Problemen oplossen met bidirectioneel doorsturen van detectie en datacenter-verbindingen

Inhoud

Inleiding

Dit document beschrijft problemen met de datalink-verbinding die mogelijk kunnen ontstaan op vEdge-routers nadat u met succes verbinding hebt gemaakt met het besturingsplane, maar er is nog steeds geen datalink tussen de sites.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van Cisco-softwaregedefinieerde SDWAN-oplossing (Wide Area Network).

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

> Opmerking: Alle opdrachtoutput die in dit document wordt gepresenteerd, komt van vEdge-routers, maar de probleemoplossing is dezelfde als de router die IOS®-XE SDWAN-software uitvoert. Gebruik het sleutelwoord **van** dwan om de zelfde output op IOS:-XE SDWAN software te krijgen. Bijvoorbeeld; **toon sdwan controleverbindingen** in plaats van **tonen controleverbindingen**.

Informatie over het besturingsplane

Local Properties controleren

Om de status van de WAN-interfaces (Wide Area Network) op een vEdge te controleren, **gebruikt** u de **besturing van de lokale eigenschappen van een interface-lijst**. In deze uitvoer kunt u het RFC 4787 Type netwerkadresomzetting (NAT) zien. Wanneer de vEdge achter een NAT-apparaat staat (Firewall, router, etc.), worden Publiek en Private IPv4-adres, Publiek en Private Source User Datagram Protocol (UDP)-poorten gebruikt om de gegevensvliegtuigtunnels te bouwen. U kunt ook de status van de tunnelinterface, de kleur en het maximale aantal geconfigureerde bedieningsverbindingen vinden.

```
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
```

Met deze gegevens kunt u bepaalde informatie identificeren over hoe de gegevenstunnels moeten worden gebouwd en welke poorten u vanuit het routerperspectief moet verwachten om te gebruiken wanneer u de gegevenstunnels vormt.

Aansluitingen controleren

Het is van belang ervoor te zorgen dat de kleur die geen datatununtunnels vormt, wel een regelverbinding heeft met de controllers in de overlay. Anders stuurt de vEdge geen informatie over Transport Locator (TLOC) naar vSmart via Overlay Management Protocol (OMP). U kunt er

zeker van zijn of dit al dan niet is met het gebruik van de opdracht **Show control connecties** en u kunt op de **state-**connectie **zoeken**.

```
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
```

Als de interface die geen datastuntunnels vormt probeert aan te sluiten, kunt u deze oplossen door de besturingsverbindingen via die kleur succesvol op te halen. Of, u kunt errond werken door de **max-controle-connecties 0** in de geselecteerde interface onder het vak van de tunnelinterface in te stellen.

```
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
 !
```

> Opmerking: Soms kan je de opdracht **geen control-connecties** gebruiken om hetzelfde doel te bereiken. Deze opdracht bevat echter geen maximum aantal bedieningsverbindingen. Deze opdracht wordt vanaf 15.4 afgevoerd en mag niet op nieuwere software worden gebruikt.

Overlay Management-Protocol

Controleer of de OMP-TLOC's vanaf de vEdge geadverteerd zijn

Zoals u hebt opgemerkt, kan in de vorige stap OMP TLOCs niet worden verzonden omdat de interface probeert om bedieningsverbindingen via die kleur te vormen en niet in staat is om de

controllers te bereiken. Controleer dus of de kleur die de data tunnels niet werken of omhoog komen de TLOC voor die bepaalde kleur naar de vSmarts stuurt. Gebruik de opdracht **show omp tlocs geadverteerd** om de TLOC's te controleren die naar de OMP-peers worden verzonden.

Voorbeeld: Kleuren **splitsen** en **goud**. Er wordt geen TLOC naar vSmart verzonden voor kleurenmodellen.

```
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
```

Voorbeeld: Kleuren **splitsen** en **goud**. TLOC wordt voor beide kleuren verzonden.

```
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
```

Opmerking: Voor informatie over lokaal gegenereerde besturingsplane wordt het veld "VANAF PEER" ingesteld op 0.0.0.0. Wanneer u lokaal gemaakte informatie opzoekt, dient u deze op basis van deze waarde bij elkaar te passen.

