¿Por qué los extremos no pueden establecer túneles IPSec si se está utilizando NAT?

Contenido

Introducción

Este documento describe el problema que puede surgir cuando los routers vEdge utilizan la encapsulación IPSec para los túneles del plano de datos y un dispositivo está detrás del dispositivo de traducción de direcciones de red (NAT) que realiza NAT simétrica (RFC3489) o asignación dependiente de direcciones (RFC4787), mientras que otro tiene acceso directo a Internet (DIA) o algún otro tipo de NAT configurado en la interfaz del lado del transporte.

Antecedentes

> **Nota:** Este artículo se aplica únicamente a los routers vEdge y se escribió en función del comportamiento observado en el software vEdge 18.4.1 y 19.1.0. En las versiones más recientes, el comportamiento puede ser diferente. Consulte la documentación o póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) en caso de dudas.

Para el propósito de la demostración, el problema se reprodujo en el laboratorio del TAC de SD-WAN. La configuración de los dispositivos se resume en la tabla siguiente:

nombre del host	Site-ID	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
vbono	1	10.10.10.231	192.168.0.231	192.168.0.231

La configuración del lado del transporte es bastante genérica en ambos dispositivos. Esta es la configuración de 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 demostrar el problema en este documento, el firewall de Virtual Adaptive Security Appliance (ASAv) reside entre dos routers vEdge. ASAv está realizando traducciones de direcciones de acuerdo con estas reglas:

- Si el tráfico de vEdge1 está destinado a controladores, los puertos de origen 12346-12426 se traducen a 52346-52426
- Si el tráfico de vEdge1 está destinado a conexiones del plano de datos a otros sitios, los puertos de origen 12346-12426 se traducen a 42346-42426
- El resto del tráfico de vEdge1 también se asigna a la misma dirección pública (198.51.100.232)

Esta es la configuración NAT de ASAv para referencia:

```
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

Escenario de trabajo

En el estado normal, podemos observar que se establecen túneles de plano de datos, la Detección de reenvío bidireccional (BFD) está en estado **activo**.

Observe qué puerto público se utiliza en el dispositivo vEdge1 (52366) para establecer conexiones de control con 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
```

En vEdge2 no se está utilizando NAT, por lo que la dirección privada y los puertos son los mismos:

```
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
```

En las estadísticas **show tunnel** de vEdge1 podemos ver que los contadores tx/rx están 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
```

Desde la misma salida de vEdge2 puede ver que también los contadores de paquetes rx/rx están aumentando. Observe que el puerto de destino (42366) es diferente del puerto utilizado para establecer conexiones de control (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
```

Pero las sesiones BFD siguen activas en ambos 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
```

Los diferentes puertos utilizados para las conexiones de plano de datos y de control no causan ningún problema; la conectividad está en marcha.

Escenario de falla

El usuario desea activar el acceso directo a Internet (DIA) en el router vEdge2. Para ello, esta configuración se aplicó a vEdge2:

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

Y la sesión de BFD se redujo inesperadamente y, además, permanece en el estado descendente. Después de borrar las estadísticas del túnel, puede ver que el contador RX no aumenta en el resultado **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, el cliente sospechó que el problema estaba relacionado con la MTU del túnel. Si compara los resultados anteriores con los resultados de la sección "Escenario de trabajo", puede observar que en el escenario de trabajo la MTU de túnel es 1441 frente a 1442 en el escenario de error. Según la documentación, la MTU del túnel debe ser 1442 (MTU de interfaz predeterminada 1500 - 58 bytes para la sobrecarga del túnel), pero una vez que la BFD está activa, la MTU del túnel se reduce en 1 byte. Para su referencia, los resultados de **show tunnel statistics** junto con **show tunnel statistics bfd** proporcionados a continuación para el caso cuando BFD está en el estado **inactivo**:

```
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
```

Y si BFD está en estado activo:

```
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: Por cierto, podemos determinar el tamaño del paquete BFD junto con la encapsulación buscando los resultados anteriores. Tenga en cuenta que sólo se recibió un paquete BFD entre dos salidas, por lo que sustrayendo el valor de octetos BFD Echo RX 584987 - 584816 nos dará un resultado de 171 bytes. Puede ser útil para calcular con precisión el ancho de banda utilizado por el propio BFD.

