Siga el estado de salud de los túneles cuando está conectado con Internet

Contenido

Introducción

Este documento describe cómo seguir el estado de la salud de los túneles del transporte en VPN 0. En las versiones 17.2.2 y posterior, en las interfaces de transporte habilitadas Network Address Translation (NAT) se utilizan para la salida local de Internet. Usted puede seguir el estatus de la conexión de Internet con la ayuda de éstos. Si Internet llega a ser inasequible, el tráfico se reorienta automáticamente al túnel del NON-NATed en la interfaz de transporte.

Antecedentes

Para proporcionar a los usuarios en un sitio local con directo, acceso seguro a los recursos de Internet, tales como sitios web, usted puede configurar al router del vEdge para funcionar como un dispositivo NAT, que realiza el direccionamiento y la traducción de puerto (NAPT). Cuando usted habilita el NAT, permite el tráfico que sale de un router del vEdge para pasar directamente al Internet bastante que siendo backhauled a un recurso de la co-ubicación que proporcione los servicios NAT para el acceso a Internet. Si usted utiliza el NAT de esta manera en un router del vEdge, usted puede eliminar el tráfico “tromboning” y tener en cuenta las rutas eficientes, que tienen distancias más cortas, entre los usuarios en el sitio local y las aplicaciones basadas en la red que utilizan.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

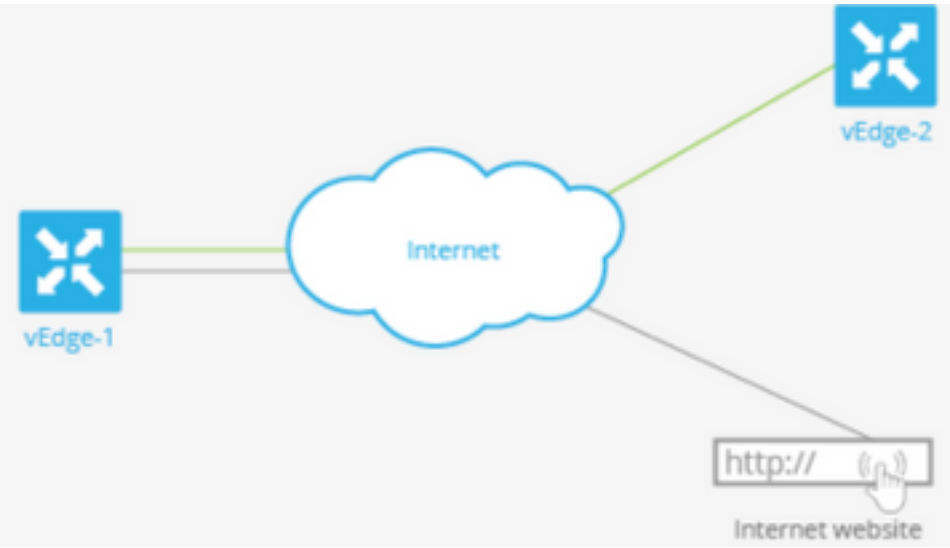
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

el router vEdge1 aquí actúa como dispositivo NAT. El router del vEdge parte su tráfico en dos flujos, que usted puede pensar en como dos túneles diferentes. Sigue habiendo dentro de la red de recubrimiento y viaja un flujo de tráfico, mostrado en el verde, entre el dos Routers en la moda usual, en los túneles IPsec seguros que forman la red de recubrimiento. El segundo flujo de tráfico, mostrado en el gris, se reorienta a través de la red del dispositivo NAT del router del vEdge y entonces de recubrimiento de los a una red pública.



Esta imagen explica cómo la funcionalidad de NAT en las fracturas del router del vEdge trafica en dos flujos (o dos túneles) de modo que algo de él permanezca dentro de la red de recubrimiento y algo vaya directamente a Internet o a otras redes públicas.

Aquí, el router del vEdge tiene dos interfaces:

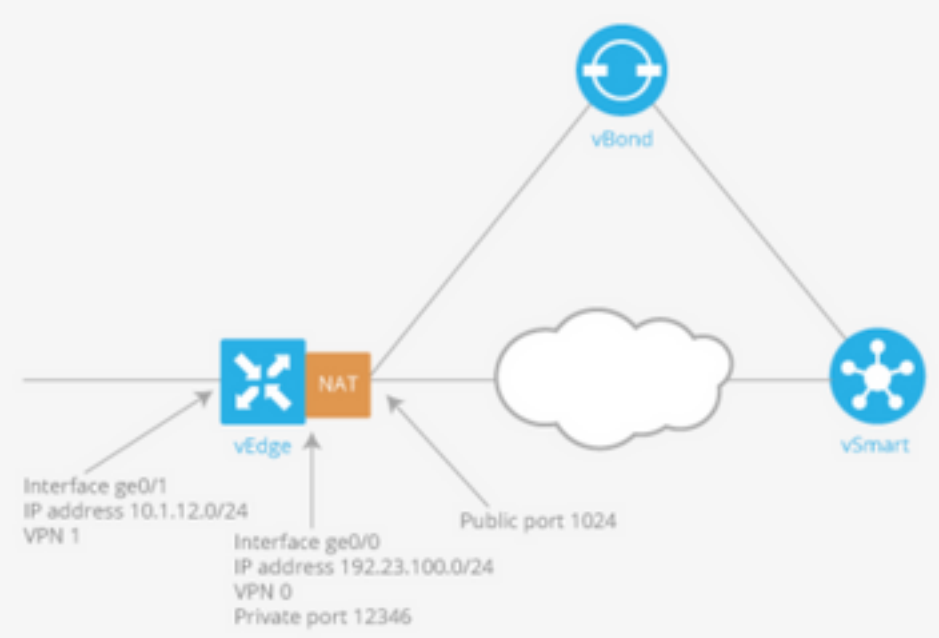
- Interconecte ge0/1 hace frente al sitio local y está en el VPN1. Su dirección IP es 10.1.12.0/24.
- Interconecte ge0/0 hace frente a la nube del transporte y está en VPN 0 (el transporte VPN). Su dirección IP es 192.23.100.0/24, y utiliza el número del puerto del valor por defecto OMP, 12346, para los túneles de la red de recubrimiento.

Para configurar al router del vEdge para actuar como dispositivo NAT de modo que un cierto tráfico del router pueda ir directamente a una red pública, usted hace tres cosas:

- Permiso NAT en el transporte VPN (VPN 0) en el WAN-transporte – haciendo frente a la interfaz, que aquí es ge0/0. Todo el tráfico que sale del router del vEdge, pasando a otros sitios de red del recubrimiento o a una red pública, pasos con esto interfaz.

- Para ordenar el tráfico de datos de otros VPN para salir del router del vEdge directamente a una red pública, habilite el NAT en esos VPN o asegúrese de que esos VPN tienen una ruta a VPN 0.

Cuando se habilita el NAT, todo el tráfico que los pasos con VPN 0 son NATed. Esto incluye el tráfico de datos del VPN1 que es destinado para una red pública y todo el tráfico de control, incluyendo el tráfico requerido establecer y mantener los túneles del avión del control DTL entre el router del vEdge y el regulador del vSmart y entre el router y el orchestrator del vBond.



Estatus de la interfaz de la pista

El seguimiento del estatus de la interfaz es útil cuando usted permite al NAT en una interfaz de transporte en VPN 0 para permitir que el tráfico de datos del router salga directamente a Internet bastante que teniendo que primero ir a un router en un centro de datos. En esta situación, habilitar el NAT en la interfaz de transporte parte el TLOC entre el router local y el centro de datos en dos, con uno que va al router remoto y el otro yendo a Internet.

Cuando usted habilita el túnel del transporte que sigue, el software sonda periódicamente la trayectoria al Internet para determinar si está para arriba. Si el software detecta que esta trayectoria está abajo, retira la ruta al destino de Internet, y el tráfico destinado a Internet entonces se rutea a través del router de centro de datos. Cuando el software detecta que está funcionando la trayectoria a Internet otra vez, la ruta a Internet está reinstalada.

Configuraciones

1. **Perseguidor de la** configuración bajo bloque de **sistema**.

el <DNS-nombre del punto final-dns-nombre > es el nombre DNS del punto final de la interfaz del túnel. Éste es el destino en el Internet al cual el router envía las sondas para determinar el estatus de la interfaz de transporte.

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

```
!
```

2. Configuración **nacional** y **perseguidor** en la interfaz de transporte.

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

3. Tráfico directo a la existencia localmente vía VPN 0.

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

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

1. La ruta predeterminado del control está en 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. El estatus del perseguidor debe estar “ENCIMA DE” en la interfaz VPN 0 de la demostración.

```
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. Busque la entrada de la ruta “NAT” en el 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. Compruebe varias veces que el Default Route del servicio-lado señale a la interfaz de transporte con el NAT encendido.

```
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
```

Troubleshooting

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Asegúrese de que el punto final-IP o el punto final-dns-nombre sea algo en Internet que puede responder a los pedidos de HTTP. También, verifique que la dirección IP del punto final no sea lo mismo que la interfaz de transporte. En el caso, el “estatus del perseguidor” mostrará como “abajo”.

```
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. Aquí está un ejemplo que se puede utilizar para verificar que los paquetes salen a Internet. Por ejemplo, 8.8.8.8 es Google DNS. Los paquetes del VPN1 son originados.

```
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
```

Verifique los filtros de translación NAT. Usted verá que el filtro NAT está construido para el 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      -
```