حالة حماية مسار الأنفاق عند الاتصال بالإنترنت

المحتويات

المقدمة

يوضح هذا المستند كيفية تعقب الحالة الصحيحة لأنفاق النقل في VPN 0. في الإصدارات 17.2.2 والإصدارات الأحدث، يتم إستخدام واجهات النقل التي تم تمكين ترجمة عنوان الشبكة (NAT) لها للخروج من الإنترنت المحلي. يمكن تعقب حالة اتصال الإنترنت بتعليمات من وظائف. إذا أصبح الإنترنت غير متاح، تتم إعادة توجيه حركة المرور تلقائيا إلى النفق غير NATed على واجهة النقل.

معلومات أساسية

من أجل تزويد المستخدمين في موقع محلي بإمكانية وصول مباشرة وآمنة إلى موارد الإنترنت، مثل مواقع الويب، يمكن تكوين الموجه vEdge ليعمل كجهاز nat، الذي يقوم بتنفيذ كل من ترجمة العنوان والمنفذ (NAPT). عندما يمكن أن تسمح حركة مرور nat، وهي حركة مرور مباشرة إلى الإنترنت بدلا من أن يكون حولت إلى مكان خارج من vEdge مسجاج تخديد أن يمر مباشرة إلى الإنترنت. إذا كنت تستخدم NAT بهذه الطريقة على موجه vEdge، فيمكنك القضاء على "التحكم في" حركة المرور والسماح للطرق الفعالة، التي لها مسافات أقصر، بين المستخدمين في الموقع المحلي والتطبيقات المستندة إلى الشبكة التي يستخدمونها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

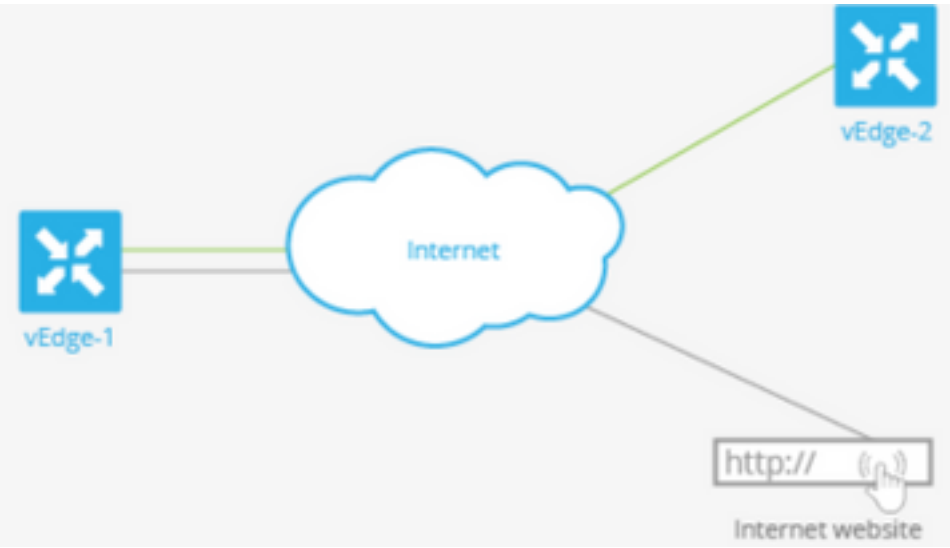
ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة

يعمل الموجه vEdge1 هنا كجهاز nat. يقوم موجه vEdge بتقسيم حركة المرور الخاصة به إلى دفعتين، والتي يمكنك اعتبارها نفقين منفصلين. يبقى تدفق حركة مرور واحد، كما هو موضح بالأخضر، داخل الشبكة التغشية ويتنقل بين الموجهين بالطريقة المعتادة، على أنفاق IPsec الآمنة التي تشكل الشبكة التغشية. يتم إعادة توجيه تدفق حركة المرور الثاني، كما هو موضح بالرمادي، من خلال جهاز NAT الخاص بالموجه vEdge ثم خارج الشبكة الفرعية إلى شبكة عامة.



توضح هذه الصورة كيفية تقسيم وظيفة NAT على موجه VEdge حركة المرور إلى دفعتين (أو نفقين) حتى يظل بعضها داخل الشبكة الفرعية ويذهب بعضها مباشرة إلى الإنترنت أو الشبكات العامة الأخرى.

