

특정 사이트를 선호하는 지역 인터넷 브레이크아웃 사이트로 선택하는 방법

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[솔루션 1:Next-Hop 변경을 위한 중앙 집중식 데이터 정책 사용](#)

[솔루션 2:필요한 GRE\IPSec\NAT Default Route to OMP을 삽입합니다.](#)

[솔루션 3:DIA에 중앙 데이터 정책이 사용되는 경우 OMP에 기본 경로를 삽입합니다.](#)

[솔루션 4:로컬 DIA를 사용할 때 OMP에 기본 경로를 삽입합니다.](#)

[관련 정보](#)

소개

이 문서에서는 DIA(Direct Internet Access) 및 중앙 집중식 데이터 정책의 도움으로 특정 지사 vEdge를 기본 지역 인터넷 브레이크아웃으로 구성하기 위해 SD-WAN 패브릭을 구성하는 방법에 대해 설명합니다. 예를 들어 지역 사이트에서 Zscaler®와 같은 중앙 집중식 서비스를 사용하고 기본 인터넷 종료 지점으로 사용해야 하는 경우 이 솔루션이 유용할 수 있습니다. 이러한 구축을 위해서는 전송 VPN에서 GRE(Generic Routing Encapsulation) 또는 IPSec(Internet Protocol Security) 터널을 구성해야 하며 데이터 흐름은 트래픽이 직접 인터넷에 도달하는 일반 DIA 솔루션과 다릅니다.

사전 요구 사항

요구 사항

Cisco에서는 이 주제에 대해 알고 있는 것이 좋습니다.

- SD-WAN 정책 프레임워크에 대한 기본적인 이해

사용되는 구성 요소

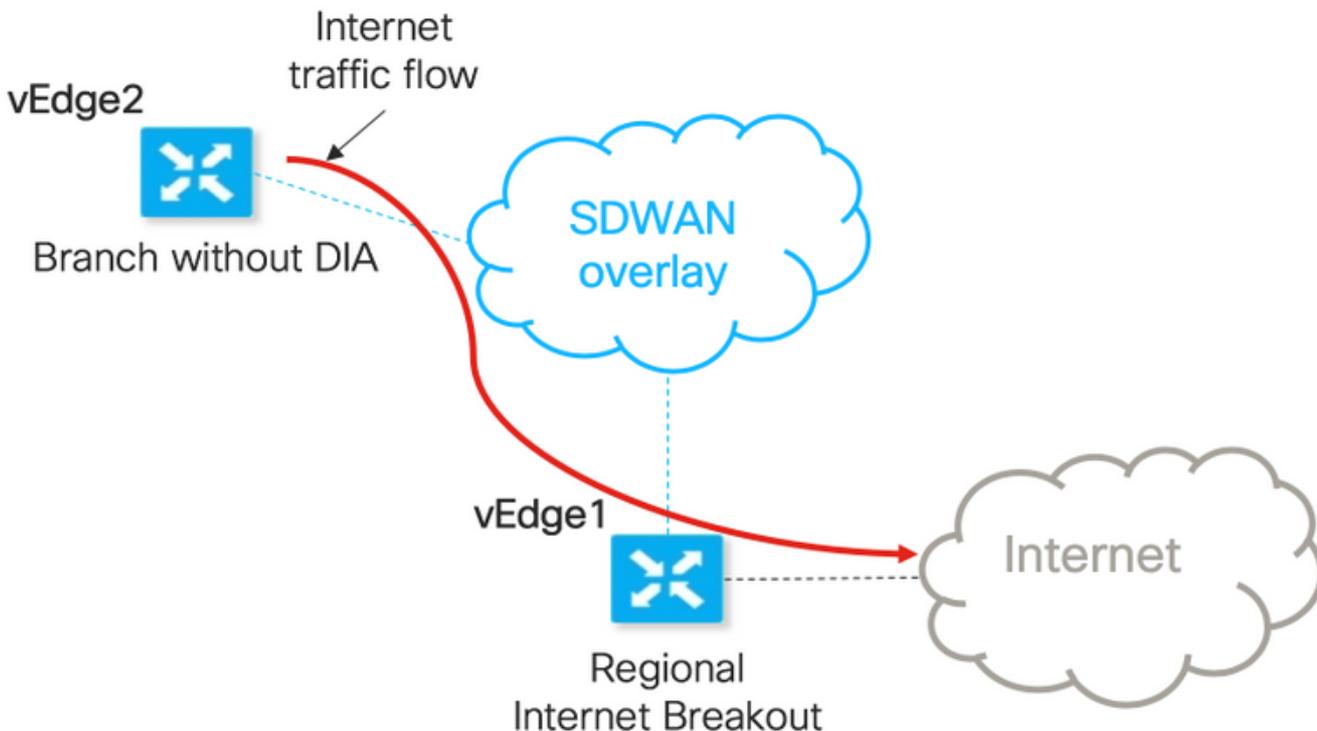
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- vEdge 라우터
- 18.3.5 소프트웨어 버전이 포함된 vSmart Controller

