

장애 시나리오가 있는 여러 사이트에서 동일한 VPN에 대해 중복 IP 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[사양](#)

[솔루션](#)

[구성](#)

[Branch-1 구성](#)

[Branch-2 구성](#)

[DC-라우터 컨피그레이션](#)

[vSmart 정책](#)

[장애 조치 시나리오](#)

[Branch-1 트래픽 흐름 일반 시나리오](#)

[Branch-2 트래픽 흐름 일반 시나리오](#)

[실패 시나리오](#)

[Branch-1 실패 시나리오](#)

[Branch-2 실패 시나리오](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[추가 정보](#)

[시나리오-1](#)

[시나리오 2](#)

[요구 사항\(UTD 검사를 사용하는 SS-NAT\)](#)

[해결 방법](#)

소개

이 문서에서는 SD-WAN 오버레이의 여러 사이트에서 동일한 VPN에 주소 공간이 중복되는 시나리오를 설명합니다. 샘플 네트워크, 일반/장애 조치 시나리오의 트래픽 동작, 컨피그레이션 및 확인을 보여 줍니다.

사전 요구 사항

요구 사항

SD-WAN에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- SD-WAN Controller 버전 20.6.3
- Cisco IOS® XE(컨트롤러 모드에서 실행) 17.6.3a
- 호스트 디바이스(CSR1000V) 17.3.3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.


배경 정보

여기에서 당신은 이 기사에 사용된 약어 목록을 찾을 수 있습니다.

- 보안 인터넷 게이트웨이 - SIG
- 가상 라우팅 및 포워딩 - VRF
- 가상 사설망 - VPN
- 직접 인터넷 액세스 - DIA
- 네트워크 주소 변환 - NAT
- 멀티 프로토콜 레이블 스위칭 - MPLS
- Service Side Network Address Translation - SS-NAT
- 데이터 센터 - DC
- 오버레이 관리 프로토콜 - OMP
- 인터넷 프로토콜 - IP

서비스 측 NAT: 서비스 측 NAT에 대한 자세한 내용은 Cisco [문서를 참조하십시오](#).

네트워크 다이어그램

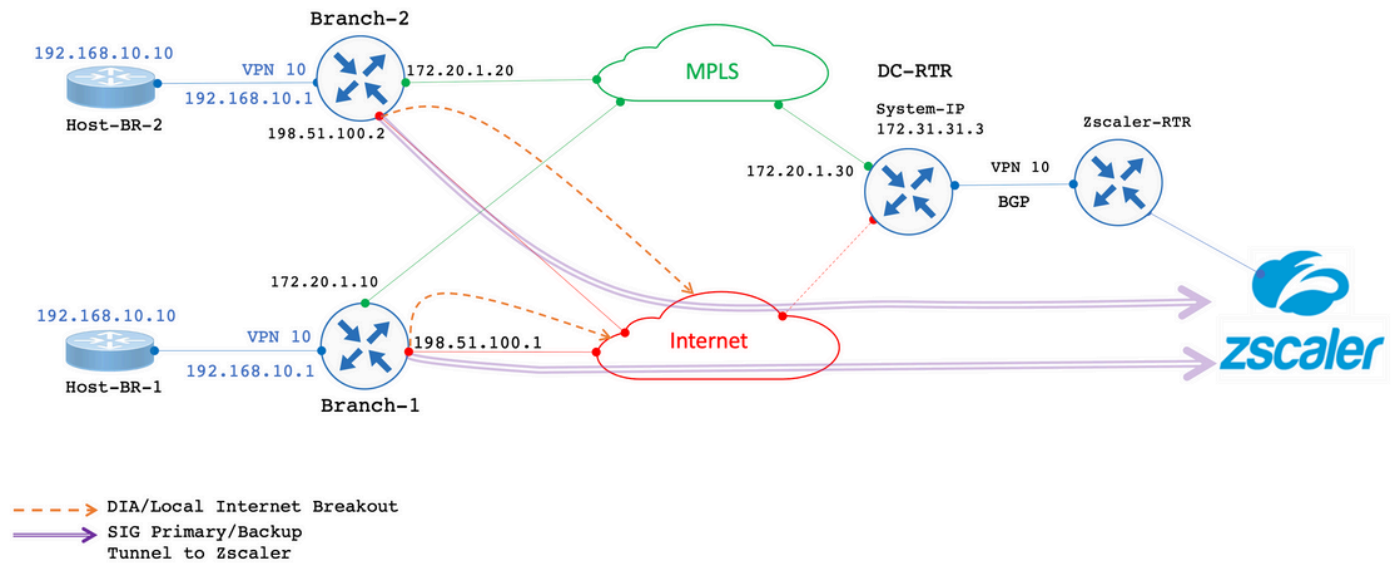
 참고: 이 토폴로지에서는 각 브랜치 라우터의 서비스 VPN 10에서 호스팅되는 디바이스에 중복 IP 192.168.10.0/24이 구성되어 있습니다.

