Configurar IP Sobreposto para a Mesma VPN em Vários Locais com Cenários de Falha

Contents

Introdução

Este documento descreve o cenário com espaços de endereço sobrepostos na mesma VPN em vários locais na sobreposição de SD-WAN. Ele descreve o exemplo de rede, o comportamento do tráfego em cenários normais/de failover, a configuração e a verificação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento de SD-WAN.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador SD-WAN versão 20.6.3
- Cisco IOS® XE (executado no modo controlador) 17.6.3a
- Dispositivos de host (CSR1000V) 17.3.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Aqui você pode encontrar uma lista de acrônimos usados neste artigo.

- Gateway de Internet Seguro - SIG
- Roteamento e encaminhamento virtual - VRF
- Rede Virtual Privada - VPN
- Acesso direto à Internet - DIA
- Tradução de Endereço de Rede - NAT
- Multi-Protocol Label Switching - MPLS
- Conversão de endereço de rede do lado do serviço - SS-NAT
- Data center - DC
- Protocolo de gerenciamento de sobreposição - OMP
- Protocolo IP

Consulte o documento da Cisco para obter mais detalhes sobre o NAT do lado do serviço: NAT do lado do serviço

Diagrama de Rede

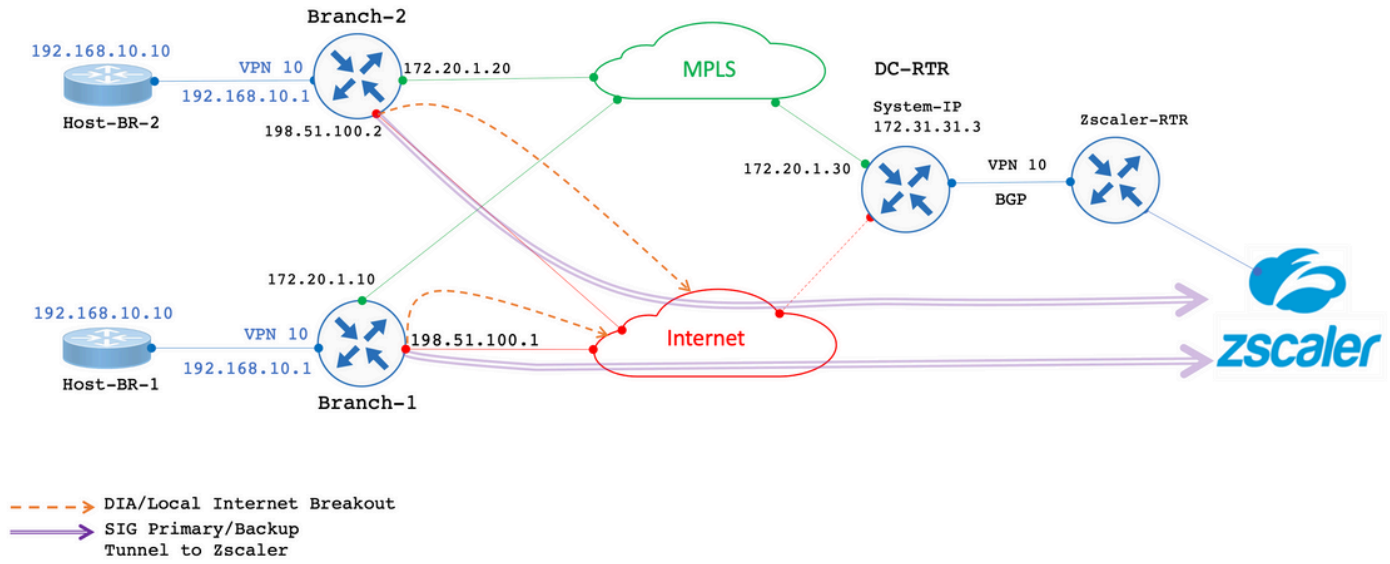
Observação: nesta topologia, os dispositivos hospedados no serviço VPN 10 de cada roteador de filial têm IP 192.168.10.0/24 sobreposto configurado.

