配置多个站点间具有故障场景的同一VPN的重叠IP

目录

简介

本文档介绍在SD-WAN重叠中的多个站点上使用同一VPN中重叠地址空间的场景。它描述了示例网络、正常/故障转移场景中的流量行为、配置和验证。

先决条件

要求

Cisco建议您应具备SD-WAN的相关知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- SD-WAN控制器版本20.6.3
- Cisco IOS® XE（在控制器模式下运行）17.6.3a
- 主机设备(CSR1000V) 17.3.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

您可以在此处找到本文中使用的缩写词列表。

- 安全互联网网关- SIG
- 虚拟路由和转发- VRF
- 虚拟专用网络- VPN
- 直接互联网接入- DIA
- 网络地址转换- NAT
- 多协议标签交换- MPLS
- 服务端网络地址转换- SS-NAT
- 数据中心- DC
- 重叠管理协议- OMP
- Internet协议- IP

有关服务端NAT：服务端NAT的详细信息，请参阅思科文档

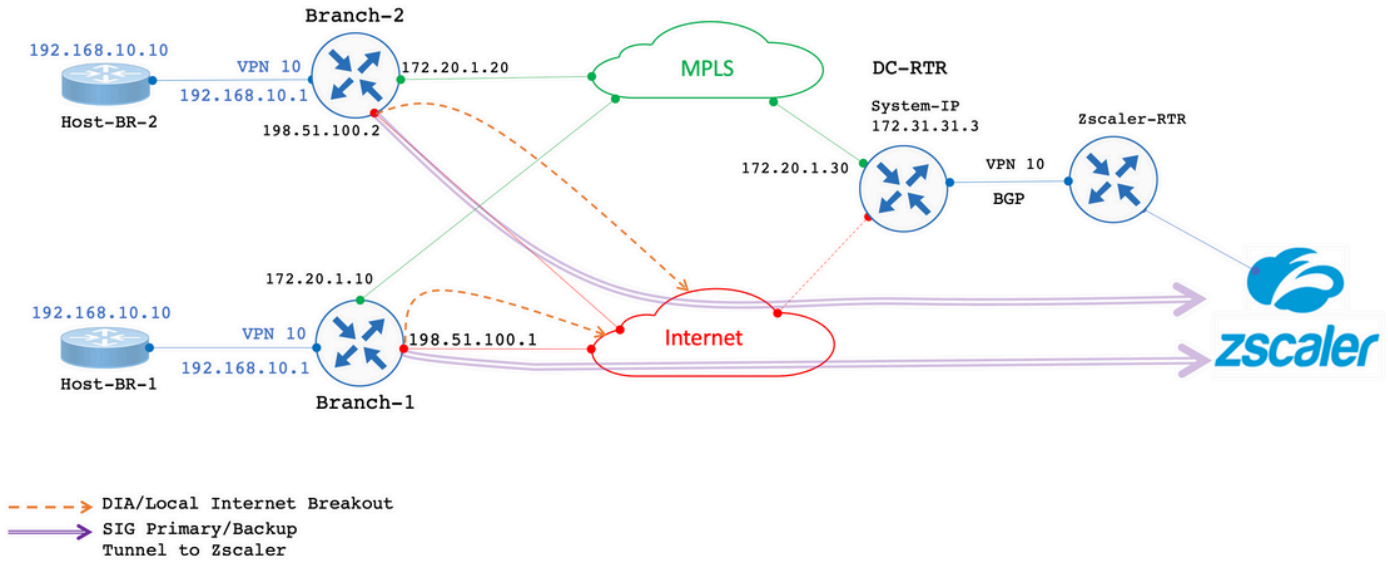
网络图

注意：在此拓扑中，每个分支路由器的服务VPN 10中托管的设备都配置了重叠的IP 192.168.10.0/24。

在此特定拓扑中，有1个DC（DC只有MPLS传输，但在实际场景中可能有多个传输）和2个通过MPLS和互联网传输连接到SD-WAN重叠的分支机构位置。所有位置都配置了服务VPN 10。分支机构将SIG隧道（主隧道和备用隧道）配置到Zscaler。DIA针对特定目标IP进行配置，以绕过Zscaler。如果分支机构出现互联网链路故障，预计所有流量必须通过MPLS传输发送到DC。

eBGP在服务VPN 10上配置，在DC端使用Zscaler路由器。DC路由器从Zscaler路由器接收默认路由并将其重分配到OMP。

注意：本实验场景中提到的公有IP地址取自文档RFC5737。



规格

- 在服务端VPN 10上为Branch 1和Branch 2使用重叠的IP地址。
- 在典型场景中，当MPLS和互联网传输启用时，来自VPN 10的流量必须通过SIG隧道退出。
- 对于特定IP目标前缀，流量必须绕过SIG隧道并通过DIA退出。
- 如果互联网链路发生故障，来自VPN 10的所有/互联网绑定的流量必须通过DC退出。

