为什么无法的vEdges设立IPSec隧道，如果NAT使用？

Contents

Introduction

本文描述可能出现的问题，当vEdge路由器使用IPSec封装数据层面隧道时，并且一个设备是在进行对称NAT (RFC3489)或地址从属的映射(RFC4787)的网络地址转换(NAT)设备后，而别的有直接互联网访问(DIA)或在传输边接口配置的某个其他种NAT。

背景信息

> **Note**:此条款为只有vEdge路由器是可适用的和被写了根据被看到的工作情况在vEdge软件18.4.1和19.1.0。在更新的版本中工作情况可能是不同的。与文档请咨询或在疑惑的情况下请与Cisco技术支持中心(TAC)联系。

为演示的目的，问题在SD-WAN TAC实验室被再次产生了。设备设置在表里被总结这里：

主机名-	站点id	系统IP	专用IP	公共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

传输旁边配置是相当通用的在两个设备。这是vEdge1的配置：

```
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
```

为了展示在本文的问题，虚拟可适应的安全工具(ASAv)防火墙驻留在两vEdge路由器之间。ASAv根据这些规则执行地址转换：

- 如果从vEdge1的数据流供控制器使用，源端口12346-12426被转换到52346-52426
- 如果从vEdge1的数据流供与其他站点的数据层面连接使用，源端口12346-12426被转换到42346-42426
- 从vEdge1的其他数据流也被映射对同一个公共地址(198.51.100.232)

这是ASAv NAT配置供参考：

```
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
```

问题

工作的方案

在正常状态下，我们能观察数据层面隧道设立，双向转发检测(BFD)在**UP状态。**

请注意哪个公共端口在vEdge1设备(52366)使用建立与控制器的控制连接：

```
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
```

在vEdge2没有使用NAT，因此专用地址和端口是相同的：

```
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
```

在**显示隧道statisticsfrom** vEdge1我们能看到tx/rx计数器增加：

```
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
```

从vEdge2的同样输出您能看到rx/rx信息包计数器增加。请注意目的地端口(42366)是与用于的端口不同建立控制连接(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
```

但是BFD会话仍然在两个设备：

```
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
```

用于控制和数据层面连接的不同的端口不导致任何问题，连接到位。

故障情景

用户希望对enable (event)直接互联网访问(DIA)在vEdge2路由器。为了执行如此，此配置被运用了于vEdge2 ：

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

而且并且BFD会话在downstate意外地断开了和坚持。在清除隧道统计数据后您能看到RX计数器不增加输出的**显示隧道统计数据**：

```
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
```

最初，用户怀疑该问题建立隧道MTU。如果以上输出与“工作的方案”部分的输出比较，您能注意那在工作的方案隧道MTU是1441与1442在失败的方案。 凭文档，隧道MTU应该是1442 (1500默认接口MTU -顶上的隧道的58个字节)，但是，一旦BFD是UP，隧道MTU由1个字节降低。供您的参考，输出从**显示隧道统计数据**与一起**显示隧道**为案件下面所提供的**统计数据bfd，**当BFD在**故障状态时**：

```
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
```

并且，如果BFD在UP状态：

```
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:顺便说一句，我们能与封装一起确定BFD信息包大小通过查找到以上输出。 注意仅一个BFD信息包收到了在两个输出之间，因此减去Bfd echo RX八位位组值584987 - 584816将产生我们171-byte结果。精密地计算BFD使用的带宽可以是有用的。

在**故障状态**滞留的BFD的原因明显地是没有MTU，然而NAT配置。这是唯一的事更改在**工作的方案**和**出故障的方案之间**。您能看到这里由于DIA配置， Nat static映射由vEdge2在转换表里自动地创建允许数据层面IPSec信息数据流旁路：

```
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        -
```

正如你看到的端口52366使用而不是42366。这是因为vEdge2期待52366端口和了解它从OMP vSmart做通告的TLOCs ：

```
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
```

