特定のサイトを地域インターネットブレークアウトとして選択する方法

内容

概要

このドキュメントでは、ダイレクトインターネットアクセス(DIA)と一元化されたデータポリシーを使用して、特定のブランチvEdgeを優先される地域インターネットブレークアウトとして設定するSD-WANファブリックの設定方法について説明します。このソリューションは、地域サイトがZscaler®などの中央集中型サービスを使用し、優先インターネット出口として使用する場合などに役立ちます。このような展開では、Generic Routing Encapsulation(GRE)またはInternet Protocol Security(IPSec)トンネルをトランスポートVPNから設定する必要があり、トラフィックがインターネットに直接到達する通常のDIAソリューションとはデータフローが異なります。

前提条件

要件

次の項目に関する専門知識があることが推奨されます。

- SD-WANポリシーフレームワークに関する基本的な知識。

使用するコンポーネント

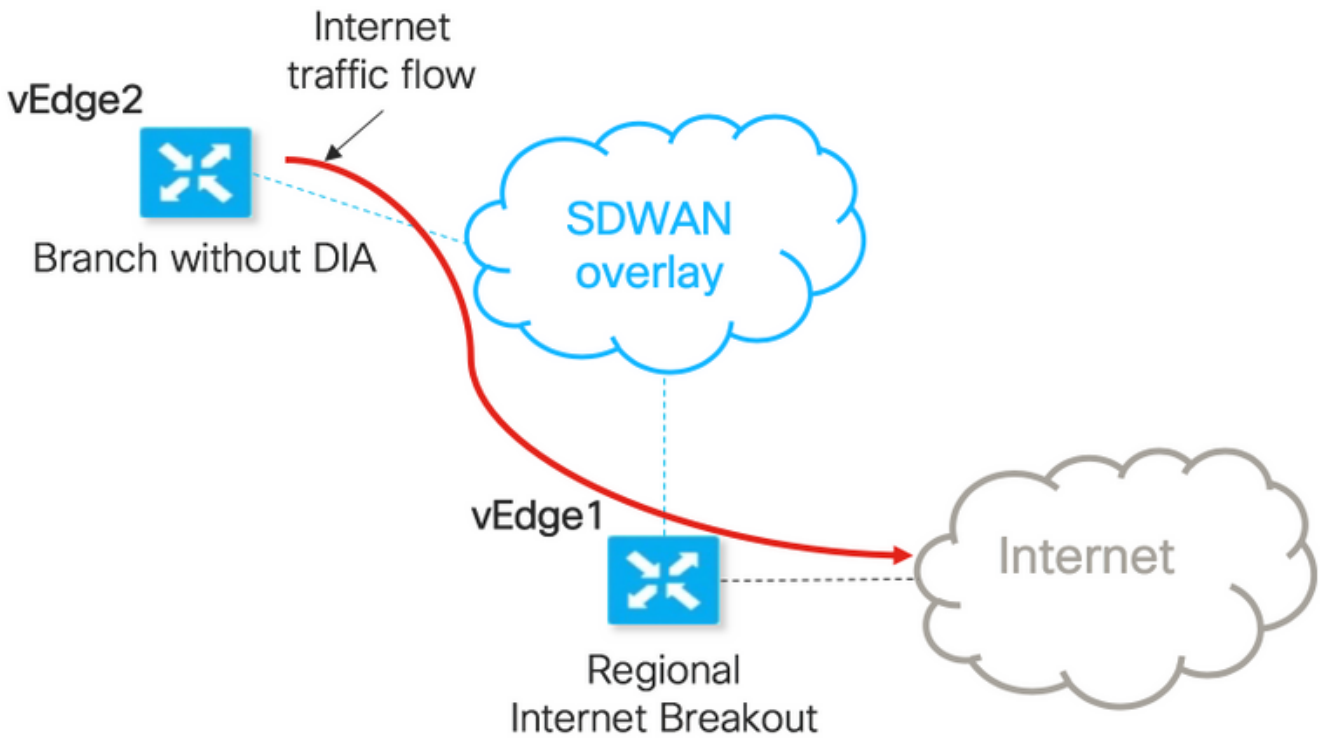
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- vEdgeルータ
- vSmart Controller(18.3.5ソフトウェアバージョン)。

背景説明

インターネットに到達する必要があるvEdge2からのサービスVPNトラフィックは、データプレーントンネルを使用して別のブランチvEdge1に転送されます。vEdge1は、ローカルインターネットブレークアウト用にDIAが設定されたルータです。

