تكوين توصيفات IPSec (وضع الكبح التلقائي) على RV160 و RV260

يوضح هذا المستند كيفية إنشاء ملف تعريف جديد لأمان بروتوكول الإنترنت (IPsec) باستخدام وضع الكبح التلقائي على موجهات من السلسلة RV160 و RV260.

يضمن IPsec توفر اتصال خاص آمن لديك عبر الإنترنت. وهو يعطي مضيفين أو أكثر الخصوصية، النزاهة، والأصالة لنقل المعلومات الحساسة عبر الإنترنت. شائع إستخدام IPsec في الشبكة الخاصة الظاهرية (VPN) ويتم تنفيذه على طبقة IP ويمكن أن يساعد إستخدامه العديد من التطبيقات التي تفتقر إلى الأمان. يتم إستخدام شبكة VPN لتوفير آلية اتصال آمنة للبيانات الحساسة ومعلومات IP التي يتم إرسالها من خلال شبكة غير آمنة مثل الإنترنت. وهو يوفر حلا مرنا للمستخدمين عن بعد وللمؤسسة 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 المرحلة الأولى والمرحلة الثانية في الوضع التلقائي بالإضافة إلى وضع الحفظ اليدوي. تنشئ المرحلة 1 المفاتيح المشتركة مسبقا لإنشاء اتصال آمن مصدق. المرحلة 2 هي المكان الذي يتم فيه تشفير حركة المرور. يمكنك تكوين معظم معلمات IPsec مثل البروتوكول والوضع والخوارزمية والسرية الكاملة لإعادة التوجيه (PFS) وفترة بقاء اقتران الأمان (SA) وبروتوكول إدارة المفاتيح.

لاحظ أنه عند تكوين شبكة VPN من موقع إلى موقع، سيحتاج الموجه البعيد إلى الحصول على إعدادات ملف التعريف نفسها الخاصة بالموجه المحلي لديك.

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

لتكوين ملف تعريف IPsec وشبكة VPN من موقع إلى موقع باستخدام معالج إعداد VPN، الرجاء النقر فوق الارتباط: تكوين معالج إعداد VPN على RV160 و RV260.

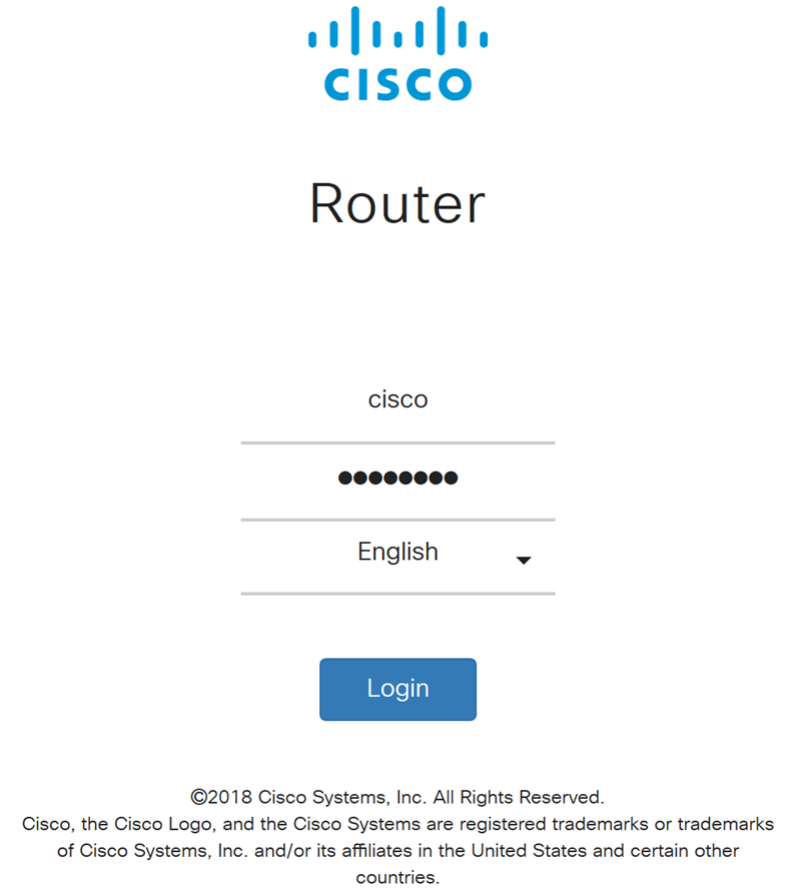
لتكوين شبكة VPN من موقع إلى موقع، الرجاء مراجعة المستند: تكوين شبكة VPN من موقع إلى موقع على RV160 و RV260.

- RV160
- RV260

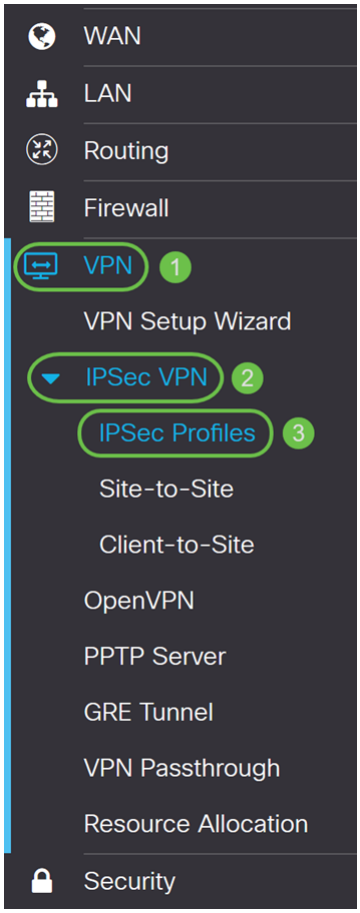
- 1.0.00.13

IPsec

الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب على الموجه الخاص بك.

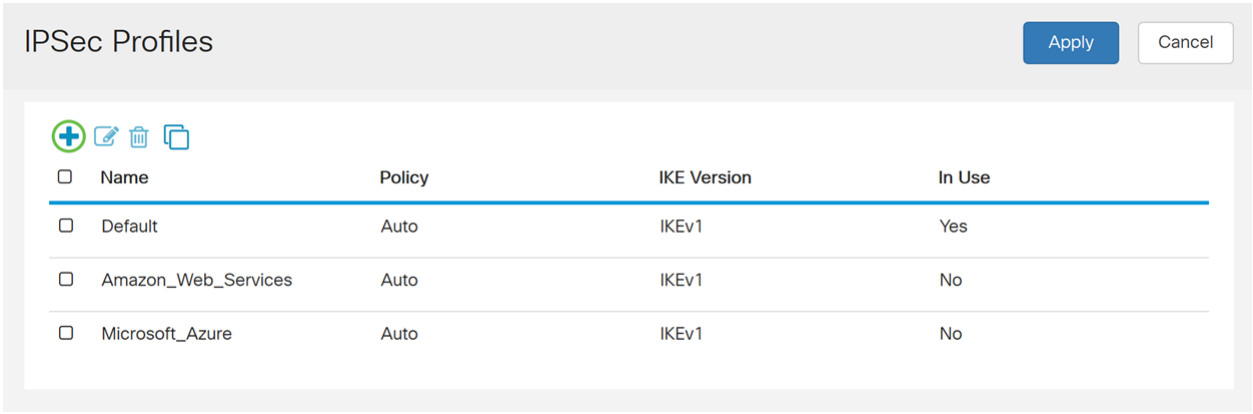


الخطوة 2. انتقل إلى **IPSec VPN > VPN > توصيفات IPSec**.



