Rastrear o status da integridade dos túneis quando conectado à Internet

Contents

Introduction

Este documento descreve como rastrear o status de integridade dos túneis de transporte no VPN 0. Nas versões 17.2.2 e posteriores, as interfaces de transporte ativadas para Network Address Translation (NAT) são usadas para saída da Internet local. Você pode rastrear o status da conexão com a Internet com a ajuda deles. Se a Internet ficar indisponível, o tráfego será automaticamente redirecionado para o túnel não NAT na interface de transporte.

Informações de Apoio

Para fornecer aos usuários em um local acesso direto e seguro a recursos da Internet, como sites, você pode configurar o roteador vEdge para funcionar como um dispositivo NAT, que executa a conversão de endereço e porta (NAPT). Quando você habilita o NAT, ele permite que o tráfego que sai de um roteador vEdge passe diretamente para a Internet em vez de ser transferido para uma instalação de co-localização que fornece serviços NAT para acesso à Internet. Se você usar o NAT dessa forma em um roteador vEdge, poderá eliminar o "trombone" de tráfego e permitir rotas eficientes, que tenham distâncias menores, entre os usuários no local e os aplicativos baseados na rede que eles usam.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

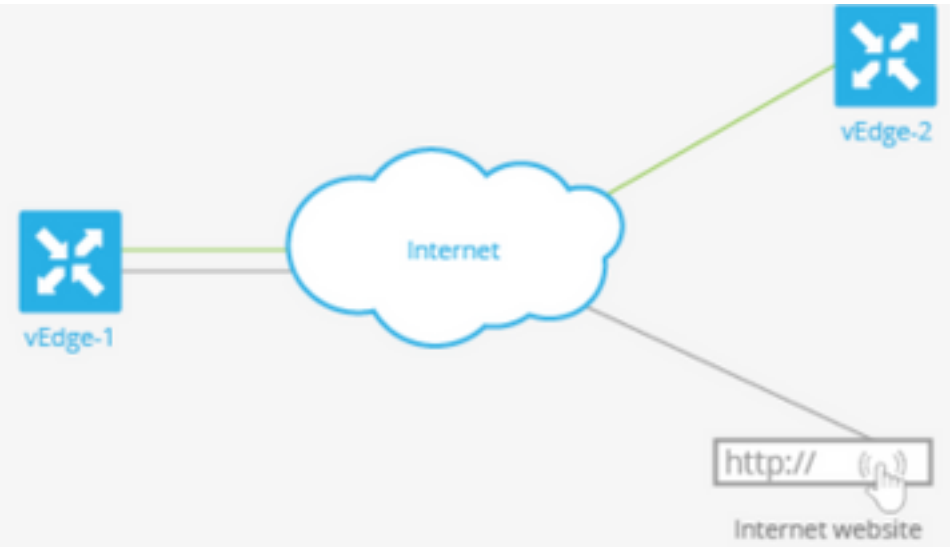
Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede

O roteador vEdge1 aqui atua como um dispositivo NAT. O roteador vEdge divide o tráfego em dois fluxos, que você pode imaginar como dois túneis separados. Um fluxo de tráfego, mostrado em verde, permanece dentro da rede de sobreposição e viaja entre os dois roteadores da maneira usual, nos túneis IPsec seguros que formam a rede de sobreposição. O segundo fluxo de tráfego, mostrado em cinza, é redirecionado através do dispositivo NAT do roteador vEdge e, em seguida, da rede de sobreposição para uma rede pública.



Essa imagem explica como a funcionalidade NAT no roteador vEdge divide o tráfego em dois fluxos (ou dois túneis) de modo que alguns permaneçam na rede sobreposta e outros vão diretamente para a Internet ou outras redes públicas.

Aqui, o roteador vEdge tem duas interfaces:

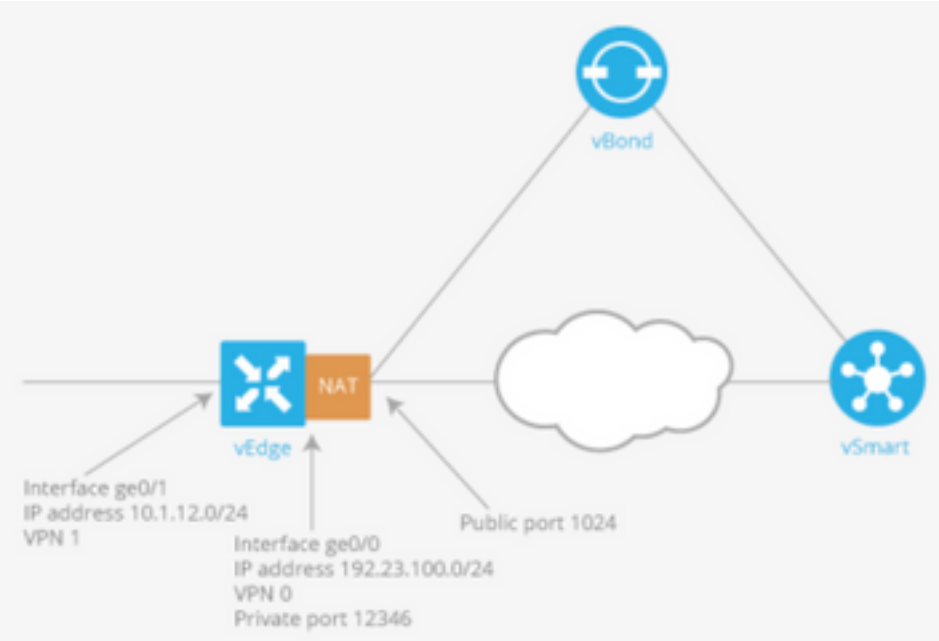
- A interface ge0/1 enfrenta o site local e está na VPN 1. Seu endereço IP é 10.1.12.0/24.
- A interface ge0/0 enfrenta a nuvem de transporte e está no VPN 0 (o transporte VPN). Seu endereço IP é 192.23.100.0/24 e usa o número de porta OMP padrão, 12346, para túneis de rede sobrepostos.

Para configurar o roteador vEdge para atuar como um dispositivo NAT de modo que algum tráfego do roteador possa ir diretamente para uma rede pública, você faz três coisas:

- Ative o NAT na VPN de transporte (VPN 0) na interface para transporte da WAN, que aqui é ge0/0. Todo o tráfego que sai do roteador vEdge, indo para outros locais de rede sobrepostos ou para uma rede pública, passa por essa interface.
- Para direcionar o tráfego de dados de outras VPNs para sair do roteador vEdge diretamente para uma rede pública, ative a NAT nessas VPNs ou assegure que essas VPNs tenham uma

rota para a VPN 0.

Quando o NAT é ativado, todo o tráfego que passa pelo VPN 0 é NATed. Isso inclui o tráfego de dados da VPN 1 destinado a uma rede pública e todo o tráfego de controle, incluindo o tráfego necessário para estabelecer e manter túneis de plano de controle DTLS entre o roteador vEdge e o controlador vSmart e entre o roteador e o orquestrador vBond.



Monitorar status da interface

O rastreamento do status da interface é útil quando você habilita o NAT em uma interface de transporte na VPN 0 para permitir que o tráfego de dados do roteador saia diretamente para a Internet, em vez de ter que primeiro ir para um roteador em um data center. Nessa situação, a ativação do NAT na interface de transporte divide o TLOC entre o roteador local e o data center em dois, com um indo para o roteador remoto e o outro indo para a Internet.

Quando você habilita o rastreamento de túnel de transporte, o software sonda periodicamente o caminho para a Internet para determinar se ele está ativado. Se o software detectar que esse caminho está inoperante, ele retira a rota para o destino da Internet e o tráfego destinado à Internet é roteado através do roteador do data center. Quando o software detecta que o caminho para a Internet está novamente funcionando, a rota para a Internet é reinstalada.

Configurações

1. Configure o **rastreador** no bloco **do sistema**.

endpoint-dns-name <*dns-name*> é o nome DNS do endpoint da interface do túnel. Esse é o destino na Internet para o qual o roteador envia sondas para determinar o status da interface de transporte.

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

2. Configure **nat** e **tracker** na interface de transporte.

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

3. Direcionar o tráfego para o existente localmente via VPN 0.

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. A verificação da rota padrão está em 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. O status do rastreador deve ser 'UP' em 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. Procure a entrada da rota 'NAT' no 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. Verifique se a rota padrão do lado do serviço aponta para a interface de transporte com NAT ativado.

```
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
```

Troubleshoot

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Certifique-se de que o endpoint-ip ou endpoint-dns-name seja algo na Internet que possa responder às solicitações HTTP. Além disso, verifique se o endereço IP do ponto final não é o mesmo da interface de Transporte. No caso, "Status do rastreador" será exibido como "Inativo".

```
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. Aqui está um exemplo que pode ser usado para verificar se os pacotes saem para a Internet. Por exemplo, 8.8.8.8 é o Google DNS. Os pacotes da VPN 1 são 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 os filtros de tradução NAT. Você verá que o filtro NAT foi criado para o 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      -
```