Konfigurieren des VPN-Setup-Assistenten auf dem RV160 und dem RV260

Ziel

In diesem Dokument wird die Konfiguration des VPN-Einrichtungsassistenten auf dem RV160 und dem RV260 erläutert.

Einführung

Technologie hat sich weiterentwickelt, und Geschäfte werden häufig außerhalb des Büros abgewickelt. Geräte sind mobiler, und Mitarbeiter arbeiten häufig von zu Hause oder unterwegs. Dies kann einige Sicherheitslücken verursachen. Ein virtuelles privates Netzwerk (VPN) ist eine hervorragende Möglichkeit, externe Mitarbeiter mit einem sicheren Netzwerk zu verbinden. Mit einem VPN kann ein Remote-Host so agieren, als ob er mit dem gesicherten Netzwerk vor Ort verbunden wäre.

Ein VPN stellt eine verschlüsselte Verbindung über ein weniger sicheres Netzwerk wie das Internet her. Sie gewährleistet ein angemessenes Maß an Sicherheit für die angeschlossenen Systeme. Ein Tunnel wird als privates Netzwerk eingerichtet, das Daten sicher mit branchenüblichen Verschlüsselungs- und Authentifizierungsverfahren senden kann, um die gesendeten Daten zu schützen. Ein VPN für den Remote-Zugriff ist für die Sicherung der Verbindung in der Regel entweder auf Internet Protocol Security (IPsec) oder Secure Socket Layer (SSL) angewiesen.

VPNs bieten Layer-2-Zugriff auf das Zielnetzwerk; Dazu ist ein Tunneling-Protokoll wie Point-to-Point Tunneling Protocol (PPTP) oder Layer 2 Tunneling Protocol (L2TP) erforderlich, das über die Basis-IPsec-Verbindung ausgeführt wird. Das IPsec-VPN unterstützt Site-to-Site-VPN für einen Gateway-to-Gateway-Tunnel. So kann ein Benutzer beispielsweise den VPN-Tunnel in einer Zweigstelle so konfigurieren, dass er sich am Firmenstandort mit dem Router verbindet, sodass die Zweigstelle sicher auf das Unternehmensnetzwerk zugreifen kann. IPsec VPN unterstützt auch Client-to-Server-VPN für den Host-to-Gateway-Tunnel. Das VPN zwischen Client und Server ist nützlich, wenn von Laptop/PC von zu Hause aus über einen VPN-Server eine Verbindung mit einem Unternehmensnetzwerk hergestellt wird.

Der Router der Serie RV160 unterstützt 10 Tunnel, der Router der Serie RV260 20 Tunnel. Der VPN-Setup-Assistent führt den Benutzer bei der Konfiguration einer sicheren Verbindung für einen Site-to-Site-IPsec-Tunnel an. Dies vereinfacht die Konfiguration, indem komplexe und optionale Parameter vermieden werden, sodass jeder Benutzer den IPsec-Tunnel schnell und effizient einrichten kann.

Anwendbare Geräte

- RV160
- RV260

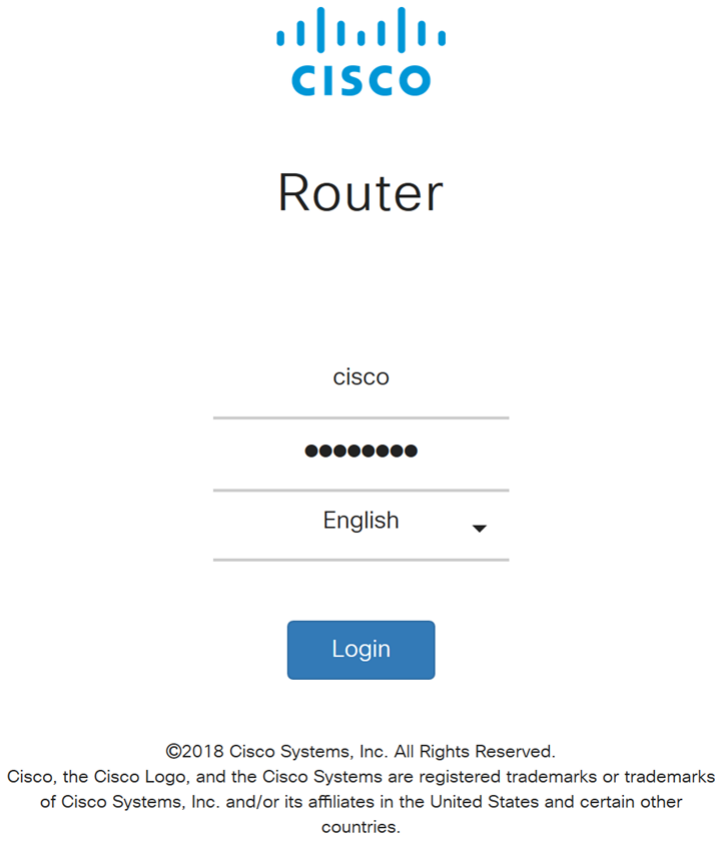
Softwareversion

- 1,0 0,13

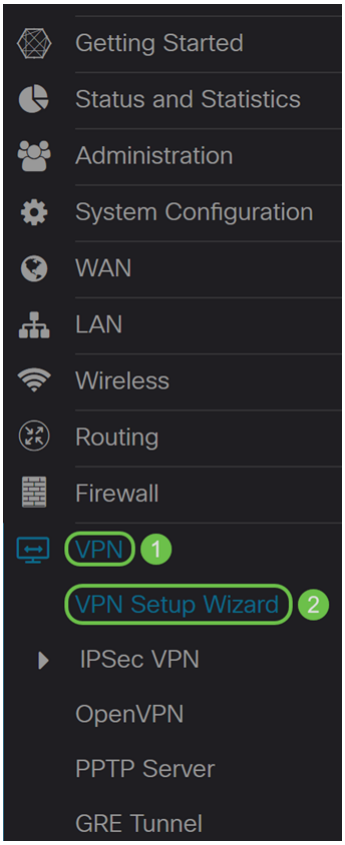
Konfiguration des VPN-Setup-Assistenten auf dem lokalen Router

Schritt 1: Melden Sie sich auf der Webseite für die Konfiguration Ihres lokalen Routers an.

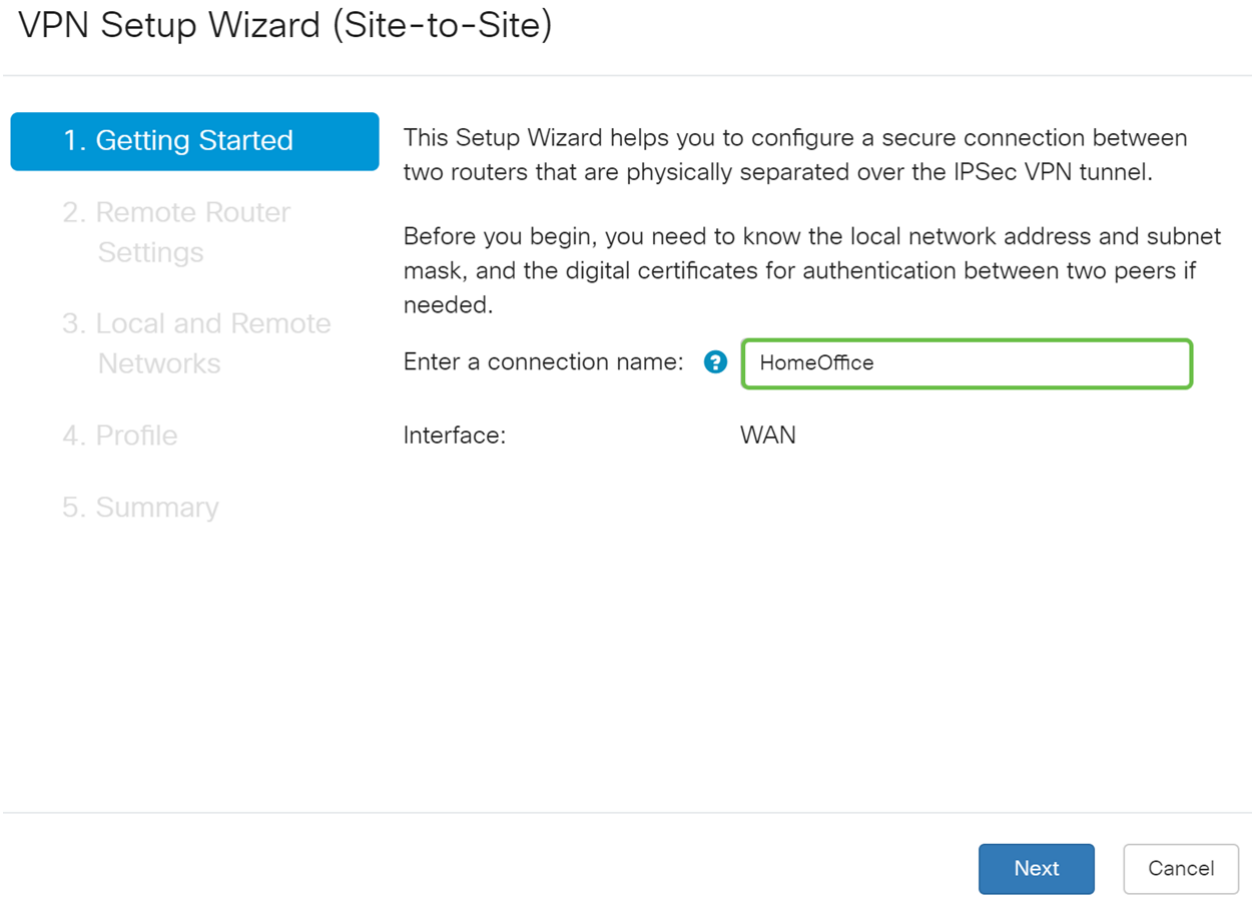
Hinweis: Der lokale Router wird als Router A und der Remote-Router als Router B bezeichnet. In diesem Dokument werden zwei RV160 verwendet, um den VPN-Setup-Assistenten zu demonstrieren.



