¿Cómo se selecciona un sitio concreto para convertirse en una ruptura de Internet regional preferida?

Contenido

Introducción

Este documento describe cómo configurar el entramado SD-WAN para configurar un vEdge de sucursal determinado como ruptura de Internet regional preferida con la ayuda de Direct Internet Access (DIA) y la política de datos centralizada. Esta solución podría ser útil, por ejemplo, cuando un sitio regional utiliza algún servicio centralizado como Zscaler® y debería utilizarse como punto de salida preferido de Internet. Esta implementación requiere que los túneles Generic Routing Encapsulation (GRE) o Internet Protocol Security (IPSec) se configuren desde una VPN de transporte y el flujo de datos sea diferente de la solución DIA normal, donde el tráfico llega directamente a Internet.

Prerequisites

Requirements

Cisco le recomienda que tenga conocimiento acerca de este tema:

- Comprensión básica del marco de políticas SD-WAN.

Componentes Utilizados

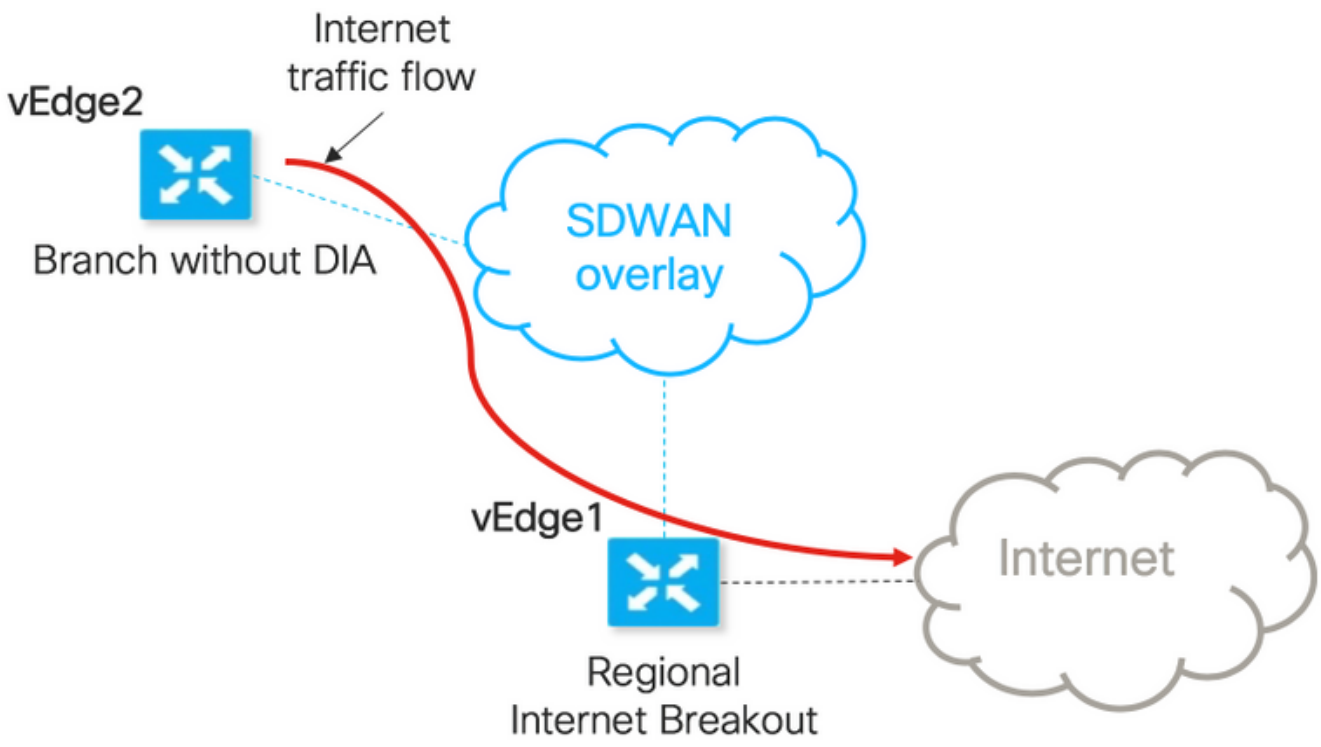
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Routers vEdge
- vSmart Controller con versión de software 18.3.5.

