インターネット接続時のトンネルヘルスステータスの追跡

内容

概要

このドキュメントでは、VPN 0でトランスポートトンネルのヘルスステータスを追跡する方法について説明します。リリース17.2.2以降では、Network Address Translation（NAT；ネットワークアドレス変換）対応のトランスポートインターフェイスがローカルインターネット出口に使用されます。インターネット接続のステータスは、これらのヘルプを使用して追跡できます。インターネットが使用できなくなった場合、トラフィックはトランスポートインターフェイスの非NAT化トンネルに自動的にリダイレクトされます。

背景説明

ローカルサイトのユーザにWebサイトなどのインターネットリソースへの直接かつ安全なアクセスを提供するために、vEdgeルータをNATデバイスとして設定し、アドレス変換(NAPT)とポート変換(NAPT)の両方を実行できます。 NATを有効にすると、vEdgeルータから出るトラフィックは、インターネットアクセス用のNATサービスを提供するコロケーションファシリティにバックホールされるのではなく、インターネットに直接渡されます。この方法でvEdgeルータでNATを使用すると、トラフィックの「トロンボーン」を排除し、ローカルサイトのユーザと使用するネットワークベースのアプリケーションとの間の距離が短い効率的なルートを許可できます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

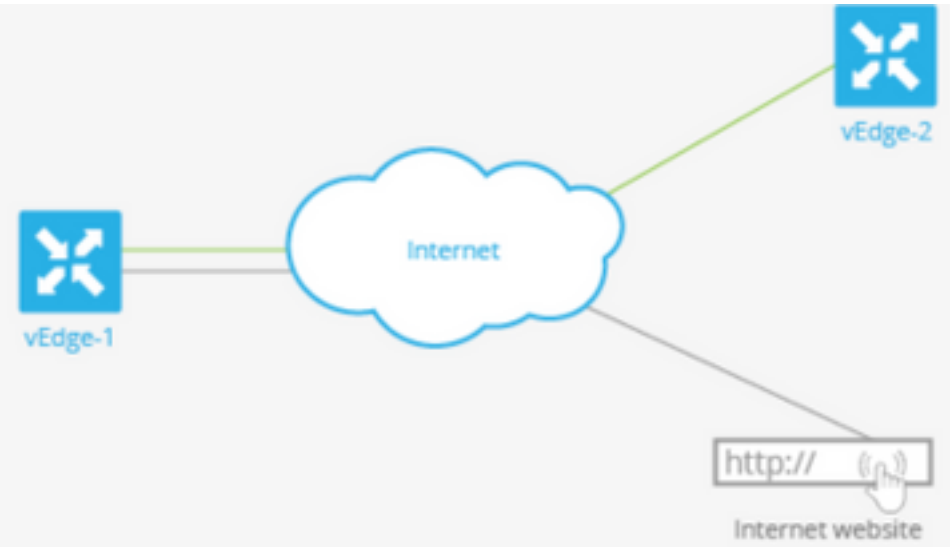
このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図

ここで、vEdge1ルータはNATデバイスとして機能します。vEdgeルータはトラフィックを2つのフローに分割し、2つの個別のトンネルと考えることができます。緑色で示された1つのトラフィックフローはオーバーレイネットワーク内に残り、オーバーレイネットワークを形成するセキュアなIPsecトンネル上の2つのルータ間を通常の方法で移動します。2番目のトラフィックストリームはグレーで示され、vEdgeルータのNATデバイスを経由してオーバーレイネットワークからパブリックネットワークにリダイレクトされます。



次の図は、vEdgeルータのNAT機能がトラフィックを2つのフロー（または2つのトンネル）に分割して、一部がオーバーレイネットワークに残り、一部がインターネットやその他のパブリックネットワークに直接移動する方法を示しています。

