Por que as vEdges não podem estabelecer túneis IPSec se o NAT está sendo usado?

Contents

Introduction

Este documento descreve o problema que pode surgir quando os roteadores vEdge estão usando o encapsulamento IPSec para túneis de plano de dados e um dispositivo está por trás do dispositivo NAT (Network Address Translation) executando NAT simétrico (RFC3489) ou mapeamento dependente de endereço (RFC4787), enquanto outro possui acesso direto à Internet (DIA) ou algum outro tipo de NAT configurado na interface lateral de transporte.

Informações de Apoio

> **Note**: Este artigo se aplica somente a roteadores vEdge e foi escrito com base no comportamento visto nos software vEdge 18.4.1 e 19.1.0. Nas versões mais recentes, o comportamento pode ser diferente. Consulte a documentação ou entre em contato com o Cisco Technical Assistance Center (TAC) em caso de dúvidas.

Para a demonstração, o problema foi reproduzido no laboratório do TAC de SD-WAN. As configurações dos dispositivos estão resumidas na tabela aqui:

hostname	ID do site	system-ip	private-ip	public-ip
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

A configuração do lado do transporte é bastante genérica em ambos os dispositivos. Esta é a

configuração do 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
```

Para demonstrar o problema neste documento, o firewall do Virtual Adaptive Security Appliance (ASAv) reside entre dois roteadores vEdge. O ASAv está fazendo traduções de endereços de acordo com estas regras:

- Se o tráfego do vEdge1 for destinado a controladores, as portas origem 12346-12426 serão convertidas para 52346-52426
- Se o tráfego do vEdge1 for destinado a conexões de plano de dados com outros sites, as portas de origem 12346-12426 serão convertidas para 42346-42426
- Todo o tráfego restante do vEdge1 também é mapeado para o mesmo endereço público (198.51.100.232)

Esta é a configuração de NAT do ASAv para referência:

```
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

Cenário de trabalho

No estado normal, podemos observar que os túneis de plano de dados estão estabelecidos, a detecção de encaminhamento bidirecional (BFD) está em estado **ativo**.

Observe que porta pública usada no dispositivo vEdge1 (52366) para estabelecer conexões de controle com controladores:

```
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
```

No vEdge2, nenhum NAT está sendo usado, portanto, o endereço privado e as portas são iguais:

```
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
```

Nas estatísticas **show tunnel** do vEdge1, podemos ver que os contadores tx/rx estão aumentando:

```
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
```

Na mesma saída do vEdge2, também é possível ver que os contadores de pacotes rx/rx estão aumentando. Observe que a porta de destino (42366) é diferente da porta usada para estabelecer conexões de controle (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
```

Mas as sessões BFD ainda estão ativas em ambos os dispositivos:

```
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
```

Diferentes portas usadas para controle e conexões de plano de dados não causam nenhum problema, a conectividade está estabelecida.

Cenário de falha

O usuário deseja habilitar o Direct Internet Access (DIA) no roteador vEdge2. Para fazer isso, essa configuração foi aplicada ao vEdge2:

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

E a sessão do BFD caiu inesperadamente e, além disso, permanece no estado inferior. Após limpar as estatísticas do túnel, você pode ver que o contador RX não aumenta na saída **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
```

Inicialmente, o cliente suspeitou que o problema estava relacionado ao MTU do túnel. Se você comparar as saídas acima com as saídas da seção "Cenário de trabalho", você pode observar que no cenário de funcionamento o MTU do túnel é 1441 versus 1442 no cenário de falha. Com base na documentação, o MTU do túnel deve ser 1442 (1500 MTU de interface padrão - 58 bytes para overhead de túnel), mas quando o BFD estiver ativo, o MTU do túnel será reduzido em 1 byte. Para sua referência, as saídas de **show tunnel statistics** junto com **show tunnel statistics bfd** fornecidas abaixo para o caso quando BFD está em **estado inativo**:

```
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 o BFD estiver no estado ativo:

```
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
```

> **Note**: A propósito, podemos determinar o tamanho do pacote BFD junto com o encapsulamento, observando as saídas acima. Observe que apenas um pacote BFD foi recebido entre duas saídas, portanto, subtraindo o valor 584987 - 584816 dos Octetos de Eco BFD, nos dará um resultado de 171 bytes. Pode ser útil calcular com precisão a largura de banda usada pelo próprio BFD.

O motivo para o BFD travado no estado **inativo** não é MTU, mas configuração de NAT obviamente. Esta é a única coisa alterada entre o **cenário de trabalho** e o **cenário de falha**. Você pode ver aqui que, como resultado da configuração do DIA, o mapeamento estático NAT foi criado automaticamente pelo vEdge2 na tabela de conversão para permitir o desvio de tráfego IPSec do plano de dados:

```
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        -
```

Como você pode ver, a porta 52366 está sendo usada em vez de 42366. Isso ocorre porque o vEdge2 espera a porta 52366 e a aprendeu com as TLOCs OMP anunciadas pelo 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
```

Solução

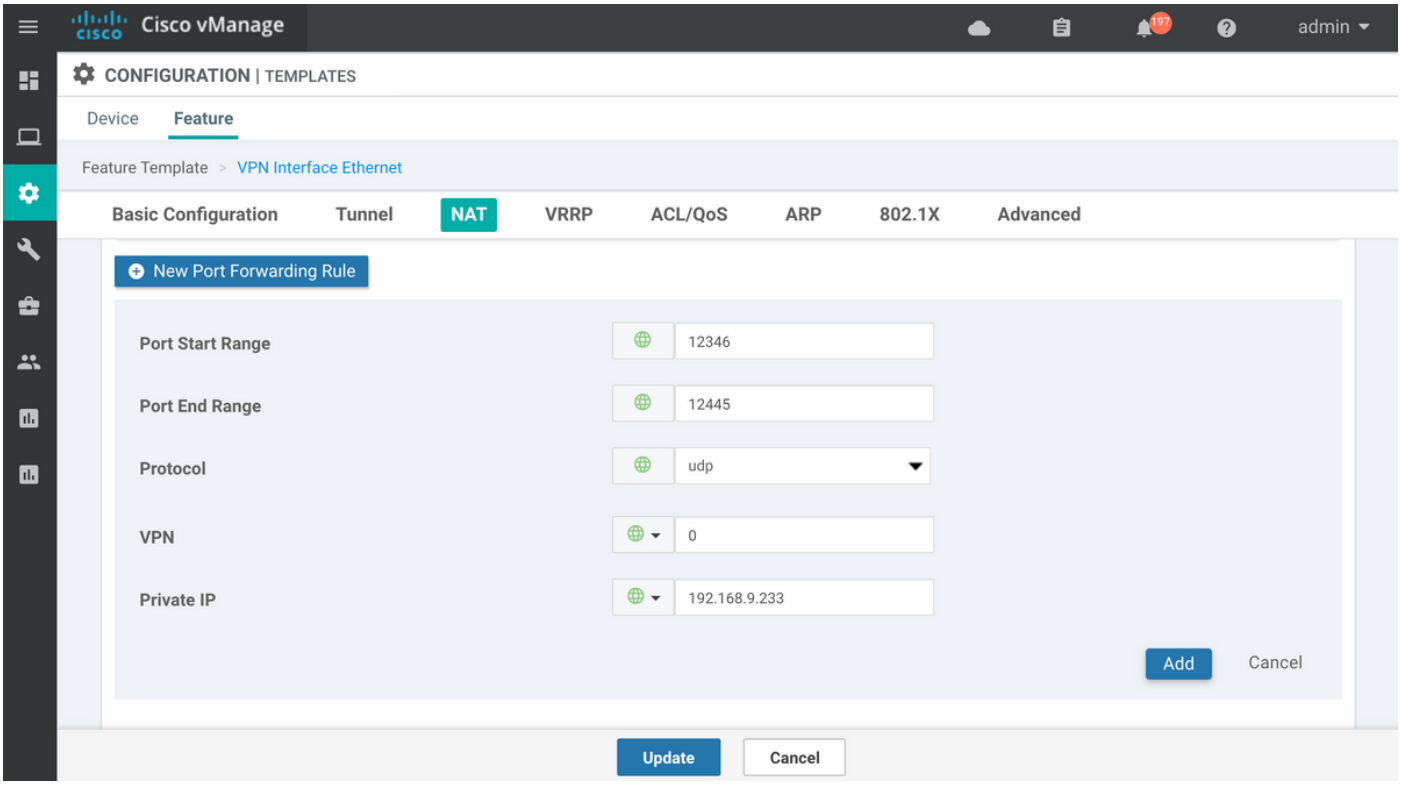
NAT Port-Forward

