تكوين الإعدادات المتقدمة لشبكة VPN من موقع إلى موقع وتجاوز الفشل على RV160 و RV260

الهدف

الهدف من هذا المستند هو توضيح كيفية تكوين الإعدادات المتقدمة لشبكة VPN من موقع إلى موقع وتجاوز الأعطال على RV160 و RV260.

المقدمة

تعد الشبكة الخاصة الظاهرية (VPN) طريقة رائعة لربط العاملين عن بعد بشبكة آمنة. تسمح الشبكة الخاصة الظاهرية (VPN) للمضيف البعيد بالعمل كما لو كان متصلا بالشبكة الآمنة في الموقع. في شبكة VPN من موقع إلى موقع، يتصل الموجه المحلي في موقع واحد بموجه بعيد من خلال نفق شبكة VPN. يقوم هذا النفق بتضمين البيانات بشكل آمن باستخدام تقنيات التشفير والمصادقة المتوافقة مع معايير الصناعة لتأمين البيانات المرسلة. يجب إجراء تكوين مطابق على كلا جانبي الاتصال لإنشاء اتصال شبكة VPN ناجح من موقع إلى موقع. توفر تهيئة الشبكة الخاصة الظاهرية (VPN) المتقدمة من موقع إلى موقع مرونة تكوين التكوينات الاختيارية لنفق الشبكة الخاصة الظاهرية (VPN).

يعد تجاوز الفشل ميزة قوية تضمن وجود اتصال دائم بين هذين الموقعين. ويكون ذلك مفيدا عندما يكون تجاوز الأخطاء مهما. يحدث تجاوز الفشل عندما يكون الموجه الأساسي معطلا. عند هذه النقطة، سيقوم الموجه الثانوي أو الموجه الاحتياطي بتولي الأمر وتوفير اتصال. وهذا من شأنه أن يساعد في منع نقطة واحدة من الفشل.

الأجهزة القابلة للتطبيق

- RV160
- RV260

إصدار البرامج

- 1.0.00.13

المتطلبات الأساسية

قبل تكوين الإعدادات المتقدمة وتجاوز الفشل لشبكة VPN من موقع إلى موقع على RV160 و RV260، ستحتاج إلى تكوين ملف تعريف IPsec وشبكة VPN من موقع إلى موقع على الموجه المحلي والبعيد. فيما يلي قائمة بالمقالات التي يمكن أن تساعدك على تكوينها. لديك الخيار لاستخدام معالج إعداد VPN الذي سيساعدك في تكوين كل من ملف تعريف IPsec وكذلك شبكة VPN من موقع إلى موقع أو يمكنك تكوينها بشكل منفصل ومتابعتها على طول المستندين الواردين أدناه.

1. تكوين معالج إعداد VPN على RV160 و RV260

أو

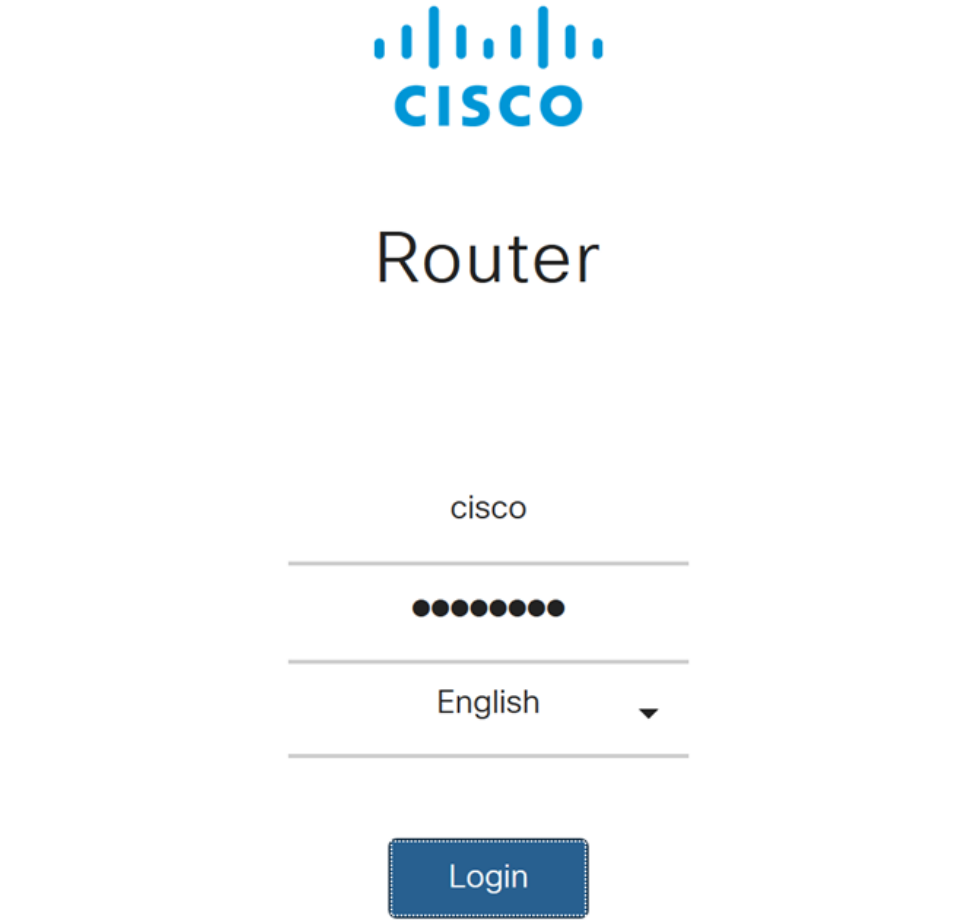
1. تكوين توصيفات IPSec (وضع الكيلات التلقائية) على RV160 و RV260 (إختياري)

2. تكوين شبكة VPN من موقع إلى موقع على RV160 و RV260

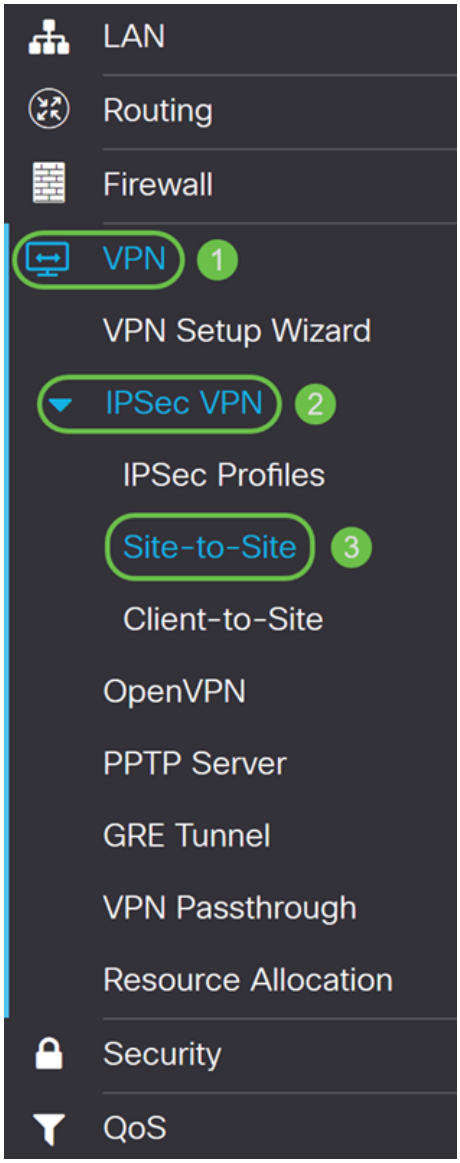
تكوين الإعدادات المتقدمة لشبكة VPN من موقع إلى موقع

يجب تكوين الإعدادات المتقدمة بنفس الطريقة على كلا جانبي اتصال VPN.

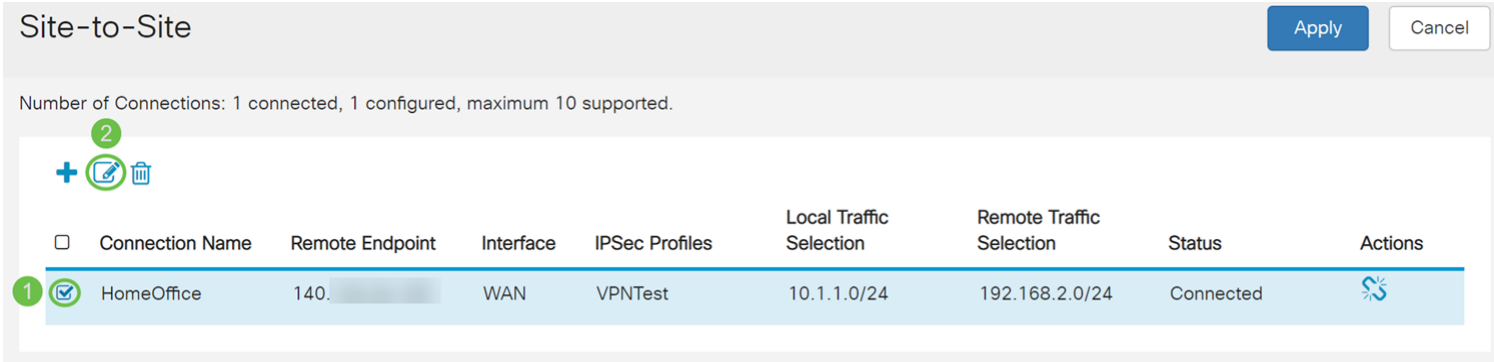
الخطوة 1. قم بتسجيل الدخول إلى الأداة المساعدة لتكوين الويب.



