NATが使用されている場合、vEdgeがIPSecトンネルを確立できない理由

内容

概要

このドキュメントでは、vEdgeルータがデータプレーントンネルにIPSecカプセル化を使用し、1つのデバイスが対称NAT(RFC3489)またはアドレス依存マッピング(RFC4787)を実行するネットワークアドレス変換(NAT)デバイスのの背後にある問題についてを説明しますトランスポート側インターフェイスに設定されているNATの他のタイプ。

背景説明

> **注：**この記事は vEdge ルータにのみ適用され、vEdge ソフトウェア 18.4.1 および 19.1.0 で見られる動作に基づいて記述されています。 新しいリリースでは、動作が異なる可能性があります。不明な点がある場合は、マニュアルを参照するか、Cisco Technical Assistance Center（TAC）にお問い合わせください。

このデモでは、SD-WAN TAC ラボで問題を再現しました。デバイス設定は、次の表のとおりです。

ホスト名	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
vbond	1	10.10.10.231	192.168.0.231	192.168.0.231

トランスポート側の設定は、両方のデバイスでごく一般的なものです。vEdge1 の設定は、次のとおりです。

```
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 の設定は、次のとおりです。

```
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
```

このドキュメントでの問題のデモのために、仮想適応型セキュリティアプライアンス（ASAv）ファイアウォールが 2 つの vEdge ルータの間に存在します。ASAv は、次のルールに従ってアドレス変換を実行しています。

- vEdge1 からのトラフィックがコントローラに向かう場合、送信元ポート 12346 ～ 12426 は 52346 ～ 52426 に変換されます。
- vEdge1 からのトラフィックが他のサイトへのデータプレーン接続を目的としている場合、送信元ポート 12346 ～ 12426 は 42346 ～ 42426 に変換されます。
- vEdge1 からの他のすべてのトラフィックも、同じパブリックアドレス（198.51.100.232）にマッピングされます。

参考までに、ASAv NAT 設定は、次のとおりです。

```
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
```

問題

正常動作シナリオ

通常の状態では、データプレーントンネルが確立され、Bidirectional Forwarding Detection（BFD）が稼働（up）状態になっていることが分かります。

コントローラとの制御接続を確立するために vEdge1 デバイスで使用されているパブリックポート（52366）に注意してください。

```
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
```

vEdge2 では NAT は使用されていないため、プライベートアドレスとポートは同じです。

```
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
```

vEdge1 からの **show tunnel statistics** で、tx/rx カウンタが増加していることが分かります。

```
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
```

vEdge2 からの同じ出力で、rx/rx パケットカウンタが増加していることも分かります。宛先ポート（42366）が制御接続の確立に使用されるポート（52366）と異なっていることに注意してください。

```
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
```

ただし、BFD セッションは両方のデバイスで引き続き稼働しています。

```
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
```

制御プレーンとデータプレーンの接続に異なるポートを使用しても、問題は発生せず、接続が確立されています。

障害シナリオ

ユーザーは、vEdge2 ルータでダイレクト インターネット アクセス (DIA) を有効にしたいと考えています。そのために、次の設定を vEdge2 に適用しました。

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

また、BFD セッションが予期せずにダウンしており、しかもダウン状態が続いています。トンネル統計情報をクリアした後の **show tunnel statistics** の出力で、RX カウンタが増加していないことが分かります。

```
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
```

当初、ユーザーは、トンネル MTU に関連する問題であると考えていました。上記の出力と「正常動作シナリオ」セクションの出力を比較すると、正常動作シナリオではトンネル MTU が 1441 であるのに対して、障害シナリオでは 1442 であることが分かります。マニュアルによると、トンネル MTU は 1442 (デフォルトインターフェイス MTU の 1500 バイト - トンネルオーバーヘッドの 58 バイト) である必要がありますが、BFD が稼働状態になると、トンネル MTU は 1 バイト減少します。参考までに、BFD がダウン (**down**) 状態のときの **show tunnel statistics** と **show tunnel statistics bfd** の出力は、次のとおりです。

```
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
```

また、BFD が稼働状態の場合は、次のとおりです。

