排除双向转发检测和数据层面连接问题故障

Contents

Introduction

本文描述数据层面在vEdge路由器也许出现的连接问题，在您成功连接到控制层面后，但是仍有站点之间的没有数据层面连接。

Prerequisites

Requirements

Cisco建议您有Cisco软件被定义的广域网络(SDWAN)解决方案知识。

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.

Note:在本文提交的all命令输出是从vEdge路由器，但是故障排除方法将是相同的为运行IOS ® - XE SDWAN软件的路由器。请使用**sdwan**关键字为了得到在IOS ®的同样输出- XE SDWAN软件。例如; **显示sdwan控制连接**而不是**表示控制连接**。

控制层面信息

检查控制本地属性

为了检查广域网络(广域网)的状况在vEdge建立接口，使用show命令**控制本地属性WAN接口列表**。在此输出中，您能看到RFC 4787网络地址转换(NAT)类型。当vEdge是在NAT设备(防火墙、路由器等等)时，公共和专用的IPv4地址后，公共和专用的来源用户数据报协议(UDP)端口用于构建数据层面隧道。您能也找到隧道接口、颜色和控制连接的最大数量的状态被配置的。

```
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
```

有此数据，您能识别关于如何必须构建数据隧道，并且什么的某一信息端口您应该期望路由器透视图为了使用，当您形成数据隧道时。

检查控制连接

请注意不形成数据层面隧道的颜色有一控制已建立连接用在重叠的控制器。否则， vEdge不发送传输定位器(TLOC)信息到vSmart通过重叠管理协议(OMP)。您能保证它是否是UP或不与使用请**显示控制连接**命令，并且寻找状态**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
```

如果不形成数据隧道的接口设法连接，您能通过达到控制连接的成功的建立解决它通过该颜色。或者，您能在它附近工作在设置在所选接口的最大控制**连接旁边0**在隧道接口部分下。

```
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
 !
```

> **Note**:有时，您能使用no命令控制**连接**为了达到同一个目标。然而，该命令不设立控制连接的最大数量。此命令从15.4开始在更新的软件贬抑并且不应该使用。

重叠管理协议

检查OMP TLOCs是否从vEdges做通告

因为您在上一步注意了， OMP TLOCs不可能被发送，因为接口尝试对格式控制连接通过该颜色并且不能到达控制器。因此，检查，如果数据建立隧道的颜色不工作或出来发送该特定的颜色的TLOC到vSmarts。请使用被发送到OMP对等体**做通告的**show命令**omp tlocs**为了检查TLOCs。

示例：颜色**mpls**和**金子**。TLOC没有被发送到颜色mpls的vSmart。

```
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**金子**。TLOC为两个颜色被发送。

```
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
```

Note:对于所有本地生成的控制层面信息，“从对等体”字段将设置为0.0.0.0。当您寻找本地产生的信息时，请保证匹配基于此值。

检查vSmart是否接受并且通告TLOCs

即然您知道您的TLOCs做通告对vSmart，请确认从正确的对等体接受TLOCs并且通告它对另一vEdge。

示例：vSmart从1.1.1.20 vEdge1接受TLOCs。

```
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        -
```

万一看不到TLOCs或您发现所有其他代码这里，您能检查这些：

```
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        -
```

检查是否没有阻拦TLOCs的策略。

show run策略控制策略-请寻找在vSmart拒绝您的从做通告的TLOCs或被接受的所有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.
```

Note:如果TLOC被拒绝或无效，不会做通告对其他vEdges。

保证策略不过滤TLOC，当从vSmart做通告。您能看到TLOC在vSmart被接受，但是您在另一vEdge将看不到它。

示例 1：与TLOC的vSmart在C，I，R。

```
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看不到从来vEdge2的颜色蓝色的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，您能看到TLOC为什么不出现在vEdge1。

```
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 session命令

这些是寻找的关键事在输出中：

```
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** ：并列系统IP

- **来源和远程TLOC颜色**：这是有用了解什么TLOC您期望接受和发送。
- 源 IP：它是**专用的**来源IP。如果是在NAT后，此信息不会显示这里(能在使用看到**显示控制**在本文的开始解释)的本地**属性<wan-interface-list>**。
- **DST公有IP** ：它不管怎么样是目的地vEdge使用形成数据层面隧道，如果是在NAT后。（示例：vEdges直接地附加互联网或者多协议标签交换(MPLS)链路)
- **DST公共端口：** 公共NAT vEdge使用为了形成数据层面隧道到远程vEdge的端口。
- **转变**：次数BFD会话从NA更改其状态，向上反之亦然。

Show命令隧道统计数据

显示隧道统计数据能显示关于数据层面隧道的信息，您能容易地看到是否是发送或收到一个特定IPSec隧道的信息包在vEdges之间。这可帮助您了解信息包是否在每个末端做它和查出在节点之间的连通性问题。

