إعدادات نهج تبادل مفتاح الإنترنت (IKE) على موجهات VPN RV130 و RV130W

الهدف

تبادل مفتاح الإنترنت (IKE) هو بروتوكول يؤسس اتصال آمن بين شبكتين. باستخدام IKE، يتم تشفير الحزم وتأمينها وإلغاء تأمينها باستخدام المفاتيح المستخدمة من قبل طرفين.

تحتاج إلى إنشاء نهج Internet Key Exchange قبل تكوين نهج VPN. راجع تكوين سياسة VPN على RV130 و RV130W للحصول على مزيد من المعلومات.

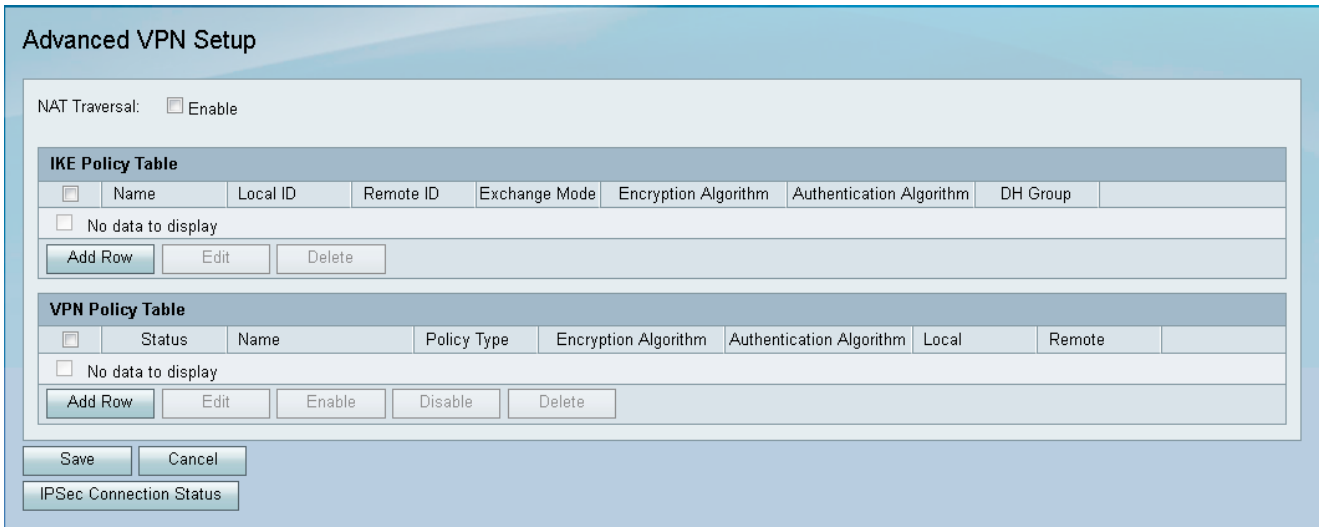
الهدف من هذا المستند هو توضيح كيفية إضافة ملف تعريف IKE إلى موجهات VPN RV130 و RV130W.

الأجهزة القابلة للتطبيق

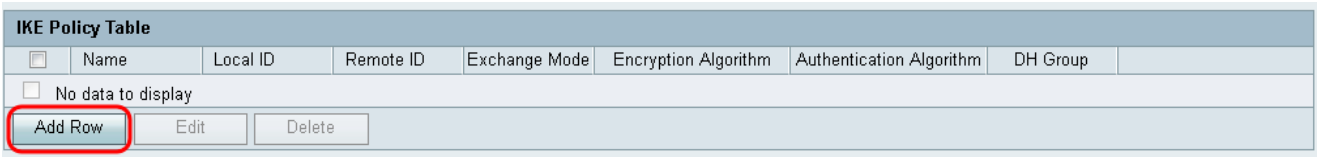
• RV130
• RV130W

خطوات إجرائية

الخطوة 1. أستخدم الأداة المساعدة لتكوين الموجه لاختيار VPN > IPSec VPN من موقع إلى موقع > إعداد VPN المتقدم من القائمة الموجودة على اليسار. تظهر صفحة إعداد VPN المتقدم:

