Overlappende IP voor hetzelfde VPN via meerdere locaties met foutscenario's configureren

Inhoud

Inleiding

Dit document beschrijft het scenario met overlappende adresruimten in hetzelfde VPN over meerdere sites in de SD-WAN-overlay. Het toont het voorbeeldnetwerk, het verkeersgedrag in normale/failover-scenario's, configuratie en verificatie.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van SD-WAN.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- SD-WAN controller versie 20.6.3
- Cisco IOS® XE (uitgevoerd in controllermodus) 17.6.3a
- Host Devices (CSR1000V) 17.3.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Hier vindt u een lijst van acroniemen die in dit artikel worden gebruikt.

- Secure Internet Gateway - SIG
- Virtuele routing en doorsturen - VRF
- Virtual Private Network - VPN
- Direct Internet Access - DICOM
- Netwerkadresomzetting - NAT
- Multi-Protocol Label Switching - MPLS
- Netwerkadresomzetting aan servicekant - S-NAT
- Datacenter - DC
- Overlay Management Protocol - OMP
- Internet-protocol - IP

Raadpleeg het Cisco-document voor meer informatie over de servicekant NAT: Service-side NAT

Netwerkdiagram

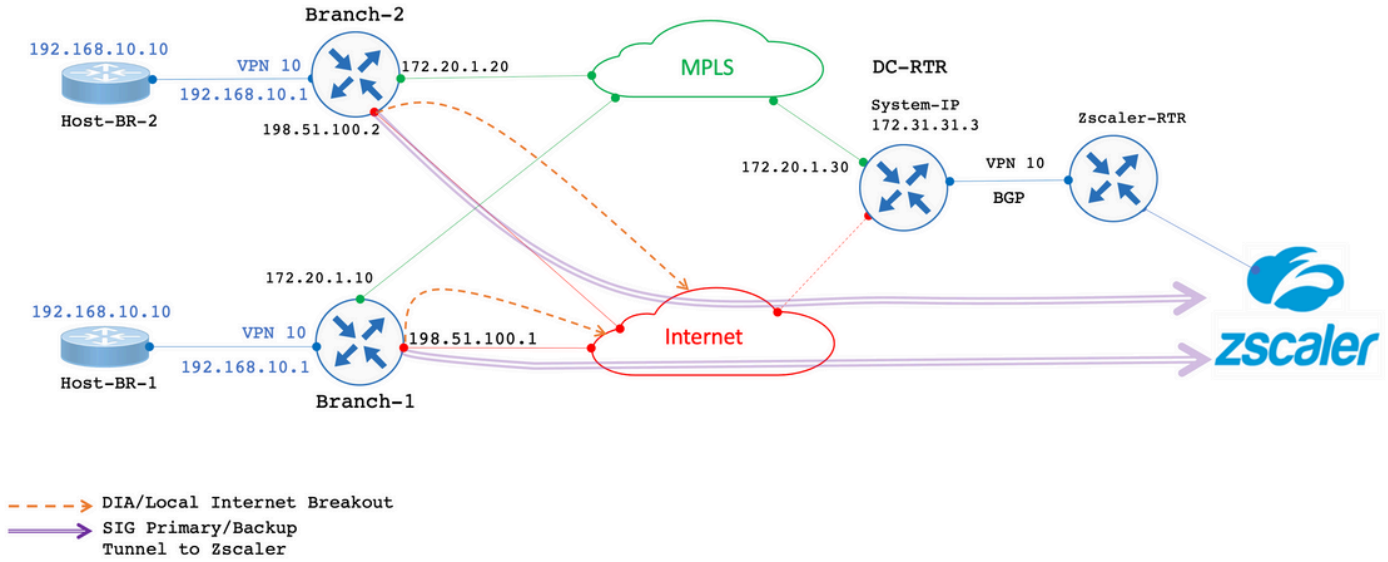
Opmerking: in deze topologie hebben apparaten die worden gehost in service VPN 10 van elke vertakking router overlappende IP 192.168.10.0/24 geconfigureerd.