ネットワーク図



ホスト名	vEdge1	vEdge2
ホストロール	DIA（地域インターネットブレークアウト）を備えたブランチデバイス	DIAが設定されていないブランチデバイス
VPN 0		
Transport Locations(TLOC)1	biz-internet、ip: 192.168.110.6/24	biz-internet、ip: 192.168.110.5/2
Transport Locations(TLOC)2	パブリックインターネット、ip: 192.168.109.4/24	パブリックインターネット、ip: 192.168.109.5/24
サービスVPN 40	インターフェイスge0/1、ip: 192.168.40.4/24	インターフェイスge0/2、ip: 192.168.50.5/24

設定

解決策 1：ネクストホップを変更するための一元化されたデータポリシーの使用。

vEdge2には、vEdge1およびその他のサイトとのデータプレーントンネルが確立されています（フルメッシュ形式の接続）

vEdge1には、**ip route 0.0.0.0/0 vpn 0でDIAが設定されています。**

vSmart中央集中型データポリシー設定：

```
policy
 data-policy DIA_vE1
  vpn-list VPN_40
   sequence 5
    match
     destination-data-prefix-list ENTERPRISE_IPs
    !
    action accept
    !
   !
   sequence 10
    action accept
     set
      next-hop 192.168.40.4
     !
    !
   !
   default-action accept
  !
 !
!
lists
  vpn-list VPN_40
   vpn 40
  !
  data-prefix-list ENTERPRISE_IPs
   ip-prefix 10.0.0.0/8
   ip-prefix 172.16.0.0/12    ip-prefix 192.168.0.0/16 ! apply-policy site-list SITE2 data-
policy DIA_vE1 from-service
```

vEdge2：特別な設定は必要ありません。

ポリシーが正しく適用されたかどうかを確認する手順を次に示します。

1. vEdge2にポリシーがないことを確認します。

```
vedge2# show policy from-vsmart
% No entries found.
```

2.転送情報ベース(FIB)プログラミングをチェックします。インターネット上の宛先のルート不在(Blackhole)が表示されます。

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Blackhole
```

3. vSmart設定のapply-policyセクションでvSmart data-policyを適用**するか**、vManage GUIでアクティブにします。

4. vEdge2がvSmartからデータポリシーを正常に受信したことを確認します。

```
vedge2# show policy from-vsmart
from-vsmart data-policy DIA_vE1
 direction from-service
 vpn-list VPN_40
  sequence 5
   match
    destination-data-prefix-list ENTERPRISE_IPs
```

```
   action accept
  sequence 10
   action accept
    set
     next-hop 192.168.40.4
  default-action accept
from-vsmart lists vpn-list VPN_40
 vpn 40
from-vsmart lists data-prefix-list ENTERPRISE_IPs
 ip-prefix 10.0.0.0/8
 ip-prefix 172.16.0.0/12
 ip-prefix 192.168.0.0/16
```

5.インターネット上の宛先に対して可能なルートを示すForwarding Information Base(FIB)プログラミングをチェックします。

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 4
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.110.6 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.110.6 12346 Color: public-internet
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.109.4 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.109.4 12346 Color: public-internet
```

6.インターネット上の宛先への到達可能性を確認します。

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.392 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.346 ms
^C
--- 173.37.145.84 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.345/0.361/0.392/0.021 ms
```

ここでは、vEdge1の設定手順について説明します。

1.トランスポートインターフェイスでネットワークアドレス変換(NAT)をアクティブにします。ここで、DIAを使用します。

```
vpn 0
 !
 interface ge0/0
  description "DIA interface"
  ip address 192.168.109.4/24
 nat <<<<==== NAT activated for a local DIA !
```

2.サービスVPNにスタティックルートip route 0.0.0.0/0 vpn 0を追加し、DIAをアクティブ化します。

```
vpn 40
 interface ge0/4
  ip address 192.168.40.4/24
```

```
 no shutdown
!
ip route 0.0.0.0/0 vpn 0     <<<<==== Static route for DIA !
```

3. RIBにNATルートが含まれているかどうかを確認します。

```
vedge1# show ip route vpn 40 | include nat
40 0.0.0.0/0 nat - ge0/0 - 0 - - - F,S
```

4. DIAが動作していること、およびNAT変換でvEdge2から173.37.145.84へのインターネット制御メッセージプロトコル(ICMP)セッションを確認できることを確認します

