Waarom kunnen vEdge-tunnels niet opzetten als NAT wordt gebruikt?

Inhoud

Inleiding

Dit document beschrijft het probleem dat kan ontstaan wanneer vEdge-routers IPSec-insluiting gebruiken voor datatootunnels en één apparaat achter Network Address Translation (NAT)-apparaat dat symmetrische NAT (RFC3489) of adresafhankelijke toewijzing (RFC4787) doet, terwijl een ander type Direct Internet Access (DIA) of een ander type NAT dat op de transportzijde is geconfigureerd is.

Achtergrondinformatie

> Opmerking: Dit artikel is alleen van toepassing op vEdge-routers en is geschreven op basis van het gedrag dat u hebt gezien in vEdge-software 18.4.1 en 19.1.0. In nieuwere releases kan het gedrag anders zijn. Raadpleeg de documentatie of neem contact op met het Cisco Technical Assistance Center (TAC) voor twijfel.

Ten behoeve van de demonstratie werd het probleem gereproduceerd in het SD-WAN TAC lab. De instellingen van het apparaat worden hier in de tabel samengevat:

hostname	steunpunt	systeemip	privé-ip	publiciteit
rand1	232	10.10.10.232	192.168.10.232	198.51.100.232
rand2	233	10.10.10.233	192.168.9.233	192.168.9.233
slim	1	10.10.10.228	192.168.0.228	192.168.0.228
obligatie	1	10.10.10.231	192.168.0.231	192.168.0.231

De configuratie aan de kant van het transport is vrij generiek op beide apparaten. Dit is de

configuratie van vEdge1:

```
vpn 0
 interface ge0/0
  ip address 192.168.10.232/24
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no 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
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0 192.168.10.11
!
```

vEdge2:

```
interface ge0/1
  ip address 192.168.9.233/24
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no 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
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0 192.168.9.1
```

Om het probleem in dit document te laten zien, bevindt de Virtual Adaptive Security Appliance (ASAv) firewall zich tussen twee vEdge-routers. ASAv doet adresvertalingen volgens deze regels:

- Indien verkeer vanaf vEdge1 bestemd is voor controllers, worden de bronpoorten 12346-12426 vertaald naar 52346-52426
- Indien het verkeer vanaf vEdge1 bestemd is voor datapoorten op andere locaties, worden bronpoorten 12346-12426 vertaald naar 42346-42426
- Al het andere verkeer vanaf vEdge1 is ook in kaart gebracht op hetzelfde openbare adres (198.51.100.232)

Dit is ASAv NAT-configuratie ter referentie:

```
object network VE1
 host 192.168.10.232
object network CONTROLLERS
 subnet 192.168.0.0 255.255.255.0
object network VE1_NAT
 host 198.51.100.232
object service CONTROL
 service udp source range 12346 12445 destination range 12346 12445
object service CC_NAT_CONTROLLERS
 service udp source range 52346 52445 destination range 12346 12445
object service CC_NAT_OTHER
 service udp source range 42346 42445 destination range 12346 12445
object network ALL
 subnet 0.0.0.0 0.0.0.0
nat (ve1-iface,ve2-iface) source static VE1 VE1_NAT destination static CONTROLLERS CONTROLLERS
service CONTROL CC_NAT_CONTROLLERS
nat (ve1-iface,ve2-iface) source static VE1 VE1_NAT destination static ALL ALL service CONTROL
CC_NAT_OTHER
nat (ve1-iface,ve2-iface) source dynamic VE1 VE1_NAT
```

Probleem

Werkscenario

In de normale toestand kunnen we zien dat datatootunnels worden geïnstalleerd, Bidirectional Forwarding Detection (BFD) in **up** state is.

Let op welke openbare poort gebruikt is op vEdge1-apparaat (52366) om bedieningsverbindingen met controllers tot stand te brengen:

```
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                    198.51.100.232  52366  192.168.10.232  ::
12366    2/1  biz-internet     up     2      no/yes/no   No/No  0:00:00:28   0:11:59:17  N    5
```

Op vEdge2 wordt geen NAT gebruikt, dus privé-adres en poorten zijn hetzelfde:

```
vEdge2# 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
--------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------
-----------
ge0/1                   192.168.9.233   12366  192.168.9.233   ::
12366    2/1  biz-internet     up     2      no/yes/no   No/No  0:00:00:48   0:11:58:53  N    5
```

In de **show tunnel** statistieken van vEdge1 zien we dat de hoeveelheid TX/RX tellers toeneemt:

```
vEdge1# show tunnel statistics dest-ip 192.168.9.233

TCP
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     192.168.10.232  192.168.9.233  12366   12366  10.10.10.233  biz-internet  biz-internet
1441    223      81163      179      40201      1202
```