In deze specifieke topologie, is er 1 DC (DC heeft alleen MPLS transport, maar in een echt scenario kunnen er meerdere transporten zijn) en 2 Branch locaties die connectiviteit hebben met SD-WAN overlay over MPLS en Internet transport. Service VPN 10 is geconfigureerd in alle

locaties. Branches hebben SIG-tunnel (Primair en back-up) geconfigureerd naar Zscaler. DIA is ingesteld voor bepaalde specifieke IP-doelapparaten om de Zscaler te omzeilen. In het geval van een storing van de internetverbinding bij filialen, wordt verwacht dat al het verkeer naar DC via MPLS-transport moet worden verzonden.

eBGP is op service VPN 10 geconfigureerd met de Zscaler-router aan het DC-uiteinde. DC router ontvangt standaard route van Zscaler router en wordt herverdeeld in OMP.

Opmerking: de openbare IP-adressen die in dit laboratoriumscenario worden vermeld, zijn afkomstig uit documentatie RFC5737.



Specificaties

- Leverage overlappende IP-adressen voor Branch-1 en Branch-2 aan de servicekant VPN 10.

- In een typisch scenario, wanneer MPLS en het vervoer van Internet omhoog zijn, moet het Verkeer van VPN 10 via SIG Tunnel weggaan.
- Voor specifieke IP-doelprefixes moet verkeer de SIG-tunnel omzeilen en via DIA afsluiten.
- In het geval van een storing in de internetverbinding moet All/Internet-bound verkeer van VPN 10 via DC worden afgesloten.

Oplossing

Om aan deze eis te voldoen, wordt SD-WAN gebruikt voor Service Side NAT en DIA met Data beleid.

- Service Side NAT is geconfigureerd op elke branch router met verschillende NAT-pool IP-adressen.
- In het geval van een storing van de internetverbinding wanneer het verkeer naar SD-WAN-

overlay wordt verzonden, is de bron-IP NATed naar het IP-adres van de geconfigureerde NAT-pool.
- DC router ziet het post-NAT adres voor overlappende subnetten.

Opmerking: om normaal verkeer via SIG Tunnel van VPN 10 af te beelden, wordt Public IP 192.0.2.100 gebruikt en voor een specifieke bestemming, via DIA, wordt 192.0.2.1 gebruikt. De bijbehorende configuraties worden weergegeven in het configuratiegedeelte.

Configureren

Configuratie van groep 1

Vak-1 routerconfiguratie is als volgt.

```
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
!
```

Configuratie van groep 2

Vak-2 routerconfiguratie is als volgt.

```
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
!
```

Configuratie van DC-router

De configuratie van de DC-router is als volgt.

```
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-beleid

vSmart-beleidsconfiguratie ziet er als volgt uit.

Opmerking: Houd er rekening mee dat het beleid voor beide vestigingen **nat pool 1** wordt aangeroepen, maar er zijn twee verschillende IP-pools geconfigureerd voor elke vestiging (172.16.2.0/30 voor Branch-1 en 172.16.2.8/30 voor 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
!
```

failover-scenario's

Branch-1 Traffic Flow Normal scenario

Wanneer beide transporten omhoog zijn zoals in de output, door gebrek verkeers uitgangen via de primaire SIG-tunnel **Tunnel100512**. Wanneer de hoofdtunnel door het verkeer gaat, gaat de switch naar de back-uptunnel **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 toont aan dat het verkeer de SIG-tunnel neemt.

<#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#
```

Het verkeer naar een specifieke bestemming **192.0.2.1** verloopt via DIA (NATed naar WAN IP-adres).

<#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 Traffic Flow Normal scenario

Gelijkaardig gedrag wordt waargenomen op de router van tak-2 eveneens.

<#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
```