解决方案

为了实现此要求，使用了SD-WAN功能服务端NAT和带数据策略的DIA。

- 服务端NAT在每个分支路由器上使用不同的NAT池IP地址配置。
- 如果流量发送到SD-WAN重叠时Internet链路出现故障，源IP将从配置的NAT池NAT到IP地址。
- DC路由器会看到重叠子网的NAT后地址。

注意：要描述通过VPN 10的SIG隧道的正常数据流，使用公共IP 192.0.2.100，而对于特定目标，通过DIA使用192.0.2.1。相应的配置显示在配置部分中。

配置

Branch-1配置

Branch 1路由器的配置如下所示。

```
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-Router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策略配置如下所示。

注意：请注意，两个分支的策略中均 **nat pool 1** 被调用，但每个分支机构配置了两个不同的IP池(Branch-1为172.16.2.0/30，Branch-2为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
!

故障切换方案

Branch 1的流量正常场景

当两个传输均如输出所示运行时，默认情况下流量通过主SIG隧道 **Tunnel100512**退出。 当主隧道关闭时，流量交换到备用隧道 **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显示流量通过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#
```

发往特定目的地的流量 **192.0.2.1** 通过DIA（NAT转换到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的流量正常场景

在Branch 2路由器上也观察到类似行为。

<#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
```

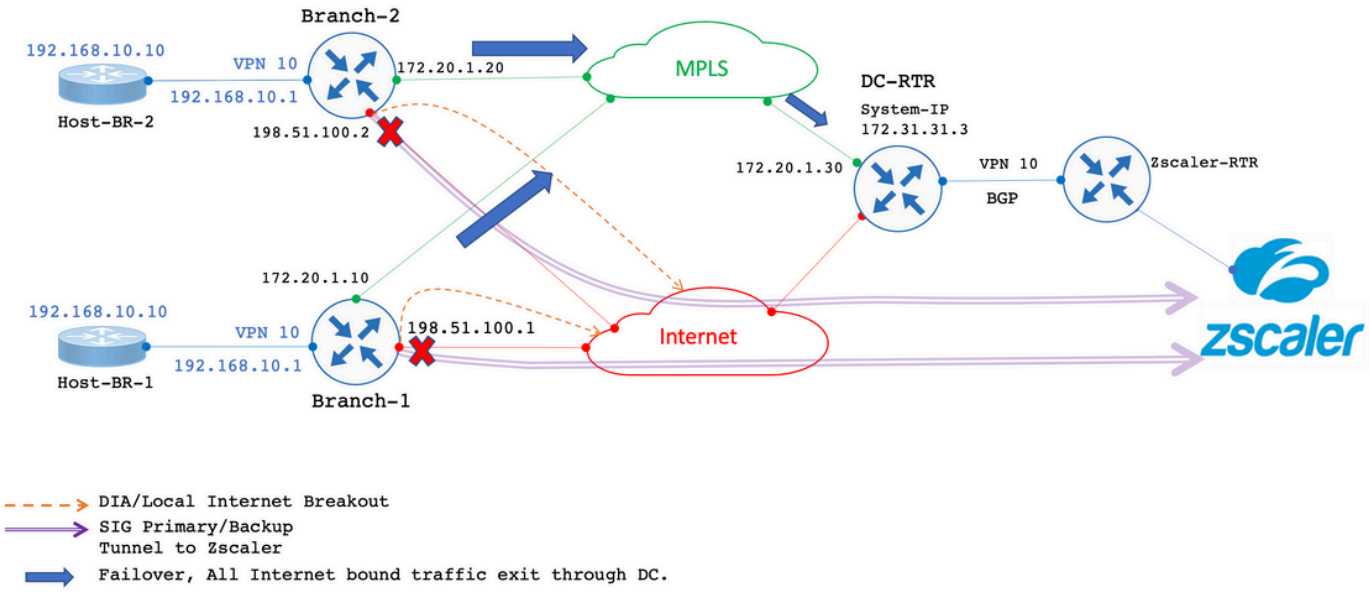
198.51.100.2:1

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

故障场景

Branch 1的故障场景

本节介绍在Internet故障期间的行为。



Internet链路因管理原因关闭，以模拟Internet故障链路。

<#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#

输出显示，在Internet链路故障情形中，Branch 1路由器通过OMP从DC路由器接收默认路由。**172.31.31.3**是DC路由器的系统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>

发往192.0.2.100的数据流会通过NAT转换到服务端NAT池，然后通过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结果显示流量采用DC路径。172.20.1.30是DC路由器的MPLS传输广域网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#
```

