Überwachung des Tunnelstatus bei Verbindung mit dem Internet

Inhalt

[Einführung](#)
[Hintergrundinformationen](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Schnittstellenstatus verfolgen](#)
[Konfigurationen](#)
[Überprüfen](#)
[Fehlerbehebung](#)

Einführung

In diesem Dokument wird beschrieben, wie der Status von Transporttunneln in VPN 0 nachverfolgt wird. In den Versionen 17.2.2 und höher werden bei Network Address Translation (NAT) aktivierte Transportschnittstellen für den lokalen Internetanschluss verwendet. Mithilfe dieser können Sie den Status der Internetverbindung nachverfolgen. Wenn das Internet nicht mehr verfügbar ist, wird der Datenverkehr automatisch an den Nicht-NAT-Tunnel auf der Transportschnittstelle umgeleitet.

Hintergrundinformationen

Um Benutzern an einem lokalen Standort direkten, sicheren Zugriff auf Internetressourcen wie Websites zu ermöglichen, können Sie den vEdge-Router so konfigurieren, dass er als NAT-Gerät fungiert, das sowohl die Adressen- als auch die Port-Übersetzung (NAPT) durchführt. Wenn Sie NAT aktivieren, kann der Datenverkehr, der von einem vEdge-Router ausgeht, direkt an das Internet weitergeleitet werden, anstatt an eine Kolokationsstelle zurückgeleitet zu werden, die NAT-Dienste für den Internetzugriff bereitstellt. Wenn Sie auf diesem Weg auf einem vEdge-Router NAT verwenden, können Sie Datenverkehrsengpässe vermeiden und effiziente Routen mit kürzeren Entfernungen zwischen Benutzern am lokalen Standort und den von ihnen verwendeten netzwerkbasierten Anwendungen ermöglichen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

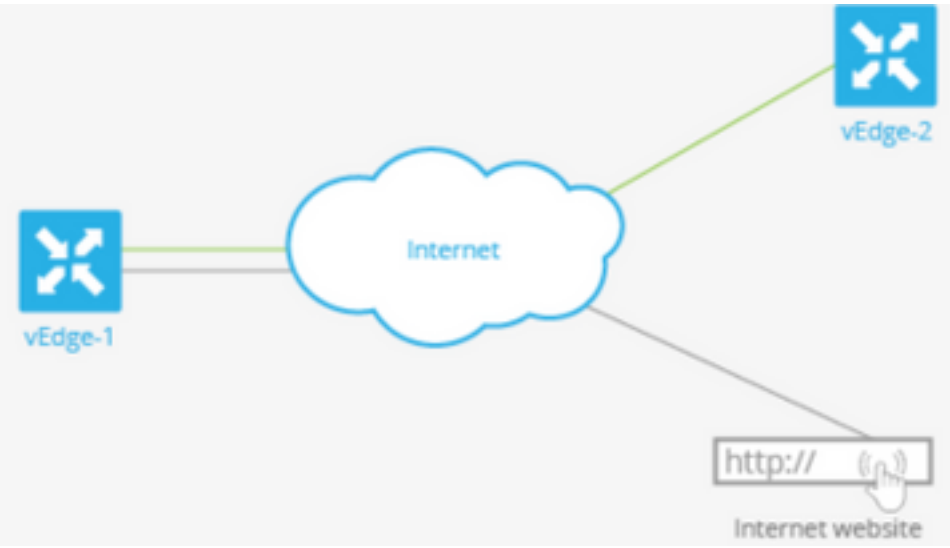
Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm

Der vEdge1-Router fungiert hier als NAT-Gerät. Der vEdge-Router teilt den Datenverkehr in zwei Flüsse auf, die Sie sich als zwei separate Tunnel vorstellen können. Ein grün angezeigter Datenverkehrsfluss verbleibt innerhalb des Overlay-Netzwerks und verläuft wie gewohnt zwischen den beiden Routern in den sicheren IPsec-Tunneln, die das Overlay-Netzwerk bilden. Der zweite Datenverkehrsstrom (grau dargestellt) wird über das NAT-Gerät des vEdge-Routers umgeleitet und anschließend aus dem Overlay-Netzwerk in ein öffentliches Netzwerk geleitet.



In diesem Bild wird erläutert, wie die NAT-Funktion des vEdge-Routers den Datenverkehr in zwei Datenflüsse (oder zwei Tunnel) aufteilt, sodass ein Teil davon im Overlay-Netzwerk verbleibt und ein Teil direkt in das Internet oder andere öffentliche Netzwerke geleitet wird.

Hier hat der vEdge-Router zwei Schnittstellen:

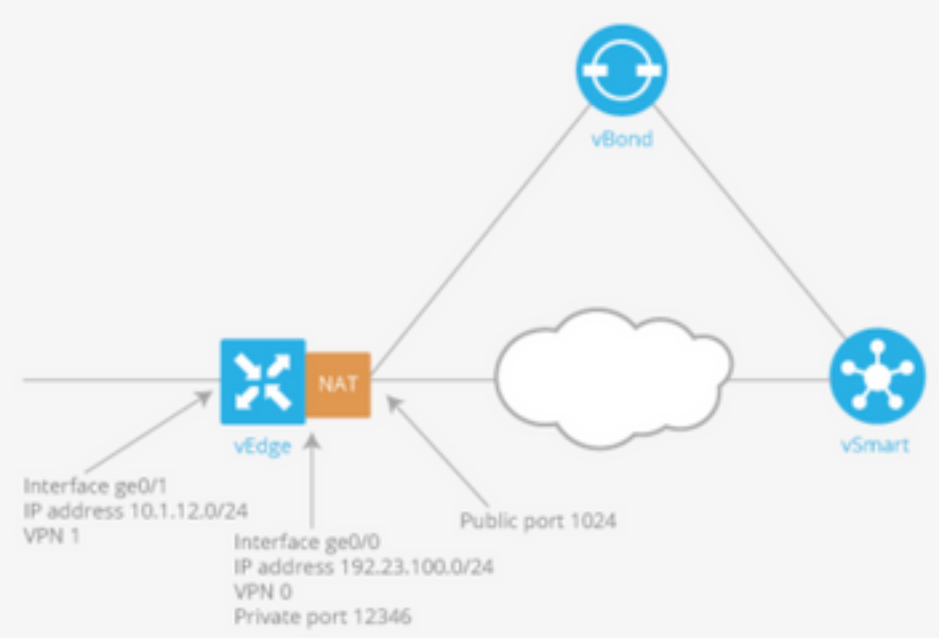
- Die Schnittstelle ge0/1 ist mit dem lokalen Standort verbunden und befindet sich in VPN 1. Die IP-Adresse lautet 10.1.12.0/24.
- Die Schnittstelle ge0/0 weist eine Verbindung zur Transport-Cloud auf und befindet sich in VPN 0 (dem Transport-VPN). Die IP-Adresse lautet 192.23.100.0/24, und für Overlay-Netzwerk-Tunnel wird die Standard-OMP-Portnummer 12346 verwendet.

Um den vEdge-Router so zu konfigurieren, dass er als NAT-Gerät fungiert, sodass ein Teil des Datenverkehrs vom Router direkt an ein öffentliches Netzwerk geleitet werden kann, müssen Sie drei Schritte ausführen:

- Aktivieren Sie NAT im Transport-VPN (VPN 0) an der WAN-Transportschnittstelle, die hier ge0/0 lautet. Der gesamte vom vEdge-Router ausgehende Datenverkehr, der entweder zu anderen Overlay-Netzwerkstandorten oder zu einem öffentlichen Netzwerk geleitet wird,

durchläuft diese Schnittstelle.
- Um Datenverkehr von anderen VPNs direkt vom vEdge-Router an ein öffentliches Netzwerk zu leiten, aktivieren Sie NAT in diesen VPNs, oder stellen Sie sicher, dass diese VPNs eine Route zu VPN 0 haben.

Wenn NAT aktiviert ist, wird der gesamte Datenverkehr, der über VPN 0 geleitet wird, NATed. Dies umfasst sowohl den Datenverkehr von VPN 1, der für ein öffentliches Netzwerk bestimmt ist, als auch den gesamten Kontrollverkehr, einschließlich des Datenverkehrs, der für die Einrichtung und Wartung von Tunneln auf der DTLS-Kontrollebene zwischen dem vEdge-Router und dem vSmart-Controller sowie zwischen dem Router und dem vBond-Orchestrator erforderlich ist.



Schnittstellenstatus verfolgen

Das Nachverfolgen des Schnittstellenstatus ist nützlich, wenn Sie NAT auf einer Transportschnittstelle in VPN 0 aktivieren, damit der Datenverkehr vom Router direkt in das Internet übertragen kann, anstatt zuerst zu einem Router in einem Rechenzentrum wechseln zu müssen. In dieser Situation teilt die Aktivierung von NAT auf der Transportschnittstelle die TLOC-Verbindung zwischen dem lokalen Router und dem Rechenzentrum in zwei Bereiche auf, wobei der eine zum Remote-Router und der andere zum Internet führt.

Wenn Sie die Transporttunnelverfolgung aktivieren, überprüft die Software regelmäßig den Pfad zum Internet, um festzustellen, ob dieser aktiv ist. Wenn die Software erkennt, dass dieser Pfad ausgefallen ist, zieht sie die Route zum Internet-Ziel zurück, und der für das Internet bestimmte Datenverkehr wird dann über den Rechenzentrums-Router geleitet. Wenn die Software erkennt, dass der Pfad zum Internet wieder funktioniert, wird die Route zum Internet neu installiert.

Konfigurationen

1. Konfigurieren Sie **Tracker** unter dem **System**-Block.

endpoint-dns-name<*dns-name*> ist der DNS-Name des Endpunkts der Tunnelschnittstelle. Dies ist das Ziel im Internet, an das der Router Prüfungen sendet, um den Status der Transportschnittstelle zu ermitteln.

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

2. Konfigurieren Sie **nat** und **tracker** auf der Transportschnittstelle.

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

3. Standortbasierter Datenverkehr über VPN 0

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Die Standardroute ist 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. Der Tracker-Status muss in der angezeigten Schnittstelle VPN 0 'UP' sein.

```
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. Suchen Sie in der RIB nach dem Eintrag für die NAT-Route.

```
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. Überprüfen Sie, ob die Standardroute von der Service-Seite auf die Transport-Schnittstelle zeigt, wobei NAT aktiviert ist.

```
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
```

Fehlerbehebung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Stellen Sie sicher, dass der Endpunkt-IP- oder Endpunkt-DNS-Name eine Funktion im Internet ist, die auf HTTP-Anfragen reagieren kann. Überprüfen Sie außerdem, ob die IP-Adresse des Endpunkts nicht mit der Transportschnittstelle identisch ist. In diesem Fall wird "Tracker-Status" als "Down" angezeigt.

```
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. Dieses Beispiel kann verwendet werden, um zu überprüfen, ob Pakete ins Internet gehen. 8.8.8.8 ist beispielsweise Google DNS. Pakete von VPN 1 werden von der Quelle bereitgestellt.

```
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
```

Überprüfen Sie die NAT-Übersetzungsfilter. Sie sehen, dass der NAT-Filter für das Internet Control Message Protocol (ICMP) erstellt wurde.

```
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      -
```