمكن عرض النتائج باستخدام أوامر show المشار إليها أدناه. لحزم الدخول، هناك عالمة 'isBFD' والتي يتم تعيينها على '1' (صحيح) لحركة مرور BFD.

<#root>

```
vedge# show packet-trace statistics
packet-trace statistics 0
 source-ip             192.168.29.39
 source-port           12346
 destination-ip        192.168.16.29
 destination-port      12346
 source-interface      ge0_0
 destination-interface loop0.1
 decision              FORWARD
 duration              25
packet-trace statistics 1
 source-ip             192.168.29.39
 source-port           12346
 destination-ip        192.168.16.29
 destination-port      12346
 source-interface      ge0_0
 destination-interface loop0.1
 decision              FORWARD
 duration              14
packet-trace statistics 2
 source-ip             192.168.29.39
 source-port           12346
 destination-ip        192.168.16.29
 destination-port      12346
 source-interface      ge0_0
 destination-interface loop0.1
 decision              FORWARD
 duration              14

vedge# show packet-trace detail 0
================================================================================================================
Pkt-id           src_ip(ingress_if)            dest_ip(egress_if)           Duration           Decision
================================================================================================================
0         192.168.29.39:12346 (ge0_0)    192.168.16.29:12346 (loop0.1)        25 us              FORWARD
INGRESS_PKT:
00 50 56 84 79 be 00 50 56 84 3c b5 08 00 45 c0 00 96 ab 40 40 00 3f 11 e0 c1 c0 a8 1d 27 c0
a8 10 1d 30 3a 30 3a 00 82 00 00 a0 00 01 02 00 00 0e 3f 4b 65 07 bc 61 03 38 71 93 53 58
88 d8 08 41 95 7c 1a ff 8b cc b4 d0 d8 61 44 40 67 cc 1a 01 fd 1f c4 45 95 ea 7e 15 c9 08
2e b6 63 84 00
EGRESS_PKT:
a1 5e fe 11 00 00 00 00 00 00 00 00 00 04 00 0c 04 00 41 01 02 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 04 00 00 00 00 00 00 00 02 00 3a 30 3a 30 1d 10 a8 c0 00 00 00 00 00 00
00 00 00 00 00 00 01 00 00 00 27 1d a8 c0 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
a4 00 01 00 00
```

```
Feature Data
-----------------------------------
TOUCH : fp_proc_packet
core_id: 2
DSCP: 48
-----------------------------------
TOUCH : fp_proc_packet2
core_id: 2
DSCP: 48
-----------------------------------
TOUCH : fp_ip_forward
core_id: 2
DSCP: 48
-----------------------------------
TOUCH : fp_ipsec_decrypt
core_id: 2
DSCP: 48
-----------------------------------
FP_TRACE_FEAT_IPSEC_DATA:
src_ip : 192.168.29.39
src_port : 3784
dst_ip : 192.168.16.29
dst_port : 3784
isBFD : 1
core_id: 2
DSCP: 48
-----------------------------------
TOUCH : fp_send_pkt
core_id: 2
DSCP: 48
-----------------------------------
TOUCH : fp_hw_x86_pkt_free
core_id: 2
DSCP: 48
-----------------------------------
TOUCH : fp_proc_remote_bfd_
core_id: 2
DSCP: 48
-----------------------------------
TOUCH : BFD_ECHO_REPLY
core_id: 2
DSCP: 48
-----------------------------------
TOUCH : fp_hw_x86_pkt_free
core_id: 2
DSCP: 48
```

يتم التقاط حزم Egress BFD بطريقة مماثلة. تحدد هذه النتائج النوع المحدد، سواء طلب صدى أو رد.

vedge# debug packet-trace condition vpn 0 destination-ip 192.168.29.39
بدء حالة تتبع الحزم ل vedge#debug
vEdge# debug حالة تتبع الحزم