배경 정보

인터넷에 도달해야 하는 vEdge2의 서비스 VPN 트래픽은 데이터 평면 터널을 사용하여 다른 브랜치 vEdge1로 전달됩니다.vEdge1은 DIA가 로컬 인터넷 분할을 위해 구성된 라우터입니다.

네트워크 다이어그램



호스트 이름	vEdge1	vEdge2
호스트 역할	DIA가 있는 지사 장치(지역별 인터넷 분할)	DIA가 구성되지 않은 지사 장치
VPN 0		
TLOC(전송 위치) 1	biz-internet, ip: 192.168.110.6/24	biz-internet, ip: 192.168.110.5/24
전송 위치(TLOC) 2	공용 인터넷, ip: 192.168.109.4/24	공용 인터넷, ip: 192.168.109.5/24
서비스 VPN 40	인터페이스 ge0/1, ip: 192.168.40.4/24	인터페이스 ge0/2, ip: 192.168.50.4/24

구성

솔루션 1:Next-Hop 변경을 위한 중앙 집중식 데이터 정책 사용

vEdge2에는 vEdge1 및 기타 사이트(풀 메시 스타일 연결)와 함께 설정된 데이터 플레인 터널이 있습니다.

vEdge1에는 `ip route 0.0.0.0/0 vpn 0`으로 구성된 DIA가 있습니다.

vSmart 중앙 집중식 데이터 정책 구성:

```

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 - 특별한 구성이 필요하지 않습니다.

여기에서 정책이 올바르게 적용되었는지 확인하는 단계를 찾을 수 있습니다.

1. vEdge2에 정책이 없는지 확인합니다.

```

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

```

2. FIB(Forwarding Information Base) 프로그래밍을 확인합니다. 인터넷에서 대상에 대한 경로 부재 (Blackhole)가 표시되어야 합니다.

```

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. vSmart 컨피그레이션의 **적용 정책** 섹션에서 vSmart 데이터 정책을 적용하거나 vManage GUI에서 활성화합니다.

4. vEdge2가 vSmart에서 데이터 정책을 성공적으로 수신했는지 확인합니다.

```

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. 인터넷에서 목적지에 대한 가능한 경로를 표시하는 FIB(Forwarding Information Base) 프로그래밍을 확인합니다.

```
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. 인터넷에서 목적지에 연결할 수 있는지 확인합니다.

```
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
```

여기서 vEdge1 컨피그레이션 단계를 확인할 수 있습니다.

1. DIA를 사용해야 하는 전송 인터페이스에서 NAT(Network Address Translation)를 활성화합니다.

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

2. DIA를 활성화하려면 서비스 VPN에 고정 경로 ip 경로 0.0.0.0/0 vpn 0을 추가합니다.

```
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. RIB에 NAT 경로가 포함되어 있는지 확인합니다.

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

4. DIA가 작동하는지 확인하고 NAT 변환에서 vEdge2에서 173.37.145.84에 대한 ICMP(Internet

Control Message Protocol) 세션을 볼 수 있는지 확인합니다.

