¿Cómo seleccionar un sitio particular para ser un desbloqueo regional preferido de Internet?

Contenido

Introducción

Este documento describe cómo configurar la tela SD-WAN para configurar el vEdge determinado de la bifurcación como desbloqueo regional preferido de Internet con la ayuda del acceso a internet directo (diámetro) y de la directiva centralizada de los datos. Esta solución podría ser útil en caso de que, por ejemplo, cuando un sitio regional utiliza un cierto servicio centralizado como Zscaler® y se debe utilizar como punto de salida preferido de Internet. Tal despliegue requiere el Generic Routing Encapsulation (GRE) o la seguridad de protocolos en Internet (IPSec) hace un túnel para ser configurada de un transporte VPN y del flujo de datos es diferente de la solución regular diámetro, donde el tráfico alcanza Internet directamente.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de este tema:

- Comprensión básica del Marco de políticas SD-WAN.

Componentes Utilizados

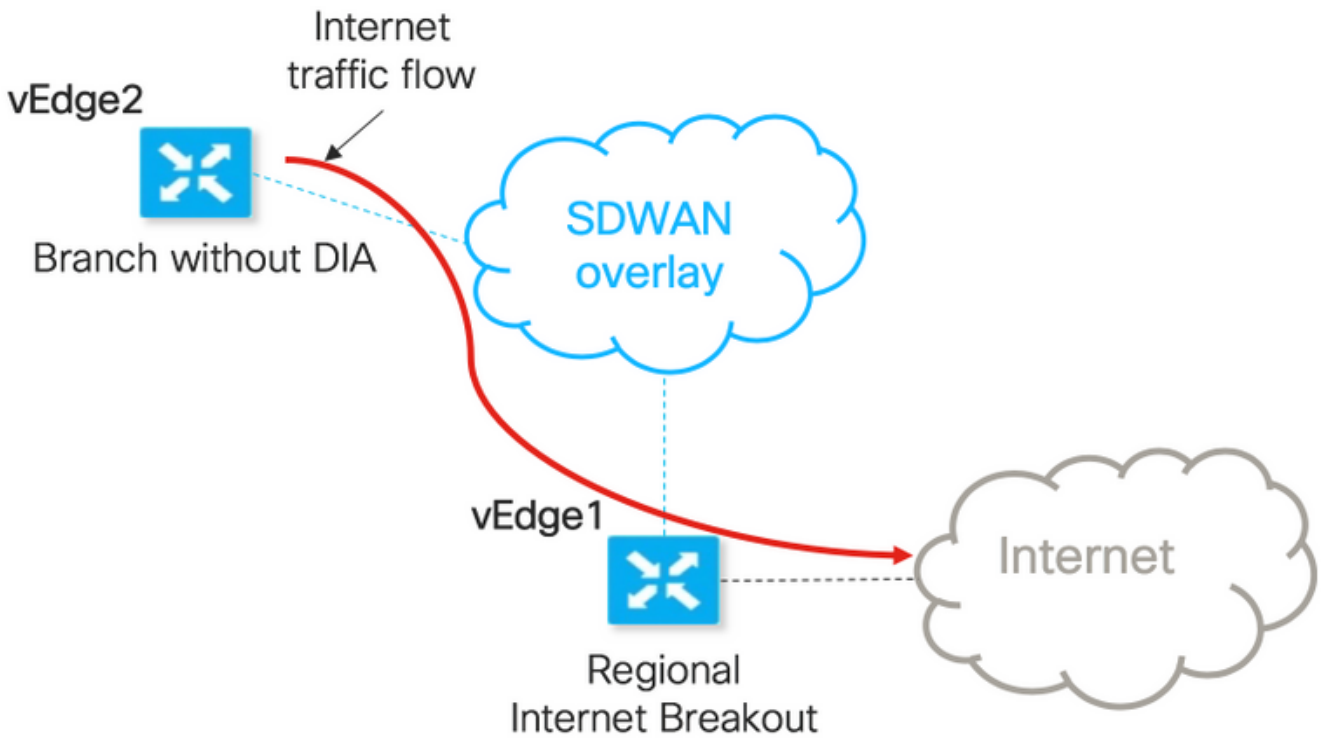
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Routers del vEdge
- regulador del vSmart con la versión de software 18.3.5.

