كيف يمكنك إختيار موقع معين ليكون بمثابة الاختراق الإقليمي المفضل للإنترنت؟

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين بنية SD-WAN لتكوين خادم vEdge فرعي معين كحل إقليمي مفضل للتجميع عبر الإنترنت بمساعدة الوصول المباشر إلى الإنترنت (DIA) وسياسة البيانات المركزية. وقد يكون هذا الحل مفيدا في حالة إستخدام موقع إقليمي، على سبيل المثال، لخدمة مركزية مثل Zscaler® ويُنبغي إستخدامه كنقطة خروج مفضلة من الإنترنت. يتطلب هذا النشر تضمين التوجيه العام (GRE) أو أنفاق أمان بروتوكول الإنترنت (IPSec) التي يتم تكوينها من شبكة VPN للنقل وتدفق البيانات بشكل مختلف عن حل DIA العادي، حيث تصل حركة المرور إلى الإنترنت مباشرة.

المتطلبات الأساسية

المتطلبات

يوصي cisco أن يتلقى أنت معرفة من هذا موضوع:

- المفهوم الأساسي لإطار سياسات شبكة SD-WAN.

المكونات المستخدمة

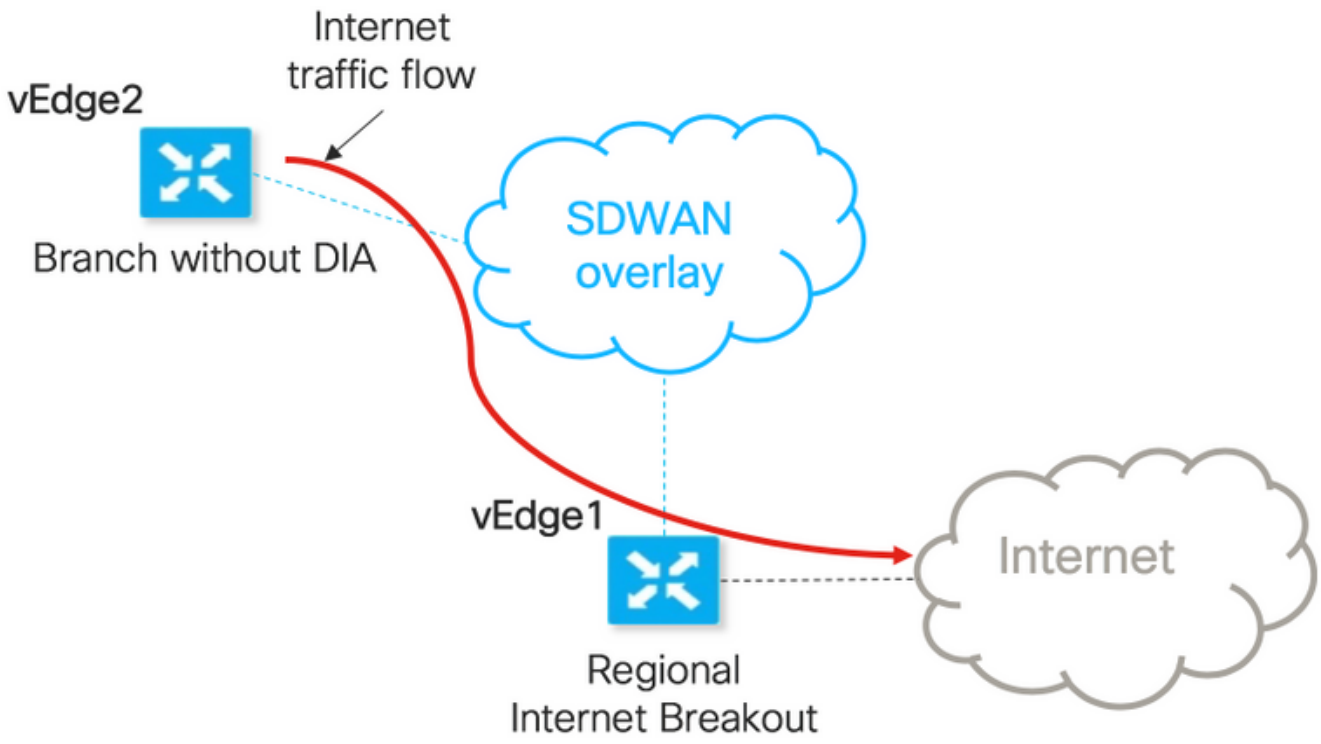
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- موجهات vEdge
- وحدة التحكم vSmart مع إصدار برنامج 18.3.5.

معلومات أساسية

تتم إعادة توجيه حركة مرور VPN للخدمة من vEdge2، التي يجب أن تصل إلى الإنترنت، إلى فرع آخر vEdge1، باستخدام أنفاق مستوى البيانات. vEdge1 هو الموجه حيث تم تكوين DIA لظهور الإنترنت المحلي.

