複数サイト間での同じVPNに対する重複IPの設定（障害シナリオ）

内容

はじめに

このドキュメントでは、SD-WANオーバーレイの複数のサイト間で同じVPN内のアドレス空間が重複するシナリオについて説明します。この図は、サンプルネットワーク、通常/フェールオーバーシナリオでのトラフィックの動作、設定、および検証を示しています。

前提条件

要件

SD-WANに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- SD-WANコントローラバージョン20.6.3
- Cisco IOS® XE（コントローラモードで実行）17.6.3a
- ホストデバイス(CSR1000V)17.3.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ここでは、この記事で使用されている略語のリストを見つけることができます。

- セキュアインターネットゲートウェイ – シグニチャ
- Virtual Routing and Forwarding(VRF):VRF
- バーチャルプライベートネットワーク – VPN
- インターネットへの直接アクセス – DIA
- ネットワークアドレス変換 – NAT
- マルチプロトコルラベルスイッチング(MPLS)
- サービス側のネットワークアドレス変換 – SS-NAT
- データセンター – DC
- オーバーレイ管理プロトコル – OMP
- インターネットプロトコル – IP

サービス側NATの詳細については、シスコのドキュメント『サービス側NAT』を参照してください。

ネットワーク図

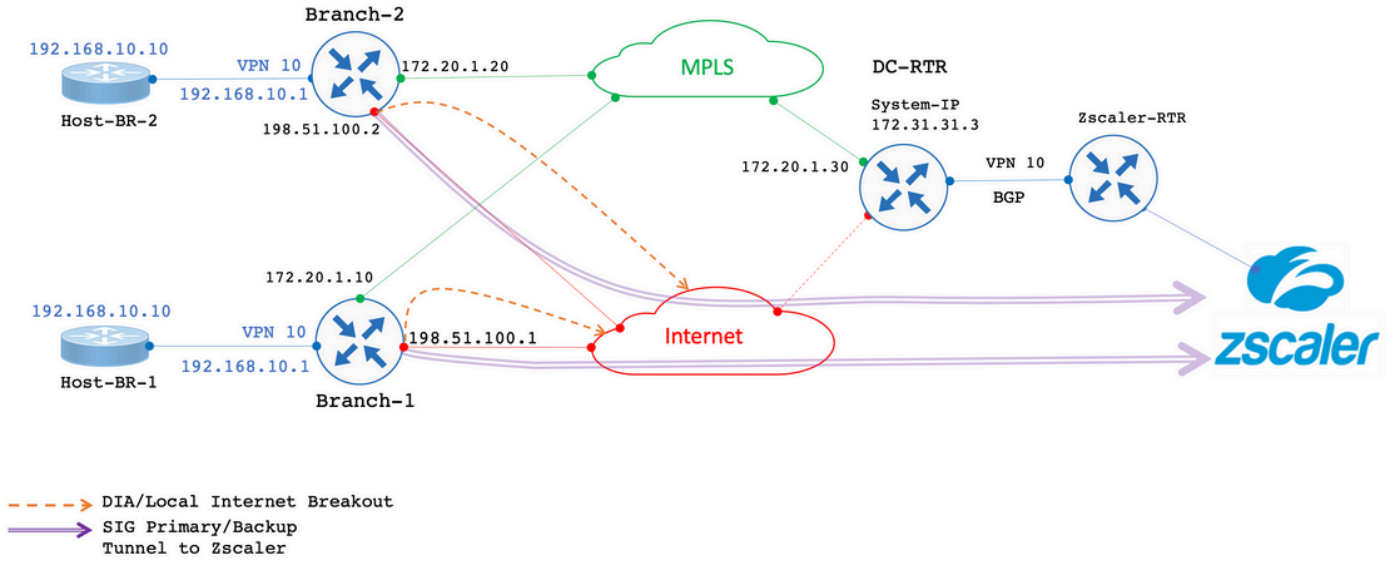
注：このトポロジでは、各ブランチルータのサービスVPN 10でホストされているデバイスに重複するIP 192.168.10.0/24が設定されています。

