تكوين الإعداد المتقدم للشبكة الخاصة الظاهرية (VPN) على الموجه RV130 وأ RV130W

الهدف

الشبكة الخاصة الظاهرية (VPN) هي اتصال آمن يتم إنشاؤه داخل الشبكة أو بين الشبكات. تعمل شبكات VPN على عزل حركة مرور البيانات بين البيئات المضيفة والشبكات غير المصرح بها. والشبكات المحددة من حركة مرور البيئات المضيفة تتصل شبكة VPN من موقع إلى موقع (من بوابة إلى بوابة) بالشبكات الخاصة الظاهرية (VPN) الكاملة بعضها البعض، مما يحافظ على الأمان من خلال إنشاء نفق عبر مجال عام يعرف أيضا باسم الإنترنت. فكل موقع ال يحتاج إلا إلى اتصال محلي بنفس الشبكة العامة، وبالتالي توفير المال على – خطوط مستأجرة خاصة طويلة.

تعود الشبكات الخاصة الظاهرية (VPN) بفائدة على الشركات بطريقة تجعلها قابلة للتوسيع بدرجة كبيرة، وتبسط مخطط الشبكة، وتحسن الإنتاجية من خلال تقليل وقت السفر والتكلفة للمستخدمين عن بعد.

تبادل مفتاح الإنترنت (IKE) هو بروتوكول يستخدم لإنشاء اتصال آمن للاتصال في شبكة VPN. يسمى هذا الاتصال الآمن اقتران أمان (SA). يمكن إنشاء سياسات IKE لتعريف معلمات الأمان المراد إستخدامها في هذه العملية مثل مصادقة النظير وخوارزميات التشفير وما إلى ذلك. لكي تعمل شبكة VPN بشكل صحيح، يجب أن تكون نهج IKE لكل نقطتي النهاية متطابقة.

يهدف هذا المقال إلى عرض كيفية تكوين إعداد VPN المتقدم على موجه RV130 أو RV130W، والذي يغطي إعدادات نهج IKE وإعدادات نهج VPN.

الأجهزة القابلة للتطبيق

·الطراز RV130
· الطراز RV130W

إصدار البرامج

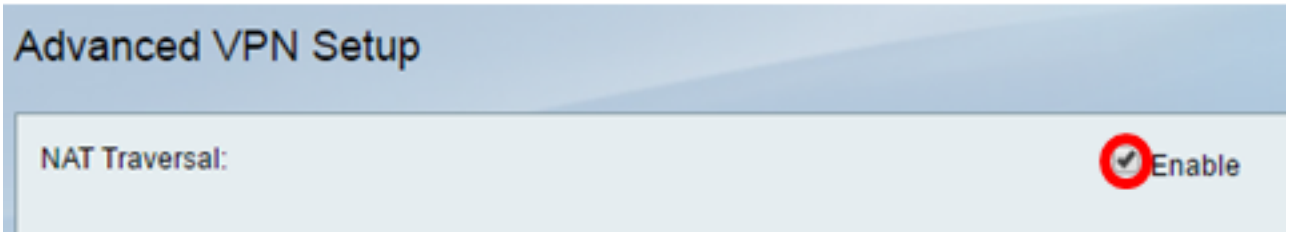
•1.0.3.22

تكوين إعداد VPN المتقدم

إضافة/تحرير إعدادات نهج تبادل مفتاح الإنترنت (IKE)

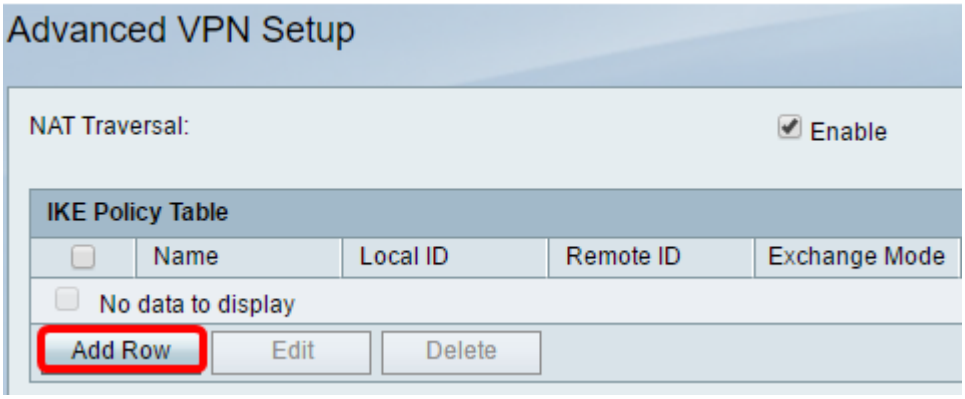
الخطوة 1. سجل الدخول إلى الأداة المساعدة المستندة إلى الويب واختر VPN > VPN من موقع إلى موقع IPSec VPN > إعداد VPN المتقدم.

الخطوة 2. (إختياري) فحص ال **يمكن** تدقيق صندوق في NAT Traversal إن أنت تريد أن إجراء NAT يمكن شبكة ترجمة عنوان (NAT) إجتياز ل ال VPN توصيل. يسمح إجتياز NAT إتصال VPN بين البوابات التي تستخدم NAT. أختر هذا الخيار إذا كان إتصال VPN لديك يمر عبر بوابة تدعم NAT.



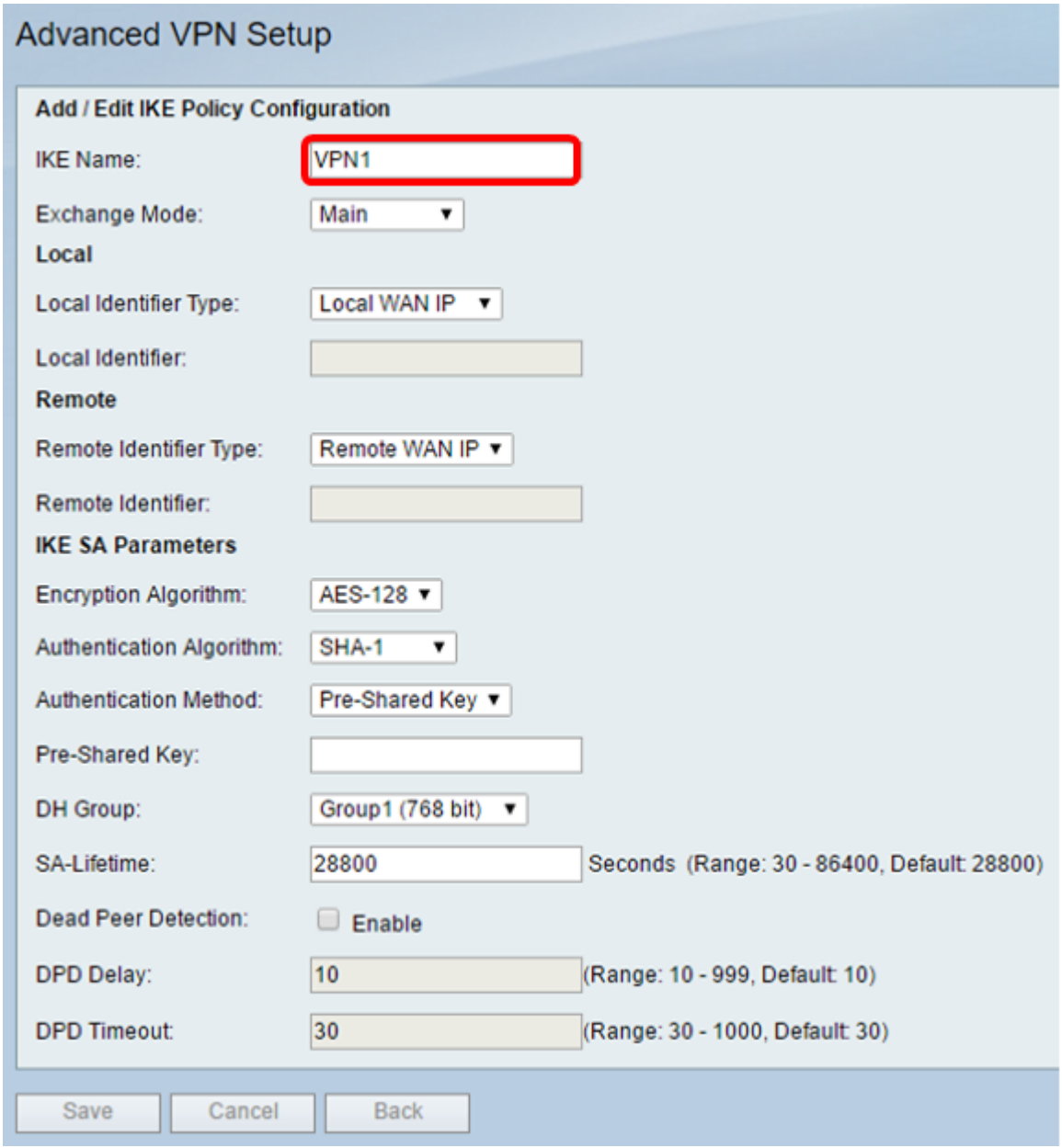
الخطوة 3. في "جدول نهج IKE"، انقر فوق **إضافة صف** لإنشاء نهج IKE جديد.

ملاحظة: إذا تم تكوين الإعدادات الأساسية، فسيحتوي الجدول التالي على إعداد VPN الأساسي الذي تم إنشاؤه. يمكنك تحرير سياسة IKE موجودة عن طريق تحديد خانة الاختيار للنهج ثم انقر فوق **تحرير**. تغييرات صفحة إعداد VPN المتقدمة:



الخطوة 4. في حقل *اسم IKE*، أدخل اسما فريدا لنهج IKE.

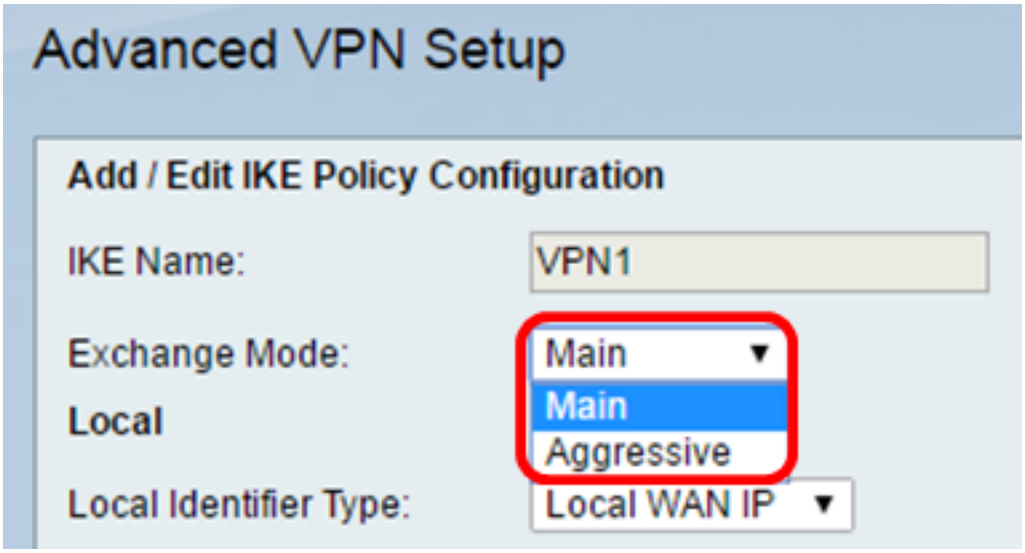
ملاحظة: إذا تم تكوين الإعدادات الأساسية، فسيتم تعيين اسم الاتصال الذي تم إنشاؤه كاسم IKE. في هذا المثال، VPN1 هو اسم IKE المختار.



الخطوة 5. من القائمة المنسدلة وضع Exchange، أختر خيارا.

- رئيسي — يسمح هذا خيار ال IKE سياسة أن يفاوض ال VPN نفق مع أمن أعلى من عدواني أسلوب. انقر على هذا الخيار إذا كان اتصال VPN أكثر أمانا أولوية على سرعة التفاوض.
- عدوانية — يتيح هذا الخيار لسياسة IKE إنشاء اتصال أسرع ولكن أقل أمانا من الوضع الرئيسي. انقر على هذا الخيار إذا كان اتصال الشبكة الخاصة الظاهرية (VPN) الأسرع أولوية على الأمان العالي.