الرسم التخطيطي للشبكة



اسم المضيف	vEdge1	vEdge2
دور المضيف	جهاز فرعي مزود ب DIA (اتصال إنترنت إقليمي)	جهاز فرعي لم يتم تكوين DIA عليه
VPN 0		
مواقع النقل (TLOC) 1	biz-internet، ip: 192.168.110.6/24	biz-internet، ip: 192.168.110.5/24
مواقع النقل (TLOC) 2	الإنترنت العام، بروتوكول الإنترنت: 192.168.109.4/24	الإنترنت العام، بروتوكول الإنترنت: 192.168.109.5/24
Service VPN 40	الواجهة ge0/1، ip: 192.168.40.4/24	الواجهة ge0/2، ip: 192.168.50.5/2

التكوينات

الحل 1: إستخدام نهج البيانات المركزي لتغيير الخطوة التالية.

يحتوي الطراز vEdge2 على نفق مستوى بيانات تم إنشاؤه باستخدام الطراز vEdge1 ومواقع أخرى (اتصال نمط الشبكة الكاملة)

يحتوي vEdge1 على DIA التي تم تكوينها باستخدام **IP route 0.0.0.0/0 VPN 0**.

تكوين سياسة البيانات المركزية vSmart:

```
policy
 data-policy DIA_vE1
  vpn-list VPN_40
   sequence 5
    match
     destination-data-prefix-list ENTERPRISE_IPs
    !
    action accept
    !
   !
   sequence 10
    action accept
     set
      next-hop 192.168.40.4
     !
    !
   !
   default-action accept
  !
 !
!
lists
  vpn-list VPN_40
   vpn 40
  !
  data-prefix-list ENTERPRISE_IPs
   ip-prefix 10.0.0.0/8
   ip-prefix 172.16.0.0/12    ip-prefix 192.168.0.0/16 ! apply-policy site-list SITE2 data-
policy DIA_vE1 from-service
```

vEdge2 - ال يتطلب أي تكوين خاص.

هناك العديد من الخطوات التي يمكنك اتباعها للتحقق من أن النهج قد تم تطبيقه بشكل صحيح.

1. تأكد من عدم وجود هذه السياسة من الخادم vEdge2:

```
vedge2# show policy from-vsmart
% No entries found.
```

2. تحقق من برمجة قاعدة معلومات إعادة التوجيه. لا يزال المسار الافتراضي (بالكامل) للوجهة على الإنترنت:

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Blackhole
```

3. تطبيق سياسة بيانات vSmart من قسم **apply-policy** في تكوين vSmart أو التنشيط في واجهة المستخدم الرسومية (GUI) vManage.

4. تأكد من أن vEdge2 قد تلقى سياسة بيانات بنجاح من vSmart:

```
vedge2# show policy from-vsmart
from-vsmart data-policy DIA_vE1
 direction from-service
 vpn-list VPN_40
  sequence 5
   match
    destination-data-prefix-list ENTERPRISE_IPs
   action accept
```

```
  sequence 10
   action accept
    set
     next-hop 192.168.40.4
  default-action accept
from-vsmart lists vpn-list VPN_40
 vpn 40
from-vsmart lists data-prefix-list ENTERPRISE_IPs
 ip-prefix 10.0.0.0/8
 ip-prefix 172.16.0.0/12
 ip-prefix 192.168.0.0/16
```

5. التحقق من برمجة قاعدة معلومات إعادة التوجيه (FIB)، التي تظهر المسارات المحتملة للوجهة على الإنترنت:

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 4
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.110.6 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.110.6 12346 Color: public-internet
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.109.4 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.109.4 12346 Color: public-internet
```

6. تأكيد إمكانية الوصول إلى الوجهة على الإنترنت:

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.392 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.346 ms
^C
--- 173.37.145.84 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.345/0.361/0.392/0.021 ms
```

هنا يمكنك العثور على خطوات تكوين vEdge1.

1. تنشيط ترجمة عنوان الشبكة (NAT) على واجهة النقل، حيث يجب إستخدام DIA:

```
vpn 0
 !
 interface ge0/0
  description "DIA interface"
  ip address 192.168.109.4/24
 nat <<<<==== NAT activated for a local DIA !
```

2. أضف المسار الثابت **ip route 0.0.0.0/0 VPN 0** في شبكة VPN خدمة لتنشيط DIA:

```
vpn 40
 interface ge0/4
  ip address 192.168.40.4/24
  no shutdown
 !
 ip route 0.0.0.0/0 vpn 0     <<<<==== Static route for DIA !
```

3. تحقق مما إذا كان RIB يحتوي على مسار NAT:

```
vedge1# show ip route vpn 40 | include nat
40 0.0.0.0/0 nat - ge0/0 - 0 - - - F,S
```

4. تأكد من أن DIA يعمل ويمكننا رؤية جلسة بروتوكول رسائل التحكم في الإنترنت (ICMP) إلى 173.37.145.84 من vEdge2 في ترجمات NAT

