

Konfiguration überlappender IP-Adressen für dasselbe VPN an mehreren Standorten mit Fehlerszenarien

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdiagramm](#)

[Spezifikation](#)

[Lösung](#)

[Konfigurieren](#)

[Konfiguration von Zweigstelle 1](#)

[Konfiguration von Zweigstelle 2](#)

[Konfiguration des RZ-Routers](#)

[vSmart-Richtlinie](#)

[Failover-Szenarien](#)

[Datenverkehrsfluss in der Außenstelle 1 - Normales Szenario](#)

[Datenverkehrsfluss in Zweigstelle 2 - Normales Szenario](#)

[Fehlerszenarien](#)

[Fehlerszenario für Zweigstelle 1](#)

[Branch-2-Fehlerszenario](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zusätzliche Informationen](#)

[Szenario-1](#)

[Szenario-2](#)

[Anforderung \(Service Side NAT \(SS-NAT\) mit UTD-Inspektion\)](#)

[Problemumgehung](#)

Einleitung

In diesem Dokument wird das Szenario mit sich überschneidenden Adressräumen im gleichen VPN über mehrere Standorte hinweg im SD-WAN-Overlay beschrieben. Es zeigt das Beispielnetzwerk, das Datenverkehrsverhalten in Normal-/Failover-Szenarien, die Konfiguration und die Überprüfung.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie Kenntnisse über SD-WAN haben.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- SD-WAN-Controller Version 20.6.3
- Cisco IOS® XE (im Controllermodus) 17.6.3a
- Host-Geräte (CSR1000V) 17.3.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Hier finden Sie eine Liste der in diesem Artikel verwendeten Akronyme.

- Sicheres Internet-Gateway - SIG
- Virtual Routing and Forwarding - VRF
- Virtual Private Network - VPN
- Direkter Internetzugang - DIA
- Network Address Translation - NAT
- Multi-Protocol Label Switching - MPLS
- Adressumwandlung im serviceseitigen Netzwerk - SS-NAT
- Rechenzentrum - RZ
- Overlay Management Protocol - OMP
- Internetprotokoll - IP

Weitere Einzelheiten zum serviceseitigen NAT: [serviceseitiges NAT](#) finden Sie im Dokument von Cisco.


