

Seguimiento del estado de los túneles cuando se conecta a Internet

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Estado de la interfaz de seguimiento](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo realizar el seguimiento del estado de los túneles de transporte en VPN 0. En las versiones 17.2.2 y posteriores, las interfaces de transporte habilitadas para la traducción de direcciones de red (NAT) se utilizan para la salida local de Internet. Puede realizar un seguimiento del estado de la conexión a Internet con la ayuda de estos. Si Internet deja de estar disponible, el tráfico se redirige automáticamente al túnel no NATed en la interfaz de transporte.

Antecedentes

Para proporcionar a los usuarios de un sitio local acceso directo y seguro a los recursos de Internet, como los sitios web, puede configurar el router vEdge para que funcione como dispositivo NAT, que realiza la traducción de direcciones y de puertos (NAPT). Cuando habilita la NAT, permite que el tráfico que sale de un router vEdge pase directamente a Internet en lugar de volverse a una instalación de ubicación conjunta que proporciona servicios NAT para el acceso a Internet. Si utiliza NAT de esta manera en un router vEdge, puede eliminar el tráfico "tromboning" y permitir rutas eficientes, que tengan distancias más cortas, entre los usuarios del sitio local y las aplicaciones basadas en la red que utilizan.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

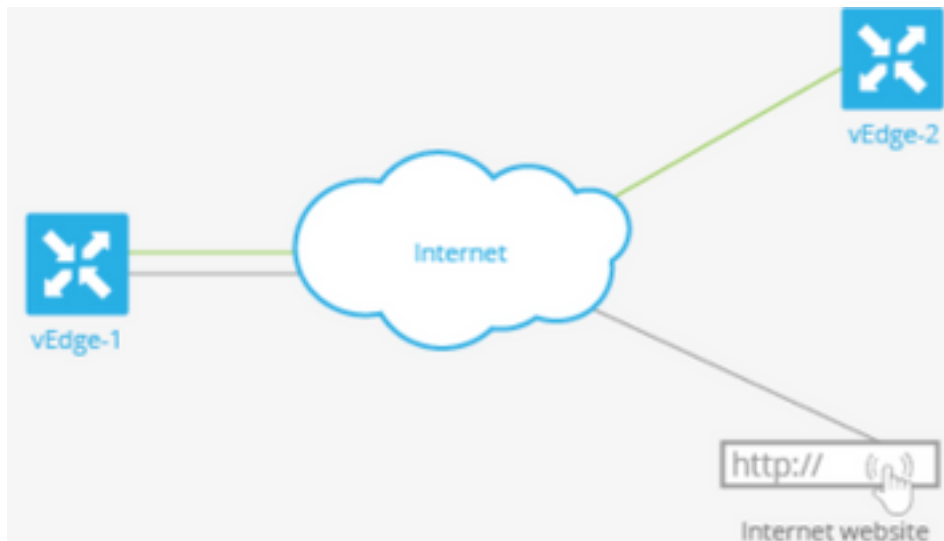
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 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 vEdge divide su tráfico en dos flujos, que se pueden considerar dos túneles independientes. Un flujo de tráfico, mostrado en verde, permanece dentro de la red superpuesta y viaja entre los dos routers de la manera habitual, en los túneles IPsec seguros que forman la red superpuesta. El segundo flujo de tráfico, que se muestra en gris, se redirige a través del dispositivo NAT del router vEdge y, a continuación, sale de la red superpuesta a una red pública.



Esta imagen explica cómo la funcionalidad de NAT en el router vEdge divide el tráfico en dos flujos (o dos túneles) de modo que parte de él permanezca dentro de la red superpuesta y algunos vayan directamente a Internet u otras redes públicas.

Aquí, el router vEdge tiene dos interfaces:

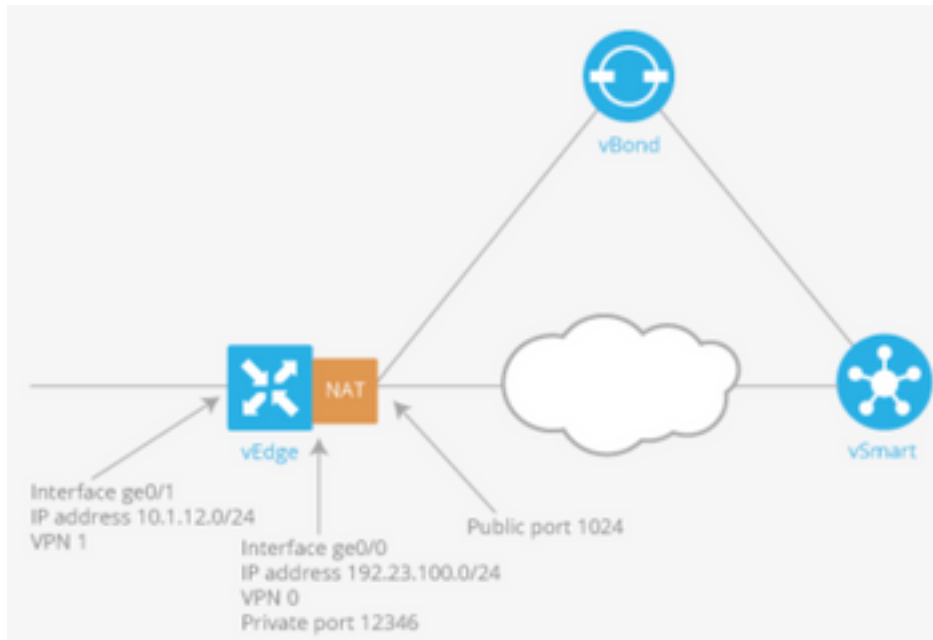
- La interfaz ge0/1 se dirige al sitio local y está en VPN 1. Su dirección IP es 10.1.12.0/24.
- La interfaz ge0/0 se enfrenta a la nube de transporte y está en VPN 0 (la VPN de transporte). Su dirección IP es 192.23.100.0/24 y utiliza el número de puerto OMP predeterminado, 12346, para los túneles de red superpuestos.