الخطوة 3. في جدول *توصيفات IPSec*، انقر على **إضافة** لإنشاء توصيف IPsec جديد. هناك أيضا خيارات

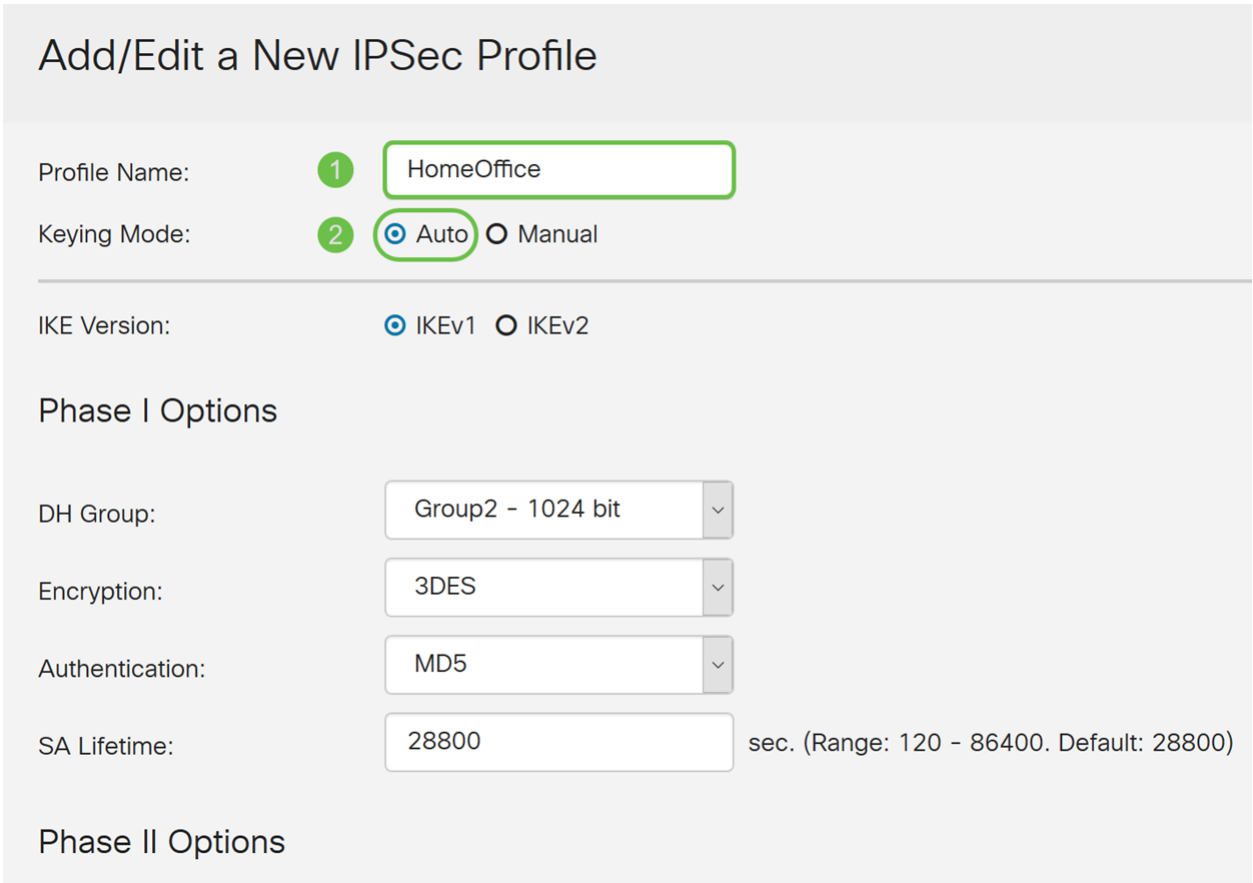
لتحرير، حذف، أو نسخ ملف تخصيص.



الخطوة 4. أدخل اسم ملف تخصيص وحدد وضع الكي (تلقائي أو يدوي).

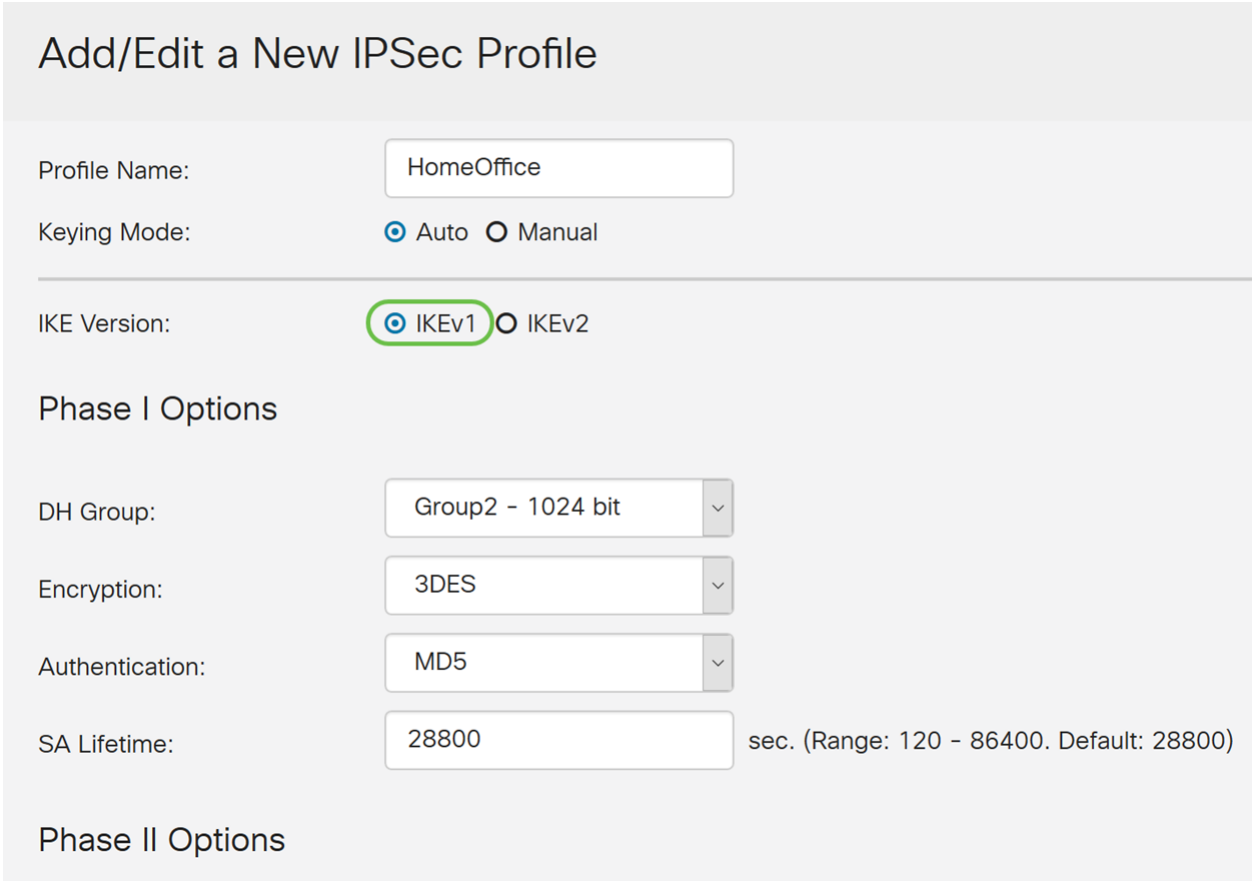
تم إدخال **HomeOffice** كاسم *ملف التعريف*.

