Perché vEdges non è in grado di stabilire tunnel IPSec quando si usa il protocollo NAT?

Sommario

Introduzione

In questo documento viene descritto il problema che può verificarsi quando i router vEdge utilizzano l'incapsulamento IPSec per i tunnel del piano dati e un dispositivo è dietro un dispositivo NAT (Network Address Translation) che esegue un NAT simmetrico (RFC3489) o un Mapping dipendente dall'indirizzo (RFC4787), mentre un altro dispositivo ha un accesso diretto a Internet (DIA) o un altro tipo di NAT configurato sull'interfaccia lato trasporto.

Premesse

> **Nota:** Questo articolo è applicabile solo ai router vEdge ed è stato scritto in base al comportamento rilevato nel software vEdge versione 18.4.1 e 19.1.0. Nelle versioni più recenti il comportamento può essere diverso. In caso di dubbi, consultare la documentazione o contattare il Cisco Technical Assistance Center (TAC).

Ai fini della dimostrazione, il problema è stato riprodotto nel laboratorio SD-WAN TAC. Le impostazioni dei dispositivi sono riepilogate nella tabella seguente:

hostname	id-sito	ip-sistema	private-ip	ip pubblico
vedge1	232	10.10.10.232	192.168.10.232	198.51.100.232
vedge2	233	10.10.10.233	192.168.9.233	192.168.9.233
vsmart	1	10.10.10.228	192.168.0.228	192.168.0.228
vbond	1	10.10.10.231	192.168.0.231	192.168.0.231

La configurazione lato trasporto è piuttosto generica su entrambi i dispositivi. Questa è la

configurazione di 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
```

Per illustrare il problema in questo documento, il firewall di Virtual Adaptive Security Appliance (ASAv) risiede tra due router vEdge. ASAv sta effettuando le traduzioni degli indirizzi in base a queste regole:

- Se il traffico proveniente da vEdge1 è destinato ai controller, le porte di origine 12346-12426 vengono convertite in 52346-52426
- Se il traffico proveniente da vEdge1 è destinato a connessioni del piano dati ad altri siti, le porte di origine 12346-12426 vengono convertite in 42346-42426
- Tutto il resto del traffico proveniente da vEdge1 viene inoltre mappato allo stesso indirizzo pubblico (198.51.100.232)

Questa è la configurazione ASAv NAT di riferimento:

```
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
```

Problema

Scenario di lavoro

Nello stato normale, si può osservare che i tunnel del piano dati sono stabiliti, il rilevamento dell'inoltro bidirezionale (BFD) è in stato **attivo**.

Si noti la porta pubblica utilizzata sul dispositivo vEdge1 (52366) per stabilire connessioni di controllo con i controller:

```
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
```

Su vEdge2 non viene utilizzato NAT, pertanto l'indirizzo privato e le porte sono uguali:

```
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
```

Nella schermata **show tunnel** statistics from vEdge1 è possibile osservare l'aumento dei contatori tx/rx:

```
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
```

Dallo stesso output di vEdge2 è possibile vedere come anche i contatori dei pacchetti rx/rx siano in aumento. Si noti che la porta di destinazione (42366) è diversa dalla porta utilizzata per stabilire le connessioni di controllo (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
```

Ma le sessioni BFD sono ancora attive su entrambi i dispositivi:

```
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
```

Le diverse porte utilizzate per le connessioni del control plane e del data plane non causano alcun problema, in quanto la connettività è attiva.

Scenario di errore

L'utente desidera abilitare Direct Internet Access (DIA) sul router vEdge2. A tale scopo, questa configurazione è stata applicata a vEdge2:

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

E la sessione del BFD si è interrotta in modo inaspettato e oltretutto rimane al ribasso. Dopo aver cancellato le statistiche del tunnel, è possibile vedere che il contatore RX non aumenta nell'output **show tunnel statistics**:

```
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
```

Inizialmente, il cliente sospettava che il problema fosse relativo all'MTU del tunnel. Se si confrontano gli output sopra riportati con quelli della sezione "Scenario di lavoro", è possibile notare che nello scenario di lavoro l'MTU del tunnel è 1441 rispetto a 1442 nello scenario con errore. In base alla documentazione, l'MTU del tunnel deve essere 1442 (1500 MTU dell'interfaccia predefinita - 58 byte per il sovraccarico del tunnel), ma una volta attivo il BFD, l'MTU del tunnel viene ridotta di 1 byte. Per consultazione, gli output di **show tunnel statistics** e **show tunnel statistics bfd** vengono forniti di seguito per i casi in cui BFD è **nello** stato **inattivo**:

```
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
```

