لماذا يتعذّر على vEdges إنشاء أنفاق IPSec إذا كانت ترجمة عناوين الشبكة (NAT) قيد الاستخدام؟

المحتويات

المقدمة

يصف هذا المستند المشكلة التي قد تنشأ عندما تستخدم موجهات vEdge تضمين IPSec الذي لأنفاق مستوى البيانات، ويكون أحد الأجهزة خلف جهاز ترجمة عنوان الشبكة (NAT) الذي يقوم بعمل NAT (RFC3489) أو التخطيط المعتمد على العنوان (RFC4787)، بينما يكون لدى الآخر الوصول المباشر إلى الإنترنت (DIA) أو نوع آخر من NAT تم تكوينه على واجهة جانب النقل.

معلومات أساسية

> **ملاحظة**: تنطبق هذه المقالة على موجهات vEdge فقط، وقد تمت كتابتها استنادا إلى السلوك الملحوظ في برنامج vEdge 18.4.1 و 19.1.0. قد يكون سلوك الإصدارات الأحدث مختلفا. يرجى الرجوع إلى الوثائق أو الاتصال بمركز المساعدة التقنية (TAC) من Cisco في حالة وجود شكوك.

لغرض العرض التوضيحي، تم تكرار المشكلة في مختبر SD-WAN TAC. تم تلخيص إعدادات الأجهزة في الجدول هنا:

اسم المضيف	معرف الموقع	IP لنظام	خاص-ip	عام-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

فبون 1 دن	10.10.10.231	192.168.0.231	192.168.0.231

تكوين جانب النقل عام تمامًا على كل الجهازين. هذا هو تكوين 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
```

لتوضيح المشكلة الواردة في هذا المستند، يوجد جدار حماية جهاز الأمان القابل للتكيف الظاهري (ASAv) بين موجهات vEdge. يقوم ASAv بترجمات العناوين وقفل هذه القواعد:

- إذا كانت حركة المرور من vEdge1 مخصصة لوحدات التحكم، فإن منافذ المصدر 12346-12426 يتم ترجمتها إلى 52346-52426
- إذا كانت حركة المرور من vEdge1 مخصصة لاتصالات مستوى البيانات بالمواقع الأخرى، فسيتم ترجمة منافذ المصدر 12346-12426 إلى 42346-42426
- كما يتم تعيين جميع حركات المرور الأخرى من vEdge1 على نفس العنوان العام

(198.51.100.232)
هذا ASAv nat تشكيل لمرجع:

```
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
```

المشكلة

سيناريو العمل

في الحالة العادية، يمكنني مالحظة إنشاء أنفاق مستوى البيانات، اكتشاف إعادة التوجيه ثنائي الإتجاه (BFD) في حالة **قوق**.

الرجاء مالحظة المنفذ العام المستخدم على جهاز vEdge1 (52366) لإنشاء إتصالات التحكم باستخدام وحدات التحكم:

```
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
```

في vEdge2 الا يتم إستخدام NAT، وبالتالي فإن العنوان الخاص والمنافذ هي نفسها:

```
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
```

في إحصائيات **show tunnel** من vEdge1 يمكنني رؤية زيادة عدادات tx/rx:

```
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
```

من نفس المخرجات من vEdge2 يمكنك أن ترى بالإضافة إلى أن عدادات حزم rx/rx تزايد. الرجاء ملاحظة أن منفذ الوجهة (42366) مختلف عن المنفذ المستخدم لإنشاء إتصالات التحكم (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
```

ولكن جلسات عمل BFD لا تزال قيد التشغيل على كل الجهازين:

```
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
```

ال تتسبب المنافذ المختلفة المستخدمة للتحكم واتصالات مستوى البيانات في أي مشاكل، كما أن الاتصال في موضعه.

