RV160 مادختساب Core Soft VPN لي‌مع نيوكت RV260 و

الهدف

الهدف من هذا المستند هو توضيح كيفية تكوين الإعدادات اللازمة لتوصيل عميل Microsoft VPN عبر موجهات من السلسلة RV160 أو RV260.

مقدمة عن أساسيات الشبكة الخاصة الظاهرية (VPN)

تعد الشبكة الخاصة الظاهرية (VPN) طريقة رائعة لربط المستخدمين عن بعد بشبكة آمنة. وهو يؤسس اتصال مشفر عبر شبكة أقل أمانا مثل الإنترنت.

تؤسس نفق الشبكة الخاصة الظاهرية (VPN) شبكة خاصة يمكنها إرسال البيانات بشكل آمن باستخدام التشفير والمصادقة. تستخدم مكاتب الشركات غالبا اتصال الشبكة الخاصة الظاهرية (VPN) نظرا لأنه من المفيد والضروري على حد سواء للسماح لموظفيها بالوصول إلى مواردهم الداخلية، حتى إذا كانوا خارج المكتب.

يدعم الموجه RV160 ما يصل إلى 10 أنفاق للشبكة الخاصة الظاهرية (VPN)، كما يدعم الموجه RV260 ما يصل إلى 20 نفقا.

ستقوم هذه المقالة بالمرور عليك عبر الخطوات اللازمة لتكوين الموجه RV160/RV260 وعميل الشبكة الخاصة الظاهرية (VPN) البسيط. ستتعلم كيفية إنشاء مجموعة مستخدمين وحساب مستخدم وملف تعريف IPsec وملف تعريف من العميل إلى الموقع. على عميل Show Soft VPN، ستتعلم كيفية تكوين علامات التبويب "عام" و"العميل" و"تحليل الاسم" و"المصادقة" و"المرحلة 1" و"المرحلة 2".

ما هي الإيجابيات والسلبيات إذا أردت إستخدام شبكة خاصة ظاهرية (VPN)؟

وتعالج شبكات VPN سيناريوهات حالات الاستخدام الحقيقي الشائعة في العديد من الصناعات وأنواع الأعمال. يوضح الجدول التالي بعض إيجابيات إستخدام شبكة خاصة ظاهرية (VPN) وسلبياتها.

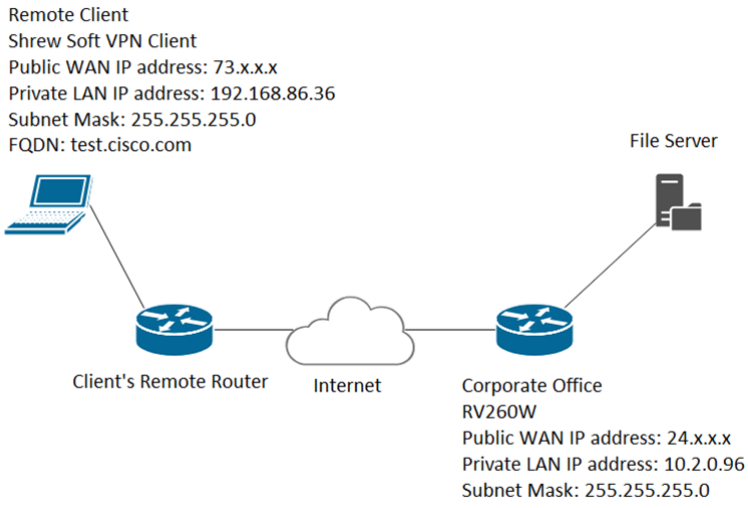
إيجابيات	مخاريط
يوفر إتصالات وآمان وسهولة في الوصول مع حقوق وصول مصممة خصيصا للمستخدمين الأفراد، مثل الموظفين أو المقاولين أو الشركاء.	يمكن أن تحدث سرعة اتصال بطيئة. ويتطلب تعزيز التشفير الوقت والموارد لضمان عدم الكشف عن الهوية وكذلك الأمن. يتطلب تشفير حركة مرور الشبكة عادة زيادة المصاريف العامة. قد تكون قادرا على العثور على إثنين من مزودي الشبكات الخاصة الظاهرية (VPN) ممن يحافظان على سرعة اتصال جيدة مع الحفاظ على السرية والأمان في الوقت نفسه، ولكن عادة ما تكون الخدمات مدفوعة الأجر لهما.
تعمل على تحسين الإنتاجية من خلال توسيع شبكة الشركة والتطبيقات.	المخاطر الأمنية المحتملة بسبب التكوينات الخاطئة. قد يكون تصميم شبكة خاصة ظاهرية (VPN) وتنفيذها أمرا معقدا. من الضروري أن تعهد لمحترف متمرس لتكوين شبكة VPN الخاصة بك للتأكد من

	عدم تعرض شبكتك للخطر.
تقليل تكاليف الاتصالات وزيادة المرونة.	إذا حدثت حالة تكون فيها الحاجة إلى إضافة بنية أساسية جديدة أو مجموعة جديدة من التكوينات، فقد تنشأ مشاكل فنية بسبب عدم التوافق، خصوصا إذا كان يتضمن منتجات أو موردين مختلفين غير الذين تستخدمها بالفعل.
الموقع الجغرافي الفعلي للمستخدمين محمي ولا يتعرض للشبكات العامة أو المشتركة مثل الإنترنت.	
حماية بيانات الشبكة ومواردها السرية.	
تسمح الشبكة الخاصة الظاهرية (VPN) بإضافة مستخدمين جدد أو مجموعة مستخدمين جدد دون الحاجة إلى مكونات إضافية أو تكوين معقد.	

طوبولوجيا

هذه طوبولوجيا بسيطة للشبكة.

ملاحظة: تم تمويه عنوان IP لواجهة WAN العامة.



الأجهزة القابلة للتطبيق

- RV160
- RV260

إصدار البرامج

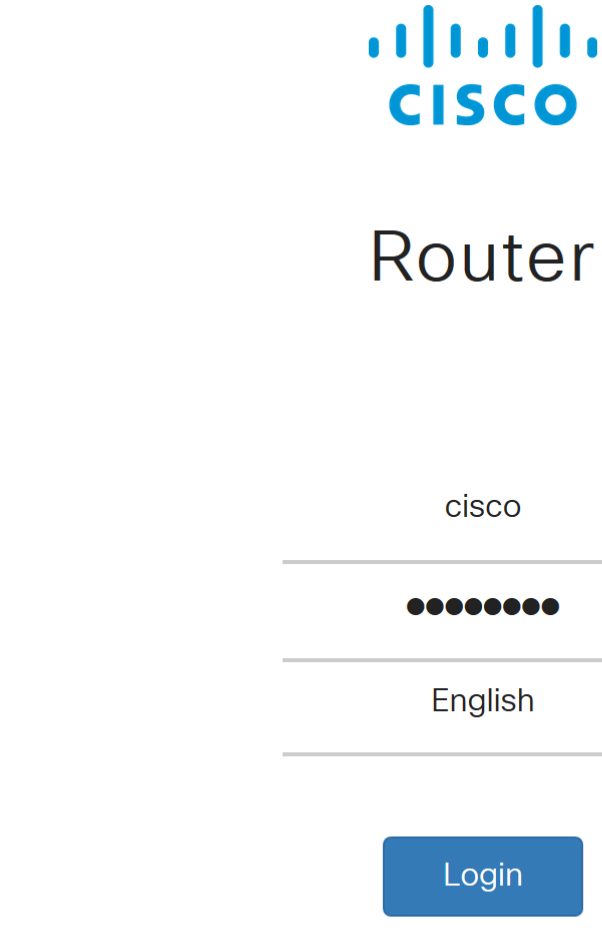
- 1.0.0.xx (RV160 و RV260)
- يوصى ب 2.2.1 نظرا لأن 2.2.2 قد تكون لديها مشاكل في الاتصال بالموجهات الخاصة بنا (تنزيل عميل VPN البسيط Show Soft)

جدول المحتويات

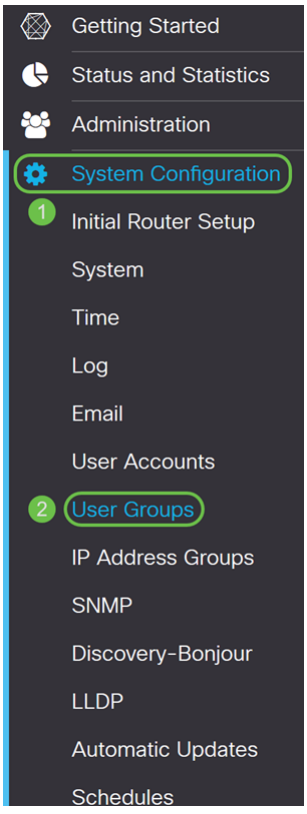
إنشاء مجموعات مستخدمين

ملاحظة هامة: الرجاء ترك حساب المسؤول الافتراضي في مجموعة الإدارة وإنشاء حساب مستخدم جديد ومجموعة مستخدمين ل Show Soft. إذا قمت بنقل حساب المسؤول الخاص بك إلى مجموعة مختلفة، فستمنع نفسك من تسجيل الدخول إلى الموجه.

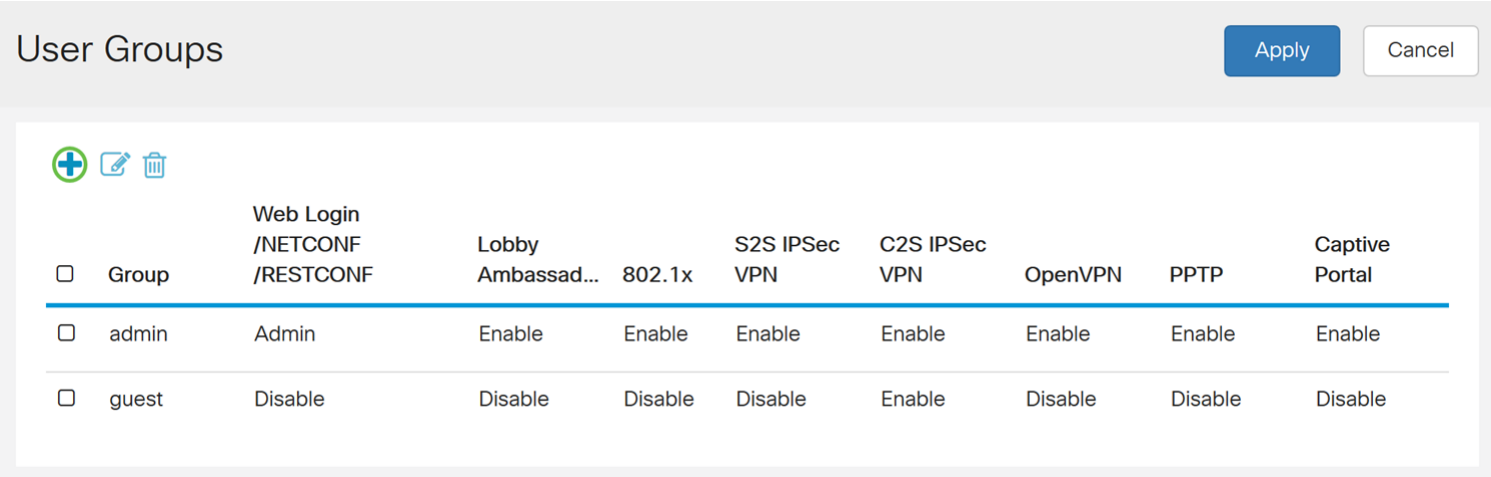
الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب.



الخطوة 2. انتقل إلى **تكوين النظام > مجموعات المستخدمين**.

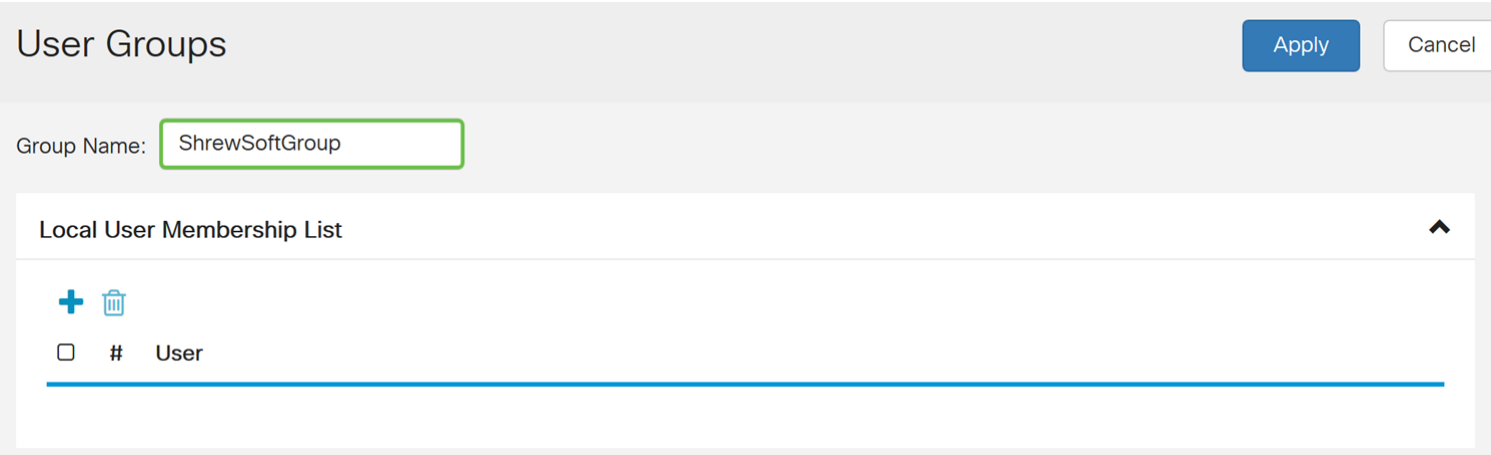


الخطوة 3. انقر فوق أيقونة **الإضافة** لإضافة مجموعة مستخدمين جديدة.

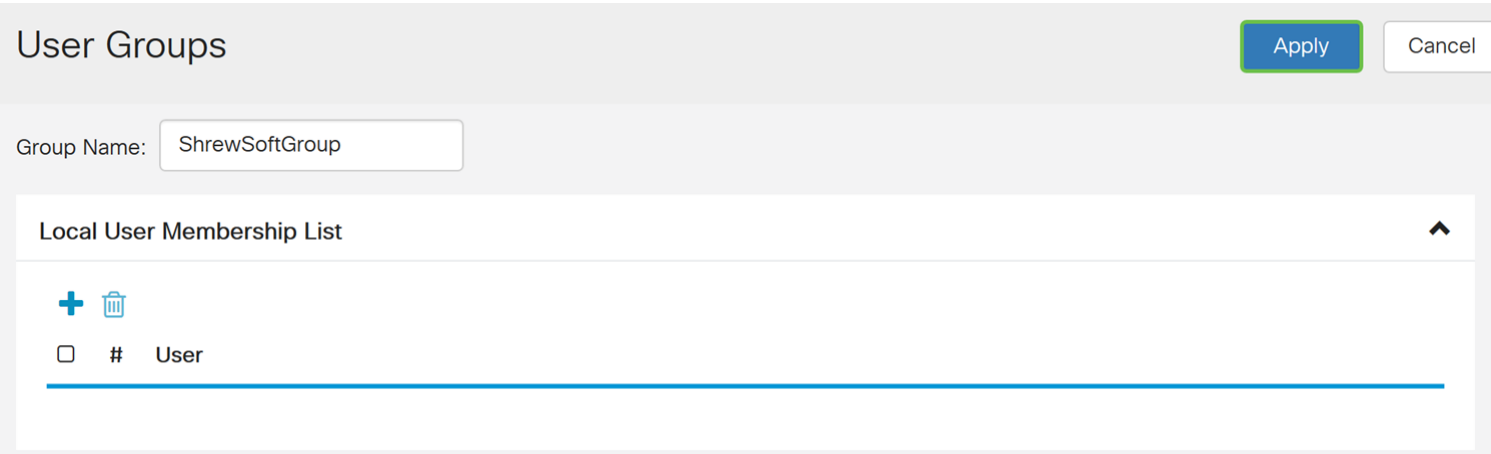


الخطوة 4. أدخل اسما للمجموعة في حقل *اسم المجموعة*.

سنستخدم **ShrewSoftGroup** كمثال لنا.

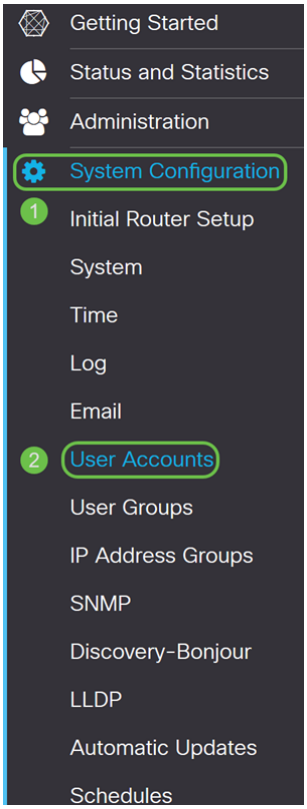


الخطوة 5. اضغط على **تطبيق** لإنشاء مجموعة جديدة.

