인터넷에 연결된 경우 터널 상태 추적

목차

소개

이 문서에서는 VPN 0에서 전송 터널의 상태를 추적하는 방법에 대해 설명합니다. 릴리스 17.2.2 이상에서는 NAT(Network Address Translation) 지원 전송 인터페이스가 로컬 인터넷 종료에 사용됩니다.이러한 도움말의 도움을 받아 인터넷 연결 상태를 추적할 수 있습니다.인터넷을 사용할 수 없게 되면 트래픽은 전송 인터페이스에서 비 NATed 터널로 자동으로 리디렉션됩니다.

배경 정보

로컬 사이트의 사용자에게 웹 사이트와 같은 인터넷 리소스에 대한 직접 보안 액세스를 제공하기 위해 vEdge 라우터가 NAT 디바이스로 작동하도록 구성하여 NAPT(Address and Port Translation)를 모두 수행합니다. NAT를 활성화하면 인터넷 액세스를 위한 NAT 서비스를 제공하는 공동 위치 시설로 백홀되는 대신 vEdge 라우터에서 나가는 트래픽이 인터넷으로 직접 전달되도록 허용합니다.vEdge 라우터에서 이러한 방식으로 NAT를 사용하는 경우 트래픽 "제어"를 제거하고 로컬 사이트의 사용자와 사용하는 네트워크 기반 애플리케이션 간에 더 짧은 거리를 가진 효율적인 경로를 허용할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

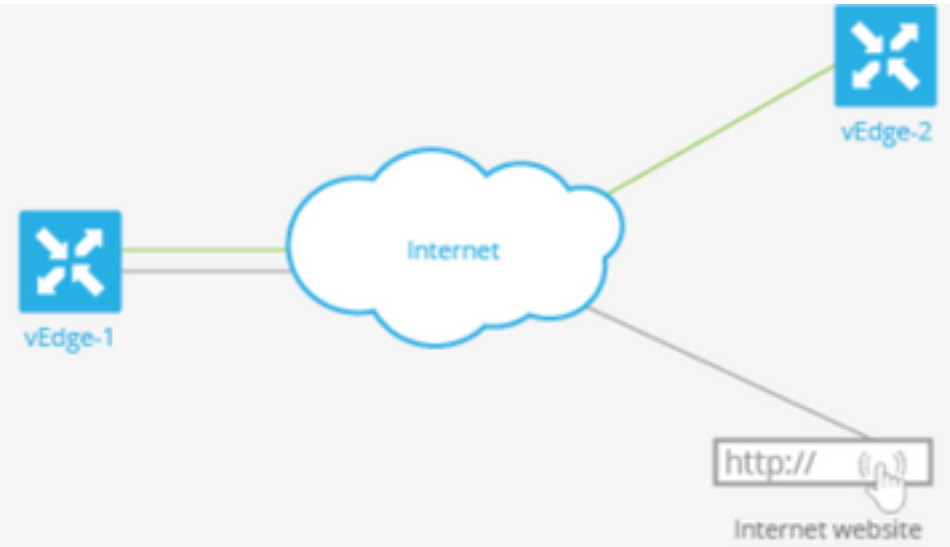
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의

잠재적인 영향을 이해해야 합니다.

구성

네트워크 다이어그램

여기서 vEdge1 라우터는 NAT 장치 역할을 합니다.vEdge 라우터는 트래픽을 두 개의 플로우로 분할하며, 이를 두 개의 개별 터널로 생각할 수 있습니다.녹색으로 표시된 하나의 트래픽 흐름은 오버레이 네트워크 내에 남아 있으며, 오버레이 네트워크를 형성하는 보안 IPsec 터널에서 일반적인 방식으로 두 라우터 간에 이동합니다.회색으로 표시된 두 번째 트래픽 스트림은 vEdge 라우터의 NAT 디바이스를 통해 리디렉션된 다음 오버레이 네트워크에서 공용 네트워크로 리디렉션됩니다.



이 이미지는 vEdge 라우터의 NAT 기능이 트래픽을 두 개의 플로우(또는 두 개의 터널)로 분할하는 방식을 설명하며, 이 중 일부는 오버레이 네트워크 내에 남아 있고 일부는 인터넷 또는 기타 공용 네트워크로 직접 이동됩니다.

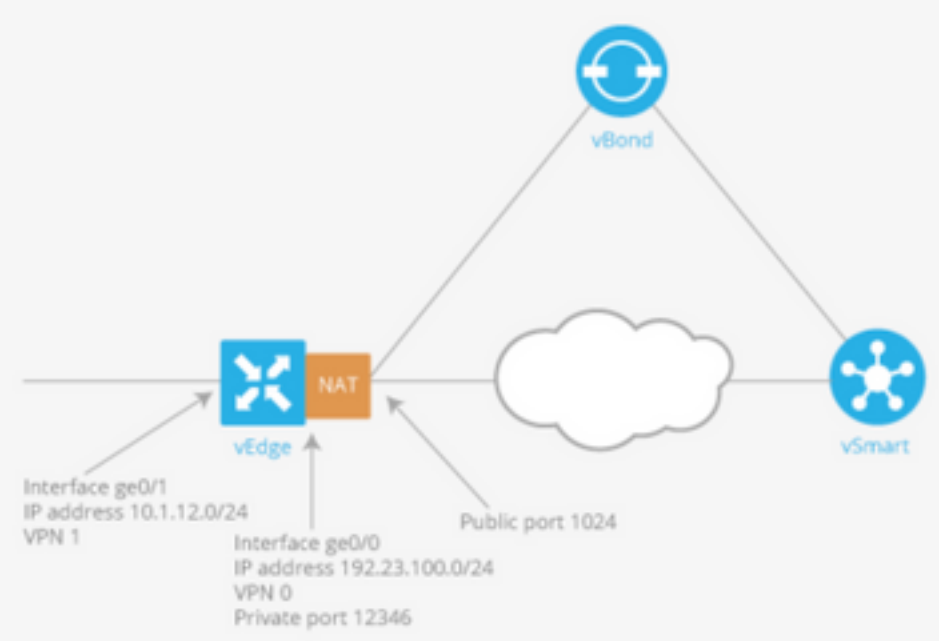
vEdge 라우터에는 두 개의 인터페이스가 있습니다.

