Configuración de IP superpuesta para la misma VPN en varios sitios con escenarios de fallas

Contenido

Introducción

Este documento describe el escenario con superposición de espacios de dirección en la misma VPN a través de múltiples sitios en la superposición SD-WAN. Representa la red de ejemplo, el comportamiento del tráfico en escenarios normales/de failover, la configuración y la verificación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos de SD-WAN.

Componentes Utilizados

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

- Controlador SD-WAN versión 20.6.3
- Cisco IOS® XE (ejecución en modo de controlador) 17.6.3a
- Dispositivos host (CSR1000V) 17.3.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Aquí puede encontrar una lista de acrónimos utilizados en este artículo.

- Gateway de Internet seguro - SIG
- Routing y reenvío virtual - VRF
- Red privada virtual: VPN
- Acceso directo a Internet - DIA
- Traducción de direcciones de red - NAT
- Switching de etiquetas multiprotocolo - MPLS
- Traducción de direcciones de red del lado de servicio - SS-NAT
- Data Center - DC
- Protocolo de administración de superposición - OMP
- Protocolo de Internet: IP

Consulte el documento de Cisco para obtener más detalles sobre la NAT del lado de servicio: [NAT del lado de servicio]

Diagrama de la red

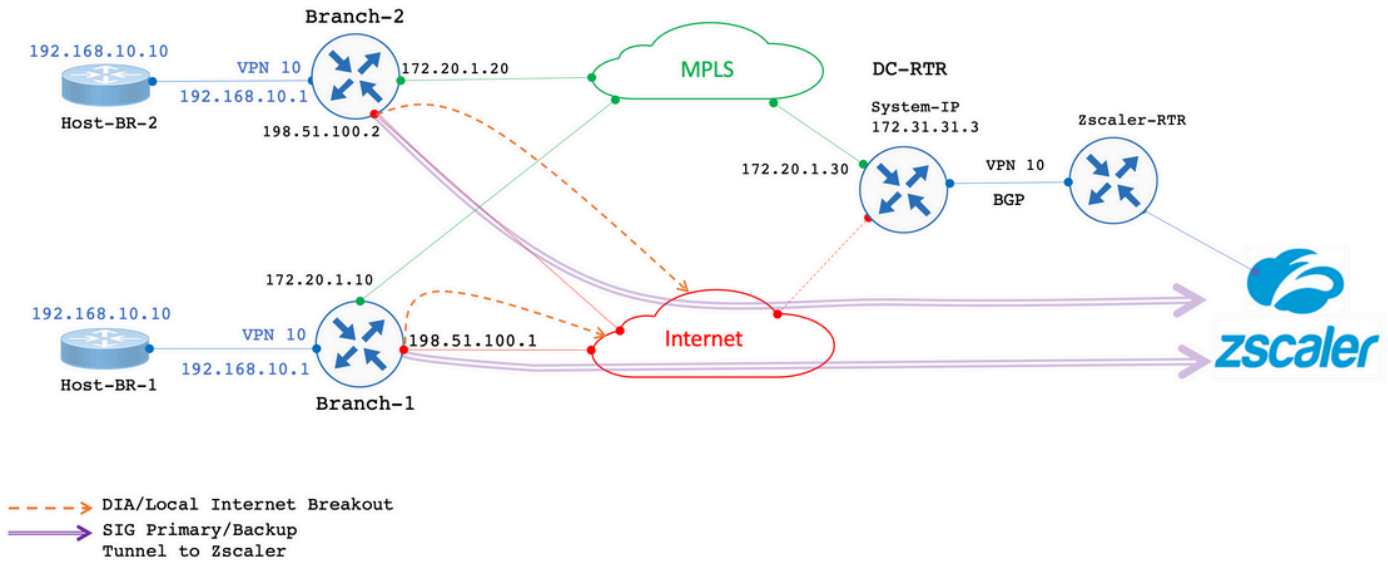
Nota: En esta topología, los dispositivos alojados en el servicio VPN 10 de cada router de sucursal tienen IP 192.168.10.0/24 configurado.

