تكوين حل FlexVPN والتحقق منه

المحتويات

- المقدمة
- المتطلبات الأساسية
  - المتطلبات
  - المكونات المستخدمة
- معلومات أساسية
  - IKEv2 مقابل IKEv1
  - قابلية التطوير
  - الميزات الرئيسية
  - توجيه
  - سياسة التخويل
  - FlexVPN مقابل تقنيات أخرى
- الرسم التخطيطي للشبكة
- التكوين
  - تكوين FlexVPN من موقع إلى موقع
    - الخطوة 1: تكوين الموجه A
    - الخطوة 2: تكوين الموجه B
    - التحقق من الصحة
  - FlexVPN بتقنية Hub-and-Talk
    - الخطوة 1: تكوين الموزع
    - الخطوة 2: التكوين الذي تم التحدث به
    - التحقق من الصحة
  - تحدث إلى FlexVPN الذي يتحدث
    - الخطوة 1: تكوين الموزع
    - الخطوة 2: تحدث عن تكوين
    - الخطوة 3: تحدث في التكوين B
    - التحقق من الصحة
- استكشاف الأخطاء وإصلاحها

المقدمة

يصف هذا المستند بيئة الشبكة الخاصة الظاهرية (Flex)، ويقدم مميزاتها، ويشرح كيفية تكوين كل مخطط FlexVPN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- IOS و Cisco IOS XE
- تبادل مفتاح الإنترنت (IKE) الإصدار 2
- أمان بروتوكول الإنترنت (IPsec)
- FlexVPN

المكونات المستخدمة

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

- Cisco IOS XE Amsterdam-17.3.6

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

FlexVPN هو حل شبكة خاصة ظاهرية (VPN) متعدد الاستخدامات وشامل تقدمه Cisco، مصمم للتعامل مع مجموعة متنوعة من أنواع عمل الشبكات ومتطلبات الاتصال على مستوى متعدد. وبالاعتماد على بروتوكول IKEv2 (تبادل مفتاح الإنترنت الإصدار 2)، تم تصميم FlexVPN لتبسيط تكوين شبكة VPN وإدارتها ونشرها، مما يعمل على زيادة فعالية مجموعة متنوعة من شبكات من أنواع مختلفة عبر أنواع متعددة من السيناريوهات التي يتم تكوينها وخطوات وأوامر الأدوات VPN (من موقع إلى موقع والوصول عن بعد وما إلى ذلك). ويعد هذا التناسق على تقليل الأخطاء ويعجل عملية النشر أكثر سهولة.

IKEv2 مقابل IKEv1

تستفيد FlexVPN من IKEv2، التي تدعم الخوارزميات المشفرة الحديثة مثل AES (معيار التشفير المتقدم) و SHA-256 (خوارزمية التجزئة الآمنة). وتوفر هذه الخوارزميات تشفيرا قويا وسلامة البيانات، مما يحمي البيانات المرسلة عبر الشبكة الخاصة الظاهرية (VPN) من أن يتم اعتراضها أو التلاعب بها.

يقدم IKEv2 المزيد من طرق المصادقة مقارنة ب IKEv1. وإلى جانب مفتاح مشترك مسبقا (PSK) وأنواع مصادقة مختلطة وقائمة على الشهادة، يسمح IKEv2 للعميل باستخدام بروتوكول المصادقة المتوسع (EAP) لمصادقة العميل.

في FlexVPN، يستخدم EAP لمصادقة العميل، ويعمل الموجه كترحيل، ويمرر رسائل EAP بين العميل وخادم EAP الخلفي، وهو خادم RADIUS عادة. تدعم شبكة FlexVPN العديد من طرق EAP، بما في ذلك EAP-TLS و EAP-PEAP و EAP-PSK وغيرها، لضمان عملية المصادقة.

يوضح الجدول الاختلافات بين وظائف IKEv1 و IKEv2:

	IKEv2	IKEv1
رسائل إنشاء البروتوكول	4 رسائل	6 رسائل
دعم EAP	نعم (رسالة إضافية)	لا
التفاوض للاتحادات الامنيه	رسالتان إضافيتان	3 رسائل إضافية

التشغيل عبر UDP 500/4500	نعم	نعم
إجتياز NAT (NAT-T)	نعم	نعم
مهام إعادة الإرسال والإقرار	نعم	نعم
توفير الحماية للهوية وآلية الحماية من رفض الخدمة (DoS) والسرية التامة لإعادة التوجيه (PFS)	نعم	نعم
دعم شفرات الجيل التالي	نعم	ال

قابلية التطوير

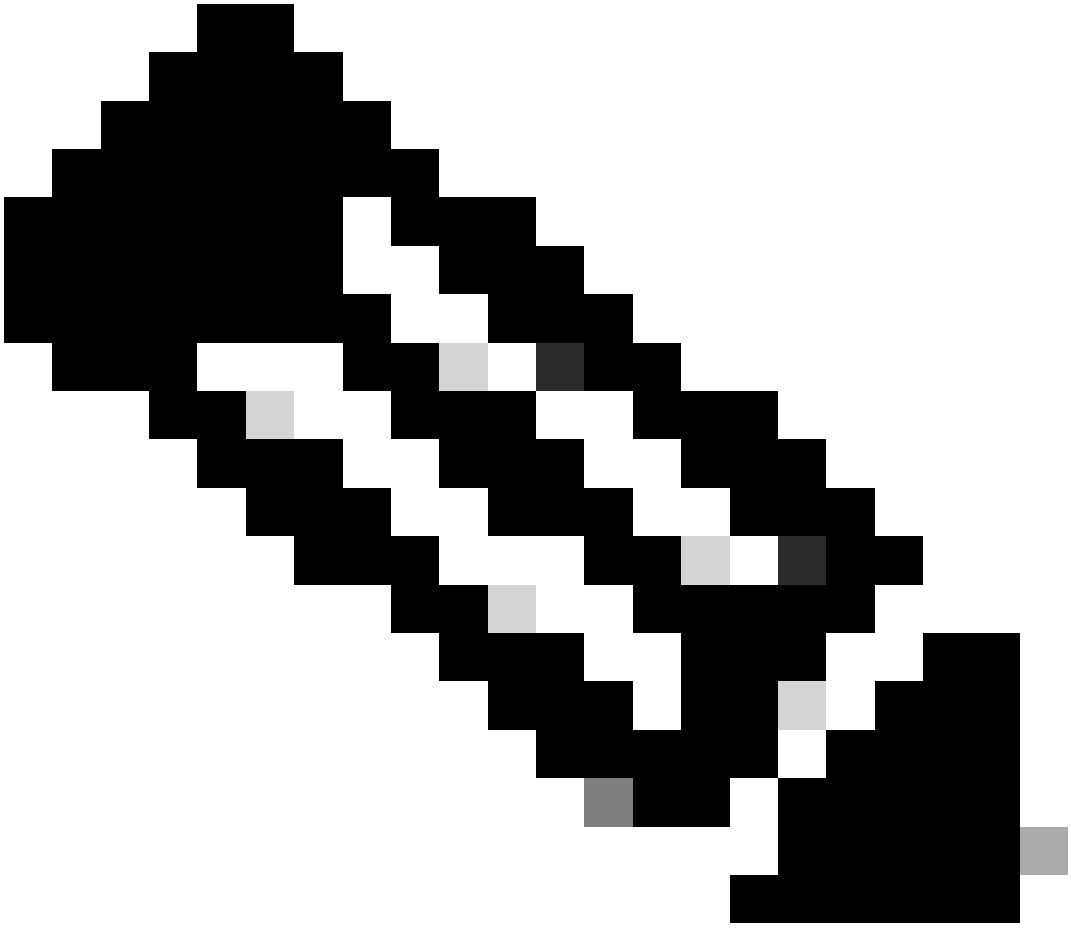
يمكن توسعة شبكة FlexVPN بسهولة تامة من المكاتب الصغيرة إلى شبكات الشركات الكبيرة. وهذا يجعل منه خيارا مثاليا للمؤسسات التي يتوفر بها عدد كبير من المستخدمين عن بعد ممن يحتاجون إلى الوصول الآمن والموثوق إلى الشبكة.