解决方案

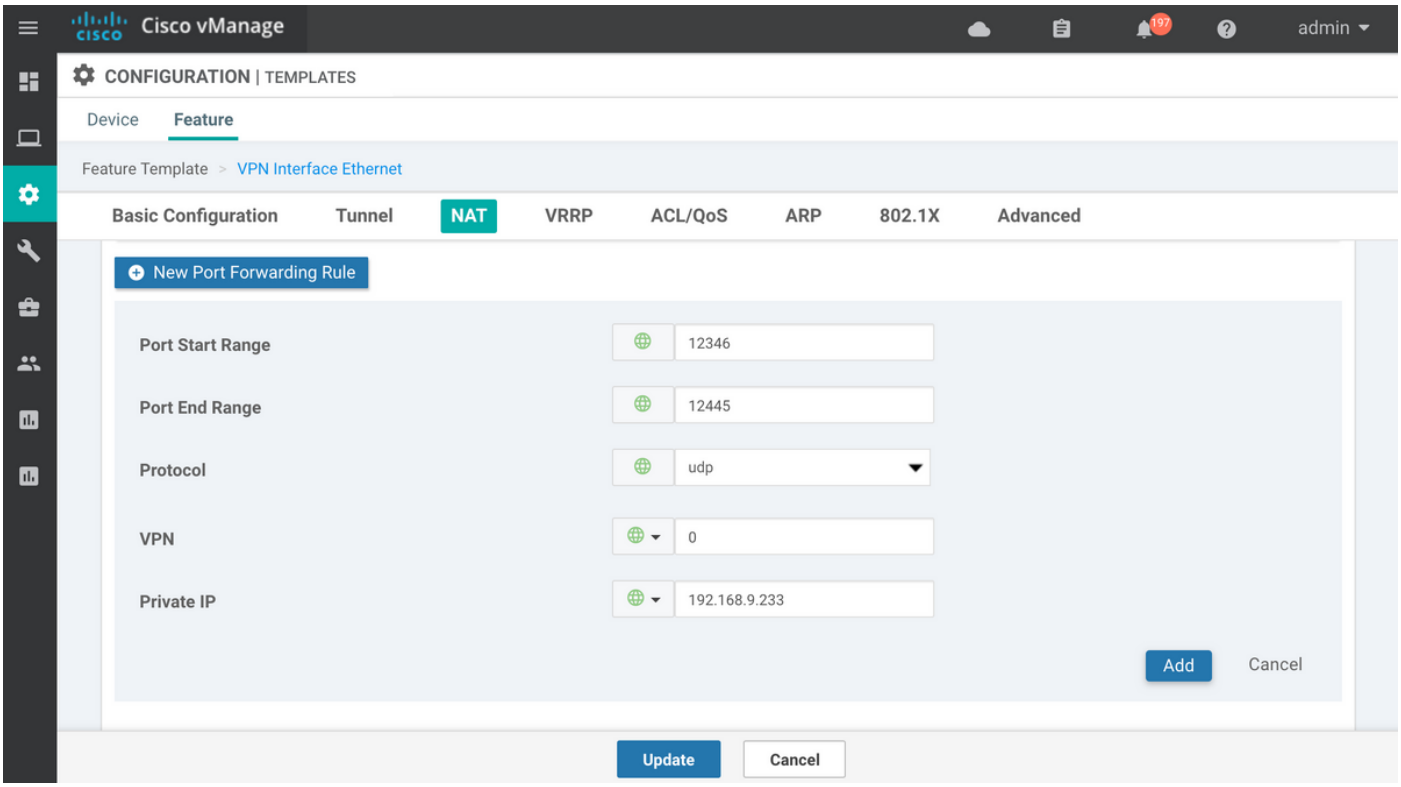
NAT Port-forward

从第一扫视，这样问题类型的解决方法是简单的。您能配置在vEdge2传输接口的静态NAT免税端口转发强有力地绕过数据层面连接的过滤从所有来源：

```
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
   !
  !
 !
!
```

