排除双向转发检测和数据平面连接问题

目录

简介

本文档介绍在成功连接到控制平面但站点之间仍然没有数据平面连接后，vEdge路由器上可能出现的数据平面连接问题。

先决条件

要求

思科建议您了解思科软件定义广域网(SDWAN)解决方案。

使用的组件

本文档不限于特定的软件和硬件版本。

注意：本文档中显示的所有命令输出均来自vEdge路由器，但运行IOS®-XE SDWAN软件的路由器的故障排除方法将相同。使用**sdwan**关键字可在IOS®-XE SDWAN软件上获得相同的输出。例如： **show sdwan control connections而**不是**show control connections**。

控制平面信息

检查控制本地属性

要检查vEdge上广域网(WAN)接口的状态，请使用命令**show control local-properties wan-interface-list**。在此输出中，您可以看到RFC 4787网络地址转换(NAT)类型。当vEdge位于NAT设备（防火墙、路由器等）后面时，公有和私有IPv4地址、公有和私有源用户数据报协议(UDP)端口用于构建数据平面隧道。您还可以找到隧道接口的状态、颜色和配置的最大控制连接数。

```
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
           Note: Requires minimum two vbonds to learn the NAT type

           PUBLIC          PUBLIC PRIVATE         PRIVATE          PRIVATE
MAX   RESTRICT/           LAST        SPI TIME   NAT  VM
INTERFACE  IPv4            PORT   IPv4            IPv6             PORT    VS/VM COLOR
STATE CNTRL  CONTROL/   LR/LB   CONNECTION   REMAINING  TYPE CON

STUN                                           PRF
------------------------------------------------------------------------------------------------
---------------------------------------------------------------
ge0/0      203.0.113.225   4501   10.19.145.2     ::               12386    1/1  gold
up    2    no/yes/no   No/No  7:02:55:13   0:09:02:29  N    5
ge0/1      10.20.67.10     12426  10.20.67.10     ::               12426    0/0  mpls
up    2    yes/yes/no  No/No  0:00:00:01   0:11:40:16  N    5
```

通过此数据，您可以从路由器的角度确定有关必须如何构建数据隧道以及在形成数据隧道时应使用哪些端口的特定信息。

检查控制连接

必须确保不形成数据平面隧道的颜色确实与重叠中的控制器建立控制连接。否则，vEdge不会通过重叠管理协议(OMP)将传输定位器(TLOC)信息发送到vSmart。 使用show control connections命令可以确保它是否处于启**用状态**，并查找状态连**接**。

```
vEdge1# show control connections
                                                                                       PEER
PEER                                              CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                    PRIV
PEER                                    PUB                                               GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                              PORT
PUBLIC IP                               PORT  LOCAL COLOR     STATE           UPTIME      ID
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
--
vsmart  dtls 1.1.1.3         3          1      203.0.113.13                          12446
203.0.113.13                          12446 gold            up              7:03:18:31  0
```

```
vbond   dtls -               0          0      203.0.113.12                         12346
203.0.113.12                        12346 mpls            connect                     0
vmanage dtls 1.1.1.1         1          0      203.0.113.14                         12646
203.0.113.14                        12646 gold            up              7:03:18:31  0
```

如果未形成数据隧道的接口尝试连接，可以通过该颜色成功启动控制连接来解决该问题。或者，可以通过在隧道接口部分下的**选定接口中设**置max-control-connections 0来绕过它。

```
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
 !
```

> **注意：**有时，您可以使用命令**no control-connections**来实现相同的目标。但是，该命令不建立最大数量的控制连接。此命令从15.4开始弃用，不应用于较新的软件。

重叠管理协议

检查OMP TLOC是否从vEdge通告

正如您注意到的，在上一步中，无法发送OMP TLOC，因为接口尝试通过该颜色形成控制连接，并且无法到达控制器。因此，检查数据隧道无法工作或出现的颜色是否将该特定颜色的TLOC发送到vSmarts。使用命令**show omptlocs advertised**检查发送到OMP对等体的TLOC。

示例：颜色**mpls**和金**色**。不向vSmart发送TLOC for color mpls。

```
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


PUBLIC           PRIVATE
ADDRESS                                                                    PSEUDO
PUBLIC                   PRIVATE  PUBLIC  IPV6     PRIVATE  IPV6     BFD
```

```
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP
PORT    PRIVATE IP       PORT     IPV6    PORT    IPV6     PORT     STATUS
------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------
ipv4     1.1.1.10         gold             ipsec  0.0.0.0          C,Red,R   1
203.0.113.225    4501    10.19.145.2      12386    ::      0       ::       0       up
         1.1.1.20         mpls             ipsec  1.1.1.3          C,I,R     1       10.20.67.20
12386   10.20.67.20      12386    ::      0       ::       0        down
         1.1.1.20         blue             ipsec  1.1.1.3          C,I,R     1
198.51.100.187   12406   10.19.146.2      12406    ::      0       ::       0       up
         1.1.1.30         mpls             ipsec  1.1.1.3          C,I,R     1       10.20.67.30
12346   10.20.67.30      12346    ::      0       ::       0        down
         1.1.1.30         gold             ipsec  1.1.1.3          C,I,R     1       192.0.2.129
12386   192.0.2.129      12386    ::      0       ::       0        up
         1.1.1.40         mpls             ipsec  1.1.1.3          C,I,R     1       10.20.67.40
12426   10.20.67.40      12426    ::      0       ::       0        down
         1.1.1.40         gold             ipsec  1.1.1.3          C,I,R     1
203.0.113.226    12386   203.0.113.226    12386    ::      0       ::       0       up
```

示例：颜色mpls和金色。TLOC会针对这两种颜色发送。

```
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


PUBLIC           PRIVATE
ADDRESS                                                                      PSEUDO
PUBLIC                   PRIVATE  PUBLIC  IPV6    PRIVATE  IPV6     BFD
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP
PORT    PRIVATE IP       PORT     IPV6    PORT    IPV6     PORT     STATUS
------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------
ipv4     1.1.1.10         gold             ipsec  1.1.1.3          C,I,R     1
203.0.113.225    4501    10.19.145.2      12386    ::      0       ::       0       up
         1.1.1.20         mpls             ipsec  0.0.0.0          C,Red,R   1       10.20.67.20
12386   10.20.67.20      12386    ::      0       ::       0        up
         1.1.1.20         blue             ipsec  0.0.0.0          C,Red,R   1
198.51.100.187   12406   10.19.146.2      12406    ::      0       ::       0       up
         1.1.1.30         mpls             ipsec  1.1.1.3          C,I,R     1       10.20.67.30
12346   10.20.67.30      12346    ::      0       ::       0        up
         1.1.1.30         gold             ipsec  1.1.1.3          C,I,R     1       192.0.2.129
     12386   192.0.2.129      12386    ::      0       ::       0        up
         1.1.1.40         mpls             ipsec  1.1.1.3          C,I,R     1       10.20.67.40
12426   10.20.67.40      12426    ::      0       ::       0        up
         1.1.1.40         gold             ipsec  1.1.1.3          C,I,R     1
203.0.113.226    12386   203.0.113.226    12386    ::      0       ::       0       up
```

