Configuration du chevauchement des adresses IP pour le même VPN sur plusieurs sites avec des scénarios d'échec

Table des matières

Introduction

Ce document décrit le scénario avec des espaces d'adressage se chevauchant dans le même VPN sur plusieurs sites dans la superposition SD-WAN. Il décrit l'exemple de réseau, le comportement du trafic dans des scénarios normaux/de basculement, la configuration et la vérification.

Conditions préalables

Exigences

Cisco recommande que vous ayez une bonne connaissance du SD-WAN.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur SD-WAN version 20.6.3
- Cisco IOS® XE (exécution en mode contrôleur) 17.6.3a
- Périphériques hôtes (CSR1000V) 17.3.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Vous trouverez ici une liste des acronymes utilisés dans cet article.

- Passerelle Internet sécurisée - SIG
- Routage et transfert virtuels - VRF
- Réseau privé virtuel - VPN
- Accès Internet direct - DIA
- Traduction d'adresses réseau - NAT
- Commutation multiprotocole par étiquette - MPLS
- Traduction d'adresses réseau côté service - SS-NAT
- Data center - DC
- Protocole de gestion de superposition - OMP
- Protocole Internet - IP

Référez-vous au document Cisco pour plus de détails sur la NAT côté service : NAT côté service

Diagramme du réseau

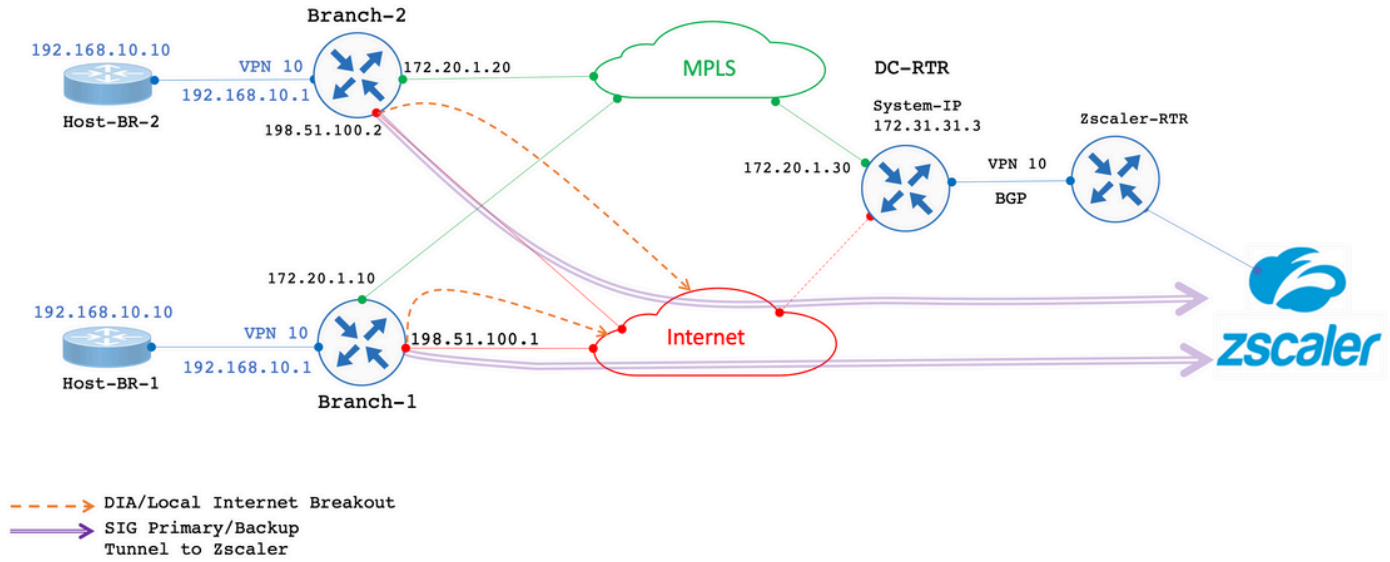
Remarque : dans cette topologie, les périphériques hébergés dans le service VPN 10 de chaque routeur de filiale ont un chevauchement IP 192.168.10.0/24 configuré.