这里范围12346到12446适应所有可能的初始端口(12346， 12366， 12386， 12406和12426正端口偏移量)。 关于此的更多信息请参见“Viptela配置的防火墙端口”。

如果设备功能模板使用而不是CLI模板，则达到同样，我们需要更新或添加对应的传输(VPN 0)如镜像所显示，接口的新的VPN以太网功能模板与**新的端口转发规则**， ：



明确ACL

并且，与明确ACL的另一个解决方案是可能的。如果含蓄ACL**记录**被配置在策略部分下，您可以注意在**/var/log/tmplog/vdebug**文件的下列信息：

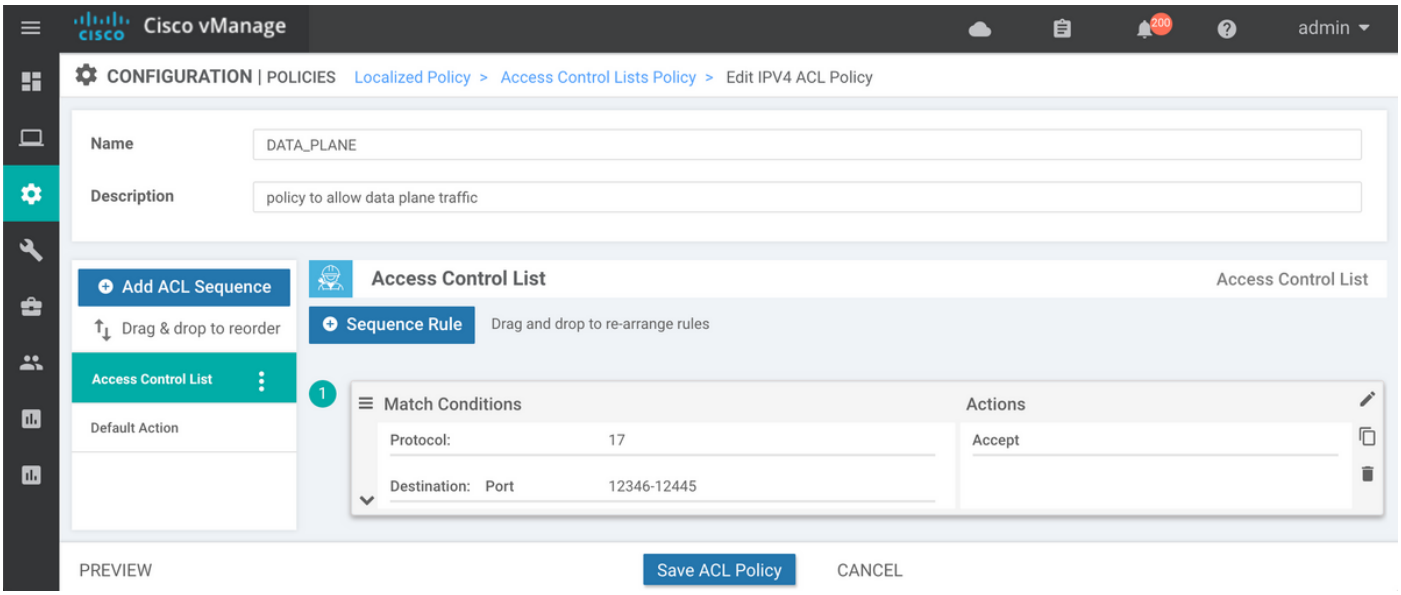
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