> **注意**：对于任何本地生成的控制平面信息，“FROM PEER”字段将设置为0.0.0.0。当您查找本地生成的信息时，请确保根据此值进行匹配。

检查vSmart是否接收并通告TLOC

现在您知道您的TLOC已通告到vSmart，请确认它从正确的对等体接收TLOC并将其通告给其他vEdge。

示例：vSmart从1.1.1.20 vEdge1接收TLOC。

```
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


PUBLIC           PRIVATE
ADDRESS                                                                      PSEUDO
PUBLIC                   PRIVATE  PUBLIC  IPV6    PRIVATE  IPV6     BFD
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP
PORT    PRIVATE IP       PORT     IPV6    PORT    IPV6     PORT     STATUS
------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------
ipv4     1.1.1.10         gold             ipsec  1.1.1.10         C,I,R     1
203.0.113.225  4501    10.19.145.2      12386    ::      0       ::       0        -
         1.1.1.20         mpls             ipsec  1.1.1.20         C,I,R     1       10.20.67.20
12386   10.20.67.20      12386    ::      0       ::       0        -
         1.1.1.20         blue             ipsec  1.1.1.20         C,I,R     1
198.51.100.187   12406   10.19.146.2      12406    ::      0       ::       0        -
         1.1.1.30         mpls             ipsec  1.1.1.30         C,I,R     1       10.20.67.30
12346   10.20.67.30      12346    ::      0       ::       0        -
         1.1.1.30         gold             ipsec  1.1.1.30         C,I,R     1       192.0.2.129
12386   192.0.2.129      12386    ::      0       ::       0        -
         1.1.1.40         mpls             ipsec  1.1.1.40         C,I,R     1       10.20.67.40
12426   10.20.67.40      12426    ::      0       ::       0        -
         1.1.1.40         gold             ipsec  1.1.1.40         C,I,R     1
203.0.113.226    12386   203.0.113.226    12386    ::      0       ::       0        -
```

如果您没有看到TLOC，或者您在此处看到任何其他代码，您可以检查以下代码：

```
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


PUBLIC           PRIVATE
ADDRESS                                                                      PSEUDO
PUBLIC                   PRIVATE  PUBLIC  IPV6    PRIVATE  IPV6     BFD
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP
PORT    PRIVATE IP       PORT     IPV6    PORT    IPV6     PORT     STATUS
------------------------------------------------------------------------------------------------
```

```
----------------------------------------------------------------------------------
ipv4     1.1.1.10         gold             ipsec  1.1.1.10         C,I,R     1
203.0.113.225    4501    10.19.145.2      12386    ::      0       ::       0        -
         1.1.1.20         mpls             ipsec  1.1.1.20         C,I,R     1       10.20.67.20
12386   10.20.67.20      12386    ::      0       ::       0        -
         1.1.1.20         blue             ipsec  1.1.1.20         Rej,R,Inv 1
198.51.100.187   12406   10.19.146.2      12406    ::      0       ::       0        -
         1.1.1.30         mpls             ipsec  1.1.1.30         C,I,R     1       10.20.67.30
12346   10.20.67.30      12346    ::      0       ::       0        -
         1.1.1.30         gold             ipsec  1.1.1.30         C,I,R     1       192.0.2.129
    12386   192.0.2.129      12386    ::      0       ::       0        -
         1.1.1.40         mpls             ipsec  1.1.1.40         C,I,R     1       10.20.67.40
12426   10.20.67.40      12426    ::      0       ::       0        -
         1.1.1.40         gold             ipsec  1.1.1.40         C,I,R     1
203.0.113.226    12386   203.0.113.226    12386    ::      0       ::       0        -
```

检查是否没有阻止TLOC的策略。

show run policy control-policy — 查找拒绝在vSmart中通告或接收TLOC的任何tloc列表。

```
vSmart1(config-policy)# sh config
policy
 lists
  tloc-list SITE20
   tloc 1.1.1.20 color blue encap ipsec
  !
 !
 control-policy SDWAN
  sequence 10
   match tloc
    tloc-list SITE20
   !
   action reject ----> here we are rejecting the TLOC 1.1.1.20,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 it to the OMP table.
```

注意：如果TLOC被拒绝或无效，则不会通告给其他vEdge。

确保从vSmart通告策略时不过滤TLOC。您可以看到TLOC在vSmart上收到，但在另一个vEdge上看不到。

示例 1：在C、I、R中使用TLOC的vSmart

```
vSmart1# show omp tlocs
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
```

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


PUBLIC           PRIVATE
ADDRESS                                                                      PSEUDO
PUBLIC                   PRIVATE  PUBLIC  IPV6    PRIVATE  IPV6     BFD
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP
PORT    PRIVATE IP       PORT     IPV6    PORT    IPV6     PORT     STATUS
------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------
ipv4     1.1.1.10         mpls             ipsec  1.1.1.10         C,I,R     1       10.20.67.10
12406   10.20.67.10      12406    ::      0       ::       0        -
         1.1.1.10         gold            ipsec   1.1.1.10         C,I,R     1
203.0.113.225    4501    10.19.145.2      12386    ::      0       ::       0        -
         1.1.1.20         mpls             ipsec  1.1.1.20         C,I,R     1       10.20.67.20
12386   10.20.67.20      12386    ::      0       ::       0        -
         1.1.1.20         blue             ipsec  1.1.1.20         C,I,R     1
198.51.100.187   12426   10.19.146.2      12426    ::      0       ::       0        -
         1.1.1.30         mpls             ipsec  1.1.1.30         C,I,R     1       10.20.67.30
12346   10.20.67.30      12346    ::      0       ::       0        -
         1.1.1.30         gold             ipsec  1.1.1.30         C,I,R     1       192.0.2.129
12386   192.0.2.129      12386    ::      0       ::       0        -
         1.1.1.40         mpls             ipsec  1.1.1.40         C,I,R     1       10.20.67.40
12426   10.20.67.40      12426    ::      0       ::       0        -
         1.1.1.40         gold             ipsec  1.1.1.40         C,I,R     1
203.0.113.226    12386   203.0.113.226    12386    ::      0       ::       0        -
```

示例 2：vEdge1看不到来自vEdge2的蓝色的TLOC。它只看到MPLS TLOC。

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


PUBLIC           PRIVATE
ADDRESS                                                                      PSEUDO
PUBLIC                   PRIVATE  PUBLIC  IPV6    PRIVATE  IPV6     BFD
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP
PORT    PRIVATE IP       PORT     IPV6    PORT    IPV6     PORT     STATUS
------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------
ipv4     1.1.1.10         mpls             ipsec  0.0.0.0          C,Red,R   1       10.20.67.10
12406   10.20.67.10      12406    ::      0       ::       0        up
         1.1.1.10         gold             ipsec  0.0.0.0          C,Red,R   1
203.0.113.225    4501    10.19.145.2      12386    ::      0       ::       0        up
         1.1.1.20         mpls             ipsec  1.1.1.3          C,I,R     1       10.20.67.20
12386   10.20.67.20      12386    ::      0       ::       0        up
         1.1.1.30         mpls             ipsec  1.1.1.3          C,I,R     1       10.20.67.30
12346   10.20.67.30      12346    ::      0       ::       0        up
         1.1.1.30         gold             ipsec  1.1.1.3          C,I,R     1       192.0.2.129
12386   192.0.2.129      12386    ::      0       ::       0        up
```

```
         1.1.1.40         mpls             ipsec  1.1.1.3          C,I,R     1       10.20.67.40
12426   10.20.67.40      12426    ::      0       ::       0        up
         1.1.1.40         gold             ipsec  1.1.1.3          C,I,R     1
203.0.113.226    12386   203.0.113.226    12386    ::      0       ::       0        up
```