- 인터페이스 ge0/1은 로컬 사이트를 향하고 VPN 1에 있습니다. IP 주소는 10.1.12.0/24입니다.
- 인터페이스 ge0/0은 전송 클라우드를 향하고 VPN 0(전송 VPN)에 있습니다. IP 주소는 192.23.100.0/24이며 오버레이 네트워크 터널에 기본 OMP 포트 번호 12346을 사용합니다.

라우터의 일부 트래픽이 공용 네트워크로 직접 이동할 수 있도록 vEdge 라우터가 NAT 디바이스 역할을 하도록 구성하려면 다음 세 가지 작업을 수행합니다.

- WAN 전송 연결 인터페이스의 VPN(VPN 0)에서 NAT를 활성화합니다(여기서 ge0/0). vEdge 라우터에서 나가는 모든 트래픽은 다른 오버레이 네트워크 사이트 또는 공용 네트워크로 이동하여 이 인터페이스를 통과합니다.
- 다른 VPN의 데이터 트래픽이 vEdge 라우터에서 직접 공용 네트워크로 나가도록 하려면 해당 VPN에서 NAT를 활성화하거나 해당 VPN에 VPN 0에 대한 경로가 있는지 확인합니다.

NAT가 활성화된 경우 VPN 0을 통해 전달되는 모든 트래픽은 NATed입니다.여기에는 공용 네트워크를 대상으로 하는 VPN 1의 데이터 트래픽과 모든 제어 트래픽이 모두 포함됩니다. 여기에는 vEdge 라우터와 vSmart 컨트롤러 간, 라우터와 vBond 오케스트레이터 간의 DTLS 제어 평면 터널을 설정하고 유지하는 데 필요한 트래픽도 포함됩니다.



인터페이스 상태 추적

인터페이스 상태를 추적하는 것은 VPN 0의 전송 인터페이스에서 NAT를 활성화하여 데이터 센터의 라우터로 먼저 이동할 필요 없이 라우터에서 데이터 트래픽이 인터넷으로 직접 나가도록 할 때 유용합니다.이 경우 전송 인터페이스에서 NAT를 활성화하면 로컬 라우터와 데이터 센터 간에 TLOC가 두 개로 분할되며, 하나는 원격 라우터로, 다른 하나는 인터넷으로 이동합니다.

전송 터널 추적을 활성화하면 소프트웨어가 인터넷 경로를 주기적으로 프로브하여 작동 여부를 확인합니다.소프트웨어가 이 경로가 다운된 것을 감지하면 인터넷 목적지로 경로를 철회하고 인터넷으로 향하는 트래픽은 데이터 센터 라우터를 통해 라우팅됩니다.소프트웨어가 인터넷 경로가 다시 작동하고 있음을 감지하면 인터넷 경로가 다시 설치됩니다.

구성

1. **시스템** 블록 아래에 **추적기**를 구성합니다.

endpoint-dns-name<*dns-name*>은 터널 인터페이스의 엔드포인트의 DNS 이름입니다.라우터가 전송 인터페이스의 상태를 확인하기 위해 프로브를 전송하는 인터넷의 목적지입니다.

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

2 . 전송 인터페이스에서 nat 및 추적기를 구성합니다.

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

3 . VPN 0을 통해 로컬로 트래픽을 전송합니다.

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

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1. 기본 확인 경로는 VPN 0에 있습니다.

```
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. show interface VPN 0에서 추적기 상태가 'UP'이어야 합니다.

```
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. RIB에서 'NAT' 경로 항목을 찾습니다.

```
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. 서비스 측의 기본 경로가 NAT가 설정된 전송 인터페이스를 가리키는지 교차 확인합니다.

```
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
```

문제 해결

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1. 엔드포인트 IP 또는 엔드포인트-dns-name이 HTTP 요청에 응답할 수 있는 인터넷에 있는지 확인합니다. 또한 엔드포인트 IP 주소가 전송 인터페이스와 동일하지 않은지 확인합니다.이 경우 "Tracker Status(추적기 상태)"가 "Down(다운)"으로 표시됩니다.

```
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. 다음은 패킷이 인터넷으로 전송되는지 확인하는 데 사용할 수 있는 예입니다.예를 들어 8.8.8.8은 Google DNS입니다.VPN 1의 패킷은 소싱됩니다.

```
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
```

NAT 변환 필터를 확인합니다.NAT 필터가 ICMP(Internet Control Message Protocol)용으로 구축되어 있음을 확인할 수 있습니다.

```
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      -
```