يتم تحديد **تلقائي** *لوضع التعبئة*.



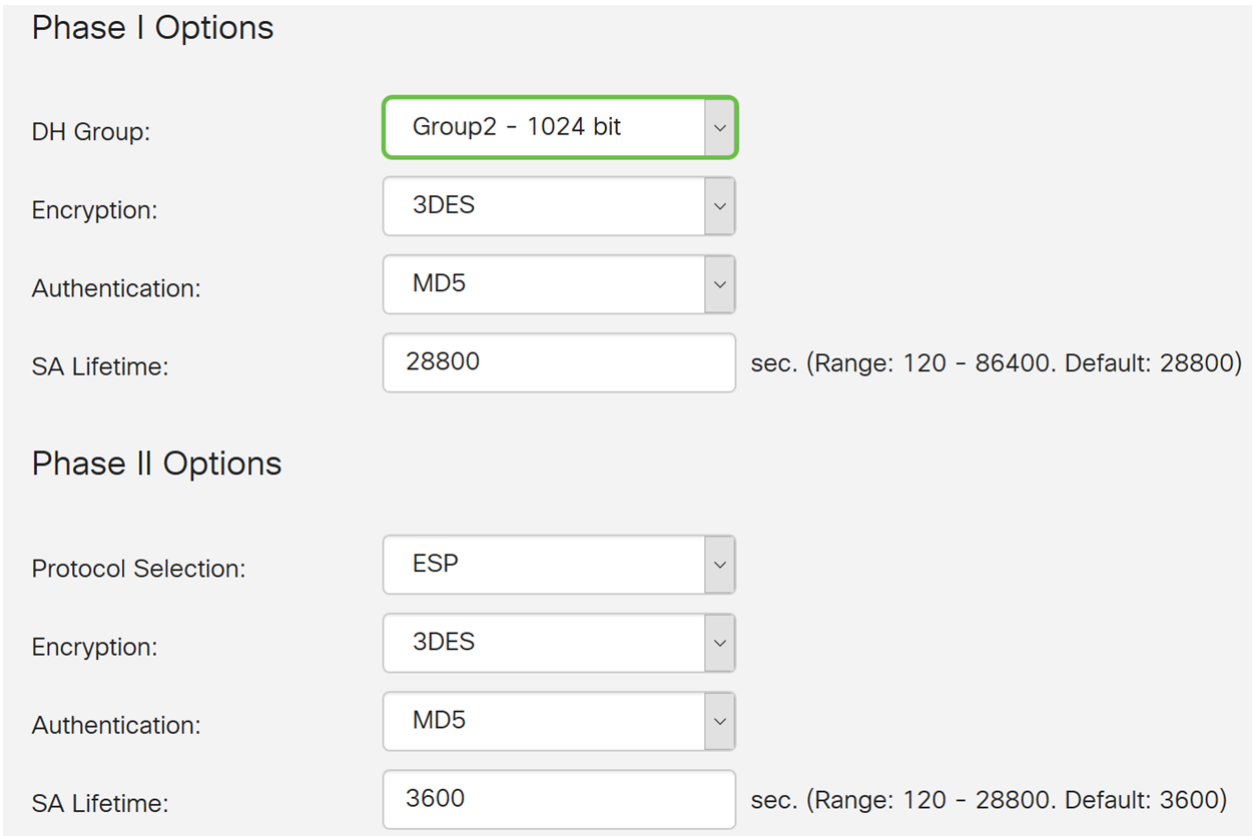
الخطوة 5. أختر *Internet Key Exchange الإصدار 1 (IKEv1)* أو *Internet Key Exchange الإصدار 2 (IKEv2)* كإصدار ل IKE. IKE هو بروتوكول هجين يقوم بتنفيذ تبادل مفاتيح Oakley وتبادل مفاتيح Skeme داخل إطار عمل رابطة أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP). يحدد كل من أوكلي وسكيمي كيفية الحصول على مواد تثبيت المفاتيح المصدق عليها، ولكن برنامج سكايمي يتضمن أيضا خدمة تحديث المفاتيح السريع. يوفر IKE مصادقة أقران IPsec، ويفاوض مفاتيح IPsec، ويتفاوض على اقترانات أمان IPsec. يعد IKEv2 أكثر فعالية لأنه يتطلب حزمة أقل لإجراء تبادل المفاتيح، كما يدعم المزيد من خيارات المصادقة بينما يقوم IKEv1 فقط بالمصادقة على المفتاح المشترك والمصادقة المستندة إلى الشهادة. في هذا المثال، تم تحديد **IKEv1** كإصدار IKE.

ملاحظة: إذا كان جهازك يدعم IKEv2، يوصى باستخدام IKEv2. إذا كانت أجهزتك لا تدعم IKEv2، فاستخدم IKEv1.