이 특정 토폴로지에는 MPLS 및 인터넷 전송을 통해 SD-WAN 오버레이에 연결되는 1개의 DC(DC에는 MPLS 전송만 있지만 실제 시나리오에서는 여러 전송이 있을 수 있음)와 2개의 브랜치 위치가 있습니다. 모든 위치에 서비스 VPN 10이 구성되어 있습니다. 브랜치에는 Zscaler에 구성된 SIG 터널(기본 및 백업)이 있습니다. DIA는 특정 대상 IP가 Zscaler를 우회하도록 구성됩니다. 브랜치에서 인터넷 링크 장애가 발생할 경우 모든 트래픽을 MPLS 전송을 통해 DC로 전송해야 합니다.

eBGP는 서비스 VPN 10에서 Zscaler 라우터가 DC 끝에 있는 상태로 구성됩니다. DC 라우터는

Zscaler 라우터에서 기본 경로를 받아 OMP로 재배포됩니다.

 참고: 이 실습 시나리오에 언급된 공용 IP 주소는 설명서 RFC5737에서 가져옵니다.




사양

- 서비스 측 VPN 10에서 Branch-1 및 Branch-2에 대해 중복되는 IP 주소를 활용합니다.
- 일반적인 시나리오에서 MPLS 및 인터넷 전송이 가동 중일 경우 VPN 10의 트래픽은 SIG 터널을 통해 종료해야 합니다.
- 특정 IP 대상 접두사의 경우 트래픽은 SIG 터널을 우회하여 DIA를 통해 종료해야 합니다.
- 인터넷 링크 장애의 경우 VPN 10에서 모든/인터넷 바인딩 트래픽이 DC를 통해 종료되어야 합니다.

솔루션

요구 사항을 충족하기 위해 SD-WAN 기능인 서비스 측 NAT 및 DIA with Data 정책이 사용됩니다.

- 서비스 측 NAT는 서로 다른 NAT 풀 IP 주소로 각 브랜치 라우터에 구성됩니다.
- 트래픽이 SD-WAN 오버레이로 전송될 때 인터넷 링크 실패의 경우, 소스 IP는 구성된 NAT 풀의 IP 주소로 NAT됩니다.
- DC 라우터에는 겹치는 서브넷에 대한 사후 NAT 주소가 표시됩니다.

 참고: VPN 10에서 SIG 터널을 통한 일반 트래픽을 표시하려면 공용 IP 192.0.2.100이 사용되고 특정 목적지에는 DIA를 통해 192.0.2.1이 사용됩니다. 해당 컨피그레이션은 컨피그레이션 섹션에 나와 있습니다.

구성

Branch-1 구성

Branch-1 라우터 컨피그레이션은 다음과 같습니다.

```
vrf definition 10
  rd 1:10
  !
address-family ipv4
  route-target export 1:10
  route-target import 1:10
exit-address-family
!
interface GigabitEthernet2
description "Internet TLOC"
ip address 198.51.100.1 255.255.255.0
ip nat outside
!
interface GigabitEthernet3
description "MPLS TLOC"
ip address 172.20.1.10 255.255.255.0
!
interface GigabitEthernet4
description "Service Side VPN 10"
vrf forwarding 10
ip address 192.168.10.1 255.255.255.0
!
interface Tunnel2
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
!
interface Tunnel3
ip unnumbered GigabitEthernet3
tunnel source GigabitEthernet3
tunnel mode sdwan
!
interface Tunnel100512
ip address 10.10.1.1 255.255.255.252
tunnel source GigabitEthernet2
tunnel destination 203.0.113.1
tunnel vrf multiplexing
!
interface Tunnel100513
ip address 10.10.1.5 255.255.255.252
tunnel source GigabitEthernet2
tunnel destination 203.0.113.2
tunnel vrf multiplexing
!
ip sdwan route vrf 10 0.0.0.0/0 tunnel active Tunnel100512 backup Tunnel100513
ip nat pool natpool1 172.16.2.1 172.16.2.2 prefix-length 30
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat inside source list global-list pool natpool1 vrf 10 match-in-vrf overload
ip nat route vrf 10 192.0.2.1 255.255.255.255 global
!
ip route 0.0.0.0 0.0.0.0 198.51.100.100
ip route 0.0.0.0 0.0.0.0 172.20.1.100
!
```