Netzwerkdiagramm

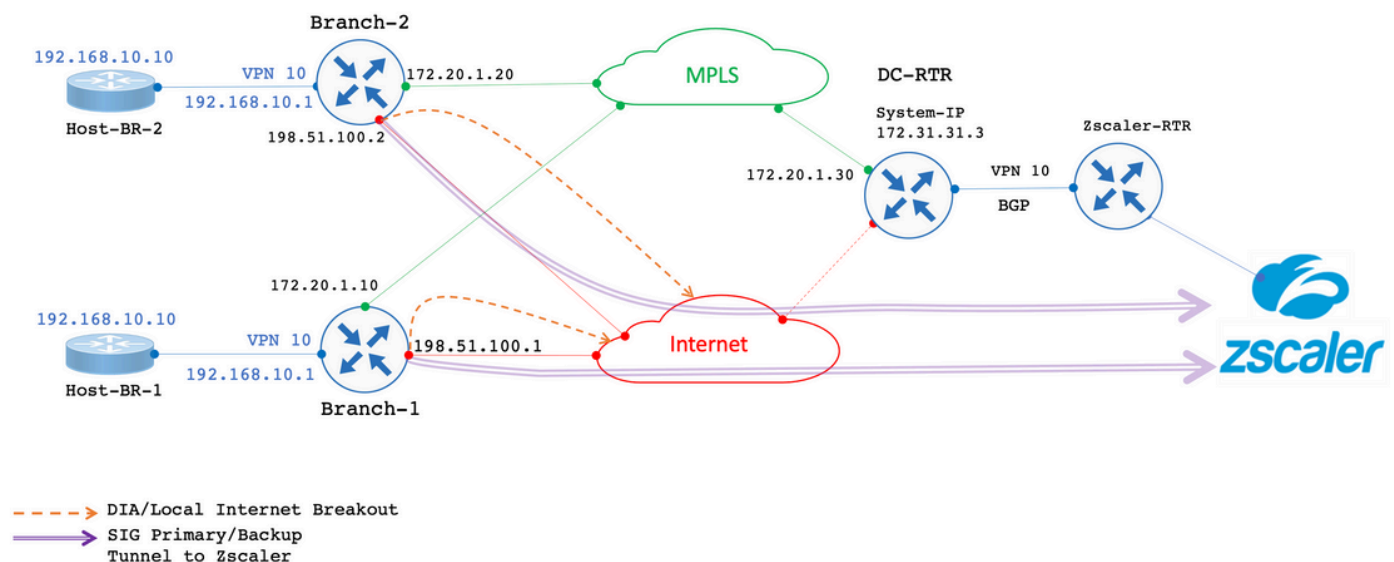


Hinweis: In dieser Topologie ist für die Geräte, die im Service-VPN 10 der Zweigstellen-Router gehostet werden, die überlappende IP 192.168.10.0/24 konfiguriert.

In dieser speziellen Topologie gibt es ein Rechenzentrum (Rechenzentrum verfügt nur über MPLS-Transport, in einem echten Szenario können jedoch mehrere Transporte durchgeführt werden) und zwei Außenstellen, die über eine Verbindung mit dem SD-WAN-Overlay über MPLS und Internettransport verfügen. Service-VPN 10 wird an allen Standorten konfiguriert. In Zweigstellen ist der SIG-Tunnel (primär und Backup) für Zscaler konfiguriert. DIA wird für bestimmte Ziel-IPs konfiguriert, um den Zscaler zu umgehen. Bei einem Ausfall der Internetverbindung in Zweigstellen muss der gesamte Datenverkehr über MPLS-Transport an das Rechenzentrum gesendet werden.

eBGP wird auf dem Service-VPN 10 mit dem Zscaler-Router am DC-Ende konfiguriert. Der RZ-Router empfängt die Standardroute vom Zscaler-Router und wird in OMP umverteilt.

 Hinweis: Die in diesem Lab-Szenario erwähnten öffentlichen IP-Adressen stammen aus der Dokumentation RFC 5737.




Spezifikation

- Nutzen Sie sich überschneidende IP-Adressen für Zweigstellen-1 und Zweigstellen-2 auf dem serviceseitigen VPN 10.
- In einem typischen Szenario muss bei aktiviertem MPLS und Internettransport der Datenverkehr von VPN 10 über den SIG-Tunnel beendet werden.
- Für bestimmte IP-Zielpräfixe muss der Datenverkehr den SIG-Tunnel umgehen und über DIA beenden.
- Bei einem Ausfall der Internetverbindung muss der gesamte/internetgebundene Datenverkehr von VPN 10 über das Rechenzentrum beendet werden.

Lösung

Um diese Anforderung zu erfüllen, verwendet das SD-WAN Service Side NAT und DIA mit Datenrichtlinie.

- Die serviceseitige NAT wird auf jedem Zweigstellen-Router mit unterschiedlichen NAT-Pool-IP-Adressen konfiguriert.
- Bei einem Ausfall der Internetverbindung, wenn der Datenverkehr an das SD-WAN-Overlay gesendet wird, wird die Quell-IP über den konfigurierten NAT-Pool an die IP-Adresse weitergeleitet.
- Der RZ-Router erkennt die Post-NAT-Adresse bei sich überschneidenden Subnetzen.

 Hinweis: Zur Darstellung des normalen Datenverkehrs über den SIG-Tunnel von VPN 10 wird die öffentliche IP 192.0.2.100 verwendet. Für ein bestimmtes Ziel wird über DIA 192.0.2.1 verwendet. Entsprechende Konfigurationen sind im Konfigurationsabschnitt dargestellt.

Konfigurieren

Konfiguration von Zweigstelle 1

Die Konfiguration des Zweigstellen-1-Routers ist wie folgt.

```
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
!

