مثال تكوين FlexVPN HA Dual Hub

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين تصميم تكرار كامل للمكاتب البعيدة التي تتصل بمركز بيانات عبر شبكة VPN المستندة إلى IPSec عبر وسيط شبكة غير آمن، مثل الإنترنت.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مكونات التقنية التالية:

- بروتوكول العبارة الحدودية (BGP) كبروتوكول توجيه داخل مركز البيانات وبين الخوادم والمراكز في تغشية شبكة VPN.

- اكتشاف إعادة التوجيه ثنائي الاتجاه (BFD) آلية توقوم باكتشاف الارتباطات أسفل (الموجه للأسفل) التي تعمل داخل مركز البيانات فقط (وليس عبر الأنفاق المتداخلة).

- برنامج Cisco IOS® FlexVPN بين لوحات التوزيع والأقسام الفرعية، مع تمكين إمكانات التحدث عبر توحيل قصير المدى.

- تضمين التوجيه العام (GRE) النفقي بين محوري لتمكين الاتصال عبر المحاذية، حتى عندما تكون المحددات متصلة بمراكز مختلفة.

- تعقب الكائن المحسن والمسارات الثابتة المرتبطة بالكائنات المتعقبة.

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

عندما تقوم بتصميم حلول الوصول عن بعد لمركز البيانات، غالبا ما يكون التوافر العالي (HA) أحد المتطلبات الأساسية لتطبيقات المستخدم الحيوية للمهام.

يتيح الحل الوارد في هذا المستند إمكانية الاكتشاف السريع والاسترداد من سيناريوهات الأعطال التي يتم فيها تعطل أحد مراكز إنهاء شبكات VPN بسبب مشاكل في إعادة التحميل أو التزقية أو الطاقة. تستخدم جميع موجهات المكاتب البعيدة (الفرعية) بعد ذلك مركز التشغيل الآخر مباشرة عند اكتشاف مثل هذا الفشل.

فيما يلي ميزات هذا التصميم:

- إسترداد الشبكة بسرعة فائقة من سيناريو دعم شبكة VPN

- لا توجد عمليات مزامنة إعلان حالة معقدة (مثل اقترانات أمان IPSec (SAs)، واقتران أمان الإنترنت، وشبكات الأمان لبروتوكول إدارة المفاتيح (ISAKMP)، وتوجيه التشفير) بين مراكز شبكات VPN

- لا توجد مشاكل متعلقة بعدم إعادة التشغيل بسبب التأخير في مزامنة رقم تسلسل حمولة أمان التضمين (ESP) مع HA في حالة IPSec

- يمكن أن تستخدم لوحات التوزيع الخاصة بالشبكة الخاصة الظاهرية (VPN) أجهزة برامج مختلفة تستند إلى Cisco IOS/IOS-XE

- خيارات تنفيذ موازنة الأحمال المرنة مع BGP كبروتوكول التوجيه الذي يتم تشغيله في تغشية الشبكة الخاصة الظاهرية (VPN)

- توجيه واضح ويمكن قراءته على جميع الأجهزة التي لا تحتوي على آليات مخفية تعمل في الخلفية

- إمكانية الاتصال المباشر عبر الهاتف

- جميع ميزات FlexVPN، لتضمين كامل المصادقة والتفويض والمحاسبة (AAA) ووجودة الخدمة لكل نفق (QoS)