当您检查策略时，您可以看到TLOC为何不出现在vEdge1上。

```
vSmart1# show running-config policy
policy
 lists
  tloc-list SITE20
   tloc 1.1.1.20 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
 !
!
```

双向转发检测

了解show bfd sessions命令

以下是输出中需要查找的关键内容：

```
vEdge-2# show bfd sessions
                                      SOURCE TLOC      REMOTE TLOC
DST PUBLIC                      DST PUBLIC         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR            SOURCE IP
IP                              PORT        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME
TRANSITIONS
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------
1.1.1.10         10       down        blue             gold             10.19.146.2
203.0.113.225                   4501        ipsec  7           1000           NA              7
1.1.1.30         30       up          blue             gold             10.19.146.2
192.0.2.129                     12386       ipsec  7           1000           0:00:00:22      2
1.1.1.40         40       up          blue             gold             10.19.146.2
203.0.113.226                   12386       ipsec  7           1000           0:00:00:22      1
1.1.1.40         40       up          mpls             mpls
10.20.67.10                     10.20.67.40                     12426       ipsec  7
1000           0:00:10:11      0
```

- **系统IP**:对等体系统IP

- **源和远程TLOC颜色**:这对于了解您希望接收和发送的TLOC非常有用。
- **源 IP：**它是私**有**源IP。如果您在NAT后面，则此信息不会显示在此处(使用**show control local-properties <wan-interface-list>可**以看到此信息，本文档开头对此进行了说明)。
- **DST公共IP**:vEdge正使用它来形成数据平面隧道，无论它是否在NAT后面。（示例：直接连接到互联网或多协议标签交换(MPLS)链路的vEdge
- **DST PUBLIC PORT:**vEdge用于形成到远程vEdge的数据平面隧道的公共NAT端口。
- **过渡**:BFD会话更改其状态的次数，从NA更改为UP，反之亦然。

命令show tunnel statistics

show tunnel statistics可显示有关数据平面隧道的信息，您可以轻松查看是在vEdge之间为特定IPSEC隧道发送还是接收数据包。这有助于您了解数据包是否在每一端生成，并隔离节点之间的连接问题。

在本例中，当您多次运行命令时，您会注意到tx-pkts或rx-pkts中**的增量**或**无增量**。

> **提示：**如果tx-pkts的计数器增加，则将数据传输到对等体。如果rx-pkts不增加，则表示您未从对等体接收数据。在此情况下，检查另一端并确认tx-pkts是否递增。

```
TCP
vEdge2# show tunnel statistics

TUNNEL SOURCE DEST TUNNEL MSS PROTOCOL SOURCE IP DEST IP PORT PORT SYSTEM IP LOCAL COLOR REMOTE
COLOR MTU tx-pkts tx-octets rx-pkts rx-octets ADJUST -----------------------------------------
-------------------------------------------------------------------------------------------------
-------------------- ipsec      172.16.16.147  10.88.244.181   12386   12406  1.1.1.10
public-internet  default          1441    38282    5904968    38276    6440071    1361
ipsec     172.16.16.147  10.152.201.104  12386   63364  100.1.1.100  public-internet  default
1441    33421    5158814    33416    5623178    1361
ipsec     172.16.16.147  10.152.204.31   12386   58851  1.1.1.90     public-internet  public-
internet  1441    12746    1975022    12744    2151926    1361
ipsec     172.24.90.129  10.88.244.181   12426   12406  1.1.1.10     biz-internet     default
1441    38293    5906238    38288    6454580    1361
ipsec     172.24.90.129  10.152.201.104  12426   63364  100.1.1.100  biz-internet     default
1441    33415    5157914    33404    5621168    1361
ipsec     172.24.90.129  10.152.204.31   12426   58851  1.1.1.90     biz-internet     public-
internet  1441    12750    1975622    12747    2152446    1361

TUNNEL                                  SOURCE
DEST
TUNNEL                                         MSS
PROTOCOL  SOURCE IP      DEST IP         PORT    PORT   SYSTEM IP    LOCAL COLOR      REMOTE
COLOR     MTU     tx-pkts  tx-octets  rx-pkts  rx-octets  ADJUST
-------------------------------------------------------------------------------------------------
---------------------------------------------------------------
ipsec     172.16.16.147  10.88.244.181   12386   12406  1.1.1.10     public-internet
default          1441    39028    6020779    39022    6566326    1361
ipsec     172.16.16.147  10.152.201.104  12386   63364  100.1.1.100  public-internet
default          1441    34167    5274625    34162    5749433    1361
ipsec     172.16.16.147  10.152.204.31   12386   58851  1.1.1.90     public-internet  public-
internet  1441    13489    2089069    13487    2276382    1361
ipsec     172.24.90.129  10.88.244.181   12426   12406  1.1.1.10     biz-internet
default          1441    39039    6022049    39034    6580835    1361
ipsec     172.24.90.129  10.152.201.104  12426   63364  100.1.1.100  biz-internet
default          1441    34161    5273725    34149    5747259    1361
```

```
ipsec     172.24.90.129  10.152.204.31   12426   58851  1.1.1.90     biz-internet     public-
internet  1441    13493    2089669    13490    2276902    1361
```