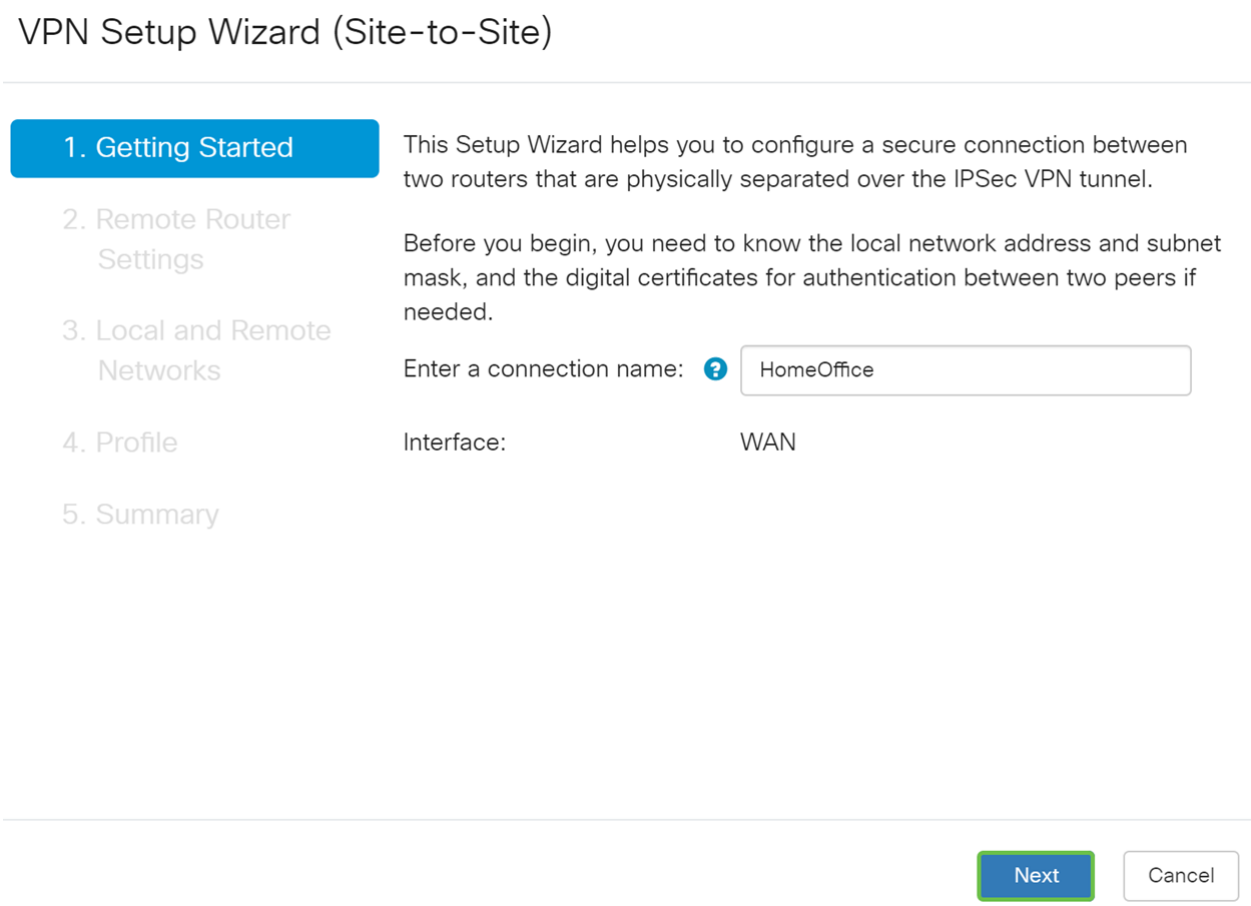
Schritt 2: Navigieren Sie zu **VPN > VPN Setup Wizard (VPN-Einrichtungsassistent)**.



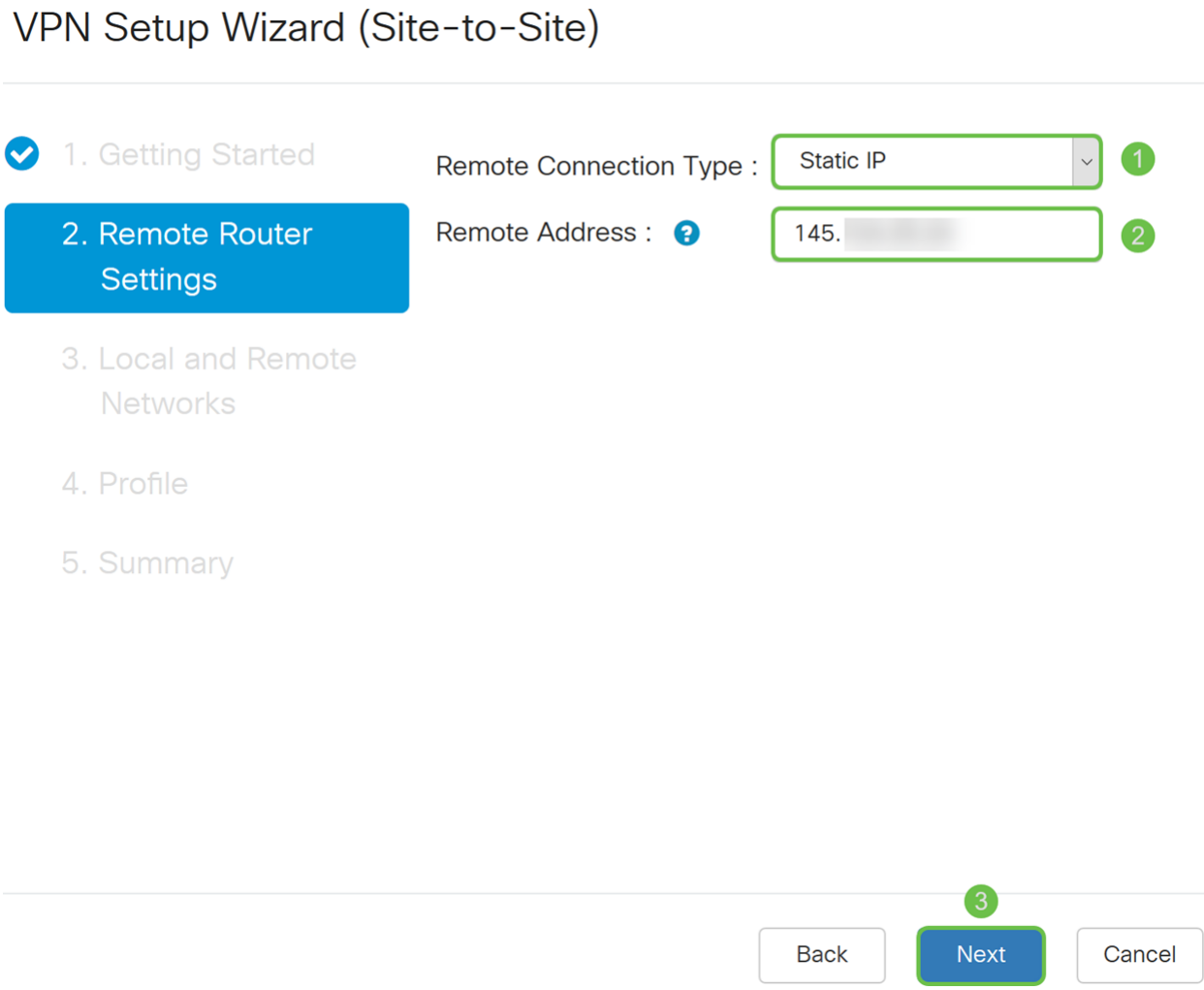
Schritt 3: Geben Sie im Abschnitt *Getting Started* (*Getting Started*) im Feld **Geben Sie einen** Verbindungsnamen ein. Wir haben in **HomeOffice** als unseren Verbindungsnamen eingegeben.