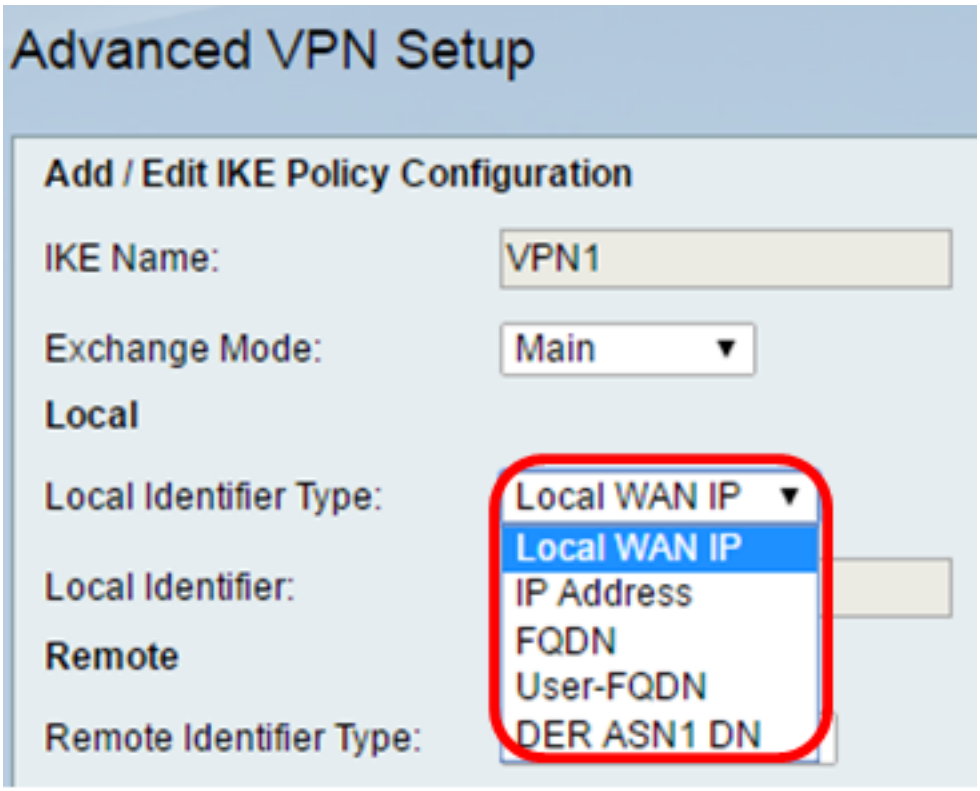
ملاحظة: في هذا المثال، يتم إختيار Main.



الخطوة 6. أختر من القائمة المنسدلة للنوع "معرف محلي" لتحديد أو تحديد اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) للموجه المحلي لديك. الخيارات هي:

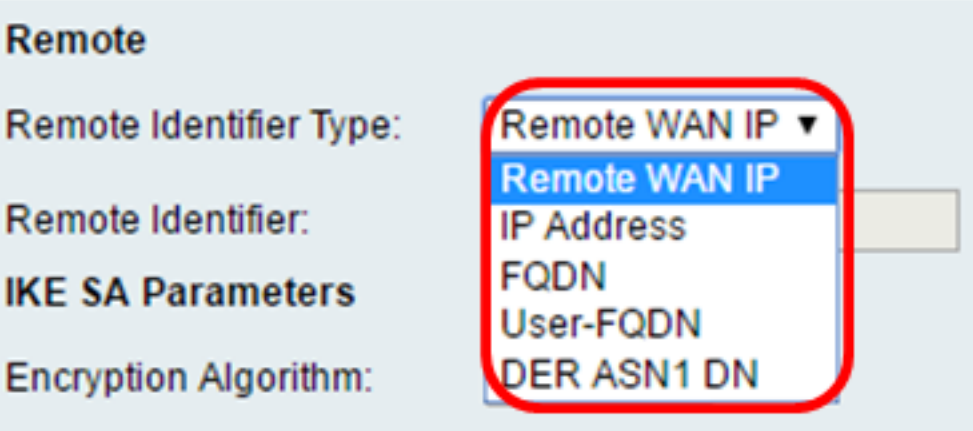
- يستخدم موجه IP لشبكة WAN المحلية عنوان IP (شبكة WAN) كمعرف رئيسي. يتصل هذا الخيار عبر الإنترنت. يؤدي إختيار هذا الخيار إلى إستخراج حقل *المعرف المحلي* أدناه.
- عنوان IP — يسمح النقر فوق هذا بإدخال عنوان IP في حقل *المعرف المحلي*.
- FQDN — يسمح اسم مجال مؤهل بالكامل (FQDN) أو اسم المجال الخاص بك مثل http://www.example.com بإدخال اسم المجال أو عنوان IP الخاص بك في حقل *المعرف المحلي*.
- user-FQDN — هذا الخيار هو عنوان بريد إلكتروني للمستخدم مثل user@email.com. أدخل اسم مجال أو عنوان IP في حقل *المعرف المحلي*.
- DER ASN1 DN — هذا الخيار هو نوع معرف للاسم المميز (DN) الذي يستخدم تدوين صياغة تجريدي لقواعد الترميز المميزة (DER ASN1) لإرسال المعلومات. يحدث ذلك عندما يكون نفق VPN مقترنا بشهادة مستخدم. إذا تم إختيار هذا الخيار، فأدخل اسم مجال أو عنوان IP في حقل *المعرف المحلي*.

ملاحظة: في هذا المثال، يتم إختيار IP لشبكة WAN المحلية.



الخطوة 7. أختر من القائمة المنسدلة "نوع المعرف البعيد" لتحديد اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) للموجه البعيد لديك أو تعيينه. الخيارات هي عنوان IP و IP و FQDN و FQDN للمستخدم و DER ASN1 DN عن بعد.

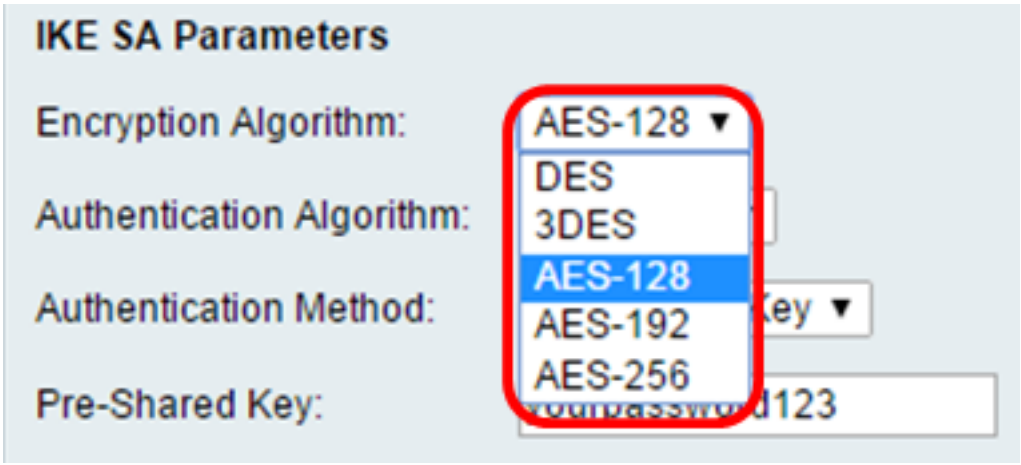
ملاحظة: في هذا المثال، يتم إختيار IP لشبكة WAN البعيدة.



الخطوة 8. أختر خيارا من القائمة المنسدلة لخوارزمية التشفير.

- DES — معيار تشفير البيانات (DES) هو طريقة تشفير قديمة من فئة 56 بت ليست طريقة تشفير آمنة للغاية، ولكنها قد تكون مطلوبة للتوافق مع الإصدارات السابقة.
- 3DES — معيار تشفير البيانات الثلاثي (3DES) هو طريقة تشفير بسيطة 168-بت تستخدم لزيادة حجم المفتاح لأنها تقوم بتشفير البيانات ثلاث مرات. يوفر ذلك أمانا أكثر من DES ولكن أمان أقل من AES.
- AES-128 — يستخدم معيار التشفير المتقدم مع مفتاح 128-بت (AES-128) مفتاح 128-بت لتشفير AES. يتميز نظام التشفير المتطور (AES) بأنه أكثر سرعة وأمنا من نظام اكتشاف التشفير المتطور (DES). وبشكل عام، يعتبر معيار التشفير المتطور أكثر سرعة وأمنا من معيار تشفير البيانات الثلاثي (AES-128. (3DES هو خوارزمية التشفير الافتراضية وهو أسرع ولكنه أقل أمانا من AES-192 و AES-256.
- AES-192 — يستخدم AES-192 مفتاح 192-بت لتشفير AES. يتميز الطراز AES-192 بأنه أكثر بطئا وأمنا مقارنة بالطراز AES-128، كما أنه أسرع ولكن أقل أمانا من الطراز AES-256.
- AES-256 — يستخدم AES-256 مفتاح 256-بت لتشفير AES. يتميز الطراز AES-256 بأنه أكثر بطئا ولكنه أكثر أمانا من الطرازين AES-128 و AES-192.

ملاحظة: في هذا المثال، يتم تحديد AES-128.

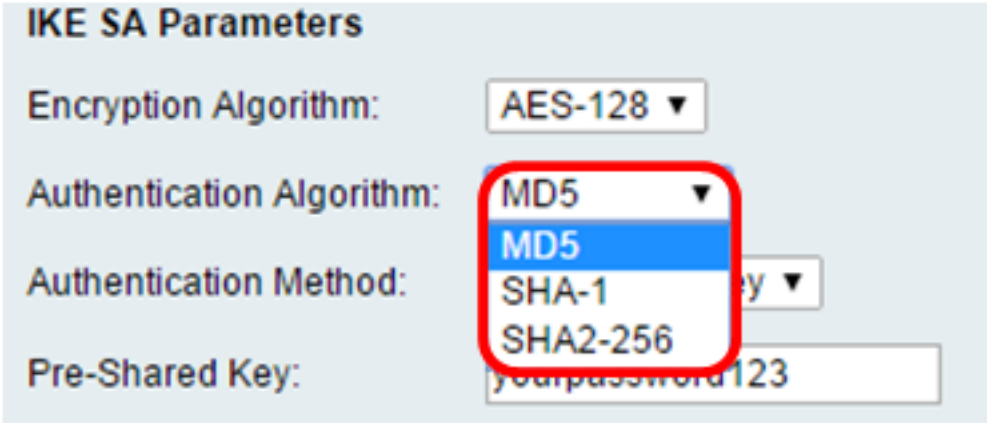


الخطوة 9. من القائمة المنسدلة لخوارزمية المصادقة، أختر من الخيارات التالية:

- MD5 — Message Digest 5 (MD5) هي خوارزمية مصادقة تستخدم قيمة تجزئة 128 بت للمصادقة. الطراز MD5 أقل أمانا، ولكنه أسرع من الطرازين SHA-1 و SHA2-256.

- SHA-1 — تستخدم وظيفة التجزئة الآمنة 1 (SHA-1) قيمة تجزئة 160 بت للمصادقة. SHA-1 أبطأ ولكنه أكثر أمانا من MD5. SHA-1 هو خوارزمية المصادقة الافتراضية وهو أسرع ولكنه أقل أمانا من SHA2-256.
- SHA2-256 — تستخدم خوارزمية التجزئة الآمنة 2 مع قيمة تجزئة 256 بت (SHA2-256) قيمة تجزئة 256 بت للمصادقة. يتميز الطراز SHA2-256 بأنه أكثر بطئا وأمانا مقارنة بالطرازين MD5 و SHA-1.

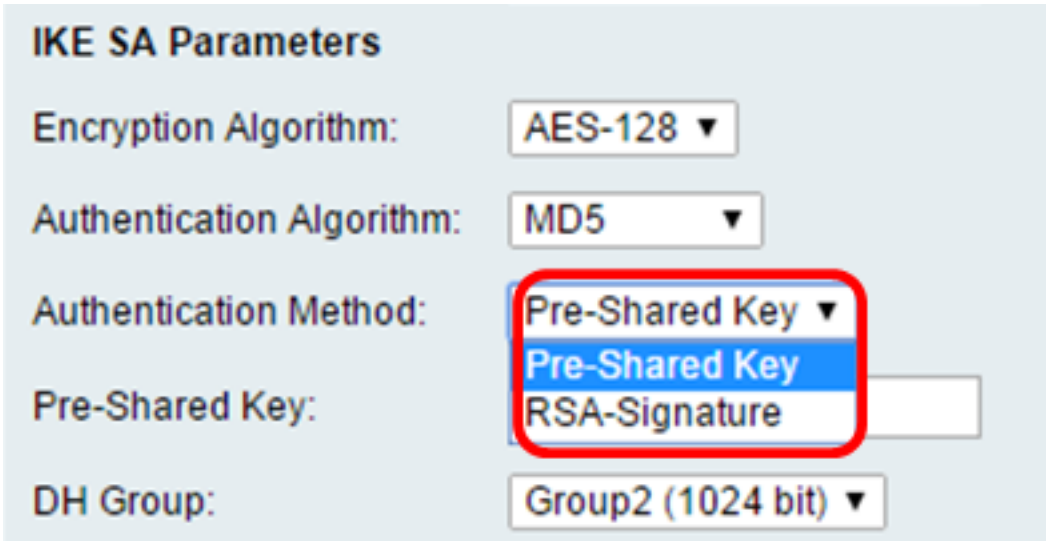
ملاحظة: في هذا المثال، يتم إختيار MD5.