另一个有用的命**令是show tunnel statistics bfd，**可用于检查特定数据平面隧道中发送和接收的BFD数据包数：

```
vEdge1# show tunnel statistics bfd

BFD   BFD   BFD     BFD
                                                       BFD      BFD
PMTU  PMTU  PMTU    PMTU
TUNNEL                                  SOURCE  DEST   ECHO TX  ECHO RX  BFD ECHO   BFD ECHO
TX    RX    TX      RX
PROTOCOL  SOURCE IP      DEST IP        PORT    PORT   PKTS     PKTS     TX OCTETS  RX OCTETS
PKTS  PKTS  OCTETS  OCTETS
------------------------------------------------------------------------------------------------
---------------------------
ipsec     192.168.109.4  192.168.109.5  4500    4500   0        0        0          0          0
0     0       0
ipsec     192.168.109.4  192.168.109.5  12346   12366  1112255  1112253  186302716  186302381
487   487   395939  397783
ipsec     192.168.109.4  192.168.109.7  12346   12346  1112254  1112252  186302552  186302210
487   487   395939  397783
ipsec     192.168.109.4  192.168.110.5  12346   12366  1112255  1112253  186302716  186302381
487   487   395939  397783
```

访问列表

查看show bfd sessions输出后，访问列表是有用且必**要的**步骤。既然已知专用IP和公有IP和端口，您可以创建访问控制列表(ACL)，以与SRC_PORT、DST_PORT、SRC_IP、DST_IP匹配。这有助于您确认是否正在接收和发送BFD消息。

在此可以找到ACL配置的示例：

```
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
!
```

```
!
!
```

在本例中，此ACL使用两个序列。序列10与从此vEdge发送到对等体的BFD消息匹配。序列20则相反。

它与源（专用）**端口**和目的（公共）**端口**匹配。如果vEdge使用NAT，请确保检查正确的源端口和目标端口。

要检查每个序列计数器的命中数，请**发出show policy access-list counters <access-list name>**

```
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
```

网络地址转换

如何使用工具stun-client检测NAT映射和过滤

如果已完成上述所有步骤且您在NAT后面，则下一步是确定UDP NAT遍历(RFC 4787)映射和过滤行为。当vEdge位于NAT设备后面时，此工具对于发现本地vEdge外部IP地址非常有用。此命令获取设备的端口映射，并可选择性地发现本地设备和服务器(公共服务器：例如google stun server)。

> **注意**：有关更多详细信息，请访问：Docs Viptela - STUN客户端

```
vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 12386 --
verbosity 2 stun.l.google.com 19302"
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
```

在较新的软件版本中，语法可能略有不同：

```
vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 --localport
12386 --verbosity 2 stun.l.google.com 19302"
```

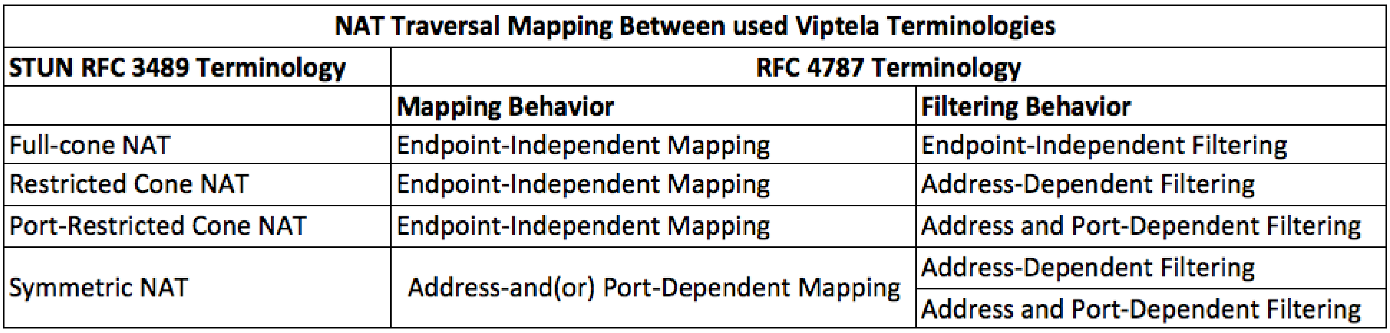
在本示例中，使用Google STUN服务器的UDP源端口12386执行完整NAT检测测试。此命令的输出将根据RFC 4787为您提供NAT行为和NAT过滤类型。

> **注意**：当您使用**tools stun**时，请记住允许隧道接口中的STUN服务，否则它将无法运行。**使用allow-service stun**让stun数据通过。

```
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
 !
!
```

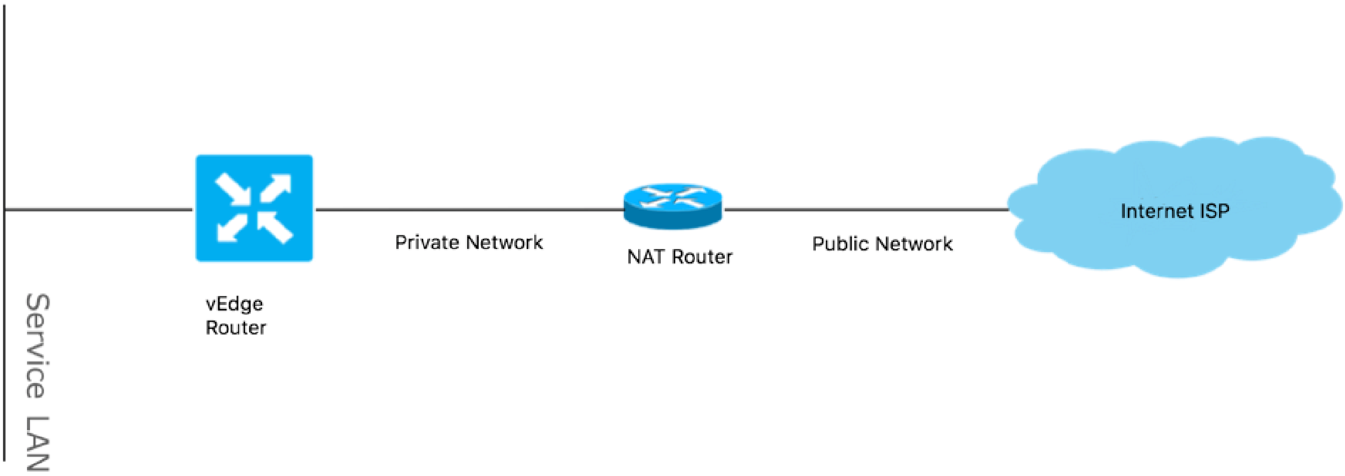
这显示了STUN术语（全锥NAT）与RFC 4787（UDP的NAT行为）之间的映射。



