針對故障場景中的多個站點配置同一VPN的重疊IP

目錄

簡介

本文檔介紹在SD-WAN重疊中的多個VPN中地址空間重疊的場景。它描述了示例網路、正常/故障切換情況下的流量行為、配置和驗證。

必要條件

需求

Cisco建議您應具備SD-WAN的相關知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- SD-WAN控制器版本20.6.3
- Cisco IOS® XE（在控制器模式下運行） 17.6.3a
- 主機裝置(CSR1000V) 17.3.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

您可以在此處找到本文中使用的縮寫詞清單。

- 安全網際網路閘道- SIG
- 虛擬路由和轉送- VRF
- 虛擬私人網路- VPN
- 直接網際網路存取- DIA
- 網路地址轉換- NAT
- 多重協定標籤交換- MPLS
- 服務端網路位址翻譯- SS-NAT
- 資料中心- DC
- 重疊管理通訊協定- OMP
- Internet協定- IP

有關服務端NAT：服務端NAT的詳細資訊，請參閱Cisco文檔

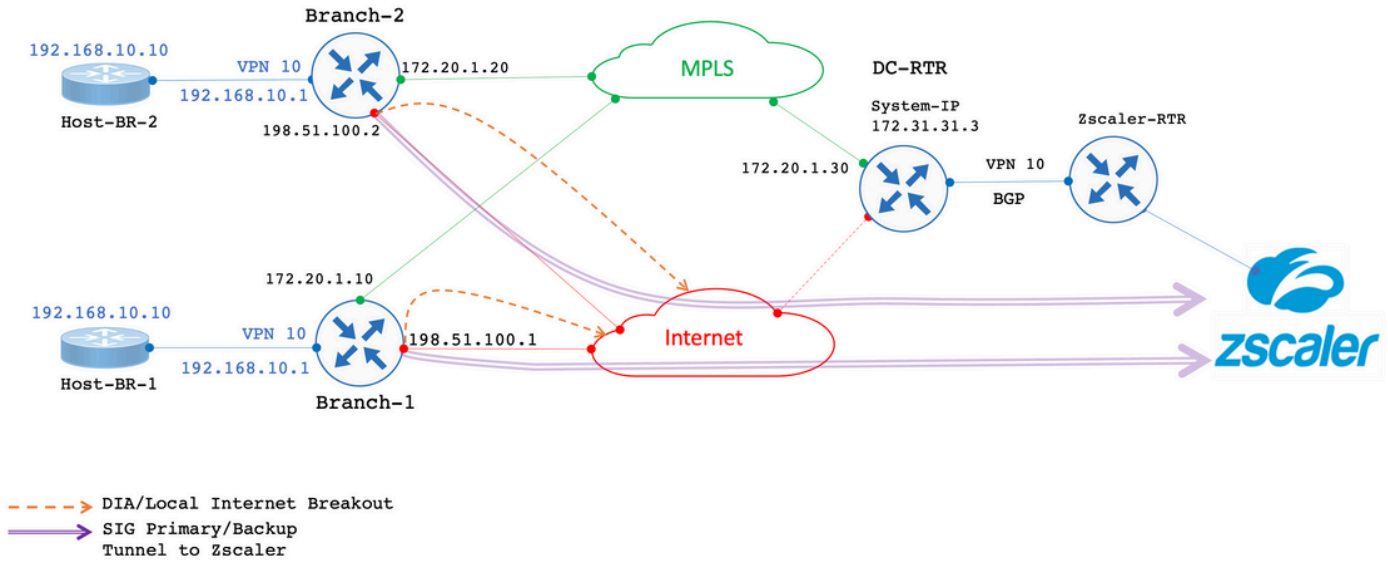
網路圖表

注意：在此拓撲中，每個分支路由器的服務VPN 10中託管的裝置都配置了重疊的IP 192.168.10.0/24。

在此特定拓撲中，有1個DC（DC只有MPLS傳輸，但在實際場景中可能有多個傳輸）和2個分支機構位置透過MPLS和Internet傳輸連線到SD-WAN覆蓋。所有位置都配置了服務VPN 10。分支已將SIG隧道（主隧道和備用隧道）配置為Zscaler。DIA針對特定目標IP進行配置，以繞過Zscaler。如果分支機構的Internet鏈路發生故障，則所有流量必須透過MPLS傳輸傳送到DC。

eBGP在服務VPN 10上配置，DC端使用Zscaler路由器。DC路由器接收來自Zscaler路由器的預設路由，並將其重分配到OMP中。

注意：本實驗場景中提到的公用IP地址取自文檔RFC5737。



規格

- 利用服務端VPN 10上Branch-1和Branch-2的IP地址重疊。
- 在典型場景中，當MPLS和網際網路傳輸啟動時，來自VPN 10的流量必須透過SIG隧道退出。
- 對於特定IP目標字首，流量必須繞過SIG隧道並透過DIA退出。
- 如果Internet鏈路發生故障，來自VPN 10的所有/Internet繫結流量必須透過DC退出。