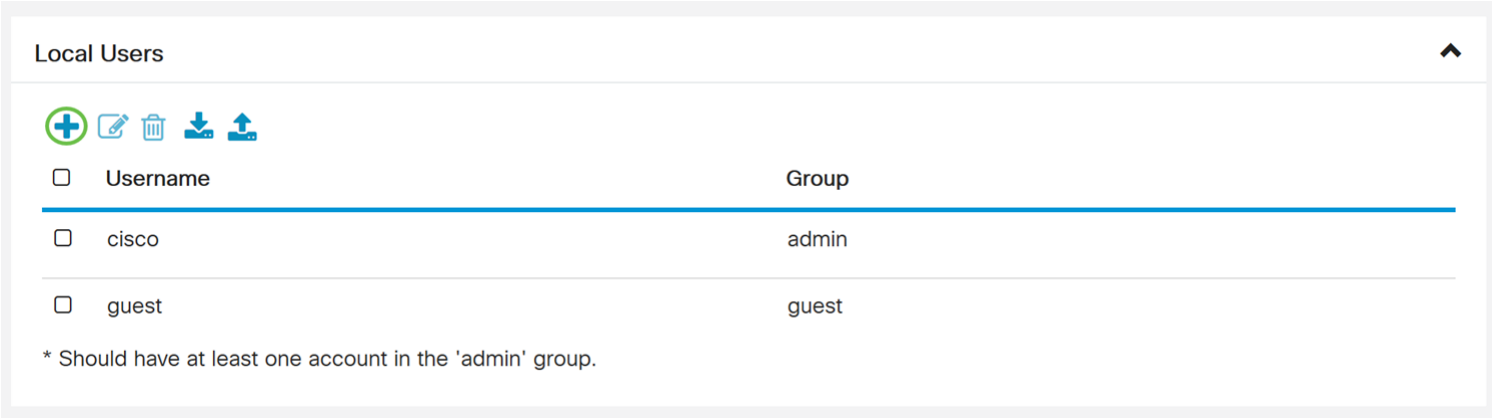


إنشاء حسابات مستخدمين

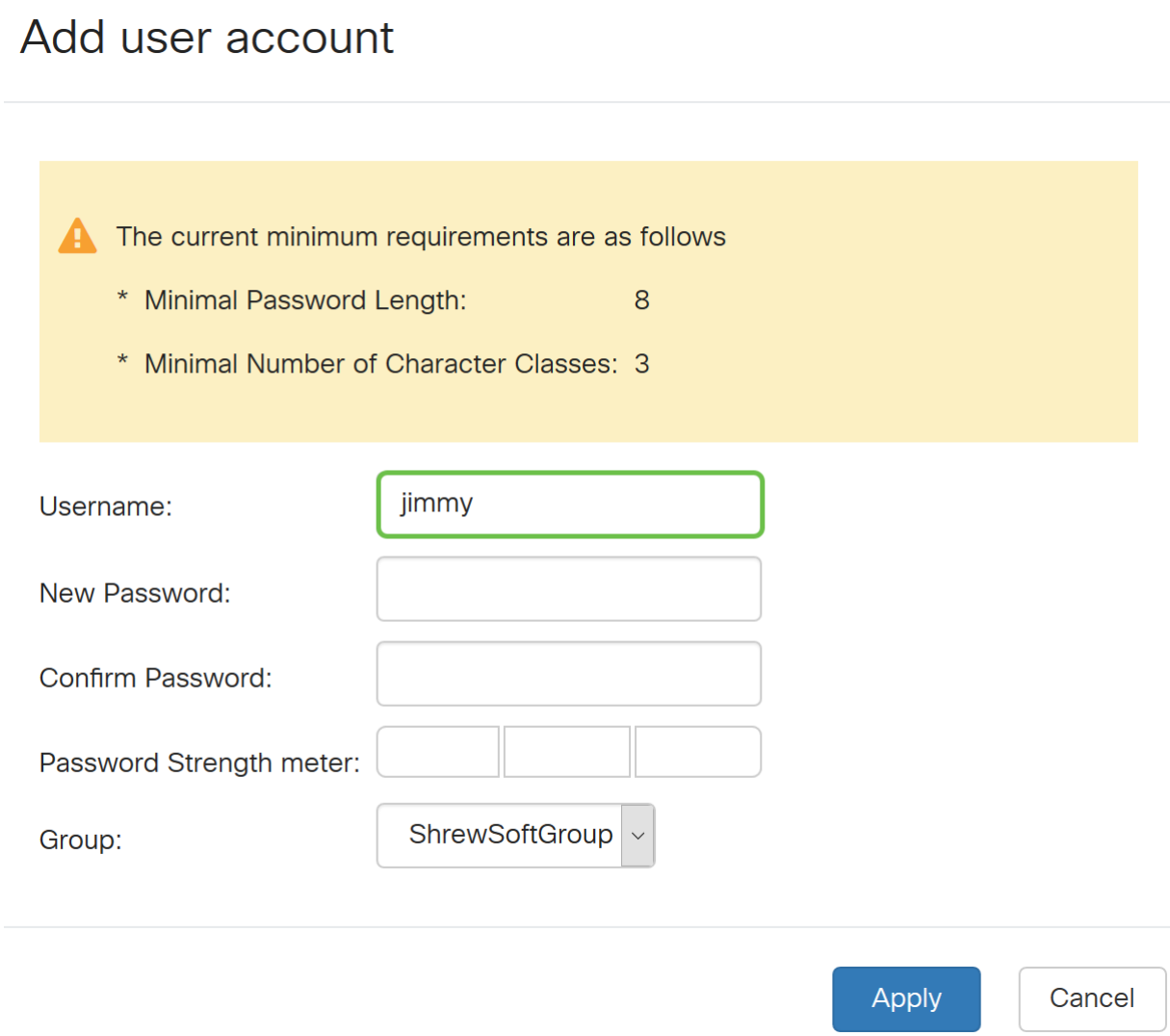
الخطوة 1. انتقل إلى **تكوين النظام > حسابات المستخدمين**.



الخطوة 2. قم بالتمرير لأسفل إلى جدول *المستخدمين المحليين* واضغط على أيقونة **زائد** لإضافة مستخدم جديد.

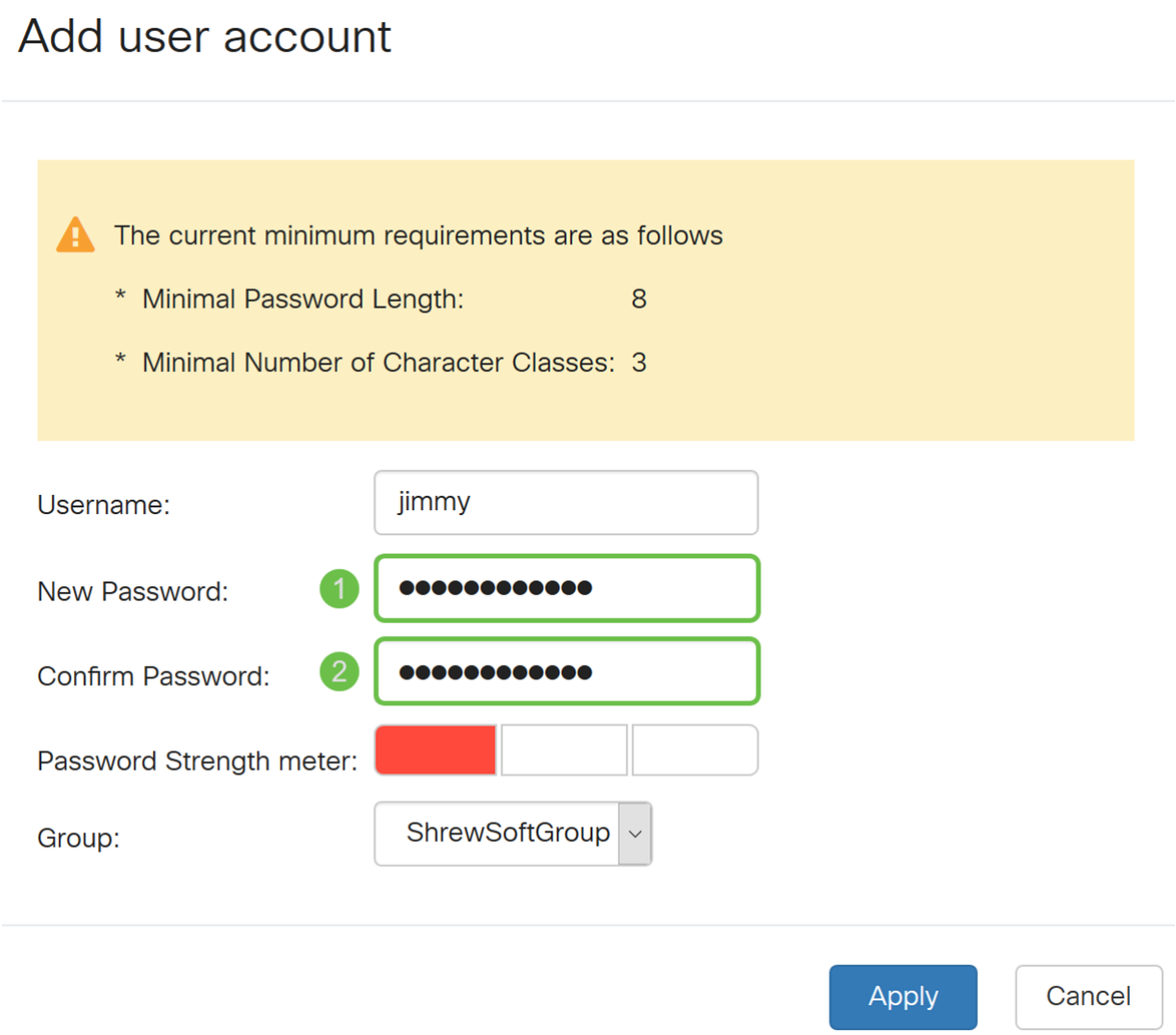


الخطوة 3. يتم فتح صفحة *إضافة حسابات مستخدمين*. أدخل اسم مستخدم للمستخدم.

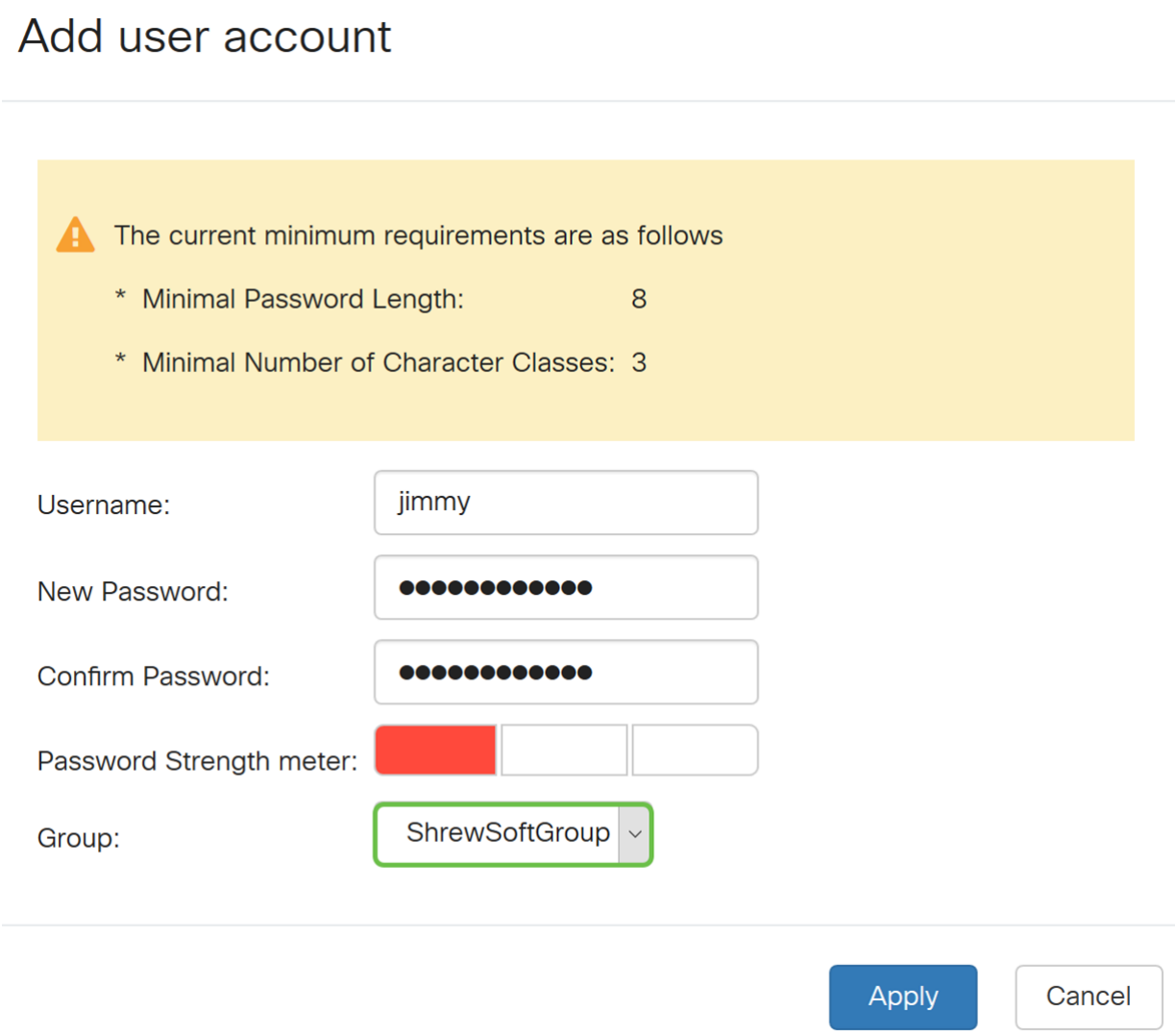


الخطوة 4. أدخل كلمة مرور في حقل *كلمة المرور الجديدة*. أعد إدخال نفس كلمة المرور في حقل *تأكيد كلمة المرور*. في هذا المثال، سنستخدم **CiscoTest123** ككلمة المرور.

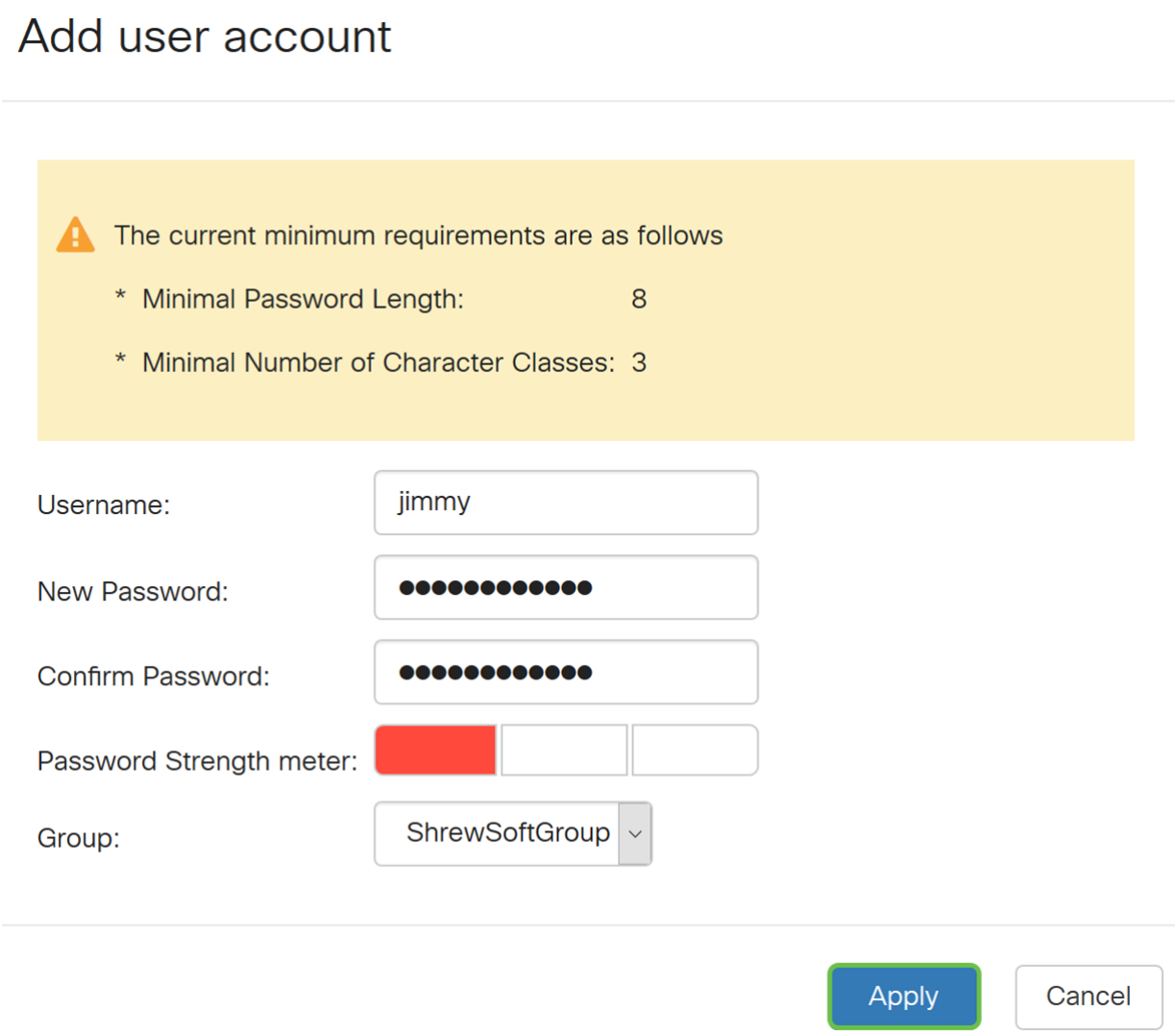
ملاحظة: كلمة المرور المستخدمة هنا هي مثال. يوصى بجعل كلمة المرور أكثر تعقيدا.



الخطوة 5. في القائمة المنسدلة مجموعة ، حدد مجموعة تريد أن يكون المستخدم فيها.

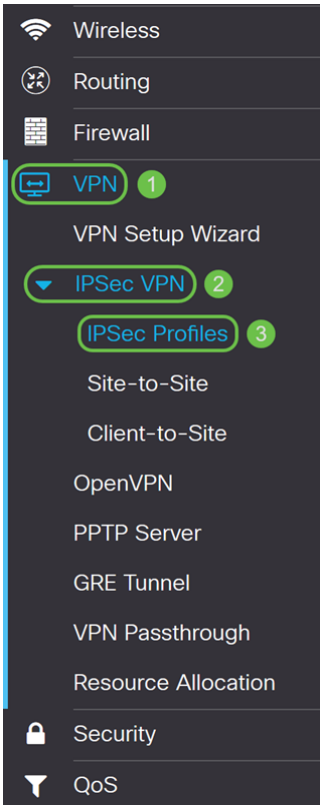


الخطوة 6. اضغط على **تطبيق** لإنشاء حساب مستخدم جديد.



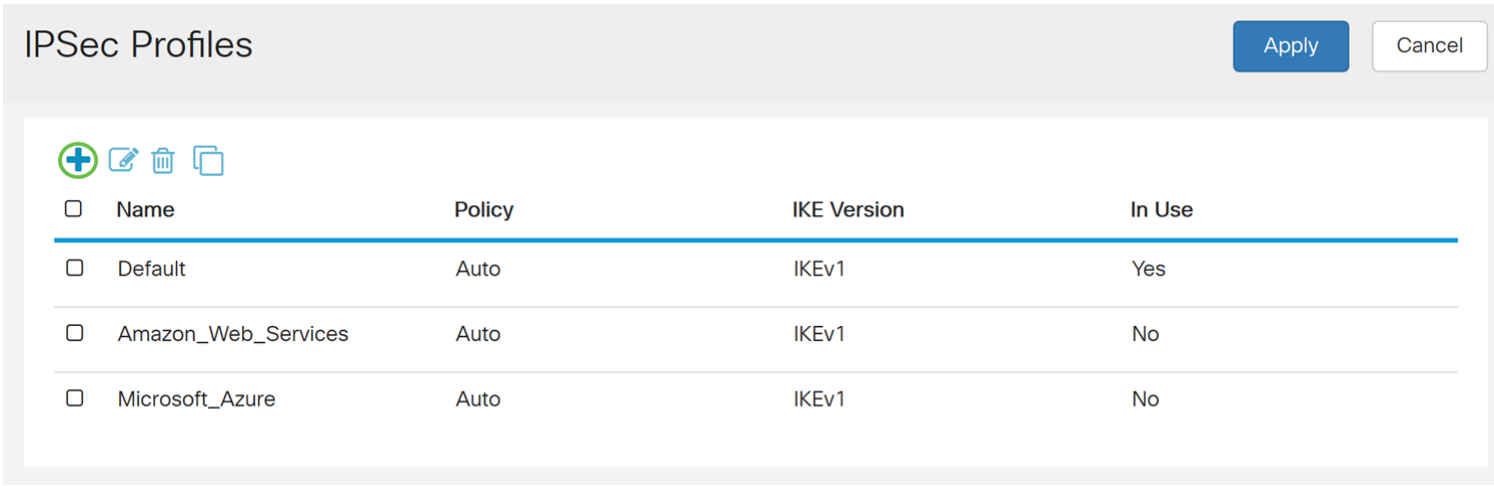
تكوين ملف تعريف IPsec

الخطوة 1. انتقل إلى **VPN > IPSec VPN > توصيفات IPSec**.