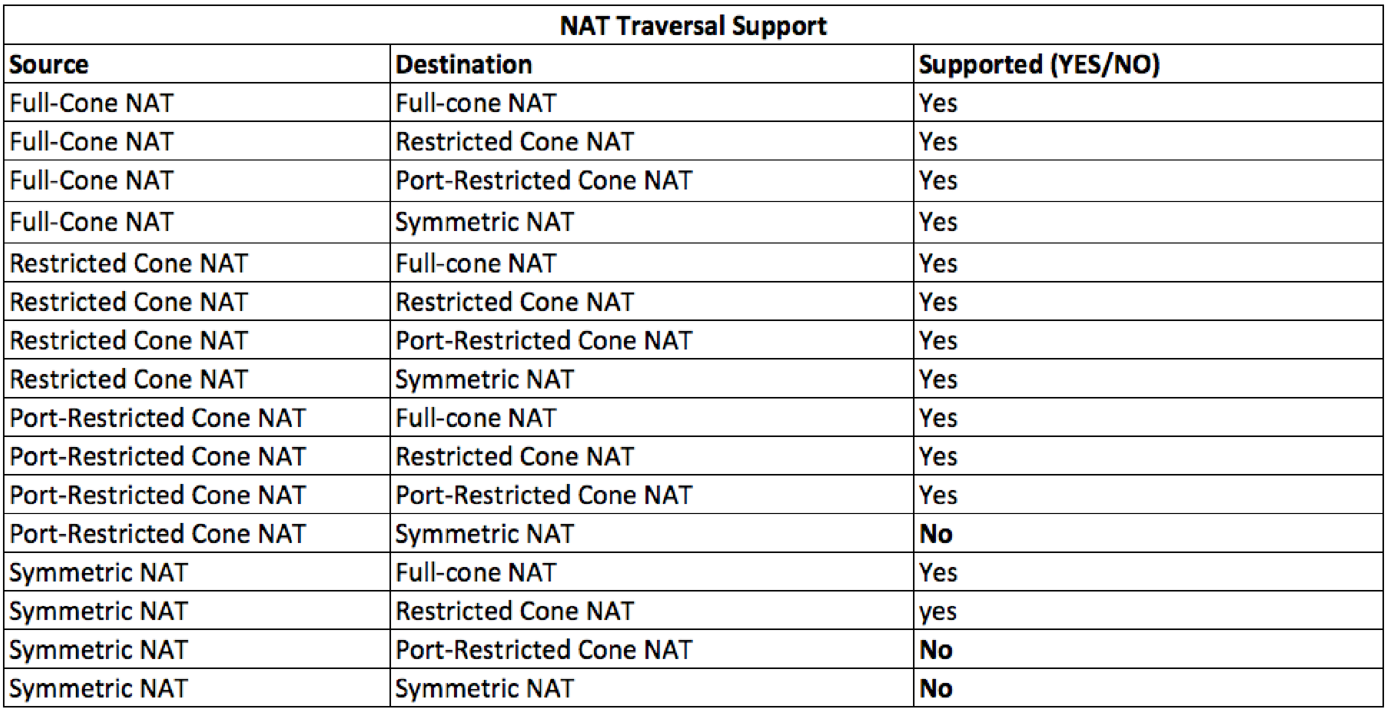
NAT Traversal Mapping Between used Viptela Terminologies		
STUN RFC 3489 Terminology	**RFC 4787 Terminology**	
	Mapping Behavior	**Filtering Behavior**
Full-cone NAT	Endpoint-Independent Mapping	Endpoint-Independent Filtering
Restricted Cone NAT	Endpoint-Independent Mapping	Address-Dependent Filtering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

数据平面隧道支持的NAT类型

在大多数情况下，您的公共颜色（如商业互联网或公共互联网）可以直接连接到互联网。在其他情况下，vEdge广域网接口和实际互联网服务提供商后面会有一个NAT设备，因此vEdge可以有私有IP，而其他设备（路由器、防火墙等）可以是具有公有IP地址的设备。



如果NAT类型不正确，则可能是不允许形成数据平面隧道的最常见原因之一。这些是支持的NAT类型。



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**

防火墙

如果已检查NAT及其不在不受支持的源和目标类型中，则防火墙可能正在阻止用于形成数据平面隧道的端口。

确保这些端口在用于数据平面连接的防火墙中处于打开状态：vEdge到vEdge数据平面：

UDP 12346到13156

对于从vEdge到控制器的控制连接：

UDP 12346到13156

TCP 23456到24156

确保打开这些端口以成功连接数据平面隧道。

检查用于数据平面隧道的源端口和目标端口时，可以使用**show tunnel statistics或**show bfd **sessions |选项卡，**但不显**示bfd会话。**它不显示任何源端口，只显示您可以看到的目标端口：

```
vEdge1# show bfd sessions
                                      SOURCE TLOC      REMOTE TLOC
DST PUBLIC                      DST PUBLIC         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR            SOURCE IP
IP                              PORT        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME
TRANSITIONS
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
-------------
192.168.30.105   50       up          biz-internet     biz-internet     192.168.109.181
192.168.109.182                 12346       ipsec  7           1000           1:21:28:05      10
192.168.30.105   50       up          private1         private1         192.168.110.181
192.168.110.182                 12346       ipsec  7           1000           1:21:26:13      2
```

```
vEdge1# show bfd sessions | tab

                                          SRC    DST                     SITE
DETECT      TX
SRC IP           DST IP           PROTO  PORT   PORT   SYSTEM IP        ID    LOCAL COLOR   COLOR
STATE  MULTIPLIER  INTERVAL  UPTIME      TRANSITIONS
-------------------------------------------------------------------------------------------------
---------------------------------------------------------------
192.168.109.181  192.168.109.182  ipsec  12346  12346  192.168.30.105  50    biz-internet  biz-
internet  up     7           1000      1:21:28:05  10
192.168.110.181  192.168.110.182  ipsec  12346  12346  192.168.30.105  50    private1
private1      up     7           1000      1:21:26:13  2
```

注意：有关所用SD-WAN防火墙端口的详细信息，请点击。

安全

如果您看到ACL计数器正在增加入站和出站流量，请检查多次迭代，**显示系统统计数据**差异，并确保没有丢弃。

```
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
```

在此输出中，**rx_replay_integrity_drops**会随着show system statistics diff命令的每**次迭代而**增加。

```
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
```

首先，在vEdge**上执行请求**安全ipsec-rekey。然后，执行show system statistics diff的**多次迭代，**查看是否仍看**到rx_replay_integrity_drops**。如果有，请检查您的安全配置。