الخطوة 10. في القائمة المنسدلة لطريقة المصادقة، أختر من الخيارات التالية:

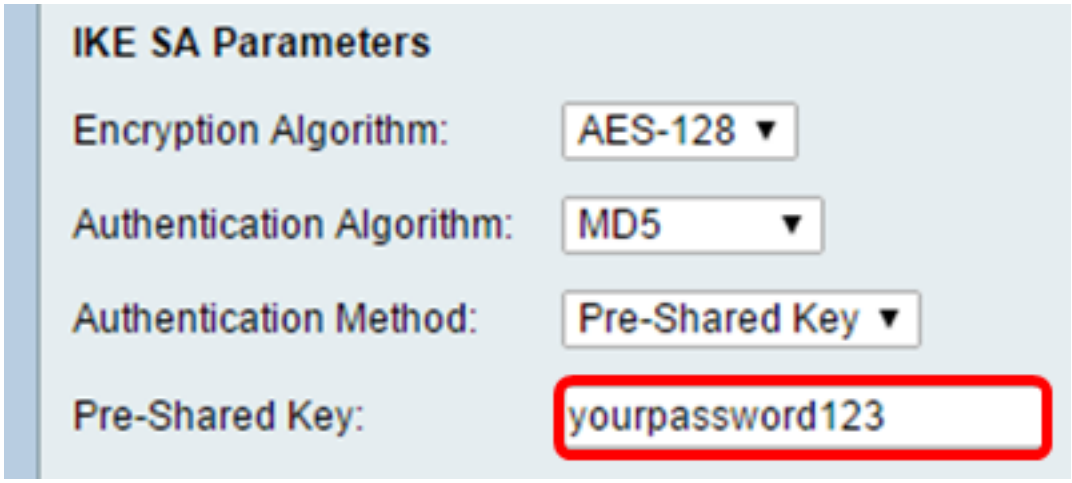
- مفتاح مشترك مسبقا — يتطلب هذا الخيار كلمة مرور تتم مشاركتها مع نظير IKE.
- توقيع RSA — يستخدم هذا الخيار شهادات لمصادقة التوصيل. إذا تم إختيار هذا الخيار، يتم تعطيل حقل مفتاح مشترك مسبقا. تخطي الخطوة 12.

ملاحظة: في هذا المثال، يتم إختيار مفتاح مشترك مسبقا.



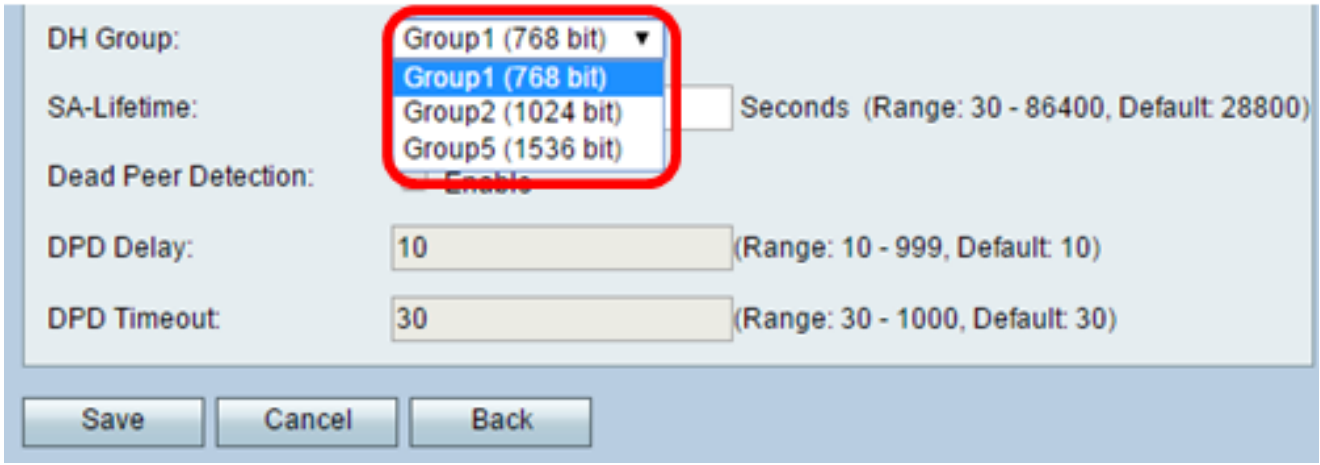
الخطوة 11. في حقل *مفتاح مشترك مسبقا*، أدخل كلمة مرور يتراوح طولها بين 8 و 49 حرفا.

ملاحظة: في هذا المثال، يتم إستخدام كلمة المرور 123.

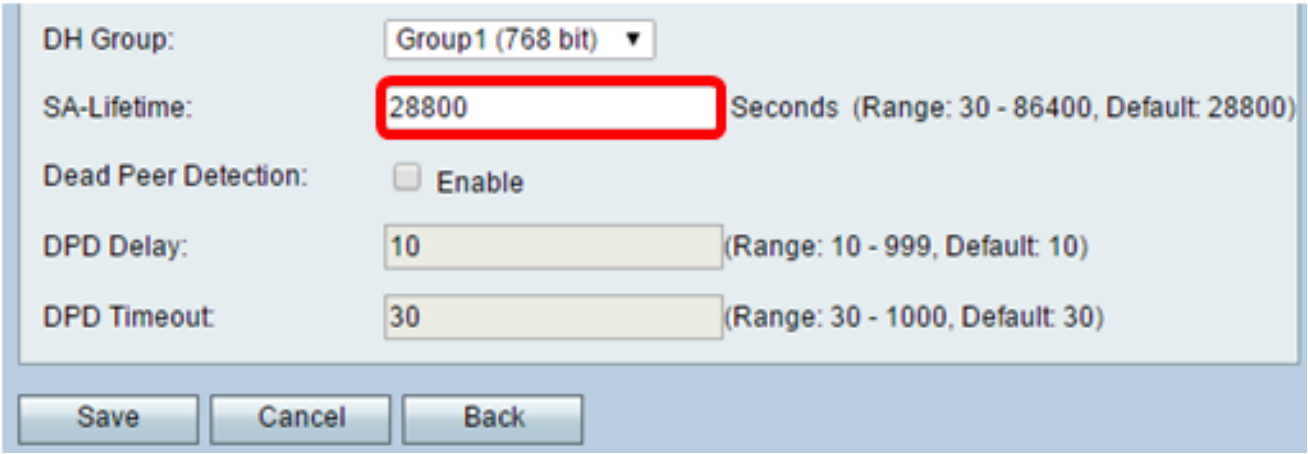


الخطوة 12. من القائمة المنسدلة لمجموعة DH، أختر خوارزمية مجموعة DH (Diffie-Hellman) التي تستخدمها IKE. يمكن للمضيفين في مجموعة DH تبادل المفاتيح دون معرفة بعضهم البعض. كلما كان رقم بت المجموعة أعلى، كلما كان الأمان أفضل.

ملاحظة: في هذا المثال، يتم إختيار المجموعة 1.

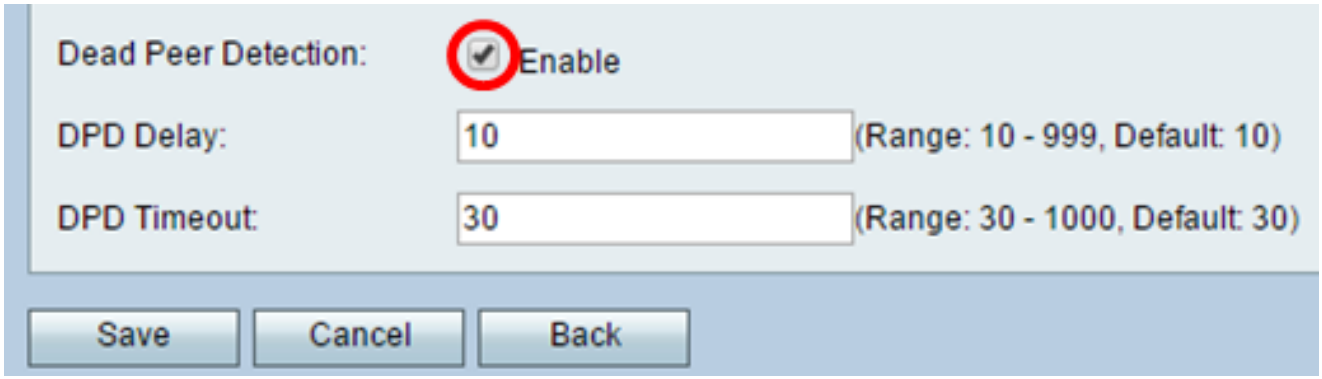


الخطوة 13. في حقل *SA-Life*، أدخل المدة التي تستمر فيها sa بالثواني ل VPN قبل تجديد SA. المدى from 30 to 86400 ثاني. الافتراضي هو 28800.



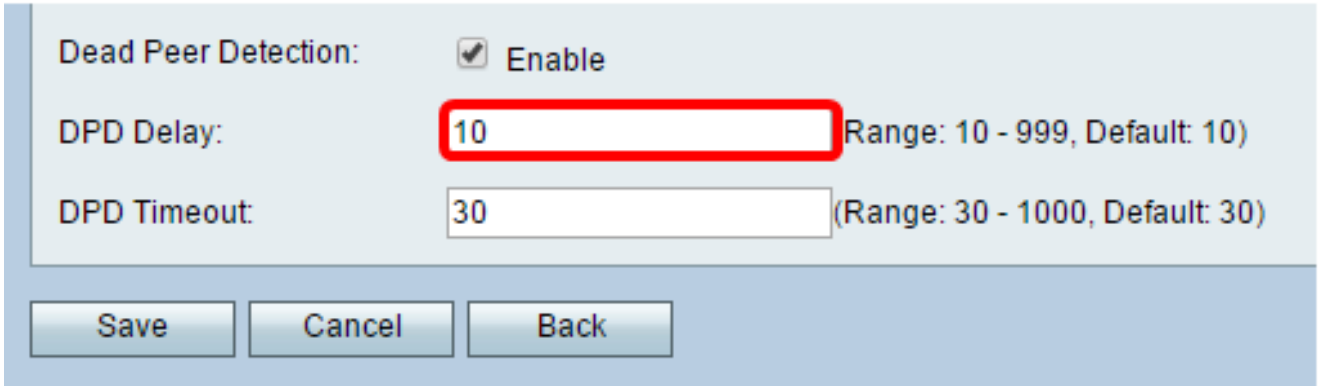
الخطوة 14. (إختياري) حدد خانة الاختيار **تمكين** اكتشاف النظير غير الصحيح لتمكين اكتشاف النظير (DPD). يراقب DPD نظراء IKE ليروا ما إذا كان النظير قد توقف عن العمل أو لا يزال حيا. إذا تم الكشف عن النظير على أنه معطل، يقوم الجهاز بحذف اقتران أمان IPsec و IKE. يمنع DPD إهدار موارد الشبكة على الأقران غير الناشطين.

ملاحظة: إذا لم تكن ترغب في تمكين كشف النظير الميت، انتقل إلى الخطوة 17.



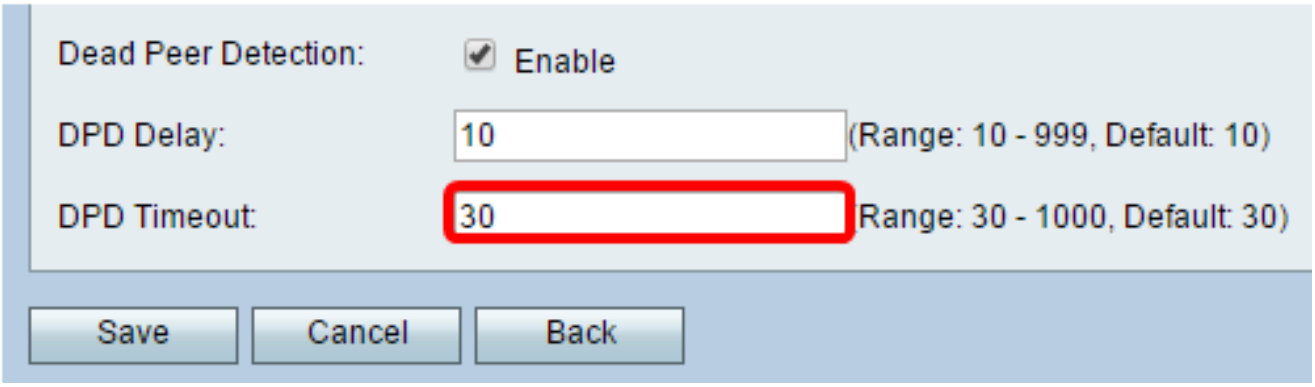
الخطوة 15. (إختياري) إذا قمت بتمكين DPD في الخطوة 14، فأدخل عدد المرات (بالثواني) التي يتم فيها التحقق من النشاط في حقل *تأخير DPD*.

ملاحظة: تأخر DPD هو الفاصل الزمني بالثواني بين رسائل DPD R-U-THERE المتتالية. يتم إرسال رسائل DPD R-U-THERE فقط عندما تكون حركة مرور IPsec خاملة. القيمة الافتراضية هي 10.