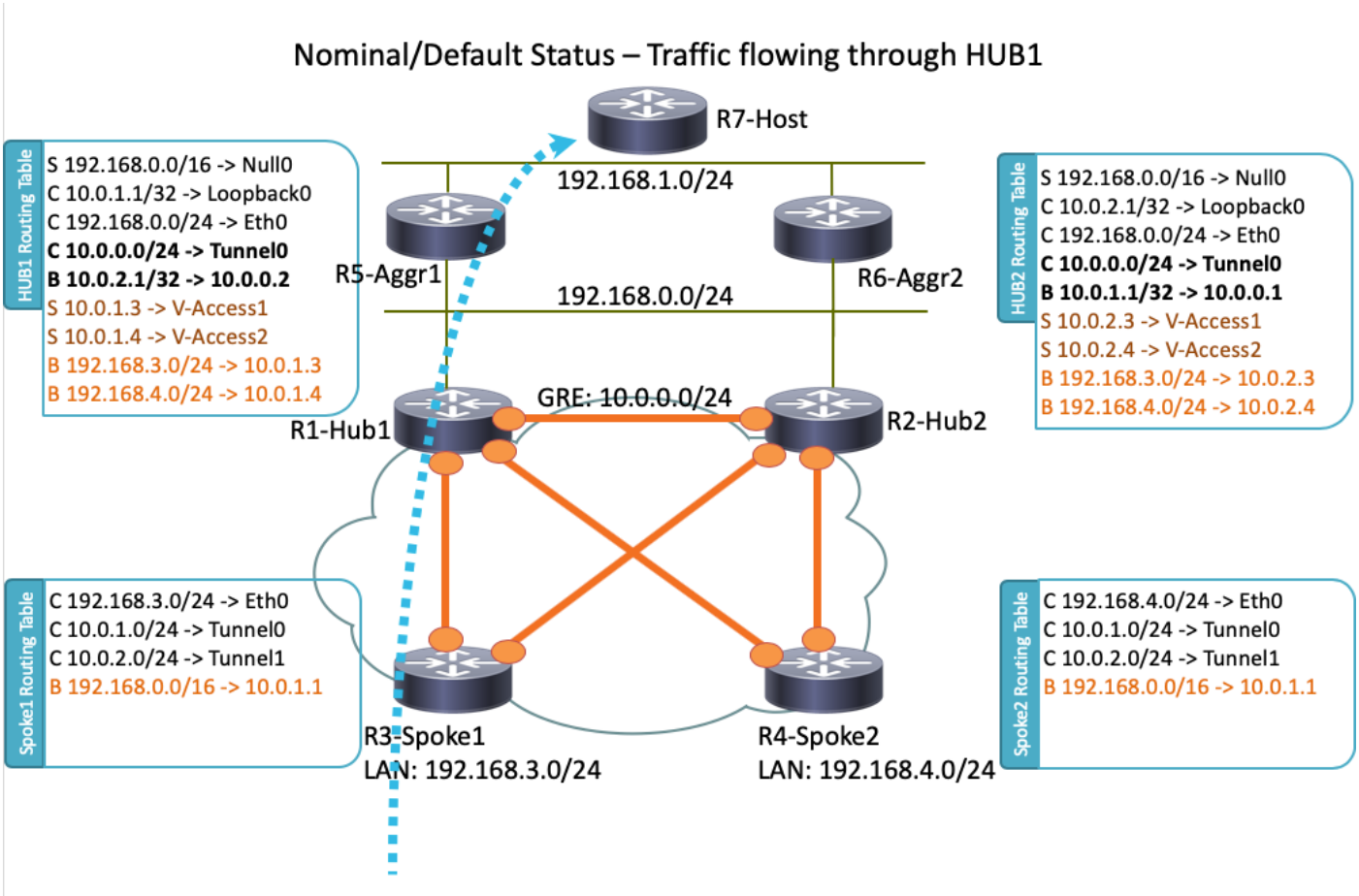
التكوين

يقدم هذا القسم أمثلة سيناريوهات ويصف كيفية تكوين تصميم تكرار كامل للمكاتب البعيدة التي تتصل بمركز البيانات من خلال الشبكة الخاصة الظاهرية (VPN) القائمة على بروتوكول IPSec عبر وسط شبكة غير آمن.

> **ملاحظة**: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

هذا هو مخطط الشبكة المستخدم في هذا المستند:



> **ملاحظة**: تقوم جميع الموجهات التي يتم إستخدامها في هذا المخطط بتشغيل الإصدار 15.2(4)M1 من Cisco IOS، وتستخدم سحابة الإنترنت نظام عنونة 172.16.0.0/24.

سيناريو العمليات العادية

في سيناريو تشغيل عادي، عندما تكون جميع الموجهات قيد التشغيل والتشغيل، تقوم جميع الموجهات المحكية بتوجيه حركة المرور عبر الموزع الافتراضي (R1-HUB1). ويتحقق

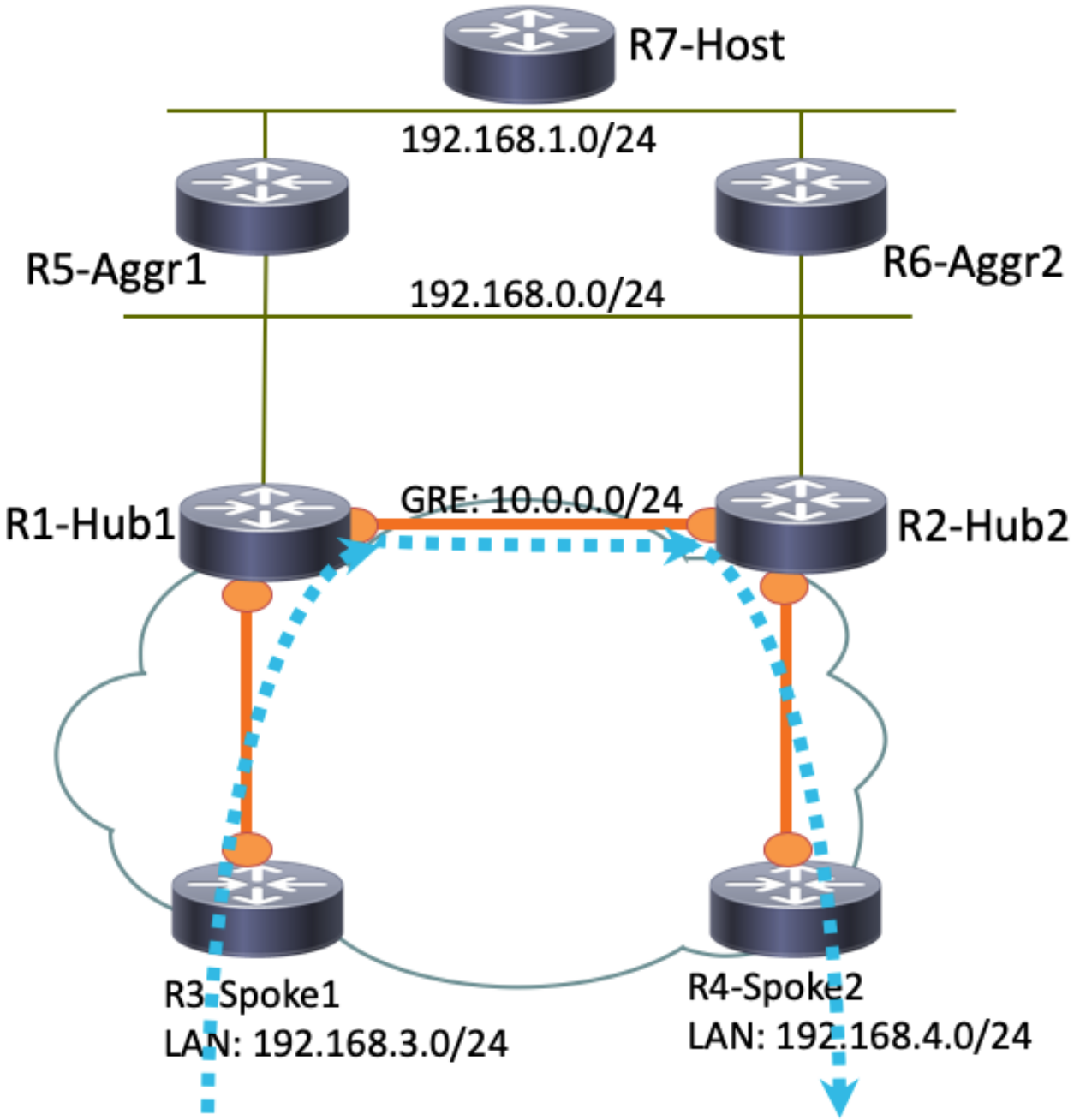
تفضيل التوجيه هذا عند تعيين التفضيل المحلي الافتراضي لبروتوكول BGP على 200 (راجع الأقسام التي تتبع للحصول على تفاصيل). ويمكن تعديل هذا الإجراء استنادا إلى متطلبات النشر، مثل موازنة حمل حركة مرور البيانات.