Dans cette topologie spécifique, il y a 1 DC (DC n'a que le transport MPLS, mais dans un scénario

réel il peut y avoir plusieurs transports) et 2 filiales qui ont une connectivité à la superposition SD-WAN sur MPLS et le transport Internet. Le service VPN 10 est configuré dans tous les emplacements. Les filiales ont un tunnel SIG (principal et de secours) configuré sur Zscaler. DIA est configuré pour que certaines adresses IP de destination spécifiques contournent le Zscaler. En cas de défaillance de la liaison Internet au niveau des filiales, tout le trafic doit être envoyé au data center via le transport MPLS.

eBGP est configuré sur le service VPN 10 avec le routeur Zscaler à l'extrémité DC. Le routeur DC reçoit la route par défaut du routeur Zscaler et est redistribué dans OMP.

Remarque : les adresses IP publiques mentionnées dans ce scénario de travaux pratiques proviennent de la documentation RFC5737.



Spécification

- Exploitez les adresses IP qui se chevauchent pour Branch-1 et Branch-2 sur le VPN 10 côté service.

- Dans un scénario typique, lorsque MPLS et le transport Internet sont activés, le trafic provenant du VPN 10 doit quitter via le tunnel SIG.
- Pour des préfixes de destination IP spécifiques, le trafic doit contourner le tunnel SIG et quitter via DIA.
- En cas de défaillance de la liaison Internet, le trafic All/Internet en provenance du VPN 10 doit sortir via le DC.

Solution

Pour répondre à cette exigence, les fonctionnalités SD-WAN de NAT côté service et DIA avec politique de données sont utilisées.

- La fonction NAT côté service est configurée sur chaque routeur de filiale avec des adresses IP de pool NAT différentes.
- En cas de défaillance de la liaison Internet lorsque le trafic est envoyé à la superposition SD-WAN, l'adresse IP source est convertie en adresse IP à partir du pool NAT configuré.
- Le routeur DC voit l'adresse post-NAT pour les sous-réseaux qui se chevauchent.

Remarque : pour représenter le trafic normal via le tunnel SIG à partir du VPN 10, l'adresse IP publique 192.0.2.100 est utilisée et, pour une destination spécifique, via DIA, 192.0.2.1 est utilisée. Les configurations correspondantes sont indiquées dans la section Configuration.

Configurer

Configuration de Branch-1

La configuration du routeur Branch-1 est la suivante.

```
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
!
```

Configuration de Branch-2

La configuration du routeur Branch-2 est la suivante.

```
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
!
```

Configuration du routeur DC

La configuration du routeur CC est la suivante.

```
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
!
```

Politique vSmart

La configuration de la stratégie vSmart est la suivante.

Remarque : notez que **nat pool 1** est appelé dans la stratégie pour les deux filiales. Toutefois, deux pools d'adresses IP différents sont configurés pour chaque filiale (172.16.2.0/30 pour Branch-1 et 172.16.2.8/30 pour 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
!
```

Scénario normal de flux de trafic de Branch-1

Lorsque les deux transports sont actifs comme indiqué dans le résultat, le trafic par défaut sort par le tunnel SIG principal **Tunnel100512**. Lorsque le tunnel principal tombe en panne, le trafic passe au tunnel de secours **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 indique que le trafic emprunte le tunnel 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#
```

Le trafic vers une destination spécifique **192.0.2.1** prend la sortie via DIA (adresse IP NAT vers 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#
```

Scénario normal de flux de trafic de Branch-2

Un comportement similaire est également observé sur le routeur 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
```

