Solucionar problemas de detecção de encaminhamento bidirecional e conexões de plano de dados

Contents

Introduction

Este documento descreve os problemas de conexão do plano de dados que podem surgir nos roteadores vEdge depois que você se conecta com êxito ao plano de controle, mas ainda não há conectividade do plano de dados entre os locais.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento da solução Cisco Software Defined Wide Area Network (SDWAN).

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

> **Note**: Todas as saídas de comando apresentadas neste documento são de roteadores vEdge, mas a abordagem de solução de problemas será a mesma para o roteador que executa o software IOS®-XE SDWAN. Use a palavra-chave **sdwan** para obter as mesmas saídas no software IOS®-XE SDWAN. Por exemplo; **mostrar conexões de controle sdwan** em vez de **mostrar conexões de controle**.

Informações do plano de controle

Verificar propriedades locais do controle

Para verificar o status das interfaces da rede de longa distância (WAN) em um vEdge, use o comando **show control local-properties wan-interface-list**. Nesta saída, você pode ver o tipo de conversão de endereço de rede (NAT - Network Address Translation) RFC 4787. Quando o vEdge está por trás de um dispositivo NAT (Firewall, Roteador, etc.), endereço IPv4 público e privado, as portas UDP (Public and Private Source User Datagram Protocol) são usadas para criar os túneis de plano de dados. Você também pode encontrar o estado da interface do túnel, a cor e o número máximo de conexões de controle configuradas.

```
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
```

Com esses dados, você pode identificar determinadas informações sobre como os túneis de dados devem ser construídos e quais portas você deve esperar da perspectiva dos roteadores para usar quando formar os túneis de dados.

Verificar conexões de controle

Éimportante garantir que a cor que não forma túneis de plano de dados tenha uma conexão de controle estabelecida com os controladores na sobreposição. Caso contrário, o vEdge não envia as informações do Transport Locator (TLOC) para o vSmart via Overlay Management Protocol

(OMP). Você pode verificar se está ativo ou não com o uso do comando **show control connections** e procurar o estado **connect**.

```
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
```

Se a interface que não forma túneis de dados tentar se conectar, você poderá resolvê-la ao obter êxito na ativação das conexões de controle por meio dessa cor. Ou você pode contorná-lo configurando o **max-control-connections 0** na interface selecionada na seção de interface de túnel.

```
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**: Às vezes, você pode usar o comando **no control-connections** para alcançar o mesmo objetivo. No entanto, esse comando não estabelece um número máximo de conexões de controle. Este comando é preterido a partir de 15.4 e não deve ser usado em software mais recente.

Protocolo de gerenciamento de sobreposição

Verifique se as TLOCs de OMP são anunciadas nas bordas

Como você observou, na etapa anterior, os TLOCs de OMP não podem ser enviados porque a interface tenta formar conexões de controle por essa cor e não consegue acessar os

controladores. Então, verifique se a cor em que os túneis de dados não funcionam ou chegam envia a TLOC para essa cor específica para o vSmarts. Use o comando **show omp tlocs anunciados** para verificar as TLOCs enviadas aos pares OMP.

Exemplo: Cores **mpls** e **ouro**. Nenhuma TLOC é enviada ao vSmart para mpls coloridos.

```
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
```

Exemplo: Cores **mpls** e **ouro**. A TLOC é enviada para ambas as cores.

```
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: Para qualquer informação de plano de controle gerada localmente, o campo "FROM PEER" será definido como 0.0.0.0. Ao procurar informações originadas localmente, assegure-se de corresponder com base nesse valor.

Verifique se o vSmart recebe e anuncia as TLOCs

Agora que você sabe que suas TLOCs são anunciadas para o vSmart, confirme se ele recebe TLOCs do peer correto e as anuncia para o outro vEdge.

Exemplo: O vSmart recebe as TLOCs do 1.1.1.20 vEdge1.

```
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        -
```

Caso não veja os TLOCs ou veja outros códigos aqui, você pode verificar estes:

```
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        -
```

Verifique se não há nenhuma política que bloqueie as TLOCs.

show run policy control-policy -look for any tloc-list que rejeita que seus TLOCs sejam anunciados ou recebidos no vSmart.

```
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: Se uma TLOC for Rejeitada ou Inválida, ela não será anunciada aos outros vEdges.

Certifique-se de que uma política não filtre a TLOC quando ela for anunciada do vSmart. Você pode ver que a TLOC é recebida no vSmart, mas não a verá no outro vEdge.

Exemplo 1: vSmart com TLOC em 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        -
```

