Como selecionar um site específico para ser uma reunião à parte da Internet regional preferida?

Contents

Introduction

Este documento descreve como configurar a malha SD-WAN para configurar um vEdge de filial específico como a divisão regional de Internet preferida com a ajuda do Direct Internet Access (DIA) e da política de dados centralizada. Essa solução pode ser útil no caso, por exemplo, de um site regional usar algum serviço centralizado, como o Zscaler®, e ser usado como um ponto de saída preferencial da Internet. Essa implantação exige que túneis Generic Routing Encapsulation (GRE) ou Internet Protocol Security (IPSec) sejam configurados a partir de uma VPN de transporte e o fluxo de dados é diferente da solução DIA regular, onde o tráfego chega diretamente à Internet.

Prerequisites

Requirements

A Cisco recomenda ter conhecimento deste tópico:

- Entendimento básico da SD-WAN Policy Framework.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

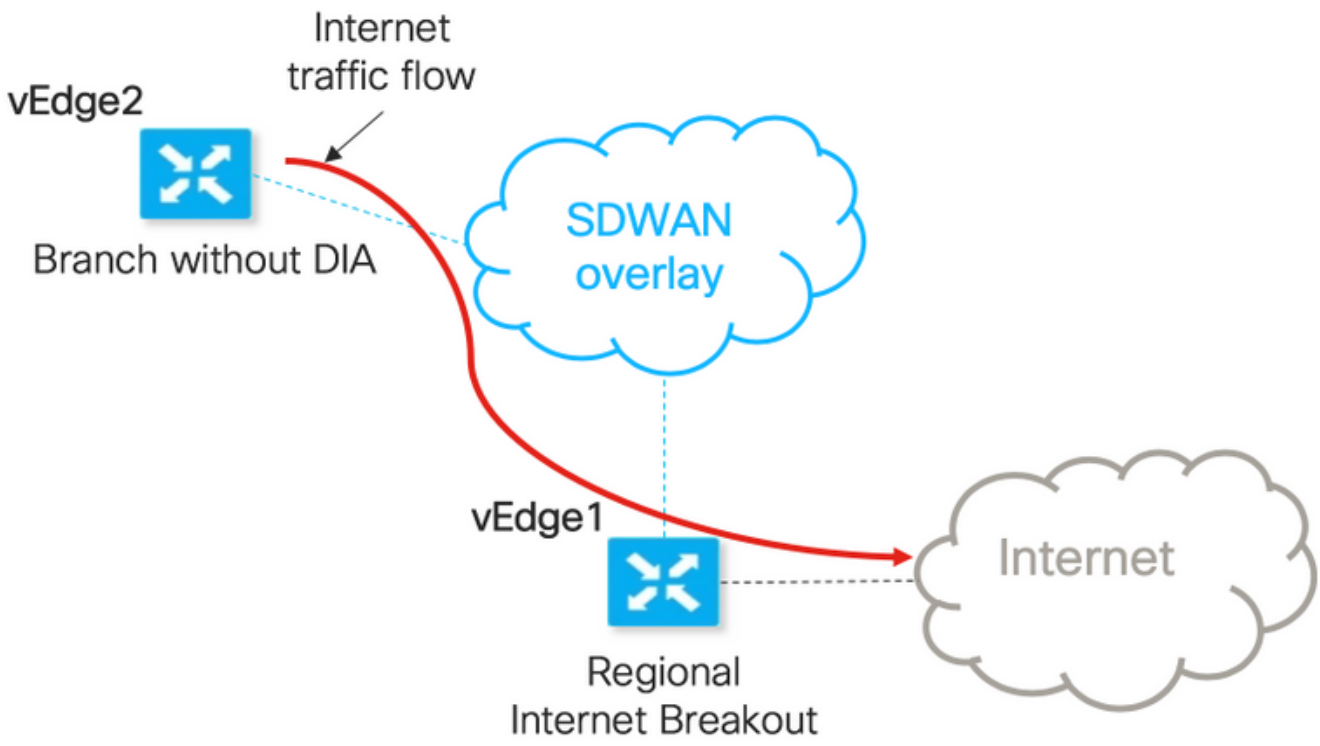
- Roteadores vEdge

- vSmart Controller com versão de software 18.3.5.

