Suivi de l'état de santé des tunnels lorsqu'ils sont connectés à Internet

Contenu

Introduction

Ce document décrit comment suivre l'état de santé des tunnels de transport dans VPN 0. Dans les versions 17.2.2 et ultérieures, les interfaces de transport NAT (Network Address Translation) sont utilisées pour la sortie Internet locale. Vous pouvez suivre l'état de la connexion Internet à l'aide de ceux-ci. Si Internet devient indisponible, le trafic est automatiquement redirigé vers le tunnel non NATed sur l'interface de transport.

Informations générales

Afin de fournir aux utilisateurs d'un site local un accès direct et sécurisé aux ressources Internet, telles que les sites Web, vous pouvez configurer le routeur vEdge pour qu'il fonctionne en tant que périphérique NAT, qui effectue à la fois la traduction d'adresses et de ports (NAPT). Lorsque vous activez la fonction NAT, elle permet au trafic sortant d'un routeur vEdge de passer directement à Internet plutôt que d'être réacheminé vers un site de colocalisation qui fournit des services NAT pour l'accès à Internet. Si vous utilisez NAT de cette manière sur un routeur vEdge, vous pouvez éliminer le trafic tromboning et autoriser des routes efficaces, qui ont des distances plus courtes, entre les utilisateurs du site local et les applications réseau qu'ils utilisent.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

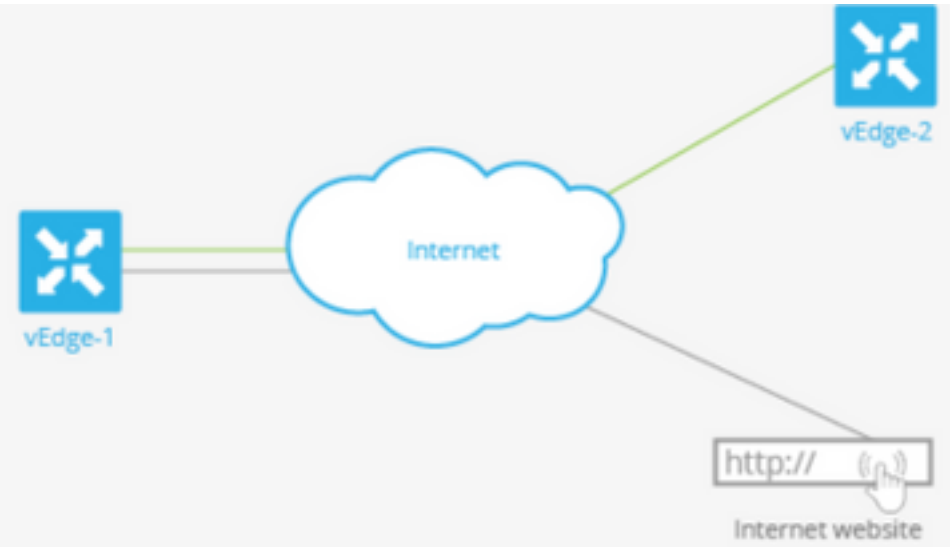
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Diagramme du réseau

Le routeur vEdge1 agit ici en tant que périphérique NAT. Le routeur vEdge divise son trafic en deux flux, que vous pouvez considérer comme deux tunnels distincts. Un flux de trafic, affiché en vert, reste dans le réseau de superposition et circule entre les deux routeurs de la manière habituelle, sur les tunnels IPsec sécurisés qui forment le réseau de superposition. Le deuxième flux de trafic, affiché en gris, est redirigé par le périphérique NAT du routeur vEdge, puis par le réseau de superposition vers un réseau public.



Cette image explique comment la fonctionnalité NAT sur le routeur vEdge divise le trafic en deux flux (ou deux tunnels) de sorte que certains restent dans le réseau de superposition et d'autres se dirigent directement vers Internet ou d'autres réseaux publics.

Ici, le routeur vEdge comporte deux interfaces :