Antecedentes

El tráfico VPN de servicio de vEdge2, que debe llegar a Internet, se reenvía a otra sucursal vEdge1 mediante túneles del plano de datos. vEdge1 es el router donde DIA se configura para la interrupción local de Internet.

Diagrama de la red



Nombre del host	vEdge1	vEdge2
rol de host	Dispositivo de sucursal con DIA (ruptura regional de Internet)	Dispositivo de sucursal que no ti DIA configurado
VPN 0		
Ubicaciones de transporte (TLOC) 1	biz-internet, ip: 192.168.110.6/24	biz-internet, ip: 192.168.110.5/24
Ubicaciones de transporte (TLOC) 2	public-internet, ip: 192.168.109.4/24	public-internet, ip: 192.168.109.5
VPN de servicio 40	Interfaz ge0/1, ip: 192.168.40.4/24	Interfaz ge0/2, ip: 192.168.50.5/2

Configuraciones

Solución 1: Uso de la política de datos centralizada para cambiar el siguiente salto.

vEdge2 tiene establecido un túnel de plano de datos con vEdge1 y otros sitios (conectividad de malla completa)

vEdge1 tiene DIA configurado con **ip route 0.0.0.0/0 vpn 0**.

Configuración de la política de datos 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: no requiere ninguna configuración especial.

Aquí puede encontrar los pasos para realizar la verificación si una política se aplicó correctamente.

1. Compruebe que la política no existe en vEdge2:

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

2. Compruebe la programación de la Base de información de reenvío (FIB). Debería mostrar la ausencia de ruta (Blackhole) para el destino en 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 la política de datos vSmart en la sección **política de aplicación** de la configuración vSmart o active en la GUI de vManage.

4. Compruebe que vEdge2 ha recibido correctamente la política de datos de 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 la programación de la Base de información de reenvío (FIB), que muestra las rutas posibles para el destino en 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 el alcance al destino en 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
```

Aquí puede encontrar los pasos de configuración de vEdge1.

1. Active la traducción de direcciones de red (NAT) en la interfaz de transporte, donde se debe utilizar DIA:

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

2. Agregue la ruta estática **ip route 0.0.0.0/0 vpn 0** en una VPN de servicio para activar 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 si RIB contiene la ruta NAT:

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

4. Confirme que DIA funciona y podemos ver sesión de protocolo de mensajes de control de Internet (ICMP) a 173.37.145.84 desde vEdge2 en traducciones 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 -
```

Nota: Esta solución no nos permite organizar la redundancia o el uso compartido de la carga con diferentes salidas regionales.