تحدث إلى- كلم (إخصار)

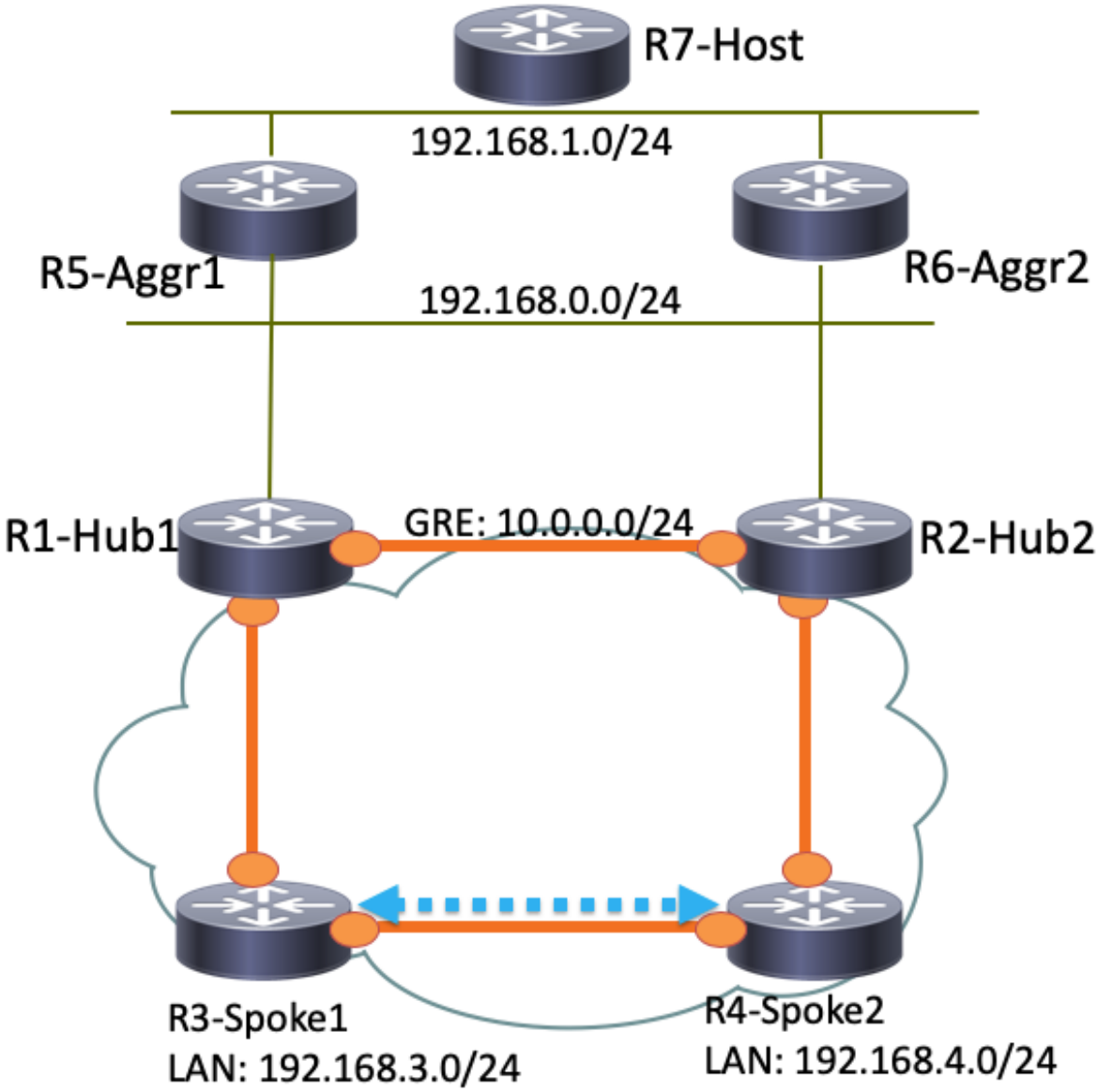
إذا قام R3-Talk1 ببدء اتصال ب R4-Talk2، يتم إنشاء نفق Dynamic Talk-Speaker باستخدام تكوين التحويل قصير المدى.