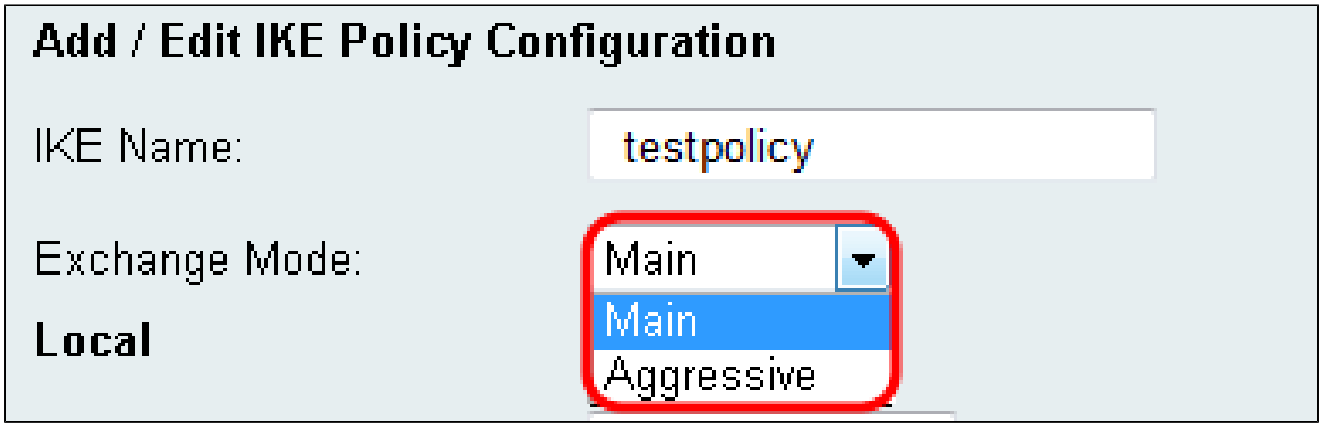


الخطوة 2. تحت جدول نهج IKE، انقر فوق إضافة صف. تظهر نافذة جديدة:



الخطوة 3. أدخل اسم لنهج IKE في حقل اسم IKE.

الخطوة 4. من القائمة المنسدلة وضع Exchange، أختر الوضع الذي يتم فيه إستخدام تبادل المفاتيح لإنشاء اتصال آمن.

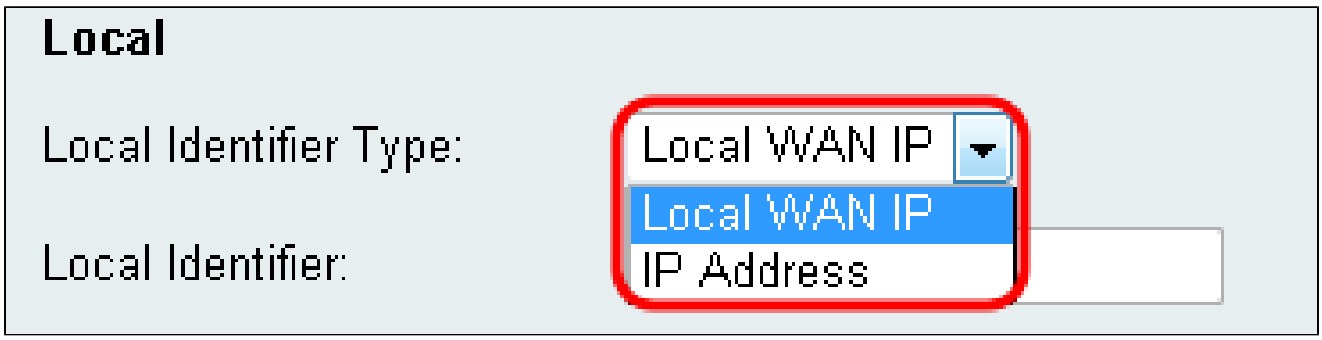


يتم تحديد الخيارات المتاحة على النحو التالي:

· الرئيسية - تحمي هوية الأقران لزيادة الأمان.

· فائقة — لا توفر حماية لهوية النظير ولكن توفر اتصالا أسرع.

الخطوة 5. من القائمة المنسدلة نوع المعرف المحلي أختر نوع الهوية التي يحتوي عليها ملف التعريف.

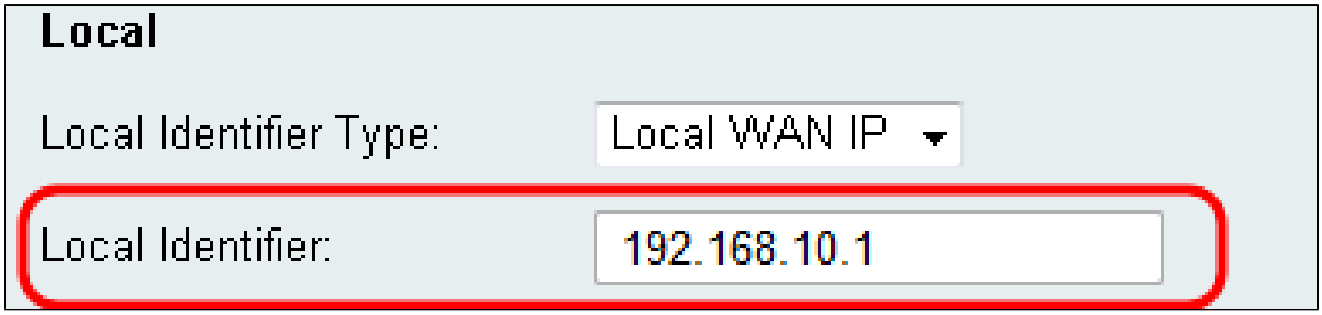


يتم تحديد الخيارات المتاحة على النحو التالي:

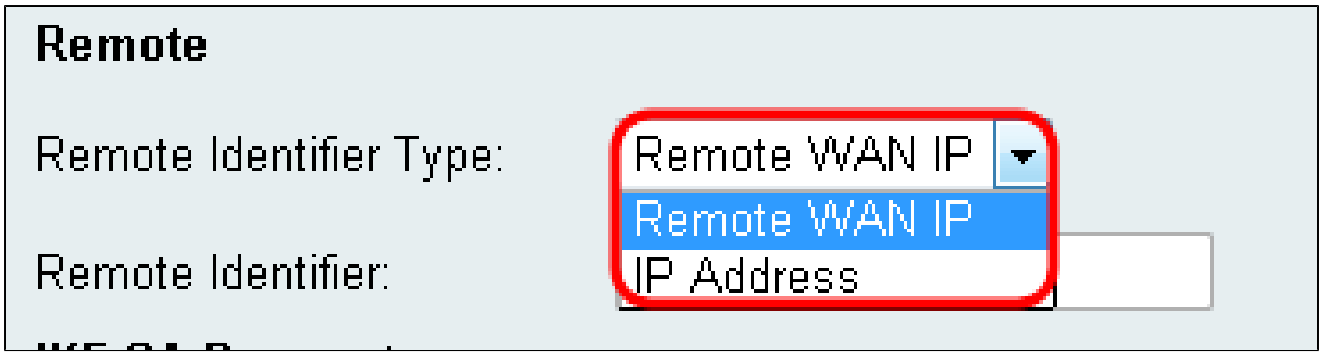
· بروتوكول الإنترنت (IP) لشبكة WAN المحلية — يتصل عبر الإنترنت.

· عنوان IP — سلسلة فريدة من الأرقام منفصلة بفترات تعرف كل جهاز يستخدم بروتوكول الإنترنت للاتصال عبر الشبكة.

الخطوة 6. (إختياري) إذا تم تحديد عنوان IP من القائمة المنسدلة في الخطوة 5، فأدخل عنوان IP المحلي في حقل المعرف المحلي.



الخطوة 7. من القائمة المنسدلة نوع المعرف البعيد أختر نوع الهوية التي يتضمنها ملف التعريف.

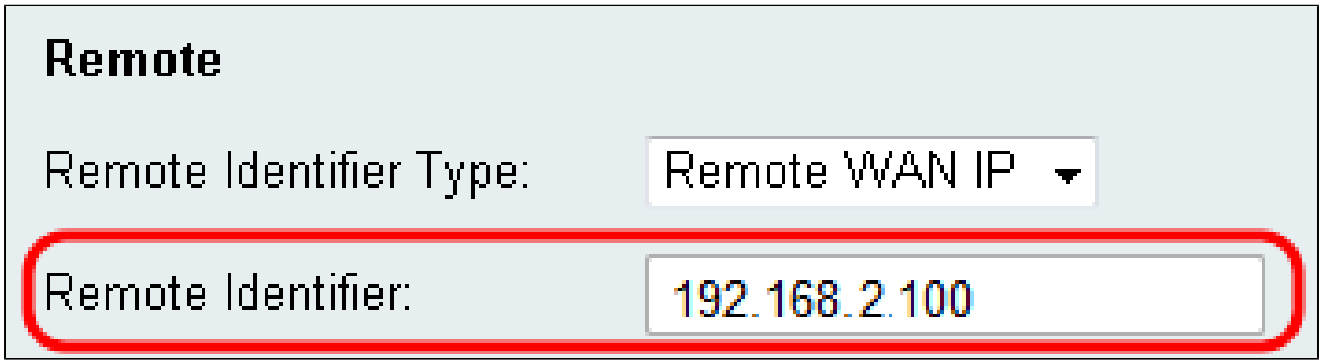


يتم تحديد الخيارات المتاحة على النحو التالي:

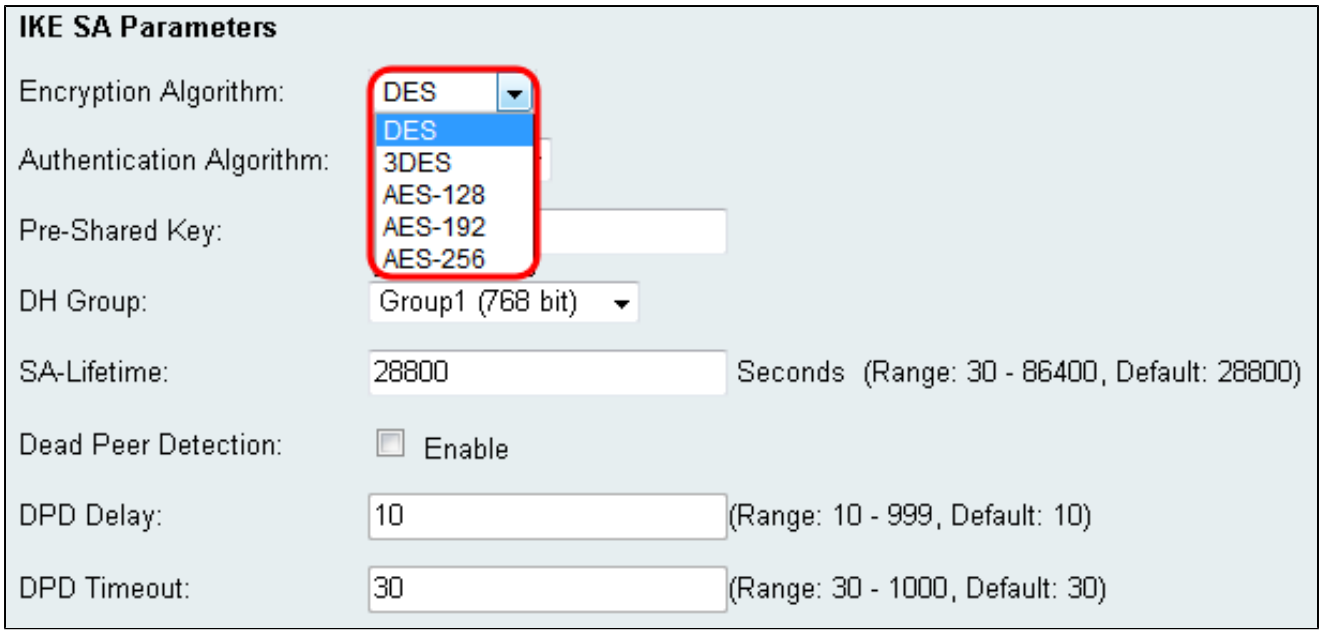
· بروتوكول الإنترنت (IP) لشبكة WAN المحلية — يتصل عبر الإنترنت.

· عنوان IP — سلسلة فريدة من الأرقام منفصلة بفترات تعرف كل جهاز يستخدم بروتوكول الإنترنت للاتصال عبر الشبكة.

الخطوة 8. (إختياري) إذا تم تحديد عنوان IP من القائمة المنسدلة في الخطوة 7، فأدخل عنوان IP البعيد في حقل المعرف البعيد.



الخطوة 9. من القائمة المنسدلة لخوارزمية التشفير، أختر خوارزمية لتشفير الاتصالات. يتم إختيار AES-128 كافتراضي.



يتم سرد الخيارات المتاحة كما يلي من أدنى إلى أعلى مستوى من التأمين:

· معيار تشفير البيانات — DES.

· معيار 3DES — المعيار الثلاثي لتشفير البيانات.

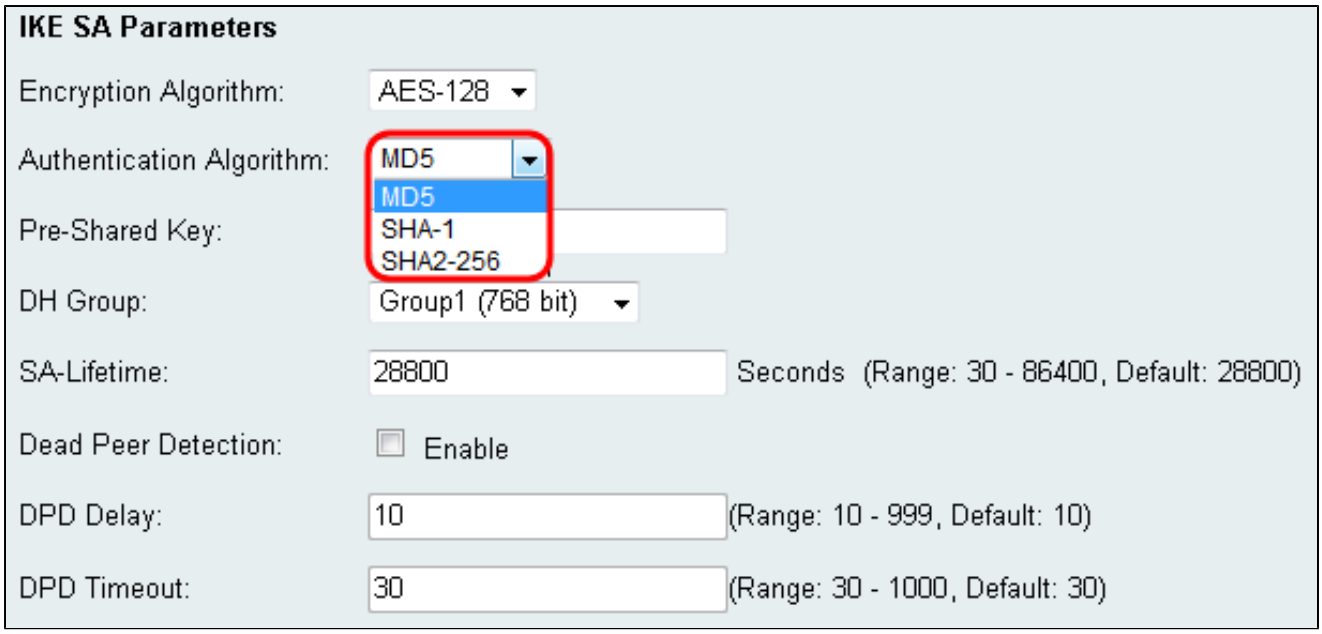
· الطراز AES-128 — يستخدم معيار التشفير المتقدم مفتاح إصدار 128 بت.