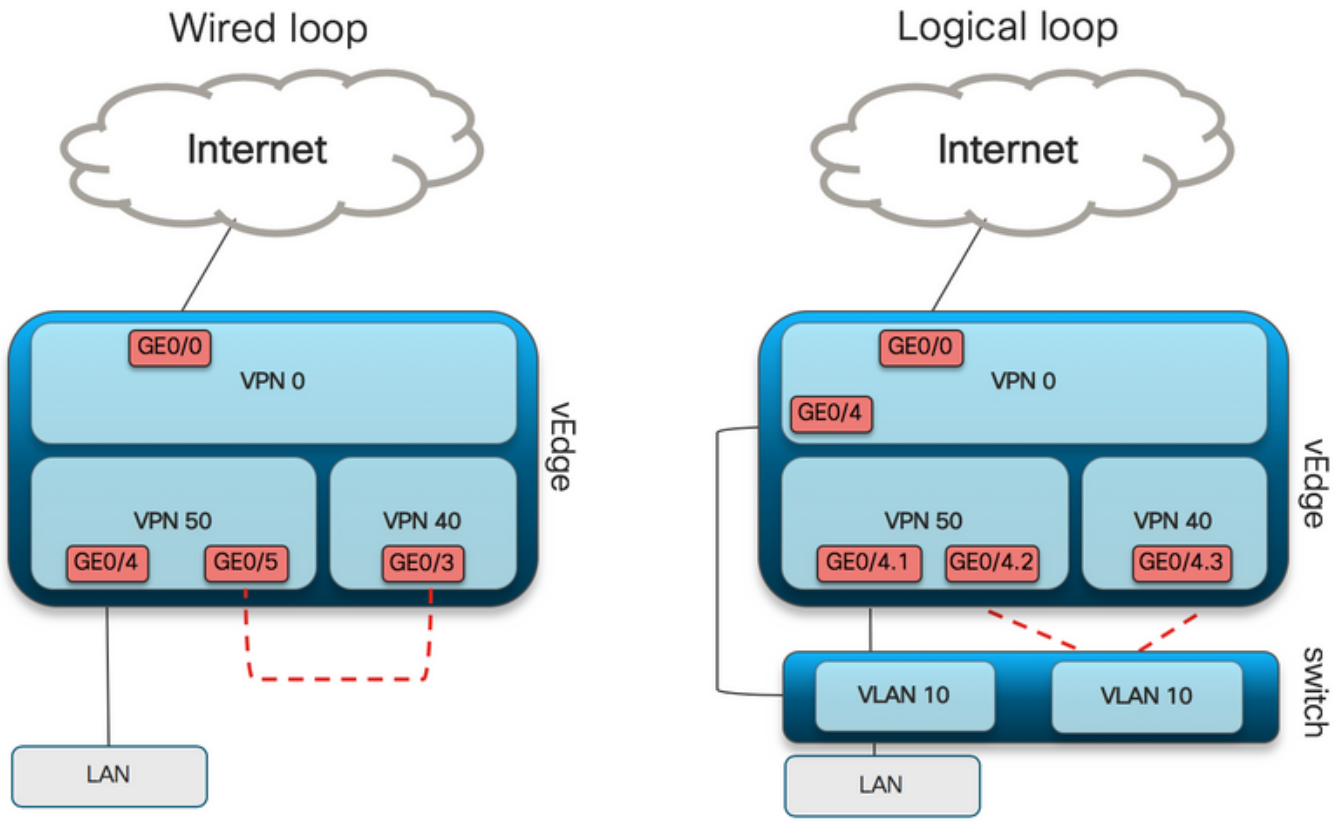
No funciona con routers IOS-XE

Solución 2: Inyectar GRE\IPSec\NAT Default Route to OMP requerido.

A partir de ahora, no hay posibilidad de obtener la ruta predeterminada, señalando el túnel GRE/IPSec en vEdge1, que se anunciará a través de OMP a vEdge2 (redistribución del protocolo OMP de ruta nat). Tenga en cuenta que el comportamiento puede cambiar en futuras versiones de software.

Nuestro objetivo es crear una ruta predeterminada estática regular (**ruta IP 0.0.0.0/0 <dirección IP de siguiente salto>**) que pueda ser originada por vEdge2 (dispositivo preferido para DIA) y propagada a través de OMP.

Para lograrlo, se crea una VPN falsa en vEdge1 y se realiza un loop de puerto físico con el cable. El loop se crea entre los puertos asignados a la VPN ficticia y el puerto en la VPN deseada que requiere una ruta estática predeterminada. Además, puede crear un loop con sólo una interfaz física conectada al switch con VLAN ficticia y dos subinterfaces asignadas a las VPNs correspondientes en la siguiente imagen:



Aquí puede encontrar el ejemplo de configuración de vEdge1.