> **تلميح**: للحصول على مزيد من التفاصيل، ارجع إلى دليل التكوين الذي يتم التحدث به عن تكوين FlexVPN.

إذا كان R3-Talk1 متصل فقط ب R1-HUB1، وكان R4-TALK2 متصل فقط ب R2-HUB2، يمكن تحقيق اتصال تحدث مباشرة مع نفق GRE من نقطة إلى نقطة الذي يمتد بين المحاور. في هذه الحالة، يظهر مسار حركة المرور الأولية بين R3-Talk1 و R4-Talk2 مشابها لهذا:



ونظرا لأن R1-Hub1 يستقبل الحزمة على واجهة الوصول الظاهري، والتي تحتوي على نفس معرف شبكة بروتوكول تحليل الخطوة (NHRP) التالي كما هو الحال في نفق GRE، يتم إرسال إشارة حركة المرور إلى R3-Talk1. يؤدي هذا إلى تشغيل إنشاء نفق ديناميكي يتم التحدث إليه:



جداول ومخرجات التوجيه لسيناريو التشغيل العادي

فيما يلي جدول توجيه R1-HUB1 في سيناريو تشغيلي منتظم:

```
R1-HUB1# show ip route
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
       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

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
```

```
S        10.0.0.0/8 is directly connected, Null0
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.1/32 is directly connected, Tunnel0
C        10.0.1.1/32 is directly connected, Loopback0
S        10.0.1.2/32 is directly connected, Virtual-Access1
S        10.0.1.3/32 is directly connected, Virtual-Access2
B        10.0.2.1/32 [200/0] via 10.0.0.2, 00:05:40
B        10.0.2.3/32 [200/0] via 10.0.0.2, 00:05:40
B        10.0.2.4/32 [200/0] via 10.0.0.2, 00:05:40
B        10.0.5.1/32 [200/0] via 192.168.0.5, 00:05:40
B        10.0.6.1/32 [200/0] via 192.168.0.6, 00:05:40
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.0.0/24 is directly connected, Ethernet0/0
L        172.16.0.1/32 is directly connected, Ethernet0/0
S     192.168.0.0/16 is directly connected, Null0
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, Ethernet0/2
L        192.168.0.1/32 is directly connected, Ethernet0/2
B     192.168.1.0/24 [200/0] via 192.168.0.5, 00:05:40
B     192.168.3.0/24 [200/0] via 10.0.1.4, 00:05:24
B     192.168.4.0/24 [200/0] via 10.0.1.5, 00:05:33
```

فيما يلي جدول توجيه R3-TALK1 في سيناريو عمليات منتظم بعد إنشاء النفق الذي يتحدث إليه مع R4-TALK2:

```
R3-SPOKE1#  show ip route
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
       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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
B        10.0.0.0/8 [200/0] via 10.0.1.1, 00:06:27
H        10.0.0.1/32 is directly connected, 00:06:38, Tunnel1
S   %    10.0.1.1/32 is directly connected, Tunnel0
C        10.0.1.3/32 is directly connected, Tunnel0
H        10.0.1.4/32 is directly connected, 00:01:30, Virtual-Access1
S        10.0.2.1/32 is directly connected, Tunnel1
C        10.0.2.3/32 is directly connected, Tunnel1
H        10.0.2.4/32 [250/1] via 10.0.2.3, 00:01:30, Virtual-Access1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.0.0/24 is directly connected, Ethernet0/0
L        172.16.0.3/32 is directly connected, Ethernet0/0
B     192.168.0.0/16 [200/0] via 10.0.1.1, 00:06:27
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Ethernet0/1
L        192.168.3.3/32 is directly connected, Ethernet0/1
     192.168.4.0/32 is subnetted, 1 subnets
H        192.168.4.4 [250/1] via 10.0.1.3, 00:01:30, Virtual-Access1
```

في R3-Talk1، يحتوي جدول BGP على إدخالين لشبكة 192.168.0.0/16 بتفضيلات محلية مختلفة (يفضل R1-Hub1):

```
R3-SPOKE1#show ip bgp 192.168.0.0/16
BGP routing table entry for 192.168.0.0/16, version 8
```

```
Paths: (2 available, best #2, table default)
 Not advertised to any peer
 Refresh Epoch 1
 Local
   10.0.2.1 from 10.0.2.1 (10.0.2.1)
     Origin incomplete, metric 0, localpref 100, valid, internal
     rx pathid: 0, tx pathid: 0
 Refresh Epoch 1
  Local
    10.0.1.1 from 10.0.1.1 (10.0.1.1)
     Origin incomplete, metric 0, localpref 200, valid, internal, best
     rx pathid: 0, tx pathid: 0x0
```

فيما يلي جدول توجيه R5-AGGR1 في سيناريو تشغيلي منتظم:

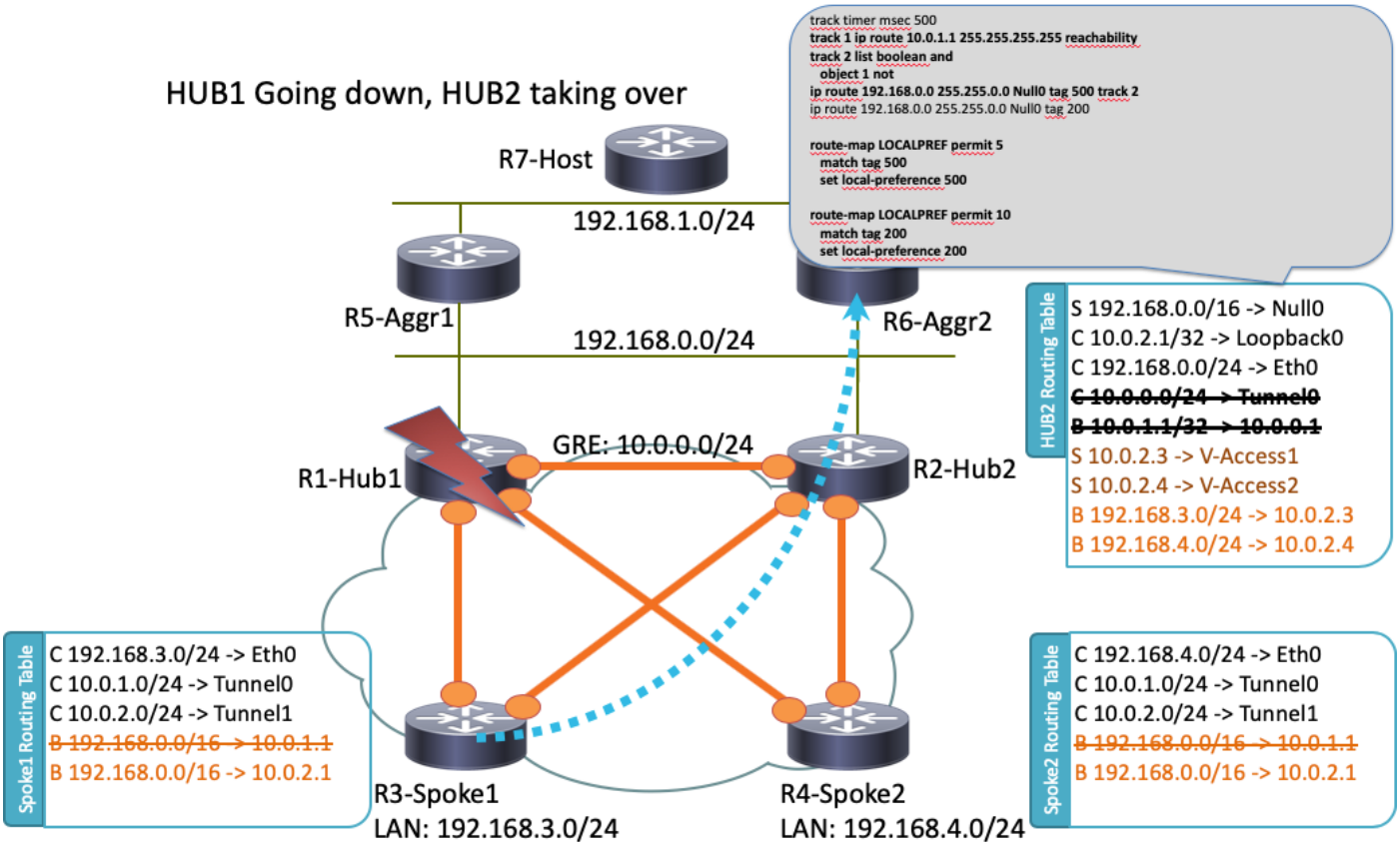
```
R5-LAN1#show ip route
     10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
B        10.0.0.0/8 [200/0] via 192.168.0.1, 00:07:22
B        10.0.0.0/24 [200/0] via 192.168.0.1, 00:07:22
B        10.0.1.1/32 [200/0] via 192.168.0.1, 00:07:22
B        10.0.1.3/32 [200/0] via 192.168.0.1, 00:07:17
B        10.0.1.4/32 [200/0] via 192.168.0.1, 00:07:16
B        10.0.2.1/32 [200/0] via 192.168.0.2, 15:44:13
B        10.0.2.3/32 [200/0] via 192.168.0.2, 15:44:13
B        10.0.2.4/32 [200/0] via 192.168.0.2, 15:44:13
C        10.0.5.1/32 is directly connected, Loopback0
B        10.0.6.1/32 [200/0] via 192.168.0.6, 00:07:22
     172.16.0.0/24 is subnetted, 1 subnets
B        172.16.0.0 [200/0] via 192.168.0.1, 00:07:22
B     192.168.0.0/16 [200/0] via 192.168.0.1, 00:07:22
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, Ethernet0/0
L        192.168.0.5/32 is directly connected, Ethernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1
L        192.168.1.5/32 is directly connected, Ethernet0/1
B     192.168.3.0/24 [200/0] via 10.0.1.3, 00:07:06
B     192.168.4.0/24 [200/0] via 10.0.1.4, 00:07:15
```

فيما يلي جدول توجيه R7-Host في سيناريو تشغيلي منتظم:

```
R7-HOST#show ip route
S*    0.0.0.0/0 [1/0] via 192.168.1.254
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/0
L        192.168.1.7/32 is directly connected, Ethernet0/0
```

سيناريو فشل HUB1

فيما يلي سيناريو أسفل R1-HUB1 (بسبب إجراءات مثل انقطاع التيار الكهربائي أو الترقية):



في هذا السيناريو، يحدث هذا التسلسل للأحداث:

1. يكتشف BFD على R2-HUB2 وعلى موجهات تجميع شبكات LAN R5-AGGR1 و R6-AGGR2 حالة فشل R1-HUB1. وتتيجة لهذا، تنهار علاقات منطقة الحدود بين الولايات المتحدة وباكستان على الفور.