```
vedge1# show ip nat filter | tab
```

PUBLIC		PRIVATE			PRIVATE		PRIVATE						
NAT	NAT	SOURCE	DEST	FILTER	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 -													

참고: 이 솔루션은 리던던시를 구성하거나 다른 지역별 출구 사용량으로 로드 공유를 구성할 수 없습니다.

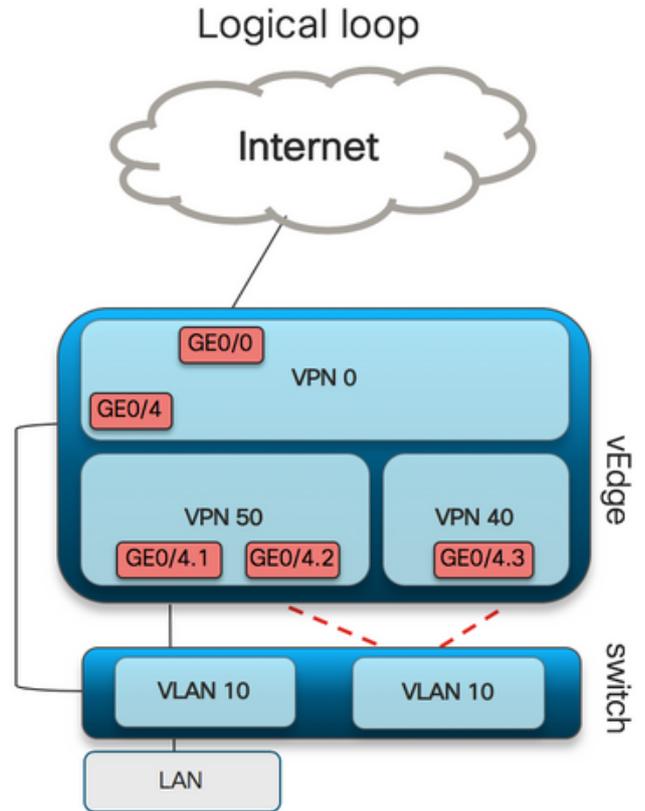
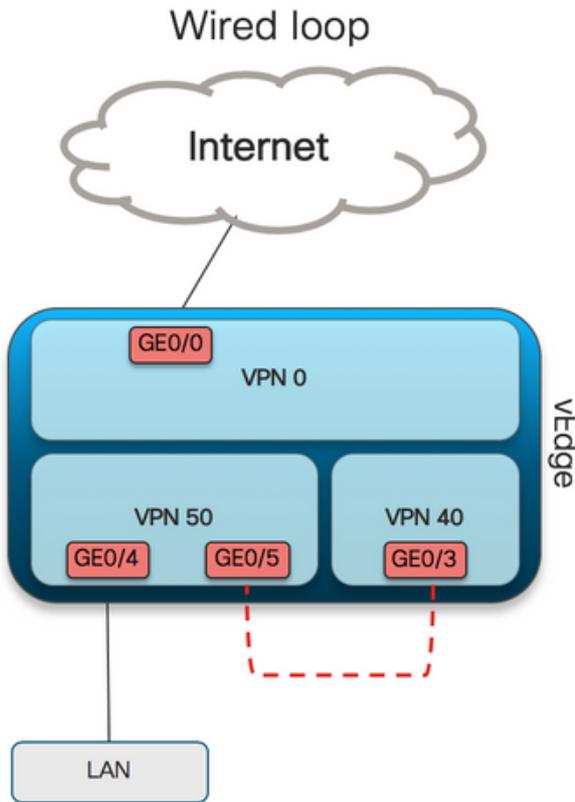
IOS-XE 라우터에서 작동하지 않음

솔루션 2: 필요한 GREIPSec\NAT Default Route to OMP을 삽입합니다.

현재로서는 vEdge1의 GREIPSec 터널을 가리키는 기본 경로를 OMP to vEdge2를 통해 광고할 가능성이 없습니다(재배포 nat route OMP 프로토콜). 향후 소프트웨어 버전에서는 동작이 변경될 수 있습니다.

당사의 목표는 vEdge2(DIA에 선호되는 디바이스)에 의해 시작되어 OMP를 통해 전파될 수 있는 일반 고정 기본 경로(IP route 0.0.0.0/0 <next-hop IP addr>)를 생성하는 것입니다.

이를 위해 더미 VPN이 vEdge1에 생성되고 물리적 포트 루프가 케이블로 수행됩니다. 루프는 더미 VPN에 할당된 포트와 고정 기본 경로가 필요한 원하는 VPN의 포트 간에 생성됩니다. 또한 아래의 그림에서 더미 VLAN과 해당 VPN에 할당된 두 개의 하위 인터페이스와 함께 스위치에 연결된 하나의 물리적 인터페이스로 루프를 생성할 수 있습니다.



vEdge1 컨피그레이션 예는 다음과 같습니다.

1. 더미 VPN을 생성합니다.

