Pourquoi vEdges ne peut-il pas établir de tunnels IPSec si NAT est utilisé ?

Contenu

Introduction

Ce document décrit le problème qui peut survenir lorsque les routeurs vEdge utilisent l'encapsulation IPSec pour les tunnels du plan de données et qu'un périphérique est derrière le périphérique NAT (Network Address Translation) qui fait de la NAT symétrique (RFC3489) ou du mappage dépendant de l'adresse (RFC4787), tandis qu'un autre dispose d'un accès direct à Internet (DIA) ou un autre type de NAT configuré sur l'interface côté transport.

Informations générales

> **Note**: Cet article s'applique uniquement aux routeurs vEdge et a été écrit en fonction du comportement observé dans les logiciels vEdge 18.4.1 et 19.1.0. Dans les versions plus récentes, le comportement peut être différent. Veuillez consulter la documentation ou contacter le centre d'assistance technique Cisco (TAC) en cas de doute.

Pour les besoins de la démonstration, le problème a été reproduit dans le TP du centre d'assistance technique SD-WAN. Les paramètres des périphériques sont résumés dans le tableau ci-dessous :

nom de l'hôte	id-site	system-ip	private-ip	public-ip
évitement1	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 configuration côté transport est assez générique sur les deux périphériques. Voici la configuration 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
```

Afin de démontrer le problème dans ce document, le pare-feu ASAv (Virtual Adaptive Security Appliance) réside entre deux routeurs vEdge. ASAv effectue des traductions d'adresses conformément aux règles suivantes :

- Si le trafic de vEdge1 est destiné aux contrôleurs, les ports source 12346-12426 sont traduits en 52346-52426
- Si le trafic de vEdge1 est destiné aux connexions de plan de données vers d'autres sites, les ports sources 12346-12426 sont traduits en 42346-42426
- Tout autre trafic provenant de vEdge1 est également mappé à la même adresse publique (198.51.100.232)

Voici la configuration NAT ASAv à titre de référence :

```
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
```

Problème

Scénario de travail

Dans l'état normal, nous pouvons observer que des tunnels de plan de données sont établis, la détection de transfert bidirectionnel (BFD) est en état **actif**.

Notez le port public utilisé sur le périphérique vEdge1 (52366) pour établir des connexions de contrôle avec les contrôleurs :

```
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
```

Sur vEdge2, aucune NAT n'est utilisée, de sorte que l'adresse privée et les ports sont identiques :

```
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
```

Dans les statistiques **show tunnel** de vEdge1, nous pouvons voir que les compteurs tx/rx augmentent :

```
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
```

Àpartir du même résultat de vEdge2, vous pouvez voir que les compteurs de paquets rx/rx sont en train d'augmenter. Notez que le port de destination (42366) est différent du port utilisé pour établir des connexions de contrôle (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
```

Mais les sessions BFD sont toujours actives sur les deux périphériques :

```
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
```

Différents ports utilisés pour les connexions de contrôle et de plan de données ne posent aucun problème, la connectivité est en place.

Scénario d'échec

L'utilisateur souhaite activer l'accès direct à Internet (DIA) sur le routeur vEdge2. Pour ce faire, cette configuration a été appliquée à vEdge2 :

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

Et la session BFD a chuté de manière inattendue et reste en outre dans l'état déprimé. Après avoir effacé les statistiques de tunnel, vous pouvez voir que le compteur RX n'augmente pas dans la sortie **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
```

Initialement, le client soupçonnait ce problème lié à la MTU du tunnel. Si vous comparez les sorties ci-dessus aux sorties de la section « Scénario de travail », vous pouvez remarquer que dans le scénario de travail, la MTU du tunnel est de 1 441 contre 1 442 dans le scénario d'échec. D'après la documentation, le MTU du tunnel doit être 1442 (1500 MTU de l'interface par défaut - 58 octets pour la surcharge du tunnel), mais une fois le BFD activé, le MTU du tunnel est abaissé de 1 octet. Pour votre référence, les sorties de **show tunnel statistics** ainsi que **show tunnel statistics bfd** fournies ci-dessous pour le cas où BFD est en **état** de **panne** :

```
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
```

Et si BFD est en état actif :

```
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**: Au fait, nous pouvons déterminer la taille des paquets BFD avec l'encapsulation en recherchant les sorties ci-dessus. Notez qu'un seul paquet BFD a été reçu entre deux sorties, ce qui sous-tend la valeur d'octet Echo RX BFD 584987 - 584816 nous donnera un résultat de 171 octets. Il peut être utile de calculer précisément la bande passante utilisée par le BFD lui-même.