Branch-2 구성

Branch-2 라우터 컨피그레이션은 다음과 같습니다.

```
vrf definition 10
rd 1:10
!
address-family ipv4
route-target export 1:10
route-target import 1:10
exit-address-family
!
address-family ipv6
exit-address-family
!
interface GigabitEthernet2
description "Internet TLOC"
ip address 198.51.100.2 255.255.255.0
ip nat outside
!
!
interface GigabitEthernet3
description "MPLS TLOC"
ip address 172.20.1.20 255.255.255.0
!
interface GigabitEthernet4
description "Service Side VPN 10"
vrf forwarding 10
ip address 192.168.10.1 255.255.255.0
!
interface Tunnel2
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
!
interface Tunnel3
ip unnumbered GigabitEthernet3
tunnel source GigabitEthernet3
tunnel mode sdwan
!
interface Tunnel100512
ip address 10.10.2.1 255.255.255.252
tunnel source GigabitEthernet2
tunnel destination 203.0.113.1
tunnel vrf multiplexing
!
interface Tunnel100513
ip address 10.10.2.5 255.255.255.252
tunnel source GigabitEthernet2
tunnel destination 203.0.113.2
tunnel vrf multiplexing
!
!
ip sdwan route vrf 10 0.0.0.0/0 tunnel active Tunnel100512 backup Tunnel100513
ip nat route vrf 10 192.0.2.1 255.255.255.255 global
ip nat pool natpool1 172.16.2.9 172.16.2.10 prefix-length 30
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat inside source list global-list pool natpool1 vrf 10 match-in-vrf overload
!
```

```
ip route 0.0.0.0 0.0.0.0 198.51.100.100
ip route 0.0.0.0 0.0.0.0 172.20.1.100
!
```


DC-라우터 컨피그레이션

DC 라우터 컨피그레이션은 다음과 같습니다.

```
vrf definition 10
rd 1:10
!
address-family ipv4
route-target export 10:10
route-target import 10:10
exit-address-family
!
interface Tunnel2
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
!
interface GigabitEthernet2
ip address 172.20.1.30 255.255.255.0
description "MPLS TLOC"
!
interface GigabitEthernet4
description "Service Side VPN 10"
vrf forwarding 10
ip address 172.31.19.19 255.255.255.252
!
router bgp 10
bgp log-neighbor-changes
distance bgp 20 200 20
!
address-family ipv4 vrf 10
redistribute omp
neighbor 172.31.19.20 remote-as 100
neighbor 172.31.19.20 activate
neighbor 172.31.19.20 send-community both
exit-address-family
!
!
ip route 0.0.0.0 0.0.0.0 172.20.1.100
!
```

vSmart 정책

vSmart 정책 컨피그레이션은 다음과 같습니다.

 참고: 두 브랜치에 대한 정책에서 **nat pool 1** 호출되지만 각 브랜치에 대해 서로 다른 두 IP 풀이 구성되어 있습니다 (Branch-1의 경우 172.16.2.0/30, Branch-2의 경우 172.16.2.8/30).

<#root>

```
data-policy _VPN10-VPN20_1-Branch-A-B-Central-NAT-DIA
vpn-list VPN10
sequence 1
match
source-ip 192.168.10.0/24
!
action accept

nat pool 1

!
default-action accept
!
site-list BranchA-B
site-id 11
site-id 22
!
site-list DC
site-id 33
!
vpn-list VPN10
vpn 10
!
prefix-list _AnyIpv4PrefixList
ip-prefix
0.0.0.0/0

!e 32
!
apply-policy
site-list BranchA-B
data-policy _VPN10_1-Branch-A-B-Central-NAT-DIA from-service
!
```

장애 조치 시나리오

Branch-1 트래픽 흐름 일반 시나리오

출력에 표시된 대로 두 전송이 모두 가동 상태인 경우 기본적으로 기본 SIG 터널을 통해 트래픽이 **Tunnel100512** 종료됩니다. 기본 터널이 다운되면 트래픽이 백업 터널로 **Tunnel100513** 전환됩니다.