المميزات الرئيسية

- التكوين الديناميكي والأنفاق حسب الطلب:
  - يتم بدء اتصال FlexVPN، ويقوم النظام بإنشاء واجهة وصول افتراضية استنادا إلى قالب تم تكوينه مسبقا. تعمل هذه الواجهة كنقطة نهاية النفق لمدة الاتصال. وبمجرد انتهاء الحاجة إلى النفق، يتم تدمير واجهة الوصول الظاهرية، مما يعمل على توفير موارد النظام.

- المرونة أثناء النشر:
  - نموذج المحور والكلام: يتصل المحور المركزي بالعديد من المكاتب الفرعية. تعمل شبكة FlexVPN على تبسيط عملية إعداد هذه الاتصالات من خلال إطار عمل واحد، مما يجعلها مثالية للشبكات الكبيرة.
  - طبولوجيا الشبكة الكاملة والشبكة الجزئية: يمكن لجميع المواقع التواصل مباشرة دون المرور عبر مركز مركزي، مما يقلل من التأخير ويحسن الأداء.

- توفر عال وتكرار:
  - لوحات التوزيع المكررة: يدعم مراكز متعددة للنسخ الاحتياطي. في حالة فشل أحد المحاور، يمكن أن تتصل الفروع بموزع آخر، مما يضمن اتصال مستمر.
  - موازنة التحميل: وهذا يعمل على توزيع إتصالات الشبكة الخاصة الظاهرية (VPN) عبر أجهزة متعددة لتجنب تحميل أي جهاز واحد بشكل زائد، وهو ما يعد أمرا بالغ الأهمية للحفاظ على الأداء في عمليات النشر الكبيرة.



ملاحظة: يوفر الدليل التالي المزيد من المعلومات حول تكوين موازنة الأحمال لاتصال لوحات التوزيع.

تكوين موازن حمل IKEv2

- مصادقة وتفويض قابلان للتطوير:
  - دمج المصادقة والتفويض والمحاسبة (AAA): يعمل مع خوادم AAA مثل Cisco ISE أو RADIUS للإدارة المركزية لمسوغات وسياسات المستخدم الضرورية للاستخدام على نطاق واسع.
  - وحدات PKI والشهادات: يدعم البنية الأساسية للمفتاح العام (PKI) والشهادات الرقمية من أجل المصادقة الآمنة، والتي تكون قابلة للتطوير أكثر من إستخدام مفتاح مشترك مسبقا، خاصة في البيئات الكبيرة.

توجيه

تم تصميم وظيفة التوجيه في FlexVPN لتحسين قابلية التطوير والإدارة الفعالة لاتصالات VPN المتعددة والسماح بطريقة ديناميكية لتوجيه حركة مرور البيانات إلى كل

واحد منها. المكونات والآليات الأساسية التالية التي تجعل توجيه FlexVPN فعالا:

- واجهة القالب الظاهري: هذا قالب تكوين يتضمن جميع الإعدادات اللازمة لاتصال VPN، مثل تعيين عنوان IP ومصدر النفق وإعدادات IPsec. في هذه الواجهة تم تكوين الأمرip unnumbered لاقتراض عنوان IP، عادة من إسترجاع بدلا من تكوين عنوان IP محدد كمصدر للنفق. هذا يمكن لا نفس قالب أن يستعمل ب كل يتحدث، يسمح كل يتكلم أن يستعمل مصدره عنوان.

- واجهة الوصول الظاهري: هذه واجهات تم إنشاؤها ديناميكيا وترث إعداداتها من واجهة القالب الظاهري. في كل مرة يتم فيها إنشاء اتصال VPN جديد، يتم إنشاء واجهة وصول افتراضية جديدة استنادا إلى القالب الظاهري. وهذا يعني أن كل جلسة من جلسات عميل الشبكة الخاصة الظاهرية (VPN) تحتوي على واجهة فريدة خاصة بها، مما يعمل على تبسيط الإدارة والقياس.

- بروتوكولات التوجيه الديناميكية: وهو يعمل مع بروتوكولات التوجيه مثل OSPF و EIGRP و BGP عبر أنفاق شبكة VPN. يؤدي ذلك إلى إستمرار تحديث معلومات التوجيه تلقائيا، وهو أمر مهم للشبكات الكبيرة والديناميكية.

- يقوم IKEv2 بالإعلان عن الموجهات من خلال السماح لخادم FlexVPN بدفع سمات الشبكة إلى العميل، والذي يقوم بتثبيت هذه الموجهات على واجهة النفق. يقوم العميل أيضا بإعلام شبكاته الخاصة بالخادم أثناء تبادل وضع التكوين، مما يتيح تحديثات المسار على كلا النهايتين.

- NHRP (بروتوكول تحليل الخطوة (Hop) التالية) هو بروتوكول تحليل العنوان الديناميكي المستخدم في المخططات المحورية والمكملة لتعيين عناوين IP العامة إلى نقاط نهاية VPN الخاصة. وهو يمكن الأصداف من اكتشاف عناوين IP أخرى للاتصال المباشر.

سياسة التخويل

يمكن تكوين سياسة تفويض IKEv2 ل FlexVPN للتحكم في جوانب مختلفة من اتصال VPN. يحدد نهج تخويل IKEv2 نهج التخويل المحلي ويحتوي على سمات محلية و/أو عن بعد:

- يتم تطبيق السمات المحلية، مثل توجيه إعادة توجيه الشبكة الخاصة الظاهرية (VRF) ونهج جودة الخدمة، محليا.
- يتم دفع السمات البعيدة، مثل المسارات، إلى النظير عبر وضع التكوين.
- أستخدم الأمر crypto ikev2 authorization policy لتحديد السياسة المحلية.
- تتم الإشارة إلى سياسة تفويض IKEv2 من ملف تعريف IKEv2 من خلال أمر تفويض AAA.

يوفر هذا الجدول نظرة عامة على معلمات المفاتيح التي يمكن تكوينها بموجب نهج تخويل IKEv2.

الوصف	باراميتر
التكامل مع خوادم AAA للتحقق من مستخدم الوصول والحساب وتخويل المستخدم. يمكن أن يحدد النهج ما إذا كان يتم التحقق من الصحة محليا على الموجه أو عن	AAA

بعد، مثل من خلال خادم RADIUS.	
يدفع إعدادات التكوين إلى العميل، مثل قيم مهلة الخمول، ورموز keepalives، و DNS، وتعيين خادم WINS، وما إلى ذلك.	تكوين العميل
يسمح بالتكوينات المختلفة لمختلف العملاء استنادا إلى هويتهم أو عضويتهم في المجموعة.	التكوين الخاص بالعميل
يتيح هذا التكوين لحركة مرور معينة أن تمر عبر نفق VPN. وهذا ما يؤدي إلى تنفيذ حقن المسار الذي يتم دفعه إلى عميل VPN على اتصال ناجح.	مجموعة المسارات