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

如果您有上述配置，请尝试将**ah-no-id**添加到ipsec下的authentication-type。

```
vEdge1# show running-config security
security
ipsec
authentication-type sha1-hmac ah-sha1-hmac ah-no-id
!
!
```

> **提示：**ah-no-id启用AH-SHA1 HMAC和ESP HMAC-SHA1的修改版本，该版本忽略数据包外部IP报头中的ID字段。此选项容纳一些非Viptela设备，包括Apple AirPort Express NAT，该设备有一个错误，导致IP报头中的ID字段（一个不可变字段）被修改。在验证类型列表中配置ah-no-id选项，使Viptela AH软件忽略IP报头中的ID字段，以便Viptela软件可以与这些设备配合工作

DSCP标记流量的ISP问题

默认情况下，从vEdge路由器到控制器的所有控制和管理流量都通过DTLS或TLS连接传输，并标有DSCP值CS6（48十进制）。 对于数据放置隧道流量，vEdge路由器使用IPsec或GRE封装来相互发送数据流量。对于数据平面故障检测和性能测量，路由器会定期相互发送BFD数据包。这些BFD数据包还标有DSCP值CS6（48十进制）。

从ISP的角度看，这些类型的流量将被视为DSCP值为CS6的UDP流量，因为vEdge路由器和SD-WAN控制器会复制默认情况下标记到外部IP报头的DSCP。

如果tcpdump在传输ISP路由器上运行，可能会是这样：

```
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
```

如图所示，所有数据包都标有TOS字节0xc0，也称为DS字段（即十进制192或二进制110 000 00）。前6个高位与十进制或CS6中的DSCP位值48对应。

输出中的前2个数据包对应于控制平面隧道，其余2个数据包对应于数据平面隧道流量。根据数据包长度和TOS标记，它可以高度自信地断定它是BFD数据包（RX和TX方向）。 这些数据包也标有CS6。

有时，某些服务提供商，特别是MPLS L3 VPN/MPLS L2 VPN服务提供商可能会维护与客户的SLA不同，并且可以根据不同的客户DSCP标记处理不同类别的流量。例如，您可能拥有优质服务来优先处理DSCP EF和CS6语音和信令流量。由于优先级流量几乎始终受到管制，即使未超过上行链路的总带宽，因此可以看到此类流量丢包，因此BFD会话也可能抖动。

在某些情况下，如果服务提供商路由器上的专用优先级队列被饿死，您将看不到正常流量的任何丢包(例如从vEdge路由器运行简单**ping**)，因为此类流量标有默认DSCP值0，如下所示（TOS字节）：

```
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
```

但同时，您的BFD会话将抖动：

```
show bfd history
                                                       DST PUBLIC       DST PUBLIC
RX      TX
SYSTEM IP        SITE ID  COLOR            STATE       IP               PORT        ENCAP  TIME
PKTS    PKTS    DEL
------------------------------------------------------------------------------------------------
---------------------------------------
192.168.30.4     13       public-internet  up          192.168.109.4    12346       ipsec  2019-
05-01T03:54:23+0200 127     135     0
192.168.30.4     13       public-internet  up          192.168.109.4    12346       ipsec  2019-
05-01T03:54:23+0200 127     135     0
192.168.30.4     13       public-internet  down        192.168.109.4    12346       ipsec  2019-
05-01T03:55:28+0200 140     159     0
192.168.30.4     13       public-internet  down        192.168.109.4    12346       ipsec  2019-
05-01T03:55:28+0200 140     159     0
192.168.30.4     13       public-internet  up          192.168.109.4    12346       ipsec  2019-
05-01T03:55:40+0200 361     388     0
192.168.30.4     13       public-internet  up          192.168.109.4    12346       ipsec  2019-
05-01T03:55:40+0200 361     388     0
192.168.30.4     13       public-internet  down        192.168.109.4    12346       ipsec  2019-
05-01T03:57:38+0200 368     421     0
192.168.30.4     13       public-internet  down        192.168.109.4    12346       ipsec  2019-
05-01T03:57:38+0200 368     421     0
192.168.30.4     13       public-internet  up          192.168.109.4    12346       ipsec  2019-
05-01T03:58:05+0200 415     470     0
192.168.30.6     13       public-internet  up          192.168.109.4    12346       ipsec  2019-
05-01T03:58:05+0200 415     470     0
192.168.30.6     13       public-internet  down        192.168.109.4    12346       ipsec  2019-
05-01T03:58:25+0200 464063  464412  0
```

此处**nping** 可方便地进行故障排除：

```
vedge2# tools nping vpn 0 options "--tos 0x0c --icmp --icmp-type echo --delay 200ms -c 100 -q"
192.168.109.7
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
```

调试BFD

有时，如果需要进行更深入的调查，您可能希望在vEdge路由器上运行BFD调试。转发流量管理器(FTM)负责vEdge路由器上的BFD操作，因此您需**要调试ftm bfd**。所有调试输出都存储在