ここで、vEdgeルータには2つのインターフェイスがあります。

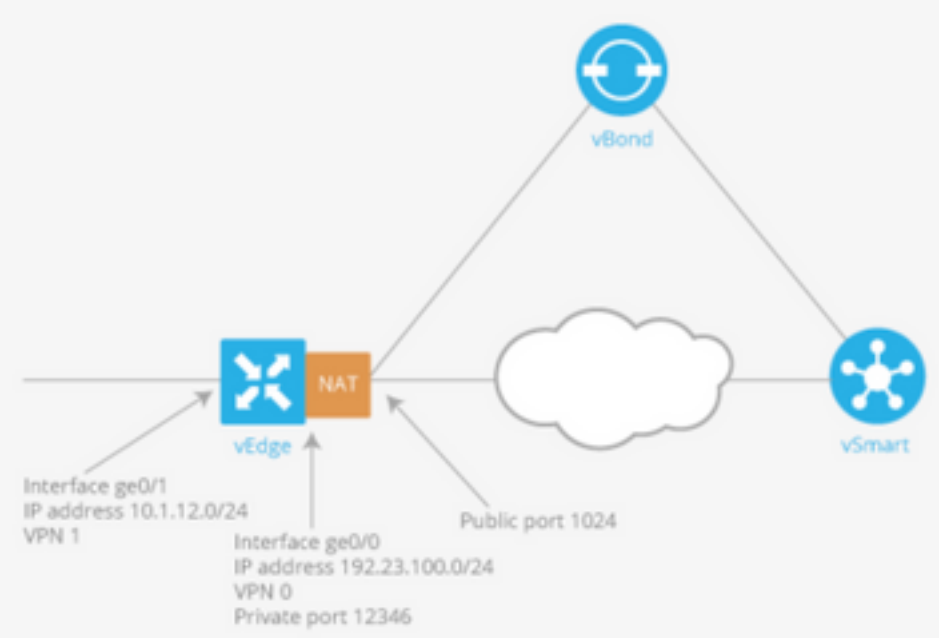
- インターフェイスge0/1はローカルサイトに面しており、VPN 1にあります。そのIPアドレスは10.1.12.0/24です。
- インターフェイスge0/0はトランスポートクラウドに面しており、VPN 0（トランスポートVPN）にあります。 そのIPアドレスは192.23.100.0/24で、オーバーレイネットワークトンネルにはデフォルトのOMPポート番号12346が使用されます。

ルータからの一部のトラフィックがパブリックネットワークに直接送信されるようにvEdgeルータをNATデバイスとして機能するように設定するには、次の3つのことを行います。

- WANトランスポート側インターフェイス上のトランスポートVPN(VPN 0)でNATを有効にします。これはge0/0です。vEdgeルータから出るすべてのトラフィックは、他のオーバーレイネットワークサイトまたはパブリックネットワークに向かいます。

- 他のVPNからのデータトラフィックをvEdgeルータから直接パブリックネットワークに送信するには、これらのVPNでNATを有効にするか、これらのVPNにVPN 0へのルートがあることを確認します。

NATが有効な場合、VPN 0を通過するすべてのトラフィックはNAT処理されます。これには、パブリックネットワークを宛先とするVPN 1からのデータトラフィックと、vEdgeルータとvSmartコントローラ間およびルータとvBondオーケストレータ間のDTLSコントロールプレーントンネルの確立と維持に必要なトラフィックの両方が含まれます。



インターフェイスのステータスの追跡

インターフェイスステータスのトラッキングは、VPN 0のトランスポートインターフェイスでNATを有効にして、ルータからのデータトラフィックをデータセンターのルータに最初に送信するのではなく、インターネットに直接送信できるようにすると便利です。この状況では、トランスポートインターフェイスでNATを有効にすると、ローカルルータとデータセンターの間のTLOCが2つに分割され、一方がリモートルータに、もう一方がインターネットに分割されます。

トランスポートトンネルのトラッキングを有効にすると、ソフトウェアはインターネットへのパスを定期的にプローブして、それがアップ状態であるかどうかを判別します。このパスがダウンしていることがソフトウェアで検出されると、インターネットの宛先へのルートが取り消され、インターネット宛てのトラフィックはデータセンタールータを経由してルーティングされます。インターネットへのパスが再び機能していることをソフトウェアが検出すると、インターネットへのルートが再インストールされます。

設定

1.システムブロックの下にトラッカーを設定します。

endpoint-dns-name <*dns-name*> は、トンネルインターフェイスのエンドポイントのDNS名です。これは、トランスポートインターフェイスのステータスを判別するためにルータがプローブを送信するインターネット上の宛先です。

```
system
 tracker tracker
```

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

2. トランスポートインターフェイスでnatとtrackerを設定します。

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

を選択します。 VPN 0経由でローカルに存在するトラフィックにトラフィックを転送します。

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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

1.VPN 0のデフォルトルートの確認

```
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. show interface VPN 0では、Tracker Statusが「UP」である必要があります。

```
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. RIBで「NAT」ルートエントリを探します。

```
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.サービス側からのデフォルトルートが、NATがオンのトランスポートインターフェイスを指していることをクロスチェックします。

```
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
```

トラブルシュート

ここでは、設定が正常に機能しているかどうかを確認します。

1. endpoint-ipまたはendpoint-dns-nameが、HTTP要求に応答できるインターネット上にあることを確認します。また、エンドポイントのIPアドレスがトランスポートインターフェイスと同じでないことを確認してください。この場合、「トラッカーのステータス」は「ダウン」と表示されます。

```
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.パケットがインターネットに送信されることを確認するために使用できる例を次に示します。たとえば、8.8.8.8はGoogle DNSです。VPN 1からのパケットは送信元です。

```
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
```

NATトランスレーショナルフィルタを確認します。NATフィルタがインターネット制御メッセージプロトコル(ICMP)用に構築されていることがわかります。

```
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      -
```