تكوين IKEv2 على موجه من السلسلة RV34x

الهدف من هذا المستند هو توضيح كيفية تكوين ملف تعريف IPsec باستخدام IKEv2 على موجهات سلسلة RV34x.

والآن يدعم الإصدار 1.0.02.16 من البرنامج الثابت لموجهات سلسلة RV34x الإصدار 2 من تبادل مفتاح الإنترنت (IKEv2) للشبكة الخاصة الظاهرية (VPN) من موقع إلى موقع والشبكة الخاصة الظاهرية (VPN) من عميل إلى موقع. IKE هو بروتوكول هجين يقوم بتنفيذ تبادل مفاتيح Oakley وتبادل مفاتيح Skeme داخل إطار عمل رابطة أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP). يوفر IKE مصادقة أقران IPsec، ويفاوض مفاتيح IPsec، ويتفاوض على اقترانات أمان IPsec.

لا يزال IKEv2 يستخدم منفذ UDP 500، ولكن هناك بعض التغييرات التي تريد ملاحظتها. تتم إدارة ميزة "اكتشاف النظير غير الهام" (DPD) بشكل مختلف، وهي الآن مدمجة. يتم تقليل تفاوض اقتران الأمان (SA) إلى 4 رسائل كحد أدنى. كما يدعم هذا التحديث الجديد مصادقة بروتوكول المصادقة المتوسع (EAP) الذي أصبح الآن قادرا على الاستفادة من خادم AAA وحماية رفض الخدمة.

يوضح الجدول التالي بشكل أكبر الاختلافات بين IKEv1 و IKEv2

IKEv1	IKEv2
تفاوض المرحلة الثانية (الوضع الرئيسي مقابل الوضع القوي)	تفاوض SA أحادي المرحلة (مبسط)
	دعم الشهادات المحلية/البعيدة
	تحسين التعامل مع التصادم
	ميكانيكا إعادة التشكيل المحسنة
	NAT Traversal مدمج
	دعم EAP لخوادم AAA

يضمن IPsec توفر اتصال خاص آمن لديك عبر الإنترنت. وهو يعطي مضيفين أو أكثر الخصوصية، النزاهة، والأصالة لنقل المعلومات الحساسة عبر الإنترنت. يتم إستخدام IPsec بشكل شائع في الشبكة الخاصة الظاهرية (VPN) ويتم تنفيذه في طبقة IP التي تساعد في إضافة الأمان إلى العديد من التطبيقات غير الآمنة. يتم إستخدام شبكة VPN لتوفير آلية اتصال آمنة للبيانات الحساسة ومعلومات IP التي يتم إرسالها من خلال شبكة غير آمنة مثل الإنترنت. كما يوفر حلا مرنا للمستخدمين عن بعد والمؤسسة لحماية أي معلومات حساسة من الأطراف الأخرى على الشبكة نفسها.

لكي يتم تشفير طرفي نفق VPN وتكوينه بنجاح، يحتاج كلا منهما إلى الموافقة على طرق التشفير وفك التشفير والمصادقة. يعد ملف تعريف IPsec هو التكوين المركزي في IPsec الذي يحدد الخوارزميات مثل التشفير والمصادقة ومجموعة Diffie-Hellman (DH) للتفاوض من المرحلتين الأولى والثانية في الوضع التلقائي بالإضافة إلى وضع الحفظ اليدوي. تحدد المرحلة الأولى المفاتيح المشتركة مسبقا لإنشاء اتصال آمن مصدق. المرحلة الثانية هي التي يتم فيها تشفير حركة المرور. يمكنك تكوين معظم معلمات IPsec مثل البروتوكول (حمولة أمان التضمين (ESP))، ورأس المصادقة (AH)، والوضع (النفق، النقل)، والخوارزميات (التشفير، التكامل، Diffie-Hellman)، والسرية التامة لإعادة التوجيه (PFS)، ودورة حياة SA، وبروتوكول إدارة المفاتيح (تبادل مفتاح الإنترنت (IKEv1 - IKE) و IKEv2).

يمكن العثور على معلومات إضافية حول تقنية IPsec من Cisco في هذا الارتباط: مقدمة عن تقنية Cisco IPSec.

من المهم ملاحظة أنه عند تكوين شبكة VPN من موقع إلى موقع، يتطلب الموجه البعيد تكوين ملف تعريف IPsec نفسه الذي يتطلبه الموجه المحلي لديك.

فيما يلي جدول لتكوين كل من الموجه المحلي والموجه البعيد. في هذا المستند، سنقوم بتكوين الموجه المحلي باستخدام الموجه A.

الحقول	الموجه المحلي (الموجه A)	الموجه عن بعد (الموجه B)
اسم ملف التعريف	الداخلية	RemoteOffice
وضع الحفظ	تلقائي	تلقائي
إصدار IKE	IKEv2	IKEv2
خيارات المرحلة الأولى	**خيارات المرحلة الأولى**	**خيارات المرحلة الأولى**
مجموعة DH	المجموعة 2 - 1024 بت	المجموعة 2 - 1024 بت
تشفير	إيه إس-192	إيه إس-192
المصادقة	SHA2-256	SHA2-256
مدة البقاء	28800	28800
خيارات المرحلة الثانية	**خيارات المرحلة الثانية**	**خيارات المرحلة الثانية**
تحديد البروتوكول	ESP	ESP
تشفير	إيه إس-192	إيه إس-192
المصادقة	SHA2-256	SHA2-256
مدة البقاء	3600	3600
سرية إعادة التوجيه المثالية	ممكن	ممكن
مجموعة DH	المجموعة 2 - 1024 بت	المجموعة 2 - 1024 بت

