

# Come selezionare un particolare sito da utilizzare come Internet Breakout regionale preferito?

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazioni](#)

[Soluzione 1: Utilizzo centralizzato delle regole sui dati per modificare l'hop successivo.](#)

[Soluzione 2: Inject Argomento necessario di tipo GRE\IPSec\NAT. Route predefinito a OMP.](#)

[Soluzione 3: Immettere la route predefinita per OMP quando si utilizzano i criteri dati centralizzati per DIA.](#)

[Soluzione 4: Inserire il percorso predefinito per OMP quando viene utilizzato DIA locale.](#)

[Informazioni correlate](#)

## Introduzione

Questo documento descrive come configurare SD-WAN fabric per configurare una particolare filiale vEdge come breakout Internet regionale preferito con l'aiuto di Direct Internet Access (DIA) e policy di dati centralizzati. Questa soluzione potrebbe essere utile nel caso, ad esempio, in cui un sito regionale utilizza un servizio centralizzato come Zscaler® e dovrebbe essere utilizzato come punto di uscita Internet preferito. Questa distribuzione richiede la configurazione dei tunnel GRE (Generic Routing Encapsulation) o IPSec (Internet Protocol Security) da una VPN di trasporto e un flusso di dati diverso dalla normale soluzione DIA, in cui il traffico raggiunge Internet direttamente.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza di questo argomento:

- Conoscenze base di SD-WAN Policy Framework.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

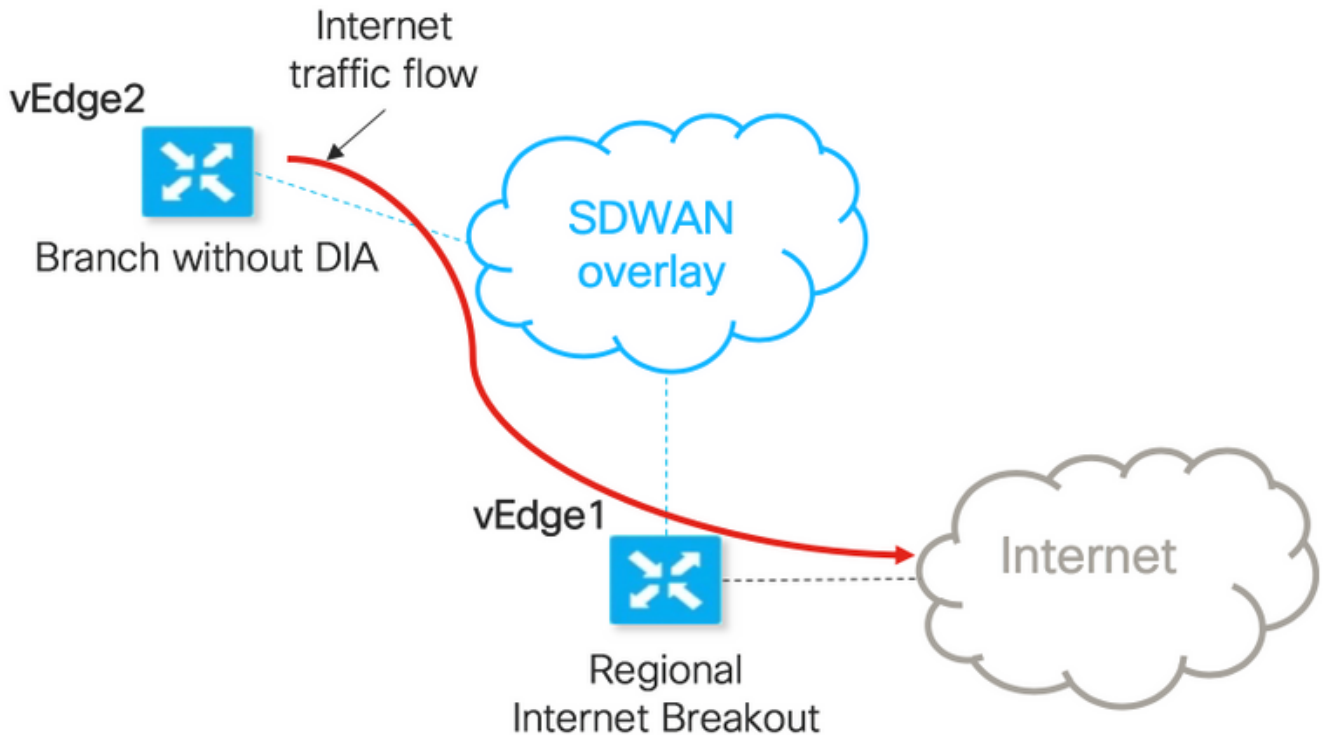
- Router vEdge

- vSmart Controller con versione software 18.3.5.