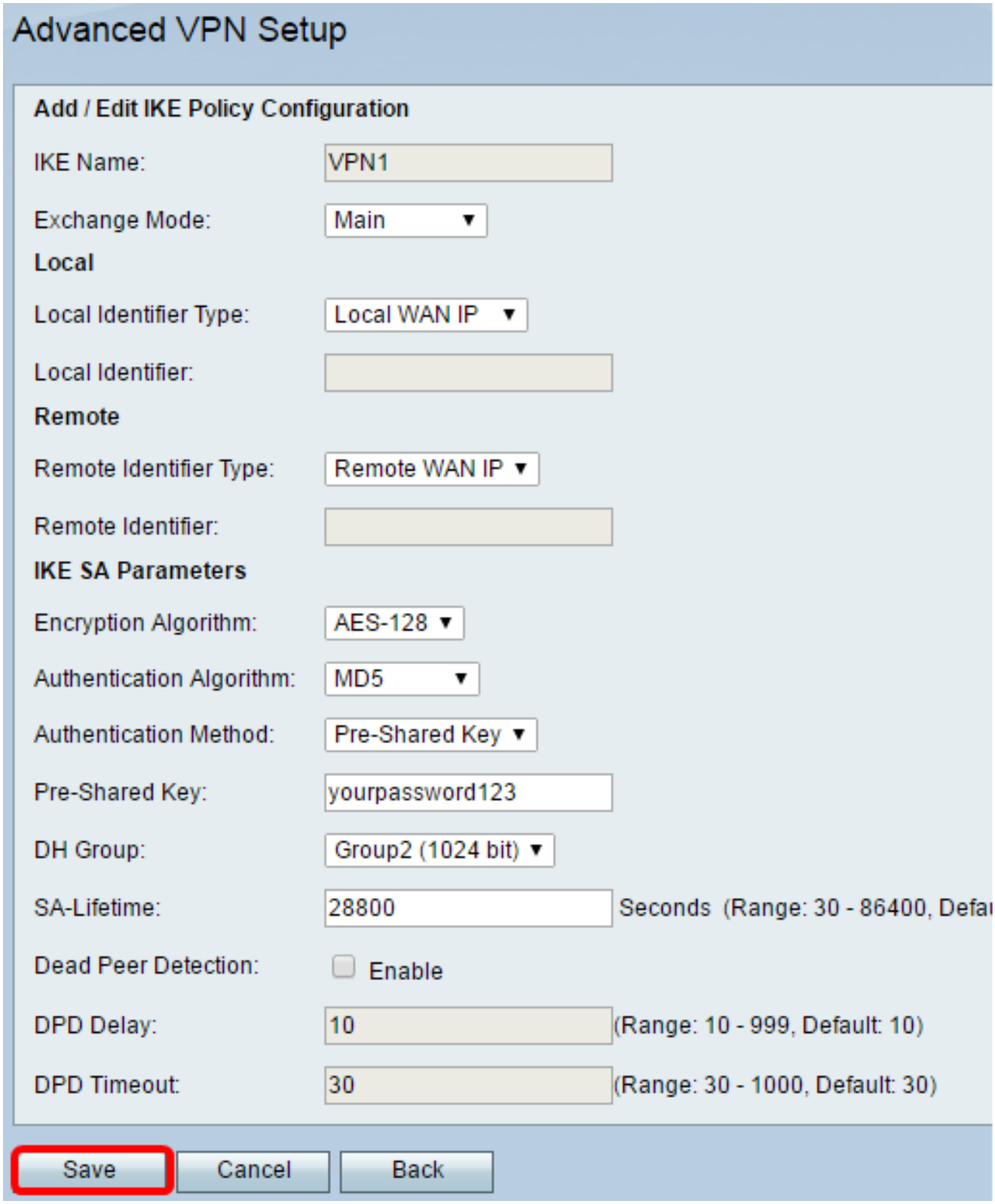


الخطوة 16. (إختياري) إذا قمت بتمكين DPD في الخطوة 14، فأدخل عدد الثواني التي يجب انتظارها قبل إسقاط النظير غير النشط في حقل *مهلة DPD*.

ملاحظة: هذا هو الحد الأقصى للوقت الذي يجب أن ينتظر فيه الجهاز لتلقي إستجابة لرسالة DPD قبل إعتبار النظير ميتا. القيمة الافتراضية هي 30.



الخطوة 17. طقطقة **حفظ**.



ملاحظة: تظهر صفحة إعداد VPN المتقدمة الرئيسية مرة أخرى.

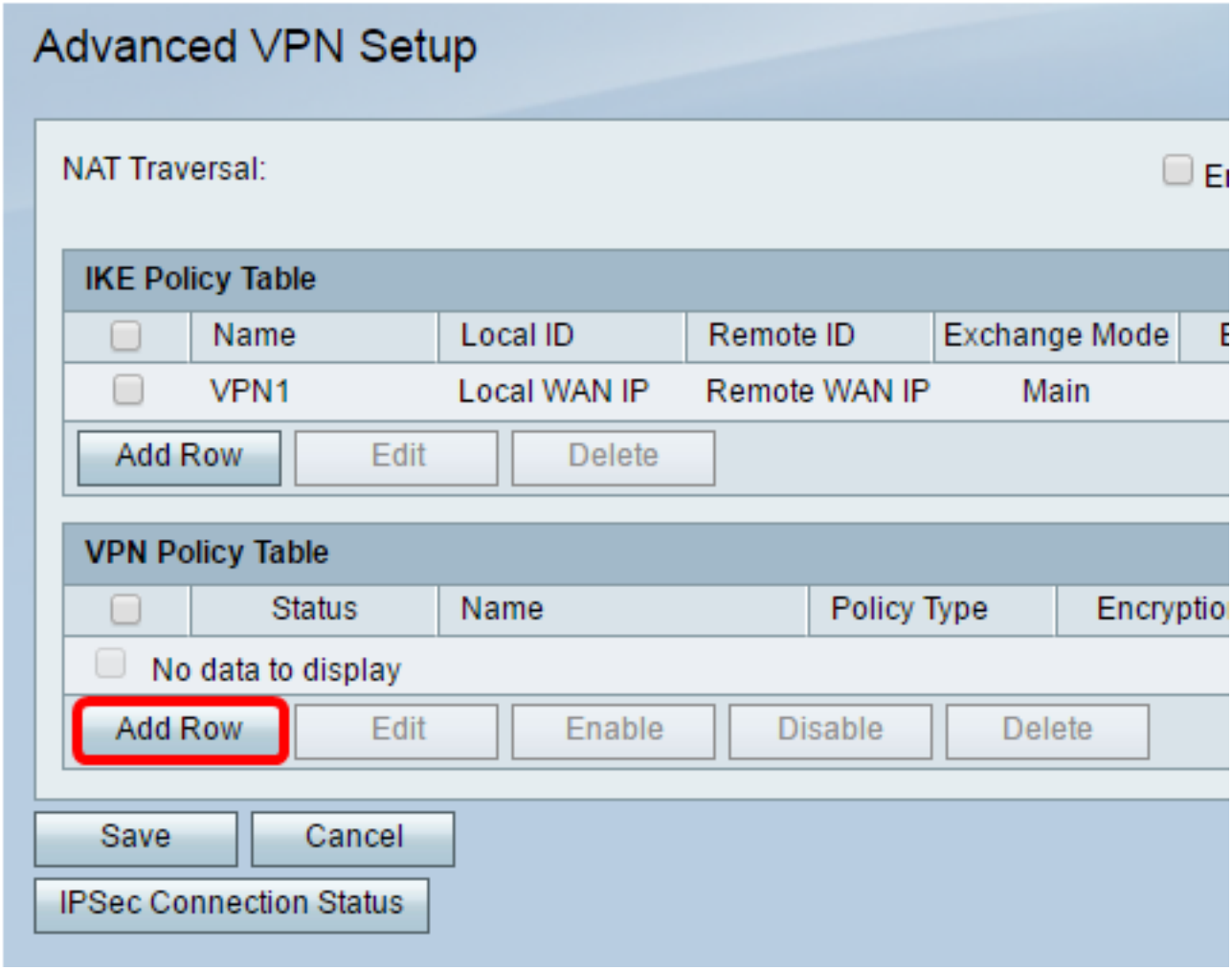
يجب أن تكون قد انتهيت الآن من تكوين إعدادات نهج IKE بنجاح على الموجه.

تكوين إعدادات نهج VPN

ملاحظة: لكي تعمل شبكة VPN بشكل صحيح، يجب أن تكون سياسات شبكات VPN لكلا نقطتي النهاية متطابقة.

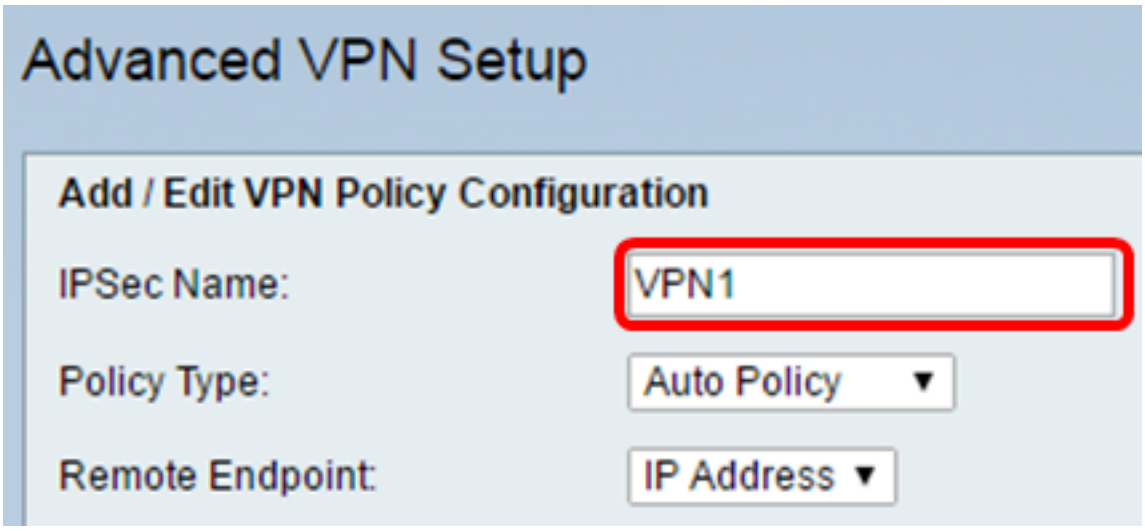
الخطوة 1. في "جدول سياسة شبكة VPN"، انقر فوق **إضافة صف** لإنشاء سياسة شبكة VPN جديدة.

ملاحظة: يمكنك أيضا تحرير سياسة VPN عن طريق تحديد خانة الاختيار للنهج وانقر فوق **تحرير**. سوف تظهر صفحة إعداد VPN المتقدم:



الخطوة 2. في حقل *اسم IPSec* ضمن منطقة تكوين إضافة/تحرير VPN، أدخل اسما لنهج VPN.

ملاحظة: في هذا المثال، يتم إستخدام VPN1.



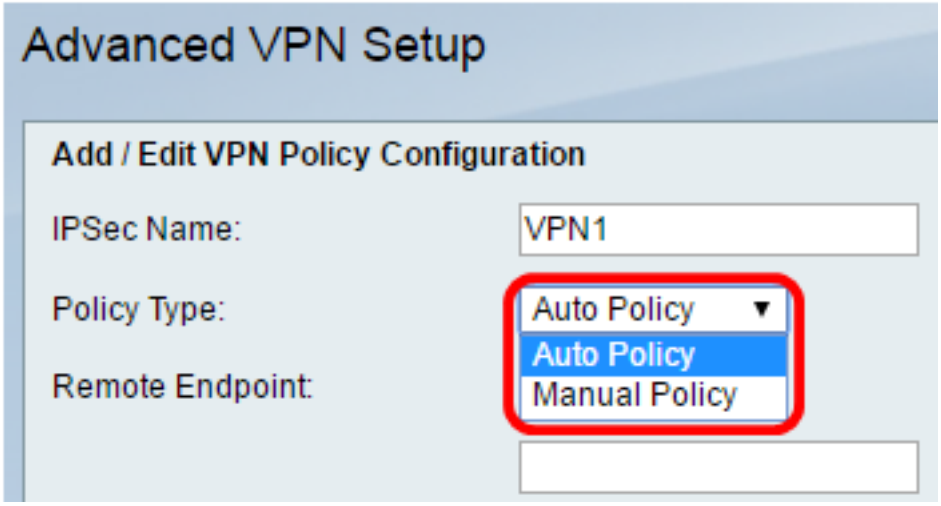
الخطوة 3. من القائمة المنسدلة "نوع النهج"، أختر خيارا.

- نهج يدوي — يسمح هذا الخيار لك بتكوين المفاتيح يدويا لتشفير البيانات وسلامتها لنفق VPN. في حالة إختيار هذا الخيار، يتم تمكين إعدادات التكوين ضمن منطقة معلمات النهج اليدوي. تابع الخطوات حتى يتم تحديد حركة

المرور عن بعد. انقر هنا لمعرفة الخطوات.

- النهج التلقائي — يتم تعيين معلمات النهج تلقائيا. يستخدم هذا الخيار سياسة IKE لسلامة البيانات وتشفيرها لعمليات تبادل المفاتيح. في حالة إختيار هذا الخيار، يتم تمكين إعدادات التكوين ضمن منطقة معلمات النهج التلقائي. انقر هنا لمعرفة الخطوات. تأكد من أن بروتوكول IKE الخاص بك يتفاوض تلقائيا بين نقطتي نهاية VPN.

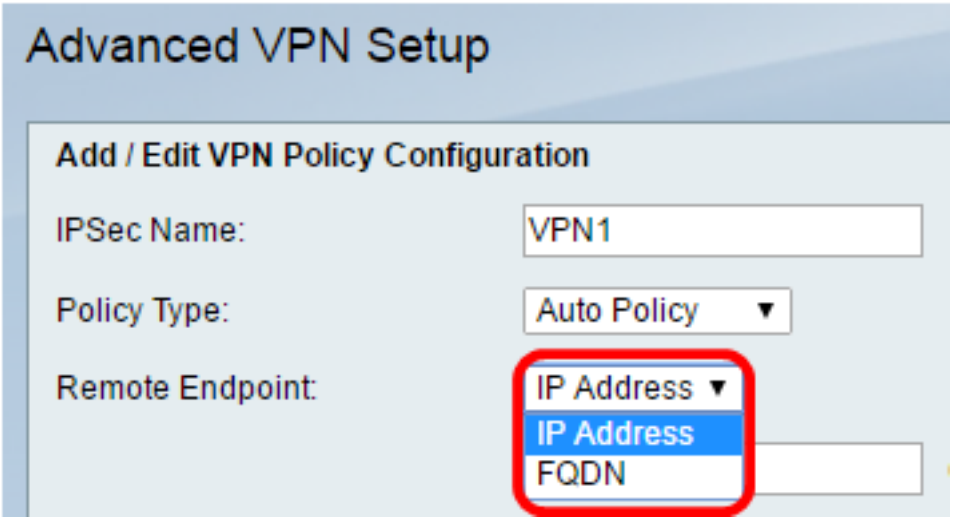
ملاحظة: في هذا المثال، يتم إختيار نهج تلقائي.



