Tieni traccia dello stato dei tunnel quando connesso a Internet

Sommario

Introduzione

In questo documento viene descritto come tenere traccia dello stato di integrità dei tunnel di trasporto nella VPN 0. Nelle versioni 17.2.2 e successive, le interfacce di trasporto abilitate NAT (Network Address Translation) vengono utilizzate per l'uscita Internet locale. È possibile tenere traccia dello stato della connessione Internet con l'aiuto di questi. Se Internet non è più disponibile, il traffico viene reindirizzato automaticamente al tunnel non NAT sull'interfaccia di trasporto.

Premesse

Per fornire agli utenti di un sito locale un accesso diretto e sicuro alle risorse Internet, ad esempio i siti Web, è possibile configurare il router vEdge in modo che funzioni come dispositivo NAT, che esegue sia la conversione degli indirizzi che delle porte (NAPT, Port Translation). Quando si abilita NAT, il traffico in uscita da un router vEdge passa direttamente a Internet anziché essere ritrasportato a una struttura di co-locazione che fornisce servizi NAT per l'accesso a Internet. Se si utilizza NAT in questo modo su un router vEdge, è possibile eliminare il traffico "tromboning" e consentire percorsi efficienti, con distanze più brevi, tra gli utenti del sito locale e le applicazioni basate sulla rete che utilizzano.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

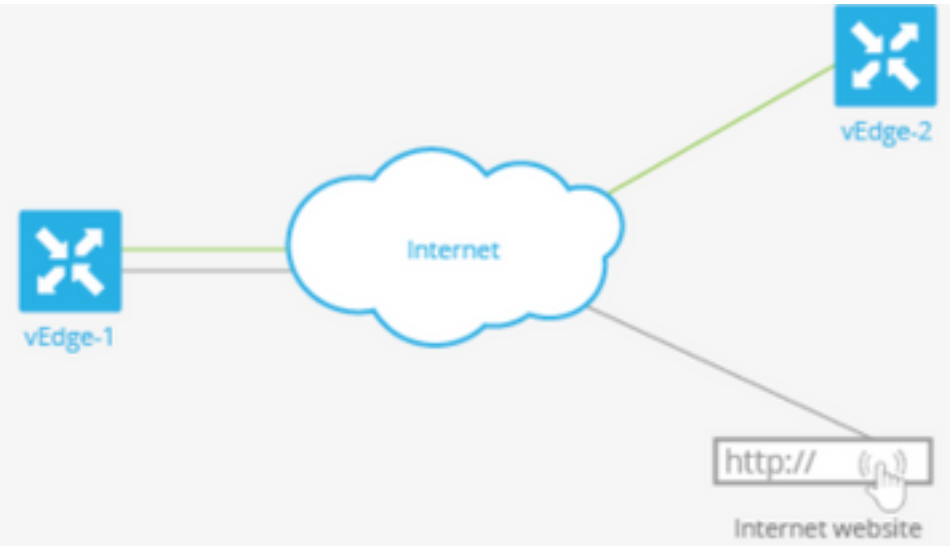
Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

Il router vEdge1 qui funge da dispositivo NAT. Il router vEdge suddivide il traffico in due flussi, che possono essere considerati come due tunnel separati. Un flusso di traffico, mostrato in verde, rimane all'interno della rete di sovrapposizione e viaggia tra i due router nella maniera usuale, sui tunnel IPsec sicuri che formano la rete di sovrapposizione. Il secondo flusso di traffico, visualizzato in grigio, viene reindirizzato a una rete pubblica attraverso il dispositivo NAT del router vEdge e quindi fuori dalla rete di sovrimpressione.



Questa immagine spiega come la funzionalità NAT sul router vEdge suddivida il traffico in due flussi (o due tunnel) in modo che alcuni di essi rimangano all'interno della rete sovrapposta e altri vadano direttamente a Internet o ad altre reti pubbliche.

In questo caso, il router vEdge ha due interfacce:

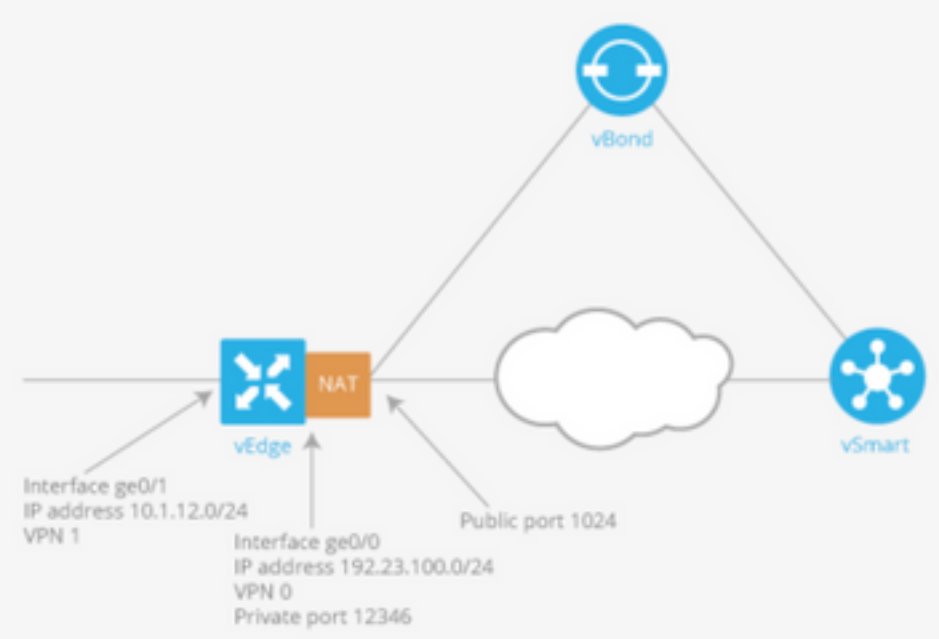
- L'interfaccia ge0/1 si trova sul sito locale e sulla VPN 1. L'indirizzo IP è 10.1.12.0/24.
- L'interfaccia ge0/0 è rivolta al cloud di trasporto ed è nella VPN 0 (la VPN di trasporto). Il suo indirizzo IP è 192.23.100.0/24 e usa il numero di porta OMP predefinito, 12346, per sovrapporre i tunnel di rete.

Per configurare il router vEdge in modo che agisca come dispositivo NAT in modo che parte del traffico proveniente dal router possa raggiungere direttamente una rete pubblica, è necessario eseguire tre operazioni:

- Abilitare NAT nella VPN (VPN 0) di trasporto sull'interfaccia con connessione WAN, che qui è ge0/0. Tutto il traffico in uscita dal router vEdge, diretto ad altri siti di rete sovrapposti o a una rete pubblica, passa attraverso questa interfaccia.
- Per indirizzare il traffico di dati da altre VPN in modo da uscire dal router vEdge direttamente

a una rete pubblica, abilitare NAT in tali VPN o verificare che tali VPN dispongano di una route alla VPN 0.

Quando NAT è abilitato, tutto il traffico che passa attraverso la VPN 0 è associato a NAT. Ciò include sia il traffico di dati dalla VPN 1 destinata a una rete pubblica sia tutto il traffico di controllo, incluso il traffico necessario per stabilire e mantenere i tunnel del control plane DTLS tra il router vEdge e il controller vSmart e tra il router e l'orchestrator vBond.



Registra stato interfaccia

Tenere traccia dello stato dell'interfaccia è utile quando si abilita NAT su un'interfaccia di trasporto nella VPN 0 per consentire al traffico di dati dal router di uscire direttamente a Internet, anziché dover prima passare a un router in un centro dati. In questa situazione, abilitando NAT sull'interfaccia di trasporto, il TLOC tra il router locale e il centro dati viene suddiviso in due, con uno che va al router remoto e l'altro che va a Internet.

Quando si abilita il rilevamento del tunnel di trasporto, il software analizza periodicamente il percorso verso Internet per determinare se è attivo. Se il software rileva che il percorso è inattivo, ritira il percorso verso la destinazione Internet e il traffico destinato a Internet viene instradato attraverso il router del centro dati. Quando il software rileva che il percorso a Internet è nuovamente funzionante, il percorso a Internet viene reinstallato.

Configurazioni

1. Configurare **tracker** nel blocco **di sistema**.

endpoint-dns-name<*nome-dns*> è il nome DNS dell'endpoint dell'interfaccia del tunnel. Questa è la destinazione su Internet a cui il router invia le richieste per determinare lo stato dell'interfaccia di trasporto.

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

2. Configurare **nat** e **tracker** sull'interfaccia di trasporto.

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

3. Indirizzare il traffico verso il server locale esistente tramite VPN 0.

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

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

1. La route predefinita di controllo è nella 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. Lo stato del tracciatore deve essere 'UP' in 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. Cercare l'immissione di route 'NAT' nella 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. Verifica incrociata che il percorso predefinito dal lato servizio punti all'interfaccia di trasporto con NAT attivato.

```
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
```

Risoluzione dei problemi

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Verificare che il nome dell'endpoint-ip o dell'endpoint-dns sia disponibile su Internet in grado di rispondere alle richieste HTTP. Verificare inoltre che l'indirizzo IP dell'endpoint non sia uguale all'interfaccia di trasporto. In questo caso, "Tracker Status" (Stato tracciatore) verrà visualizzato come "Down" (Inattivo).

```
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. Di seguito è riportato un esempio che può essere usato per verificare che i pacchetti siano scaricati su Internet. Ad esempio, 8.8.8.8 è Google DNS. I pacchetti della VPN 1 hanno origine.

```
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
```

Verificare i filtri di conversione NAT. Il filtro NAT è stato creato per il protocollo 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      -
```