Siga o estado de saúde dos túneis quando conectado ao Internet

Índice

Introdução

Este documento descreve como seguir o estado da saúde dos túneis do transporte em VPN 0. Nas liberações 17.2.2 e mais atrasado, em interfaces de transporte permitidas Network Address Translation (NAT) são usados para a saída local do Internet. Você pode seguir o estado da conexão com o Internet com a ajuda destes. Se o Internet se torna não disponível, o tráfego está reorientado automaticamente ao túnel do NON-NATed na interface de transporte.

Informações de Apoio

A fim fornecer usuários em uma site local com o direto, acesso seguro aos recursos de Internet, tais como Web site, você pode configurar o roteador do vEdge para funcionar como um dispositivo NAT, que execute o endereço e a tradução de porta (NAPT). Quando você permite o NAT, permite o tráfego que retira de um roteador do vEdge para passar diretamente ao Internet um pouco do que sendo backhaul a uma facilidade do co-lugar que proporcione serviços NAT para o acesso ao Internet. Se você usa o NAT desta maneira em um roteador do vEdge, você pode eliminar o tráfego “que tromboning” e permiti-lo as rotas eficientes, que têm umas distâncias mais curtos, entre os usuários na site local e os aplicativos Com base na rede que usam.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

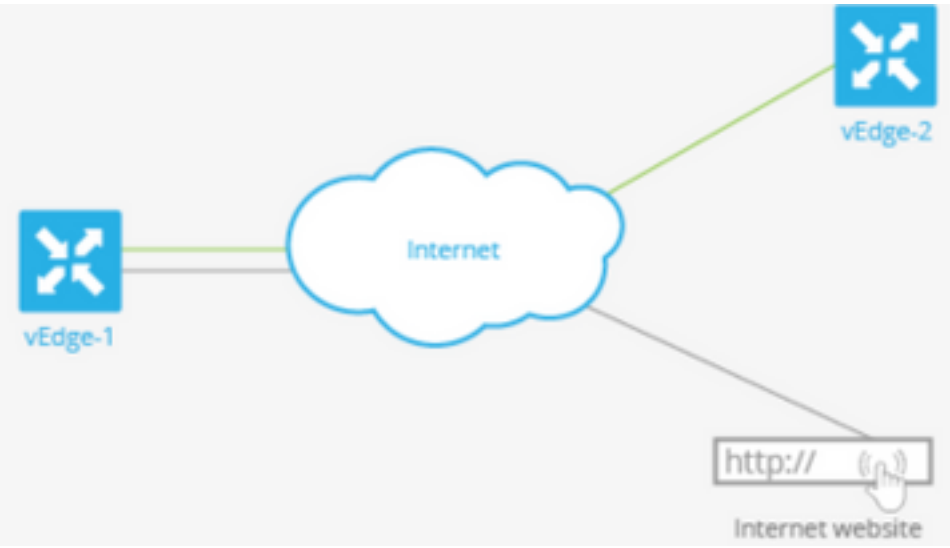
Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. 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 do vEdge racha seu tráfego em dois fluxos, que você pode pensar como de dois túneis separados. Um fluxo de tráfego, mostrado no verde, permanece dentro da rede de folha de prova e viaja entre os dois Roteadores na forma usual, nos túneis de IPsec seguros que formam a rede de folha de prova. O segundo fluxo de tráfego, mostrado no cinza, é reorientado através do dispositivo NAT do roteador do vEdge e então fora da rede de folha de prova a uma rede pública.



Esta imagem explica como a funcionalidade de NAT nas separações do roteador do vEdge trafica em dois fluxos (ou em dois túneis) de modo que alguma dele permaneça dentro da rede de folha de prova e algumas vão diretamente ao Internet ou a outras redes públicas.

Aqui, o roteador do vEdge tem duas relações:

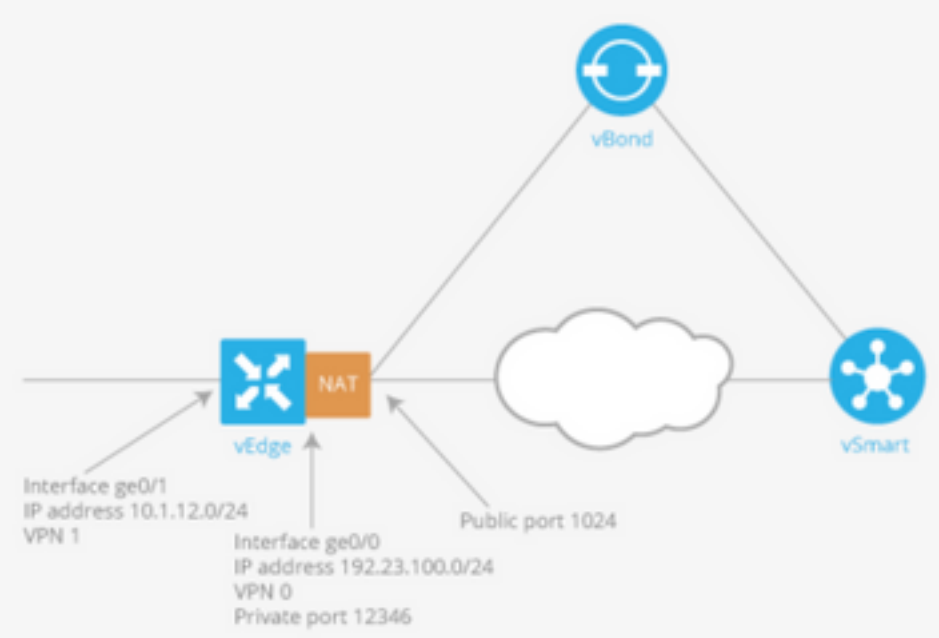
- Conecte ge0/1 enfrenta a site local e está no VPN1. Seu endereço IP de Um ou Mais Servidores Cisco ICM NT é 10.1.12.0/24.
- Conecte ge0/0 enfrenta a nuvem do transporte e está em VPN 0 (o transporte VPN). Seu endereço IP de Um ou Mais Servidores Cisco ICM NT é 192.23.100.0/24, e usa o número de porta do padrão OMP, 12346, para túneis da rede de folha de prova.

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

- Permita o NAT no transporte VPN (VPN 0) no WAN-transporte – enfrentando a relação, que é aqui ge0/0. Todo o tráfego que retira do roteador do vEdge, indo a outras sites de rede da folha de prova ou a uma rede pública, passa através desta relação.

- Para dirigir o tráfego de dados de outros VPN para retirar do roteador do vEdge diretamente a uma rede pública, permita o NAT naqueles VPN ou assegure-se de que aqueles VPN tenham uma rota a VPN 0.

Quando o NAT for permitido, todo o tráfego que as passagens com VPN 0 são NATed. Isto inclui o tráfego de dados do VPN1 que é destinado para rede pública e todo o tráfego de controle, incluindo o tráfego exigido estabelecer e manter túneis do plano do controle DTL entre o roteador do vEdge e o controlador do vSmart e entre o roteador e o orchestrator do vBond.



Status da interface da trilha

Seguir o status da interface é útil quando você permite o NAT em uma interface de transporte em VPN 0 de permitir que o tráfego de dados do roteador retire diretamente ao Internet um pouco do que tendo que primeiramente ir a um roteador em um centro de dados. Nesta situação, permitir o NAT na interface de transporte racha o TLOC entre o roteador local e o centro de dados em dois, com o um que vai ao roteador remoto e o outro que vai ao Internet.

Quando você permite o túnel do transporte que segue, o software sonda periodicamente o trajeto ao Internet para determinar se está acima. Se o software detecta que este trajeto está para baixo, retira a rota ao destino do Internet, e o tráfego destinado ao Internet é distribuído então através do roteador do centro de dados. Quando o software detecta que o trajeto ao Internet está funcionando outra vez, a rota ao Internet é reinstalada.

Configurações

1. Configurar o **perseguidor** sob o bloco de **sistema**.

o <dns-nome do valor--dns-nome > é o nome de DNS do valor-limite da interface de túnel. Este é o destino no Internet a que o roteador envia pontas de prova para determinar o estado da interface de transporte.

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

```
!
```

2. Configurar **nat** e o **perseguidor na** interface de transporte.

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

3. Tráfego direto à existência localmente através de 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 rota padrão da verificação 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 estado do perseguidor deve estar “ACIMA DE” na relação VPN 0 da mostra.

```
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 que o Default-route do serviço-lado aponta à interface de transporte com o NAT sobre.

```
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

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

1. Assegure-se de que o valor--IP ou o valor--dns-nome sejam algo no Internet que pode responder aos pedidos do HTTP. Também, verifique que o endereço IP de Um ou Mais Servidores Cisco ICM NT do valor-limite não é o mesmo que a interface de transporte. No caso, do “o estado perseguidor” mostrará como “para baixo”.

```
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. Está aqui um exemplo que possa ser usado a fim verificar que os pacotes saem ao Internet. Por exemplo, 8.8.8.8 é Google DNS. Os pacotes do VPN1 são originado.

```
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 translational NAT. Você verá que o filtro NAT está construído 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      -
```