الخطوة 4. من القائمة المنسدلة "نقطة النهاية البعيدة"، أختر خيارا.

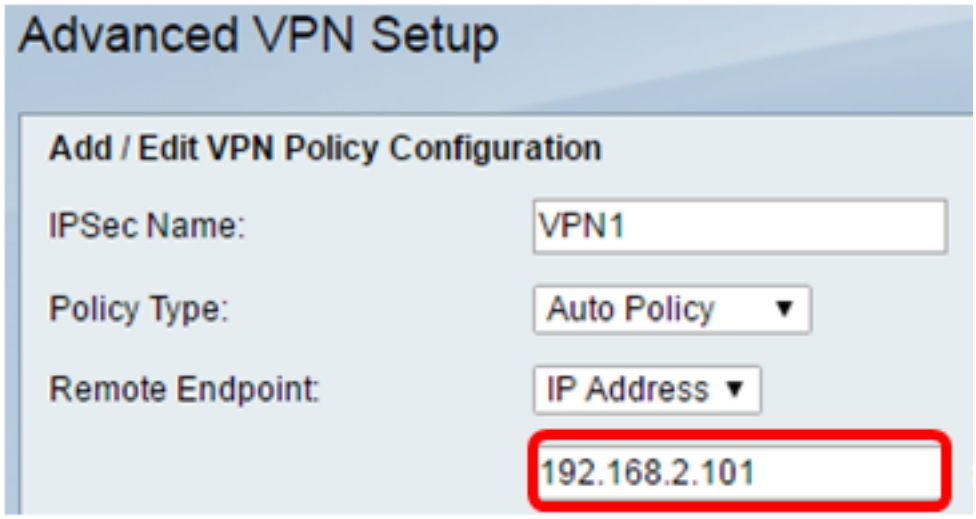
- عنوان IP — يحدد هذا الخيار الشبكة البعيدة بواسطة عنوان IP عام.
- FQDN — اسم مجال كامل لجهاز كمبيوتر معين أو مضيف معين أو الإنترنت. يتكون FQDN من جزأين: اسم المضيف واسم المجال. لا يمكن تمكين هذا الخيار إلا عند تحديد **نهج تلقائي** في الخطوة 3.

ملاحظة: على سبيل المثال، يتم إختيار عنوان IP.

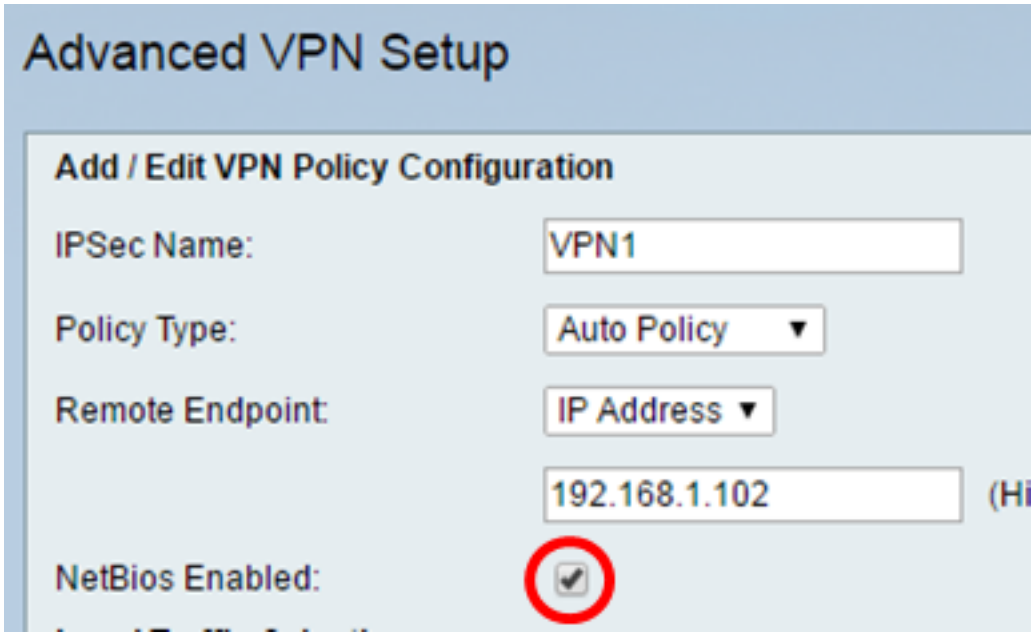


الخطوة 5. في حقل *نقطة النهاية البعيدة*، أدخل إما عنوان IP العام أو اسم المجال للعنوان البعيد.

ملاحظة: في هذا المثال، يتم إستخدام 192.168.2.101.



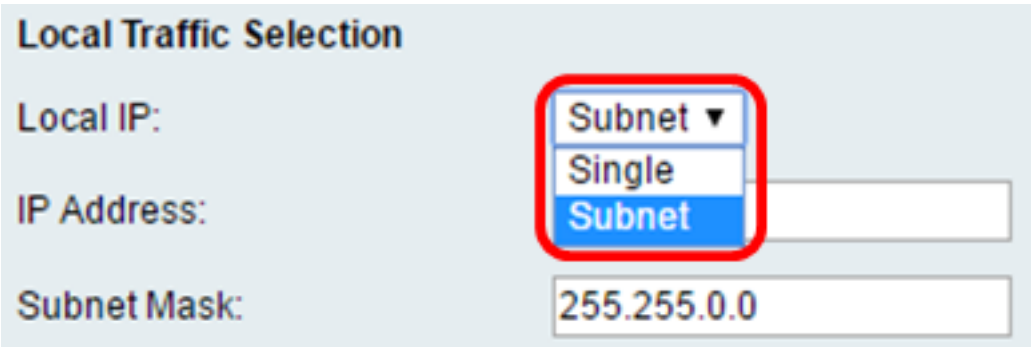
الخطوة 6. (إختياري) حدد خانة الاختيار **تمكين NetBIOS** إذا كنت تريد تمكين عمليات بث نظام الإدخال/الإخراج الأساسي للشبكة (NetBIOS) من خلال اتصال VPN. يسمح NetBIOS للمضيفين بالاتصال مع بعضهم البعض ضمن شبكة المنطقة المحلية (LAN).



الخطوة 7. من القائمة المنسدلة IP المحلية تحت منطقة تحديد حركة المرور المحلية، أختر خيارا.

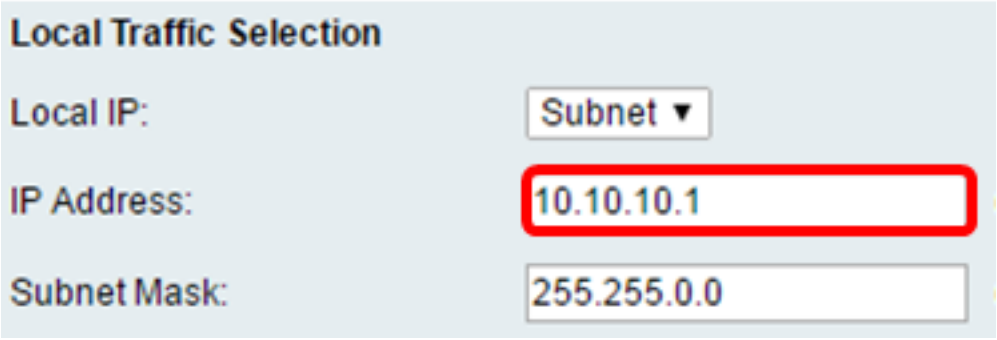
- أحادي — يحدد السياسة بمضيف واحد.
- الشبكة الفرعية — تسمح للمضيفين داخل نطاق عنوان IP بالاتصال بشبكة VPN.

ملاحظة: في هذا المثال، يتم إختيار الشبكة الفرعية.



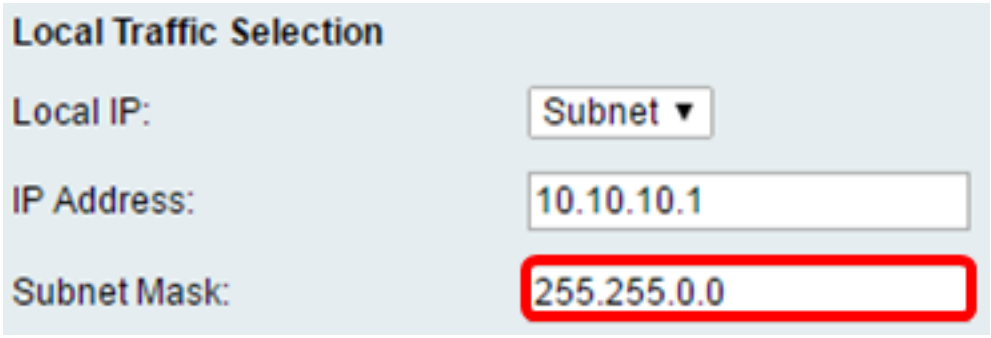
الخطوة 8. في حقل عنوان IP، أدخل المضيف أو عنوان IP للشبكة الفرعية أو المضيف المحلي.

ملاحظة: في هذا المثال، يتم إستخدام عنوان IP للشبكة الفرعية المحلية على 10.10.10.1.



الخطوة 9. (إختياري) إذا تم تحديد الشبكة الفرعية في الخطوة 7، فأدخل قناع الشبكة الفرعية للعميل في حقل *قناع الشبكة الفرعية*. يتم تعطيل حقل قناع الشبكة الفرعية إذا تم إختيار أحادي في الخطوة 1.

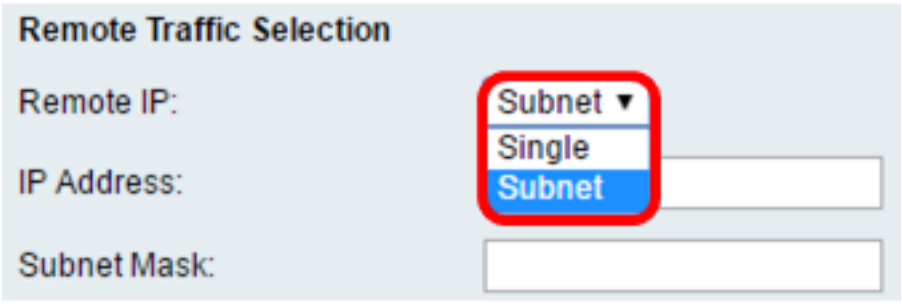
ملاحظة: في هذا المثال، يتم إستخدام قناع الشبكة الفرعية 255.255.0.0.



الخطوة 10. من القائمة المنسدلة IP البعيدة ضمن منطقة تحديد حركة المرور عن بعد، أختر خيارا.

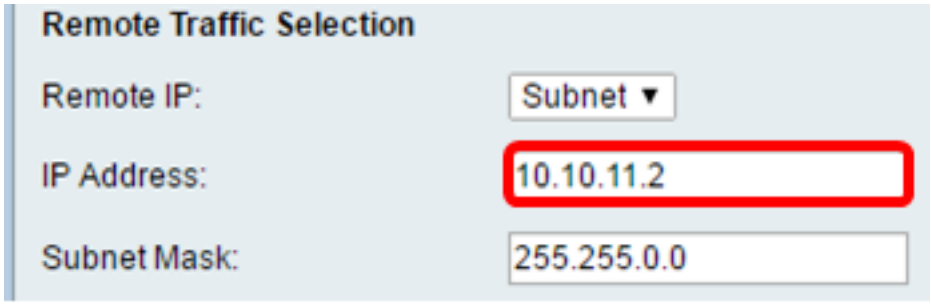
- أحادي — يحدد السياسة بمضيف واحد.
- الشبكة الفرعية — تسمح للمضيفين داخل نطاق عنوان IP بالاتصال بشبكة VPN.

ملاحظة: في هذا المثال، يتم إختيار الشبكة الفرعية.



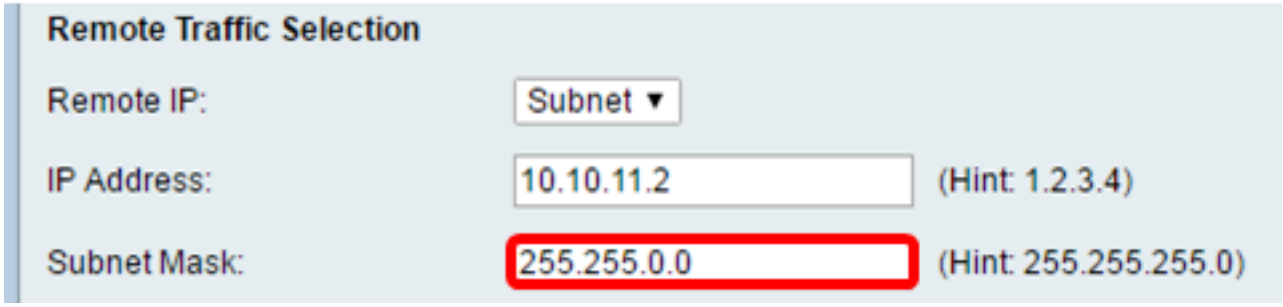
الخطوة 11. دخلت المدى من عنوان من المضيف أن يكون جزء من ال VPN في *العنوان* مجال. إذا تم تحديد **أحادي** في الخطوة 10، فأدخل عنوان IP.