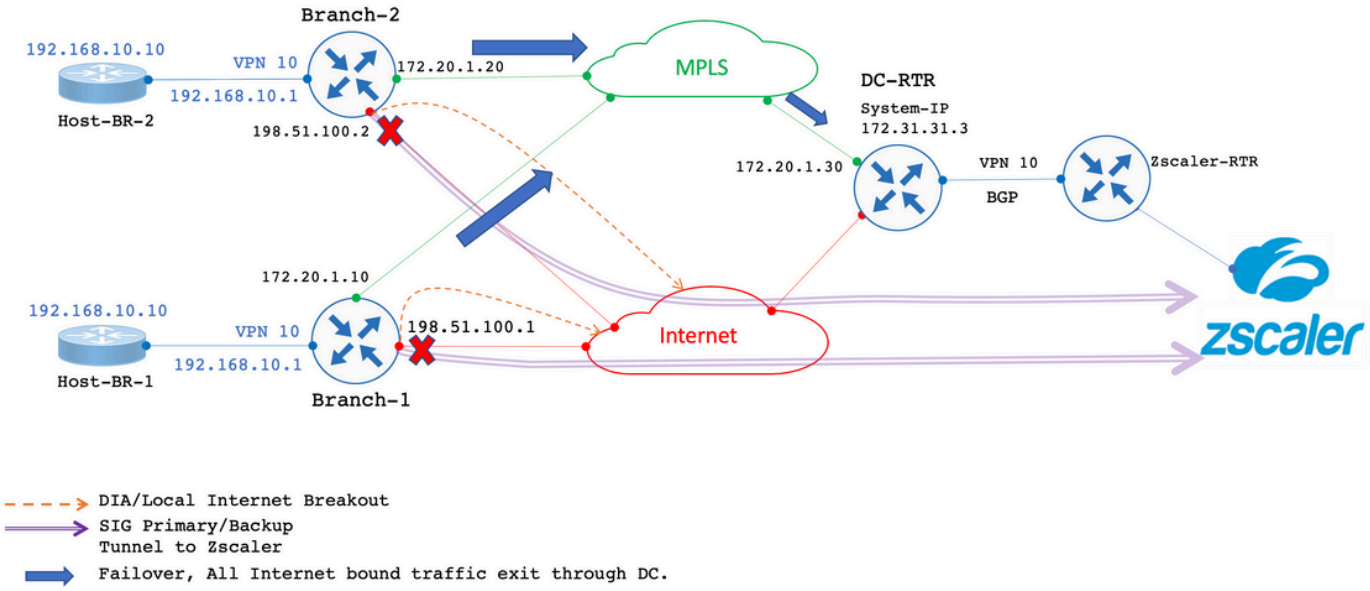
198.51.100.2:1

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

Faalscenario's

Vak-1-failliet scenario

In dit gedeelte wordt beschreven hoe u reageert tijdens een internetfout.



De internetverbinding wordt administratief afgesloten om een link naar een internetfout te simuleren.

<#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#
```

De output toont aan dat tijdens het scenario van de internetverbindingsmislukking, de router Branch-1 de standaardroute van de router van gelijkstroom via OMP ontvangt. **172.31.31.3** is systeem-IP voor de router van gelijkstroom.

<#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>
```

192.0.2.100 Verkeer bestemd om NATed te krijgen naar de NAT-pool van de servicekant en uitgangen 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#
```

De resultaten van Traceroute tonen verkeer neemt de weg van DC. 172.20.1.30 is het MPLS WAN-IP voor transport van de DC-router.

<#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 TRANSITIONS

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#

Het verkeer dat voor specifieke IP 192.0.2.1 is bestemd, krijgt ook NATed naar de NAT-pool aan de servicekant en verlaat via 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>
```

Configuratie van gegevensbeleid vanuit 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

Vak-2-faillietscenario

Gelijkaardig gedrag wordt ook waargenomen in de routers van Tak-2 wanneer er een Internet failover is.

<#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-routingstatus

De routeringstabel neemt de gegevens op van de DC-router.

Zoals in de output wordt getoond, kan de router van DC overlappende IP adressen van beide takken met **post-NAT IP**afgeleid van het **SS-NAT pool** (172.16.2.0 en 172.16.2.8) in plaats van daadwerkelijke LAN IP onderscheiden **192.168.10.0/24172.31.31.1** en **172.31.31.2** zijn **system-ip** gevormd voor tak-1/tak-2. System-IP **172.31.31.10** behoort tot **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 -
```

Verifiëren

Er is momenteel geen specifieke verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Aanvullende informatie

Scenario 1

In scenario's waarin Controllers op versie 20.3.4 zijn, en cEdge 17.3.3a of lagere versies met dezelfde configuraties draait, wordt opgemerkt dat in normale/failover scenario's het verkeer NATed aan de servicekant NAT-pool krijgt en de stroom verbreekt.

cEdge legt vast:

<#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
```

Output wordt opgenomen van cEdge-runs op de 17.3.3a-versie. Het verkeer dat via de SIG Tunnel wordt bestemd krijgt NATed naar de SS-

NAT pool en wordt gedropt. Vanaf versie 17.3.6 is een fix beschikbaar.