```
vedge1# show ip nat filter | tab

                            PRIVATE                              PRIVATE  PRIVATE
PUBLIC  PUBLIC
NAT  NAT                    SOURCE         PRIVATE DEST   SOURCE   DEST     PUBLIC SOURCE
PUBLIC DEST    SOURCE  DEST    FILTER       IDLE        OUTBOUND  OUTBOUND   INBOUND  INBOUND
VPN  IFNAME  VPN  PROTOCOL  ADDRESS        ADDRESS        PORT     PORT     ADDRESS
ADDRESS        PORT    PORT    STATE        TIMEOUT     PACKETS   OCTETS     PACKETS  OCTETS
DIRECTION
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
------
0 ge0/0 40 icmp 192.168.50.5 173.37.145.84 9269 9269 192.168.109.4 173.37.145.84 9269 9269
established 0:00:00:02 10 840 10 980 -
```

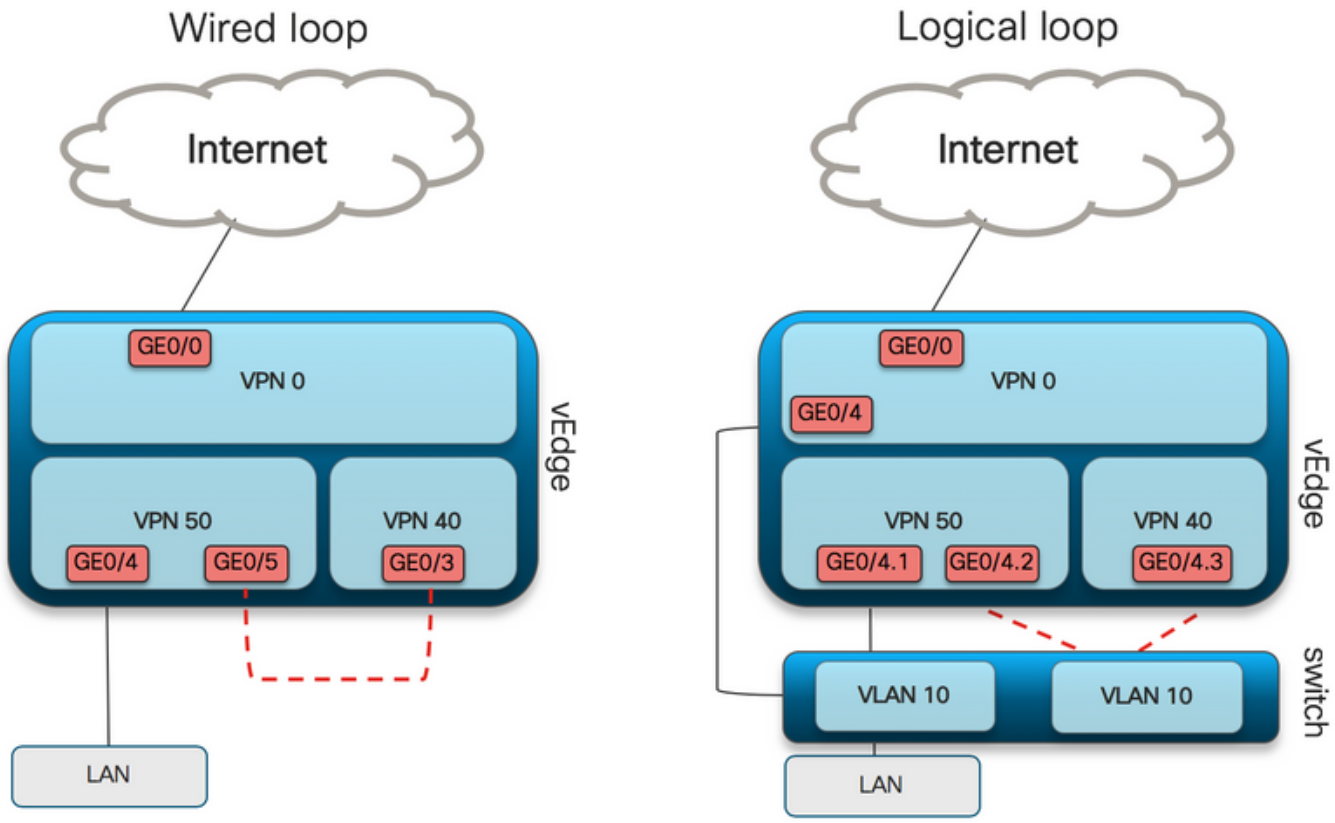
ملاحظة: لا يتيح لنا هذا الحل تنظيم التكرار أو مشاركة الأحمال باستخدام منافذ إقليمية مختلفة.
لا يعمل مع موجهات IOS-XE

الحل 2: إدخال المسار الافتراضي إلى OMP بالطول GRE\IPSec\NAT.

حتى الآن، لا توجد إمكانية للحصول على المسار الافتراضي، مع الإشارة إلى نفق GRE\IPSec على vEdge1، للإعلان عنه من خلال OMP إلى vEdge2 (إعادة توزيع المسار عبر بروتوكول OMP). الرجاء ملاحظة أن السلوك قد يتغير في إصدارات البرامج المستقبلية.

يمكن (ip route 0.0.0.0/0 <next-hop ip addr>) منظم ثابت افتراضي مسار إنشاء هو هدفنا إنشاؤه بواسطة vEdge2 (الجهاز المفضل ل DIA) وزيادة نشره عبر OMP.

للتحقيق ذلك، يتم إنشاء شبكة VPN وهمية على vEdge1 ويتم إجراء حلقة منفذ بطبيعي برمجوا VPN ال في ميناء وهمي إلى يعين ميناء بين نشطوة حلقة أنشطة. بالكل استخدام طوق مع نشطوة حلقة خطية يستطيع أنت، أيضا. ممر تقصير تكيكيات استاس بلطتي أي إلى يعين فرعي قران اثنان إلى يمكن أن تكون ربط إلى المفتاح مع VLAN وهمي و قران بطبيعي واحد VPNs على لثامي الصورة أدناه:



هنا يمكنك العثور على مثال تكوين vEdge1.

1. إنشاء شبكة VPN وهمية:

```
vpn 50
 interface ge0/3
description DIA_for_region ip address 192.168.111.2/30 no shutdown ! ip route 0.0.0.0/0 vpn 0
<<<<==== NAT activated for a local DIA
 ip route 10.0.0.0/8 192.168.111.1 <<<<==== Reverse routes, pointing to loop interface GE0/3
ip route 172.16.0.0/12 192.168.111.1
ip route 192.168.0.0/16 192.168.111.1 !
```

2. تحقق من FIB أن توجيه DIA، مشيرا إلى واجهة NAT، تمت إضافته بنجاح إلى جدول التوجيه:

```
vedge1# show ip route vpn 50 | i nat
50     0.0.0.0/0 nat - ge0/0 - 0 - - - F,S
```

3. شبكة VPN للخدمة المستخدمة لأغراض الإنتاج، حيث يتم تكوين المسار الافتراضي العادي (والذي سيكون OMP قادرا على الإعلان عنه):

```
vpn 40
 interface ge0/4
  description CORPORATE_LAN
  ip address 192.168.40.4/24
  no shutdown
 !
 interface ge0/5
description LOOP_for_DIA ip address 192.168.111.1/30 no shutdown ! ip route 0.0.0.0/0
192.168.111.2 <<<<==== Default route, pointing to loop interface GE0/5 omp advertise connected
advertise static ! !
```

4. تحقق من RIB بحثا عن وجود المسار الافتراضي الذي يشير إلى واجهة التكرار:

```
vedge1# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 static - ge0/5 192.168.111.2 - - - - F,S
```

5. تحقق من أن الإصدار vEdge1 المعلن عن المسار الافتراضي عبر بروتوكول OMP:

```
vedge1# show omp routes detail | exclude not\ set

-------------------------------------------------
omp route entries for vpn 40 route 0.0.0.0/0 <<<<==== Default route OMP entry ------------------
-------------------------------- RECEIVED FROM: peer 0.0.0.0 <<<<==== OMP route is locally
originated path-id 37 label 1002 status C,Red,R Attributes: originator 192.168.30.4 type
installed tloc 192.168.30.4, public-internet, ipsec overlay-id 1 site-id 13 origin-proto static
origin-metric 0 ADVERTISED TO: peer 192.168.30.3 Attributes: originator 192.168.30.4 label 1002
path-id 37 tloc 192.168.30.4, public-internet, ipsec site-id 13 overlay-id 1 origin-proto static
origin-metric 0
```

6. تحقق من أن جهاز الطرف vEdge2 تلقى المسار الافتراضي عبر بروتوكول OMP، والذي يشير إلى vEdge1

```
vedge2# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 omp - - - - 192.168.30.4 public-internet ipsec F,S
```

7. تأكد من إمكانية الوصول إلى 173.37.145.84:

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=2 ttl=62 time=0.518 ms
64 bytes from 173.37.145.84: icmp_seq=5 ttl=62 time=0.604 ms
^C
--- 192.168.109.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.518/0.563/0.604/0.032 ms
```