它解释根本原因并且您需要明显地允许在访问控制表(ACL)的流入数据层面信息包在象这样的vEdge2 ：

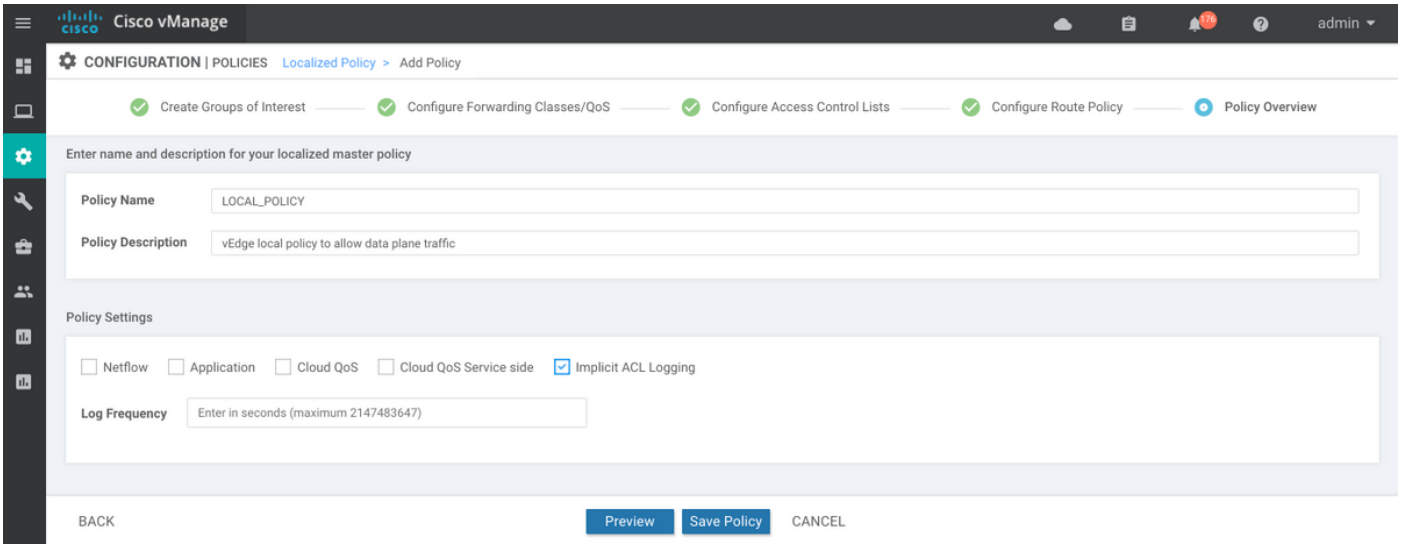
```
vpn 0
```

```
 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 ! !
```