Exemplo 2: O vEdge1 não vê a TLOC do azul colorido do vEdge2. Ele vê apenas 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
```

Ao verificar a política, você pode ver por que a TLOC não aparece no 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
 !
!
```

Detecção de encaminhamento bidirecional

Entender o comando show bfd sessions

Estes são os principais itens a serem procurados na saída:

```
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
```

- **IP DO SISTEMA**: peer system-ip
- **COR DA FONTE E DO TLOC REMOTO**: Isso é útil para saber qual TLOC você espera receber e enviar.
- **IP DE ORIGEM:** É o IP **de** origem **privada**. Se você estiver por trás de um NAT, essas informações não serão exibidas aqui (elas podem ser vistas com o uso de **show control local-properties <wan-interface-list>** que é explicado no início do documento).
- **IP PÚBLICO DST**: É o destino que o vEdge está usando para formar o túnel do plano de dados, independentemente de estar ou não atrás do NAT. (Exemplo: Bordas diretamente conectadas à Internet ou links de MPLS (Multi-Protocol Label Switching)
- **PORTA PÚBLICA DST:** porta NAT pública usada pelo vEdge para formar o túnel do plano de dados para o vEdge remoto.
- **TRANSIÇÕES**: Número de vezes que a sessão BFD alterou seu status, de NA para UP e vice-versa.

Comando show tunnel statistics

O **comando show tunnel statistics** pode exibir informações sobre os túneis de plano de dados. Você pode ver facilmente se está enviando ou recebendo pacotes para um túnel IPSEC específico entre os vEdges. Isso pode ajudá-lo a entender se os pacotes estão fazendo isso em cada extremidade e isolar problemas de conectividade entre os nós.

No exemplo, quando você executa o comando várias vezes, você pode notar um incremento ou nenhum incremento no **tx-pkts** ou no **rx-pkts**.

> **Tip**: Se seu contador para incremento tx-pkts, você está transmitindo dados para o peer. Se o rx-pkts não aumentar, isso significa que você não está recebendo dados do seu peer.

Nesse caso, verifique a outra extremidade e confirme se o tx-pkts está aumentando.

```
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
```

Outro comando útil é **show tunnel statistics bfd** que pode ser usado para verificar o número de pacotes BFD enviados e recebidos dentro de um túnel de plano de dados específico:

```
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
```

Lista de acesso

Uma lista de acesso é uma etapa útil e necessária após você observar a saída **show bfd sessions**. Agora que os IPs e portas privados e públicos são conhecidos, você pode criar uma lista de controle de acesso (ACL) para corresponder ao SRC_PORT, DST_PORT, SRC_IP, DST_IP. Isso pode ajudá-lo a confirmar se você está recebendo e enviando mensagens BFD ou não.

Aqui você pode encontrar um exemplo de uma configuração de ACL:

```
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
!
!
!
```

No exemplo, essa ACL usa duas sequências. A sequência 10 corresponde às mensagens BFD que são enviadas deste vEdge para o peer. A sequência 20 faz o oposto.

Corresponde às portas de origem (**privada**) e de destino (**pública**). Se o vEdge usar NAT, verifique as portas de origem e de destino corretas.

Para verificar os acertos em cada contador de sequência, emita o comando **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
```

Conversão de endereço de rede

Como usar ferramentas stun-client para detectar mapeamento e filtragem de NAT

Se você executou todas as etapas mencionadas e está por trás do NAT, a próxima etapa é identificar o comportamento de mapeamento e filtragem do NAT UDP (RFC 4787). Essa ferramenta é realmente útil para descobrir o endereço IP externo do vEdge quando o vEdge está localizado atrás de um dispositivo NAT. Esse comando obtém um mapeamento de porta para o dispositivo e, opcionalmente, descobre propriedades sobre o NAT entre o dispositivo local e um servidor (servidor público: exemplo google stun server).

> **Note**: Para obter informações mais detalhadas, visite: Docs Viptela - Cliente STUN

```
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
```

Nas versões mais recentes do software, a sintaxe pode ser um pouco diferente:

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

Neste exemplo, você executa um teste de detecção de NAT completo com o uso da porta de origem UDP 12386 para o servidor Google STUN. A saída desse comando fornecerá o comportamento de NAT e o tipo de filtragem de NAT com base no RFC 4787.

> **Note**: Ao usar **ferramentas stun**, lembre-se de permitir o serviço STUN na interface do túnel, caso contrário ele não funcionará. Use **allow-service stun** para permitir a passagem dos dados stun.