Para configurar el router vEdge para que actúe como dispositivo NAT de modo que parte del tráfico del router pueda ir directamente a una red pública, usted hace tres cosas:

- Habilite NAT en la VPN de transporte (VPN 0) en la interfaz de transporte WAN, que aquí es ge0/0. Todo el tráfico que sale del router vEdge, que va a otros sitios de red superpuestos o a una red pública, pasa a través de esta interfaz.
- Para dirigir el tráfico de datos de otras VPN para salir del router vEdge directamente a una

red pública, habilite NAT en esas VPN o asegúrese de que esas VPN tengan una ruta a VPN 0.

Cuando se habilita NAT, todo el tráfico que pasa a través de VPN 0 se NATed. Esto incluye tanto el tráfico de datos de VPN 1 destinado a una red pública como todo el tráfico de control, incluido el tráfico necesario para establecer y mantener túneles del plano de control DTLS entre el router vEdge y el controlador vSmart y entre el router y el orquestador vBond.



Estado de la interfaz de seguimiento

El seguimiento del estado de la interfaz es útil cuando se habilita NAT en una interfaz de transporte en VPN 0 para permitir que el tráfico de datos del router salga directamente a Internet en lugar de tener que ir primero a un router en un Data Center. En esta situación, al habilitar NAT en la interfaz de transporte, el TLOC entre el router local y el Data Center se divide en dos, uno se dirige al router remoto y el otro a Internet.

Cuando habilita el seguimiento del túnel de transporte, el software sondea periódicamente la ruta a Internet para determinar si está activa. Si el software detecta que esta trayectoria está inactiva, retira la ruta al destino de Internet y, a continuación, el tráfico destinado a Internet se rutea a través del router del Data Center. Cuando el software detecta que la ruta a Internet vuelve a funcionar, la ruta a Internet se reinstala.

Configuraciones

1. Configure **tracker** bajo el **bloque system**.

el **terminal-dns-name <dns-name>** es el nombre DNS del punto final de la interfaz de túnel. Este es el destino en Internet al que el router envía sondas para determinar el estado de la interfaz de transporte.

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



```
-----
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 ruta 'NAT' en la 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
```

| 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. Verifique que la ruta predeterminada del lado del servicio apunte a la interfaz de transporte con NAT activada.

```
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
```

| 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 | | | | | |

Troubleshoot

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Asegúrese de que terminal-ip o terminal-dns-name sea algo en Internet que pueda responder a las solicitudes HTTP. Además, verifique que la dirección IP del terminal no sea la misma que la interfaz de transporte. En el caso, "Estado del localizador" se mostrará como "Abajo".

```
vEdge# show interface ge0/0
```

```
TCP      IF      IF      IF
```

| VPN | INTERFACE | AF | TYPE | IP ADDRESS | ADMIN | OPER | TRACKER | ENCAP | PORT | TYPE | MTU | HWADDR |
|-----|-----------|----|--------|------------|--------|---------|---------|-------|------|------|-----|--------|
| | MBPS | | DUPLEX | ADJUST | STATUS | STATUS | STATUS | TYPE | | | | |
| | | | | 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. Este es un ejemplo que se puede utilizar para verificar que los paquetes salgan a Internet. Por ejemplo, 8.8.8.8 es Google DNS. Los paquetes de VPN 1 se originan.

```
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 traducción NAT. Verá que el filtro NAT se ha creado para protocolo de mensajes de control de Internet (ICMP).

```
vEdge# show ip nat filter
```

| NAT | NAT | | | PRIVATE | | PRIVATE | PRIVATE | PUBLIC | |
|------|--------|-------|-------------|------------|----------|----------|---------|------------|---------|
| DEST | SOURCE | DEST | | SOURCE | PRIVATE | DEST | SOURCE | DEST | SOURCE |
| | | | FILTER | IDLE | OUTBOUND | OUTBOUND | INBOUND | INBOUND | PUBLIC |
| VPN | IFNAME | VPN | PROTOCOL | ADDRESS | ADDRESS | PORT | PORT | ADDRESS | ADDRESS |
| | PORT | PORT | STATE | TIMEOUT | PACKETS | OCTETS | PACKETS | OCTETS | |
| 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 | - |