Warum können vEdges IPSec-Tunnel nicht einrichten, wenn NAT verwendet wird?

Inhalt

Einführung
Hintergrundinformationen
Problem
Arbeitsszenario
Fehlerszenario
Lösung
NAT-Port-Forward
Explizite ACL
Weitere Überlegungen
Schlussfolgerung

Einführung

Dieses Dokument beschreibt das Problem, das auftreten kann, wenn vEdge-Router IPSec-Kapselung für Datenebenentunnel verwenden und ein Gerät hinter einem Network Address Translation (NAT)-Gerät steht, das Symmetric NAT (RFC3489) oder Address Dependent Mapping (RFC4787) ausführt, während ein anderes Gerät Direct Internet Access (DIA) oder einen anderen NAT-Typ auf dem konfigurierten Transportseitige Schnittstelle.

Hintergrundinformationen

> **Hinweis**: Dieser Artikel gilt nur für vEdge-Router und wurde basierend auf dem Verhalten der vEdge-Software 18.4.1 und 19.1.0 geschrieben. Bei neueren Versionen kann das Verhalten unterschiedlich sein. Bei Zweifeln wenden Sie sich bitte an das Cisco Technical Assistance Center (TAC).

Für die Demonstration wurde das Problem im SD-WAN TAC Lab wiedergegeben. Die Geräteeinstellungen sind in der folgenden Tabelle zusammengefasst:

Hostname	Standort-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
Obligation	1	10.10.10.231	192.168.0.231	192.168.0.231

Die Transportseitenkonfiguration ist auf beiden Geräten recht allgemein. Dies ist die Konfiguration von 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
```

Um das Problem in diesem Dokument zu veranschaulichen, befindet sich die ASAv-Firewall (Virtual Adaptive Security Appliance) zwischen zwei vEdge-Routern. ASAv führt Adressenübersetzungen gemäß den folgenden Regeln durch:

- Wenn der Datenverkehr vom vEdge1 für Controller bestimmt ist, werden die Quellports 12346-12426 in 52346-52426 übersetzt
- Wenn Datenverkehr von vEdge1 für Datenebenenverbindungen zu anderen Standorten bestimmt ist, werden die Quellports 12346-12426 in 42346-42426 umgewandelt
- Der gesamte andere Datenverkehr aus vEdge1 ist ebenfalls derselben öffentlichen Adresse zugeordnet (198.51.100.232).

Dies ist die ASAv NAT-Konfiguration als Referenz:

```
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
```

Problem

Arbeitsszenario

Im normalen Zustand können wir beobachten, dass Datenebenentunnels eingerichtet sind, die Bidirectional Forwarding Detection (BFD) ist **betriebsbereit**.

Beachten Sie, welcher öffentliche Port auf dem vEdge1-Gerät (52366) zum Herstellen von Steuerungsverbindungen mit Controllern verwendet wurde:

```
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
```

Auf dem vEdge2 wird keine NAT verwendet, daher sind private Adressen und Ports identisch:

```
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
```

In den **show tunnel** statistics from vEdge1 sehen wir, dass die tx/rx-Zähler inkrementieren:

```
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
```

Aus derselben Ausgabe von vEdge2 können Sie sehen, dass Rx-/Rx-Paketzähler inkrementieren. Beachten Sie, dass sich der Zielport (42366) vom Port zum Herstellen von Steuerungsverbindungen (52366) unterscheidet:

```
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
```

BFD-Sitzungen sind jedoch auf beiden Geräten immer noch aktiv:

```
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
```

Unterschiedliche Ports, die für die Verbindungen der Kontroll- und Datenebene verwendet werden, verursachen keine Probleme, da die Verbindung eingerichtet ist.

Fehlerszenario

Der Benutzer möchte Direct Internet Access (DIA) auf dem vEdge2-Router aktivieren. Hierzu wurde diese Konfiguration auf vEdge2 angewendet:

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

Und die BFD-Sitzung ging unerwartet verloren und bleibt darüber hinaus in einem Downstate. Nach dem Löschen von Tunnelstatistiken können Sie sehen, dass der RX-Zähler in der Ausgabe **show tunnel statistics** nicht erhöht:

```
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


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
```

Zunächst hatte der Kunde das Problem im Zusammenhang mit Tunnel-MTU vermutet. Wenn Sie die oben aufgeführten Ausgaben mit Ausgaben aus dem Abschnitt "Working Scenario" vergleichen, können Sie bemerken, dass im Szenario Tunnel MTU 1441 gegenüber 1442 im Szenario ausgefallen ist. Basierend auf der Dokumentation sollte die Tunnel-MTU 1442 (1500 Standard-Schnittstellen-MTU - 58 Byte für Tunnel-Overhead) betragen, aber sobald BFD aktiv ist, wird die Tunnel-MTU um 1 Byte gesenkt. Als Referenz werden Ausgaben aus der **Anzeige von Tunnelstatistiken** sowie **die** unten angegebene **Tunnelstatistik bfd** für den Fall **angezeigt**, dass BFD im **ausgefallenen** Zustand ist:

```
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
```

Wenn BFD aktiv ist:

```
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
```

Hinweis: Übrigens können wir die BFD-Paketgröße zusammen mit der Kapselung ermitteln, indem wir die oben aufgeführten Ausgänge betrachten. Beachten Sie, dass zwischen zwei Ausgängen nur ein BFD-Paket empfangen wurde, sodass der Wert 584987-584816 für die Umrechnung des BFD-Echo-RX-Oktets 171 Byte ergeben wird. Es kann sinnvoll sein, die von BFD selbst verwendete Bandbreite genau zu berechnen.

Der Grund für BFD, der im **ausgefallenen** Zustand feststeckt, ist nicht die MTU, sondern die NAT-Konfiguration. Dies ist die einzige Änderung, die zwischen **Arbeitsszenario** und **Fehlgeschlagen** geändert wurde. Sie können hier sehen, dass infolge der DIA-Konfiguration von vEdge2 automatisch eine statische NAT-Zuordnung in der Übersetzungstabelle erstellt wurde, um die Umgehung des IPSec-Datenverkehrs auf Datenebene zu ermöglichen:

```
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        -
```

Wie Sie sehen, wird Port 52366 anstelle von 42366 verwendet. Der Grund hierfür ist, dass vEdge2

den 5236-Port erwartet und von den von vSmart angekündigten OMP-TLOCs gelernt hat:

```
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
```

Lösung

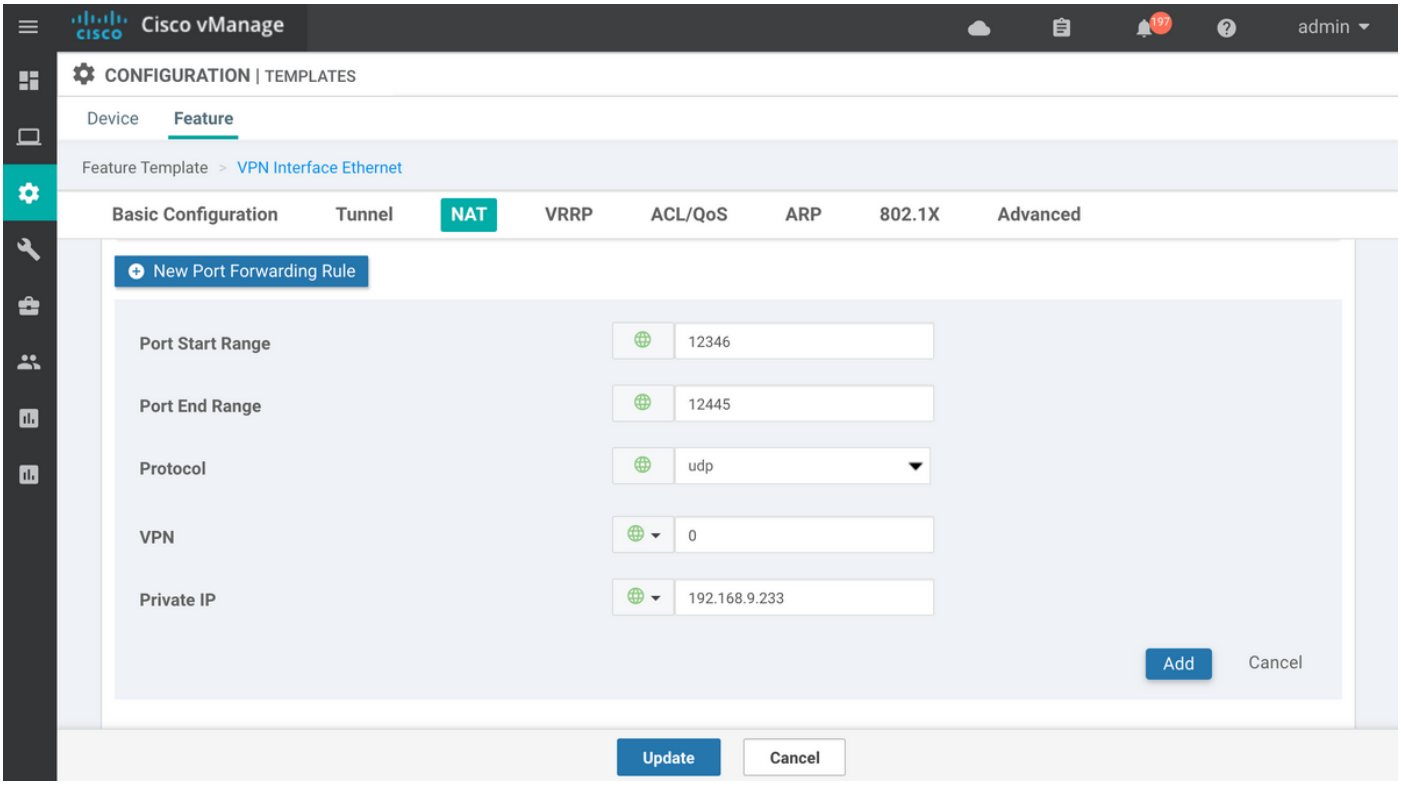
NAT-Port-Forward

Auf den ersten Blick ist die Problemumgehung für solche Probleme einfach. Sie können die statische NAT-Freistellungs-Port-Weiterleitung an der vEdge2-Transportschnittstelle so konfigurieren, dass die Filterung für Datenebenenverbindungen von beliebigen Quellen kraftvoll umgangen wird:

```
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
   !
  !
 !
!
```

Im Bereich 12346 bis 12446 sind alle möglichen Anfangsports untergebracht (12346, 12366, 12386, 12406 und 12426 plus Port-Offset). Weitere Informationen hierzu finden Sie unter "Firewall-Ports für IP-Bereitstellungen".

Wenn anstelle der CLI-Vorlage Gerätefunktionsvorlagen verwendet werden, muss das Gleiche für die entsprechende Transportschnittstelle (VPN 0) mit der **New Port Forwarding Rule** (**Neue Port-Weiterleitungsregel)** aktualisiert oder hinzugefügt werden, wie im Bild gezeigt:



Explizite ACL

Eine weitere Lösung mit expliziter ACL ist ebenfalls möglich. Wenn **die implizite Protokollierung** unter dem **Richtlinienabschnitt** konfiguriert ist, wird möglicherweise die folgende Meldung in der **/var/log/tmplog/vdebug-**Datei angezeigt:

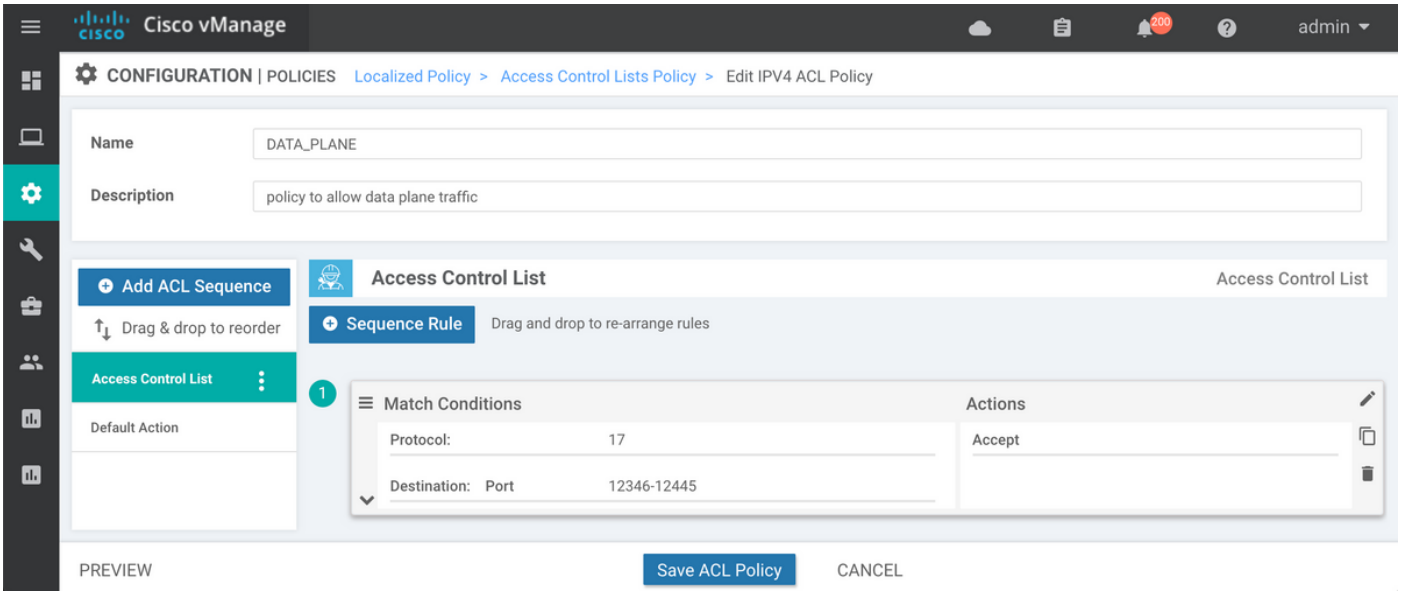
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

Es wird die Ursache erläutert. Daher müssen eingehende Datenebenenpakete in der Zugriffskontrollliste (ACL) auf dem vEdge2 explizit zugelassen werden. Beispiel:

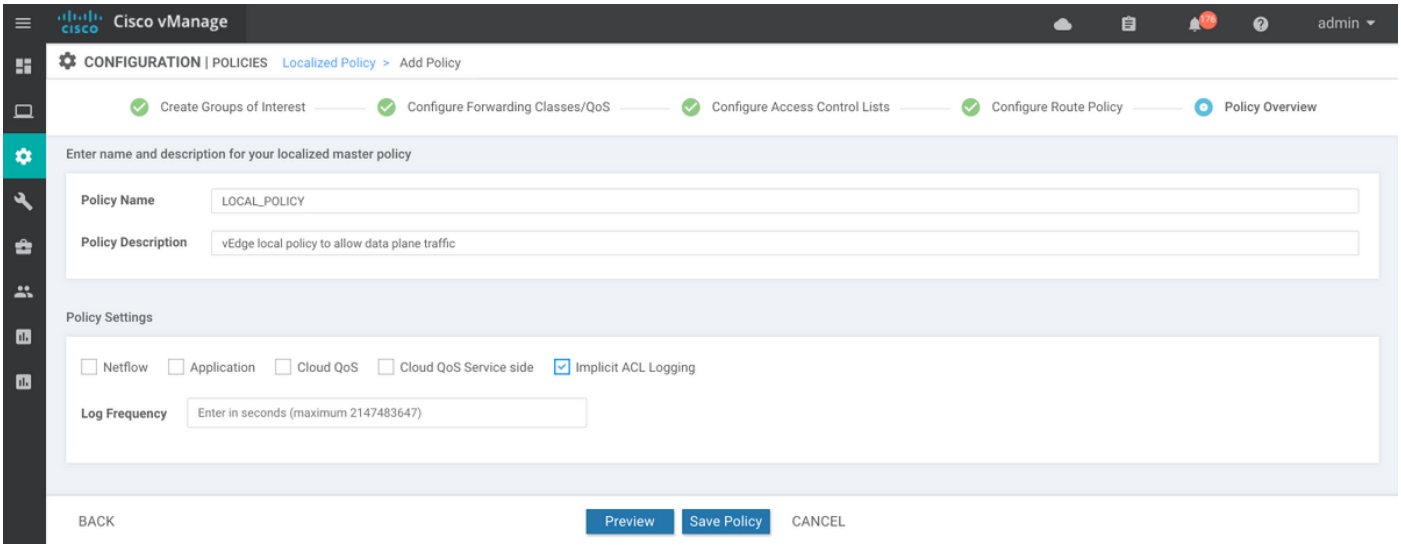
```
vpn 0
 interface ge0/1
  ip address 192.168.9.233/24
  nat
   respond-to-ping
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no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

