

如何选择特定站点作为首选地区互联网分组？

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[解决方案 1：用于更改下一跳的集中数据策略使用。](#)

[解决方案 2：需要注入GRE/IPSec\NAT Default Route to OMP。](#)

[解决方案 3：当用于DIA的集中数据策略时，插入到OMP的默认路由。](#)

[解决方案 4：使用本地DIA时，插入到OMP的默认路由。](#)

[相关信息](#)

简介

本文档介绍如何配置SD-WAN交换矩阵，以便借助直接互联网接入(DIA)和集中式数据策略将特定分支机构vEdge配置为首选区域互联网分支。此解决方案在以下情况下非常有用：例如，当区域站点使用Zscaler®等集中服务，并应用作首选的互联网出口点时。此类部署需要从传输VPN配置通用路由封装(GRE)或互联网协议安全(IPSec)隧道，且数据流与常规DIA解决方案不同，后者的流量直接到达互联网。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解SD-WAN策略框架。

使用的组件

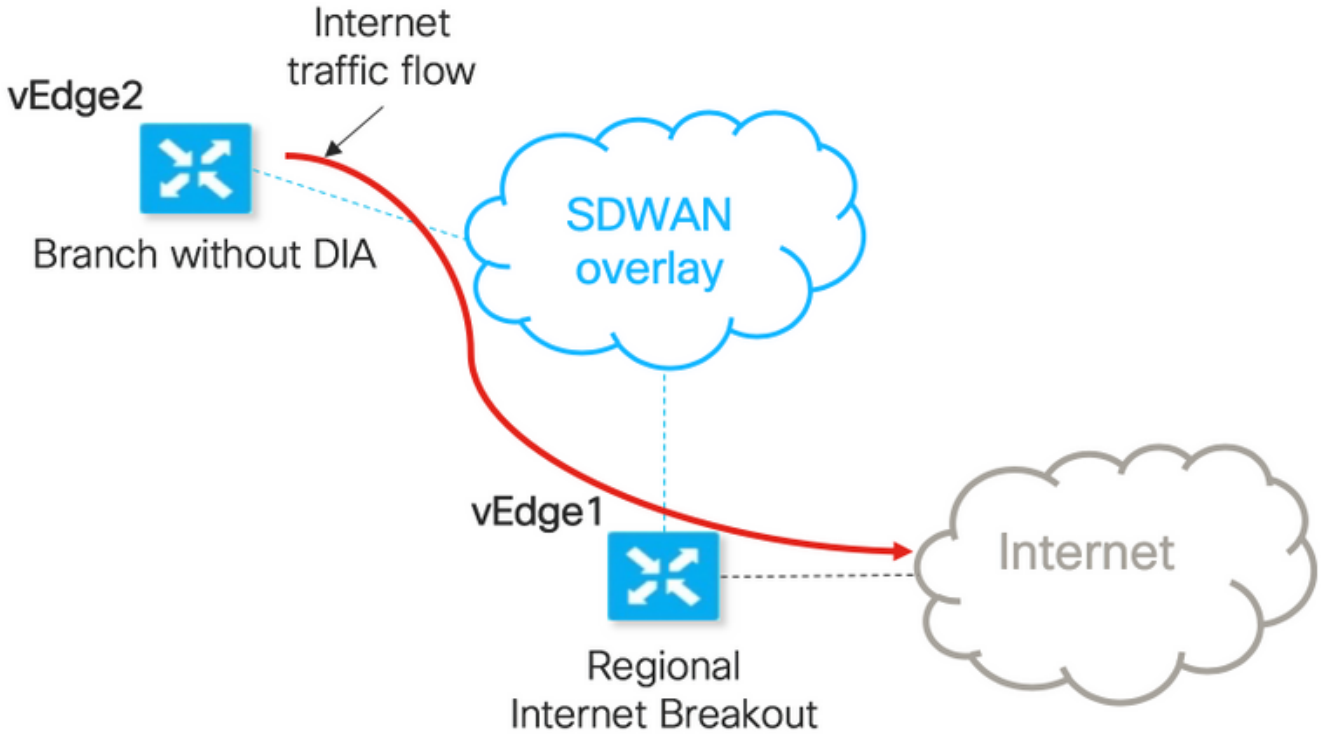
本文档中的信息基于以下软件和硬件版本：

- vEdge路由器
- 带18.3.5软件版本的vSmart控制器。

背景信息

来自vEdge2的应到达互联网的服务VPN流量会使用数据平面隧道转发到另一个分支vEdge1。vEdge1是DIA配置用于本地互联网分支的路由器。

网络图



主机名	vEdge1	vEdge2
主机角色	具有DIA (区域互联网分支) 的分支机构设备	未配置DIA的分支设备
VPN 0		
传输位置(TLOC)1	biz-internet , ip:192.168.110.6/24	biz-internet , ip:192.168.110.5/24
传输位置(TLOC)2	公共互联网、ip: 192.168.109.4/24	公共互联网、ip: 192.168.109.5/24
服务VPN 40	接口ge0/1,ip: 192.168.40.4/24	接口ge0/2,ip:192.168.50.5/24

配置

解决方案 1：用于更改下一跳的集中数据策略使用。

vEdge2与vEdge1和其他站点建立了数据平面隧道 (全网状连接)

vEdge1的DIA配置了ip route 0.0.0.0/0 vpn 0。

vSmart集中式数据策略配置：

```
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 — 不需要任何特殊配置。

在此，您可以找到在正确应用策略时执行验证的步骤。