```
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
```

注：なお、上記の出力を調べることで、カプセル化をともなう BFD パケットのサイズを確認することができます。2 つの出力間で受信された BFD パケットは 1 つだけであるため、BFD エコーの RX オクテット値を減算する（584987 - 584816）と、171 バイトという結果が得られます。これは、BFD 自体が使用する帯域幅を正確に計算するために役立ちます。

BFD が**ダウン**状態のままになっている原因は、MTU ではなく、明らかに NAT 設定です。**正常動作シナリオ**と**障害シナリオ**の間で異なっているのはこれだけです。ここで、DIA 設定の結果として vEdge2 によって NAT スタティックマッピングが変換テーブルに自動作成され、データプレーン IPSec トラフィックバイパスが可能になっていることが分かります。

```
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        -
```

出力を見ると、ポート 42366 の代わりにポート 52366 が使用されています。 これは、vEdge2 が 52366 ポートを予期しており、それを vSmart によってアドバタイズされた OMP TLOC から学習したためです。

```
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
```

解決方法

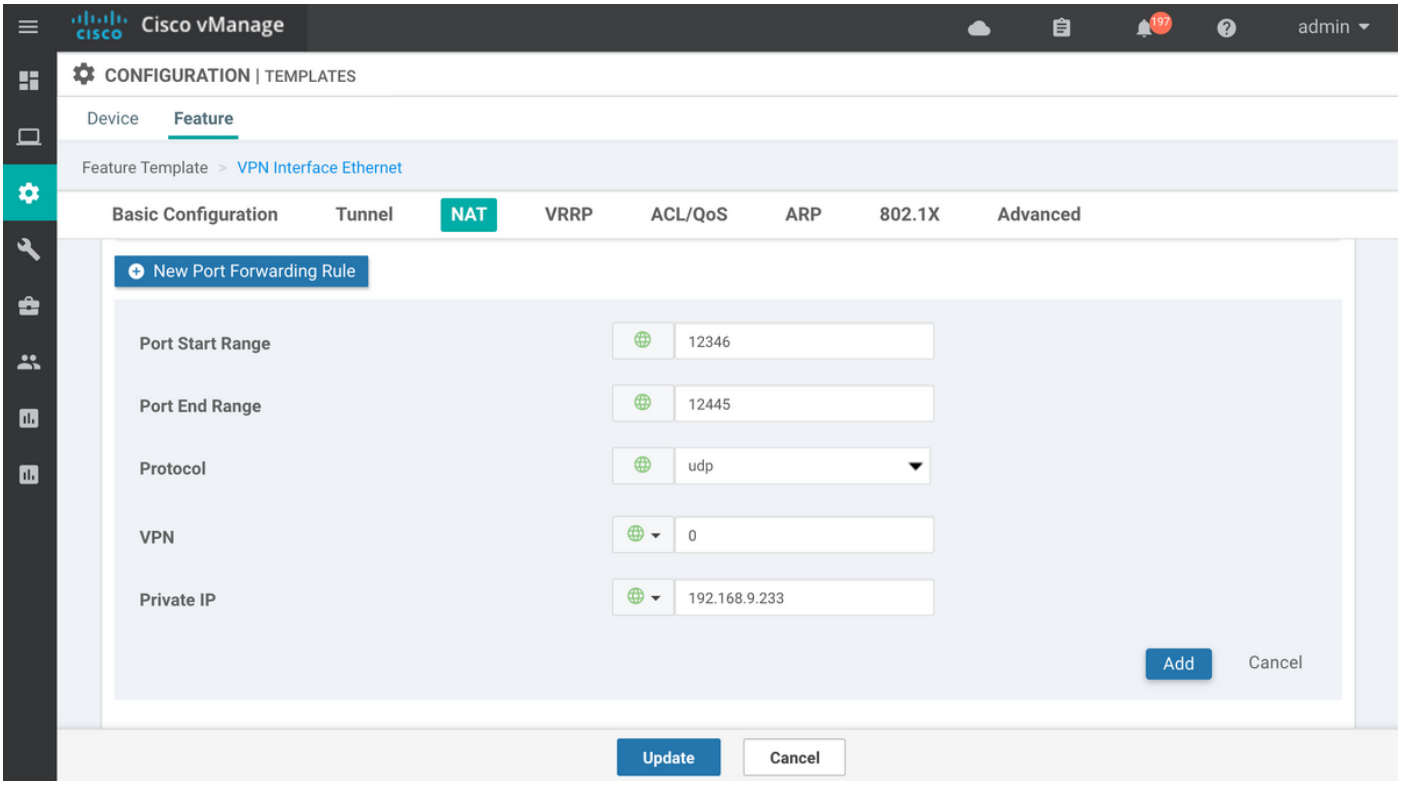
NAT ポートフォワーディング

一見して、このような問題の回避策は簡単です。任意の送信元からのデータプレーン接続に対するフィルタ処理を強制的にバイパスするように、vEdge2 トランスポート インターフェイスでの静的 NAT 免除ポートフォワーディングを設定できます。