Vanaf dezelfde uitvoer van vEdge2 kunt u zien dat tellers van rx-/rx-pakketten ook toenemen. Merk op dat de bestemmingshaven (42366) verschilt van de haven die wordt gebruikt om controleverbindingen aan te leggen (52366):

```
vEdge2# show tunnel statistics dest-ip 198.51.100.232

TCP
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     192.168.9.233  198.51.100.232  12366   42366  10.10.10.232  biz-internet  biz-internet
1441    296      88669      261      44638      1201
```

Maar BFD sessies zijn nog steeds in beide richtingen:

```
vEdge1# show bfd sessions site-id 233 | tab

                                    SRC    DST                 SITE
DETECT      TX
SRC IP          DST IP         PROTO  PORT   PORT   SYSTEM IP     ID    LOCAL COLOR   COLOR
STATE  MULTIPLIER  INTERVAL  UPTIME      TRANSITIONS
```

```
------------------------------------------------------------------------------------------------
------------------------------------------------------
192.168.10.232  192.168.9.233  ipsec  12366  12366  10.10.10.233  233   biz-internet  biz-
internet  up     7           1000      0:00:02:42  0



vEdge2# show bfd sessions site-id 232 | tab

                                     SRC    DST                  SITE
DETECT      TX
SRC IP          DST IP          PROTO  PORT   PORT   SYSTEM IP     ID    LOCAL COLOR   COLOR
STATE  MULTIPLIER  INTERVAL  UPTIME      TRANSITIONS
------------------------------------------------------------------------------------------------
------------------------------------------------------
192.168.9.233  198.51.100.232  ipsec  12366  52366  10.10.10.232  232   biz-internet  biz-
internet  up     7           1000      0:00:03:00  0
```

Verschillende poorten die gebruikt worden voor controle- en dataplatingen veroorzaken geen problemen, er is connectiviteit.

Foutenscenario

De gebruiker wil Direct Internet Access (DIA) op vEdge2-router inschakelen. Om dit te doen, werd deze configuratie toegepast op vEdge2:

```
vpn 0
 interface ge0/1
  nat
   respond-to-ping
  !
 !
!
vpn 1
 ip route 0.0.0.0/0 vpn 0
!
```

En de BFD-sessie ging onverwacht omlaag en blijft bovendien in de slechte staat steken. Na het verruimen van tunnelstatistieken kunt u zien dat RX teller niet toeneemt in de output van toontunnelstatistieken:

```
vEdge2# show tunnel statistics dest-ip 198.51.100.232


TCP
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     192.168.9.233  198.51.100.232  12346   52366  10.10.10.232  biz-internet  biz-internet
1442    282      48222      0        0          1368

vEdge2# show bfd sessions site-id 232
                                     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
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
-------------
10.10.10.232     232      down        biz-internet     biz-internet     192.168.9.233
198.51.100.232                  52366       ipsec  7           1000           NA              0

vEdge2# show tunnel statistics dest-ip 198.51.100.232


TCP
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     192.168.9.233  198.51.100.232  12346   52366  10.10.10.232  biz-internet  biz-internet
1442    285      48735      0        0          1368
```