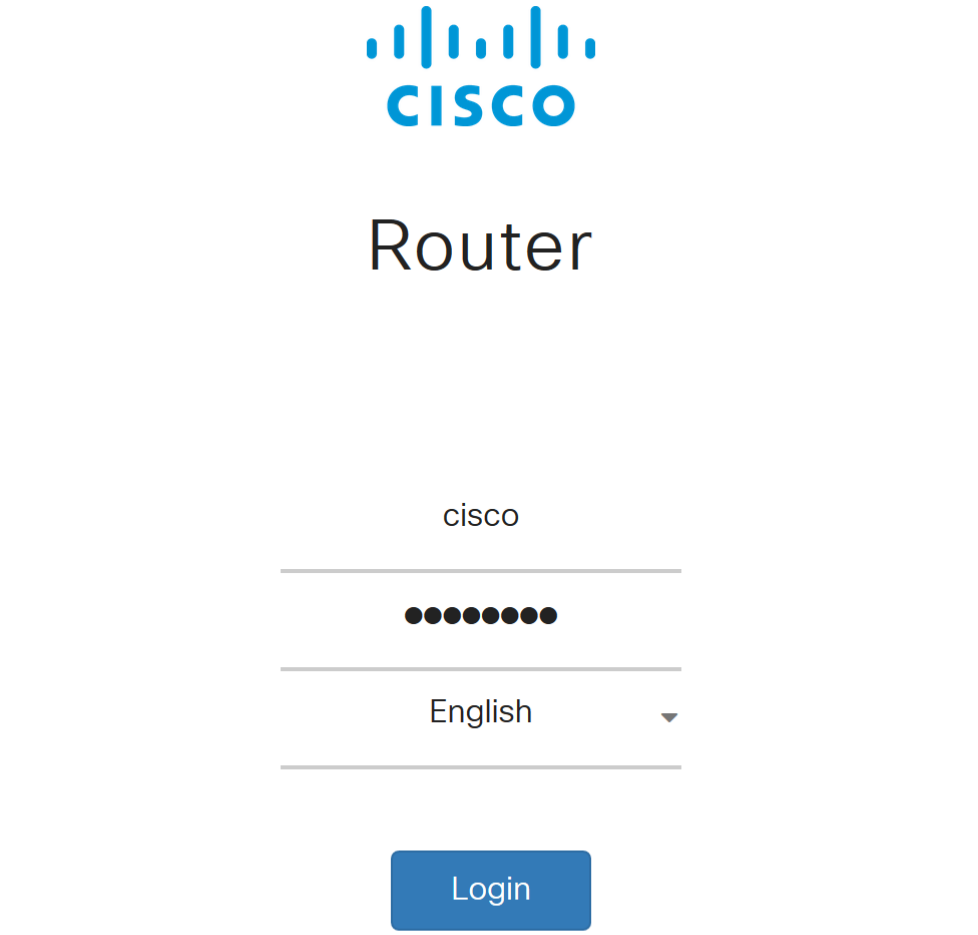
لمعرفة كيفية تكوين شبكة VPN من موقع إلى موقع على RV34x، انقر فوق الارتباط: تكوين شبكة VPN من موقع إلى موقع على RV34x.

- الطراز RV34x

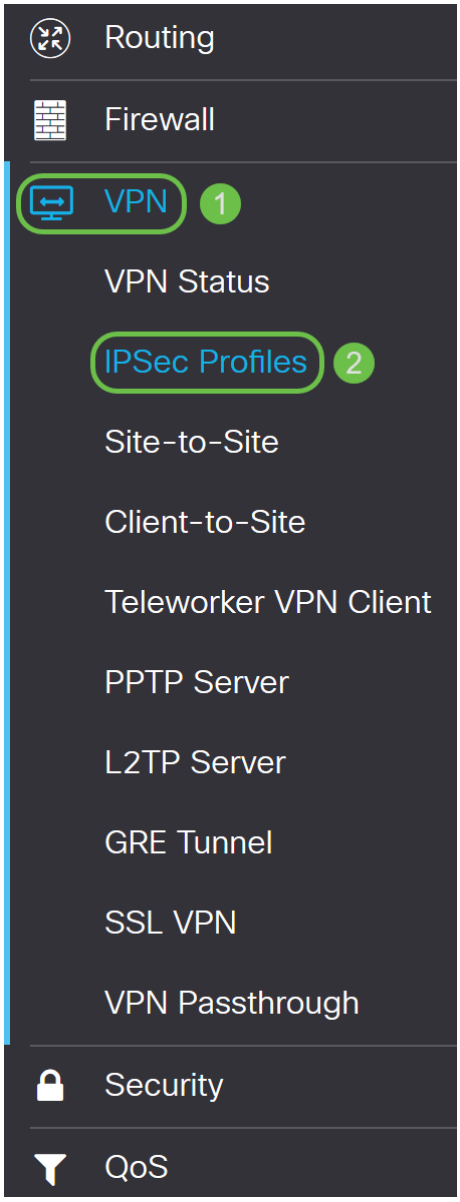
1.0.02.16•

IKEv2 IPsec

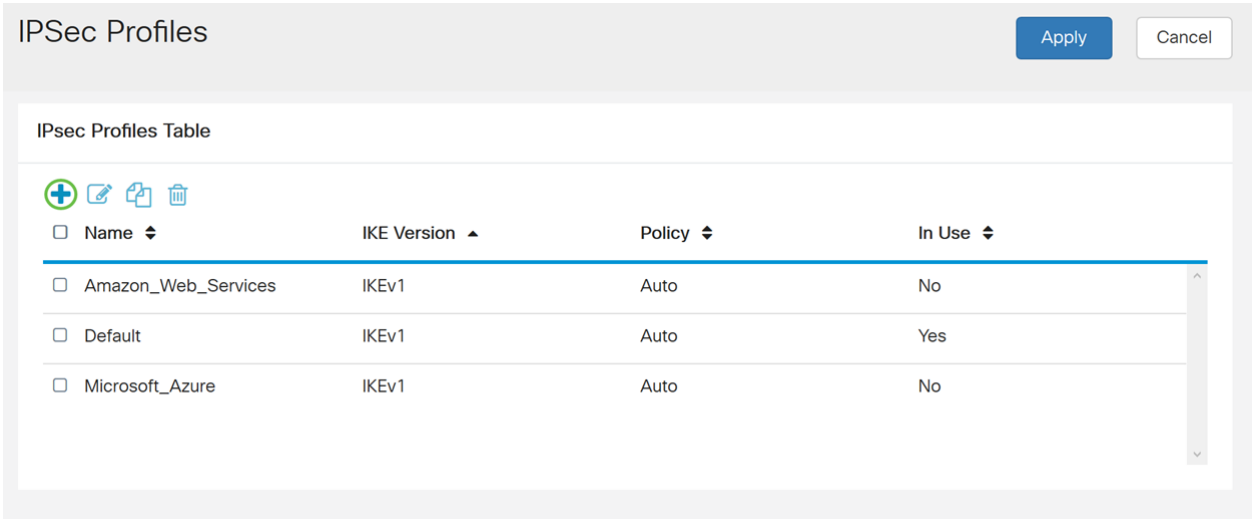
الخطوة 1. سجل الدخول إلى صفحة تكوين الويب الخاصة بالموجه المحلي لديك (الموجه A).



الخطوة 2. انتقل إلى **VPN > توصيفات IPSec**.



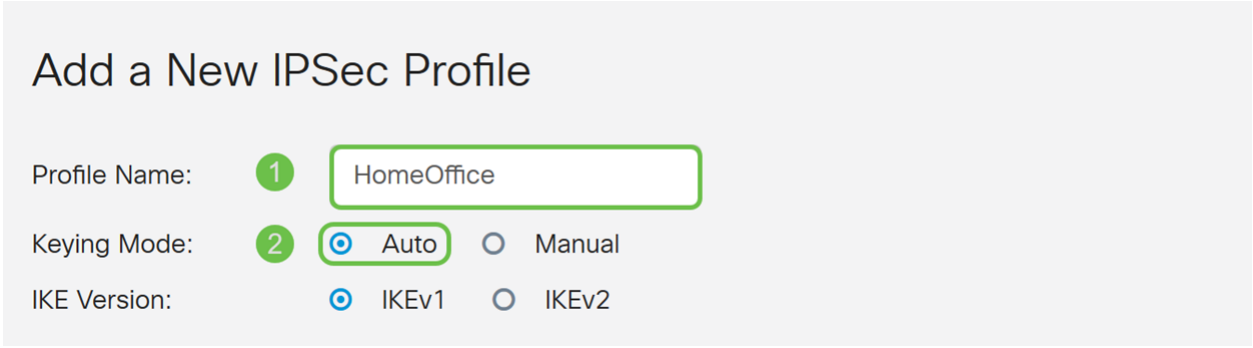
الخطوة 3. في جدول *توصيفات IPSec*، انقر على **إضافة** لإنشاء توصيف IPsec جديد. هناك أيضا خيارات لتحرير، حذف، أو نسخ ملف تخصيص. يسمح لك نسخ توصيف بمضاعفة توصيف موجود بالفعل في *جدول توصيفات IPsec* بسرعة. إذا احتجت في أي وقت إلى إنشاء توصيفات متعددة بنفس التكوين، فإن الاستنساخ سيوفر عليك بعض الوقت.