Nessa topologia específica, há 1 DC (o DC tem apenas transporte MPLS, no entanto, em um cenário real, pode haver vários transportes) e 2 filiais que têm conectividade com a sobreposição de SD-WAN sobre MPLS e transporte de Internet. O serviço VPN 10 é configurado em todos os locais. As filiais têm túnel SIG (primário e backup) configurado para Zscaler. O DIA é configurado para determinados IPs de destino específicos para ignorar o Zscaler. Em caso de falha de link da

Internet em filiais, espera-se que todo o tráfego seja enviado para DC via transporte MPLS.

O eBGP é configurado no serviço VPN 10 com o roteador Zscaler na extremidade DC. O roteador DC recebe a rota padrão do roteador Zscaler e é redistribuído no OMP.

Observação: os endereços IP públicos mencionados neste cenário de laboratório são obtidos da documentação RFC5737.



Especificação

- Aproveite a sobreposição de endereços IP para Branch-1 e Branch-2 no VPN 10 do lado do serviço.

- Em um cenário típico, quando o MPLS e o transporte da Internet estão ativos, o tráfego da VPN 10 deve sair pelo túnel SIG.
- Para prefixos de destino IP específicos, o tráfego deve ignorar o Túnel SIG e sair via DIA.
- Em caso de falha de link da Internet, todo o tráfego de destino da Internet da VPN 10 deve sair pelo DC.

Solução

Para atingir o requisito, os recursos de SD-WAN NAT do lado do serviço e DIA com política de dados são usados.

- O NAT do lado do serviço é configurado em cada roteador da filial com diferentes endereços IP do pool do NAT.
- Em caso de falha de link da Internet quando o tráfego é enviado à sobreposição de SD-WAN, o IP de origem é convertido em NAT para o endereço IP do pool de NAT configurado.
- O roteador DC vê o endereço pós-NAT para sub-redes sobrepostas.

Observação: para representar o tráfego normal via túnel SIG da VPN 10, o IP público 192.0.2.100 é usado e, para um destino específico, via DIA, 192.0.2.1 é usado. As configurações correspondentes são mostradas na seção de configuração.

Configurar

Configuração de Branch-1

A configuração do roteador Branch-1 é a seguinte:

```
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
!
```

Configuração de Branch-2

A configuração do roteador Branch-2 é a seguinte:

```
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
!
```

Configuração do roteador DC

A configuração do roteador DC é a seguinte.

```
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

A configuração da política vSmart é a seguinte.

> Observação: observe que **nat pool 1** é chamado na política para ambas as filiais, no entanto, há dois pools de IP diferentes configurados para cada filial (172.16.2.0/30 para Branch-1 e 172.16.2.8/30 para Branch-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
!
```

Cenários de failover

Cenário normal de fluxo de tráfego Branch-1

Quando ambos os transportes estão ativos, como mostrado na saída, por padrão o tráfego sai através do túnel SIG primário **Tunnel100512**. Quando o túnel principal fica inativo, o tráfego muda para o túnel de backup **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#
```

O traceroute mostra que o tráfego toma o 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#

O tráfego para um destino específico **192.0.2.1** sai via DIA (NATed para endereço IP 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#
```

Cenário normal do fluxo de tráfego da filial 2

Um comportamento semelhante também é observado no roteador Branch-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#