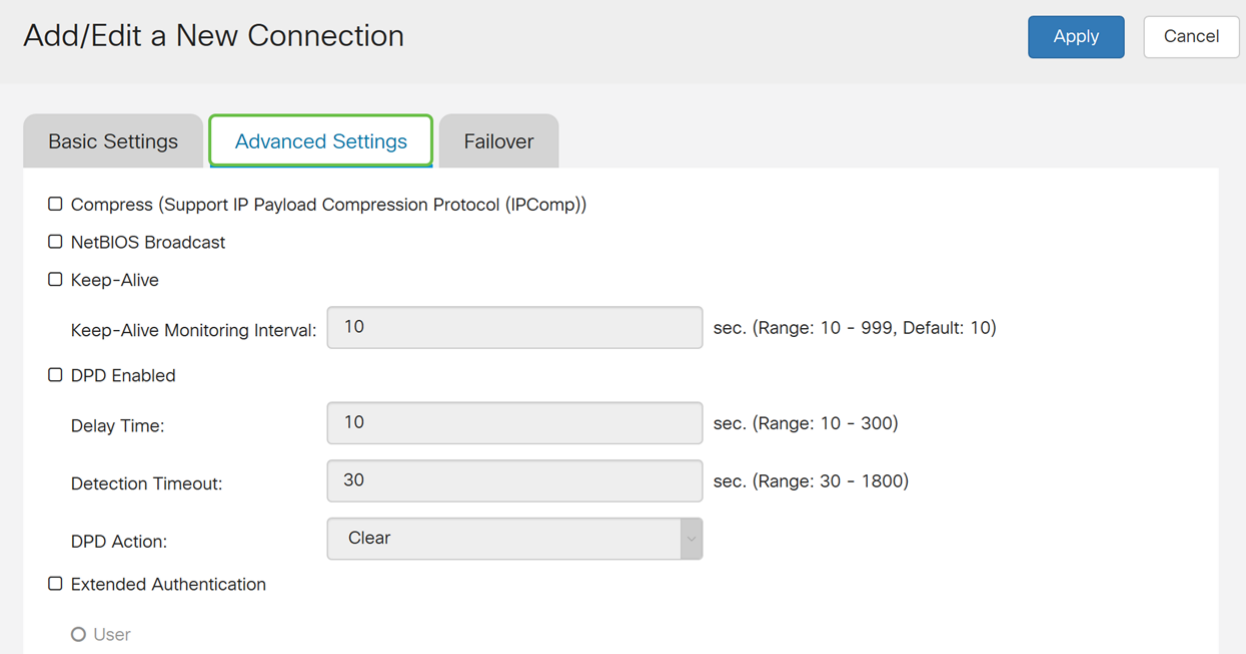
الخطوة 2. انتقل إلى **VPN > IPSec VPN > من موقع إلى موقع**.



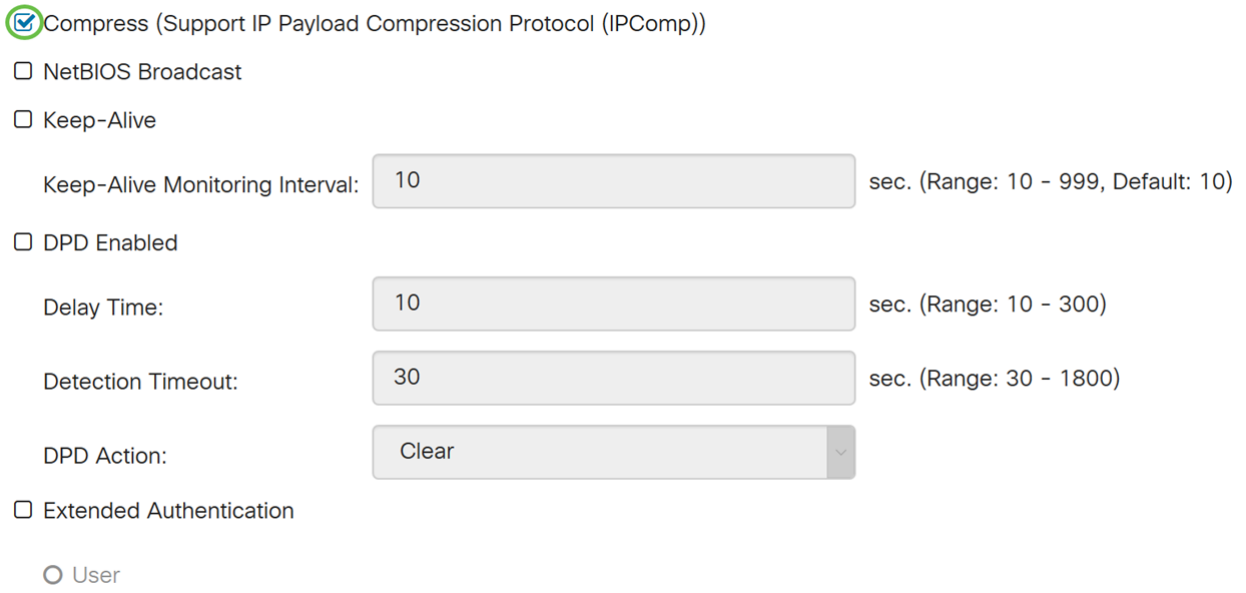
الخطوة 3. حدد خانة الاختيار الخاصة بالاتصال الذي تريد تحريره. ثم اضغط على أيقونة **القلم والورق** لتحرير الاتصال. في هذا المثال، يتم تحديد الاتصال المسمى HomeOffice.



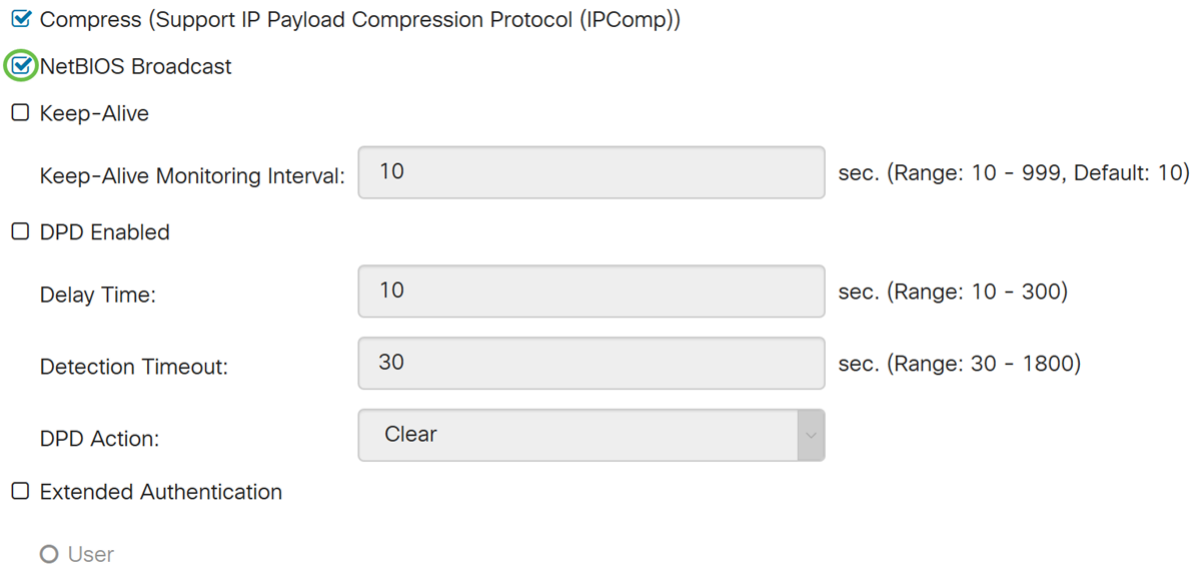
الخطوة 4. انقر على علامة التبويب **إعدادات متقدمة**.



