Risoluzione dei problemi di rilevamento inoltro bidirezionale e connessioni del piano dati

Sommario

Introduzione

In questo documento vengono descritti i problemi di connessione del piano dati che potrebbero verificarsi sui router vEdge dopo la connessione al piano di controllo, ma non è ancora disponibile la connettività del piano dati tra i siti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della soluzione SDWAN (Software Defined Wide Area Network) di Cisco.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Nota:** Tutti gli output dei comandi presentati in questo documento provengono da router vEdge, ma l'approccio per la risoluzione dei problemi sarà lo stesso per il router con software IOS®-XE SDWAN. Usare la parola chiave **sdwan** per ottenere gli stessi output sul software IOS®-XE SDWAN. Ad esempio, **visualizzare le connessioni dei controlli sdwan** anziché **mostrare le connessioni dei controlli**.

Informazioni sul piano di controllo

Controllo proprietà locali controllo

Per controllare lo stato delle interfacce WAN (Wide Area Network) su un vEdge, usare il comando **show control local-properties wan-interface-list**. In questo output, è possibile vedere il tipo RFC 4787 Network Address Translation (NAT). Quando vEdge è dietro un dispositivo NAT (firewall, router, ecc.), gli indirizzi IPv4 pubblici e privati, le porte UDP (Public and Private Source User Datagram Protocol) vengono utilizzate per costruire i tunnel del piano dati. È anche possibile trovare lo stato dell'interfaccia del tunnel, il colore e il numero massimo di connessioni di controllo configurate.

```
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
```

Grazie a questi dati, è possibile identificare alcune informazioni su come costruire i tunnel di dati e sulle porte da usare nella prospettiva dei router quando si formano i tunnel di dati.

Controlla connessioni di controllo

Èimportante assicurarsi che il colore che non forma i tunnel del piano dati abbia una connessione di controllo stabilita con i controller nella sovrapposizione. In caso contrario, vEdge non invia le informazioni TLOC (Transport Locator) a vSmart tramite OMP (Overlay Management Protocol). È possibile verificare se è attivo o meno utilizzando il comando **show control connections** e cercare lo stato **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 l'interfaccia che non forma i tunnel di dati tenta di connettersi, è possibile risolverlo attivando con successo le connessioni di controllo tramite quel colore. In alternativa, è possibile risolvere il problema impostando il valore **max-control-connections 0** nell'interfaccia selezionata nella sezione tunnel interface (interfaccia tunnel).

```
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
 !
```

> **Nota:** A volte, è possibile utilizzare il comando **no control-connections** per raggiungere lo stesso obiettivo. Tuttavia, questo comando non stabilisce un numero massimo di connessioni di controllo. Questo comando è deprecato a partire dalla versione 15.4 e non deve essere utilizzato con software più recente.

Overlay Management Protocol

Controllare se i TLOC OMP sono annunciati dai bordi

Come si è notato, nel passaggio precedente, i TLOC OMP non possono essere inviati perché l'interfaccia tenta di formare connessioni di controllo tramite quel colore e non è in grado di raggiungere i controller. Verificare quindi se il colore non funzionante o non funzionante nei tunnel dati invia il TLOC per quel particolare colore a vSmarts. Per controllare i TLOC inviati ai peer OMP, utilizzare il comando **show omp tlocs annunciato**.

Esempio: Colori **mpls** e **gold**. Nessun TLOC inviato a vSmart per mpls a colori.

```
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
```

Esempio: Colori **mpls** e **gold**. Viene inviato TLOC per entrambi i colori.

```
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
```

Nota: Per qualsiasi informazione sul control plane generata localmente, il campo "FROM PEER" (PEER DA) verrà impostato su 0.0.0.0. Quando si cercano informazioni originate localmente, assicurarsi di trovare una corrispondenza in base a questo valore.