الخطوة 4. أدخل اسم ملف تخصيص وحدد وضع الكي (تلقائي أو يدوي). لا يجب أن يتطابق اسم ملف التعريف مع الموجه الآخر الخاص بك ولكن يجب أن يتطابق وضع الكي.

تم إدخال **HomeOffice** كاسم *ملف التعريف*.

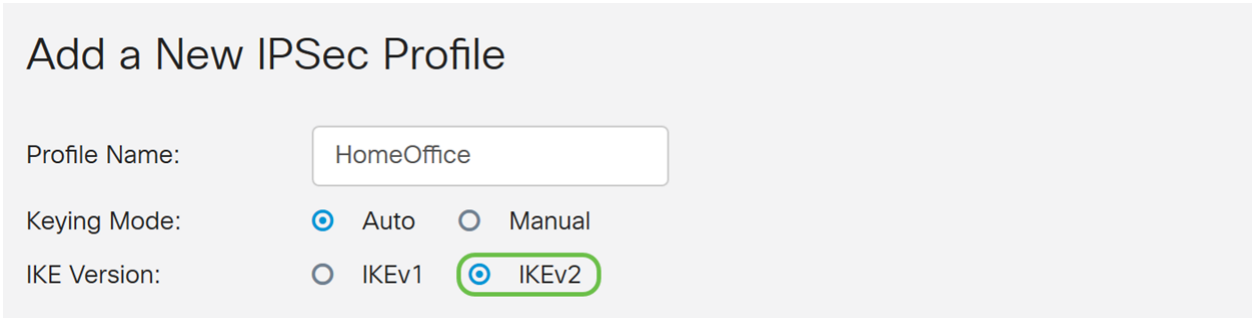
يتم تحديد **تلقائي** *لوضع* الربط.



الخطوة 5. أختر **IKEv1** أو **IKEv2** ليكون *إصدار IKE* الخاص بك. IKE هو بروتوكول مختلط يطبق تبادل مفاتيح Oakley وتبادل مفاتيح Skeme داخل إطار عمل ISAKMP. يحدد كل من أوكلي وسكيمي كيفية الحصول على مواد تثبيت المفاتيح المصدق عليها، ولكن برنامج سكامي يتضمن أيضا إنعاش سريع للمفتاح. يعد IKEv2 أكثر فعالية لأنه يحتاج إلى حزم أقل لإجراء عمليات تبادل المفاتيح، ويدعم المزيد من خيارات المصادقة، بينما يقوم IKEv1 فقط بالمصادقة المستندة إلى المفاتيح المشتركة والشهادات.

في هذا المثال، تم تحديد **IKEv2** كإصدار IKE.

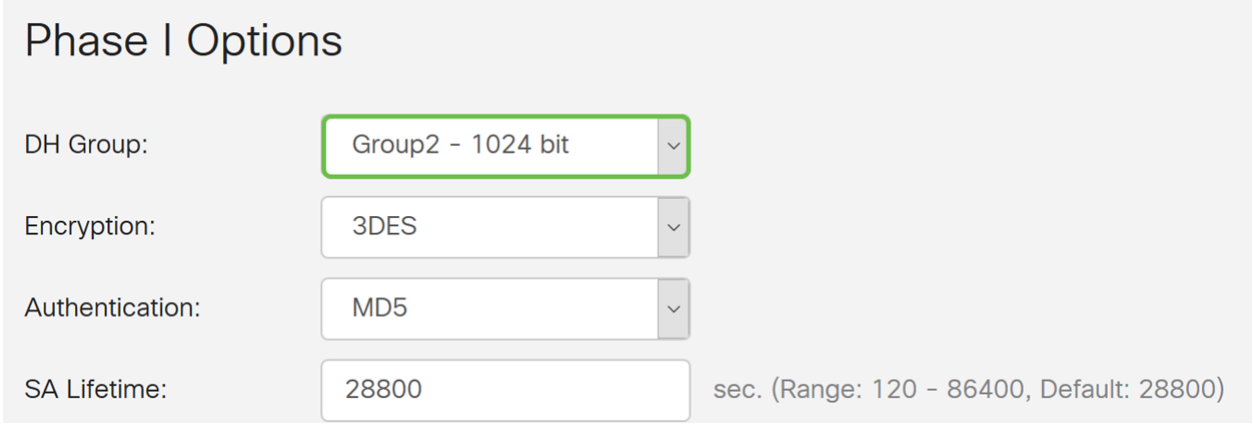
ملاحظة: إذا كانت أجهزتك تدعم IKEv2، يوصى باستخدام IKEv2. إذا لم تدعم أجهزتك IKEv2، فاستخدم IKEv1.



الخطوة 6. تقوم المرحلة الأولى بإعداد المفاتيح التي ستستخدمها لتشفير البيانات في المرحلة الثانية وتبادلها. في قسم *المرحلة الأولى*، حدد مجموعة DH. DH هو بروتوكول تبادل مفاتيح، مع مجموعتين من أطوال المفاتيح الأساسية الأساسية المختلفة، **المجموعة 2 - 1024 بت** والمجموعة **5 - 1536 بت**.

تم إختيار **المجموعة 2 - 1024 بت** لهذا العرض التوضيحي.