```
vedge1# show ip nat filter | tab

                            PRIVATE                         PRIVATE  PRIVATE
PUBLIC  PUBLIC
NAT  NAT                    SOURCE          PRIVATE DEST    SOURCE   DEST     PUBLIC 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 40 icmp 192.168.50.5 173.37.145.84 9269 9269 192.168.109.4 173.37.145.84 9269 9269
established 0:00:00:02 10 840 10 980 -
```

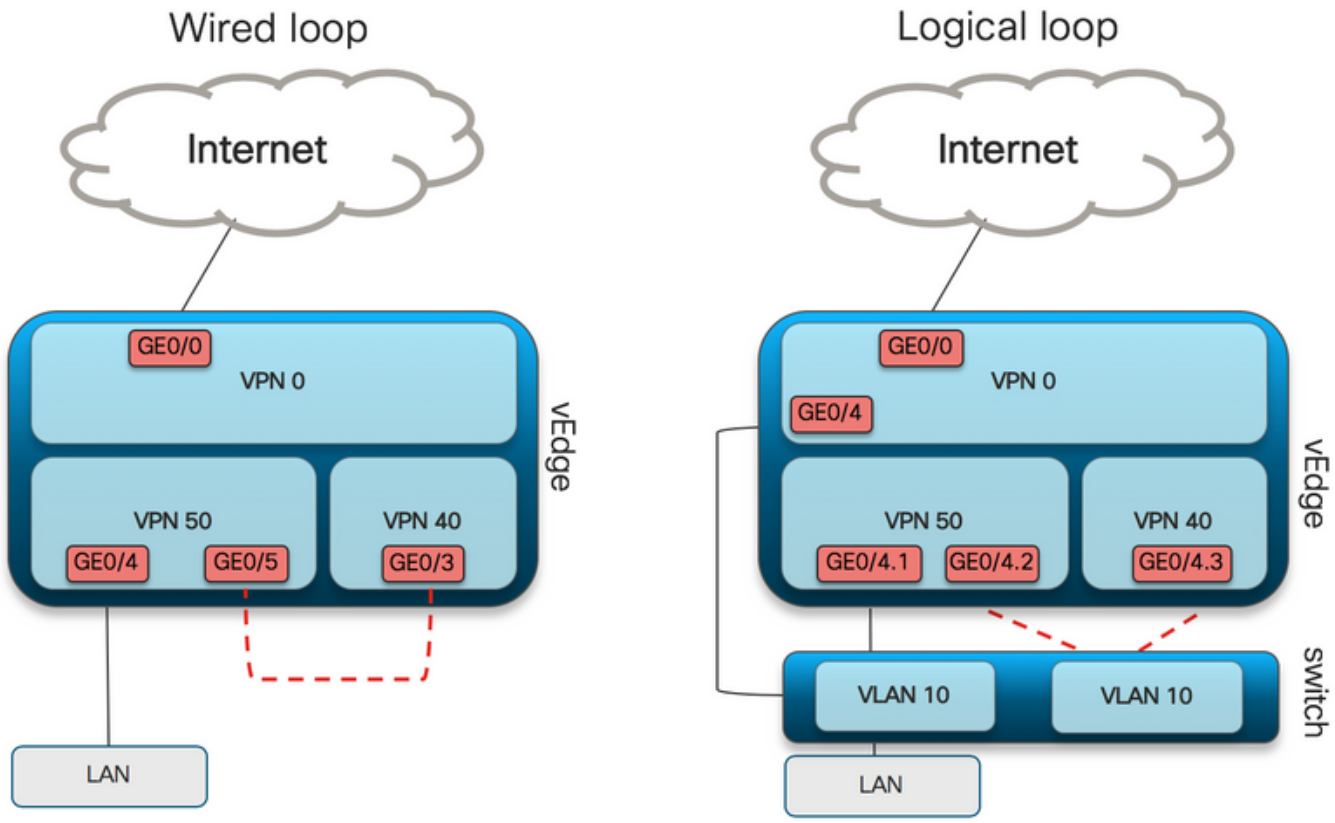
注：このソリューションでは、地域ごとに異なるEXITを使用して冗長性やロードシェアリングを編成することはできません。
IOS-XEルータでは動作しない

解決策 2：必要なGRE\IPSec\NAT Default Route to OMPを挿入します。

現時点では、vEdge1のGRE\IPSecトンネルを指すデフォルトルートを、OMPを介してvEdge2(nat route OMP protocol)にアドバタイズする可能性はありません。 今後のソフトウェアバージョンでは、動作が変化する可能性があることに注意してください。

ここでの目的は、vEdge2（DIAに推奨されるデバイス）から発信され、さらにOMPを介して伝搬される通常のスタティックデフォルトルート(**IPルート0.0.0.0/0 <ネクストホップIPアドレス>**)を作成することです。

そのために、vEdge1にダミーVPNを作成し、ケーブルで物理ポートループを行います。ダミーVPNに割り当てられたポートと、スタティックデフォルトルートを必要とする目的のVPN内のポートとの間にループが作成されます。 また、次の図に示すように、ダミーのVLANを持つスイッチに接続された1つの物理インターフェイスと、対応するVPNに割り当てられた2つのサブインターフェイスだけでループを作成できます。



次に、vEdge1の設定例を示します。

1.ダミーVPNを作成します。