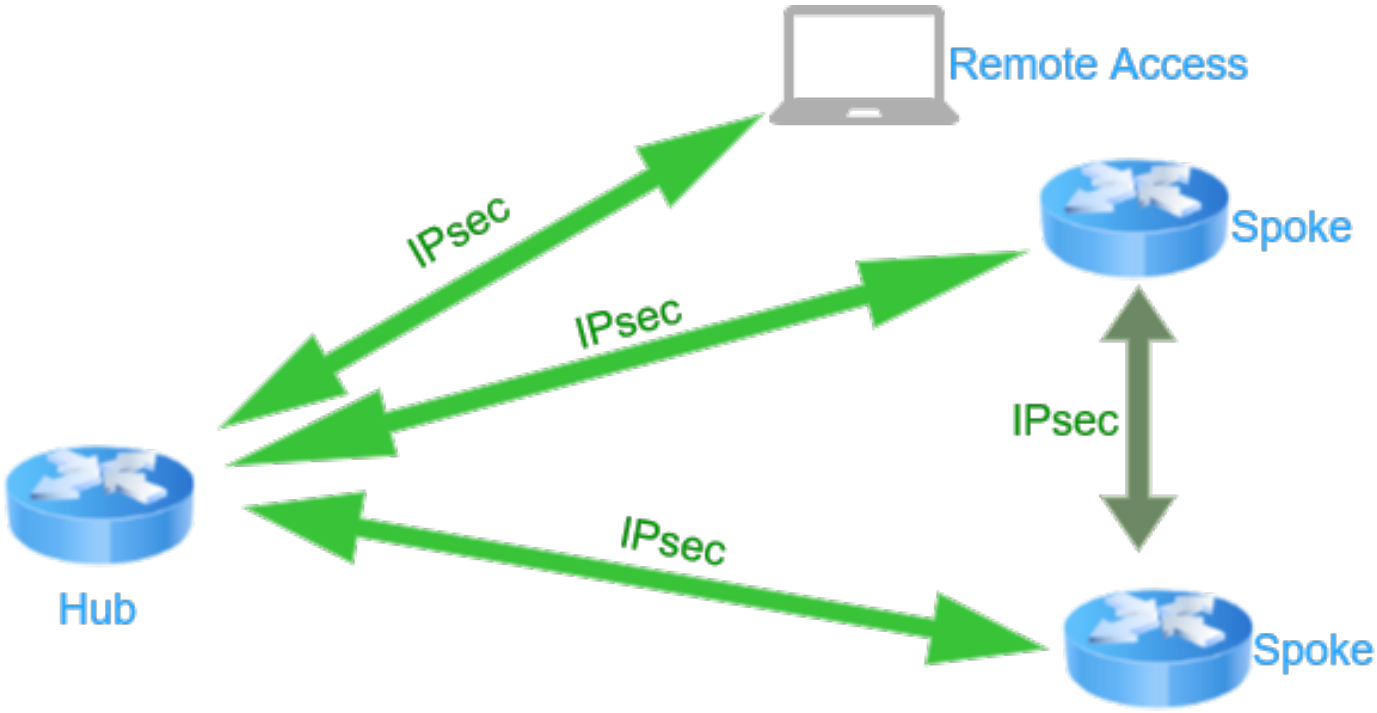
FlexVPN مقابل تقنيات أخرى

توفر شبكة FlexVPN مجموعة من المميزات التي تجعلها خيارا جذابا لبيئات الشبكات الحديثة. من خلال توفير إطار عمل موحد، تعمل شبكة FlexVPN على تبسيط عمليتي التهيئة والإدارة وتحسين الأمان ودعم قابلية التطوير وضمان قابلية التشغيل البيني وتقليل التعقيد.

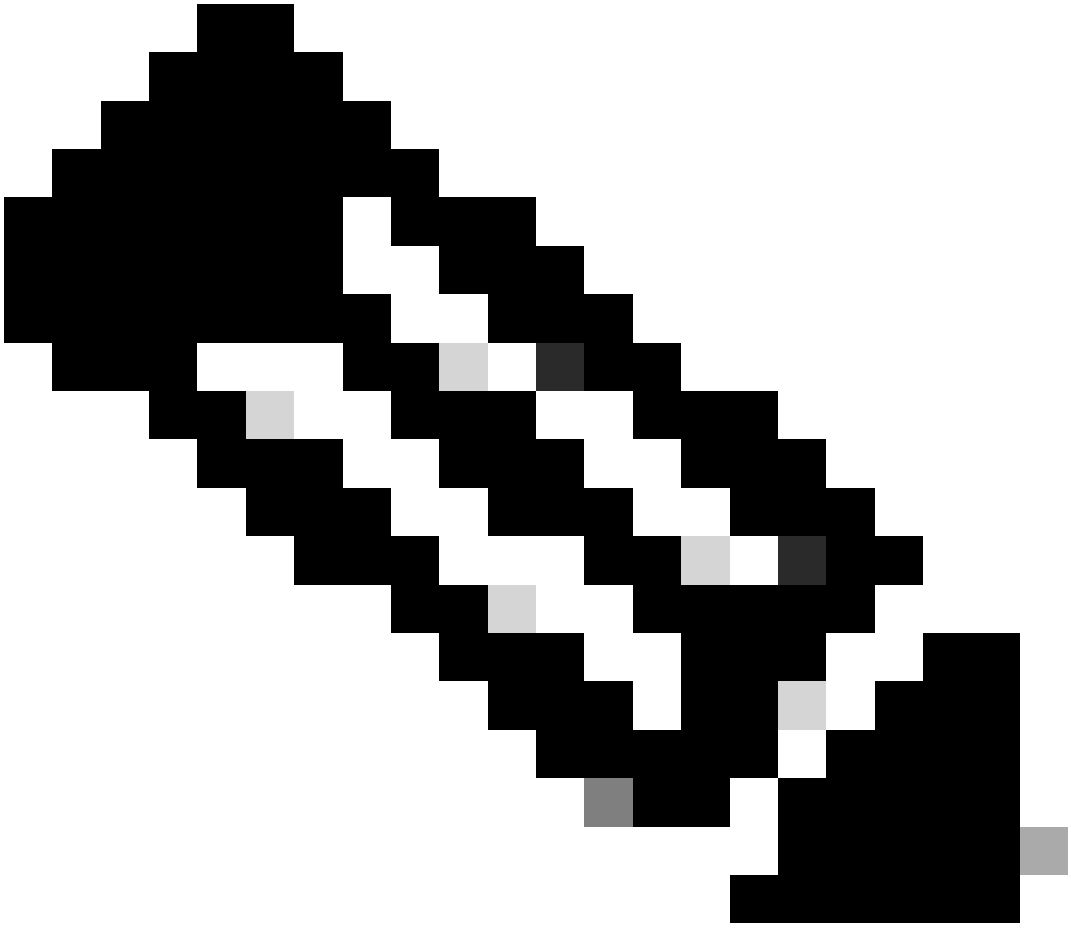
	خريطة التشفير	DMVPN	FlexVPN
التوجيه الديناميكي	لا	نعم	نعم
اتصال مباشر ديناميكي	لا	نعم	نعم
شبكة VPN للوصول عن بعد	نعم	لا	نعم
ضغط التهيئة	لا	لا	نعم
تكوين النظير	لا	لا	نعم
جودة خدمة النظير	لا	نعم	نعم
تكامل خادم AAA	لا	لا	نعم

الرسم التخطيطي للشبكة

تسمح شبكة FlexVPN بإنشاء أنفاق بين الأجهزة، مما يعمل على إنشاء اتصال بين الموزع والأخاديد. كما يتيح إنشاء أنفاق للاتصال المباشر بين الخوادم والاتصال لمستخدمي شبكات VPN للوصول عن بعد، كما هو موضح في الرسم التخطيطي.



الرسم التخطيطي FlexVPN



ملاحظة: لا تتم تغطية تكوين شبكة VPN للوصول عن بعد في هذا الدليل. للحصول على تفاصيل حول تكوينه، ارجع إلى الدليل:

تكوين وحدة الاستقبال والبث FlexVPN للوصول عن بعد لعميل آمن (AnyConnect) IKEv2 باستخدام قاعدة بيانات المستخدم المحلي

التكوين

تتميز شبكة FlexVPN ببساطة تهيئتها. وتتجلى هذه البساطة في كل التكوين المتناسق المستخدم لأنواع مختلفة من شبكات VPN. توفر شبكة FlexVPN كل تكوين مباشرة يمكن تطبيقها بشكل عام، مع عمليات تهيئة إختيارية أو خطوات إضافية متوفرة وفقا للميزات أو المتطلبات المحددة للمخطط:

- اقتراح IKEv2: تعريف الخوارزميات المستخدمة في التفاوض حول اقتران أمان IKEv2 (SA). وبمجرد إنشائه، قم بإرفاق هذا الاقتراح بنهج IKEv2 حتى يتم تحديده أثناء التفاوض.