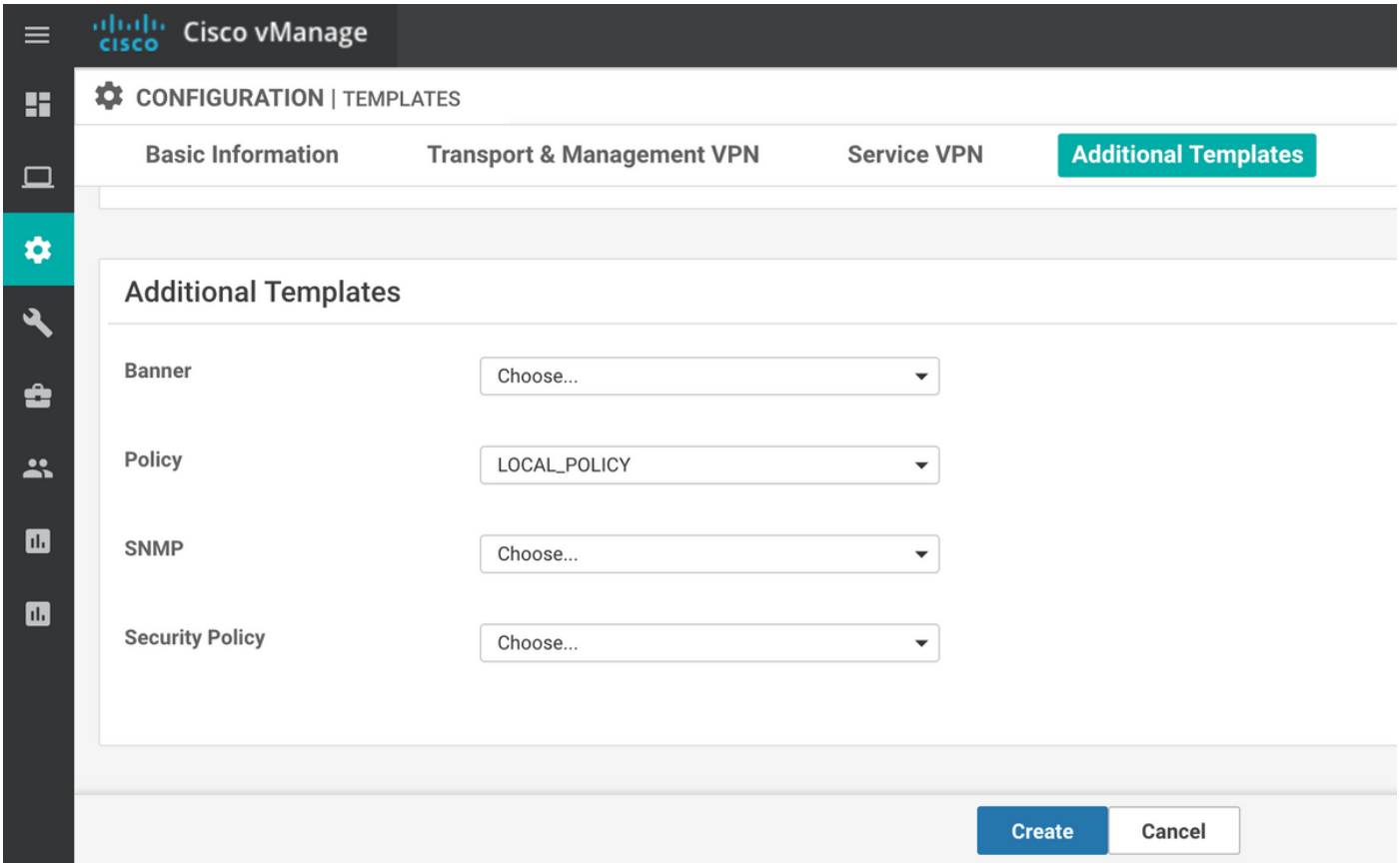
如果设备使用功能模板，则您需要创建本地化的策略和配置在**Configure访问控制列表**向导步骤的ACL ：