```
vpn 50
 interface ge0/3
description DIA_for_region ip address 192.168.111.2/30 no shutdown ! ip route 0.0.0.0/0 vpn 0
<<<<==== NAT activated for a local DIA
 ip route 10.0.0.0/8 192.168.111.1 <<<<==== Reverse routes, pointing to loop interface GE0/3
ip route 172.16.0.0/12 192.168.111.1
ip route 192.168.0.0/16 192.168.111.1 !
```

2. NATインターフェイスを指すDIAルートがルーティングテーブルに正常に追加されたFIBを確認します。

```
vedge1# show ip route vpn 50 | i nat
50      0.0.0.0/0 nat - ge0/0 - 0 - - - F,S
```

3.通常のデフォルトルートが設定されている（OMPがアドバタイズできる）実稼働の目的で使用されるサービスVPN:

```
vpn 40
 interface ge0/4
  description CORPORATE_LAN
  ip address 192.168.40.4/24
  no shutdown
 !
 interface ge0/5
description LOOP_for_DIA ip address 192.168.111.1/30 no shutdown ! ip route 0.0.0.0/0
192.168.111.2 <<<<==== Default route, pointing to loop interface GE0/5 omp advertise connected
advertise static ! !
```

4. RIBで、ループインターフェイスをポイントするデフォルトルートがないかどうかを確認しま

す。

```
vedge1# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 static - ge0/5 192.168.111.2 - - - - F,S
```

5. vEdge1がOMP:

```
vedge1# show omp routes detail | exclude not\ set

----------------------------------------------------
omp route entries for vpn 40 route 0.0.0.0/0 <<<<==== Default route OMP entry ------------------
-------------------------------- RECEIVED FROM: peer 0.0.0.0 <<<<==== OMP route is locally
originated path-id 37 label 1002 status C,Red,R Attributes: originator 192.168.30.4 type
installed tloc 192.168.30.4, public-internet, ipsec overlay-id 1 site-id 13 origin-proto static
origin-metric 0 ADVERTISED TO: peer 192.168.30.3 Attributes: originator 192.168.30.4 label 1002
path-id 37 tloc 192.168.30.4, public-internet, ipsec site-id 13 overlay-id 1 origin-proto static
origin-metric 0
```

6.vEdge2は設定を必要とせず、デフォルトルートはvEdge1をポイントするOMP経由で受信されます

```
vedge2# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 omp - - - - 192.168.30.4 public-internet ipsec F,S
```

7. 173.37.145.84への到達可能性を確認します。

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=2 ttl=62 time=0.518 ms
64 bytes from 173.37.145.84: icmp_seq=5 ttl=62 time=0.604 ms
^C
--- 192.168.109.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.518/0.563/0.604/0.032 ms
```