```
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
   !
  !
 !
!
```

12346 ~ 12446の範囲は、すべての可能な初期ポート（12346、12366、12386、12406、および12426とポートオフセットを加えた）に対応します。 詳細については、『Firewall Ports for Viptela Deployments』を参照してください。

CLI テンプレートの代わりにデバイス機能テンプレートを使用している場合は、図に示されているように、対応するトランスポート（vpn 0）インターフェイスの新しい VPN イーサネット機能テンプレートを**新しいポートフォワーディング ルール**で更新または追加する必要があります。



明示的 ACL

また、明示的 ACL を使用した別の解決方法も可能です。ポリシー（policy）セクションで implicit-acl-logging が設定されている場合、/var/log/tmplog/vdebug ファイルに次のメッセージが含まれていることがあります。

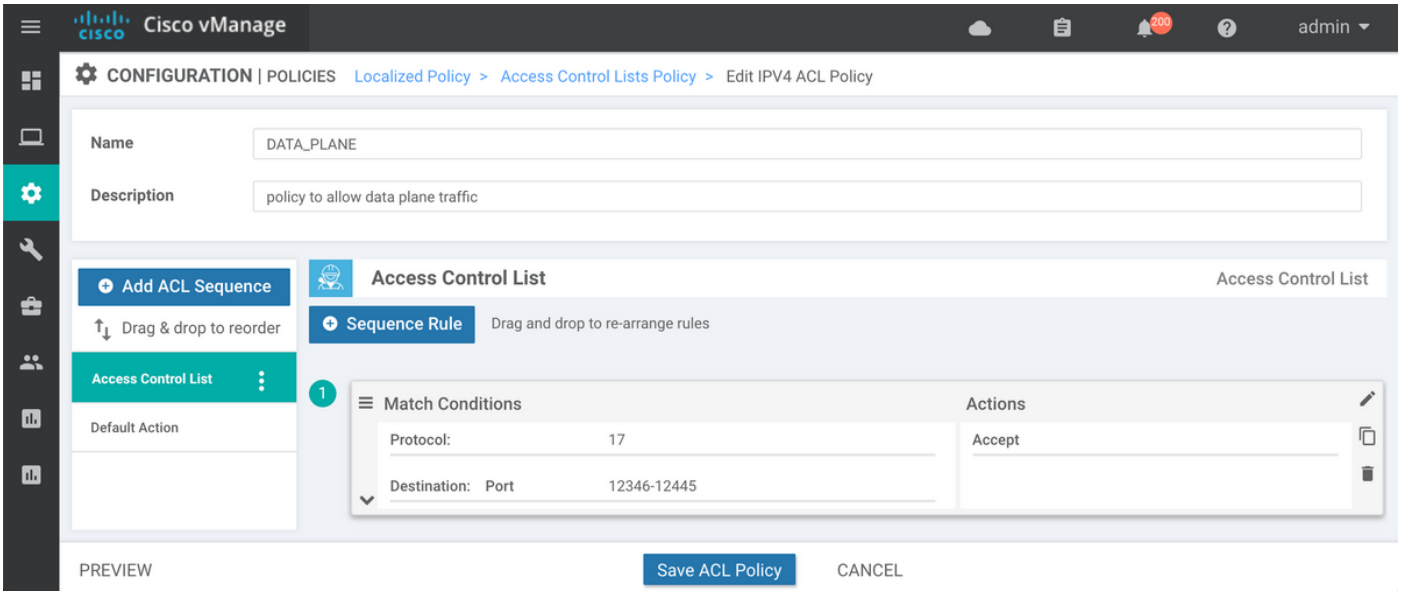
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

ここでは根本原因が説明されており、それに従って、次のように vEdge2 のアクセス制御リスト（ACL）で着信データプレーンパケットを明示的に許可する必要があります。

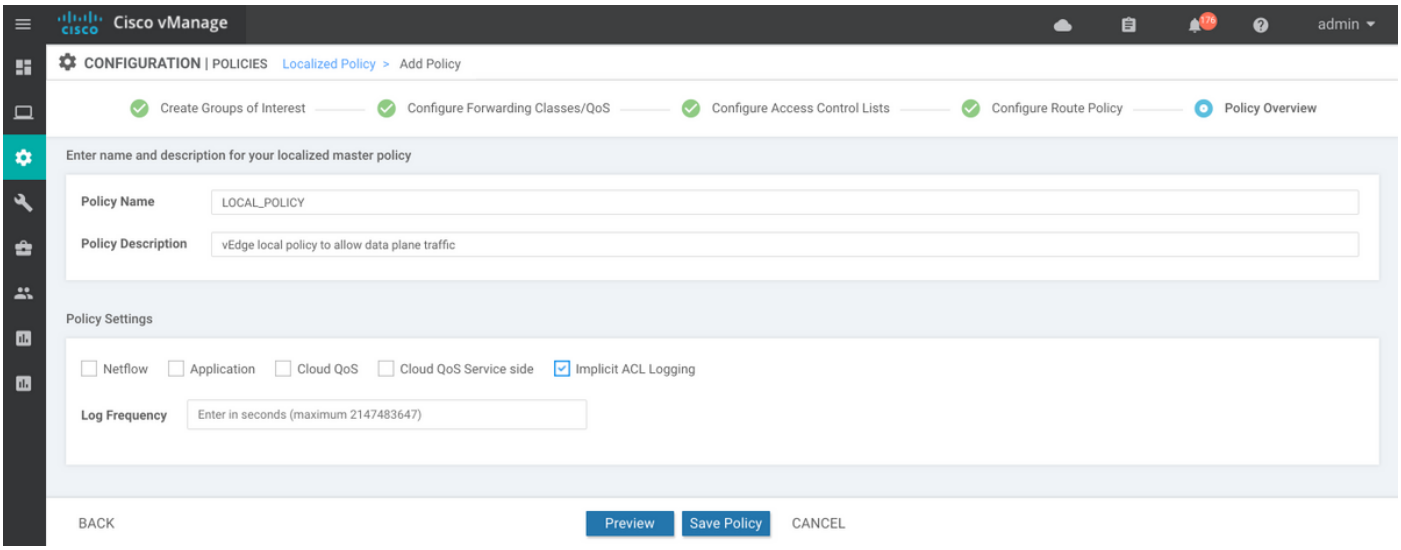
```
vpn 0
 interface ge0/1
  ip address 192.168.9.233/24
  nat
   respond-to-ping
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no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

