تكوين معالج إعداد VPN على RV160 و RV260

يوضح هذا المستند كيفية تكوين معالج إعداد VPN على RV160 و RV260.

وقد تطورت التكنولوجيا، وغالبا ما يجري تسيير الأعمال خارج المكتب. الأجهزة أكثر قابلية للتنقل والموظفين غالبا ما يعملون من المنزل أو أثناء سفرهم. قد يتسبب ذلك في حدوث بعض الثغرات الأمنية. 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.

تقوم الشبكة الخاصة الظاهرية (VPN) بتأسيس اتصال مشفر عبر شبكة أقل أمانا مثل الإنترنت. فهي تضمن مستوى مناسبا من الأمان للنظم المتصلة. يتم إنشاء نفق كشبكة خاصة يمكنها إرسال البيانات بشكل آمن باستخدام تقنيات التشفير والمصادقة المتوافقة مع معايير الصناعة لتأمين البيانات المرسلة. تعتمد شبكة VPN للوصول عن بعد عادة على أمان بروتوكول الإنترنت (IPsec) أو طبقة مأخذ التوصيل الآمنة (SSL) لتأمين الاتصال.

توفر شبكات VPN وصول الطبقة 2 إلى الشبكة الهدف؛ وتتطلب هذه الشبكات بروتوكول نفق مثل بروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP) أو بروتوكول الاتصال النفقي من الطبقة 2 (L2TP) الذي يعمل عبر اتصال IPsec الأساسي. تدعم الشبكة الخاصة الظاهرية (VPN) ل IPsec شبكة VPN من موقع إلى موقع لنفق من عبارة إلى عبارة. على سبيل المثال، يمكن للمستخدم تكوين نفق VPN في موقع فرعي للاتصال بالموجه في موقع الشركة، حتى يمكن للموقع الفرعي الوصول بشكل آمن إلى شبكة الشركة. كما تدعم الشبكة الخاصة الظاهرية (VPN) ل IPsec شبكة VPN من العميل إلى الخادم للنفق من المضيف إلى البوابة. تعد الشبكة الخاصة الظاهرية (VPN) من العميل إلى الخادم مفيدة عند الاتصال من الكمبيوتر المحمول/الكمبيوتر الشخصي من المنزل إلى شبكة شركة من خلال خادم الشبكة الخاصة الظاهرية (VPN).

يدعم الموجه من السلسلة RV160 10 أنفاق، بينما يدعم الموجه من السلسلة RV260 20 نفقا. يرشد معالج إعداد VPN المستخدم عند تكوين اتصال آمن لنفق IPsec من موقع إلى موقع. وهذا يعمل على تبسيط التكوين من خلال تجنب المعلمات المعقدة والاختيارية، وبهذا يمكن لأي مستخدم إعداد نفق IPsec بطريقة سريعة وفعالة.

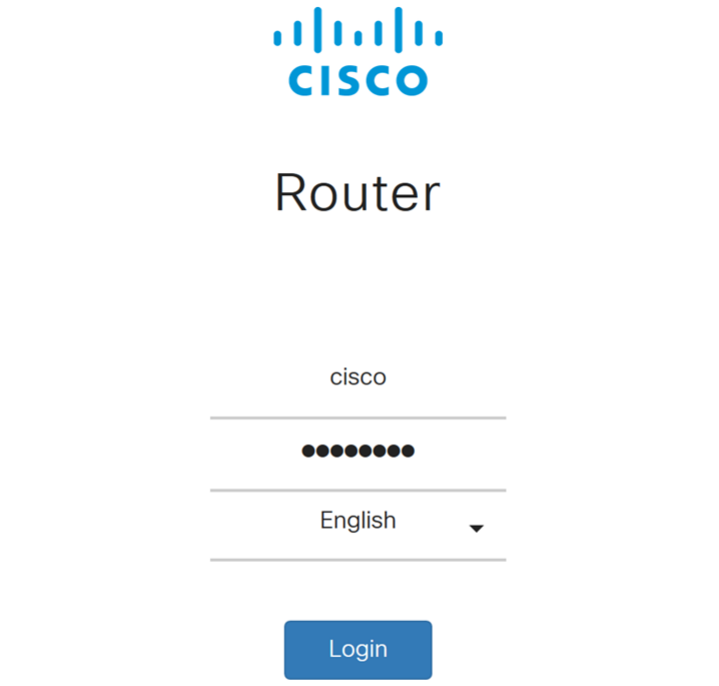
- الطراز RV160
- الطراز RV260

- 1.0.0.13

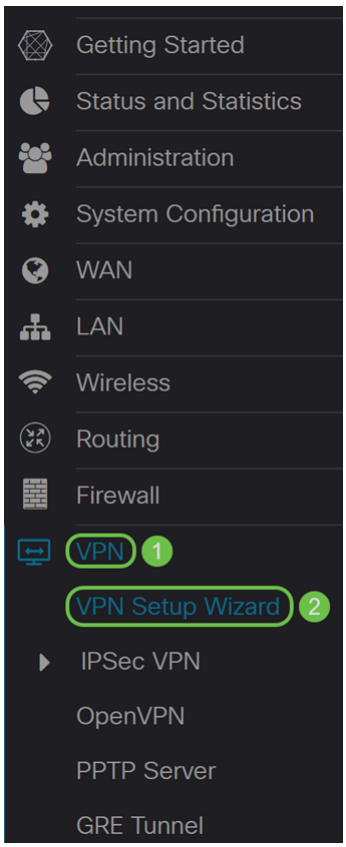
VPN

الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب على الموجه المحلي لديك.

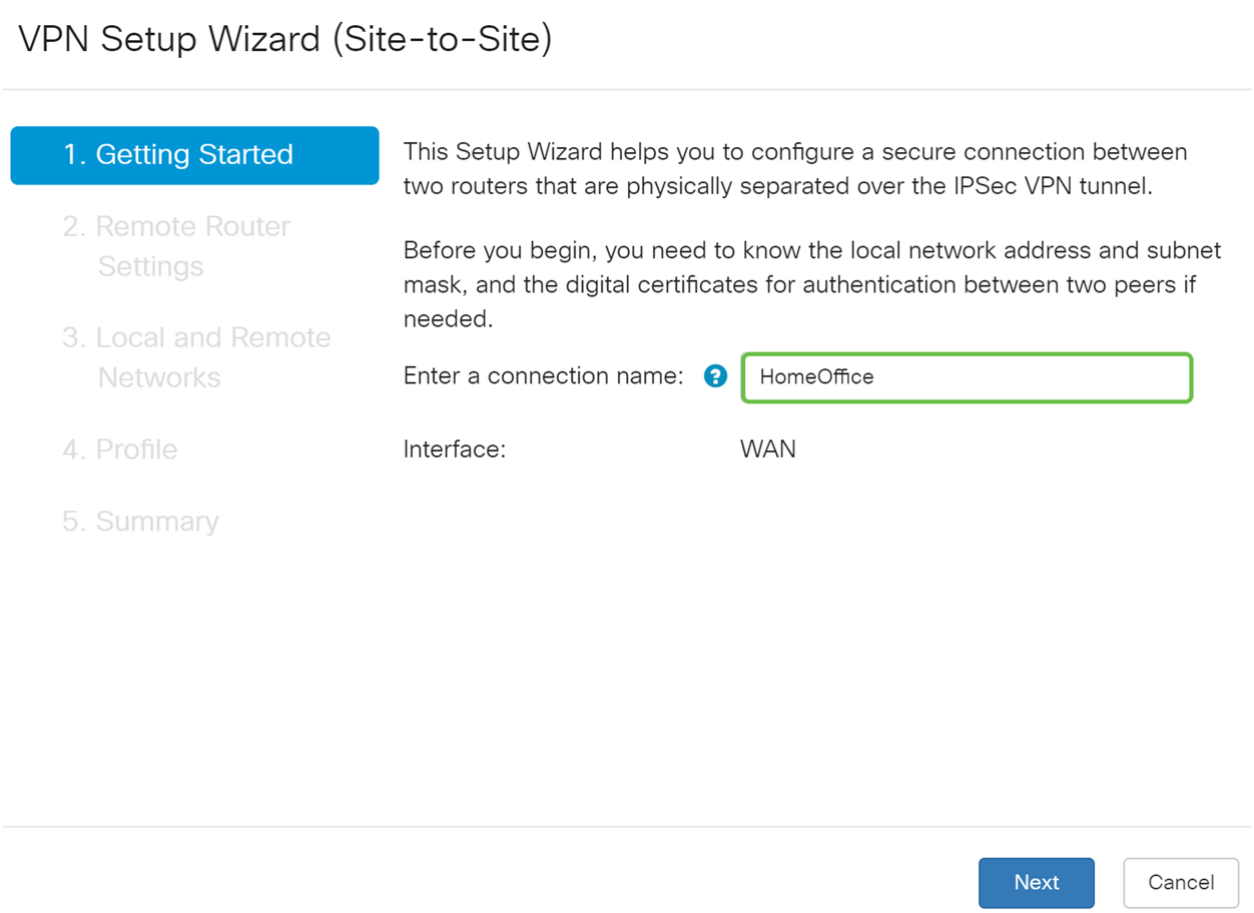
ملاحظة: سنحيل الموجه المحلي كالموجه A والموجه البعيد كموجه B. في هذا المستند، سنستخدم إثنين من RV160 لتوضيح معالج إعداد VPN.



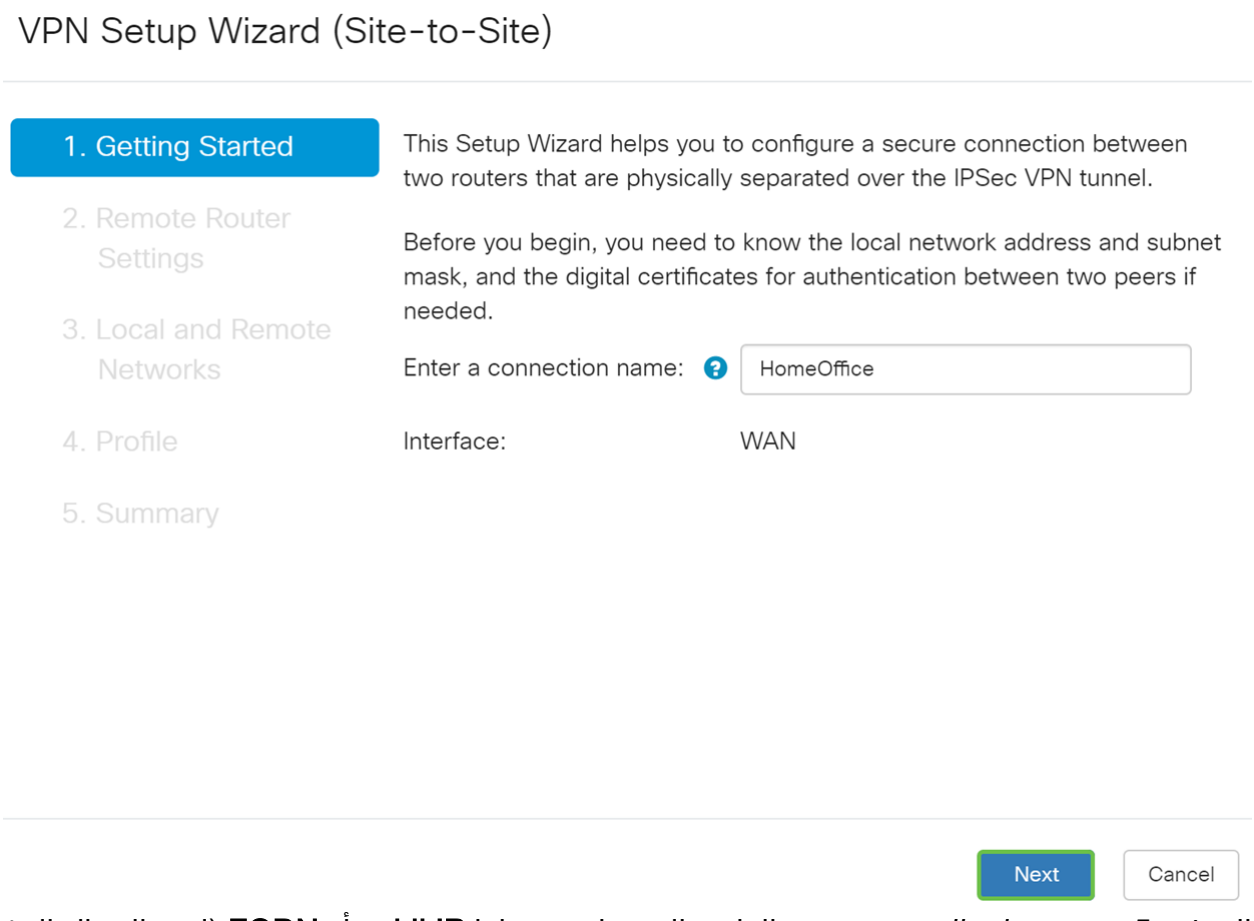
الخطوة 2. انتقل إلى **معالج إعداد VPN > VPN**.



الخطوة 3. في قسم *يحصل يبدأ* ، أدخل اسم اتصال في الحقل **أدخل اسم اتصال**. لقد أدخلنا في HomeOffice كاسم اتصال لنا.