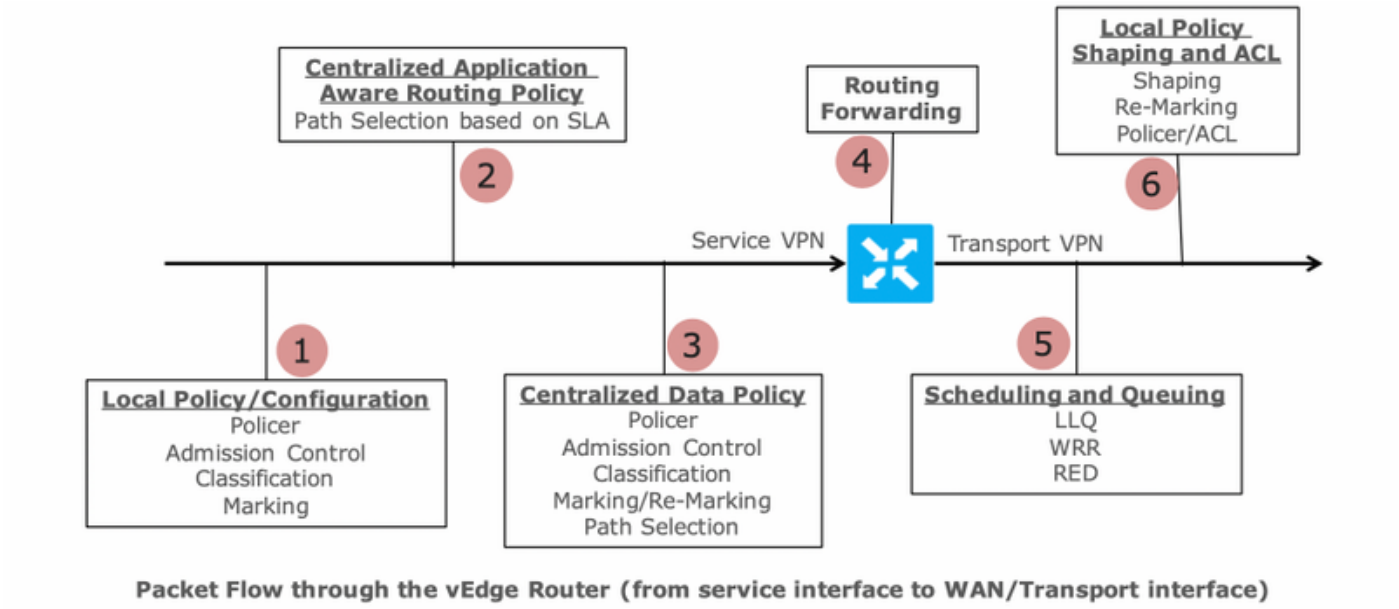
注：このソリューションを使用すると、地域ごとに異なるEXITを使用して冗長性やロードシェアリングを編成できます。

IOS-XEルータでは動作しない

解決策 3：DIAに中央集中型データポリシーが使用されている場合、OMPにデフォルトルートを挿入します。

ローカルDIAに集中型のデータポリシーが使用されている場合は、デフォルトルートを挿入する方法として考えられますが、このスタティックデフォルトルートの使用であるDIAを持つ地域デバイスを指します。**ip route 0.0.0.0/0 Null0**。

内部パケットフローにより、ブランチから到達したトラフィックはデータポリシーによりDIAに到達し、Null0へのルートには到達しません。ここからわかるように、ネクストホップ検索はポリシーの展開後にのみ行われます。



Packet Flow through the vEdge Router (from service interface to WAN/Transport interface)

vEdge2には、vEdge1やその他のサイトとのデータプレーントンネルが確立されています（フルメッシュ形式の接続）。 特別な設定は必要ありません。

vEdge1には、一元化されたデータポリシーでDIAが設定されています。

ここでは、vEdge1の設定手順について説明します。

1.トランスポートインターフェイスでネットワークアドレス変換(NAT)をアクティブにします。ここで、DIAを使用します。

```
vpn 0
 !
 interface ge0/0
  description "DIA interface"
  ip address 192.168.109.4/24
 nat <<<<==== NAT activated for a local DIA !
```

2.サービスVPNにスタティックルート**ip route 0.0.0.0/0 null0を追加**し、デフォルトをブランチにアドバタイズします。

```
vpn 40
 interface ge0/4
  ip address 192.168.40.4/24
  no shutdown
 !
 ip route 0.0.0.0/0 null0     <<<<==== Static route to null0 that will be advertised to branches
via OMP !
```

3. RIBにデフォルトルートが含まれているかどうかを確認します。

```
vedge1# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 static - - - 0 - - - B,F,S
```