## Premesse

Il traffico VPN del servizio da vEdge2, che dovrebbe raggiungere Internet, viene inoltrato a un'altra diramazione vEdge1, utilizzando tunnel del piano dati. vEdge1 è il router in cui DIA è configurata per l'interruzione di Internet locale.

## Esempio di rete



Nome host	vEdge 1	vEdge2
Ruolo host	Dispositivo di succursale con DIA (Regional Internet Breakout)	Dispositivo di diramazione senza configurato
VPN 0		
1 TLOC (Transport Locations)	biz-internet, ip: 192.168.110.6/24	biz-internet, ip: 192.168.110.5/24
2 TLOC (Transport Locations)	internet-pubblico, ip: 192.168.109.4/24	internet-pubblico, ip: 192.168.109.5/24
Service VPN 40	Interfaccia ge0/1, ip: 192.168.40.4/24	Interfaccia ge0/2, ip: 192.168.50.4/24

## Configurazioni

### Soluzione 1: Utilizzo centralizzato delle regole sui dati per modificare l'hop successivo.

vEdge2 dispone di un tunnel del piano dati stabilito con vEdge1 e altri siti (connettività in stile rete completa)

Per vEdge1, il comando DIA è configurato con `ip route 0.0.0.0/0 vpn 0`.

Configurazione delle regole dei dati centralizzate 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 - non richiede alcuna configurazione speciale.

Qui è possibile trovare i passi per eseguire la verifica se un criterio è stato applicato correttamente.

1. Verificare che i criteri non siano presenti in vEdge2:

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

2. Controllare la programmazione FIB (Forwarding Information Base). Deve mostrare l'assenza di route (blackhole) per la destinazione su 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. Applicare i criteri dati vSmart nella sezione **apply-policy** della configurazione vSmart o attivarli nell'interfaccia utente di vManage.

4. Verificare che vEdge2 abbia ricevuto correttamente i criteri dati da 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. Controllare la programmazione Forwarding Information Base (FIB), che mostra possibili percorsi per la destinazione su 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. Confermare la raggiungibilità alla destinazione su 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

```

Qui è possibile trovare i passaggi di configurazione di vEdge1.

### 1. Attivare Network Address Translation (NAT) sull'interfaccia di trasporto, dove DIA deve essere utilizzato:

```

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

```

### 2. Aggiungere la route statica ip route 0.0.0.0/0 vpn 0 in una VPN di servizio per attivare 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. Verificare se RIB contiene la route NAT:

```

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

```

### 4. Confermare che DIA funziona e possiamo vedere la sessione Internet Control Message Protocol (ICMP) a 173.37.145.84 da vEdge2 nelle traduzioni NAT

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

PUBLIC		PUBLIC		PRIVATE		PRIVATE		PRIVATE		
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:** Questa soluzione non consente di organizzare la ridondanza o la condivisione del carico con diverse uscite regionali.

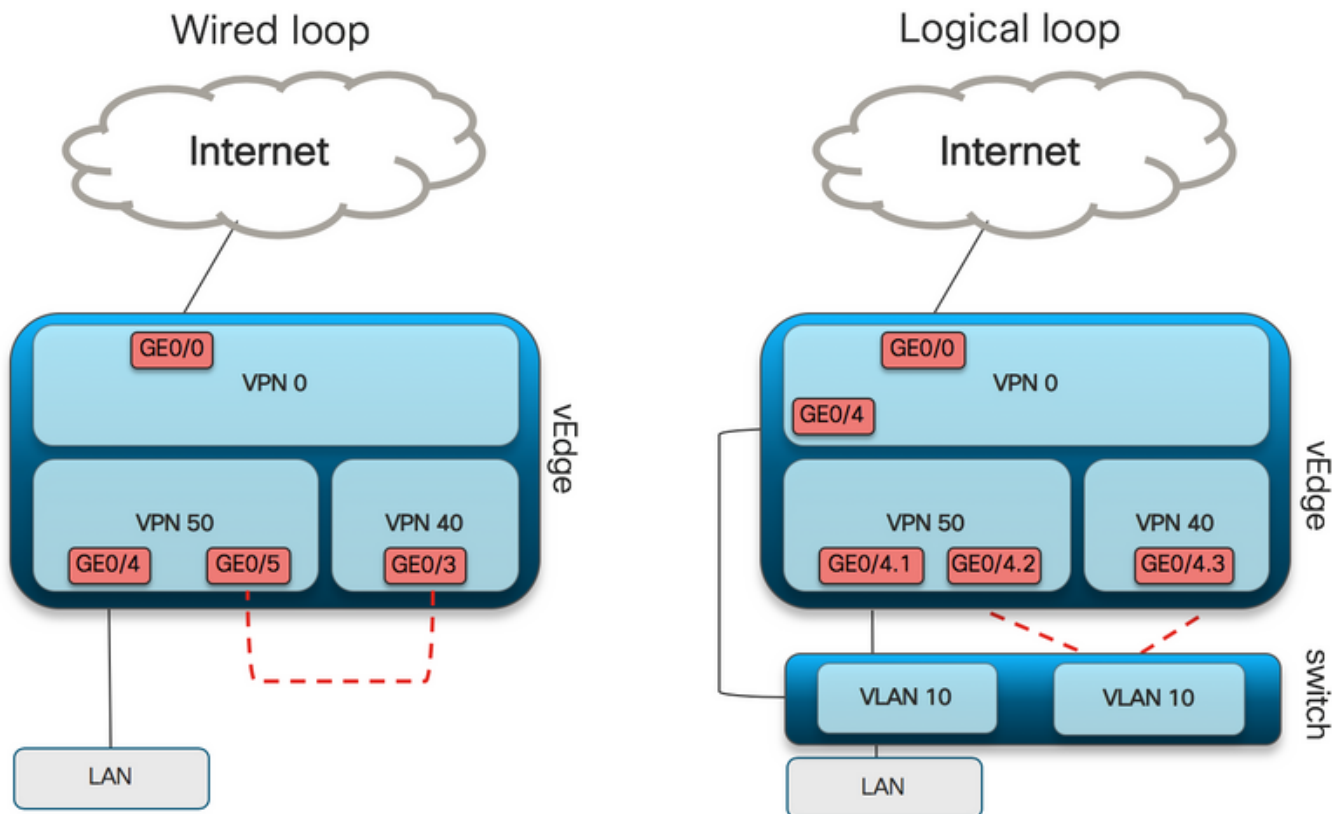
Non funziona con i router IOS-XE

## Soluzione 2: Inject Argomento necessario di tipo GRE\IPSec\NAT. Route predefinito a OMP.

Al momento non è possibile ottenere la route predefinita, che punta al tunnel GRE\IPSec su vEdge1, da annunciare tramite OMP a vEdge2 (ridistribuire il protocollo OMP route NAT). Il comportamento potrebbe cambiare nelle versioni software future.

Il nostro obiettivo è creare una normale route statica predefinita (**IP route 0.0.0.0/0 <indirizzo IP dell'hop successivo>**) che potrebbe essere originata da vEdge2 (dispositivo preferito per DIA) e ulteriormente propagata tramite OMP.

Per ottenere questo risultato, viene creata una VPN fittizia su vEdge1 e viene eseguito un loop della porta fisica con il cavo. Viene creato un loop tra le porte assegnate a una VPN fittizia e la porta nella VPN desiderata che richiede una route statica predefinita. Inoltre, è possibile creare un loop solo con un'interfaccia fisica collegata allo switch con una VLAN fittizia e due sottointerfacce assegnate alle VPN corrispondenti, come mostrato nell'immagine seguente:



Qui è possibile trovare l'esempio di configurazione di vEdge1.

#### 1. Creare una VPN fittizia:

```
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. Verificare su FIB che la route DIA, che punta all'interfaccia NAT, sia stata aggiunta correttamente alla tabella di routing:

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

#### 3. VPN di servizio utilizzata per scopi di produzione, in cui è configurato un percorso predefinito regolare (che OMP potrà pubblicizzare):

```
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. Verificare che il RIB non presenti una route predefinita che punta all'interfaccia 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. Verificare che vEdge1 abbia annunciato il ciclo di lavorazione predefinito tramite 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 non richiede alcuna configurazione. Il percorso predefinito viene ricevuto tramite OMP, che punta 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. Confermare la raggiungibilità 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
```