1. Cree una VPN falsa:

```
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 FIB que la ruta DIA, que apunta a la interfaz NAT, se agregó correctamente a la tabla de ruteo:

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

3. VPN de servicio utilizada con fines de producción, donde se configura la ruta predeterminada normal (que OMP podrá 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 la presencia de la ruta predeterminada que apunta a la interfaz 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 que vEdge1 anunciara la ruta predeterminada a través de 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 no requiere ninguna configuración; la ruta predeterminada se recibe a través de OMP, que apunta a 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 la disponibilidad a 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
```

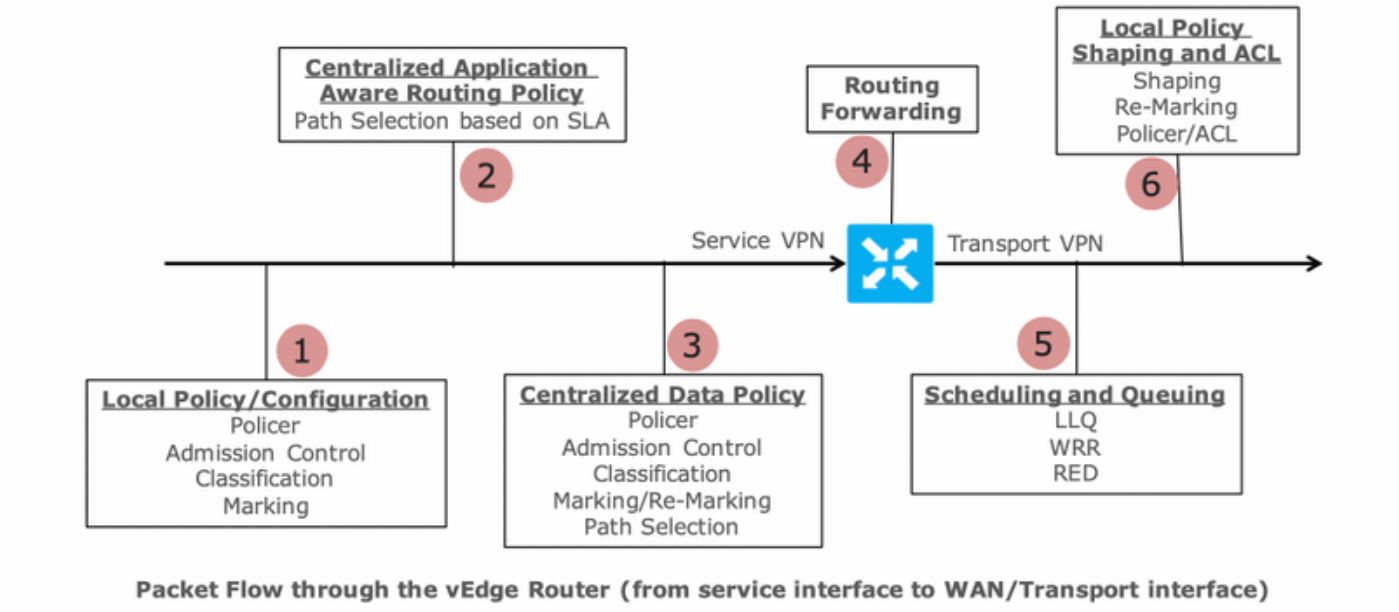
Nota: Esta solución le permite organizar la redundancia o el uso compartido de la carga con diferentes salidas regionales.

No funciona con routers IOS-XE

Solución 3: Inyectar Ruta Predeterminada a OMP cuando se usa Política de Datos Centralizada para DIA.

Cuando se utiliza la política de datos centralizada para el DIA local, la forma posible de inyectar la ruta predeterminada, señala a un dispositivo regional con DIA que es el uso de esta ruta estática predeterminada: **ip route 0.0.0.0/0 Null0**.

Debido al flujo de paquetes interno, el tráfico que llega de las sucursales llega a DIA gracias a la política de datos y nunca llega a la ruta a Null0. Como puede ver aquí, la búsqueda de siguiente salto sólo se produce después de una implementación de políticas.



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

vEdge2 tiene establecido un túnel de plano de datos con vEdge1 y otros sitios (conectividad de malla completa). No requiere ninguna configuración especial.

vEdge1 tiene DIA configurado con política de datos centralizada.

Aquí puede encontrar los pasos de configuración de vEdge1.