La raison pour laquelle le BFD est resté dans l'état **down** n'est pas MTU, mais la configuration NAT évidemment. C'est la seule chose qui a changé entre le **scénario de travail** et le **scénario d'échec**. Vous pouvez voir ici qu'à la suite de la configuration DIA, le mappage statique NAT a été automatiquement créé par vEdge2 dans la table de traduction pour permettre le contournement du trafic IPSec du plan de données :

```
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        -
```

Comme vous pouvez le voir, le port 52366 est utilisé au lieu du port 42366. En effet, vEdge2

attend le port 52366 et l'a appris des TLOC OMP annoncés par 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
```

Solution

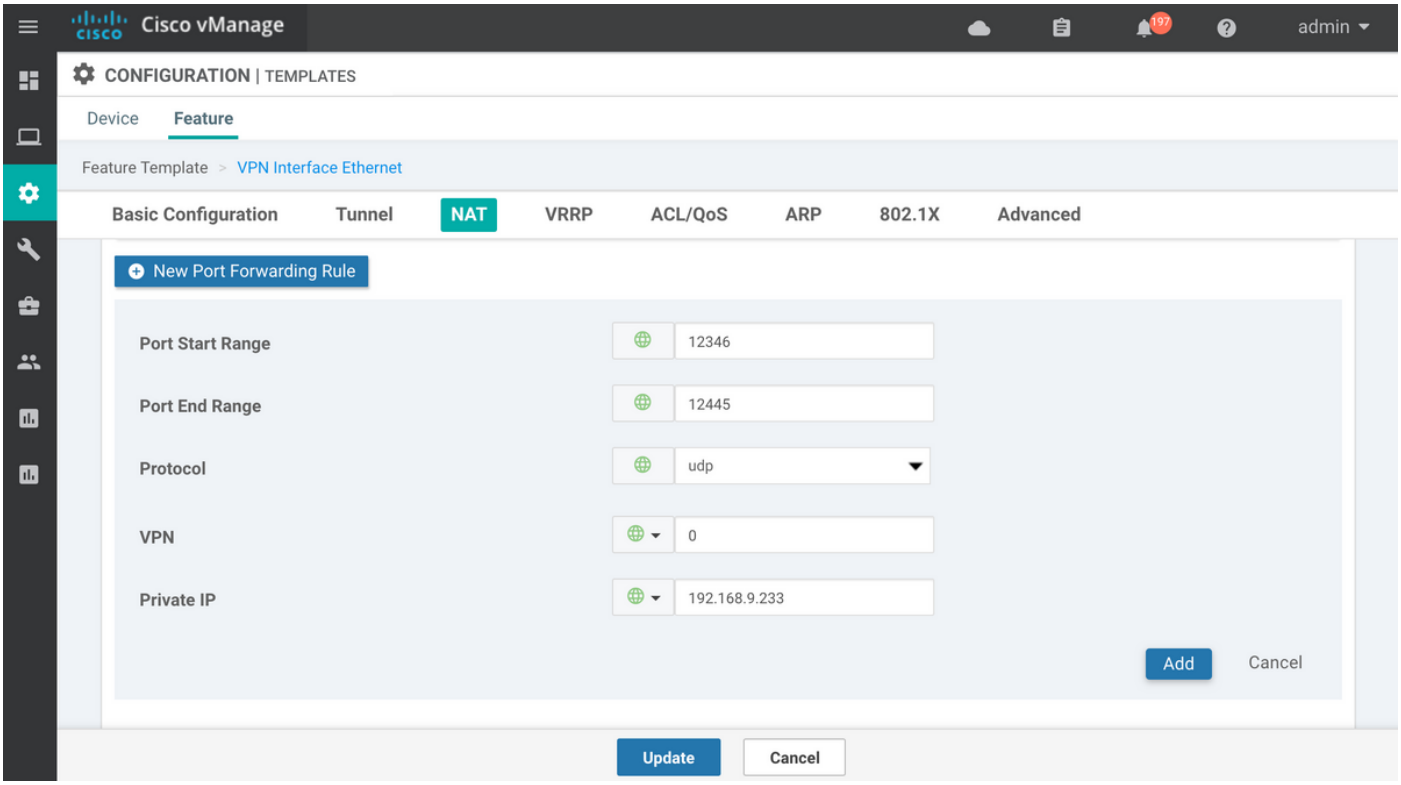
Transfert de port NAT

De prime abord, la solution à ce type de problèmes est simple. Vous pouvez configurer le transfert de port d'exemption NAT statique sur l'interface de transport vEdge2 pour contourner le filtrage pour les connexions de plan de données à partir de n'importe quelle source avec force :