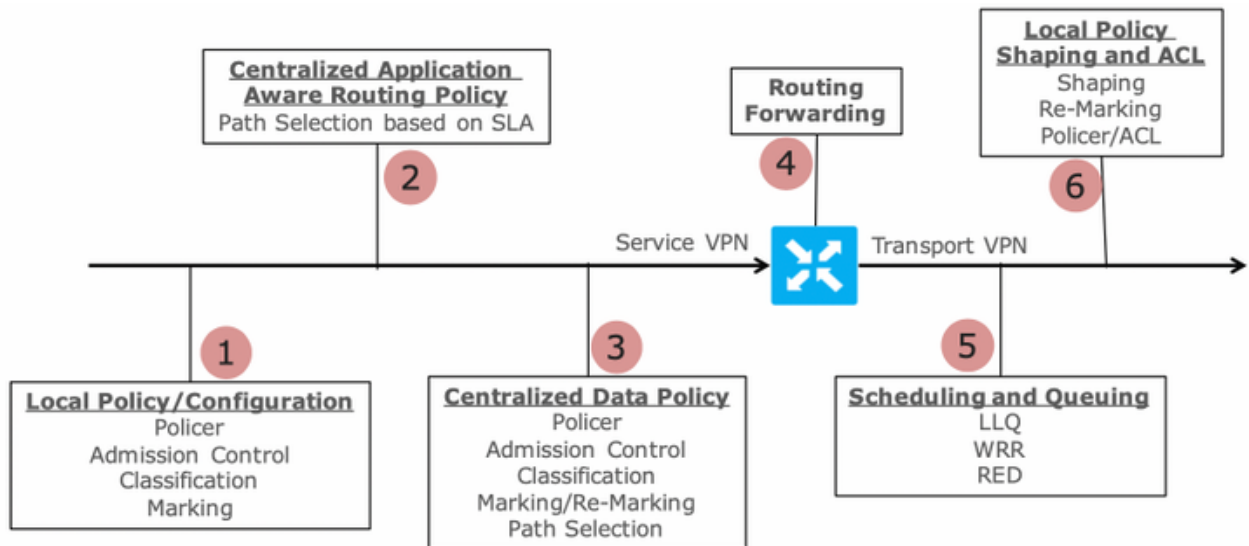
**Nota:** Questa soluzione consente di organizzare la ridondanza o la condivisione del carico con diverse uscite regionali.

Non funziona con i router IOS-XE

## Soluzione 3: Immettere la route predefinita per OMP quando si utilizzano i criteri dati centralizzati per DIA.

Quando si utilizzano i criteri dei dati centralizzati per il DIA locale, il modo possibile per inserire il percorso predefinito, punta a un dispositivo regionale con DIA che è l'uso di questo percorso statico predefinito: **ip route 0.0.0.0/0 Null0**.

A causa del flusso di pacchetti interno, il traffico che arriva dalle filiali raggiunge DIA grazie ai criteri dati e non raggiunge mai la route verso Null0. Come si può vedere qui, la ricerca dell'hop successivo avviene solo dopo una distribuzione dei criteri.



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

vEdge2 dispone di un tunnel del piano dati stabilito con vEdge1 e altri siti (connettività in stile a maglia completa). Non richiede alcuna configurazione speciale.

vEdge1 dispone di DIA configurato con criteri di gestione dei dati centralizzati.

Qui è possibile trovare i passaggi di configurazione di vEdge1.

1. Attivare Network Address Translation (NAT) sull'interfaccia di trasporto, dove DIA deve essere utilizzato:

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

2. Aggiungere la route statica **ip route 0.0.0.0/0 null0** in una VPN del servizio per annunciare il valore predefinito alle diramazioni:

```
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. Verificare se RIB contiene il ciclo di lavorazione predefinito:

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

4. Verificare che vEdge1 abbia annunciato la route predefinita tramite 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. Verificare che il criterio non sia presente in vEdge1 e che DIA non sia abilitato:

```

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

```

6. Controllare la programmazione FIB (Forwarding Information Base). Dovrebbe mostrare l'assenza route (Blackhole) per la destinazione su Internet perché DIA non è abilitato:

```

vedgel# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.40.4 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Blackhole

```

Configurazione centralizzata delle regole dei dati vSmart per 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

```

Applicare i criteri dati vSmart nella sezione **apply-policy** della configurazione vSmart o attivarli nell'interfaccia utente di vManage.