سيناريو الفشل

يرغب المستخدم في تمكين الوصول المباشر إلى الإنترنت (DIA) على موجه vEdge2.
للقيام بذلك، تم تطبيق هذا التكوين على vEdge2:

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

و إنخفضت جلسة عمل BFD بشكل غير متوقع و عالوة على ذلك بقيت في حالة الإنخفاض.
إحصائيات النفق إخراج في زيادة RX ال عداد أن ترى أن يمكنك، النفق إحصائيات مسح بعد show:

```
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
```

في البداية، اشتبه العميل في أن المشكلة تتعلق بالوحدة الحرارية المتعددة (MTU) "سيناريو العمل"، للنفق. إذا قمت بمقارنة المخرجات الواردة أعلاه مع المخرجات من قسم وي سيناريو العمل MTU هو 1441 مقابل 1442 في السيناريو يمكنك ملاحظة أن في سيناريو العمل الفاشل. استنادا إلى الوثائق، يجب أن تكون وحدة الحد الأقصى للنقل (MTU) عبر النفق وحدة الحد الأقصى للنقل (MTU) الافتراضية للواجهة - 58 بايت للنفاق (1500 1442) الزائدة)، ولكن بمجرد تشغيل وحدة الحد الأقصى للنقل (BFD)، يتم خفض وحدة الحد الأقصى للنقل (MTU) عبر النفق بمقدار 1 بايت. لمرجعك، فخرجات من **show إحصائيات** الموفرة أدناه لحالة عندما يكون BFD في حالة **أسفل**: **show tunnel bfd** مع **show tunnel إحصائيات**

```
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
```

وإذا كان BFD في حالة ما:

```
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
```

> **ةظحالم**: رظنلا لالخ نم نيمضتلا ةيلمع عم BFD ةمزح مجح ديدحت اننكمي ،ةبسانملاب ،نيجرخم نيب طقف ةدحاو BFD ةمزح يقلت مت هنأ ظحال .هالعأ ةدراولا تاجرخملا ىلإ (584987 - 584816) تايناملثلل BFD RX ىدص لاسرإ ةميق ميسقت نإف يلاتلابو يددرتلا قاطنلا باسح ديفملا نم نوكي دقو .تياب 171 ةعس ةجيتن انيطعيس ةقدب هسفن BFD لبق نم مدختسملا.

ببسلا فوقول BFD يف ةلاحلا **ىلفسلا** سيل MTU، نكل ليكشت NAT حوضوب. اذه وه انه تيأر عيطتسي تنأ. **لشفلا ويرانيس** و **لمعلا ويرانيس** نيب ريغت يذلا ديحولا ءيشلا نأ ةجيتن نم DIA ليكشت، NAT ساكن إستاتيكي يطخت تاقولت ايئاقلت ب vEdge2 يف ةمجرتلا ةلواط نأ حمسي تايطعم ىوتسم تانايب IPSec ةكرح رورم زواجت:

```
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        -
```

52366 ذفنمو عقوتي vEdge2 نأل كلذو .42366 نم الدب تلمعتسا نوكي 52366 ءانيم ،ىرت امك