```
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. NAT 인터페이스를 가리키는 DIA 경로가 라우팅 테이블에 성공적으로 추가되었는지 FIB를 확인합니다.

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

3. 프로덕션 용도로 사용되는 서비스 VPN(일반 기본 경로가 구성된 경우 OMP에서 광고할 수 있음)

```
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. RIB에서 루프 인터페이스를 가리키는 기본 경로가 있는지 확인합니다.

```
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. vEdge1에서 OMP를 통해 기본 경로를 광고했는지 확인합니다.

```
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. vEdge2에는 어떤 컨피그레이션도 필요하지 않습니다. 기본 경로는 OMP를 통해 수신되며, vEdge1을 가리킵니다.

```
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. 연결 173.37.145.84 확인

```
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
```

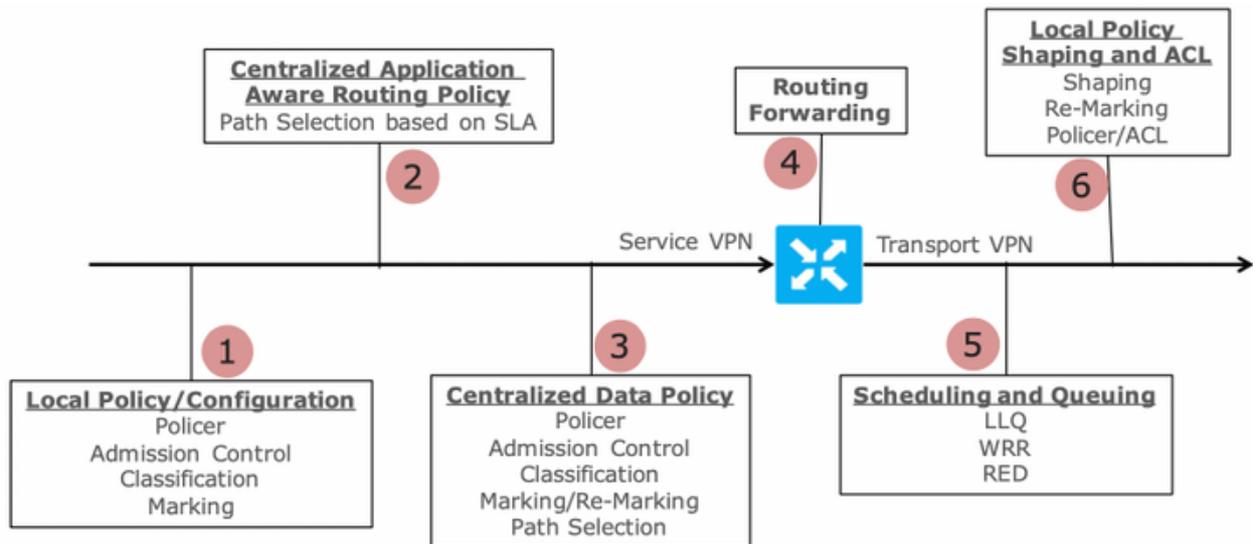
참고: 이 솔루션을 사용하면 리던던시 또는 로드 공유를 서로 다른 지역별 출구 사용량으로 구성할 수 있습니다.

IOS-XE 라우터에서 작동하지 않음

솔루션 3: DIA에 중앙 데이터 정책이 사용되는 경우 OMP에 기본 경로를 삽입합니다.

중앙 집중식 데이터 정책이 로컬 DIA에 사용되는 경우 기본 경로를 삽입하는 가능한 방법으로 이 고정 기본 경로의 사용인 DIA가 있는 지역 디바이스를 가리킵니다(ip route 0.0.0.0/0 Null0).