<#root>

Branch-1#

```
show ip route vrf 10
```

Routing Table: 10

<SNIP>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```
S* 0.0.0.0/0 [2/0], Tunnel100512
```

```
192.0.2.0/32 is subnetted, 1 subnets  
n Nd 192.0.2.1 [6/0], 3d02h, Null0  
n Ni 172.16.2.0 [7/0], 3d04h, Null0  
m 172.16.2.8 [251/0] via 172.31.31.2, 3d01h, Sdwan-system-intf  
Branch-1#
```

Traceroute는 트래픽이 SIG 터널을 사용함을 보여줍니다.

```
<#root>
```

```
Host-BR-1#
```

```
ping 192.0.2.100
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/49/101 ms  
Host-BR-1#
```

```
Host-BR-1#
```

```
traceroute 192.0.2.100 numeric
```

```
Type escape sequence to abort.  
Tracing the route to 192.0.2.100  
VRF info: (vrf in name/id, vrf out name/id)  
1 192.168.10.1 38 msec 7 msec 4 msec  
  
2 203.0.113.1  
  
79 msec * 62 msec  
Host-BR-1#
```

특정 대상에 대한 트래픽은 **192.0.2.1** DIA(NATed to WAN IP address)를 통해 종료됩니다.

```
<#root>
```

```
Host-BR-1#
```

```
ping 192.0.2.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/49/101 ms  
Host-BR-1#
```

```
Branch-1#sh ip nat translation
```



```
Pro Inside global Inside local Outside local Outside global
icmp
198.51.100.1:1
  192.168.10.10:1 192.0.2.1:1 192.0.2.1:1
Total number of translations: 1
Branch-1#
```

Branch-2 트래픽 흐름 일반 시나리오

Branch-2 라우터에서도 유사한 동작이 관찰됩니다.

<#root>

Branch-2#

```
show ip route vrf 10
```

Routing Table: 10

<SNIP>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```
s* 0.0.0.0/0 [2/0], Tunnel100512
```

```
  192.0.2.0/32 is subnetted, 1 subnets
n Nd 192.0.2.1 [6/0], 00:00:08, Null0
m 172.16.2.0 [251/0] via 172.31.31.1, 3d01h, Sdwan-system-intf
n Ni 172.16.2.8 [7/0], 3d04h, Null0
```

Branch-2#

<#root>

Host-BR-2#

```
ping 192.0.2.100
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/49/101 ms

Host-BR-2#

Host-BR-2#t

```
traceroute 192.0.2.100 numeric
```

Type escape sequence to abort.

Tracing the route to 192.0.2.100

VRF info: (vrf in name/id, vrf out name/id)

```
1 192.168.10.1 38 msec 7 msec 4 msec
```

```
2 203.0.113.1
```

```
79 msec * 62 msec
```

```
Host-BR-2#
```

```
<#root>
```

```
Host-BR-2#
```

```
ping 192.0.2.1
```

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

```
Sending 5, 100-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/49/101 ms
```

```
Host-BR-2#
```

```
Branch-2#
```

```
show ip nat translation
```

```
Pro Inside global Inside local Outside local Outside global  
icmp
```

```
198.51.100.2:1
```

```
192.168.10.10:1 192.0.2.1:1 192.0.2.1:1
```

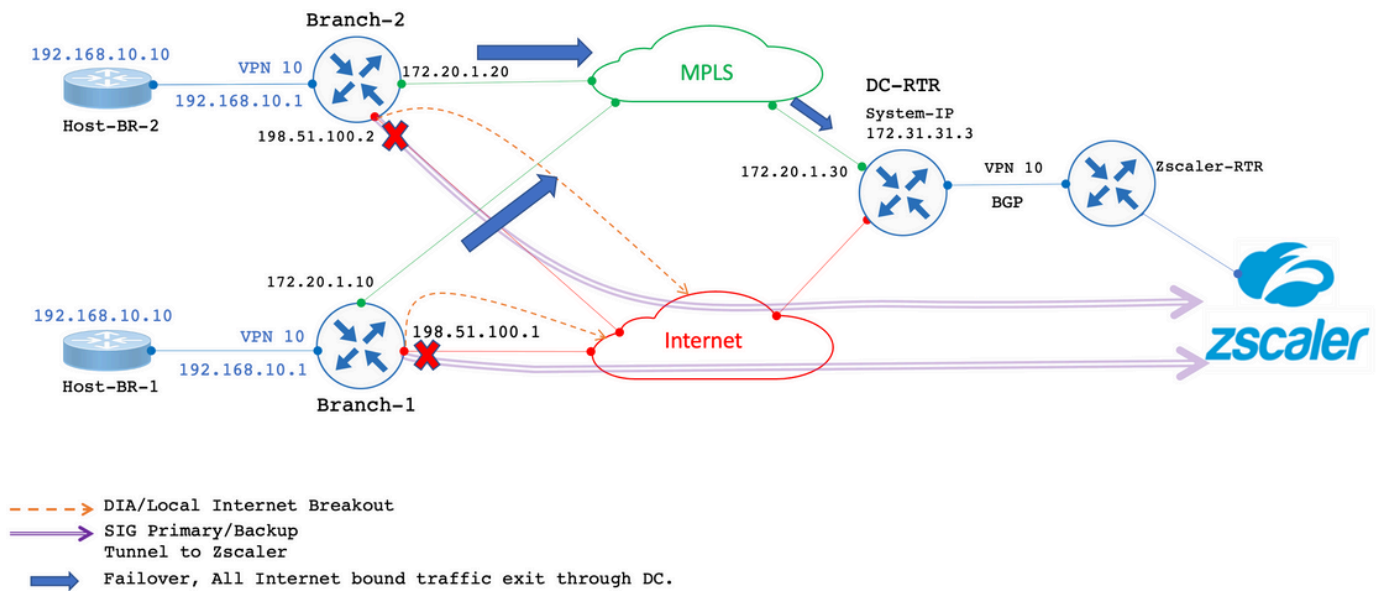
```
Total number of translations: 1
```