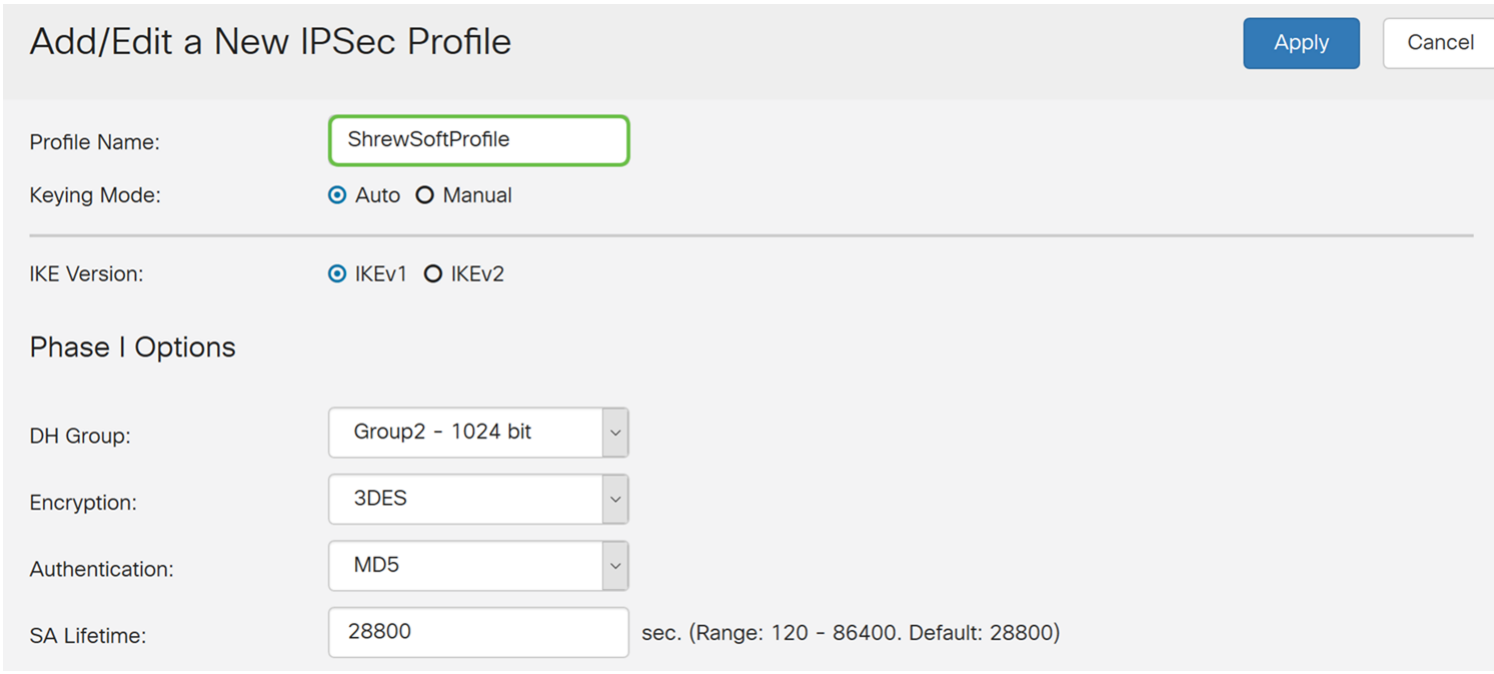


ملاحظة: للحصول على مزيد من الإيضاح حول كيفية تكوين توصيفات IPsec، انقر على الرابط للاطلاع على المقالة: تكوين توصيفات IPsec (وضع الحفظ التلقائي) على RV160 و RV260

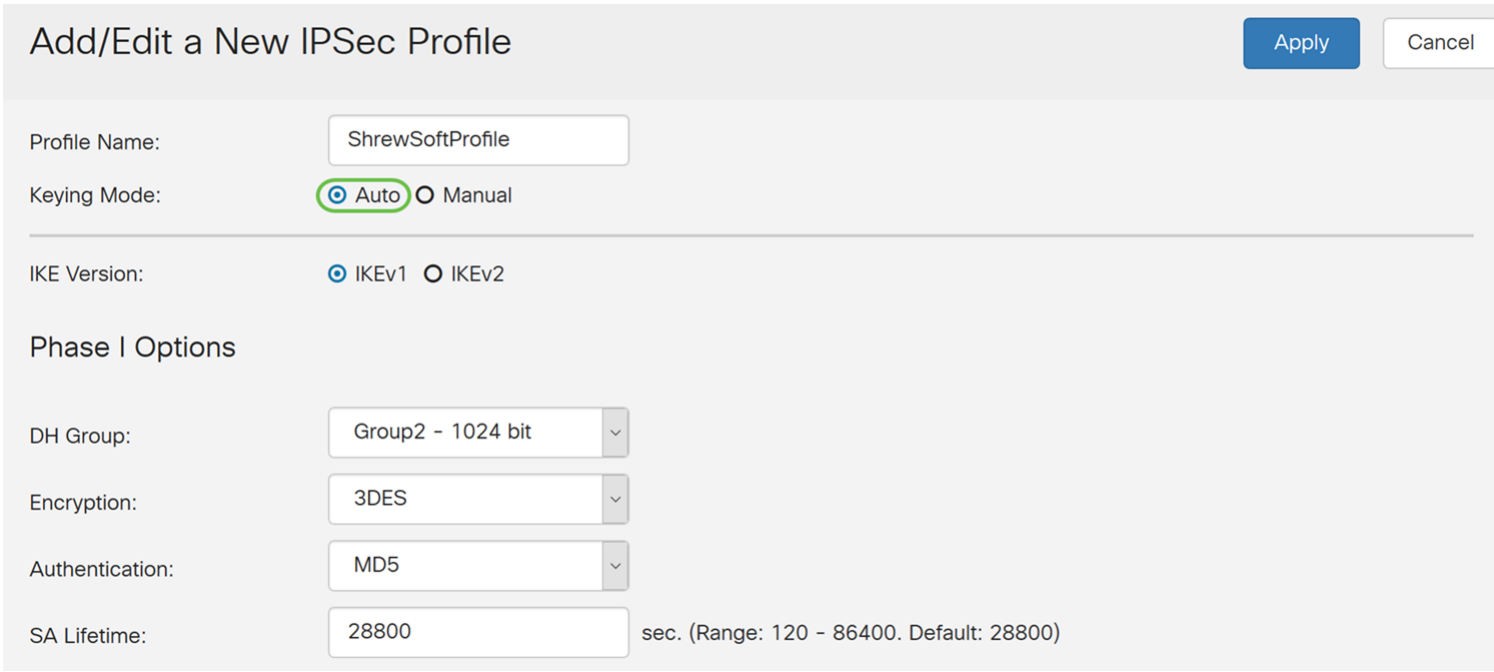
الخطوة 2. انقر على أيقونة **الإضافة** لإضافة ملف تعريف IPsec جديد.



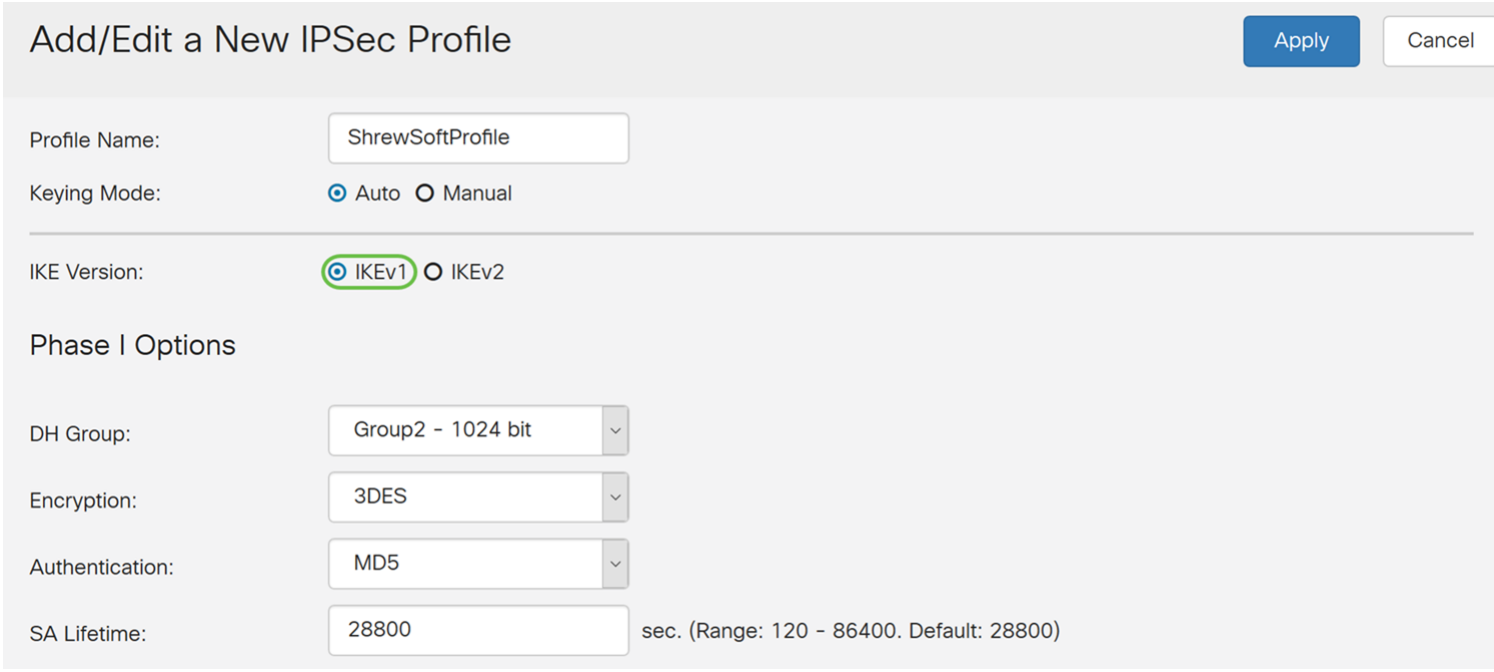
الخطوة 3. أدخل اسم للتوصيف في حقل *اسم التوصيف*. سنقوم بإدخال **ShrewSoftProfile** كاسم ملف التعريف الخاص بنا.



الخطوة 4. حدد **تلقائي** ل *أسلوب الكي*.



الخطوة 5. حدد إما **IKEv1** أو **IKEv2** كإصدار *IKE*. في هذا المثال، تم تحديد IKEv1.



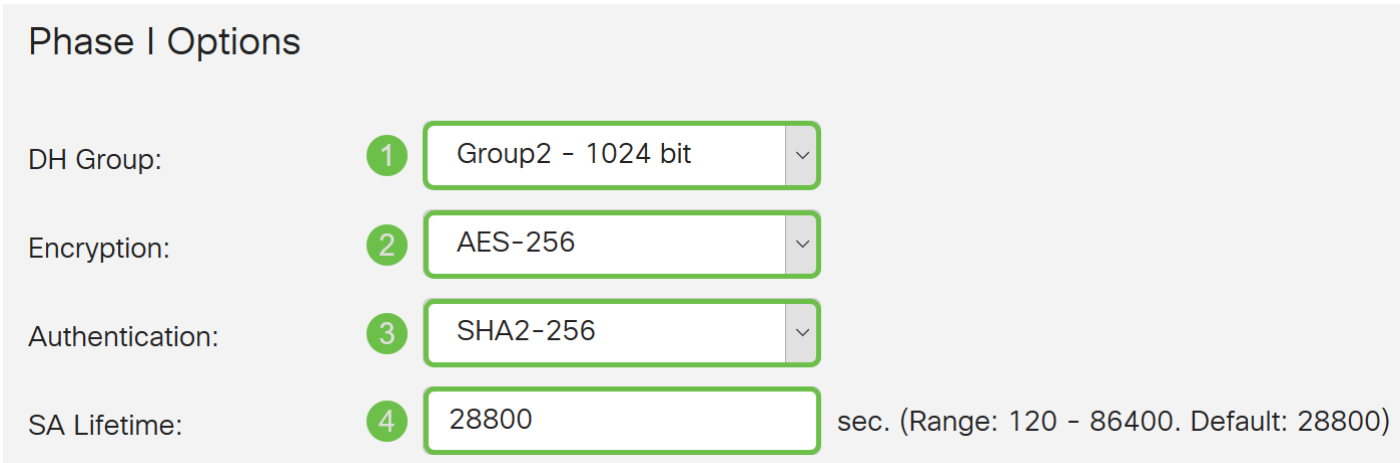
الخطوة 6. تحت قسم *خيارات المرحلة الأولى*، هذا ما قمنا بتكوينه لهذه المقالة.

مجموعة DH: **المجموعة 2 - 1024 بت**

التشفير: **AES-256**

المصادقة: **SHA2-256**

مدة البقاء: **28800**



الخطوة 7. ضمن *خيارات المرحلة الثانية*، هذا ما قمنا بتكوينه لهذه المقالة.

تحديد البروتوكول: **ESP**

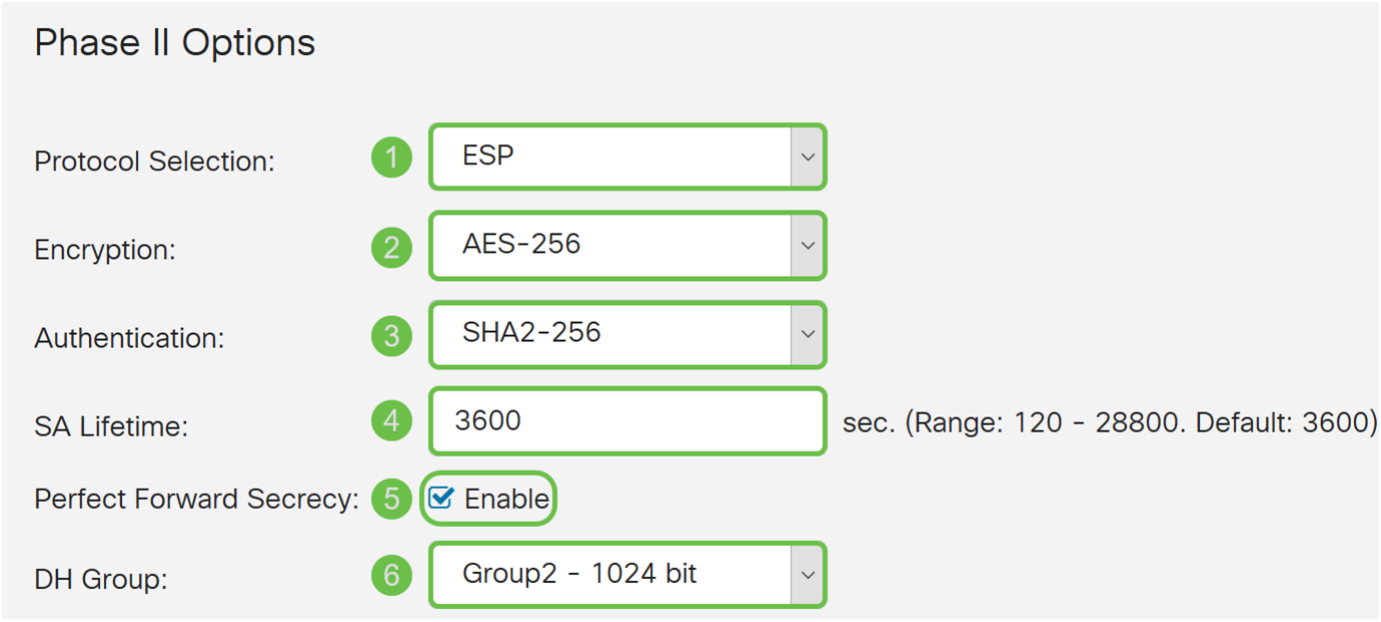
التشفير: **AES-256**

المصادقة: **SHA2-256**

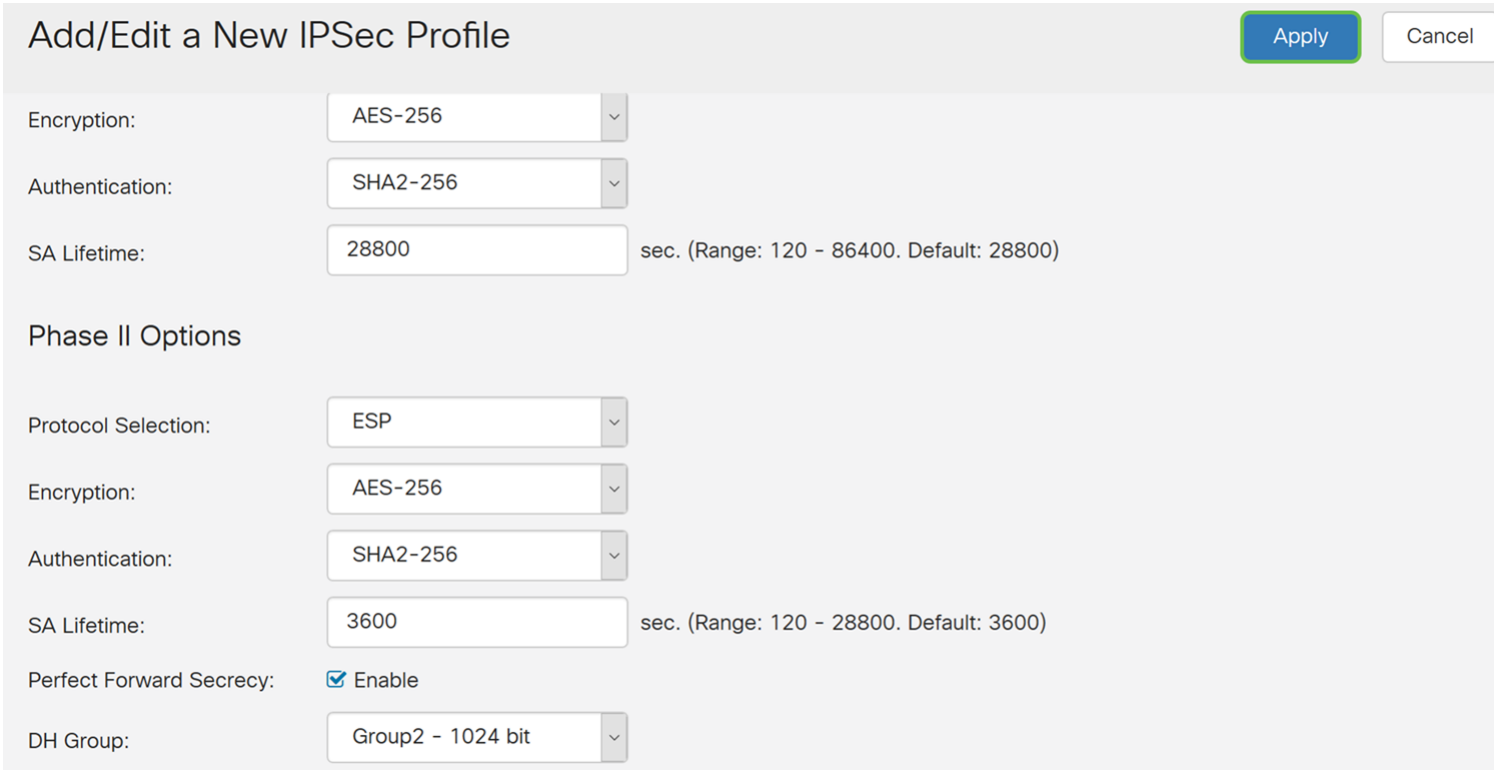
مدة البقاء: **3600**

سرية إعادة التوجيه المثالية: **ممكنة**

مجموعة DH: **المجموعة 2 - 1024 بت**

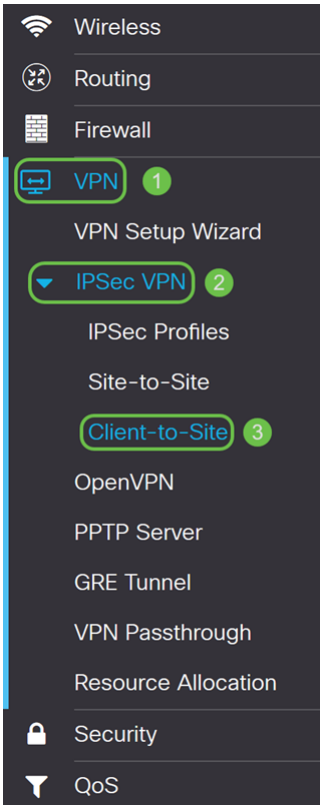


الخطوة 8. انقر على **تطبيق** لإنشاء ملف تعريف IPsec الجديد.

