تم التحديث عبر FlexVPN في تصميم لوحة وصل مكررة مع مثال تكوين كتلة عميل FlexVPN

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
التكوين
مخططات الشبكة
شبكة النقل
شبكة ترابية
التكوين الأساسي للملتمس والمحور
تم التحديث عن تعديل التكوين
Speech Configuration - كتلة تكوين العميل
تكوين كامل النطق - المرجع
تكوين الموزع
خطبا
عنوان تراكب الموزع
توجيه
إستخدام ملخصات الشبكة
أنفاق تتحدث
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية تكوين تحدث في شبكة FlexVPN باستخدام كتلة تكوين عميل FlexVPN في سيناريو تتوفر فيه مراكز متعددة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- FlexVPN
- بروتوكولات التوجيه من Cisco

المكونات المستخدمة

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

- موجه الخدمة المتكاملة (ISR Cisco G2 Series Integrated Service Router)
- Cisco IOS®، الإصدار 15.2M

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

معلومات أساسية

لأغراض التكرار، قد يحتاج الشخص الذي يتحدث إليه إلى الاتصال بمراكز متعددة. حيث تسمح الوحدات الاحتياطية على الجانب المتصل بالتشغيل المستمر دون حدوث نقطة فشل واحدة على جانب الموزع.

إن تصميمي لوحة الوصل المتكررة FlexVPN الأكثر شيوعا اللذين يستخدمان التكوين الذي يتم التحدث به هما:

- **نهج السحابة المزدوجة**، حيث يكون للخطيب نفقين منفصلين ينطلقان إلى كلا المركزين في جميع الأوقات.
- **نهج تجاوز الفشل**، حيث يكون للخطيب نفق نشط مع محور واحد في أي نقطة زمنية معينة.

ولكل من النهجين مجموعة فريدة من إيجابياته وسلبياته.

مقاربة	إيجابيات	مخاريط
سحابة مزدوجة	• إسترداد أسرع في حالة فشل، استنادا إلى مؤقتات بروتوكول التوجيه • إمكانات أكبر لتوزيع حركة المرور بين المحاور، نظرا لأن الاتصالات بكلا المركزين نشطة	• ت

تجاوز الفشل	• سهولة التهيئة - مضمنة في شبكة FlexVPN • لا يعتمد على بروتوكول التوجيه في فشل

وتصف هذه الوثيقة النهج الثاني.

التكوين

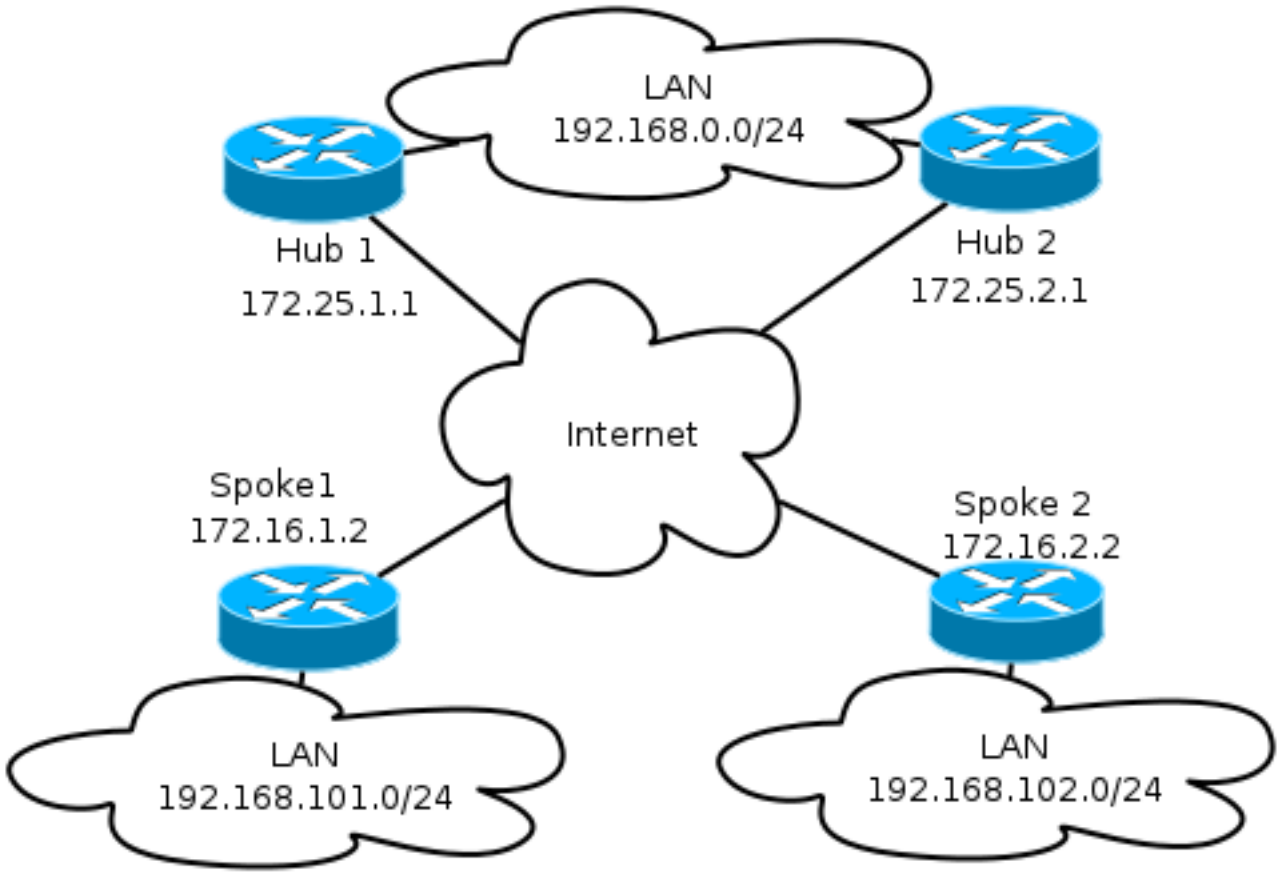
ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