Informações de Apoio

O tráfego de VPN de serviço do vEdge2, que deve chegar à Internet, é encaminhado para outro vEdge1 de filial, usando túneis de plano de dados. vEdge1 é o roteador no qual o DIA foi configurado para breakout de Internet local.

Diagrama de Rede



Nome do host	vEdge1	vEdge2
Função de host	Dispositivo de filial com DIA (Internet breakout regional)	Dispositivo de filial sem DIA configurado
VPN 0		
Locais de transporte (TLOC) 1	biz-internet, ip: 192.168.110.6/24	biz-internet, ip: 192.168.110.5/24
Locais de transporte (TLOC) 2	internet pública, ip: 192.168.109.4/24	internet pública, ip: 192.168.109
VPN de serviço 40	Interface ge0/1, ip: 192.168.40.4/24	Interface ge0/2, ip: 192.168.50.5

Configurações

Solução 1: Uso centralizado da política de dados para alterar o próximo salto.

O vEdge2 tem um túnel de plano de dados estabelecido com o vEdge1 e outros sites (conectividade em estilo de malha completa)

vEdge1 tem DIA configurado com **ip route 0.0.0.0/0 vpn 0**.

Configuração da política de dados centralizada vSmart:

```
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 - não exige nenhuma configuração especial.

Aqui você pode encontrar as etapas para executar a verificação se uma política foi aplicada corretamente.

1. Verifique se a política está ausente do vEdge2:

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

2. Verifique a programação da Base de Informações de Encaminhamento (FIB). Deve mostrar a ausência da rota (Blackhole) para o destino na Internet:

```
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. Aplique a política de dados do vSmart na seção **apply-policy** da configuração do vSmart ou ative na GUI do vManage.

4. Verifique se o vEdge2 recebeu com êxito a política de dados do vSmart:

```
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. Verifique a programação da Base de Informações de Encaminhamento (FIB), que mostra as possíveis rotas para o destino na Internet:

```
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. Confirme a acessibilidade ao destino na Internet:

```
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
```

Aqui você pode encontrar as etapas de configuração do vEdge1.

1. Ative a Network Address Translation (NAT) na interface de transporte, onde o DIA deve ser usado:

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

2. Adicione a rota estática **ip route 0.0.0.0/0 vpn 0** em uma VPN de serviço para ativar o 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. Verifique se o RIB contém a rota NAT:

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

4. Confirme se o DIA funciona e podemos ver a sessão Internet Control Message Protocol (ICMP) para 173.37.145.84 a partir do vEdge2 em conversões NAT

```
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 -
```

Note: Esta solução não nos permite organizar redundância ou compartilhamento de carga com diferentes saídas regionais.