E se BFD è nello stato attivo:

```
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
```

> **Nota:** A proposito, possiamo determinare le dimensioni del pacchetto BFD insieme all'incapsulamento guardando agli output sopra riportati. Notare che solo un pacchetto BFD è stato ricevuto tra due output, quindi substrando il valore 584987 - 584816 dell'eco BFD ci darà un risultato di 171 byte. Può essere utile per calcolare con precisione l'ampiezza di banda utilizzata dal BFD stesso.

Il motivo per cui il BFD è rimasto bloccato **nello** stato **down** non è l'MTU, ma ovviamente la configurazione NAT. Questa è l'unica cosa che è cambiata tra **Scenario di lavoro** e **Scenario non riuscito**. È possibile osservare che, come risultato della configurazione DIA, il mapping statico NAT è stato creato automaticamente da vEdge2 nella tabella di conversione per consentire il bypass del traffico IPSec del piano dati:

```
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        -
```

Come si può vedere, la porta 52366 viene utilizzata invece della 42366. Ciò è dovuto al fatto che vEdge2 prevede la porta 52366 e l'ha appresa dai TLOC OMP annunciati da 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
```

Soluzione

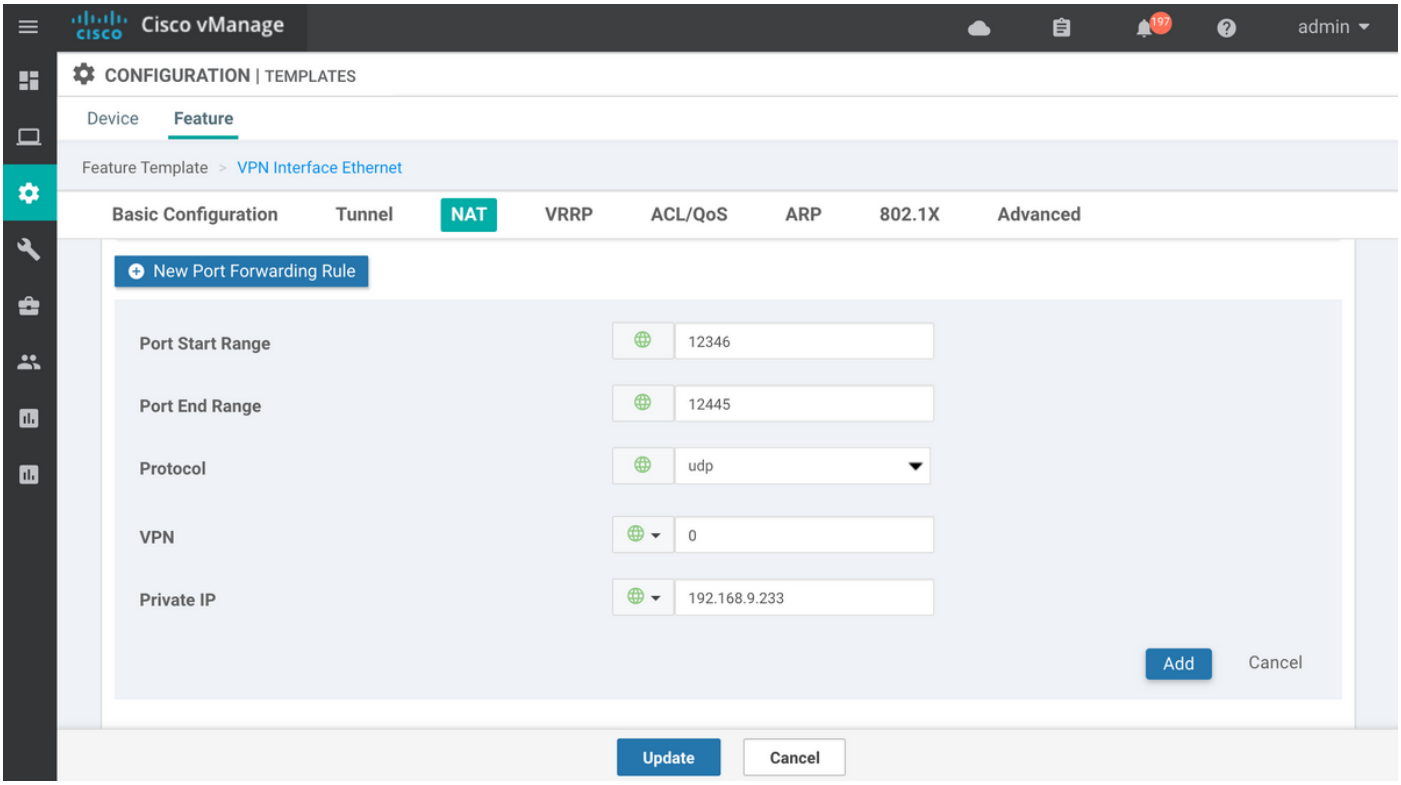
Porta NAT - Avanti

A prima vista, la soluzione di questo tipo di problemi è semplice. È possibile configurare l'inoltro della porta di esenzione NAT statica sull'interfaccia di trasporto vEdge2 in modo da ignorare il filtro per le connessioni del piano dati da qualsiasi origine forzatamente:

```
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
   !
  !
 !
!
```

L'intervallo da 12346 a 12446 supporta tutte le porte iniziali possibili (12346, 12366, 12386, 12406 e 12426 più l'offset della porta). Per ulteriori informazioni, vedere "Porte del firewall per le distribuzioni Viptela".

Se si utilizzano i modelli di funzionalità del dispositivo anziché il modello CLI, per ottenere lo stesso risultato è necessario aggiornare o aggiungere un nuovo modello di funzionalità VPN Ethernet per l'interfaccia di trasporto corrispondente (vpn 0) con la **nuova regola di inoltro porta**, come mostrato nell'immagine:



ACL esplicito

Inoltre, è possibile usare un'altra soluzione con un ACL esplicito. Se è stato configurato **implicit-acl-logging** nella sezione **policy**, è possibile che nel file **/var/log/tmplog/vdebug venga visualizzato il** seguente messaggio:

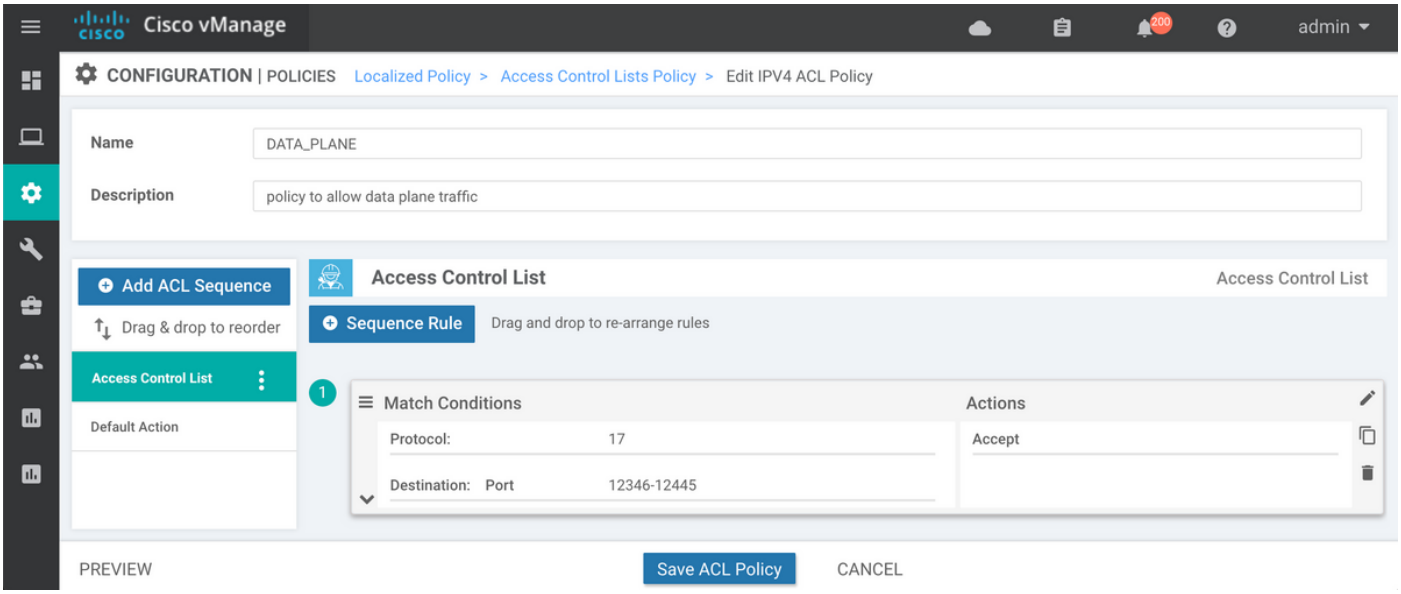
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

Spiega la causa principale, quindi è necessario consentire esplicitamente i pacchetti data plane in ingresso nell'Access Control List (ACL) su vEdge2, come segue:

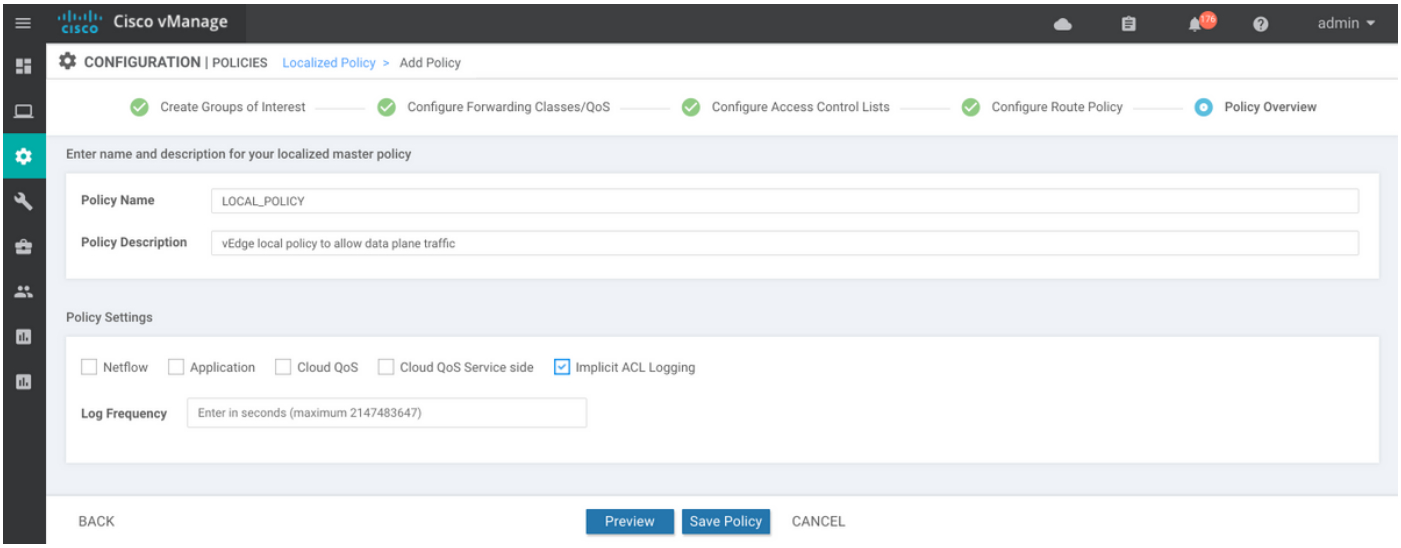
```
vpn 0
 interface ge0/1
  ip address 192.168.9.233/24
  nat
   respond-to-ping
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no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