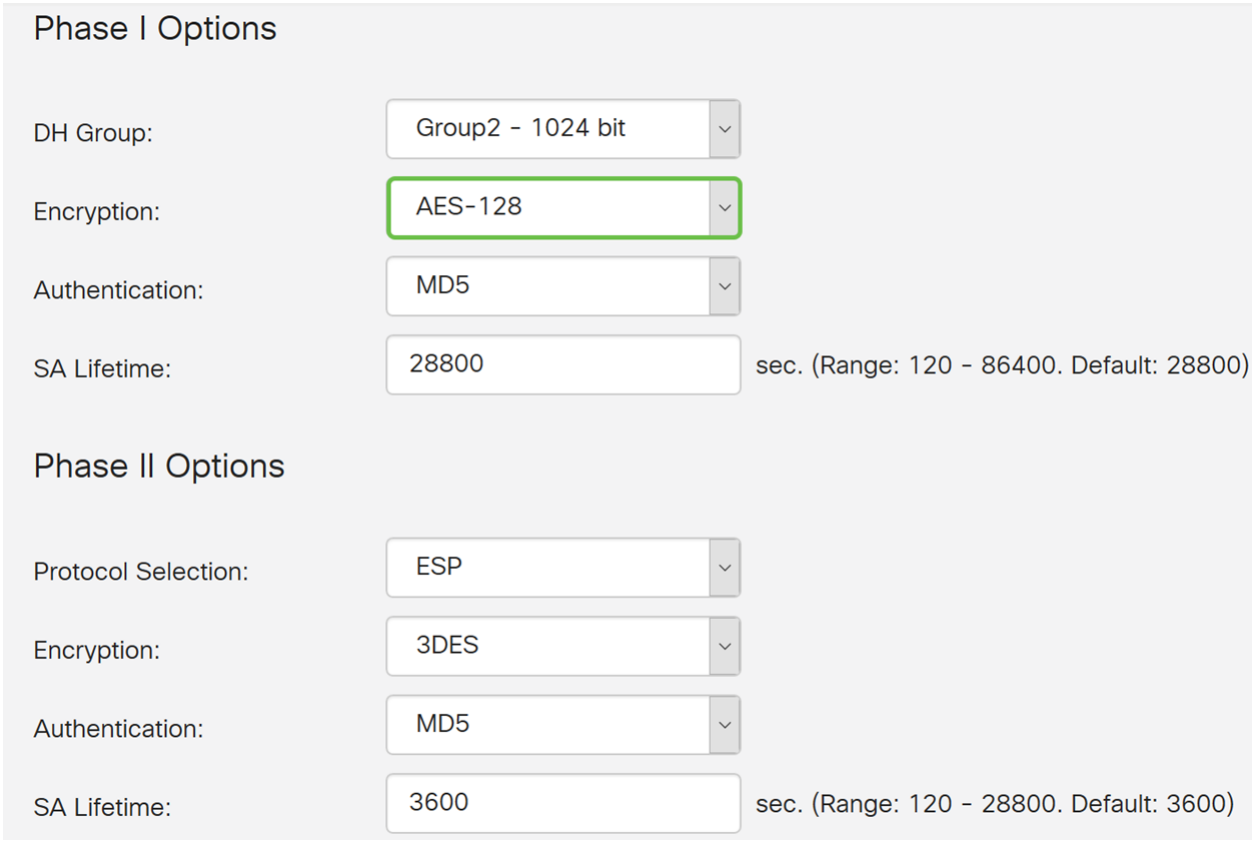
الخطوة 6. تقوم المرحلة الأولى بإعداد المفاتيح التي ستستخدمها لتشفير البيانات في المرحلة الثانية وتبادلها. في قسم *المرحلة الأولى*، حدد مجموعة DH. Diffie-Hellman (DH) هو بروتوكول تبادل مفاتيح، مع مجموعتين من أطوال المفاتيح الأساسية الأساسية المختلفة، **والمجموعة 2 - 1024 بت** والمجموعة **5 - 1536 بت**.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



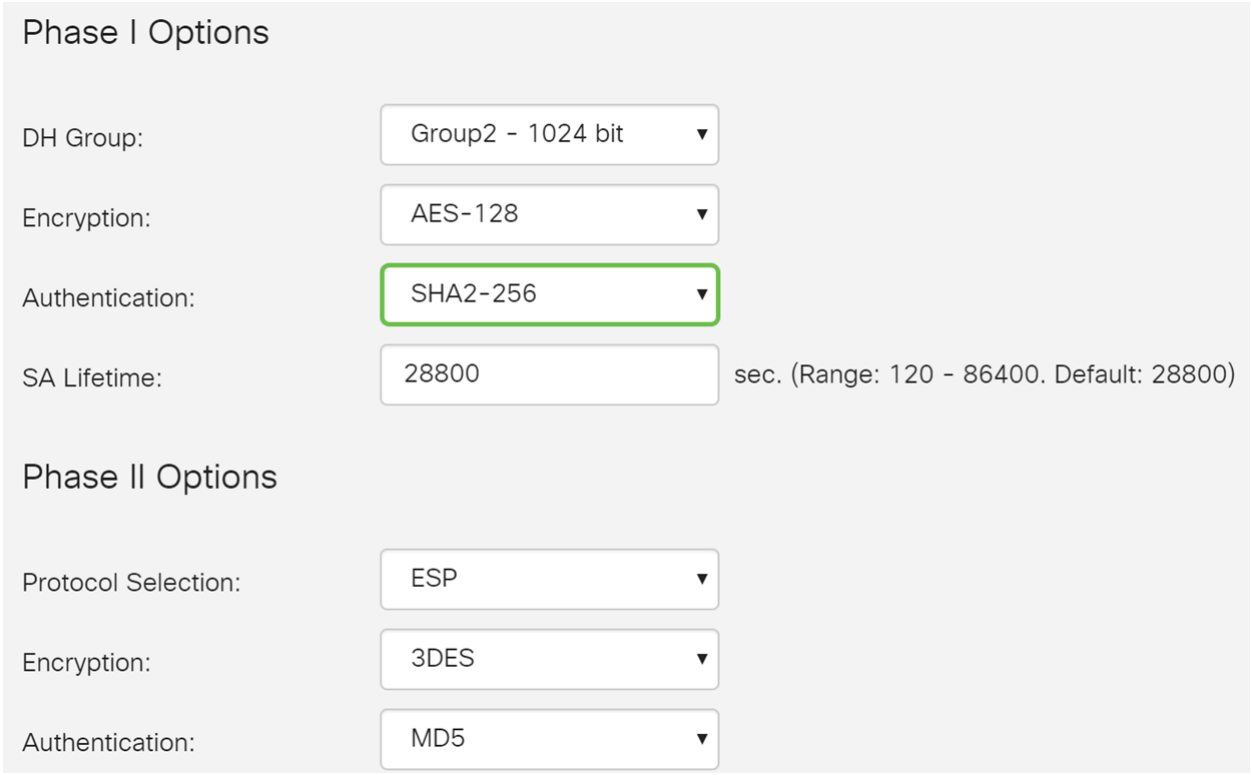
الخطوة 7. حدد خيار تشفير (**3DES**، أو **AES-128**، أو **AES-192**، أو **AES-256**) من القائمة المنسدلة. تحدد هذه الطريقة الخوارزمية المستخدمة لتشفير حزم ESP/ISAKMP وفك تشفيرها. يستخدم المعيار الثلاثي لتشفير البيانات (3DES) تشفير DES ثلاث مرات ولكنه الآن عبارة عن خوارزمية قديمة. وهذا يعني أنه يجب إستخدامه فقط عندما لا يكون هناك بدائل أفضل لأنه يوفر مستوى أمنيا هامشيا ومقبولا في الوقت نفسه. يجب على المستخدمين إستخدامها فقط إذا كانت مطلوبة للتوافق مع الإصدارات السابقة لأنها عرضة لبعض هجمات "التصادم الكلي". لا يوصى باستخدام معيار 3DES لأنه لا يعتبر آمنا. 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-128** كخيار تشفير خاص بنا.

ملاحظة: فيما يلي بعض الموارد الإضافية التي قد تساعد: تكوين أمان شبكات VPN باستخدام IPsec وتشفير 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**).