Aanvankelijk vermoedde de klant dat het probleem met de MTU van de Tunnel zich voordeed. Als je uitgangen hierboven vergelijkt met uitgangen van het gedeelte "Working Scenario", dan kan je opmerken dat in een werkscenario de MTU 1441 tegen 1442 is in het mislukte scenario. Gebaseerd op de documentatie, zou de MTU van de Tunnel 1442 moeten zijn (1500 standaard MTU - 58 bytes voor overhead), maar eens BFD Tunnel is, Tunnel, Tunnel. Het MTU wordt met 1 bytes verlaagd. Voor uw referentie **tonen** output van **tunnelstatistieken** samen met **tonen tunnelstatistieken** die hieronder worden verstrekt voor gevallen wanneer BFD in **lagere** staat is:

```
vEdge1# show tunnel statistics dest-ip 192.168.9.233 ; show tunnel statistics bfd dest-ip
192.168.9.233


TCP
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     192.168.10.232  192.168.9.233  12346   12346  10.10.10.233  biz-internet  biz-internet
1442    133      22743      0        0          1362


                                                        BFD   BFD   BFD     BFD     BFD   BFD
BFD     BFD
                                                        ECHO  ECHO  ECHO    ECHO    PMTU  PMTU
PMTU    PMTU
TUNNEL                                    SOURCE  DEST  TX    RX    TX      RX      TX    RX
TX      RX
PROTOCOL  SOURCE IP       DEST IP         PORT    PORT   PKTS  PKTS  OCTETS  OCTETS  PKTS  PKTS
OCTETS  OCTETS
-------------------------------------------------------------------------------------------
----------------
ipsec     192.168.10.232  192.168.9.233  12346   12346  133   0     22743   0       0     0
0       0

vEdge1# show tunnel statistics dest-ip 192.168.9.233 ; show tunnel statistics bfd dest-ip
```

```
192.168.9.233


TCP
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     192.168.10.232  192.168.9.233  12346   12346  10.10.10.233  biz-internet  biz-internet
1442    134      22914      0        0          1362


                                                          BFD   BFD   BFD     BFD     BFD   BFD
BFD     BFD
                                                          ECHO  ECHO  ECHO    ECHO    PMTU  PMTU
PMTU    PMTU
TUNNEL                                    SOURCE  DEST    TX    RX    TX      RX      TX    RX
TX      RX
PROTOCOL  SOURCE IP       DEST IP         PORT    PORT    PKTS  PKTS  OCTETS  OCTETS  PKTS  PKTS
OCTETS  OCTETS
-------------------------------------------------------------------------------------------------
----------------
ipsec     192.168.10.232  192.168.9.233  12346   12346  134   0     22914   0       0     0
0       0
```

En als BFD in staat is:

```
vEdge1# show tunnel statistics dest-ip 192.168.9.233 ; show tunnel statistics bfd dest-ip
192.168.9.233 ;


TCP
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     192.168.10.232  192.168.9.233  12346   12346  10.10.10.233  biz-internet  biz-internet
1441    3541     610133     3504     592907     1361


                                                          BFD   BFD   BFD     BFD     BFD   BFD
BFD     BFD
                                                          ECHO  ECHO  ECHO    ECHO    PMTU  PMTU
PMTU    PMTU
TUNNEL                                    SOURCE  DEST    TX    RX    TX      RX      TX    RX
TX      RX
PROTOCOL  SOURCE IP       DEST IP         PORT    PORT    PKTS  PKTS  OCTETS  OCTETS  PKTS  PKTS
OCTETS  OCTETS
-------------------------------------------------------------------------------------------------
----------------
ipsec     192.168.10.232  192.168.9.233  12346   12346  3522  3491  589970  584816  19    13
20163   8091

vEdge1# show tunnel statistics dest-ip 192.168.9.233 ; show tunnel statistics bfd dest-ip
192.168.9.233 ;
```

```
TCP
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     192.168.10.232  192.168.9.233  12346   12346  10.10.10.233  biz-internet  biz-internet
1441    3542     610297     3505     593078     1361


                                                          BFD   BFD   BFD     BFD     BFD   BFD
BFD     BFD
                                                          ECHO  ECHO  ECHO    ECHO    PMTU  PMTU
PMTU    PMTU
TUNNEL                                    SOURCE  DEST    TX    RX    TX      RX      TX    RX
TX      RX
PROTOCOL  SOURCE IP       DEST IP         PORT    PORT    PKTS  PKTS  OCTETS  OCTETS  PKTS  PKTS
OCTETS  OCTETS
-------------------------------------------------------------------------------------------------
----------------
ipsec     192.168.10.232  192.168.9.233  12346   12346  3523  3492  590134  584987  19    13
20163   8091
```

> Opmerking: Trouwens, we kunnen de BFD-pakketgrootte en de insluiting bepalen door naar boven te kijken naar uitgangen. Merk op dat er slechts één BFD-pakket is ontvangen tussen twee uitgangen, waardoor de BFD Echo RX Octets waarde 584987 - 584816 ons 171-byte resultaat zal opleveren. Het kan nuttig zijn om de bandbreedte precies te berekenen die door BFD zelf wordt gebruikt.

De reden dat BFD in een lagere toestand vastzat is niet MTU, maar NAT-configuratie natuurlijk. Dit is het enige dat tussen het **werkscenario** en het **mislukte scenario** is veranderd. U kunt hier zien dat als resultaat van DIA-configuratie, NAT statische mapping automatisch door vEdge2 in de vertaaltabel is gemaakt om een omzeilingstaaf voor het gegevensvlak IPSec-verkeer mogelijk te maken:

```
vEdge2# show ip nat filter nat-vpn 0 nat-ifname ge0/1 vpn 0 protocol udp 192.168.9.233
198.51.100.232

                           PRIVATE                        PRIVATE  PRIVATE
PUBLIC  PUBLIC
NAT  NAT                   SOURCE         PRIVATE DEST    SOURCE   DEST     PUBLIC SOURCE
PUBLIC DEST     SOURCE  DEST    FILTER       IDLE        OUTBOUND  OUTBOUND  INBOUND  INBOUND
VPN  IFNAME  VPN  PROTOCOL  ADDRESS        ADDRESS         PORT     PORT     ADDRESS
ADDRESS         PORT    PORT    STATE        TIMEOUT     PACKETS   OCTETS    PACKETS  OCTETS
DIRECTION
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
------
0    ge0/1   0    udp       192.168.9.233  198.51.100.232  12346    52366    192.168.9.233
198.51.100.232  12346   52366   established  0:00:00:59  53        8321      0        0        -
```