4. vEdge1がOMP:

```
vedge1# show omp routes detail | exclude not\ set
```

```
-------------------------------------------------
omp route entries for vpn 40 route 0.0.0.0/0 <<<<==== Default route OMP entry ------------------
-------------------------------- RECEIVED FROM: peer 0.0.0.0 <<<<==== OMP route is locally
originated path-id 37 label 1002 status C,Red,R Attributes: originator 192.168.30.4 type
installed tloc 192.168.30.4, public-internet, ipsec overlay-id 1 site-id 13 origin-proto static
origin-metric 0 ADVERTISED TO: peer 192.168.30.3 Attributes: originator 192.168.30.4 label 1002
path-id 37 tloc 192.168.30.4, public-internet, ipsec site-id 13 overlay-id 1 origin-proto static
origin-metric 0
```

5. vEdge1にポリシーが存在せず、DIAが有効になっていないことを確認します。

```
vedge1# show policy from-vsmart
% No entries found.
```

6. Forwarding Information Base(FIB)プログラミングをチェックします。DIAが有効でない場合、インターネット上の宛先のルート不在(Blackhole)が表示されます。

```
vedge1# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.40.4 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Blackhole
```

DIAのvSmart中央集中型データポリシー設定：

```
policy
 data-policy DIA_vE1
  vpn-list VPN_40
   sequence 5
    match
     destination-data-prefix-list ENTERPRISE_IPs
    action accept
   sequence 10
    action accept
     nat-use vpn0             <<<<==== NAT reference for a DIA default-action accept lists
vpn-list VPN_40    vpn 40   data-prefix-list ENTERPRISE_IPs    ip-prefix 10.0.0.0/8    ip-prefix
172.16.0.0/12    ip-prefix 192.168.0.0/16
site-list SITE1
site-id 1001 apply-policy site-list SITE1 <<<<==== policy applied to vEdge1 data-policy DIA_vE1
from-service
```

vSmartの設定のapply-policyセクションでvSmart data-policyを適用するか、vManage GUIでアクティブにします。

7. vEdge1がvSmartからデータポリシーを正常に受信したことを確認します。

```
vedge1# show policy from-vsmart
from-vsmart data-policy DIA_vE1
 direction from-service
 vpn-list VPN_40
  sequence 5
   match
    destination-data-prefix-list ENTERPRISE_IPs
   action accept
  sequence 10
   action accept
nat-use vpn0 default-action accept from-vsmart lists vpn-list VPN_40 vpn 40 from-vsmart lists
data-prefix-list ENTERPRISE_IPs ip-prefix 10.0.0.0/8 ip-prefix 172.16.0.0/12    ip-prefix
192.168.0.0/16
```

8.インターネット上の宛先に対して可能なルートを示すForwarding Information Base(FIB)プログ

ラミングをチェックします。

```
vedge1# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.40.4 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Remote
Remote IP:173.37.145.84, Interface ge0/0 Index: 4
```

9.インターネット上の宛先への到達可能性を確認します。

```
vedge1# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.192 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.246 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.236 ms ^C --- 173.37.145.84 ping
statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2000ms rtt
min/avg/max/mdev = 0.245/0.221/0.192/0.021 ms
```

vEdge2検証手順：

1.デフォルトルートが正常に受信され、RIBにインストールされたことを確認します。

```
vEdge2# sh ip route vpn 40 | include 0.0.0.0
40     0.0.0.0/0           omp              -         -           -                -
192.168.30.4   biz-internet     ipsec  F,S
40 0.0.0.0/0 omp - - - - 192.168.30.4 public-internet ipsec F,S
```

2.インターネット上の宛先に対して可能なルートを示すForwarding Information Base(FIB)プログラミングをチェックします。

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 4
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.110.6 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.110.6 12346 Color: public-internet
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.109.4 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.109.4 12346 Color: public-internet
```

3.インターネット上の宛先への到達可能性を確認します。

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.382 ms
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.392 ms 64 bytes from 173.37.145.84:
icmp_seq=3 ttl=63 time=0.346 ms ^C --- 173.37.145.84 ping statistics --- 3 packets transmitted,
3 received, 0% packet loss, time 2000ms rtt min/avg/max/mdev = 0.392/0.361/0.346/0.023 ms
```

4. DIAが動作していること、およびNAT変換でvEdge2から173.37.145.84へのインターネット制御メッセージプロトコル(ICMP)セッションを確認できることを確認します

```
vedge1# show ip nat filter | tab
```

```
                              PRIVATE                         PRIVATE   PRIVATE
PUBLIC   PUBLIC
NAT   NAT                     SOURCE          PRIVATE DEST    SOURCE    DEST      PUBLIC 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 40 icmp 192.168.50.5 173.37.145.84 9175 9175 192.168.109.4 173.37.145.84 9175 9175
established 0:00:00:04 18 1440 18 1580 -
```

