# Hoe een bepaalde site te selecteren als een bevoorrechte regionale internetdoorbraak?

## Inhoud



## Inleiding

In dit document wordt beschreven hoe u SD-WAN kunt configureren om bepaalde aftakking vEdge te configureren als meest geprefereerde regionale internetdoorbraak met behulp van Direct Internet Access (DIA) en een gecentraliseerd gegevensbeleid. Deze oplossing zou bijvoorbeeld nuttig kunnen zijn wanneer een regionale site een gecentraliseerde service zoals Zscaler® gebruikt en zou moeten worden gebruikt als een voorkeurspunt voor het afsluiten van internet. Zulke plaatsing vereist Generic Routing Encapsulation (GRE) of Internet Protocol Security (IPSec) tunnels om te worden geconfigureerd van een transport VPN en gegevensstroom is anders dan de reguliere DIA-oplossing, waar verkeer direct internet bereikt.

## Voorwaarden

### Vereisten

Cisco raadt aan dat u kennis hebt van dit onderwerp:

- Basis begrip van SD-WAN beleidskader.

### Gebruikte componenten

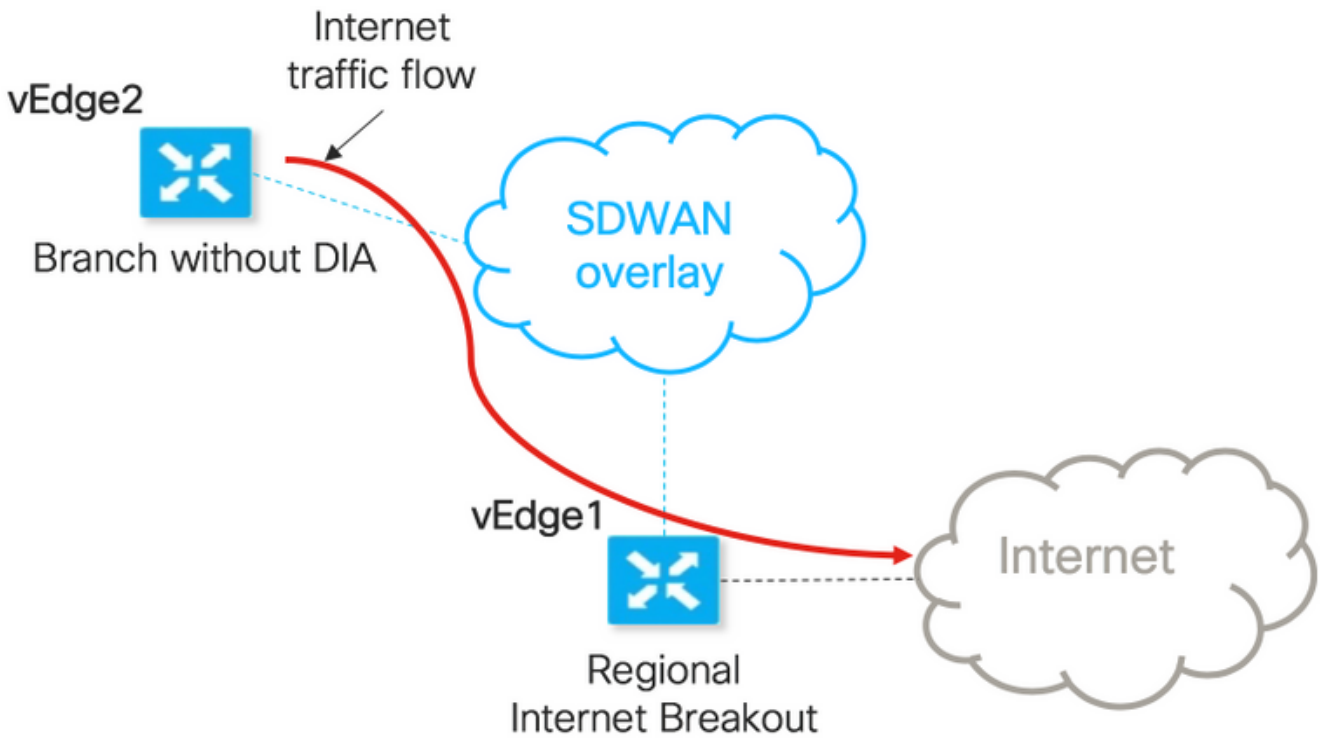
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- vEdge-routers
- vSmart Controller met 18.3.5 softwareversie.