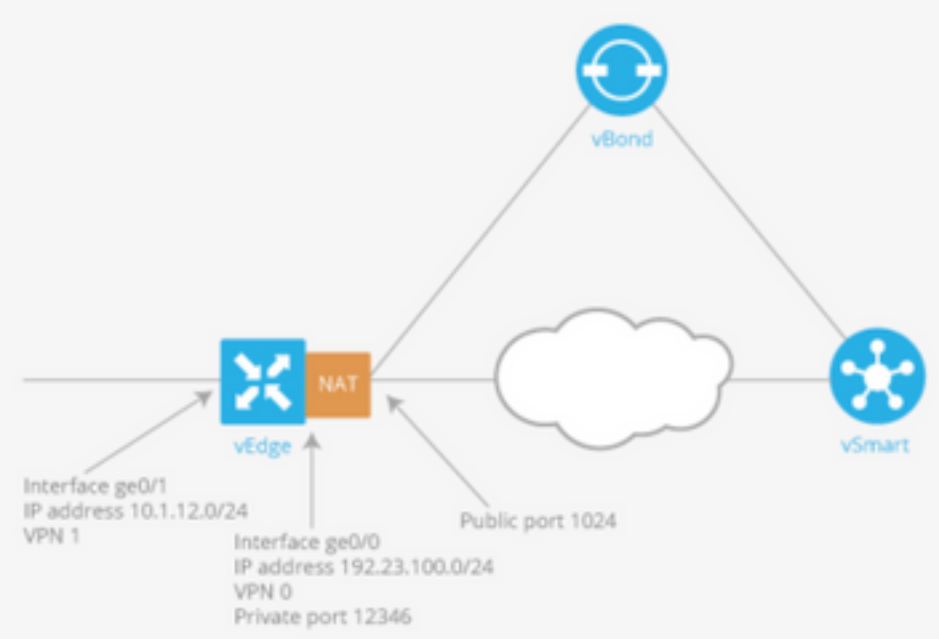
- L'interface ge0/1 fait face au site local et se trouve dans VPN 1. Son adresse IP est 10.1.12.0/24.
- L'interface ge0/0 fait face au cloud de transport et se trouve dans le VPN 0 (le VPN de transport). Son adresse IP est 192.23.100.0/24 et utilise le numéro de port OMP par défaut, 12346, pour les tunnels réseau de superposition.

Afin de configurer le routeur vEdge pour qu'il agisse en tant que périphérique NAT afin qu'un certain trafic du routeur puisse accéder directement à un réseau public, vous devez effectuer trois opérations :

- Activez NAT dans le VPN de transport (VPN 0) sur l'interface orientée transport WAN, qui est ici ge0/0. Tout le trafic sortant du routeur vEdge, qui se rend soit à d'autres sites de réseau de superposition, soit à un réseau public, passe par cette interface.

- Pour diriger le trafic de données d'autres VPN vers un réseau public à partir du routeur vEdge, activez la NAT dans ces VPN ou assurez-vous que ces VPN ont une route vers VPN 0.

Lorsque NAT est activé, tout le trafic qui passe par VPN 0 est NATed. Cela inclut à la fois le trafic de données du VPN 1 destiné à un réseau public et tout le trafic de contrôle, y compris le trafic requis pour établir et gérer les tunnels du plan de contrôle DTLS entre le routeur vEdge et le contrôleur vSmart et entre le routeur et l'orchestrateur vBond.



État de l'interface de suivi

Le suivi de l'état de l'interface est utile lorsque vous activez NAT sur une interface de transport dans le VPN 0 pour permettre au trafic de données du routeur de sortir directement vers Internet plutôt que d'avoir à d'abord se rendre sur un routeur dans un centre de données. Dans ce cas, l'activation de la NAT sur l'interface de transport divise le TLOC entre le routeur local et le centre de données en deux, l'une allant au routeur distant et l'autre à Internet.

Lorsque vous activez le suivi des tunnels de transport, le logiciel analyse périodiquement le chemin vers Internet pour déterminer s'il est actif. Si le logiciel détecte que ce chemin est arrêté, il retire la route vers la destination Internet et le trafic destiné à Internet est alors acheminé via le routeur du centre de données. Lorsque le logiciel détecte que le chemin vers Internet fonctionne à nouveau, la route vers Internet est réinstallée.

Configurations

1. Configurez **tracker** sous le bloc **système**.

endpoint-dns-name <*dns-name*> est le nom DNS du point de terminaison de l'interface de tunnel. Il s'agit de la destination sur Internet à laquelle le routeur envoie des sondes pour déterminer l'état de l'interface de transport.

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

2. Configurez **nat** et **tracker** sur l'interface de transport.

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

3. Trafic direct vers local via VPN 0.

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

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

1. La route par défaut de vérification est dans 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. L'état du suivi doit être 'UP' dans la commande 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. Recherchez l'entrée de route 'NAT' dans le 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. Vérifiez que la route par défaut du côté service pointe vers l'interface de transport avec NAT activé.

```
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
```

Dépannage

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Assurez-vous que la propriété endpoint-ip ou endpoint-dns-name est quelque chose sur Internet qui peut répondre aux requêtes HTTP. Vérifiez également que l'adresse IP du point de terminaison n'est pas identique à celle de l'interface de transport. Dans le cas présent, l'option « État du suivi » s'affiche comme « Absent ».

```
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. Voici un exemple qui peut être utilisé afin de vérifier que les paquets vont vers Internet. Par exemple, 8.8.8.8 est Google DNS. Les paquets de VPN 1 sont source.

```
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
```

Vérifiez les filtres de traduction NAT. Vous verrez que le filtre NAT est conçu pour le protocole ICMP (Internet Control Message Protocol).

```
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      -
```