```
Branch-2#
```

실패 시나리오

Branch-1 실패 시나리오

이 섹션에서는 인터넷 오류 동안의 동작에 대해 설명합니다.



인터넷 링크가 관리상 종료되어 인터넷 장애 링크를 시뮬레이션합니다.

<#root>

Branch-1#

show sdwan control local-properties

<SNIP>

```

PUBLIC PUBLIC PRIVATE PRIVATE PRIVATE MAX
INTERFACE IPv4 PORT IPv4 IPv6 PORT VS/VM COLOR STATE CNTRL
-----

```

```
GigabitEthernet2 198.51.100.1 12346 198.51.100.1 :: 12346 1/0 biz-internet down
```

```
GigabitEthernet3 172.20.1.10 12346 172.20.1.10 :: 12346 1/1 mpls up
```

Branch-1#

출력은 인터넷 링크 오류 시나리오 중에 Branch-1 라우터가 OMP를 통해 DC 라우터로부터 기본 경로를 수신함을 보여줍니다. 172.31.31.3은 DC 라우터의 시스템 IP입니다.

<#root>

Branch-1#

show ip route vrf 10

<SNIP>

Gateway of last resort is

```
172.31.31.3
```

```
to network 0.0.0.0
```

```
m* 0.0.0.0/0 [251/0] via 172.31.31.3
```

```
, 00:01:17, Sdwan-system-intf  
<SNIP>
```

NAT를 192.0.2.100 서비스 측 NAT 풀로 보내고 DC를 통해 나가는 트래픽이 목적지입니다.

```
<#root>
```

```
Host-BR-1#
```

```
ping 192.0.2.100
```

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

```
Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/37/103 ms
```

```
Host-BR-1#
```

```
<#root>
```

```
Branch-1#
```

```
show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global  
icmp
```

```
172.16.2.1:3
```

```
192.168.10.1:3 192.0.2.100:3 192.0.2.100:3
```

```
Total number of translations: 1
```

```
Branch-1#
```

Traceroute 결과는 트래픽이 DC 경로를 사용함을 보여줍니다. 172.20.1.30은 DC 라우터의 MPLS 전송 WAN IP입니다.

```
<#root>
```

```
Host-BR-1#
```

```
traceroute 192.0.2.100 numeric
```

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

```
Tracing the route to 192.0.2.100
```

```
1 192.168.10.1 26 msec 5 msec 3 msec
```

```
2 172.20.1.30
```

```
10 msec 5 msec 27 msec  
<SNIP>
```

```
<#root>
```

```
Branch-1#
```

```
show sdwan bfd sessions
```

```
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX  
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec) UPTIME TRANSITION  
-----  
172.31.31.2 22 up mpls mpls 172.20.1.10 172.20.1.20 12406 ipsec 7 1000 0:14:56:54 0  
172.31.31.3 33 up mpls mpls 172.20.1.10 172.20.1.30 12406 ipsec 7 1000 0:14:56:57 0
```

```
Branch-1#
```

또한 특정 IP 192.0.2.1로 향하는 트래픽은 서비스 측 NAT 풀로 NATed를 얻고 DC를 통해 빠져나갑니다.

