تكوين ملف تعريف أمان بروتوكول الإنترنت (IPSec) على موجه من السلسلة RV34x

الهدف

يوفر أمان بروتوكول الإنترنت (IPSec) أنفاقا آمنة بين نظراين، مثل موجهين. يجب تحديد الحزم التي تعد حساسة ويجب إرسالها من خلال هذه الأنفاق الآمنة، بالإضافة إلى المعلمات التي يجب إستخدامها لحماية هذه الحزم الحساسة من خلال تحديد خصائص هذه الأنفاق. بعد ذلك، عندما يرى نظير IPsec حزمة حساسة كهذه، فإنه يقوم بإعداد النفق الآمن المناسب وإرسال الحزمة عبر هذا النفق إلى النظير البعيد.

عند تنفيذ IPsec في جدار حماية أو موجه، فإنه يوفر أمانا قويا يمكن تطبيقه على جميع حركة المرور التي تعبر النطاق. لا تتحمل حركة المرور داخل الشركة أو مجموعة العمل نفقات المعالجة المتعلقة بالأمان الزائدة.

الهدف من هذا المستند هو توضيح كيفية تكوين ملف تعريف IPSec على موجه من السلسلة RV34x.

الأجهزة القابلة للتطبيق

- RV34x Series

إصدار البرامج

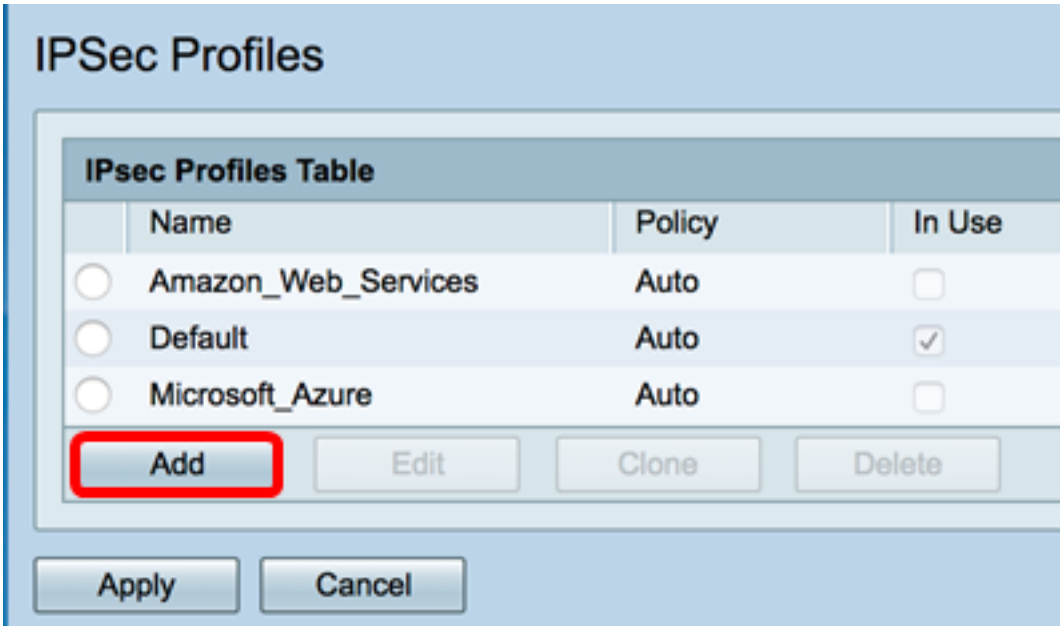
- 1.0.1.16

تكوين ملف تعريف IPSec

إنشاء ملف تعريف IPSec

الخطوة 1. سجل الدخول إلى الأداة المساعدة المستندة إلى الويب في الموجه واختر **VPN > توصيفات IPSec**.

الخطوة 2. يظهر جدول توصيفات IPsec التوصيفات الموجودة. انقر على **إضافة** لإنشاء توصيف جديد.



الخطوة 3. قم بإنشاء اسم للتوصيف في حقل *اسم التوصيف*. يجب أن يحتوي اسم ملف التعريف على أحرف أبجدية رقمية فقط وعلامة سفلية (_) للحروف الخاصة.

ملاحظة: في هذا المثال، يتم إستخدام IPSec_VPN كاسم ملف تعريف IPSec.