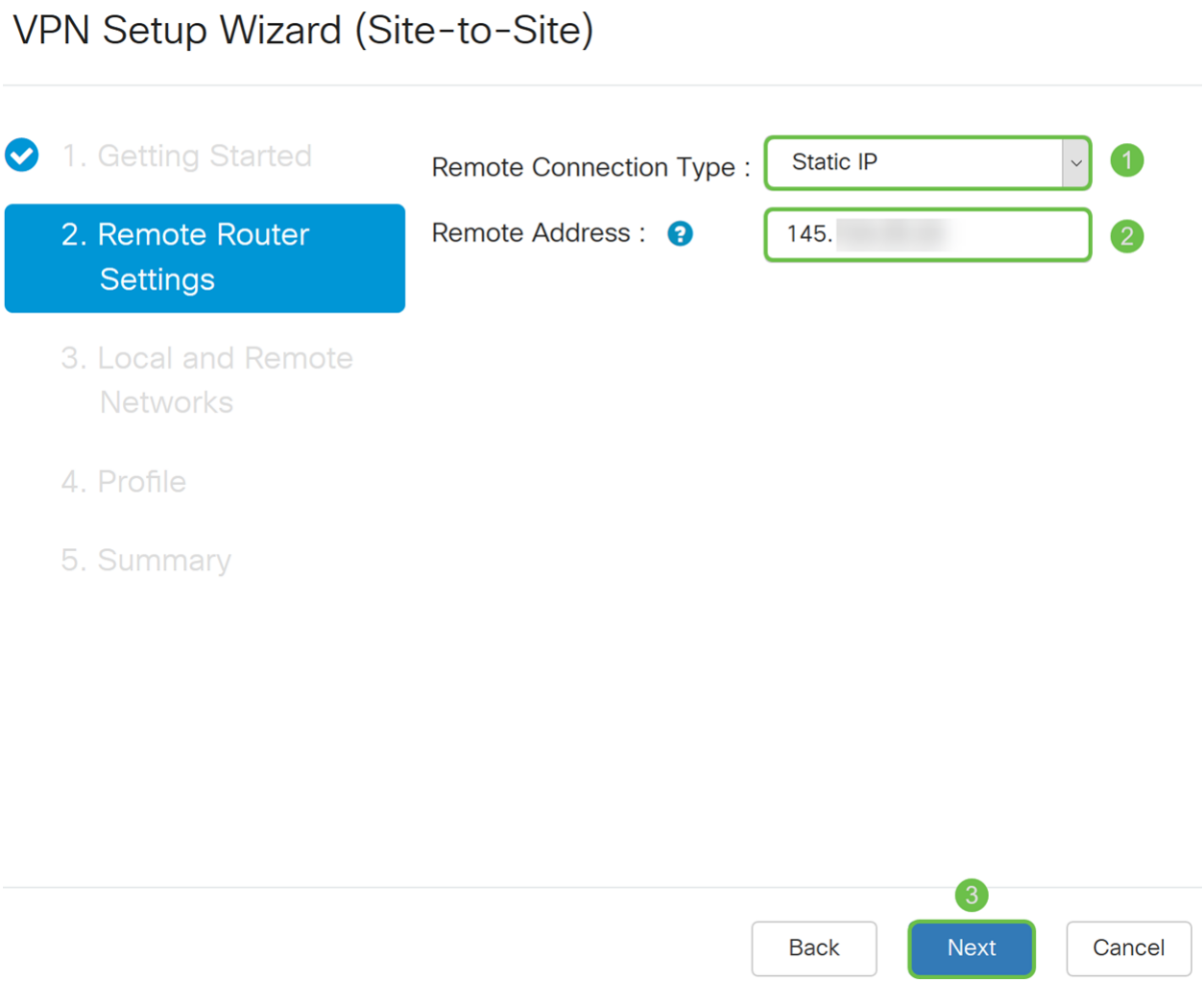


الخطوة 4. في حقل *الواجهة*، حدد واجهة من القائمة المنسدلة إذا كنت تستخدم RV260. يحتوي RV160 على إرتباط WAN فقط لذلك لن تتمكن من تحديد واجهة من القائمة المنسدلة. انقر على **التالي** للمتابعة إلى قسم *إعدادات الموجه البعيد*.

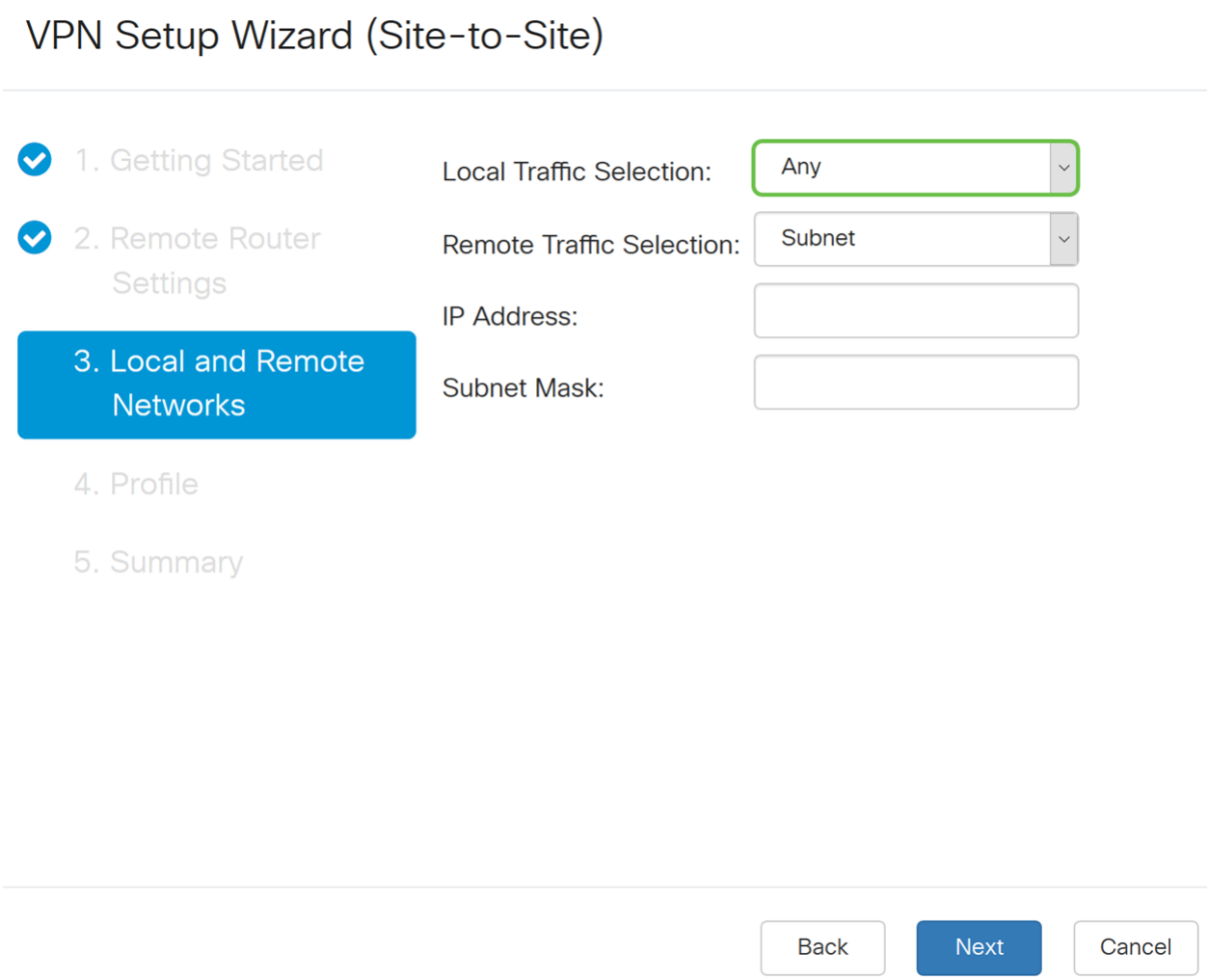


الخطوة 5. حدد *نوع اتصال عن بعد* من القائمة المنسدلة. حدد إما **IP الثابت** أو **FQDN** (اسم المجال المؤهل بالكامل) ثم أدخل إما عنوان IP الخاص بشبكة WAN أو FQDN الخاص بالبوابة التي ترغب في الاتصال بها

في حقل *العنوان البعيد*. في هذا المثال، تم تحديد **IP ساكن إستاتيكي** وتم إدخال عنوان IP للموجه البعيد WAN (الموجه B). ثم انقر فوق **التالي** للانتقال إلى المقطع التالي.

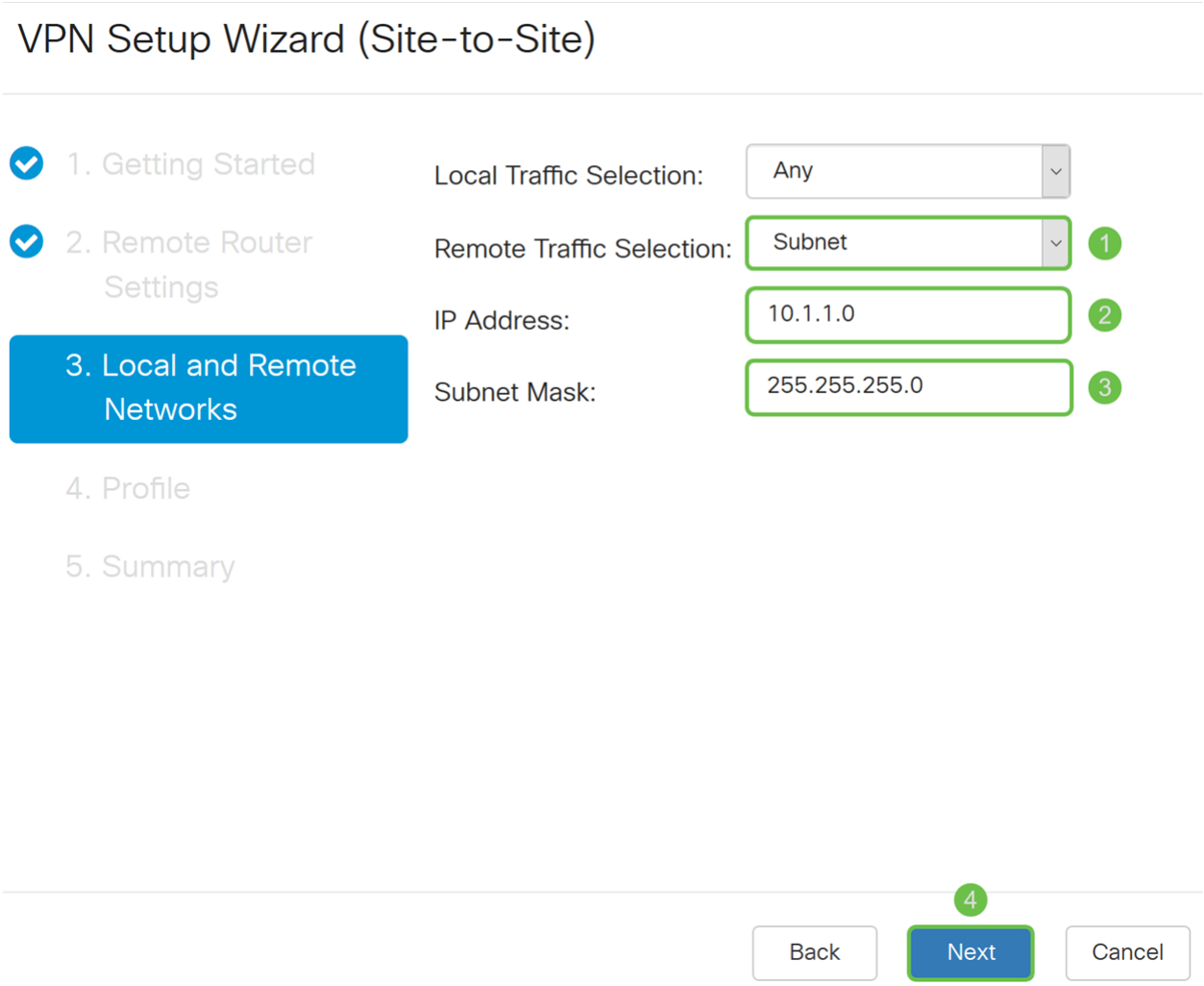


الخطوة 6. في قسم *الشبكة المحلية والبعيدة، ضمن تحديد حركة المرور المحلية*، حدد IP المحلي (**الشبكة الفرعية، أو المفرد،** أو *أي*) من القائمة المنسدلة. إذا قمت بتحديد **الشبكة الفرعية**، فأدخل عنوان IP للشبكة الفرعية وقناع الشبكة الفرعية. إذا قمت بتحديد **أحادي**، فأدخل عنوان IP. في حالة تحديد **أي**، انتقل إلى الخطوة التالية لتكوين *تحديد حركة مرور البيانات عن بعد*.

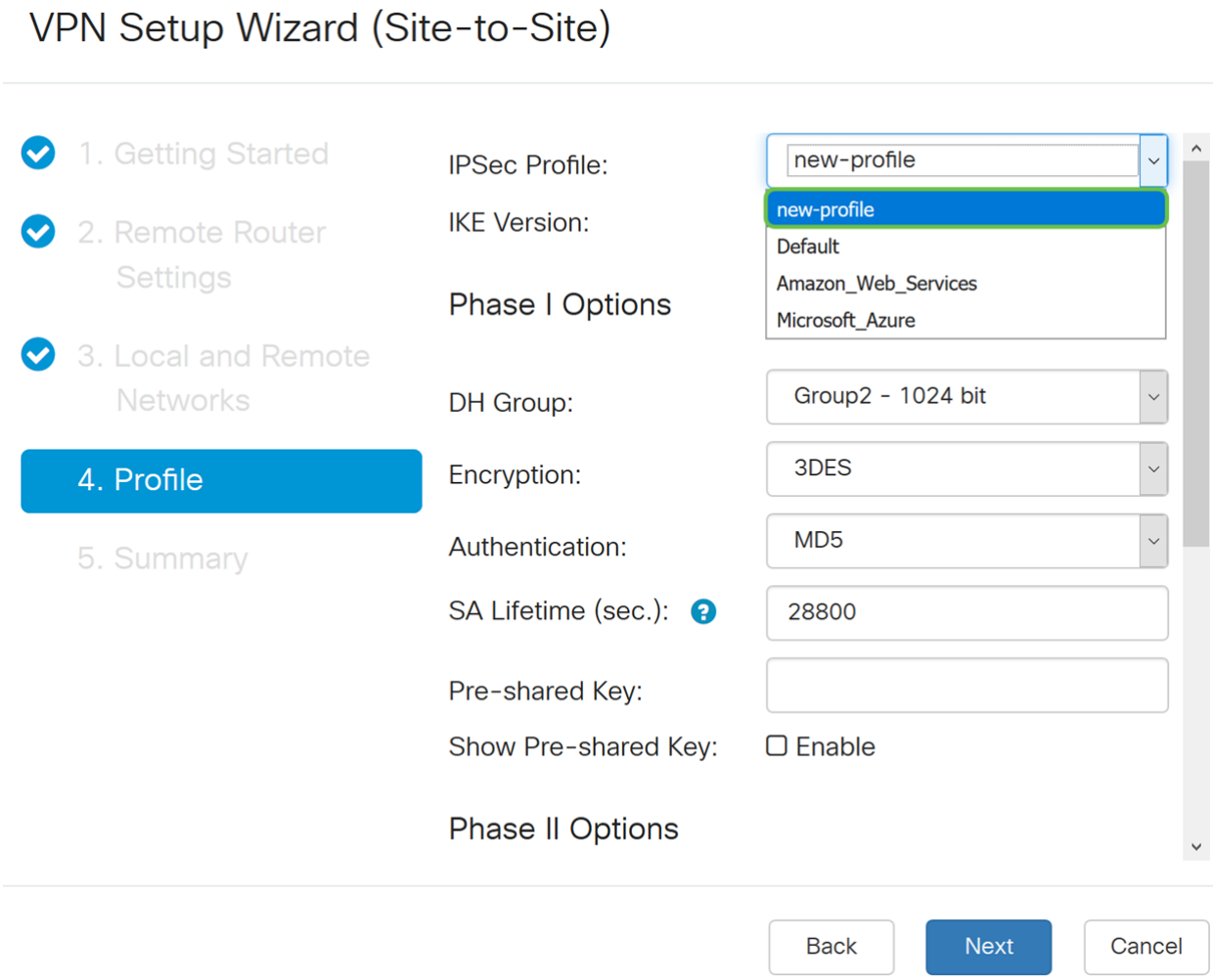


الخطوة 7. في *تحديد حركة المرور عن بعد*، حدد *IP عن بعد* (**الشبكة الفرعية أو** أحادي أو *أو* أي) *من القائمة المنسدلة*. إذا قمت بتحديد **الشبكة الفرعية**، فأدخل عنوان IP الشبكة الفرعية وقناع الشبكة الفرعية للموجه البعيد (الموجه B). إذا قمت بتحديد **أحادي**، فأدخل عنوان IP. ثم انقر على **التالي** لتكوين قسم *التوصيف*.