En esta topología específica, hay 1 DC (DC solo tiene transporte MPLS, pero en un escenario real puede haber varios transportes) y 2 ubicaciones de sucursal que tienen conectividad a la superposición SD-WAN sobre MPLS y transporte de Internet. El servicio VPN 10 está configurado en todas las ubicaciones. Las sucursales tienen un túnel SIG (principal y de reserva) configurado

en Zscaler. DIA está configurado para que ciertas IP de destino específicas omitan Zscaler. En caso de que el link de Internet falle en las sucursales, se espera que todo el tráfico se envíe al DC a través del transporte MPLS.

eBGP se configura en el servicio VPN 10 con el router Zscaler en el extremo DC. El router DC recibe la ruta predeterminada del router Zscaler y se redistribuye en OMP.

Nota: Las direcciones IP públicas mencionadas en este escenario de laboratorio se toman de la documentación RFC5737.



Especificación

- Aproveche las direcciones IP superpuestas para la sucursal 1 y la sucursal 2 en la VPN 10 del lado del servicio.

- En un escenario típico, cuando MPLS y el transporte de Internet están activos, el tráfico de VPN 10 debe salir a través del túnel SIG.
- Para prefijos de destino IP específicos, el tráfico debe omitir el túnel SIG y salir a través de DIA.
- En caso de fallo del enlace de Internet, todo el tráfico entrante o saliente de Internet desde VPN 10 debe salir a través del DC.

Solución

Para lograr el requisito, se utilizan las funciones de SD-WAN NAT del lado de servicio y DIA con política de datos.

- La NAT del lado de servicio se configura en cada router de sucursal con diferentes direcciones IP de grupos de NAT.
- En caso de fallo del enlace de Internet cuando el tráfico se envía a la superposición SD-

WAN, la IP de origen se NATed a la dirección IP del conjunto NAT configurado.
- El router DC ve la dirección post-NAT para las subredes superpuestas.

Nota: Para representar el tráfico normal a través del túnel SIG desde VPN 10, se utiliza la IP pública 192.0.2.100 y para un destino específico, a través de DIA, se utiliza 192.0.2.1. Las configuraciones correspondientes se muestran en la sección de configuración.

Configurar

Configuración de la sucursal 1

La configuración del router Branch-1 es la siguiente.

```
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
!
```

Configuración de la sucursal 2

La configuración del router de la sucursal 2 es la siguiente.

```
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
!
```

Configuración del router DC

La configuración del router DC es la siguiente.

```
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
!
```

Política vSmart

La configuración de la política vSmart es la siguiente.

> Nota: tenga en cuenta que **nat pool 1** se llama en la política para ambas sucursales; sin embargo, hay dos grupos IP diferentes configurados para cada sucursal (172.16.2.0/30 para la sucursal 1 y 172.16.2.8/30 para la sucursal 2).

<#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

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

Escenarios de Failover

Situación normal de flujo de tráfico de la sucursal 1

Cuando ambos transportes están activos como se muestra en la salida, el tráfico por defecto sale a través del túnel SIG primario **Tunnel100512**. Cuando el túnel principal deja de funcionar, el tráfico pasa al túnel de respaldo **Tunnel100513**.

<#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#
```

Traceroute muestra que el tráfico toma el túnel SIG.

<#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#
```

El tráfico a un destino específico **192.0.2.1** sale a través de DIA (NAT a dirección IP de WAN).

<#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#
```

Situación normal de flujo de tráfico de la sucursal 2

También se observa un comportamiento similar en el router de la sucursal 2.

<#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
```