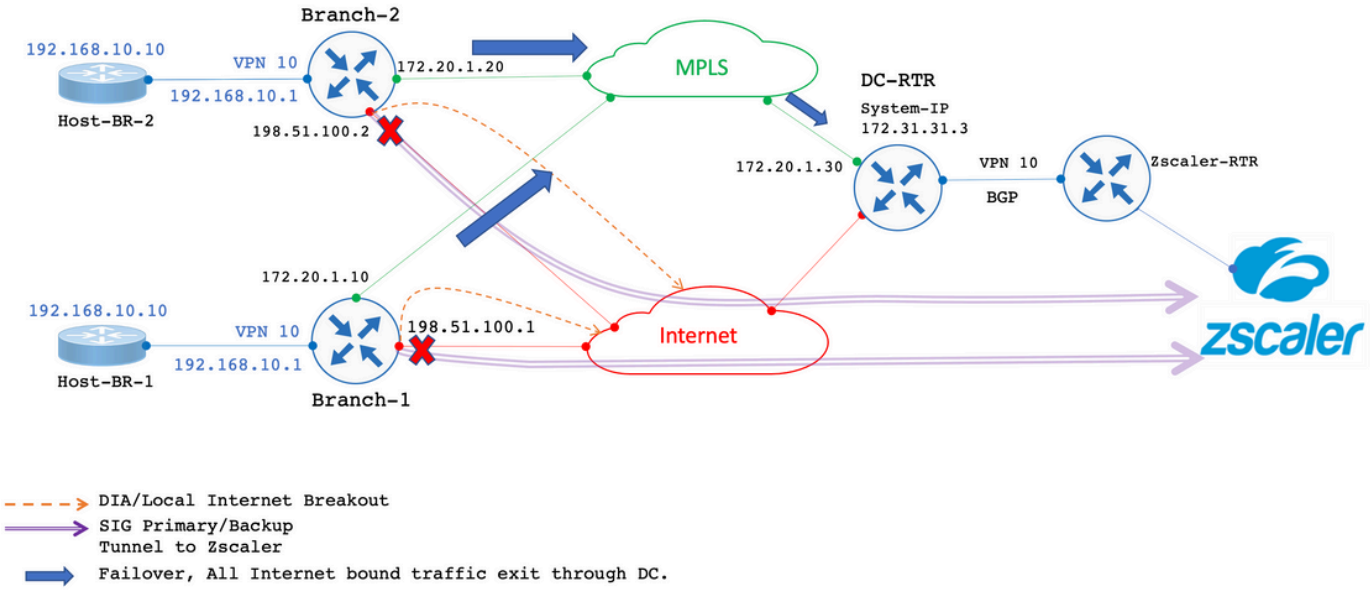
show ip nat translation

```
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#
```

Cenários de falha

Cenário de falha da filial 1

Esta seção descreve o comportamento durante a falha da Internet.



O link de Internet é administrativamente desligado para simular um link de falha 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#
```

As saídas mostram que, durante o cenário de falha de link da Internet, o roteador Branch-1 recebe a rota padrão do roteador DC via OMP.

172.31.31.3é o IP do sistema do roteador 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>

O tráfego destinado a 192.0.2.100 recebe NAT para o pool NAT do lado do serviço e sai por 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#

Os resultados do traceroute mostram que o tráfego toma o caminho do DC. 172.20.1.30 é o IP WAN de transporte MPLS do roteador 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#

O tráfego destinado ao IP específico 192.0.2.1 também recebe NAT para o pool NAT do lado do serviço e sai por 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>
```

Configuração da política de dados enviada por push do 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

Cenário de falha da filial 2

Um comportamento semelhante também é observado nos roteadores Branch-2 quando há um failover da 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
```

Status de roteamento do roteador DC

A tabela de roteamento captura do roteador DC.

Como mostrado na saída, o roteador DC é capaz de diferenciar endereços IP sobrepostos de ambas as filiais com os **post-NAT IP**derivados **SS-NAT pool** (172.16.2.0 e 172.16.2.8) em vez do IP LAN real **192.168.10.0/24172.31.31.1** e **172.31.31.2** são os **system-ip** configurados para Branch-1/Branch-2. System-IP **172.31.31.10** pertence 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 -
```

Verificar

No momento, não há nenhum procedimento de verificação específico disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações adicionais

Cenário-1

Em cenários em que os controladores estão na versão 20.3.4 e o cEdge executa a versão 17.3.3a ou versões anteriores com as mesmas configurações, observa-se que, em cenários normais/de failover, o tráfego recebe NAT para o pool de NAT do lado do serviço e interrompe o fluxo.

Capturas do cEdge:

<#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

A saída é capturada de execuções do cEdge na versão 17.3.3a. O tráfego destinado através do túnel SIG recebe NATed para o pool SS-NAT e é descartado. Uma correção está disponível a partir da versão 17.3.6.