مخططات الشبكة

تظهر هذه المخططات المخططات كلا من مخططات مخططات النقل والمخططات المتفرعة.

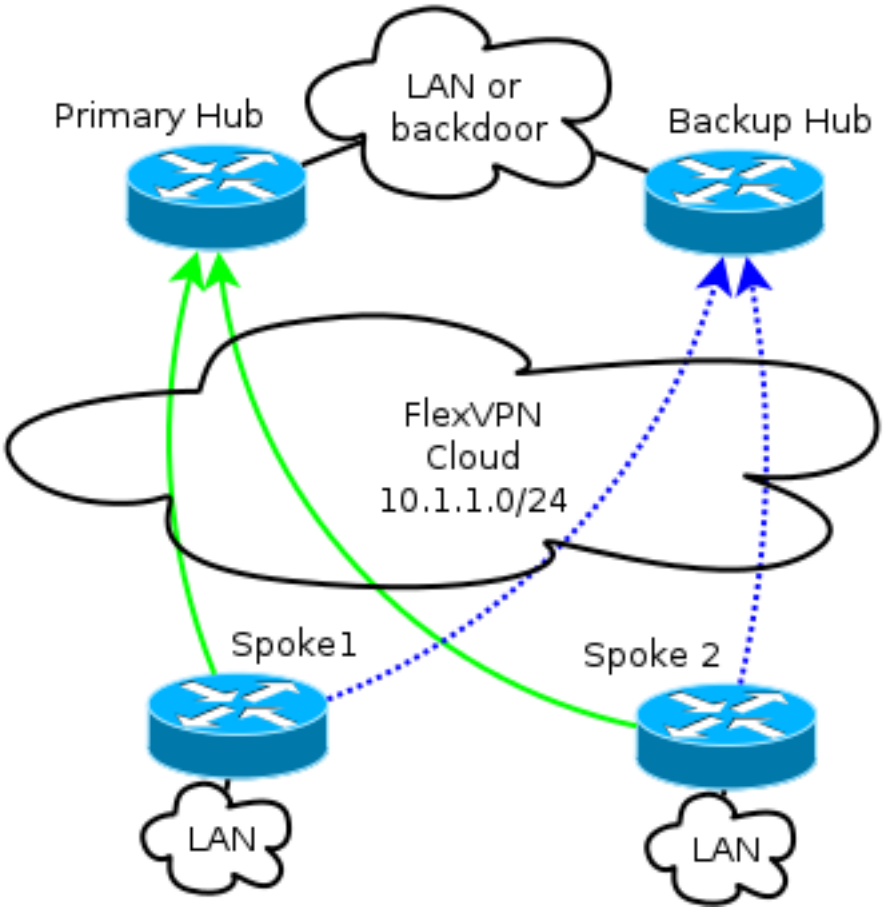
شبكة النقل

يوضح هذا المخطط شبكة النقل الأساسية التي يتم إستخدامها عادة في شبكات FlexVPN.



شبكة ترابية

يوضح هذا المخطط الشبكة الفرعية مع الاتصال المنطقي الذي يوضح كيفية عمل تجاوز الفشل. خلال العملية العادية، يحافظ كل من Talk 1 و Talk 2 على علاقة مع محور واحد فقط.