raceroute 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
```

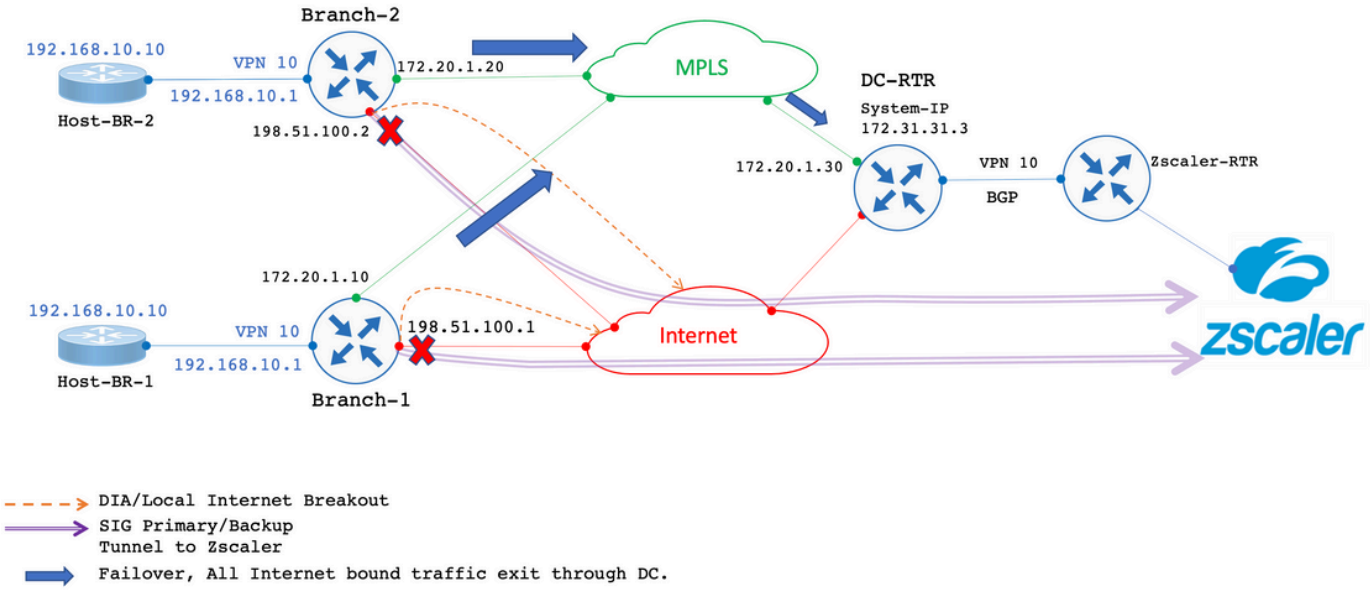
198.51.100.2:1

```
 192.168.10.10:1 192.0.2.1:1 192.0.2.1:1
Total number of translations: 1
Branch-2#
```

Escenarios de fallos

Escenario de fallo de la sucursal 1

En esta sección se describe el comportamiento durante el fallo de Internet.



El enlace de Internet se apaga administrativamente para simular un enlace de fallo de Internet.

<#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#
```

Los resultados muestran que durante el escenario de falla del link de Internet, el router Branch-1 recibe la ruta predeterminada del router DC a través de OMP. **172.31.31.3** es la dirección IP del sistema para el router DC.

<#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>

El tráfico destinado a 192.0.2.100 obtiene NATed al conjunto NAT del lado del servicio y sale a través del DC.

<#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#

Los resultados de traceroute muestran que el tráfico toma la ruta DC. 172.20.1.30 es la IP de WAN de transporte MPLS del router DC.

<#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#

El tráfico destinado a IP 192.0.2.1 específica también recibe NATed al conjunto NAT del lado del servicio y sale a través del DC.

<#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>
```

Configuración de la política de datos transferida desde vSmart:

<#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

Escenario de fallo de la sucursal 2

También se observa un comportamiento similar en los routers de la sucursal 2 cuando hay una falla de Internet.

<#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

Estado de enrutamiento del router DC

La tabla de ruteo captura desde el router DC.

Como se muestra en el resultado, el router DC puede diferenciar las direcciones IP superpuestas de ambas ramas con el **post-NAT IP**derivado de **SS-NAT pool** (172.16.2.0 y 172.16.2.8) en lugar de la IP LAN real **192.168.10.0/24172.31.31.1** y **172.31.31.2** son el **system-ip** configurado para la sucursal-1/sucursal-2. System-IP **172.31.31.10** pertenece a **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 -
```

Verificación

Actualmente no hay ningún procedimiento de verificación específico disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Additional Information

Escenario 1

En los escenarios donde los controladores están en la versión 20.3.4 y cEdge ejecuta la versión 17.3.3a o versiones inferiores con las mismas configuraciones, se observa que en escenarios normales/de failover el tráfico se NATed al conjunto NAT del lado del servicio y rompe el flujo.