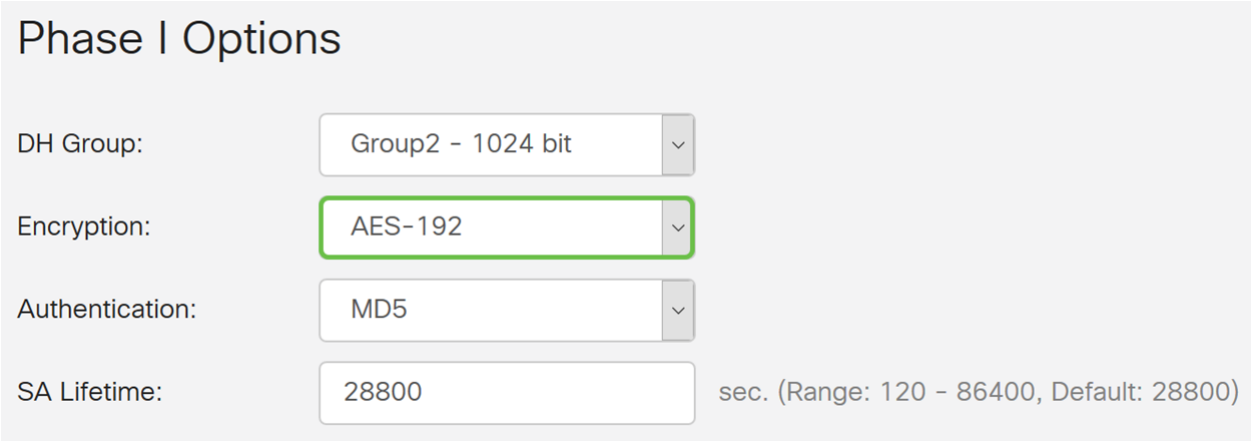
ملاحظة: للحصول على سرعة أكبر وأمان أقل، أختر المجموعة 2. من أجل سرعة أبطأ وأمان أعلى، أختر مجموعة 5. يتم تحديد المجموعة 2 كمجموعة افتراضية.



الخطوة 7. حدد خيار تشفير (**3DS**، أو **AES-128**، أو **AES-192**، أو **AES-256**) من القائمة المنسدلة. تحدد هذه الطريقة الخوارزمية المستخدمة لتشفير حزم ESP/ISAKMP وفك تشفيرها. يستخدم المعيار الثلاثي لتشفير البيانات (3DES) تشفير DES ثلاث مرات ولكنه الآن خوارزمية قديمة ويجب إستخدامه فقط عندما لا تكون هناك بدائل أخرى، لأنه لا يزال يوفر مستوى أمان هامشيا ولكن مقبولا. يجب على المستخدمين إستخدامها فقط إذا كانت مطلوبة للتوافق مع الإصدارات السابقة لأنها عرضة لبعض هجمات "التصادم الكلي". معيار التشفير المتقدم (AES) هو خوارزمية تشفير تم تصميمها لتكون أكثر أمانا من DES. يستخدم معيار التشفير المتطور (AES) حجما أكبر للمفتاح مما يضمن أن النهج الوحيد المعروف لفك تشفير الرسالة هو أن يقوم الدخيل بتجريب كل مفتاح ممكن. يوصى باستخدام AES إذا كان الجهاز الخاص بك يمكنه دعمه.

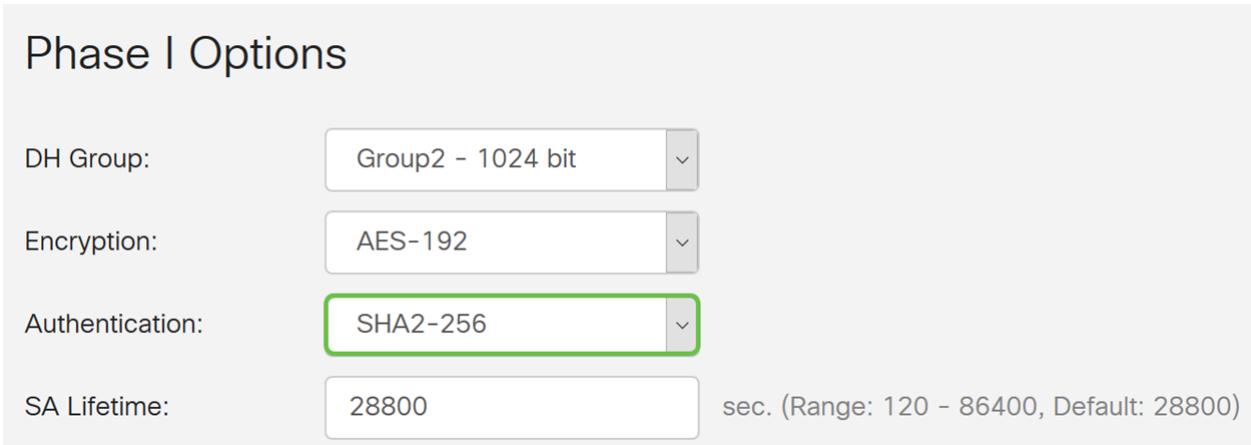
في هذا المثال، قمنا بتحديد **AES-192** كخيار تشفير خاص بنا.

ملاحظة: انقر على الارتباطات التشعبية للحصول على معلومات إضافية حول تكوين أمان شبكات VPN باستخدام IPsec أو تشفير الجيل التالي.



الخطوة 8. يحدد أسلوب المصادقة كيفية التحقق من صحة حزم رأس ESP. هذه هي خوارزمية التجزئة المستخدمة في المصادقة للتحقق من صحة ذلك الجانب أ والجانب ب حقا هما من يقولون أنهما. يعتبر MD5 خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 128 بت وهي أسرع من SHA1. إن SHA1 عبارة عن خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 160 بت بينما ينتج SHA2-256 خلاصة 256 بت. يوصى بإجراء SHA2-256 لأنه أكثر أمانا. تأكد من أن كلا طرفي نفق VPN يستخدمان نفس طريقة المصادقة. حدد مصادقة (**MD5 أو SHA1** أو **SHA2-256**).

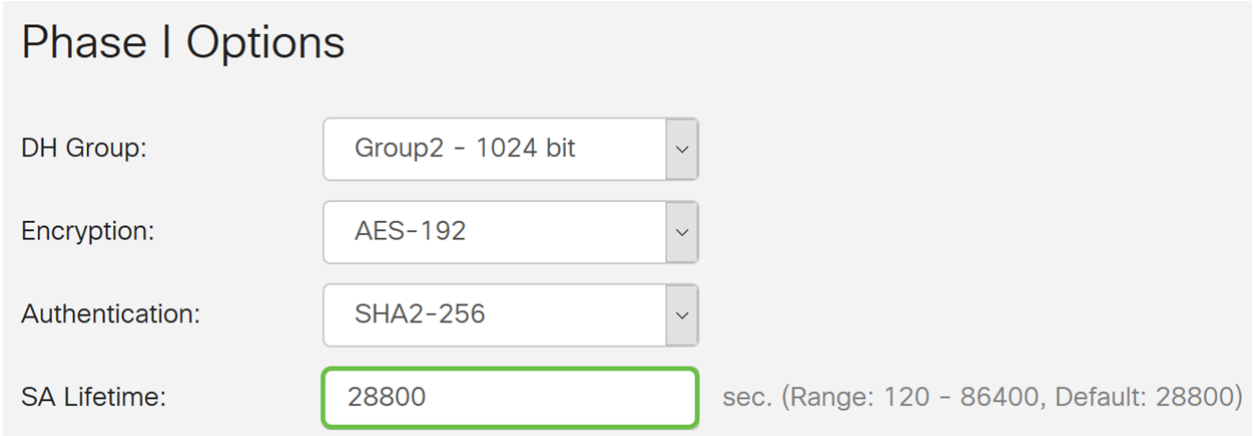
تم تحديد **SHA2**-256 لهذا المثال.