# Achtergrondinformatie

Het verkeer van VPN van de dienst van vEdge2, dat het internet zou moeten bereiken, wordt aan een andere tak vEdge1 doorgestuurd, met gebruik van datalootunnels. vEdge1 is de router waar DIA voor een plaatselijke internetdoorbraak is ingesteld.

## Netwerkdiagram




| Host name | vEdge1 | vEdge2 |
|---|---|---|
| Host rol | Vestigingsapparaat dat DIA heeft (regionale Internet breakout) | Vestigingsapparaat dat geen DIA heeft ingesteld |
| VPN 0 | | |
| Vervoerlocaties (TLOC) 1 | biz-internet, ip: 192.168.110.6/24 | biz-internet, ip: 192.168.110.5/24 |
| Vervoerlocaties (TLOC) 2 | publiek-internet, ip: 192.168.109.4/24 | publiek-internet, ip: 192.168.109 |
| Service VPN 40 | Interface ge0/1, ip: 192.168.40.4/24 | Interface ge0/2, ip: 192.168.50.5 |

# Configuraties

## Oplossing 1: Gecentraliseerde benadering voor gegevensbeleid om de volgende hop te wijzigen.

vEdge2 heeft een datalunnel die met vEdge1 en andere locaties is ingesteld (modulesterconnectiviteit)

vEdge1 heeft DIA ingesteld met **ip-route 0.0.0.0/0 vpn 0**.

vSmart gecentraliseerde datacommunicatie:

```
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 - heeft geen speciale configuratie nodig.

Hier kunt u stappen vinden om verificatie uit te voeren als een beleid correct is toegepast.

1. Controleer of vEdge2-beleid niet bestaat:

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

2. Controleer het doorsturen van een informatieve basis (FIB)-programma. Hierin moet de afwezigheid van route (Blackgat) voor de bestemming op internet zijn aangegeven:

```
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. Pas vSmart-gegevensbeleid toe onder sectie **van toepassing-beleid** van vSmart-configuratie of activeer in vManager GUI.

4. Controleer of vEdge2 met succes het gegevensbeleid van vSmart heeft ontvangen:

```
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. Controleer Forwarding Information Base (FIB)-programmering, die mogelijke routes voor de bestemming op internet toont:

```
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. Bevestiging van de bereikbaarheid op de bestemming op het 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
```

Hier vindt u de vEdge1-configuratiestappen.

1. Activeer Network Address Translation (NAT) op de transportinterface waar DIA moet worden gebruikt:

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

2. Voeg statische route **ip route 0.0.0.0/0 VPN 0** in een Service VPN toe om DIA te activeren:

```
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. Controleer of RIB NAT-route bevat:

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

4. Bevestig dat DIA werkt en we kunnen ICMP-sessie (Internet Control Message Protocol) (Internet Control Message Protocol) naar 17.37.145.84 van vEdge2 in NAT-vertalingen zien

```
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 -
```

Opmerking: Deze oplossing stelt ons niet in staat redundantie te organiseren of het delen van de lading te delen met verschillende regionale exits gebruik.