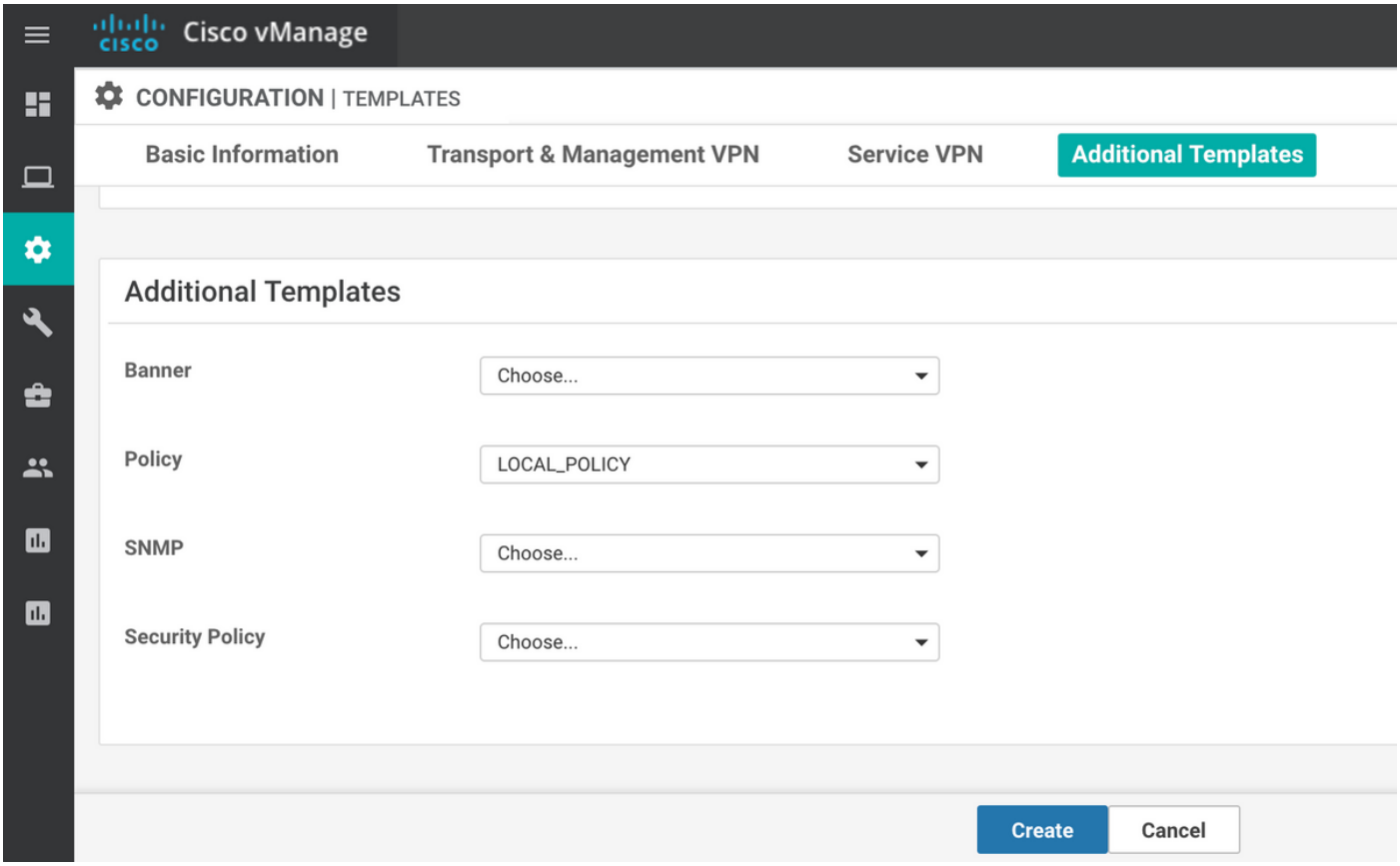
デバイス機能テンプレートを使用している場合は、ローカライズされたポリシーを作成し、[アクセス制御リストの設定（Configure Access Control Lists）] ウィザードステップで ACL を設定する必要があります。