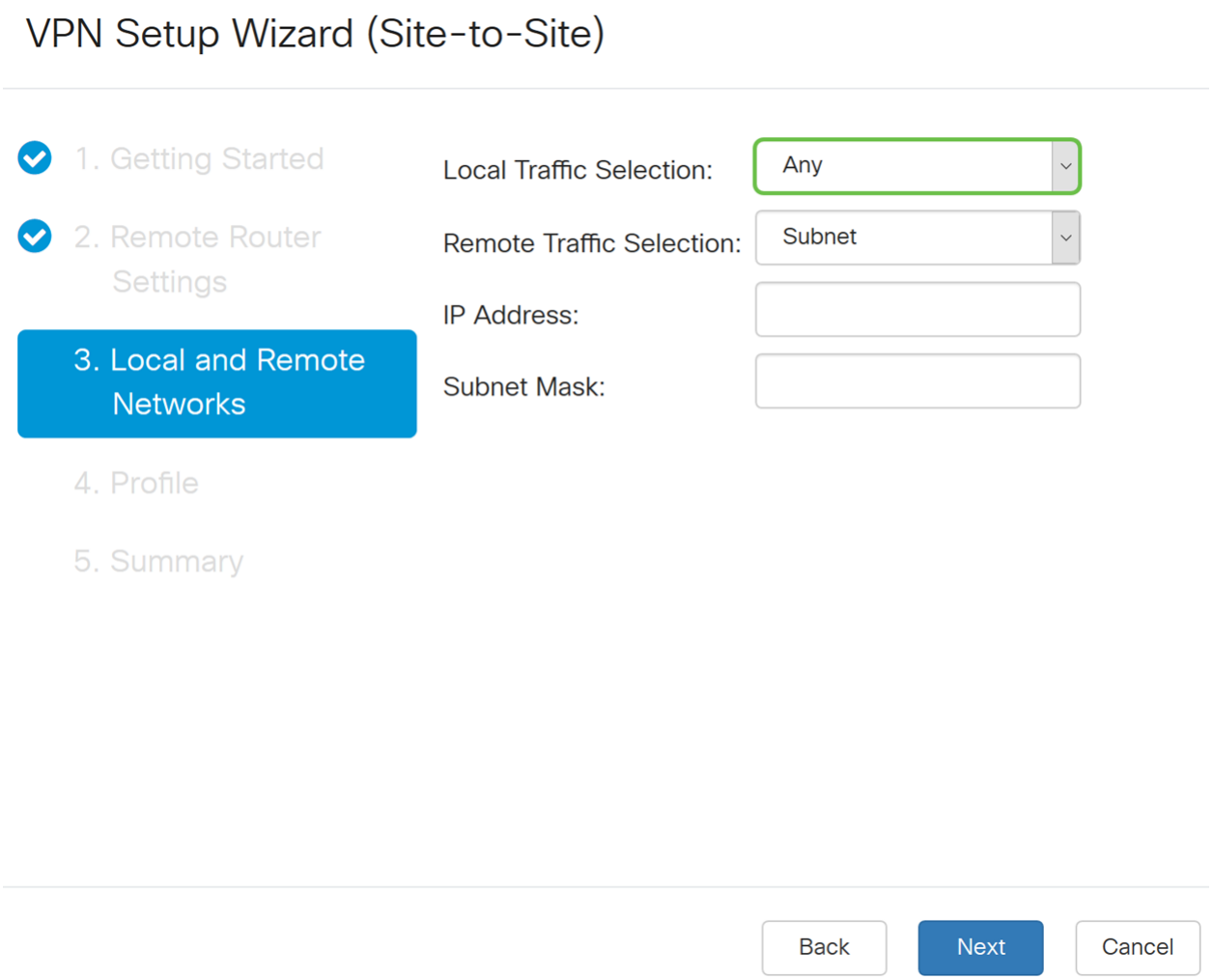
Schritt 4: Wenn Sie einen RV260 verwenden, wählen Sie im Feld "*Interface*" (Schnittstelle) aus der Dropdown-Liste eine Schnittstelle aus. Der RV160 verfügt nur über einen WAN-Link. Daher können Sie in der Dropdown-Liste keine Schnittstellen auswählen. Klicken Sie auf **Weiter**, um zum Abschnitt *Remote Router Settings* zu gelangen.



Schritt 5: Wählen Sie einen *Remote-Verbindungstyp* aus der Dropdown-Liste aus. Wählen Sie entweder **Static IP** oder **FQDN** (Fully Qualified Domain Name) aus, und geben Sie dann entweder die WAN-IP-Adresse oder den FQDN des Gateways ein, das Sie im Feld *Remote Address (Remote-Adresse) verbinden möchten*. In diesem Beispiel wurde **statische IP** ausgewählt und die WAN-IP-Adresse (Router B) des Remote-Routers eingegeben. Klicken Sie anschließend auf **Weiter**, um zum nächsten Abschnitt zu wechseln.

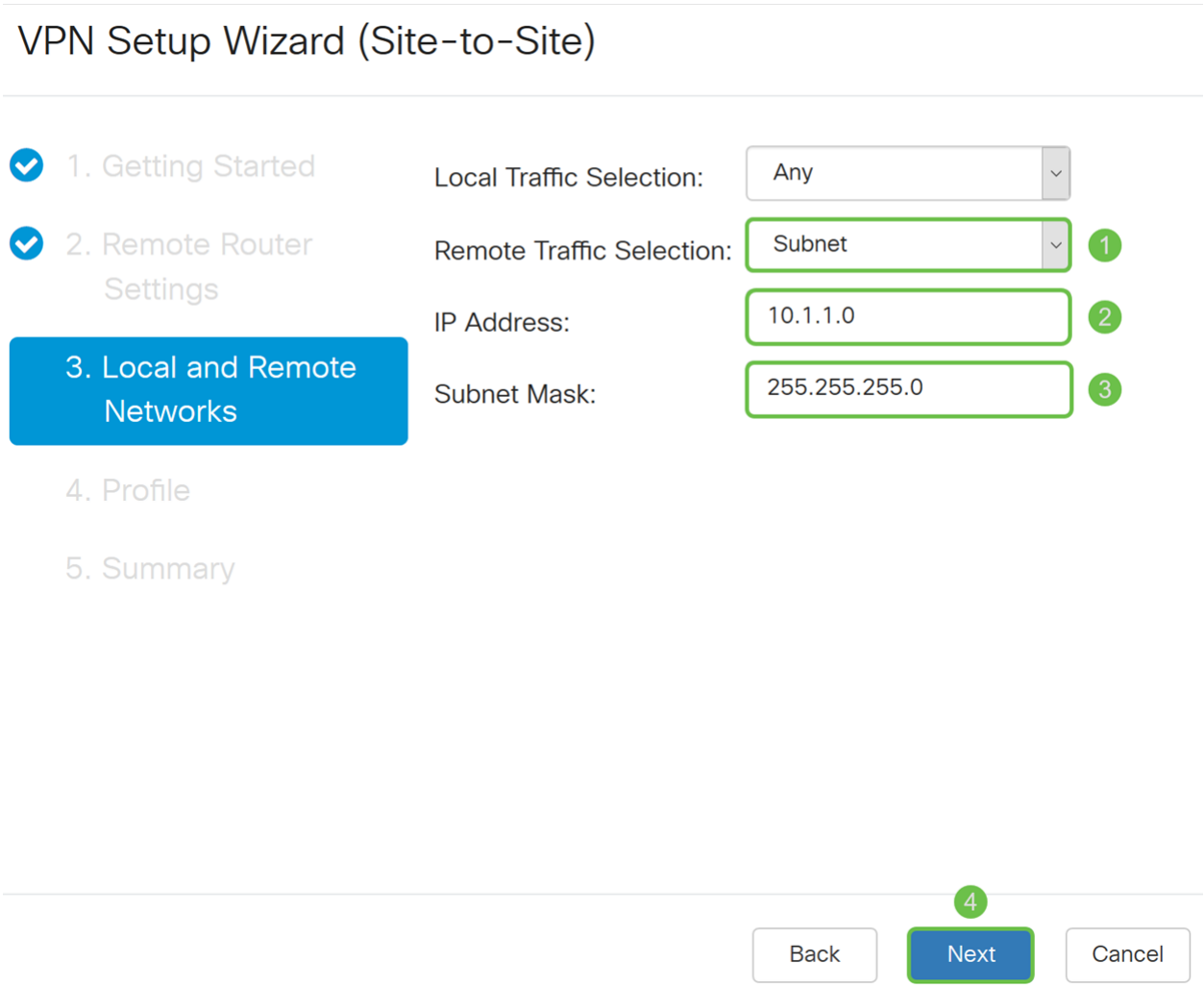


Schritt 6: Wählen Sie im Abschnitt *Lokales und Remote-Netzwerk* unter *Lokale Datenverkehrsauswahl* die lokale IP (**Subnetz, Einzel** oder **Beliebig**) aus der Dropdown-Liste aus. Wenn Sie **Subnetz** auswählen, geben Sie die Subnetz-IP-Adresse und die Subnetzmaske ein. Wenn Sie **Single** auswählen, geben Sie eine IP-Adresse ein. Wenn **Any (Beliebig)** ausgewählt wurde, fahren Sie mit dem nächsten Schritt fort, um die *Remote-Datenverkehrsauswahl* zu konfigurieren.