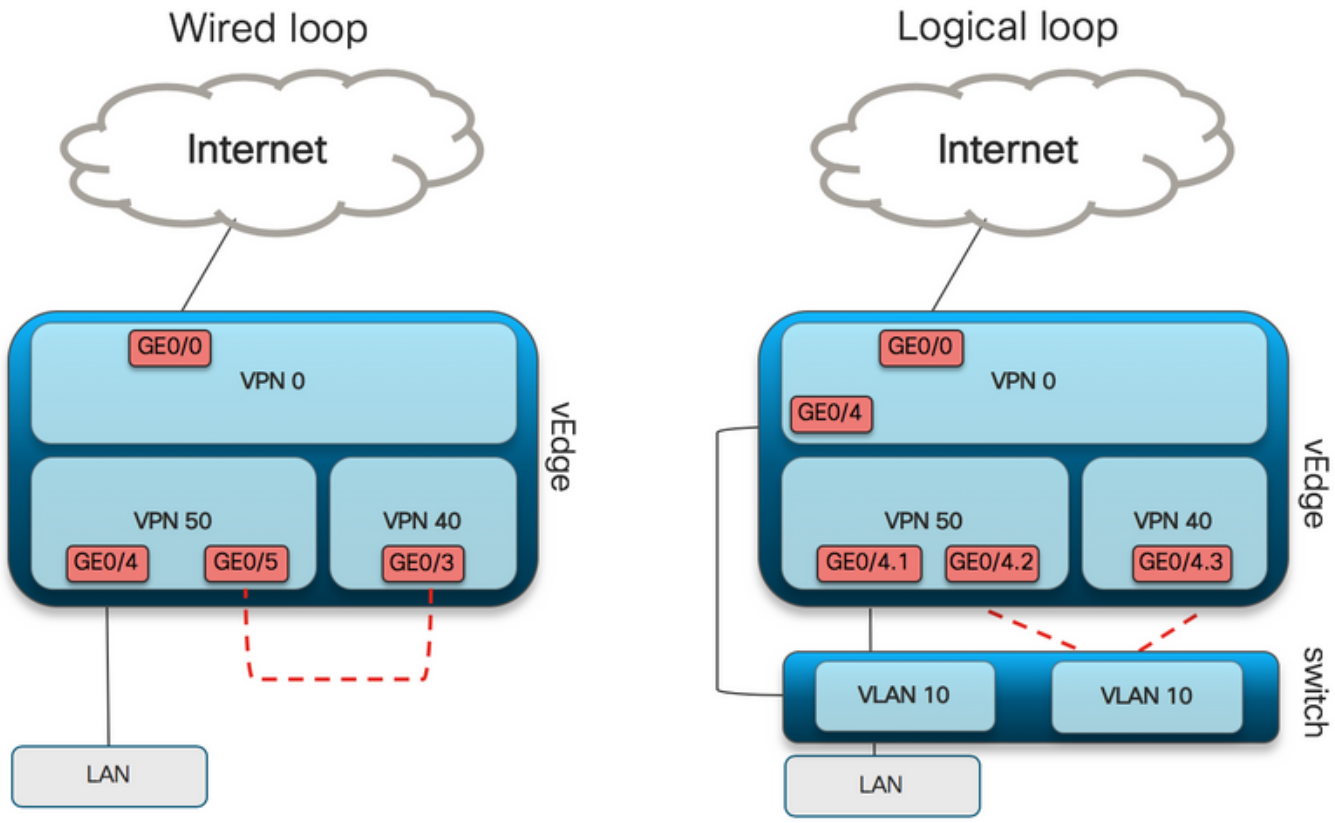
Werkt niet met IOS-XE routers

## Oplossing 2: Injecteer verplicht GRE\IPSec\NAT Default Route to OMP.

Tot nu toe is er geen mogelijkheid om de standaardroute te krijgen, wijzend naar de GRE\IPSec-tunnel op vEdge1, die via OMP aan vEdge2 moet worden geadverteerd (herverdeel in route OMP-protocol). Houd er rekening mee dat gedrag in toekomstige softwareversies kan veranderen.

Ons doel is om een regelmatige statische standaardroute (**IP route 0.0.0.0/0 <next-hop-IP addr>**) te maken die door vEdge2 (apparaat dat voor DIA voorkeur heeft) kan worden gegenereerd en verder via OMP kan worden gepropageerd.

Om dit te bereiken, wordt dummy VPN gemaakt op vEdge1 en wordt een fysieke poortlus uitgevoerd met kabel. Lijn wordt gecreëerd tussen poorten die aan VPN zijn toegewezen en poorten in het gewenste VPN dat statische standaardroute vereist. U kunt ook een lus maken met slechts één fysieke interface die aan de switch is gekoppeld met dummy VLAN en twee sub-interfaces toegewezen aan corresponderende VPN's in het onderstaande beeld:




Hier vindt u een voorbeeld van de vEdge1-configuratie.