Cenário-2

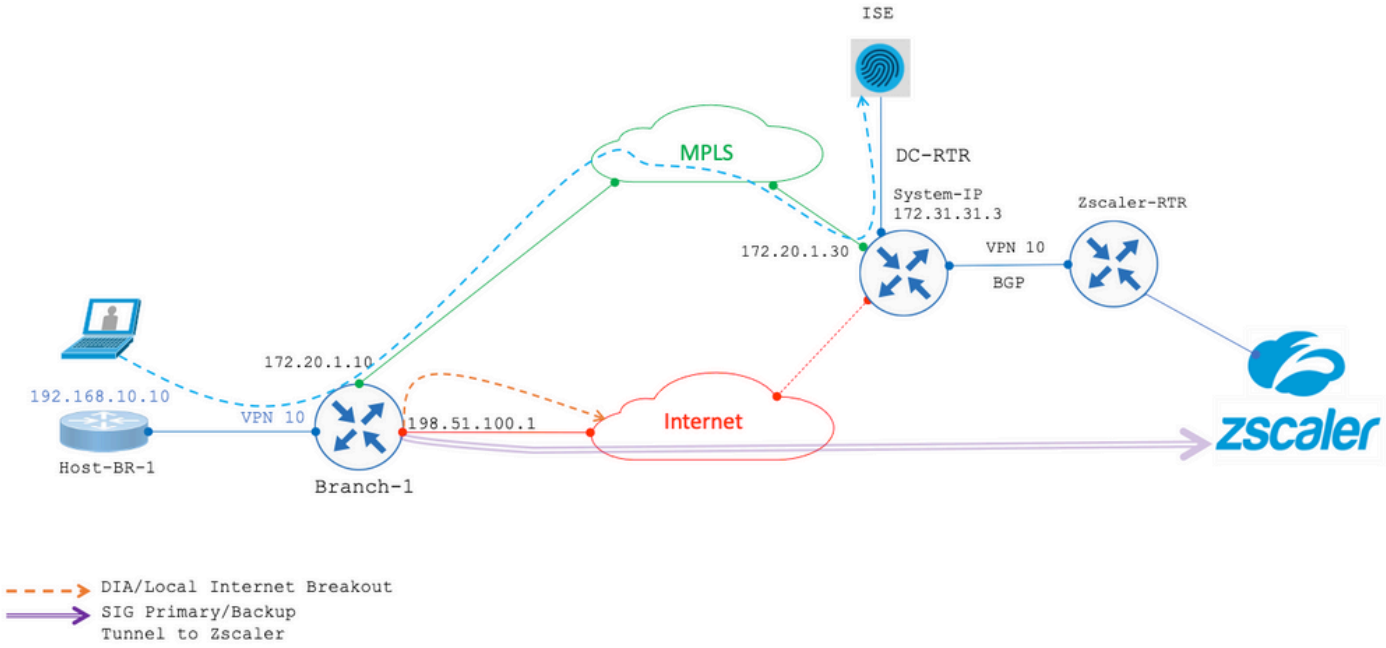
Requisito (NAT do lado do serviço (SS-NAT) com inspeção de UTD)

Suponha que o usuário tenha solicitado estes requisitos:

1. Quando os transportes pela Internet e MPLS estão operacionais, os clientes sem fio na VPN 10 podem ser direcionados ao ISE no Data Center para autenticação. Além disso, o tráfego da VPN 10 que viaja através da sobreposição de SD-WAN pode passar por inspeção. Como esse tráfego faz parte da sobreposição, a VPN 10 utiliza o recurso SS-NAT. [UTD + SS-NAT]