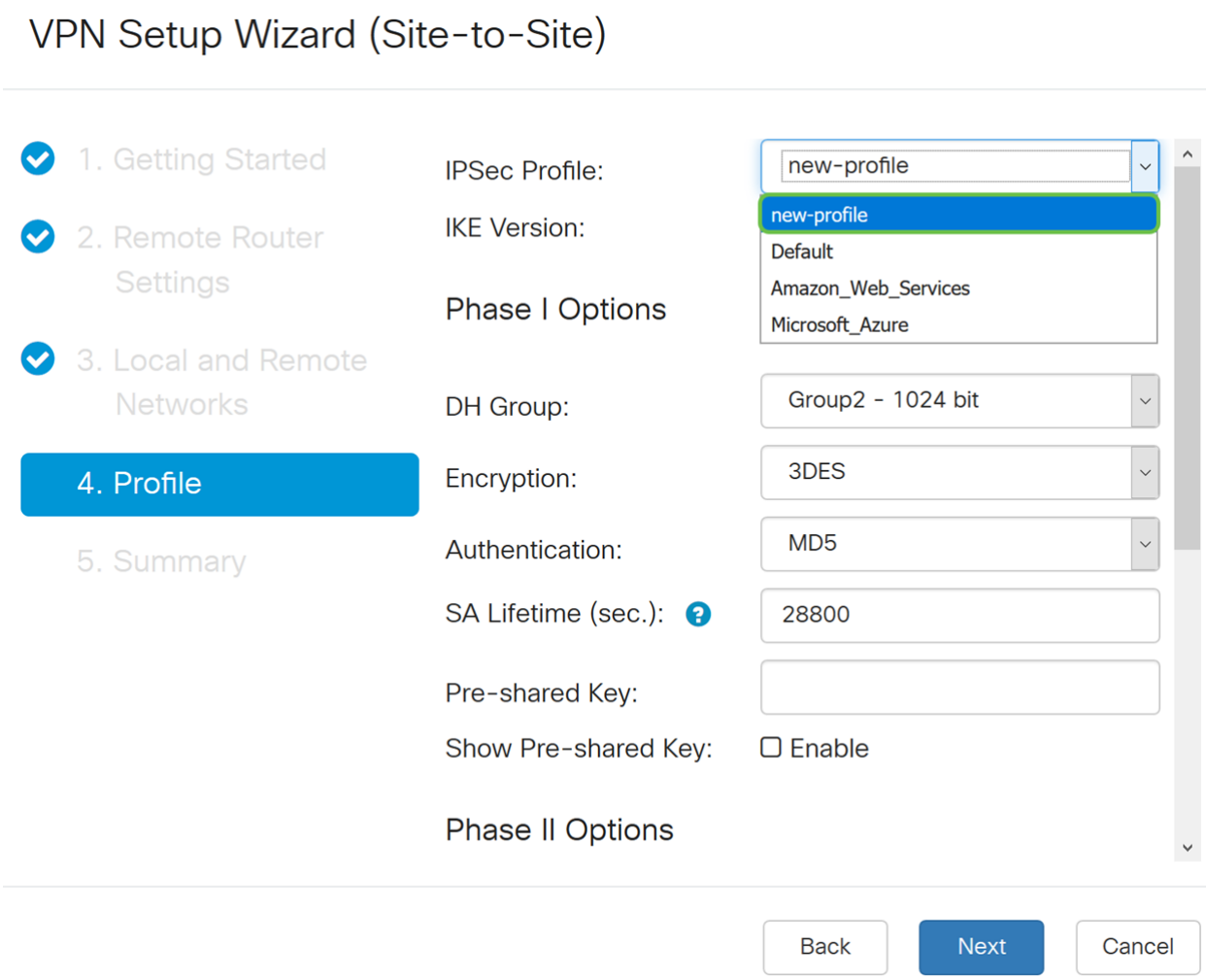


Schritt 7: Wählen Sie in der *Remote-Datenverkehrsauswahl* die *Remote-IP* (**Subnetz,Einzel**, **Beliebig) aus der Dropdown-Liste aus.** Wenn Sie **Subnetz** auswählen, geben Sie die Subnetz-IP-Adresse und die Subnetzmaske des Remote-Routers (Router B) ein. Wenn Sie **Single** auswählen, geben Sie die IP-Adresse ein. Klicken Sie anschließend auf **Weiter**, um den Abschnitt *"Profil"* zu konfigurieren.

Hinweis: Wenn Sie **Any (Beliebig)** für die *Auswahl von lokalem Datenverkehr* ausgewählt haben, müssen Sie **Subnetz** oder **Einzel** für die *Remote-Datenverkehrsauswahl* auswählen.

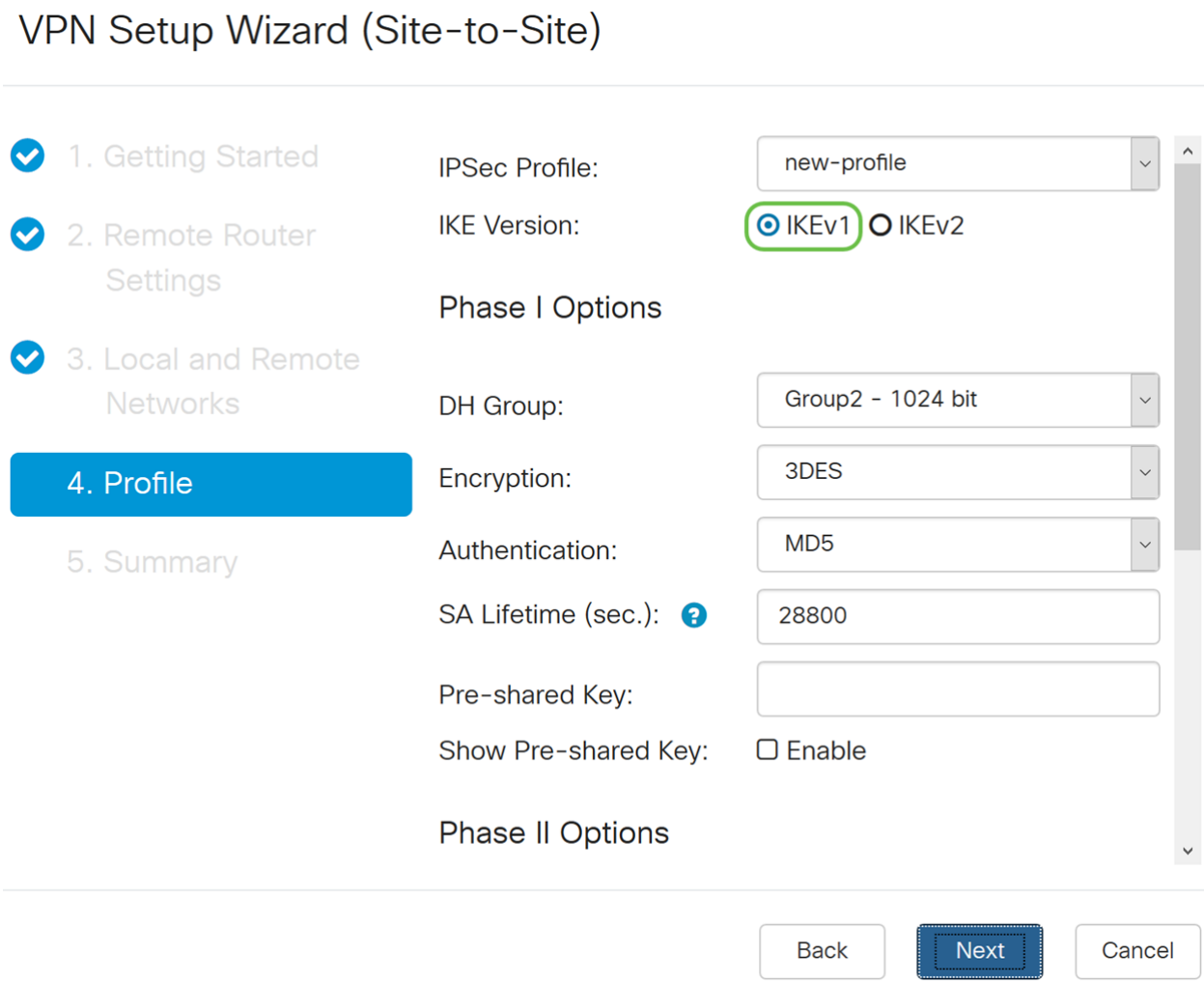


Schritt 8: Wählen Sie im Abschnitt *Profile* einen Namen für das IPsec-Profil aus der Dropdown-Liste aus. Für diese Demonstration wurde **neues Profil** als IPsec-Profil ausgewählt.