```

Konfiguration von Zweigstelle 2

Die Konfiguration des Zweigstellen-2-Routers ist wie folgt.

```

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
!

```

Konfiguration des RZ-Routers

Die Konfiguration des RZ-Routers ist wie folgt.

```


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-Richtlinie

Die Konfiguration der vSmart-Richtlinie ist wie folgt.

 **Hinweis:** Beachten Sie, dass in der Richtlinie für beide Zweigstellen aufgerufen **nat pool 1** wird. Es sind jedoch zwei verschiedene IP-Pools für jede Zweigstelle konfiguriert (172.16.2.0/30 für Zweigstelle-1 und 172.16.2.8/30 für Zweigstelle-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

!e 32
!
apply-policy
site-list BranchA-B
```

```
data-policy _VPN10_1-Branch-A-B-Central-NAT-DIA from-service
!
```

Failover-Szenarien

Datenverkehrsfluss in der Außenstelle 1 - Normales Szenario

Wenn beide Transportnetze aktiv sind, wie in der Ausgabe gezeigt, verlässt der Datenverkehr standardmäßig den primären SIG-Tunnel **Tunnel100512**. Wenn der primäre Tunnel ausfällt, wechselt der Datenverkehr zum Backup-Tunnel **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 zeigt, dass der Datenverkehr den SIG-Tunnel durchquert.

```
<#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#
```

Der Datenverkehr zu einem bestimmten Ziel **192.0.2.1** wird über DIA (NAT an WAN-IP-Adresse) weitergeleitet.

```
<#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#
```

Datenverkehrsfluss in Zweigstelle 2 - Normales Szenario

Ein ähnliches Verhalten ist auch auf dem Zweigstellen-2-Router zu beobachten.

```
<#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

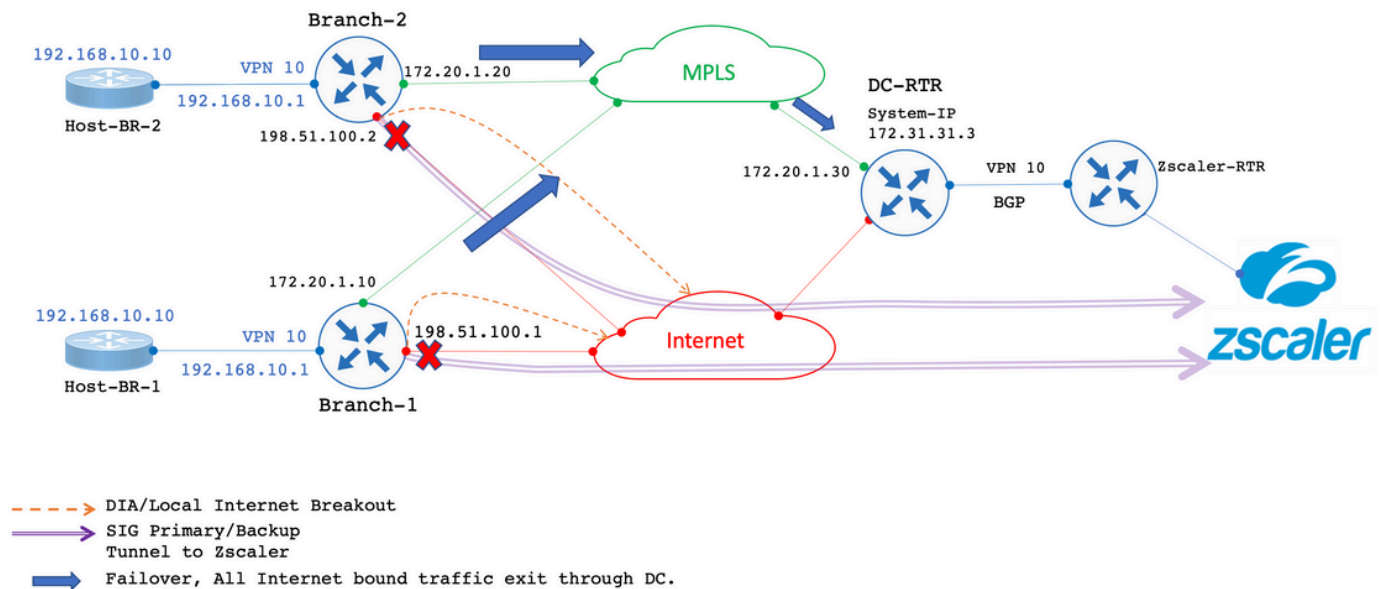
Total number of translations: 1

Branch-2#

Fehlerszenarien

Fehlerszenario für Zweigstelle 1

In diesem Abschnitt wird das Verhalten bei einem Internetausfall beschrieben.



Die Internetverbindung wurde vom Administrator deaktiviert, um einen Internetausfall zu simulieren.

