连接到Internet时跟踪隧道运行状况

目录

简介

本文档介绍如何在VPN 0中跟踪传输隧道的运行状况。在17.2.2版及更高版本中，启用网络地址转换(NAT)的传输接口用于本地互联网退出。借助这些工具，您可以跟踪互联网连接的状态。如果互联网变得不可用，流量将自动重定向到传输接口上的非NAT隧道。

背景信息

为了为本地站点的用户提供对互联网资源（如网站）的直接、安全访问，您可以将vEdge路由器配置为NAT设备，执行地址和端口转换(NAPT)。 启用NAT时，它允许从vEdge路由器流出的流量直接传输到互联网，而不是回传到为互联网访问提供NAT服务的代管机构。如果在vEdge路由器上以这种方式使用NAT，则可以消除流量“串流”，并允许在本地站点的用户与他们使用的基于网络的应用程序之间建立距离较短的高效路由。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

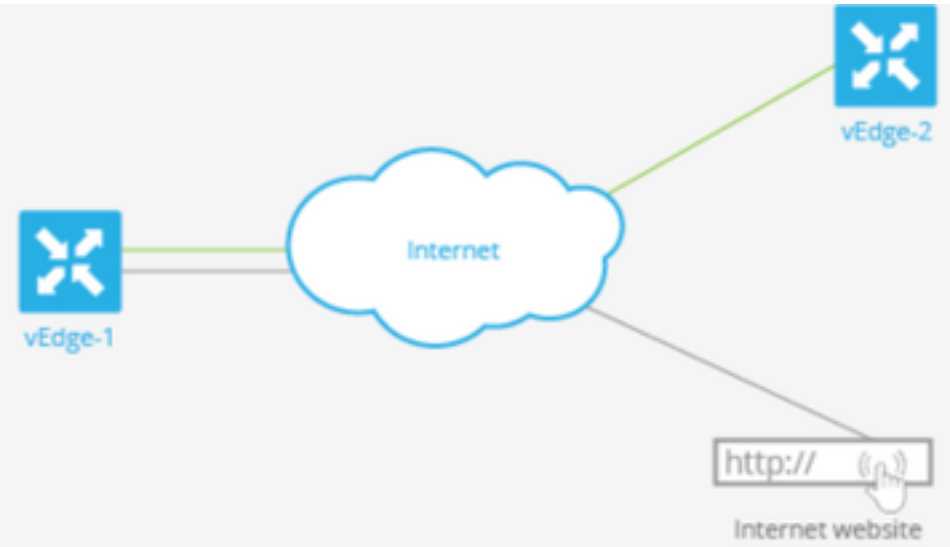
本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图

此处的vEdge1路由器用作NAT设备。vEdge路由器将其流量分成两个流，您可以将其视为两个独立的隧道。一个流量（以绿色显示）保留在重叠网络中，并以通常方式在构成重叠网络的安全IPsec隧道上在两台路由器之间传输。第二个流量流（以灰色显示）通过vEdge路由器的NAT设备重定向，然后从重叠网络转出到公共网络。