```
<#root>
```

```
Host-BR-1#
```

```
ping 192.0.2.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/37/103 ms  
Host-BR-1#
```

```
<#root>
```

```
Branch-1#
```

```
show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global  
icmp  
172.16.2.1:4  
192.168.10.10:4 192.0.2.1:4 192.0.2.1:4  
Total number of translations: 1  
Branch-1#
```

```
<#root>
```

Host-BR-1#

```
traceroute 192.0.2.1 numeric
```

Type escape sequence to abort.
Tracing the route to 192.0.2.1

```
1 192.168.10.1 26 msec 5 msec 3 msec
```

```
2 172.20.1.30
```

```
10 msec 5 msec 27 msec
```

<SNIP>

vSmart에서 푸시된 데이터 정책 구성:

<#root>

Branch-1#

```
show sdwan policy from-vsmart
```

```
from-vsmart data-policy _VPN10-VPN20_1-Branch-A-B-Central-NAT-DIA  
direction
```

```
from-service
```

```
vpn-list
```

```
VPN10
```

```
sequence 1
```

```
match
```

```
source-ip
```

```
192.168.10.0/24
```

```
action accept
```

```
count NAT_VRF10_BRANCH_A_B_-968382210
```

```
nat pool 1
```

```
!
```

```
from-vsmart lists vpn-list VPN10
```

```
vpn 10
```

```
!
```

```
Branch-1#
```

```
Branch-1#
```

```
show run | sec "natpool1"
```

<SNIP>

```
ip nat pool
```

```
natpool1
```

172.16.2.1

172.16.2.2

prefix-length 30

Branch-2 실패 시나리오

인터넷 장애 조치가 있을 경우 Branch-2 라우터에서도 유사한 동작이 관찰됩니다.

<#root>

Branch-2#

show sdwan control local-properties

<SNIP>

```
PUBLIC PUBLIC PRIVATE PRIVATE PRIVATE MAX
INTERFACE IPv4 PORT IPv4 IPv6 PORT VS/VM COLOR STATE CNTRL
```

```
GigabitEthernet2 198.51.100.2 12346 198.51.100.2 :: 12346 1/0 biz-internet down
```

```
GigabitEthernet3 172.20.1.20 12346 172.20.1.20 :: 12346 1/1 mpls up
```

Branch-2#

<#root>

Branch-2#

show ip route vrf 10

<SNIP>

Gateway of last resort is

172.31.31.3

to network 0.0.0.0

```
m* 0.0.0.0/0 [251/0] via 172.31.31.3
```

```
, 00:10:17, Sdwan-system-intf
```

<SNIP>

<#root>

Host-BR-2#

ping 192.0.2.100

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 10/37/103 ms

Host-BR-2#

<#root>

Branch-2#

show ip nat translations

| Pro | Inside global | Inside local | Outside local | Outside global |
|-----|---------------|--------------|---------------|----------------|
|-----|---------------|--------------|---------------|----------------|

icmp

172.16.2.9:3

192.168.10.1:3

192.0.2.100:3

192.0.2.100:3

Total number of translations: 1

Branch-2#

<#root>

Host-BR-2#

traceroute 192.0.2.100 numeric

Type escape sequence to abort.

Tracing the route to 192.0.2.100

1 192.168.10.1 26 msec 5 msec 3 msec

2 172.20.1.30

10 msec 5 msec 27 msec

<SNIP>

<#root>

Host-BR-2#

ping 192.0.2.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 10/37/103 ms

Host-BR-2#

<#root>

Branch-2#

show ip nat translations

| Pro | Inside global | Inside local | Outside local | Outside global |
|------|-----------------|--------------|---------------|----------------|
| icmp | | | | |
| | 172.16.2.9:4 | | | |
| | 192.168.10.10:4 | 192.0.2.1:4 | 192.0.2.1:4 | |

Total number of translations: 1

Branch-2#

<#root>

Host-BR-2#

traceroute 192.0.2.1 numeric

Type escape sequence to abort.

Tracing the route to 192.0.2.1

1 192.168.10.1 26 msec 5 msec 3 msec

2 172.20.1.30

10 msec 5 msec 27 msec

<SNIP>

<#root>

Branch-2#

show sdwan policy from-vsmart

from-vsmart data-policy _VPN10-VPN20_1-Branch-A-B-Central-NAT-DIA
direction

from-service

vpn-list

VPN10

sequence 1

match

source-ip

192.168.10.0/24

action accept