```
<#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#
```

Die Ausgabe zeigt, dass der Branch-1-Router beim Ausfall der Internetverbindung die Standardroute vom DC-Router über OMP empfängt.

172.31.31.3 ist die System-IP-Adresse für den DC-Router.

```
<#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>

Der an bestimmte Datenverkehr 192.0.2.100 wird per NAT an den serviceseitigen NAT-Pool geleitet und verlässt diesen über das Rechenzentrum.

<#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#

Die Ergebnisse der Traceroute zeigen, dass der Datenverkehr den DC-Pfad nutzt. 172.20.1.30 ist die WAN-IP-Adresse für den MPLS-Transport des Routers im Rechenzentrum.

<#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#

Datenverkehr, der an die spezifische IP 192.0.2.1 gerichtet ist, wird ebenfalls per NAT an den serviceseitigen NAT-Pool geleitet und läuft über DC ab.

<#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>

Konfiguration der Datenrichtlinie über 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
```

Branch-2-Fehlerszenario

Ein ähnliches Verhalten tritt auch bei Zweigstellen-2-Routern auf, wenn ein Internet-Failover vorliegt.

```
<#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

```

Routing-Status des RZ-Routers

Die Routing-Tabelle wird vom DC-Router erfasst.

Wie in der Ausgabe gezeigt, kann der DC-Router sich überschneidende IP-Adressen aus beiden Zweigstellen unterscheiden, wobei die IP-Adressen aus den **post-NAT IP** Zweigstellen (**SS-NAT pool** 172.16.2.0 und 172.16.2.8) und nicht aus der eigentlichen LAN-IP stammen **192.168.10.0/24** 172.31.31.1 und 172.31.31.2 für Zweigstelle-1/Zweigstelle-2 **system-ip** konfiguriert sind. System-IP **172.31.31.10** gehört zu **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 -

Überprüfung

Für diese Konfiguration ist derzeit kein spezielles Prüfverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zusätzliche Informationen

Szenario-1

In Szenarien, in denen Controller in Version 20.3.4 ausgeführt werden und cEdge 17.3.3a oder frühere Versionen mit denselben Konfigurationen ausführt, wird beobachtet, dass in Normal-/Failover-Szenarien der Datenverkehr per NAT an den serviceseitigen NAT-Pool geleitet wird und den Datenfluss unterbricht.

cEdge-Aufnahmen:

<#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
```

Die Ausgabe wird von cEdge-Läufen in der Version 17.3.3a erfasst. Der über den SIG-Tunnel bestimmte Datenverkehr wird per NAT an den SS-NAT-Pool weitergeleitet und verworfen. Eine Korrektur ist ab Version 17.3.6 verfügbar.