```
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
```

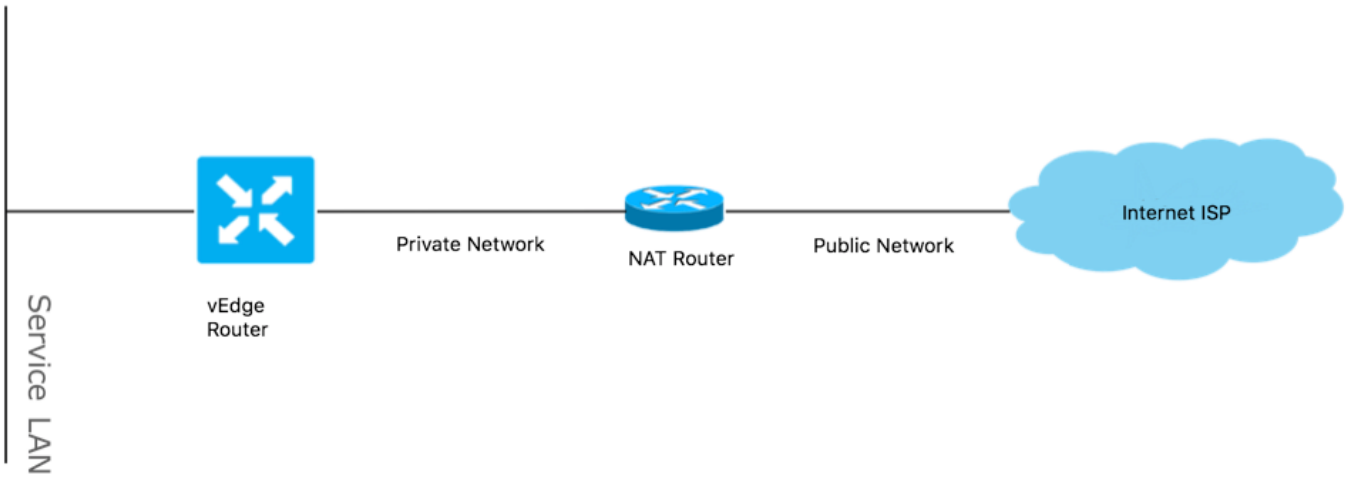
```
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   allow-service stun
  !
  no shutdown
 !
!
```

Mostra o mapeamento entre a terminologia STUN (Full-Cone NAT) e RFC 4787 (Comportamento NAT para 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

Tipos de NAT suportados para túneis de plano de dados

Na maioria dos casos, as cores públicas, como Internet em empresas ou Internet pública, podem ser diretamente conectadas à Internet. Em outros casos, haverá um dispositivo NAT por trás da interface WAN vEdge e o provedor de serviços de Internet real, de modo que o vEdge possa ter um IP privado e o outro dispositivo (roteador, firewall, etc.) possa ser o dispositivo com endereços IP públicos.



Se você tiver um tipo de NAT incorreto, poderá ser um dos motivos mais comuns que não permitem a formação de túneis de plano de dados. Esses são os tipos de NAT suportados.

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**

Firewalls

Se você já tiver verificado o NAT e ele não estiver nos tipos de Origem e Destino não suportados, é possível que um Firewall esteja bloqueando as portas usadas para formar os túneis do plano de dados.

Certifique-se de que essas portas estejam abertas nas conexões do plano de dados do Firewall: Plano de dados vEdge para vEdge:

UDP 12346 a 13156

Para conexões de controle do vEdge para controladores:

UDP 12346 a 13156

TCP 23456 a 24156

Certifique-se de abrir essas portas para obter uma conexão bem-sucedida dos túneis do plano de dados.

Ao verificar as portas origem e destino usadas para túneis de plano de dados, você pode usar **show tunnel statistics** ou **show bfd sessions | guia** mas não **show bfd sessions.** Ele não exibirá nenhuma porta de origem, somente portas de destino como você pode ver:

```
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
```

Note: Mais informações sobre as portas de firewall SD-WAN usadas podem ser encontradas aqui.

Security

Se você vir que seu contador de ACL está aumentando na entrada e na saída, verifique se várias iterações **mostram as estatísticas do sistema diff** e se certifique de que não há descartes.

```
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
```

Nesta saída, **rx_replay_Integrity_drops** aumenta com cada iteração do comando **show system statistics diff**.