1. Active la traducción de direcciones de red (NAT) en la interfaz de transporte, donde se debe utilizar DIA:

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

2. Agregue la ruta estática **ip route 0.0.0.0/0 null0** en una VPN de servicio para anunciar la ruta predeterminada a las sucursales:

```
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 si RIB contiene la ruta predeterminada:

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

4. Verifique que vEdge1 anunciara la ruta predeterminada a través de 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. Compruebe que la política no existe en el vEdge1 y que el DIA no está habilitado:

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

6. Compruebe la programación de la Base de información de reenvío (FIB). Debe mostrar la ausencia de ruta (Blackhole) para el destino en Internet ya que DIA no está habilitado:

```
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
```

Configuración de política de datos 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 la política de datos vSmart en la sección **política de aplicación** de la configuración vSmart o active en la GUI de vManage.

7. Compruebe que vEdge1 ha recibido correctamente la política de datos de 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 la programación de la Base de información de reenvío (FIB), que muestra las rutas

posibles para el destino en 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 el alcance al destino en 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
```

Pasos de verificación de vEdge2:

1. Confirme que la ruta predeterminada se recibió e instaló correctamente en 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 la programación de la Base de información de reenvío (FIB), que muestra las rutas posibles para el destino en 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 el alcance al destino en 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 que DIA funciona y podemos ver sesión de protocolo de mensajes de control de Internet (ICMP) a 173.37.145.84 desde vEdge2 en traducciones 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 -
```

Nota: Esta solución permite organizar la redundancia o el uso compartido de la carga con diferentes salidas regionales.