- نهج IKEv2: يربط المقترح بمثيل التوجيه وإعادة التوجيه الظاهري (VRF) أو عنوان IP المحلي. إرتباط النهج باقتراح IKEv2.

- حلقة مفاتيح IKEv2: يحدد مفاتيح مشتركة مسبقا (PSKs)، والتي يمكن أن تكون غير متماثلة إذا تم إستخدامها لمصادقة النظير.

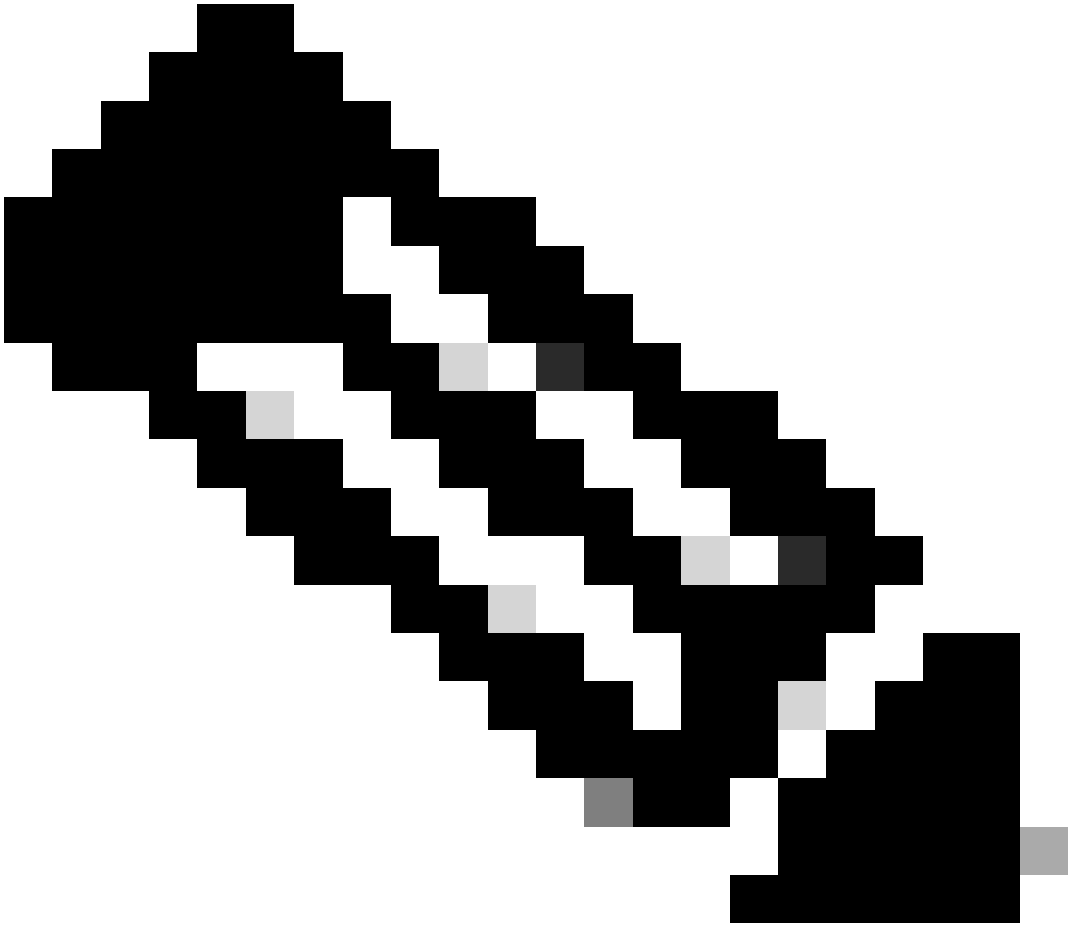
- TrustPoint (إختياري): تكوين سمات مرجع الهوية والشهادة (CA) لمصادقة النظير عند إستخدام البنية الأساسية للمفاتيح العام (PKI) كطريقة مصادقة.

- دمج المصادقة والتفويض والمحاسبة (AAA) (إختياري): تقوم FlexVPN بدمج خوادم AAA، مثل Cisco ISE (Identity Services Engine) أو خوادم RADIUS كطريقة مصادقة.

- ملف تعريف IKEv2: يقوم بتخزين المعلمات غير القابلة للتداول ل IKE SA، مثل عنوان نظير VPN وطرق المصادقة. الا يوجد ملف تعريف IKEv2 افتراضي، لذلك يجب تكوين ملف تعريف وإرفاقه بملف تعريف IPsec على الباديء. في حالة إستخدام مصادقة PSK، يشير ملف تعريف IKEv2 إلى حلقة المفاتيح IKEv2. إذا تم إستخدام طريقة مصادقة PKI أو مصادقة AAA، فإنها تشير إلى هنا.

- مجموعة تحويل IPsec: تحديد مجموعة من الخوارزميات المقبولة ل IPsec SA.

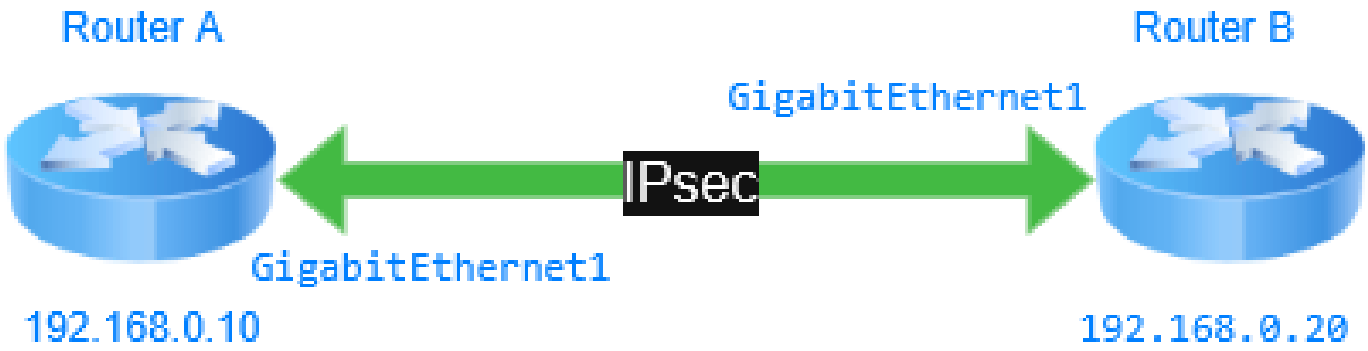
- ملف تعريف IPsec: يقوم بدمج إعدادات FlexVPN في ملف تعريف واحد يمكن تطبيقه على واجهة. يشير ملف التعريف هذا إلى مجموعة تحويل IPsec وملف تعريف IKEv2.



ملاحظة: تستخدم أمثلة التكوين مفاتيح مشتركة مسبقا لتوفير عرض توضيحي مباشر لتكوين FlexVPN وبساطته. بينما يمكن إستخدام مفاتيح مشتركة مسبقا للنشر السهل والمخططات الصغيرة، فإن طرق المصادقة (AAA) وأ PKI تكون أكثر ملاءمة للطرز الأكبر والتفويض والمحاسبة.