· الطراز AES-192 — يستخدم معيار التشفير المتقدم مفتاح إصدار 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 مع انخفاض الأداء. يوصى باستخدام الطراز AES-128 لأنه يوفر أفضل حل وسط بين السرعة والأمان.

الخطوة 10. من القائمة المنسدلة خوارزمية المصادقة، أختر خوارزمية لمصادقة إتصالاتك. يتم إختيار SHA-1 كافتراضي.



يتم تحديد الخيارات المتاحة على النحو التالي:

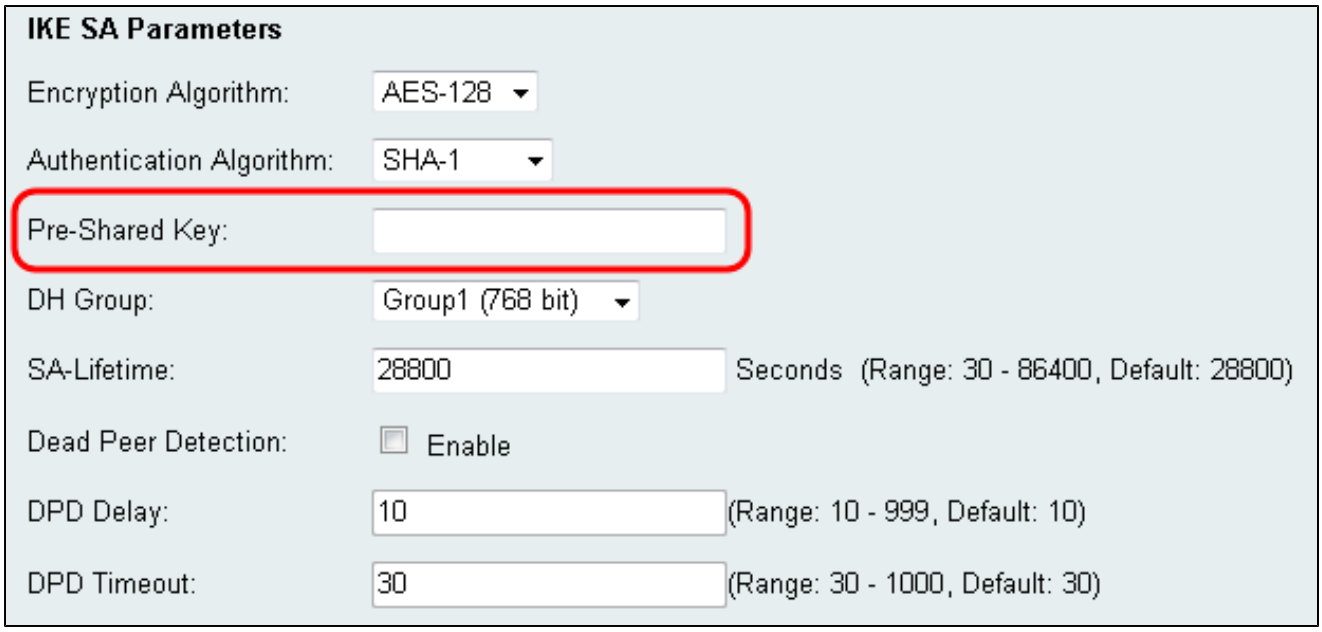
· MD5 — تحتوي خوارزمية ملخص الرسالة على قيمة تجزئة 128 بت.

· SHA-1 — تحتوي خوارزمية التجزئة الآمنة على قيمة تجزئة 160 بت.