Scenario 2

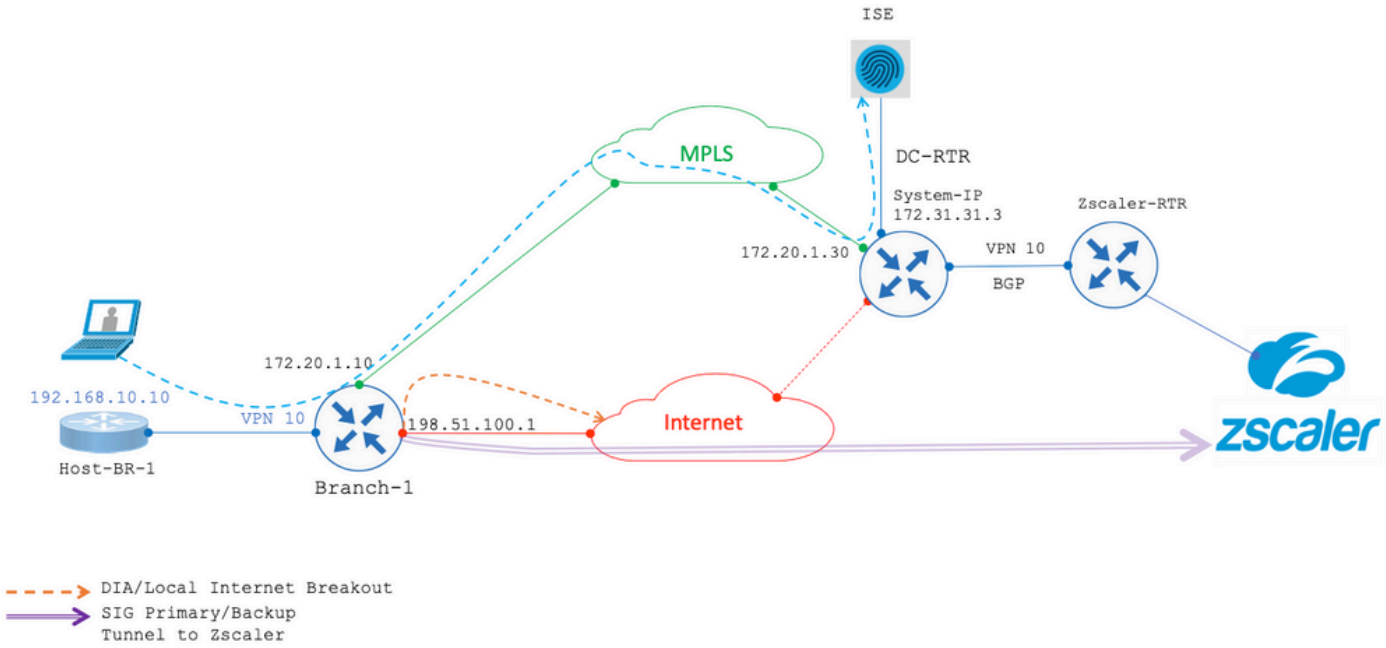
Eis (Service Side NAT (SS-NAT) met UTD-inspectie)

Veronderstel de gebruiker deze vereisten heeft gevraagd:

1. Wanneer zowel het internet- als MPLS-transport operationeel zijn, kunnen draadloze clients in VPN 10 voor verificatie naar ISE in het datacenter worden geleid. Bovendien kan VPN 10-verkeer via de SD-WAN-overlay worden geïnspecteerd. Aangezien dit verkeer deel uitmaakt van de overlay, maakt VPN 10 gebruik van de SS-NAT-functie. [UTD + SS-NAT]