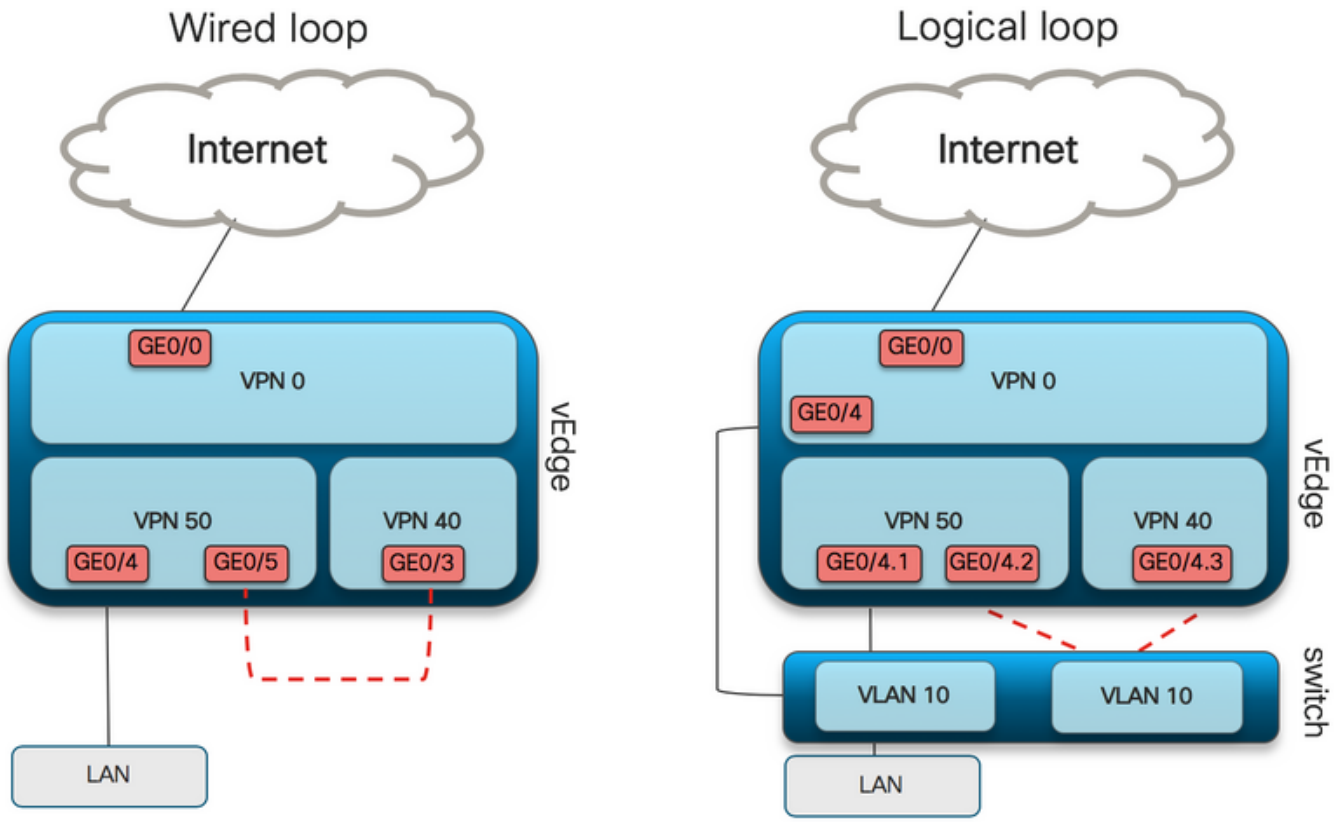
Não funciona com roteadores IOS-XE

Solução 2: Injeção necessária GRE\IPSec\NAT Default Route to OMP.

A partir de agora, não há possibilidade de obter a rota padrão, apontando para o túnel GRE\IPSec no vEdge1, a ser anunciada por meio de OMP para vEdge2 (redistribuir o protocolo de OMP de rota nat). Observe que o comportamento pode mudar em versões futuras do software.

Nosso objetivo é criar uma rota padrão estática regular (**rota IP 0.0.0.0/0 <endereço IP do próximo salto>**) que possa ser originada pelo vEdge2 (dispositivo preferido para DIA) e propagada ainda mais via OMP.

Para isso, a VPN fictícia é criada no vEdge1 e um loop de porta física é executado com cabo. O loop é criado entre as portas atribuídas à VPN fictícia e a porta na VPN desejada, o que exige uma rota padrão estática. Além disso, você pode criar um loop com apenas uma interface física conectada ao switch com VLAN fictícia e duas subinterfaces atribuídas às VPNs correspondentes na figura abaixo:



Aqui você pode encontrar o exemplo de configuração do vEdge1.