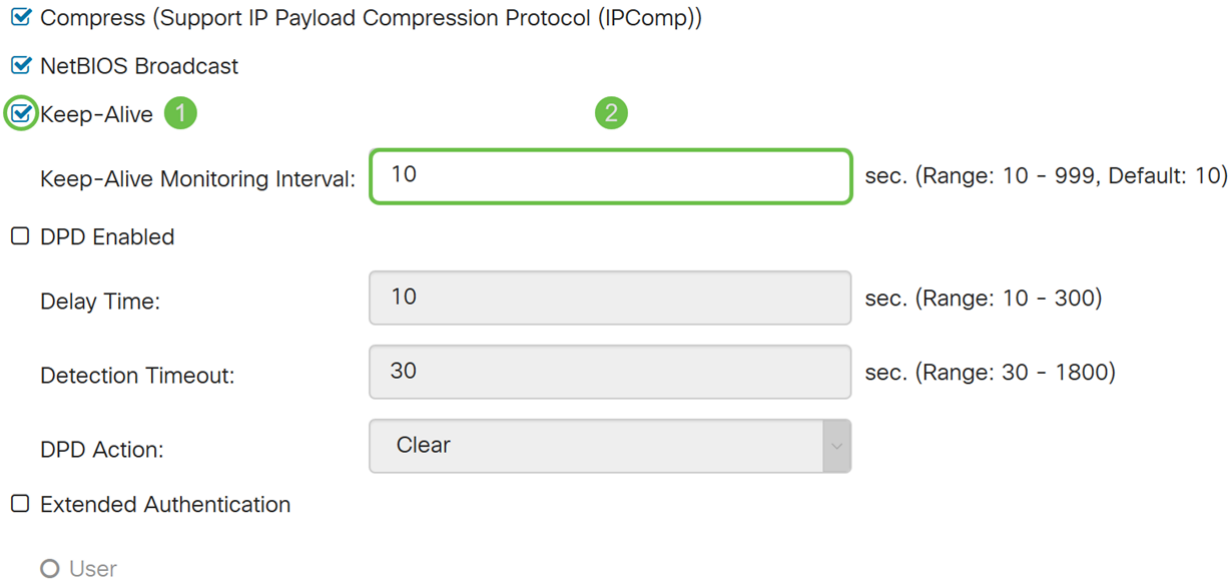
الخطوة 5. حدد خانة الاختيار **ضغط (دعم بروتوكول ضغط حمولة IP (IPComp** لتمكين الموجه من اقتراح الضغط عند بدء إتصاله. يقلل هذا البروتوكول من حجم مخططات بيانات IP. إذا رفض المستجيب هذا الاقتراح، فلن يقوم الموجه بتنفيذ الضغط. عندما يكون الموجه هو المستجيب، فإنه يقبل الضغط، حتى إذا لم يتم تمكين الضغط. إذا قمت بتمكين هذه الميزة لهذا الموجه، فستحتاج إلى تمكينها على الموجه البعيد (الطرف الآخر من النفق).



الخطوة 6. تستخدم رسائل البث لدقة الأسماء في شبكات Windows لتعريف الموارد مثل أجهزة الكمبيوتر والطابعات وخوادم الملفات. يتم إستخدام هذه الرسائل من قبل بعض تطبيقات البرامج وميزات Windows مثل حي الشبكة. لا تتم إعادة توجيه حركة مرور بث LAN عادة عبر نفق VPN. ومع ذلك، يمكنك تحديد هذا المربع للسماح بإعادة بث بث NetBIOS من أحد طرفي النفق إلى الطرف الآخر. حدد خانة الاختيار **بث NetBIOS** للتمكين.

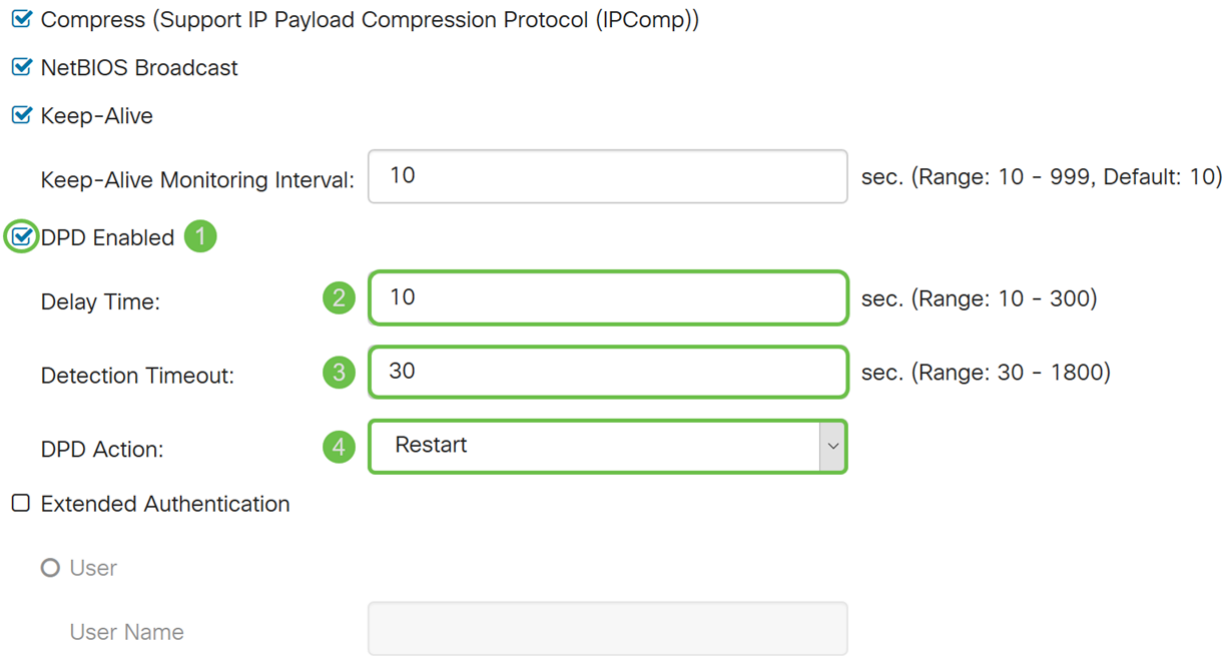


الخطوة 7. حدد خانة الاختيار **الاحتفاظ** بقيد الحياة لتمكين الموجه من محاولة إعادة إنشاء اتصال VPN في فواصل زمنية منتظمة. أدخل عدد الثواني لتعيين الفاصل الزمني للمراقبة قيد الحياة في حقل *الفاصل الزمني للمراقبة قيد الحياة*. المدى 10-999 from ثاني.



الخطوة 8. تحقق من **تمكين ميزة "اكتشاف النظير الميت (DPD)"** لتمكين DPD. وهو يرسل رسائل HELLO/ACK دورية للتحقق من حالة نفق VPN. يجب تمكين خيار DPD على كلا طرفي نفق VPN. حدد الفاصل الزمني بين رسائل HELLO/ACK في حقل الفاصل الزمني بإدخال ما يلي:

- وقت التأخير - أدخل وقت التأخير بالثواني بين كل رسالة Hello. المدى 10 - 300 from ثاني والقيمة الافتراضية هي 10.
- مهلة الكشف - أدخل المهلة بالثواني للإعلان عن وفاة النظير. المدى 30 - 1800 from ثاني.
- إجراء DPD - الإجراء الذي يجب إتخاذه بعد مهلة DPD. حدد **مسح** أو **إعادة التشغيل** من القائمة المنسدلة.

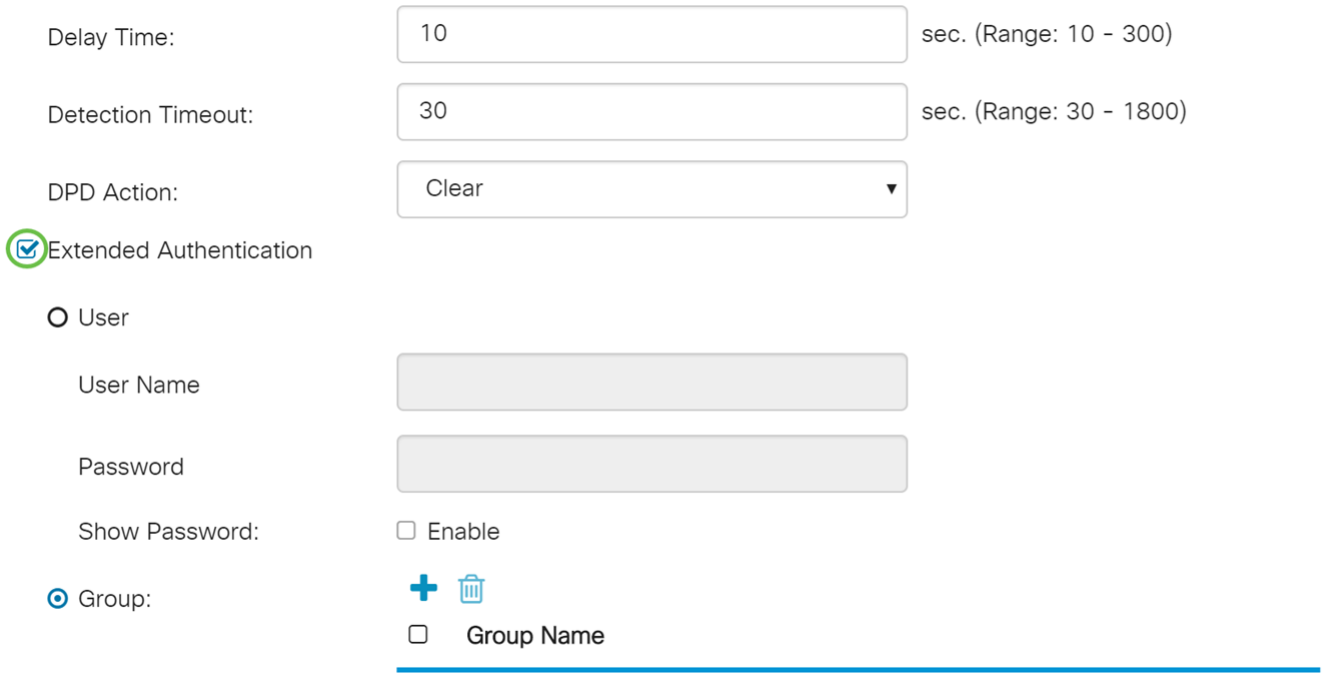


الخطوة 9. تحقق من **المصادقة الموسعة** إذا أردت تمكين المصادقة الموسعة. وسيوفر ذلك مستوى إضافيا من المصادقة يتطلب من المستخدمين عن بعد المفتاح في بيانات الاعتماد الخاصة بهم قبل منحهم حق الوصول إلى شبكة VPN. للحصول على مصادقة موسعة للعمل، يجب أن يستخدم الموقع الرئيسي مصادقة المجموعة ويجب أن يستخدم الموقع البعيد مصادقة المستخدم. في الخطوات القليلة التالية، سنقوم بتكوين الموقع الرئيسي لاستخدام مصادقة المجموعة.