ملاحظة: في المثال التالي، يتم إستخدام 10.10.11.2.



الخطوة 12. (إختياري) إذا تم تحديد **الشبكة الفرعية** في الخطوة 10، فأدخل قناع الشبكة الفرعية لعنوان IP للشبكة الفرعية في حقل *قناع الشبكة الفرعية*.

ملاحظة: في المثال التالي، يتم إستخدام 255.255.0.0.

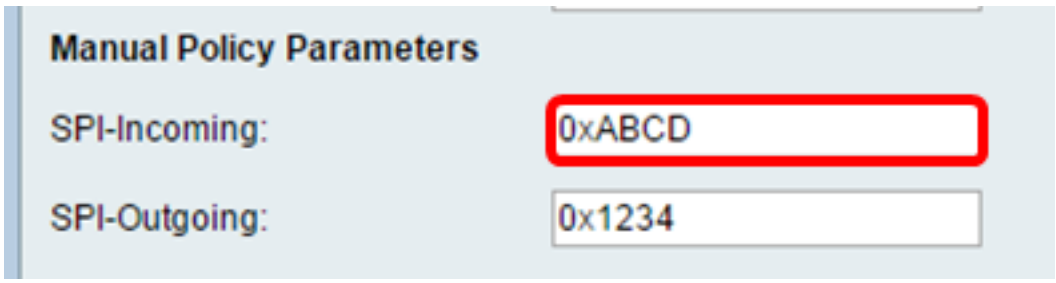


سياسة يدوية محددات

ملاحظة: يمكن تحرير هذه الحقول فقط في حالة إختيار **النهج اليدوي**.

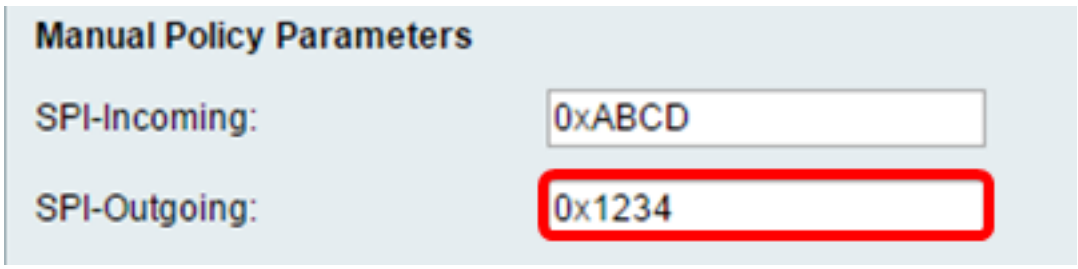
الخطوة 1. في حقل *SPI-Incoming*، أدخل من ثلاثة إلى ثمانية أحرف سداسية عشرية لعلامة فهرس معلمات الأمان (SPI) لحركة المرور الواردة على اتصال VPN. ال SPI استعملت بطاقة أن يميز الحركة مرور من واحد جلسة من الحركة مرور من آخر جلسة.

ملاحظة: لهذا المثال، يتم إستخدام 0xABCD.



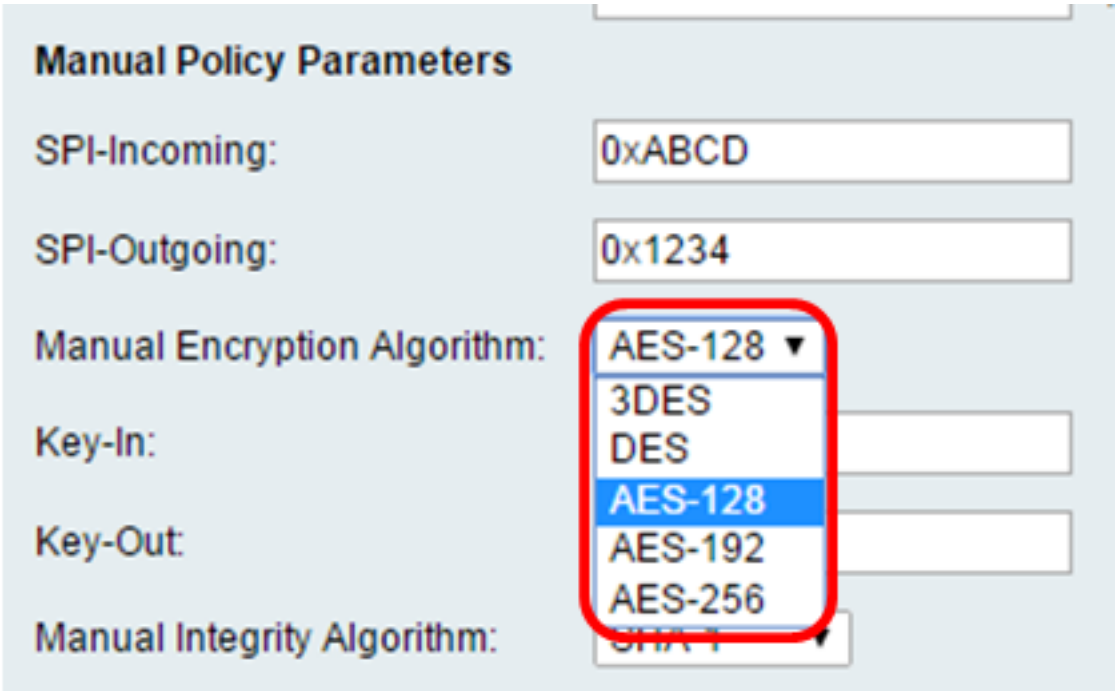
الخطوة 2. في حقل *SPI-Outgoing*، أدخل من ثلاثة إلى ثمانية أحرف سداسية عشرية لعلامة SPI لحركة المرور الصادرة على اتصال VPN.

ملاحظة: لهذا المثال، يتم إستخدام 0x1234.



الخطوة 3. من القائمة المنسدلة لخوارزمية التشفير اليدوي، أختر خيارا. الخيارات هي DES و 3DES و AES-128 و AES-192 و AES-256.

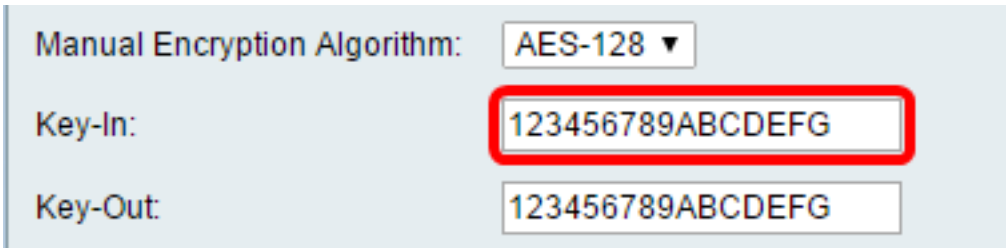
ملاحظة: في هذا المثال، يتم إختيار AES-128.



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

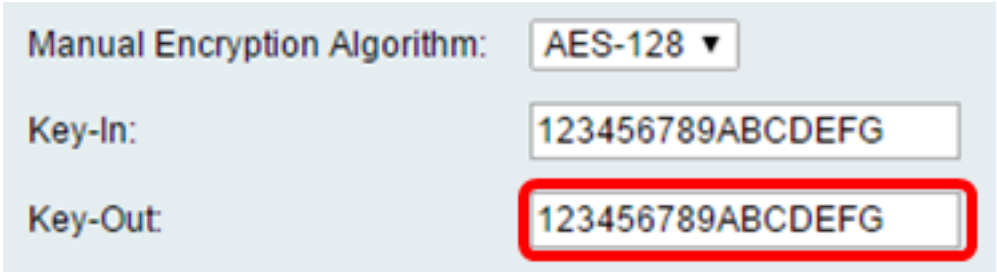
- يستخدم DES مفتاح 8 حروف.
- يستخدم معيار 3DES مفتاح مكون من 24 حرف.
- يستخدم AES-128 مفتاح 16 حرف.
- يستخدم AES-192 مفتاح مكون من 24 حرف.
- يستخدم AES-256 مفتاح 32 حرفا.

ملاحظة: في هذا المثال، يتم إستخدام 123456789ABCDEFG.



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

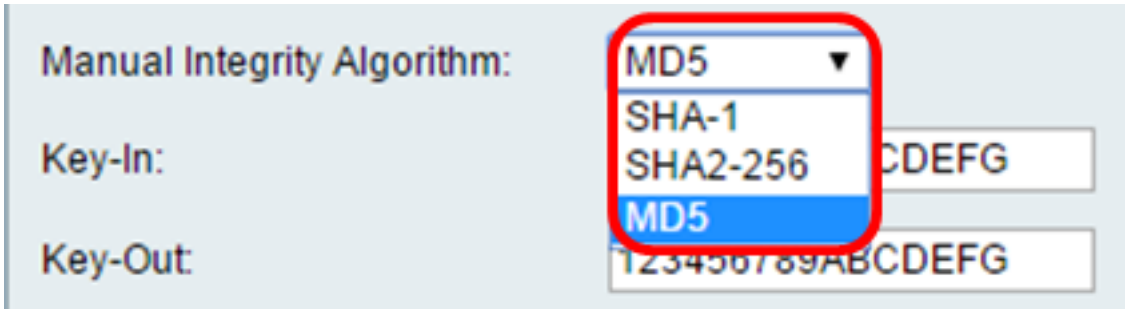
ملاحظة: في هذا المثال، يتم إستخدام 123456789ABCDEFG.



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

- 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 16 حرف.
- يستخدم SHA-1 مفتاح مكون من 20 حرف.
- يستخدم SHA2-256 مفتاح 32 حرفا.

ملاحظة: في هذا المثال، يتم إستخدام 123456789ABCDEFG.

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 123456789ABCDEFG.

أوت٥ معلمات النهج

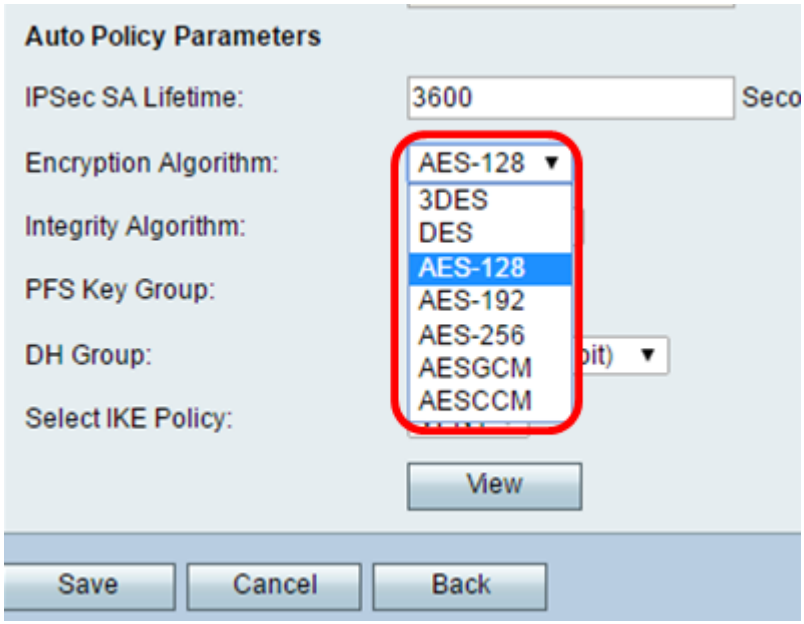
ملاحظة: قبل إنشاء نهج VPN تلقائي، تأكد من إنشاء نهج IKE استنادا إلى ما تريد إنشاء نهج VPN التلقائي.لا يمكن تحرير هذه الحقول إلا إذا تم تحديد **نهج تلقائي** في الخطوة 3.

الخطوة 1. في حقل *IPSec SA-Life*، أدخل المدة التي تستمر بالثواني التي تستمر فيها SA قبل التجديد. المدى from 30-86400. الافتراضي هو 3600.

الخطوة 2. من القائمة المنسدلة لخوارزمية التشفير، أختر خيارا. الخيارات هي:

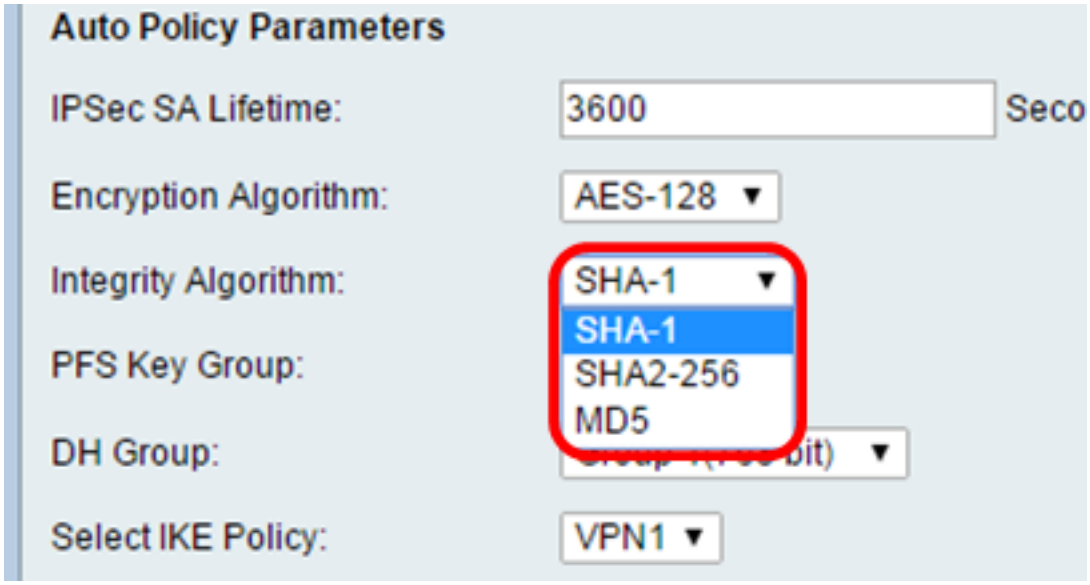
ملاحظة: في هذا المثال، يتم إختيار AES-128.