الخطوة 4. انقر على زر إختيار لتحديد طريقة تبادل المفاتيح التي سيستخدمها التوصيف للمصادقة. الخيارات هي:

- تلقائي — يتم تعيين معلمات النهج تلقائيا. يستخدم هذا الخيار سياسة Internet Key Exchange (IKE) لسلامة البيانات وتشفيرها لعمليات تبادل المفاتيح. في حالة إختيار هذا الخيار، يتم تمكين إعدادات التكوين ضمن منطقة معلمات النهج التلقائي. انقر هنا لتكوين الإعدادات التلقائية.
- يدوي — يسمح هذا الخيار لك بتكوين المفاتيح يدويا لتشفير البيانات وسلامتها نفق الشبكة الخاصة الظاهرية (VPN). في حالة إختيار هذا الخيار، يتم تمكين إعدادات التكوين ضمن منطقة معلمات النهج اليدوي. انقر هنا لتكوين الإعدادات اليدوية.

ملاحظة: على سبيل المثال، تم إختيار "تلقائي".

تكوين الإعدادات التلقائية

الخطوة 1. في منطقة خيارات المرحلة الأولى، أختر مجموعة Diffie-Hellman (DH) المناسبة التي سيتم إستخدامها مع المفتاح في المرحلة 1 من القائمة المنسدلة لمجموعة DH. Diffie-Hellman هو بروتوكول تبادل مفاتيح مشفر يتم إستخدامه في الاتصال لتبادل مجموعات المفاتيح المشتركة مسبقا. يتم تحديد قوة الخوارزمية بواسطة وحدات بت. الخيارات هي:

- المجموعة 1 - 768 بت — يحسب المفاتيح أبطأ، لكنه أكثر أمانا من المجموعة 2.
- المجموعة 2 - 1024 بت — يحسب المفاتيح ببطء، لكنها الأكثر أمانا.
- المجموعة 5 - 1536-بت — تحسب المفاتيح بطيء، لكنها الأكثر أمانا.

ملاحظة: في هذا المثال، يتم إختيار المجموعة 2-1024.

الخطوة 2. من القائمة المنسدلة للتشفير، أختر طريقة التشفير المناسبة لتشفير حمولة الأمان (ESP) وفك تشفيرها واقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP). الخيارات هي:

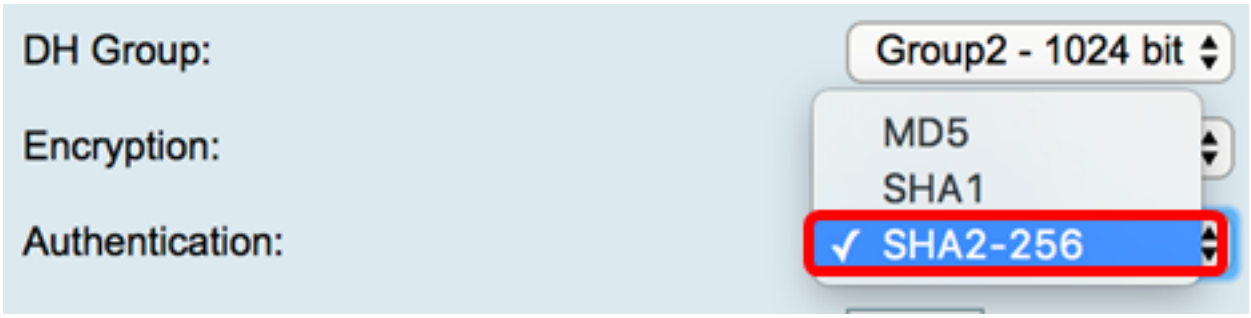
- معيار 3DES — المعيار الثلاثي لتشفير البيانات.
- الطراز AES-128 — يستخدم معيار التشفير المتقدم مفتاح إصدار 128 بت.
- AES-192 — يستخدم معيار التشفير المتقدم مفتاح 192-بت.
- الطراز AES-256 — يستخدم معيار التشفير المتقدم مفتاح إصدار 256 بت.

ملاحظة: AES هي الطريقة القياسية للتشفير عبر DES و 3DES لزيادة أدائه وأمنه. سيؤدي إطالة مفتاح AES إلى زيادة الأمان باستخدام أداء منخفض. على سبيل المثال، يتم إختيار AES-256.