发往特定IP 192.0.2.1的流量也将NAT转换为服务端NAT池，并通过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>
```

从vSmart推送的数据策略配置：

<#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的故障场景

当发生Internet故障切换时，在Branch-2路由器上也会出现类似行为。

<#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路由器路由状态

路由表从DC路由器捕获信息。

如输出所示，DC路由器能够用 **post-NAT IP**派生自 **SS-NAT pool**（172.16.2.0和172.16.2.8）而不是实际的LAN IP来区分两个分支机构中的重叠IP地址， **192.168.10.0/24172.31.31.1** 并 **172.31.31.2** 且是为Branch-1/Branch-2配 **system-ip** 置的。System-IP **172.31.31.10** 属于 **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 -
```

验证

当前没有可用于此配置的特定验证过程。

故障排除

目前没有针对此配置的故障排除信息。

其他信息

场景1

在控制器使用版本20.3.4，而cEdge使用相同配置运行17.3.3a或更低版本的情况下，可以观察到，在正常/故障切换情况下，流量会通过NAT转换到服务端NAT池，并中断流量。

cEdge捕获：

```
<#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
```

捕获在17.3.3a版本上运行的cEdge的输出。通过SIG隧道发往的流量通过NAT转换到SS-NAT池并被丢弃。从17.3.6版开始提供修复。

场景2

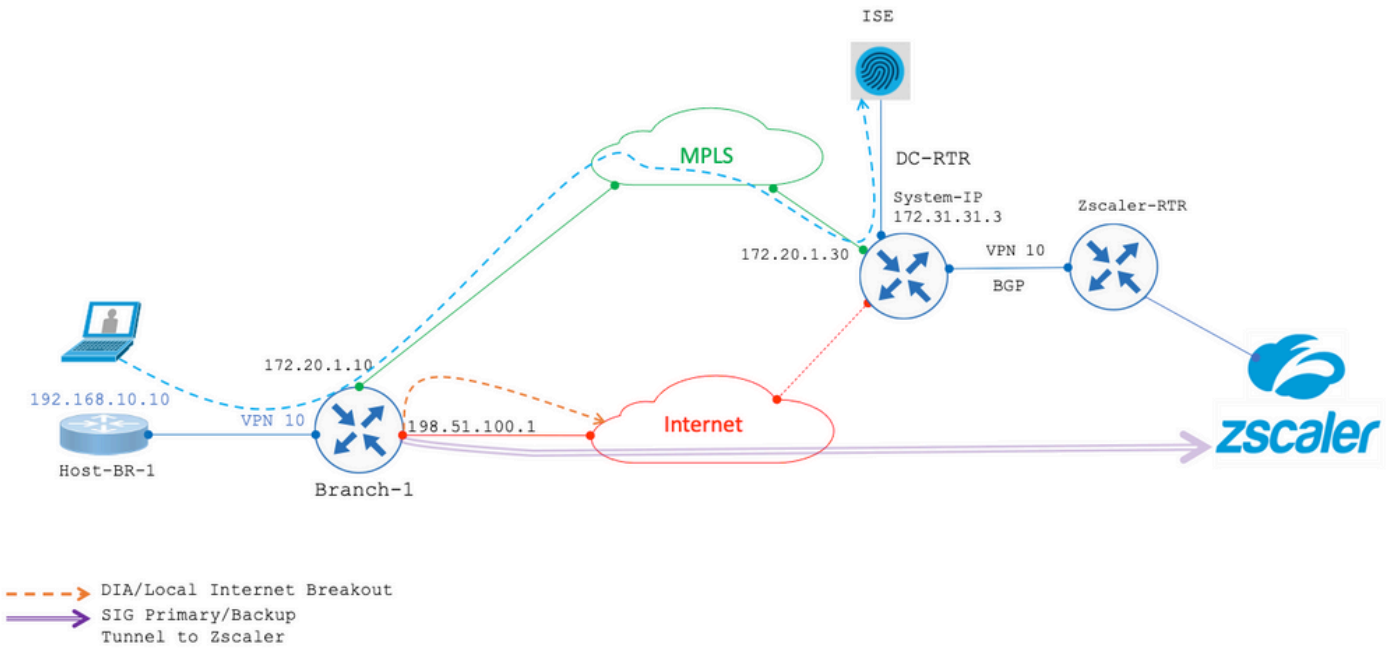
要求(带UTD检测的服务端NAT (SS-NAT))