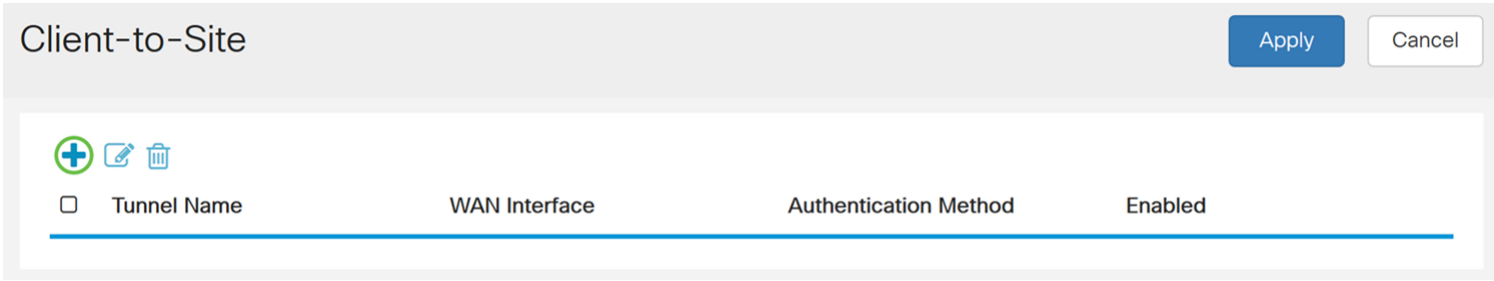


تكوين عميل إلى موقع

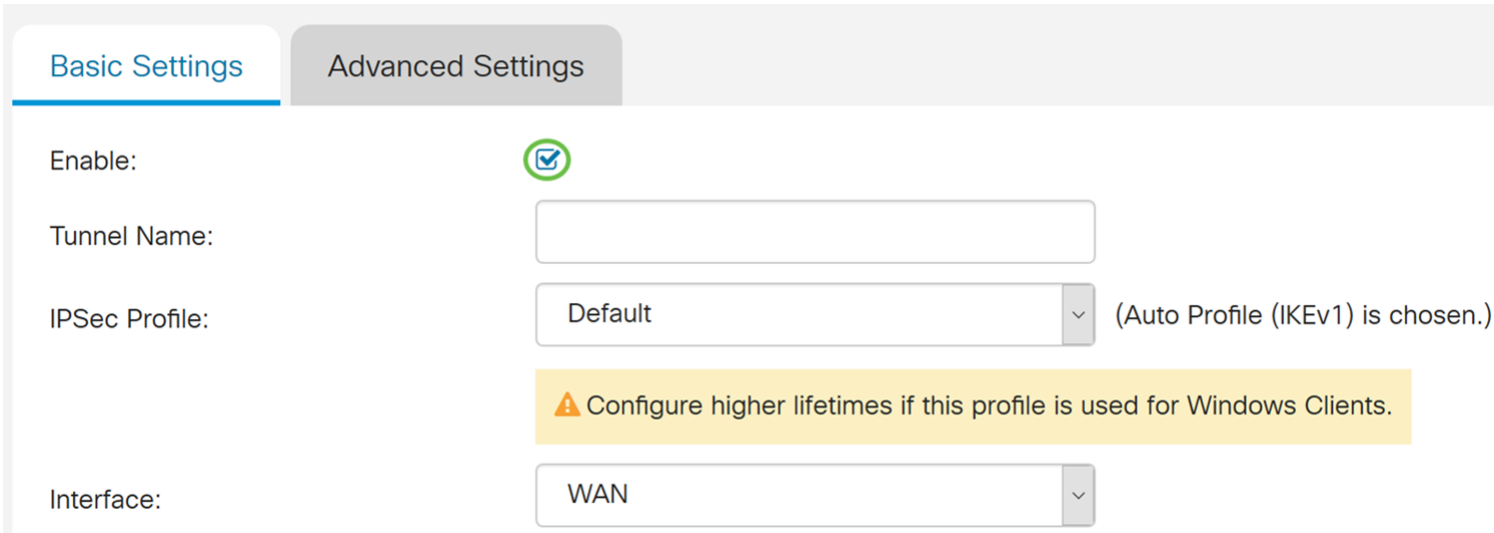
الخطوة 1. انتقل إلى **IPSec VPN > VPN > من عميل إلى موقع**.



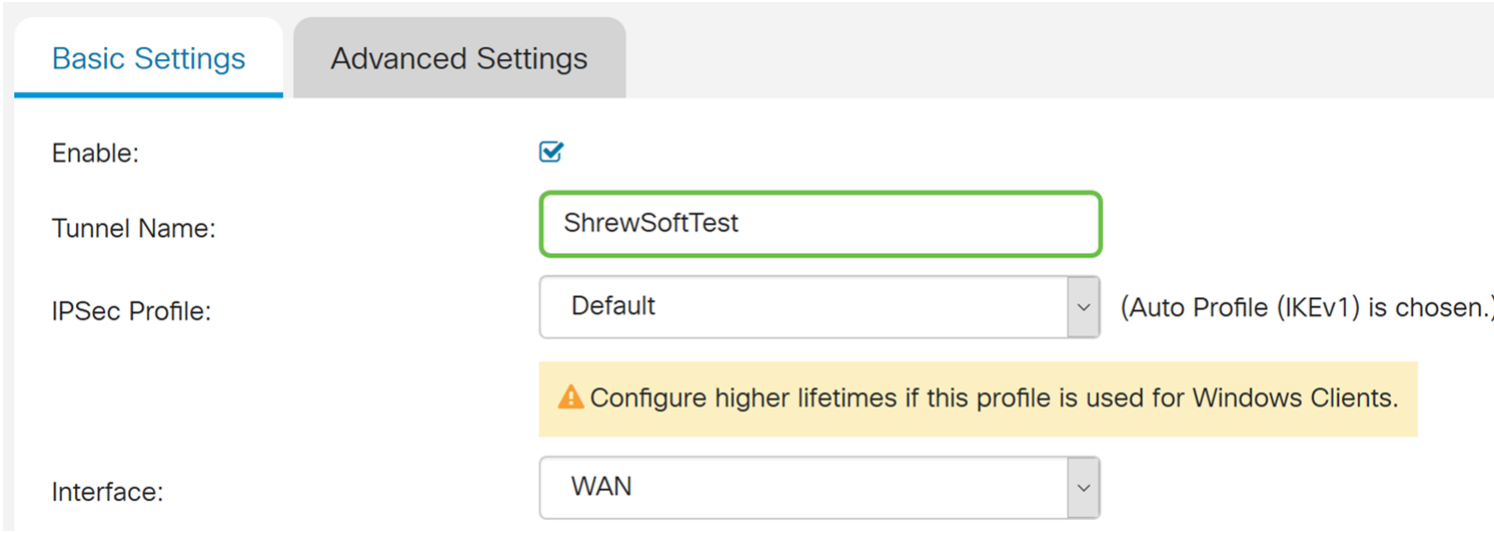
الخطوة 2. انقر فوق أيقونة **الجمع** لإضافة نفق جديد.



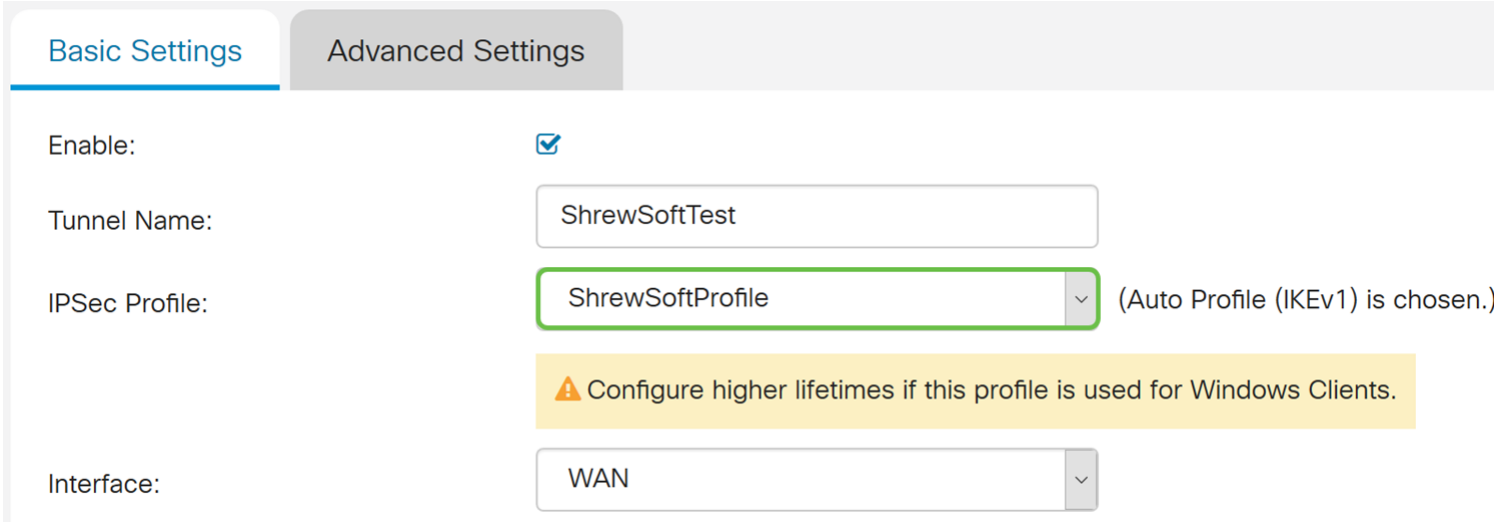
الخطوة 3. حدد خانة الاختيار **تمكين** لتمكين النفق.



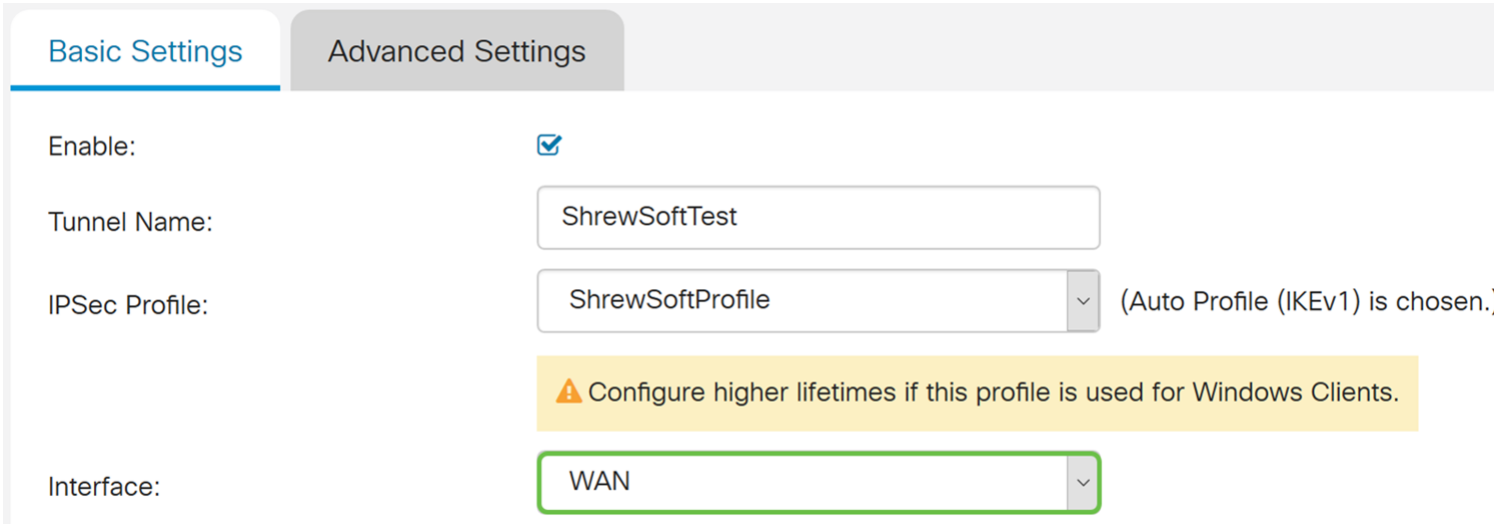
الخطوة 4. أدخل اسم للنفق في حقل *اسم النفق*.



الخطوة 5. في القائمة المنسدلة *ملف تعريف IPSec*، حدد ملف تعريف تريد إستخدامه. سنختار ShrewSoftProfile الذي تم إنشاؤه في القسم السابق: تكوين ملف تعريف IPsec.



الخطوة 6. من القائمة المنسدلة *الواجهة*، حدد الواجهة التي تريد إستخدامها. سنستخدم شبكة **WAN** كواجهة لنا لتوصيل النفق.

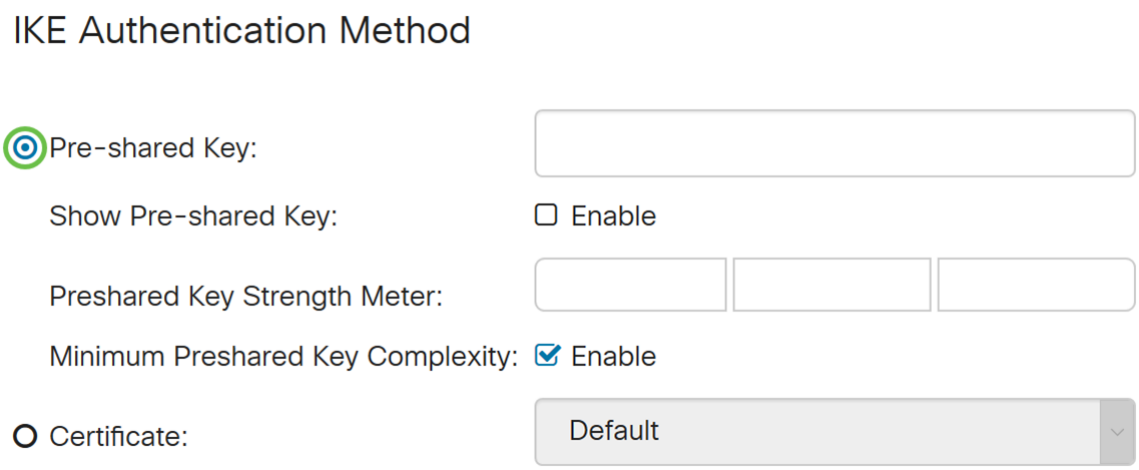


الخطوة 7. تحت قسم *طريقة مصادقة IKE*، حدد إما *مفتاح مشترك مسبقا* أو *شهادة*. سنستخدم **مفتاح مشترك مسبقا** كطريقة مصادقة IKE.

ملاحظة: يصادق نظراء IKE بعضهم البعض عن طريق حساب حزمة مصقولة من البيانات التي تتضمن المفتاح المشترك مسبقا وإرسالها. إذا كان النظير المستقبل قادرا على إنشاء التجزئة نفسها بشكل مستقل باستخدام المفتاح المشترك مسبقا الخاص به، فإنه يعرف أنه يجب على كلا النظرين مشاركة نفس السر، وبالتالي مصادقة

النظير الآخر. لا يتم تطوير المفاتيح المشتركة مسبقا بشكل جيد لأنه يجب تكوين كل نظير IPsec باستخدام مفاتيح مشتركة مسبقا لكل نظير آخر يقوم بإنشاء جلسة عمل معه.

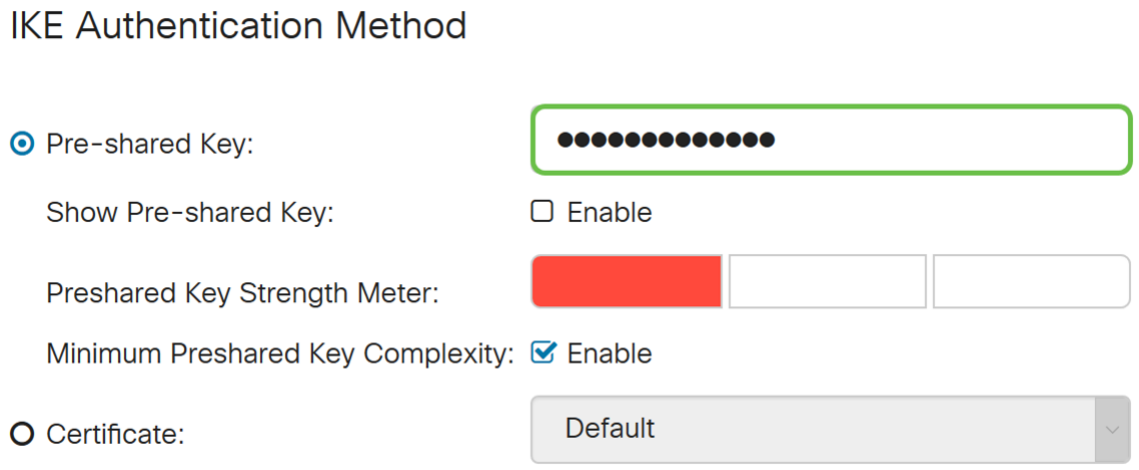
تستخدم الشهادة شهادة رقمية تحتوي على معلومات مثل اسم الشهادة أو عنوانها ورقم تسلسلي وتاريخ انتهاء صلاحيتها ونسخة من المفتاح العام لحاملها.



الخطوة 8. أدخل المفتاح المشترك مسبقا الذي تريد إستخدامه للمصادقة. يمكن أن يكون المفتاح المشترك مسبقا هو ما تريده. يجب أن يكون المفتاح المشترك مسبقا الذي تم تكوينه على عميل Shrew Soft VPN هو نفسه هنا عند تكوينه.

في هذا المثال، سنستخدم **CiscoTest123!** كمفتاح مشترك مسبقا.

ملاحظة: المفتاح المشترك مسبقا الذي تم إدخاله هنا هو مثال. يوصى بإدخال مفتاح مشترك مسبقا أكثر تعقيدا.

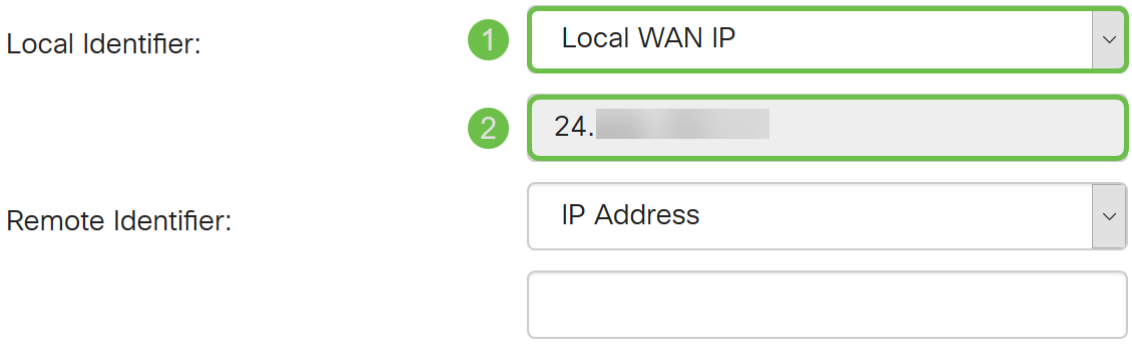


الخطوة 9. حدد *المعرف المحلي* من القائمة المنسدلة. يتم تعريف الخيارات التالية على أنها:

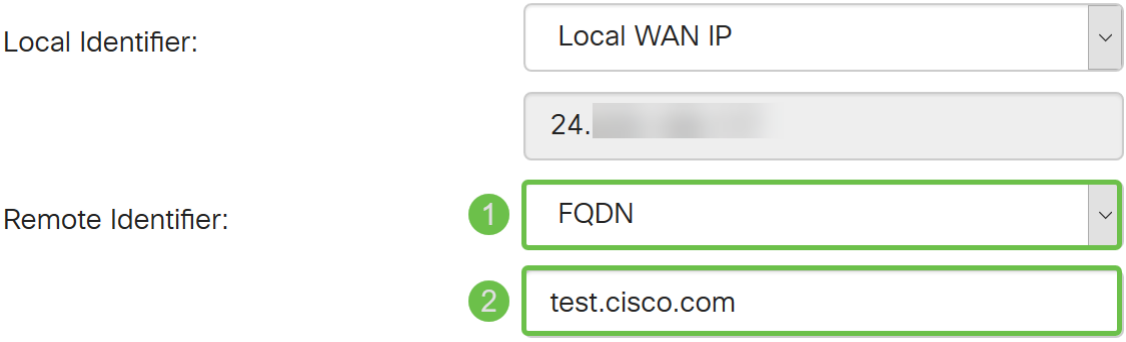
- WAN IP المحلي - يستخدم هذا الخيار عنوان IP الخاص بواجهة شبكة المنطقة الواسعة (WAN) لبوابة VPN
- عنوان IP - يسمح هذا الخيار لك بإدخال عنوان IP يدويا لاتصال VPN. ستحتاج إلى إدخال عنوان IP لواجهة WAN الخاصة بالموجه في الموقع (المكتب).
- FQDN - يستخدم هذا الخيار اسم المجال المؤهل بالكامل (FQDN) الخاص بالموجه عند إنشاء اتصال VPN.
- User FQDN (المستخدم) - يتيح لك هذا الخيار إستخدام اسم مجال كامل لمستخدم معين على الإنترنت.