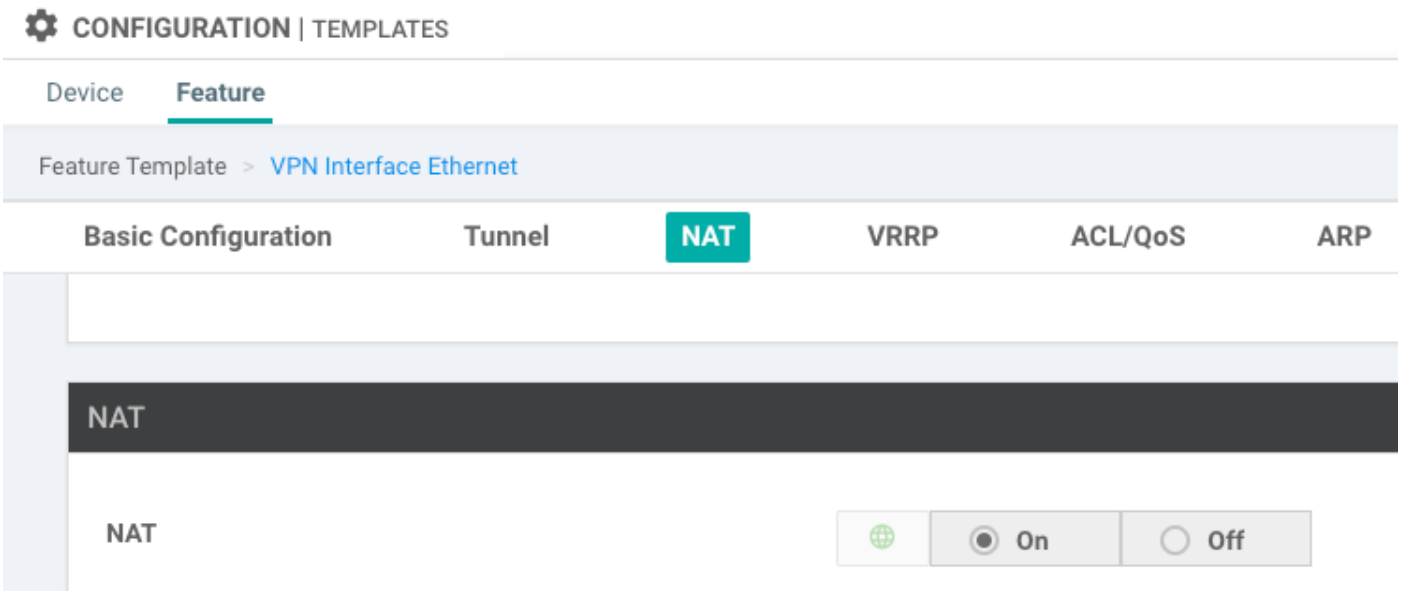
注：このソリューションを使用すると、様は、地域ごとに異なるEXITを使用して冗長性やロードシェアリングを編成できます。
IOS-XEルータでは動作しない

解決 4:ローカルDIA使用時にデフォルトルートをOMPに挿入します。

このソリューションは、IOS-XEおよびViptela OSベースのSD-WANルータの両方に使用できます。

簡単に説明すると、このソリューションでは、DIA(0.0.0.0/0 Null0)のデフォルトルートが、Null0を指す2つのサブネットワーク0.0.0.0/1と128.0.0.0/1に分割されます。この手順は、ブランチにアドバタイズするデフォルトルートと、ローカルDIAに使用されるルートののの重複をを回避します。DIAに使用されるIOS-XEルートのアドミニストレーティブディスタンス(AD)は6ですが、スタティックデフォルトのADは1です。解決策は、地域DIAが2つの異なる場所に設定されている場合に冗長スキーマを使用できることです。