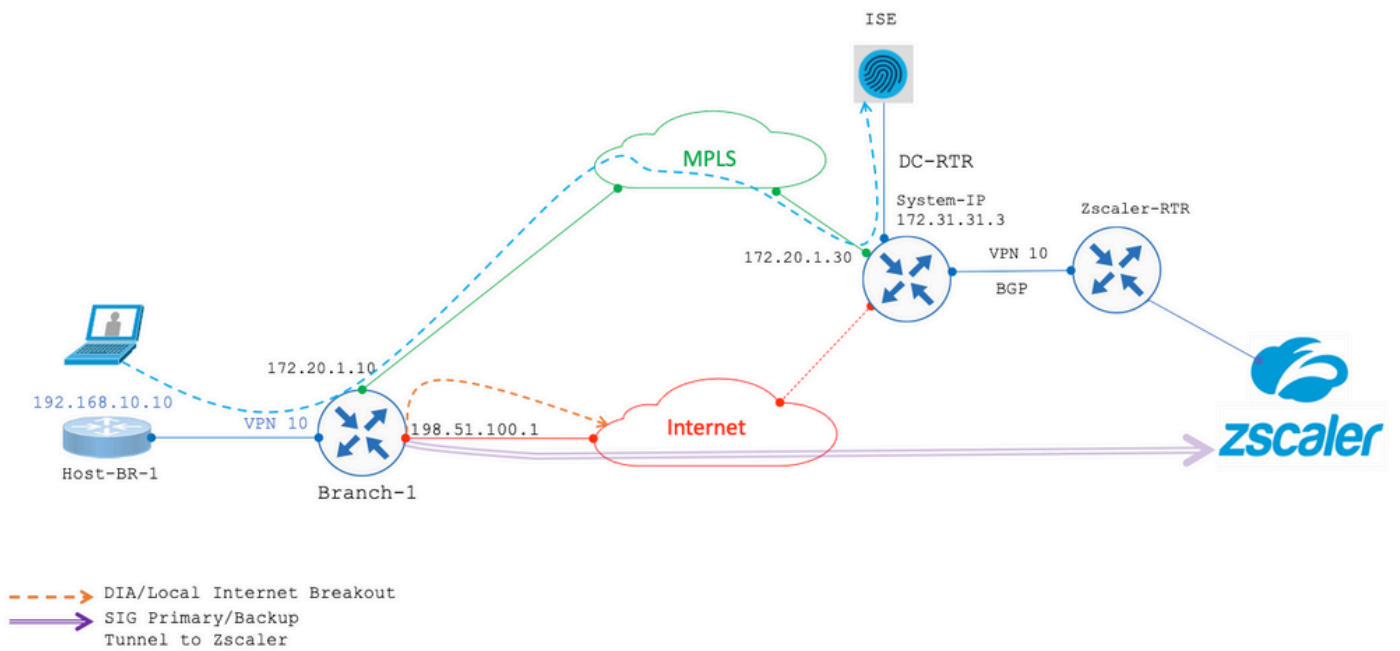
Szenario-2

Anforderung (Service Side NAT (SS-NAT) mit UTD-Inspektion)

Angenommen, der Benutzer hat folgende Anforderungen gestellt:

1. Wenn sowohl der Internet- als auch der MPLS-Transport funktionsfähig sind, können Wireless-Clients in VPN 10 zur Authentifizierung an die ISE im Rechenzentrum weitergeleitet werden. Außerdem kann der VPN 10-Datenverkehr, der über das SD-WAN-Overlay übertragen wird, überprüft werden. Da dieser Datenverkehr Teil des Overlays ist, nutzt VPN 10 die SS-NAT-Funktion. [UTD + SS-NAT]
2. Wenn der Internet-Transport nicht mehr verfügbar ist, kann der gesamte Datenverkehr von VPN 10, einschließlich Wireless- und kabelgebundenem Datenverkehr, mithilfe des MPLS-Transports über das Overlay geleitet werden. Dieser Verkehr kann auch einer Überprüfung unterzogen werden. [UTD + SS-NAT]

Mit diesen Anforderungen soll ein sicherer und überwachter Datenverkehrsfluss für VPN 10 in Zweigstelle 1 unter unterschiedlichen Netzwerkbedingungen sichergestellt werden.