الخطوة 9. تخبرك *مدة صلاحية (sec) SA* مقدار الوقت الذي يكون فيه IKE SA نشطا في هذه المرحلة. وعندما تنتهي مدة صلاحية الخدمات الاجتماعية بعد انتهاء مدة صلاحية كل منها، تبدأ مفاوضات جديدة من أجل إجراء مفاوضات جديدة. المدى from 120 to 86400 افتراضيا 28800.

سنستخدم القيمة الافتراضية ل **28800** ثانية كعمر SA الخاص بنا للمرحلة الأولى.

ملاحظة: يوصى بأن تكون مدة البقاء للمساعد الخاص بك في المرحلة الأولى أطول من فترة بقائك على قيد الحياة للمرحلة الثانية. إذا جعلت المرحلة الأولى أقصر من المرحلة الثانية، ثم سيكون عليك إعادة التفاوض النفق ذهابا وإيابا بشكل متكرر مقارنة بنفق البيانات. إن نفق البيانات هو ما يحتاج إلى مزيد من الأمان ومن الأفضل أن تكون مدة البقاء في المرحلة الثانية أقصر من المرحلة الأولى.

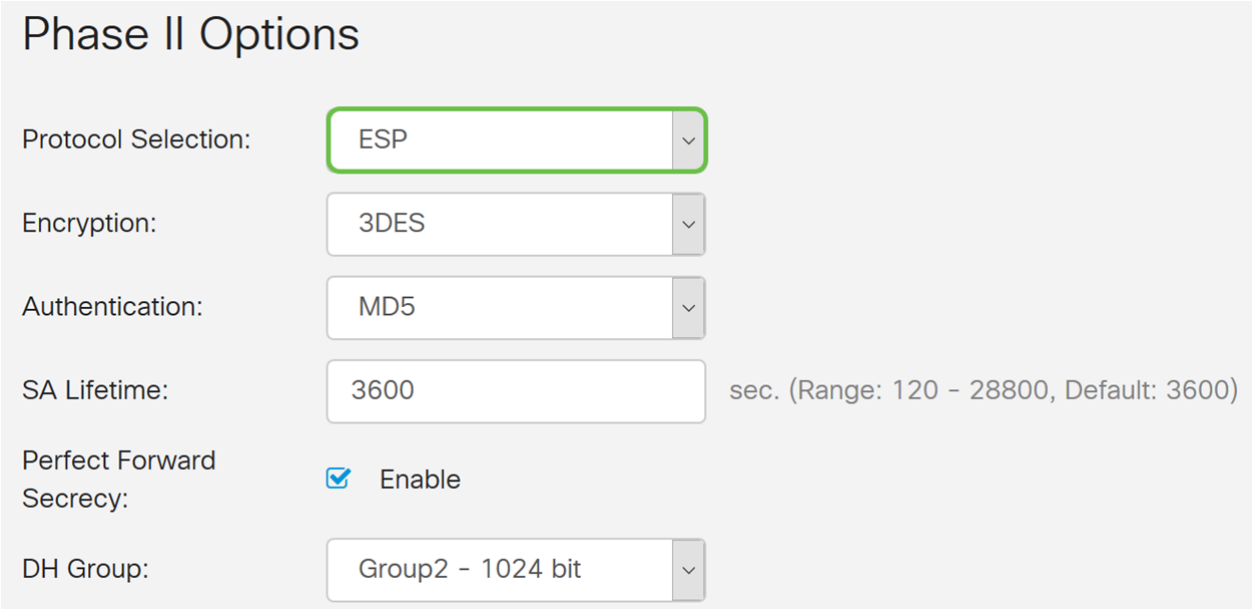


الخطوة 10. المرحلة الثانية هي المكان الذي يمكنك فيه تشفير البيانات التي يتم تمريرها ذهابا وإيابا. في *خيارات المرحلة 2*، حدد بروتوكولا من القائمة المنسدلة:

- حمولة أمان التضمين (ESP) - حدد ESP لتشفير البيانات وأدخل التشفير.

- رأس المصادقة (AH) - حدد هذا الخيار لسلامة البيانات في الحالات التي تكون فيها البيانات غير سرية، وبعبارة أخرى، لا يتم تشفيرها ولكن يجب مصادقتها. يتم إستخدامه فقط للتحقق من مصدر حركة المرور ووجهتها.

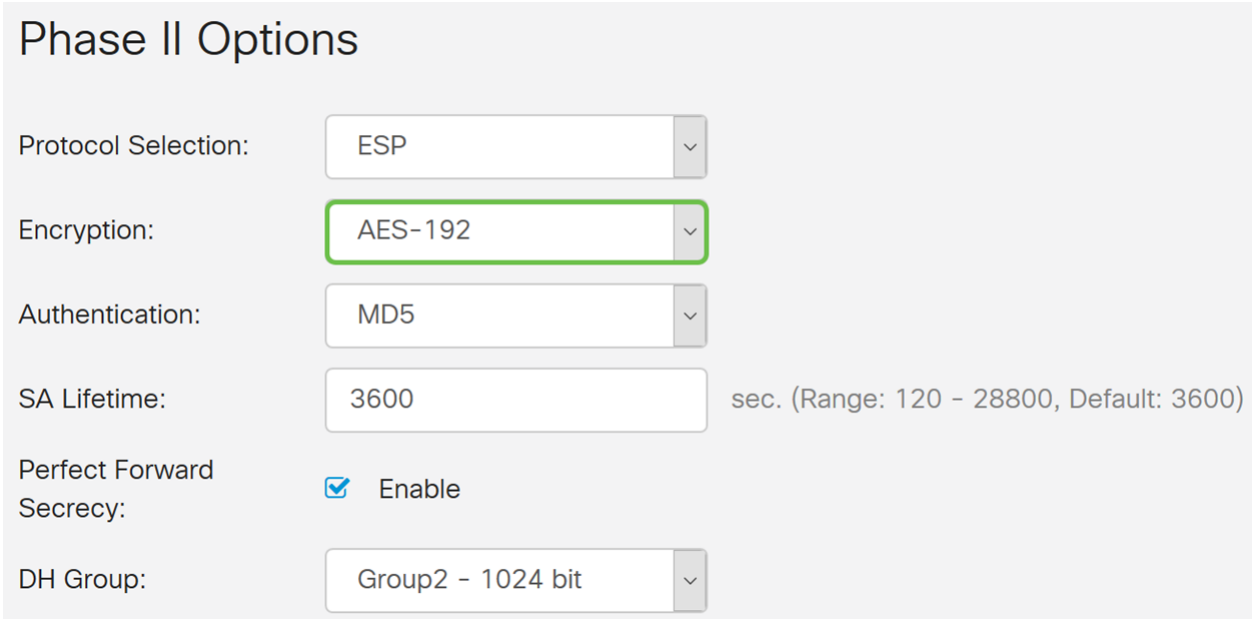
في هذا المثال، سنستخدم **ESP** كميزة *تحديد البروتوكول* الخاصة بنا.