```
count NAT_VRF10_BRANCH_A_B_-968382210
```

```
nat pool 1
```

```
!  
from-vsmart lists vpn-list VPN10-VPN20  
  vpn 10  
!  
Branch-2#
```

```
Branch-2#
```

```
show run | sec "natpool1"
```

```
<SNIP>  
ip nat pool
```

```
natpool1
```

```
172.16.2.9
```

```
172.16.2.9
```

```
prefix-length 30
```

DC 라우터 라우팅 상태

라우팅 테이블은 DC 라우터에서 캡처됩니다.

출력에 표시된 것처럼, DC 라우터는 실제 LAN IP 대신 **SS-NAT pool** (172.16.2.0 및 172.16.2.8)에서 **post-NAT IP**파생된 를 사용하여 두 브랜치에서 중복 IP 주소 **192.168.10.0/24**를 구분할 수 **172.31.31.2** 있으며 Branch-1/Branch-2에 대해 **system-ip** 구성됩니다. System-IP가 **172.31.31.10** 속합니다 vSmart.

```
<#root>
```

```
DC-RTR#
```

```
show ip route vrf 10
```

```
Routing Table: 10
```

```
<SNIP>
```

```
m
```

```
172.16.2.0
```

```
[251/0] via 172.31.31.1, 02:44:25, Sdwan-system-intf  
m
```

```
172.16.2.8
```

```
[251/0] via 172.31.31.2, 02:43:33, Sdwan-system-intf  
m
```

```
192.168.10.0
```

```
[251/0] via
172.31.31.2
, 03:01:35, Sdwan-system-intf
[251/0] via
172.31.31.1
, 03:01:35, Sdwan-system-intf
```

DC-RTR#

show sdwan omp routes

<SNIP> PATH ATTRIBUTE
VPN PREFIX FROM PEER ID LABEL STATUS TYPE TLOC IP COLOR ENCAP PREFERENCE