在示例中，当您多次时运行命令，您不能注意一个增量或增量在**tx-pkts**或**RXpkts**。

> **提示**：如果您的tx-pkts的计数器增加，您传达数据给对等体。如果您的RXpkts不增加，意味着您从您的对等体不接受数据。在此事件，请检查另一个末端并且确认tx-pkts是否增加。

```
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**显示隧道**可以使用检查BFD发送的数据包的编号和在特定的数据层面隧道内被接受的**统计数据bfd** ：

```
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
```

访问列表

在您查看**show bfd session**输出后，访问列表是有用和必要步骤。即然专用和公共IP和端口知道，您能创建访问控制表(ACL)配比SRC_PORT， DST_PORT， SRC_IP， DST_IP。这可帮助您确认是否您是收到和传送BFD信息。

您能找到ACL配置的示例：

```
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
```

在示例中，此ACL使用两个顺序。顺序10匹配从此vEdge传送到对等体的BFD信息。顺序20执行对面。

它配比来源(**专用的**)端口和目的地(**公共**)端口。如果vEdge使用NAT，请保证检查正确的来源和目的地端口。

要检查在每个顺序计数器的命中发出**show policy访问列表计数器<access列表name>**

```
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
```

网络地址转换

如何使用工具STUN客户端发现NAT映射和过滤

如果实行了被提及的所有步骤，并且是在NAT后，下一步是识别映射和过滤工作情况的UDP NAT横越(RFC 4787)。当该vEdge在NAT设备后时，位于此工具是确实有用发现本地vEdge外部IP地址。此命令获得映射为设备的端口和可选地发现关于NAT的属性在本地设备和服务器(公共服务器之间：示例谷歌Stun服务器)。

> **Note**:详细信息访问：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
```

在更新的软件版本，语法可以是不同的位：

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

在本例中，您执行一个充分的NAT检测测试与使用UDP源端口12386到谷歌STUN服务器。此命令的输出将产生您NAT工作情况和根据RFC 4787的NAT过滤器类型。

Note:当您使用时**工具使**，切记允许在隧道接口的STUN服务震惊，否则不会运作。请使用允许**服务Stun**为了让Stun数据通行证。

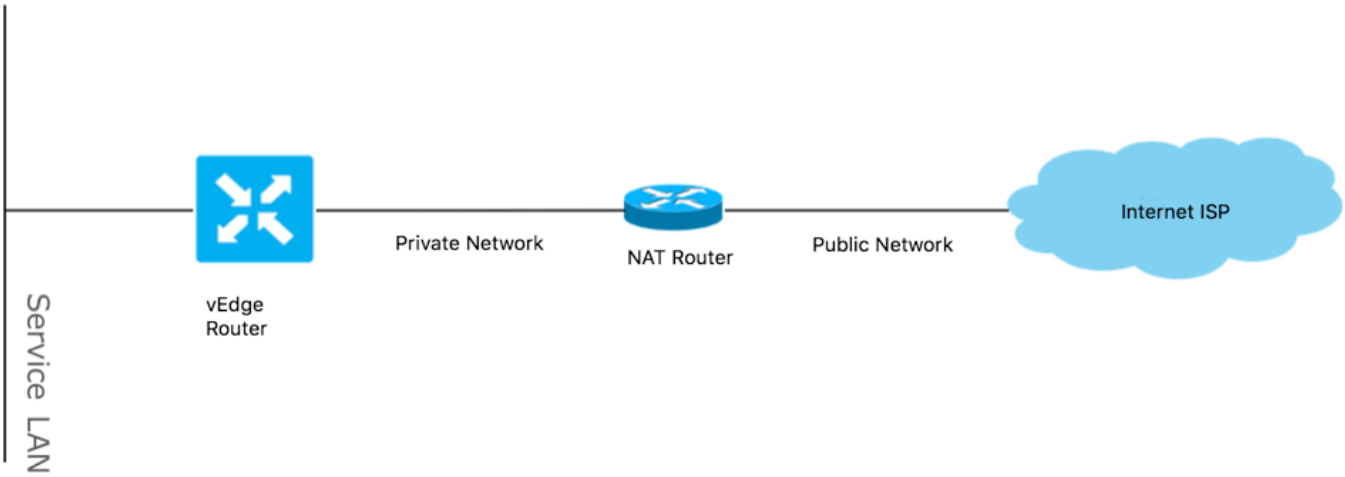
```
vEdge1# show running-config vpn 0 interface ge0/0
vpn 0
 interface ge0/0
  ip address 10.19.145.2/30
  !
  tunnel-interface
   encapsulation ipsec
   color gold
   max-control-connections 1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   no allow-service icmp
   no allow-service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

这显示STUN术语(FULL锥体NAT)和RFC 4787 (NAT之间的映射性能上为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

数据层面隧道的支持的NAT类型

在大多案件，您的公共颜色类似事务互联网或公共互联网可以直接地连接互联网。在某些情况下，那里是在vEdge广域网接口和实际互联网服务提供商后的一个NAT设备，因此vEdge能有私有IP，并且其它设备(路由器、防火墙等等)可以是有面对IP地址的公共的设备。



如果有一种不正确NAT类型，则可能潜在是不允许数据层面隧道的形成多数常见原因的之一。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

如果已经登记了NAT和其不不支持的来源和目的地类型，很可能，防火墙阻拦用于的端口形成数据层面隧道。

保证这些端口是开放的在数据层面连接的防火墙：对vEdge数据层面的vEdge ：

UDP 12346到13156

控制连接从vEdge到控制器：

UDP 12346到13156

TCP 23456到24156

保证您打开这些端口为了达到数据层面隧道的成功的连接。

当您检查用于数据层面隧道时和目的地端口的来源，您能使用**显示隧道统计数据**或**show bfd session|不是选项，但是show bfd session。**它不会显示任何源端口，只有目的地端口，您能看到：