وتعلمه من وحدات التحكم في الوصول إلى البنية الأساسية (OMP) المعلن عنه اةطساوب 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
```

الحل

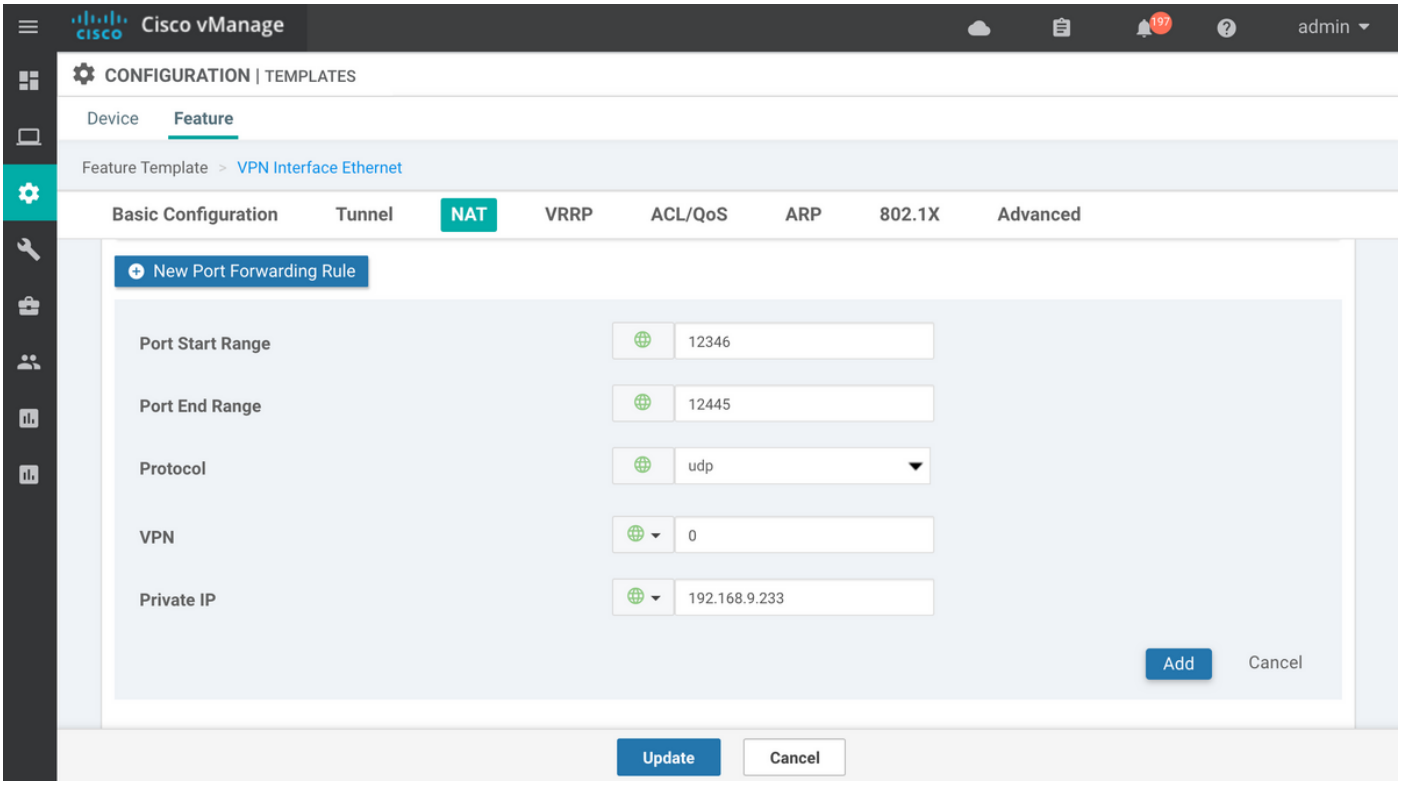
nat Port-forward

للوهلة الأولى قد يكون الحل لمثل هذا النوع من المشاكل بسيطا. أنت تستطيع عيشكلت ل يفصيي زواجتي نأ نراق لقن vEdge2 على forwarding ءانيم ءافعإ nat يكيتاتسإ ناكس معطيات مستوى توصيل من أي مصدر بقوة:

```
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
   !
  !
 !
!
```

النطاق هنا من 12346 إلى 12446 يستوعب جميع المنافذ الأولية الممكنة (12346 و 12366 و 12386 و 12406 و 12426 بالإضافة إلى مزيد من موازنة المنفذ). لمزيد من المعلومات حول هذا الأمر، ارجع إلى "منافذ جدار الحماية لعمليات نشر Viptela".

إذا كانت لديك قواعد صارمة من جدار الحماية، فقم بتعديل الأوامر مثل واجهة باقية تدريجيًا للأحرف من خلال تحديد مزيد من VPN جديد أو إضافته لواجهة النقل نفس الإجراء، المطابقة (VPN 0) باستخدام **قاعدة إعادة توجيه المنافذ الجديدة**، كما هو موضح في الصورة:



قائمة تحكم في الوصول (ACL) صريحة

كما يمكن إستخدام حل آخر مع قائمة تحكم في الوصول (ACL) واضحة. إذا تم تكوين **تسجيل قائمة التحكم في الوصول المضمنة** تحت قسم **السياسة**، فقد تلاحظ الرسالة التالية في الملف **/var/log/tmplog/vdebug:**

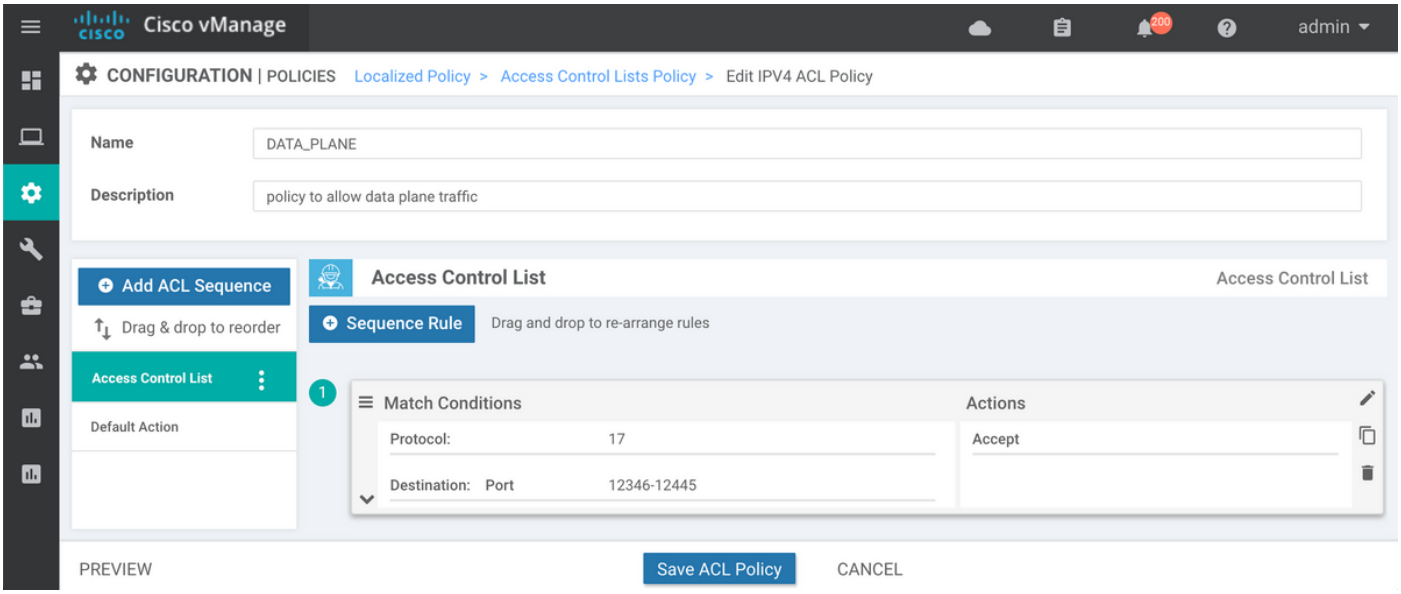
```
local7.notice: Jun  8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG
vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192  inbound-acl, Implicit-ACL, Result:
denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu
```

وهو يشرح السبب الجذري والتالي يلزمك السماح بشكل صريح بحزم مستوى البيانات الواردة في قائمة التحكم في الوصول (ACL) على vEdge2 بهذا الشكل:

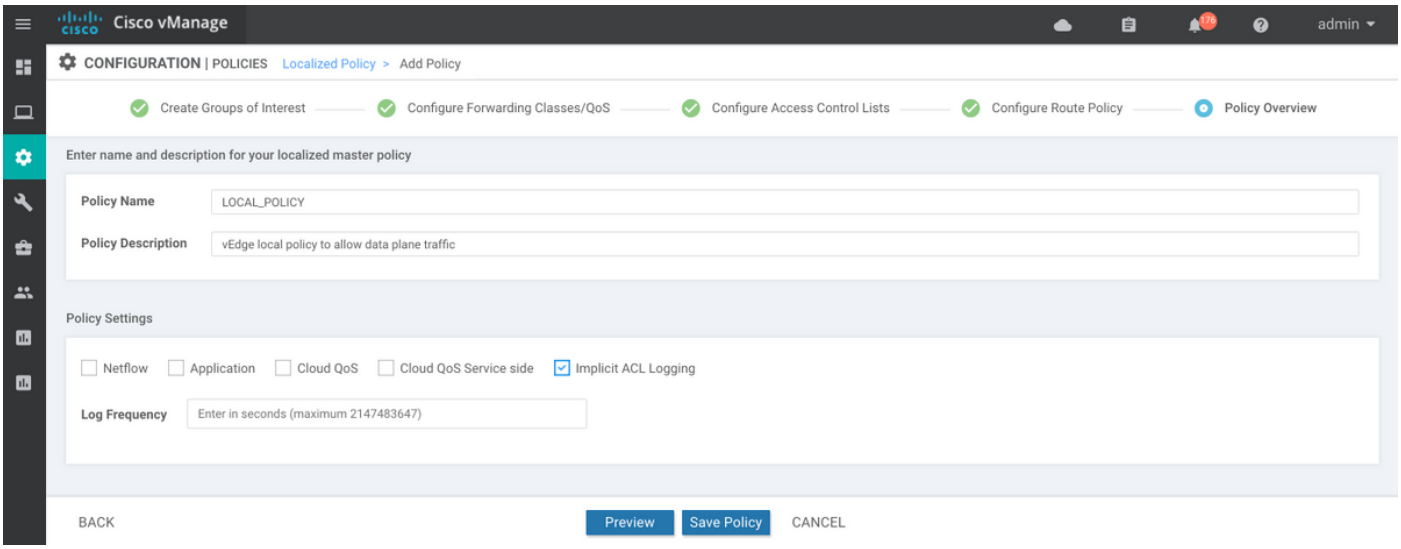
```
vpn 0
 interface ge0/1
  ip address 192.168.9.233/24
  nat
   respond-to-ping
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no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