في هذا المثال، سنختار **WAN IP المحلي** كمعرف محلي.

ملاحظة: سيتم ملء IP المحلي لشبكة WAN للموجه تلقائيا.



الخطوة 10. في القائمة المنسدلة *المعرف البعيد* ، حدد إما **عنوان IP** أو **FQDN** أو **المستخدم FQDN**. ثم أدخل الاستجابة المناسبة مما قمت بتحديده. في هذا المثال، سنقوم بتحديد **FQDN** ودخول **test.cisco.com**.



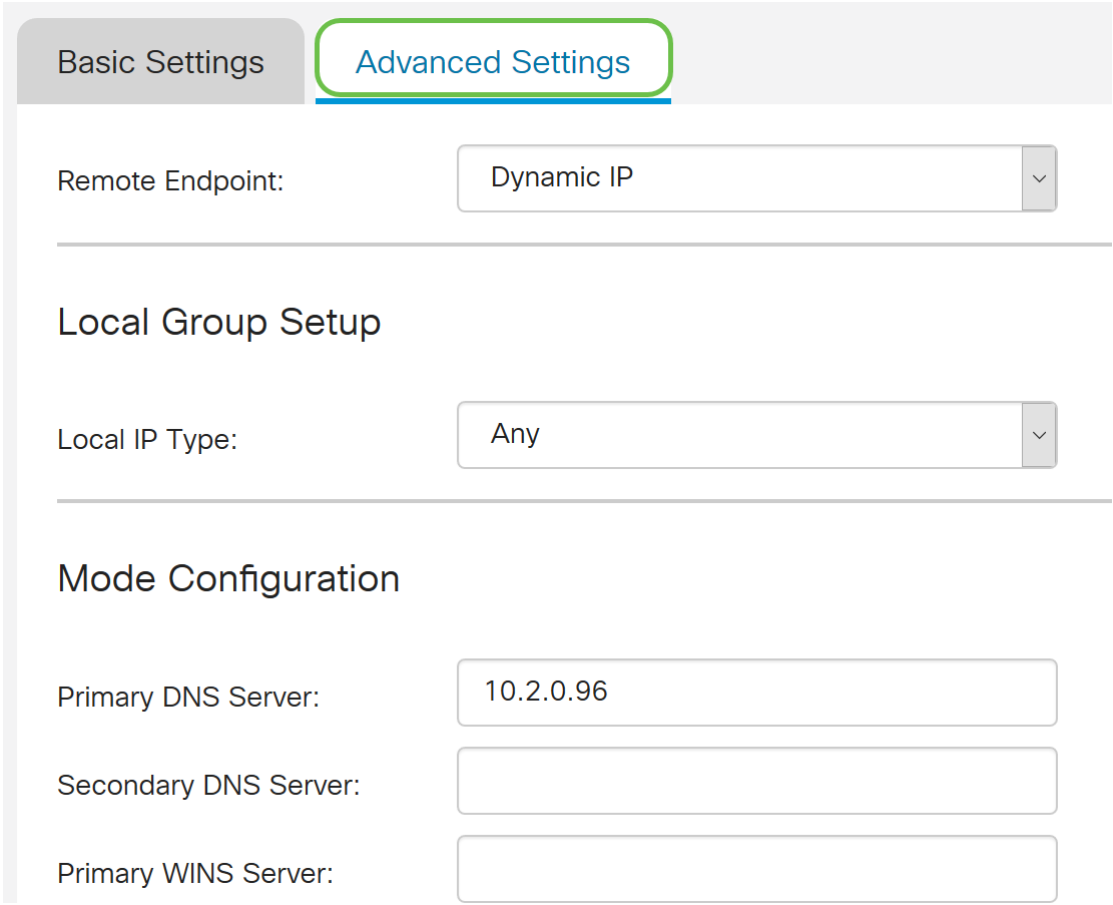
الخطوة 11. حدد خانة الاختيار **مصادقة موسعة** للتمكين. وسيوفر ذلك مستوى إضافيا من المصادقة يتطلب من المستخدمين عن بعد المفتاح في بيانات الاعتماد الخاصة بهم قبل منحهم حق الوصول إلى شبكة VPN.

إذا قمت بتمكين *المصادقة الموسعة*، انقر فوق أيقونة **زائد** لإضافة مجموعة مستخدمين. حدد المجموعة من القائمة المنسدلة التي تريد إستخدامها للمصادقة الموسعة. سنختار **ShrewSoftGroup** كمجموعة.

الخطوة 12. في *نطاق التجمع لشبكة LAN الخاصة بالعميل*، أدخل نطاق عناوين IP التي يمكن تعيينها لعميل VPN في حقل *بدء IP* و*نهاية IP*. يجب أن يكون هذا مجموعة من العناوين التي لا تتداخل مع عناوين الموقع.

سندخل **10.2.1.1** كعنوان *Start IP* و**10.2.1.254** كعنوان *IP الطرفي*.

الخطوة 13. (إختياري) انقر على علامة التبويب **إعدادات متقدمة**.



الخطوة 14. (إختياري) هنا يمكنك تحديد عنوان IP لنقطة النهاية البعيدة. سنستخدم في هذا الدليل **IP الديناميكي**، حيث إن عنوان IP الخاص بالعميل النهائي غير ثابت.

يمكنك أيضا تحديد الموارد الداخلية التي ستكون متوفرة ضمن *إعداد المجموعة المحلية*.

إذا قمت بتحديد **Any**، فستتوفر جميع الموارد الداخلية.

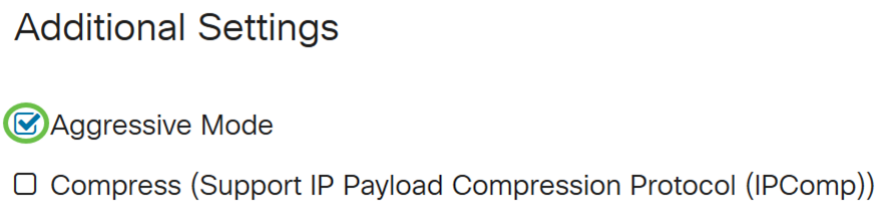
يمكنك أيضا إختيار إستخدام خوادم DNS و WINS الداخلية. لذلك تحتاج إلى تحديدها ضمن *تكوين الوضع*.

لديك أيضا إمكانية إستخدام النفق الكامل أو المقسم وتقسيم DNS.

قم بالتمرير لأسفل إلى *إعدادات إضافية*. حدد خانة الاختيار **Aggressive Mode** لتمكين الوضع المتميز. الوضع العدواني هو عندما يتم ضغط التفاوض ل IKE SA في ثلاث حزم مع جميع بيانات SA المطلوبة ليتم تمريرها من قبل البادئ. المفاوضات أسرع ولكن لديهم قابلية للتأثر بهويات التبادل في نص واضح.

ملاحظة: معلومات إضافية عن الوضع الرئيسي مقابل الوضع القوي، يرجى الاطلاع على الوضع الرئيسي مقابل الوضع القوي

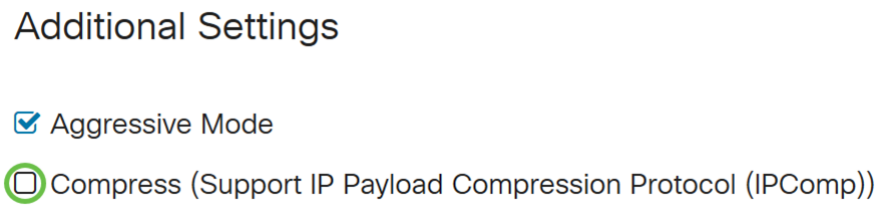
في هذا المثال، سنقوم بتمكين **Aggressive Mode**.



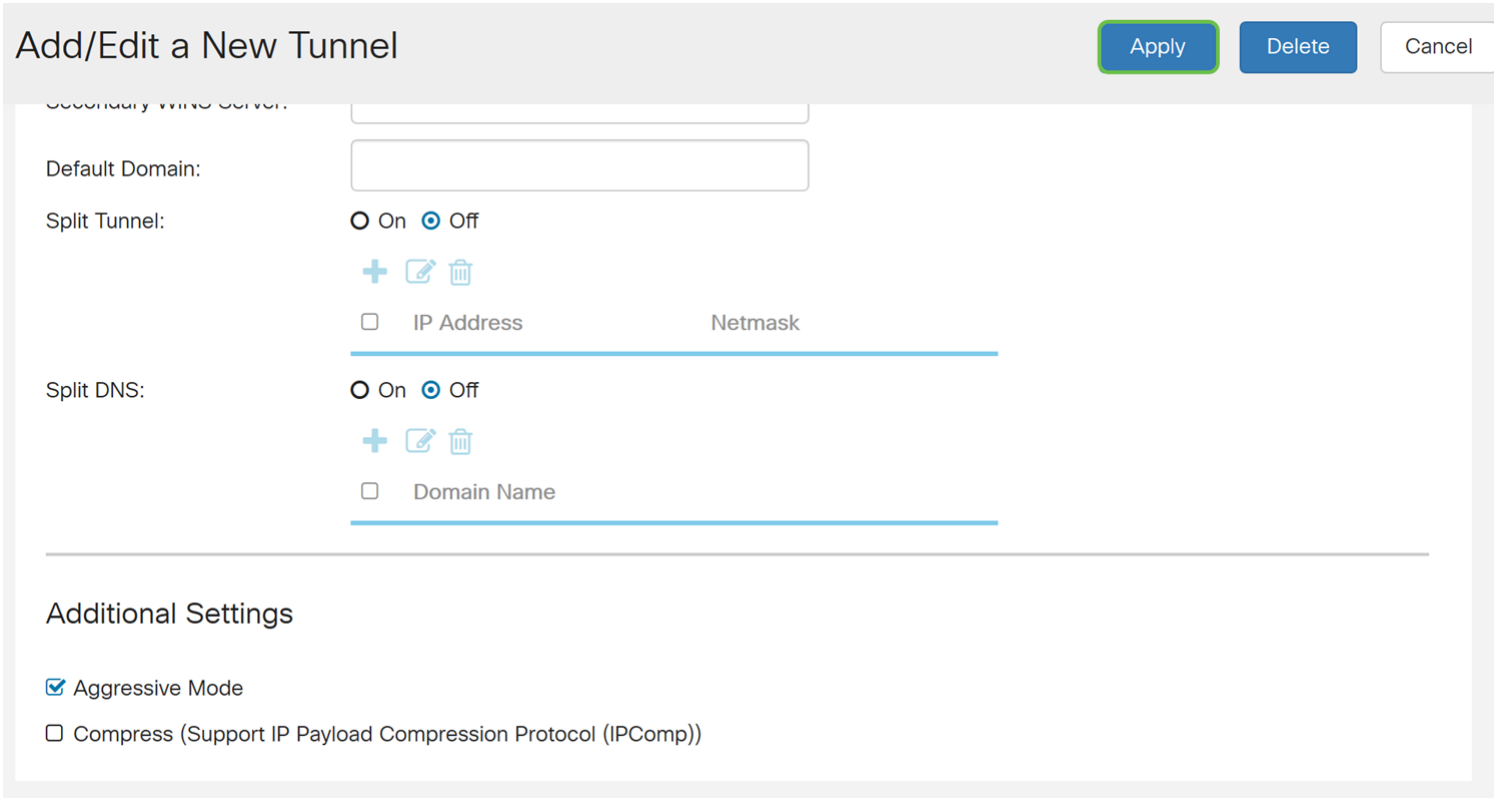
الخطوة 15. (إختياري) حدد خانة الاختيار **ضغط (دعم بروتوكول ضغط حمولة IP (IPComp))** لتمكين الموجه من اقتراح الضغط عند بدء إتصاله. هذا بروتوكول يقلل من حجم مخططات بيانات IP. إذا رفض المستجيب هذا الاقتراح، فلن يقوم الموجه بتنفيذ الضغط. عندما يكون الموجه هو المستجيب، فإنه يقبل الضغط، حتى إذا لم

يتم تمكين الضغط.

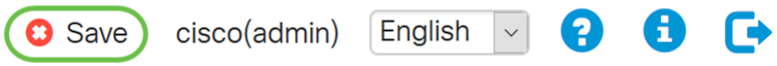
سنترك *الضغط* بدون تحديد.



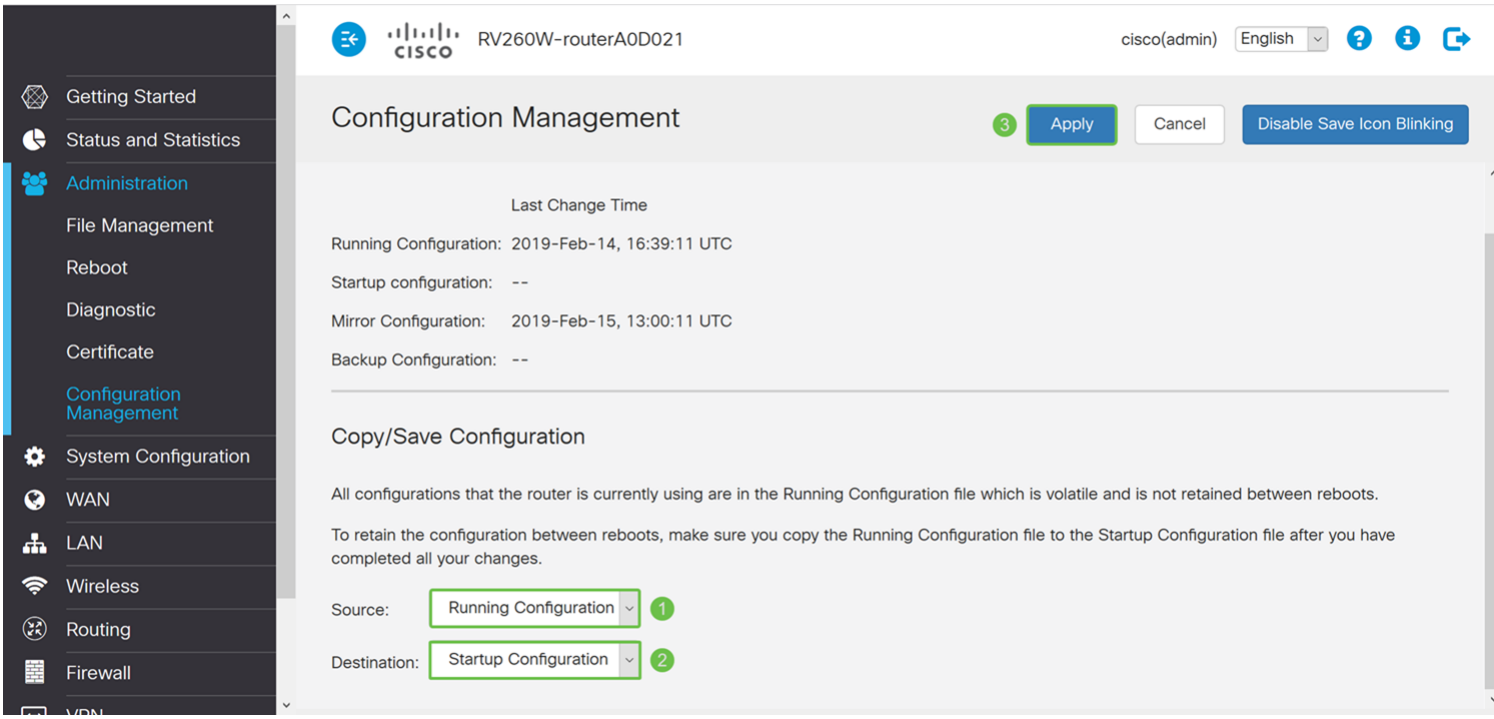
الخطوة 16. انقر فوق **تطبيق** لإضافة النفق الجديد.



الخطوة 17. انقر فوق أيقونة **الوميض حفظ** في أعلى صفحة تكوين الويب.



الخطوة 18. تظهر صفحة *إدارة التكوين*. في قسم تكوين النسخ/الحفظ، تأكد من أن حقل *المصدر* لديه **تكوين جار** *والوجهة* به **تكوين بدء التشغيل**. ثم اضغط على **تطبيق**. 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 بالتكوين الخاص بك بين عمليات إعادة التمهيد.

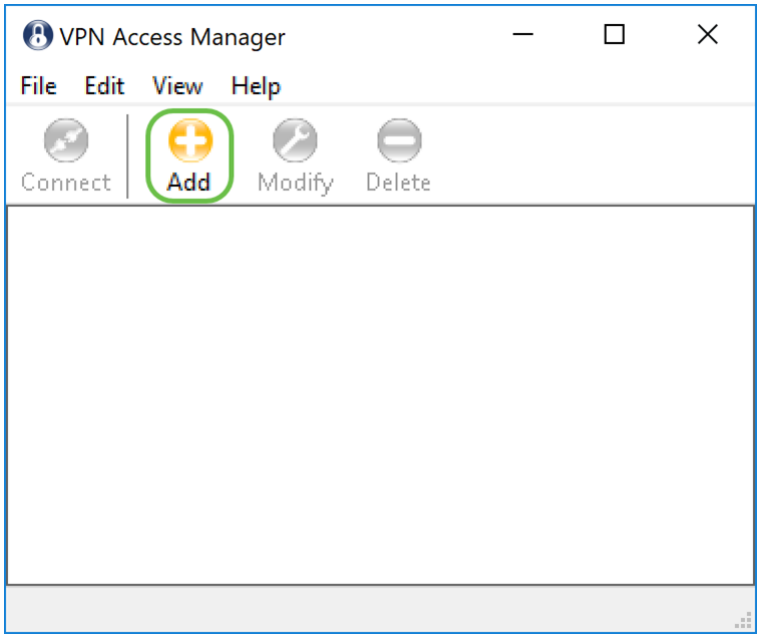


تكوين زبون Core Soft VPN

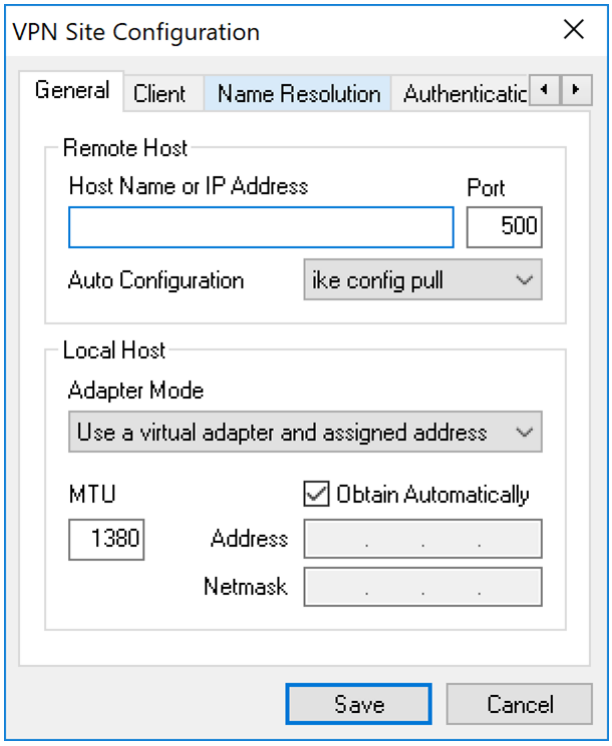
إذا لم تقم بتنزيل Shrew Soft VPN Client، فلا تتردد في تنزيل العميل بالنقر فوق هذا الارتباط: قم بتنزيل Soft VPN Client ل Windows. سنستخدم الإصدار القياسي. إذا كنت قد قمت بالفعل بتنزيل Shrew Soft VPN Client، فلا تتردد في المتابعة إلى الخطوة الأولى.