この特定のトポロジでは、1 DC（DCにはMPLSトランスポートしかありませんが、実際のシナリオでは複数のトランスポートが存在する可能性があります）と、MPLSおよびインターネットトランスポート経由でSD-WANオーバーレイに接続できる2つのブランチロケーションがあります。サービスVPN 10はすべての場所で設定されています。ブランチでは、Zscalerに対してSIGトンネル（プライマリおよびバックアップ）が設定されています。DIAは、Zscalerをバイパスする特

定の宛先IP用に設定されています。ブランチでインターネットリンク障害が発生した場合、すべてのトラフィックがMPLSトランスポートを介してDCに送信される必要があると想定されます。

eBGPは、DC側のZscalerルータを使用してサービスVPN 10で設定されます。DCルータはZscalerルータからデフォルトルートを受信し、OMPに再配布されます。

注：このラボシナリオに記載されているパブリックIPアドレスは、ドキュメントRFC5737から取得されたものです。



仕様

- サービス側のVPN 10でBranch-1とBranch-2のIPアドレスを重複させる

- 一般的なシナリオでは、MPLSとインターネットトランスポートが稼働している場合、VPN 10からのトラフィックはSIGトンネル経由で送信される必要があります。
- 特定のIP宛先プレフィックスでは、トラフィックはSIGトンネルをバイパスし、DIA経由で終了する必要があります。
- インターネットリンクに障害が発生した場合、VPN 10からのすべてのインターネットバウンドトラフィックは、DC経由で終了する必要があります。

解決方法

この要件を満たすために、SD-WANではサービス側のNATとデータポリシー付きのDIAが使用されます。

- サービス側NATは、各ブランチルータで異なるNATプールIPアドレスを使用して設定されます。
- トラフィックがSD-WANオーバーレイに送信されるインターネットリンクに障害が発生した場合、送信元IPは、設定されたNATプールからIPアドレスにNAT変換されます。
- DCルータは重複するサブネットのポストNATアドレスを認識します。

注:VPN 10からのSIGトンネルを介した通常のトラフィックを示すために、パブリックIP 192.0.2.100を使用し、DIAを介した特定の宛先に対しては192.0.2.1を使用します。対応する設定は、設定セクションに示されています。

設定

ブランチ1の設定

Branch-1ルータの設定は次のとおりです。

```
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
!
```

Branch-2の設定

Branch-2ルータの設定は次のとおりです。

```
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
!
```

DCルータの設定

DCルータの設定は次のとおりです。

```
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ポリシー

vSmartポリシーの設定は次のとおりです。

注: **nat pool 1** は両方のブランチのポリシーで呼び出されますが、各ブランチには2つの異なるIPプールが設定されています(Branch-1には172.16.2.0/30、Branch-2には172.16.2.8/30)。

<#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
!
```

フェールオーバーシナリオ

ブランチ1トラフィックフローの通常のシナリオ

両方のトランスポートが出力に示すように起動すると、デフォルトで、トラフィックはプライマリSIGトンネル **Tunnel100512**を経由して送信されます。 プライマリトンネルがダウンすると、トラフィックスイッチがバックアップトンネルである **Tunnel100513**に切り替わります。

<#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は、トラフィックがSIGトンネルを通過することを示します。