ملاحظة: في الرسم التخطيطي، تظهر الخطوط الخضراء الصلبة اتصال واتجاه Internet Key Exchange الإصدار 2 (IKEv2/Flex session)، وتشير الخطوط الزرقاء المنقطة إلى اتصال النسخ الاحتياطي في حالة فشل جلسة عمل IKE (Internet Key Exchange) إلى الموزع الرئيسي.

تمثل عناوين **24/** تجمع العناوين الذي تم تعيينه لهذه السحابة، وليس عنونة الواجهة الفعلية. وذلك لأن موزع FlexVPN يقوم عادة بتخصيص عنوان IP ديناميكي للواجهة التي يتم التحدث بها، ويعتمد على المسارات التي يتم إدخالها بشكل ديناميكي عبر أوامر التوجيه في كتلة تفويض FlexVPN.

التكوين الأساسي للملتمس والمحور

يعتمد التكوين الأساسي للمحور والمحور على مستندات الترحيل من DMVPN (Dynamic Multipoint VPN) إلى FlexVPN. يتم وصف هذا التكوين في ترحيل FlexVPN: النقل الثابت من DMVPN إلى FlexVPN على مقالة الأجهزة نفسها.

تم التحدث عن تعديل التكوين

Speech Configuration - كتلة تكوين العميل

يجب توسيع التكوين الذي تم التحدث به بواسطة كتلة تكوين العميل.

في التكوين الأساسي، يتم تحديد العديد من الأقران. يتم إعتبار النظير صاحب أعلى تفضيل (أقل رقم) قبل الآخرين.

```
crypto ikev2 client flexvpn Flex_Client
```

```
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

يجب تغيير تكوين النفق للسماح باختيار وجهة النفق بشكل ديناميكي، استنادا إلى كتلة تكوين عميل FlexVPN.

```
interface Tunnel1
tunnel destination dynamic
```

من المهم للغاية تذكر أن كتلة تكوين عميل FlexVPN مرتبطة بواجهة، وليس بملف تعريف IKEv2 أو ملف تعريف أمان بروتوكول الإنترنت (IPsec).

توفر كتلة تكوين العميل خيارات متعددة لضبط وقت تجاوز الفشل والعمليات، والتي تتضمن تتبع إستخدام الكائنات والنسخ الاحتياطي للطلب ووظائف مجموعات النسخ الاحتياطي.

مع التهيئة الأساسية، يعتمد النطق على DPDs من أجل اكتشاف ما إذا كان النطق غير متجاوب، ويثير ذلك تغييرا بمجرد إعلان وفاة النظير. خيار إستخدام DPD ليس سريعا، بسبب كيفية عمل DPDs. قد يحتاج المسؤول إلى تحسين التكوين عن طريق تعقب الكائن أو إجراء تحسينات مشابهة.

لمزيد من المعلومات، ارجع إلى فصل **تكوين عميل FlexVPN** من دليل تكوين Cisco IOS، والذي يتم ربطه في قسم **المعلومات ذات الصلة** في نهاية هذا المستند.

تكوين كامل النطق - المرجع

```
crypto logging session

crypto ikev2 keyring Flex_key
 peer Spokes
  address 0.0.0.0 0.0.0.0
  pre-shared-key local cisco
  pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

crypto ipsec transform-set IKEv2 esp-gcm
 mode transport

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 description FlexVPN tunnel
 ip address negotiated
 ip mtu 1400
 ip nhrp network-id 2
```

```
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 2000
tunnel source Ethernet0/0
tunnel destination dynamic
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

تكوين الموزع

في حين أن غالبية تكوين المحور تظل كما هي، عدة جوانب يجب معالجتها. وتتعلق معظمها بحالة يتصل فيها فرع أو أكثر بمحور واحد، في حين تظل فروع أخرى متصلة بمحور آخر.

خطبا

نظرا لأن المحولات تحصل على عناوين IP من لوحات التوزيع، فمن المرغوب عادة أن تقوم لوحات التوزيع بتعيين العناوين من شبكات فرعية مختلفة أو جزء مختلف من شبكة فرعية.

على سبيل المثال:

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```
الموزع 2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```
وهذا يؤدي إلى منع إنشاء التداخل، حتى إذا لم يتم توجيه العناوين خارج سحابة FlexVPN، وهو ما قد يضعف أستكشاف الأخطاء وإصلاحها.