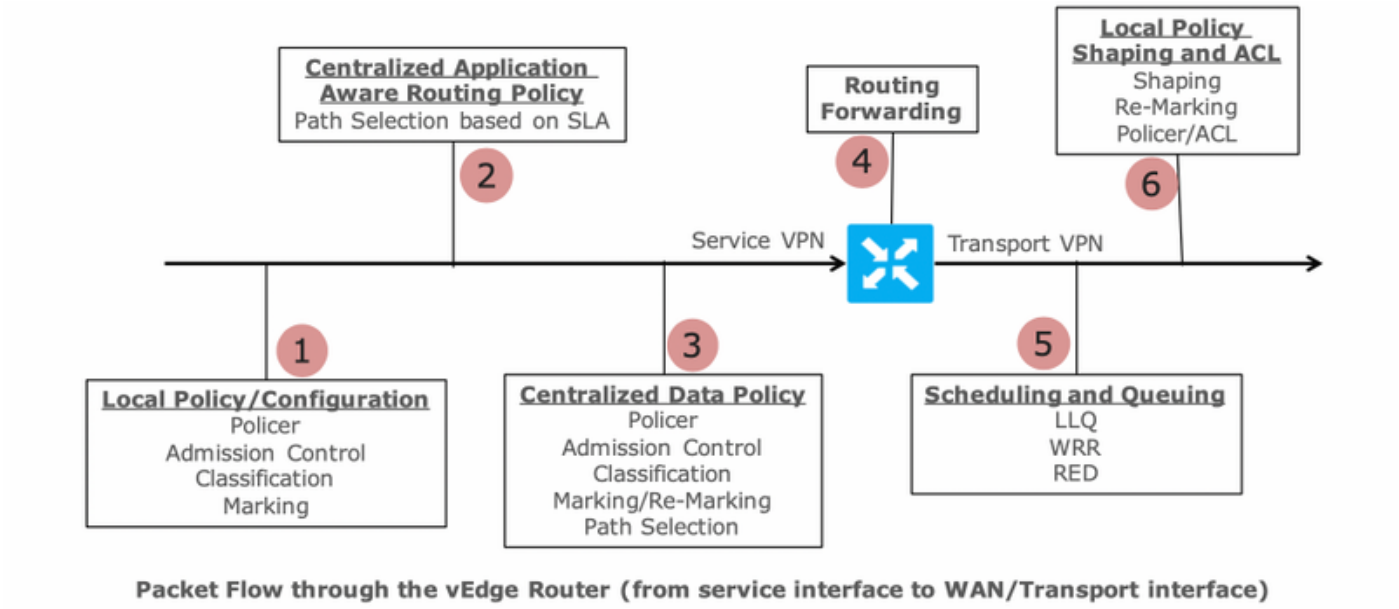
ملاحظة: يتيح لك هذا الحل تنظيم التكرار وأ مشاركة الأحمال باستخدام مخارج إقليمية مختلفة.

الـ يعمل مع موجهات IOS-XE

الحل 3: تضمين المسار الافتراضي إلى بروتوكول إدارة الأنظمة المفتوحة (OMP) عند إستخدام نهج بيانات مركزي لـ DIA.

عند إستخدام سياسة البيانات المركزية لـ DIA المحلية، وهي الطريقة الممكنة لضخ المسار الافتراضي، فإنها تشير إلى جهاز إقليمي مع DIA وهو إستخدام هذا المسار الافتراضي الثابت: **ip route 0.0.0.0/0 null0**.

نظرا لتدفق الحزمة الداخلي، تصل حركة المرور التي تصل من الفروع إلى DIA بفضل سياسة البيانات، والا تصل مطلقا إلى المسار إلى Null0. كما ترى هنا، فإن البحث عن الخطوة التالية يحدث فقط بعد نشر النهج.



Packet Flow through the vEdge Router (from service interface to WAN/Transport interface)

يحتوي الطراز vEdge2 على نفق مستوى بيانات تم إنشاؤه باستخدام الطراز vEdge1 ومواقع أخرى (اتصال نمط الشبكة الكاملة). لا يتطلب أي تكوين خاص.

يتميز الطراز vEdge1 بتهيئة DIA مع سياسة بيانات مركزية.

هنا يمكنك العثور على خطوات تكوين vEdge1.

1. تنشيط ترجمة عنوان الشبكة (NAT) على واجهة النقل، حيث يجب إستخدام DIA:

```
vpn 0
 !
 interface ge0/0
  description "DIA interface"
  ip address 192.168.109.4/24
 nat <<<<==== NAT activated for a local DIA !
```

2. أضف المسار الثابت **ip route 0.0.0.0/0 null0** في شبكة VPN للخدمة للإعلان عن الإعداد الافتراضي للفرع:

```
vpn 40
 interface ge0/4
  ip address 192.168.40.4/24
  no shutdown
 !
 ip route 0.0.0.0/0 null0     <<<<==== Static route to null0 that will be advertised to branches
via OMP !
```

3. تحقق مما إذا كان RIB يحتوي على المسار الافتراضي:

```
vedge1# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 static - - - 0 - - - B,F,S
```