Zoals u kunt zien, wordt poort 52366 gebruikt in plaats van 42366. Dit komt doordat vEdge2 52366 poorten verwacht en het geleerd heeft van OMP TLOCs geadverteerd door vSmart:

```
vEdge2# show omp tlocs ip 10.10.10.232 | b PUBLIC

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     10.10.10.232     biz-internet     ipsec  10.10.10.228     C,I,R     1
198.51.100.232   52366   192.168.10.232   12346    ::      0       ::       0        down
```

Oplossing

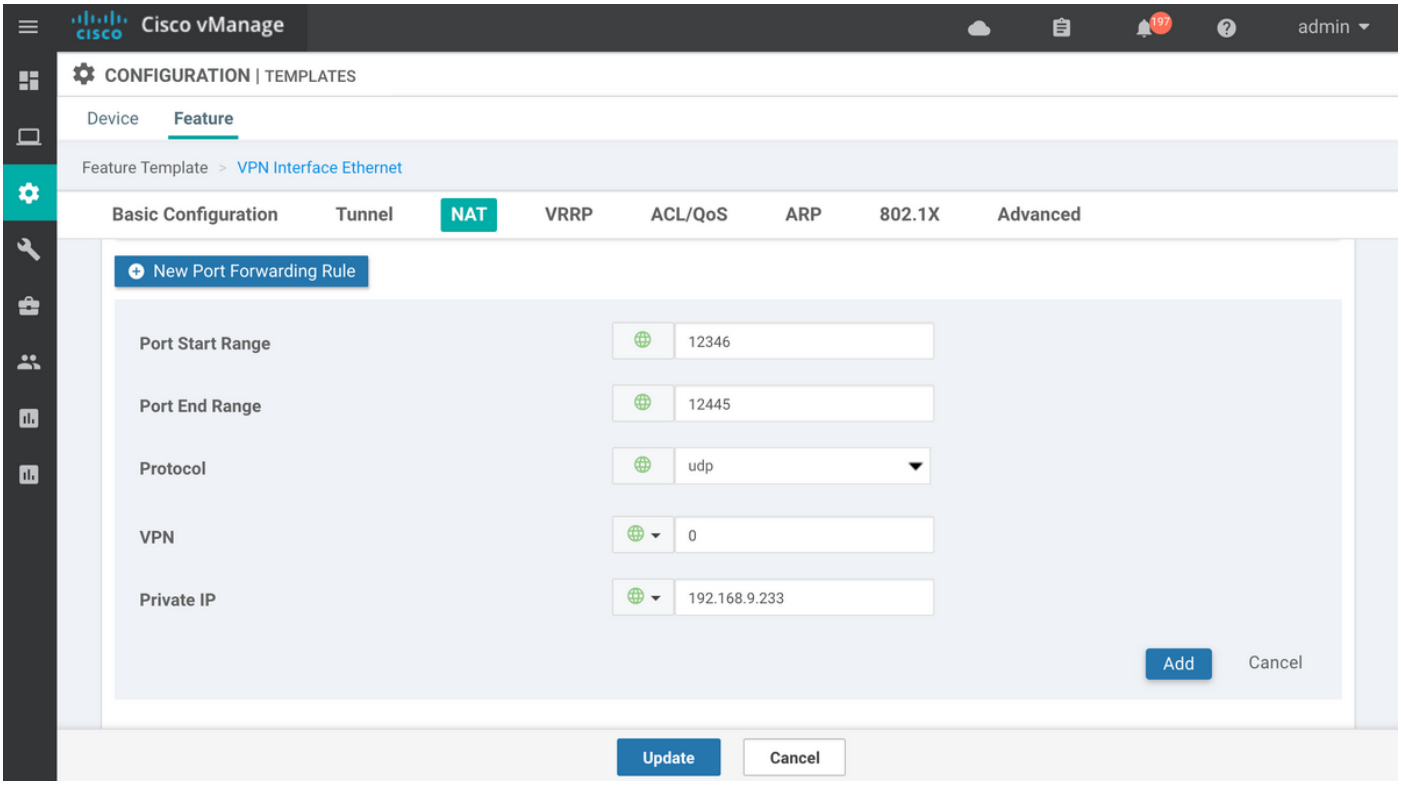
NAT poortvoorwaarts

Vanaf het eerste gezicht is het werken rondom dit soort problemen eenvoudig. U kunt het statische NAT vrijstellingspoort op vEdge2-transportinterface configureren om het filteren voor dataplatingen vanaf elke bron forceert:

```
vpn 0
 interface ge0/1
  nat
   respond-to-ping
   port-forward port-start 12346 port-end 12445 proto udp
    private-vpn        0
    private-ip-address 192.168.9.233
   !
  !
 !
!
```