الخطوة 11. حدد خيار تشفير (**3DES**، أو **AES-128**، أو **AES-192**، أو **AES-256**) من القائمة المنسدلة. تحدد هذه الطريقة الخوارزمية المستخدمة لتشفير حزم ESP/ISAKMP وفك تشفيرها.

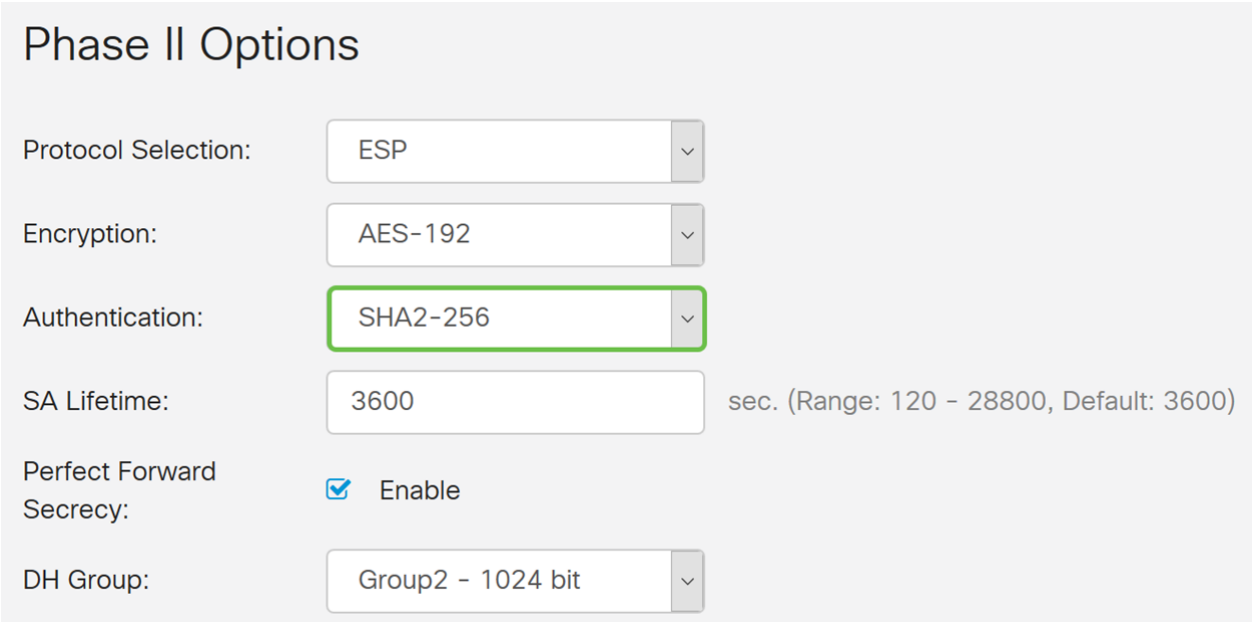
في هذا المثال، سنستخدم **AES-192** كخيار تشفير خاص بنا.

ملاحظة: انقر على الارتباطات التشعبية للحصول على معلومات إضافية حول تكوين أمان شبكات VPN باستخدام IPsec أو تشفير الجيل التالي.

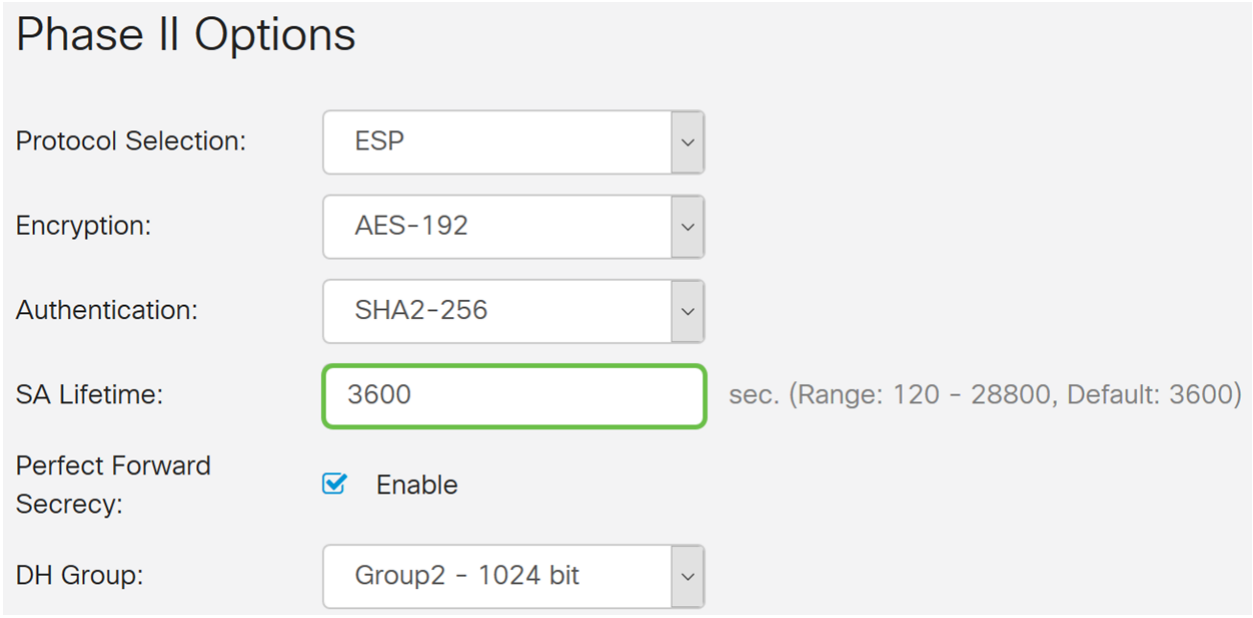


الخطوة 12. يحدد أسلوب المصادقة كيفية التحقق من صحة حزم رؤوس بروتوكول حمولة الأمان التضمين (ESP). حدد مصادقة (**MD5 أو SHA1** أو **SHA2-256**).