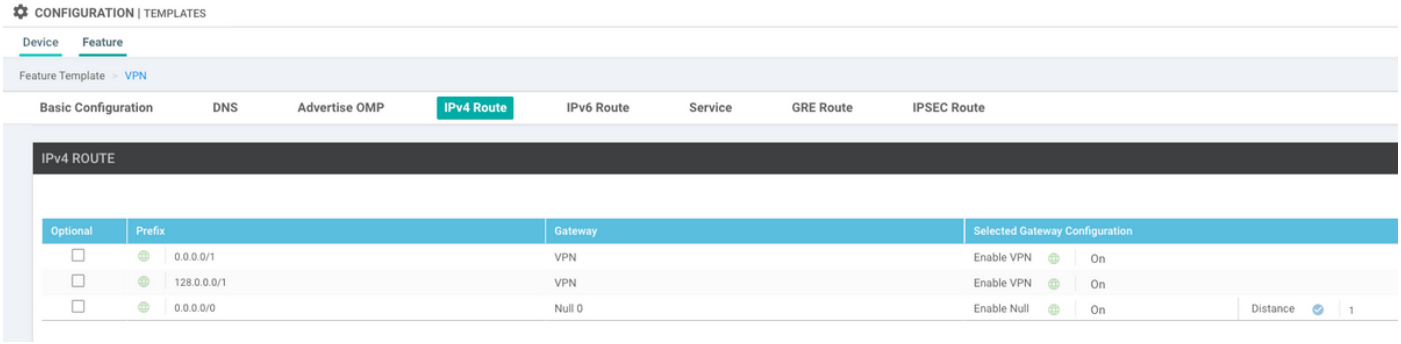
1.トランスポートインターフェイスでNATをアクティブにする



2.サービスVPNの機能テンプレートで、DIAを使用する必要がある場合は、次のスタティックIPv4ルートを追加します。

- 0.0.0.0/1およびVPNを指す128.0.0.0/1これらのルートはDIAに使用されます

- 0.0.0.0/0がNull 0をポイントしています。このルートは、OMP経由でブランチにアドバタイズするために使用されます（ソリューション3と同様）。



3.ルートがRIBに正常に追加されたことを確認します。

```
cedge1#show ip route vrf 40

Routing Table: 40
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP,  D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type
1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA, i - IS-IS, su - IS-IS summary,
L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route, o - ODR, P -
periodic downloaded static route, H - NHRP, l - LISP
       a - application route, + - replicated route, % - next hop override, p - overrides from
PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Null0                          <<<<==== Static route to null0
that will be advertised to branches via OMP n Nd 0.0.0.0/1 [6/0], 00:08:23, Null0 <<<<==== DIA
route n Nd 128.0.0.0/1 [6/0], 00:08:23, Null0 <<<<==== DIA route 192.40.1.0/32 is subnetted, 1
subnets m 192.40.1.1 [251/0] via 192.168.30.207, 3d01h 192.40.2.0/32 is subnetted, 1 subnets m
192.40.2.1 [251/0] via 192.168.30.208, 3d01h
```

4. DIAがローカルで正常に動作していることを確認します。

```
cedge1#ping vrf 40 173.37.145.84
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.84, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

5.デフォルトルートがブランチに正常にアドバタイズされ、RIBにインストールされていることを確認します

```
cedge3#show ip route vrf 40

Routing Table: 40
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP
external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type
1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA, i - IS-IS, su - IS-IS summary,
L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route, o - ODR, P -
periodic downloaded static route, H - NHRP, l - LISP
       a - application route, + - replicated route, % - next hop override, p - overrides from
PfR
```

```
Gateway of last resort is 192.168.30.204 to network 0.0.0.0

m*    0.0.0.0/0 [251/0] via 192.168.30.204, 00:02:45    <<<<==== Default route that advertised
via OMP 192.40.1.0/32 is subnetted, 1 subnets m 192.40.11.1 [251/0] via 192.168.30.204, 00:02:45
192.40.13.0/32 is subnetted, 1 subnets C 192.40.13.1 is directly connected, Loopback40
```

6. DIAがローカルで正常に動作していることを確認します。

```
cedge3#ping vrf 40 173.37.145.84
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.84, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

7. Regional DIAルータでNAT変換が成功したことを確認します。

```
cedge1#show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
icmp 192.168.109.204:1     192.40.13.1:1         173.37.145.84:1       173.37.145.84:1
Total number of translations: 1
```

注：このソリューションを使用すると、様は、地域ごとに異なるEXITを使用して冗長性やロードシェアリングを編成できます。

注： CSCvr72329 – 拡張要求「NAT route redistribution to OMP」

関連情報

- **一元化されたデータポリシー**
- **集中型データポリシーの設定**
- **一元化されたデータポリシーの設定例**
- **OMPルーティングプロトコル**
- **OMPの設定**