```
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
   !
  !
 !
!
```

Ici, la plage 12346 à 12446 prend en charge tous les ports initiaux possibles (12346, 12366, 12386, 12406 et 12426 plus port-offset). Pour plus d'informations à ce sujet, référez-vous à « Ports de pare-feu pour les déploiements de vidéo ».

Si des modèles de fonctionnalités de périphérique sont utilisés à la place du modèle CLI, alors pour obtenir la même chose, nous devons mettre à jour ou ajouter un nouveau modèle de fonctionnalité VPN Ethernet pour l'interface de transport correspondante (vpn 0) avec **la nouvelle règle de transfert de port**, comme illustré dans l'image :



ACL explicite

En outre, une autre solution avec une liste de contrôle d'accès explicite est possible. Si **implicit-acl-logging** est configuré dans la section **policy**, vous pouvez remarquer le message suivant dans le fichier **/var/log/tmplog/vdebug** :

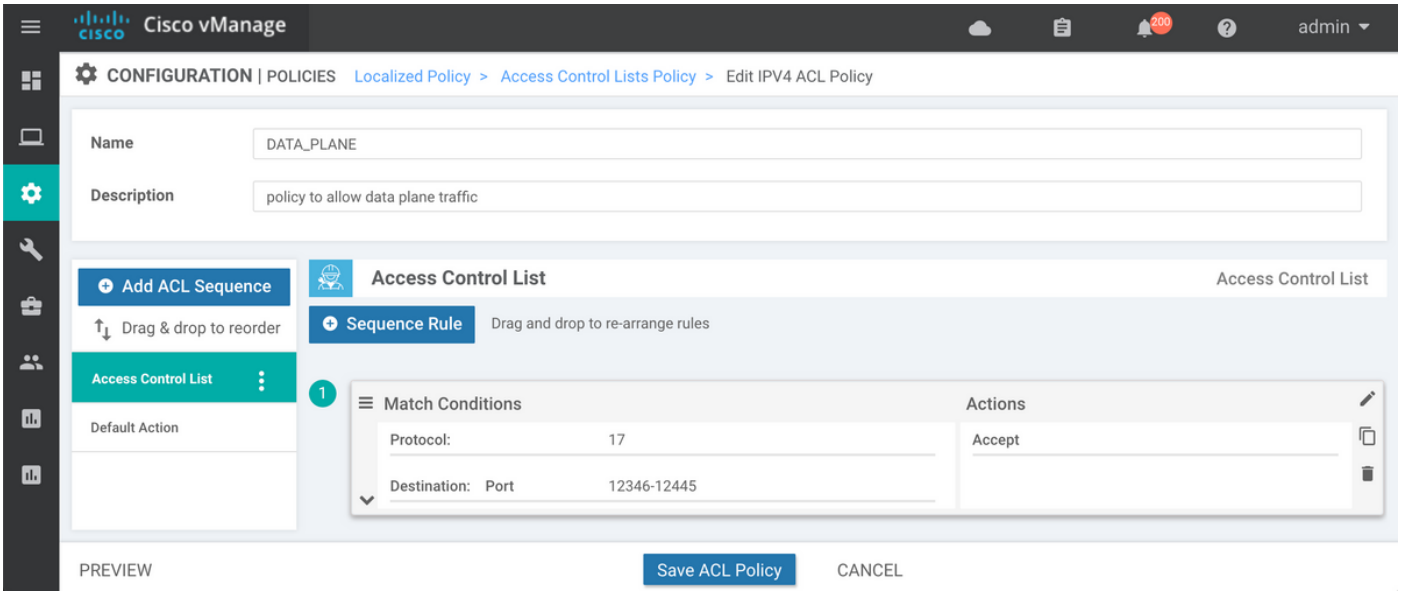
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

Il explique la cause première et, par conséquent, vous devez explicitement autoriser les paquets de plan de données entrants dans la liste de contrôle d'accès (ACL) sur vEdge2 comme ceci :

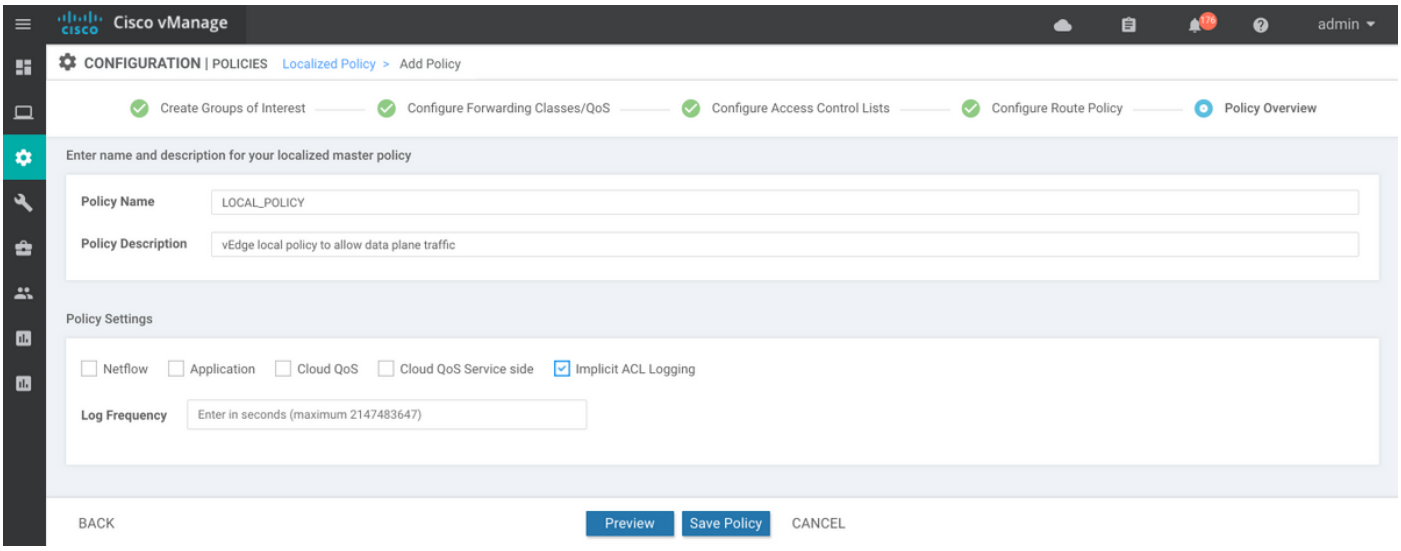
```
vpn 0
 interface ge0/1
  ip address 192.168.9.233/24
  nat
   respond-to-ping
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no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