<#root>

```
vedge# show packet-trace statistics
```

```
packet-trace statistics 0
 source-ip             192.168.16.29
 source-port           3784
 destination-ip        192.168.29.39
 destination-port      3784
 source-interface      loop0.0
 destination-interface ge0_0
 decision              FORWARD
 duration              15
packet-trace statistics 1
 source-ip             192.168.16.29
 source-port           3784
 destination-ip        192.168.29.39
 destination-port      3784
 source-interface      loop0.0
 destination-interface ge0_0
 decision              FORWARD
 duration              66
packet-trace statistics 2
 source-ip             192.168.16.29
 source-port           3784
 destination-ip        192.168.29.39
 destination-port      3784
 source-interface      loop0.0
 destination-interface ge0_0
 decision              FORWARD
 duration              17

vedge# show packet-trace details 0
================================================================================================================
Pkt-id           src_ip(ingress_if)            dest_ip(egress_if)           Duration           Decision
================================================================================================================
0         192.168.16.29:3784 (loop0.0)   192.168.29.39:3784 (ge0_0)           15 us             FORWARD
INGRESS_PKT:
45 c0 00 4f 00 00 40 00 ff 11 cc 48 c0 a8 10 1d c0 a8 1d 27 0e c8 0e c8 00 3b 00 00 80 c0 07
00 00 00 00 01 00 00 00 01 00 0f 42 40 00 0f 42 40 00 0f 42 40 01 00 0c 01 00 00 1d 3b b1
c9 89 d7 03 00 0f c0 a8 10 1d 30 3a c0 a8 1d 27 30 3a a3 96 07 3b 47 1c 60 d1 d5 76 4c 72
78 1f 9a 0d 00
EGRESS_PKT:
00 50 56 84 3c b5 00 50 56 84 79 be 08 00 45 c0 00 96 ab 40 40 00 3f 11 e0 c1 c0 a8 10 1d c0
a8 1d 27 30 3a 30 3a 00 82 00 00 a0 00 01 01 00 00 5c 3d 88 9a c7 28 23 1b e6 18 ea fe 73
1b b9 e3 79 bf d9 f4 72 41 96 c1 47 07 44 56 77 5a a2 fb 43 59 c1 97 59 47 62 21 77 d4 f4
47 8b 30 b0 00
Feature Data
-----------------------------------
TOUCH : fp_send_bfd_pkt
core_id: 0
DSCP: 48
-----------------------------------
TOUCH : BFD_ECHO_REPLY
core_id: 0
DSCP: 48
-----------------------------------
TOUCH : fp_ipsec_loopback_f
core_id: 0
DSCP: 48
-----------------------------------
TOUCH : fp_send_pkt
core_id: 0
DSCP: 48
-----------------------------------
TOUCH : fp_ip_forward
```

```
core_id: 2
DSCP: 48
----------------------------------
TOUCH : fp_send_ip_packet
core_id: 2
DSCP: 48
----------------------------------
TOUCH : fp_send_pkt
core_id: 2
DSCP: 48
----------------------------------
TOUCH : fp_hw_x86_pkt_free
core_id: 2
DSCP: 48
vedge# show packet-trace details 1
================================================================================================================
Pkt-id           src_ip(ingress_if)            dest_ip(egress_if)           Duration           Decision
================================================================================================================
1         192.168.16.29:3784 (loop0.0)   192.168.29.39:3784 (ge0_0)           66 us              FORWARD
INGRESS_PKT:
45 c0 00 56 00 00 40 00 ff 11 cc 41 c0 a8 10 1d c0 a8 1d 27 0e c8 0e c8 00 42 00 00 80 c0 07
00 00 00 00 01 00 00 00 01 00 0f 42 40 00 0f 42 40 00 0f 42 40 01 00 0c 00 00 00 1d b8 35
a8 09 88 03 00 0f c0 a8 10 1d 30 3a c0 a8 1d 27 30 3a 04 00 07 01 00 05 a6 38 ff 7e 06 1e
da 23 19 d5 00
EGRESS_PKT:
00 50 56 84 3c b5 00 50 56 84 79 be 08 00 45 c0 00 9d ab 40 40 00 3f 11 e0 ba c0 a8 10 1d c0
a8 1d 27 30 3a 30 3a 00 89 00 00 a0 00 01 01 00 00 5c 3e 2d 3b 9e 81 aa 10 26 54 7f 47 5c
d8 81 4f 23 2e 3c 39 1e 94 b2 f4 fb a4 ba 98 54 73 99 8f 2e 95 d7 69 fb 91 41 96 93 03 5b
a4 e4 e8 82 00
Feature Data
----------------------------------
TOUCH : fp_send_bfd_pkt
core_id: 0
DSCP: 48
----------------------------------
TOUCH : BFD_ECHO_REQUEST
core_id: 0
DSCP: 48
----------------------------------
TOUCH : fp_ipsec_loopback_f
core_id: 0
DSCP: 48
----------------------------------
TOUCH : fp_send_pkt
core_id: 0
DSCP: 48
----------------------------------
TOUCH : fp_ip_forward
core_id: 2
DSCP: 48
----------------------------------
TOUCH : fp_send_ip_packet
core_id: 2
DSCP: 48
----------------------------------
TOUCH : fp_send_pkt
core_id: 2
DSCP: 48
----------------------------------
TOUCH : fp_hw_x86_pkt_free
core_id: 2
DSCP: 48
```

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

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).