解決方案

為實現這一要求，使用了SD-WAN功能服務端NAT和帶資料策略的DIA。

- 服務端NAT在每個分支路由器上配置有不同的NAT池IP地址。
- 如果流量傳送到SD-WAN重疊時出現Internet鏈路故障，則會將源IP從配置的NAT池NAT到IP地址。
- DC路由器看到重疊子網的NAT後地址。

注意：要描述從VPN 10到SIG隧道的正常資料流，使用公共IP 192.0.2.100；對於特定目標，使用DIA 192.0.2.1。相應的配置顯示在配置部分中。

設定

Branch-1配置

Branch-1路由器的配置如下。

```
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配置

Branch-2路由器的配置如下。

```
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路由器配置

DC路由器配置如下。

```
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策略

vSmart策略配置如下。

注意：請注意，兩個分支的策略中均 **nat pool 1** 被呼叫，但每個分支都配置了兩個不同的IP池(Branch-1為172.16.2.0/30，Branch-2為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
!

容錯移轉案例

Branch-1流量正常場景

當兩個傳輸都如輸出所示運行時，預設情況下流量透過主SIG隧道 **Tunnel100512**退出。 當主隧道關閉時，流量會切換到備用隧道 **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**顯示流量透過**SIG**隧道。**

<#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#
```

發往特定目的地的流量 192.0.2.1 透過DIA（NAT**連線到**WAN IP**地址）退出。**

<#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流量正常場景

在Branch-2路由器上也觀察到類似行為。

<#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
```

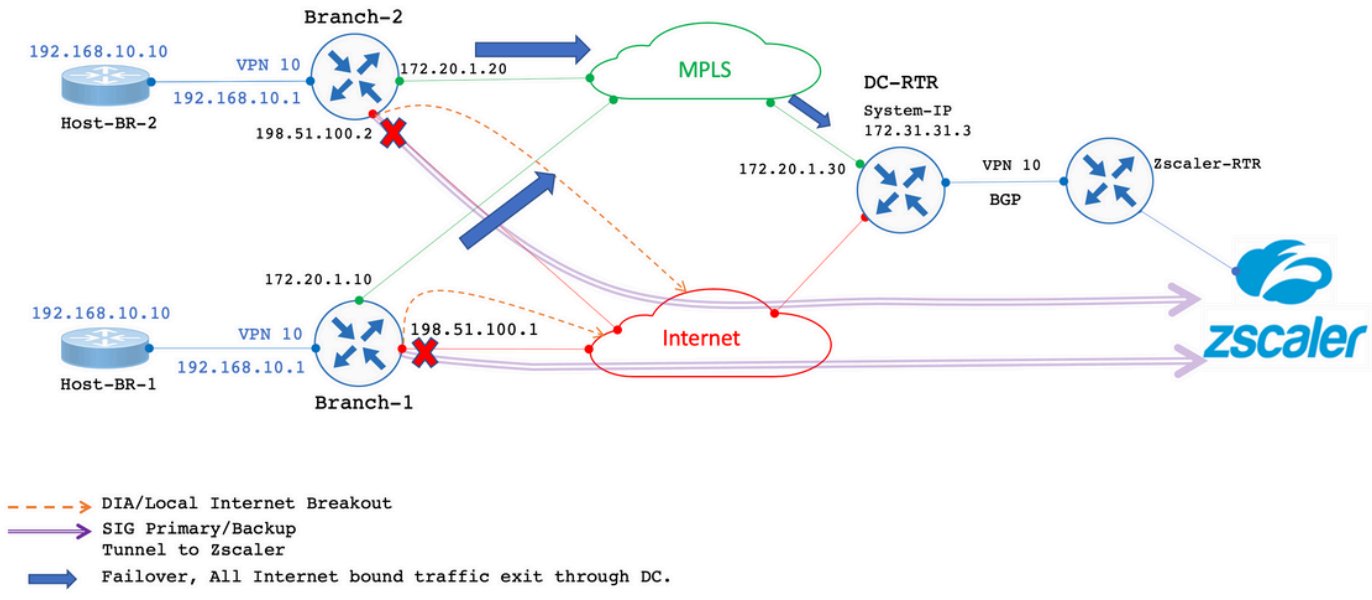
198.51.100.2:1

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

失敗案例

Branch-1故障場景

本節說明網際網路失敗期間的行為。



Internet鏈路被管理性關閉以模擬Internet故障鏈路。

<#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#

輸出顯示，在Internet鏈路故障情況下，Branch 1路由器透過OMP從DC路由器接收預設路由。**172.31.31.3**是DC路由器的系統IP。

<#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>

發往192.0.2.100的流量被NAT轉換成服務端NAT池，然後透過DC退出。

<#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結果顯示，流量採用DC路徑。172.20.1.30是DC路由器的MPLS傳輸WAN IP。

<#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#
```