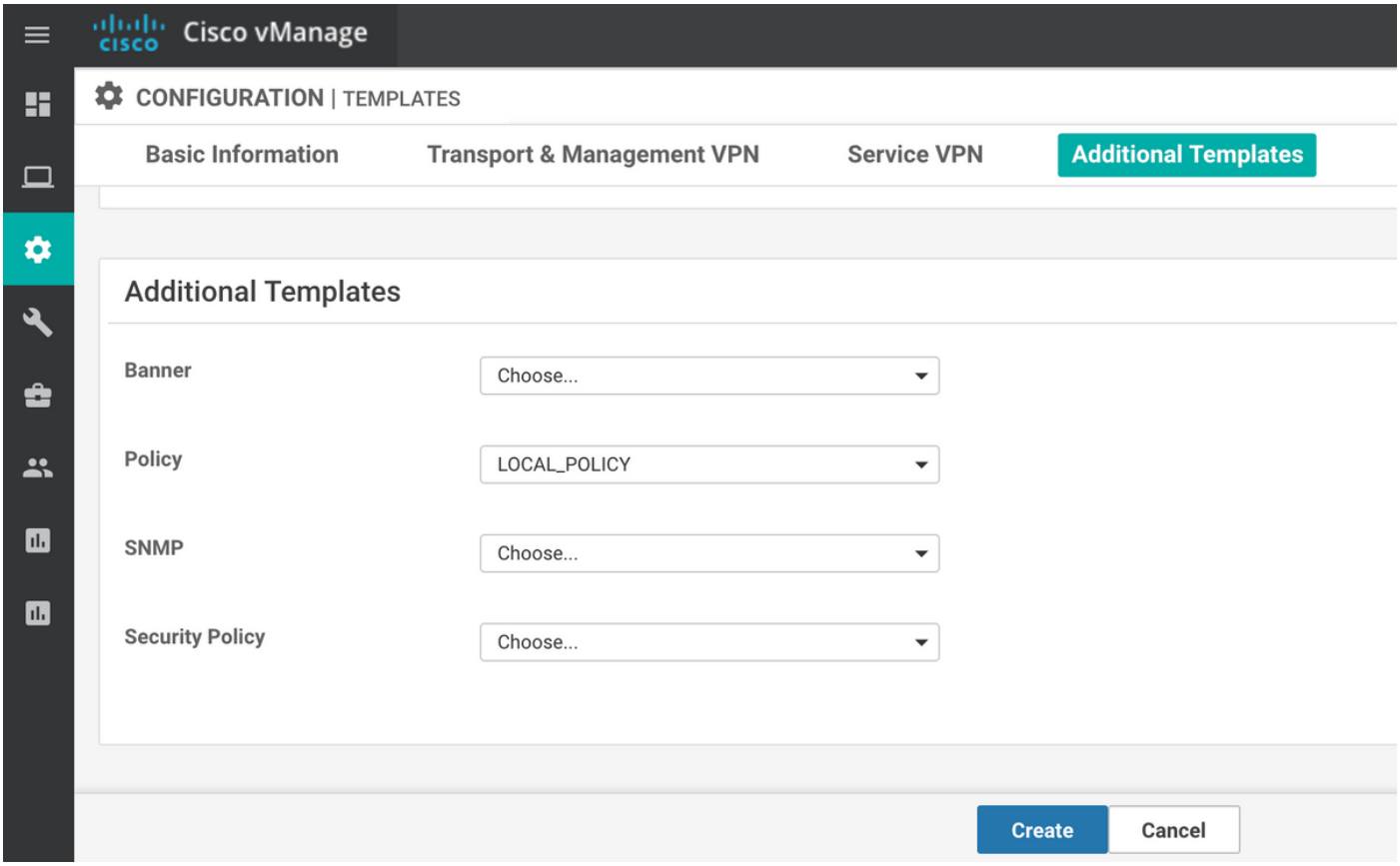
Wenn Gerätefunktionsvorlagen verwendet werden, müssen Sie eine lokalisierte Richtlinie erstellen und die Zugriffskontrollliste im Assistenten **für die Konfiguration von Zugriffskontrolllisten** konfigurieren:



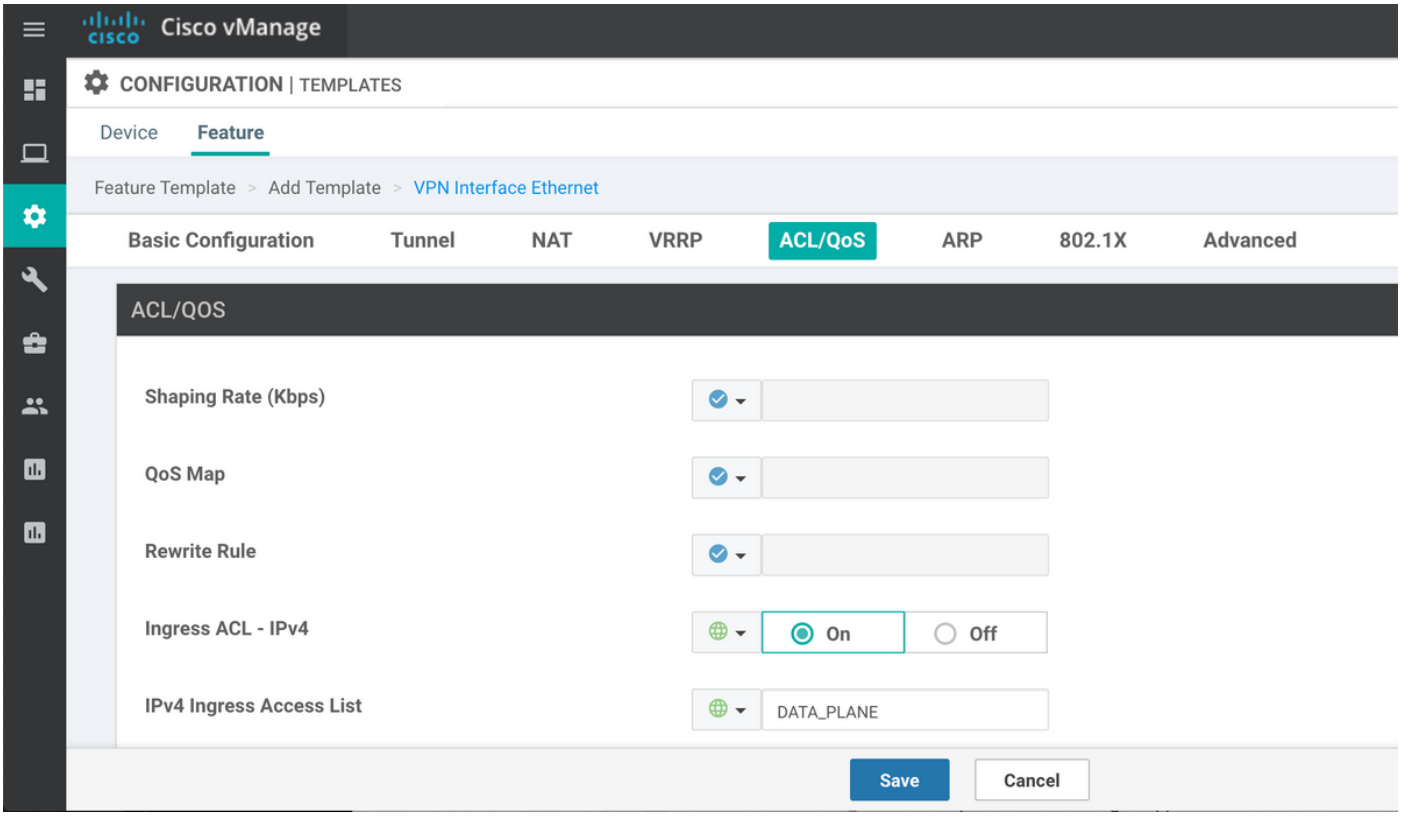
Wenn **implizite ACL-Protokollierung** noch nicht aktiviert ist, empfiehlt es sich, diese Option im letzten Schritt zu aktivieren, bevor Sie auf die Schaltfläche **Save Policy (Richtlinie speichern) klicken**:



Auf lokalisierte Richtlinien (in unserem Fall **LOCAL_POLICY** genannt) sollte in der Gerätevorlage verwiesen werden:



Anschließend sollte ACL (**DATA_PLANE** in unserem Fall) unter "VPN Interface Ethernet Feature Template" (Ethernet-Feature-Vorlage für VPN-Schnittstellen) in Eingangsrichtung (in) angewendet werden:



Nachdem die ACL konfiguriert und auf die Schnittstelle angewendet wurde, um den Datenverkehr auf der Datenebene zu umgehen, wird die BFD-Sitzung wieder in den **Betriebszustand versetzt**:

```
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
```

Weitere Überlegungen

Bitte beachten Sie, dass die Problemumgehung mit der ACL viel praktischer ist als die NAT-Port-Weiterleitung, da Sie die Zuordnung auch basierend auf den Quelladressen des Remote-Standorts vornehmen können, um die Sicherheit zu erhöhen und DDoS-Angriffe auf Ihr Gerät zu verhindern, z. B.:

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

Beachten Sie außerdem, dass bei anderem eingehenden Datenverkehr (der nicht mit **zugelassenen Diensten** angegeben ist), z. B. bei **iperf-Standard-**Port 5001 explizite ACL **seq 20** wie in diesem Beispiel, dies keine Auswirkungen im Vergleich zum Datenverkehr auf der Datenebene hat:

```
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
   !
  !
```

Für die Funktion von **iperf** ist weiterhin die NAT-Regel für die Port-Weiterleitung erforderlich:

```
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
   !
  !
 !
!
```

Schlussfolgerung

Dieses Verhalten wird bei vEdge-Routern erwartet, da es durch die Einzelheiten des NAT-Softwaredesigns verursacht wird und nicht vermieden werden kann.