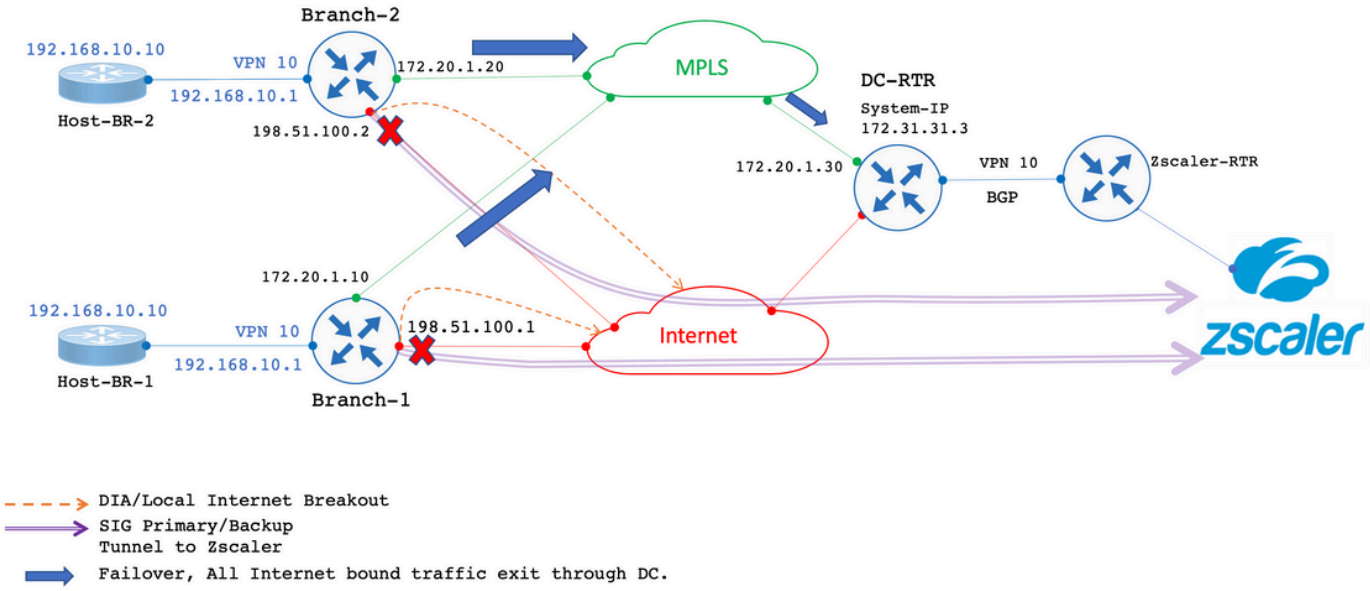
198.51.100.2:1

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

Scénarios de défaillance

Scénario de défaillance de Branch-1

Cette section décrit le comportement au cours d'une panne Internet.



La liaison Internet est désactivée par l'administrateur pour simuler une liaison Internet défaillante.

<#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#
```

Les résultats montrent que, dans le scénario d'une défaillance de liaison Internet, le routeur Branch-1 reçoit la route par défaut du routeur DC via OMP. **172.31.31.3** est l'adresse IP système du routeur 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>

Le trafic destiné à 192.0.2.100 obtient NATed vers le pool NAT côté service et sort via 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#

Les résultats de la commande traceroute indiquent que le trafic emprunte le chemin DC. 172.20.1.30 est l'adresse IP WAN de transport MPLS du routeur 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#
```

Le trafic destiné à l'adresse IP 192.0.2.1 spécifique reçoit également la traduction d'adresses réseau vers le pool NAT côté service et sort via le contrôleur de domaine.

<#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>

Configuration de la politique de données poussée depuis 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

Scénario de défaillance de Branch-2

Un comportement similaire est également observé dans les routeurs Branch-2 en cas de basculement 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
```

État de routage du routeur CC

La table de routage capture les données du routeur DC.

Comme le montre le résultat, le routeur DC est capable de différencier les adresses IP qui se chevauchent des deux branches avec l'adresse **post-NAT IP**dérivée du **SS-NAT pool** (172.16.2.0 et 172.16.2.8) au lieu de l'adresse IP LAN réelle **192.168.10.0/24172.31.31.1** et **172.31.31.2** sont **system-ip** configurés pour Branch-1/Branch-2. System-IP **172.31.31.10** appartient à **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 -

Vérifier

Aucune procédure de vérification spécifique n'est actuellement disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Additional Information

Scénario-1

Dans les scénarios où les contrôleurs sont sur la version 20.3.4, et cEdge exécute 17.3.3a ou versions inférieures avec les mêmes configurations, il est observé, que dans les scénarios normaux / de basculement le trafic obtient NATed au pool NAT côté service et casse le flux.

Captures 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
```

Le résultat est capturé à partir des exécutions cEdge sur la version 17.3.3a. Le trafic destiné via le tunnel SIG reçoit NAT vers le pool SS-NAT et est abandonné. Un correctif est disponible à partir de la version 17.3.6.