Verificare che vSmart riceva e annunci i TLOC

Ora che si è a conoscenza che i TLOC vengono pubblicizzati su vSmart, confermare che riceve i TLOC dal peer corretto e pubblicizzarli sull'altro vEdge.

Esempio: vSmart riceve i TLOC dalla versione 1.1.1.20 di 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        -
```

Se i TLOC non sono visualizzati o se sono visualizzati altri codici, verificare quanto segue:

```
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        -
```

Verificare se non esistono criteri che bloccano i TLOC.

show run policy control-policy-cerca qualsiasi elenco di contatti che impedisca l'annuncio o la ricezione dei TLOC nello 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.
```

Nota: Se un TLOC viene rifiutato o non valido, non verrà annunciato agli altri spigoli.

Assicurarsi che un criterio non filtri il TLOC quando viene annunciato da vSmart. È possibile notare che il TLOC viene ricevuto su vSmart, ma non verrà visualizzato sull'altro vEdge.

Esempio 1: vSmart con TLOC in 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        -
```

Esempio 2: vEdge1 non vede il TLOC di colore blu di vEdge2. Vede solo il TLOC MPLS.

```
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
```

Quando si controlla il criterio, è possibile verificare il motivo per cui il TLOC non viene visualizzato sul 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
 !
!
```

Rilevamento inoltro bidirezionale

Informazioni sul comando show bfd sessions

Di seguito sono riportati gli elementi chiave da cercare nell'output:

```
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 SISTEMA**: Peer system-ip
- **SOURCE (ORIGINE) e REMOTE TLOC COLOR (CONTROLLO REMOTO)**: Ciò è utile per conoscere il valore di TLOC che si prevede di ricevere e inviare.
- **IP DI ORIGINE:** Si tratta dell'IP di origine **privata**. Se si è dietro un NAT, queste informazioni non verranno visualizzate qui (è possibile visualizzarle utilizzando il comando **show control local-properties <wan-interface-list>** spiegato all'inizio del documento).
- **IP PUBBLICO DST**: Si tratta della destinazione utilizzata da vEdge per formare il tunnel Data Plane, indipendentemente dal fatto che si trovi dietro NAT o meno. (Esempio: Spigoli collegati direttamente a Internet o collegamenti MPLS (Multi-Protocol Label Switching)
- **DST PUBLIC PORT:** porta pubblica NAT utilizzata dal vEdge per formare il tunnel Data Plane sul vEdge remoto.
- **TRANSIZIONI**: Numero di volte in cui lo stato della sessione BFD è stato modificato, da NA a UP e viceversa.

Comando show tunnel statistics

Il comando **show tunnel statistics** può visualizzare informazioni sui tunnel del piano dati, e permette di verificare facilmente se si inviano o ricevono pacchetti per un particolare tunnel IPSEC tra i bordi. In questo modo è possibile capire se i pacchetti vengono creati su entrambe le estremità e isolare i problemi di connettività tra i nodi.

Nell'esempio, quando si esegue il comando più volte, è possibile notare un incremento o nessun incremento in **tx-pkts** o **rx-pkts**.

> **Suggerimento**: Se il contatore per l'incremento di tx-pkts viene utilizzato, i dati vengono trasmessi al peer. Se il pkts rx non aumenta, significa che non si ricevono dati dal peer. In questo caso, controllare l'altra estremità e verificare se il pacchetto tx è in aumento.

```
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
```

Un altro comando utile è **show tunnel statistics bfd**, che può essere usato per controllare il numero di pacchetti BFD inviati e ricevuti in un particolare tunnel data plane:

```
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
```

Elenco accessi

L'elenco degli accessi è un passaggio utile e necessario dopo aver esaminato l'output **show bfd session**. Ora che gli IP e le porte pubblici e privati sono noti, è possibile creare un elenco di controllo di accesso (ACL) che corrisponda a SRC_PORT, DST_PORT, SRC_IP, DST_IP. Ciò consente di confermare se si ricevono e inviano messaggi BFD.

Di seguito è riportato un esempio di configurazione di un 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
!
!
!
```

Nell'esempio, questo ACL usa due sequenze. La sequenza 10 corrisponde ai messaggi BFD inviati da questo vEdge al peer. La sequenza 20 fa l'opposto.