發往特定IP 192.0.2.1的流量也被NAT連線到服務端NAT池並透過DC退出。

<#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>
```

從vSmart推送的資料策略配置：

<#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故障場景

在發生Internet故障切換時，Branch-2路由器中也會出現類似行為。

<#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路由器路由狀態

路由表從DC路由器捕獲資訊。

如輸出所示，DC路由器能夠使用 **post-NAT IP**派生 **SS-NAT pool**（172.16.2.0和172.16.2.8）而不是實際的LAN IP來區分兩個分支中的重疊IP地址， **192.168.10.0/24172.31.31.1** 且 **172.31.31.2** 是為Branch-1/Branch-2配 **system-ip** 置的。System-IP **172.31.31.10** 屬於 **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 -
```

驗證

目前沒有適用於此組態的具體驗證程式。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

其他資訊

案例1

在控制器使用版本20.3.4，而cEdge使用相同配置運行17.3.3a或更低版本的情況下，可以觀察到，在正常/故障轉移情況下，流量被NAT連線到服務端NAT池，並中斷流量。

cEdge擷取：

<#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
```

從17.3.3a版上運行的cEdge捕獲輸出。透過SIG隧道發往的流量透過NAT轉換到SS-NAT池並被丟棄。從17.3.6版開始提供修復。

案例2

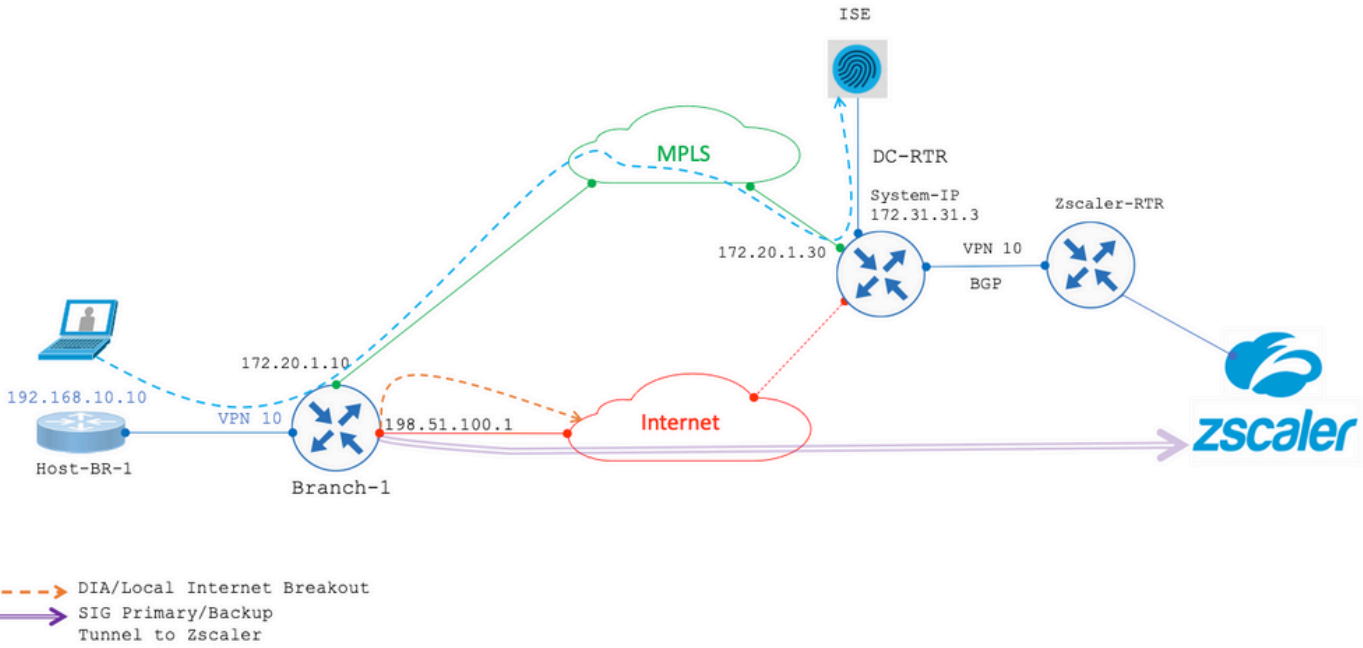
需求(含UTD檢查的服務端NAT (SS-NAT))

假設使用者已要求下列需求：

1. 當網際網路和MPLS傳輸均正常運行時，VPN 10中的無線客戶端可以定向到資料中心中的ISE進行身份驗證。此外，透過SD-WAN重疊傳輸的VPN 10流量可以接受檢查。由於此流量是重疊的一部分，VPN 10使用SS-NAT功能。[UTD + SS-NAT]

