تكوين IP المتداخل ل VPN نفسه عبر مواقع متعددة مع سيناريوهات الفشل

المحتويات

المقدمة

يصف هذا المستند السيناريو مع مسافات عنوان متداخلة في شبكة VPN نفسها عبر مواقع متعددة في تغشية SD-WAN. وهو يصف الشبكة العينة وسلوك حركة المرور في السيناريوهات الخاصة/سيناريوهات تجاوز الفشل والتكوين والتحقق.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بشبكة SD-WAN.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- SD-WAN Controller، الإصدار 20.6.3
- Cisco IOS® XE (تشغيل في وضع وحدة التحكم) 17.6.3a
- أجهزة المضيف (CSR1000V) 17.3.3

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

هنا يمكنكم ان تجدوا قائمة باالختصارات المستعملة في هذه المقالة.

- بوابة الإنترنت الآمنة - SIG
- التوجيه الظاهري وإعادة التوجيه - VRF
- الشبكة الخاصة الظاهرية - VPN
- الوصول المباشر إلى الإنترنت - DIA
- ترجمة عنوان الشبكة - NAT
- Multi-Protocol Label Switching - MPLS
- ترجمة عنوان الشبكة الجانبية للخدمة - SS-NAT
- مركز البيانات - التيار المستمر
- بروتوكول إدارة التغشية - OMP
- بروتوكول الإنترنت - IP

راجع مستند Cisco للحصول على مزيد من التفاصيل حول NAT: NAT من جانب الخدمة

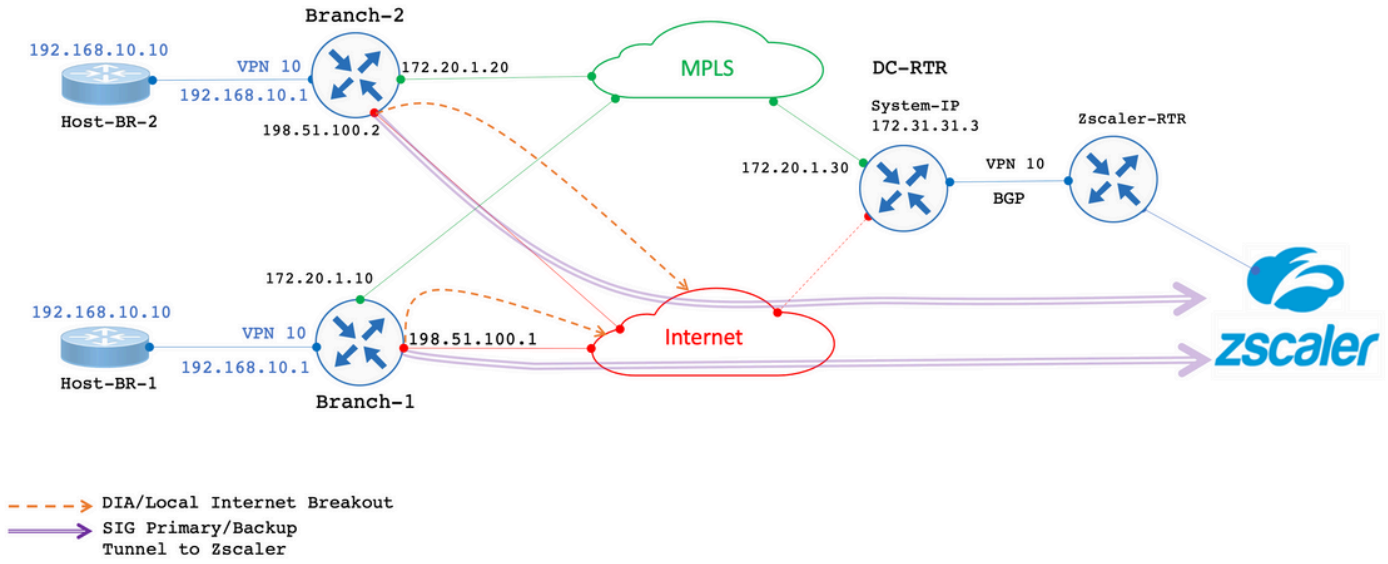
الرسم التخطيطي للشبكة

ملاحظة: في هذا المخطط، تحتوي الأجهزة المستضافة في الخدمة VPN 10 من كل موجه فرعي على IP 192.168.10.0/24 تم تكوينه.