/var/log/tmplog/vdebug文件中，如果希望控制台上有这些消息(类似于Cisco IOS®**终端监控器**行为)，则可以使用**monitor start /var/log/tmplog/vdebug**。要停止日志记录，可以使**用monitor stop /var/log/tmplog/vdebug**。以下是由于超时而关闭的BFD会话的输出外观(IP地址为192.168.110.6的远程TLOC不再可达):

```
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1008]: BFD-
session TNL 192.168.110.5:12366->192.168.110.6:12346,l-tloc(32771)->r-tloc(32772),TLOC
192.168.30.5:biz-internet->192.168.30.6:public-internet IPSEC: BFD Session STATE update,
New_State :- DOWN, Reason :- LOCAL_TIMEOUT_DETECT Observed latency :- 7924, bfd_record_index :-
8, Hello timer :- 1000, Detect Multiplier :- 7
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_proc_tunnel_public_tloc_msg[252]:
tun_rec_index 13 tloc_index 32772 public tloc 0.0.0.0/0
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_increment_wanif_bfd_flap[2427]: BFD-
session TNL 192.168.110.5:12366->192.168.110.6:12346, : Increment the WAN interface counters by
1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1119]: BFD-
session TNL 192.168.110.5:12366->192.168.110.6:12346,l-tloc(32771)->r-tloc(32772),TLOC
192.168.30.5:biz-internet->192.168.30.6:public-internet IPSEC BFD session history update, old
state 3 new state 1 current  flap count 1 prev_index 1 current 2
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1140]: Attempting to add TLOC :
from_ttm 0 origin remote tloc-index 32772 pub 192.168.110.6:12346 pub v6 :::0 system_ip
192.168.30.6 color 5 spi 333
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]:
(32771:32772) proto 50 src 192.168.110.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]:
(32770:32772) proto 50 src 192.168.109.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD
session creation. Remote-tloc: tloc-index 32772, system-ip 192.168.30.6, color 5 encap 2from
local WAN Interface ge0_0
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]:
(32771:32772) proto 50 src 192.168.110.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD
session creation. Remote-tloc: tloc-index 32772, system-ip 192.168.30.6, color 5 encap 2from
local WAN Interface ge0_1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]:
(32770:32772) proto 50 src 192.168.109.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session
TNL 192.168.110.5:12366->192.168.110.6:12346,l-tloc(32771)->r-tloc(32772),TLOC 192.168.30.5:biz-
internet->192.168.30.6:public-internet IPSEC: session sa index changed from 484 to 484
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32771:32772) src
192.168.110.5:12366 dst 192.168.110.6:12346 record index 8 ref-count 1 sa-idx 484
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session
TNL 192.168.109.5:12366->192.168.110.6:12346,l-tloc(32770)->r-tloc(32772),TLOC
192.168.30.5:public-internet->192.168.30.6:public-internet IPSEC: session sa index changed from
485 to 485
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32770:32772) src
192.168.109.5:12366 dst 192.168.110.6:12346 record index 9 ref-count 1 sa-idx 485
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1008]: BFD-
session TNL 192.168.109.5:12366->192.168.110.6:12346,l-tloc(32770)->r-tloc(32772),TLOC
192.168.30.5:public-internet->192.168.30.6:public-internet IPSEC: BFD Session STATE update,
New_State :- DOWN, Reason :- LOCAL_TIMEOUT_DETECT Observed latency :- 7924, bfd_record_index :-
9, Hello timer :- 1000, Detect Multiplier :- 7
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_proc_tunnel_public_tloc_msg[252]:
tun_rec_index 14 tloc_index 32772 public tloc 0.0.0.0/0
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_increment_wanif_bfd_flap[2427]: BFD-
session TNL 192.168.109.5:12366->192.168.110.6:12346, : Increment the WAN interface counters by
1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1119]: BFD-
session TNL 192.168.109.5:12366->192.168.110.6:12346,l-tloc(32770)->r-tloc(32772),TLOC
192.168.30.5:public-internet->192.168.30.6:public-internet IPSEC BFD session history update, old
state 3 new state 1 current  flap count 1 prev_index 1 current 2
```

```
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1140]: Attempting to add TLOC :
from_ttm 0 origin remote tloc-index 32772 pub 192.168.110.6:12346 pub v6 :::0 system_ip
192.168.30.6 color 5 spi 333
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]:
(32771:32772) proto 50 src 192.168.110.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]:
(32770:32772) proto 50 src 192.168.109.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD
session creation. Remote-tloc: tloc-index 32772, system-ip 192.168.30.6, color 5 encap 2from
local WAN Interface ge0_0
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]:
(32771:32772) proto 50 src 192.168.110.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD
session creation. Remote-tloc: tloc-index 32772, system-ip 192.168.30.6, color 5 encap 2from
local WAN Interface ge0_1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]:
(32770:32772) proto 50 src 192.168.109.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session
TNL 192.168.110.5:12366->192.168.110.6:12346,l-tloc(32771)->r-tloc(32772),TLOC 192.168.30.5:biz-
internet->192.168.30.6:public-internet IPSEC: session sa index changed from 484 to 484
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32771:32772) src
192.168.110.5:12366 dst 192.168.110.6:12346 record index 8 ref-count 1 sa-idx 484
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session
TNL 192.168.109.5:12366->192.168.110.6:12346,l-tloc(32770)->r-tloc(32772),TLOC
192.168.30.5:public-internet->192.168.30.6:public-internet IPSEC: session sa index changed from
485 to 485
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32770:32772) src
192.168.109.5:12366 dst 192.168.110.6:12346 record index 9 ref-count 1 sa-idx 485
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_send_bfd_msg[499]: Sending BFD
notification Down notification to TLOC id 32772
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1140]: Attempting to add TLOC :
from_ttm 1 origin remote tloc-index 32772 pub 192.168.110.6:12346 pub v6 :::0 system_ip
192.168.30.6 color 5 spi 333
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]:
(32771:32772) proto 50 src 192.168.110.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_set_del_marker_internal[852]:
(32770:32772) proto 50 src 192.168.109.5:12366 dst 192.168.110.6:12346 ref_count 1
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 creation. Remote-tloc: tloc-index 32772, system-ip 192.168.30.6, color 5 encap 2from
local WAN Interface ge0_0
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]:
(32771:32772) proto 50 src 192.168.110.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_create[238]: Attempting BFD
session creation. Remote-tloc: tloc-index 32772, system-ip 192.168.30.6, color 5 encap 2from
local WAN Interface ge0_1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_clear_delete_marker[828]:
(32770:32772) proto 50 src 192.168.109.5:12366 dst 192.168.110.6:12346 ref_count 1
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session
TNL 192.168.110.5:12366->192.168.110.6:12346,l-tloc(32771)->r-tloc(32772),TLOC 192.168.30.5:biz-
internet->192.168.30.6:public-internet IPSEC: session sa index changed from 484 to 484
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32771:32772) src
192.168.110.5:12366 dst 192.168.110.6:12346 record index 8 ref-count 1 sa-idx 484
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_sa[1207]: BFD-session
TNL 192.168.109.5:12366->192.168.110.6:12346,l-tloc(32770)->r-tloc(32772),TLOC
192.168.30.5:public-internet->192.168.30.6:public-internet IPSEC: session sa index changed from
485 to 485
log:local7.debug: May  7 16:23:09 vedge2 FTMD[674]: ftm_tloc_add[1653]: BFD (32770:32772) src
192.168.109.5:12366 dst 192.168.110.6:12346 record index 9 ref-count 1 sa-idx 485
log:local7.info: May  7 16:23:09 vedge2 FTMD[674]: %Viptela-vedge2-ftmd-6-INFO-1400002:
Notification: 5/7/2019 14:23:9 bfd-state-change severity-level:major host-name:"vedge2" system-
ip:192.168.30.5 src-ip:192.168.110.5 dst-ip:192.168.110.6 proto:ipsec src-port:12366 dst-
port:12346 local-system-ip:192.168.30.5 local-color:"biz-internet" remote-system-ip:192.168.30.6
remote-color:"public-internet" new-state:down deleted:false flap-reason:timeout
```

```
log:local7.info: May  7 16:23:09 vedge2 FTMD[674]: %Viptela-vedge2-ftmd-6-INFO-1400002:
Notification: 5/7/2019 14:23:9 bfd-state-change severity-level:major host-name:"vedge2" system-
ip:192.168.30.5 src-ip:192.168.109.5 dst-ip:192.168.110.6 proto:ipsec src-port:12366 dst-
port:12346 local-system-ip:192.168.30.5 local-color:"public-internet" remote-system-
ip:192.168.30.6 remote-color:"public-internet" new-state:down deleted:false flap-reason:timeout
```