Àprimeira vista, a solução para este tipo de problemas é simples. Você pode configurar o encaminhamento de porta de isenção de NAT estático na interface de transporte do vEdge2 para ignorar a filtragem de conexões de plano de dados de qualquer fonte com força:

```
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
   !
  !
 !
!
```

Aqui o intervalo de 12346 a 12446 acomoda todas as portas iniciais possíveis (12346, 12366, 12386, 12406 e 12426 mais o desvio de porta). Para obter mais informações sobre isso, consulte "Portas de firewall para implantações Viptela".

Se os Modelos de recurso de dispositivo estiverem sendo usados em vez do modelo CLI, então para alcançar o mesmo objetivo, precisamos atualizar ou adicionar um novo Modelo de recurso Ethernet VPN para a interface de transporte correspondente (vpn 0) com a **Nova regra de encaminhamento de porta**, conforme mostrado na imagem:



ACL explícita

Além disso, outra solução com uma ACL explícita é possível. Se **implicit-acl-logging** estiver configurado na seção **de política**, você poderá observar a seguinte mensagem no arquivo **/var/log/tmplog/vdebug**:

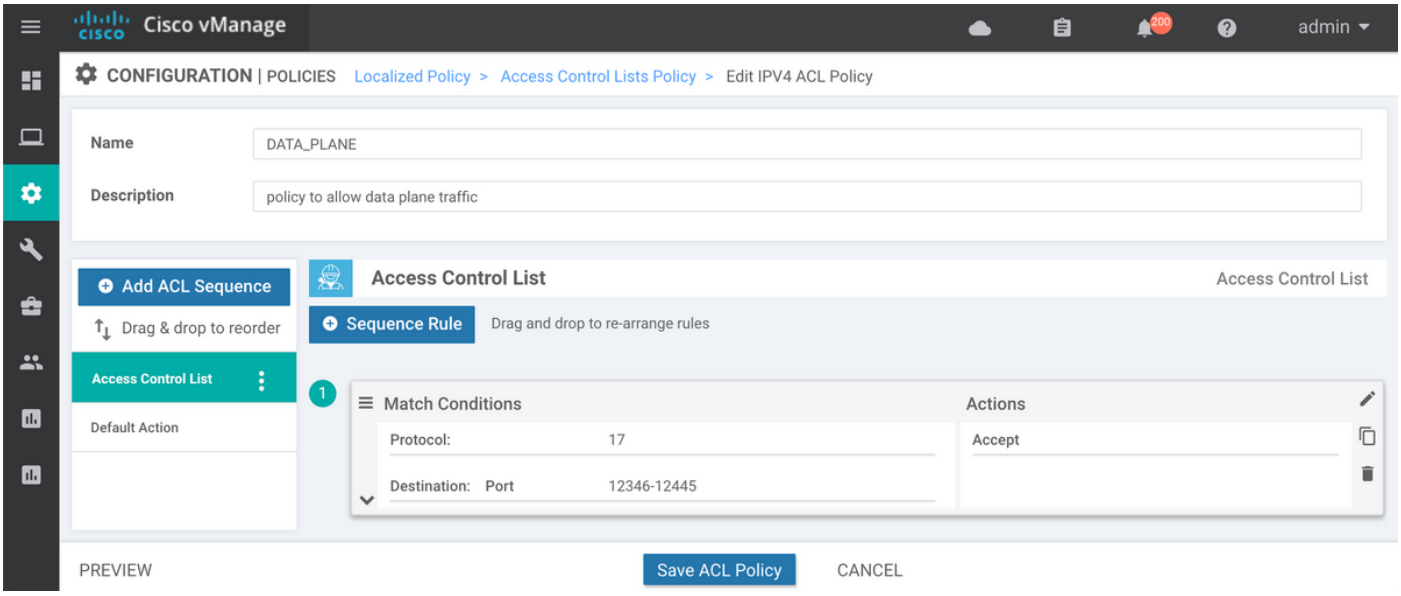
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