Controleer of de vSmart de TLOC's ontvangt en adverteert

Nu u weet dat uw TLOCs aan vSmart worden geadverteerd, bevestig dat deze TLOCs van de juiste peer ontvangt en naar de andere vEdge adverteert.

Voorbeeld: vSmart ontvangt de TLOC's van 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        -
```

Voor het geval u de TLOC's niet ziet of u hier geen andere codes ziet, kunt u deze controleren:

```
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        -
```

Controleer of er geen beleid is dat de TLOC's blokkeert.

Stel beleidscontrole-beleid-op voor elke tloc-lijst die uw TLOCs ervan afwijst dat ze in het vSmart geadverteerd of ontvangen worden.

```
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.
```

> Opmerking: Als een TLOC wordt verworpen of ongeldig wordt, wordt deze niet naar de andere vEdge geadverteerd.

Zorg ervoor dat een beleid de TLOC niet filtert wanneer het van de vSmart wordt geadverteerd. U kunt zien dat de TLOC is ontvangen op vSmart, maar u ziet het niet op de andere vEdge.

Voorbeeld 1: vSmart met 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        -
```

Voorbeeld 2: vEdge1 ziet de TLOC niet van gekleurd blauw dat van vEdge2 komt. Het ziet alleen

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
```

Wanneer u het beleid controleert, kunt u zien waarom de TLOC niet op vEdge1 verschijnt.

```
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
 !
!
```

Detectie van bidirectionele doorsturen

Begrijp de opdracht van de showbips

Dit zijn de belangrijkste dingen die je in de output kunt vinden:

```
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
```

- SYSTEEM IP: Het systeem van peers-ip
- TLOC-KLEUR VOOR BRON- EN AFSTANDEN: Dit is handig om te weten wat TLOC je verwacht te ontvangen en te verzenden.
- BRON IP: Het is de privé-bron-IP. Als u achter een NAT zit, wordt deze informatie hier niet weergegeven (dit kan worden gezien met het gebruik van toonaangevende controle lokale eigenschappen <wan-interface-list> die aan het begin van het document wordt uitgelegd).
- OPENBARE IP VAN DST: Het is de bestemming die de vEdge gebruikt om de Data Plane-tunnel te vormen, ongeacht of deze achter NAT staat of niet. (Voorbeeld: Straalingen die rechtstreeks op internet zijn aangesloten of MPLS-koppelingen (Multi-Protocol Label Switching)
- OPENBARE POORT VAN DST: Openbare NAT-poort die door vEdge wordt gebruikt om de datalunnel naar de externe vEdge te vormen.
- OVERGANG: Aantal keren dat de BFD-sessie zijn status heeft gewijzigd, van NA naar UP en vice versa.

Tunnelstatistieken

De tonen tunnelstatistieken kunnen informatie over de gegevensvliegtuigtunnels tonen, kunt u gemakkelijk zien of u pakketten voor een bepaalde IPSEC-tunnel tussen de vRanden verzenden of ontvangt. Dit kan u helpen te begrijpen als pakketten het op elk eind maken, en verbindings kwesties tussen de knopen isoleren.

In het voorbeeld, wanneer u de opdracht meerdere keren uitvoert, kunt u een toename of geen toename in de belastingpkts of rx-pkts opmerken.

Tip: Als je teller voor de verhoging van de belastingtarieven is, geef je gegevens door naar de peer. Als uw rx-pkts niet verhogen betekent dit dat u geen gegevens van uw peer ontvangt. Controleer in dit geval het andere uiteinde en bevestig of de belastingpekts verhogen.