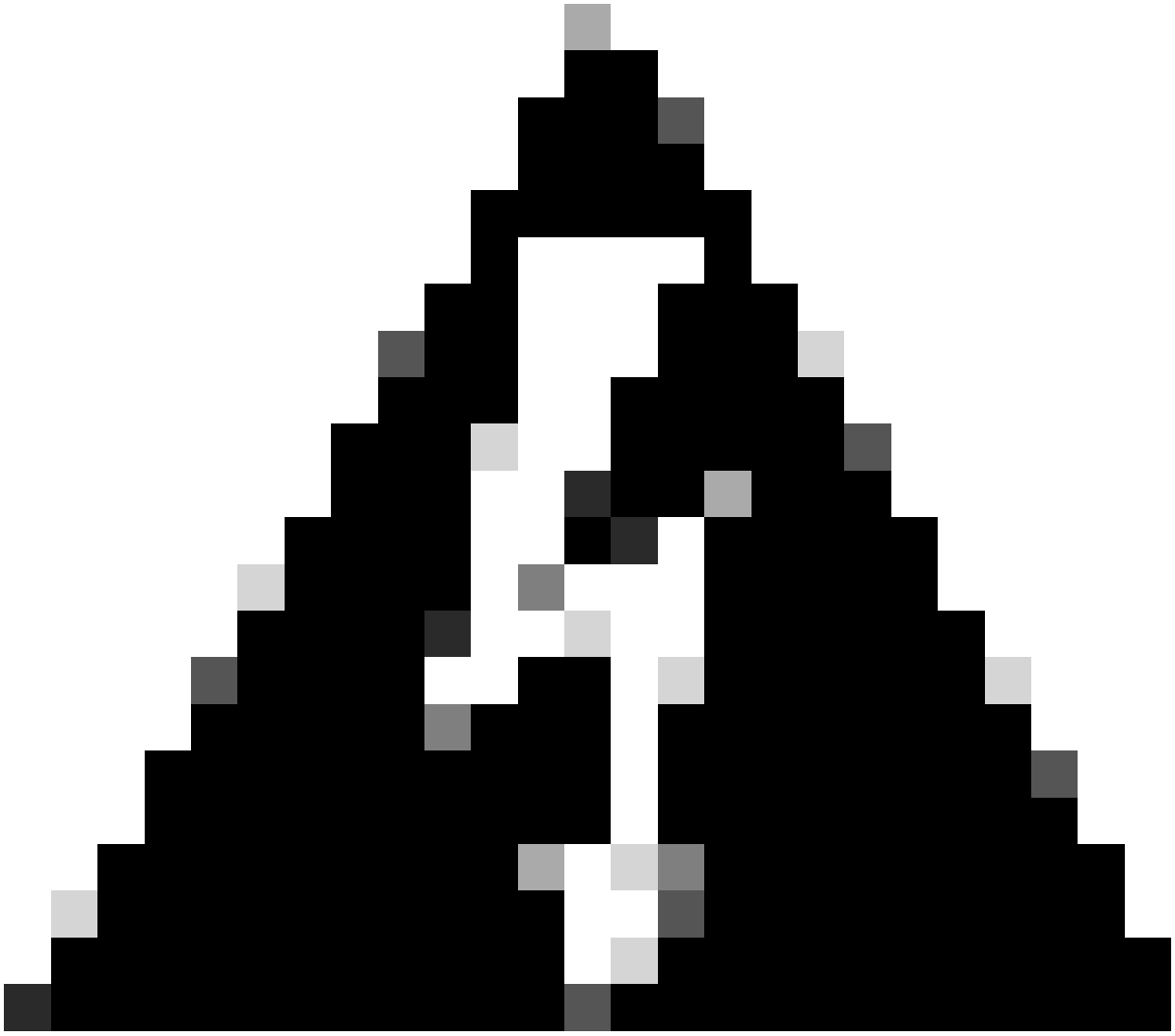
2. Als het internettransport niet beschikbaar is, kan al het verkeer vanaf VPN 10, inclusief zowel draadloos als bekabeld verkeer, via de overlay worden geleid met behulp van het MPLS-transport. Dit verkeer kan ook worden gecontroleerd. [UTD + SS-NAT]

Deze vereisten hebben tot doel veilige en gecontroleerde verkeersstromen voor VPN 10 in Branch-1 onder verschillende netwerkomstandigheden te garanderen.