1. Crie uma VPN fictícia:

```
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. Verifique se a rota DIA, que aponta para a interface NAT, foi adicionada com êxito à tabela de roteamento:

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

3. VPN de serviço usada para fins de produção, onde a rota padrão regular é configurada (qual OMP será capaz de anunciar):

```
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. Verifique o RIB quanto à presença da rota padrão que aponta para a interface de loop:

```
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. Verifique se o vEdge1 anunciou a rota padrão via 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. O vEdge2 não exige nenhuma configuração, a rota padrão é recebida via OMP, que aponta para o vEdge1

```
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. Confirme a acessibilidade para 173.37.145.84:

```
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
```

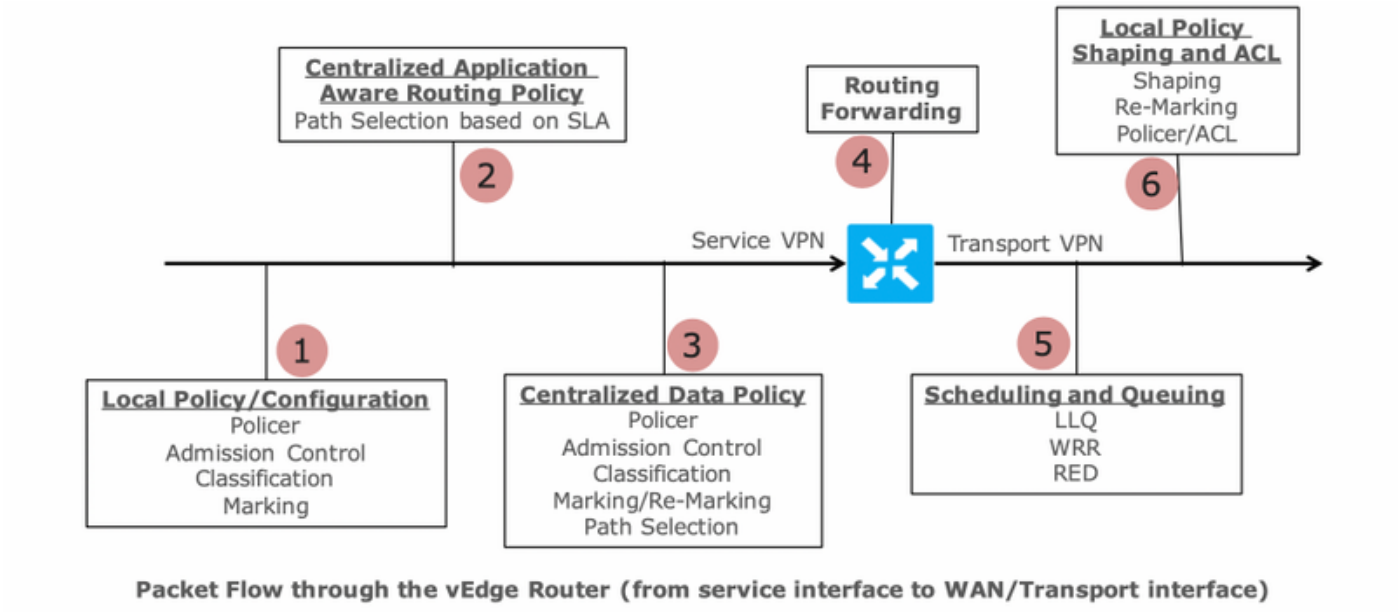
Note: Essa solução permite organizar a redundância ou o compartilhamento de carga com diferentes saídas regionais.

Não funciona com roteadores IOS-XE

Solução 3: Injete a rota padrão para OMP quando a política de dados centralizada for usada para DIA.

Quando a política de dados centralizada é usada para o DIA local, a maneira possível de injetar a rota padrão, ela aponta para um dispositivo regional com o DIA que é o uso dessa rota padrão estática: **ip route 0.0.0.0/0 Null0**.

Devido ao fluxo de pacotes internos, o tráfego que chega das filiais alcança o DIA graças à política de dados e nunca alcança a rota Null0. Como você pode ver aqui, a pesquisa do próximo salto acontece somente após uma implantação de política.



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

O vEdge2 tem um túnel de plano de dados estabelecido com o vEdge1 e outros sites (conectividade em estilo full-mesh). Não exige nenhuma configuração especial.

O vEdge1 tem o DIA configurado com política de dados centralizada.

Aqui você pode encontrar as etapas de configuração do vEdge1.