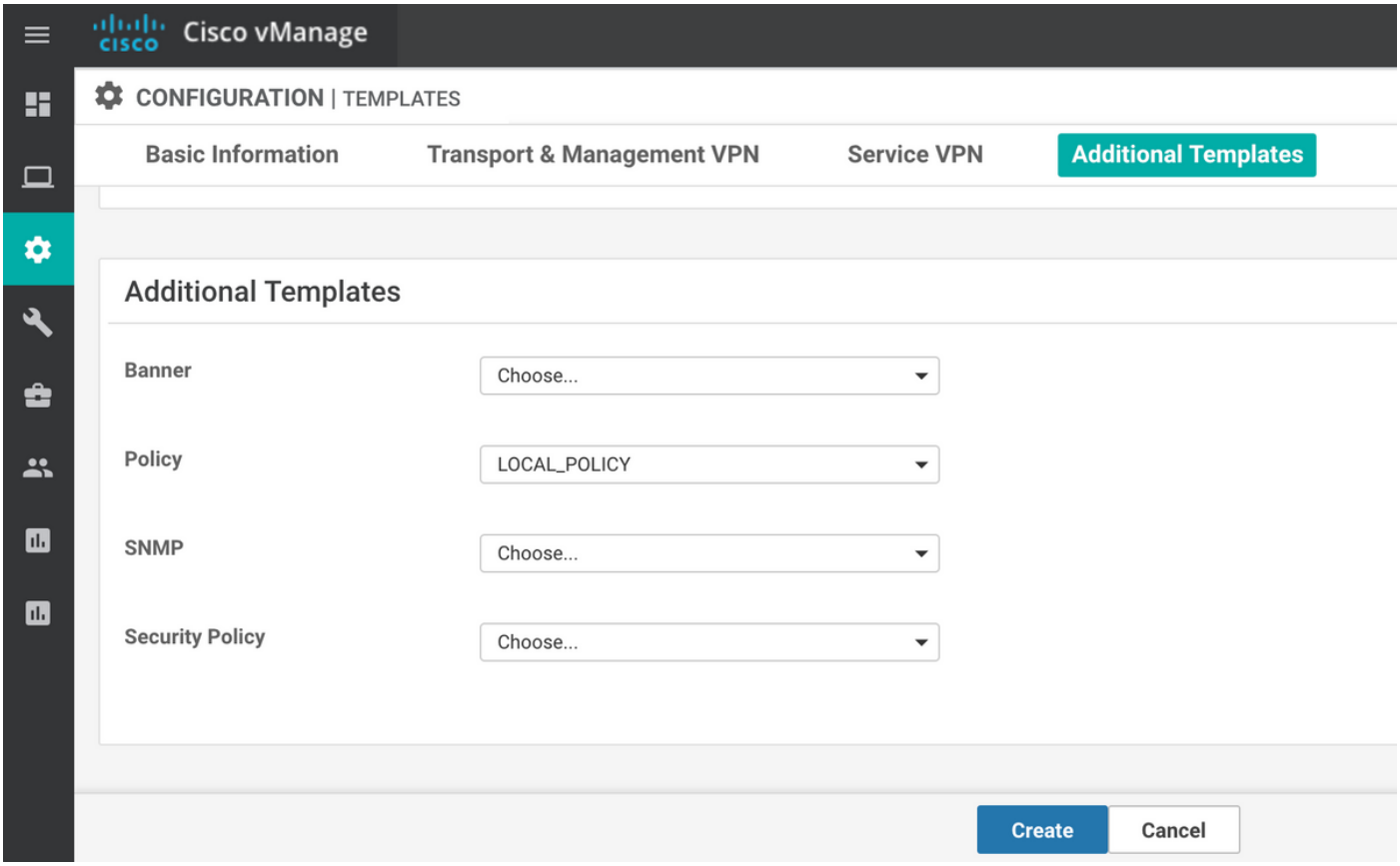
Si des modèles de fonctionnalités de périphérique sont utilisés, vous devez créer une stratégie localisée et configurer la liste de contrôle d'accès à l'étape **de l'**Assistant **Configuration des listes de contrôle d'accès** :