<#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#

特定の宛先へのトラフィックは、DIA（NATでWAN IPアドレスに変換）を経由して出口に **192.0.2.1** 到達します。

<#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トラフィックフローの通常のシナリオ

同様の動作がBranch-2ルータでも見られます。

<#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#
```

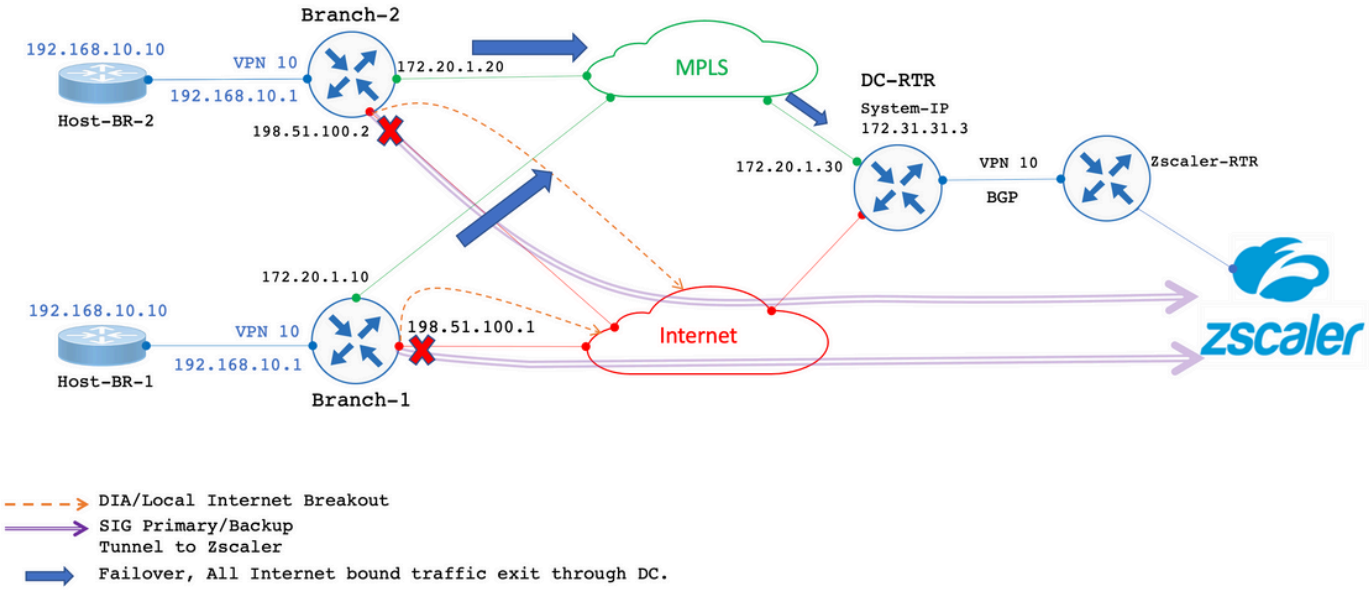
<#root>

```
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#
```

障害シナリオ

Branch-1障害シナリオ

この項では、インターネット障害時の動作について説明します。



インターネットリンクは、インターネット障害リンクをシミュレートするために、管理上シャットダウンされます。

<#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#
```

出力には、インターネットリンク障害シナリオの間に、Branch-1ルータがOMPを介してDCルータからデフォルトルートを受信することが示されています。**172.31.31.3**は、DCルータのシステムIPです。

<#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>

宛先が192.0.2.100のトラフィックは、サービス側のNATプールにNATされ、DC経由で送信されます。

<#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#

tracerouteの結果は、トラフィックがDCパスを通ることを示しています。172.20.1.30は、DCルータのMPLSトランスポートWAN IPです。

<#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#
```

特定のIP 192.0.2.1宛てのトラフィックも、サービス側のNATプールにNATされ、DC経由で送信されます。

<#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>

vSmartからプッシュされるデータポリシー設定：

<#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障害シナリオ

同様の動作は、インターネットフェールオーバーがある場合のBranch-2ルータでも見られます。

<#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ルータのルーティングステータス

ルーティングテーブルはDCルータからキャプチャします。

出力に示されているように、DCルータは、実際のLAN IPではなく **post-NAT IP導 SS-NAT pool** 出されたアドレス（172.16.2.0および172.16.2.8）を使用して両方のブランチから重複するIPアドレスを区別するこ **192.168.10.0/24172.31.31.1** と **172.31.31.2** ができ、Branch-1/Branch-2用に設 **system-ip** 定されています。System-IP **172.31.31.10** は **vSmart**に属しています。

<#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 -
```

確認

現在のところ、この設定に固有の確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

追加情報

シナリオ1

コントローラがバージョン20.3.4であり、cEdgeが同じ設定で17.3.3a以下のバージョンを実行するシナリオでは、通常/フェールオーバーシナリオで、トラフィックがサービス側のNATプールにNATされ、フローが中断されることが確認されています。

cEdgeキャプチャ：

<#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

出力は、17.3.3aバージョンで稼働するcEdgeからキャプチャしたものです。SIGトンネルを経由して送信されたトラフィックは、SS-NATプールでネットワークアドレス変換(NAT)され、廃棄されます。バージョン17.3.6以降では修正が提供されています。