4. تحقق من أن الإصدار vEdge1 المعلن عن المسار الافتراضي عبر بروتوكول OMP:

```
vedge1# show omp routes detail | exclude not\ set

----------------------------------------------------
```

```
omp route entries for vpn 40 route 0.0.0.0/0 <<<<==== Default route OMP entry ------------------
-------------------------------- RECEIVED FROM: peer 0.0.0.0 <<<<==== OMP route is locally
originated path-id 37 label 1002 status C,Red,R Attributes: originator 192.168.30.4 type
installed tloc 192.168.30.4, public-internet, ipsec overlay-id 1 site-id 13 origin-proto static
origin-metric 0 ADVERTISED TO: peer 192.168.30.3 Attributes: originator 192.168.30.4 label 1002
path-id 37 tloc 192.168.30.4, public-internet, ipsec site-id 13 overlay-id 1 origin-proto static
origin-metric 0
```

5. تأكد من عدم وجود هذه السياسة على vEdge1 ومن عدم تمكين DIA:

```
vedge1# show policy from-vsmart
% No entries found.
```

6. التحقق من برمجة قاعدة معلومات إعادة التوجيه. يجب أن تظهر عدم وجود مسار (BlackHole) للوجهة على الإنترنت حيث أن DIA غير ممكنة:

```
vedge1# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.40.4 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Blackhole
```

تهيئة سياسة البيانات المركزية vSmart ل DIA:

```
policy
 data-policy DIA_vE1
  vpn-list VPN_40
   sequence 5
    match
     destination-data-prefix-list ENTERPRISE_IPs
    action accept
   sequence 10
    action accept
     nat-use vpn0             <<<<==== NAT reference for a DIA default-action accept lists
vpn-list VPN_40    vpn 40   data-prefix-list ENTERPRISE_IPs    ip-prefix 10.0.0.0/8    ip-prefix
172.16.0.0/12    ip-prefix 192.168.0.0/16
site-list SITE1
site-id 1001 apply-policy site-list SITE1 <<<<==== policy applied to vEdge1 data-policy DIA_vE1
from-service
```

تطبيق سياسة بيانات vSmart ضمن قسم **apply-policy** لتكوين vSmart أو التنشيط في واجهة المستخدم الرسومية (GUI) vManage.

7. تأكد من أن vEdge1 قد تلقى سياسة بيانات بنجاح من vSmart:

```
vedge1# show policy from-vsmart
from-vsmart data-policy DIA_vE1
 direction from-service
 vpn-list VPN_40
  sequence 5
   match
    destination-data-prefix-list ENTERPRISE_IPs
   action accept
  sequence 10
   action accept
nat-use vpn0 default-action accept from-vsmart lists vpn-list VPN_40 vpn 40 from-vsmart lists
data-prefix-list ENTERPRISE_IPs ip-prefix 10.0.0.0/8 ip-prefix 172.16.0.0/12    ip-prefix
192.168.0.0/16
```

8. راجع برمجة قاعدة معلومات إعادة التوجيه (FIB) التي توضح المسارات المحتملة للوجهة على الإنترنت:

```
vedge1# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.40.4 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Remote
Remote IP:173.37.145.84, Interface ge0/0 Index: 4
```

9. تأكيد إمكانية الوصول إلى الوجهة على الإنترنت:

```
vedge1# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.192 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.246 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.236 ms ^C --- 173.37.145.84 ping
statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2000ms rtt
min/avg/max/mdev = 0.245/0.221/0.192/0.021 ms
```

خطوات التحقق من الخادم vEdge2:

1. تأكد من تلقي المسار الافتراضي وتثبيته بنجاح في RIB:

```
vEdge2# sh ip route vpn 40 | include 0.0.0.0
40     0.0.0.0/0           omp              -         -           -                -
192.168.30.4   biz-internet     ipsec  F,S
40 0.0.0.0/0 omp - - - - 192.168.30.4 public-internet ipsec F,S
```

2. التحقق من برمجة قاعدة معلومات إعادة التوجيه (FIB)، التي تظهر المسارات المحتملة للوجهة على الإنترنت:

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 4
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.110.6 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.110.6 12346 Color: public-internet
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.109.4 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.109.4 12346 Color: public-internet
```

3. تأكيد إمكانية الوصول إلى الوجهة على الإنترنت:

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.382 ms
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.392 ms 64 bytes from 173.37.145.84:
icmp_seq=3 ttl=63 time=0.346 ms ^C --- 173.37.145.84 ping statistics --- 3 packets transmitted,
3 received, 0% packet loss, time 2000ms rtt min/avg/max/mdev = 0.392/0.361/0.346/0.023 ms
```