الخطوة 3. من القائمة المنسدلة للمصادقة، أختر أسلوب مصادقة يحدد كيفية مصادقة ESP و ISAKMP. الخيارات هي:

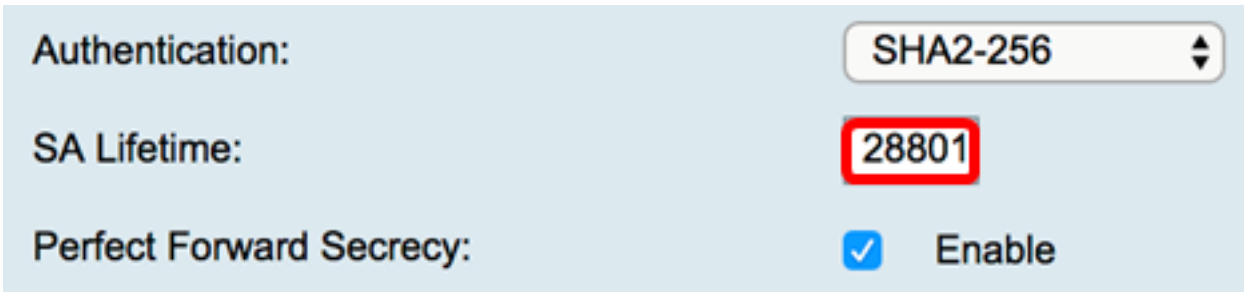
- MD5 — خوارزمية ملخص الرسالة تحتوي على قيمة تجزئة 128 بت.
- SHA-1 — تحتوي خوارزمية التجزئة الآمنة على قيمة تجزئة 160-بت.
- SHA2-256 — خوارزمية التجزئة الآمنة مع قيمة تجزئة 256-بت.

ملاحظة: MD5 و SHA هما دالتا تجزئة مشفرتان. تأخذ قطعة من البيانات، تضغطها، وتنشئ مخرجات سداسية عشرية فريدة لا يمكن إعادة إنتاجها. في هذا المثال، يتم إختيار SHA2-256.

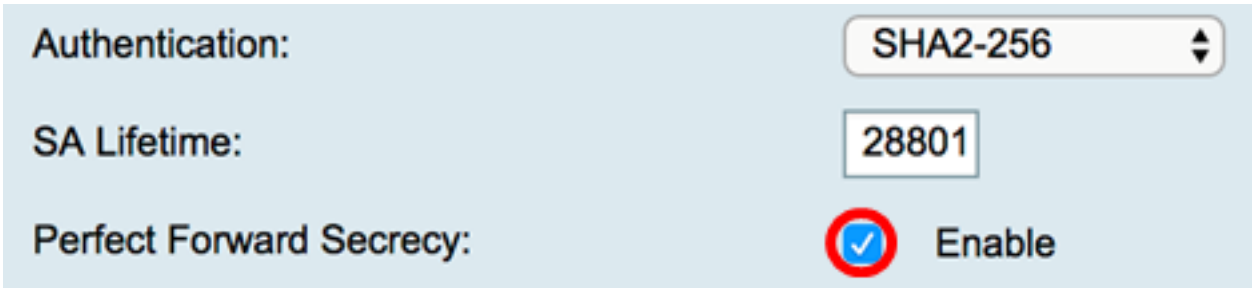


الخطوة 4. في حقل *عمر SA*، أدخل قيمة تتراوح بين 120 و 86400. هذه هي المدة الزمنية التي سيظل فيها اقتران أمان تبادل مفاتيح الإنترنت (IKE) نشطا في هذه المرحلة. القيمة الافتراضية هي 28800.

ملاحظة: في هذا المثال، يتم إستخدام 28801.

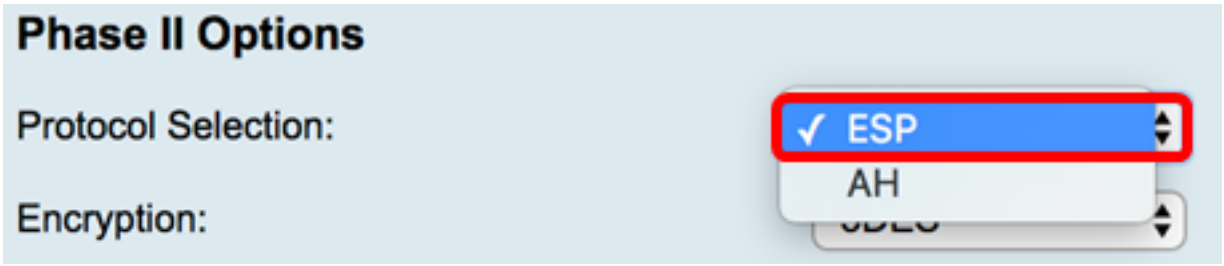


الخطوة 5. (إختياري) حدد خانة الاختيار **enable perfect forward secret** لإنشاء مفتاح جديد لتشفير حركة مرور IPSec والمصادقة.