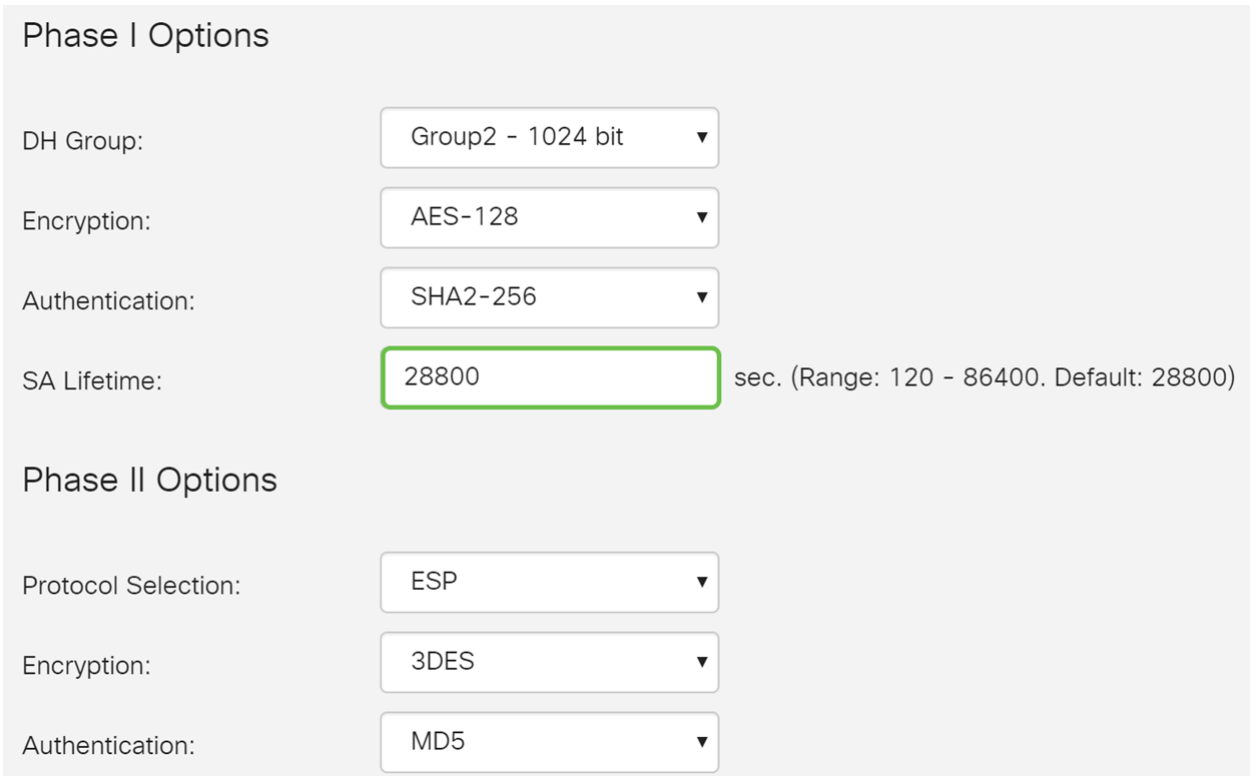
تم تحديد **SHA2**-256 لهذا المثال.



الخطوة 9. تخبرك *مدة صلاحية SA (sec)* 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 120 to 86400 from 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.

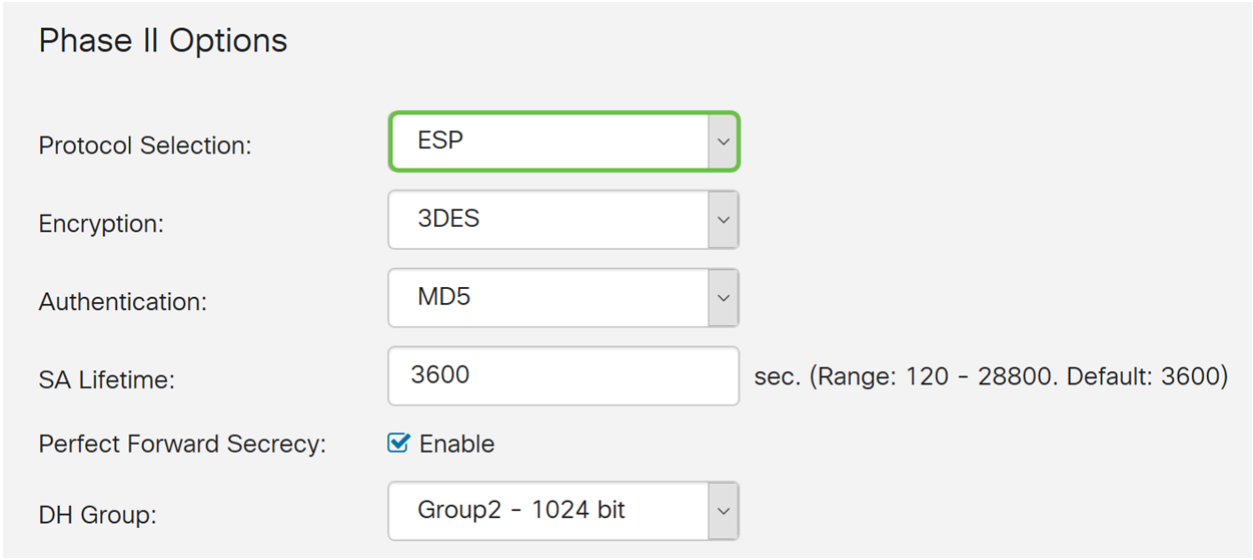


الخطوة 10. المرحلة الثانية هي المكان الذي يمكنك فيه تشفير البيانات التي يتم تمريرها ذهابا وإيابا. في خيارات *المرحلة 2*، حدد بروتوكولا من القائمة المنسدلة، الخيارات هي:

• 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.

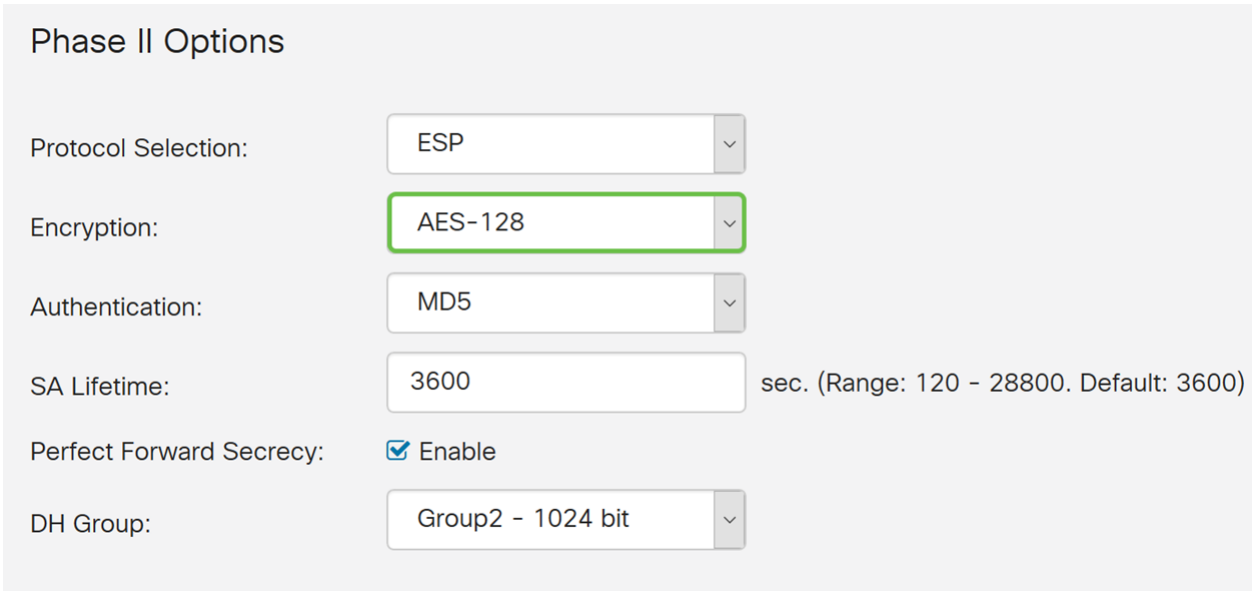
في هذا المثال، سنستخدم **ESP** كميزة *تحديد البروتوكول* الخاصة بنا.