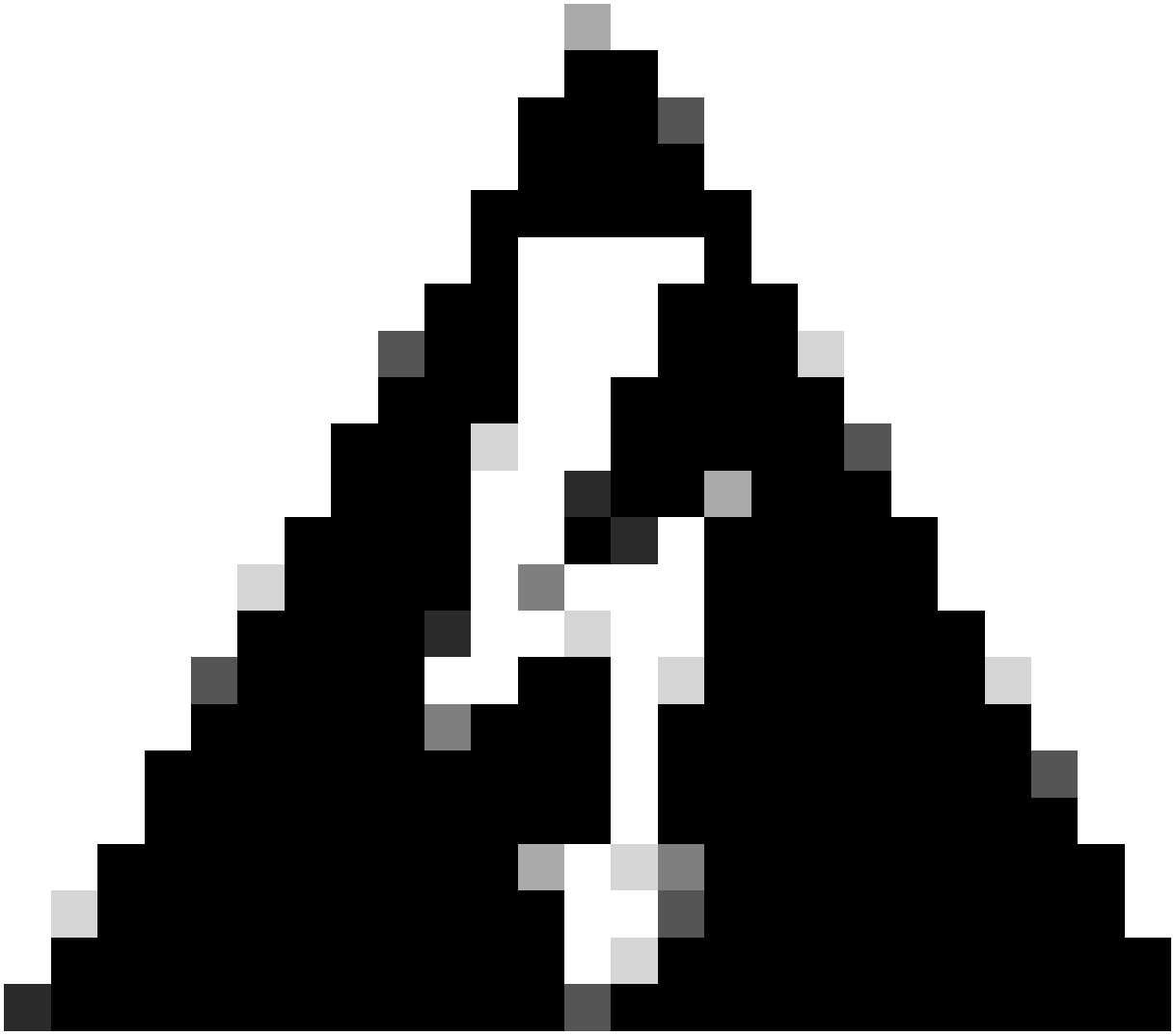
2. Se o transporte pela Internet ficar indisponível, todo o tráfego da VPN 10, incluindo o tráfego com e sem fio, poderá ser roteado através da sobreposição usando o transporte MPLS. Esse tráfego também pode ser sujeito a inspeção. [UTD + SS-NAT]

Esses requisitos têm como objetivo garantir um fluxo de tráfego seguro e monitorado para a VPN 10 em Branch-1 sob diferentes condições de rede.