1. Maak een VPN-pop:

```
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. Controleer FIB dat DIA-route, naar de NAT-interface, met succes is toegevoegd aan de routingtabel:

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

3. Service VPN die voor productiedoeleinden wordt gebruikt, waarbij de normale standaardroute is geconfigureerd (welke OMP kan adverteren):

```
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. Controleer de RIB op de aanwezigheid van standaardroute die naar de lus wijst:

```
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. Controleer of vEdge1 de standaardroute via OMP heeft geadverteerd:

```
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 heeft geen configuratie nodig, de standaardroute wordt ontvangen via OMP, wat wijst naar 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. Consolideerde bereikbaarheid tot 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
```

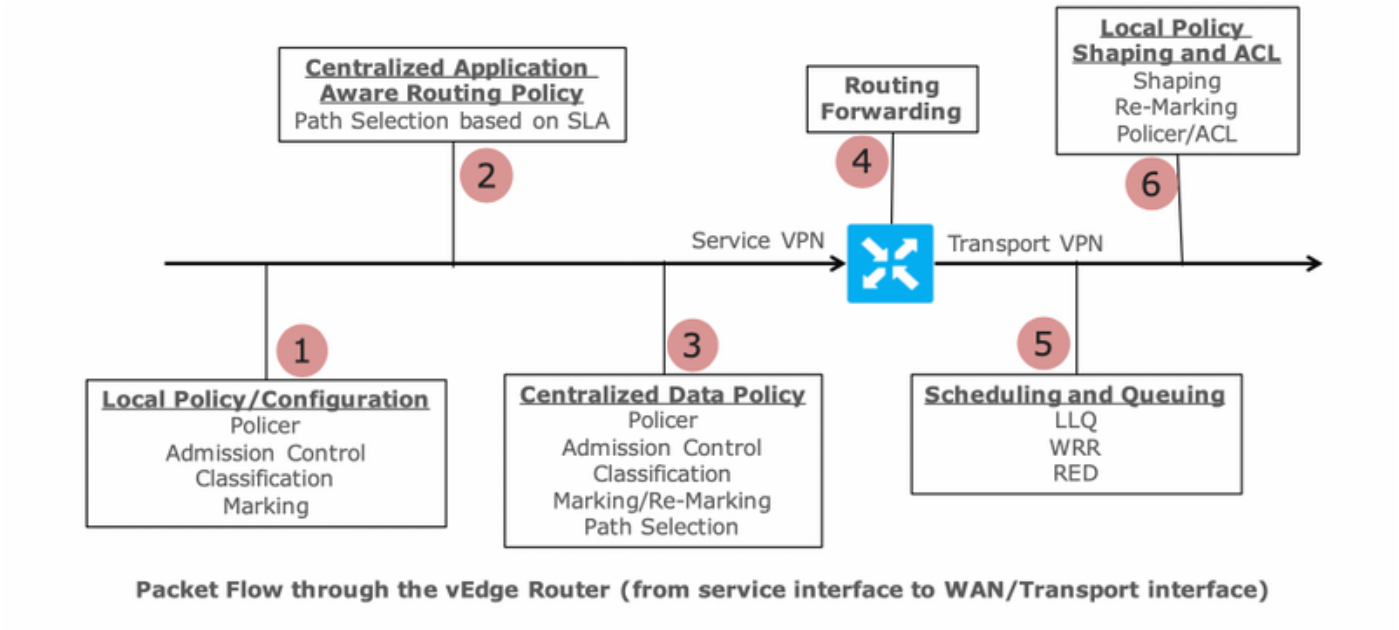
Opmerking: Deze oplossing stelt u in staat redundantie te organiseren of het delen van de lading te delen met verschillende regionale uitgangen.

Werkt niet met IOS-XE routers

## Oplossing 3: Injecteer de standaardroute aan de OMP wanneer er een gecentraliseerd gegevensbeleid voor DIA wordt gebruikt.

Wanneer gecentraliseerd data-beleid voor lokale DIA wordt gebruikt, de mogelijke manier om de standaardroute te injecteren, wijst het op een regionaal apparaat met DIA dat het gebruik van deze statische standaardroute is: **ip route 0.0.0.0/0 Null0**.

Vanwege interne pakketstroom bereikt verkeer dat uit takken komt DIA dankzij data-beleid, en bereikt nooit route naar Null0. Zoals je hier kunt zien, gebeurt de volgende-hop raadpleging alleen na een beleidsuitvoering.




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

vEdge2 heeft een datalunnel die met vEdge1 en andere locaties is ingesteld (connectiviteit met de volledige maaswijdstijl). Het heeft geen speciale configuratie nodig.

vEdge1 heeft DIA ingesteld met een gecentraliseerd gegevensbeleid.

Hier vindt u de vEdge1-configuratiestappen.

1. Activeer Network Address Translation (NAT) op de transportinterface waar DIA moet worden gebruikt:

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

2. Voeg statische route **ip route 0.0.0.0/0 nul0** in een Service VPN toe om standaard aan takken aan te geven:

```
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. Controleer of RIB de standaardroute bevat:

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

4. Controleer of vEdge1 de standaardroute via OMP heeft geadverteerd:

```
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. Controleer of het beleid niet aanwezig is op vEdge1 en dat DIA niet is ingeschakeld:

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

6. Controleer het doorsturen van het programma Information Base (FIB). Dit programma moet de afwezigheid van de route (Blackgat) voor de bestemming op het internet tonen aangezien DIA niet is ingeschakeld:

```
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
```

vSmart gecentraliseerde datacommunicatie voor 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
```

Pas vSmart data-beleid toe onder **toepassen-beleid** sectie van vSmart configuratie of activeer in vManager GUI.

7. Controleer of vEdge1 met succes het gegevensbeleid van vSmart heeft ontvangen:

```
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. Controleer Forwarding Information Base (FIB)-programmering, die mogelijke routes voor de bestemming op internet toont:

```
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. Bevestiging van de bereikbaarheid aan de bestemming op het 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
```

vEdge2-controlestappen:

1. Bevestig dat de standaardroute met succes is ontvangen en in RIB is geïnstalleerd:

```
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. Controleer Forwarding Information Base (FIB)-programma's die mogelijke routes voor de bestemming op internet weergeven:

```
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. Bevestiging van de bereikbaarheid op de bestemming op het 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. Bevestig dat DIA werkt en we kunnen ICMP-sessie (Internet Control Message Protocol) (Internet Control Message Protocol) naar 17.37.145.84 van vEdge2 in NAT-vertalingen zien