الخطوة 6. من القائمة المنسدلة تحديد البروتوكول في منطقة خيارات المرحلة الثانية، أختر نوع بروتوكول لتطبيقه على المرحلة الثانية من التفاوض. الخيارات هي:

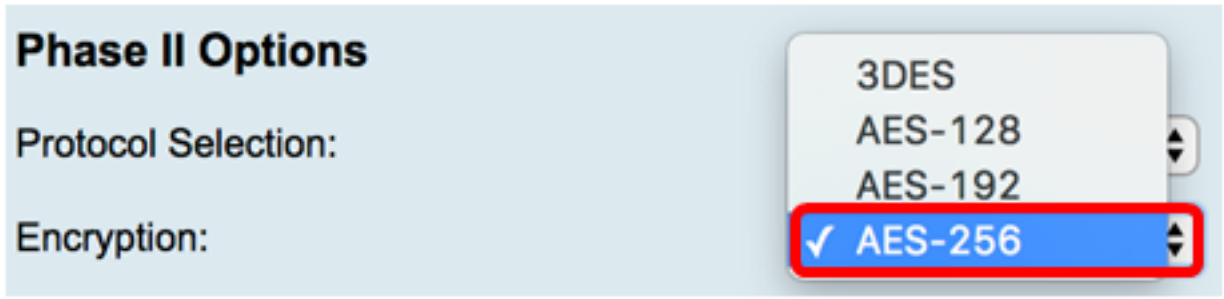
- ESP — إذا تم إختيار هذا الخيار، فانتقل إلى الخطوة 7 لاختيار طريقة تشفير حول كيفية تشفير حزم ESP وفك تشفيرها. بروتوكول أمان يوفر خدمات خصوصية البيانات ومصادقة البيانات الاختيارية والخدمات المضادة لإعادة التشغيل. يقوم ESP بتضمين البيانات المراد حمايتها.
- AH — رأس المصادقة (AH) هو بروتوكول أمان يوفر مصادقة البيانات والخدمات الاختيارية المضادة لإعادة التشغيل. تم تضمين AH في البيانات التي سيتم حمايتها (مخطط بيانات IP كامل). تخطي الخطوة 8 إذا تم إختيار هذا الخيار.



الخطوة 7. إذا تم إختيار ESP في الخطوة 6، فأختر طريقة التشفير المناسبة لتشفير ESP و ISAKMP وفك تشفيرهما من القائمة المنسدلة للتشفير. الخيارات هي:

- معيار 3DES — المعيار الثلاثي لتشفير البيانات.
- الطراز AES-128 — يستخدم معيار التشفير المتقدم مفتاح إصدار 128 بت.
- AES-192 — يستخدم معيار التشفير المتقدم مفتاح 192-بت.
- الطراز AES-256 — يستخدم معيار التشفير المتقدم مفتاح إصدار 256 بت.

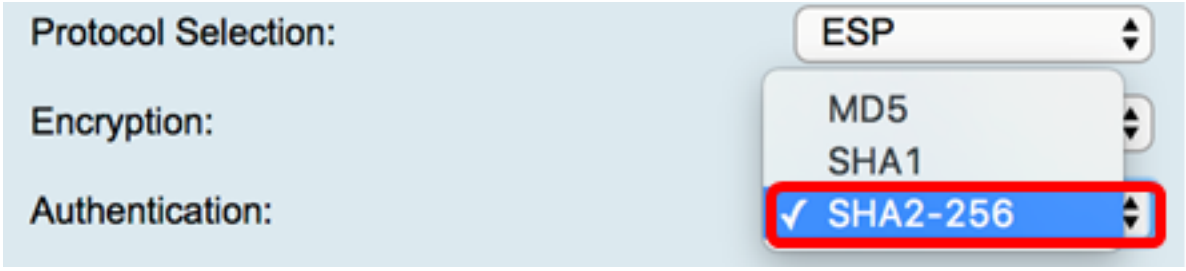
ملاحظة: في هذا المثال، يتم إختيار AES-256.



الخطوة 8. من القائمة المنسدلة للمصادقة، أختر أسلوب مصادقة يحدد كيفية مصادقة ESP و ISAKMP. الخيارات هي:

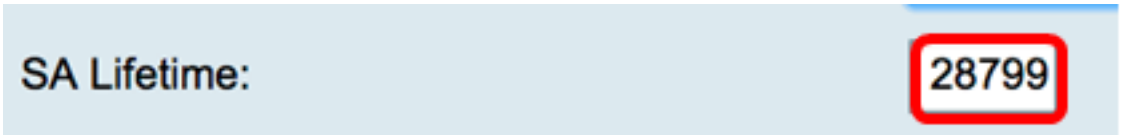
- MD5 — خوارزمية ملخص الرسالة تحتوي على قيمة تجزئة 128 بت.
- SHA-1 — تحتوي خوارزمية التجزئة الآمنة على قيمة تجزئة 160-بت.
- SHA2-256 — خوارزمية التجزئة الآمنة مع قيمة تجزئة 256-بت.