ملاحظة: إذا كنت قد حددت أي *لتحديد حركة المرور المحلية*، فيجب عليك تحديد إما **الشبكة الفرعية** أو **Single** لتحديد حركة مرور البيانات عن بعد.

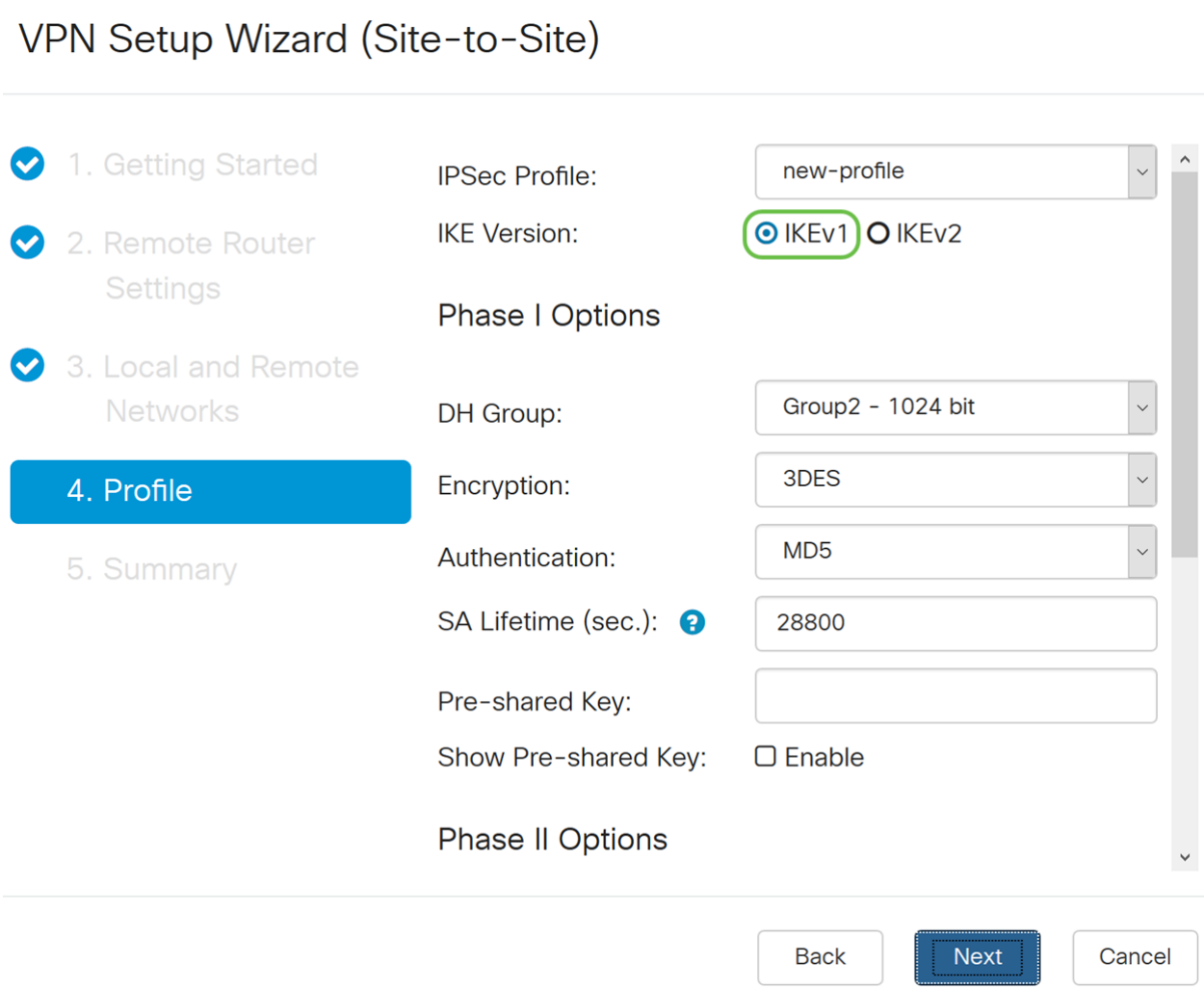


الخطوة 8. في قسم *ملف التعريف*، حدد اسم لملف تعريف IPsec من القائمة المنسدلة. لهذا العرض التوضيحي، تم تحديد **ملف تعريف جديد** كملف تعريف IPsec.



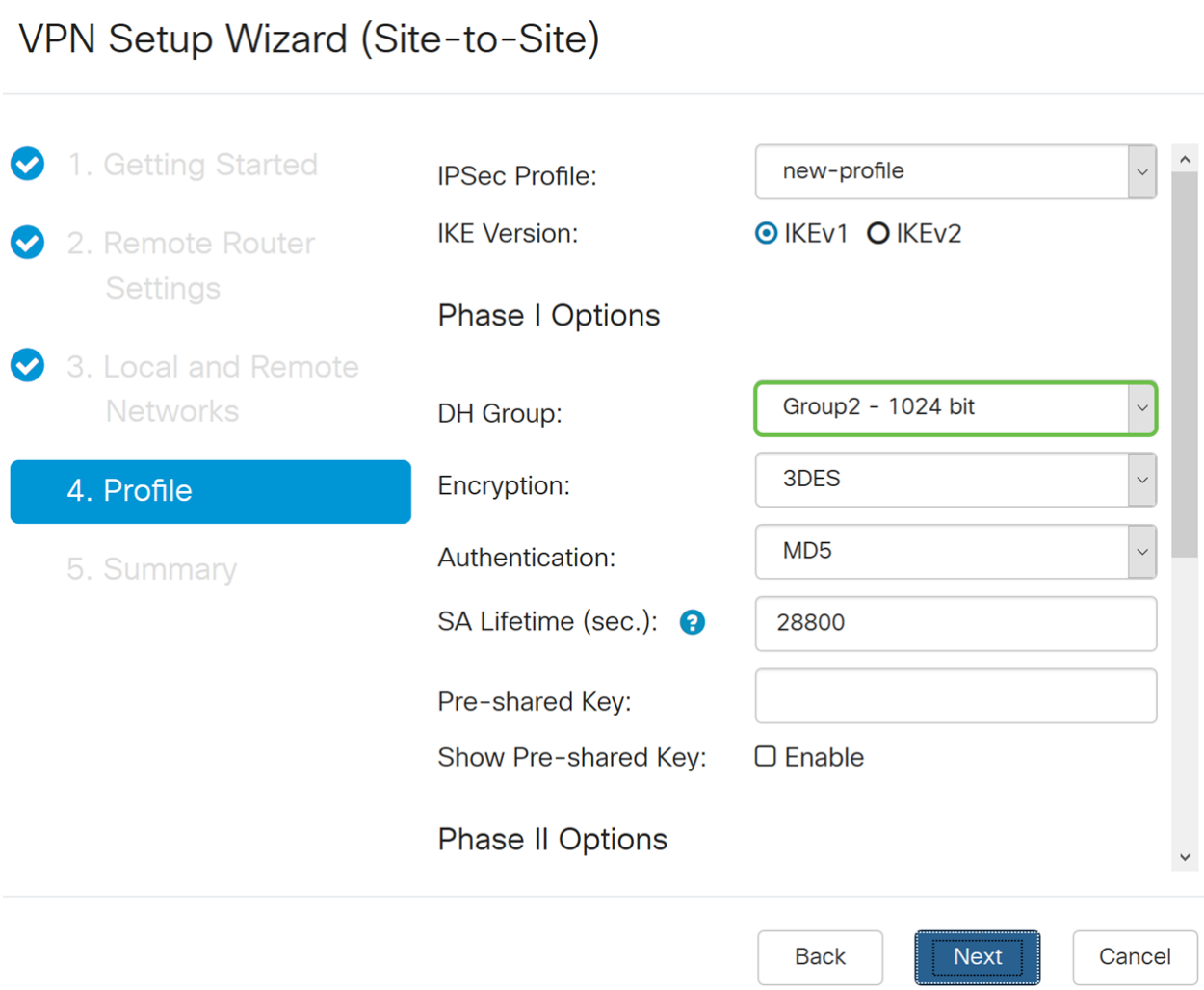
الخطوة 9. أختر IKE version 1 (**IKEv1** أو Internet Key Exchange) *IKE* كإصدار version 2 (**IKEv2** Internet Key Exchange) الخاص بك. IKE هو بروتوكول هجين يقوم بتنفيذ تبادل مفاتيح Oakley وتبادل مفاتيح Skeme داخل إطار عمل رابطة أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP). يوفر IKE مصادقة أقران IPsec، ويفاوض مفاتيح IPsec، ويتفاوض على اقترانات أمان IPsec. يعد IKEv2 أكثر فعالية لأنه يستغرق حزم أقل لإجراء تبادل المفاتيح ويدعم المزيد من خيارات المصادقة، بينما يقوم IKEv1 فقط بالمصادقة القائمة على المفاتيح المشتركة والشهادات. في هذا المثال، تم تحديد **IKEv1** كإصدار IKE.

ملاحظة: إذا كان جهازك يدعم IKEv2، يوصى باستخدام IKEv2. إذا كانت أجهزتك لا تدعم IKEv2، فاستخدم IKEv1. يحتاج كلا الموجهين (المحلي والبعيد) إلى إستخدام نفس إصدار IKE وإعدادات الأمان.



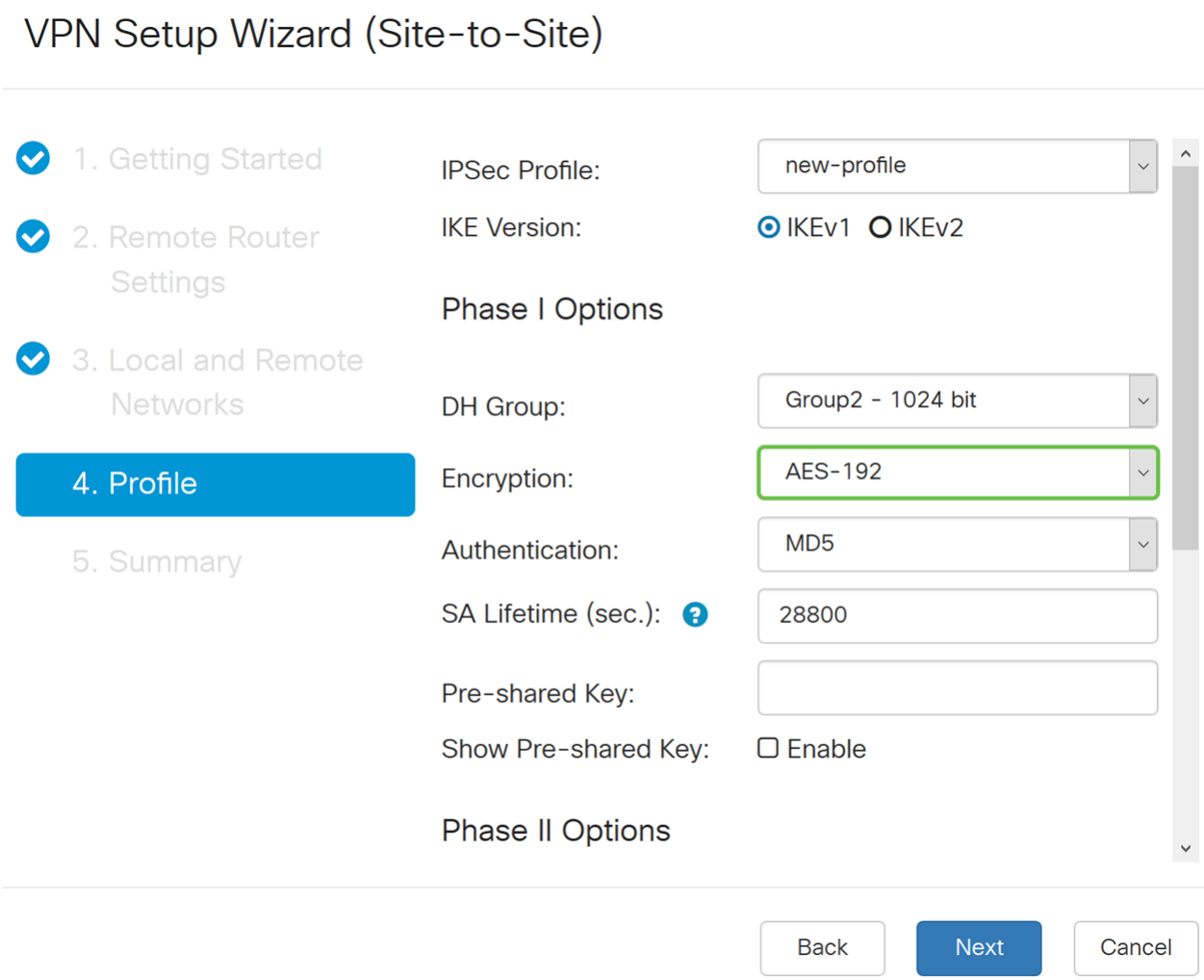
الخطوة 10. في قسم *خيارات المرحلة الأولى*، حدد مجموعة DH (Diffie-hellman) (**المجموعة 2 - 1024 بت** أو **المجموعة 5 - 1536 بت**) من القائمة المنسدلة. DH هو بروتوكول تبادل مفاتيح، مع مجموعتين من أطوال المفاتيح الأساسية المختلفة: تحتوي المجموعة 2 على ما يصل إلى 1024 وحدة بت، والمجموعة 5 على ما يصل إلى 1536 وحدة بت. سوف نستخدم **المجموعة 2 - 1024 بت** لهذا العرض التوضيحي.

ملاحظة: للحصول على سرعة أكبر وأمان أقل، أختر المجموعة 2. من أجل سرعة أبطأ وأمان أعلى، أختر مجموعة 5. يتم تحديد المجموعة 2 بشكل افتراضي.