Antecedentes

Mantenga el tráfico VPN de vEdge2, eso debe alcanzar Internet, se remite a otra bifurcación vEdge1, usando los túneles del avión de los datos. está el router vEdge1 donde diámetro configurado para el desbloqueo local de Internet.

Diagrama de la red



Nombre del host	vEdge1	vEdge2
Papel del host	Dispositivo de la bifurcación que tiene diámetro (el desbloqueo regional de Internet)	Dispositivo de la bifurcación que tiene ningún diámetro configurac
VPN 0		
Ubicaciones del transporte (TLOC) 1	negocio-Internet, IP: 192.168.110.6/24	negocio-Internet, IP: 192.168.110.5/24
Ubicaciones del transporte (TLOC) 2	público-Internet, IP: 192.168.109.4/24	público-Internet, IP: 192.168.109
Mantenga VPN 40	Interconecte ge0/1, IP: 192.168.40.4/24	Interconecte ge0/2, IP: 192.168.50.5/24

Configuraciones

Solución 1: Uso centralizado de la DATA-directiva para cambiar el Next-Hop.

vEdge2 tiene túnel plano de los datos establecido con vEdge1 y otros sitios (la Conectividad del estilo del full-mesh)

vEdge1 tiene diámetro configurado con el **vpn 0 de la ruta de IP 0.0.0.0/0**.

configuración centralizada vSmart de la DATA-directiva:

```
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 usted puede encontrar los pasos para realizar la verificación si una directiva fue aplicada correctamente.

1. Marque que la directiva está ausente de vEdge2:

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

2. Marque la programación de la Base de información de reenvío (FIB). Debe mostrar la ausencia de la 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 DATA-directiva del vSmart bajo sección de la aplicar-**directiva de la** configuración del vSmart o actívela en el vManage GUI.

4. Marque que vEdge2 recibió con éxito la DATA-directiva del 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. Marque la programación de la Base de información de reenvío (FIB), esa las rutas posibles de las demostraciones 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 accesibilidad 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 usted puede encontrar los pasos para la configuración vEdge1.

1. Active el Network Address Translation (NAT) en la interfaz de transporte, donde el diámetro debe ser utilizado:

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

2. Agregue el **vpn 0 de la ruta de IP 0.0.0.0/0 de la** Static ruta en un servicio VPN para activar el diámetro:

```
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. Marque si el 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 los trabajos y nosotros diámetro podemos considerar la sesión del Internet Control Message Protocol (ICMP) a 173.37.145.84 de vEdge2 en traducciones de 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 permite que ordenemos la Redundancia o la carga a compartir con diverso uso regional de las salidas.