2. يتعطل اكتشاف كائن المسار لـ R2-HUB2 الذي يكتشف وجود الاسترجاع R1-HUB1 (المسار 1 في مثال التكوين).

3. يقوم هذا الكائن الذي تم تتبع سقوطه بتشغيل مسار آخر للانتقال لأعلى (منطق NOT). في هذا المثال، يذهب المسار 2 لأعلى كلما انخفض المسار 1.

4. يؤدي هذا إلى تشغيل إدخال توجيه IP ثابت لإضافته إلى جدول التوجيه بسبب قيمة أقل من المسافة الإدارية الافتراضية. هنا التكوين المناسب:

```
! Routes added when second HUB is down
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2

! Default static routes are with Tag 200 and admin distance of 150
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
```

5. يعيد R2-HUB2 توزيع هذه المسارات الثابتة باستخدام تفضيل BGP محلي أكبر من القيمة التي تم تعيينها لـ R1-HUB1. في هذا المثال، يتم إستخدام تفضيل محلي **من 500** في سيناريو الفشل، بدلا من **200** التي يتم تعيينها بواسطة R1-HUB1:

```
route-map LOCALPREF permit 5
```

```
 match tag 500
 set local-preference 500
!
route-map LOCALPREF permit 10
 match tag 200
 set local-preference 200
!
```

في R3-talk1، يمكنك رؤية ذلك في مخرجات بروتوكول بوابة الحدود (BGP). لاحظ أن إدخال R1 لا يزال موجودا، ولكنه غير مستخدم:

```
R3-SPOKE1#show ip bgp 192.168.0.0/16
BGP routing table entry for 192.168.0.0/16, version 10
Paths: (2 available, best #1, table default)
 Not advertised to any peer
 Refresh Epoch 1
 Local
   10.0.2.1 from 10.0.2.1 (10.0.2.1)
      Origin incomplete, metric 0, localpref 500, valid, internal, best
      rx pathid: 0, tx pathid: 0x0
 Refresh Epoch 1
 Local
   10.0.1.1 from 10.0.1.1 (10.0.1.1)
     Origin incomplete, metric 0, localpref 200, valid, internal
     rx pathid: 0, tx pathid: 0
```

6. عند هذه النقطة، يبدأ الك المجلسين (R3-Talk1 و R4-Talk2) في إرسال حركة مرور البيانات إلى R2-HUB2. يجب أن تحدث جميع هذه الخطوات خلال ثانية واحدة. فيما يلي جدول التوجيه في Talk 3:

```
R3-SPOKE1#show ip route
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
B        10.0.0.0/8 [200/0] via 10.0.2.1, 00:00:01
S        10.0.1.1/32 is directly connected, Tunnel0
C        10.0.1.3/32 is directly connected, Tunnel0
S        10.0.2.1/32 is directly connected, Tunnel1
C        10.0.2.3/32 is directly connected, Tunnel1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.0.0/24 is directly connected, Ethernet0/0
L        172.16.0.3/32 is directly connected, Ethernet0/0
B     192.168.0.0/16 [200/0] via 10.0.2.1, 00:00:01
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Ethernet0/1
L        192.168.3.3/32 is directly connected, Ethernet0/1
```

7. فيما بعد BGP جلسة بين الفروع و R1-HUB1 إلى أسفل، و DPD كشف النظير الميت يزيل أنفاق IPSec التي تم إنشاؤها على R1-HUB1. ومع ذلك، لا يؤثر هذا على إعادة توجيه حركة مرور البيانات، نظرا لاستخدام R2-HUB2 بالفعل كبوابة إنهاء النفق الرئيسية:

```
R3-SPOKE1#show ip bgp 192.168.0.0/16
BGP routing table entry for 192.168.0.0/16, version 10
Paths: (1 available, best #1, table default)
 Not advertised to any peer
 Refresh Epoch 1
 Local
```

```
        10.0.2.1 from 10.0.2.1 (10.0.2.1)
          Origin incomplete, metric 0, localpref 500, valid, internal, best
          rx pathid: 0, tx pathid: 0x0
```

التكوينات

يوفر هذا القسم نموذج لتكوينات لوحات التوزيع والقنوات التي يتم إستخدامها في هذه المخطط.