تكوين FlexVPN من موقع إلى موقع

تم تصميم مخطط FlexVPN من موقع إلى موقع خصيصا لاتصالات VPN المباشرة بين موقعين. يتم تزويد كل موقع بواجهة نفق تحدد قناة آمنة يمكن لحركة المرور المرور المرور عبرها. يشرح التكوين كيفية إنشاء اتصال VPN مباشر بين موقعين، كما هو موضح في المخطط.



site_to_site_diagram

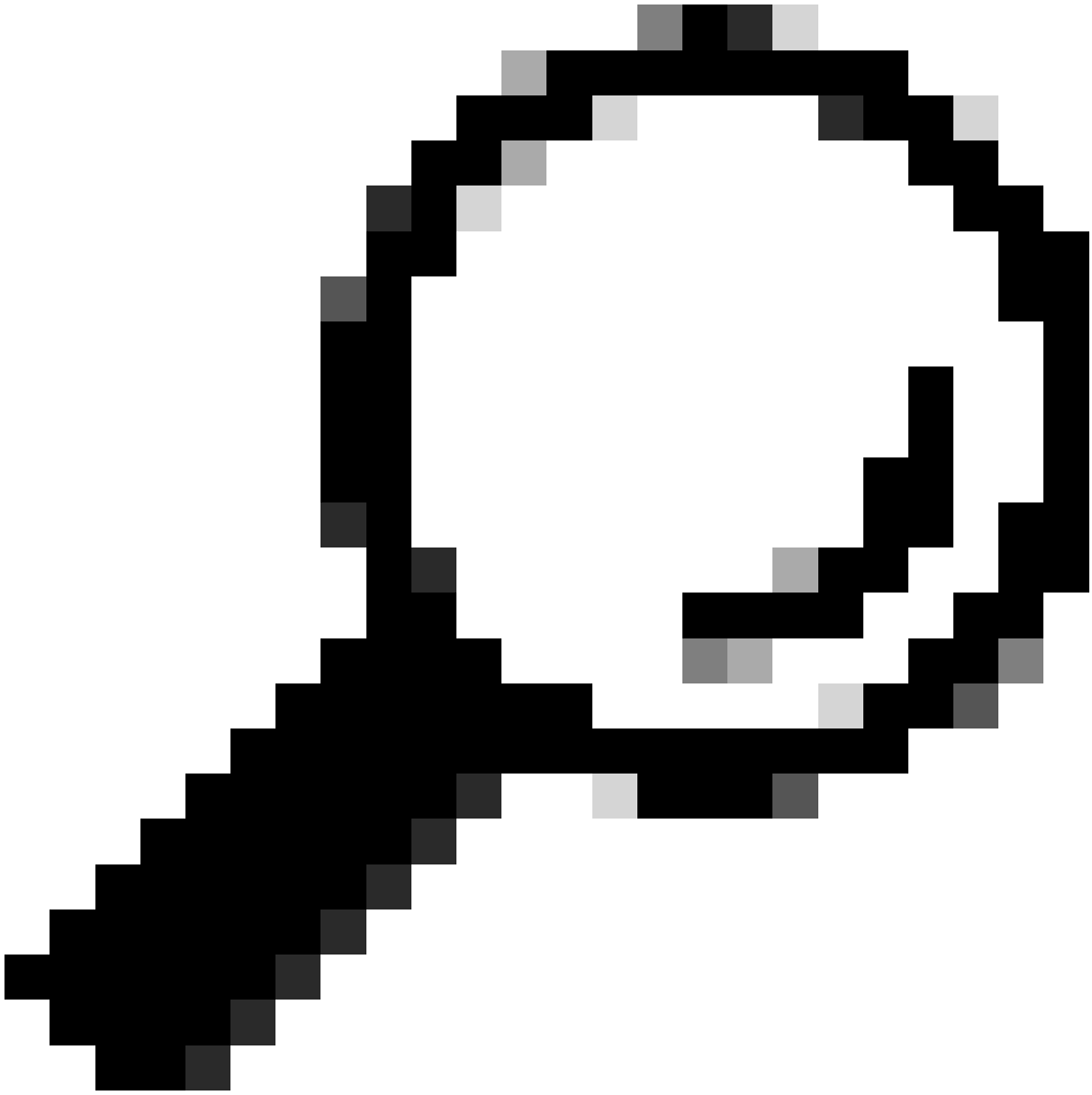
الخطوة 1: تكوين الموجه A

أ. تحديد مقترح وسياسة IKEv2.

ب. قم بتكوين حلقة مفاتيح وأدخل Pre-Shared Key حلقة مفاتيح يتم إستخدامها لمصادقة النظير.

ج. إنشاء IKEv2 profile وتعيين keyring.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.20
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.20
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```



تلميح: تقلل **IKEv2 Smart Defaults** المميزةFlexVPNالتكوين إلى الحد الأدنى من خلال تغطية معظم حالات الاستخدام. يمكنك تخصيص حالات إستخدام **IKEv2 Smart Defaults** معينة، على الرغم من أن Cisco توصي بهذه الممارسة.

د. إنشاء Transport Set وتعريف التشفير وخوارزميات التجزئة المستخدمة لحماية البيانات.

هـ. إنشاء **IPsec profile**.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
```

```
 set ikev2-profile FLEXVPN_PROFILE
!
```

و. قم بتكوين واجهة النفق.

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

ز. قم بتكوين التوجيه الديناميكي للإعلان عن واجهة النفق. بعد ذلك، يمكن أن يعلن عن الشبكات الأخرى التي يجب أن تمر عبر النفق.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

الخطوة 2: تكوين الموجه B

أ. تحديد مقترح وسياسة IKEv2.

ب. قم بتكوين a keyring لخدأو Pre-Shared Key a يتم إستخدامه لمصادقة النظير.

ج. إنشاء IKEv2 profile وتعيين keyring.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.10
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
```

```
match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```

د. إنشاء Transport Set وتعريف التشفير وخوارزميات التجزئة المستخدمة لحماية البيانات.

ه. إنشاء IPsec profile وتعيين ملف تعريف IKEv2 ومجموعة تحويل تم إنشاؤها مسبقا.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

و. قم بتكوين Tunnel interface.

```
!
interface Tunnel0
 ip address 10.1.120.20 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!
```

ز. قم بتكوين التوجيه الديناميكي للإعلان عن واجهة النفق. بعد ذلك، يمكن أن يعلن عن الشبكات الأخرى التي يجب أن تمر عبر النفق.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

التحقق من الصحة

- أستخدم الأمر show ip interface brief لمراجعة حالة واجهة النفق والتحقق من أن النفق

في حالة up/up.

<#root>

RouterB#

show ip interface brief

```
Interface              IP-Address      OK?   Method    Status   Protocol
GigabitEthernet1       192.168.0.20    YES   NVRAM     up       up
Tunnel0                10.1.120.11     YES   manual
```

up

up

1. أستخدم الأمر show crypto ikev2 sa لتأكيد إنشاء الاتصال الآمن بين الموجهات.

<#root>

RouterB#

show crypto ikev2 sa

```
IPv4 Crypto IKEv2 SA

Tunnel-id  Local                Remote               fvrf/ivrf   Status
2          192.168.0.20/500     192.168.0.10/500     none/none
```

READY

```
    Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

Life/Active Time: 86400/3139 sec

```
IPv6 Crypto IKEv2 SA
```

- أستخدم الأمر show crypto ipSec لتأكيد تشفير حركة مرور البيانات ومرورها عبر النفق عن طريق التحقق من زيادة عدادات عمليات التضمين وقطع الاتصال.