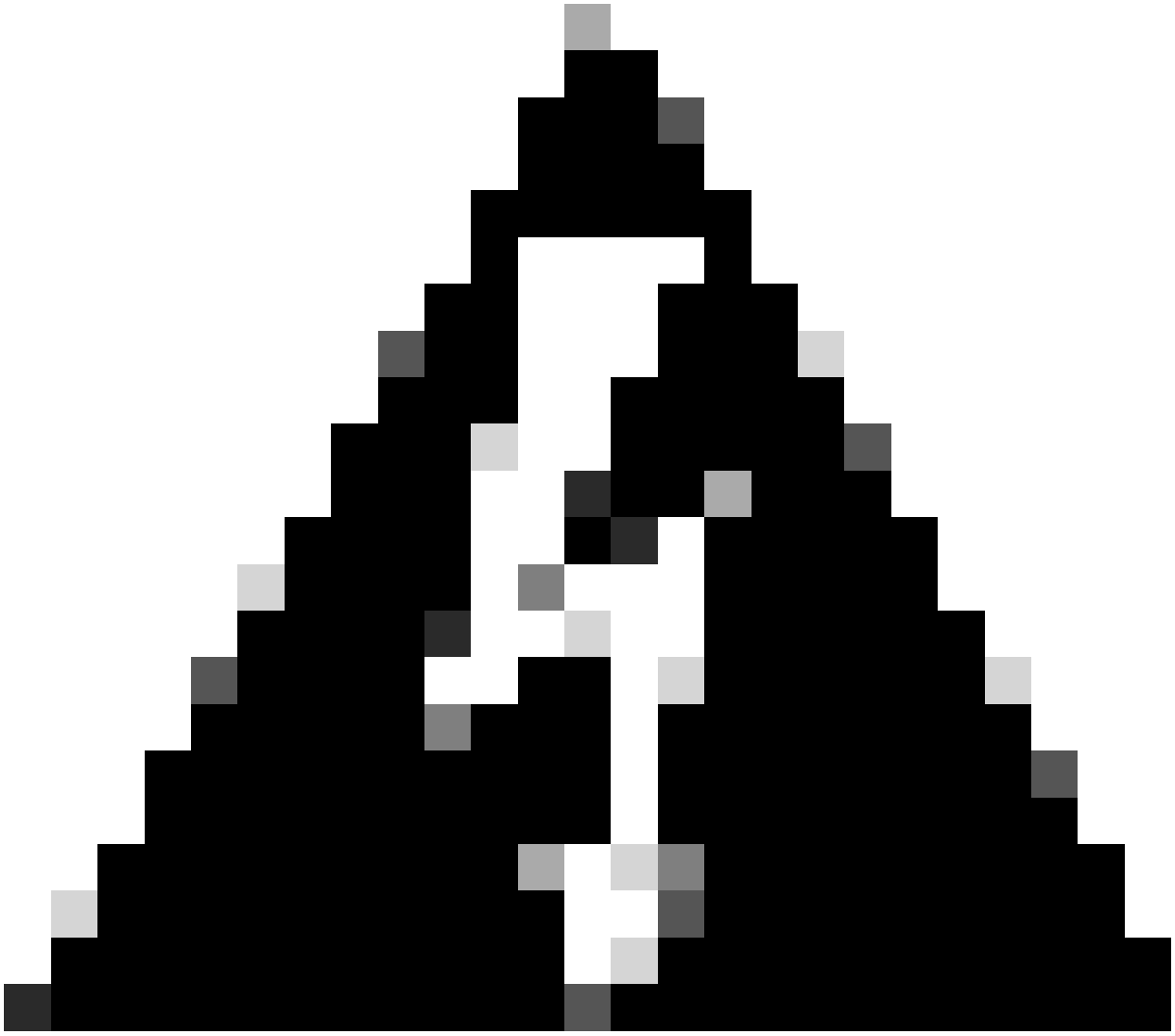
2. 如果網際網路傳輸不可用，來自VPN 10的所有流量（包括無線和有線流量）都可以使用MPLS傳輸透過重疊進行路由。此流量也可能會受到檢查。[UTD + SS-NAT]

這些要求旨在確保Branch-1中VPN 10在不同網路條件下安全且受監控的流量。



在上述兩種場景中，您都使用帶有SS-NAT組合的UTD檢測。以下是此方案的UTD配置示例。

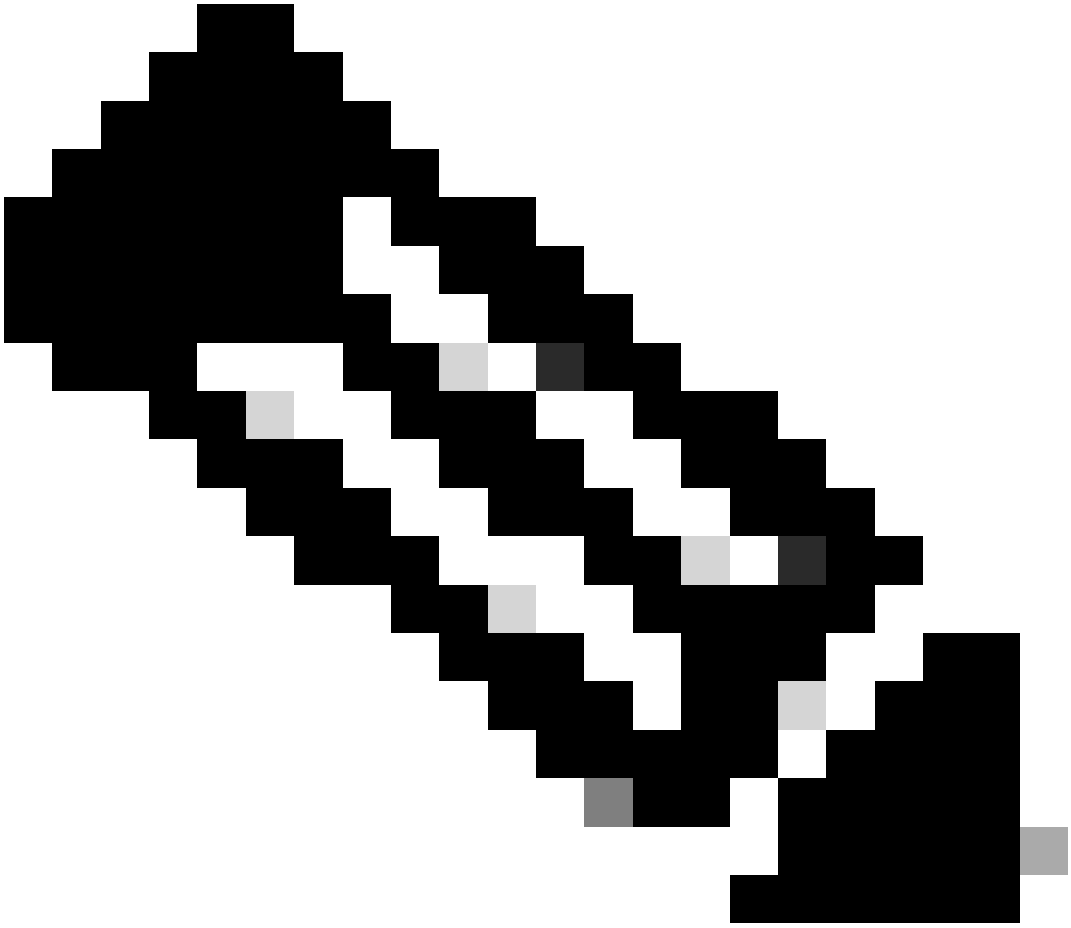
```
policy utd-policy-vrf-10
 all-interfaces
 vrf 10
 threat-inspection profile TEST_IDS_Policy
 exit
```



警告：請注意，當前不支援將UTD與SS-NAT組合。因此，此組合併不如預期般有效。未來發行版本中可能會包含此問題的修正程式。

因應措施

解決方法是停用重疊IP VPN上的UTD策略（在本例中為VPN 10）並啟用全局VPN。



注意：此配置已在17.6版本中經過測試和驗證。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。