4. تأكد من أن DIA يعمل ويمكنه توجيه جلسة بروتوكول رسائل التحكم في الإنترنت (ICMP) تمت ترجمة NAT في vEdge2 من 173.37.145.84 إلى

```
vedge1# show ip nat filter | tab

                              PRIVATE                       PRIVATE  PRIVATE
PUBLIC  PUBLIC
```

```
NAT  NAT                    SOURCE          PRIVATE DEST   SOURCE   DEST     PUBLIC SOURCE
PUBLIC DEST    SOURCE  DEST    FILTER        IDLE         OUTBOUND  OUTBOUND   INBOUND  INBOUND
VPN  IFNAME  VPN  PROTOCOL  ADDRESS         ADDRESS        PORT     PORT     ADDRESS
ADDRESS        PORT    PORT    STATE         TIMEOUT      PACKETS   OCTETS     PACKETS  OCTETS
DIRECTION
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
------
0 ge0/0 40 icmp 192.168.50.5 173.37.145.84 9175 9175 192.168.109.4 173.37.145.84 9175 9175
established 0:00:00:04 18 1440 18 1580 -
```

ملاحظة: يتيح هذا الحل تنظيم التكرار أو مشاركة الأحمال باستخدام منافذ إقليمية مختلفة.

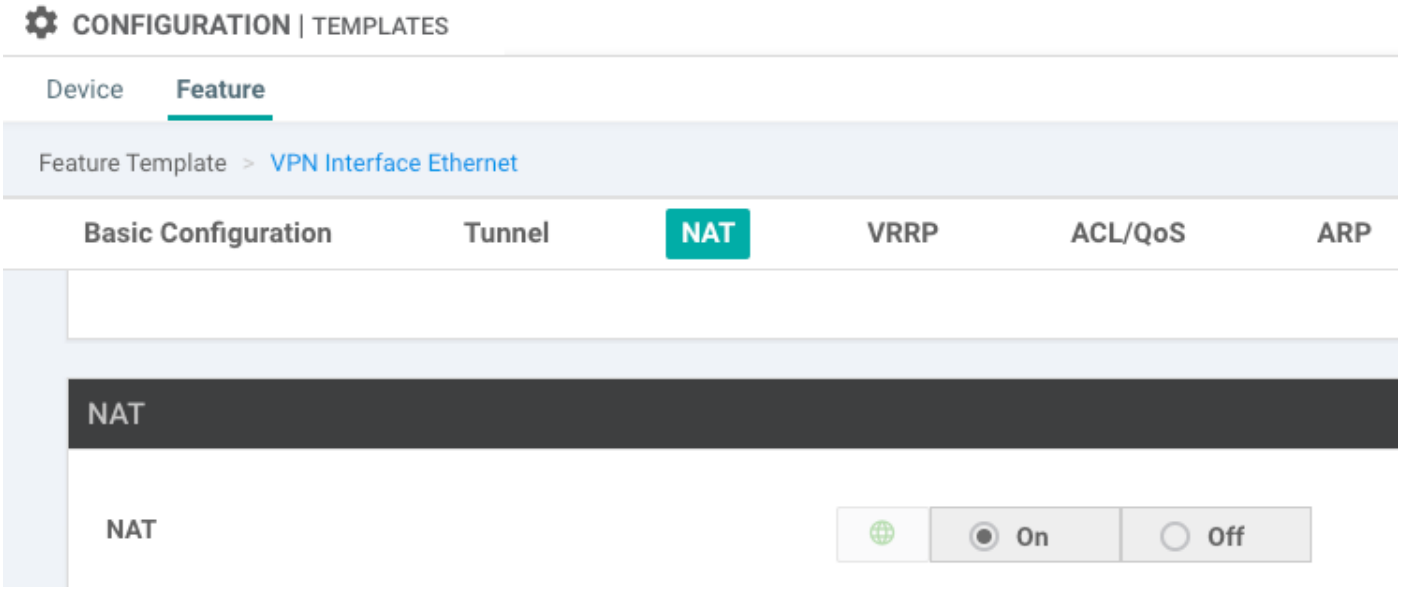
لا يعمل مع موجهات IOS-XE

الحل 4: إدخال المسار الافتراضي إلى OMP عند استخدام DIA المحلي.

يمكن استخدام هذا الحل لكل من موجهات IOS-XE و Viptela OS-WAN المستندة إلى SD.

باختصار، في هذا الحل، يتم تقسيم مسار افتراضي لـ DIA (0.0.0.0/0 Null0) إلى شبكتين فرعيتين 0.0.0.0/1 و 128.0.0.0/1 يشيران إلى Null0. ويتم القيام بهذه الخطوة لتجنب تداخل مسار افتراضي يجب الإعلان عنه للفروع والموجه الافتراضي، والذي يتم إستخدامه لـ DIA المحلي. في مسارات IOS-XE المستخدمة لبروتوكول DIA لها مسافة إدارية (AD) تساوي 6، في حين أن AD الخاص بالإعداد الافتراضي الثابت هو 1. تتمثل فائدة الحل في القدرة على إستخدام مخطط التكرار عند تكوين DIA الإقليمية في موقعين مختلفين.