- DES — طريقة تشفير قديمة 56 بت ليست طريقة تشفير آمنة جدا، ولكنها قد تكون مطلوبة للتوافق مع الإصدارات السابقة.
- 3DES — طريقة تشفير بسيطة 168 بت تستخدم لزيادة حجم المفتاح لأنها تقوم بتشفير البيانات ثلاث مرات. يوفر ذلك أمانا أكثر من DES ولكن أمان أقل من AES.
- AES-128 — يستخدم مفتاح 128-بت لتشفير AES. يتميز نظام التشفير المتطور (AES) بأنه أكثر سرعة وأمنا من نظام اكتشاف التشفير المتطور (DES). وبشكل عام، يعتبر معيار التشفير المتطور أكثر سرعة وأمنا من معيار تشفير البيانات الثلاثي (3DES). الطراز AES-128 أكثر سرعة ولكنه أقل أمانا من الطرازين AES-192 و AES-256.
- AES-192 — يستخدم مفتاح 192-بت لتشفير AES. يتميز الطراز AES-192 بأنه أكثر بطئا وأمنا مقارنة بالطراز AES-128، كما أنه أسرع ولكن أقل أمانا من الطراز AES-256.
- AES-256 — يستخدم مفتاح 256-بت لتشفير AES. يتميز الطراز AES-256 بأنه أكثر بطئا ولكنه أكثر أمانا من الطرازين AES-128 و AES-192.
- AESGCM — وضع العداد Galois القياسي للتشفير المتقدم هو وضع تشفير كتلة التشفير العام المصادق. تستخدم مصادقة إدارة المحتوى العالمي (GCM) العمليات التي تناسب بشكل خاص التنفيذ الفعال في الأجهزة، مما يجعلها جذابة بشكل خاص للتنفيذ عالي السرعة، أو للتنفيذ في دائرة فعالة ومدمجة.
- AESCCM — العداد القياسي للتشفير المتقدم مع وضع CBC-MAC هو وضع تشفير كتلة التشفير العام المصادق. CCM مناسب تماما للاستخدام في تطبيقات البرامج المضغوطة.

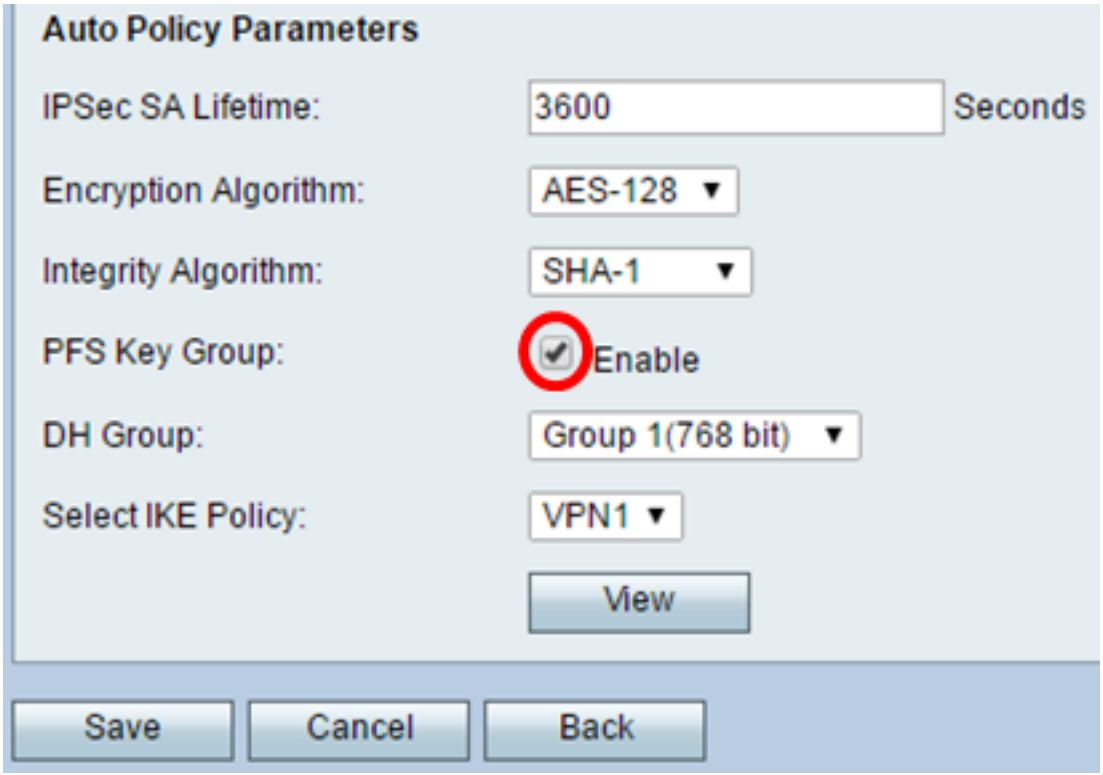


الخطوة 3. من القائمة المنسدلة لخوارزمية التكامل، أختر خيارا. الخيارات هي MD5 و SHA-1 و SHA2-256.

ملاحظة: في هذا المثال، يتم إختيار SHA-1.

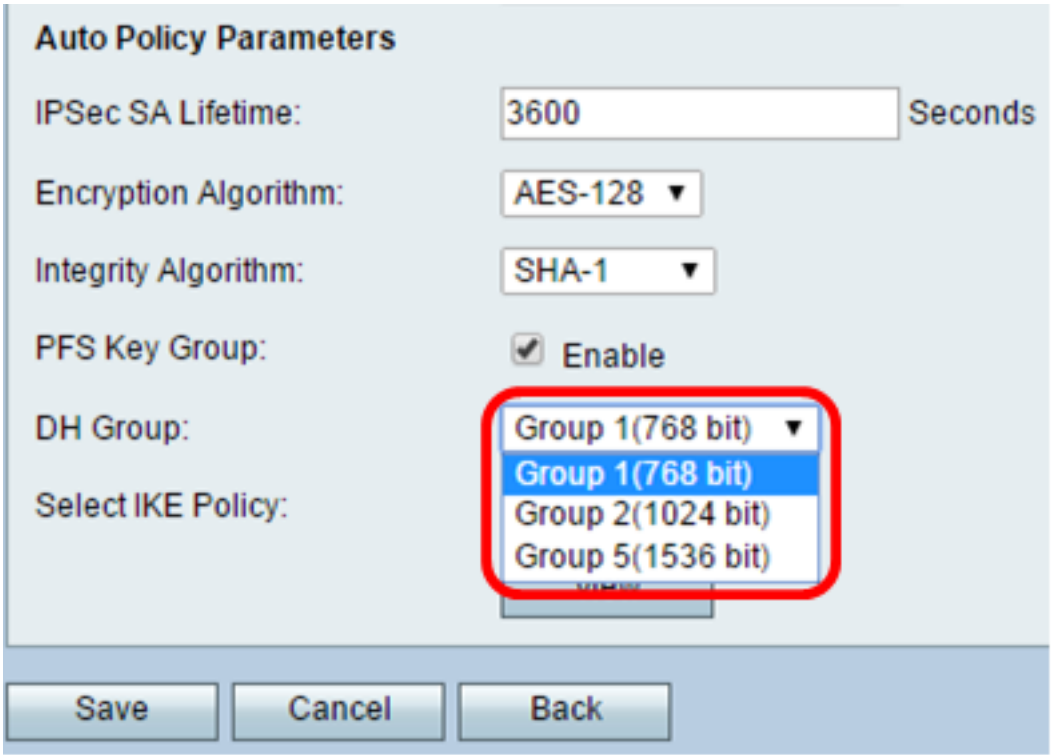


الخطوة 4. حدد خانة الاختيار **تمكين** في مجموعة مفاتيح PFS لتمكين سرية إعادة التوجيه الكاملة (PFS). تزيد PFS من أمان الشبكة الخاصة الظاهرية (VPN)، لكنها تبطئ من سرعة الاتصال.



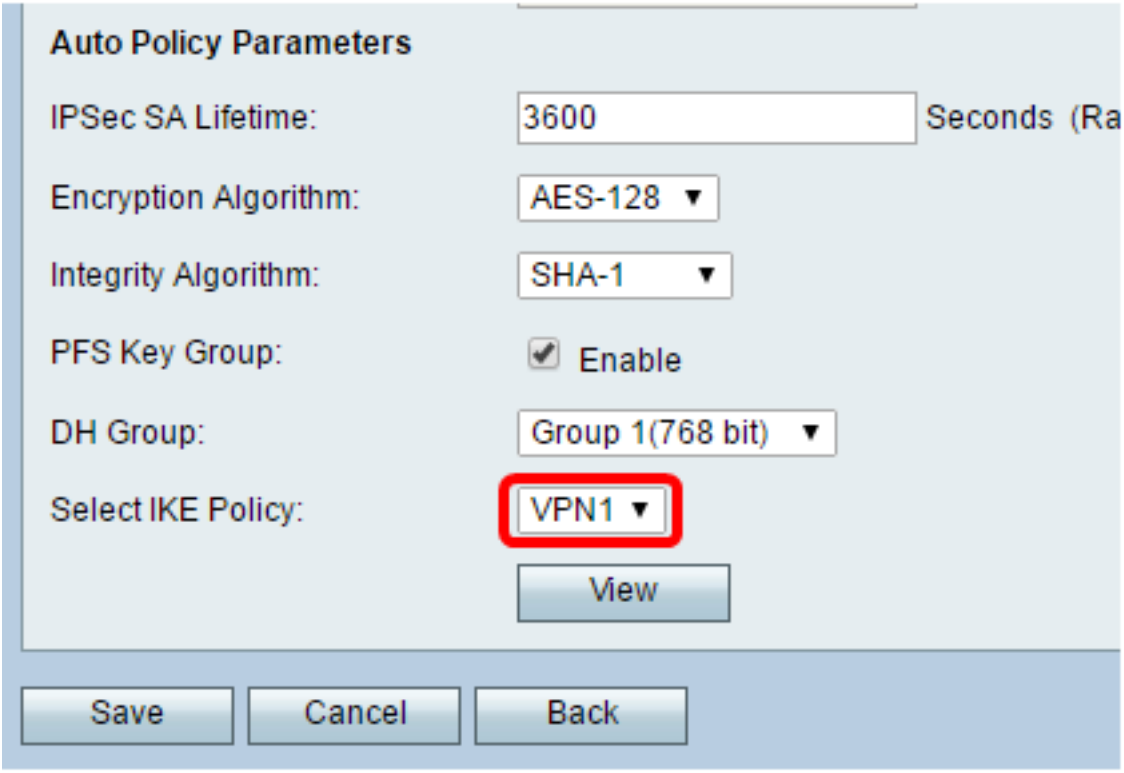
الخطوة 5. (إختياري) إذا أخترت تمكين PFS في الخطوة 4، أختر مجموعة DH للانضمام من القائمة المنسدلة مجموعة DH. كلما كان رقم المجموعة أعلى، كلما كان الأمان أفضل.

ملاحظة: على سبيل المثال، يتم إختيار المجموعة 1.

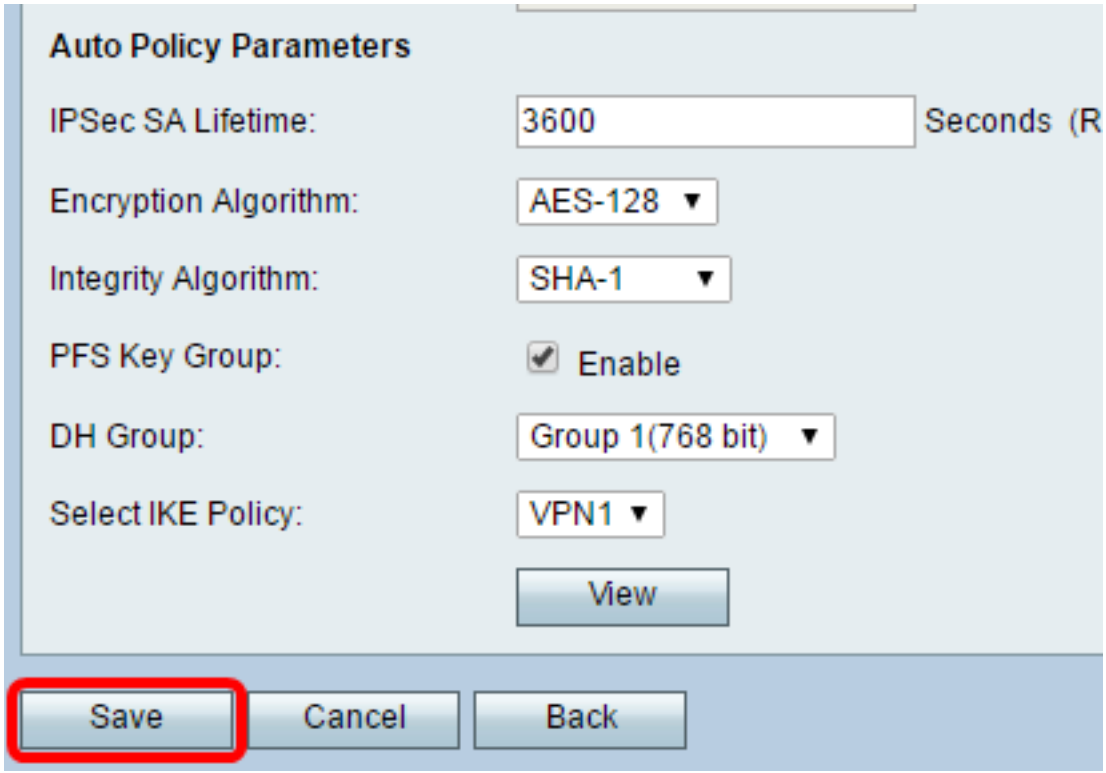


الخطوة 6. من القائمة المنسدلة تحديد نهج IKE، أختر نهج IKE الذي سيتم إستخدامه لنهج VPN.