عنوان تراكب الموزع

يمكن أن يحتفظ كلا المنفذين بعنوان IP نفسه على واجهة قالب ظاهري، ومع ذلك، يمكن أن يؤثر ذلك على أستكشاف الأخطاء وإصلاحها في بعض الحالات. يتيح خيار التصميم هذا تسهيل النشر والتخطيط، نظرا لأنه يجب أن يكون للمحادثة عنوان نظير واحد فقط لبروتوكول العبارة الحدودية (BGP).

وفي بعض الحالات، قد لا يكون مرغوبا فيه أو لازما.

توجيه

من الضروري أن تتبادل المحاور المعلومات حول القبضات المتصلة.

يجب أن تكون الموزعات قادرة على تبادل المسارات المحددة للأجهزة التي تم توصيلها بها، مع الاستمرار في توفير ملخص للمعلمات.

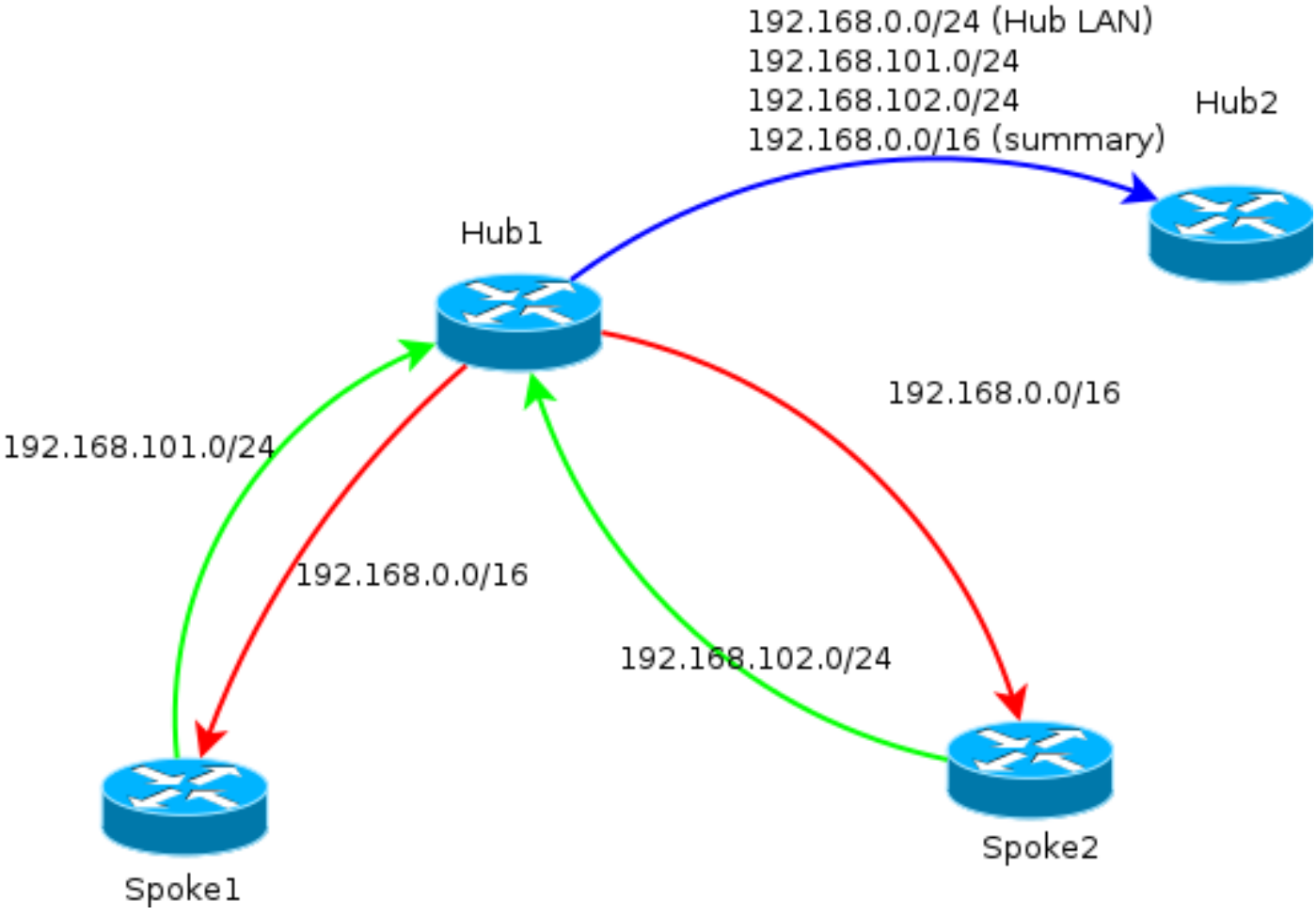
بما أن Cisco يوصي أن يستعمل أنت iBGP مع FlexVPN و DMVPN، فقط أن يوجه بروتوكول يكون أبديت.

```
 bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
 network 192.168.0.0
 neighbor Spokes peer-group
 neighbor Spokes remote-as 65001
 neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
 neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

access-list 1 permit any

route-map ALL permit 10
 match ip address 1
```