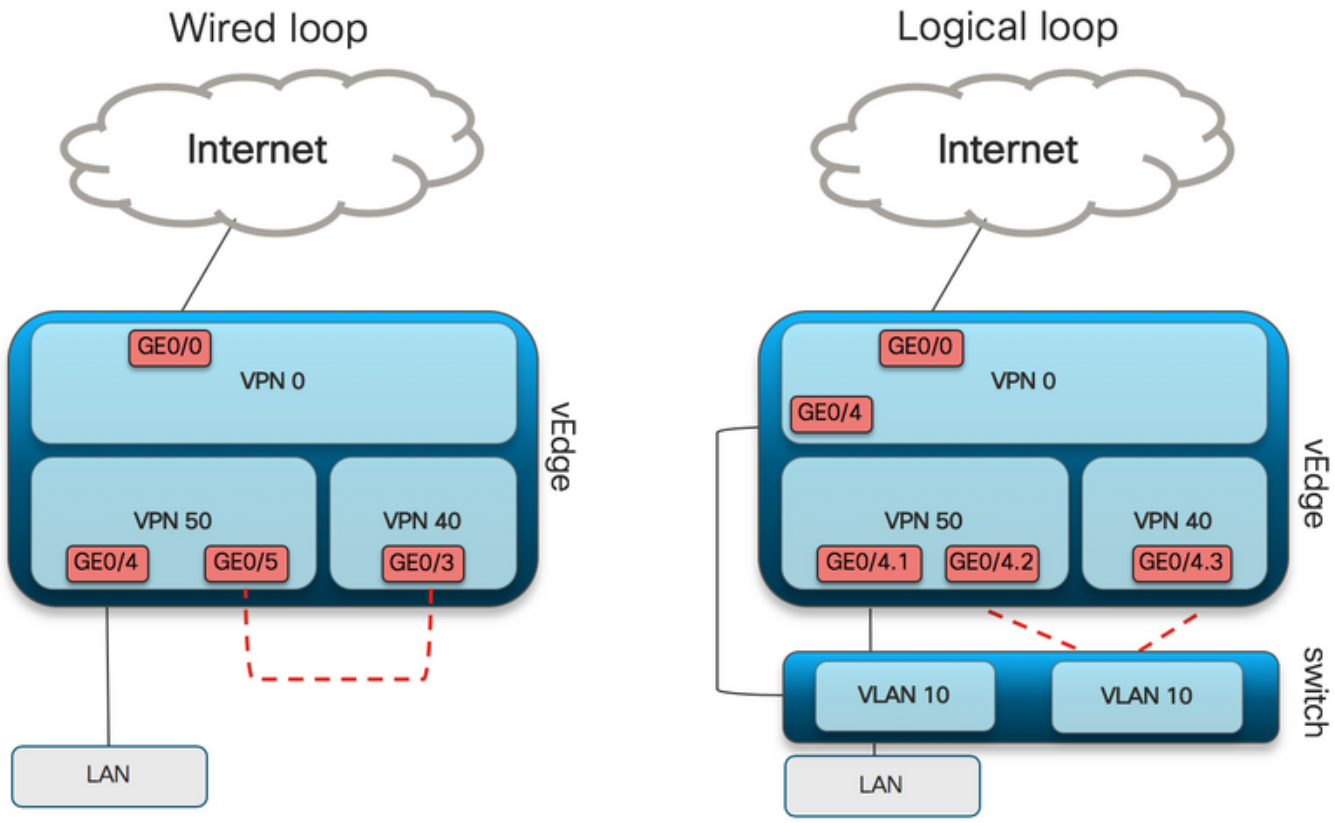
No trabaja con el Routers IOS-XE

Solución 2: Inyecte el GRE requerido \ la ruta predeterminado del IPSec \ NAT a OMP.

A partir de ahora, no hay posibilidad para conseguir la ruta predeterminado, señalando al GRE \ al túnel IPsec en vEdge1, para ser hecho publicidad con OMP a vEdge2 (redistribuya el protocolo nacional de la ruta OMP). Observe por favor que el comportamiento puede cambiar en las versiones del software futuro.

Nuestra meta es crear una Static Default ruta regular (**addr> IP del <next-salto de la ruta de IP 0.0.0.0/0**) que se podría originar por vEdge2 (dispositivo preferido para el diámetro) y propagar más lejos vía OMP.

Para alcanzar esto, el VPN simulado se crea en vEdge1 y un loop del puerto físico se realiza con el cable. El loop se crea entre los puertos asignados al VPN simulado y el puerto en el VPN deseado que requiere la Static Default ruta. También, usted puede crear un loop con apenas una interfaz física que se asocie al Switch con el VLA N simulado y dos las interfaces secundarias asignados a VPN correspondientes s en la imagen abajo:



Aquí usted puede encontrar el ejemplo de configuración vEdge1.