```
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
```

Primeiro, execute um **comando request security ipsec-**rekey no vEdge. Em seguida, passe por várias iterações de **show system statistics diff** e veja se ainda vê **rx_replay_Integrity_drops**. Em caso afirmativo, verifique a configuração de segurança.

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

Se você tiver a configuração mencionada, tente adicionar **ah-no-id** ao tipo de autenticação em ipsec.

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

> **Tip**: ah-no-id permite uma versão modificada de AH-SHA1 HMAC e ESP HMAC-SHA1 que ignora o campo ID no cabeçalho IP externo do pacote. Essa opção acomoda alguns dispositivos não Viptela, que incluem o NAT do Apple AirPort Express, que tem um bug que faz com que o campo ID no cabeçalho IP, um campo não-mutable, seja modificado. Configure a opção ah-no-id na lista de tipos de autenticação para que o software Viptela AH ignore o campo ID no cabeçalho IP para que o software Viptela possa funcionar em conjunto com esses dispositivos

Problemas de ISP com tráfego marcado de DSCP

Por padrão, todo o tráfego de controle e gerenciamento do roteador vEdge para os controladores trafega por conexões DTLS ou TLS e é marcado com um valor DSCP CS6 (48 decimais). Para tráfego de túneis de data center, os roteadores vEdge usam encapsulamento IPsec ou GRE para enviar tráfego de dados entre si. Para a detecção de falhas do plano de dados e a medição do desempenho, os roteadores enviam periodicamente uns aos outros pacotes BFD. Esses pacotes BFD também são marcados com um valor DSCP CS6 (48 decimais).

Do ponto de vista do ISP, esse tipo de tráfego será visto como tráfego UDP com o valor de DSCP CS6, também porque os roteadores vEdge e os controladores SD-WAN copiam o DSCP que marca no cabeçalho IP externo por padrão.

Aqui está como se pareceria se o tcpdump fosse executado no roteador do ISP de trânsito:

```
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
```

Como pode ser visto aqui, todos os pacotes são marcados com o byte TOS 0xc0 também conhecido como campo DS (que é igual a decimal 192 ou 110 000 00 em binário. Os primeiros 6 bits de ordem superior correspondem ao valor de 48 bits DSCP em decimal ou CS6).

Os primeiros 2 pacotes na saída correspondem a um túnel de plano de controle e os 2 que permanecem, a um tráfego de túnel de plano de dados. Com base no comprimento do pacote e na marcação TOS, ele pode concluir com alta confiança que foram pacotes BFD (direções RX e TX). Esses pacotes também são marcados com CS6.

Às vezes, alguns provedores de serviços, especialmente os provedores de serviços VPN MPLS L3 VPN/MPLS L2, podem manterSLA diferente com o cliente e pode lidar com uma classe diferente de tráfego com base na marcação DSCP do cliente de forma diferente. Por exemplo, você pode ter um serviço premium para priorizar o tráfego de sinalização e voz DSCP EF e CS6. Como o tráfego de prioridade é quase sempre policiado, mesmo que a largura de banda total de um uplink não seja excedida, para esse tipo de perda de pacote de tráfego pode ser vista e, portanto, sessões de BFD também podem estar oscilando.

Em alguns casos, observou-se que, se a fila de prioridade dedicada no roteador do provedor de serviços estiver esgotada, você não verá nenhuma queda no tráfego normal (por exemplo, executar ping simples a partir do roteador vEdge) porque esse tráfego é marcado com o valor de DSCP padrão 0 como pode ser visto aqui (byte TOS):

```
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
```

Mas, ao mesmo tempo, suas sessões BFD estarão oscilando:

```
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
```

E aqui vem **nping** útil para solucionar problemas:

```
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
```

Debug BFD

Às vezes, se for necessária uma investigação mais profunda, você pode querer executar a depuração do BFD no roteador vEdge. O FTM (Forwarding Traffic Manager, Gerenciador de Tráfego de Encaminhamento) é responsável pelas operações de BFD em roteadores vEdge e, portanto, você precisa de **debug ftm bfd**. Toda saída de depuração é armazenada no arquivo **/var/log/tmplog/vdebug** e, se você quiser ter essas mensagens no console (semelhante ao comportamento do **monitor terminal** do Cisco IOS), você pode usar o **monitor start /var/log/tmplog/vdebug**. Para interromper o registro, você pode usar o **monitor stop /var/log/tmplog/vdebug**. Veja como a saída será para a sessão BFD que fica inativa devido ao tempo limite (TLOC remoto com endereço IP 192.168.110.6 não pode mais ser alcançada):

```
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
```

Outra depuração valiosa para habilitar é que eventos de depuração do TTM (Tunnel Traffic Manager) são **eventos de depuração do ttm**. Veja a aparência do evento BFD DOWN da perspectiva do TTM:

```
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
```

Informações Relacionadas

- Documentação do produto SDWAN
- Anatomia: Uma visão interna dos tradutores de endereços de rede
- Suporte Técnico e Documentação - Cisco Systems