هنا، يحتوي موجه vEdge على واجهتين:

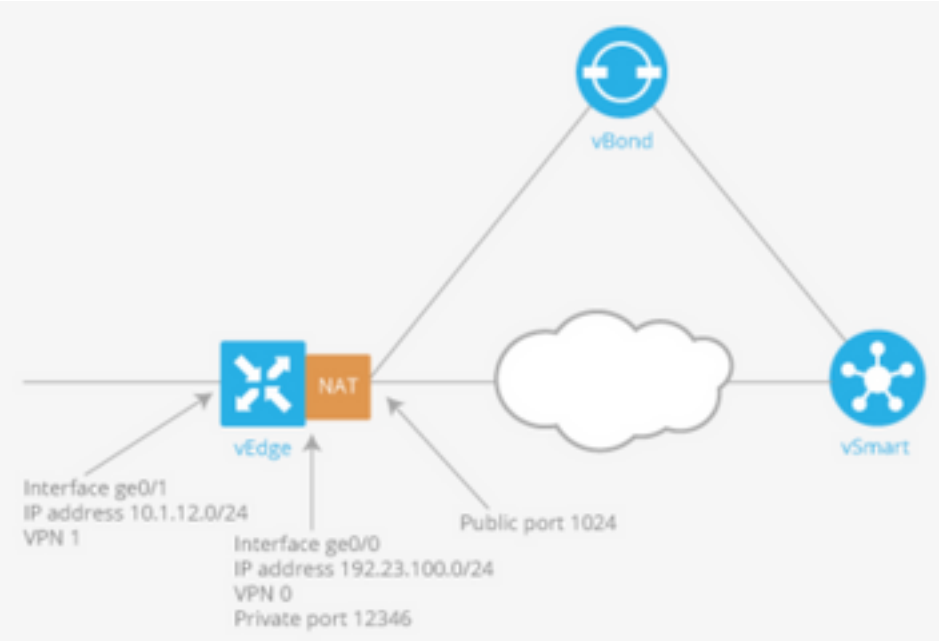
- يواجه قارن ge0/1 الموقع المحلي وهو في VPN 1. عنوان IP الخاص به هو 10.1.12.0/24.
- تواجه الواجهة ge0/0 سحابة النقل وتكون في VPN 0 (نقل VPN). عنوان IP الخاص به هو 192.23.100.0/24، وهو يستخدم رقم منفذ OMP الافتراضي، 12346، لأنفاق الشبكة المتداخلة.

in order to شكلت ال vEdge مسحاج تخديد أن يعمل كجهاز nat لذلك بعض حركة مرور من المسحاج تخديد يستطيع ذهبت مباشرة إلى شبكة عام، أنت تقوم ثلاثة أشياء:

- مكنت nat في النقل VPN (VPN 0) على ال wan-transport-interface، أي هنا ge0/0. تمر جميع حركات المرور التي تخرج من موجه VEdge، وتذهب إما إلى مواقع شبكات فرعية أخرى أو إلى شبكة عامة، عبر هذه الواجهة.
- لتوجيه حركة مرور البيانات من شبكات VPN الأخرى إلى الخروج من موجه VEdge مباشرة إلى شبكة عامة، قم بتمكين NAT في شبكات VPN هذه وأ تأكد من أن شبكات VPN هذه

لديها مسار إلى شبكة VPN 0.

عندما NAT مكنت، كل حركة مرور أن يمر عبر VPN 0 يكون NATed. وهذا يتضمن كل من حركة مرور التحكم، بما في ذلك حركة المرور المطلوبة لإنشاء وصيانة أنفاق مستوى التحكم في DTLS بين موجه vEdge ووحدة التحكم vSmart وبين الموجه ومنفذ vBond Orchestrator.



تعقب حالة الواجهة

تعقب حالة الواجهة مفيد عندما تقوم بتمكين NAT على واجهة نقل في VPN 0 للسماح بحركة مرور البيانات من الموجه إلى المخرج مباشرة إلى الإنترنت بدلا من الاضطرار إلى الانتقال أولا إلى موجه في مركز بيانات. في هذه الحالة، يؤدي تمكين NAT على واجهة النقل إلى تقسيم وحدة التحكم في الشبكة المحلية (TLOC) بين الموجه المحلي ومركز البيانات إلى قسمين، حيث يذهب أحدهما إلى الموجه البعيد ويذهب الآخر إلى الإنترنت.

عند تمكين تعقب نفق النقل، يفحص البرنامج المسار بشكل دوري إلى الإنترنت لتحديد ما إذا كان قيد التشغيل. إذا اكتشف البرنامج أن هذا المسار معطل، فإنه يسحب المسار إلى وجهة الإنترنت، ثم يتم توجيه حركة المرور الموجهة إلى الإنترنت من خلال موجه مركز البيانات. عندما يكتشف البرنامج أن المسار إلى الإنترنت يعمل مرة أخرى، يتم إعادة تثبيت المسار إلى الإنترنت.

التكوينات

1. تكوين **متتبع** ضمن كتلة **النظام**.

اسم نقطة النهاية-dns-name<*dns-name*> وهو اسم DNS لنقطة النهاية لواجهة النفق. هذا هو الوجهة على الإنترنت التي يرسل الموجه إليها المسابير لتحديد حالة واجهة النقل.

```
system
 tracker tracker
  endpoint-dns-name google.com
 !
!
```

2. شكلت **nat** و**tracker** على النقل قارن.

```
vpn 0
 interface ge0/0
  ip address 192.0.2.70/24
  nat
  !
 tracker tracker
  tunnel-interface
!
!
```

3. توجيه حركة المرور إلى الشبكات الموجودة محليا من خلال الشبكة الخاصة الظاهرية (VPN) رقم 0.

```
vpn 1
 ip route 0.0.0.0/0 vpn 0
!
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. التحقق من المسار الافتراضي هو في VPN 0.