ملاحظة: في هذا المثال، يتم إستخدام SHA2-256.



الخطوة 9. في حقل *عمر SA*، أدخل قيمة تتراوح بين 120 و 28800. هذا هو طول المدة التي سيظل فيها IKE SA نشطا في هذه المرحلة. القيمة الافتراضية هي 3600.

ملاحظة: في هذا المثال، يتم إستخدام 28799.

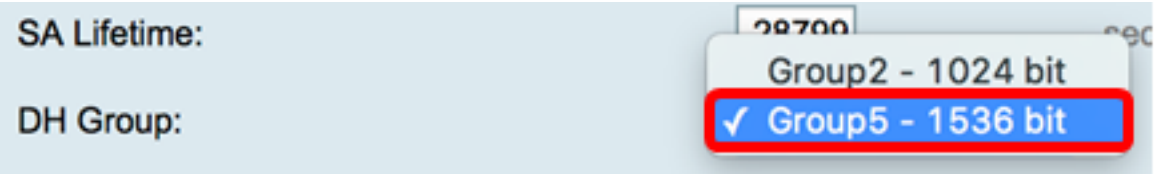


الخطوة 10. من القائمة المنسدلة لمجموعة DH، أختر مجموعة Diffie-Hellman (DH)

المناسبة التي سيتم إستخدامها مع المفتاح في المرحلة 2. الخيارات هي:

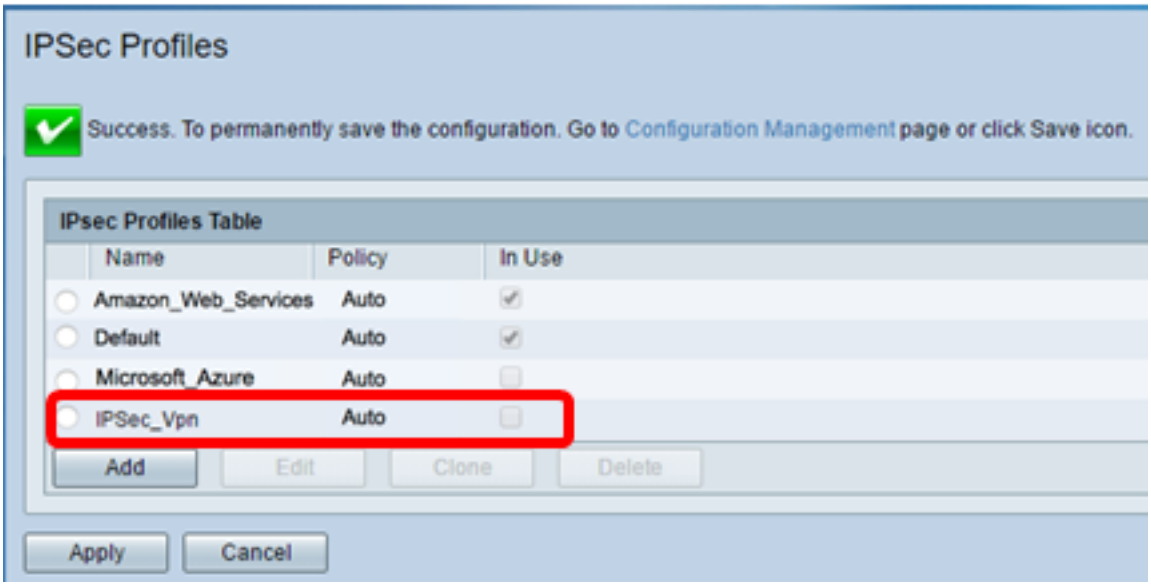
1. المجموعة 2 - 1024 بت — يحسب المفتاح أبطأ، لكنه أكثر أمانا من المجموعة
- المجموعة 5 - 1536 بت — يحسب المفتاح أبطأ، لكنه الأكثر أمانا.

ملاحظة: في هذا المثال، يتم إختيار Group5 - 1536 بت.



الخطوة 11. طقطقة Apply.

ملاحظة: ستتم إعادتك إلى جدول ملفات تعريف IPSec ويجب أن يظهر ملف تعريف IPSec الذي تم إنشاؤه حديثا الآن.