シナリオ2

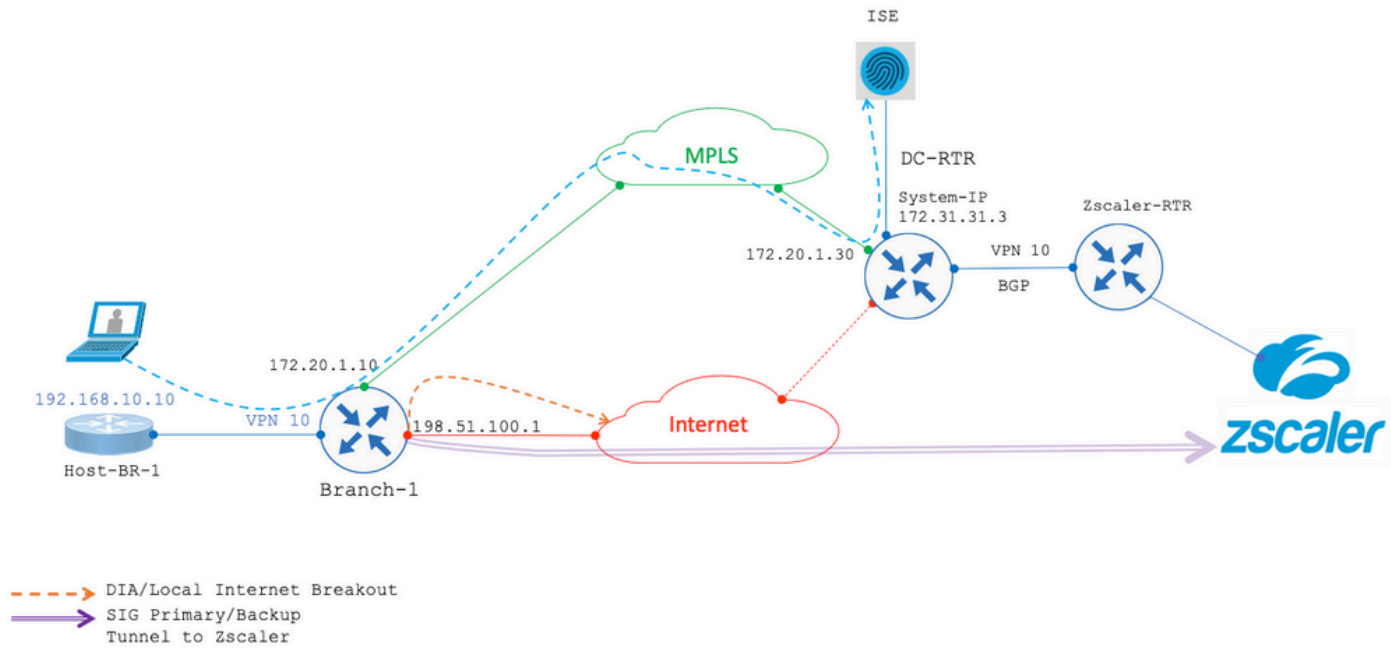
要件(サービス側NAT(SS-NAT)とUTDインスペクション)

ユーザが次の要件を要求したと仮定します。

1. インターネットとMPLSの両方のトランスポートが動作している場合、認証のためにVPN 10のワイヤレスクライアントをデータセンター内のISEに誘導できます。また、SD-WANオーバーレイを経由するVPN 10トラフィックは検査を受けることができます。このトラフィックはオーバーレイの一部であるため、VPN 10はSS-NAT機能を使用します。[UTD + SS-NAT]

2. インターネットトランスポートが使用できなくなった場合、VPN 10からのすべてのトラフィック（無線と有線の両方のトラフィックを含む）は、MPLSトランスポートを使用してオーバーレイ経由でルーティングできます。このトラフィックも検査の対象となる可能性があります。[UTD + SS-NAT]