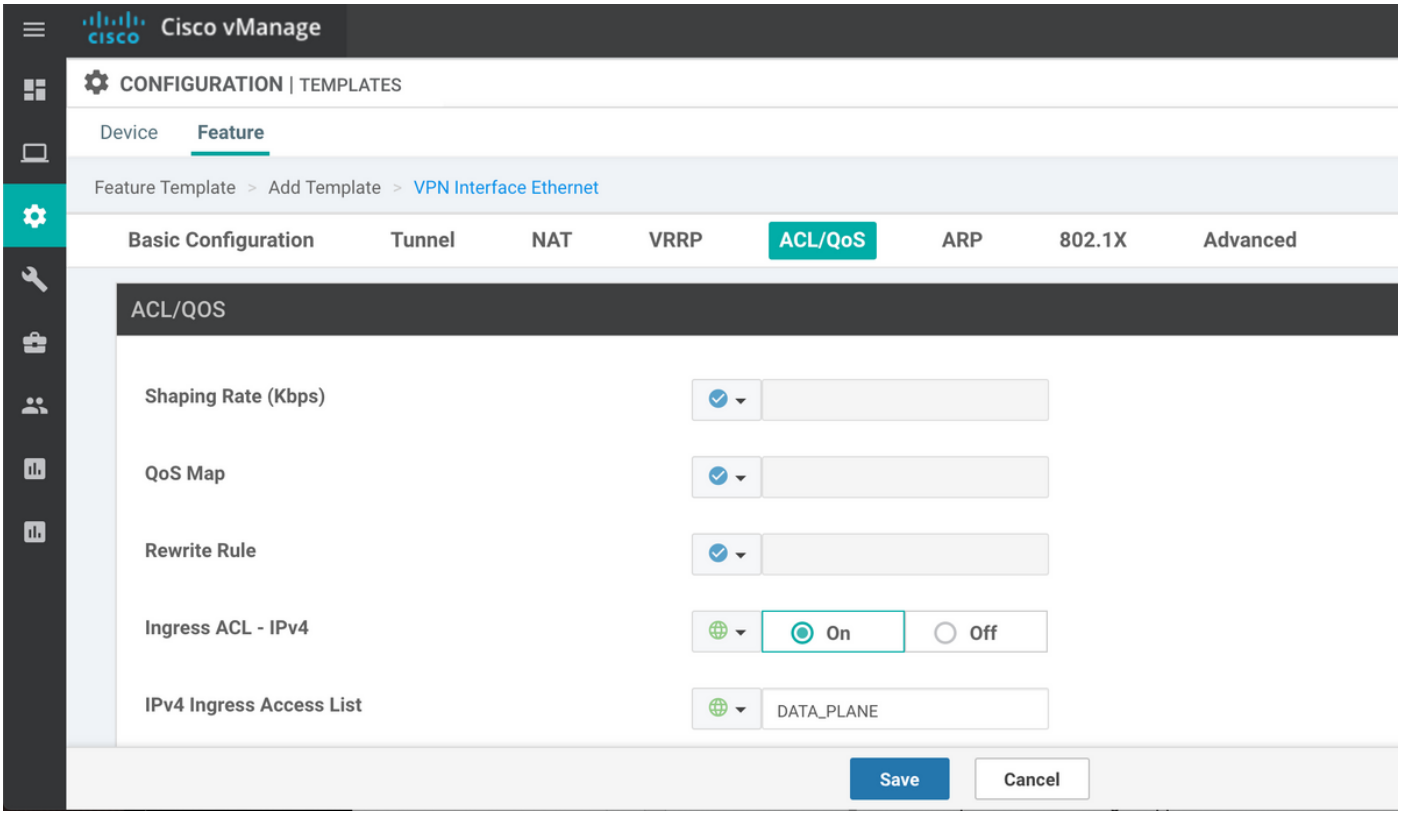
Si **implicit-acl-logging** n'est pas encore activé, il peut être judicieux de l'activer à l'étape finale avant de cliquer sur le bouton **Enregistrer la stratégie** :