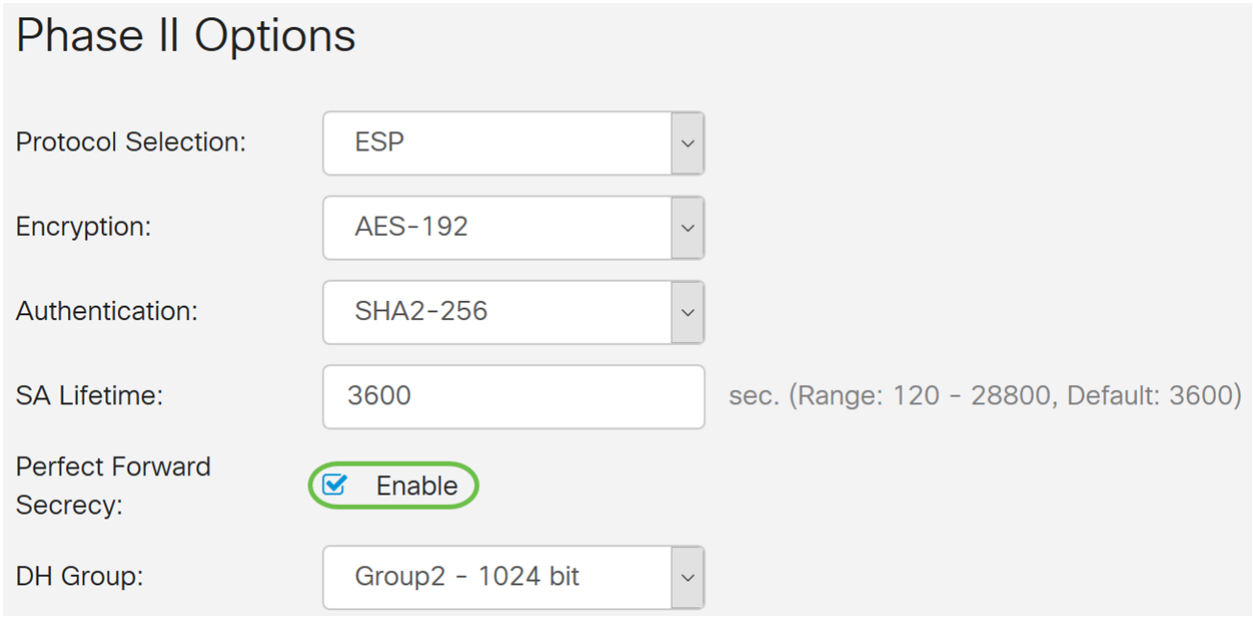
تم تحديد **SHA2**-256 لهذا المثال.



الخطوة 13. أدخل مقدار الوقت الذي يكون فيه نفق IPsec SA) VPN) نشطا في هذه المرحلة. القيمة الافتراضية للمرحلة 2 هي 3600 ثانية. سنستخدم القيمة الافتراضية لهذا العرض التوضيحي.

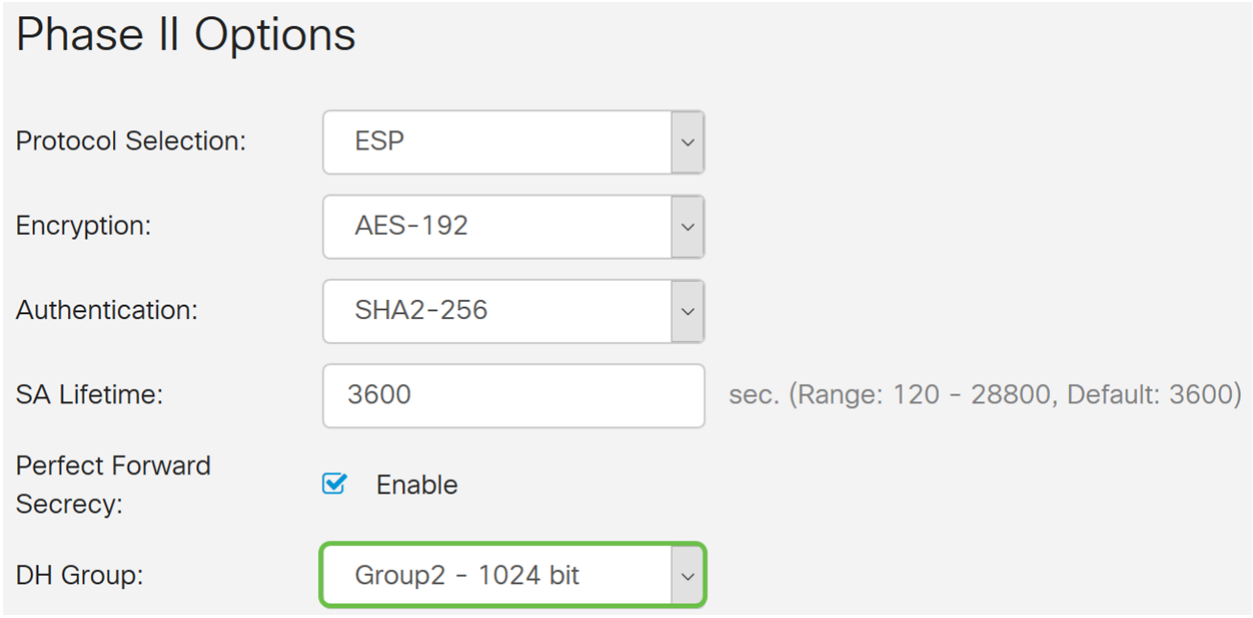


الخطوة 14. حدد **تمكين** لتمكين سرية إعادة التوجيه المثالية. عند تمكين سرية إعادة التوجيه المثالية (PFS)، تعمل مفاوضات المرحلة 2 من IKE على إنشاء مادة أساسية جديدة لتشفير حركة مرور IPsec والمصادقة. تستخدم ملفات PFS لتحسين أمن الاتصالات المنقولة عبر الإنترنت باستخدام تشفير المفتاح العام. يوصى بذلك إذا كان الجهاز الخاص بك يمكنه دعمه.

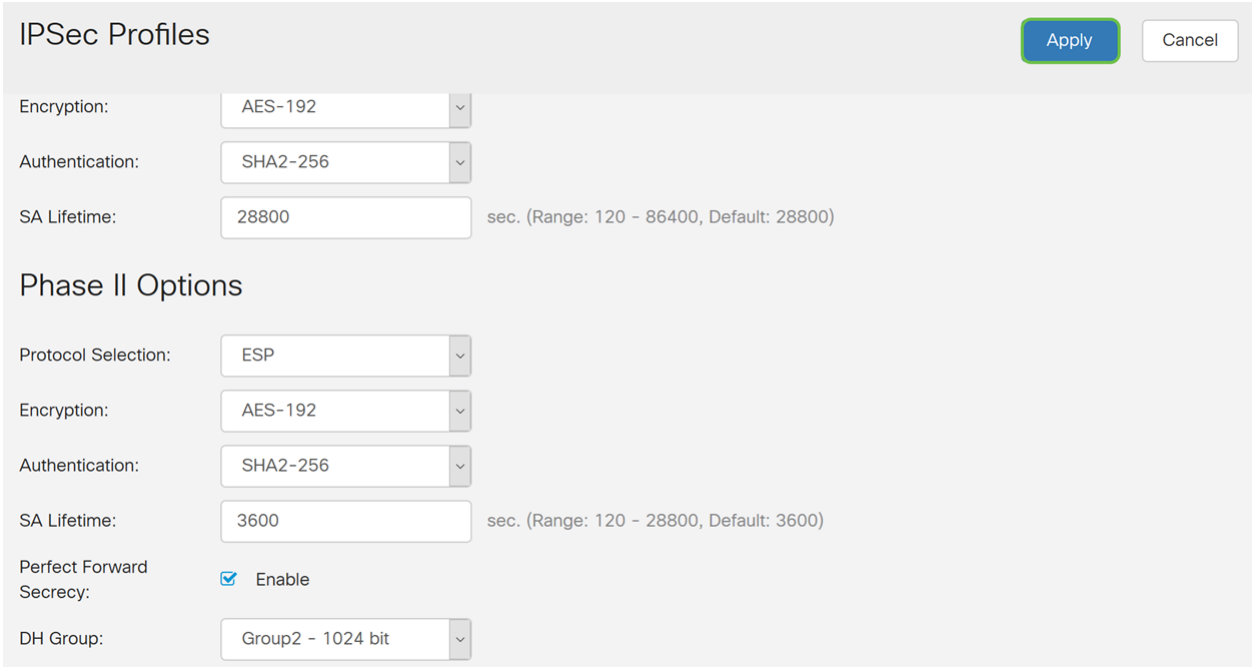


الخطوة 15. حدد مجموعة DH. Diffie-Hellman (DH) هو بروتوكول تبادل مفاتيح، مع مجموعتين من أطوال المفاتيح الأساسية الأساسية المختلفة، **والمجموعة 2 - 1024 بت** والمجموعة **5 - 1536 بت**. لقد اخترنا **المجموعة 2 - 1024 بت** لهذا العرض التوضيحي.