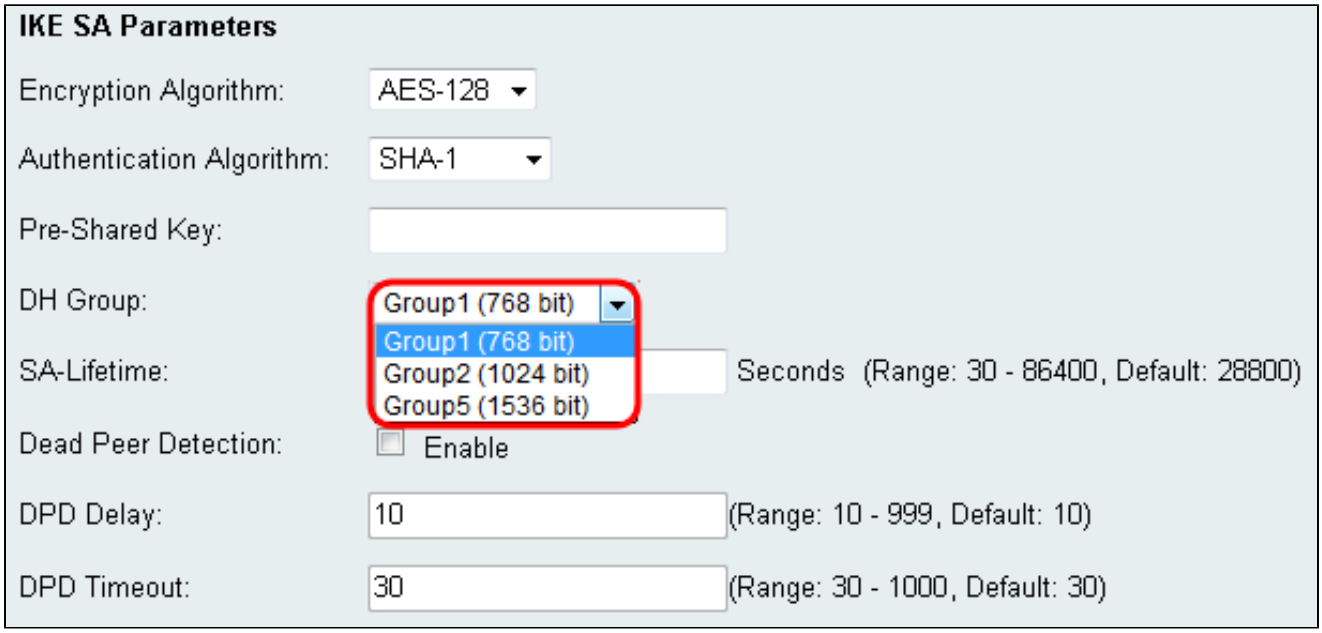
· SHA2-256 — خوارزمية التجزئة الآمنة مع قيمة تجزئة 256 بت.

ملاحظة: MD5 و SHA هما دالتا تجزئة مشفرتان. تأخذ قطعة من البيانات، تضغطها، وتنشئ مخرجات سداسية عشرية فريدة لا يمكن إعادة إنتاجها. لا يوفر MD5 بشكل أساسي أي أمان ضد التصادمات التجزئة ويجب إستخدامه فقط في إعداد بيئة الأعمال الصغيرة حيث لا تكون هناك حاجة إلى مقاومة التصادم. ويعد الطراز SHA1 خيارا أفضل من الطراز MD5 لأنه يوفر أمانا أفضل بسرعات أقل بدرجة كبيرة. من أجل تحقيق أفضل النتائج، لا يتوفر SHA2-256 على هجمات معروفة وذات أهمية عملية، وسوف يوفر أفضل مستوى من الأمان. وكما ذكر سابقا، فإن إرتفاع مستوى الأمن يعني سرعات أبطأ.

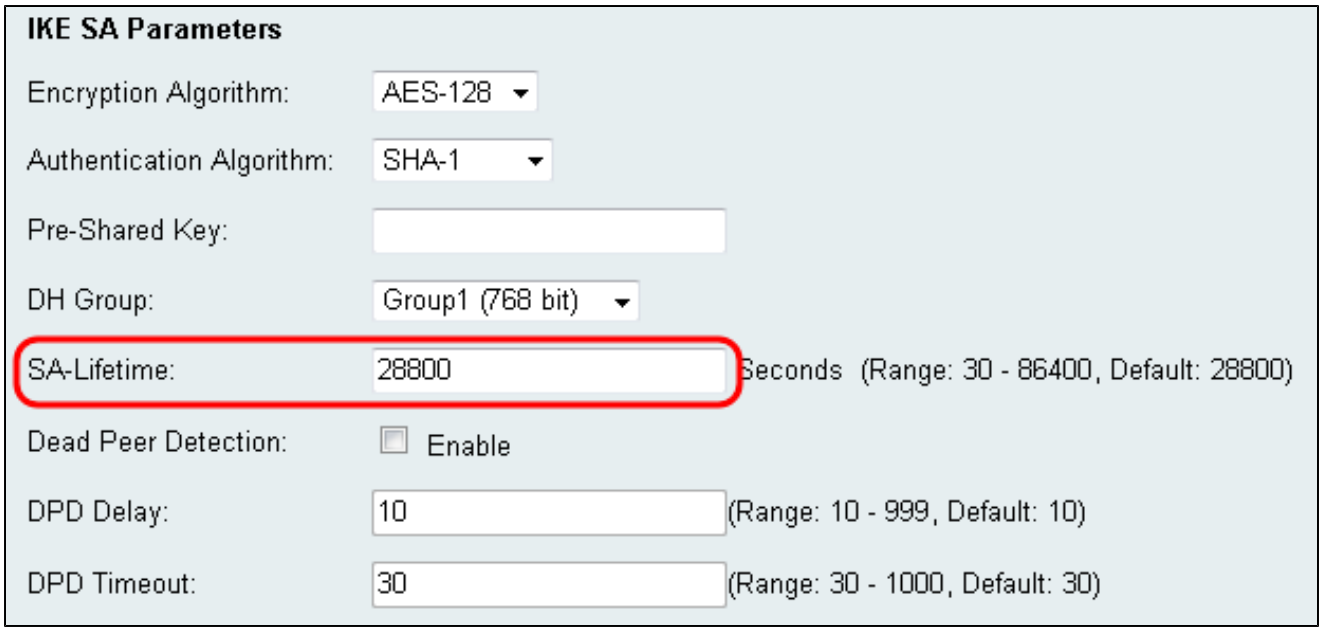
الخطوة 11. في حقل مفتاح مشترك مسبقا، أدخل كلمة مرور يتراوح طولها بين 8 و 49 حرفا.