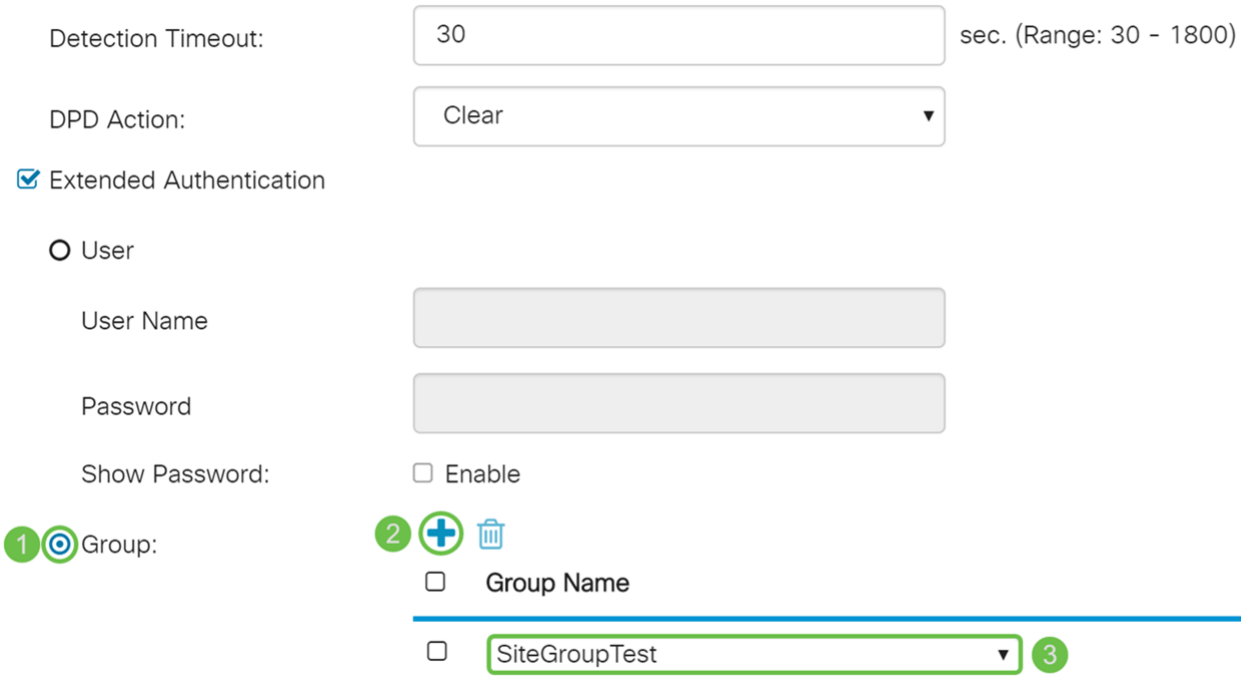
ملاحظة: يوصى بتكوين اتصال من عميل إلى موقع لمصادقة المستخدم بدلا من المصادقة الموسعة.

إذا لم تكن قد قمت بإنشاء مجموعة مستخدمين لموقعك الرئيسي، فانقر فوق الارتباط لمعرفة كيفية إنشاء مجموعة مستخدمين موجودة في هذه المقالة: إنشاء مجموعة مستخدمين للمصادقة الموسعة.

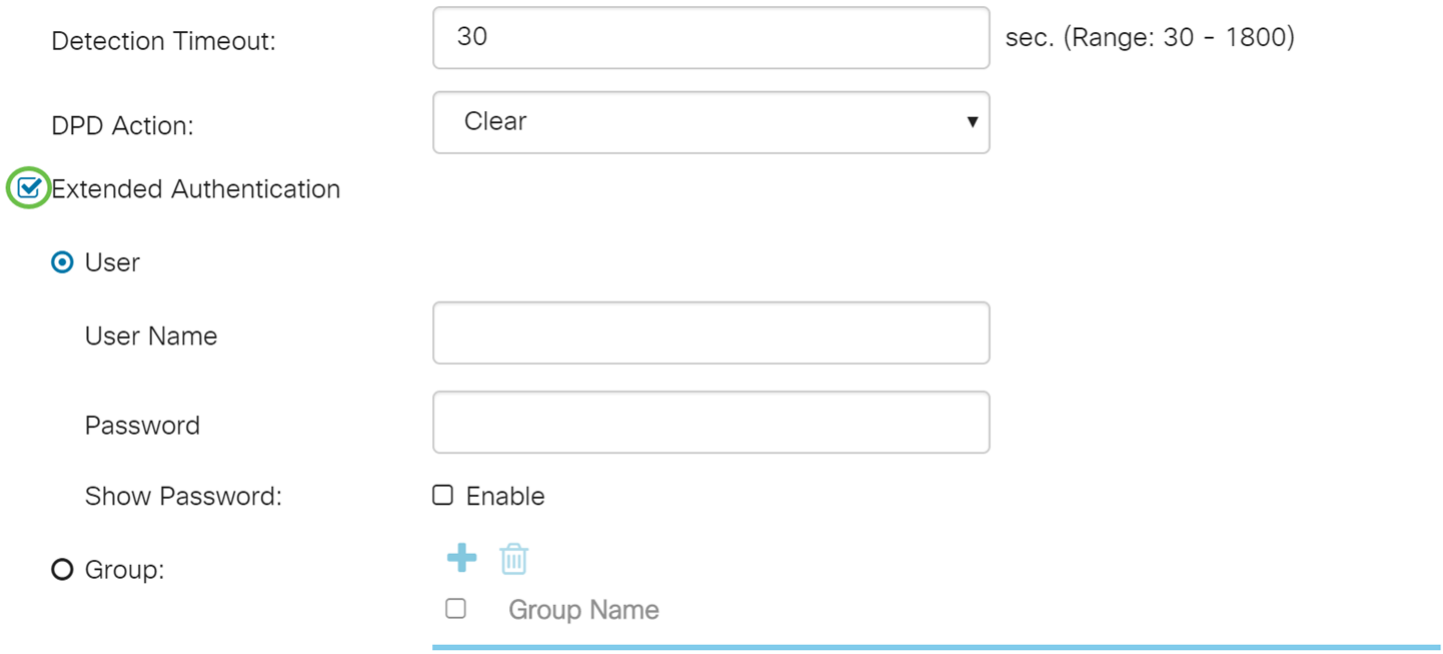
إذا كنت تريد معرفة كيفية إنشاء حسابات مستخدمين، انقر فوق الارتباط لإعادة توجيهه إلى القسم: إنشاء حساب مستخدم للمصادقة الموسعة.



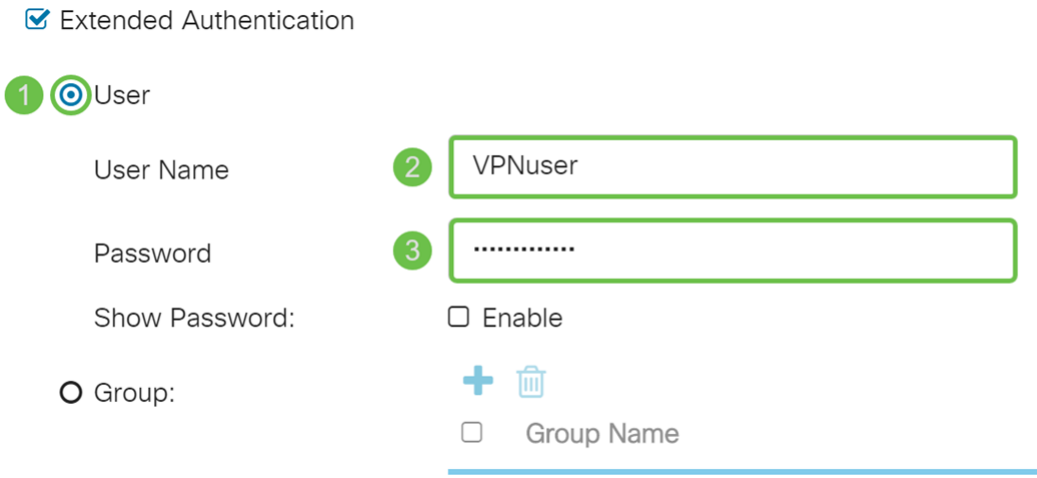
الخطوة 10. حدد **مجموعة** كمصادقة موسعة واضغط على أيقونة **زائد** لإضافة مجموعة جديدة. من القائمة المنسدلة، أختر المجموعة التي تريد إستخدامها للمصادقة. تأكد من وجود المستخدمين الذين تريد في تلك المجموعة.