تكوين R1-HUB

```
version 15.4
!
hostname R1-HUB1
!
aaa new-model
!
aaa authorization network default local
!
aaa session-id common
!
! setting track timers to the lowest possible (the lower this value is
! the faster router will react
track timer ip route msec 500
!
! Monitoring of HUB2's loopback present in routing table
! If it is present it will mean that HUB2 is alive
track 1 ip route 10.0.2.1 255.255.255.255 reachability
!
! Monitoring of loopback of R5-AGGR-1
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
! Monitoring of loopback of R6-AGGR-2
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
! Track 2 should be UP only when HUB2 is not available and both AGGRE routers are up
!
track 2 list boolean and
 object 1 not
 object 3
 object 4
!

! IKEv2 Config Exchange configuration (IP addresses for spokes are assigned from pool)
crypto ikev2 authorization policy default
 pool SPOKES
 route set interface
 route accept any tag 20
!
!
! IKEv2 profile for Spokes - Smart Defaults used
crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default default
 virtual-template 1
!
interface Loopback0
 ip address 10.0.1.1 255.255.255.255
```

```
!
! GRE Tunnel configured to second HUB. It is required for spoke-to-spoke connectivity
! to work in all possible circumstances
! no BFD echo configuration is required to avoid Traffic Indication sent by remote HUB
! (BFD echo is having the same source and destination IP address)
!
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip nhrp network-id 1
 ip nhrp redirect
 bfd interval 50 min_rx 50 multiplier 3
 no bfd echo
 tunnel source Ethernet0/2
 tunnel destination 192.168.0.2
!
interface Ethernet0/0
 ip address 172.16.0.1 255.255.255.0
!
interface Ethernet0/2
 ip address 192.168.0.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
! BGP Configuration
router bgp 1
 bgp log-neighbor-changes
! dynamic peer-groups are used for AGGR routers and SPOKES
 bgp listen range 192.168.0.0/24 peer-group DC
 bgp listen range 10.0.1.0/24 peer-group SPOKES
! BGP timers configured
 timers bgp 15 30
 neighbor SPOKES peer-group
 neighbor SPOKES remote-as 1
 neighbor DC peer-group
 neighbor DC remote-as 1
! Within DC BFD is used to determine neighbour status
 neighbor DC fall-over bfd
 neighbor 10.0.0.2 remote-as 1
! BFD is used to detect HUB2 status
 neighbor 10.0.0.2 fall-over bfd
 !
 address-family ipv4
 redistribute connected
! route-map which determines what should be the local-pref
 redistribute static route-map LOCALPREF
 neighbor SPOKES activate
! to spokes only Aggregate/Summary routes are sent
 neighbor SPOKES route-map AGGR out
 neighbor DC activate
 neighbor DC route-reflector-client
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 route-reflector-client
 exit-address-family
!
ip local pool SPOKES 10.0.1.2 10.0.1.254
!
! When HUB2 goes down Static Routes with Tag 500 are added and admin distance of 1
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
```

```
! Default static routes are with Tag 200 and admin distance of 150
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
 match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
 match tag 500
 set local-preference 500
!
route-map LOCALPREF permit 10
 match tag 200
 set local-preference 200
!
route-map LOCALPREF permit 15
 match tag 20
```

تكوين R2-HUB2

```
hostname R2-HUB2
!
aaa new-model
!
aaa authorization network default local
!
track timer ip route msec 500
!
track 1 ip route 10.0.1.1 255.255.255.255 reachability
!
track 2 list boolean and
 object 1 not
 object 3
 object 4
!
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
!
crypto ikev2 authorization policy default
 pool SPOKES
 route set interface
 route accept any tag 20
!
!
crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default default
 virtual-template 1
!
!
interface Loopback0
 ip address 10.0.2.1 255.255.255.255
!
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
```

```
 ip nhrp network-id 1
 ip nhrp redirect
 bfd interval 50 min_rx 50 multiplier 3
 no bfd echo
 tunnel source Ethernet0/2
 tunnel destination 192.168.0.1
!
interface Ethernet0/0
 ip address 172.16.0.2 255.255.255.0
!
interface Ethernet0/2
 ip address 192.168.0.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
router bgp 1
 bgp log-neighbor-changes
 bgp listen range 192.168.0.0/24 peer-group DC
 bgp listen range 10.0.2.0/24 peer-group SPOKES
 timers bgp 15 30
 neighbor SPOKES peer-group
 neighbor SPOKES remote-as 1
 neighbor DC peer-group
 neighbor DC remote-as 1
 neighbor DC fall-over bfd
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 fall-over bfd
 !
 address-family ipv4
 redistribute connected
 redistribute static route-map LOCALPREF
 neighbor SPOKES activate
 neighbor SPOKES route-map AGGR out
 neighbor DC activate
 neighbor DC route-reflector-client
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 route-reflector-client
 exit-address-family
!
ip local pool SPOKES 10.0.2.2 10.0.2.254
ip forward-protocol nd
!
!
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
 match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
 match tag 500
 set local-preference 500
!
```

```
route-map LOCALPREF permit 10
 match tag 200
 set local-preference 100
!
route-map LOCALPREF permit 15
 match tag 20
```

تكوين R3-TALK1

```
hostname R3-SPOKE1
!
aaa new-model
!
aaa authorization network default local
!
!
crypto ikev2 authorization policy default
 route set interface
!
!
crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 dpd 10 2 on-demand
 aaa authorization group psk list default default
!
! Tunnel to the HUB1
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
! Tunnel to the HUB2
!
interface Tunnel1
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
interface Ethernet0/0
description INTERNET-CLOUD
 ip address 172.16.0.3 255.255.255.0
!
interface Ethernet0/1
description LAN
 ip address 192.168.3.3 255.255.255.0
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet0/1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel protection ipsec profile default
!
router bgp 1
 bgp log-neighbor-changes
```

```
 timers bgp 15 30
 neighbor 10.0.1.1 remote-as 1
 neighbor 10.0.2.1 remote-as 1
 !
 address-family ipv4
 network 192.168.3.0
 neighbor 10.0.1.1 activate
 neighbor 10.0.2.1 activate
 exit-address-family
```