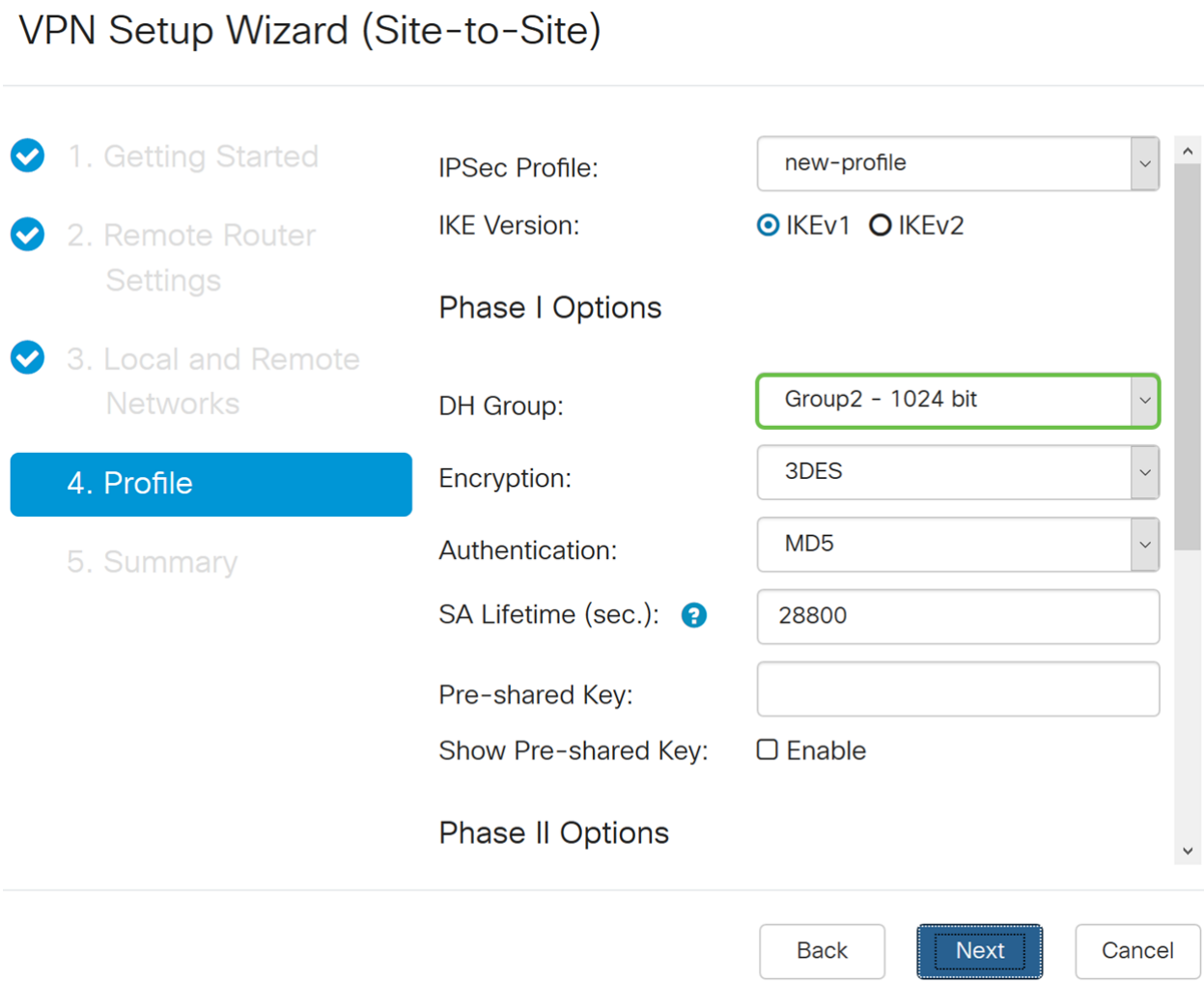
Schritt 9: Wählen Sie **IKEv1** (Internet Key Exchange Version 1) oder **IKEv2** (Internet Key Exchange Version 2) als *IKE-Version aus*. IKE ist ein Hybridprotokoll, das den Oakley-Schlüsselaustausch und den Skeme-Schlüsselaustausch innerhalb des ISAKMP-Frameworks (Internet Security Association and Key Management Protocol) implementiert. IKE stellt die Authentifizierung der IPsec-Peers bereit, handelt IPsec-Schlüssel aus und handelt IPsec-Sicherheitszuordnungen aus. IKEv2 ist effizienter, da weniger Pakete für den Schlüsselaustausch erforderlich sind und mehr Authentifizierungsoptionen unterstützt werden, während IKEv1 nur über gemeinsam genutzten Schlüssel und zertifikatbasierte Authentifizierung verfügt. In diesem Beispiel wurde **IKEv1** als unsere IKE-Version ausgewählt.

Hinweis: Wenn Ihr Gerät IKEv2 unterstützt, wird die Verwendung von IKEv2 empfohlen. Wenn Ihre Geräte IKEv2 nicht unterstützen, verwenden Sie IKEv1. Beide Router (lokal und remote) müssen die gleiche IKE-Version und die gleichen Sicherheitseinstellungen verwenden.



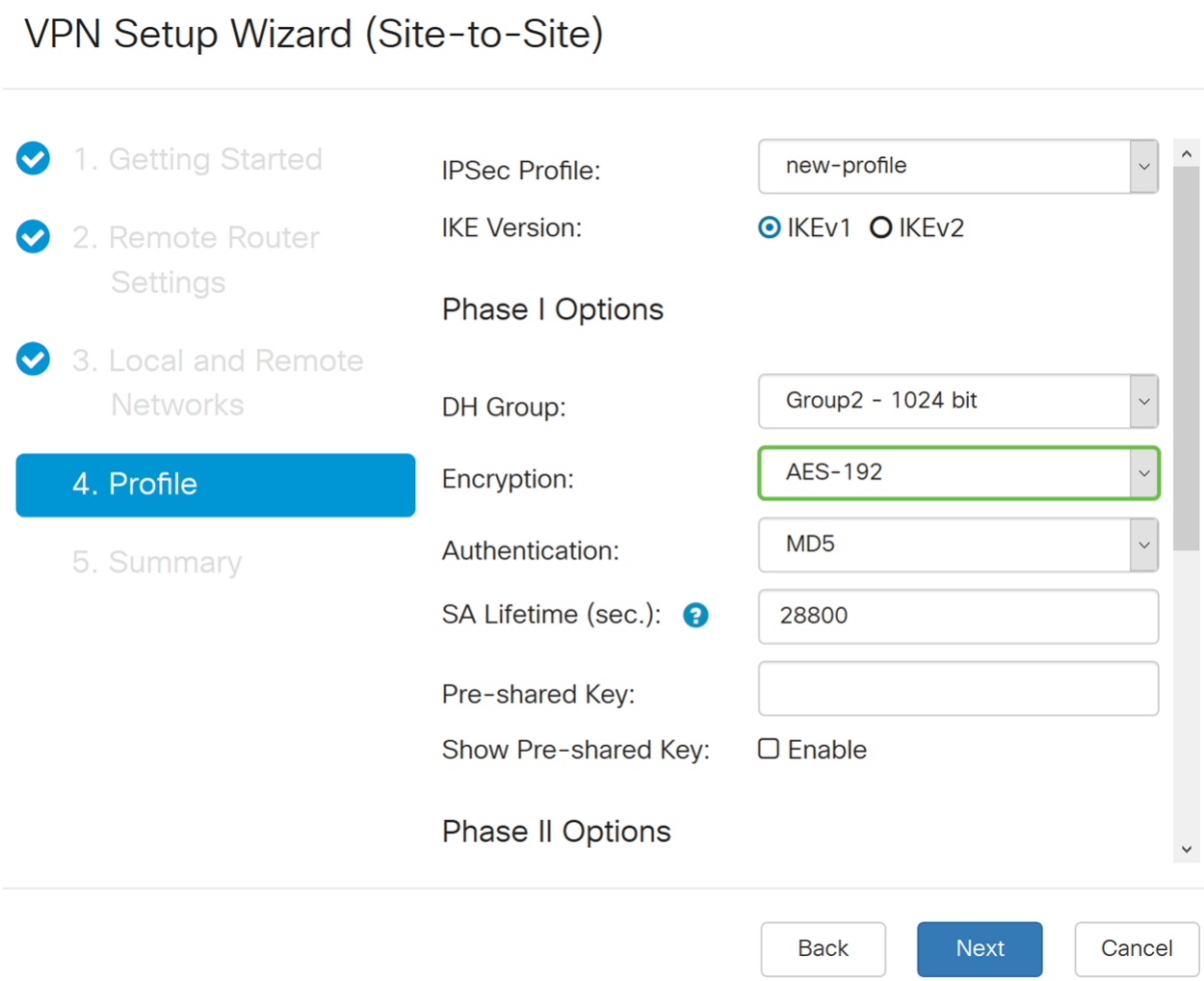
Schritt 10: Wählen Sie im Abschnitt *Phase-1-Optionen* eine DH-Gruppe (Diffie-Hellman) (**Gruppe 2 - 1024 Bit** oder **Gruppe 5 - 1536 Bit**) aus der Dropdown-Liste aus. DH ist ein Schlüsselaustauschprotokoll mit zwei Gruppen unterschiedlicher Primkey-Längen: Gruppe 2 hat bis zu 1.024 Bit, Gruppe 5 bis zu 1.536 Bit. Für diese Demonstration wird **die Gruppe 2 - 1024 Bit** verwendet.

Hinweis: Wählen Sie Gruppe 2 aus, um die Geschwindigkeit zu erhöhen und die Sicherheit zu verringern. Wählen Sie Gruppe 5 aus, um die Geschwindigkeit zu verlangsamen und die Sicherheit zu erhöhen. Gruppe 2 ist standardmäßig ausgewählt.