الخطوة 11. في الخطوات القليلة التالية، سنقوم بتكوين الموجه البعيد لاستخدام مصادقة المستخدم. في الموجه البعيد، حدد خانة الاختيار **مصادقة موسعة** لتمكين المصادقة الموسعة.



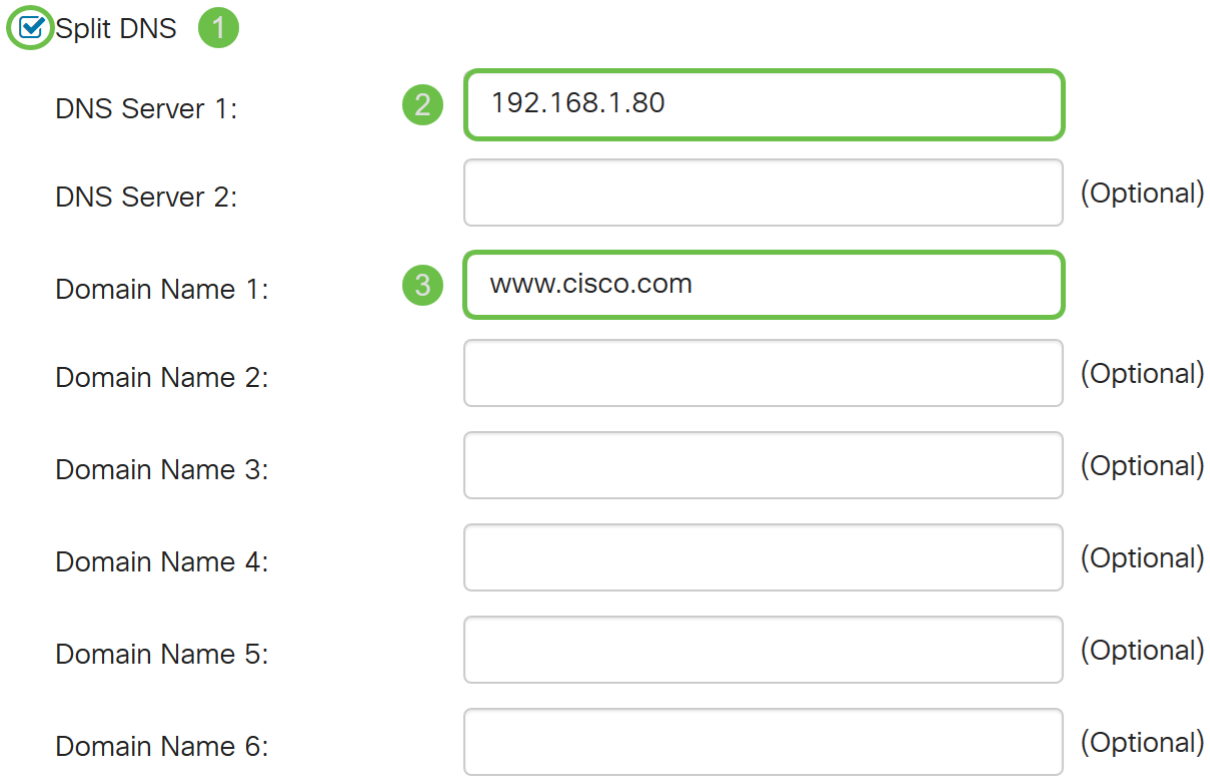
الخطوة 12. حدد **المستخدم** كمصادقة موسعة. أدخل **اسم المستخدم** و**كلمة المرور** للمستخدم في المجموعة التي تم تحديدها في الموجه الرئيسي. في هذا مثال، VPNuser و CiscoTest123! دخلت.



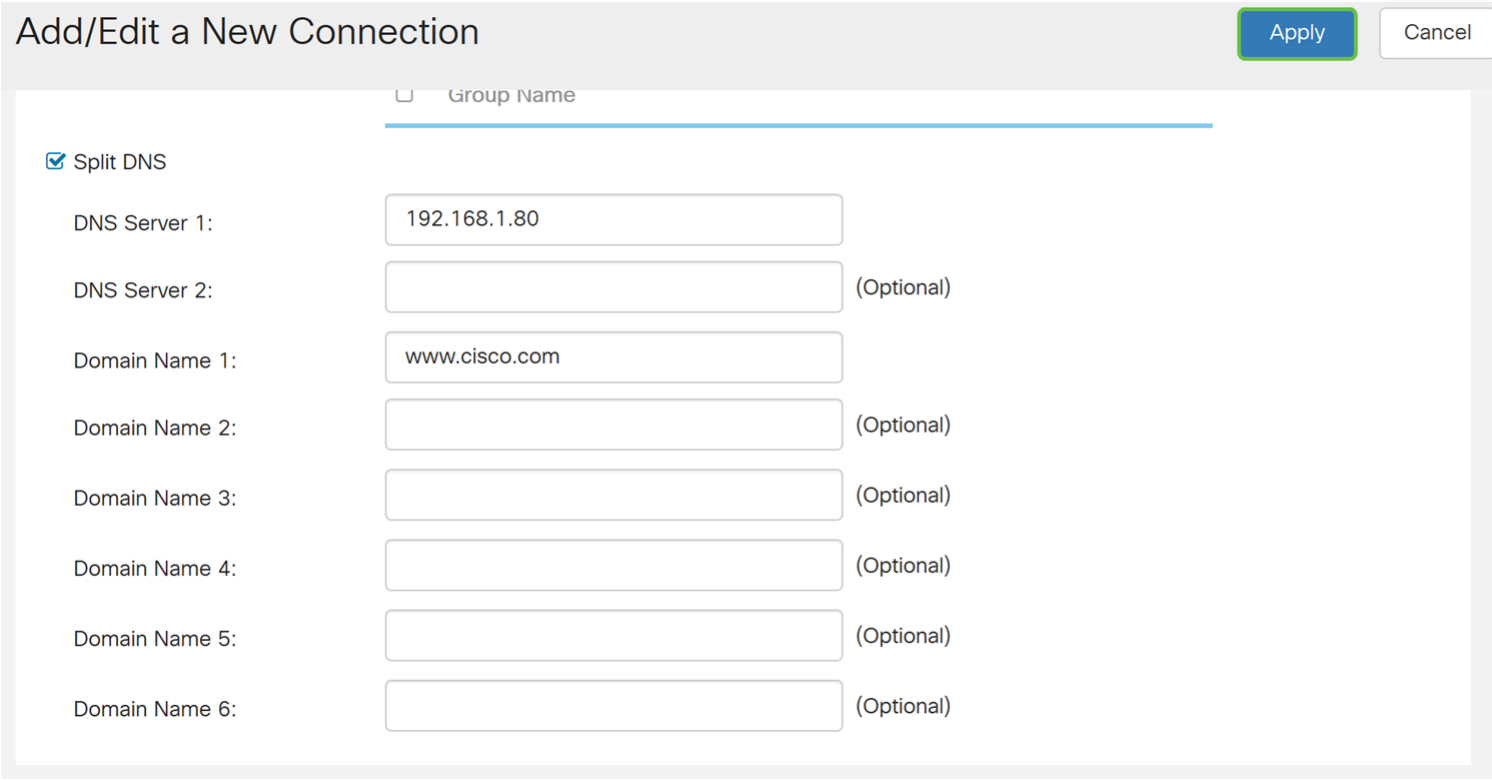
الخطوة 13. تحقق من **تقسيم DNS** للتمكين. يقوم هذا بتقسيم خادم نظام اسم المجال (DNS) وطلبات DNS الأخرى إلى خادم DNS آخر، استنادا إلى أسماء المجالات المحددة. عندما يستقبل الموجه طلب تحليل العنوان، فإنه يفحص اسم المجال. إذا طابق اسم المجال اسم مجال في إعدادات DNS المقسمة، فإنه يقوم بتمرير الطلب إلى خادم DNS المحدد داخل شبكة خادم VPN. وإلا، يتم تمرير الطلب إلى خادم DNS المحدد في إعدادات واجهة WAN (أي خادم DNS ل ISP).

يتم فصل DNS المقسم إلى منطقتين لنفس المجال. واحد لاستخدامه من قبل الشبكة الداخلية والآخر المستخدم من قبل الشبكة الخارجية. يوجه تقسيم DNS المضيفين الداخليين إلى DNS داخلي لدقة الاسم ويتم توجيه المضيفين الخارجيين إلى DNS خارجي لدقة الاسم.

إذا قمت بتمكين *تقسيم DNS*، فأدخل عنوان IP الخاص بخادم DNS لاستخدامه للمجالات المحددة. إختياريا، حدد خادم DNS ثانوي في حقل *DNS Server 2*. في *اسم المجال 1-6*، أدخل أسماء المجالات لخوادم DNS. يتم تمرير طلبات المجالات إلى خادم DNS المحدد.