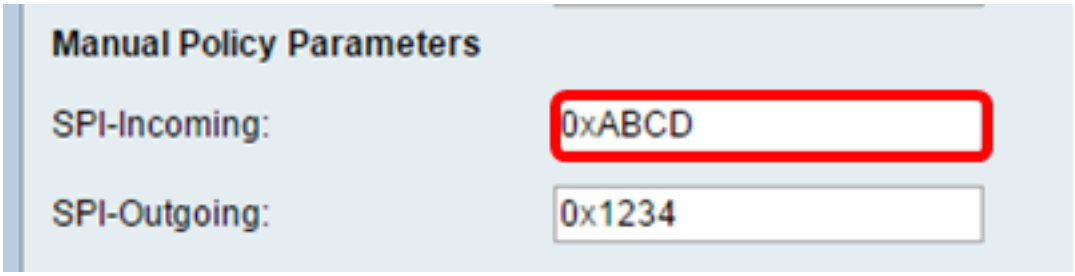
الخطوة 12. (إختياري) لحفظ التكوين بشكل دائم، انتقل إلى صفحة نسخ/حفظ التكوين أو انقر فوق Save الرمز في الجزء العلوي من الصفحة.

يجب أن تكون قد انتهيت الآن من تكوين ملف تعريف IPSec تلقائي بنجاح على موجه من السلسلة RV34x.

تكوين الإعدادات اليدوية

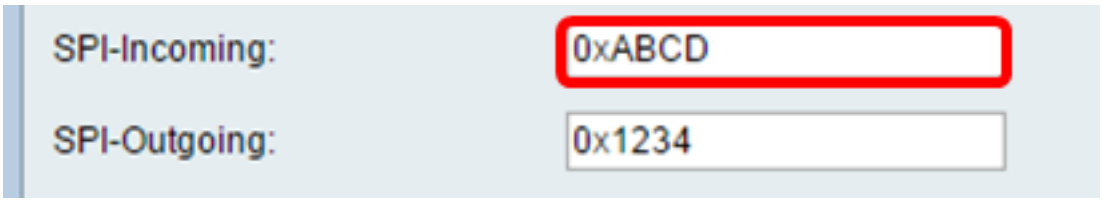
الخطوة 1. في حقل *SPI-Incoming*، أدخل رقم سداسي عشري يتراوح من 100 إلى FFFFF للعلامة فهرس معلمات الأمان (SPI) لحركة المرور الواردة على اتصال VPN. ال SPI استعملت بطاقة أن يميز الحركة مرور من واحد جلسة من الحركة مرور من آخر جلسة.

ملاحظة: لهذا المثال، يتم إستخدام 0xABCD.



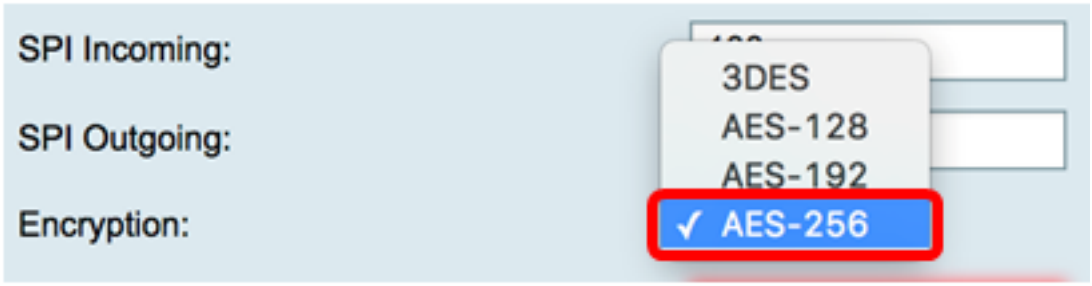
الخطوة 2. في حقل *SPI-Outgoing*، أدخل رقما سداسيا عشريا تراوح من 100 إلى FFFFF لعلامة SPI لحركة المرور الصادرة على اتصال VPN.

ملاحظة: لهذا المثال، يتم إستخدام 0x1234.



الخطوة 3. أختر خيارا من القائمة المنسدلة للتشفير. الخيارات هي 3DES و AES-128 و AES-192 و AES-256.

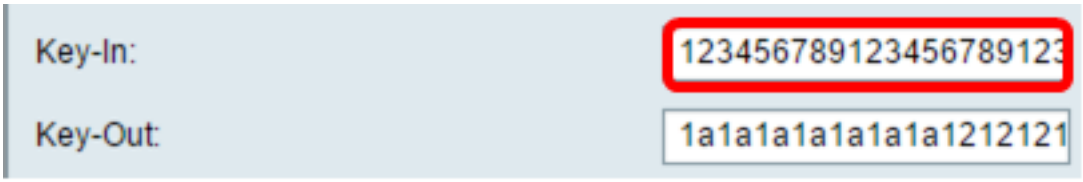
ملاحظة: في هذا المثال، يتم إختيار AES-256.