1. Cree un VPN simulado:

```
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. Marque la BOLA que la ruta diámetro, señalando a la interfaz NAT, fue agregada con éxito 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. Mantenga el VPN usado para los propósitos de la producción, donde se configura la ruta predeterminado regular (de que OMP podrá hacer publicidad):

```
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. Marque el RIB para la presencia de ruta predeterminado que señala a la interfaz del 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. Marque que vEdge1 hizo publicidad de la ruta predeterminado vía 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 predeterminado se recibe vía OMP, que señala 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 el accesibilidad 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
```

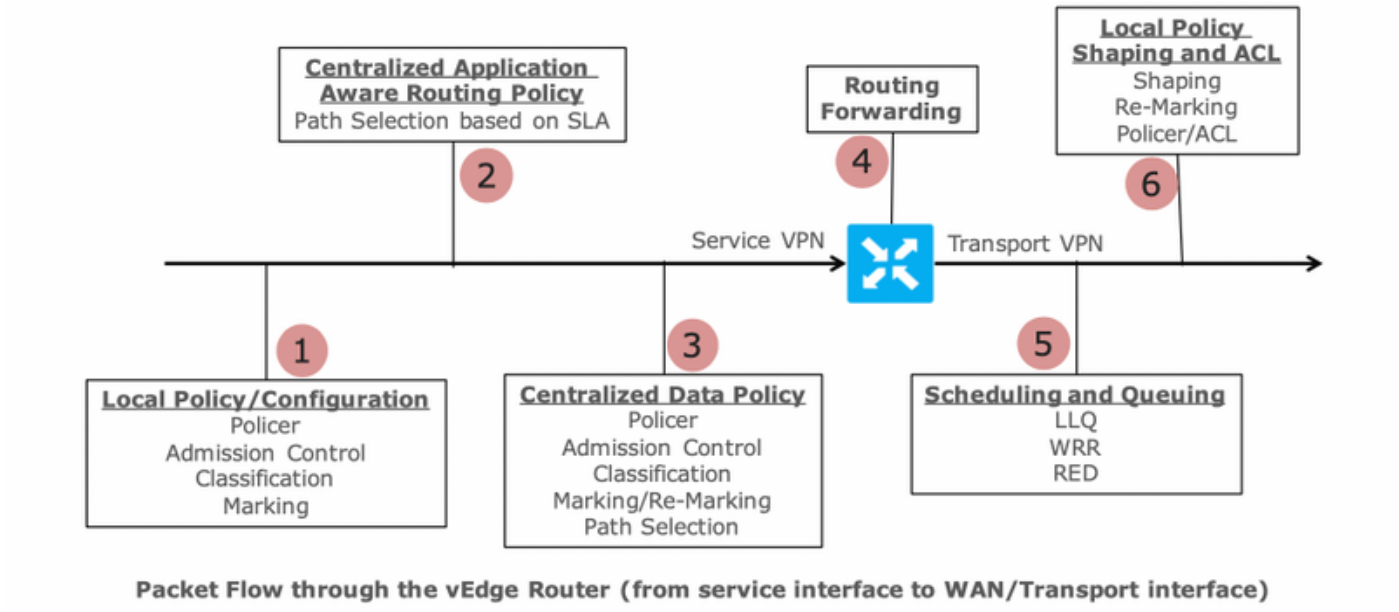
Nota: Esta solución permite que usted ordene la Redundancia o la carga a compartir con diverso uso regional de las salidas.

No trabaja con el Routers IOS-XE

Solución 3: Inyecte la ruta predeterminado a OMP cuando DATA-directiva centralizada usada para el diámetro.

Cuando la DATA-directiva centralizada se utiliza para el diámetro local, la manera posible de inyectar la ruta predeterminado, señala a un dispositivo regional con el diámetro que es el uso de esta Static Default ruta: **null0 de la ruta de IP 0.0.0.0/0**.

Debido al flujo de paquetes interno, el tráfico que llega de los gracias diámetro del alcance de las bifurcaciones a la DATA-directiva, y nunca alcanza la ruta al null0. Como usted puede ver aquí, las operaciones de búsqueda del Next-Hop suceden sólo después de una implementación de política.



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

vEdge2 tiene túnel plano de los datos establecido con vEdge1 y otros sitios (Conectividad del estilo del full-mesh). No requiere ninguna configuración especial.

vEdge1 tiene diámetro configurado con la DATA-directiva centralizada.

Aquí usted puede encontrar los pasos para la configuración vEdge1.

1. Active el Network Address Translation (NAT) en la interfaz de transporte, donde el diámetro debe ser utilizado:

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

2. Agregue el **null0 de la ruta de IP 0.0.0.0/0 de la** Static ruta en un servicio VPN para hacer publicidad del valor por defecto a las bifurcaciones:

```
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. Marque si el RIB contiene la ruta predeterminado:

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

4. Marque que vEdge1 hizo publicidad de la ruta predeterminado vía 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. Marque que la directiva está ausente en vEdge1 y que el diámetro no está habilitado:

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

6. Marque la programación de la Base de información de reenvío (FIB). Debe mostrar la ausencia de la ruta (Blackhole) para el destino en Internet pues el diámetro no se habilita:

```
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 centralizada vSmart de la DATA-directiva para el diámetro:

```
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 DATA-directiva del vSmart bajo sección de la aplicar-**directiva de la** configuración del vSmart o actívela en el vManage GUI.

7. Marque que vEdge1 recibió con éxito la DATA-directiva del 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. Marque la programación de la Base de información de reenvío (FIB), esa las rutas posibles de

las demostraciones 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 accesibilidad 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 vEdge2:

1. Confirme que la ruta predeterminado fue recibida y instalada con éxito en el 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. Marque la programación de la Base de información de reenvío (FIB), esa las rutas posibles de las demostraciones 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 accesibilidad 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 los trabajos y nosotros diámetro podemos considerar la sesión del Internet Control Message Protocol (ICMP) a 173.37.145.84 de vEdge2 en traducciones de 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 ordenar la Redundancia o la carga a compartir con diverso uso regional de las salidas.

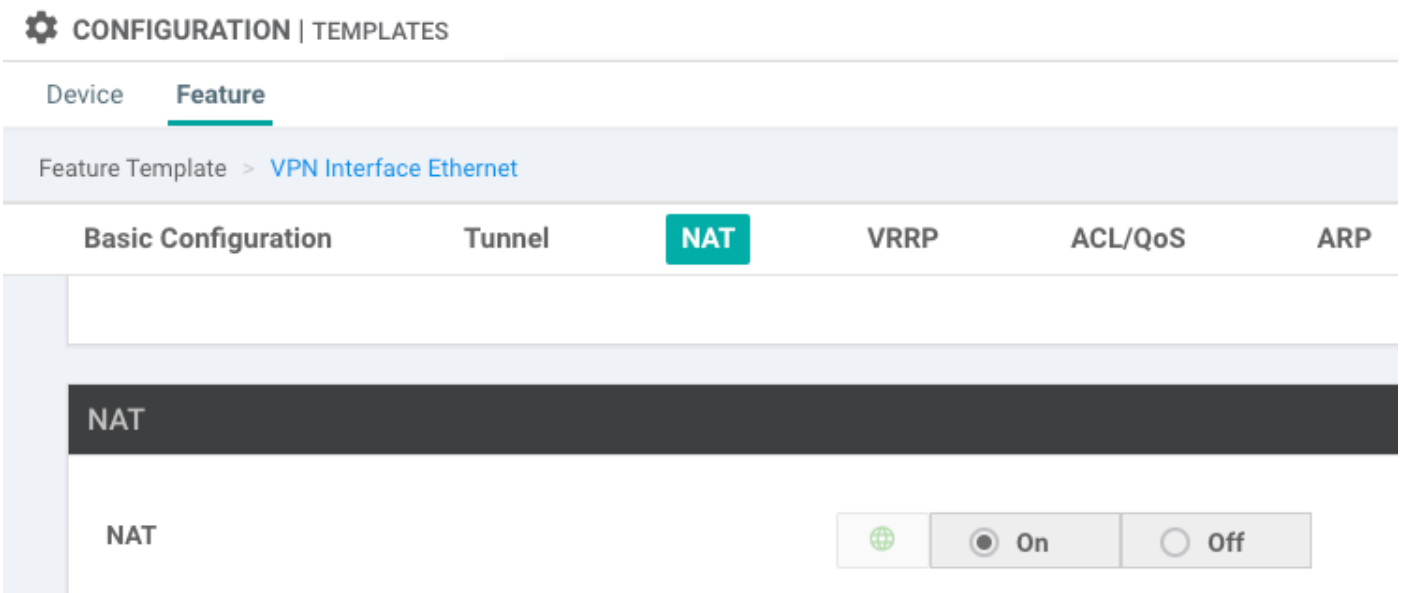
No trabaja con el Routers IOS-XE

Solución 4: Inyecte la ruta predeterminado a OMP cuando el diámetro local utilizó.