<#root>

RouterB#

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20
```

```
   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   current_peer 192.168.0.10 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669




#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

      local crypto endpt.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
      current outbound spi: 0x93DCB8AE(2480715950)
      PFS (Y/N): N, DH group: none

      inbound esp sas:


spi: 0x89C141EB(2311143915)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607913/520)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0x93DCB8AE(2480715950)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607991/3137)
```

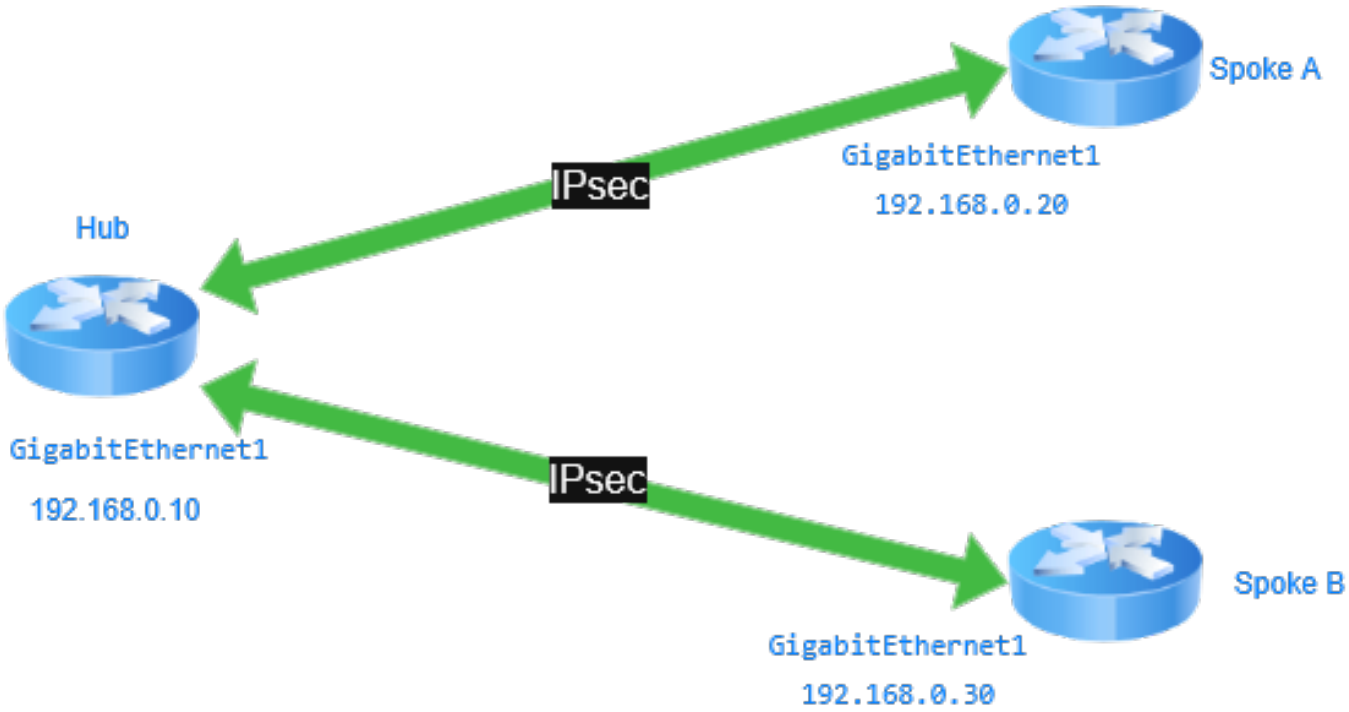
```
        IV size: 16 bytes
        replay detection support: Y

Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- أستخدم الأمر show ip eigrp neighbors لتأكيد إنشاء تجاور EIGRP مع الموقع الآخر.

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold  Uptime     SRTT    RTO    Q   Seq
                                                   (sec)            (ms)          Cnt  Num
0   10.1.120.10             Tu0                     13   00:51:26    3      1470   0   2
```

FlexVPN بتقنية Hub-and-Talk

في مخطط hub-and-talk، تتصل موجهات متعددة متكلمة بموجه مركز مركزي. هذا التكوين مثالي للسيناريوهات التي تتصل فيها الخوادم الفرعية أساسا بالموجه. في شبكة FlexVPN، يمكن تكوين الأنفاق الديناميكية لتحسين كفاءة الاتصال. يوظف الموزع توجيه IKEv2 لتوزيع المسارات إلى الموجهات المحكية، مما يضمن اتصال سلس. وكما تم الإشارة إليه في المخطط، يشرح التكوين اتصال VPN بين Hub و Talk وكيف يتم تكوين الموزع لإنشاء اتصال ديناميكي مع جبهات متعددة، كما أنه قادر على إضافة المزيد من الفروع.



الرسم التخطيطي ل Hub_and_TALK_Diagram

الخطوة 1: تكوين الموزع

أ. تحديد مقترح وسياسة IKEv2.

ب. قم بتكوين a keyring وأدخل Pre-Shared Key a يتم إستخدامه لمصادقة الفروع.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. قم بتمكين خدمات AAA على موجه الصرة، ثم حدد قائمة تفويض الشبكة المسماةFlexAuthالتي تحدد السياسات من تكوين الجهاز المحلي.

```
!
aaa new-model
```

```
 aaa authorization network FlexAuth local
!
```

د. قم بتحديد IP address pool عنوان FlexPool مسمى، يحتوي على العناوين 10.1.1.2 إلى 10.1.1.254. يتم إستخدام هذا التجمع لتعيين عنوان IP تلقائي إلى واجهة النفق الخاصة بالقنوات.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

هـ. حدد قائمة وصول IP قياسية يتم تسميتها FlexTraffic وتسمح للشبكة 10.10.1.0/24. تحدد قائمة التحكم في الوصول هذه الشبكات التي يتم دفعها إلى جهات FlexVPN للوصول إليها عبر النفق.

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

تتم الإشارة إلى قائمة الوصول وتجمع عناوين IP في **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

و. قم بإنشاء IKEv2 profile مجموعة تخيل keyring و AAA وتعيينها.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

ز. إنشاء Transport Set، تعريف التشفير وخوارزميات التجزئة المستخدمة لحماية البيانات.

ح. قم بإنشاء IPsec profile، وتعيين IKEv2 profile ام تم إنشاؤه Transport Set مسبقا.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

ط. قم بتكوين **virtual-template 1** as **type tunnel**. مرجع الواجهةIP unnumbered addressك وتطبيق **IPsec profile**

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

الخطوة 2: التكوين الذي تم التحدث به

أ. تحديد مقترح وسياسة IKEv2.

ب. قم بتكوين حلقة مفاتيح وأدخل مفاتيح مشترك مسبقا يتم إستخدامه للمصادقة على الموزع.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. قم بتمكين خدمات AAA على مجموعة الصرة، ثم حدد قائمة تفويض الشبكة المسماة **FlexAuth** التي تحدد السياسات من تكوين الجهاز المحلي. بعد ذلك، قم بتكوين سياسة تكوين الوضع لدفع عنوان IP والمسارات إلى الفروع FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

د. حدد قائمة وصول IP قياسية التي يتم تسميتها **FlexTraffic** وتسمح للشبكة 10.20.2.0/24. تحدد قائمة التحكم في الوصول (ACL) هذه الشبكات التي تتم مشاركتها بواسطة هذا التحديث لتمر عبر النفق.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

يتم تعيين قائمة الوصول في **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

ه. إنشاء IKEv2 profileمجموعة تخيل keyring و AAA وتعيينها.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
!
```

و. إنشاء مجموعة نقل وتحديد التشفير وخوارزميات التجزئة المستخدمة لحماية البيانات.

g. إنشاء ملف تعريف IPsec، وتعيين ملف تعريف IKEv2 ومجموعة النقل التي تم إنشاؤها مسبقا.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

ح. شكلت النفق قارن مع خاصية من تفاوض عنوان، أي يكون نلت من التجمع أن وه يشكل على الصرة.

```
!
interface tunnel 0
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

التحقق من الصحة

أستخدم الأمر show ip interface brief لمراجعة الوضع Tunnel والقالب الظاهري والوصول الظاهري:

- على لوحة الوصل، يحتوي القالب الظاهري على حالة للأعلى/للأسفل وهي عادية. خلقت Virtual-Access ل كل Talk أن يؤسس توصيل مع الصرة ويبدي حالة up/up.
- على ال Talk، إستلمت قارن النفق عنوان ويبدي up/up وضع.

<#root>

```
FlexVPN_HUB#
```

show ip interface brief

```
Interface              IP-Address      OK? Method Status           Protocol
GigabitEthernet1       192.168.0.10    YES NVRAM  up               up
GigabitEthernet2       10.10.1.10      YES manual up               up
Loopback1              10.1.1.1        YES manual up               up

Virtual-Access1        10.1.1.1        YES unset  up               up

 <<<<<<< This Virtual-Access has been created and is up/up
Virtual-Template1      10.1.1.1        YES unset  up
```