Hier vindt u tussen 12346 en 12446 alle mogelijke startpoorten (12346, 12366, 12386, 12406 en 12426 plus poortoffset). Raadpleeg voor meer informatie hierover "Firewallpoorten voor Viptela-implementaties".

Als de sjablonen voor apparaatfuncties worden gebruikt in plaats van de CLI-sjabloon, moeten we vervolgens nieuwe VPN Ethernet-functiesjabloon voor corresponderende transport- (vpn 0) interface met **New Port Forwarding Rule**, zoals in de afbeelding getoond:



Expliciet ACL

Ook is een andere oplossing met een expliciete ACL mogelijk. Als **impliciet-acl-logging** is ingesteld onder **beleidssectie**, kunt u het volgende bericht opmerken in het **/var/log/tmplog/vdebug** bestand:

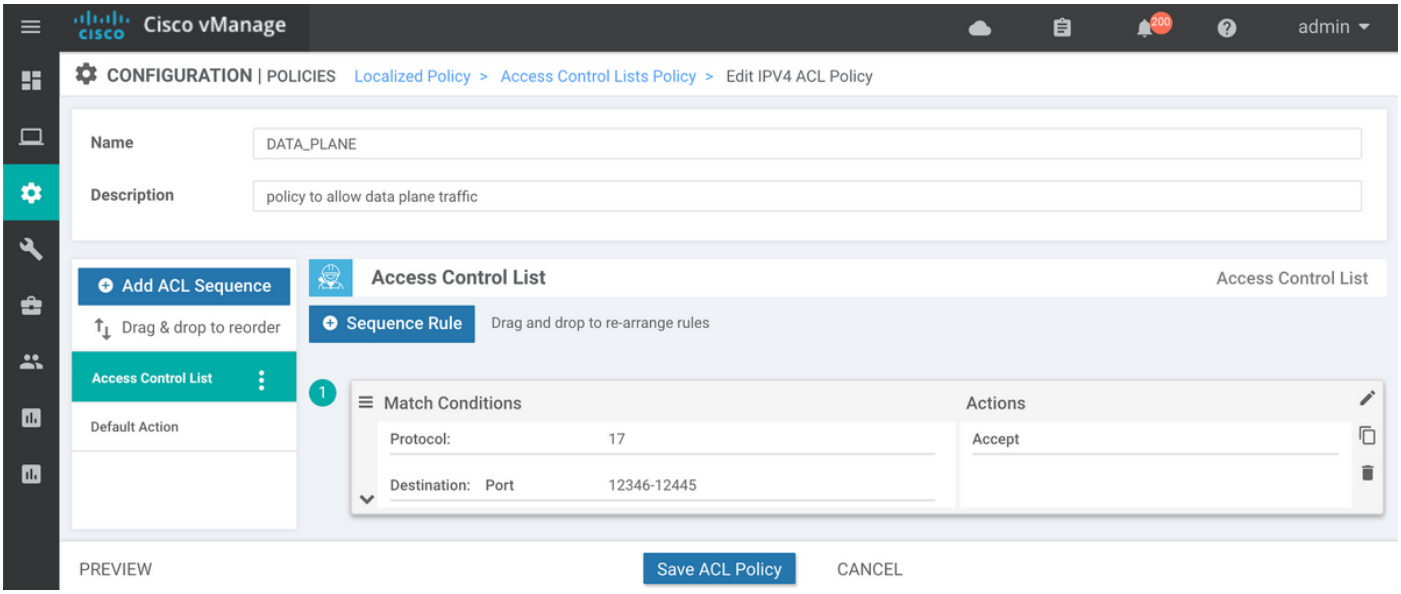
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

Het verklaart de wortel oorzaak en daarom moet u binnenkomende gegevenspakketten in de Toegangscontrolelijst (ACL) op vEdge2 expliciet toestaan zoals deze:

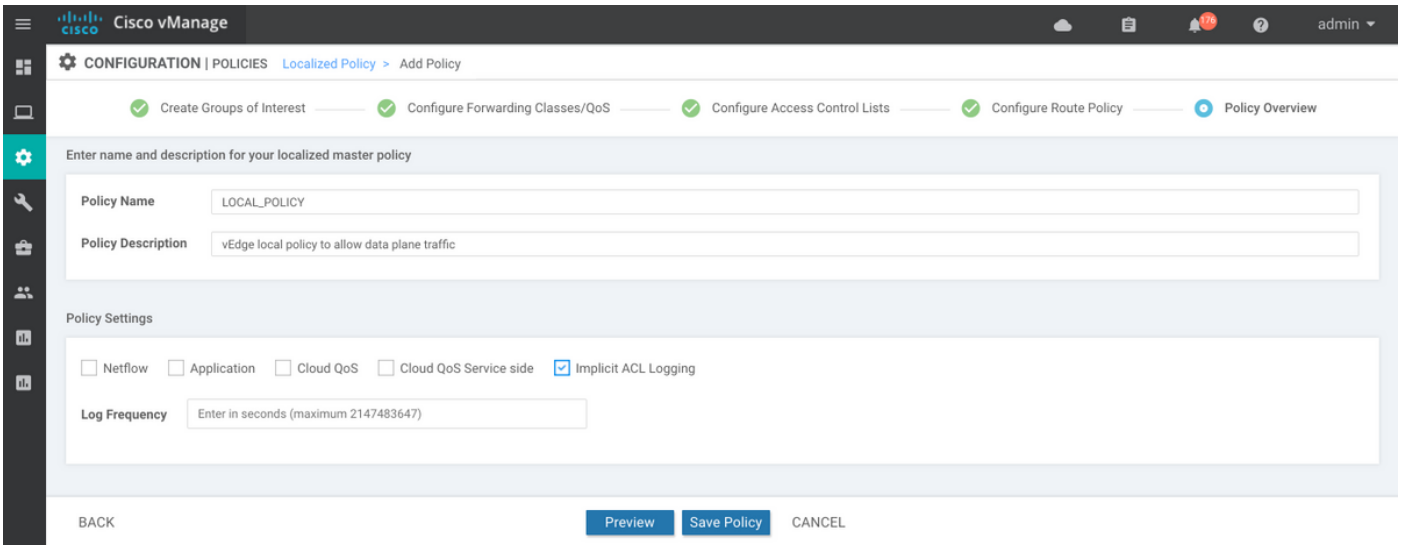
```
vpn 0
 interface ge0/1
  ip address 192.168.9.233/24
  nat
   respond-to-ping
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
```

```
  mtu      1506
  no shutdown
  access-list DATA_PLANE in
 !
!
policy
 implicit-acl-logging
 access-list DATA_PLANE
  sequence 10
   match
destination-port 12346 12445 protocol 17 ! action accept ! ! default-action drop ! !
```