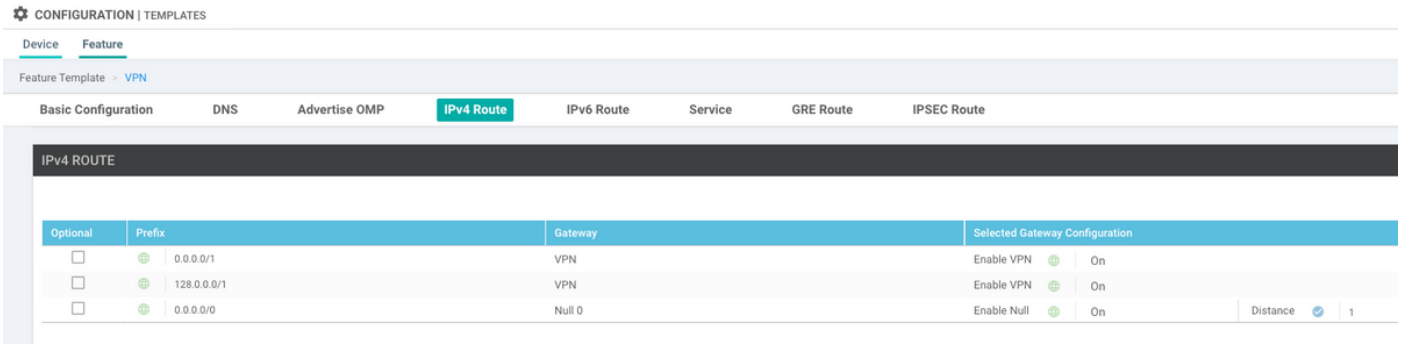
1. تنشيط NAT على واجهة نقل



2. في قالب ميزة لشبكة VPN للخدمة، حيث يجب إستخدام DIA، أضف مسارات IPv4 الثابتة التالية:

- 0.0.0.0/1 و 128.0.0.0/1 يشير إلى VPN. تستخدم هذه المسارات لـ DIA

- 0.0.0.0/0 يشير إلى قيمة خالية 0. يستخدم هذا المسار للإعلان عن طريق بروتوكول إدارة الأنظمة المفتوحة (OMP) إلى الفروع (مشابه لما هو الحال في الحل 3)



3. تأكد من إضافة المسارات بنجاح إلى RIB :

```
cedge1#show ip route vrf 40

Routing Table: 40
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP,  D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type
1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA, i - IS-IS, su - IS-IS summary,
L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route, o - ODR, P -
periodic downloaded static route, H - NHRP, l - LISP
       a - application route, + - replicated route, % - next hop override, p - overrides from
PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Null0                    <<<<==== Static route to null0
that will be advertised to branches via OMP n Nd 0.0.0.0/1 [6/0], 00:08:23, Null0 <<<<==== DIA
route n Nd 128.0.0.0/1 [6/0], 00:08:23, Null0 <<<<==== DIA route 192.40.1.0/32 is subnetted, 1
subnets m 192.40.1.1 [251/0] via 192.168.30.207, 3d01h 192.40.2.0/32 is subnetted, 1 subnets m
192.40.2.1 [251/0] via 192.168.30.208, 3d01h
```

4. تأكد من أن DIA تعمل بشكل جيد محليا:

```
cedge1#ping vrf 40 173.37.145.84
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.84, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

5. تحقق من ذلك المسار الافتراضي الذي تم الإعلان عنه بنجاح إلى أحد الفروع وتثبيته في RIB

```
cedge3#show ip route vrf 40

Routing Table: 40
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP
external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type
1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA, i - IS-IS, su - IS-IS summary,
L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route, o - ODR, P -
periodic downloaded static route, H - NHRP, l - LISP
       a - application route, + - replicated route, % - next hop override, p - overrides from
PfR
```

```
Gateway of last resort is 192.168.30.204 to network 0.0.0.0

m*    0.0.0.0/0 [251/0] via 192.168.30.204, 00:02:45    <<<<==== Default route that advertised
via OMP 192.40.1.0/32 is subnetted, 1 subnets m 192.40.11.1 [251/0] via 192.168.30.204, 00:02:45
192.40.13.0/32 is subnetted, 1 subnets C 192.40.13.1 is directly connected, Loopback40
```

6. تأكد من أن DIA تعمل بشكل جيد محليا:

```
cedge3#ping vrf 40 173.37.145.84
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.84, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

7. تحقق من نجاح ترجمة NAT لموجه DIA الإلكتروني.

```
cedge1#show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
icmp 192.168.109.204:1     192.40.13.1:1         173.37.145.84:1       173.37.145.84:1
Total number of translations: 1
```

ملاحظة: يتيح هذا الحل تنظيم التكرار أو مشاركة الأحمال باستخدام منافذ إقليمية مختلفة.

ملاحظة: CSCvr72329 - طلب تحسين "إعادة توزيع مسار NAT إلى OMP"

معلومات ذات صلة

- سياسة البيانات المركزية
- تكوين سياسة بيانات مركزية
- أمثلة تكوين سياسة البيانات المركزية
- بروتوكول توجيه OMP
- تكوين OMP

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).