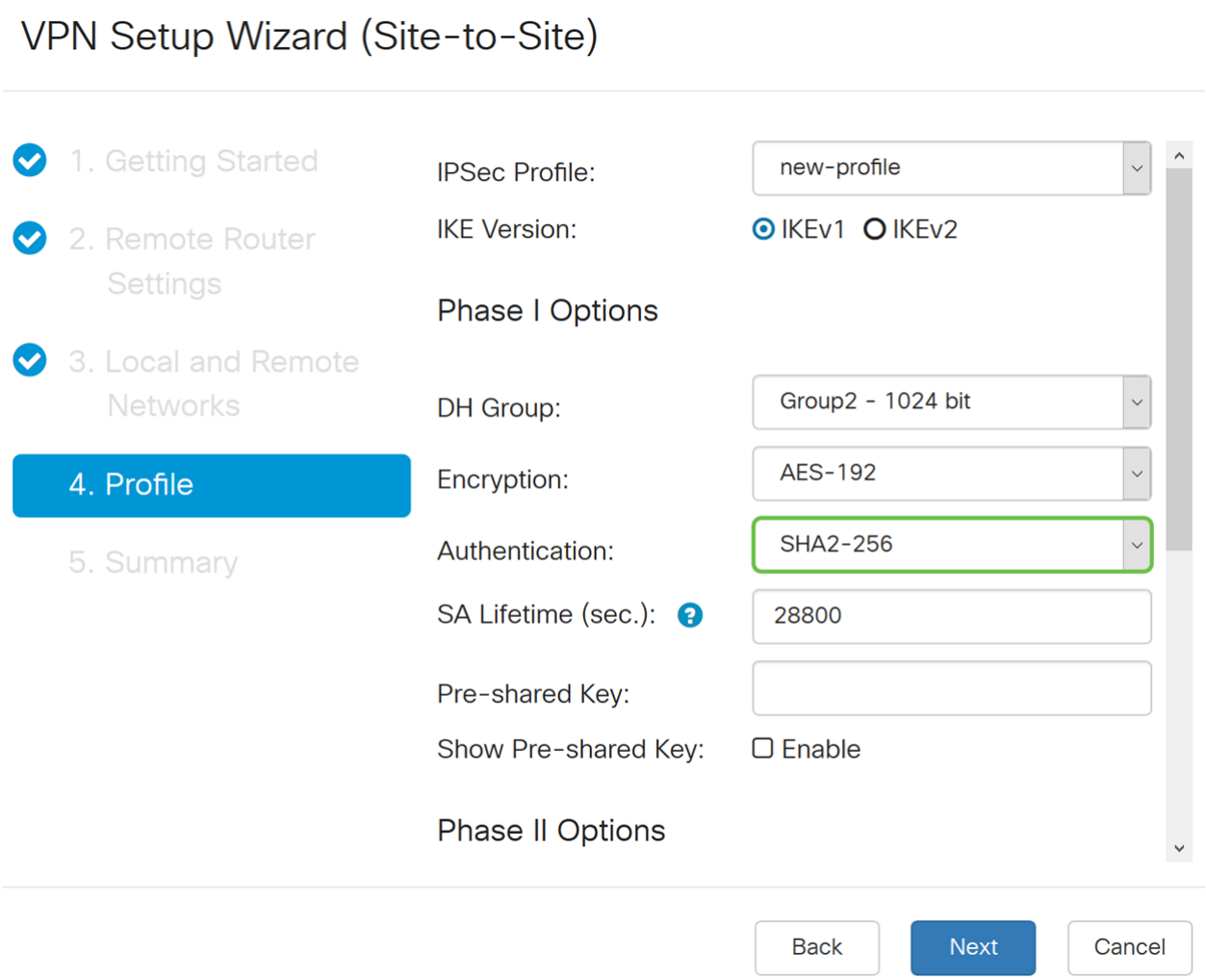


الخطوة 11. حدد خيار تشفير (**3DES أو AES-128 أو AES-192 أو AES-256**) من القائمة المنسدلة. تحدد هذه الطريقة الخوارزمية المستخدمة لتشفير حزم حمولة الأمان (ESP)/اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) أو فك تشفيرها. يستخدم المعيار الثلاثي لتشفير البيانات (3DES) تشفير DES ثلاث مرات ولكنه الآن عبارة عن خوارزمية قديمة. وهذا يعني أنه يجب إستخدامه فقط عندما لا يكون هناك بدائل أفضل لأنه يوفر مستوى أمنيا هامشيا ومقبولا في الوقت نفسه. يجب على المستخدمين إستخدامها فقط إذا كانت مطلوبة للتوافق مع الإصدارات السابقة لأنها عرضة لبعض هجمات "التصادم الكلي". معيار التشفير المتقدم (AES) هو خوارزمية تشفير تم تصميمها لتكون أكثر أمانا من DES. يستخدم معيار التشفير المتطور (AES) حجما أكبر للمفتاح مما يضمن أن النهج الوحيد المعروف لفك تشفير الرسالة هو أن يقوم الدخيل بتجريب كل مفتاح ممكن. يوصى باستخدام AES بدلا من 3DES. في هذا المثال، سنستخدم **AES-192** كخيار تشفير خاص بنا.

ملاحظة: فيما يلي بعض الموارد الإضافية التي قد تساعد: تكوين الأمان للشبكات الخاصة الظاهرية (VPNs) باستخدام IPSec وتشفير الجيل التالي.

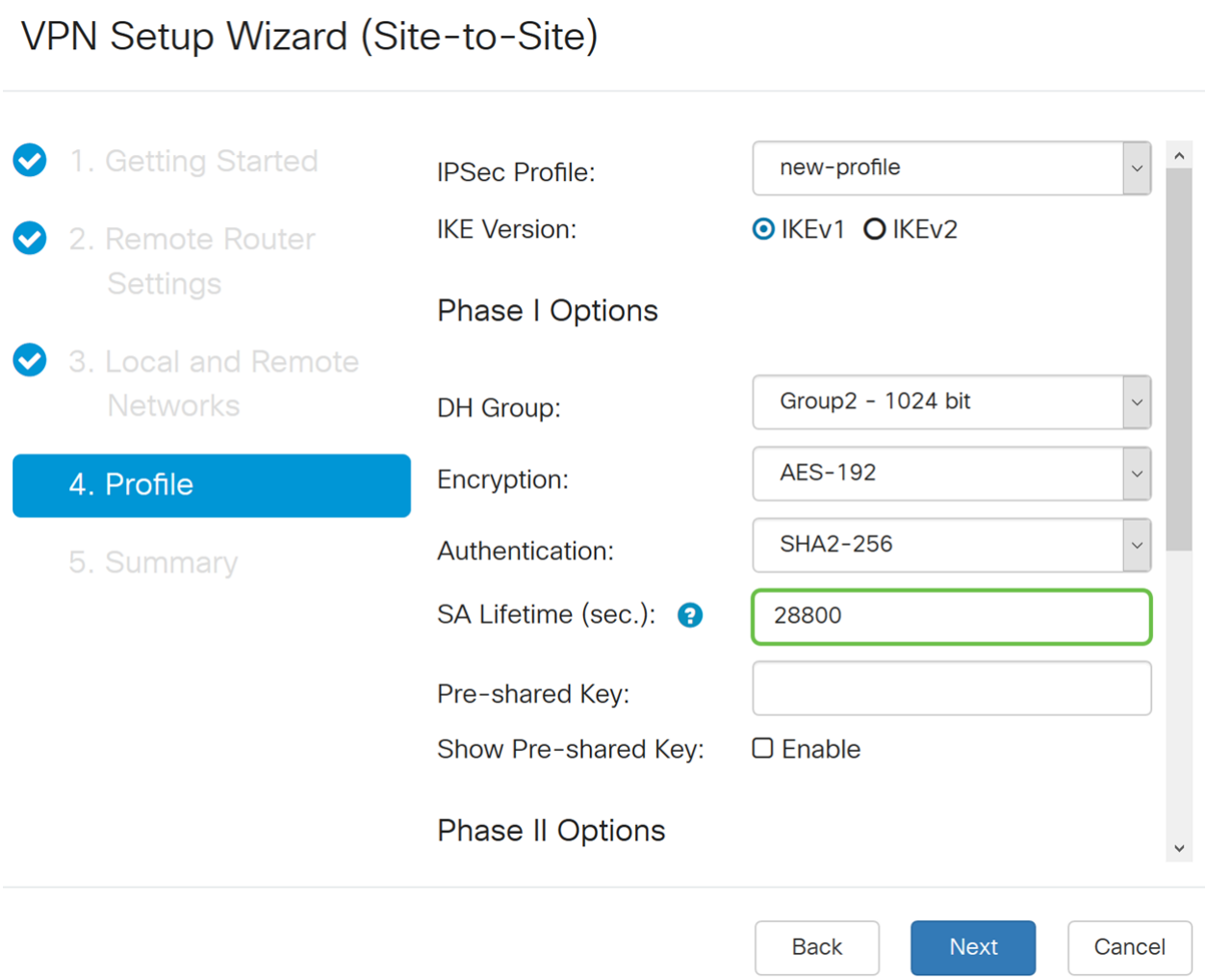


الخطوة 12. يحدد أسلوب المصادقة كيفية التحقق من صحة حزم رؤوس بروتوكول حمولة الأمان التضمين (ESP). يعتبر MD5 خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 128 بت. إن SHA1 عبارة عن خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 160 بت بينما ينتج SHA2-256 خلاصة 256 بت. يوصى بإجراء SHA2-256 لأنه أكثر أمانا. تأكد من أن كلا طرفي نفق VPN يستخدمان نفس طريقة المصادقة. حدد مصادقة (**MD5 أو SHA1** أو **SHA2-256**). تم تحديد **SHA2**-256 لهذا المثال.



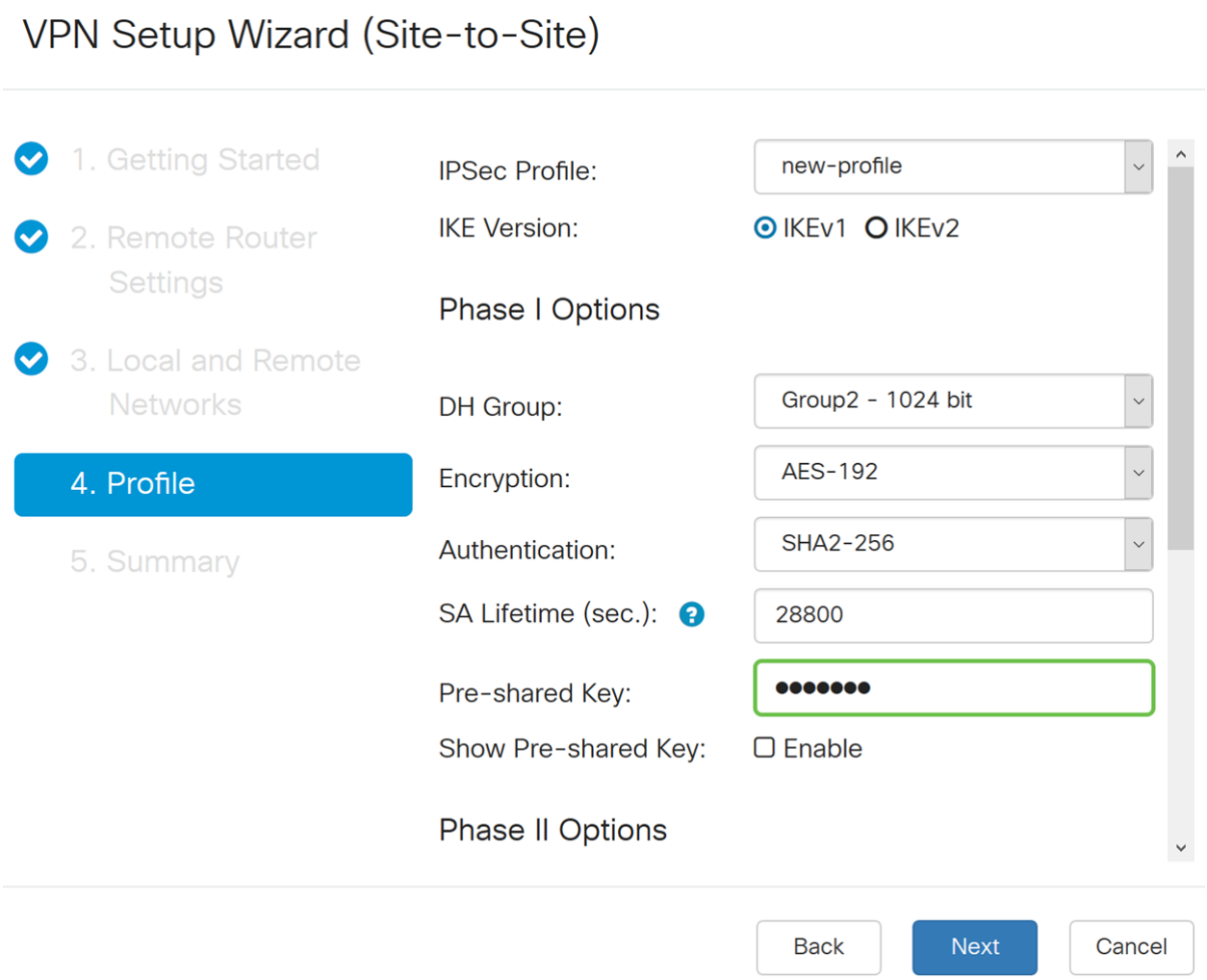
الخطوة 13. تخبرك *مدة صلاحية (sec) SA* مقدار الوقت، بالثواني، يكون IKE SA نشطا في هذه المرحلة. يتم التفاوض على اقتران أمان جديد (SA) قبل انتهاء صلاحية مدة البقاء لضمان أن وكيل خدمة (SA) جديد جاهز للاستخدام عند انتهاء صلاحية الملحق القديم. الافتراضي هو 28800 والنطاق هو من 120 إلى 86400. سنستخدم القيمة الافتراضية ل **28800** ثانية كعمر SA الخاص بنا للمرحلة الأولى.

ملاحظة: يوصى بأن تكون مدة البقاء للمساعد الخاص بك في المرحلة الأولى أطول من فترة بقائك على قيد الحياة للمرحلة الثانية. إذا جعلت المرحلة الأولى أقصر من المرحلة الثانية، ثم سيكون عليك إعادة التفاوض النفق ذهابا وإيابا بشكل متكرر مقارنة بنفق البيانات. إن نفق البيانات هو ما يحتاج إلى مزيد من الأمان ومن الأفضل أن تكون مدة البقاء في المرحلة الثانية أقصر من المرحلة الأولى.