```
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 -
```

Opmerking: Deze oplossing stelt redundantie of lastverdeling met verschillende regionale uitgangen mogelijk.

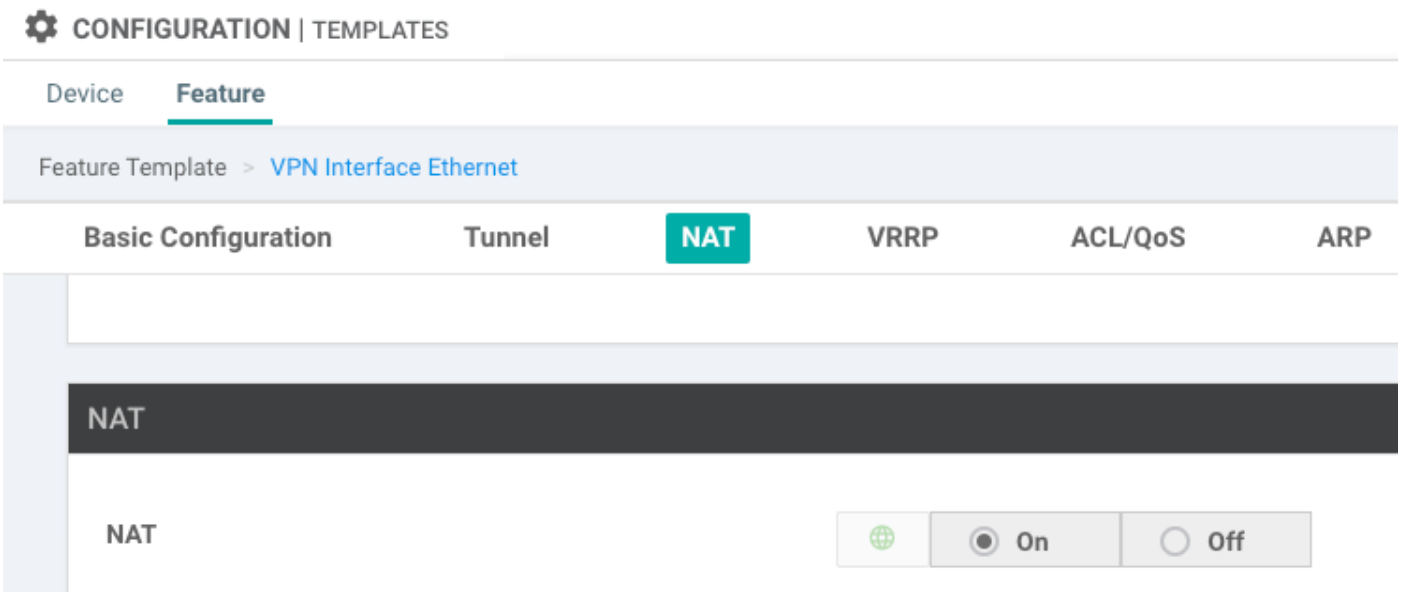
Werkt niet met IOS-XE routers

## Oplossing 4: Injecteer de standaardroute aan de OMP als lokale DIA wordt gebruikt.

Deze oplossing kan worden gebruikt voor zowel IOS-XE als Viptela OS-gebaseerde SD-WAN routers.

Kort samengevat, in deze oplossing, wordt een standaardroute voor DIA (0.0.0.0/0 Null0) in twee subnetwerken gesplitst 0.0.0.0/1 en 128.0.0.0/1 gericht op Null0. Deze stap wordt gedaan om overlapping van een standaardroute te vermijden die zou moeten worden geadverteerd aan takken en standaardroute, gebruikt voor lokale DIA. In IOS-XE routes die voor DIA worden gebruikt hebben administratieve Afstand (AD) gelijk aan 6, terwijl AD van statische standaard 1 is. Het voordeel van de oplossing is de mogelijkheid om overtolligheidsschema te gebruiken wanneer Regionale DIA op twee verschillende locaties wordt geconfigureerd.

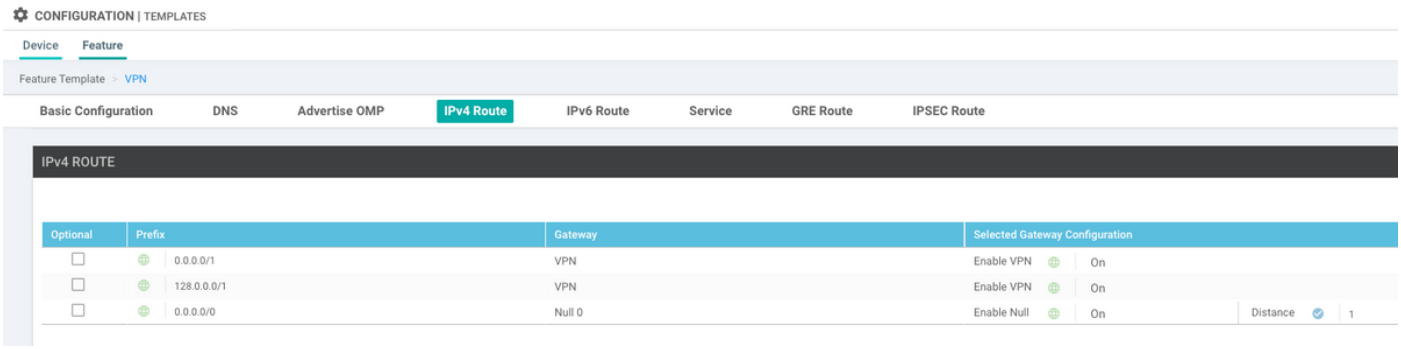
1. NAT op een transportinterface activeren




2. In een sjabloon voor een service-VPN waarin DIA moet worden gebruikt, voegt u de volgende statische IPv4-routes toe:

- 0.0.0.0/1 en 128.0.0.0/1 met uw aandacht voor VPN. Deze routes worden gebruikt voor DIA

- 0.0.0.0/0, met vermelding van Null 0. Deze route wordt gebruikt voor reclame via OMP op filialen (vergelijkbaar met oplossing 3)




3. Controleer of de routes zijn toegevoegd aan 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. Controleer of DIA goed werkt lokaal:

```
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. Controleer of de standaardroute met succes is geadverteerd op een filiaal en in RIB is geïnstalleerd

```
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. Controleer of DIA goed werkt lokaal:

```
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. Controleer op regionale DIA-router met succesvolle NAT-vertaling.

```
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
```

Opmerking: Deze oplossing stelt redundantie of lastverdeling met verschillende regionale uitgangen mogelijk.

**Opmerking:** CSCvr72329 - verzoek om versterking van "NAT-routeherdistributie naar OMP"

# Gerelateerde informatie

- Gecentraliseerd gegevensbeleid
- Gecentraliseerd gegevensbeleid configureren
- Configuratievoorbeelden van gecentraliseerd gegevensbeleid
- OMP-routingprotocol
- OMP configureren