عميل Shrew Soft VPN: علامة التبويب العامة

الخطوة 1. افتح مدير الوصول إلى الشبكة الخاصة الظاهرية (VPN) وانقر على **إضافة** لإضافة ملف تعريف جديد.

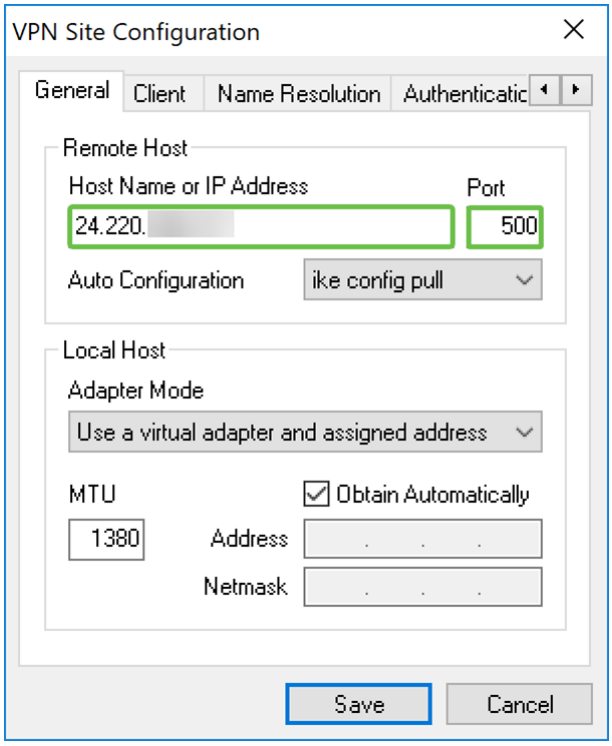


تظهر نافذة تكوين موقع *VPN*.



الخطوة 2. في قسم *المضيف البعيد* ضمن علامة التبويب *عام*، أدخل اسم المضيف العام أو عنوان IP للشبكة التي تحاول الاتصال بها. في هذا المثال، سنقوم بإدخال عنوان IP لشبكة WAN الخاص ب RV160/RV260 في الموقع لإعداد الاتصال.

ملاحظة: تأكد من تعيين رقم المنفذ على القيمة الافتراضية ل 500. لكي تعمل الشبكة الخاصة الظاهرية (VPN)، يستخدم النفق منفذ UDP 500 الذي يجب تعيينه للسماح لحركة مرور ISAKMP بأن يتم إعادة توجيهها إلى جدار الحماية.



الخطوة 3. في القائمة المنسدلة *التكوين التلقائي*، حدد أحد الخيارات. يتم تحديد الخيارات المتاحة على النحو التالي:

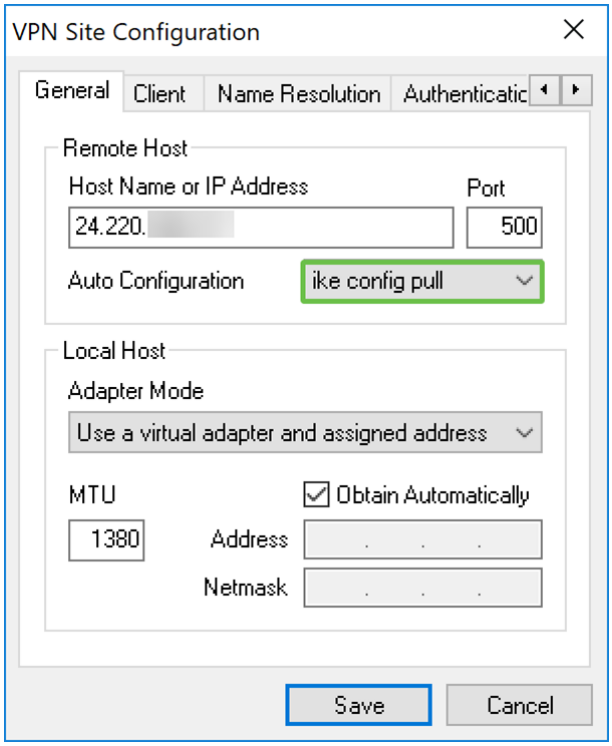
- **معطل** - تعطيل أي تكوين تلقائي للعميل

- **IKE Config Pull** - يسمح بإعداد الطلبات من جهاز كمبيوتر بواسطة العميل. بدعم من أسلوب السحب بواسطة الكمبيوتر، يرجع الطلب قائمة بالإعدادات التي يدعمها العميل.

- **Ike Config Push** - يوفر للكمبيوتر الفرصة لتقديم إعدادات للعميل من خلال عملية التكوين. بدعم من أسلوب الدفع بواسطة الكمبيوتر، يرجع الطلب قائمة بالإعدادات التي يدعمها العميل.

- **DHCP عبر IPsec** - يمنح العميل فرصة طلب الإعدادات من الكمبيوتر من خلال DHCP عبر IPsec.

في هذا المثال، سنختار **ike config pull**.

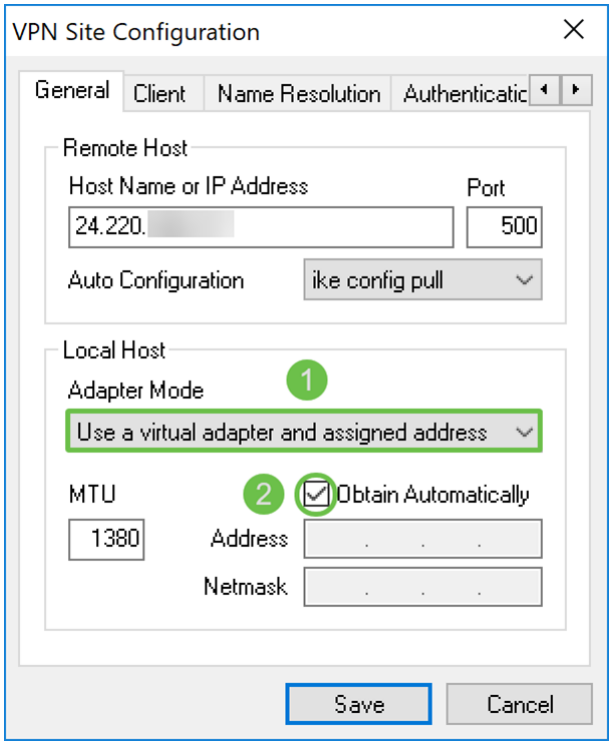


الخطوة 4. في قسم *المضيف المحلي*، أختر **إستخدام مهايئ ظاهري وعنوان معين** في *وضع المحول* القائمة المنسدلة وحدد خانة الاختيار **الحصول تلقائيا**. يتم تحديد الخيارات المتاحة على النحو التالي:

- **إستخدام مهايئ ظاهري وعنوان معين** - يسمح للعميل باستخدام مهايئ ظاهري بعنوان محدد كمصدر لاتصالات IPsec الخاصة به.

- **إستخدام مهايئ ظاهري وعنوان عشوائي** - يسمح للعميل باستخدام مهايئ ظاهري بعنوان عشوائي كمصدر لاتصالات IPsec الخاصة به.

- **إستخدام مهايئ موجود وعنوان حالي** - يسمح للعميل باستخدام المهايئ الفعلي الموجود فقط مع عنوانه الحالي كمصدر لاتصالات IPsec الخاصة به.

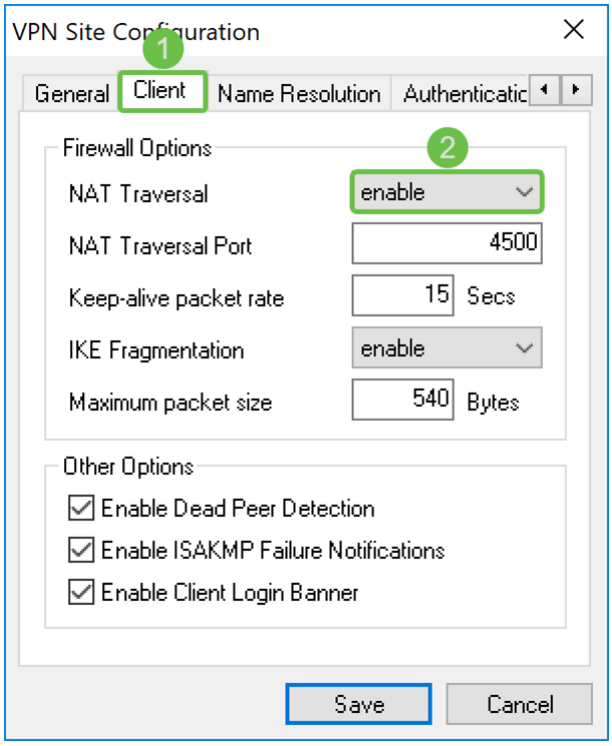


زبون Show Soft VPN: علامة التبويب العميل

الخطوة 1. انقر فوق علامة التبويب *العميل*. في القائمة المنسدلة *NAT Traversal* ، حدد نفس الإعداد الذي قمت بتكوينه على RV160/RV260 لمجاورة NAT. يتم تحديد خيارات قائمة إجتياز عنوان الشبكة (NATT) المتاحة كما يلي:

- **معطل** - لن يتم إستخدام ملحقات بروتوكول NATT.
- **Enabled** – NAT çIIN NAT .
- **Force-Draft** - سيتم إستخدام مسودة نسخة من امتدادات بروتوكول NATT بغض النظر عما إذا كانت عبارة الشبكة الخاصة الظاهرية (VPN) تشير إلى الدعم أثناء المفاوضات أو أنه تم الكشف عن NAT أم لا.
- **Force-RFC** - سيتم إستخدام إصدار RFC من بروتوكول NATT بغض النظر عما إذا كانت عبارة الشبكة الخاصة الظاهرية (VPN) تشير إلى الدعم أثناء المفاوضات أو أنه تم اكتشاف NAT أم لا.
- **force-cisco-udp** - فرض تضمين UDP لعملاء VPN دون NAT.

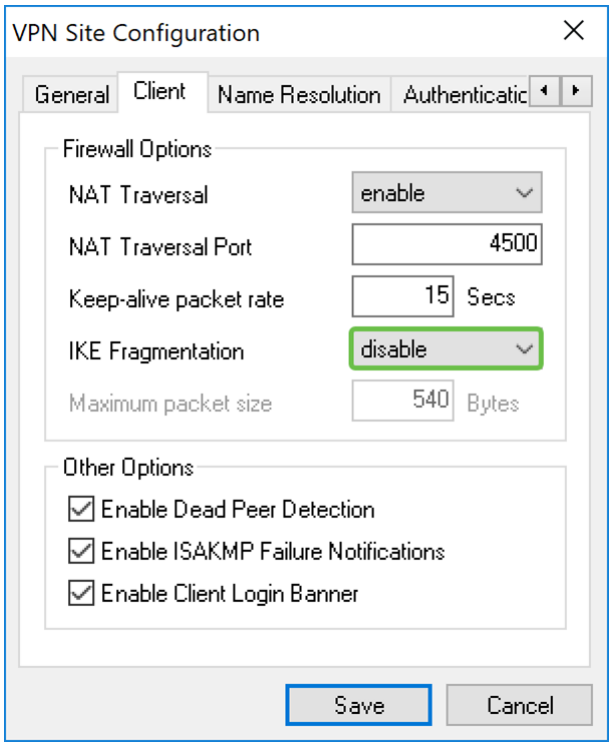
في هذا وثيقة، نحن كنت ينتقي **enable** ل NAT Traversal ويترك *NAT Traversal* *وإبقاء ربط معدل* كقيمة افتراضية.



الخطوة 2. في القائمة المنسدلة *تجزئة IKE*، حدد إما **تعطيل** أو **تمكين** أو **فرض**. يتم تحديد الخيارات على النحو التالي:

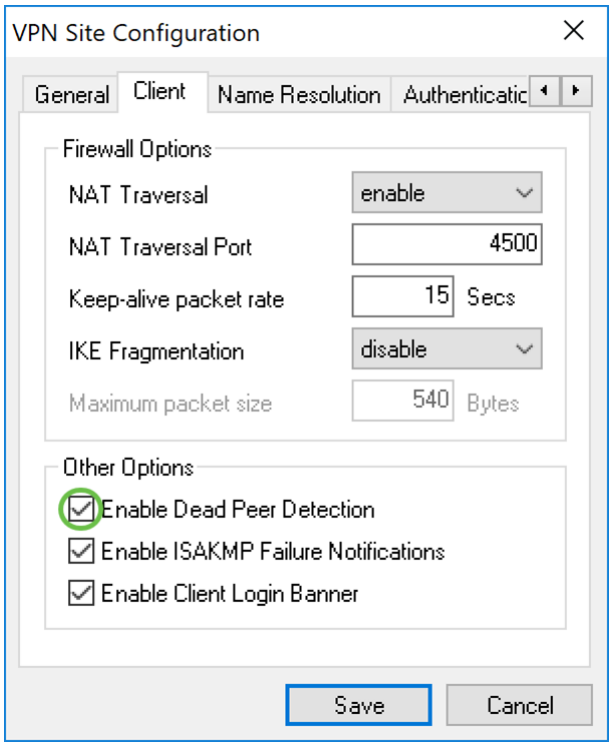
- **disable** - لن يتم إستخدام ملحق بروتوكول تجزئة IKE.
- **enable** – IKE çTIN .
- **Force** – IKE çTIN .

لقد حددنا **تعطيل** لتجزئة *IKE*.



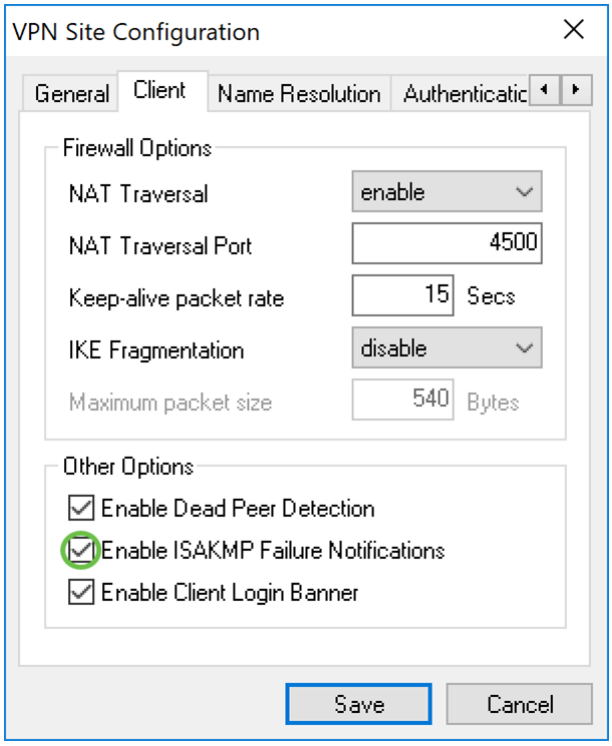
الخطوة 3. حدد خانة الاختيار **تمكين** اكتشاف النظير **الميت** لتمكين بروتوكول اكتشاف النظير الميت. في حالة تمكين هذا الخيار، سيتم إستخدامه فقط إذا كان الموجه يدعمه. وهذا يسمح للعميل والموجه بالتحقق من حالة النفق لاكتشاف الوقت الذي لم يعد فيه أحد الجوانب قادرا على الاستجابة. يكون هذا الخيار متاحا بشكل افتراضي.

في هذا المثال، سنترك "اكتشاف النظير الميت" قيد التحقق.



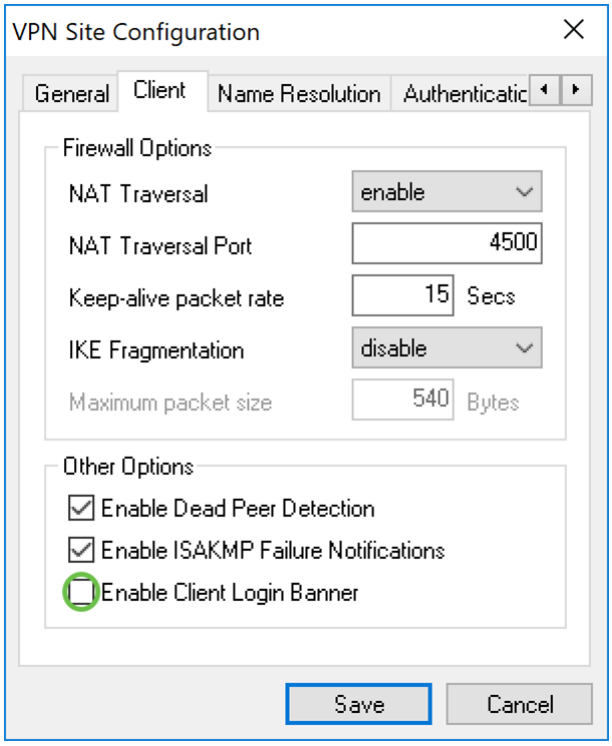
الخطوة 4. حدد خانة الاختيار **تمكين إعلام فشل ISAKMP** لتمكين إعلام فشل ISAKMP من برنامج IPsec الخاص بعميل VPN. مكنت هذا افتراضيا.

في هذا المثال، سنترك "إعلام فشل ISAKMP" محددا.



الخطوة 5. قم بإلغاء تحديد شعار **تمكين تسجيل دخول العميل** لتعطيله. سيؤدي هذا إلى عرض شعار تسجيل دخول بعد إنشاء النفق باستخدام الموجه. يجب أن يدعم الموجه تبادل المعاملات بالإضافة إلى تكوينه لإعادة توجيه شعار تسجيل دخول إلى العميل. مكنت هذا قيمة افتراضيا.

سيتم إلغاء التحقق من شعار تسجيل دخول العميل.

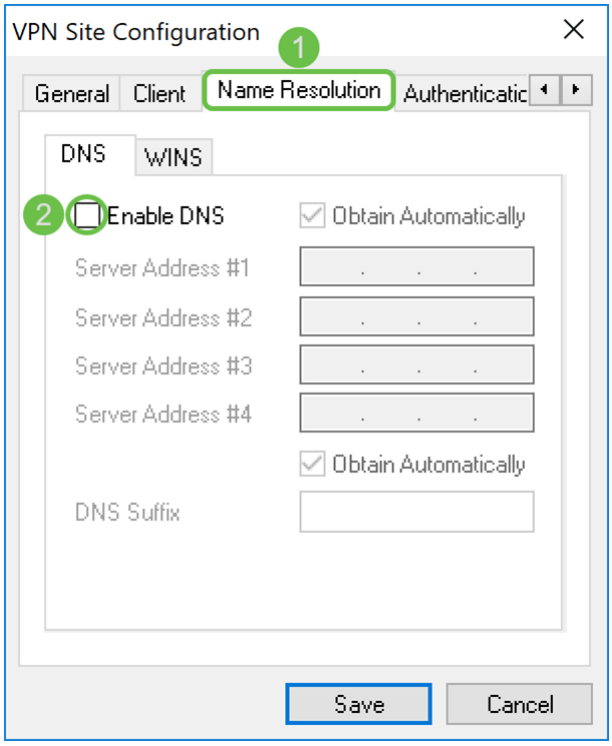


عميل Show Soft VPN: علامة التبويب تحليل الاسم

الخطوة 1. انقر فوق علامة التبويب *تحليل الاسم*، وحدد خانة الاختيار **تمكين DNS** إذا كنت تريد تمكين DNS. إذا لم تكن إعدادات DNS المحددة مطلوبة لتكوين الموقع الخاص بك، قم بإلغاء تحديد خانة الاختيار **تمكين DNS**.

إذا تم التحقق من *تمكين DNS* وتم تكوين البوابة البعيدة لدعم Configuration Exchange، يمكن للبوابة توفير إعدادات DNS تلقائيا. إذا لم تكن هناك مساحة، فتحقق من إلغاء تحديد خانة الاختيار **الحصول تلقائيا** وأدخل عنوان خادم DNS صالح يدويا.

في هذا المثال، لم يتم تحديد **تمكين DNS**.