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.

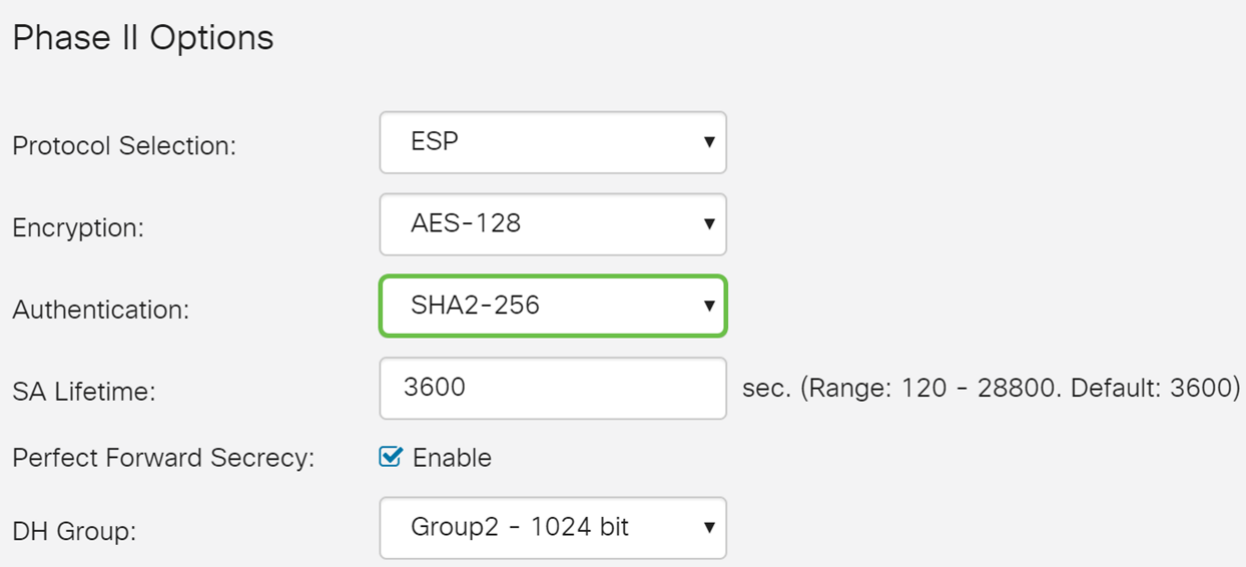
في هذا المثال، سنستخدم **AES-128** كخيار تشفير لنا.

ملاحظة: فيما يلي بعض الموارد الإضافية التي قد تساعد: تكوين أمان شبكات VPN باستخدام IPsec وتشفير الجيل التالي.

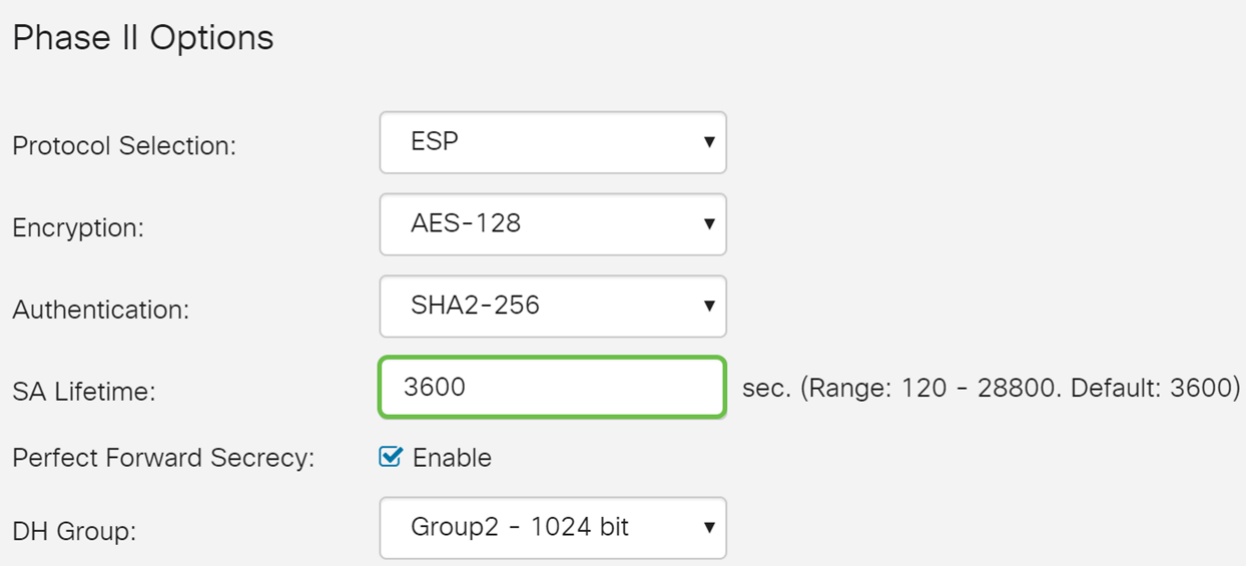


الخطوة 12. يحدد أسلوب المصادقة كيفية التحقق من صحة حزم رؤوس بروتوكول حمولة الأمان التضمين (ESP). حدد مصادقة (**MD5 أو SHA1** أو **SHA2-256**).