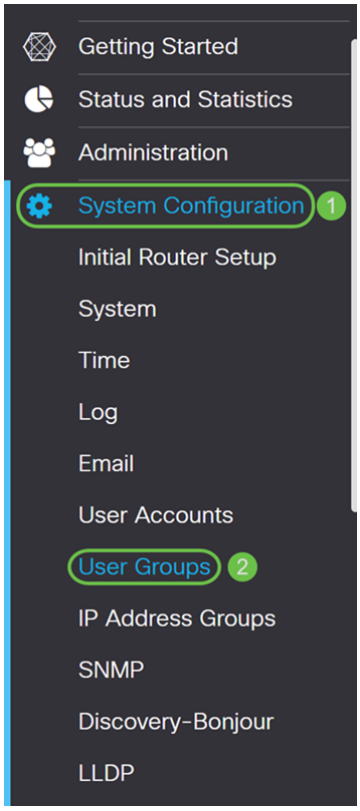


الخطوة 14. طقطقة **يطبق**.

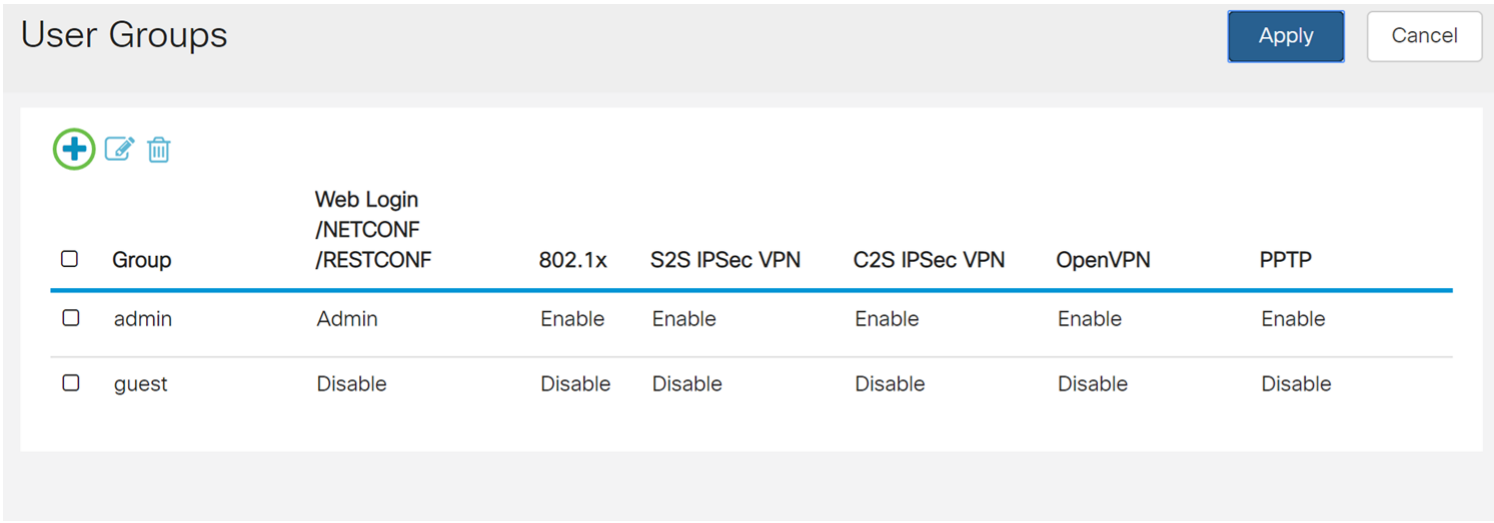


إنشاء مجموعة مستخدمين للمصادقة الموسعة

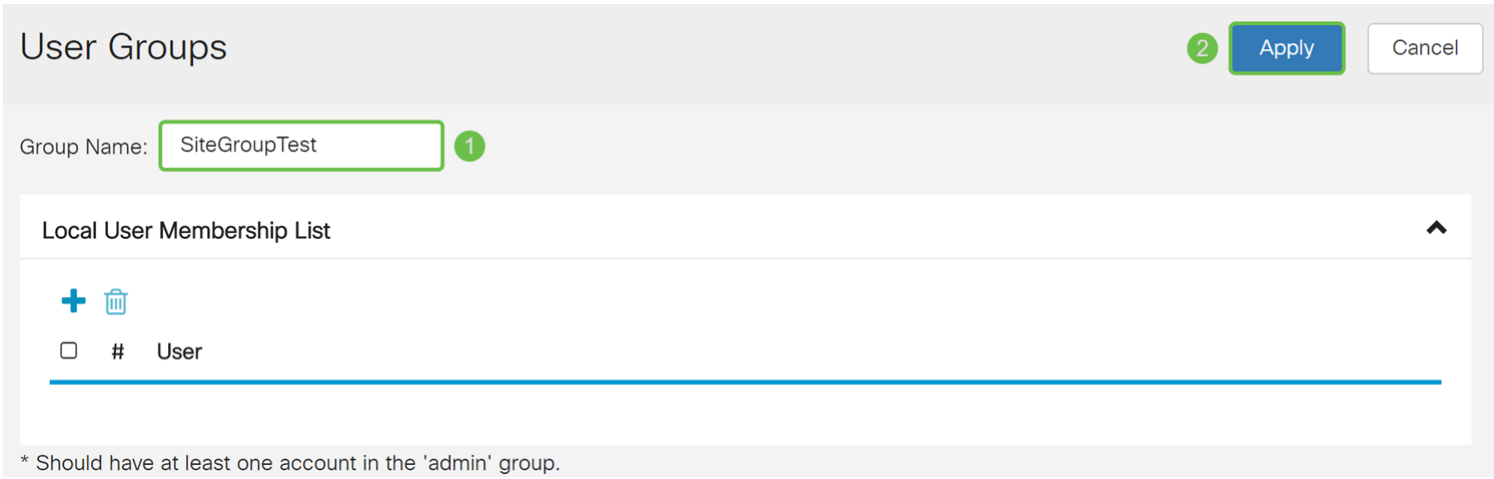
الخطوة 1. انتقل إلى **تكوين النظام > مجموعات المستخدمين**.



الخطوة 2. انقر فوق أيقونة **زائد** لإضافة مجموعة مستخدمين جديدة.



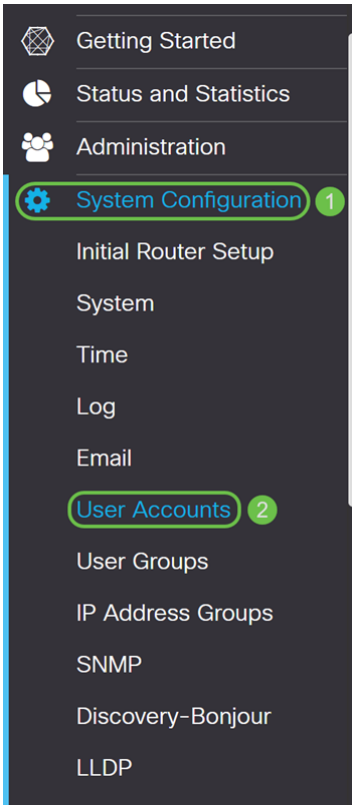
الخطوة 3. أدخل اسما في حقل *اسم المجموعة* ثم اضغط على **تطبيق**. في هذا المثال، تم إدخال SiteGroupTest كاسم للمجموعة.



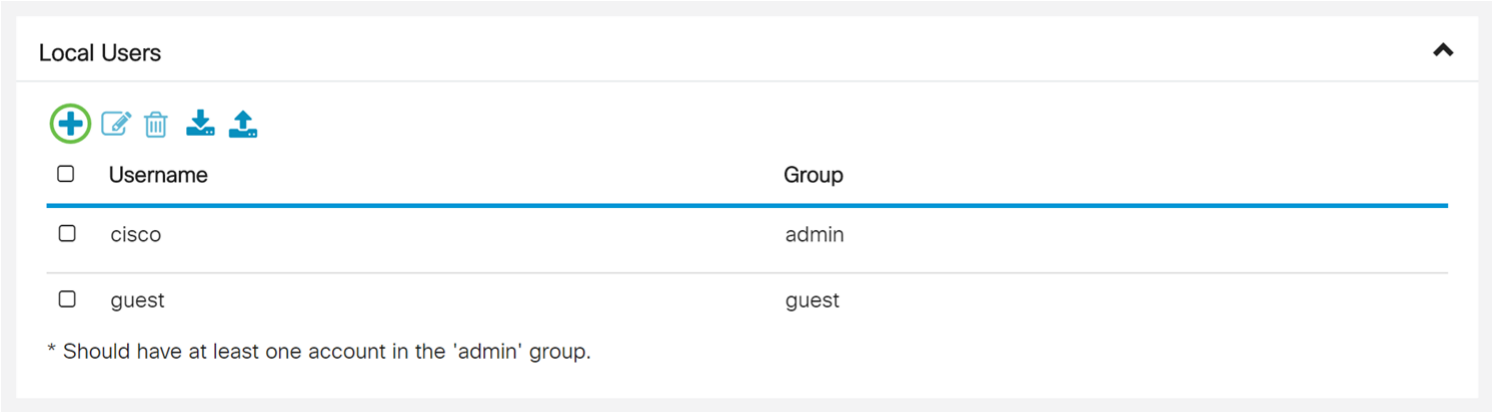
تكوين حسابات المستخدمين للمصادقة الموسعة

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.