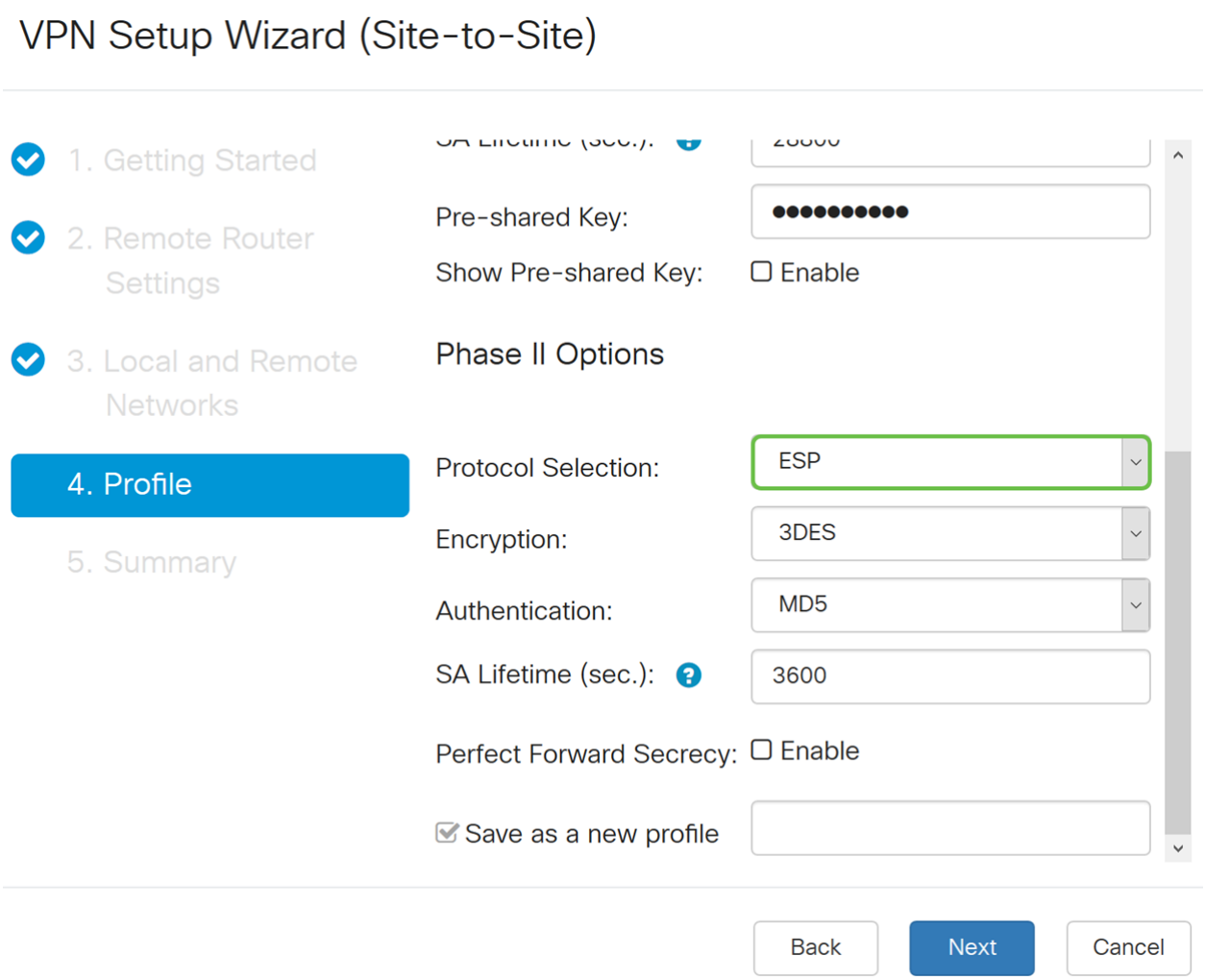
الخطوة 14. أدخل **المفتاح المشترك مسبقا** لاستخدامه لمصادقة نظير IKE البعيد. يمكنك إدخال حتى 30 حرف من لوحة المفاتيح أو قيم سداسية عشرية، مثل My_@123 أو 4d795f40313233. يجب أن يستخدم كلا طرفي نفق VPN نفس المفتاح المشترك مسبقا.

ملاحظة: نوصي بتغيير المفتاح المشترك مسبقا بشكل دوري لزيادة أمان VPN إلى الحد الأقصى.



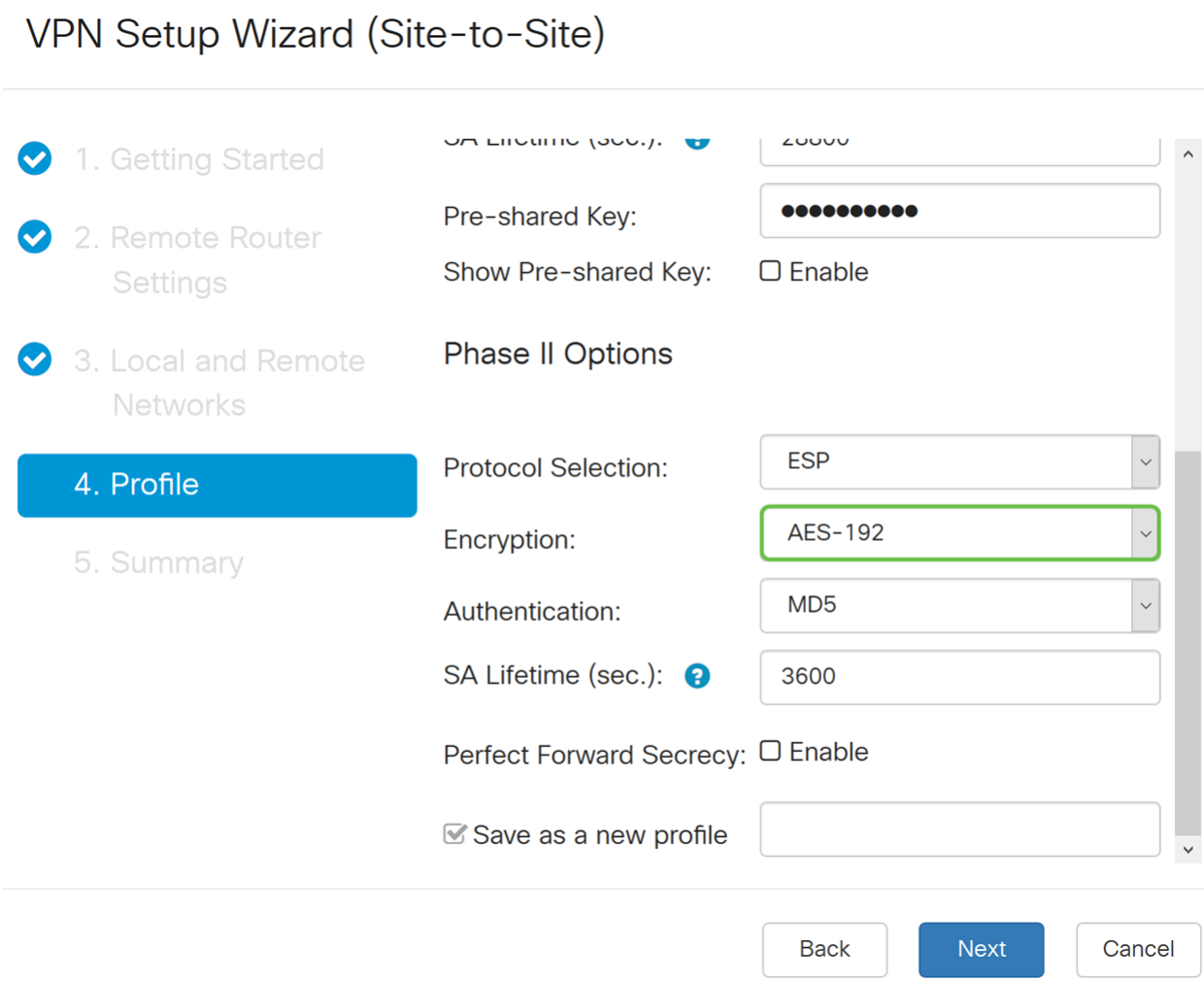
الخطوة 15. في قسم *خيارات المرحلة الثانية*، حدد بروتوكول من القائمة المنسدلة.

- **ESP** - حدد ESP لتشفير البيانات وأدخل التشفير.
- **آه** - حدد هذا الخيار لسلامة البيانات في الحالات التي تكون فيها البيانات غير سرية ولكن يجب مصادقتها.

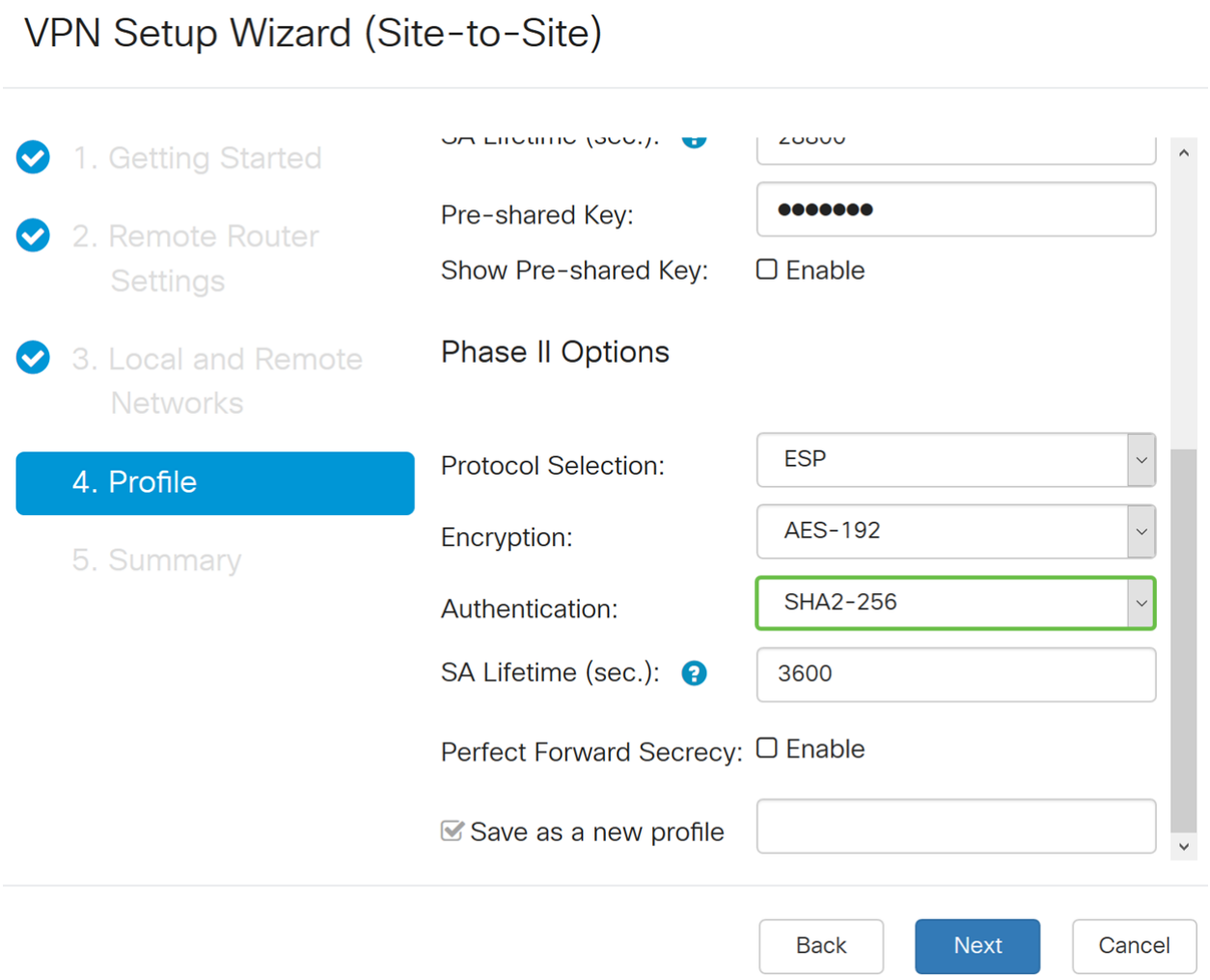


الخطوة 16. حدد خيار تشفير (**3DES أو AES-128 أو AES-192** أو **AES-256**) من القائمة المنسدلة. تحدد هذه الطريقة الخوارزمية المستخدمة لتشفير حزم حمولة الأمان (ESP)/اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) أو فك تشفيرها. يستخدم المعيار الثلاثي لتشفير البيانات (3DES) تشفير DES ثلاث مرات ولكنه الآن عبارة عن خوارزمية قديمة. وهذا يعني أنه يجب إستخدامه فقط عندما لا يكون هناك بدائل أفضل لأنه يوفر مستوى أمنيا هامشيا ومقبولا في الوقت نفسه. يجب على المستخدمين إستخدامها فقط إذا كانت مطلوبة للتوافق مع الإصدارات السابقة لأنها عرضة لبعض هجمات "التصادم الكلي". معيار التشفير المتقدم (AES) هو خوارزمية تشفير تم تصميمها لتكون أكثر أمانا من DES. يستخدم معيار التشفير المتطور (AES) حجما أكبر للمفتاح مما يضمن أن النهج الوحيد المعروف لفك تشفير الرسالة هو أن يقوم الدخيل بتجريب كل مفتاح ممكن. يوصى باستخدام AES بدلا من 3DES. في هذا المثال، سنستخدم **AES-192** كخيار تشفير خاص بنا.