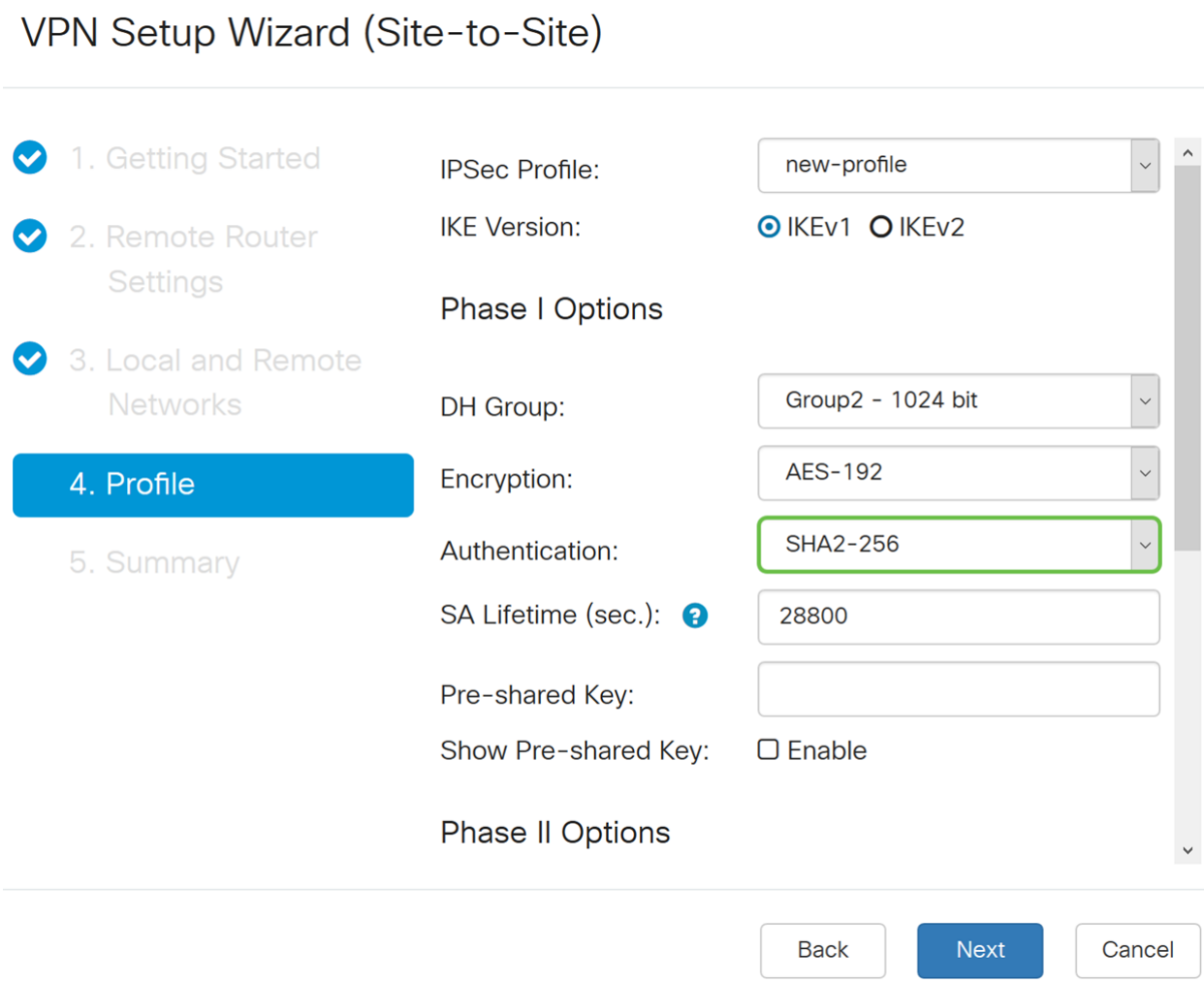


Schritt 11: Wählen Sie in der Dropdown-Liste eine Verschlüsselungsoption (**3DES, AES-128, AES-192** oder **AES-256**) aus. Diese Methode legt den Algorithmus fest, der zum Verschlüsseln oder Entschlüsseln von ESP-/ISAKMP-Paketen (Encapsulating Security Payload)/Internet Security Association- und ISAKMP-Paketen (Key Management Protocol) verwendet wird. Der Triple Data Encryption Standard (3DES) verwendet dreimal die DES-Verschlüsselung, ist aber jetzt ein Legacy-Algorithmus. Dies bedeutet, dass sie nur verwendet werden sollte, wenn es keine besseren Alternativen gibt, da sie immer noch ein marginales, aber akzeptables Sicherheitsniveau bietet. Benutzer sollten diese Daten nur dann verwenden, wenn sie für die Abwärtskompatibilität erforderlich sind, da sie für einige "Block-Kollision"-Angriffe anfällig sind. Advanced Encryption Standard (AES) ist ein Verschlüsselungsalgorithmus, der sicherer ist als DES. AES verwendet eine größere Schlüsselgröße, die sicherstellt, dass der einzige bekannte Ansatz zur Entschlüsselung einer Nachricht darin besteht, dass ein Eindringling jeden möglichen Schlüssel ausprobiert. Es wird empfohlen, AES anstelle von 3DES zu verwenden. In diesem Beispiel verwenden wir **AES-192** als Verschlüsselungsoption.

Hinweis: Hier einige weitere Ressourcen, die Ihnen helfen können: Konfigurieren der Sicherheit für VPNs mit IPSec und Verschlüsselung der nächsten Generation.

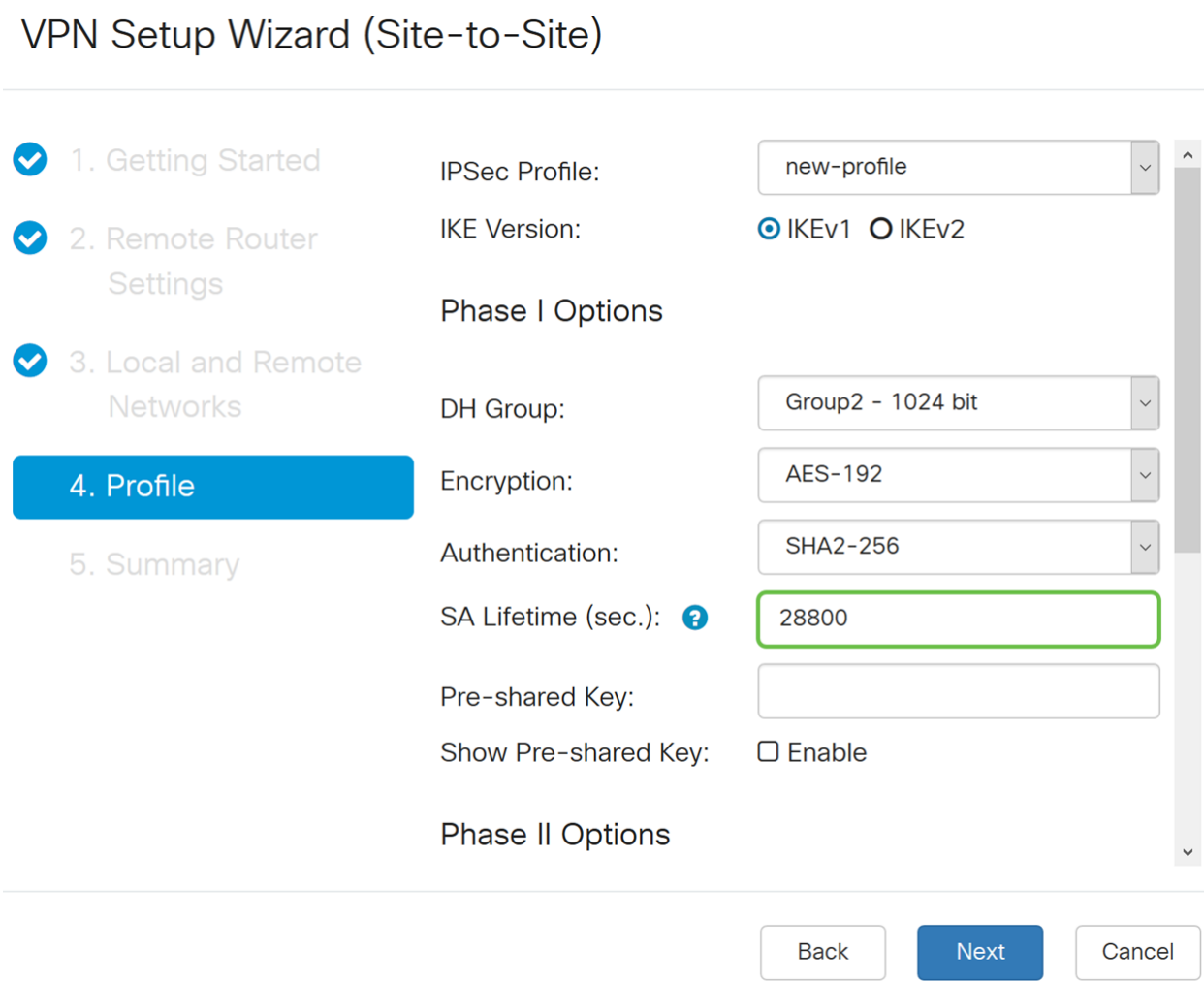


Schritt 12: Die Authentifizierungsmethode legt fest, wie die ESP-Headerpakete (Encapsulating Security Payload Protocol) validiert werden. MD5 ist ein unidirektionaler Hash-Algorithmus, der einen 128-Bit-Digest erzeugt. SHA1 ist ein unidirektionaler Hashing-Algorithmus, der ein 160-Bit-Digest erzeugt, während SHA2-256 ein 256-Bit-Digest erzeugt. SHA2-256 wird empfohlen, da es sicherer ist. Stellen Sie sicher, dass beide Enden des VPN-Tunnels dieselbe Authentifizierungsmethode verwenden. Wählen Sie eine Authentifizierung aus (**MD5, SHA1** oder **SHA2-256**). **Für** dieses Beispiel wurde **SHA2-256** ausgewählt.