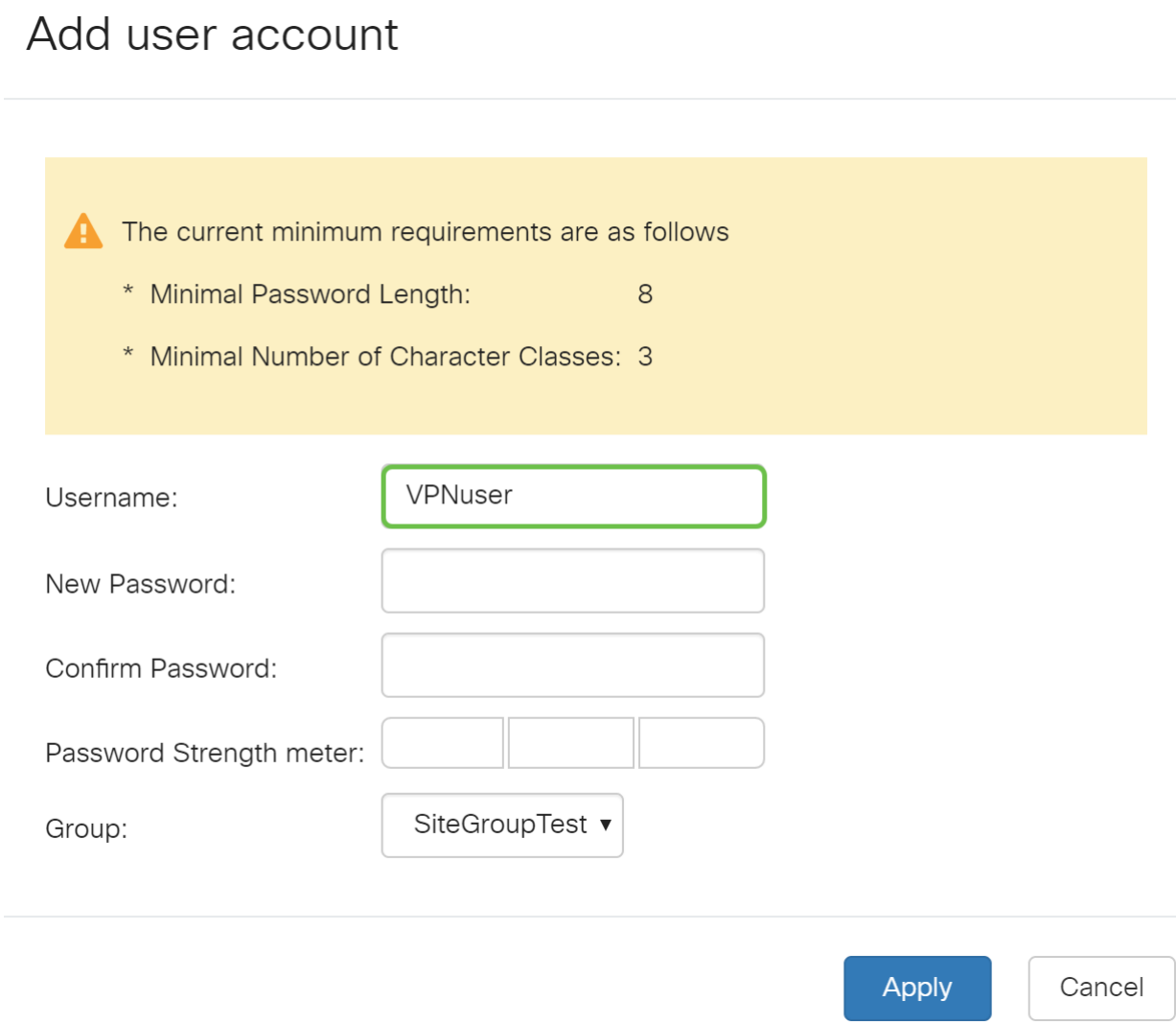
الخطوة 1. انتقل إلى **تكوين النظام > حسابات المستخدمين.**



الخطوة 2. قم بالتمرير لأسفل إلى *المستخدمين المحليين*. انقر فوق رمز **الإضافة** لإضافة مستخدم محلي جديد.

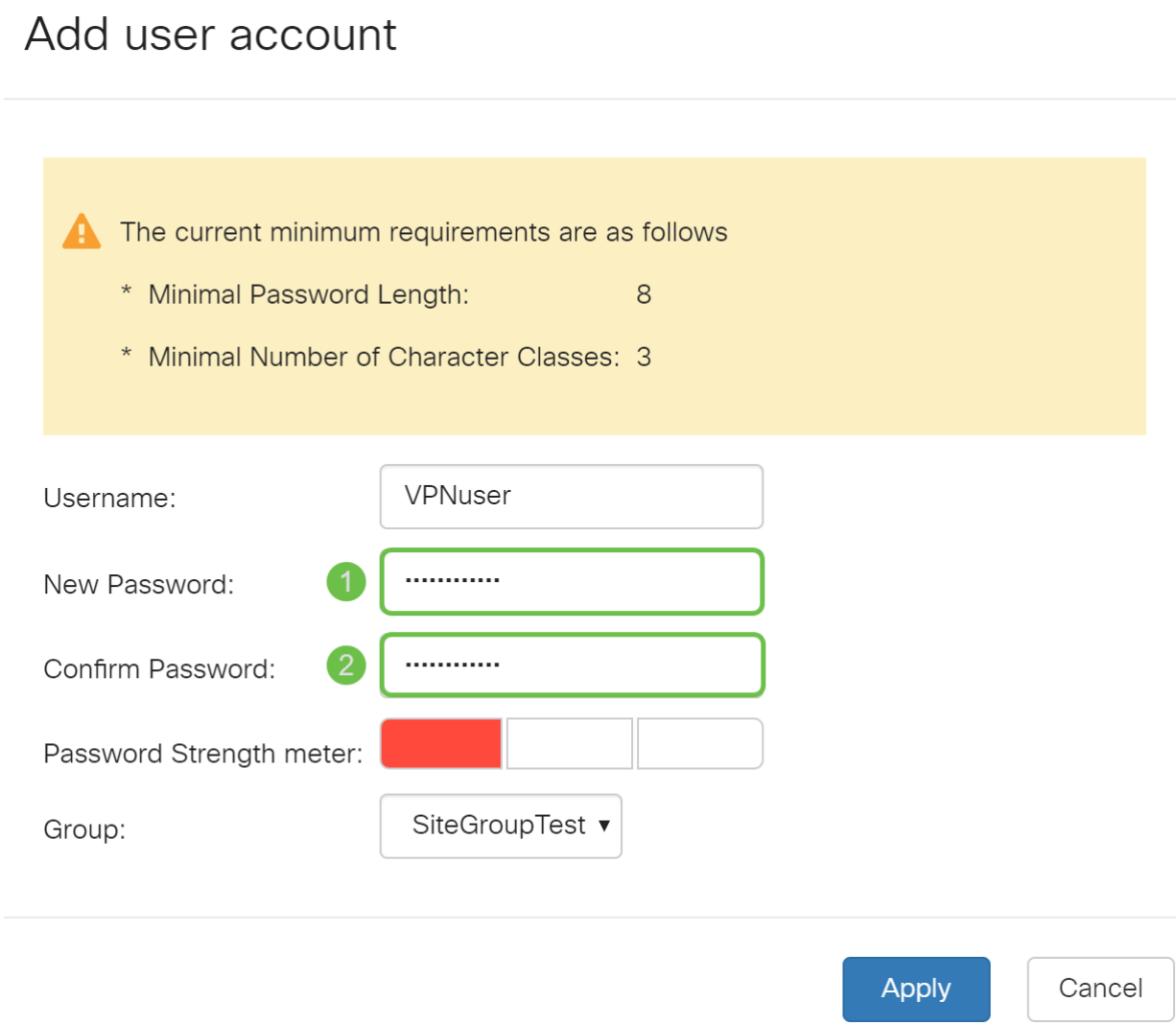


الخطوة 3. يتم فتح صفحة *إضافة حساب مستخدم*. أدخل اسم مستخدم في حقل *اسم المستخدم*. في هذا المثال، تم إدخال VPNuser كاسم مستخدم.