7. Verificare che vEdge1 abbia ricevuto correttamente i criteri dati da vSmart:

```

vedgel# 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. Controllare la programmazione Forwarding Information Base (FIB), che mostra possibili route

per la destinazione su Internet:

```
vedgel# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.40.4 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Remote
Remote IP:173.37.145.84, Interface ge0/0 Index: 4
```

## 9. Confermare la raggiungibilità alla destinazione su Internet:

```
vedgel# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.192 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.246 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.236 ms ^C --- 173.37.145.84 ping
statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2000ms rtt
min/avg/max/mdev = 0.245/0.221/0.192/0.021 ms
```

## Passaggi verifica vEdge2:

### 1. Confermare che la route predefinita è stata ricevuta e installata correttamente in 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. Controllare la programmazione Forwarding Information Base (FIB), che mostra possibili percorsi per la destinazione su 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. Confermare la raggiungibilità alla destinazione su 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. Confermare che DIA funziona e possiamo vedere la sessione Internet Control Message Protocol (ICMP) a 173.37.145.84 da vEdge2 nelle traduzioni NAT

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

```

PUBLIC PUBLIC PRIVATE PRIVATE PRIVATE
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:** Questa soluzione consente di organizzare la ridondanza o la condivisione del carico con diverse uscite regionali.  
Non funziona con i router IOS-XE

## Soluzione 4: Inserire il percorso predefinito per OMP quando viene utilizzato DIA locale.

Questa soluzione può essere utilizzata sia per i router SD-WAN basati su IOS-XE che Viptela OS.

In breve, in questa soluzione, una route predefinita per DIA (0.0.0.0/0 Null0) viene suddivisa in due sottoreti 0.0.0.0/1 e 128.0.0.0/1 che puntano a Null0. Questa operazione viene eseguita per evitare la sovrapposizione di una route predefinita che deve essere annunciata alle diramazioni e la route predefinita, utilizzata per DIA locale. Nelle route IOS-XE utilizzate per DIA, la distanza amministrativa (AD) è uguale a 6, mentre AD con valore statico predefinito è 1. Il vantaggio della soluzione è la possibilità di utilizzare lo schema di ridondanza quando il DIA regionale è configurato in due posizioni diverse.

### 1. Attivare NAT su un'interfaccia di trasporto

 CONFIGURATION | TEMPLATES

---

Device **Feature**

Feature Template > VPN Interface Ethernet

Basic Configuration Tunnel **NAT** VRRP ACL/QoS ARP

---

**NAT**

NAT  On  Off

2. In un modello di funzionalità per una VPN di servizio, in cui dovrebbe essere utilizzata la funzione DIA, aggiungere le seguenti route IPv4 statiche:

- 0.0.0.0/1 e 128.0.0.0/1 che puntano a VPN. Queste route vengono utilizzate per DIA
- 0.0.0.0/0 che punta a Null 0. Questa route viene utilizzata per la pubblicità tramite OMP alle filiali

### (simile alla soluzione 3)

CONFIGURATION | TEMPLATES

Device Feature

Feature Template - VPN

Basic Configuration DNS Advertise OMP **IPv4 Route** IPv6 Route Service GRE Route IPSEC Route

#### IPv4 ROUTE

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

Distance 1

### 3. Verificare che le route siano state aggiunte correttamente al RIB:

```
cedgel#show ip route vrf 40
```

```
Routing Table: 40
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
```

```
        n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA, i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
        ia - IS-IS inter area, * - candidate default, U - per-user static route, o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
```

```
        a - application route, + - replicated route, % - next hop override, p - overrides from PFR
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
S*    0.0.0.0/0 is directly connected, Null0                <<<<==== Static route to null0
that will be advertised to branches via OMP n Nd 0.0.0.0/1 [6/0], 00:08:23, Null0 <<<<==== DIA
route n Nd 128.0.0.0/1 [6/0], 00:08:23, Null0 <<<<==== DIA route 192.40.1.0/32 is subnetted, 1
subnets m 192.40.1.1 [251/0] via 192.168.30.207, 3d01h 192.40.2.0/32 is subnetted, 1 subnets m
192.40.2.1 [251/0] via 192.168.30.208, 3d01h
```

### 4. Verificare che DIA funzioni correttamente localmente:

```
cedgel#ping vrf 40 173.37.145.84
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 173.37.145.84, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

### 5. Verificare che la route predefinita sia stata annunciata a una filiale e installata in 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. Verificare che DIA funzioni correttamente 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. Controllare sul router DIA regionale la traduzione NAT riuscita.

```
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:** Questa soluzione consente di organizzare la ridondanza o la condivisione del carico con diverse uscite regionali.

**Nota:** [CSCvr72329 - richiesta di miglioramento "Ridistribuzione route NAT a OMP"](#)

## Informazioni correlate

- [Criteri dati centralizzati](#)
- [Configurazione dei criteri dati centralizzati](#)
- [Esempi di configurazione dei criteri dati centralizzati](#)
- [Protocollo di routing OMP](#)
- [Configurazione di OMP](#)