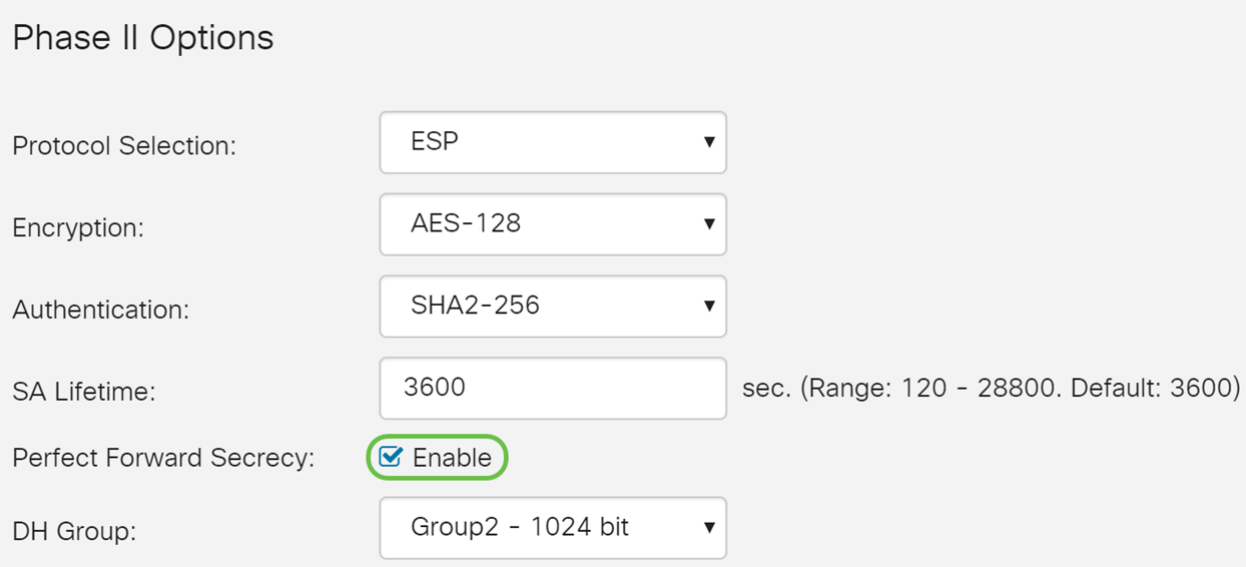
تم تحديد **SHA2**-256 لهذا المثال.



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.



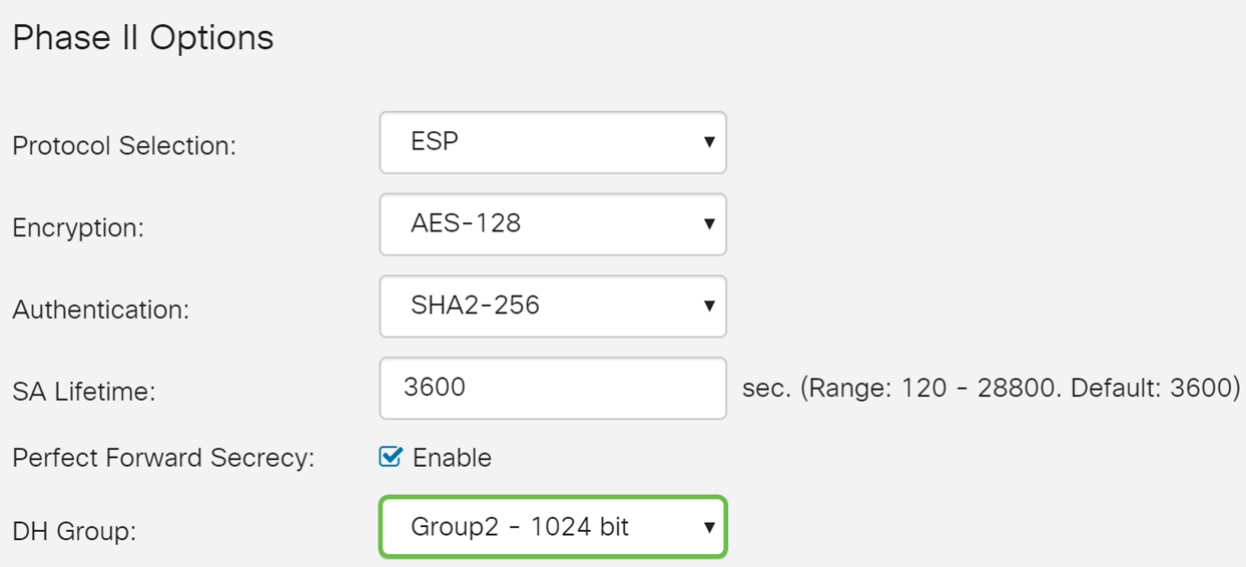
الخطوة 14. حدد **تمكين** لتمكين سرية إعادة التوجيه المثالية. عند تمكين سرية إعادة التوجيه المثالية (PFS)، تعمل مفاوضات المرحلة 2 من IKE على إنشاء مادة أساسية جديدة لتشفير حركة مرور IPsec والمصادقة. تستخدم ملفات PFS لتحسين أمن الاتصالات المنقولة عبر الإنترنت باستخدام تشفير المفتاح العام. يوصى بذلك إذا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



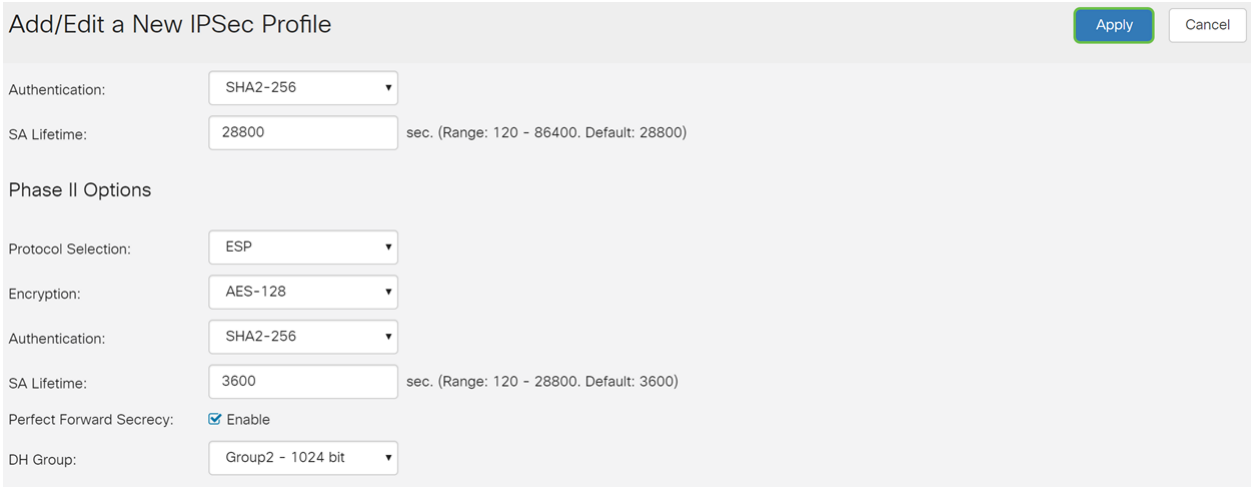
الخطوة 15. حدد مجموعة DH. Diffie-Hellman (DH) هو بروتوكول تبادل مفاتيح، مع مجموعتين من أطوال

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.