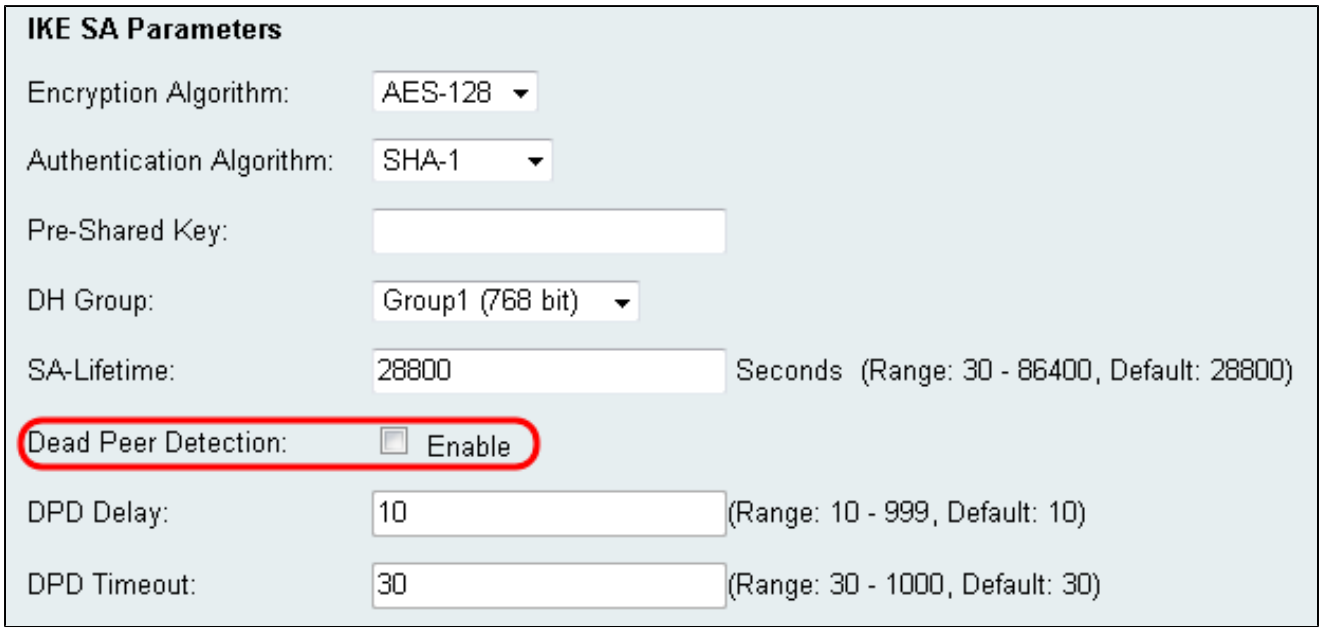
الخطوة 12. من القائمة المنسدلة مجموعة DH، أختر مجموعة DH. يشير عدد وحدات بت إلى مستوى الأمان. يجب أن يكون كل طرفي الاتصال في نفس المجموعة.



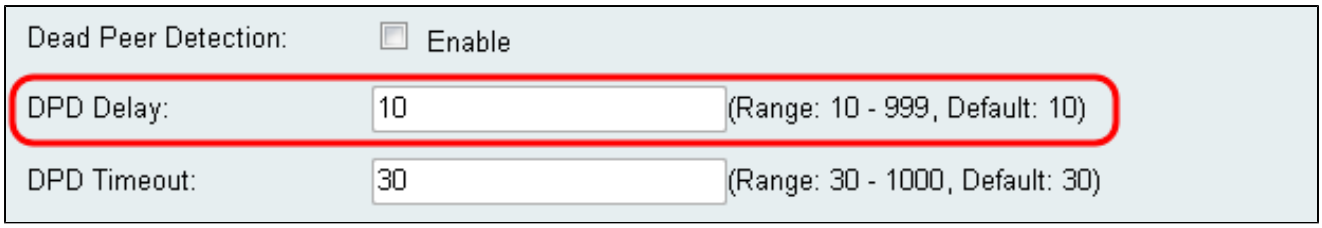
الخطوة 13. في حقل SA-Lifetime، أدخل المدة التي سيكون فيها اقتران الأمان صالحا في ثوان. التقصير 28800 ثانية.