Scénario-2

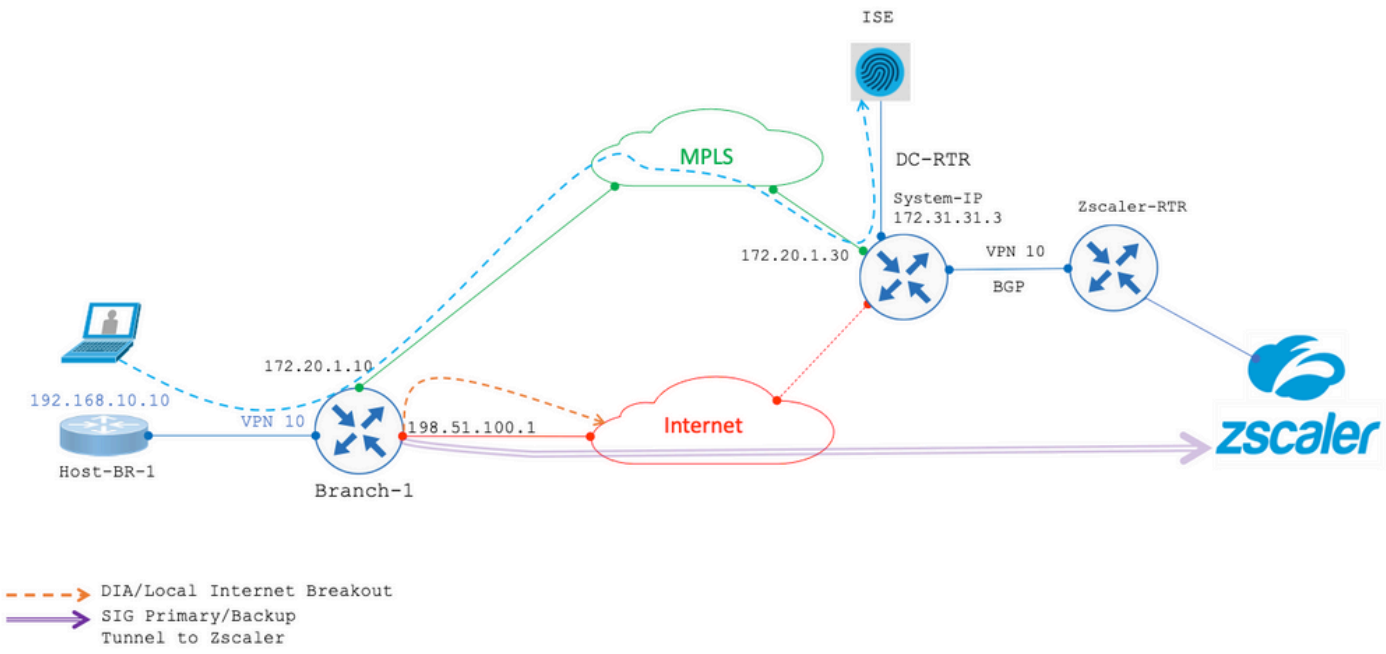
Exigence (NAT côté service (SS-NAT) avec inspection UTD)

Supposons que l'utilisateur ait demandé les conditions suivantes :

1. Lorsque les transports Internet et MPLS sont opérationnels, les clients sans fil du VPN 10 peuvent être dirigés vers ISE dans le centre de données pour authentification. En outre, le trafic VPN 10 transitant via la superposition SD-WAN peut être inspecté. Comme ce trafic fait partie de la superposition, le VPN 10 utilise la fonctionnalité SS-NAT. [UTD + SS-NAT]

2. Si le transport Internet devient indisponible, tout le trafic provenant du VPN 10, y compris le trafic sans fil et filaire, peut être routé via la superposition à l'aide du transport MPLS. Ce trafic peut également faire l'objet d'une inspection. [UTD + SS-NAT]

Ces exigences visent à assurer un flux de trafic sécurisé et surveillé pour le VPN 10 dans Branch-1 dans différentes conditions de réseau.