要启用另一个有价值的调试是隧道流量管理器(TTM)事件调试是**debug ttm events**。从TTM的角度看，BFD DOWN事件如下所示：

```
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM
Msg LINK_BFD, Client: ftmd, AF: LINK
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[413]:     Remote-
TLOC: 192.168.30.6 : public-internet : ipsec, Local-TLOC: 192.168.30.5 : biz-internet : ipsec,
Status: DOWN, Rec Idx: 13 MTU: 1441, Loss: 77, Latency: 0, Jitter: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM
Msg LINK_BFD, Client: ftmd, AF: LINK
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[413]:     Remote-
TLOC: 192.168.30.6 : public-internet : ipsec, Local-TLOC: 192.168.30.5 : public-internet :
ipsec, Status: DOWN, Rec Idx: 14 MTU: 1441, Loss: 77, Latency: 0, Jitter: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM
Msg BFD, Client: ftmd, AF: TLOC-IPV4
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[402]:     TLOC:
192.168.30.6 : public-internet : ipsec, Status: DOWN
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_af_tloc_db_bfd_status[234]:   BFD
message: I SAY WHAT WHAT tloc 192.168.30.6 : public-internet : ipsec status is 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Sent TTM Msg
TLOC_ADD, Client: ompd, AF: TLOC-IPV4
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[213]:     TLOC:
192.168.30.6 : public-internet : ipsec, Index: 32772, Origin: REMOTE, Status: DOWN, LR enabled:
0, LR hold time: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[217]:
Attributes: GROUP PREF WEIGHT GEN-ID VERSION TLOCv4-PUB TLOCv4-PRI TLOCv6-PUB TLOCv6-PRI SITE-ID
CARRIER ENCAP RESTRICT
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:
2147483661
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: 192.168.110.6:12346
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[273]:         TLOCv4-
Private: 192.168.110.6:12346
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[277]:         TLOCv6-
Public: :::0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[281]:         TLOCv6-
Private: :::0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[285]:         TLOC-
Encap: ipsec-tunnel
```

```
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[295]:
Authentication: unknown(0x98) Encryption: aes256(0xc) SPI 334 Proto ESP
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[312]:            SPI
334, Flags 0x1e           Integrity: 1, encrypt-keys: 1 auth-keys: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[317]:
Number of protocols 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[328]:
Number of encrypt types: 2
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:
Encrypt type[0] AES256-GCM
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:
Encrypt type[1] AES256-CBC
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[339]:
Number of integrity types: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[344]:
integrity type[0] HMAC_SHA1
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, Client: ftmd, AF: TLOC-IPV4
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[213]:     TLOC:
192.168.30.6 : public-internet : ipsec, Index: 32772, Origin: REMOTE, Status: DOWN, LR enabled:
0, LR hold time: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[217]:
Attributes: GROUP PREF WEIGHT GEN-ID VERSION TLOCv4-PUB TLOCv4-PRI TLOCv6-PUB TLOCv6-PRI SITE-ID
CARRIER ENCAP RESTRICT
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:
2147483661
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: 192.168.110.6:12346
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[273]:         TLOCv4-
Private: 192.168.110.6:12346
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[277]:         TLOCv6-
Public: :::0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[281]:         TLOCv6-
Private: :::0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[285]:         TLOC-
Encap: ipsec-tunnel
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[295]:
Authentication: unknown(0x98) Encryption: aes256(0xc) SPI 334 Proto ESP
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[312]:            SPI
334, Flags 0x1e           Integrity: 1, encrypt-keys: 1 auth-keys: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[317]:
Number of protocols 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[328]:
Number of encrypt types: 2
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:
Encrypt type[0] AES256-GCM
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:
```

```
Encrypt type[1] AES256-CBC
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[339]:
Number of integrity types: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[344]:
integrity type[0] HMAC_SHA1
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, Client: fpmd, AF: TLOC-IPV4
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[213]:     TLOC:
192.168.30.6 : public-internet : ipsec, Index: 32772, Origin: REMOTE, Status: DOWN, LR enabled:
0, LR hold time: 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[217]:
Attributes: GROUP PREF WEIGHT GEN-ID VERSION TLOCv4-PUB TLOCv4-PRI TLOCv6-PUB TLOCv6-PRI SITE-ID
CARRIER ENCAP RESTRICT
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:
2147483661
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: 192.168.110.6:12346
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[273]:         TLOCv4-
Private: 192.168.110.6:12346
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[277]:         TLOCv6-
Public: :::0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[281]:         TLOCv6-
Private: :::0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[285]:         TLOC-
Encap: ipsec-tunnel
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[295]:
Authentication: unknown(0x98) Encryption: aes256(0xc) SPI 334 Proto ESP
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[312]:           SPI
334, Flags 0x1e           Integrity: 1, encrypt-keys: 1 auth-keys: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[317]:
Number of protocols 0
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[328]:
Number of encrypt types: 2
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:
Encrypt type[0] AES256-GCM
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[333]:
Encrypt type[1] AES256-CBC
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[339]:
Number of integrity types: 1
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[344]:
integrity type[0] HMAC_SHA1
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_DEVICE_ADD, Client: pimd, AF: DATA-DEVICE-IPV4
log:local7.debug: May  7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[431]:     Device:
192.168.30.6, Status: 2
log:local7.info: May  7 16:58:19 vedge2 FTMD[674]: %Viptela-vedge2-ftmd-6-INFO-1400002:
```

```
Notification: 5/7/2019 14:58:19 bfd-state-change severity-level:major host-name:"vedge2" system-
ip:192.168.30.5 src-ip:192.168.110.5 dst-ip:192.168.110.6 proto:ipsec src-port:12366 dst-
port:12346 local-system-ip:192.168.30.5 local-color:"biz-internet" remote-system-ip:192.168.30.6
remote-color:"public-internet" new-state:down deleted:false flap-reason:timeout
log:local7.info: May  7 16:58:20 vedge2 FTMD[674]: %Viptela-vedge2-ftmd-6-INFO-1400002:
Notification: 5/7/2019 14:58:19 bfd-state-change severity-level:major host-name:"vedge2" system-
ip:192.168.30.5 src-ip:192.168.109.5 dst-ip:192.168.110.6 proto:ipsec src-port:12366 dst-
port:12346 local-system-ip:192.168.30.5 local-color:"public-internet" remote-system-
ip:192.168.30.6 remote-color:"public-internet" new-state:down deleted:false flap-reason:timeout
```

相关信息

- SDWAN产品文档
- 解剖学：网络地址转换器的内部情况
- 技术支持和文档 - Cisco Systems