La stratégie localisée (nommée **LOCAL_POLICY** dans notre cas) doit être référencée dans le modèle de périphérique :



Ensuite, la liste de contrôle d'accès (nommée **DATA_PLANE** dans notre cas) doit être appliquée sous VPN Interface Ethernet Feature Template en entrée (dans) :



Une fois que la liste de contrôle d'accès est configurée et appliquée à l'interface pour contourner le trafic du plan de données, la session BFD est de nouveau à l'état **up** :

```
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
```

Autres considérations

Veuillez noter que la solution de contournement avec ACL est bien plus pratique que le transfert de port NAT, car vous pouvez également faire correspondre les adresses source du site distant pour une plus grande sécurité et une protection contre les attaques DDoS sur votre périphérique, par exemple :

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

Notez également que pour tout autre trafic entrant (non spécifié avec **les services autorisés**), par exemple pour le port **iperf** par défaut 5001 ACL explicite **seq 20** comme dans cet exemple, cela n'aura aucun effet par opposition au trafic du plan de données :

```
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
   !
  !
```

Et vous avez toujours besoin d'une règle d'exemption NAT Port-Forward pour que **iperf** fonctionne :

```
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
   !
  !
 !
!
```

Conclusion

Ce comportement est attendu sur les routeurs vEdge en raison des caractéristiques de conception du logiciel NAT et ne peut pas être évité.