Em ambos os cenários mencionados anteriormente, você tem inspeção de UTD com uma combinação de SS-NAT. Aqui está um exemplo de configuração UTD para este cenário.

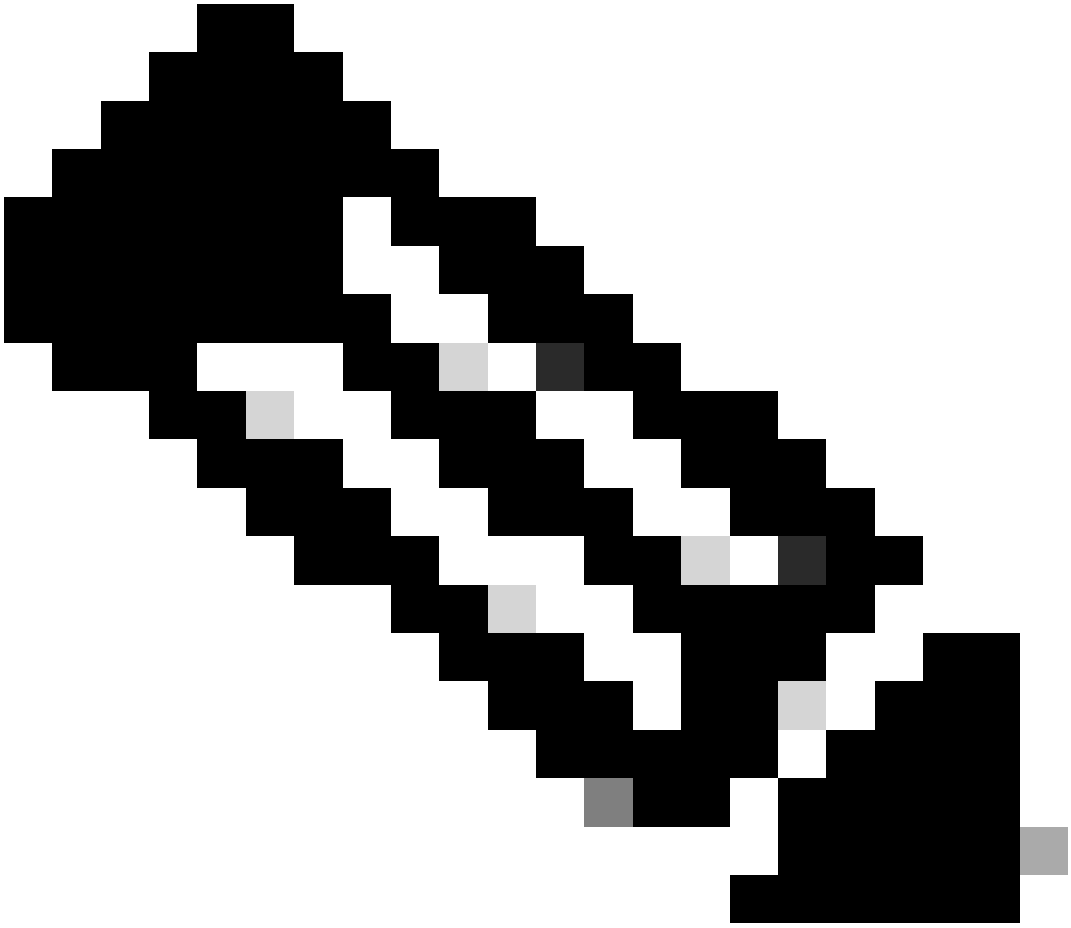
```
policy utd-policy-vrf-10
 all-interfaces
 vrf 10
 threat-inspection profile TEST_IDS_Policy
 exit
```



Aviso: Observe que, no momento, a combinação de UTD com SS-NAT não é suportada. Portanto, essa combinação não funciona como esperado. Uma correção para esse problema pode ser incluída em versões futuras.

Solução

A solução alternativa é desabilitar a política de UTD em VPN IP Sobreposta (neste caso, VPN 10) e habilitar a VPN Global.



Observação: essa configuração é testada e verificada na versão 17.6.

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.