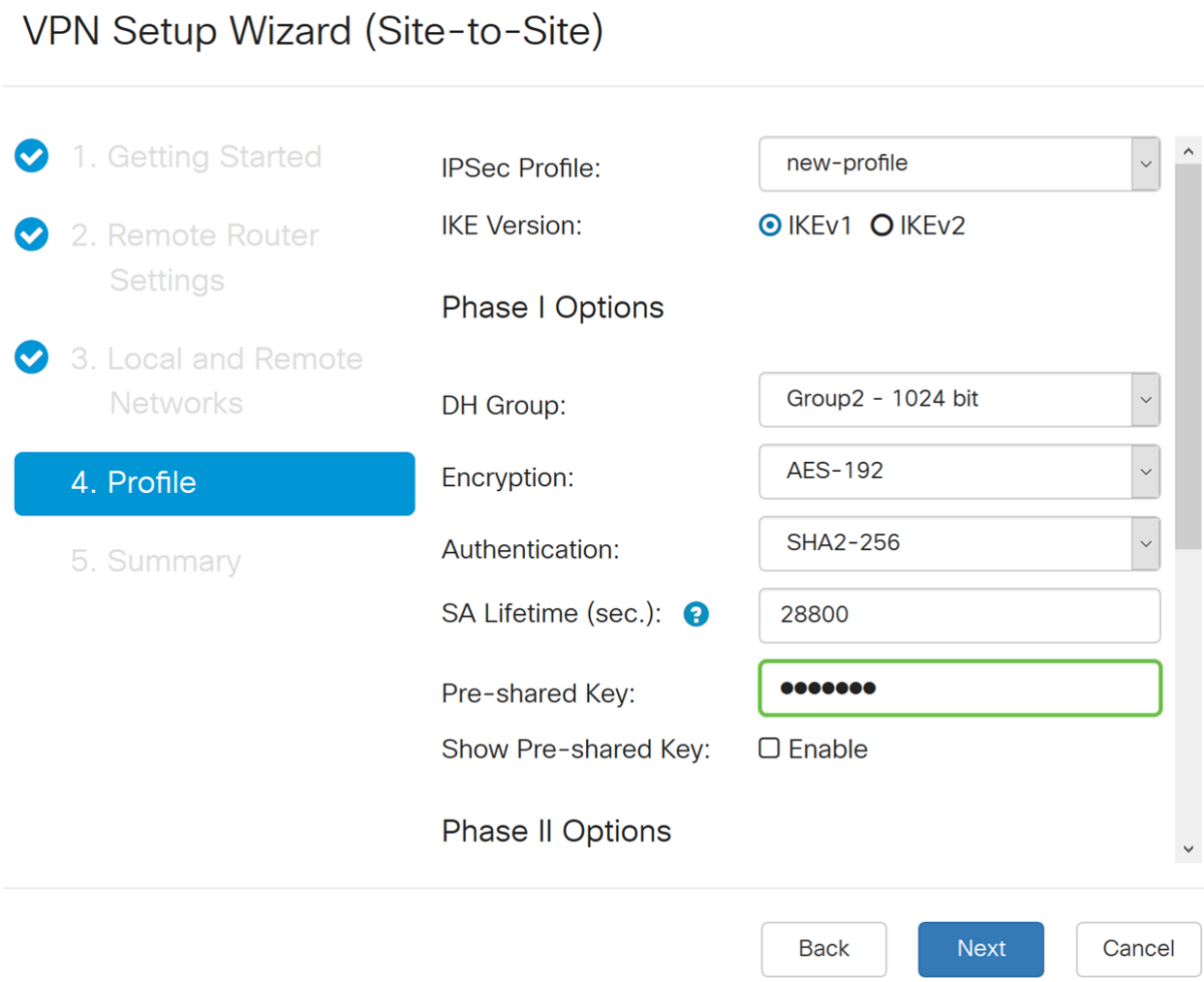
Schritt 13: Die *SA Lifetime (Sec)* gibt Ihnen die Zeitdauer (in Sekunden) an, die eine IKE SA in dieser Phase aktiv ist. Vor Ablauf der Lebensdauer wird eine neue Security Association (SA) ausgehandelt, um sicherzustellen, dass eine neue SA einsatzbereit ist, wenn die alte abläuft. Der Standardwert ist 28800 und der Bereich liegt zwischen 120 und 86400. Wir verwenden den Standardwert von **28800** Sekunden als unsere SA Lifetime für Phase I.

Hinweis: Es wird empfohlen, dass die SA-Lebensdauer in Phase I länger als die Lebensdauer der Phase II SA ist. Wenn Sie Phase I kürzer als Phase II gestalten, müssen Sie den Tunnel häufiger hin und her verhandeln als den Datentunnel. Ein Datentunnel benötigt mehr Sicherheit. Daher sollte die Lebensdauer in Phase II kürzer sein als in Phase I.



Schritt 14: Geben Sie den **Pre-shared Key ein**, der zur Authentifizierung des Remote-IKE-Peers verwendet werden soll. Sie können bis zu 30 Tastaturzeichen oder Hexadezimalwerte eingeben, z. B. My_@123 oder 4d795f40313233. An beiden Enden des VPN-Tunnels muss derselbe Pre-Shared Key verwendet werden.

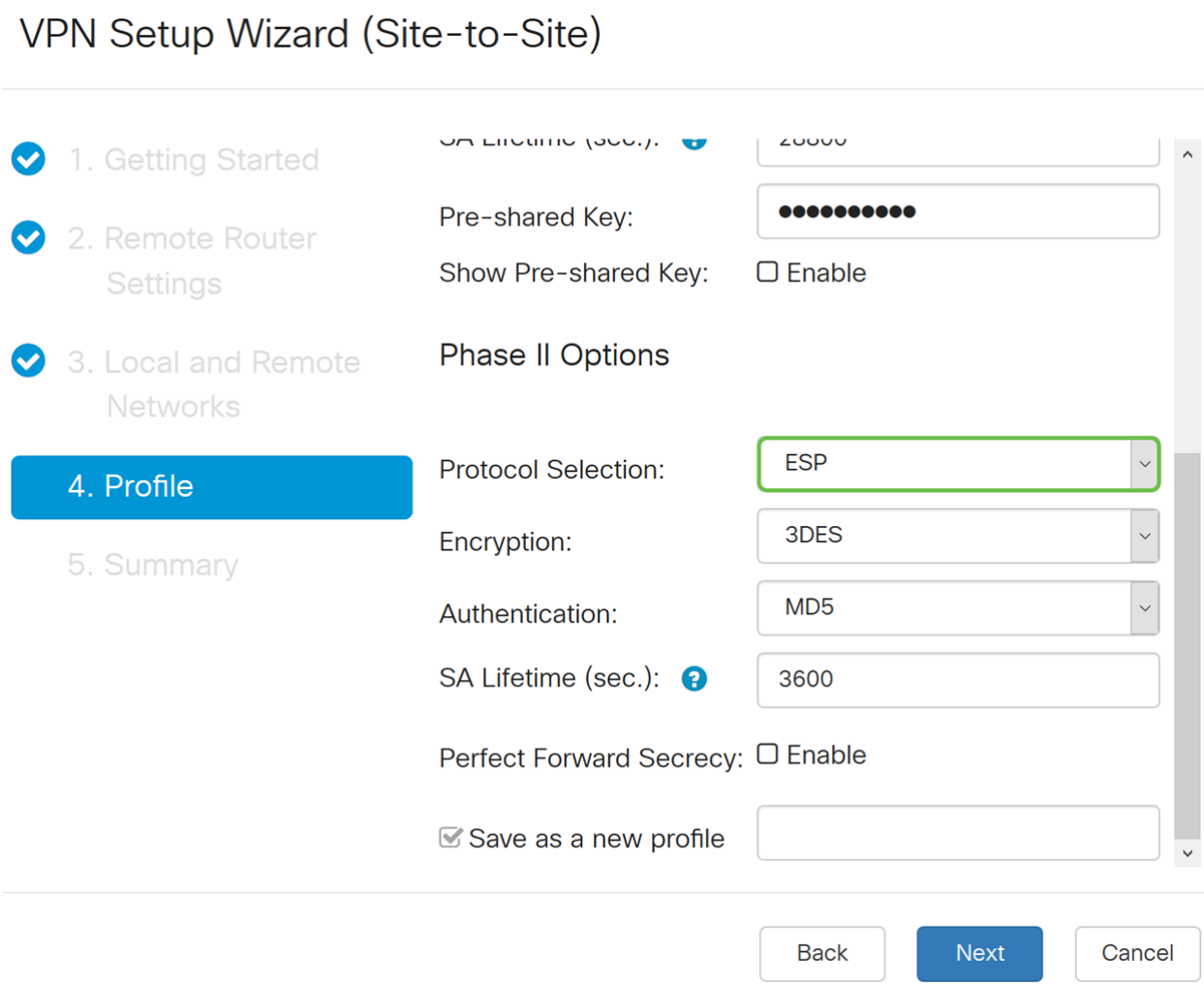
Hinweis: Wir empfehlen, den Pre-Shared Key regelmäßig zu ändern, um die VPN-Sicherheit zu maximieren.