1.检查vEdge2中是否不存在策略：

```

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

```

2.检查转发信息库(FIB)编程。它应显示Internet上目标的路由缺失（黑洞）：

```

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.在vSmart配置的apply-policy部分下应用vSmart数据策略，或在vManage GUI中激活。

4.检查vEdge2是否成功从vSmart接收了数据策略：

```

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.检查转发信息库(FIB)编程，该编程显示Internet上目的地的可能路由：

```

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. 确认到Internet上目的地的连通性：

```

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

```

在此，您可以找到vEdge1配置步骤。

1. 在应使用DIA的传输接口上激活网络地址转换(NAT):

```

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

```

2. 在服务VPN中添加静态路由ip route 0.0.0.0/0 vpn 0以激活DIA:

```

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. 检查RIB是否包含NAT路由：

```

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

```

4. 确认DIA工作正常，在NAT转换中，我们可以看到从vEdge2到173.37.145.84的Internet控制消息协议(ICMP)会话

```
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
ADDRESS	PORT	PORT	STATE	TIMEOUT	PACKETS	OCTETS	PACKETS	OCTETS

```

-----
-----
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 -

```

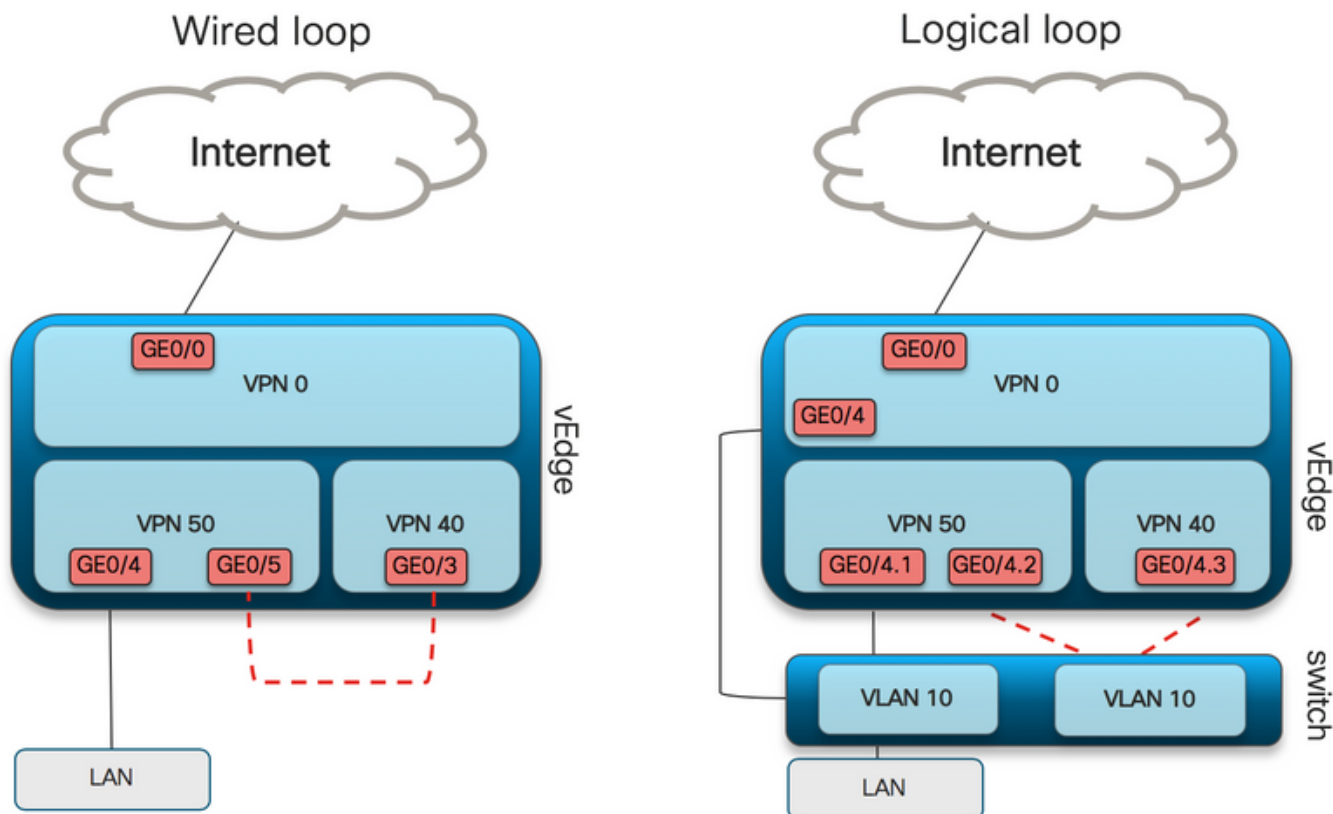
注意：此解决方案不允许我们使用不同区域退出使用情况组织冗余或负载共享。
不适用于IOS-XE路由器