```
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
```

Een andere nuttige opdracht is **om tunnelstatistieken** te **tonen** die kunnen worden gebruikt om het aantal BFD - pakketten te controleren die binnen specifieke gegevenstunnel worden verzonden en ontvangen:

```
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
```

Toegangslijst

Een toegangslijst is een nuttige en noodzakelijke stap nadat u de uitvoer van **showsessies** bekijkt. Nu de privé, en openbare IPs en poorten bekend zijn, kunt u een Toegangscontrolelijst (ACL) maken om tegen de SRC_PORT, DST_PORT, SRC_IP, DST_IP aan te passen. Dit kan u helpen bevestigen of u BFD-berichten ontvangt en verstuurt of niet.

Hier vindt u een voorbeeld van een ACL-configuratie:

```
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
!
!
!
```

In het voorbeeld, gebruikt dit ACL twee sequenties. De sequentie 10 komt overeen met de BFD-berichten die van deze vEdge naar de peer worden verzonden. Sequence 20 doet het tegenovergestelde.

Het komt overeen met de bron (**Private**) port en de bestemming (**Public**) poorten. Als de vEdge NAT gebruikt, zorg er dan voor dat u de juiste bron- en doelpoorten controleert.

Om de hits op elke sequentietalom te controleren **toont** de **tellers van de beleidstoegang van de toegangslijst <access-list>**

```
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
```

Netwerkadresomzetting

Gebruik van werktuigen vanaf een client om NAT-afbeelding en filtering te detecteren

Als u alle vermelde stappen hebt gedaan en u achter NAT staat, is de volgende stap om het gedrag van UDP NAT Traversal (RFC 4787) in kaart te brengen en te filteren. Dit gereedschap is echt handig om het lokale vEdge externe IP-adres te ontdekken wanneer die vEdge zich achter een NAT-apparaat bevindt. Deze opdracht verkrijgt een poortafbeelding voor het apparaat en ontdekt optioneel eigenschappen over NAT tussen het lokale apparaat en een server (openbare server: voorbeeld google stun server).

> Opmerking: Zie voor meer informatie: DOCS Viptela - STUN-client

```
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
```

Op nieuwere versies van software kan de syntaxis iets anders zijn:

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

In dit voorbeeld voert u een volledige NAT-detectietest uit met behulp van UDP-bronpoort 12386 naar de Google STUN-server. De uitvoer van deze opdracht geeft u NAT-gedrag en het NAT-filtertype op basis van RFC 4787.

> Opmerking: Wanneer u **gereedschappen gebruikt**, vergeet dan de STUN-service toe te staan in de tunnelinterface, anders werkt dat niet. Gebruik **een hogerservice-stut** om de gegevens van de studie door te geven.