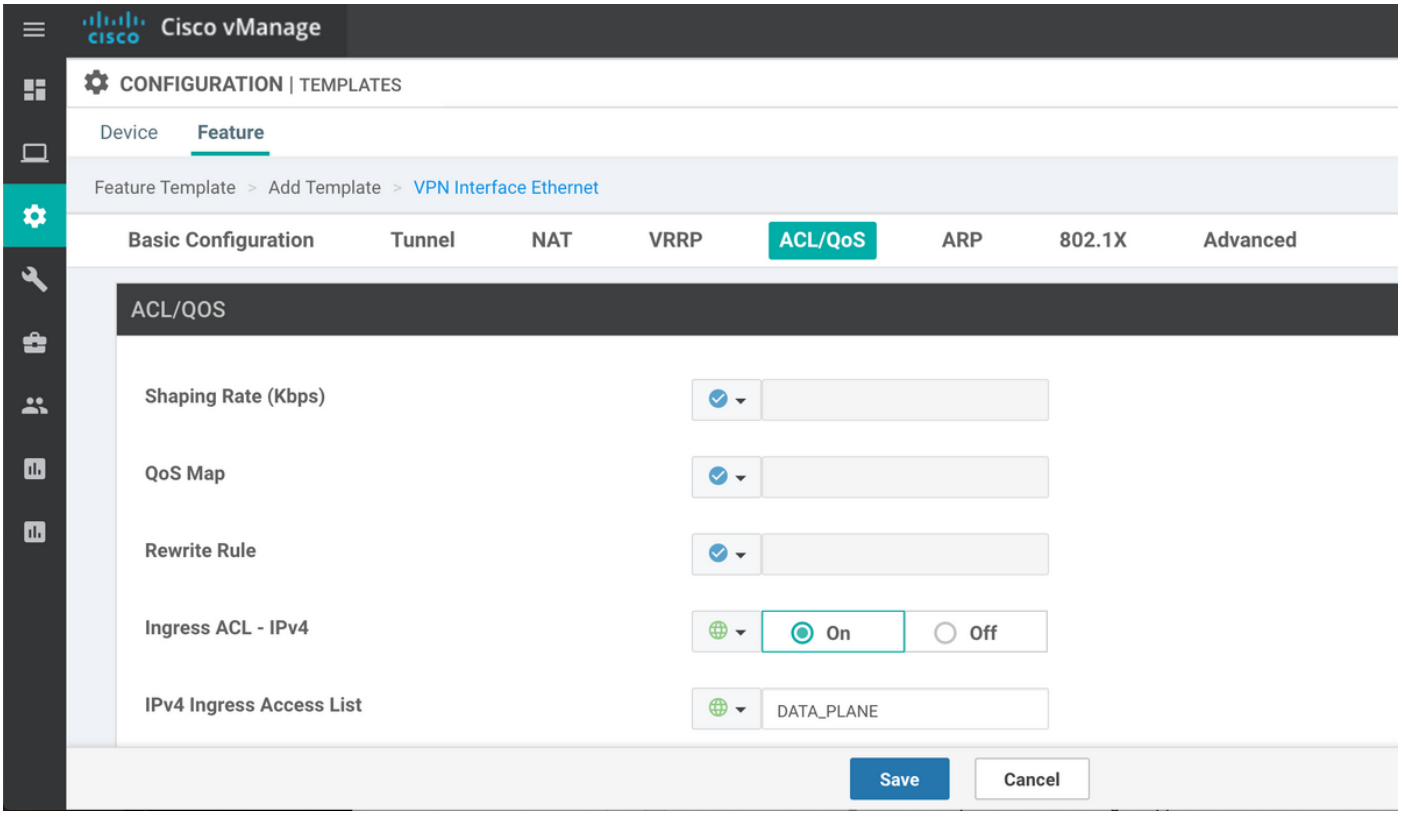
implicit-acl-logging がまだ有効になっていない場合は、[ポリシーの保存（Save Policy）] ボタンをクリックする前に、最終ステップで有効にすることをお勧めします。