في هذه الطوبولوجيا المحددة، هناك منفذ واحد (في DC يتوفر على النقل عبر خطوط MPLS فقط، ولكن في السيناريو الحقيقي يمكن أن يكون هناك عمليات نقل متعددة) وموقعان فرعيان لهما اتصال بغطاء SD-WAN عبر خطوط MPLS ونقل الإنترنت. تم تكوين شبكة VPN 10 للخدمة في جميع المواقع. تحتوي الفروع على نفق SIG (الأساسي والنسخ الاحتياطي) تم تكوينه إلى Zscaler. تم تكوين DIA لبعض عناوين IP الوجهة المحددة لتجاوز Zscaler. في حالة فشل إرتباط الإنترنت في الفروع، من المتوقع إرسال حركة مرور البيانات بالكامل إلى DC عبر نقل MPLS.

يتم تكوين eBGP على الخدمة VPN 10 باستخدام موجه Zscaler في نهاية DC. يستقبل موجه DC المسار الافتراضي من موجه Zscaler ويعاد توزيعه في OMP.

ملاحظة: يتم أخذ عناوين IP العامة المذكورة في سيناريو المختبر هذا من الوثائق RFC5737.



المواصفات

- الاستفادة من عناوين IP المتداخلة للفرع 1 والفرع-2 على الشبكة الخاصة الظاهرية (VPN) رقم 10 لجانب الخدمة.

- في سيناريو نموذجي، عند تشغيل خدمة MPLS ونقل الإنترنت، يجب إنهاء حركة المرور من شبكة VPN 10 عبر نفق SIG.
- بالنسبة للبادئات الخاصة لوجهة IP، يجب أن تتجاوز حركة المرور نفق SIG وتخرج عبر DIA.
- في حالة فشل ارتباط الإنترنت، يجب إنهاء حركة مرور جميع/حركة مرور البيانات المرتبطة بالإنترنت من VPN 10 عبر DC.

الحل

ولتحقيق هذا الشرط، يتم إستخدام SD-WAN لميزات NAT و DIA مع سياسة البيانات.

- يتم تكوين NAT الخاص بجانب الخدمة على كل موجه فرعي مع عناوين IP مختلفة لتجمع NAT.
- في حالة فشل ارتباط الإنترنت عند إرسال حركة المرور إلى تغشية SD-WAN، يتم إرسال IP المصدر إلى عنوان IP من تجمع NAT الذي تم تكوينه.
- يرى موجه وحدة التحكم بالمجال (DC) عنوان ما بعد وحدة الشبكة (NAT) للشبكات الفرعية المتداخلة.

ملاحظة: لعرض حركة المرور العادية عبر نفق SIG من VPN 10، يتم إستخدام IP العام 192.0.2.1. يتم إستخدام الإصدار DIA، عبر مضيف محدد، و192.0.2.100. يتم عرض التكوينات المقابلة في قسم التكوين.

التكوين

تكوين Branch-1

تكوين موجه Branch-1 كما يلي.

```
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
!
```

تكوين Branch-2

تكوين موجه Branch-2 وه كما يلي.

```
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
!
```

تكوين موجه DC

تكوين موجه DC هو التالي.

```
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
!
```

سياسة vSmart

إن تكوين نهج vSmart هو كما يلي.

> **ملاحظة:** يرجى ملاحظة أن **nat pool 1** قد تم إستدعاء ذلك في السياسة لكل الفرعين، وهو ذلك، هناك مجموعتان IP تم تخصيصها لكل فرع (172.16.2.0/30 و 1 للفرع 172.16.2.8/30 (2 للفرع).

<#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
!

سيناريوهات تجاوز الفشل

السيناريو العادي لتدفق حركة مرور Branch-1

عندما يكون الملف في مستوى أعلى كما هو موضح في الإخراج، تخرج حركة المرور بشكل افتراضي عبر نفق SIG الأساسي **Tunnel100512**. عند تعطل النفق الرئيسي يتم تبديل حركة المرور إلى نفق النسخ الاحتياطي **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#
```

يوضح Traceroute أن حركة المرور تأخذ نفق SIG.

<#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#

تأخذ حركة المرور إلى وجهة معينة **192.0.2.1** المخرج عبر DIA (NATed إلى عنوان IP لشبكة WAN).

<#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#
```

السيناريو العادي لتدفق حركة مرور البيانات Branch-2

يتم ملاحظة سلوك مماثل على الموجه Branch-2 أيضا.