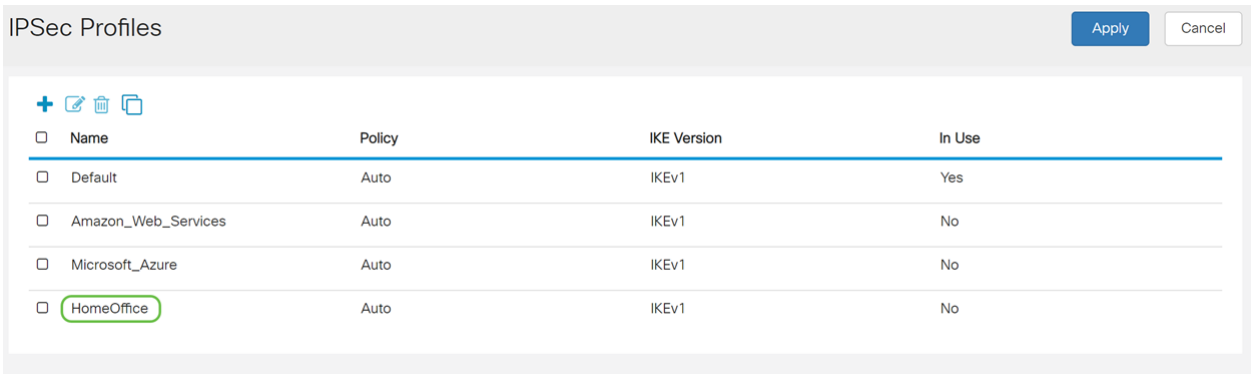


الخطوة 16. انقر على **تطبيق** لإضافة ملف تعريف IPsec جديد.

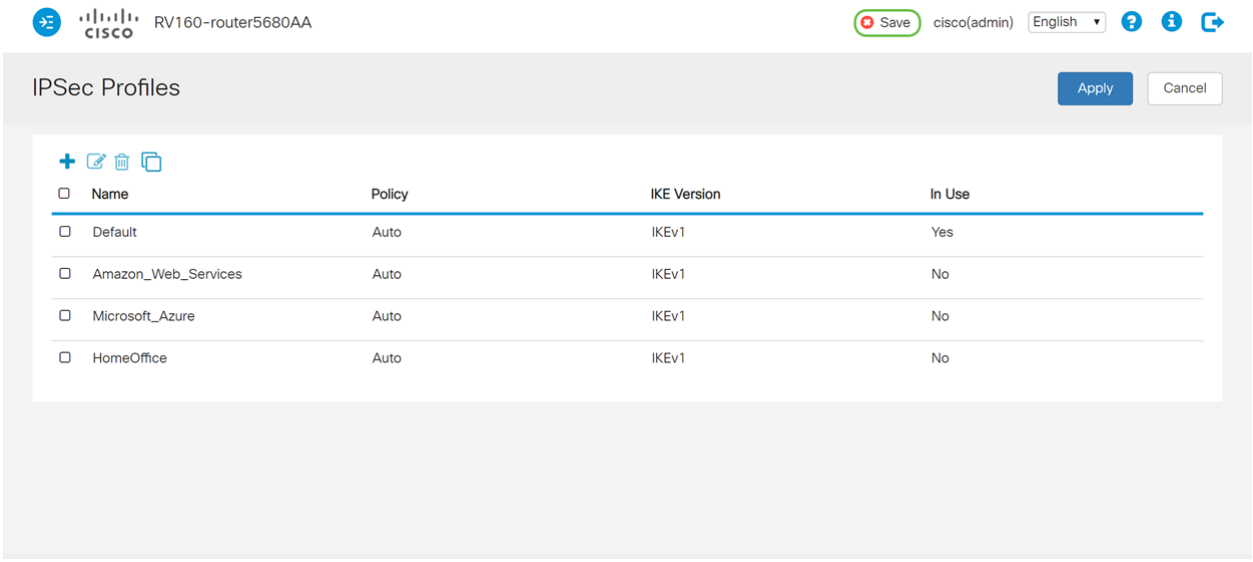


يجب عليك الآن إنشاء ملف تعريف IPsec جديد بنجاح. الرجاء المتابعة أدناه للتحقق من إضافة ملف تعريف IPsec. يمكنك أيضا اتباع الخطوات لنسخ ملف التكوين الجاري تشغيله لديك إلى ملف تكوين بدء التشغيل حتى يتم الاحتفاظ بجميع التكوين الخاص بك بين عمليات إعادة التمهيد.

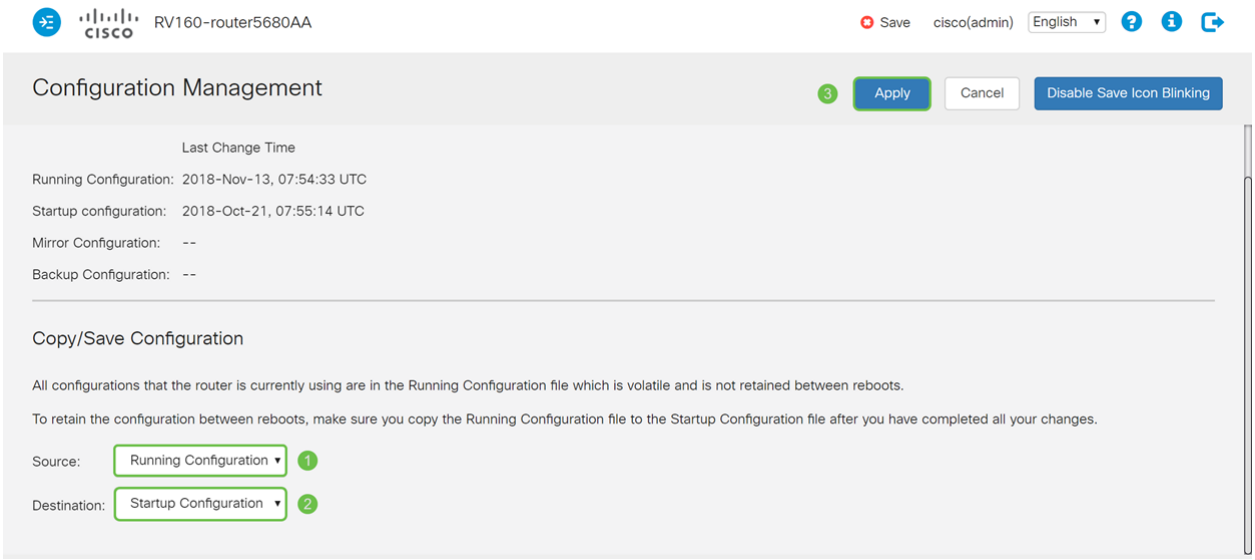
الخطوة 1. بعد النقر فوق *تطبيق*، يجب إضافة ملف تعريف IPsec الجديد.



الخطوة 2. في أعلى الصفحة، انقر فوق الزر **حفظ** للانتقال إلى *إدارة التكوين* لحفظ التكوين الجاري تشغيله إلى تكوين بدء التشغيل. الغرض من هذا هو الاحتفاظ بالتكوين بين عمليات إعادة التمهيد.



الخطوة 3. 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 التمهيد.



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).