```
FlexVPN_Spoke#
show ip interface brief
Interface              IP-Address      OK? Method  Status            Protocol
GigabitEthernet1       192.168.0.20    YES NVRAM   up                up
GigabitEthernet2       10.20.2.20      YES manual  up                up
Tunnel0                10.1.1.8        YES manual  up                up <<<<<<
The tunnel interface received an IP address from pool defined
```

- أستخدم الأمر show crypto ikev2 sa لتأكيد إنشاء الاتصال الآمن بين الصرة والمتكلم.

<#root>

```
FlexVPN_HUB#
show crypto ikev2 sa
 IPv4 Crypto IKEv2 SA
Tunnel-id Local                 Remote                fvrf/ivrf                Status
1         192.168.0.10/500      192.168.0.20/500      none/none
READY
 Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
 Life/Active Time: 86400/587 sec
 IPv6 Crypto IKEv2 SA
```

- أستخدم الأمر show crypto ipSec لتأكيد تشفير حركة مرور البيانات ومروراه عبر النفق عن طريق التحقق من زيادة عدادات عمليات التضمين وقطع الاتصال.

<#root>

```
FlexVPN_HUB#
show crypto ipsec sa
interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10
   protected vrf: (none)
```

```
   local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   current_peer 192.168.0.20 port 500
     PERMIT, flags={origin_is_acl,}

    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10



    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xAFC2F841(2948790337)
     PFS (Y/N): N, DH group: none

     inbound esp sas:


spi: 0x7E780336(2121794358)


        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h


sa timing: remaining key lifetime (k/sec): (4607998/3010)


        IV size: 16 bytes
        replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0xAFC2F841(2948790337)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-


sa timing: remaining key lifetime (k/sec): (4607998/3010)


         IV size: 16 bytes
         replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- أستخدم الأمر show ip route للتحقق من دفع المسارات إلى الخوادم:
  - تم دفع المسار ل 10.1.1.1/32 عبر حموالات تكوين IKEv2 بسبب بيان واجهة مجموعة المسارات في تكوين الصرة.
  - تم دفع المسار ل 10.10.1.0/24 عبر حموالات تكوين IKEv2 بسبب بيان FlexTraffic لمجموعة المسارات في تكوين الصرة.

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.1.1.1/32 is directly connected, Tunnel0   <<<<<<<


C        10.1.1.8/32 is directly connected, Tunnel0
S        10.10.1.0/24 is directly connected, Tunnel0  <<<<<<<


C        10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.20/32 is directly connected, GigabitEthernet1
```

- أستخدم الأمر ping للتحقق من الاتصال بالشبكات المعلن عنها.

<#root>

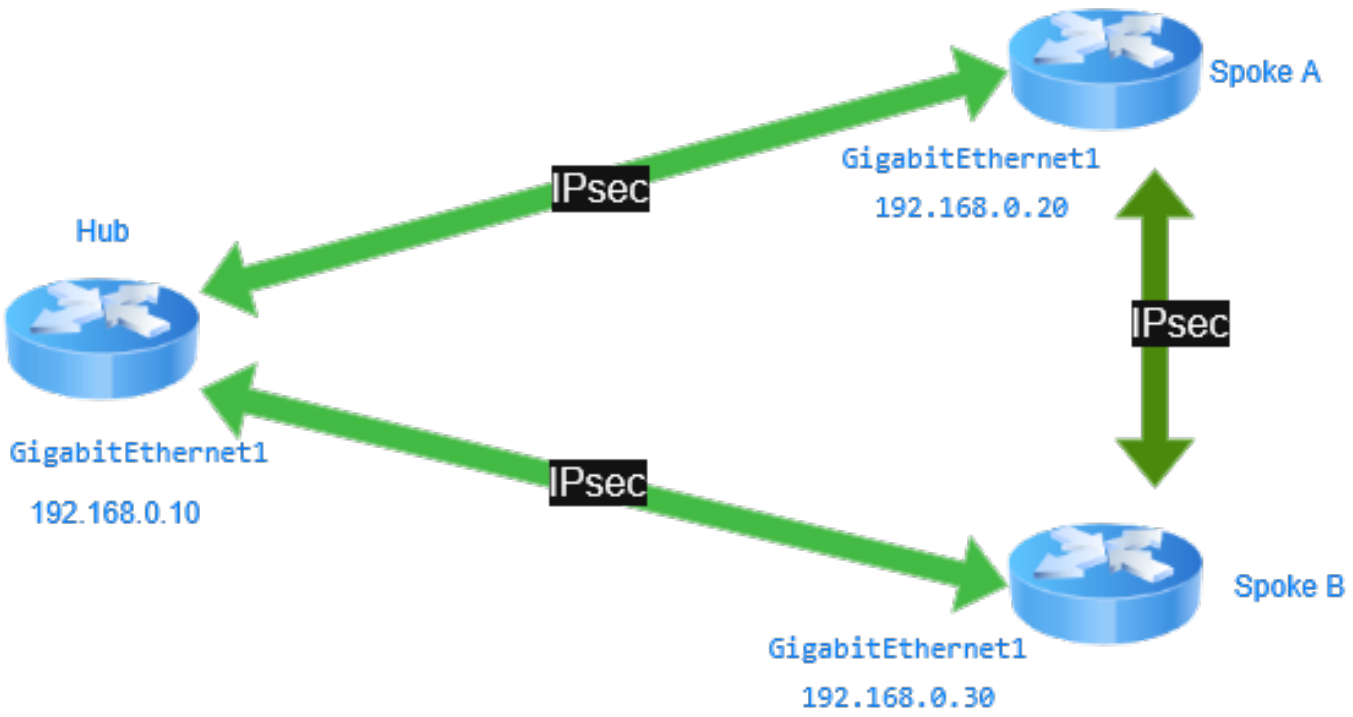
```
FlexVPN_HUB#
ping 10.20.2.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
FlexVPN_Spoke#

ping 10.10.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

تحدث إلى FlexVPN الذي يتحدث

تعمل شبكة FlexVPN في شبكة محورية وتوصيفية ذات تقنية Talk (الاتصال بالكلام) على تمكين الاتصال الديناميكي والقابل للتوطير والآمن للشبكة الخاصة الظاهرية (VPN). ويعمل الصرة كنقطة تحكم مركزية حيث يسمح NHRP للكلمات بالاستعلام عن الصرة لعناوين IP أخرى، مما يتيح محادثة مباشرة عبر أنفاق IPsec للتواصل الفعال وتقليل التأخير.

على الصرة، استعملت الألمر **ip nhrp redirect** أن يخطر ان قل مباشرة إلى محادثة إمكانية، تحسين تدفق حركة المرور بتجاوز الصرة لحركة مرور مستوى البيانات. على الأصداف، تسمح له **ip nhrp shortcut** القيادة بتهيئة أنفاق مباشرة بشكل ديناميكي مع الأخاديد الأخرى بعد تلقي إعادة التوجيه من الصرة. يشير الرسم التخطيطي إلى حركة المرور بين المركز والتحدث، ويتحدث إلى محادثة.



_talk_talk_diagram

الخطوة 1: تكوين الموزع

أ. تعريف سياسات IKEv2 ومقترحاتها.

ب. قم بتكوين a keyring لخدأو Pre-Shared Key a يتم إستخدامه لمصادقة الفرع.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. قم بتمكين خدمات AAA على موجه الموزع، ثم حدد قائمة تفويض الشبكة المسماة **FlexAuth** التي تحدد السياسات من تكوين الجهاز المحلي، ثم قم بتكوين سياسة تكوين الوضع لدفع عنوان IP والمسارات إلى الفرع FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

د. قم بتحديدIP address poolعنوان مسمى **FlexPool**, يحتوي على العناوين 10.1.1.2 حتى 10.1.1.254. يتم إستخدام هذا التجمع لتعيين عنوان IP تلقائيا إلى واجهة النفق الخاصة بالقناة.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

هـ. قم بتحديد قائمة وصول IP القياسية التي تم تسميتهاFlexTrafficوالسماح للشبكة (ACL) هذه الشبكات التي يتم دفعها إلى الفرع الأخر المتصلة بالموجه، لذلك شبكات FlexVPN، بما في ذلك الشبكات الخاصة بالفرع الأخر المتصلة بالموجه، لذلك تعرف المحولات أنه يتم الوصول إلى هذه الشبكات من خلال الموزع الأول.

```
!
ip access-list standard FlexTraffic
 permit 10.0.0.0 0.255.255.255
```

```
!
```

قائمة الوصول و يتم IP address pool تعيينها في **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

و. إنشاء IKEv2 profileمجموعة تخويل keyring و AAA و تعيينها.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

ز. إنشاء Transport Set وتعريف التشفير وخوارزميات التجزئة المستخدمة لحماية البيانات.