<#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#
```

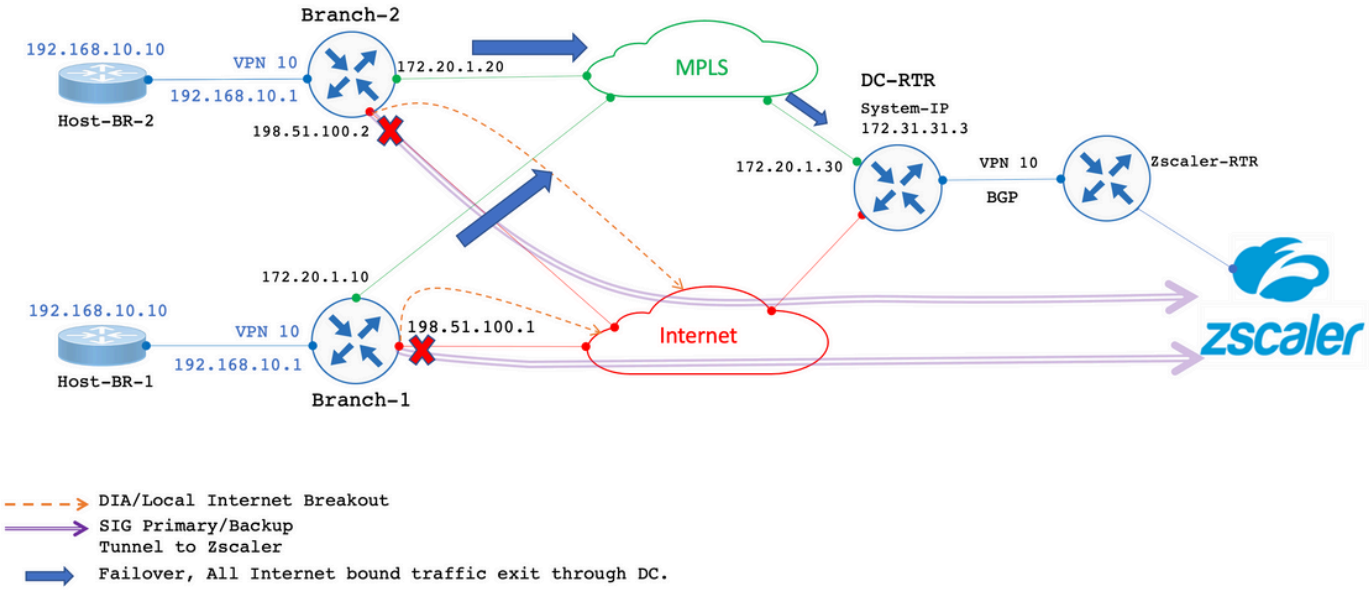
```
Host-BR-2#t

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#
```

سيناريوهات الفشل

سيناريو فشل Branch-1

يصف هذه القسم السلوك أثناء فشل الإنترنت.



تم إيقاف تشغيل ارتباط الإنترنت إداريا لمحاكاة ارتباط فشل إنترنت.

<#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#
```

توضح المخرجات أنه خلال سيناريو فشل ارتباط الإنترنت، يستقبل الموجه Branch-1 المسار الافتراضي من موجه DC عبر OMP. **172.31.31.3** هو نظام-IP لموجه DC.

<#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>
```

حركة المرور الموجهة إلى 192.0.2.100 الحصول على NATed إلى تجمع NAT الخاص بجانب الخدمة وتخرج عبر 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#
```

تظهر نتائج Traceroute حركة مرور أي مسار التي المباشر. 172.20.1.30 هو عنوان IP الخاص بشبكة WAN للنفق الخاصة بـ موجه DC.

<#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#
```

كما تحصل حركة المرور الموجهة إلى IP 192.0.2.1 محدد على NATed إلى تجمع NAT الخاص بجانب الخدمة وتخرج عبر 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>

تم دفع تكوين نهج البيانات من 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

سيناريو فشل Branch-2

كما يتم ملاحظة سلوك مماثل في الموجهات طراز Branch-2 عند حدوث تجاوز فشل في الإنترنت.

<#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

رشابملا راتيا ةوجوم هيجوت قلاح

يلتقط جدول التوجيه من موجه DC.

امك وه موضوم حف يا إلخارج، ،يمكن لموجه DC التمييز بين عناوين IP المدتخلة من الك الفرعين مع **post-NAT IP**اشتقاق **SS-NAT pool** (172.16.2.0 و 172.16.2.8) نم الدب ةكبش LAN ةيلعفلا **192.168.10.0/24172.31.31.1 172.31.31.2** من أ امك ه**system-ip** ت ل هنيوكت Branch-1/Branch-2. يتمت بروتوكول System-IP **172.31.31.10** إلى **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 -
```

التحقق من الصحة

هناك حاليا ما من تدقيق إجراء يتوفر ل هذا تشكيل.