```
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
 !
!
```

Note:可以找到关于SD-WAN使用的防火墙端口的更多信息这里。

安全

如果看到您您的ACL计数器是增加入站和outbound，请检查几个迭代**show system统计数据diff**并且保证那里是没有丢包。

```
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**增加与**diff命令show system的统计数据的**每迭代。

```
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，请执行一**请求安全ipsec键变更**在vEdge。然后，请通过**show system统计数据diff的**几迭代并且检查是否仍然看到**rx_replay_integrity_drops**。如果，检查您的安全配置。

```
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
```

如果有被提及的配置，请设法添加啊没有id到认证型的下面ipsec。

```
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
```

提示：啊没有id enable (event)的AH-SHA1 HMAC和ESP HMAC-SHA1的一个修正的版本忽略在信息包的外面IP头的ID字段。此选项适应一些非Viptela设备，那包括Apple机场Express NAT，有一个Bug的IP头导致ID字段，一个非可变的字段，被修改。配置在认证类型列表的啊没有id选项安排Viptela AH软件忽略在IP头的ID字段，以便Viptela软件能与这些设备一道工作

DSCP明显数据流的ISP问题

默认情况下，所有控制和管理数据流从vEdge路由器到控制器在DTL或TLS连接移动和标记用CS6 (48的DSCP值十进制)。对于数据请放置隧道流量、vEdge路由器使用IPsec或GRE封装彼此发送数据流量。对于数据层面故障检测和性能测定，路由器周期地互相发送BFD信息包。这些BFD信息包用CS6也标记(48的DSCP值十进制)。

从ISP的角度，默认情况下，因为vEdge路由器和SD-WAN控制器复制DSCP该标记对外面IP头那些流量类型将被看到作为与DSCP值CS6的UDP数据流。

这是它如何也许看起来象，如果tcpdump在传输ISP路由器运行：

```
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
```

和能被看到这里，亦称所有信息包用TOS字节0xc0标记与十进制192是相等的DS字段(或者110 000 00用二进制。前6个高位比特对应于DSCP在十进制或CS6的比特值48)。

保持的前2个信息包在输出中对应到控制层面隧道和2，于数据层面隧道流量。基于的信息包长度和指示的TOS，它能有高信心认为，它是BFD信息包(RX和TX方向)。这些信息包用CS6标记。

一些时间一些服务提供商和MPLS L3 VPN/MPLS特别是L2VPN服务提供商可以与用户的maintaindifferent SLA，并且能处理一个不同的流量等级根据不同地标记的用户DSCP。例如，您也许有指定优先级的优质服务DSCP EF和CS6语音和信令数据流。因为优先级数据流几乎总是被管辖，即使上行链路的总带宽没有被超出，为了此种数据流信息包丢失能被看到并且BFD会话能拍动。在某些情况下被看到了，如果在服务提供商路由器的专用的优先级队列是饥饿的，您为正常数据流将看不到所有丢包(即运行简单PING从vEdge路由器)，因为这样数据流用默认DSCP值0标记和能被看到这里(TOS字节)：

```
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
```

但是同时，您的BFD会话拍动：

```
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
```

并且这里nping来方便为了排除故障：

```
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
```

Debug bfd

一些时间，如果需要更加深刻的调查，您也许要运行BFD调试在vEdge路由器的。转发数据流管理器(FTM)对在vEdge路由器的BFD操作负责并且您需要**调试ftm bfd**。所有调试输出在**/var/log/tmplog/vdebug**文件存储，并且，如果要有在控制台的那些消息(类似于Cisco IOSTERMINAL**监控程序**工作情况)，您能使用**监控程序开始/var/log/tmplog/vdebug**。为了停止记录，您能使用**监控程序终止/var/log/tmplog/vdebug**。这是输出如何将看似类似为断开由于超时的BFD会话(与IP地址192.168.110.6的远程TLOC不再可及的) ：

```
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
```

另一重要的调试为了enable (event)是隧道流量调试是**调试ttm事件的**管理器(TTM)事件。这是BFD DOWN事件如何看起来象从TTM的角度：

```
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
```

相关信息

- SDWAN产品文档
- 解剖学：看起来内部网络地址译码器
- Technical Support & Documentation - Cisco Systems