```
vEdge# show ip route vpn 0
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive

                                          PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP
VPN    PREFIX              PROTOCOL       SUB TYPE  IF NAME     ADDR             VPN      TLOC
IP          COLOR            ENCAP  STATUS
-------------------------------------------------------------------------------------------------
-----------------------------------------------
0      0.0.0.0/0           static         -         ge0/0       192.0.2.1       -        -
            -                 -      F,S
0      192.0.2.255/32      connected      -         system      -                -        -
            -                 -      F,S
0      192.0.2.70/24       connected      -         ge0/0       -                -        -
            -                 -      F,S
```

2. يجب أن تكون حالة المتعقب 'up' في show interface vpn 0.

```
vEdge# show interface ge0/0

                                     IF      IF      IF
                        TCP
                AF                   ADMIN   OPER    TRACKER  ENCAP
          SPEED          MSS                 RX        TX
VPN  INTERFACE  TYPE  IP ADDRESS      STATUS  STATUS  STATUS   TYPE   PORT TYPE  MTU   HWADDR
          MBPS   DUPLEX  ADJUST  UPTIME       PACKETS   PACKETS
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------
```

```
0    ge0/0      ipv4  192.0.2.70/24  Up      Up      Up       null   transport  1500
12:b7:c4:d5:0c:50  1000   full    1420    19:17:56:35  21198589  24842078
```

3. ابحث عن إدخال مسار "nat" في RIB.

```
vEdge# show ip routes nat
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive

                                          PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP

VPN    PREFIX              PROTOCOL         SUB TYPE  IF NAME     ADDR             VPN      TLOC
IP          COLOR            ENCAP  STATUS
-----------------------------------------------------------------------------------------------
-----------------------------------------
1      0.0.0.0/0           nat              -         ge0/0       -                0        -
            -                  -      F,S
```

4. تحقق من أن المسار الافتراضي من جانب الخدمة يشير إلى واجهة النقل مع NAT على.

```
vEdge# show ip route vpn 1 0.0.0.0
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive

                                       PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP

VPN    PREFIX              PROTOCOL    SUB TYPE  IF NAME     ADDR             VPN      TLOC IP
      COLOR            ENCAP  STATUS
-----------------------------------------------------------------------------------------------
------------------------------
1      0.0.0.0/0           nat         -         ge0/0       -                0        -
      -                -      F,S
```

استكشاف الأخطاء وإصلاحها

استخدم هذه القسم لتأكيد عمل التكوين بشكل صحيح.

1. تأكد من أن endpoint-dns-name وأ endpoint-ip شيء على الإنترنت يمكنه الاستجابة للطلبات HTTP. تحقق أيضا من أن عنوان IP لنقطة النهاية ليس هو نفس واجهة النقل. في الحالة، سيظهر "حالة المتعقب" على أنه "أسفل".

```
vEdge# show interface ge0/0

                                    IF      IF      IF
                        TCP
             AF                     ADMIN   OPER    TRACKER  ENCAP
        SPEED          MSS                 RX        TX
```

```
VPN  INTERFACE  TYPE  IP ADDRESS      STATUS  STATUS  STATUS   TYPE   PORT TYPE  MTU   HWADDR
          MBPS   DUPLEX  ADJUST  UPTIME       PACKETS   PACKETS
-------------------------------------------------------------------------------------------
-------------------------------------------------------------
0    ge0/0      ipv4  192.0.2.70/24  Up      Up      Down     null   transport  1500
12:b7:c4:d5:0c:50  1000   full    1420    19:18:24:12  21219358  24866312
```

2. هنا مثال يمكن إستخدامه للتحقق من خروج الحزم إلى الإنترنت. على سبيل المثال، 8.8.8.8 وه Google DNS. يتم توفير الحزم من VPN 1.

```
vEdge# ping vpn 1 8.8.8.8
Ping in VPN 1
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=0.473 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=0.617 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=0.475 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=0.505 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=51 time=0.477 ms
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.473/0.509/0.617/0.058 ms
```

دقق ال nat ترجمة مرشح. سترى أنه تم إنشاء عامل تصفية NAT لبروتوكول رسائل التحكم في الإنترنت (ICMP).

```
vEdge# show ip nat filter

                            PRIVATE                       PRIVATE  PRIVATE  PUBLIC
        PUBLIC  PUBLIC

NAT  NAT                    SOURCE        PRIVATE DEST    SOURCE   DEST     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    ge0/0   1    icmp      192.0.0.70  8.8.8.8         13067    13067    192.0.2.70  8.8.8.8
      13067   13067   established  0:00:00:02  5         510       5        490      -
```

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).