In beiden oben genannten Szenarien wird die UTD-Inspektion mit einer SS-NAT-Kombination durchgeführt. Nachfolgend finden Sie die UTD-Beispielkonfiguration für dieses Szenario.

```

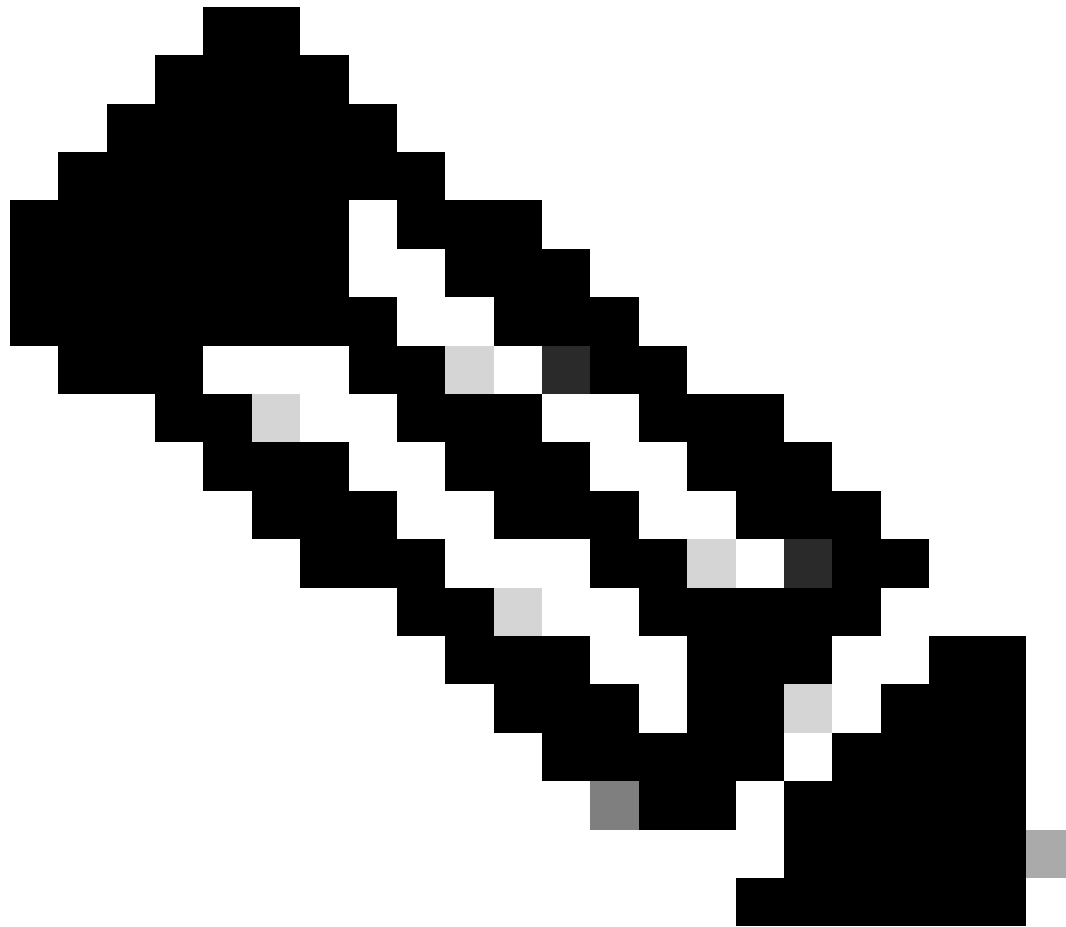
policy utd-policy-vrf-10
all-interfaces
vrf 10
threat-inspection profile TEST_IDS_Policy
exit
  
```



Warnung: Beachten Sie, dass die Kombination von UTD mit SS-NAT derzeit nicht unterstützt wird. Daher funktioniert diese Kombination nicht wie erwartet. Eine Lösung für dieses Problem könnte in zukünftigen Versionen enthalten sein.

Problemumgehung

Die Problemumgehung besteht darin, die UTD-Richtlinie für überlappendes IP-VPN (in diesem Fall VPN 10) zu deaktivieren und globales VPN zu aktivieren.



Hinweis: Diese Konfiguration wurde in der Version 17.6 getestet und verifiziert.

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


Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.