Corrisponde alle porte di origine (**Private**) e di destinazione (**Public**). Se vEdge utilizza NAT, verificare che le porte di origine e di destinazione siano corrette.

Per controllare gli accessi a ogni contatore di sequenza, usare il comando **show policy access-list counters <nome elenco accessi>**

```
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
```

Network Address Translation

Come utilizzare gli strumenti stun-client per rilevare il mapping e il filtro NAT

Se sono stati eseguiti tutti i passaggi descritti e si è dietro NAT, il passaggio successivo consiste

nell'identificare il comportamento del mapping e del filtro NAT UDP (RFC 4787). Questo strumento è molto utile per individuare l'indirizzo IP esterno vEdge locale quando il vEdge si trova dietro un dispositivo NAT. Questo comando ottiene un mapping delle porte per il dispositivo e facoltativamente individua le proprietà relative al NAT tra il dispositivo locale e un server (server pubblico: esempio di google stun server).

Nota: Per maggiori informazioni, visitare il sito: Docs Viptela - Client 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
```

Nelle versioni più recenti del software, la sintassi può essere leggermente diversa:

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

Nell'esempio, viene eseguito un test di rilevamento NAT completo con l'utilizzo della porta di origine UDP 12386 sul server Google STUN. L'output di questo comando fornirà il comportamento NAT e il tipo di filtro NAT basato sulla RFC 4787.

Nota: Quando si utilizzano **strumenti di stordimento**, tenere presente che, in caso contrario, il servizio STUN non funzionerà. Usare **allow-service stun** per far passare i dati di stordimento.

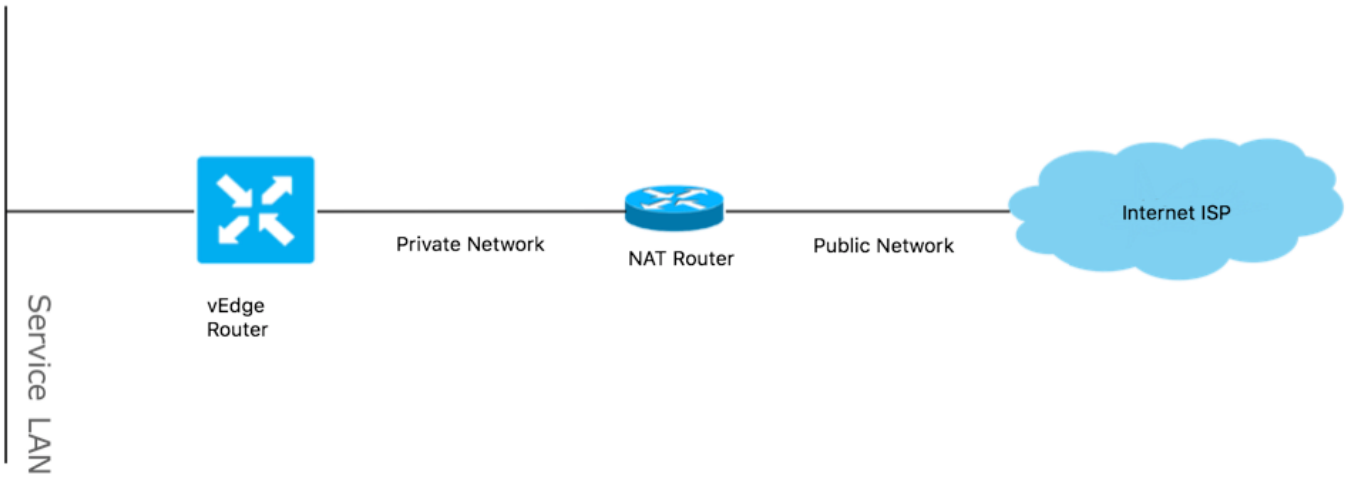
```
vEdge1# show running-config vpn 0 interface ge0/0
vpn 0
 interface ge0/0
  ip address 10.19.145.2/30
  !
  tunnel-interface
   encapsulation ipsec
   color gold
   max-control-connections 1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   no allow-service icmp
   no allow-service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