```
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
```

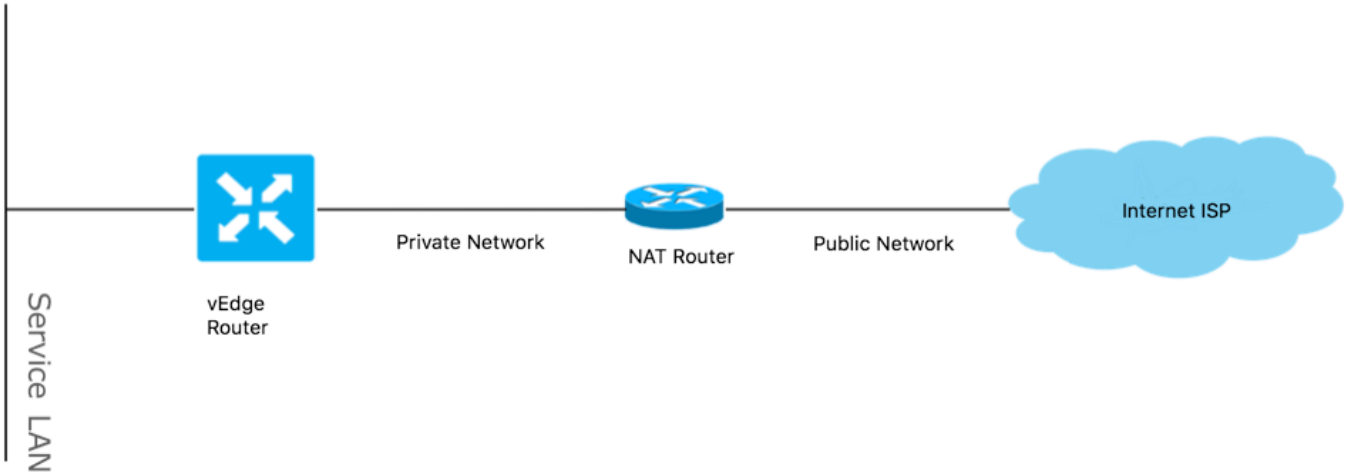
```
   max-control-connections 1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   no allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   allow-service stun
  !
  no shutdown
 !
!
```

Dit toont het in kaart brengen tussen STUN terminologie (Full-Cone NAT) en 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

Ondersteunde NAT-typen voor datacentertunnels

In de meeste gevallen kunnen je openbare kleuren als biz-internet of publiek-internet rechtstreeks op het internet worden aangesloten. In andere gevallen zal er een NAT-apparaat achter de vEdge WAN-interface en de huidige Internet Service Provider zijn, zodat de vEdge een privé-IP kan hebben en het andere apparaat (router, firewall, enzovoort) kan het apparaat zijn met de openbare naar IP-adressen.



Als u een onjuist NAT-type heeft, kan dit een van de meest voorkomende redenen zijn die de vorming van tunnels in het datacenter niet toestaan. Dit zijn de ondersteunde NAT-typen.

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

Als u al NAT en zijn niet in de niet-ondersteunde bron- en doeltypen hebt gecontroleerd, is het mogelijk dat een firewall de poorten blokkeert die gebruikt worden om de datacommunicatie te vormen.

Zorg ervoor dat deze poorten open zijn in de Firewall voor de verbindingen van het datacenter: vEdge naar vEdge-datacenter:

UDP 12346 tot 13156

Voor besturingsverbindingen van vEdge naar controllers:

UDP 12346 tot 13156

TCP 23456 tot 24156

Zorg ervoor dat u deze poorten opent om een succesvolle verbinding van de tunnels van het datacentrum te bereiken.

Wanneer u de bron en de bestemming havens controleert die voor gegevensvliegtuigtunnels worden gebruikt, kunt u **tunnelstatistieken** gebruiken of **schrijfsessies tonen | tab**, maar **toon geen ronde sessies.** Er worden geen bronpoorten weergegeven, alleen doelpoorten zoals u kunt zien:

```
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
```

Opmerking: U vindt hier meer informatie over de SD-WAN firewallpoorten.

Security

Als u ziet dat uw ACL teller binnen en uitgaande toeneemt, controleer dan meerdere iteraties **tonen systeemstatistieken diff** en zorg ervoor dat er geen druppels zijn.

```
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 deze output wordt **rx_replay_integer_drops** verhoogd met elke iteratie van de **show system statistics** opdracht.

```
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
```

Voer eerst een **verzoek om beveiliging** uit op **ipsec**-rekey op de vEdge. Vervolgens, ga door verschillende iteraties van **show system statistics diff** en zie of u nog **rx_replay_integer_drops** ziet. Kijk in de beveiligingsconfiguratie.

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

Als u de bovengenoemde configuratie hebt, probeer dan **ah-no-id** aan het authenticatietype onder ipsec toe te voegen.

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

> **Tip**: ah-no-id maakt een aangepaste versie mogelijk van AH-SHA1 HMAC en ESP HMAC-SHA1, waarmee het ID-veld in de buitenste IP-header van het pakket wordt genegeerd. Deze optie past een aantal niet-Viptela apparaten aan, die de Apple AirPort Express NAT omvatten, die een bug heeft die ervoor zorgt dat het ID veld in de IP-header, een niet-veranderbaar veld, wordt aangepast. Configureer de optie ah-no-id in de lijst met authenticatietypen om de Viptela AH-software het ID-veld in de IP-header te laten negeren, zodat de Viptela-software kan werken in combinatie met deze apparaten

ISP-problemen met DSCP gemarkeerd verkeer

Standaard reist alle controle- en beheerverkeer van de vEdge-router naar de controllers via DTLS- of TLS-verbindingen en gemarkeerd met een DSCP-waarde van CS6 (48 decimalen). Voor verkeer van datastuntunnels gebruiken vEdge-routers IPsec of GRE-insluiting om gegevensverkeer naar elkaar te verzenden. Voor de detectie en meting van gegevensvlakken verzenden routers elkaar periodiek BFD-pakketten. Deze BFD-pakketten worden ook gemarkeerd met een DSCP-waarde van CS6 (48 decimalen).