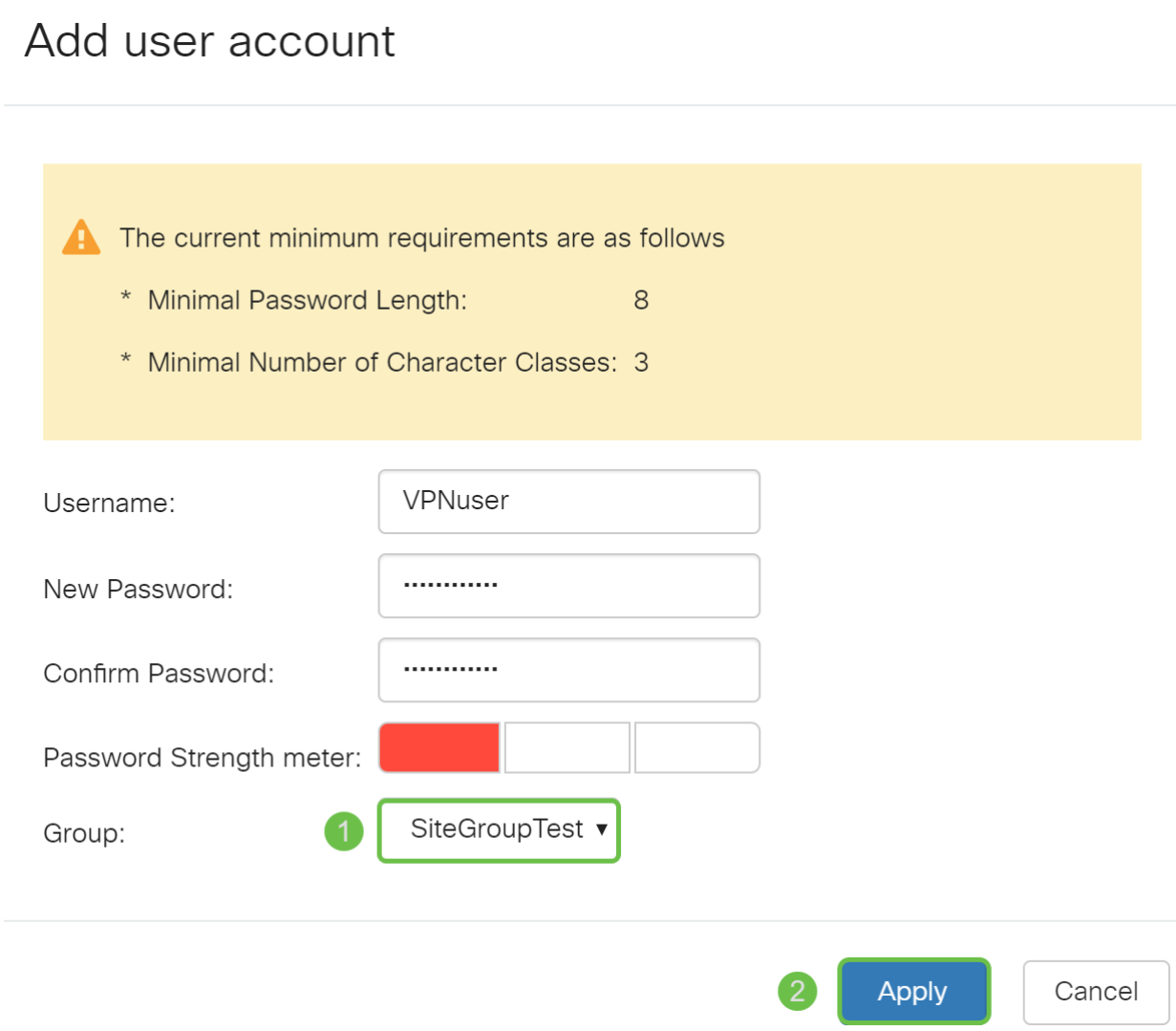


الخطوة 4. أدخل كلمة مرور في حقل *كلمة المرور الجديدة* و*تأكيد كلمة المرور*. في هذا المثال، تم إدخال !CiscoTest123.

ملاحظة: تم إستخدام كلمة المرور هذه كمثال، ومع ذلك يوصى باستخدام كلمة مرور أكثر تعقيدا.



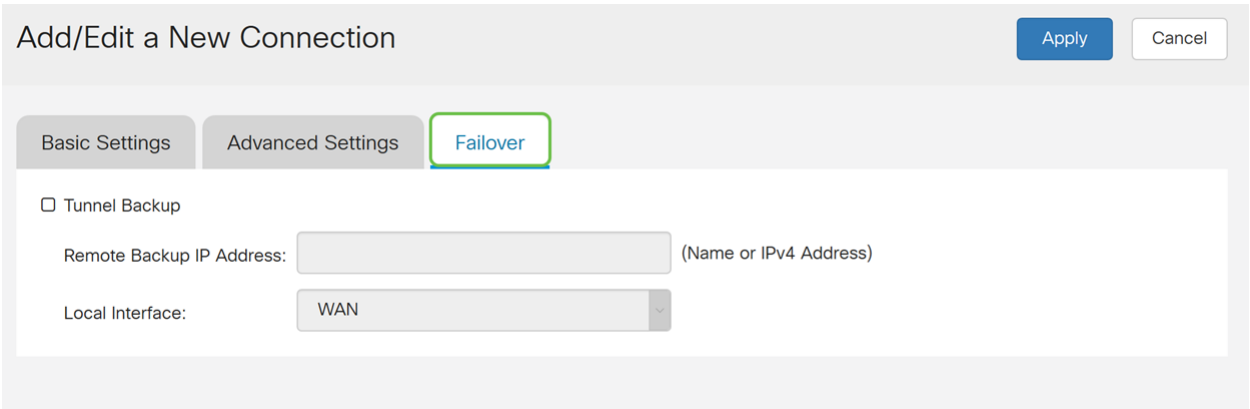
الخطوة 5. حدد مجموعة ثم اضغط على **تطبيق** لإنشاء حساب المستخدم الجديد. في هذا المثال، تم تحديد SiteGroupTest كمجموعة.



تهيئة تجاوز الفشل

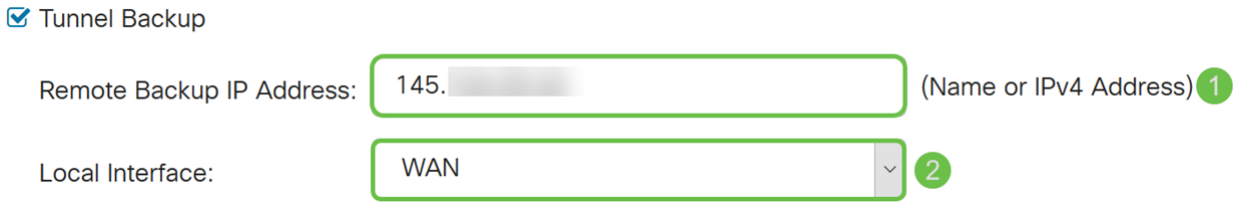
لتمكين التغلب على الأعطال من موقع إلى موقع، يجب تمكين "المحافظة على الحياة" في علامة التبويب *إعدادات متقدمة*.

الخطوة 1. انقر فوق علامة التبويب **تجاوز الفشل** لتكوين تجاوز الفشل.

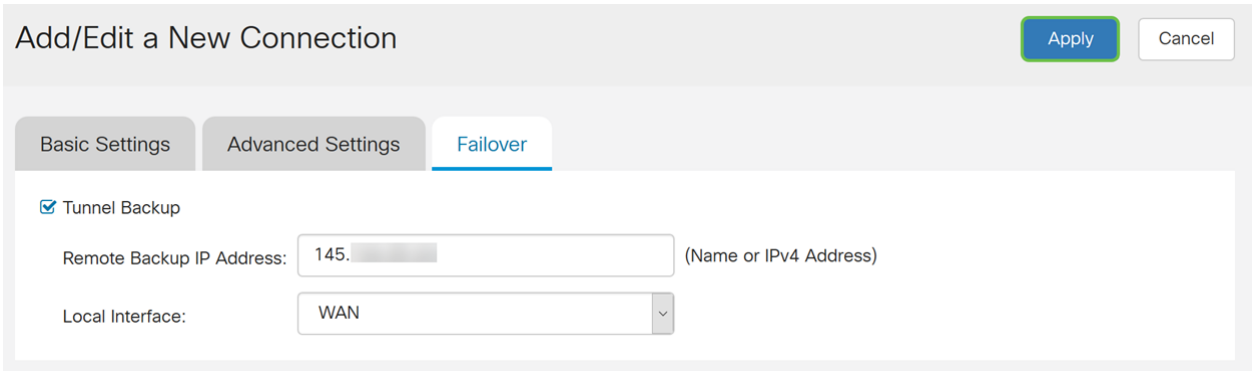


الخطوة 2. تحقق من **النسخ الاحتياطي للنفق** للتمكين. عندما يكون النفق الرئيسي معطلا، تعمل هذه الميزة على تمكين الموجه من إعادة إنشاء نفق VPN باستخدام عنوان IP بديل للنظير البعيد أو شبكة WAN محلية بديلة. تكون هذه الميزة متاحة فقط في حالة تمكين DPD.

الخطوة 3. في حقل *عنوان IP للنسخ الاحتياطي البعيد*، أدخل عنوان IP للنظير البعيد، أو أعد إدخال عنوان IP لشبكة WAN الذي تم تعيينه بالفعل للعبارة البعيدة. ثم حدد الواجهة المحلية (**WAN1** أو **WAN2** أو **USB1** أو **USB2**) من القائمة المنسدلة.



الخطوة 4. طقطقة **يطبق**.



القرار

يجب أن تكون قد انتهيت الآن من تكوين الإعدادات المتقدمة وتجاوز الفشل بنجاح للشبكة الخاصة الظاهرية (VPN) من موقع إلى موقع على شبكتي RV160 و RV260. يجب أن تظل شبكة VPN الخاصة بك من موقع إلى موقع متصلة.

عرض فيديو متعلق بهذه المقالة...

[انقر هنا لعرض المحادثات التقنية الأخرى من Cisco]

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).