يسمح هذا التكوين:

- موزع رسائل ديناميكي من العناوين المعينة للكلمات الفرعية
- شبكة الإعلانات **24/192.168.0.0**
- مسار ملخص الإعلانات **16/192.168.0.0** إلى جميع الخوادم. يقوم تكوين عنوان التجميع بإنشاء مسار ساكن إستاتيكي لتلك البادئة عبر واجهة null0، وهي مسار discard يتم إستخدامه لمنع حلقات تكرار التوجيه.
- إعادة توجيه البادئات المحددة إلى الموزع الآخر
- عميل عاكس المسار للتأكد من أن لوحات التوزيع تتبادل المعلومات التي تم تعلمها من الفروع بين بعضها البعض

يمثل هذا المخطط تبادل البادئات في BGP في هذا الإعداد، من منظور أحد المحاور.



ملاحظة: في هذا الرسم التخطيطي، يمثل الخط الأخضر المعلومات المقدمة من قبل الفروع إلى المحور، ويمثل الخط الأحمر المعلومات المقدمة من كل محور إلى الفروع (ملخص فقط)، ويمثل الخط الأزرق البادئات المتبادلة بين المحاور.

إستخدام ملخصات الشبكة

قد لا تكون الملخصات قابلة للتطبيق أو مرغوبة في بعض السيناريوهات. أستخدم الحذر عند تعيين IP للوجهة في البادئات، لأن iBGP لا يتجاوز الخطوة التالية بشكل افتراضي.

يوصى بالملخصات في الشبكات التي تغير الحالة بشكل متكرر. على سبيل المثال، قد تتطلب إتصالات الإنترنت غير المستقرة ملخصات من أجل: تجنب إزالة البادئات وإضافتها، والحد من عدد التحديثات، والسماح لمعظم البادئات بالتدرج بشكل صحيح.

أنفاق تتحدث

في السيناريو والتكوين المذكورين في القسم السابق، لا تستطيع الفروع الموجودة في مراكز مختلفة إنشاء أنفاق يتم التحدث بها مباشرة. تتدفق حركة مرور البيانات بين الفروع المتصلة بمراكز مختلفة عبر الأجهزة المركزية.

هناك حل سهل لهذا الأمر. ومع ذلك، فإنه يتطلب أن يتم تمكين بروتوكول تحليل الخطوة (Hop) التالية (NHRP) مع نفس معرف الشبكة بين المحاور. ويمكن تحقيق ذلك، على سبيل المثال، إذا قمت بإنشاء نفق تضمين التوجيه العام (GRE) من نقطة إلى نقطة بين المحاور. بعد ذلك، IPsec غير مطلوب.

التحقق من الصحة

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

يقوم الأمر **show crypto ikev2 sa** بإعلامك بمكان اتصال المحادثة حاليا.

يتيح الأمر **show crypto ikev2 client flexVPN** للمسؤول إمكانية فهم الحالة الحالية لعملية عميل FlexVPN.

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
 Current state:ACTIVE
    Peer : 172.25.1.1
 Source : Ethernet0/0
    ivrf : IP DEFAULT
    fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

يتم بنجاح تجاوز الفشل باستخدام تكوين **show logging**" تسجيل هذا الإخراج على الجهاز المتصل:

```
CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500%
                                                                  Id: 172.25.1.1
 = FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr%
                                      Server_public_addr = 172.25.1.1 172.16.2.2
LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down%
  LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up%
  CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500%
                                                                  Id: 172.25.2.1
    = FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr%
Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177 172.16.2.2
```

في هذا الإخراج، يتم قطع الاتصال من **hub 172.25.1.1**، وتقوم كتلة تكوين عميل Flex_Client بالكشف عن الفشل

وتفرض الاتصال ب **172.25.2.1** حيث يظهر نفق، ويتم تعيين IP لمكبر صوت ل **10.1.1.177**.

استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

هنا أوامر تصحيح الأخطاء ذات الصلة:

- **debug crypto ikev2**
- **تصحيح أخطاء radius**

معلومات ذات صلة

- دليل تكوين FlexVPN و Internet Key Exchange الإصدار 2، Cisco IOS الإصدار 15 M&T
- 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).