El motivo por el cual BFD se atasca en estado **inactivo** no es MTU, sino la configuración NAT obviamente. Esta es la única cosa que cambió entre el **escenario Trabajando** y el **escenario Fallido**. Aquí puede ver que como resultado de la configuración DIA, el mapping estático NAT fue creado automáticamente por vEdge2 en la tabla de traducción para permitir la desviación del tráfico IPSec del plano de datos:

```
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 puede ver, el puerto 52366 se está utilizando en lugar de 42366. Esto se debe a que vEdge2 espera un puerto 52366 y lo aprendió de las TLOC OMP anunciadas por 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
```

Solución

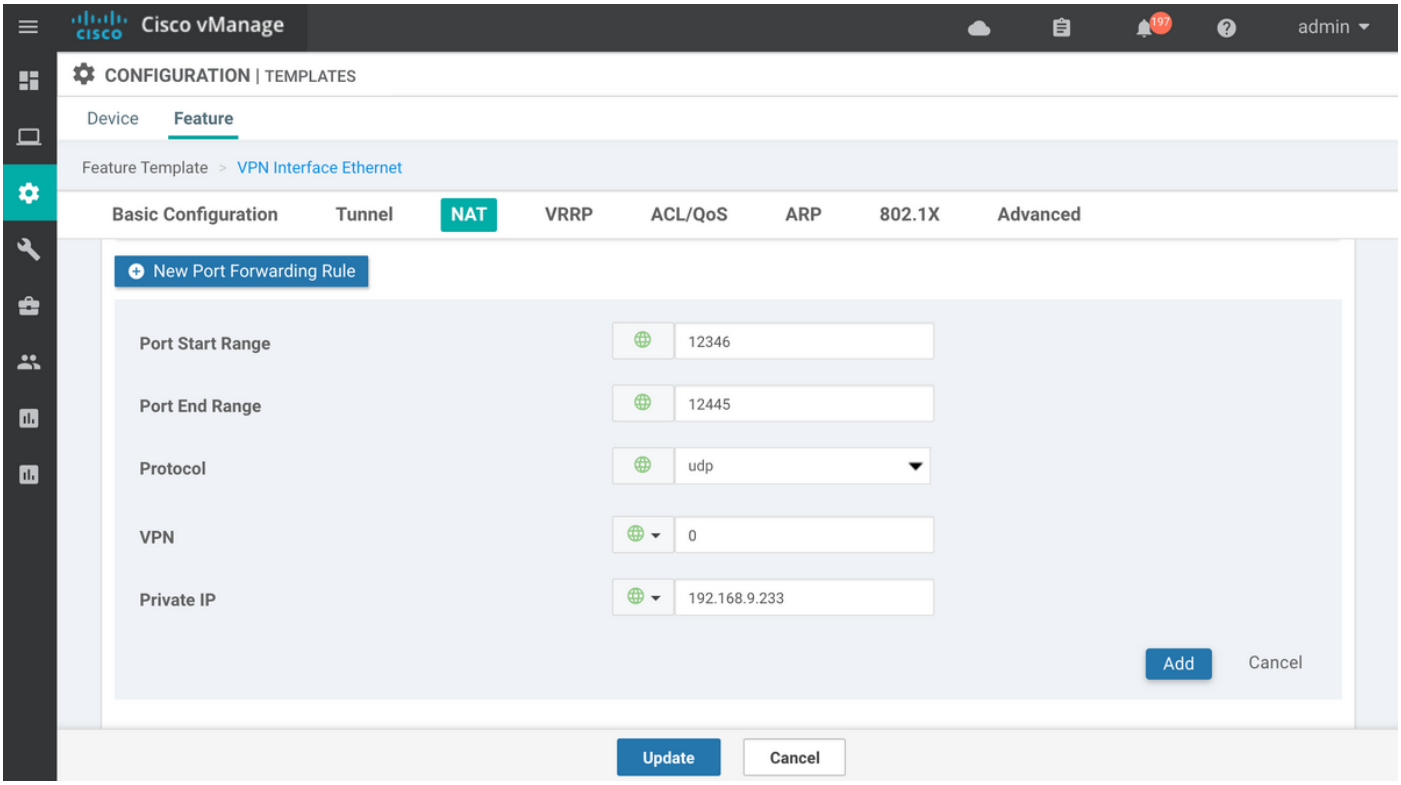
NAT Port-Forward

A primera vista, la solución temporal para este tipo de problemas es sencilla. Puede configurar el reenvío de puertos de exención de NAT estática en la interfaz de transporte vEdge2 para eludir el filtrado de las conexiones del plano de datos desde cualquier origen de forma forzosa:

```
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
   !
  !
 !
!
```

Aquí el rango 12346 a 12446 acomoda todos los puertos iniciales posibles (12346, 12366, 12386, 12406 y 12426 más el desplazamiento de puerto). Para obtener más información sobre esto, consulte "Puertos de firewall para implementaciones de Viptela".

Si se están utilizando plantillas de funciones de dispositivos en lugar de plantillas de CLI, para lograr lo mismo, necesitamos actualizar o agregar una nueva plantilla de funciones de Ethernet VPN para la interfaz de transporte correspondiente (vpn 0) con la **nueva regla de reenvío de puertos**, como se muestra en la imagen:



ACL explícita

Además, otra solución con una ACL explícita es posible. Si **implicit-acl-logging** se configura en la sección **policy**, puede notar el siguiente mensaje en el archivo **/var/log/tmplog/vdebug**:

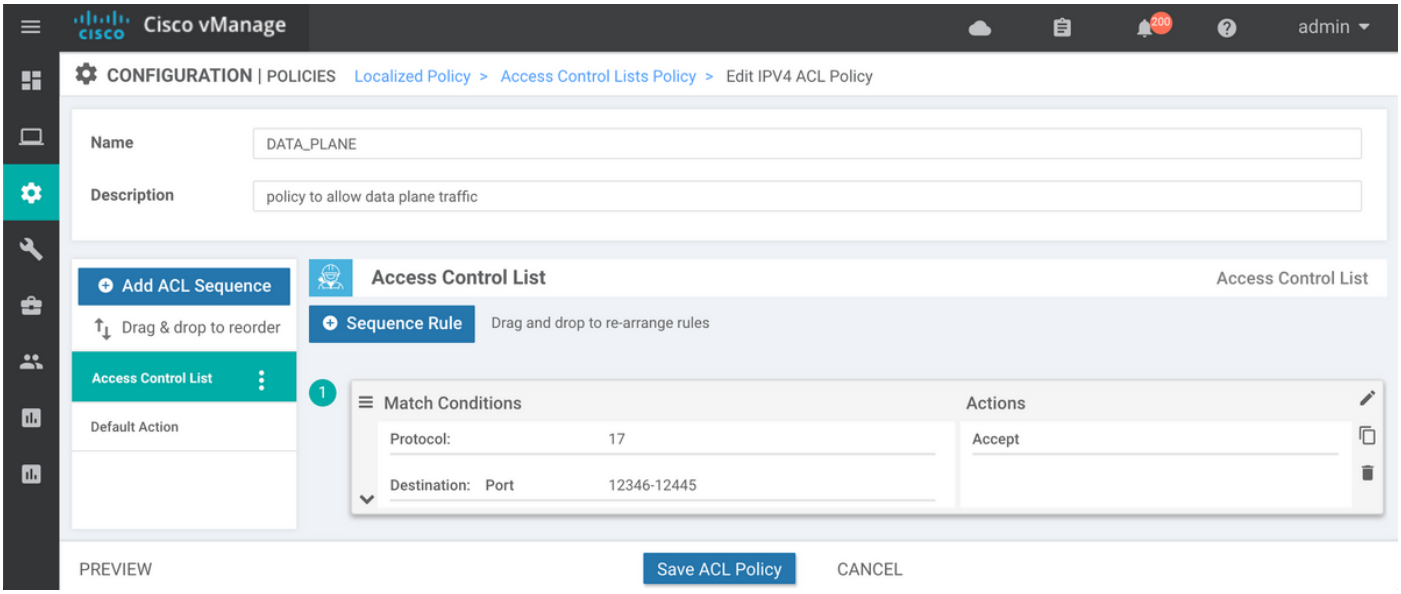
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