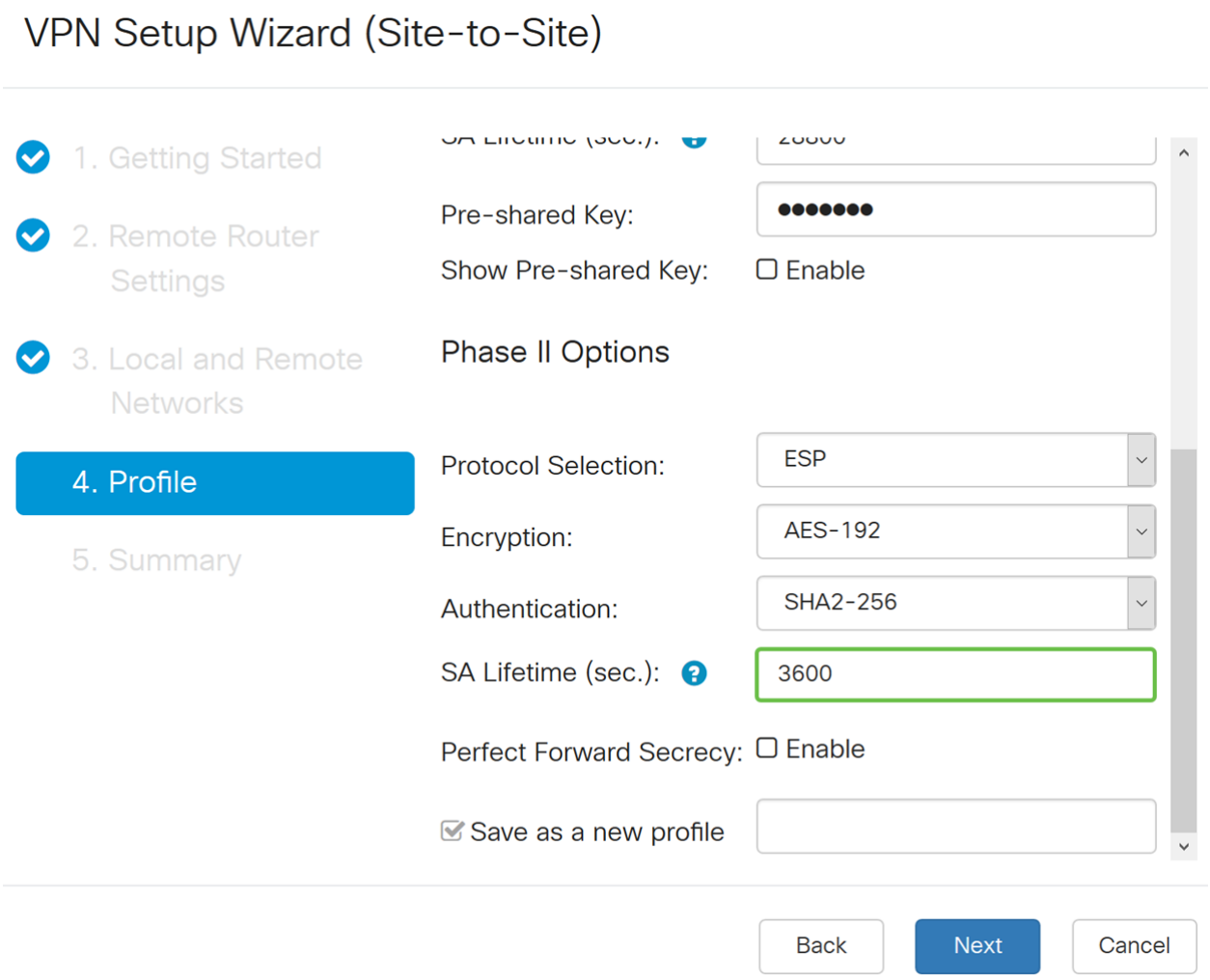
ملاحظة: فيما يلي بعض الموارد الإضافية التي قد تساعد: تكوين الأمان للشبكات الخاصة الظاهرية (VPNs) باستخدام IPSec وتشفير الجيل التالي.



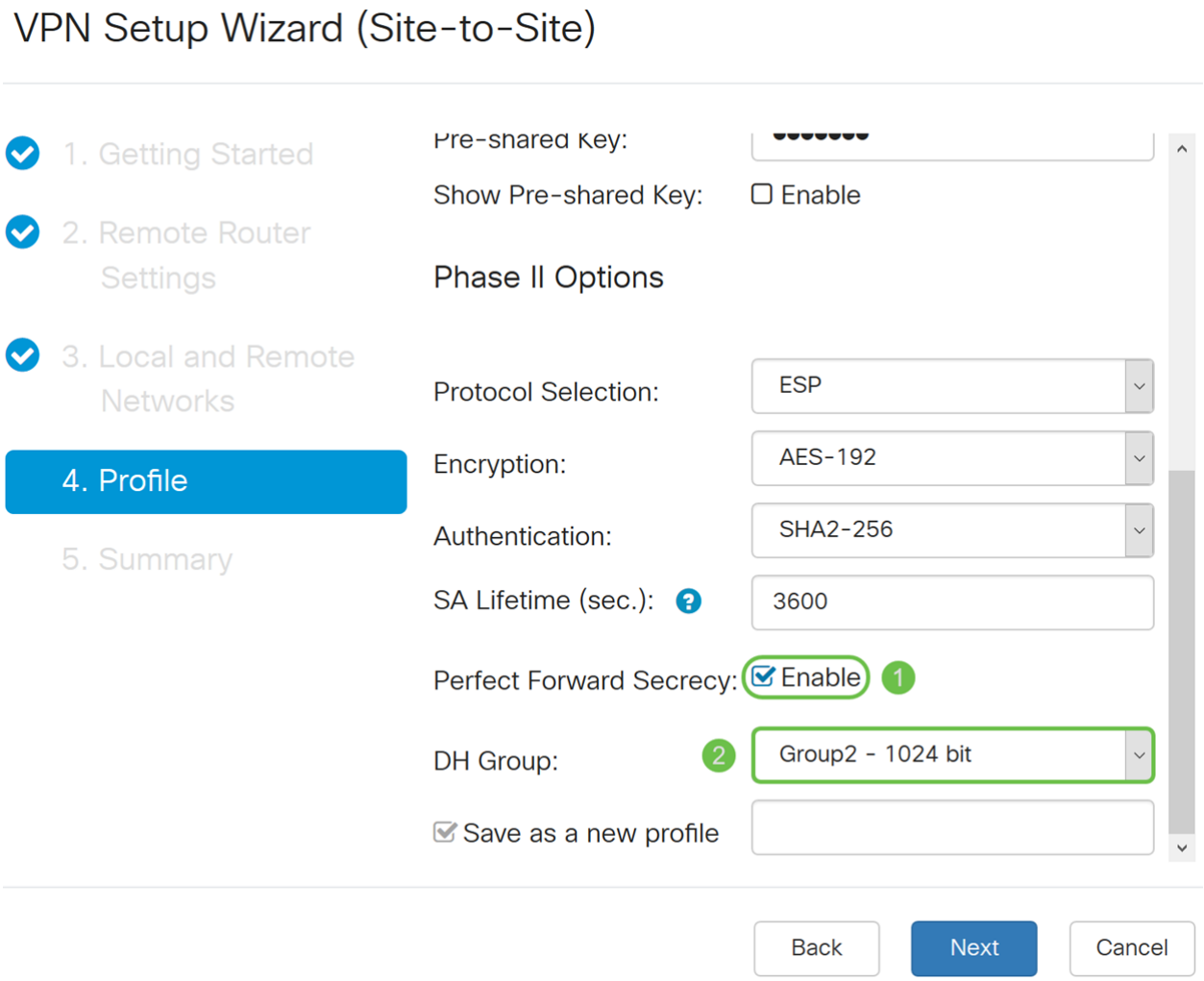
الخطوة 17. يحدد أسلوب المصادقة كيفية التحقق من صحة حزم رؤوس بروتوكول حمولة الأمان التضمين (ESP). يعتبر MD5 خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 128 بت. إن SHA1 عبارة عن خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 160 بت بينما ينتج SHA2-256 خلاصة 256 بت. يوصى بإجراء SHA2-256 لأنه أكثر أمانا. تأكد من أن كلا طرفي نفق VPN يستخدمان نفس طريقة المصادقة. حدد مصادقة (**MD5 أو SHA1** أو **SHA2-256**). تم تحديد **SHA2**-256 لهذا المثال.



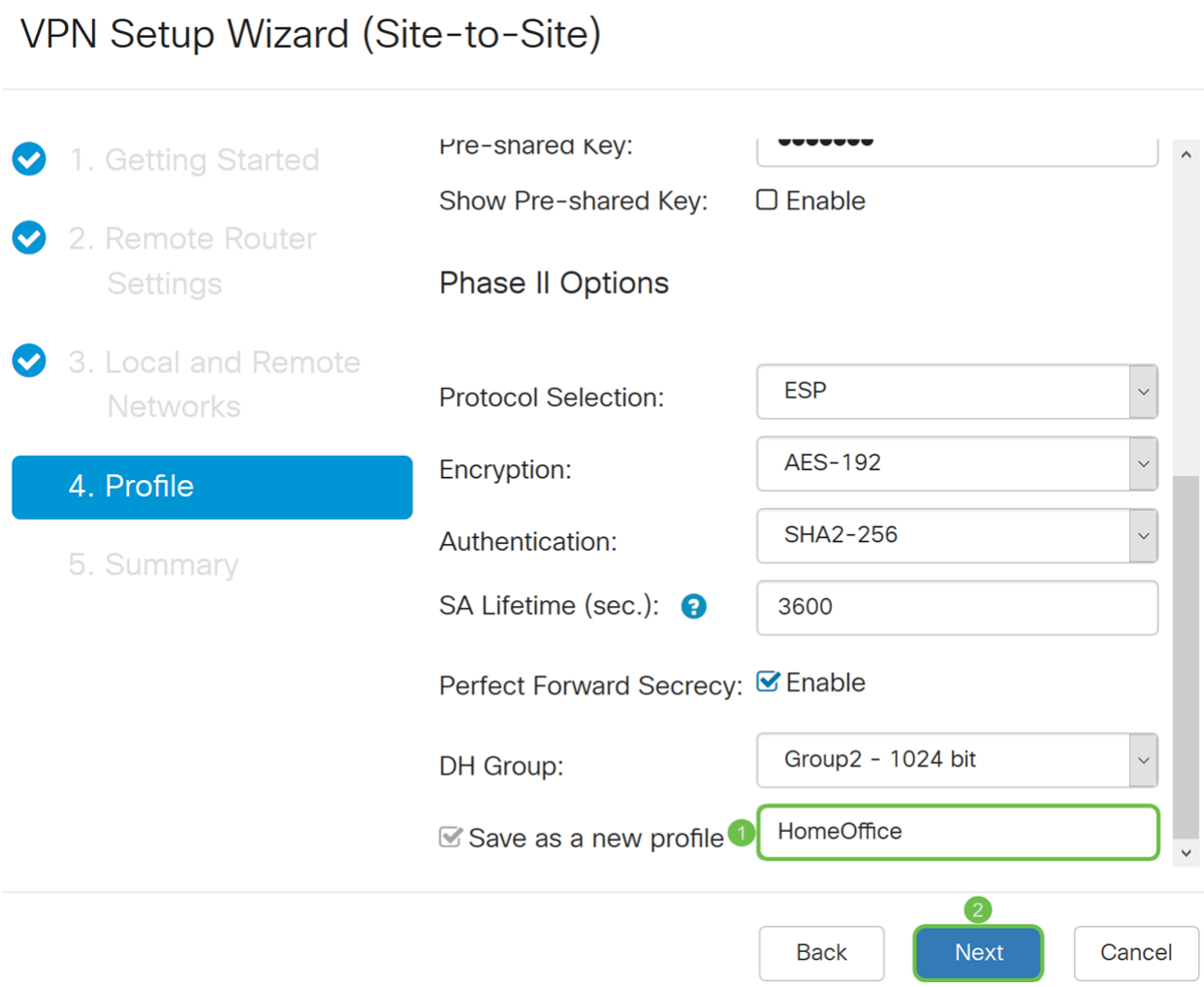
الخطوة 18. أدخل في *مدة بقاء SA (في الثانية)* وهو مقدار الوقت، بالثواني، الذي يكون فيه نفق VPN IPsec SA)) نشطا في هذه المرحلة. القيمة الافتراضية للمرحلة 2 هي 3600 ثانية.



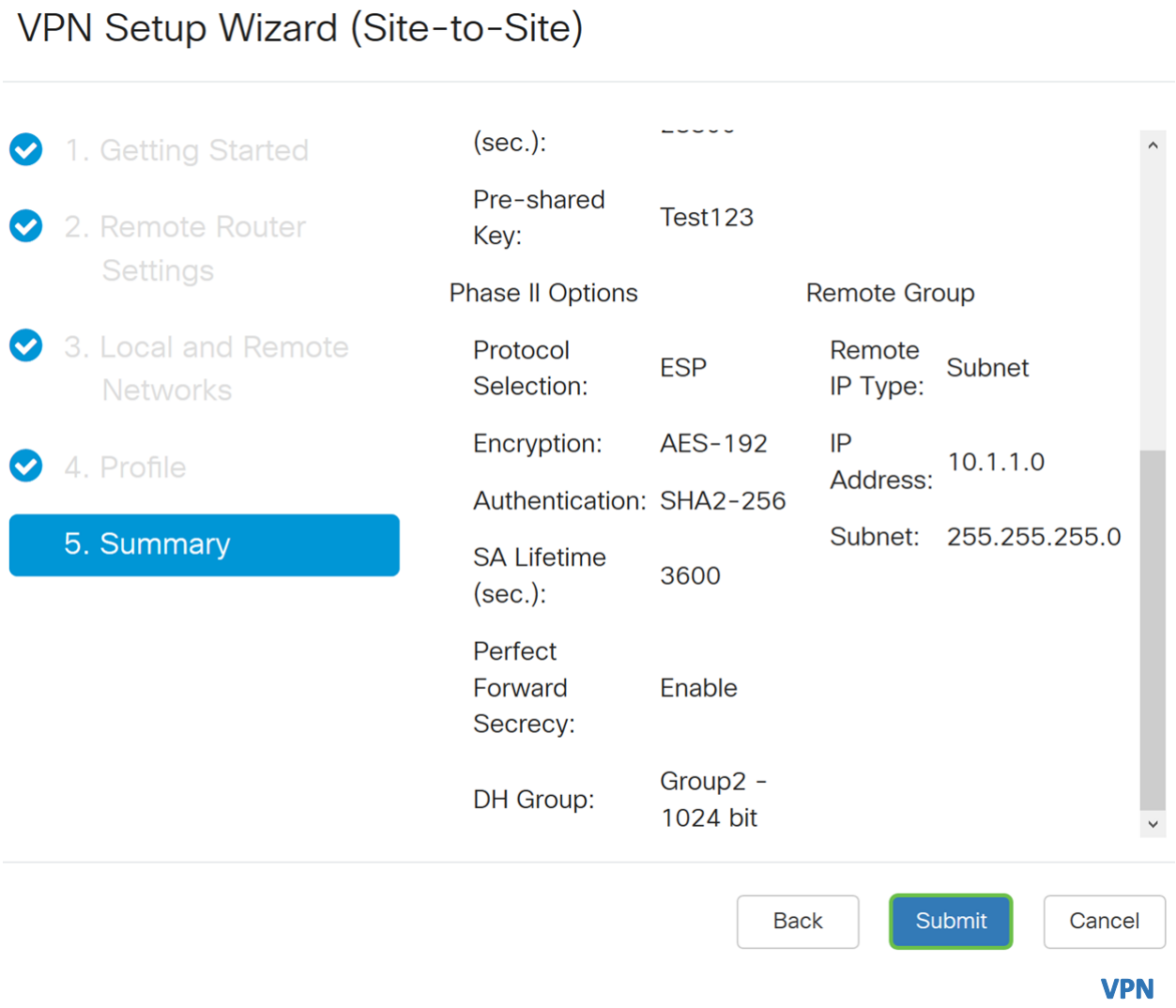
الخطوة 19. عند تمكين سرية إعادة التوجيه المثالية (PFS)، تعمل مفاوضات المرحلة 2 من IKE على إنشاء مادة أساسية جديدة لتشفير حركة مرور IPsec والمصادقة. يتم إستخدام سرية إعادة التوجيه المثالية لتحسين أمان الاتصالات المرسلة عبر الإنترنت باستخدام تشفير المفتاح العام. حدد المربع لتمكين هذه الميزة، أو قم بإلغاء تحديد المربع لتعطيل هذه الميزة. يوصى بهذه الميزة. في حالة تحديده، حدد مجموعة *DH*. في هذا المثال **يتم إستخدام** مجموعة 2 - **1024 بت**.