Questo mostra la mappatura tra la terminologia STUN (Full-Cone NAT) e la RFC 4787 (NAT Behavioral for 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

Tipi NAT supportati per tunnel Data Plane

Nella maggior parte dei casi, i colori pubblici come internet-biz o internet-pubblico possono essere collegati direttamente a internet. In altri casi, ci sarà un dispositivo NAT dietro l'interfaccia WAN vEdge e l'effettivo Internet Service Provider, quindi il vEdge può avere un IP privato e l'altro dispositivo (router, firewall, ecc.) può essere il dispositivo con gli indirizzi IP pubblici.



Se il tipo NAT non è corretto, potrebbe essere una delle cause più comuni che non consentono la formazione di tunnel Data Plane. Questi sono i tipi NAT supportati.

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**

Firewall

Se il NAT è già stato controllato e non è nei tipi di origine e destinazione non supportati, è possibile che un firewall blocchi le porte utilizzate per formare i tunnel del piano dati.

Verificare che queste porte siano aperte nel firewall per le connessioni Data Plane: vEdge to vEdge Data Plane:

UDP da 12346 a 13156

Per le connessioni di controllo da vEdge ai controller:

UDP da 12346 a 13156

da TCP 23456 a 24156

Accertarsi di aprire queste porte per completare correttamente la connessione dei tunnel del piano dati.

Quando si controllano le porte di origine e di destinazione usate per i tunnel del piano dati, è possibile usare **show tunnel statistics** o **show bfd session | scheda** ma non **mostra sessioni bfd.** Non verranno visualizzate porte di origine, ma solo porte di destinazione, come mostrato di seguito:

```
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
```

Nota: Per ulteriori informazioni sulle porte firewall SD-WAN utilizzate, consultare qui.

Sicurezza

Se si nota che il contatore ACL sta aumentando in entrata e in uscita, controllare diverse iterazioni per **visualizzare la differenza delle statistiche di sistema** e verificare che non vi siano cali.

```
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
```

In questo output, **rx_replay_integration_drops** aumenta ad ogni iterazione del 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
```

Eseguire innanzitutto una **richiesta di sicurezza ipsec**-rekey su vEdge. Quindi, eseguire diverse iterazioni di **show system statistics diff** e verificare se è ancora visibile **rx_replay_integration_drops**. In caso contrario, verificare la configurazione di protezione.

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

Se si dispone della configurazione indicata, provare ad aggiungere **ah-no-id** al tipo di autenticazione in ipsec.

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

> **Suggerimento**: ah-no-id abilita una versione modificata di AH-SHA1 HMAC ed ESP HMAC-SHA1 che ignora il campo ID nell'intestazione IP esterna del pacchetto. Questa opzione supporta alcuni dispositivi non Viptela, tra cui Apple AirPort Express NAT, che hanno un bug che provoca la modifica del campo ID nell'intestazione IP, un campo non modificabile. Configurare l'opzione ah-no-id nell'elenco dei tipi di autenticazione in modo che il software Viptela AH ignori il campo ID nell'intestazione IP in modo che il software Viptela possa funzionare insieme a questi dispositivi

Problemi dell'ISP con il traffico contrassegnato DSCP

Per impostazione predefinita, tutto il traffico di controllo e gestione dal router vEdge ai controller viene trasferito sulle connessioni DTLS o TLS e contrassegnato con un valore DSCP CS6 (48 decimali). Per il traffico dei tunnel della postazione dati, i router vEdge utilizzano l'incapsulamento IPsec o GRE per scambiare il traffico dati. Per il rilevamento degli errori del piano dati e la misurazione delle prestazioni, i router si inviano periodicamente pacchetti BFD. Questi pacchetti BFD sono contrassegnati anche con un valore DSCP CS6 (48 decimali).

Dal punto di vista dell'ISP, questo tipo di traffico verrà considerato come traffico UDP con valore DSCP CS6, in quanto i router vEdge e i controller SD-WAN copiano il DSCP che contrassegna per impostazione predefinita l'intestazione IP esterna.

Di seguito viene riportato un esempio di esecuzione di tcpdump su un router ISP di transito:

```
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
```

Come si può vedere qui, tutti i pacchetti sono contrassegnati con il byte TOS 0xc0, noto anche come campo DS (che equivale al decimale 192, o 110 000 00 in binario). I primi 6 bit di ordine superiore corrispondono ai bit DSCP (valore 48 in decimale o CS6).

I primi 2 pacchetti in uscita corrispondono a un tunnel del control plane e i 2 che rimangono, al traffico di un tunnel del data plane. In base alla lunghezza del pacchetto e al contrassegno TOS, può concludere con grande sicurezza che si tratta di pacchetti BFD (direzioni RX e TX). Anche questi pacchetti sono contrassegnati con CS6.

In alcuni casi è possibile che alcuni provider di servizi, in particolare MPLS L3 VPN/MPLS L2 VPN, mantenganoSLA diversi con il cliente e può gestire una classe diversa di traffico in base al contrassegno DSCP del cliente in modo diverso. Ad esempio, è possibile disporre di un servizio premium per assegnare priorità al traffico voce e di segnalazione DSCP EF e CS6. Poiché il traffico prioritario viene quasi sempre monitorato, anche se la larghezza di banda totale di un uplink non viene superata, per questo tipo di traffico è possibile rilevare la perdita di pacchetti e quindi anche le sessioni BFD possono lampeggiare.
In alcuni casi, è stato rilevato che se la coda di priorità dedicata sul router del provider di servizi è ridotta a icona, non si verificheranno cali per il traffico normale (ad esempio, l'esecuzione di **ping** semplice dal router vEdge) perché il traffico è contrassegnato con il valore DSCP predefinito 0, come mostrato di seguito (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
```

Ma allo stesso tempo, le sessioni del BFD lampeggiano:

```
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 qui **ping** si rivela utile per risolvere i problemi:

```
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

In alcuni casi, se è necessaria un'analisi più approfondita, è possibile eseguire il debug di BFD sul router vEdge. Forwarding Traffic Manager (FTM) è responsabile delle operazioni BFD sui router vEdge e pertanto è necessario eseguire il **debug ftm bfd**. Tutti gli output del debug sono memorizzati nel file **/var/log/tmplog/vdebug** e se si desidera che tali messaggi siano presenti sulla console (in modo simile al comportamento di Cisco IOS® **terminal monitor**), è possibile utilizzare **monitor start /var/log/tmplog/vdebug**. Per interrompere la registrazione, è possibile utilizzare **monitor stop /var/log/tmplog/vdebug**. Di seguito viene riportato l'aspetto dell'output per la sessione BFD che viene interrotta a causa del timeout (il TLOC remoto con indirizzo IP 192.168.110.6 non è più raggiungibile):

```
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
```

Un altro importante comando di debug che è possibile abilitare è il debug degli eventi di Tunnel Traffic Manager (TTM): il debug degli **eventi TTM**. Ecco come appare l'evento BFD DOWN dalla prospettiva di 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
```

Informazioni correlate

- Documentazione del prodotto SDWAN
- Anatomia: Informazioni approfondite sui traduttori di indirizzi di rete
- Documentazione e supporto tecnico – Cisco Systems