假设用户请求了以下要求：

1. 当互联网和MPLS传输均正常运行时，VPN 10中的无线客户端可以定向到数据中心中的ISE进行身份验证。此外，通过SD-WAN重叠传输的VPN 10流量可以接受检查。由于此流量是重叠的一部分，VPN 10使用SS-NAT功能。[UTD + SS-NAT]

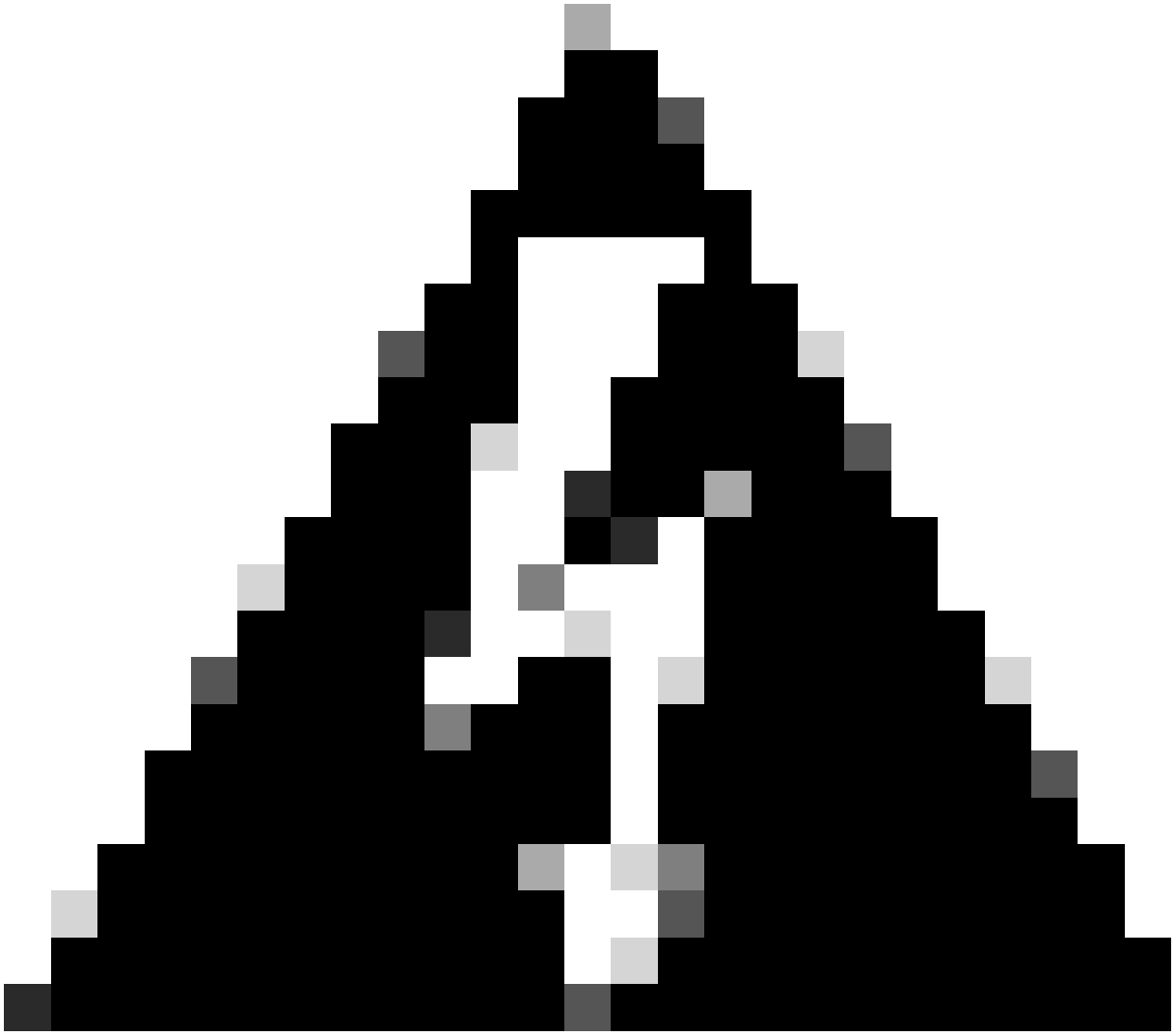
2. 如果互联网传输不可用，来自VPN 10的所有流量（包括无线和有线流量）都可以使用MPLS传输通过重叠进行路由。此流量也可能会受到检查。[UTD + SS-NAT]