الخطوة 20. في *حفظ كملف تخصيص* جديد، أدخل اسم لملف التخصيص الجديد الذي أنشأته للتو. طقطقت **بعد ذلك** أن يرى خلاصة من ك VPN تشكيل.



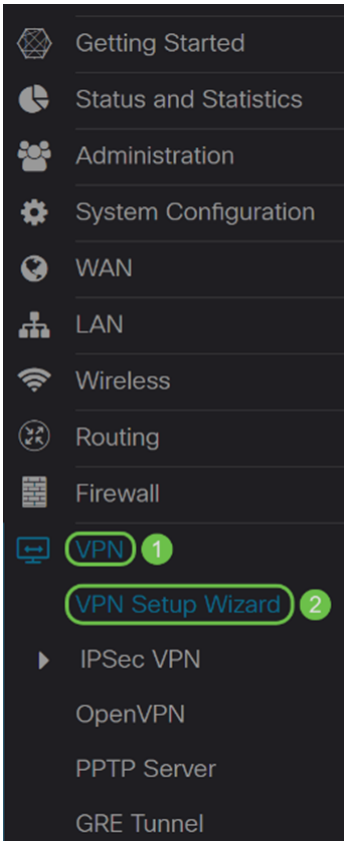
الخطوة 21. تحقق من المعلومات ثم انقر فوق **إرسال**.



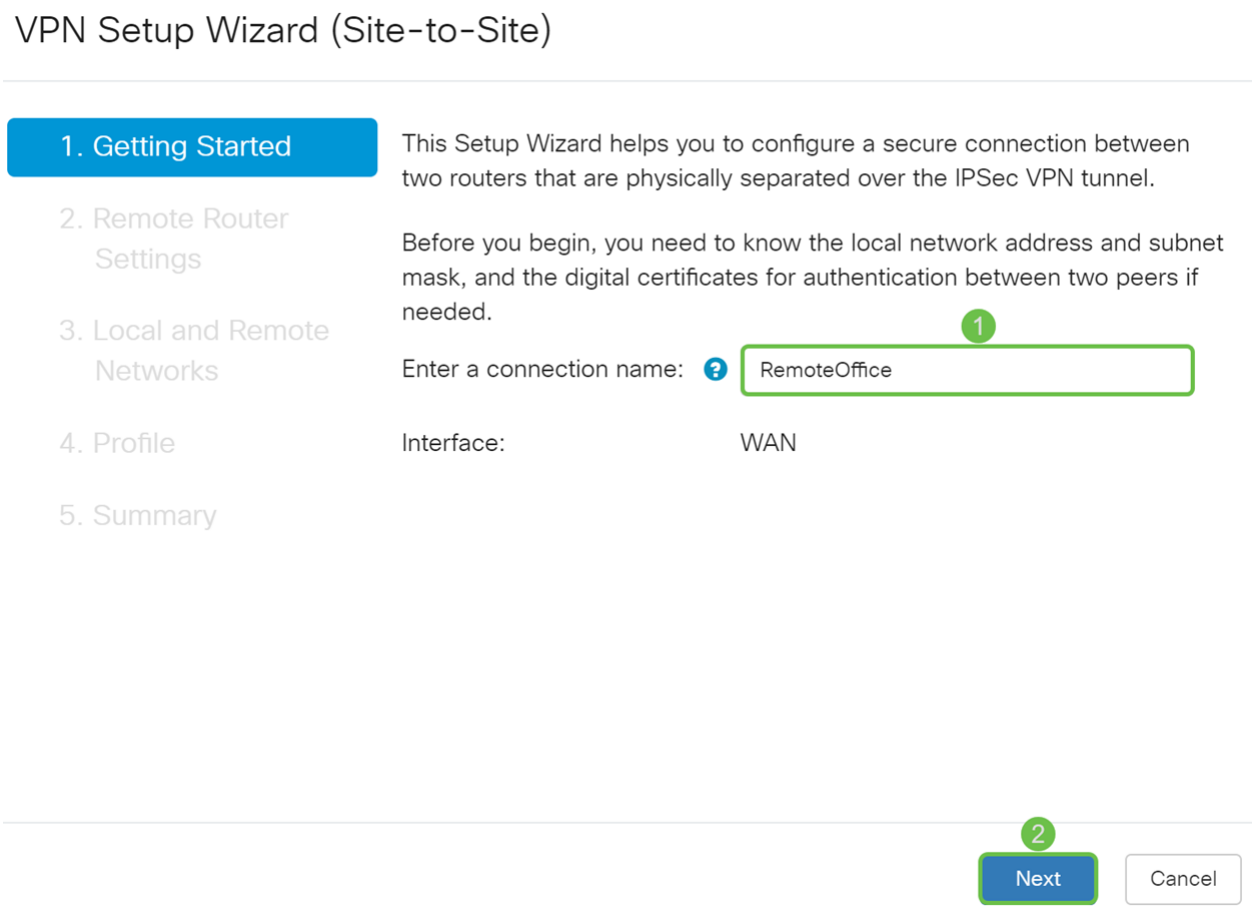
VPN

على الموجه البعيد، ستحتاج إلى تكوين إعدادات الأمان نفسها الخاصة بالموجه المحلي لديك ولكن أستخدم عنوان IP للموجه المحلي كحركة المرور عن بعد.

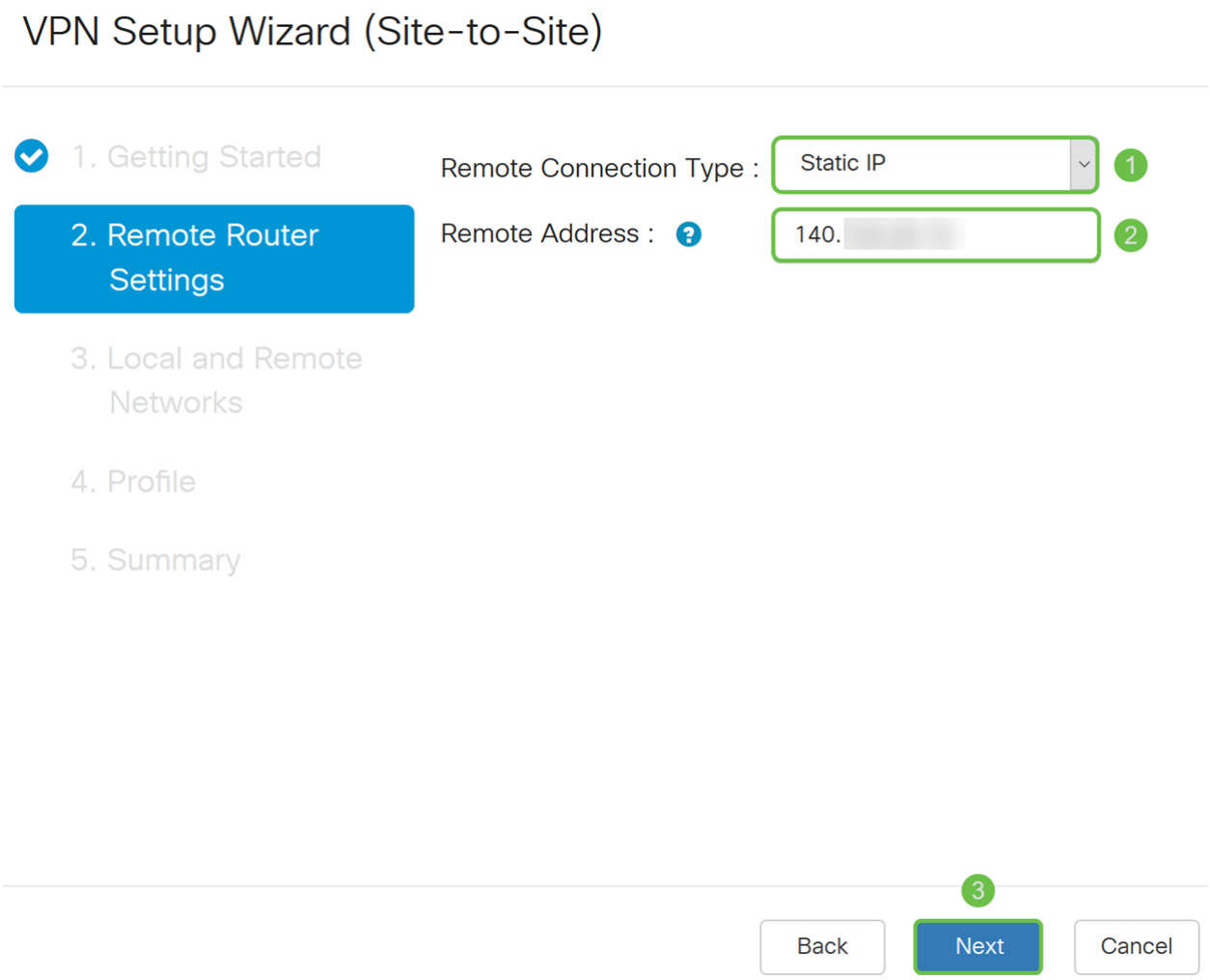
الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب على الموجه عن بعد (Router B) وانتقل إلى **معالج إعداد VPN > VPN**.



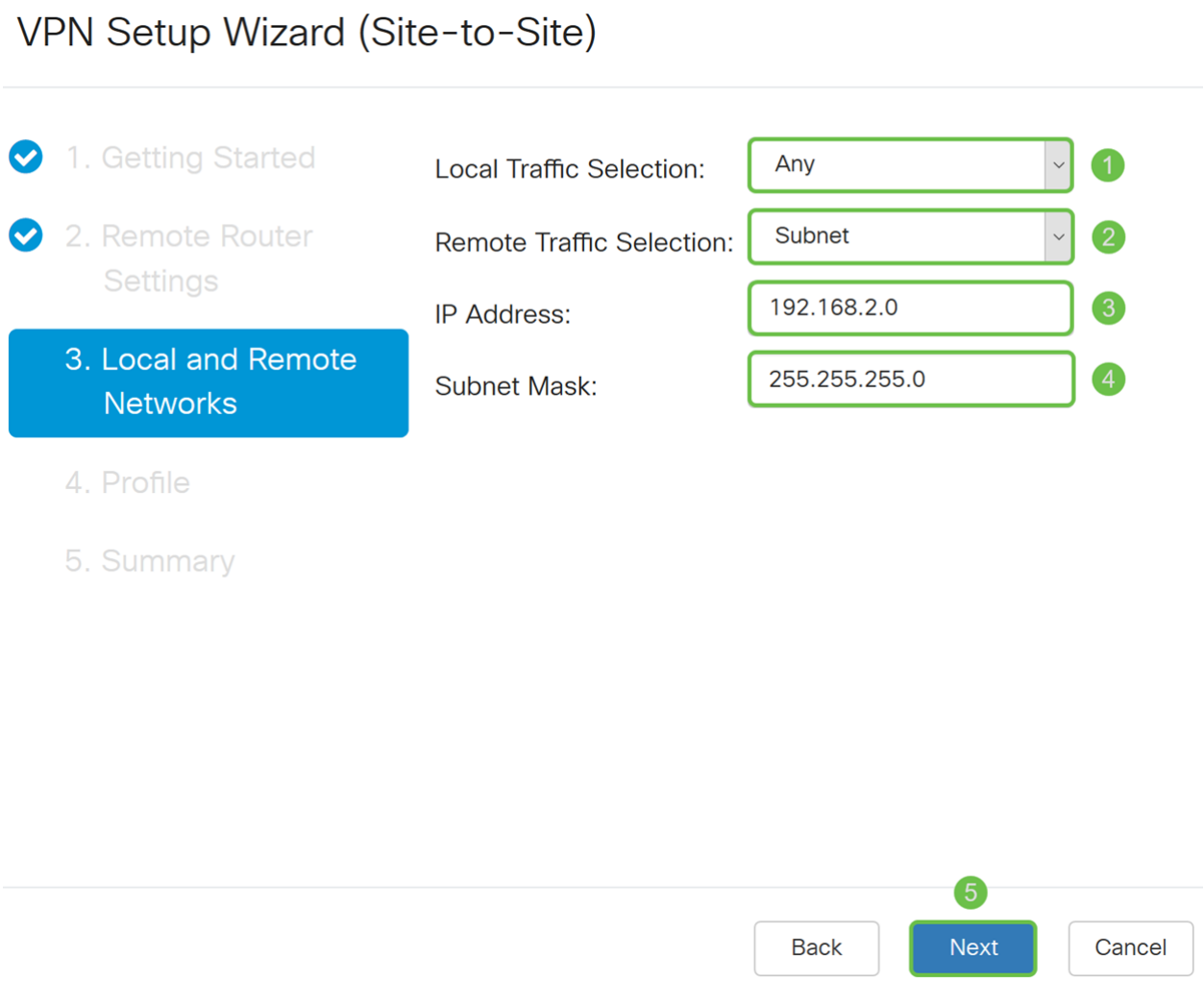
الخطوة 2. دخلت توصيل إسم واخترت القارن أن يكون استعملت ل ال VPN إن أنت تستعمل RV260. يحتوي RV160 على إرتباط WAN فقط لذلك لن تتمكن من تحديد واجهة من القائمة المنسدلة. ثم انقر فوق **التالي** للمتابعة.



الخطوة 3. في *إعدادات الموجه البعيد*، حدد *نوع الاتصال عن بعد* ثم أدخل عنوان IP لشبكة WAN للموجه A. ثم انقر فوق **التالي** للمتابعة إلى القسم التالي.