استكشاف الأخطاء وإصلاحها

لا تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات إضافية

سيناريو-1

في السيناريوهات التي تكون فيها وحدات التحكم في الإصدار 20.3.4، ويشغل cEdge الإصدار 17.3.3a أو إصدارات أقل بنفس التكوينات، يلاحظ أنه في السيناريوهات العادية/التي تتجاوز الأخطاء، تحصل حركة مرور البيانات على NATed إلى تجمع NAT الخاص بجانب الخدمة وتكسر التدفق.

مجموعات cEdge:

<#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
```

يتم التقاط الإخراج من تشغيل cEdge على الإصدار 17.3.3a. تحصل حركة المرور الموجهة عبر نفق SIG على NATed إلى بركة SS-NAT ويتم إسقاطها. يتوفر إصلاح من الإصدار 17.3.6 وما بعده.

سيناريو-2

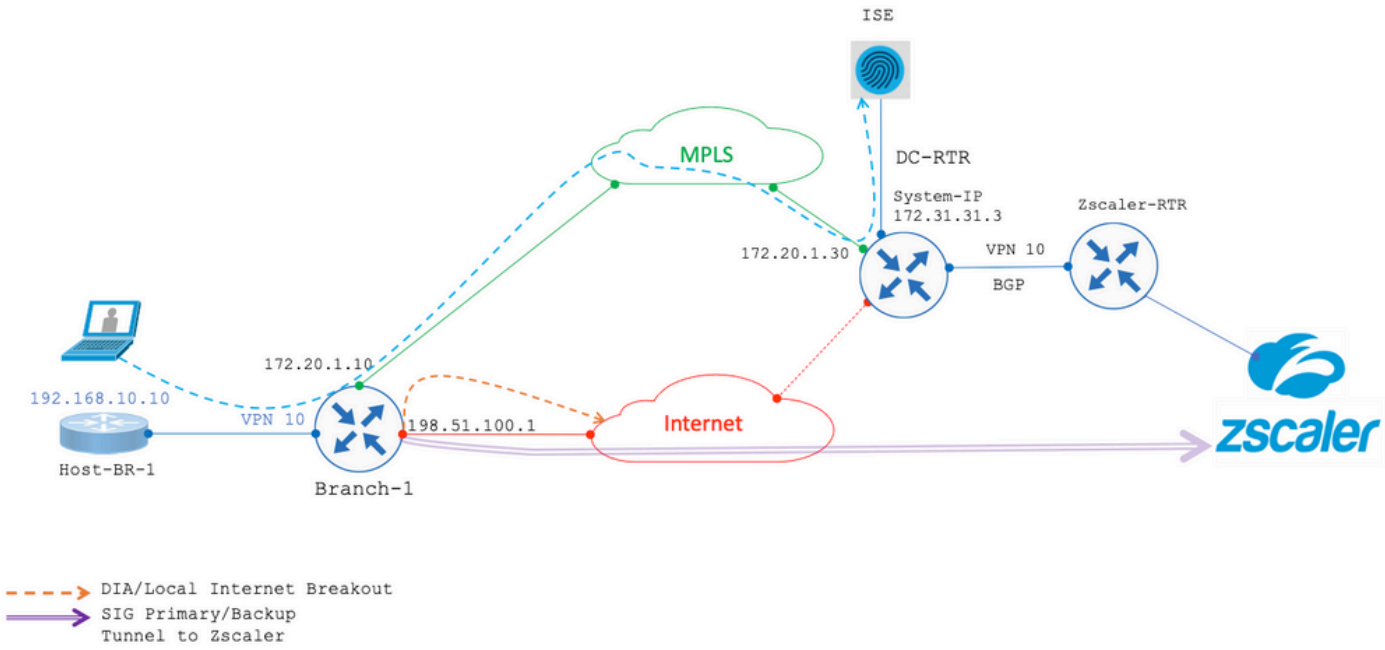
متطلب (NAT من جانب الخدمة (SS-NAT) مع فحص UTD)

لنفترض أن المستخدم طلب هذه المتطلبات:

1. عند تشغيل كل من عمليات النقل عبر الإنترنت وشبكة MPLS، يمكن توجيه العملاء اللاسلكيين في شبكة VPN 10 إلى شبكة ISE في مركز البيانات للمصادقة. وبالإضافة إلى ذلك، يمكن أن تخضع حركة مرور VPN 10 التي تنتقل عبر تغشية SD-WAN للتفتيش. بما أن حركة المرور هذه جزء من التغشية، فإن VPN 10 يستخدم ميزة SS-NAT. [UTD + SS-NAT]