Esta solución se puede utilizar para IOS-XE y el Routers basado OS de Viptela SD-WAN.

En resumen, en esta solución, una ruta predeterminado para el diámetro (0.0.0.0/0 null0) está partida en dos redes secundarios 0.0.0.0/1 y 128.0.0.0/1 que señalan al null0. Este paso se hace para evitar solapar de una ruta predeterminado que se deba hacer publicidad a las bifurcaciones y a la ruta predeterminado, usado para el diámetro local. En las rutas IOS-XE usadas para el diámetro tenga igual de la distancia administrativa (AD) a 6, mientras que el AD del estático predeterminado es 1. La ventaja de la solución es la capacidad de utilizar el esquema de la Redundancia cuando el diámetro regional se configura en dos ubicaciones diferentes.

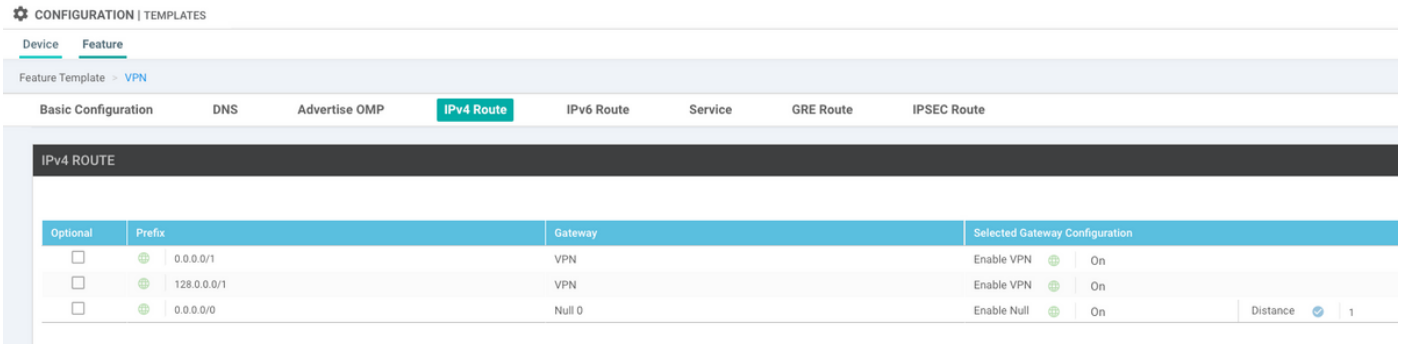
1. Active el NAT en una interfaz de transporte



2. En una plantilla de la característica para un servicio VPN, donde el diámetro debe ser utilizado agregue las rutas estáticas siguientes del IPv4:

- 0.0.0.0/1 y 128.0.0.0/1 que señalan al VPN. Estas rutas se utilizan para el diámetro

- 0.0.0.0/0 que señala al null0. Esta ruta se utiliza para hacer publicidad vía OMP a las bifurcaciones (similares como en la solución 3)



3. Marque que las rutas fueron agregadas con éxito PARA PROVEER DE COSTILLAS:

```
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. Marque que manan los trabajos diámetro 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. Marque que ruta predeterminado de divulgación con éxito a una bifurcación y instalada en el 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. Marque que manan los trabajos diámetro 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. Compruebe la traducción de NAT acertada del router regional diámetro.

```
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 ordenar la Redundancia o la carga a compartir con diverso uso regional de las salidas.

Nota: CSCvr72329 - pedido de mejora “redistribución de ruta NAT a OMP”

Información Relacionada

- Directiva centralizada de los datos
- Configurar la directiva centralizada de los datos
- Ejemplos centralizados de la configuración de la política de los datos
- Routing Protocol OMP
- Configurar OMP