내부 패킷 흐름으로 인해 브랜치에서 오는 트래픽은 데이터 정책 덕분에 DIA에 도달하고 Null0으로의 경로에 도달하지 않습니다. 여기에서 볼 수 있듯이 next-hop 조회는 정책 배포 후에만 발생합니다.



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

vEdge2에는 vEdge1 및 기타 사이트(풀 메시 스타일 연결)와 함께 설정된 데이터 플레인 터널이 있습니다. 특별한 구성이 필요하지 않습니다.

vEdge1에는 중앙 집중식 데이터 정책으로 구성된 DIA가 있습니다.

여기서 vEdge1 컨피그레이션 단계를 확인할 수 있습니다.

1. DIA를 사용해야 하는 전송 인터페이스에서 NAT(Network Address Translation)를 활성화합니다.

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

2. 서비스 VPN에서 고정 경로 ip 경로 0.0.0.0/0 null0을 추가하여 기본 경로를 브랜치에 광고합니다.

```
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. RIB에 기본 경로가 포함되어 있는지 확인합니다.

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

4. vEdge1에서 OMP를 통해 기본 경로를 광고했는지 확인합니다.

```
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. vEdge1에 정책이 없고 DIA가 활성화되지 않았는지 확인합니다.

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

6. FIB(Forwarding Information Base) 프로그래밍을 확인합니다. DIA를 사용할 수 없으므로 인터넷에서 대상에 대한 경로 부재(Blackhole)가 표시되어야 합니다.

```
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
```

DIA를 위한 vSmart 중앙 집중식 데이터 정책 구성:

```
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
```

vSmart 컨피그레이션의 **apply-policy** 섹션에서 vSmart 데이터 정책을 적용하거나 vManage GUI에서 활성화합니다.

7. vEdge1이 vSmart에서 데이터 정책을 성공적으로 수신했는지 확인합니다.

```
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. 인터넷에서 목적지에 대한 가능한 경로를 표시하는 FIB(Forwarding Information Base) 프로그래밍을 확인합니다.

```
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. 인터넷에서 목적지에 연결할 수 있는지 확인합니다.

```
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
```

vEdge2 확인 단계:

1. 기본 경로를 성공적으로 수신하여 RIB에 설치했는지 확인합니다.

```
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. 인터넷에서 목적지에 대한 가능한 경로를 표시하는 FIB(Forwarding Information Base) 프로그래밍을 확인합니다.

```
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. 인터넷에서 목적지에 연결할 수 있는지 확인합니다.

```
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. DIA가 작동하는지 확인하고 NAT 변환에서 vEdge2에서 173.37.145.84에 대한 ICMP(Internet Control Message Protocol) 세션을 볼 수 있는지 확인합니다.