ح. إنشاء IPsec profile، تعيين IKEv2 profile و Transport Set إنشاء سابق.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

ط. قم بتكوين **virtual-template 1** as **type tunnel**. راجع الواجهة كواجهة **IP unnumbered address** وقم بتطبيق **IPsec profile**.

يتم تكوين الأمر على **ip nhrp redirect** القالب الظاهري إلعالم الخوادم بإنشاء اتصال مباشر مع الفروع الأخرى للوصول إلى شبكاتها.

```
!
```

```
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

الخطوة 2: تحدث عن تكوين

أ. تعريف سياسات IKEv2 ومقترحاتها.

ب. قم بتكوين a keyring لخدأو Pre-Shared Key a يتم إستخدامه لمصادقة الفروع.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. قم بتمكين خدمات AAA على موجه الصرة، ثم حدد قائمة تفويض الشبكة المسماة **FlexAuth** التي تحدد السياسات من تكوين الجهاز المحلي. بعد ذلك، قم بتكوين سياسة تكوين الوضع لدفع عنوان IP والمسارات إلى الفروع FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

د. حدد قائمة وصول IP قياسية التي يتم تسميتها **FlexTraffic** وتسمح للشبكة 10.20.2.0/24. تحدد قائمة التحكم في الوصول هذه الشبكات التي تتم مشاركتها بواسطة هذا المقطع لتمر عبر النفق.

```
!
ip access-list standard FlexTraffic
```

```
 permit 10.20.2.0 0.0.0.255
!
```

يتم تعيين قائمة الوصول في **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

ه. إنشاء IKEv2 profileمجموعة تخويل keyring و AAA وتعيينها.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

و. إنشاء Transport Set وتعريف التشفير وخوارزميات التجزئة المستخدمة لحماية البيانات.

g. إنشاء ملف تعريف IPsec، وتعيين ملف تعريف IKEv2 ومجموعة النقل التي تم إنشاؤها مسبقا.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

ح. قم بتكوين الواجهة tunnelinterface والقالب الظاهري. حدد **Virtual-Template1** VTIs التي تم إنشاؤها لدعم **NHRP shortcuts**. أيضا، ضبطtunnel0كعنوان غير مرقم علىvirtual-template.

يتم تكوين الأمر **ip nhrp shortcut** على المحولات لتمكينها من إنشاء أنفاق مباشرة بشكل ديناميكي إلى المحولات الأخرى استنادا إلى رسائل إعادة توجيه NHRP من المصدر.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

الخطوة 3: تحدث في التكوين B

أ. تعريف سياسات IKEv2 ومقترحاتها.

ب. قم بتكوين a keyring لأدخل Pre-Shared Key a يتم إستخدامه لمصادقة الفروع.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. قم بتمكين خدمات AAA على موجه الموزع، ثم حدد قائمة تفويض الشبكة المسماة **FlexAuth** التي تحدد السياسات من تكوين الجهاز المحلي، ثم قم بتكوين سياسة تكوين الوضع لدفع عنوان IP والمسارات إلى الفروع FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

د. قم بتحديد قائمة وصول IP الخاصة بالإسكندرية التي يتم تسميتها **FlexTraffic** والسماح للشبكة 10.30.3.0/24. تحدد قائمة التحكم في الوصول (ACL) هذه الشبكات التي تتم مشاركتها بواسطة هذا المقطع لتمر عبر النفق.

```
!
ip access-list standard FlexTraffic
 permit 10.30.3.0 0.0.0.255
!
```

تتم الإشارة إلى قائمة الوصول في IKEv2 Authorization Policy.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

ه. إنشاء IKEv2 profile مجموعة تخويل keyring و AAA وتعييناها.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

و. إنشاء Transport Set وتعريف التشفير وخوارزميات التجزئة المستخدمة لحماية البيانات.

g. إنشاء IPsec profile وتعيين IKEv2 profile أو Transport Set إنشاء سابق.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

ح. قم بتكوين tunnel interface AND virtual template. حدد **Virtual-Template1** ل dVTIs أن يكون خلقت أن يسان دNHRP shortcuts. أيضا، ضبطtunnel0كعنوان غير مرقم علىvirtual-template.

يتم تكوين الأمر **ip nhrp shortcut** على المحولات لتمكينها من إنشاء أنفاق مباشرة بشكل ديناميكي إلى المحولات الأخرى استنادا إلى رسائل إعادة توجيه NHRP من المصدر.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

التحقق من الصحة

أستخدم الأمر show ip interface brief لمراجعة الوضع Tunnel والقالب الظاهري والوصول الظاهري. والآن، هناك اتصال مباشر بالخطوة:

- على المحولات، يحتوي القالب الظاهري على حالة أعلى/أسفل وهي عادية. يتم إنشاء "الوصول الظاهري" للاتصال في حالة up/up.

<#root>

FlexVPN_Spoke#

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1	192.168.0.30	YES	NVRAM	up	up
GigabitEthernet2	10.20.2.20	YES	manual	up	up
Tunnel0	**10.1.1.12**	**YES**	**manual**	**up**	**up**
Virtual-Access1	**10.1.1.12**	**YES**	**unset**	**up**	**up**
Virtual-Template1	10.1.1.12	YES	unset	up	down

- أستخدم الأمر show crypto ikev2 sa لتأكيد إنشاء الاتصال الآمن بين كل جهاز.
- أستخدم الأمر show crypto ipSec لتأكيد تشفير حركة مرور البيانات ومرورها عبر النفق عن طريق التحقق من زيادة عدادات عمليات التضمين وقطع الاتصال.
- أستخدم الأمر show ip nhrp للتحقق من إعادة توجيه حركة المرور بين الفروع.

```
<#root>

FlexVPN_Spoke#

show ip nhrp


10.1.1.10/32 via 10.1.1.10
   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:

dynamic

, Flags: router nhop rib nho
   NBMA address: 192.168.0.30

10.30.3.0/24 via 10.1.1.10


   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:

dynamic

, Flags: router rib nho
   NBMA address: 192.168.0.30
```

أستخدم الأمر show ip route للتحقق من دفع المسارات إلى المحادثة:

- ويقترن المساران بواجهة Virtual-Access1 بطريقين جديدين ويرتبطان باختصارات NHRP.
- يشير الحرف ٪ إلى تجاوز الخطوة التالية.

```
<#root>

FlexVPN_Spoke#sh ip route
<<<< Omitted >>>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Tunnel0
S        10.1.1.1/32 is directly connected, Tunnel0

S  %     10.1.1.10/32 is directly connected, Virtual-Access1


C        10.1.1.12/32 is directly connected, Tunnel0
C        10.20.2.20/32 is directly connected, GigabitEthernet2

S  %     10.30.3.0/24 is directly connected, Virtual-Access1


      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.30/32 is directly connected, GigabitEthernet1
```

- أستخدم الأمر ping للتحقق من الاتصال بالشبكات المعلن عنها.

```
<#root>

FlexVPN_Spoke#

ping 10.30.3.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. أستخدم هذه الأوامر لتصحيح أخطاء عملية تفاوض النفق:

```
debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states
```

يمكن أن تساعد عمليات تصحيح أخطاء NHRP في أستكشاف أخطاء الاتصالات التي يتم التحدث بها وإصلاحها.

```
debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing
```

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).