cEdge captura:

<#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
```

El resultado se captura de las ejecuciones de cEdge en la versión 17.3.3a. El tráfico destinado a través del túnel SIG se NATed al conjunto SS-

NAT y se descarta. Hay una corrección disponible a partir de la versión 17.3.6.

Situación 2:

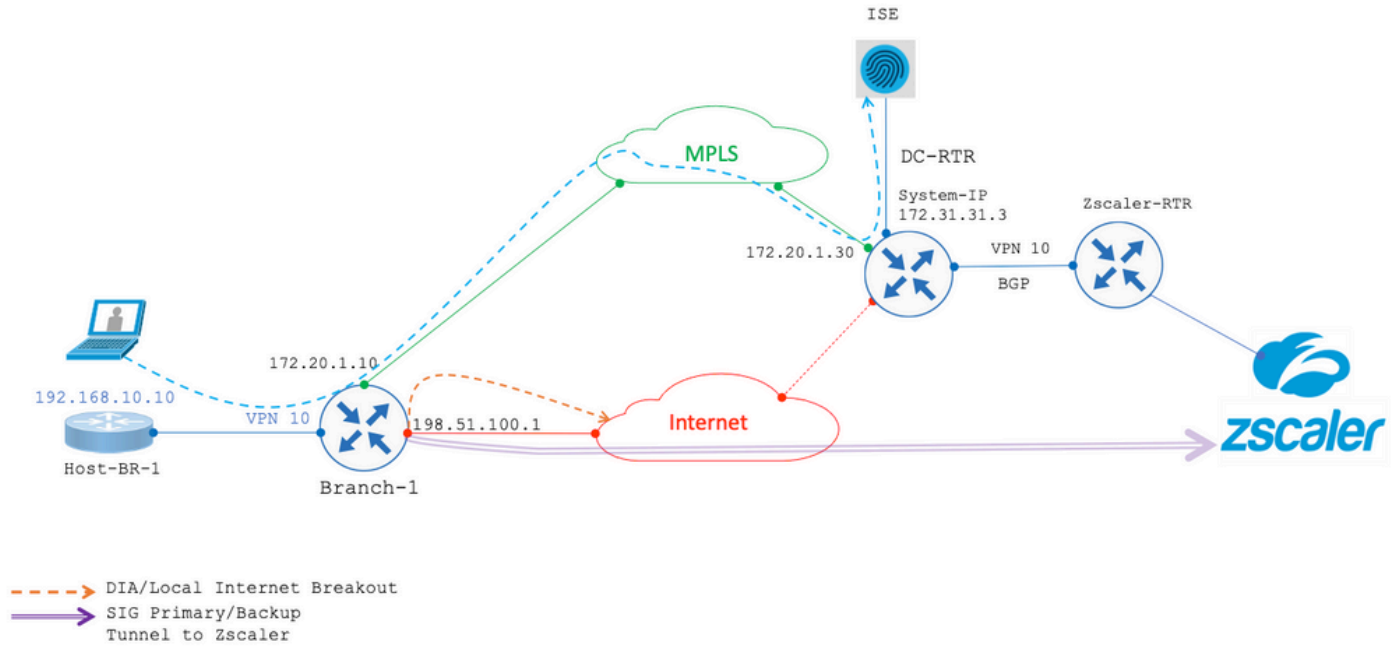
Requisito (NAT del lado de servicio (SS-NAT) con inspección UTD)

Suponga que el usuario ha solicitado estos requisitos:

1. Cuando los transportes de Internet y MPLS estén operativos, los clientes inalámbricos de VPN 10 se pueden dirigir a ISE en el Data Center para su autenticación. Además, el tráfico VPN 10 que viaja a través de la superposición SD-WAN