ローカライズされたポリシー（この例では「LOCAL_POLICY」という名前）はデバイステンプレートで参照される必要があります。



次に、ACL（この例では「**DATA_PLANE**」という名前）を、VPN インターフェイス イーサネット機能テンプレートで入力（Ingress）方向に適用する必要があります。



ACL が設定されてインターフェイスに適用され、データプレーントラフィックがバイパスされると、それ以降、BFD セッションは再び**稼働**状態になります。

```
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
```

それ以外に考慮すること

ACL を使用した回避策の方が NAT ポートフォワーディングよりもはるかに実用的であることに注意してください。これは、たとえば次のように、リモートサイトの送信元アドレスに基づく照合を行うことで、セキュリティを強化し、DDoS 攻撃からデバイスを保護することもできるためです。

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

また、他の着信トラフィック（**allowed-services** で指定されていないもの）は、たとえば、この例のようにデフォルト **iperf** ポート 5001 の明示的 ACL **seq 20** を使用する場合、データプレーントラフィックとは異なり、何の影響も受けないことに注意してください。

```
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
   !
  !
```

さらに、**iperf** が機能するには、依然として NAT ポートフォワーディング免除ルールが必要です。

```
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
   !
  !
 !
!
```

結論

これは、NAT ソフトウェアの設計上の仕様に起因する、vEdge ルータで予期される動作であり、回避することはできません。