```
vedgel# 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
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 -
```

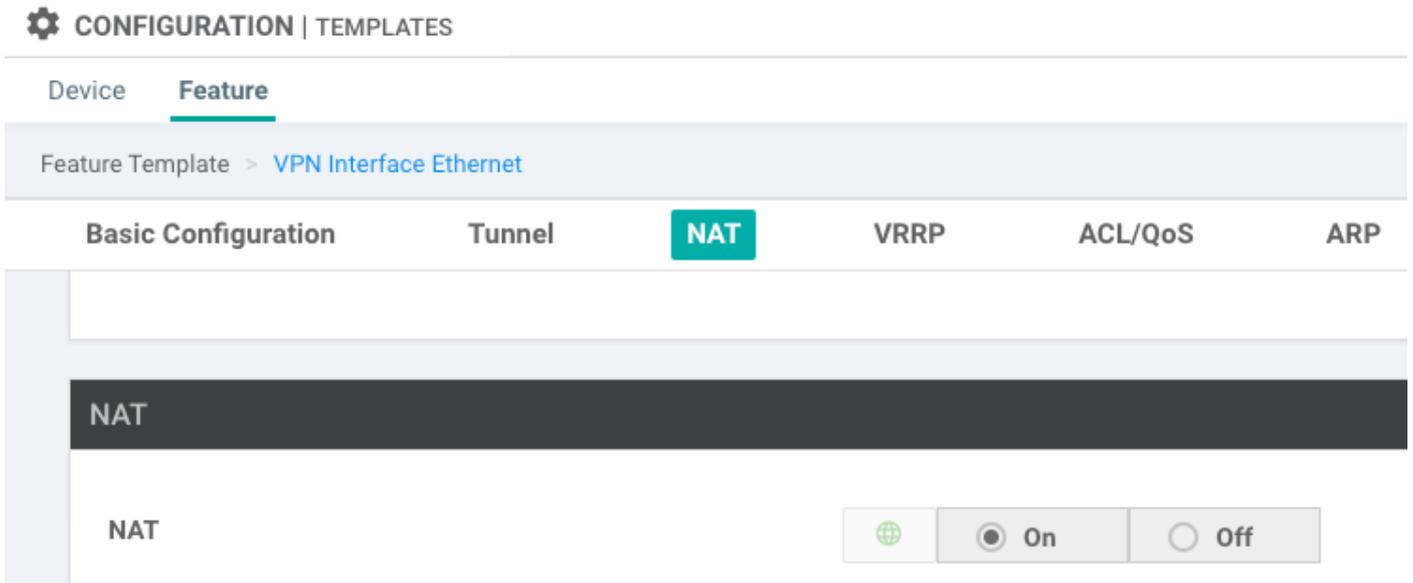
참고: 이 솔루션을 사용하면 리던던시 또는 로드 공유를 서로 다른 지역별 출구 사용량으로 구성할 수 있습니다.
IOS-XE 라우터에서 작동하지 않음

솔루션 4: 로컬 DIA를 사용할 때 OMP에 기본 경로를 삽입합니다.

이 솔루션은 IOS-XE 및 Viptela OS 기반 SD-WAN 라우터에 모두 사용할 수 있습니다.

간단히 말해, 이 솔루션에서 DIA(0.0.0.0/0 Null0)에 대한 기본 경로는 Null0을 가리키는 두 개의 하위 네트워크 0.0.0.0/1 및 128.0.0.0/1으로 분할됩니다. 이 단계는 로컬 DIA에 사용되는 기본 경로와 브랜치에 광고해야 하는 기본 경로가 중복되지 않도록 하기 위해 수행됩니다. DIA에 사용되는 IOS-XE 경로에서 AD(관리 거리)는 6이고, 고정 기본값은 1입니다. 이 솔루션의 이점은 Regional DIA가 서로 다른 두 위치에 구성된 경우 이중화 스키마를 사용할 수 있다는 것입니다.

1. 전송 인터페이스에서 NAT를 활성화합니다.



2. 서비스 VPN의 기능 템플릿에서 DIA를 사용해야 하는 경우 다음 고정 IPv4 경로를 추가합니다.

- VPN을 가리키는 0.0.0.0/1 및 128.0.0.0/1 이러한 경로는 DIA에 사용됩니다.

- 0.0.0.0/0이 Null 0을 가리킵니다. 이 경로는 OMP를 통해 브랜치에 광고하는 데 사용됩니다(솔루션 3과 유사).

IPv4 ROUTE			
Optional	Prefix	Gateway	Selected Gateway Configuration
<input type="checkbox"/>	0.0.0.0/1	VPN	Enable VPN On
<input type="checkbox"/>	128.0.0.0/1	VPN	Enable VPN On
<input type="checkbox"/>	0.0.0.0/0	Null 0	Enable Null On
			Distance 1

3. 경로가 RIB에 성공적으로 추가되었는지 확인합니다.

```
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. DIA가 로컬에서 제대로 작동하는지 확인합니다.

```
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. 기본 경로가 브랜치에 성공적으로 광고되고 RIB에 설치되었는지 확인합니다.

```
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. DIA가 로컬에서 제대로 작동하는지 확인합니다.

```
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. Regional DIA 라우터의 성공적인 NAT 변환을 확인합니다.

```
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
```

참고: 이 솔루션을 사용하면 리던던시 또는 로드 공유를 서로 다른 지역별 출구 사용량으로 구성할 수 있습니다.

참고: [CSCvr72329 - 개선 요청 "OMP로 NAT 경로 재배포"](#)

관련 정보

- [중앙 집중식 데이터 정책](#)
- [중앙 데이터 정책 구성](#)
- [중앙 데이터 정책 컨피그레이션 예](#)
- [OMP 라우팅 프로토콜](#)
- [OMP 구성](#)