puede someterse a inspección. Como este tráfico es parte de la superposición, VPN 10 utiliza la función SS-NAT. [UTD + SS-NAT]

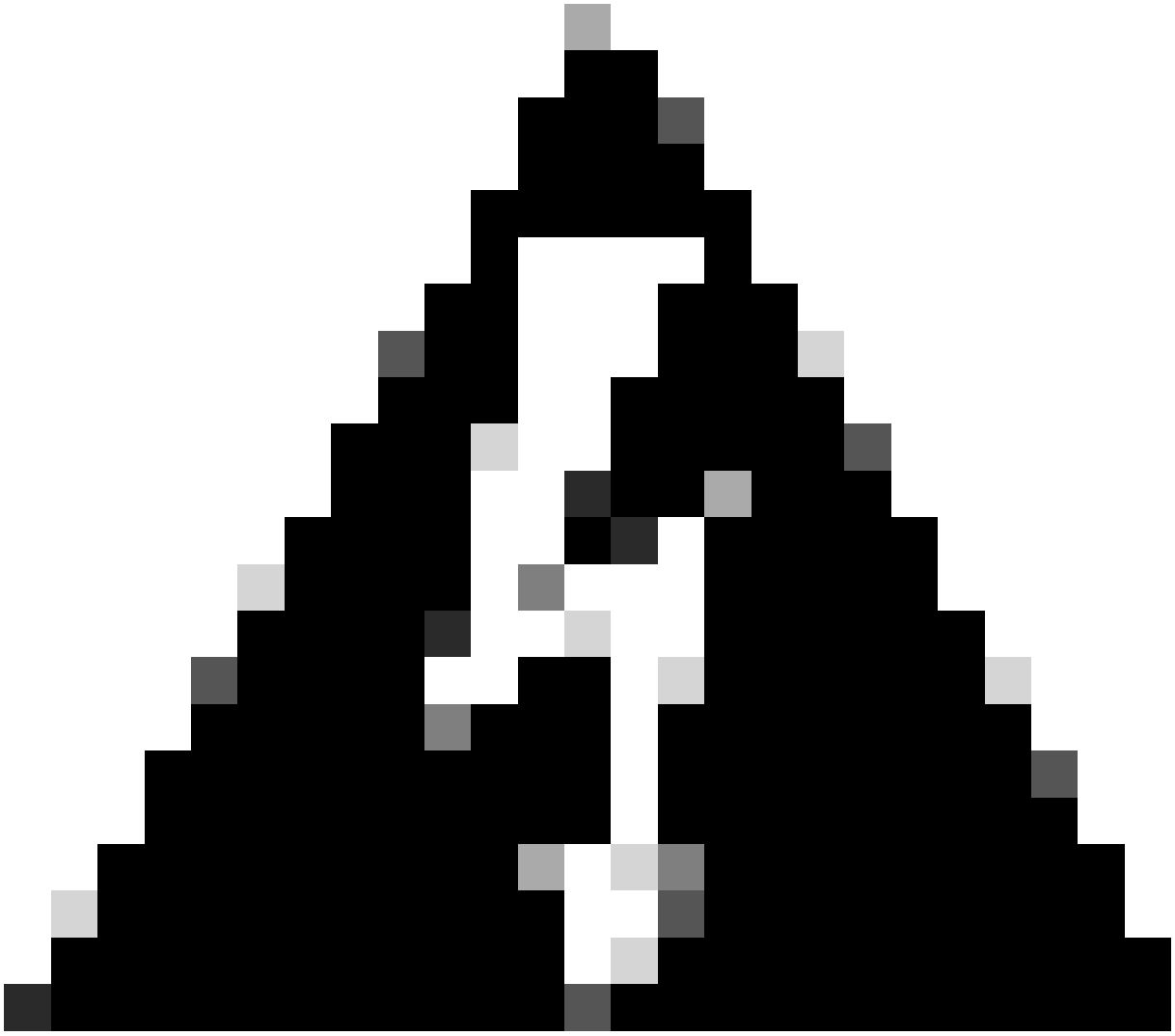
2. Si el transporte de Internet no está disponible, todo el tráfico de VPN 10, incluido el tráfico inalámbrico y el tráfico por cable, se puede enrutar a través de la superposición mediante el transporte MPLS. Este tráfico también puede estar sujeto a inspección. [UTD + SS-NAT]

El objetivo de estos requisitos es garantizar un flujo de tráfico seguro y supervisado para VPN 10 en la sucursal 1 en diferentes condiciones de red.



En ambos escenarios mencionados anteriormente, tiene la inspección UTD con una combinación SS-NAT. Este es el ejemplo de configuración de UTD para este escenario.

