Status van Tracker-tunnels wanneer aangesloten op internet

Inhoud

Inleiding

In dit document wordt beschreven hoe de gezondheidsstatus van transporttunnels in VPN 9 wordt getraceerd. In releases 17.2.2 en later worden de door NAT (Network Address Translation) enabled-enabled-transportinterfaces gebruikt voor lokale internetexit. Met behulp van deze netwerken kunt u de status van de internetverbinding bepalen. Als het internet niet beschikbaar wordt, wordt het verkeer automatisch omgeleid naar de niet-NATed-tunnel op de transportinterface.

Achtergrondinformatie

Om gebruikers op een lokale website directe, veilige toegang tot de middelen van Internet, zoals websites te geven, kunt u de vEdge-router configureren om als NAT-apparaat te functioneren, dat zowel adres als poortvertaling (NAPT) uitvoert. Wanneer u NAT toelaat, staat het verkeer toe dat van een vEdge router vertrekt om direct aan het Internet over te gaan in plaats van terugbepaald te worden aan een co-location faciliteit die NAT de diensten voor de toegang tot internet verstrekt. Als u NAT op deze manier op een vEdge-router gebruikt, kunt u "tromboning" van het verkeer elimineren en efficiënte routes mogelijk maken, die kortere afstanden hebben, tussen gebruikers op de lokale locatie en de op het netwerk gebaseerde toepassingen die ze gebruiken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

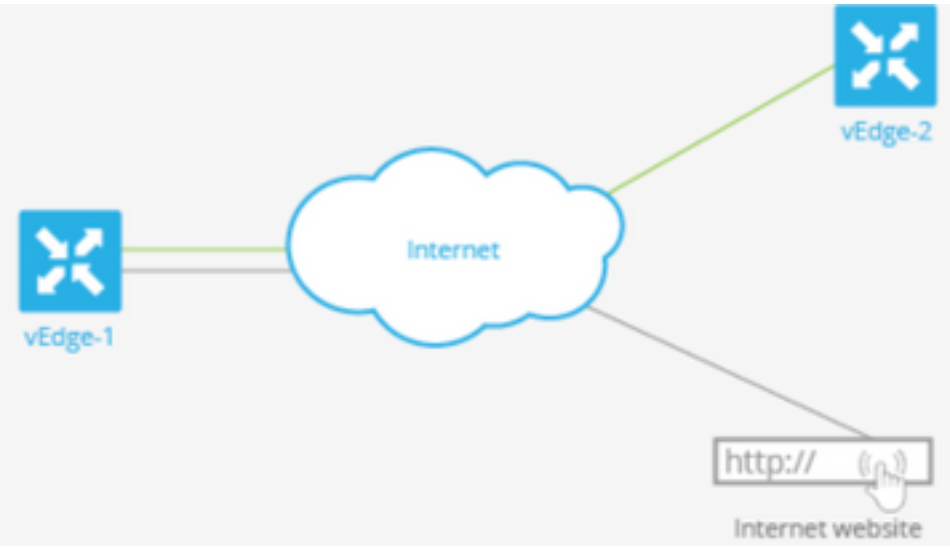
Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Netwerkdiagram

vEdge1-router werkt hier als een NAT-apparaat. De vEdge-router scheidt zijn verkeer in twee stromen, die u kunt beschouwen als twee aparte tunnels. Eén verkeersstroom, groen weergegeven, blijft binnen het overlay netwerk en reist op de gebruikelijke manier tussen de twee routers en de beveiligde IPsec-tunnels die het overlay netwerk vormen. De tweede verkeersstroom, die in grijswaarden wordt getoond, wordt door het NAT-apparaat van de vEdge-router en vervolgens uit het overlay-netwerk naar een openbaar netwerk geleid.



Dit beeld legt uit hoe de NAT-functionaliteit op de vEdge-router verkeer in twee stromen (of twee tunnels) scheidt, zodat een deel ervan binnen het overlay-netwerk blijft en een deel rechtstreeks naar internet of andere openbare netwerken gaat.

Hier heeft de vEdge-router twee interfaces:

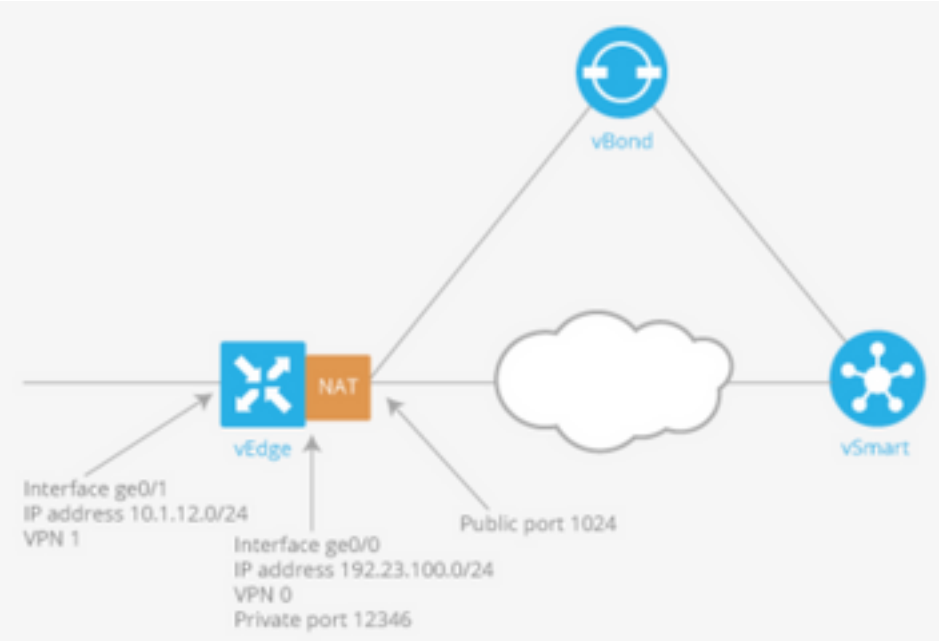
- Interface ge0/1 staat voor de lokale site en is in VPN 1. Het IP-adres is 10.1.12.0/24.
- Interface ge0/0 staat voor de transportcloud en is in VPN 0 (het transport VPN). Zijn IP-adres is 192.23.100.0/24 en het gebruikt het standaard OMP-poortnummer 12346 voor overlay netwerktunnels.

Om de vEdge-router te configureren als een NAT-apparaat te fungeren, zodat wat verkeer vanaf de router direct naar een openbaar netwerk kan gaan, doet u drie dingen:

- Schakel NAT in het transport VPN (VPN 0) op de WAN-transport-gerichte interface in (dit is ge0/0). Alle verkeer dat bestaat uit de vEdge-router, die naar andere overlay netwerksites of naar een openbaar netwerk gaat, gaat door deze interface.
- Om gegevensverkeer van andere VPN's te richten om rechtstreeks uit de vEdge-router te

komen naar een openbaar netwerk, NAT in deze VPN's mogelijk te maken of ervoor te zorgen dat die VPN's een route naar VPN 0 hebben.

Als NAT is ingeschakeld, is al het verkeer dat door VPN 0 passeert NATed. Dit omvat zowel het gegevensverkeer van VPN 1 dat bestemd is voor een openbaar netwerk als al het controleverkeer, inclusief het verkeer dat vereist is om DTLS-besturingsplantunnels tussen de vEdge-router en de vSmart-controller op te zetten en te onderhouden, en tussen de router en de vBond-orchestrator.



Interfacestatus

Het overtrekken van de interfacestatus is nuttig wanneer u NAT op een transportinterface in VPN 0 toestaat om gegevensverkeer van de router toe te staan om rechtstreeks naar het internet te verlaten in plaats van eerst naar een router in een datacenter te moeten gaan. In deze situatie splitst het inschakelen van NAT op de transportinterface de TLOC tussen de lokale router en het datacenter in twee delen, waarbij de ene naar de afstandsrouter gaat en de andere naar internet.

Wanneer u het volgen van transporttunnels mogelijk maakt, stelt de software periodiek het pad naar het internet op om te bepalen of het omhoog is. Als de software ontdekt dat dit pad plat is, trekt hij de route naar de internetbestemming in en wordt het verkeer dat naar het internet is bestemd vervolgens door de router van het datacenter verstuurd. Wanneer de software ontdekt dat het pad naar het internet opnieuw functioneert, wordt de route naar het internet opnieuw geïnstalleerd.

Configuraties

1. Het **tracker** configureren onder het **systeemvak**.

Endpoint-dns-name<*dns-name*> is de DNS-naam van het eindpunt van de tunnelinterface. Dit is de bestemming op het internet waarnaar de router sondes verstuurt om de status van de transportinterface te bepalen.

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

```
 !
!
```

2. Configureer de **kern** en **tracker** op de transportinterface.

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

3. Direct verkeer naar bestaand lokaal via VPN 0.

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

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. De standaardroute van de controle is in 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. De Tracker-status moet 'UP' zijn in DIA-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. Zoek de vermelding "NAT" op de route in de 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. Controleer of de standaardroute van de servicekant naar de transportinterface met NAT is ingeschakeld.

```
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
```

Problemen oplossen

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. Zorg ervoor dat de endpointgebeurtenissen of dns-naam op het internet iets is dat op HTTP-verzoeken kan reageren. Controleer ook of het IP-adres van het eindpunt niet hetzelfde is als de transportinterface. In het geval zal "Tracker Status" als "Down" weergeven.

```
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. Hier is een voorbeeld dat kan worden gebruikt om te verifiëren dat pakketten naar internet gaan. 8.8.8.8 is bijvoorbeeld Google DNS. Packets van VPN 1 worden gesourcet.

```
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
```

Controleer de NAT vertaalfilters. U ziet dat het NAT-filter is gebouwd voor Internet Control Message Protocol (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      -
```