Dans les deux scénarios mentionnés précédemment, vous avez l'inspection UTD avec une combinaison SS-NAT. Voici un exemple de configuration UTD pour ce scénario.

policy utd-policy-vrf-10

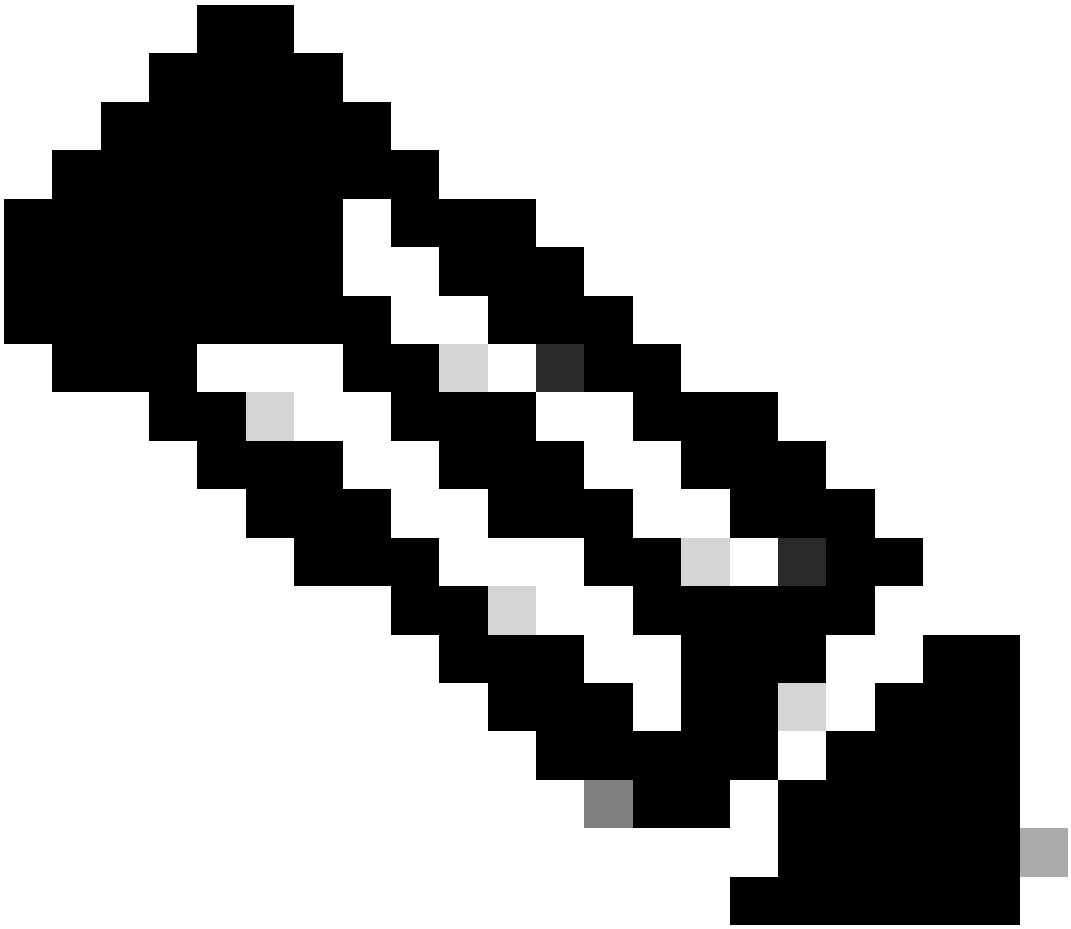
```
all-interfaces
vrf 10
threat-inspection profile TEST_IDS_Policy
exit
```

Avertissement : veuillez noter que la combinaison UTD et SS-NAT n'est actuellement pas prise en charge. Par conséquent, cette combinaison ne fonctionne pas comme prévu. Un correctif pour ce problème pourrait être inclus dans les versions futures.

Solution de contournement

La solution de contournement consiste à désactiver la stratégie UTD sur le VPN IP avec chevauchement (dans ce cas VPN 10) et à activer le

VPN global.



Remarque : cette configuration est testée et vérifiée dans la version 17.6.

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.