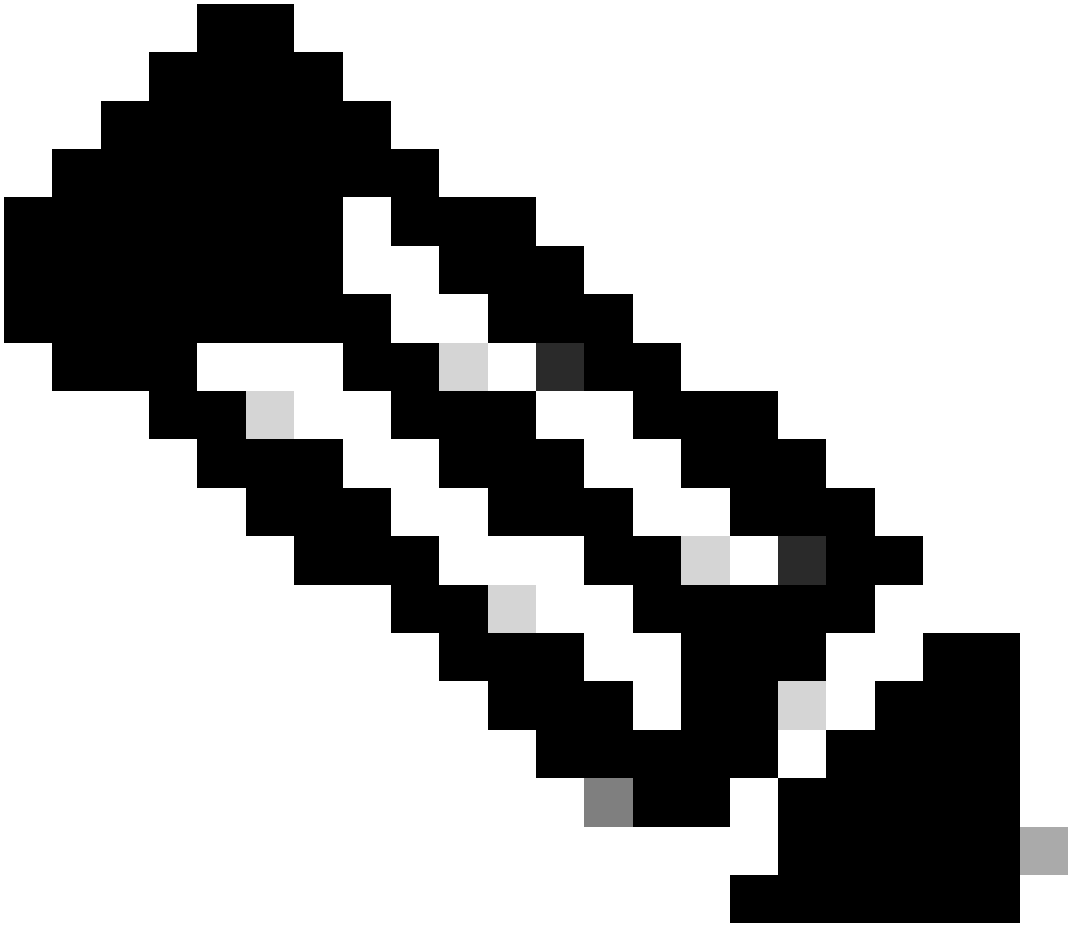
```
policy utd-policy-vrf-10
 all-interfaces
 vrf 10
 threat-inspection profile TEST_IDS_Policy
 exit
```



Advertencia: Tenga en cuenta que actualmente no se admite la combinación de UTD con SS-NAT. Por lo tanto, esta combinación no funciona como se esperaba. Es posible que en futuras versiones se incluya una solución para este problema.

Solución Aternativa

La solución alternativa es inhabilitar la política UTD en la VPN IP superpuesta (en este caso VPN 10) y habilitar la VPN global.



Nota: Esta configuración se prueba y verifica en la versión 17.6.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).