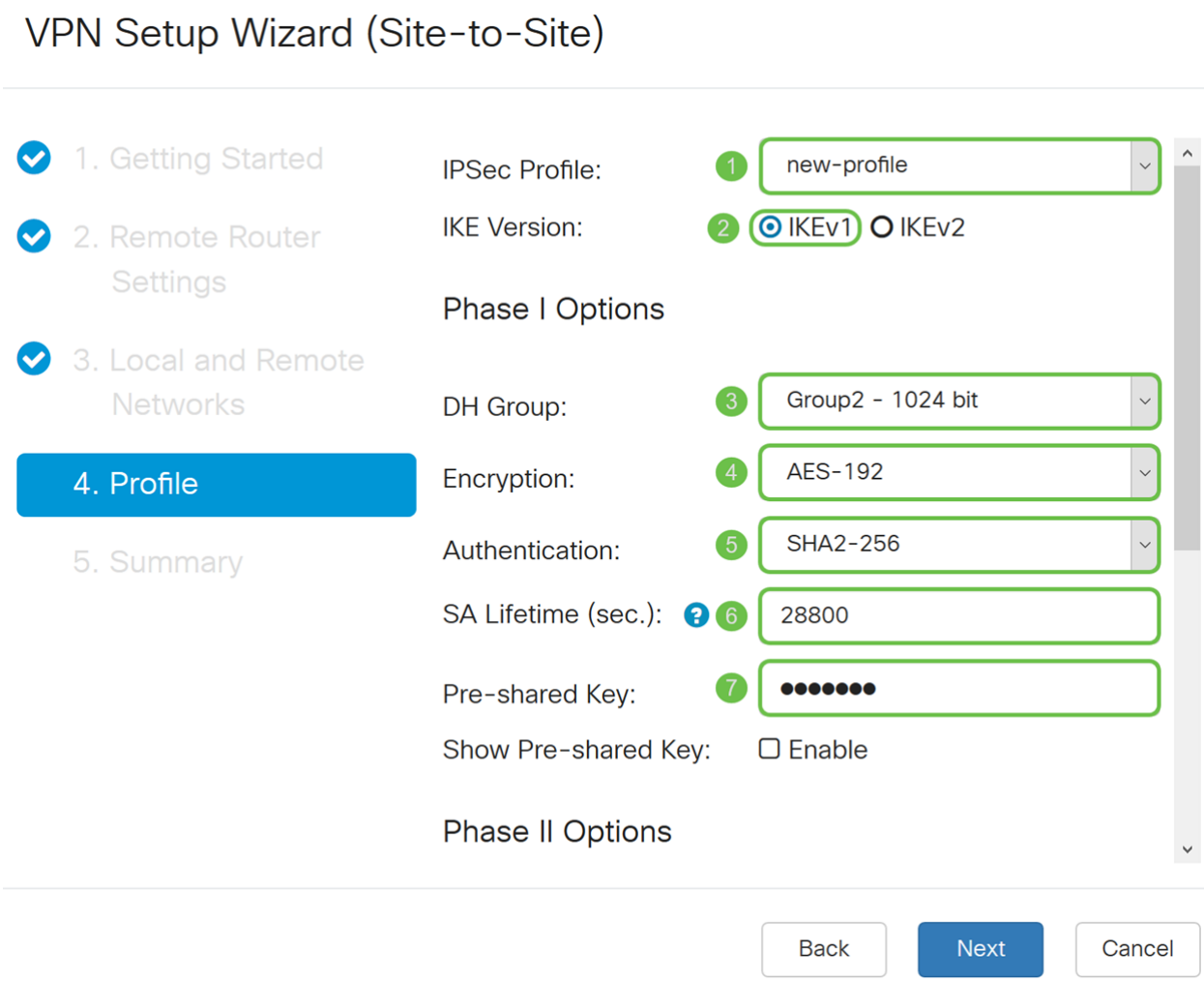


الخطوة 4. حدد حركة المرور المحلية والبعيدة. إذا كنت قد حددت **الشبكة الفرعية** في حقل *تحديد حركة مرور البيانات عن بعد*، فأدخل في الشبكة الفرعية لعنوان IP الخاص من الموجه A. ثم انقر على **التالي** لتكوين قسم *التوصيف*.

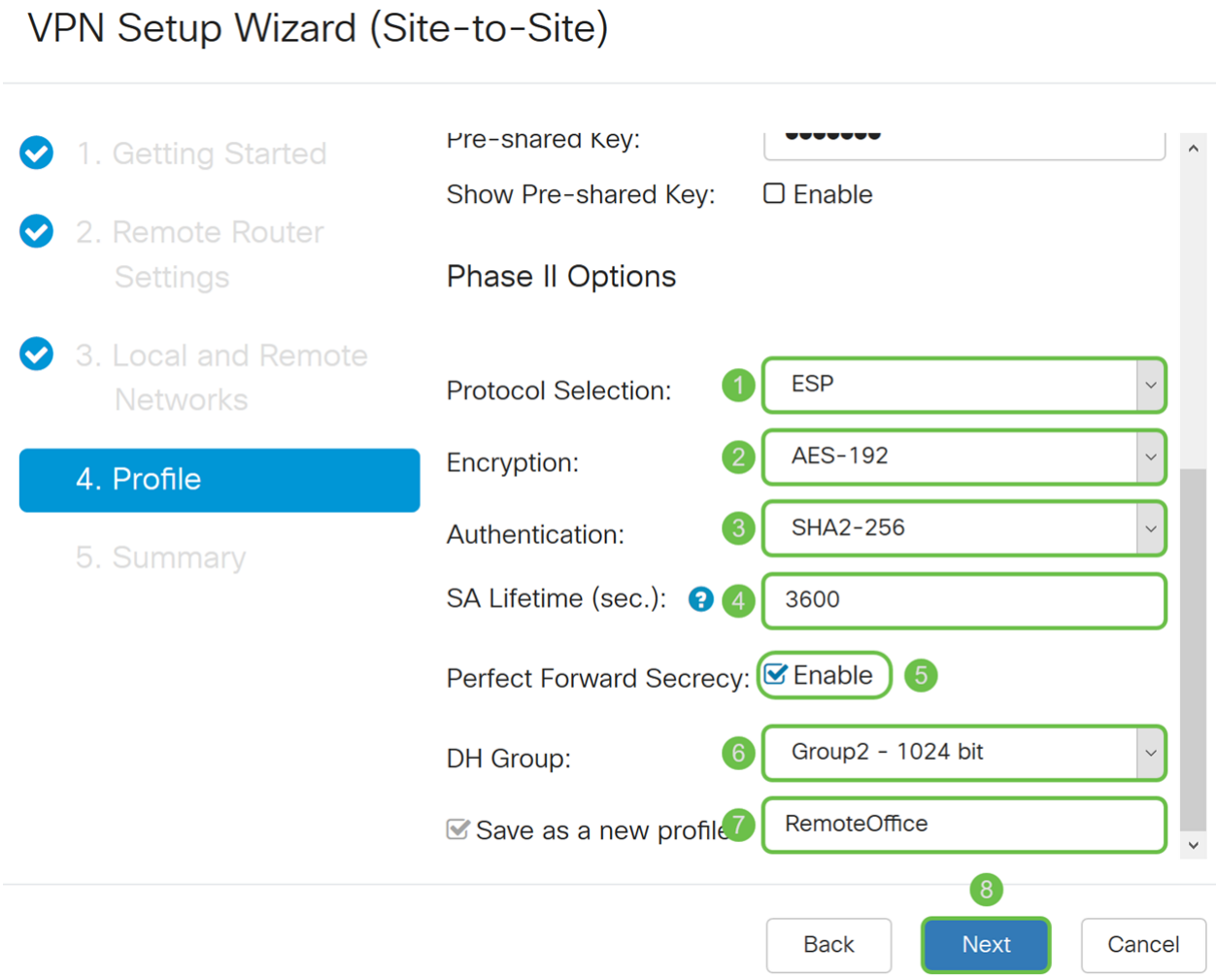


الخطوة 5. في قسم *ملف التعريف*، حدد نفس إعدادات التأمين الخاصة بالموجه A. لقد أدخلنا أيضا نفس المفتاح المشترك مسبقا مثل الموجه A. ثم انقر فوق **التالي** للانتقال إلى صفحة *الملخص*.

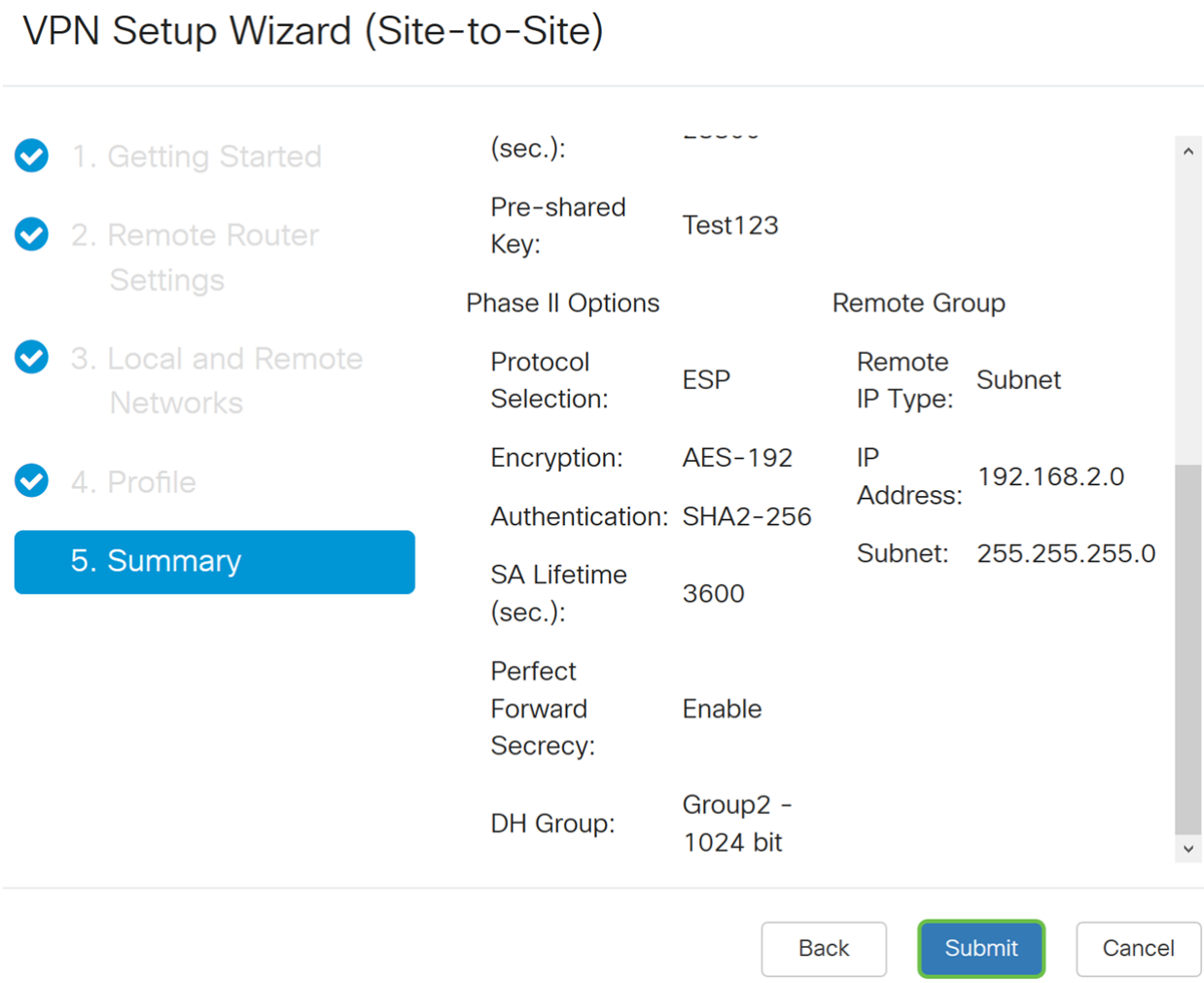
خيارات المرحلة الأولى:



خيارات المرحلة الثانية:



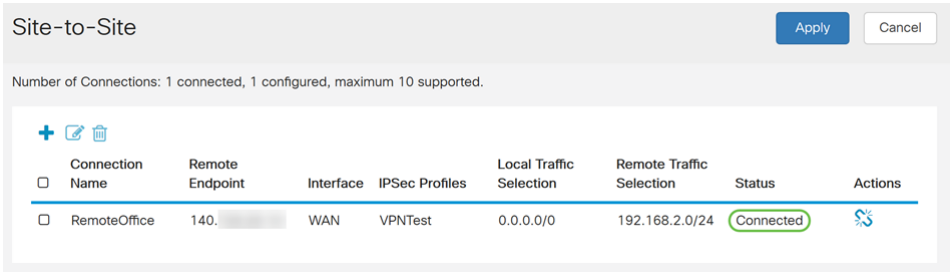
الخطوة 6. في صفحة *الملخص*، تحقق من صحة المعلومات التي قمت بتكوينها للتو. ثم انقر فوق **إرسال** لإنشاء شبكة VPN من موقع إلى موقع.



ملاحظة: توجد جميع التكوينات التي يستخدمها الموجه حاليا في ملف التكوين الجاري تشغيله والذي يكون متطايرا ولا يتم الاحتفاظ به بين عمليات إعادة التمهيد. للحفاظ على التكوين بين عمليات إعادة التمهيد، تأكد من نسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل بعد إكمال جميع التغييرات التي قمت بها. للقيام بذلك، انقر فوق الزر **حفظ** الذي يظهر في أعلى الصفحة أو انتقل إلى **إدارة > إدارة التكوين**. بعد ذلك، تأكد من أن *المصدر* يشغل التكوين *والوجهة* هي **تكوين بدء التشغيل**. طقطقة **يطبق**.

يجب أن تكون قد انتهيت بنجاح من تكوين شبكة VPN من موقع إلى موقع باستخدام معالج إعداد VPN. اتبع الخطوات التالية للتحقق من توصيل شبكة VPN من موقع إلى موقع.

الخطوة 1. للتحقق من تأسيس الاتصال، يجب أن ترى حالة *اتصال* عند التنقل إلى **VPN > IPSec VPN > موقع إلى موقع**.



الخطوة 2. انتقل إلى **الحالة والإحصاءات > حالة الشبكة الخاصة الظاهرية (VPN)** وتأكد من *تمكين* نفق الموقع إلى الموقع و*UP*.

VPN Status

Site-to-Site Tunnel Status

1 Tunnel(s) Used 9 Tunnel(s) Available

1 Tunnel(s) Enabled 1 Tunnel(s) Defined

Connection Table

Column Display Selection

No.	Name	Enable	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Action
1	RemoteOffice	Enable	UP	aes192-sha256	0.0.0.0/0	192.168.2.0/24	140.	

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).