الخطوة 4. أدخل في حقل *المفتاح* مفتاح للنهج الوارد. يعتمد طول المفتاح على الخوارزمية المختارة في الخطوة 3.

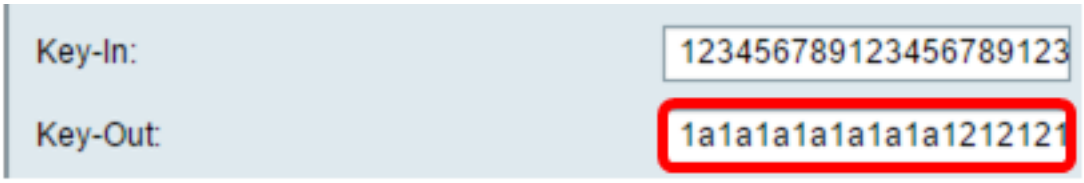
- يستخدم معيار 3DES مفتاح مكون من 48 حرف.
- يستخدم AES-128 مفتاح 32 حرفا.
- يستخدم AES-192 مفتاح مكون من 48 حرف.
- يستخدم AES-256 مفتاح 64 حرف.

ملاحظة: في هذا المثال، يتم إستخدام 123456789123456789123.



الخطوة 5. دخلت في *المفتاح خارج* مجال، مفتاح للنهج الصادر. يعتمد طول المفتاح على الخوارزمية المختارة في الخطوة 3.

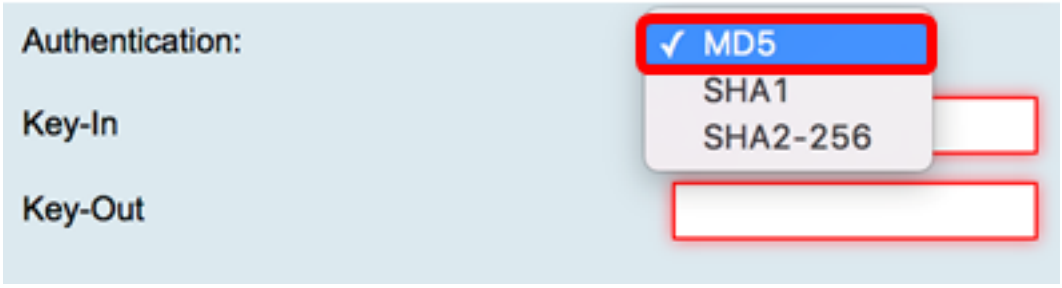
ملاحظة: في هذا المثال، يتم إستخدام 1a1a1a1a1a1a1a1a121212...



الخطوة 6. أختر خيارا من القائمة المنسدلة لخوارزمية التكامل اليدوية.

- MD5 — يستخدم قيمة تجزئة 128 بت لسلامة البيانات. يتميز الطراز MD5 بقدر أقل من الأمان ولكنه أسرع من الطرازين SHA-1 و SHA2-256.
- SHA-1 — يستخدم قيمة تجزئة 160 بت لسلامة البيانات. ويعد الطراز SHA-1 أبطأ ولكنه أكثر أمانا من الطراز MD5، كما أن الطراز SHA-1 أكثر سرعة ولكنه أقل أمانا من الطراز SHA2-256.
- SHA2-256 — يستخدم قيمة تجزئة 256 بت لسلامة البيانات. SHA2-256 أبطأ ولكنه آمن من MD5 و SHA-1.

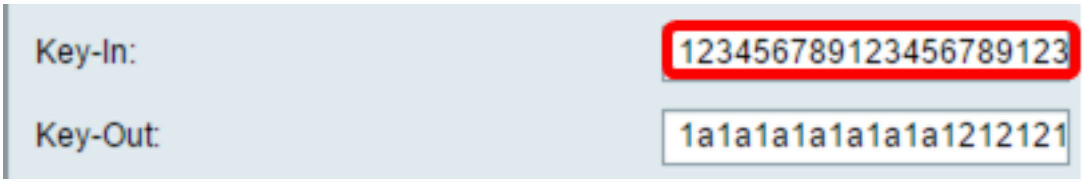
ملاحظة: في هذا المثال، يتم إختيار MD5.



الخطوة 7. دخلت في *المفتاح داخل مجال*، مفتاح للنهج الوارد. يعتمد طول المفتاح على الخوارزمية المختارة في الخطوة 6.