2. إذا أصبح النقل عبر الإنترنت غير متاح، يمكن توجيه جميع حركات المرور من شبكة VPN 10، بما في ذلك حركة المرور اللاسلكية والسلكية، عبر التغشية باستخدام النقل عبر بروتوكول MPLS. يمكن أن تخضع هذه الحركة أيضا للتفتيش. [UTD + SS-NAT]

تهدف هذه المتطلبات إلى ضمان تدفق حركة مرور البيانات الآمن والمرصد لشبكة VPN 10 في Branch-1 في ظروف شبكة مختلفة.



في كل السيناريوهين المذكورين سابقا، يكون لديك UTD فحص بمزيج من SS-NAT. وفيما يلي نموذج تكوين UTD لهذا السيناريو.

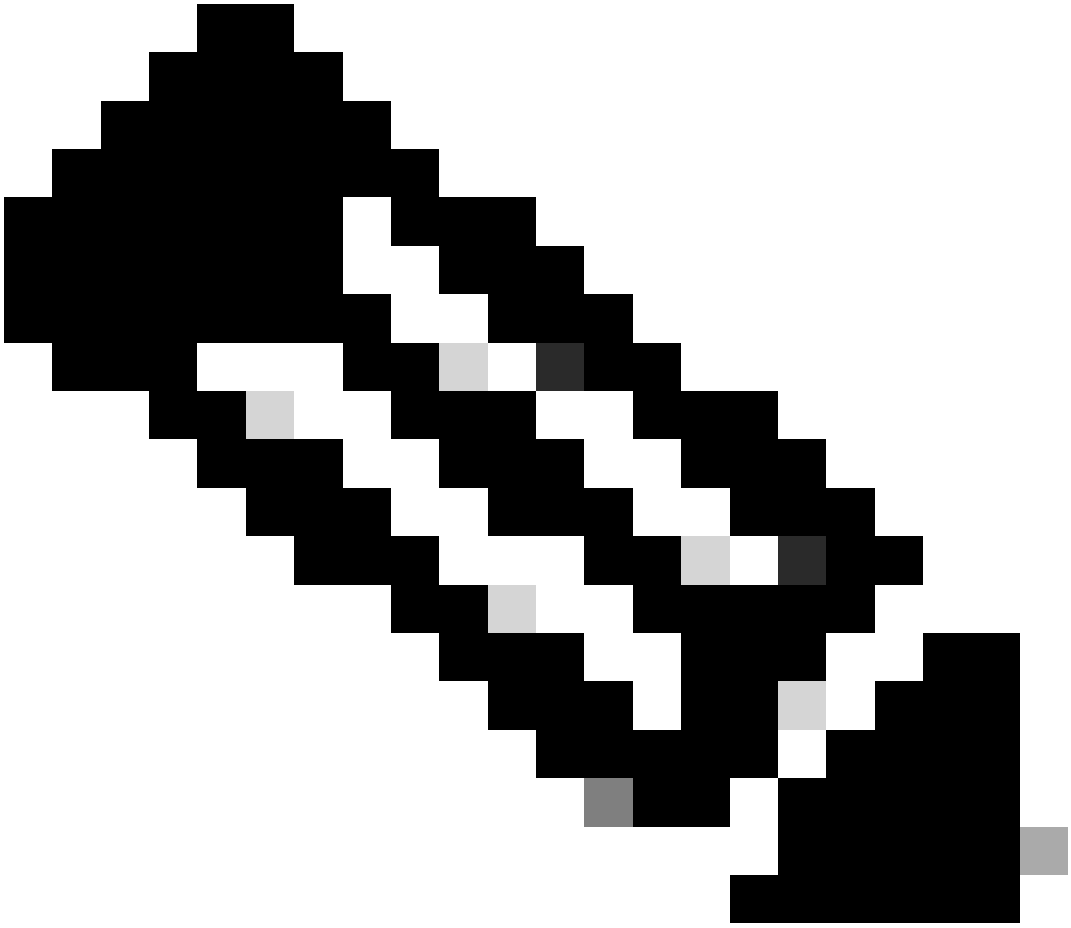
```
policy utd-policy-vrf-10
 all-interfaces
```

```
vrf 10
threat-inspection profile TEST_IDS_Policy
exit
```

تحذير: يرجى ملاحظة أن جمع UTD مع SS-NAT غير مدعوم حاليا. لذلك، لا يعمل هذا المزيج كما هو متوقع. قد يتم تضمين إصلاح لهذه المشكلة في الإصدارات المستقبلية.

الحل

ال workaround أن يعجز ال UTD سياسة على يتداخل ip VPN (في هذه الحالة VPN 10) ويمكن شامل VPN.



ةظحلام: يتم إختبار هذا التكوين والتحقق منه في الإصدار 17.6.

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).