これらの要件の目的は、さまざまなネットワーク条件下で、Branch-1のVPN 10のトラフィックフローを安全に監視することです。



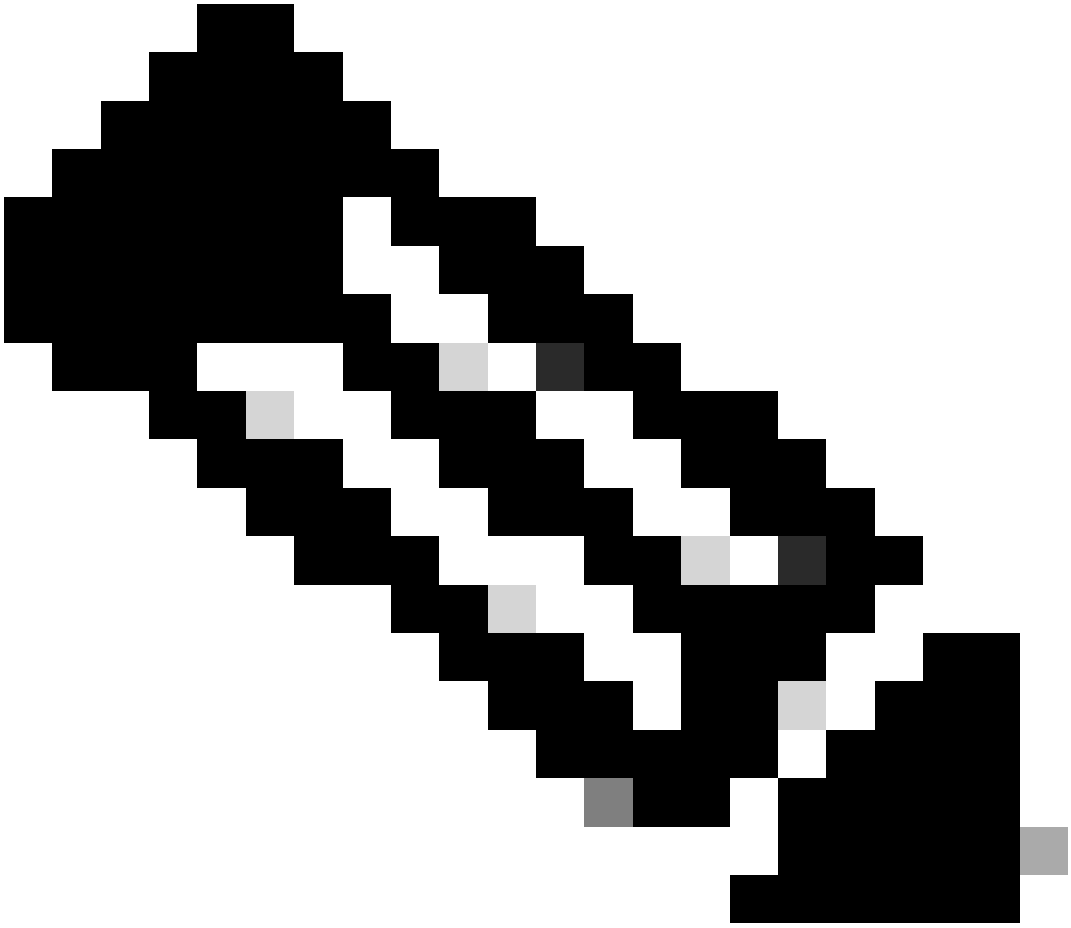
前述の両方のシナリオで、SS-NATの組み合わせを使用したUTDインスペクションを使用しています。このシナリオのUTDの設定例を次に示します。

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

警告：現在、UTDとSS-NATの組み合わせはサポートされていないことに注意してください。したがって、この組み合わせは期待どおりに動作しません。将来のリリースでは、この問題の修正が含まれる可能性があります。

回避策

回避策は、Overlapping IP VPN（この場合はVPN 10）のUTDポリシーを無効にし、Global VPNを有効にすることです。



注：この設定は、17.6バージョンでテストおよび検証されています。

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。