此图解释了vEdge路由器上的NAT功能如何将流量拆分为两个流（或两个隧道），以使其中一些流量保留在重叠网络中，而一些流量直接转到互联网或其他公共网络。

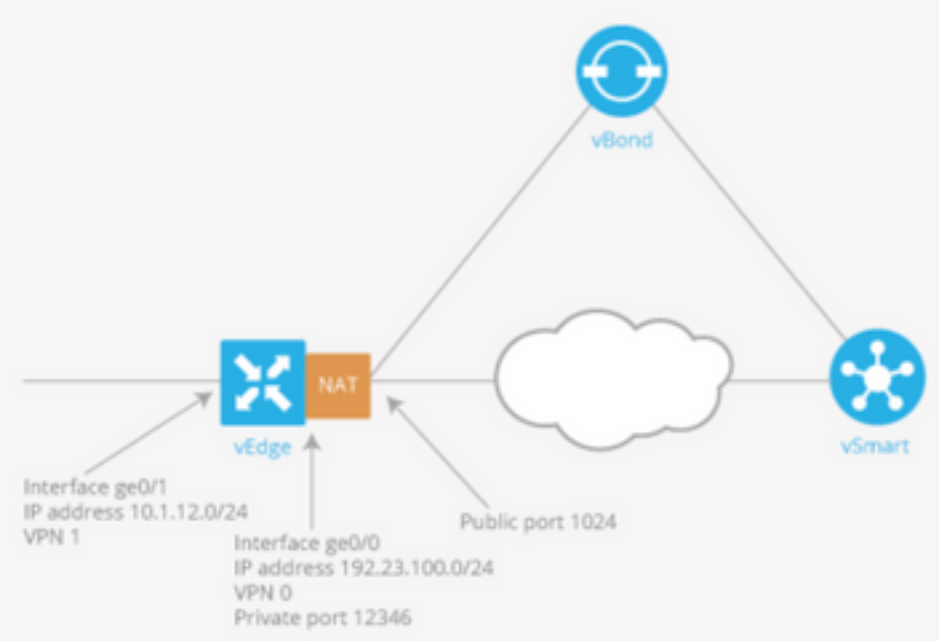
此处，vEdge路由器有两个接口：

- 接口ge0/1面向本地站点并位于VPN 1中。其IP地址为10.1.12.0/24。
- 接口ge0/0面向传输云，并位于VPN 0（传输VPN）中。 其IP地址为192.23.100.0/24，它使用默认OMP端口号12346作为重叠网络隧道。

为了将vEdge路由器配置为NAT设备，以便来自路由器的某些流量可以直接到达公共网络，您需要执行三项操作：

- 在面向广域网传输的接口（这里为ge0/0）上的传输VPN(VPN 0)中启用NAT。从vEdge路由器流出的所有流量（通往其他重叠网络站点或公共网络）都通过此接口。
- 要将来自其他VPN的数据流量直接从vEdge路由器退出到公共网络，请在这些VPN中启用NAT或确保这些VPN具有到VPN 0的路由。

启用NAT后，通过VPN 0的所有流量都会进行NAT。这包括从VPN 1发往公共网络的数据流量和所有控制流量，包括在vEdge路由器和vSmart控制器之间以及路由器和vBond协调器之间建立和维护DTLS控制平面隧道所需的流量。



跟踪接口状态

在VPN 0中的传输接口上启用NAT，以允许来自路由器的数据流量直接流出互联网，而不必首先前往数据中心的路由器时，跟踪接口状态非常有用。在这种情况下，在传输接口上启用NAT会将本地路由器和数据中心之间的TLOC拆分为两个，一个将发往远程路由器，另一个将发往互联网。

启用传输隧道跟踪时，软件会定期探测到互联网的路径以确定它是否处于工作状态。如果软件检测到此路径已关闭，它会撤回通往互联网目的地的路由，然后发往互联网的流量会通过数据中心路由器路由。当软件检测到通往互联网的路径再次正常运行时，将重新安装通往互联网的路由。

配置

1.在系统**块下配置跟踪**器。

endpoint-dns-name ***<dns-name>*是隧道接口终端的DNS名称。**这是Internet上的目的地，路由器将探测功能发送到该目的地，以确定传输接口的状态。

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

2. 在传输接**口上配置nat和**tracker。

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

3. 通过VPN 0将流量定向到本地现有流量。

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

验证

使用本部分可确认配置能否正常运行。

1.检查默认路由在VPN 0中。

```
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.在show interface VPN 0中，跟踪器状态应为“UP”。

```
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.在RIB中查找“NAT”路由条目。

```
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.交叉检查从服务端到NAT打开的传输接口的默认路由。

```
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
```

故障排除

使用本部分可确认配置能否正常运行。

1.确保endpoint-ip或endpoint-dns-name是Internet上可以响应HTTP请求的内容。另请验证终端IP地址与传输接口不同。在本例中，“跟踪器状态”将显示为“关闭”。

```
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.以下示例可用于验证数据包是否传出到Internet。例如，8.8.8.8是Google DNS。来自VPN 1的数据包来自。

```
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
```

检验NAT转换过滤器。您将看到NAT过滤器是为Internet控制消息协议(ICMP)构建的。

```
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      -
```