解决方案 2：需要注入GRE\IPSec\NAT Default Route to OMP。

到目前为止，不可能获取指向vEdge1上GRE\IPSec隧道的默认路由，通过OMP通告到vEdge2(redistribute nat route OMP protocol)。请注意，行为在未来软件版本中可能会改变。

我们的目标是创建一条常规静态默认路由(IP route 0.0.0.0/0 <下一跳IP地址>)，该路由可由vEdge2 (DIA首选设备) 发起，并通过OMP进一步传播。

为此，在vEdge1上创建虚拟VPN，并使用电缆执行物理端口环路。在分配给虚拟VPN的端口和需要静态默认路由的所需VPN中的端口之间创建环路。此外，您还可以创建一个环路，该环路仅包含一个物理接口，该接口连接到交换机，带有虚拟VLAN，两个子接口分配给下图中的相应VPN:



在这里，您可以找到vEdge1配置示例。

1.创建虚拟VPN:

```

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.检查FIB , DIA路由 (指向NAT接口) 已成功添加到路由表 :

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

3.用于生产目的的服务VPN , 其中配置了常规默认路由 (OMP将能够通告该路由) :

```
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.检查RIB是否存在指向环路接口的默认路由 :

```
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.检查vEdge1是否通过OMP通告了默认路由 :

```
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不需要任何配置 , 默认路由通过指向vEdge1的OMP接收

```
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.确认到173.37.145.84的可接通性 :

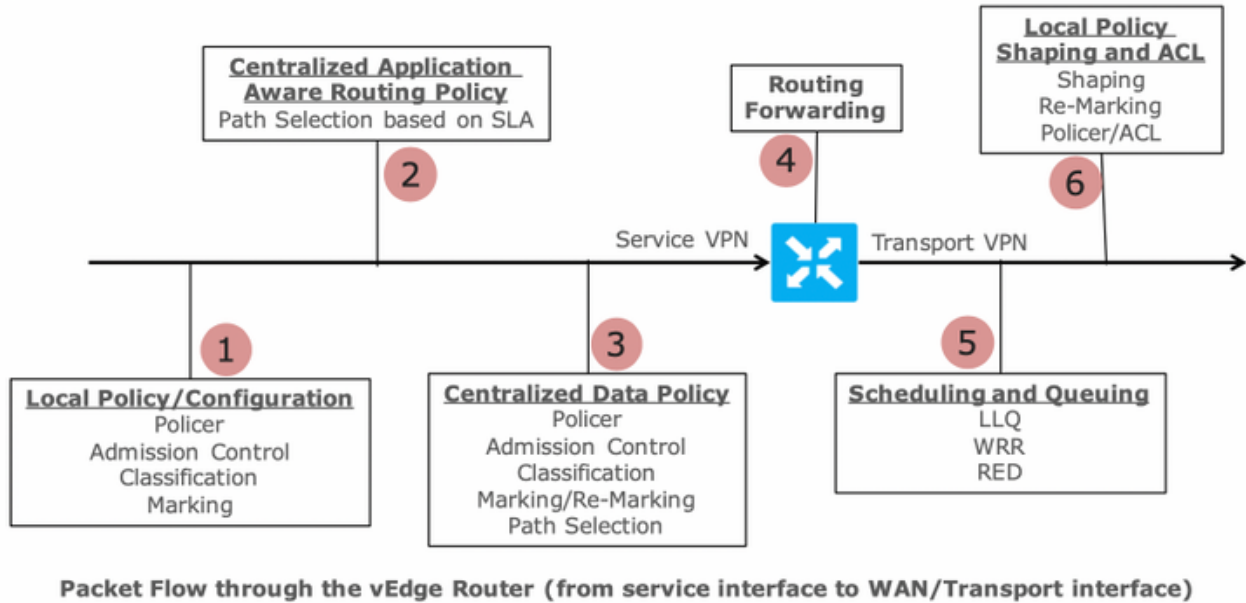
```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=2 ttl=62 time=0.518 ms
64 bytes from 173.37.145.84: icmp_seq=5 ttl=62 time=0.604 ms
^C
--- 192.168.109.5 ping statistics ---
2 packets transmitted, 2 received,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