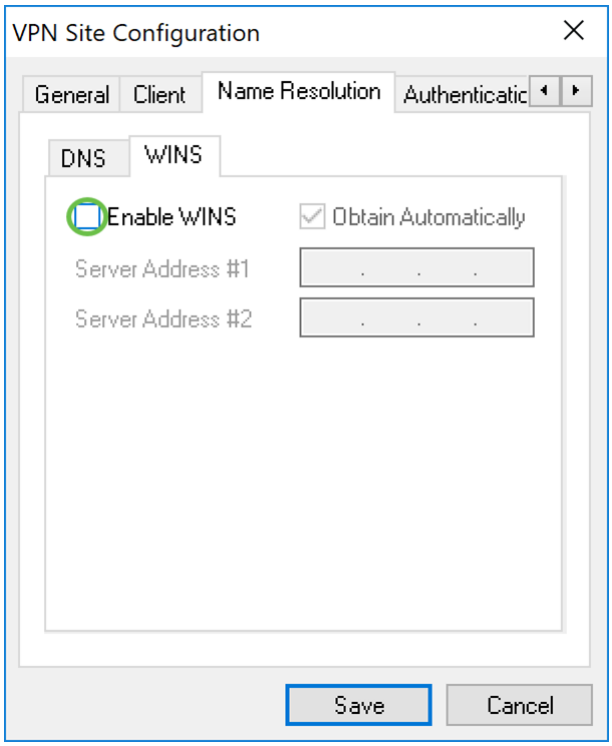


الخطوة 2. حدد خانة الاختيار **تمكين WINS** إذا كنت تريد تمكين خادم اسم إنترنت ل (WINS Windows). إذا تم تكوين البوابة البعيدة لدعم Configuration Exchange، ستتمكن البوابة من توفير إعدادات WINS تلقائيا.

إذا لم تكن هناك مساحة، فتحقق من إلغاء تحديد خانة الاختيار **الحصول تلقائيا** وأدخل يدويا عنوان خادم WINS صالح.

ملاحظة: من خلال توفير معلومات تكوين WINS، سيتمكن العميل من حل أسماء WINS باستخدام خادم موجود في الشبكة الخاصة البعيدة. يكون هذا مفيدا عند محاولة الوصول إلى موارد شبكة Windows البعيدة باستخدام اسم مسار إتفاقية التسمية الموحدة. ينتمي خادم WINS عادة إلى وحدة تحكم مجال Windows أو خادم Samba.

في هذا المثال، لم يتم تحديد **تمكين** WINS.



عميل Show Soft VPN: علامة تبويب المصادقة

الخطوة 1. انقر فوق علامة التبويب *المصادقة* ، وحدد **PSK + XAuth المتبادل** في القائمة المنسدلة *طريقة المصادقة*. يتم تحديد الخيارات المتاحة على النحو التالي:

- **RSA المختلط + XAuth** - لا توجد حاجة إلى بيانات اعتماد العميل. سيقوم العميل بمصادقة البوابة. ستكون بيانات الاعتماد على شكل ملفات شهادة PEM أو PKCS12 أو نوع ملفات مفاتيح.

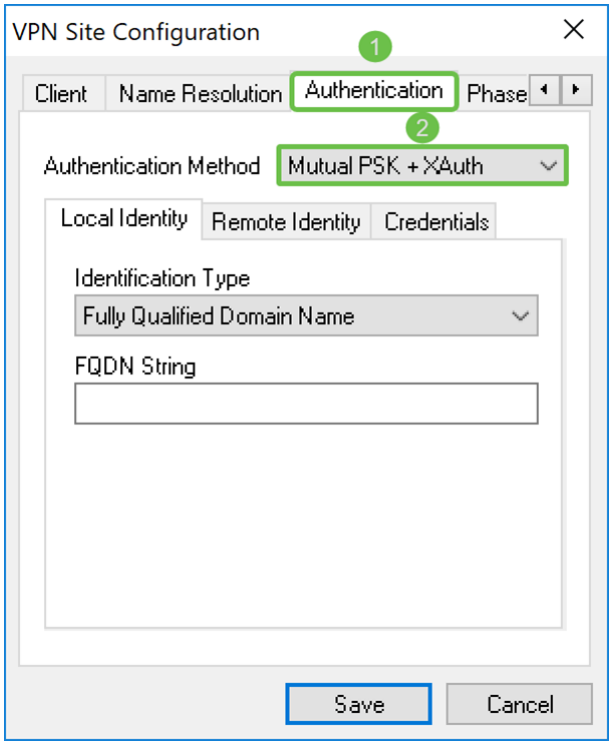
- **GRP المختلط + XAuth** - لا توجد حاجة إلى بيانات اعتماد العميل. سيقوم العميل بمصادقة البوابة. ستكون بيانات الاعتماد على شكل ملف شهادة PEM أو PKCS12 وسلسلة سرية مشتركة.

- **RSA المتبادل + XAuth** - يحتاج كل من العميل والبوابة إلى بيانات اعتماد للمصادقة. ستكون بيانات الاعتماد على شكل ملفات شهادة PEM أو PKCS12 أو نوع مفتاح.

- **PSK المتبادل + XAuth** - يحتاج كل من العميل والبوابة إلى بيانات اعتماد للمصادقة. ستكون بيانات الاعتماد في شكل سلسلة سرية مشتركة.

- **RSA المتبادل** - يحتاج كل من العميل والبوابة إلى بيانات اعتماد للمصادقة. ستكون بيانات الاعتماد على شكل ملفات شهادة PEM أو PKCS12 أو نوع مفتاح.

- **PSK المتبادل** - يحتاج كل من العميل والمعبر إلى بيانات اعتماد للمصادقة. ستكون بيانات الاعتماد في شكل سلسلة سرية مشتركة.



الخطوة 2. في علامة التبويب *الهوية المحلية*، حدد نوع التعريف ثم أدخل السلسلة المناسبة في الحقل الفارغ. يتم تعريف الخيارات التالية على أنها:

- **Any** - لا يتم قبول هذا إلا في علامة التبويب "الهوية عن بعد". سيقبل العميل أي نوع معرف وقيمة. يجب إستخدام هذا الأمر بحذر لأنه يتجاوز جزءا من عملية تعريف المرحلة الأولى من IKE.

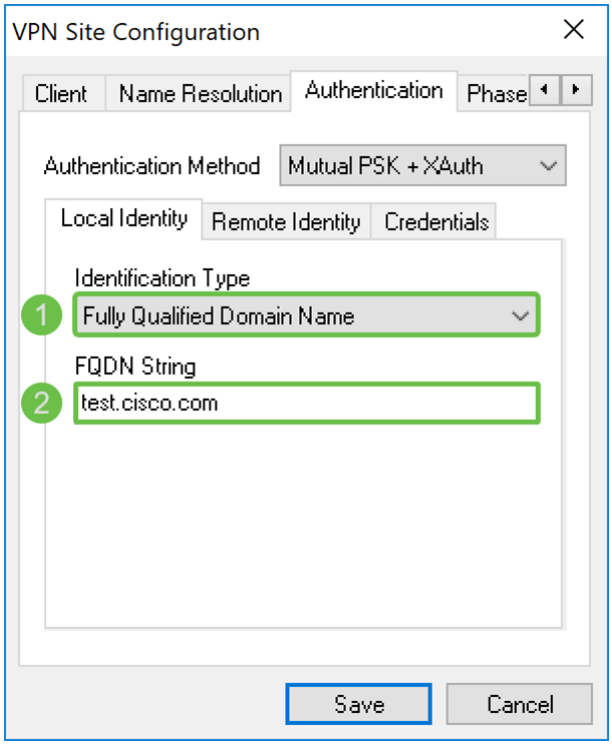
- **اسم المجال المؤهل بالكامل** - يجب أن يوفر هذا الخيار سلسلة FQDN في شكل سلسلة مجال DNS. على سبيل المثال، ستكون "cisco.com" قيمة مقبولة. يسمح العميل بتحديد هذا الخيار فقط في حالة إستخدام وضع مصادقة PSK.

- **اسم المجال المؤهل بالكامل للمستخدم** - يجب توفير سلسلة FQDN للمستخدم في شكل سلسلة user@domain. على سبيل المثال، سوف تكون "dave@cisco.com" قيمة مقبولة. لا يسمح العميل بتحديد هذا الخيار إلا إذا كان وضع مصادقة PSK قيد الاستخدام.

- **عنوان IP** - عند تحديد عنوان IP، يتم تحديد خانة الاختيار *إستخدام عنوان مضيف محلي مكتشف* تلقائيا بشكل افتراضي. وهذا يعني أن القيمة سيتم تحديدها تلقائيا. قم بإلغاء تحديد خانة الاختيار إذا كنت ترغب في إستخدام عنوان آخر غير عنوان المحول المستخدم للاتصال ببوابة العميل. بعد ذلك، أدخل سلسلة عنوان محددة. لن يسمح العميل بتحديد هذا الخيار إلا إذا كان وضع مصادقة PSK قيد الاستخدام.

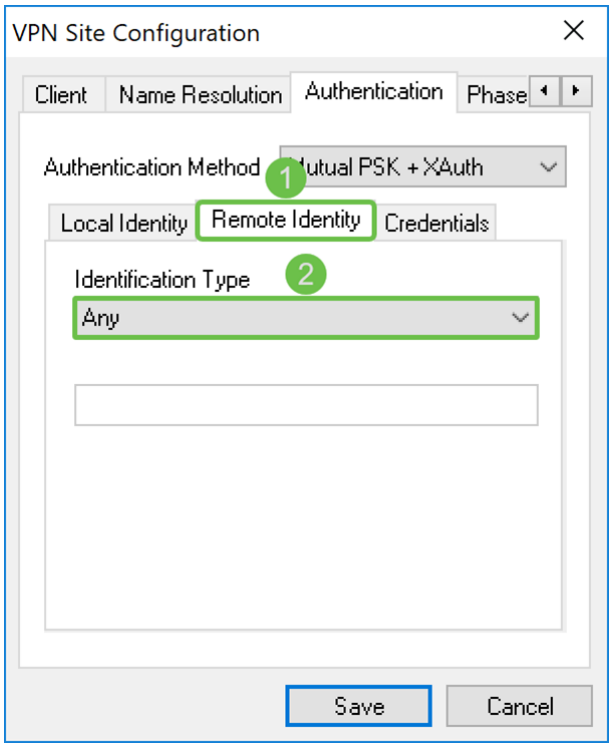
- **معرف المفتاح** - عند تحديد هذا الخيار، يجب توفير سلسلة معرف.

في هذا المثال، سنقوم بتحديد **اسم المجال المؤهل بالكامل** وإدخال **test.cisco.com** في حقل *سلسلة FQDN*.



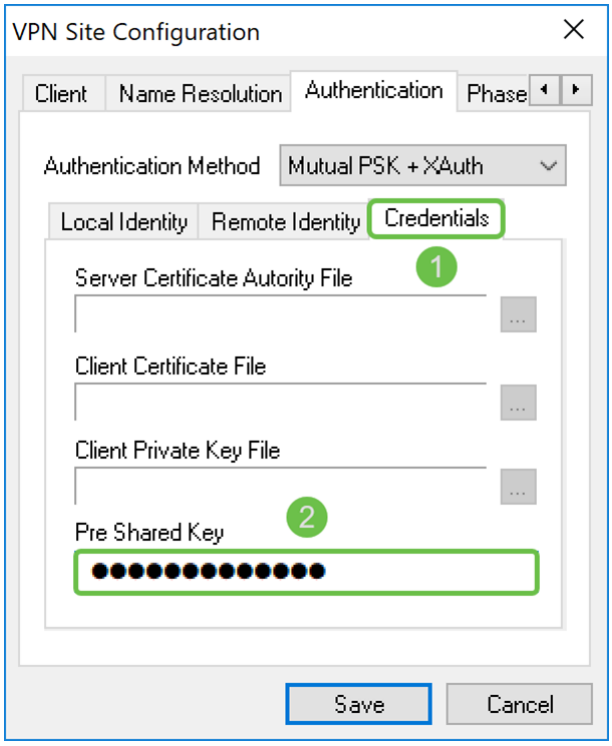
الخطوة 3. انقر فوق علامة التبويب *هوية عن بعد* وحدد نوع التعريف. وتتضمن الخيارات ما يلي: أي اسم مجال مؤهل بالكامل أو اسم مجال مؤهل بالكامل من قبل المستخدم أو عنوان IP أو معرف مفتاح.

في هذا المستند، سنستخدم **Any** كنوع التعريف الخاص بنا.



الخطوة 4. انقر فوق علامة التبويب *بيانات الاعتماد* وأدخل نفس المفتاح المشترك مسبقا الذي قمت بتكوينه على RV160/RV260.

سنقوم بإدخال **CiscoTest123!** في حقل *المفتاح المشترك مسبقا*.

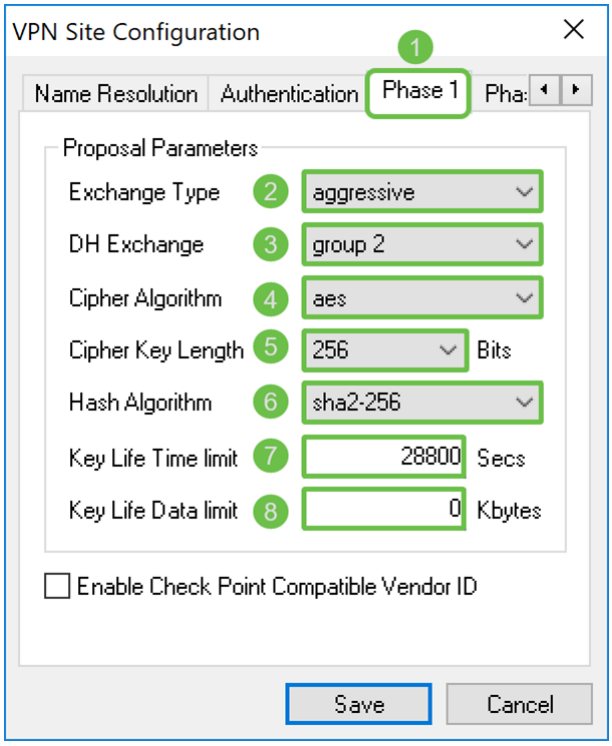


عميل Shrew Soft VPN: المرحلة 1 tab

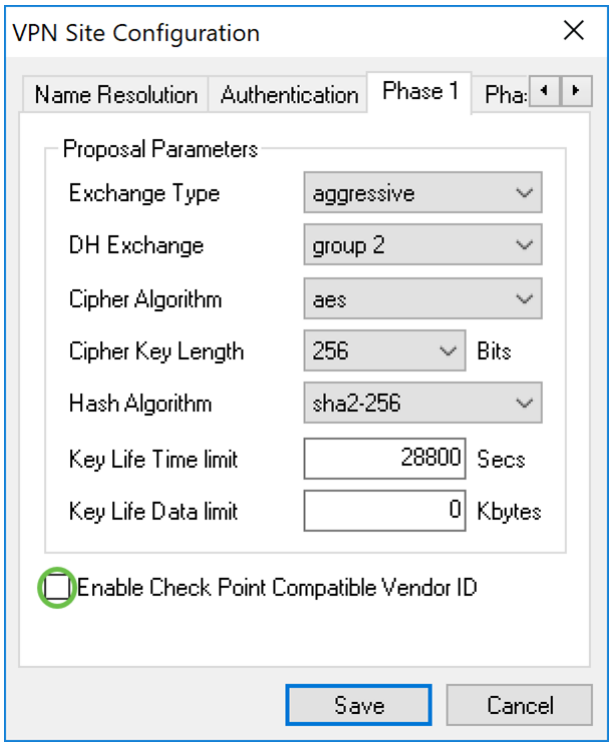
الخطوة 1. انقر فوق علامة التبويب *المرحلة 1*. قم بتكوين المعلمات التالية بحيث تكون لها نفس الإعدادات التي قمت بتكوينها ل RV160/RV260.

يجب أن تتطابق المعلمات الموجودة في Show Soft مع تكوين RV160/RV260 الذي حددته في المرحلة 1.
في هذا المستند، سيتم تعيين المعلمات في Shrew Soft على أنها:

- نوع Exchange: **عدوانية**
- تبادل DH: **المجموعة 2**
- خوارزمية التشفير: **AES**
- طول مفتاح التشفير: **256**
- خوارزمية التجزئة: **SHA2-256**
- الحد الزمني الأساسي للعمر: **28800**
- الحد الأقصى لبيانات العمر الافتراضي الأساسية: **0**



الخطوة 2. (إختياري) إذا قدمت بوابتك معرف مورد متوافق مع Cisco أثناء مفاوضات المرحلة 1، فتحقق من خانة الاختيار **تمكين معرف المورد المتوافق مع نقطة**. إذا لم توفر البوابة معرف مورد متوافق مع Cisco أو إذا كنت غير متأكد، فاترك خانة الاختيار بدون تحديد. سنترك خانة الاختيار بدون تحديد.



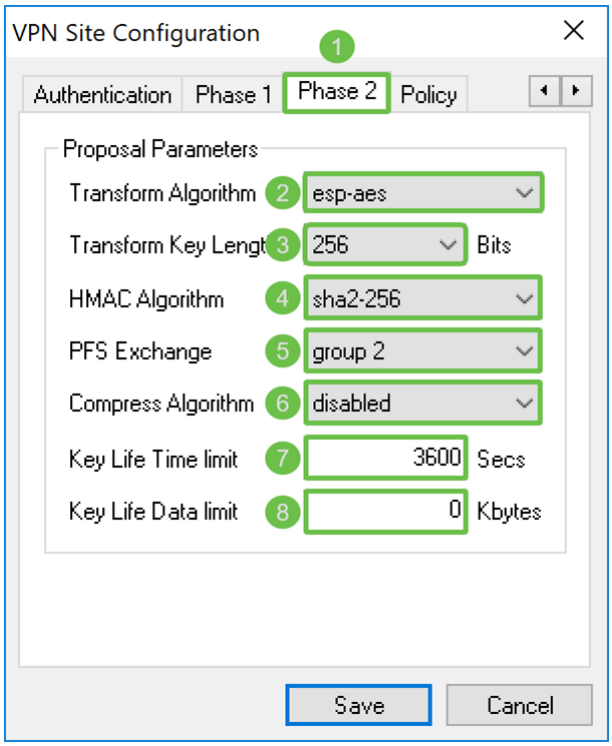
عميل Shrew Soft VPN: المرحلة 2 tab

الخطوة 1. انقر فوق علامة التبويب *المرحلة 2*. قم بتكوين المعلمات التالية بحيث تكون لها نفس الإعدادات التي قمت بتكوينها ل RV160/RV260.