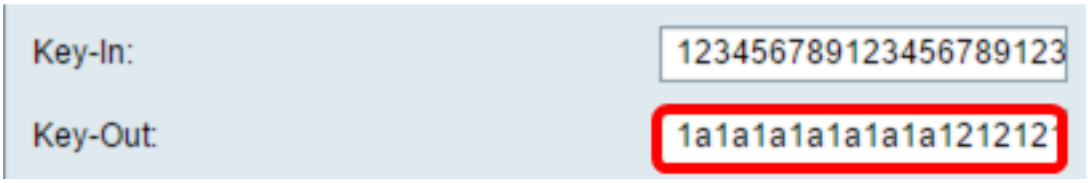
- يستخدم MD5 مفتاح مكون من 32 حرفا.
- يستخدم SHA-1 مفتاح مكون من 40 حرف.
- يستخدم SHA2-256 مفتاح 64 حرفا.

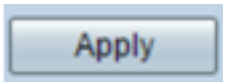
ملاحظة: في هذا المثال، يتم إستخدام 123456789123456789123.



الخطوة 8. دخلت في *المفتاح خارج مجال*، مفتاح للنهج الصادر. يعتمد طول المفتاح على الخوارزمية المختارة في الخطوة 6.

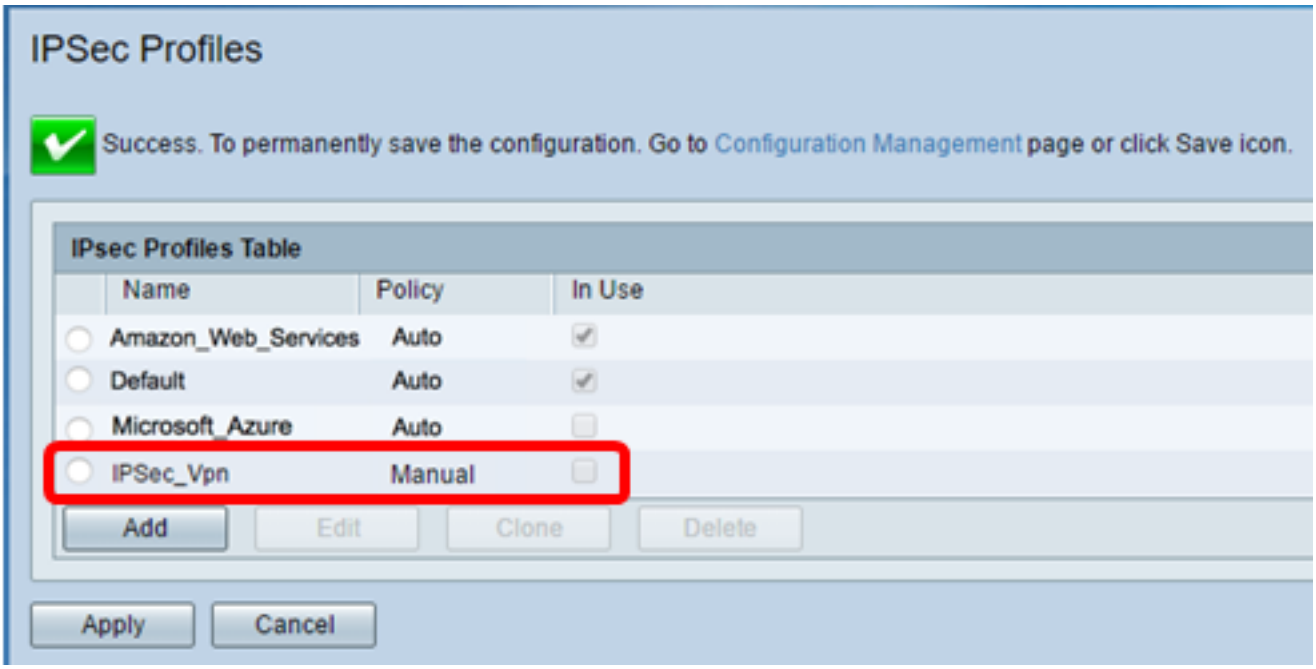
ملاحظة: في هذا المثال، يتم إستخدام 1a1a1a1a1a1a1a1a121212.....



الخطوة 9. طقطقة 

.

ملاحظة: ستتم إعادتك إلى جدول ملفات تعريف IPSec ويجب أن يظهر ملف تعريف IPSec الذي تم إنشاؤه حديثا الآن.



الخطوة 10. (إختياري) لحفظ التكوين بشكل دائم، انتقل إلى صفحة نسخ/حفظ التكوين أو انقر فوق  الرمز في الجزء العلوي من الصفحة.

يجب أن تكون قد انتهيت الآن من تكوين ملف تعريف IPSec يدويا بنجاح على موجه من السلسلة RV34x.

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).