注意：此解决方案允许您组织冗余或负载共享，并使用不同的区域出口使用情况。
不适用于IOS-XE路由器

解决方案 3：当用于DIA的集中数据策略时，插入到OMP的默认路由。

当集中式数据策略用于本地DIA时，它指向具有DIA的区域设备，该设备使用此静态默认路由：**ip route 0.0.0.0/0 Null0**。

由于内部数据包流，从分支机构到达的流量通过数据策略到达DIA，并且从不到达Null0的路由。如此处所示，下一跳查找仅在策略部署后发生。



vEdge2与vEdge1和其他站点建立了数据平面隧道（全网状连接）。它不需要任何特殊配置。

vEdge1的DIA配置了集中数据策略。

在此，您可以找到vEdge1配置步骤。

1.在应使用DIA的传输接口上激活网络地址转换(NAT):

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

2.在服务VPN中添加静态路由ip route 0.0.0.0/0 null0，将默认路由通告给分支机构：

```
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.检查RIB是否包含默认路由：

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

4.检查vEdge1是否通过OMP通告了默认路由：

```
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.检查vEdge1上是否没有策略，以及DIA是否未启用：

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

6.检查转发信息库(FIB)编程。它应显示Internet上目标的路由缺失（黑洞），因为DIA未启用：

```
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的vSmart集中式数据策略配置：

```
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
```

在vSmart配置的apply-policy部分下应用vSmart数据策略，或在vManage GUI中激活。

7.检查vEdge1是否成功从vSmart接收了数据策略：

```
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.检查转发信息库(FIB)编程，该编程显示Internet上目的地的可能路由：

```
vedgel# 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.确认到Internet上目的地的连通性：

```
vedgel# 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验证步骤：

1.确认已成功接收默认路由并将其安装到RIB中：

```
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.检查转发信息库(FIB)编程，该编程显示Internet上目的地的可能路由：

```
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.确认到Internet上目的地的连通性：

```
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.确认DIA工作正常，在NAT转换中，我们可以看到从vEdge2到173.37.145.84的Internet控制消息协议(ICMP)会话

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