تكوين R4-Talk2

```
hostname R4-SPOKE2
!
aaa new-model
!
aaa authorization network default local
!
!
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 dpd 10 2 on-demand
 aaa authorization group psk list default default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface Tunnel1
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 172.16.0.4 255.255.255.0
!
interface Ethernet0/1
 ip address 192.168.4.4 255.255.255.0
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet0/1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel protection ipsec profile default
!
router bgp 1
 bgp log-neighbor-changes
 timers bgp 15 30
 neighbor 10.0.1.1 remote-as 1
 neighbor 10.0.2.1 remote-as 1
```

```
 !
 address-family ipv4
 network 192.168.4.0
 neighbor 10.0.1.1 activate
 neighbor 10.0.2.1 activate
 exit-address-family
!
```

تكوين R5-AGGR1

```
hostname R5-LAN1
!
no aaa new-model
!
!
interface Loopback0
 ip address 10.0.5.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.5 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
! HSRP configuration on the LAN side
!
interface Ethernet0/1
 ip address 192.168.1.5 255.255.255.0
 standby 1 ip 192.168.1.254
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 1
 neighbor 192.168.0.1 fall-over bfd
 neighbor 192.168.0.2 remote-as 1
 neighbor 192.168.0.2 fall-over bfd
 !
 address-family ipv4
 redistribute connected
 redistribute static
 neighbor 192.168.0.1 activate
 neighbor 192.168.0.2 activate
 exit-address-family
```

تكوين R6-AGGR2

```
hostname R6-LAN2
!
interface Loopback0
 ip address 10.0.6.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.6 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
interface Ethernet0/1
 ip address 192.168.1.6 255.255.255.0
 standby 1 ip 192.168.1.254
 standby 1 priority 200
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 1
```

```
 neighbor 192.168.0.1 fall-over bfd
 neighbor 192.168.0.2 remote-as 1
 neighbor 192.168.0.2 fall-over bfd
 !
 address-family ipv4
 redistribute connected
 redistribute static
 neighbor 192.168.0.1 activate
 neighbor 192.168.0.2 activate
 exit-address-family
!
```

تكوين مضيف R7 (محاكاة المضيف في تلك الشبكة)

```
hostname R7-HOST
!
no aaa new-model
!
interface Ethernet0/0
 ip address 192.168.1.7 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
```

ملاحظات تكوين هامة

فيما يلي بعض الملاحظات المهمة حول التكوينات الموضحة في الأقسام السابقة:

- ويلزم وجود نفق GRE من نقطة إلى نقطة بين المركزين لتوفير الاتصال من خلال الاتصال من خلال الاتصال من خلال الاتصال المباشر للعمل في جميع السيناريوهات، وعلى وجه التحديد تضمين السيناريوهات التي لا تتصل فيها بعض الفروع إلا بأحد المركزين بينما تتصل أخرى بمركز آخر.

- يلزم تكوين **no bfd echo** في واجهة نفق GRE بين المركزين لتجنب إشارة حركة المرور التي يتم إرسالها من موزع آخر. يحتوي صدى BFD على نفس عناوين IP المصدر والوجهة، والذي يساوي عناوين IP الخاص بالموجه الذي يرسل صدى BFD. ونظرا لأنه يتم توجيه هذه الحزم مرة أخرى بواسطة الموجه الذي يستجيب، يتم إنشاء مؤشرات حركة مرور NHRP.

- في تكوين BGP، لا تكون تصفية خريطة المسار التي تعلن عن الشبكات نحو الخوادم مطلوبة، ولكنها تجعل التكوينات أكثر مثالية نظرا لأنه يتم الإعلان عن موجهات التجميع/الموجز فقط:

```
neighbor SPOKES route-map AGGR out
```

- على لوحات التوزيع، يلزم تكوين **الإعدادات المحلية ل خريطة المسار** من أجل إعداد تفضيل BGP المحلي المناسب، كما يوفق تصفية المسارات الثابتة المعاد توزيعها إلى مسارات وضع تكوين الملخص و IKEv2 فقط.

- لا يتناول هذا التصميم التكرار في مواقع Remote Office (ملكت). إذا انقطع رابط شبكة WAN على مركز الوصول، فإن شبكة VPN أيضا لا تعمل. قم بإضافة ارتباطات ثانية إلى الموجه الموجه الذي يتم التحدث به أو إضافة موجه ثان يتم التحدث به داخل نفس الموقع من أجل معالجة هذه المشكلة.

باختصار، يمكن التعامل مع تصميم التكرار الذي يتم تقديمه في هذا المستند كبديل حديث لميزة التحويل المعبر عن الحالة (SSO)/الميزة المعبر عن الحالة. يستم هذا الطراز

بمرونة فائقة ويمكن ضبطه بإحكام من أجل الوفاء بمتطلبات النشر الخاصة بك.

التحقق من الصحة

ال يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

ال تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- ورقة بيانات Cisco IOS FlexVPN
- تم التحديث إلى تكوين FlexVPN
- الدعم التقني والمستندات - Cisco Systems

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).