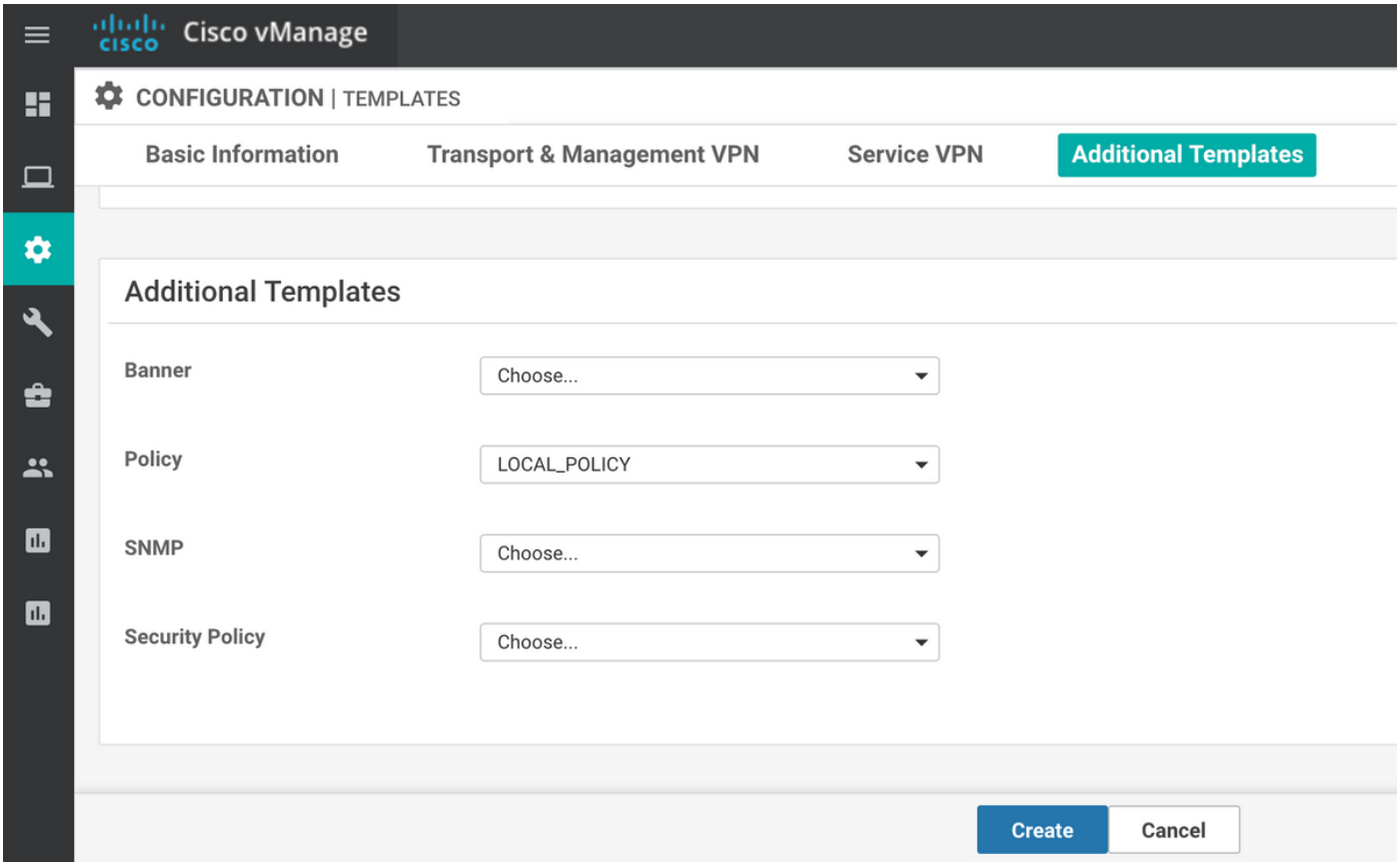
إذا كانت قوالب ميزة الجهاز قيد الاستخدام، فأنت بحاجة إلى إنشاء نهج مترجم وتكوين قائمة التحكم في الوصول على خطوة معالج **تكوين قوائم التحكم في الوصول**:



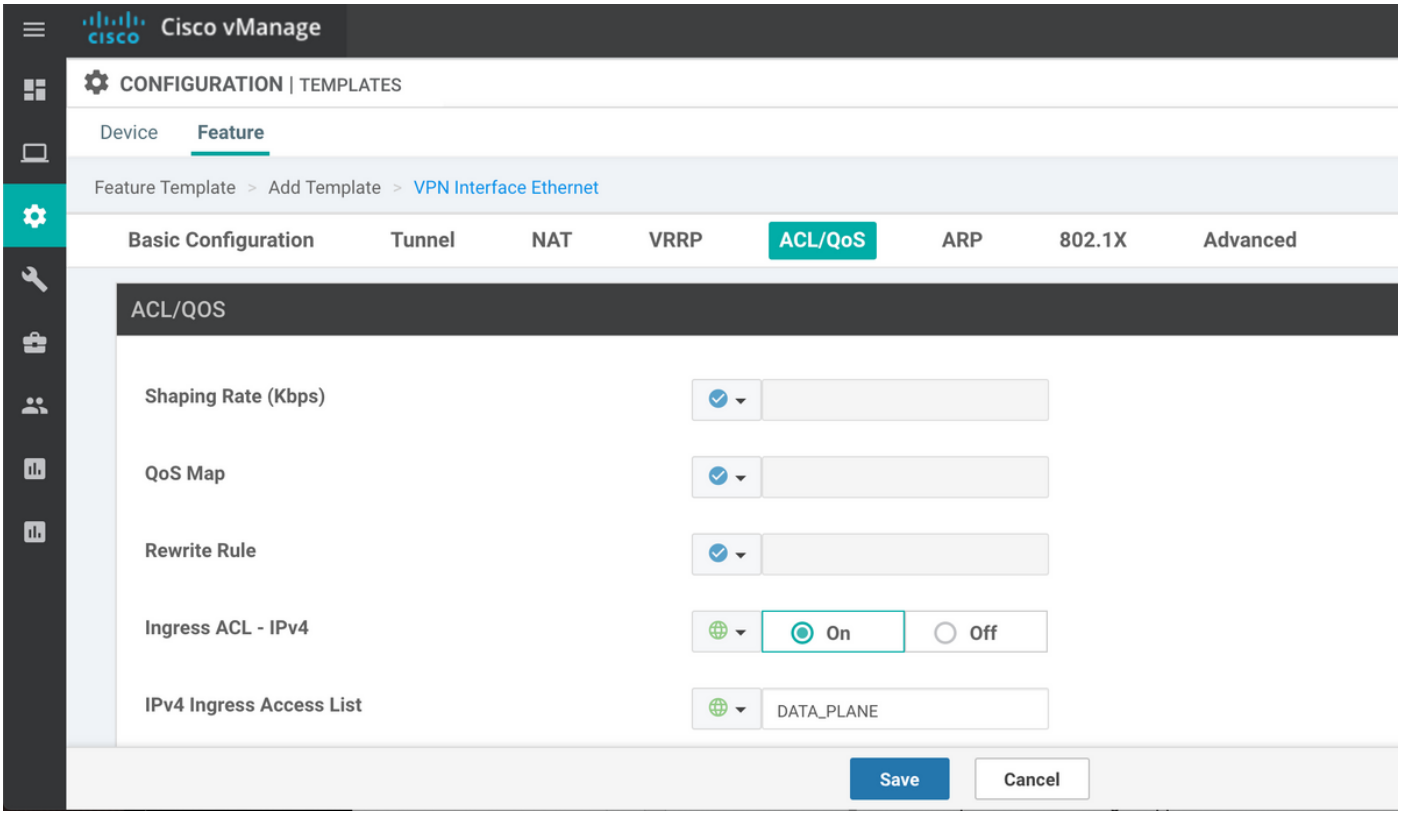
إذا لم يتم تمكين **تسجيل قائمة التحكم في الوصول الضمنية** بعد، فقد يكون من الأفضل تمكينها في الخطوة النهائية قبل النقر على زر **حفظ النهج**:



يجب الإشارة إلى النهج المترجم (المسمى **LOCAL_POLICY** في حالتنا) في قالب الجهاز:



ثم يجب تطبيق قائمة التحكم في الوصول (ACL) (المسماة **DATA_PLANE** في حالتنا) تحت قالب ميزة إيثرنت لواجهة شبكة VPN في إتجاه المدخل (في):



بمجرد تكوين قائمة التحكم في الوصول (ACL) وتطبيقها على الواجهة لتخطي حركة مرور مستوى البيانات، تصبح جلسة عمل BFD أكثر إلى حالة **up** مرة أخرى:

```
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
```

اعتبارات أخرى

يرجى ملاحظة أن الحل البديل مع قائمة التحكم في الوصول (ACL) وه أكثر عملية من إعادة توجيه منفذ NAT لأنك قد تقوم أيضا بالمطابقة استنادا إلى عناوين المصدر للموقع البعيد للحصول على مزيد من الأمان وللحماية من هجمات DDoS إلى جهازك، على سبيل المثال:

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

كما يرجى ملاحظة أنه بالنسبة لأي حركة مرور واردة أخرى (غير محددة مع **الخدمات المسموح بها**) ACL الصريح **20** مثل هذا المثال، لن يحدث هذا أي تأثير مقارنة بحركة مرور مستوى البيانات:

```
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
   !
  !
```

والا تزال بحاجة إلى قاعدة إستثناء NAT Port-forward **حتى** يعمل **iPerf**:

```
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
   !
  !
 !
!
```

القرار

هذا سلوك متوقع على موجهات vEdge ناشئ عن تفاصيل تصميم برنامج NAT والا يمكن تجنبه.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).