1. Ative a Network Address Translation (NAT) na interface de transporte, onde o DIA deve ser usado:

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

2. Adicione a rota estática **ip route 0.0.0.0/0 null0** em uma VPN de serviço para anunciar o padrão às filiais:

```
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. Verifique se o RIB contém a rota padrão:

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

4. Verifique se o vEdge1 anunciou a rota padrão via 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. Verifique se a política está ausente no vEdge1 e se o DIA não está habilitado:

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

6. Verifique a programação da Base de Informações de Encaminhamento (FIB). Ele deve mostrar a ausência da rota (Blackhole) para o destino na Internet, pois o DIA não está ativado:

```
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
```

Configuração de política de dados centralizada vSmart para DIA:

```
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
```

Aplique a política de dados do vSmart na seção **apply-policy** da configuração do vSmart ou ative na GUI do vManage.

7. Verifique se o vEdge1 recebeu com êxito a política de dados do vSmart:

```
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. Verifique a programação da Base de Informações de Encaminhamento (FIB), que mostra as

possíveis rotas para o destino na Internet:

```
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. Confirme a acessibilidade ao destino na Internet:

```
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
```

Etapas de verificação do vEdge2:

1. Confirme se a rota padrão foi recebida e instalada com êxito no RIB:

```
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. Verifique a programação da Base de Informações de Encaminhamento (FIB), que mostra as possíveis rotas para o destino na Internet:

```
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. Confirme a acessibilidade ao destino na Internet:

```
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. Confirme se o DIA funciona e podemos ver a sessão Internet Control Message Protocol (ICMP) para 173.37.145.84 a partir do vEdge2 em conversões NAT

```
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 -
```

Note: Essa solução permite organizar a redundância ou o compartilhamento de carga com diferentes saídas regionais.

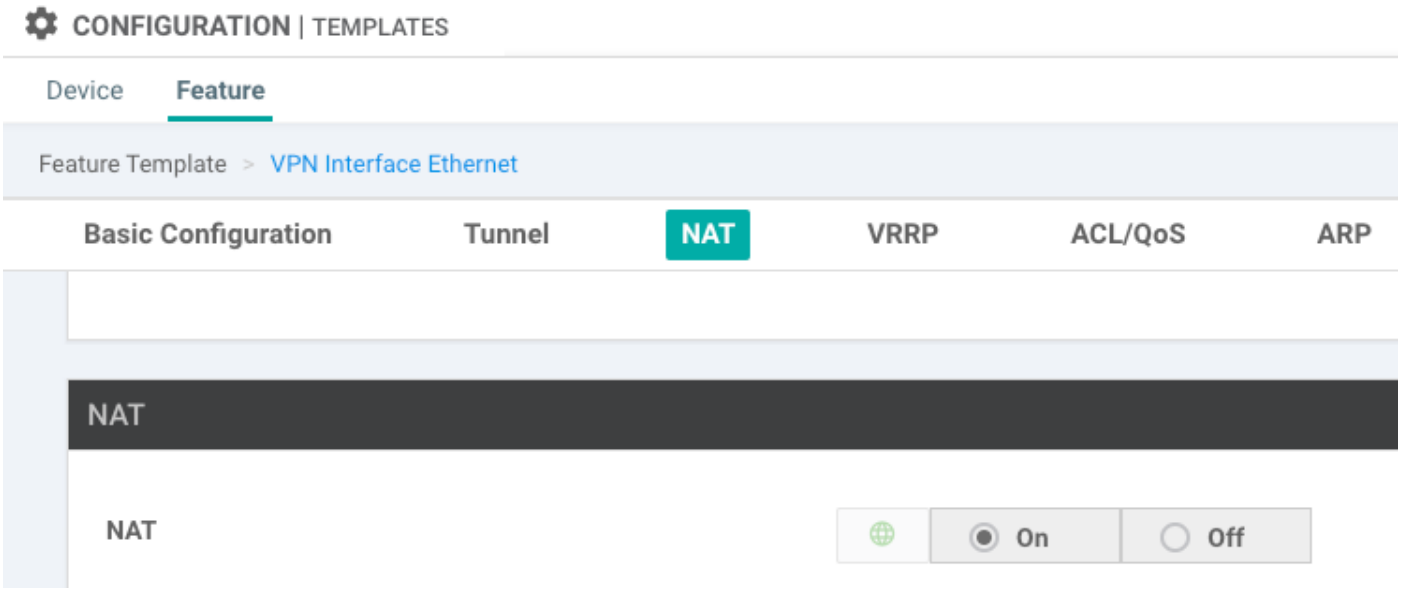
Não funciona com roteadores IOS-XE

Solução 4: Injete a rota padrão para OMP quando o DIA local for usado.