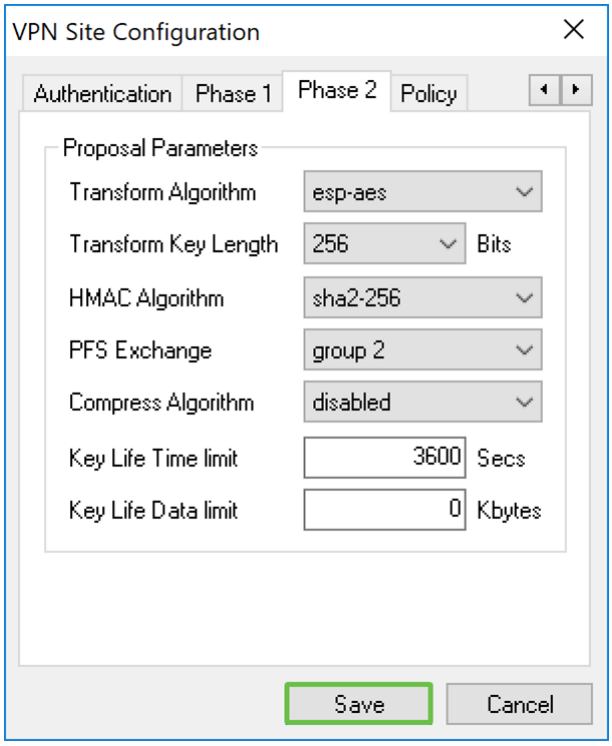
يجب أن تتطابق المعلمات مع تكوين RV160/260 في المرحلة 2 كما يلي:

- خوارزمية التحويل: **ESP-AES**
- طول مفتاح التحويل: **256**

- خوارزمية HMAC: **SHA2-256**
- PFS Exchange: **المجموعة 2**
- ضغط الخوارزمية: **معطل**
- الحد الزمني الأساسي للعمر: **3600**
- الحد الأقصى لبيانات العمر الافتراضي الأساسية: **0**



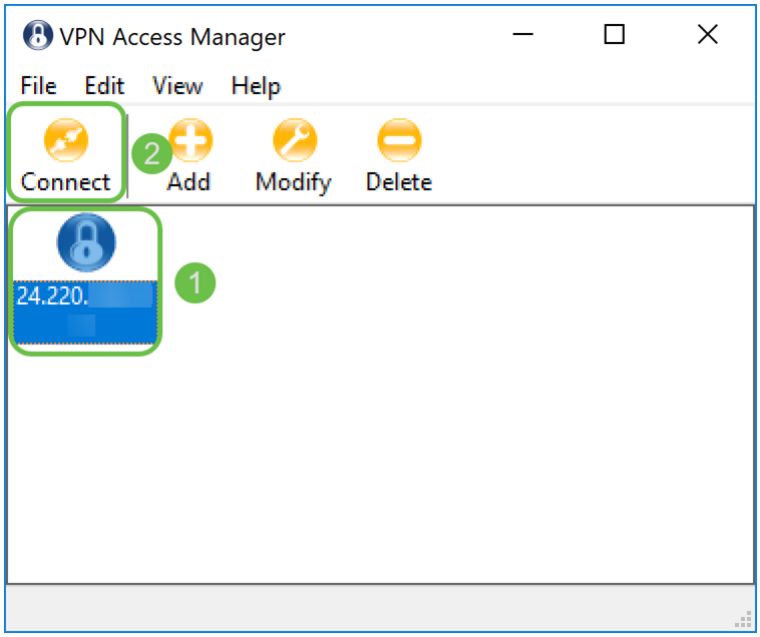
الخطوة 2. اضغط على زر **حفظ** في أسفل الصفحة لحفظ التكوين الخاص بك.



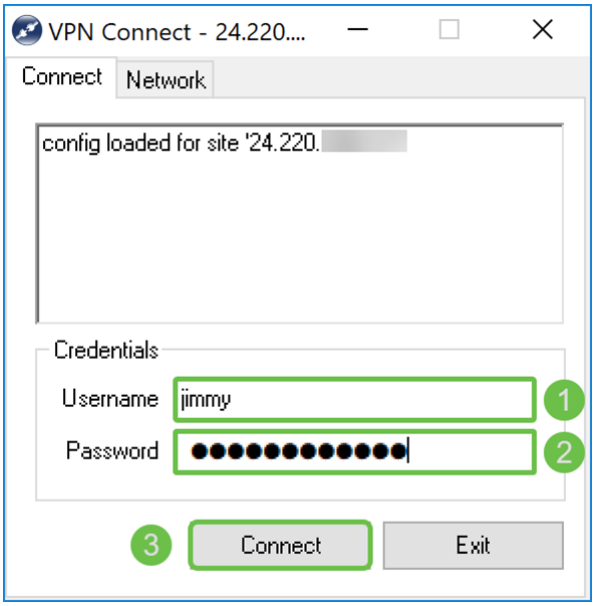
عميل Show Soft VPN: الاتصال

الخطوة 1. في *مدير الوصول إلى شبكة VPN*، حدد ملف تعريف شبكة VPN الذي أنشأته للتو. ثم اضغط على المفتاح **Connect**.

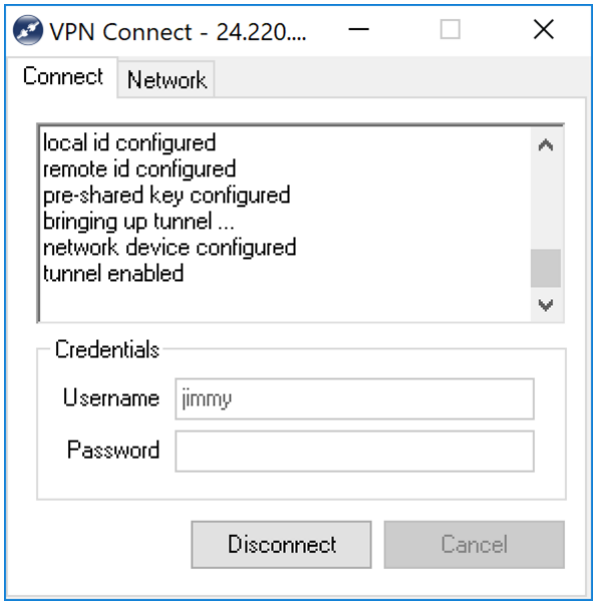
ملاحظة: إذا كنت تريد إعادة تسمية ملف تعريف VPN، انقر بزر الماوس الأيمن عليه وحدد **إعادة تسمية**. يموه جزء من عنوان IP في التوصيف لحماية تلك الشبكة.



الخطوة 2. تظهر نافذة *اتصال VPN*. أدخل اسم المستخدم وكلمة المرور اللذين أنشأا في قسم *إنشاء حساب المستخدم*. ثم اضغط على المفتاح **Connect**.

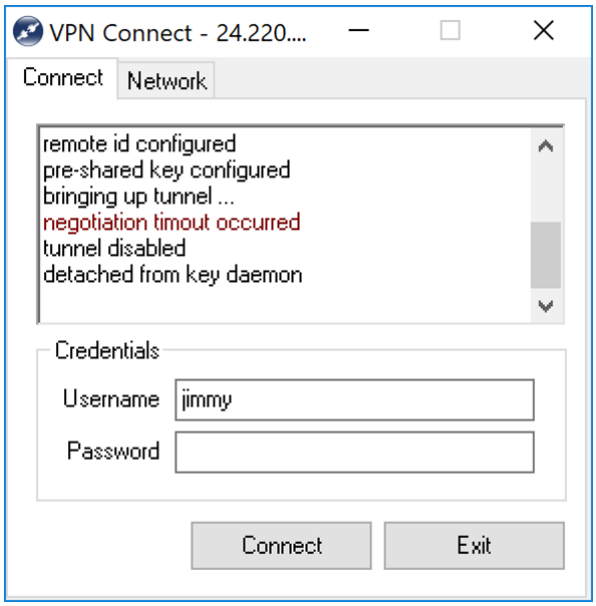


الخطوة 3. بعد الضغط على *Connect*، يتم تمرير معلومات التكوين إلى برنامج IKE Daemon مع طلب للاتصال. يتم عرض رسائل مختلفة لحالة الاتصال في نافذة الإخراج. إذا نجح الاتصال، ستحصل على رسالة تقول "تم تكوين جهاز الشبكة" و"تمكين النفق". يتغير زر *الاتصال* إلى زر *فصل*.

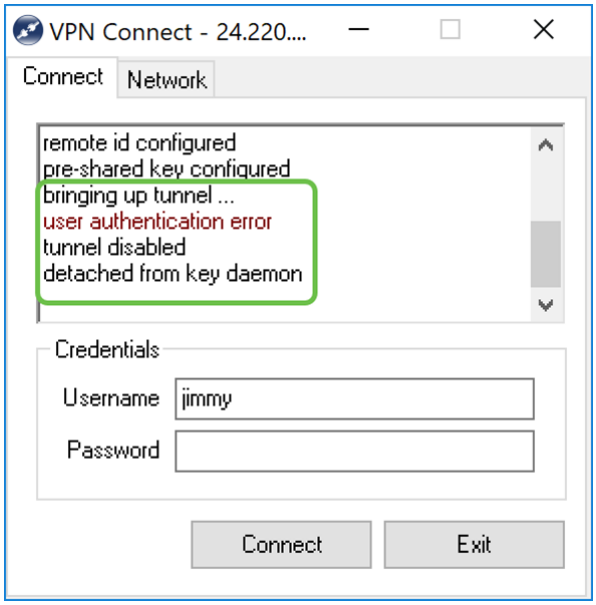


تلميحات أستكشاف أخطاء اتصال VPN وإصلاحها

إذا ظهرت لديك رسائل خطأ تقول: "تم تعطيل التفاوض"، و"تم تعطيل النفق"، و"تم فصله عن برنامج خفي أساسي". قد تحتاج إلى التحقق مرة أخرى من التكوين الخاص بك على الموجه الخاص بك واستدعاء عميل VPN السهل للتأكد من مطابقته.

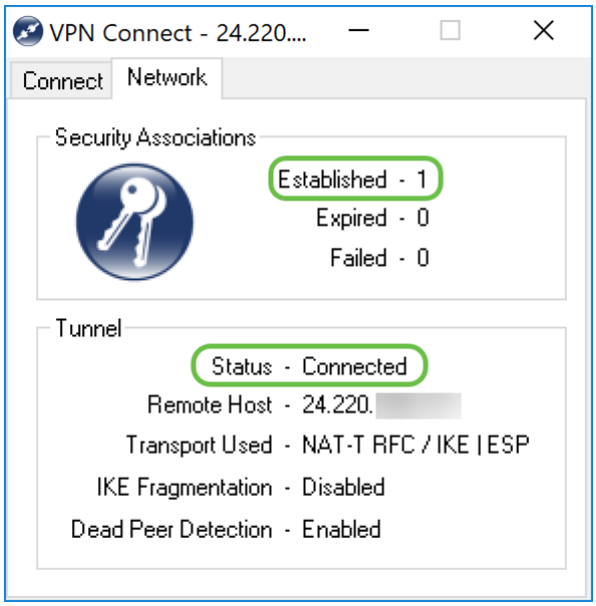


إذا ظهرت رسالة خطأ تقول، "خطأ في مصادقة المستخدم" فهذا يعني أنك قمت بإدخال كلمة المرور الخطأ لاسم المستخدم هذا. تحقق مرة أخرى من بيانات اعتماد المستخدم وتأكد من تكوينها وإدخالها بشكل صحيح.

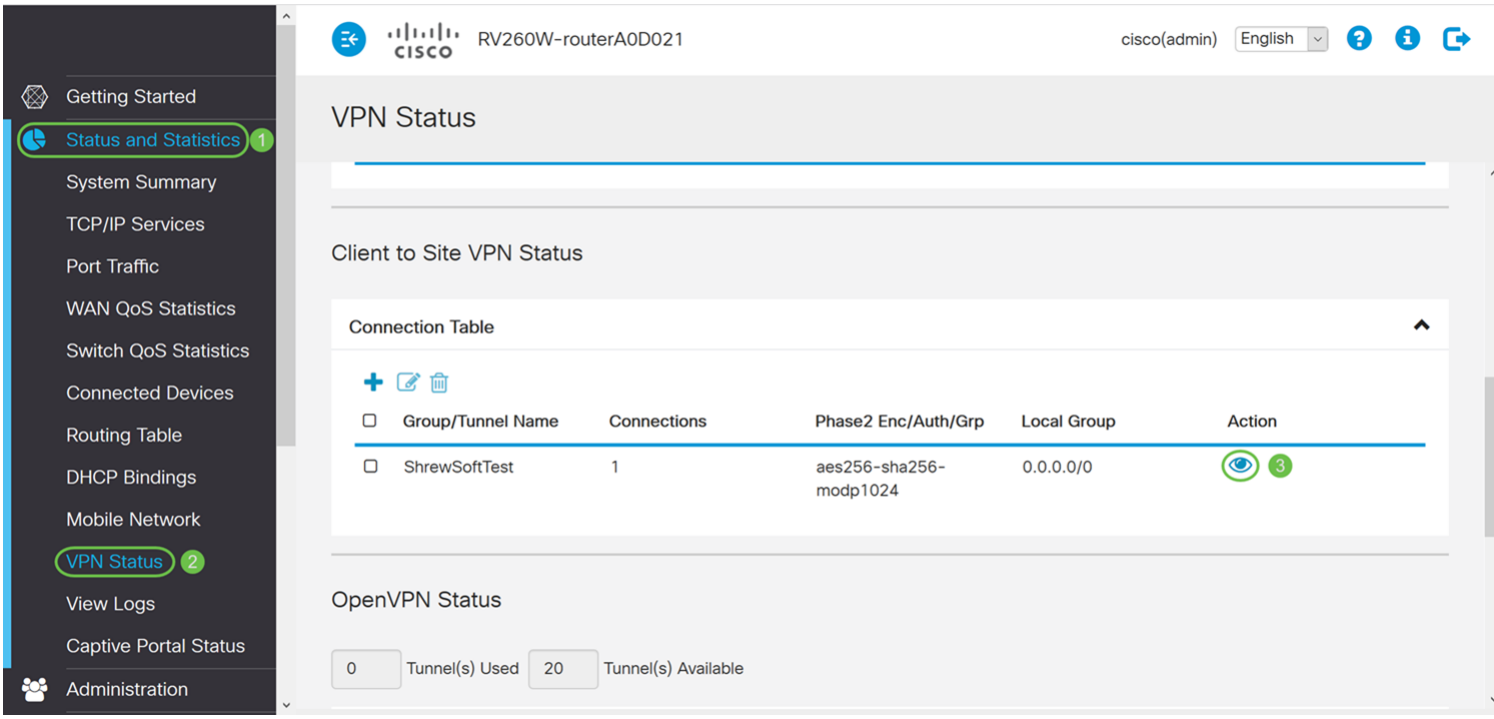


التحقق

الخطوة 1. انقر فوق علامة التبويب *الشبكة* في نافذة *اتصال VPN*. في علامة التبويب هذه، يجب أن تكون قادرا على عرض إحصائيات الشبكة الحالية للاتصال. تحت *النفق* قسم، أنت سوفت رأيت *يربط* كالحالة.

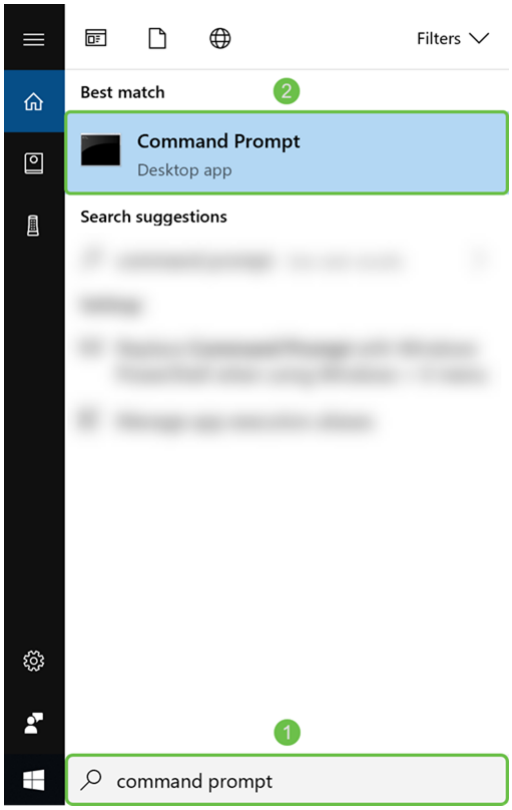


الخطوة 2. على الموجه الخاص بك، انتقل إلى **الحالة والإحصاءات > حالة الشبكة الخاصة الظاهرية (VPN)**. في صفحة *حالة VPN*، قم بالتمرير إلى *قسم* حالة *VPN الخاص بالموقع إلى العميل*. في هذا القسم، يمكنك عرض جميع إتصالات "العميل إلى الموقع". انقر أيقونة **العين** لعرض المزيد من التفاصيل.



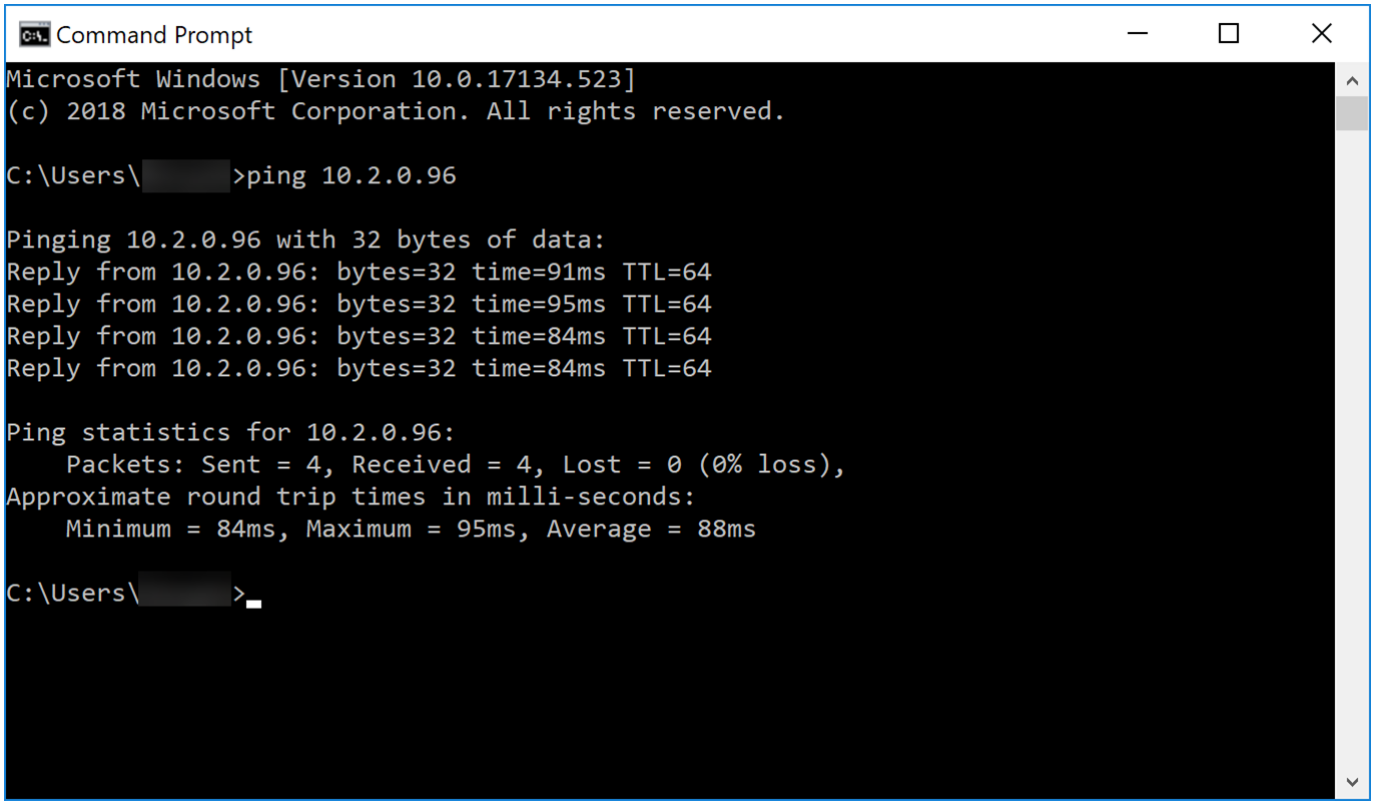
الخطوة 3. انتقل إلى شريط البحث في شريط المهام وابحث عن **موجه الأوامر**.

ملاحظة: يتم إستخدام الإرشادات التالية أدناه على نظام التشغيل Windows 10. وقد يختلف هذا النوع باختلاف نظام التشغيل الذي تستخدمه.



الخطوة 4. اكتب في الأمر بدون علامات الاقتباس، **ping [*عنوان IP الخاص للموجه*]**" ولكن أدخل عنوان IP الخاص بدلا من الكلمات. يجب أن تكون قادرا على إختبار اتصال عنوان IP الخاص بالموجه بنجاح.

في هذا المثال، سنقوم بالكتابة في 10.2.0.96. **ping 10.2.0.96** هو عنوان IP الخاص للموجه الخاص بنا.



القرار

يجب أن تكون قد تمكنت الآن من توصيل Shrew Soft VPN Client الخاص بك بنجاح باستخدام RV160 أو RV260.

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).