Explica la causa raíz y, por lo tanto, debe permitir explícitamente los paquetes del plano de datos entrantes en la Lista de control de acceso (ACL) en el vEdge2 de la siguiente manera:

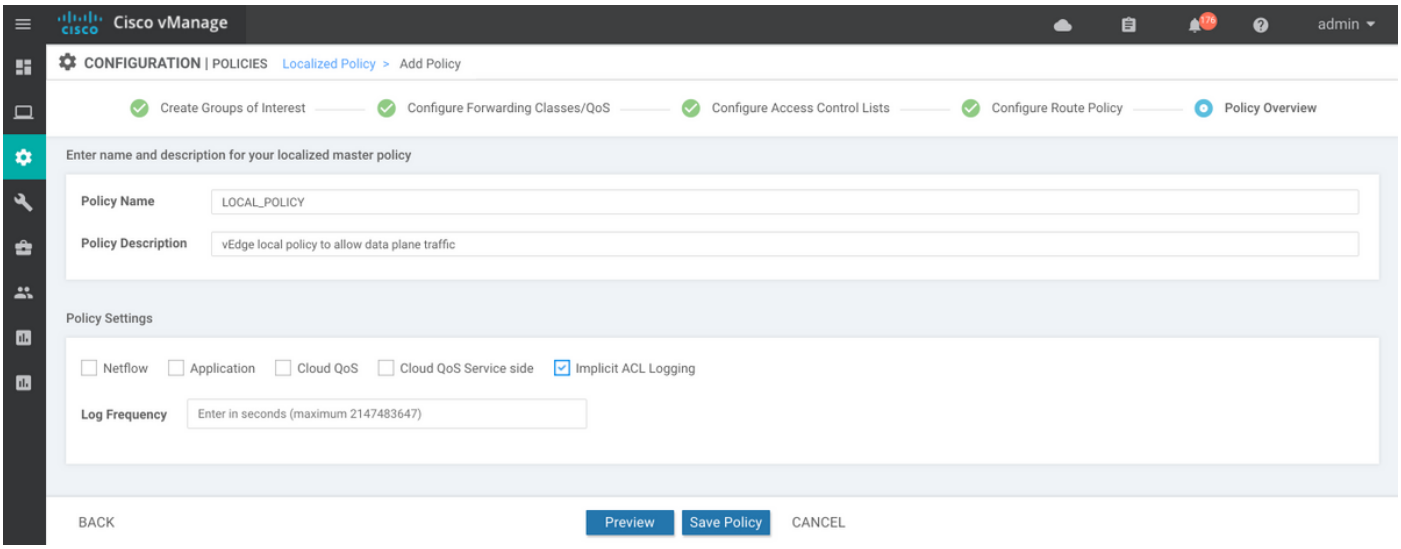
```
vpn 0
 interface ge0/1
  ip address 192.168.9.233/24
  nat
   respond-to-ping
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no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

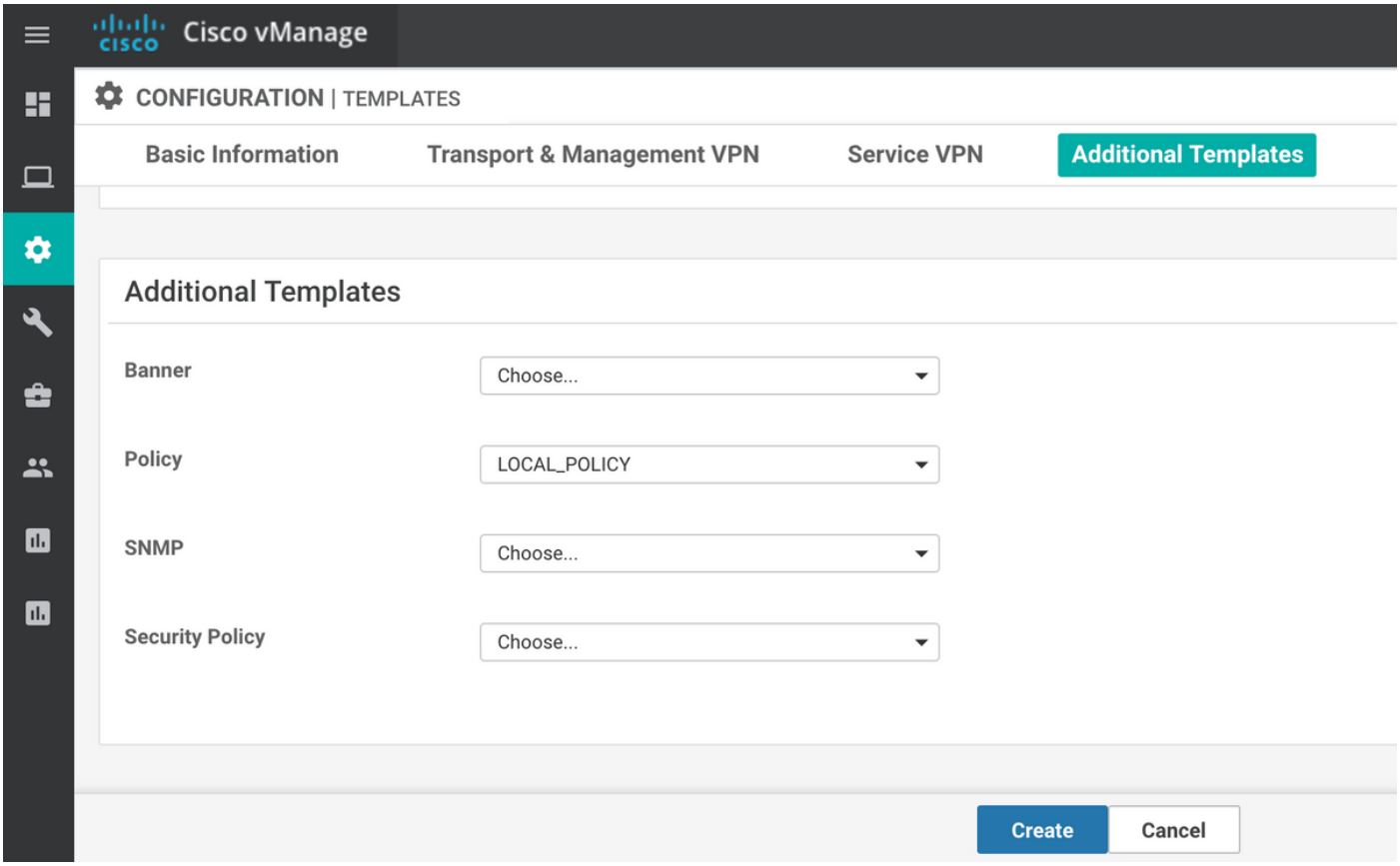
Si se están utilizando las plantillas de funciones de dispositivo, debe crear una política localizada y configurar ACL en el paso del asistente **Configurar listas de control de acceso**:



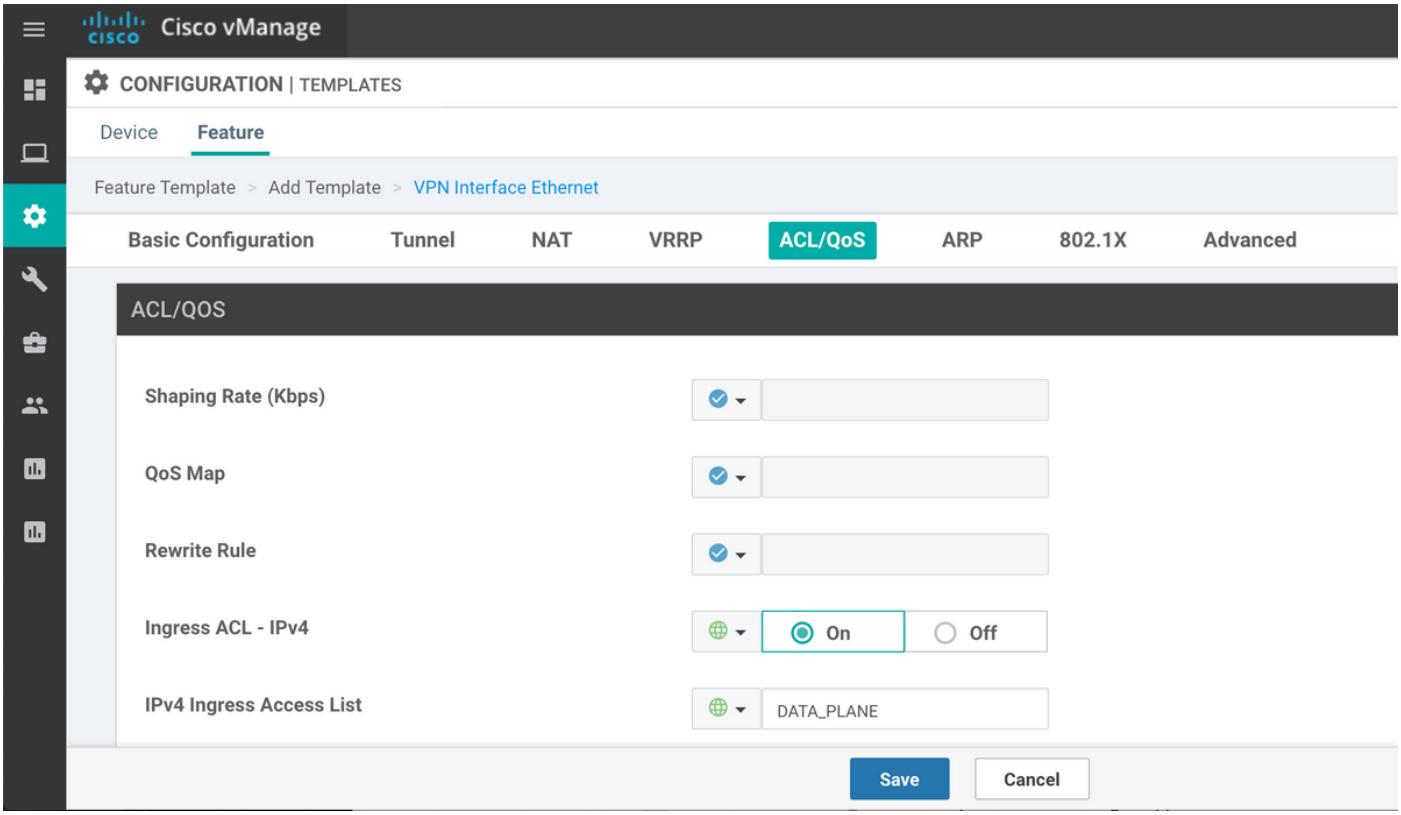
Si **implicit-acl-logging** todavía no está habilitado, podría ser una buena idea habilitarlo en el paso final antes de hacer clic en el botón **Guardar política**:



La política localizada (denominada **LOCAL_POLICY** en nuestro caso) debe ser referenciada en la plantilla de dispositivo:



Y luego la ACL (denominada **DATA_PLANE** en nuestro caso) debería aplicarse bajo la Plantilla de Función Ethernet de Interfaz VPN en la dirección de ingreso (en):



Una vez que la ACL se configura y se aplica a la interfaz para eludir el tráfico del plano de datos, la sesión BFD es más al estado **activo** nuevamente:

```
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
```

Otras consideraciones

Tenga en cuenta que la solución alternativa con ACL es mucho más práctica que el reenvío de puertos NAT, ya que también puede coincidir en función de las direcciones de origen del sitio remoto para mayor seguridad y para proteger contra ataques DDoS a su dispositivo, por ejemplo:

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

Tenga en cuenta también que para cualquier otro tráfico entrante (no especificado con **allowed-services**), por ejemplo, para **iperf** port 5001 ACL explícita **seq 20** predeterminada, como en este ejemplo, esto no tendrá ningún efecto en comparación con el tráfico del plano de datos:

```
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
   !
  !
```

Y todavía necesita una regla de exención de reenvío de puertos NAT para que **iperf** funcione:

```
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
   !
  !
 !
!
```

Conclusión

Esto es un comportamiento esperado en los routers vEdge causado por las especificaciones de diseño de software NAT y no se puede evitar.