```
-----
10 172.16.2.0/30
   172.31.31.10 6 1002 C,I,R installed
172.31.31.1 mpls
   ipsec -
   172.31.31.10 10 1002 Inv,U installed 172.31.31.1 biz-internet ipsec -
10 172.16.2.8/30
   172.31.31.10 8 1002 C,I,R installed
172.31.31.2 mpls
   ipsec -
10 192.168.10.0/24
   172.31.31.10 1 1002 C,I,R installed
172.31.31.1 mpls
   ipsec -
   172.31.31.10 2 1002 C,I,R installed
172.31.31.2 mpls
   ipsec -
   172.31.31.10 12 1002 Inv,U installed
172.31.31.1
   biz-internet ipsec -
```

다음을 확인합니다.

현재 이 구성에 사용할 수 있는 특정 확인 절차가 없습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

추가 정보

시나리오-1

컨트롤러가 버전 20.3.4에 있고 cEdge가 동일한 컨피그레이션으로 17.3.3a 이하 버전을 실행하는 시나리오에서 일반/장애 조치 시나리오에서 트래픽은 서비스 측 NAT 풀로 NAT되고 흐름이 끊어집니다.

cEdge 캡처:

<#root>

Host-BR-1#

ping 192.0.2.100

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:

U.U.U

Success rate is 0 percent (0/5)

Host-BR-1#

<#root>

Branch-1#

show ip nat translations

Pro Inside global Inside local Outside local Outside global
icmp

172.16.2.1

:3 192.168.10.1:3 192.0.2.100:3 192.0.2.100:3

Total number of translations: 1

Branch-1#

WOW-Branch-1#show run | sec "natpool1"

<SNIP>

ip nat pool

natpool1

172.16.2.1

172.16.2.2

prefix-length 30

출력은 17.3.3a 버전에서 실행되는 cEdge에서 캡처됩니다. SIG 터널을 통해 전달되는 트래픽은 SS-NAT 풀로 NAT되고 삭제됩니다.

버전 17.3.6 이상에서 수정 기능을 사용할 수 있습니다.

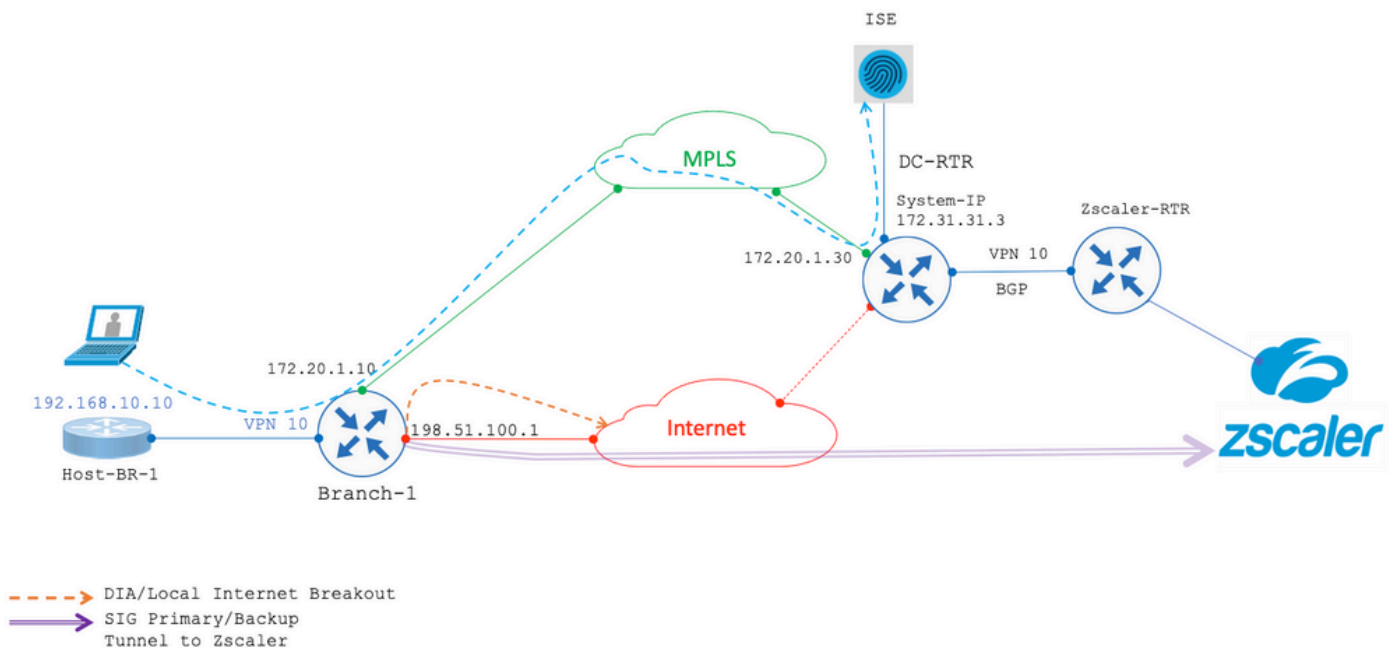
시나리오 2

요구 사항(UTD 검사를 사용하는 SS-NAT)

사용자가 다음 요구 사항을 요청했다고 가정합니다.

1. 인터넷과 MPLS 전송이 모두 작동하는 경우, VPN 10의 무선 클라이언트가 데이터 센터의 ISE로 전달되어 인증될 수 있습니다. 또한 SD-WAN 오버레이를 통해 이동하는 VPN 10 트래픽은 검사를 받을 수 있습니다. 이 트래픽은 오버레이의 일부이므로 VPN 10은 SS-NAT 기능을 사용합니다. [UTD + SS-NAT]
2. 인터넷 전송을 사용할 수 없게 되면 VPN 10의 모든 트래픽(무선 및 유선 트래픽 모두 포함)이 MPLS 전송을 사용하여 오버레이를 통해 라우팅될 수 있습니다. 이 트래픽도 검사 대상이 될 수 있습니다. [UTD + SS-NAT]

이러한 요구 사항은 서로 다른 네트워크 조건에서 Branch-1의 VPN 10에 대해 안전하고 모니터링되는 트래픽 흐름을 보장하는 것을 목표로 합니다.



앞서 언급한 두 시나리오 모두 SS-NAT 조합이 포함된 UTD 검사가 있습니다. 이 시나리오의 샘플 UTD 컨피그레이션입니다.

```
policy utd-policy-vrf-10
all-interfaces
vrf 10
threat-inspection profile TEST_IDS_Policy
exit
```



경고: 현재 UTD와 SS-NAT의 조합은 지원되지 않습니다. 따라서 이 조합은 예상대로 작동하지 않습니다. 이 문제에 대한 해결 방법은 향후 릴리스에 포함될 수 있습니다.

해결 방법

해결 방법은 Overlapping IP VPN(이 경우 VPN 10)에서 UTD 정책을 비활성화하고 Global VPN을 활성화하는 것입니다.

참고: 이 컨피그레이션은 17.6 버전에서 테스트 및 검증되었습니다.

```
policy utd-policy-vrf-global
all-interfaces
vrf global
threat-inspection profile TEST_IDS_Policy
exit
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.