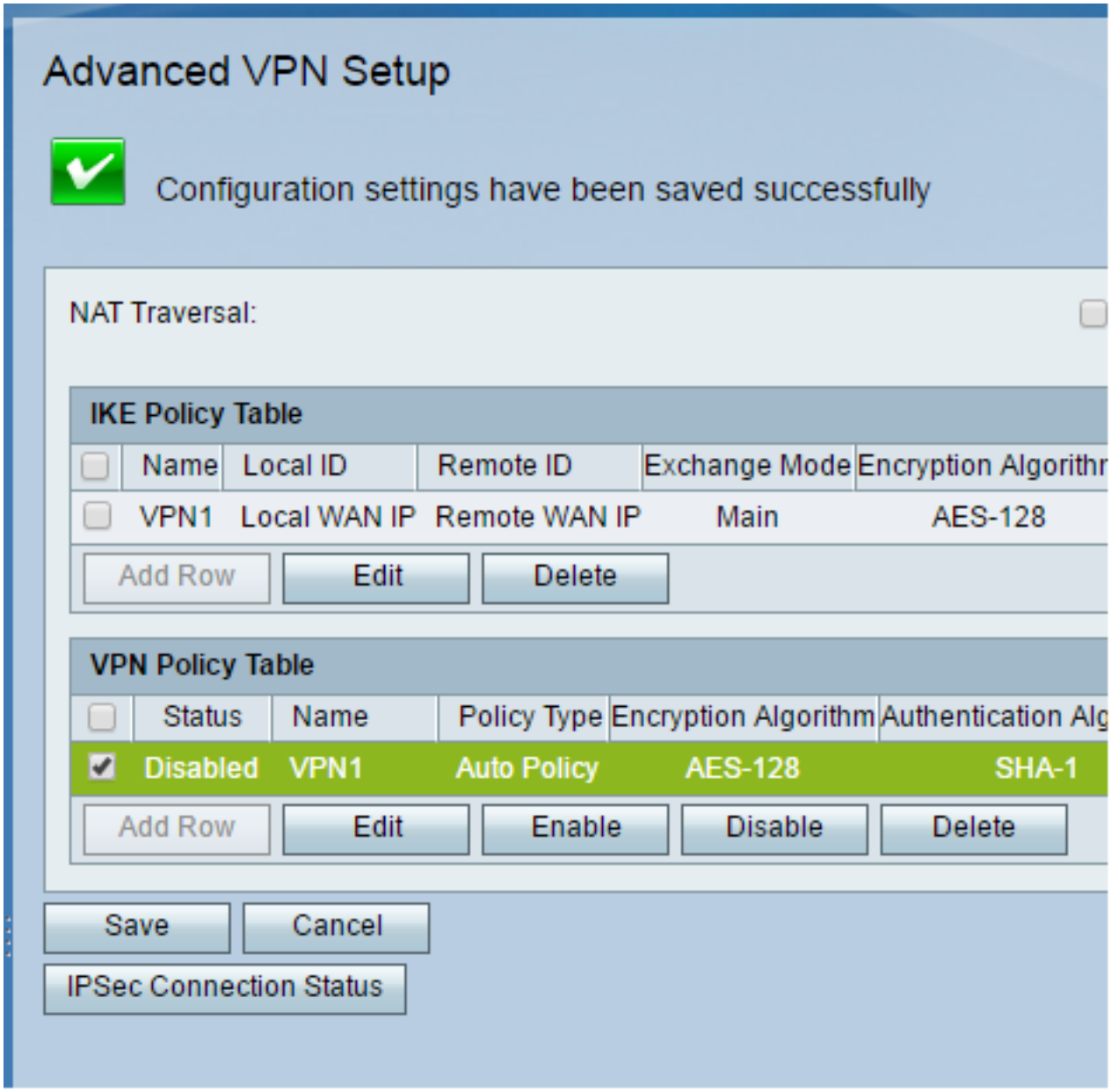
ملاحظة: في هذا المثال، تم تكوين سياسة IKE واحدة فقط لذلك يظهر نهج واحد فقط.



الخطوة 7. طقطقة **حفظ**.

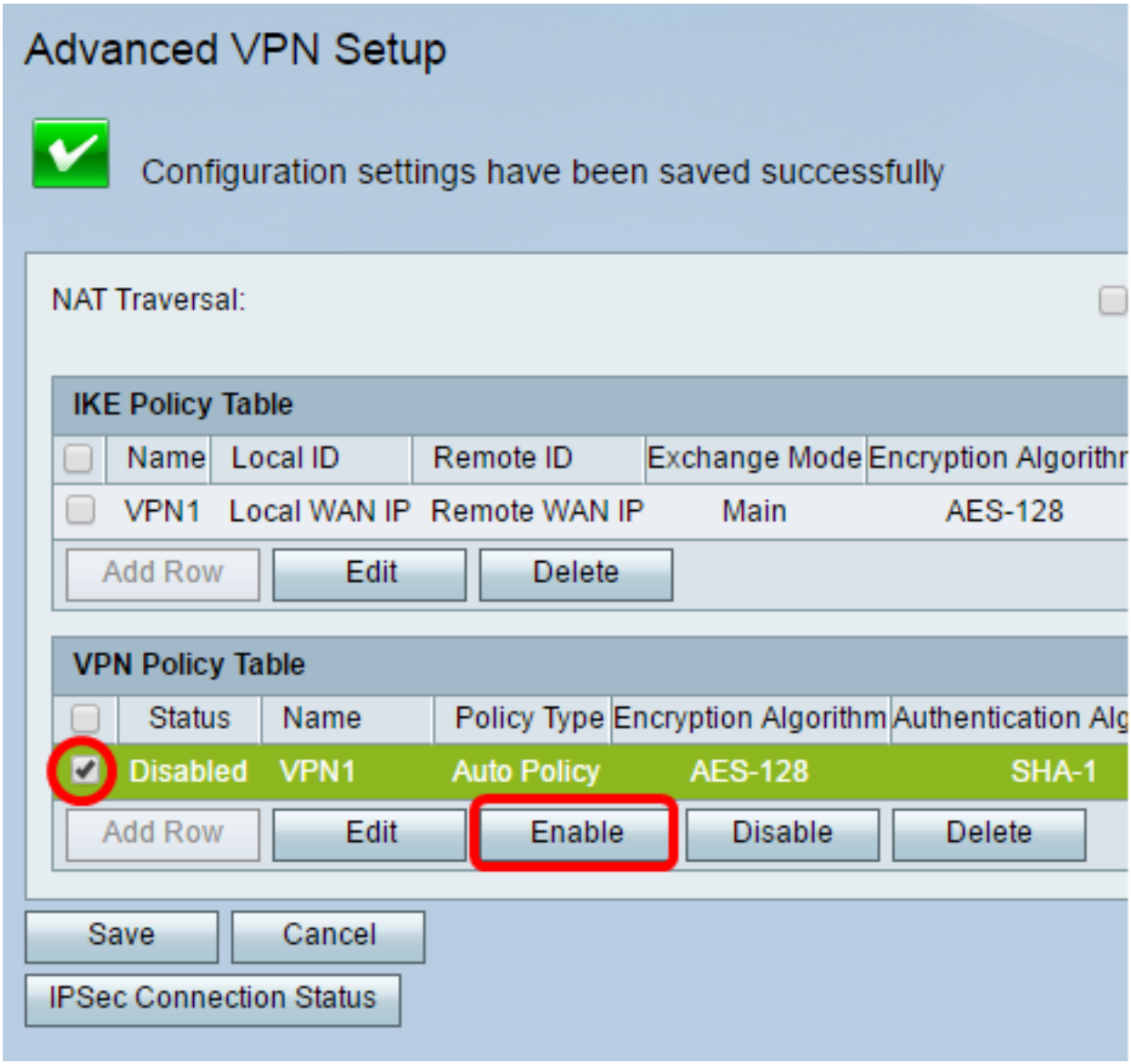


ملاحظة: تظهر صفحة إعداد VPN المتقدمة الرئيسية مرة أخرى. يجب ظهور رسالة تأكيد بأن إعدادات التكوين قد تم حفظها بنجاح.

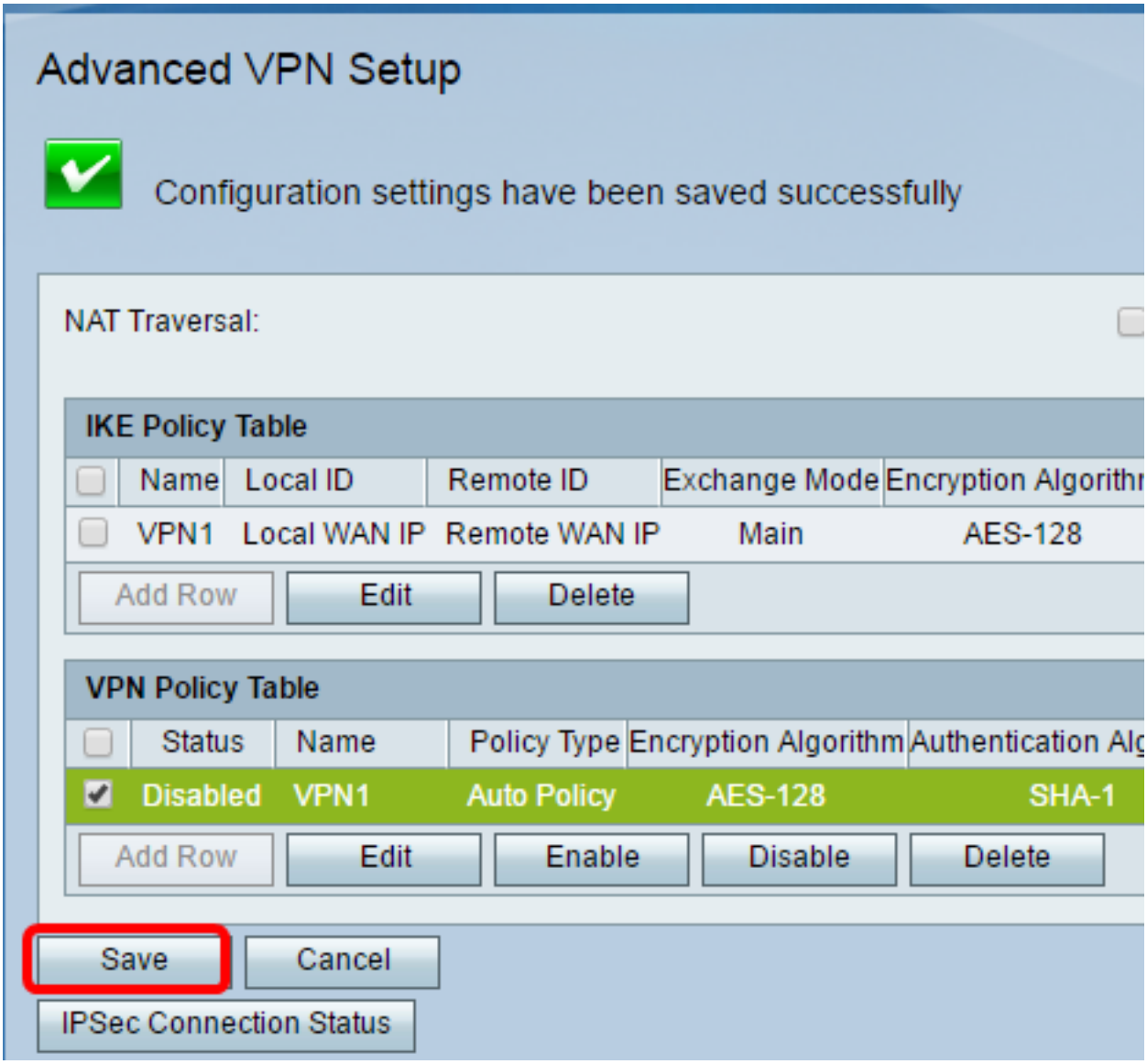


الخطوة 8. تحت ال VPN سياسة طاولة، فحصت خانة إختيار أن يختار VPN وطقطقة **يمكن**.

ملاحظة: يتم تعطيل نهج VPN الذي تم تكوينه بشكل افتراضي.



الخطوة 9. طقطقة **حفظ**.



يجب أن تكون قد انتهيت الآن من تكوين سياسة VPN بنجاح على الموجه RV130 أو RV130W الخاص بك.

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).