Vanuit het perspectief van ISP, zal dat type verkeer gezien worden als UDP-verkeer met DSCP waarde CS6, ook omdat vEdge-routers en SD-WAN controllers DSCP kopiëren die standaard naar de buitenste IP-header markeren.

Hier is hoe het eruit zou kunnen zien als tcPDump op router van doorvoerISP loopt:

```
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
```

Zoals hier te zien is, worden alle pakketten gemarkeerd met TOS byte 0xc0 ook bekend als DS veld (dat is gelijk aan decimale 192, of 110 000 00 in binair getal. Eerste 6 hoge bestelbits komen overeen met DSCP bits waarde 48 in decimale volgorde of CS6).

Eerst 2 pakketten in de uitvoer komen overeen met een besturingsplanetunnel en de 2 die overblijven met een tunnelverkeer. Op basis van de pakketlengte en de TOS-markering kan deze met groot vertrouwen concluderen dat het BFD-pakketten waren (RX- en TX-instructies). Deze pakketten worden ook gemarkeerd met CS6.

Soms kunnen sommige serviceproviders en vooral MPLS L3 VPN/MPLS L2 VPN-serviceprovidersverschillende SLA's met de klant en kunnen een andere klasse van verkeer op basis van DSCP-markering van de klant anders verwerken. U kunt bijvoorbeeld hoogwaardige service hebben om prioriteit te geven aan DSCP EF- en CS6-spraak- en signaleringsverkeer. Aangezien prioriteitsverkeer vrijwel altijd wordt gecontroleerd, zelfs als de totale bandbreedte van een uplink niet wordt overschreden, kan voor dit type verkeerspakketverlies worden gezien en kunnen BFD-sessies ook worden geflappeld.

In sommige gevallen werd gezien dat als de gewijde prioriteitswachtrij op serviceprovider-router is uitgehongerd, er geen druppels voor normaal verkeer zichtbaar zijn (bijvoorbeeld ping van vEdge-router uitvoeren) omdat dat verkeer wordt gemarkeerd met de standaard DSCP-waarde 0, zoals hier (TOS-byte) kan worden gezien:

```
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
```

Maar tegelijkertijd flauwvallen van uw BFD-sessies:

```
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
```

En hier **komt Nping** handig om het oplossen te regelen:

```
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

Soms, als het diepere onderzoek wordt vereist, zou u het zuiveren van BFD op de vEdge router kunnen willen uitvoeren. Forwarding Traffic Manager (FTM) is verantwoordelijk voor BFD-bewerkingen op vEdge-routers en daarom moet u **ftm-bfd deken** herstellen. Alle debugoutput wordt opgeslagen in **/var/log/tmplog/vdebug** bestand en als u die berichten op de console wilt hebben (gelijk aan Cisco IOS® **terminal monitor** gedrag) kunt u **monitorstart/var/log/log/stamlog/vdebug** gebruiken. Om de houtkap te stoppen, kunt u **monitorstop /var/log/tmplog/vdebug** gebruiken. Hier is hoe de output er uit zal zien als voor BFD-sessie die afneemt vanwege de tijdelijke versie (afstandsbediening met IP-adres 192.168.110.6 is niet meer bereikbaar):

```
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
```

Een ander waardevol debug om te stoppen zijn TTM-gebeurtenissen (Tunnel Traffic Manager) het **debug** van **ATM-gebeurtenissen**. Zo ziet BFD DOWN er uit vanuit het perspectief van 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
```

Gerelateerde informatie

- SDWAN-productdocumentatie
- Anatomie: Een blik in netwerkadresomzetting
- Technische ondersteuning en documentatie – Cisco Systems