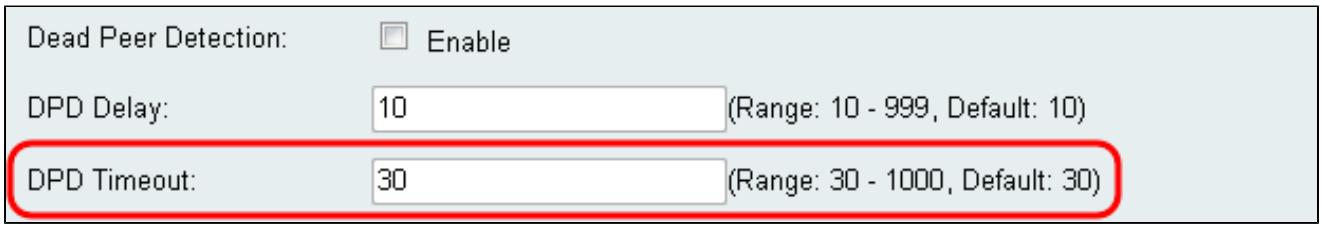
خطوة 14. (إختياري) فحصت ال يمكن تدقيق صندوق في Dead نظير كشف مجال إن نظير غير نشط. تخطي الخطوة 17 إذا لم تقم بتمكين التوصيل مع نظير يعجز أنت أن تريد".



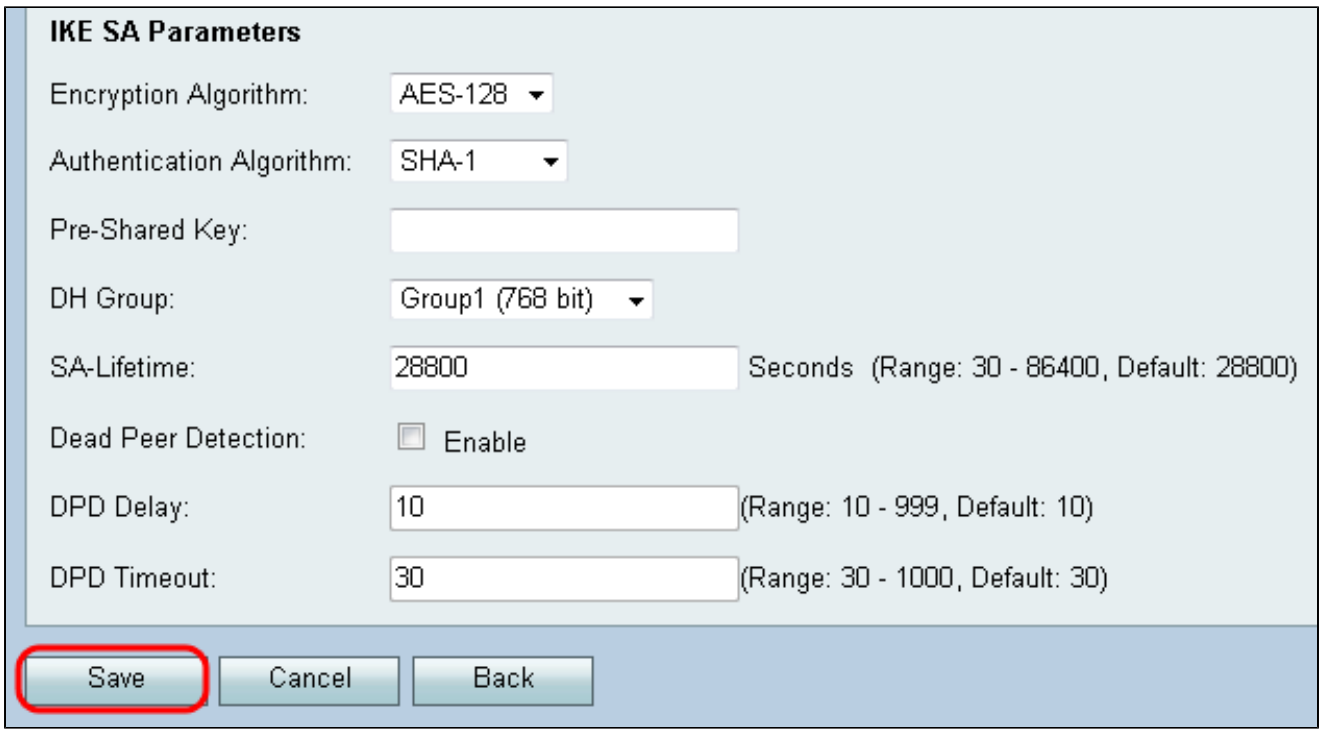
الخطوة 15. (إختياري) إذا قمت بتمكين كشف النظير الميت، فأدخل قيمة في حقل تأخير DPD. ستحدد هذه القيمة المدة التي سينتظر فيها الموجه للتحقق من اتصال العميل.



الخطوة 16. (إختياري) إذا قمت بتمكين كشف النظير غير الصحيح، فأدخل قيمة في حقل مهلة DPD. ستحدد هذه القيمة المدة التي سيظل العميل خاملا متصلا حتى تنتهي المهلة.



الخطوة 17. انقر فوق حفظ لحفظ التغييرات.



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).