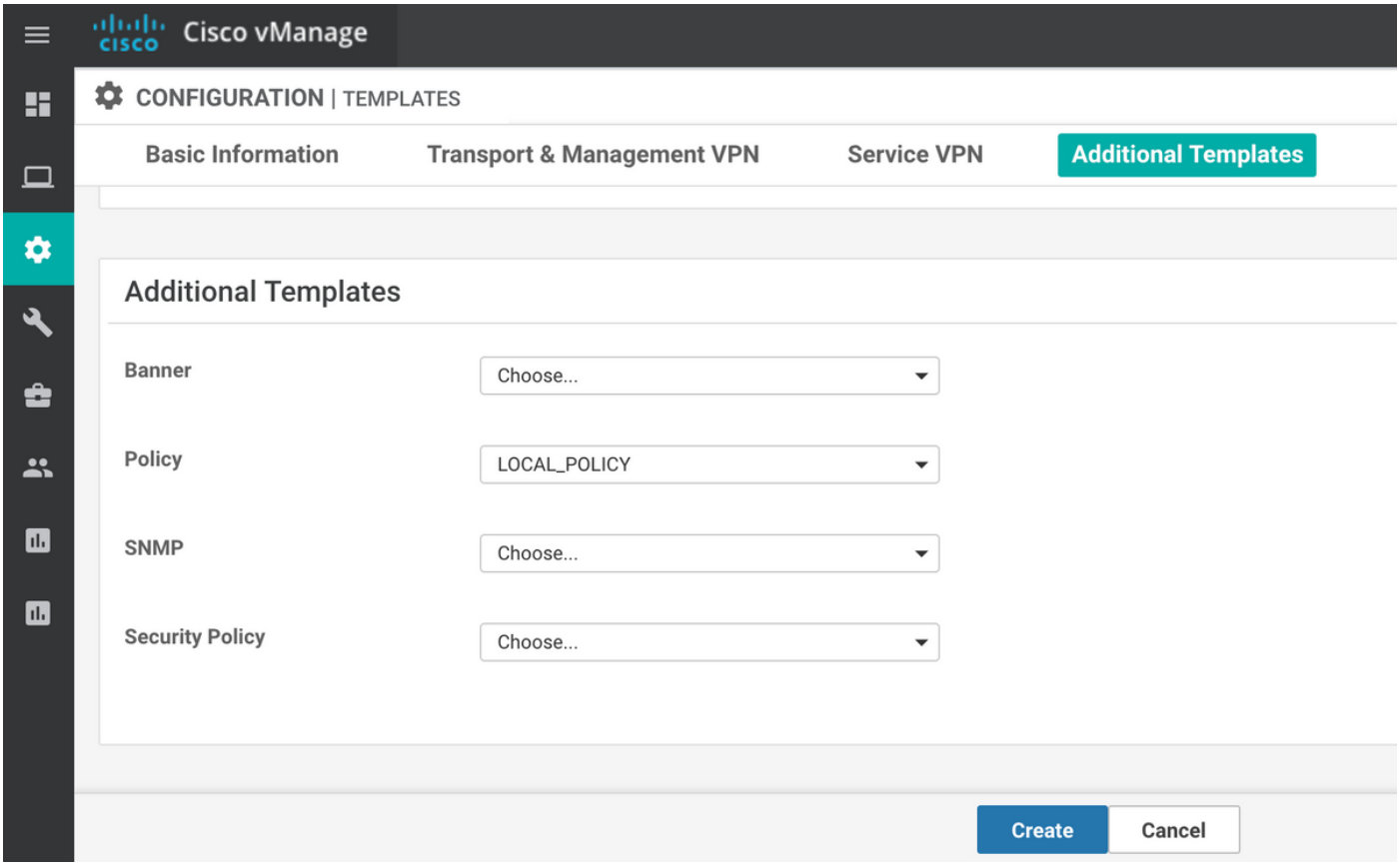
Se si utilizzano modelli di funzionalità del dispositivo, è necessario creare criteri localizzati e configurare ACL nel passaggio della procedura guidata **Configura elenchi di controllo di accesso**:



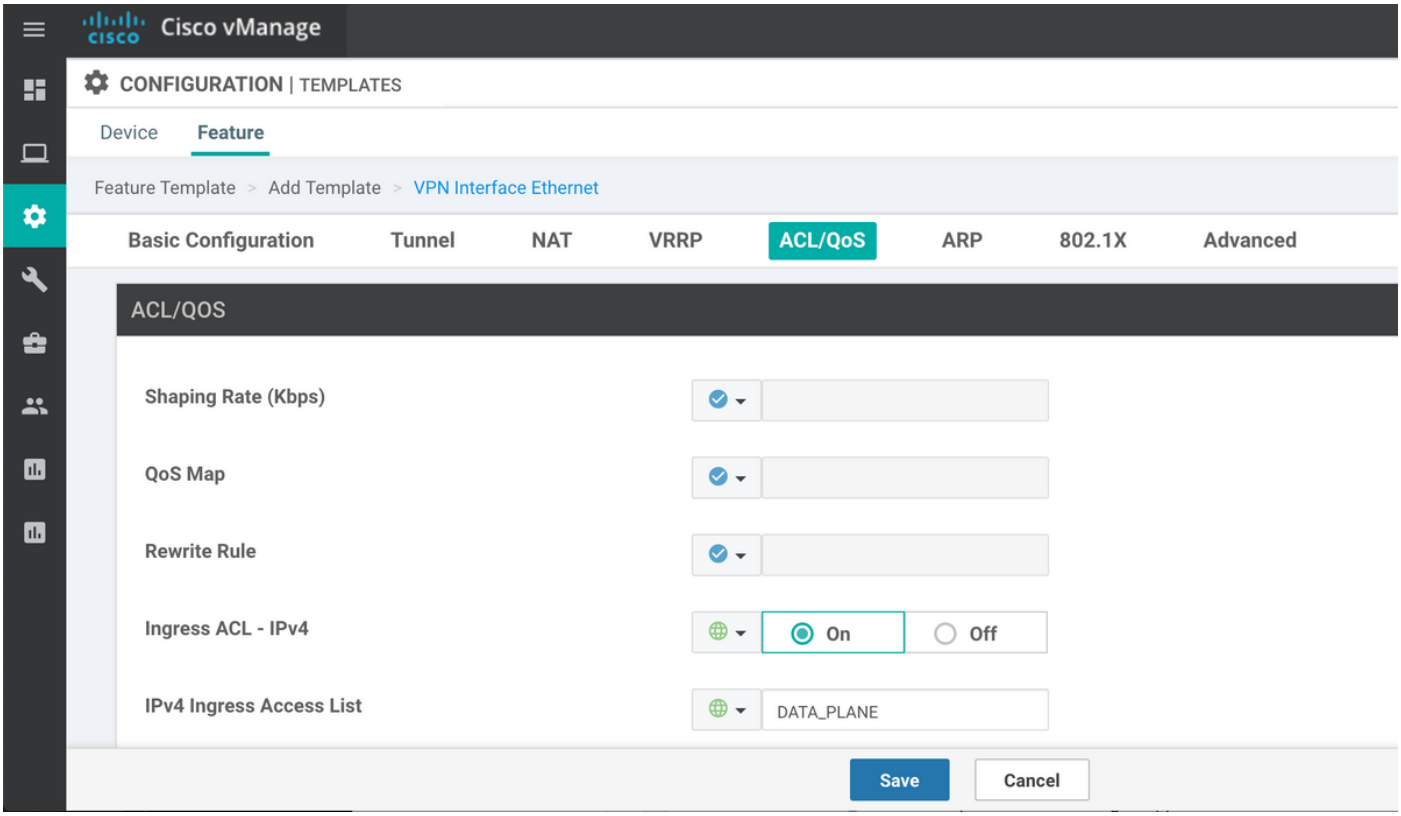
Se la funzione **di log degli acl impliciti** non è stata ancora abilitata, potrebbe essere opportuno abilitarla nell'ultimo passaggio prima di fare clic sul pulsante **Salva criterio**:



Nel modello di dispositivo è necessario fare riferimento al criterio localizzato (denominato **LOCAL_POLICY** in questo caso):



In questo caso, l'ACL (denominato **DATA_PLANE**) deve essere applicato in VPN Interface Ethernet Feature Template (Modello di funzionalità Ethernet dell'interfaccia VPN) nella direzione in entrata:



Dopo aver configurato l'ACL e averlo applicato all'interfaccia per ignorare il traffico del piano dati, la sessione BFD **ritorna** allo stato **attivo**:

```
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
```

Altre considerazioni

Notare che la soluzione degli ACL è molto più pratica dell'inoltro alla porta NAT, in quanto è possibile trovare una corrispondenza anche in base agli indirizzi di origine del sito remoto per una maggiore sicurezza e per proteggere il dispositivo dagli attacchi DDoS, ad esempio:

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

Notare anche che per qualsiasi altro traffico in entrata (non specificato con **allowed-services**), ad esempio per la porta **iperf** predefinita 5001 ACL esplicito **seq 20**, come nell'esempio, questo non avrà alcun effetto rispetto al traffico sul piano dati:

```
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
   !
  !
```

E per il funzionamento di **iperf è** ancora necessaria la regola di esenzione NAT port-forward:

```
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
   !
  !
 !
!
```

Conclusioni

Questo è il comportamento previsto sui router vEdge causato dalle specifiche di progettazione del software NAT e non può essere evitato.