Essa solução pode ser usada para roteadores SD-WAN baseados em IOS-XE e Viptela OS.

Resumindo, nesta solução, uma rota padrão para o DIA (0.0.0.0/0 Null0) é dividida em duas sub-redes 0.0.0.0/1 e 128.0.0.0/1 apontando para Null0. Essa etapa é feita para evitar a sobreposição de uma rota padrão que deve ser anunciada às filiais e à rota padrão, usada para o DIA local. Nas rotas do IOS-XE usadas para o DIA, a distância administrativa (AD) é igual a 6, enquanto a AD do padrão estático é 1. O benefício da solução é a capacidade de usar o esquema de redundância quando o DIA regional é configurado em dois locais diferentes.

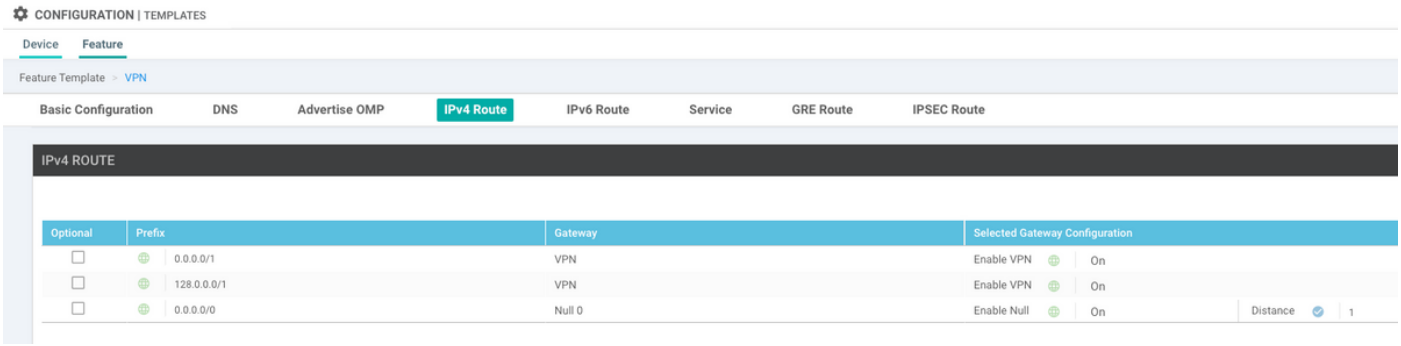
1. Ativar NAT em uma interface de transporte



2. Em um modelo de recurso para uma VPN de serviço, onde o DIA deve ser usado, adicione as seguintes rotas estáticas IPv4:

- 0.0.0.0/1 e 128.0.0.0/1 apontando para VPN. Essas rotas são usadas para o DIA

- 0.0.0.0/0 apontando para Nulo 0. Essa rota é usada para anunciar através do OMP para filiais (semelhante à da Solução 3)



3. Verifique se as rotas foram adicionadas com êxito ao RIB:

```
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. Verifique se o DIA funciona bem localmente:

```
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. Verificar se a rota padrão foi anunciada com êxito a uma filial e instalada no RIB

```
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. Verifique se o DIA funciona bem localmente:

```
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. Verifique se a tradução NAT do roteador DIA regional foi bem-sucedida.

```
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
```

Note: Essa solução permite organizar a redundância ou o compartilhamento de carga com diferentes saídas regionais.

Note: CSCvr72329 - solicitação de aprimoramento "redistribuição de rota NAT para OMP"

Informações Relacionadas

- Política de dados centralizada
- Configurando a política de dados centralizada
- Exemplos de configuração de política de dados centralizada
- Protocolo de roteamento OMP
- Configuração do OMP