```
          PRIVATE                               PRIVATE PRIVATE
PUBLIC PUBLIC
NAT NAT
PUBLIC DEST SOURCE DEST FILTER PRIVATE DEST SOURCE DEST PUBLIC SOURCE
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 -
```

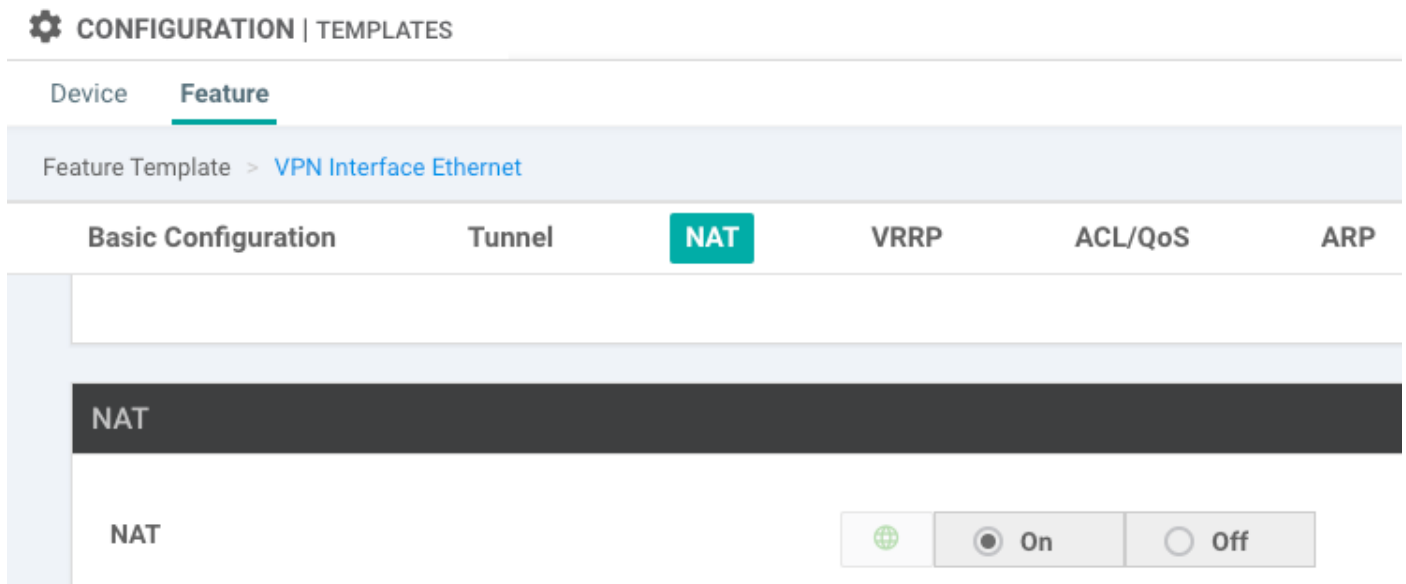
注意：此解决方案允许组织冗余或负载共享，并使用不同的区域出口使用情况。
不适用于IOS-XE路由器

解决方案 4：使用本地DIA时，插入到OMP的默认路由。

此解决方案可同时用于基于IOS-XE和Viptela OS的SD-WAN路由器。

简而言之，在此解决方案中，DIA的默认路由(0.0.0.0/0 Null0)被拆分为指向Null0的两个子网0.0.0.0/1和128.0.0.0/1。此步骤是为了避免将应通告给分支的默认路由和用于本地DIA的默认路由重叠。在用于DIA的IOS-XE路由中，管理距离(AD)等于6，而静态默认的AD为1。该解决方案的优点是当区域DIA配置在两个不同位置时，能够使用冗余方案。

1.在传输接口上激活NAT



The screenshot shows the configuration page for a VPN interface in Viptela OS. The breadcrumb path is "Feature Template > VPN Interface Ethernet". The "NAT" tab is selected among other tabs like "Basic Configuration", "Tunnel", "VRRP", "ACL/QoS", and "ARP". In the left sidebar, "NAT" is highlighted. At the bottom right, there is a toggle switch for "NAT" which is currently turned "On".

2.在服务VPN的功能模板中，应使用DIA添加以下静态IPv4路由：

- 0.0.0.0/1和128.0.0.0/1指向VPN。这些路由用于DIA
- 0.0.0.0/0指向Null 0。此路由用于通过OMP通告到分支机构（类似于解决方案3）

IPv4 ROUTE			
Optional	Prefix	Gateway	Selected Gateway Configuration
<input type="checkbox"/>	0.0.0.0/1	VPN	Enable VPN On
<input type="checkbox"/>	128.0.0.0/1	VPN	Enable VPN On
<input type="checkbox"/>	0.0.0.0/0	Null 0	Enable Null On
			Distance 1

3.检查路由是否已成功添加到RIB:

```
cedgel#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.检查DIA在本地是否运行良好:

```
cedgel#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.检查默认路由是否成功通告到分支并安装在RIB中

```
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.检查DIA在本地是否运行良好：

```
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.检查区域DIA路由器是否成功进行NAT转换。

```
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
```

注意：此解决方案允许组织冗余或负载共享，并使用不同的区域出口使用情况。

注意： [CSCvr72329 — 增强请求“NAT路由重分发到OMP”](#)

相关信息

- [集中数据策略](#)
- [配置集中数据策略](#)
- [集中数据策略配置示例](#)
- [OMP路由协议](#)
- [配置OMP](#)