这些要求旨在确保Branch 1中的VPN 10在不同网络条件下可以安全传输并受到监控。



在上述两种情况下，您都使用SS-NAT组合进行UTD检测。以下是此方案的UTD配置示例。

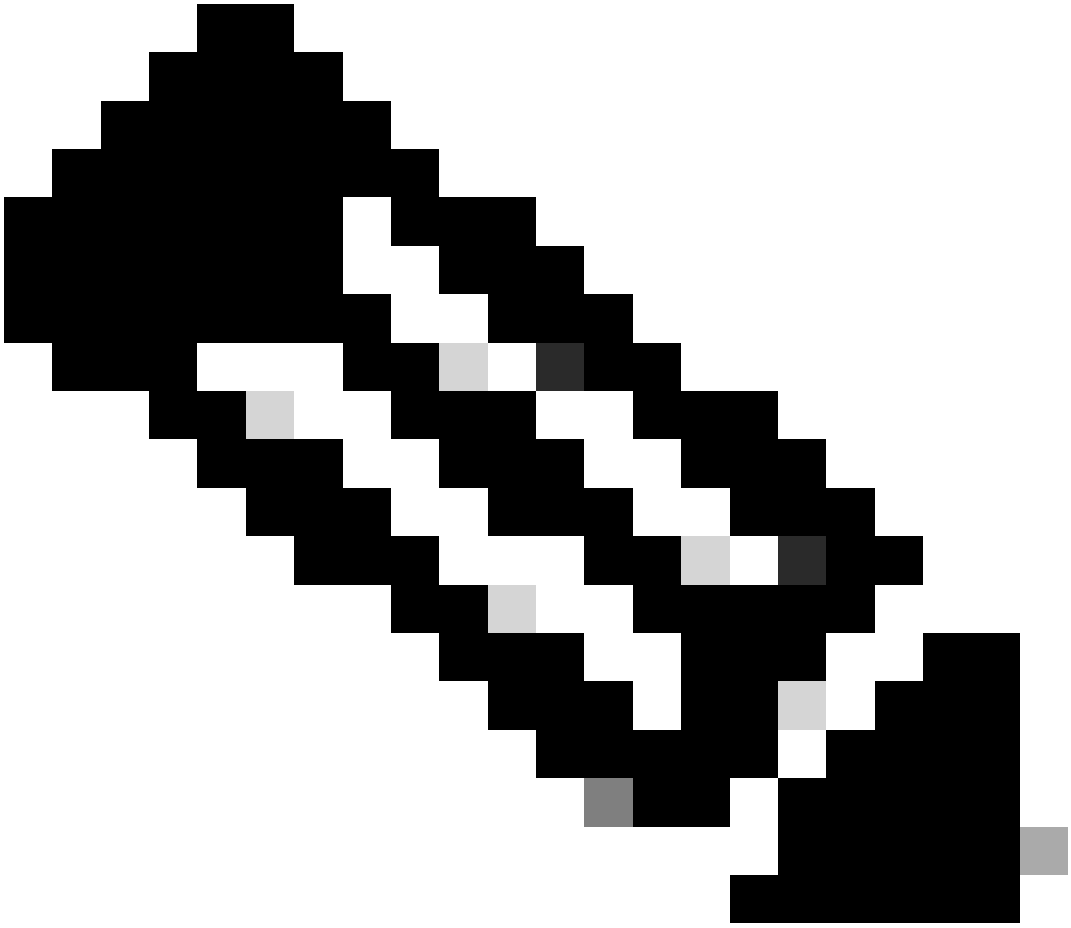
```
policy utd-policy-vrf-10
 all-interfaces
 vrf 10
 threat-inspection profile TEST_IDS_Policy
 exit
```



警告：请注意，目前不支持使用UTD与SS-NAT的组合。因此，此组合不按预期工作。未来版本中可能会包含此问题的解决方法。

解决方法

解决方法是在重叠IP VPN（本例中为VPN 10）上禁用UTD策略并启用全局VPN。



注意：此配置已在17.6版本中进行了测试和验证。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。