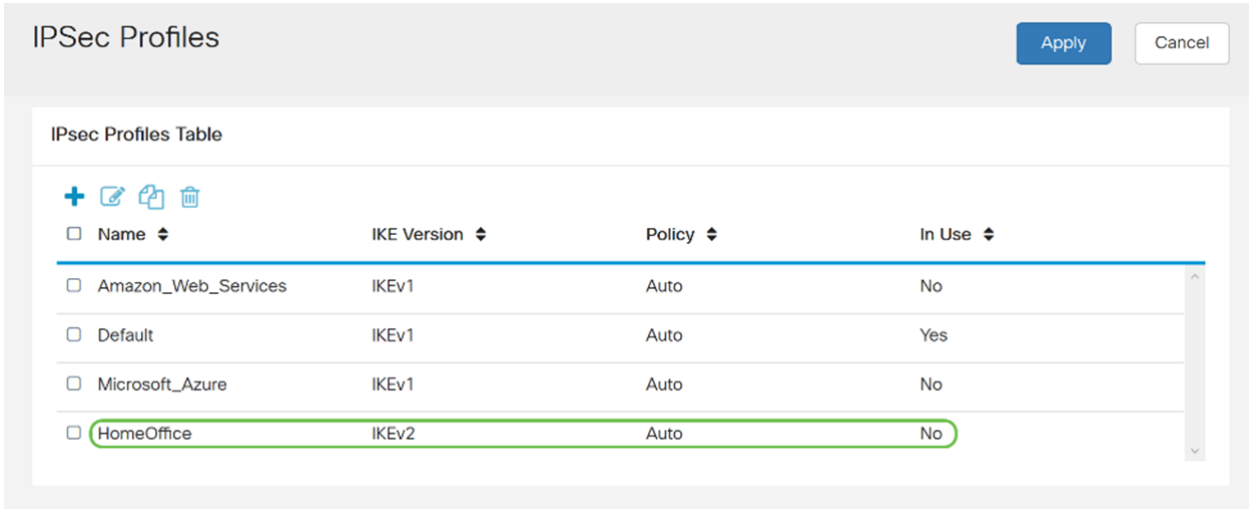
ملاحظة: للحصول على سرعة أكبر وأمان أقل، أختر المجموعة 2. من أجل سرعة أبطأ وأمان أعلى، أختر مجموعة 5. يتم تحديد المجموعة 2 بشكل افتراضي.



الخطوة 16. انقر على **تطبيق** لإضافة ملف تعريف IPsec جديد.

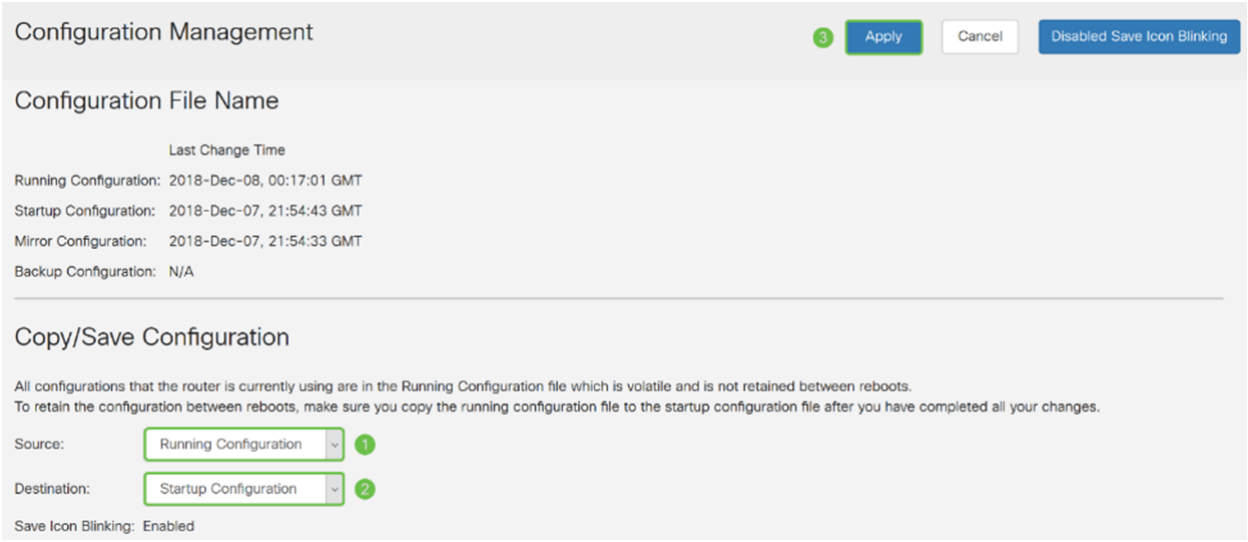


الخطوة 17. بعد النقر فوق *تطبيق*، يجب إضافة ملف تعريف IPsec الجديد.



الخطوة 18. في أعلى الصفحة، انقر فوق أيقونة **حفظ** للتنقل إلى *إدارة التكوين* لحفظ التكوين الجاري تشغيله إلى تكوين بدء التشغيل. الغرض من هذا هو الاحتفاظ بالتكوين بين عمليات إعادة التمهيد.

الخطوة 19. في إدارة التكوين، تأكد من أن *المصدر* **يشغل التكوين** وأن *الوجهة* هي تكوين بدء التشغيل. ثم اضغط على **تطبيق** لحفظ التكوين الجاري تشغيله إلى تكوين بدء التشغيل. توجد جميع التكوينات التي يستخدمها الموجه حاليا في ملف التكوين الجاري تشغيله والذي يكون متطايرا ولا يتم الاحتفاظ به بين عمليات إعادة التمهيد. سيؤدي نسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل إلى الاحتفاظ بكل التكوين بين عمليات إعادة التشغيل.



الخطوة 20. اتبع جميع الخطوات مرة أخرى لإعداد الموجه B.

يجب أن تكون قد انتهيت الآن من إنشاء ملف تعريف IPsec جديد بنجاح باستخدام IKEv2 كإصدار IKE لكلا الموجهين. أنت جاهز لتكوين شبكة VPN من موقع إلى موقع.

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).