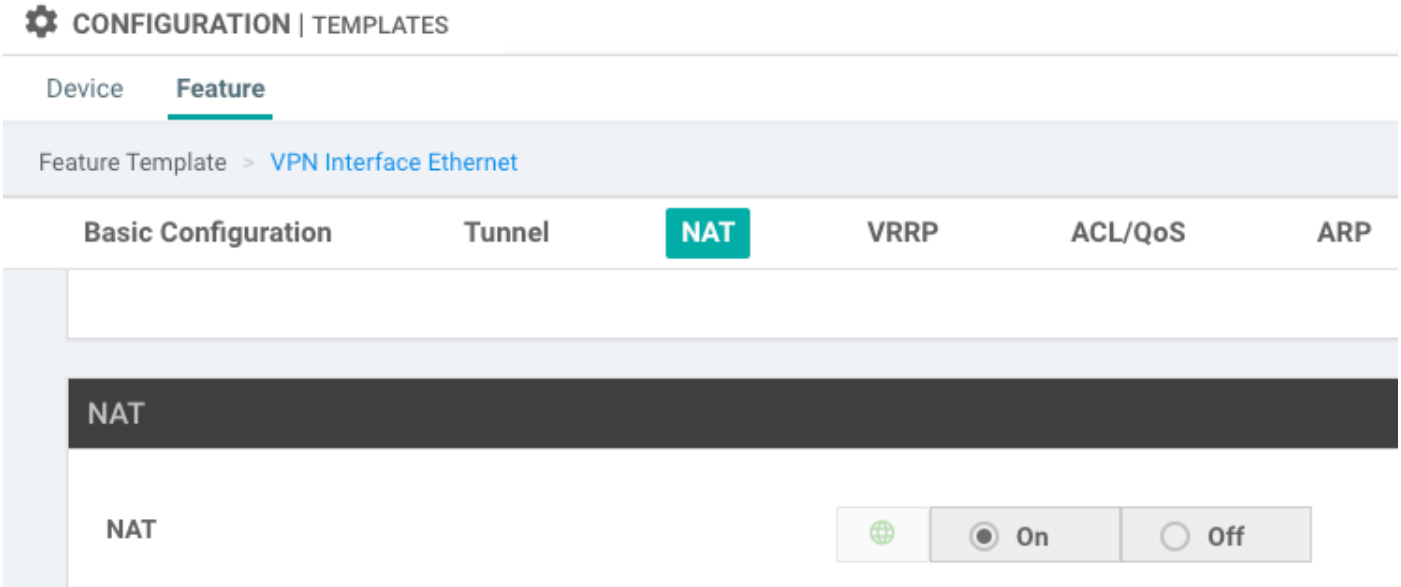
No funciona con routers IOS-XE

Solución 4: Inyectar la ruta predeterminada a OMP cuando se utiliza DIA local.

Esta solución se puede utilizar para routers SD-WAN basados en IOS-XE y en el sistema operativo Viptela.

En resumen, en esta solución, una ruta predeterminada para DIA (0.0.0.0/0 Null0) se divide en dos subredes 0.0.0.0/1 y 128.0.0.0/1 que apuntan a Null0. Este paso se realiza para evitar la superposición de una ruta predeterminada que se debe anunciar a las sucursales y a la ruta predeterminada, utilizada para el DIA local. En las rutas IOS-XE que se utilizan para DIA, la distancia administrativa (AD) es igual a 6, mientras que la AD predeterminada estática es 1. La ventaja de la solución es la capacidad de utilizar el esquema de redundancia cuando el DIA regional se configura en dos ubicaciones diferentes.

1. Activar NAT en una interfaz de transporte

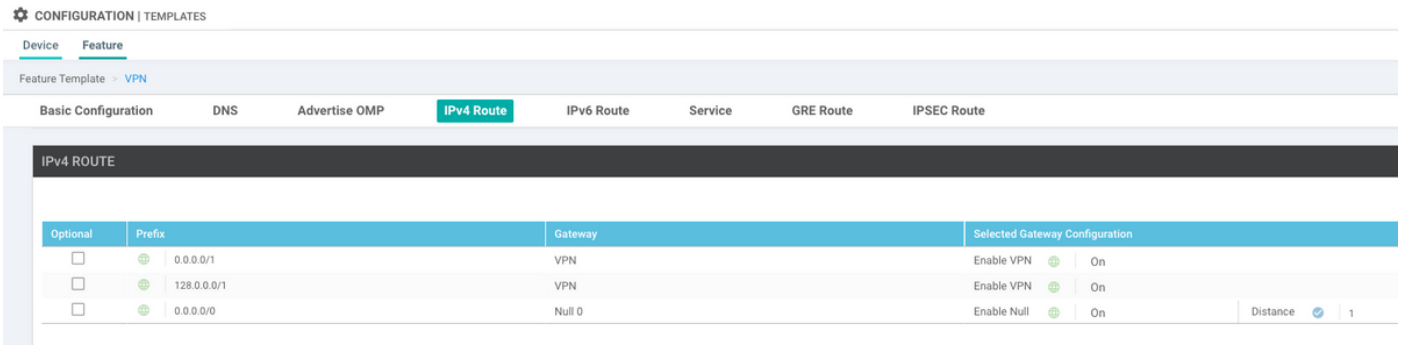


2. En una plantilla de funciones para una VPN de servicio, donde se debe utilizar DIA, agregue las siguientes rutas IPv4 estáticas:

- 0.0.0.0/1 y 128.0.0.0/1 apuntando a VPN. Estas rutas se utilizan para DIA

- 0.0.0.0/0 apuntando a Null 0. Esta ruta se utiliza para la publicidad a través de OMP para

sucursales (similar a la solución 3)



3. Verifique que las rutas se agregaron correctamente a 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 que DIA funcione bien 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. Verifique que la ruta predeterminada se haya anunciado correctamente a una sucursal e instalado en 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 que DIA funcione bien 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 la traducción NAT correcta del router DIA regional.

```
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
```

Nota: Esta solución permite organizar la redundancia o el uso compartido de la carga con diferentes salidas regionales.

Nota: CSCvr72329 - solicitud de mejora "NAT route redistribution to OMP"

Información Relacionada

- Política de datos centralizada
- Configuración de la política de datos centralizada
- Ejemplos de Configuración de Política de Datos Centralizados
- Protocolo de ruteo OMP
- Configuración de OMP