In beide eerder genoemde scenario's, hebt u UTD-inspectie met een SS-NAT combinatie. Hier is de voorbeeldconfiguratie UTD voor dit scenario.

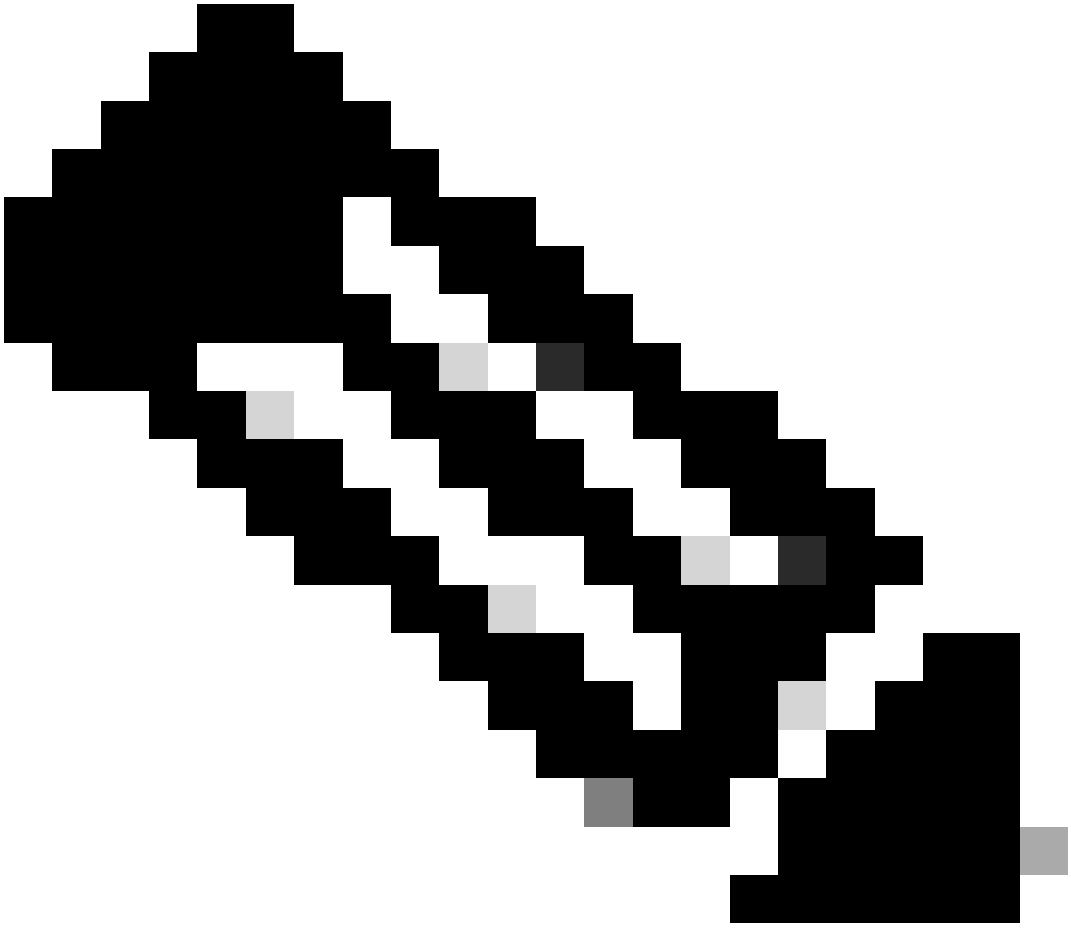
```
policy utd-policy-vrf-10
 all-interfaces
 vrf 10
 threat-inspection profile TEST_IDS_Policy
 exit
```



Waarschuwing: Houd er rekening mee dat de combinatie van UTD en SS-NAT op dit moment niet wordt ondersteund. Daarom werkt deze combinatie niet zoals verwacht. Een oplossing voor dit probleem kan worden opgenomen in toekomstige releases.

Tijdelijke oplossing

De tijdelijke oplossing is om het UTD-beleid op Overlapping IP VPN (in dit geval VPN 10) uit te schakelen en Global VPN in te schakelen.



Opmerking: deze configuratie wordt getest en geverifieerd in de versie 17.6.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.