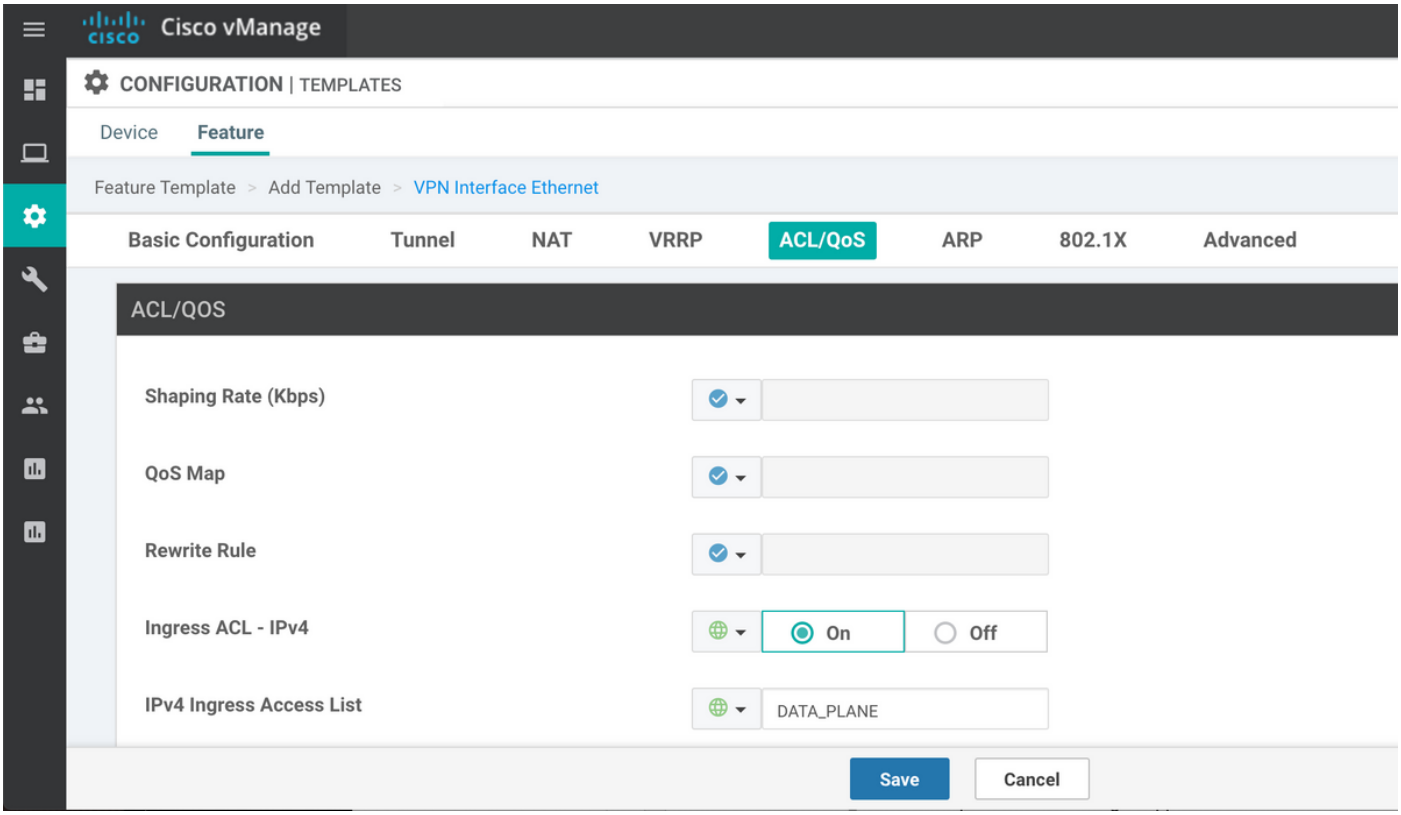
如果含蓄ACL**记录不**是启用的，它也许是一个好想法到enable (event)它在最终步骤，在请点击**保存策略**按钮前：



设备模板应该参考本地化的策略(在我们的情况的已命名**LOCAL_POLICY**) ：



ACL (在我们的情况的已命名**DATA_PLANE**)应该然后适用在VPN以太网接口在入口()方向的功能模板下：



一旦ACL设定及适用于接口绕过数据层面数据流， BFD会话再是更多对**UP状态**：

```
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
```

其他注意事项

请注意:与ACL的解决方法比NAT端口转发实用，因为您可以也配比基于远程站点的源地址更加巨大的安全的和保护免受DDoS攻击到您的设备，即：

```
 access-list DATA_PLANE
  sequence 10
```

```
   match
    source-ip        198.51.100.232/32
    destination-port 12346 12445
    protocol         17
   !
   action accept
   !
  !
```

并且请注意:对于其他流入的数据流(没指定用允许**服务**)即默认iperfport 5001明确ACL的顺序**20类似**在本例中这不会做任何效果与数据层面数据流相对：

```
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
   !
  !
```

并且您仍然需要NAT port-forward **iperf的**免税规则能工作：

```
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
   !
  !
 !
!
```

结论

这是在NAT软件设计特定造成的vEdge路由器的期望的工作情况，并且不可能避免。