Ele explica a causa raiz e, portanto, você precisa permitir explicitamente os pacotes de plano de dados recebidos na Access Control List (ACL) no vEdge2, como este:

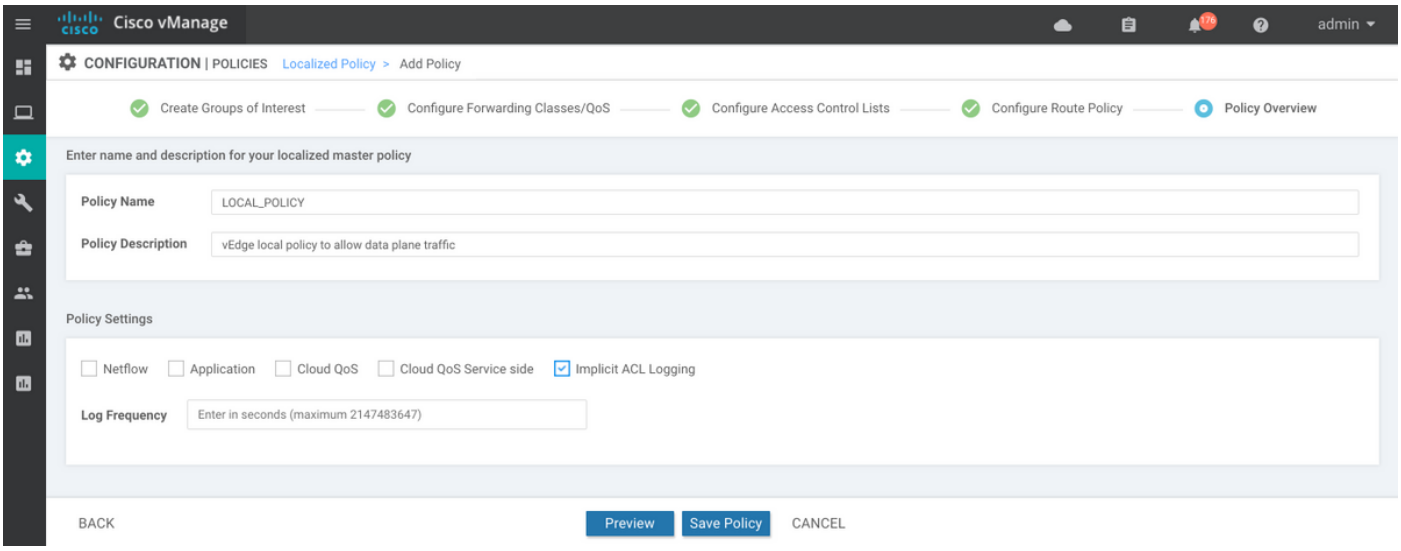
```
vpn 0
 interface ge0/1
  ip address 192.168.9.233/24
  nat
   respond-to-ping
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no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

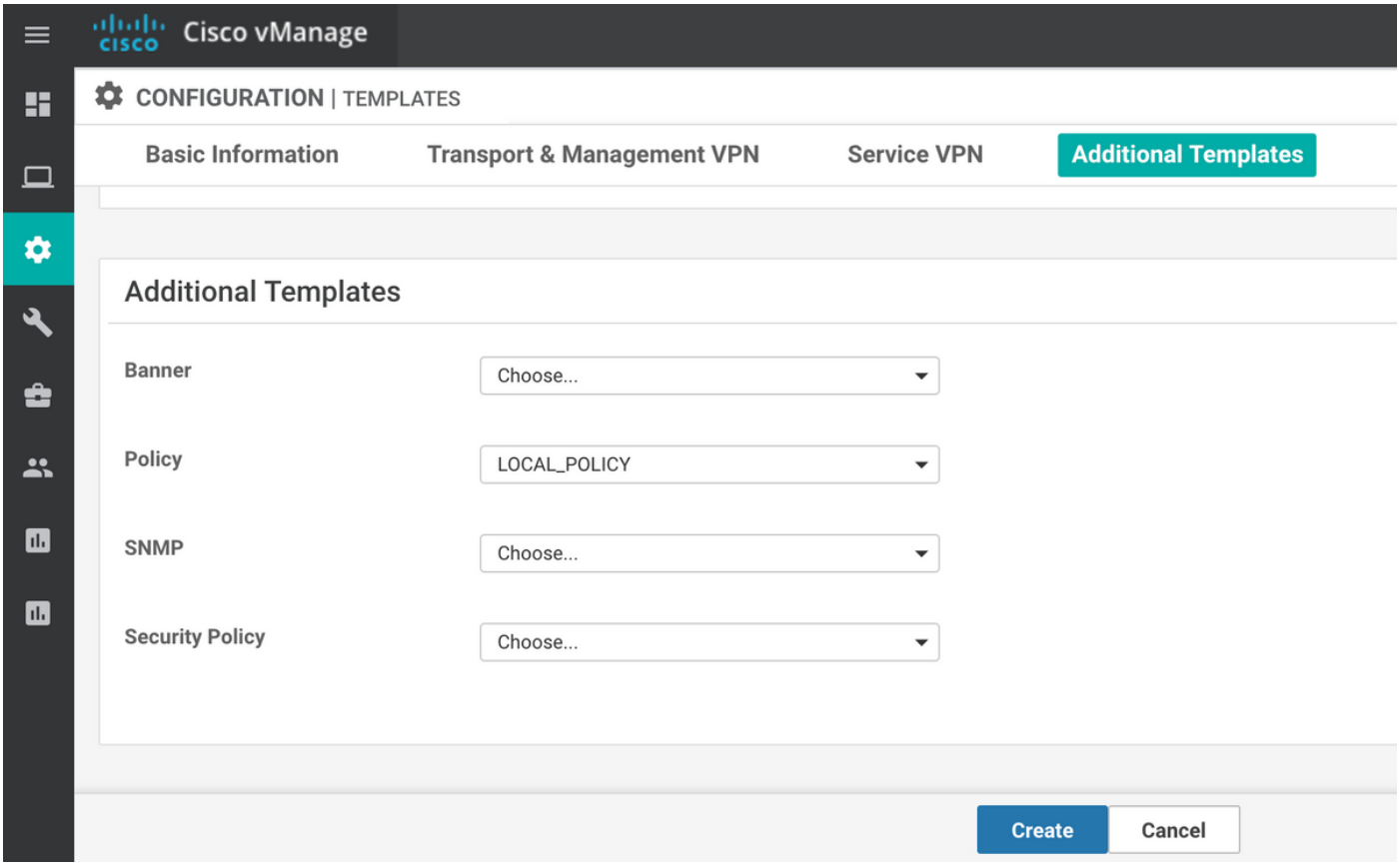
Se os Modelos de recursos do dispositivo estiverem sendo usados, você precisará criar uma política localizada e configurar a ACL na etapa do assistente **Configurar listas de controle de acesso**:



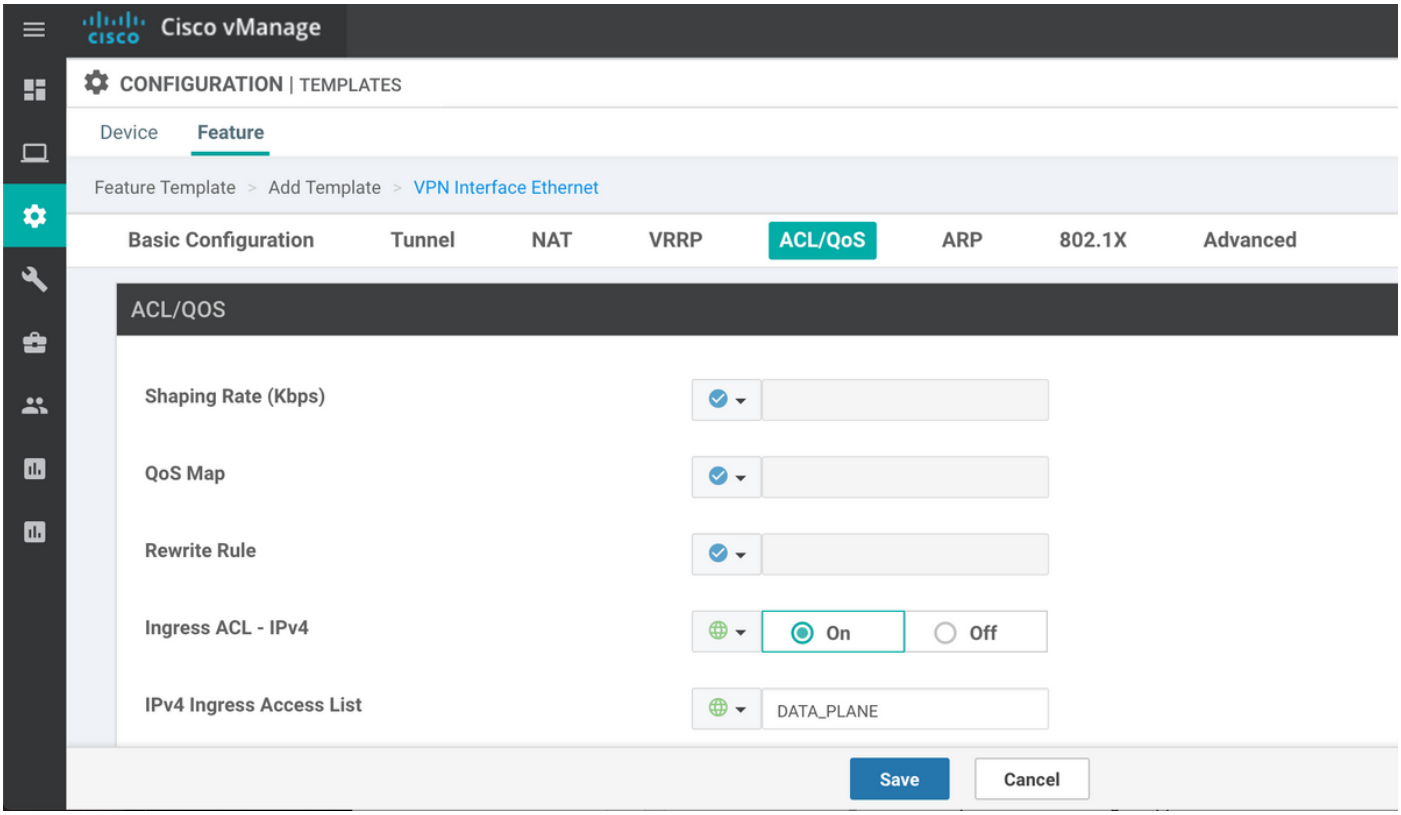
Se o **registro acl implícito** ainda não estiver ativado, pode ser uma boa ideia ativá-lo na etapa final antes de clicar no botão **Salvar política**:



A política localizada (denominada **LOCAL_POLICY**, no nosso caso) deve ser referenciada no Modelo do dispositivo:



E então a ACL (denominada **DATA_PLANE** no nosso caso) deve ser aplicada em VPN Interface Ethernet Feature Template na direção de entrada (in):



Quando a ACL é configurada e aplicada à interface para ignorar o tráfego do plano de dados, a sessão BFD é mais para o estado **ativo** novamente:

```
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
```

Outras considerações

Observe que a solução alternativa com a ACL é muito mais prática do que o encaminhamento de portas NAT, pois você também pode fazer a correspondência com base nos endereços de origem do local remoto para maior segurança e para proteger de ataques de DDoS para seu dispositivo, por exemplo:

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

Observe também que para qualquer outro tráfego de entrada (não especificado com **serviços permitidos**) por exemplo, para a porta **iperf** 5001 ACL explícita **seq 20** como neste exemplo, isso não terá efeito em vez de tráfego de plano de dados:

```
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 você ainda precisa da regra de isenção de porta de encaminhamento de NAT para **o iperf** funcionar:

```
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
   !
  !
 !
!
```

Conclusão

Esse é o comportamento esperado em roteadores vEdge causado por especificações de design do software NAT e não pode ser evitado.