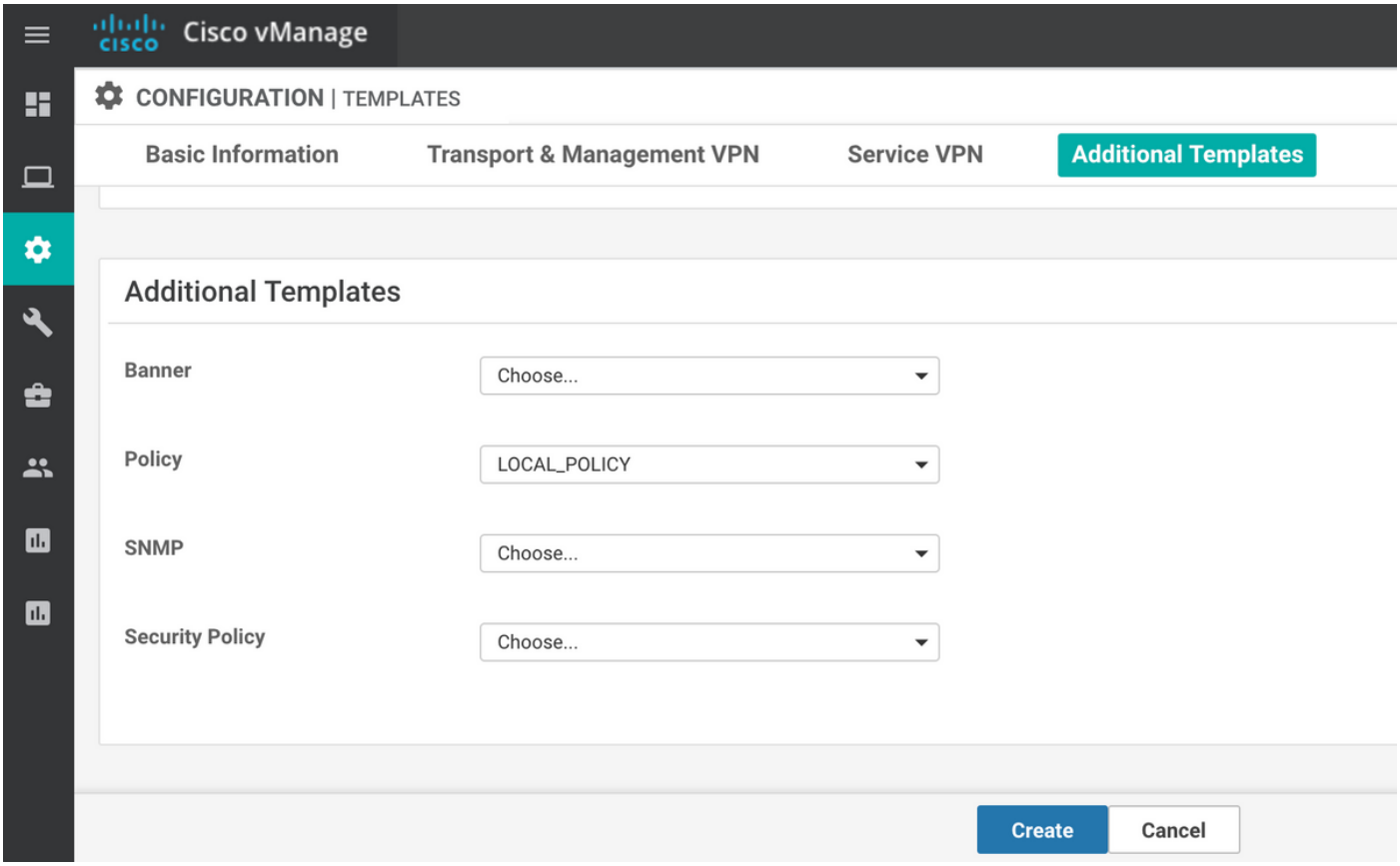
Als de sjablonen voor apparaatfuncties worden gebruikt, moet u Plaatselijk beleid maken en ACL configureren in wizard **Toegangscontrolelijsten** configureren:



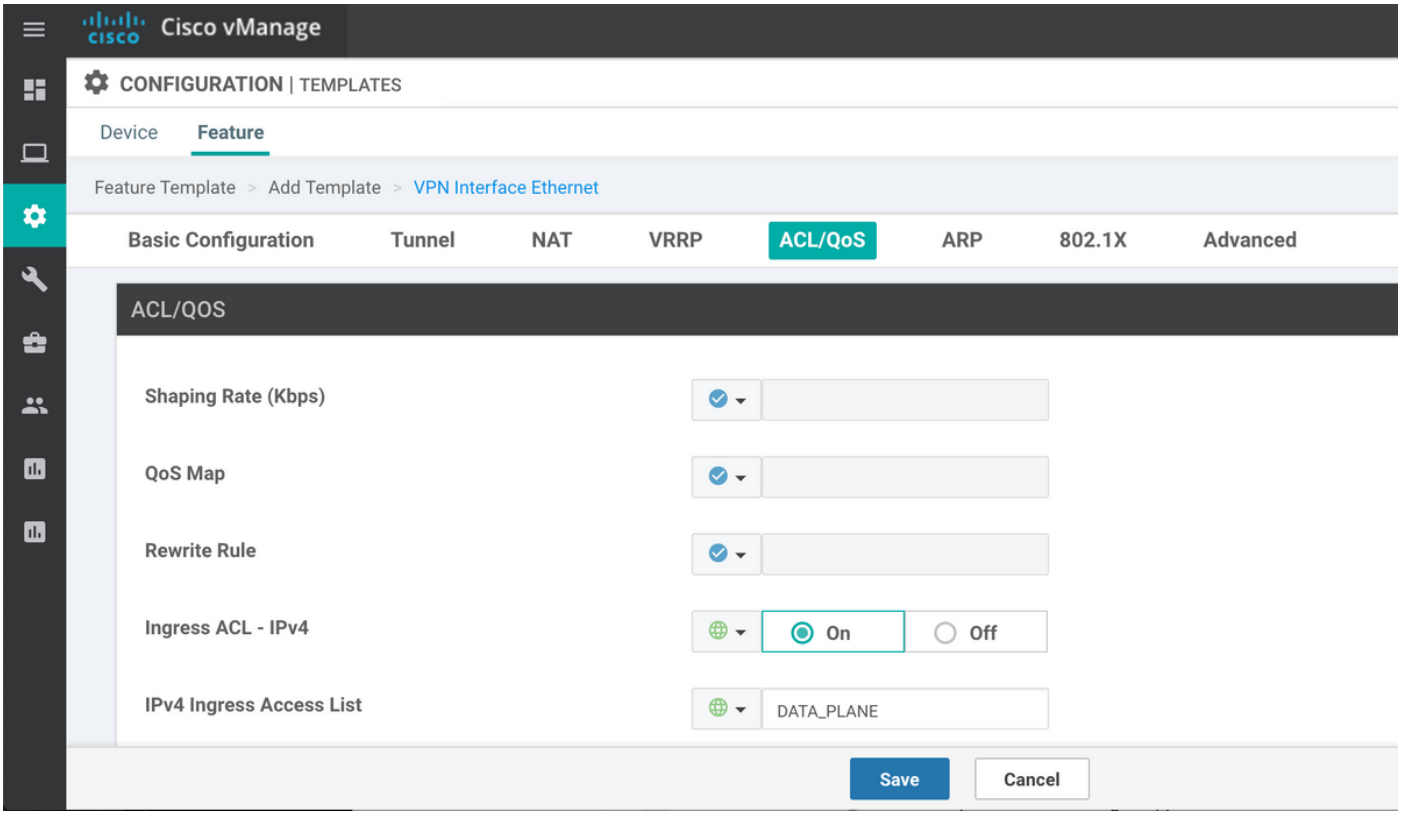
Als **impliciet-acl-logging** nog niet mogelijk is, kan het een goed idee zijn om het in de laatste stap mogelijk te maken voordat je op de knop **Opslaan beleid** klikt:



Plaatselijk beleid (in ons geval genaamd **LOCAL_POLICY**) dient te worden verwezen naar de Apparaatsjabloon:



En dan moet ACL (**genaamd DATA_PLANE** in ons geval) worden toegepast onder VPN-functiekaart Ethernet in de ingress (in) richting:



Zodra ACL is ingesteld en op de interface is toegepast om gegevensverkeer te omzeilen, is de BFD-sessie weer meer naar **de** status omhoog:

```
vEdge2# show tunnel statistics dest-ip 198.51.100.232 ; show bfd sessions site-id 232
```

```
TCP
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     192.168.9.233  198.51.100.232  12346   42346  10.10.10.232  biz-internet  biz-internet
1441    1768     304503     1768     304433     1361

                                      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
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-------------
10.10.10.232     232      up          biz-internet     biz-internet     192.168.9.233
198.51.100.232                   52346       ipsec  7           1000           0:00:14:36      0
```

Overige overwegingen

Houd er rekening mee dat het werken met ACL veel praktischer is dan NAT poortverzending, omdat u ook op basis van bronadressen van de externe site voor meer beveiliging en ter bescherming tegen DDoS-aanvallen op uw apparaat kunt kiezen, bijvoorbeeld:

```
 access-list DATA_PLANE
  sequence 10
   match
    source-ip        198.51.100.232/32
    destination-port 12346 12445
    protocol         17
   !
   action accept
   !
  !
```

Let er ook op dat voor elk ander inkomend verkeer (niet gespecificeerd met **toegestane diensten**) bijv. voor standaard **iperf** poort 5001 expliciete ACL **seq 20** zoals in dit voorbeeld, dit geen effect zal hebben in plaats van dataverkeer:

```
policy
 access-list DATA_PLANE
  sequence 10
   match
    source-ip        198.51.100.232/32
    destination-port 12346 12445
    protocol         17
   !
   action accept
   !
  !
  sequence 20
   match
    destination-port 5001
    protocol         6
```

```
   !
   action accept
   !
  !
```

En je hebt nog steeds NAT port-forward vrijstellingsregel nodig voor **iperf** om te kunnen werken:

```
vEdgeCloud2# show running-config vpn 0 interface ge0/1 nat
vpn 0
 interface ge0/1
  nat
   respond-to-ping
   port-forward port-start 5001 port-end 5001 proto tcp
    private-vpn        0
    private-ip-address 192.168.9.233
   !
  !
 !
!
```

Conclusie

Dit wordt verwacht gedrag op vEdge-routers veroorzaakt door NAT-softwareontwerpspecificaties en kan niet worden vermeden.