Schritt 15: Wählen Sie im Abschnitt *Phase II-Optionen* ein Protokoll aus der Dropdown-Liste aus.

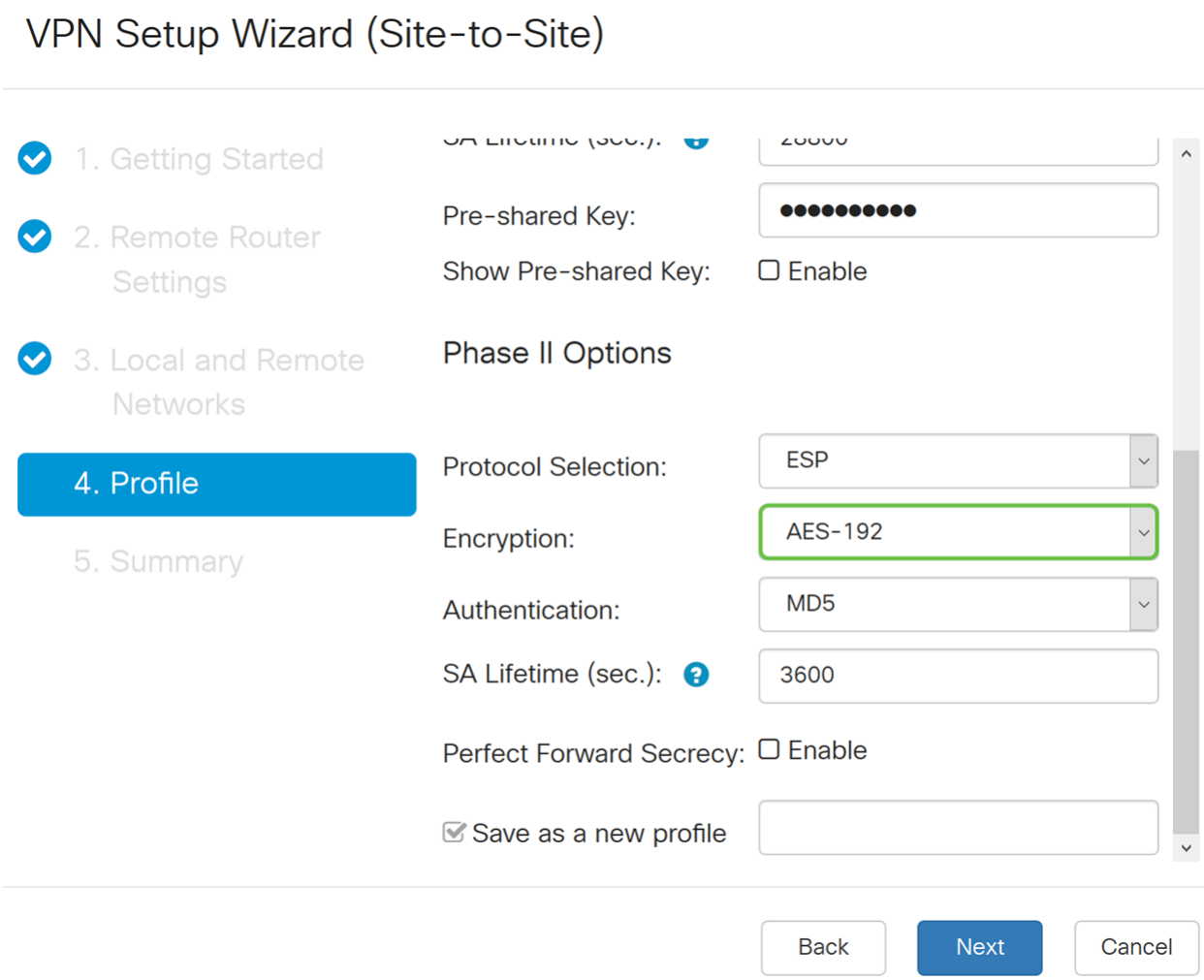
- **ESP** - Wählen Sie ESP für die Datenverschlüsselung aus, und geben Sie die Verschlüsselung ein.

- **AH** - Wählen Sie diese Option für Datenintegrität in Situationen aus, in denen Daten nicht geheim sind, aber authentifiziert werden müssen.

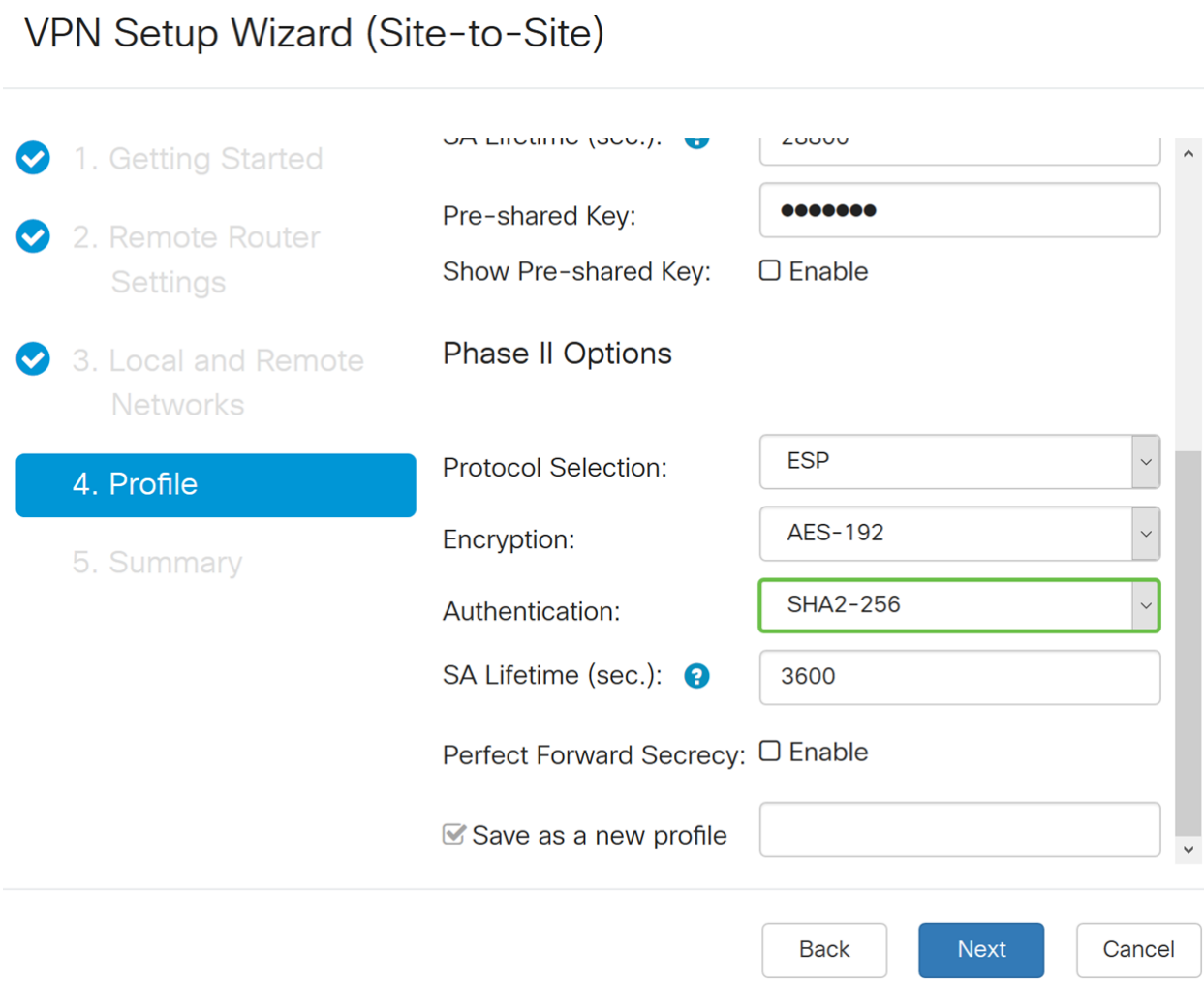


Schritt 16: Wählen Sie in der Dropdown-Liste eine Verschlüsselungsoption (**3DES, AES-128, AES-192** oder **AES-256**) aus. Diese Methode legt den Algorithmus fest, der zum Verschlüsseln oder Entschlüsseln von ESP-/ISAKMP-Paketen (Encapsulating Security Payload)/Internet Security Association- und ISAKMP-Paketen (Key Management Protocol) verwendet wird. Der Triple Data Encryption Standard (3DES) verwendet dreimal die DES-Verschlüsselung, ist aber jetzt ein Legacy-Algorithmus. Dies bedeutet, dass sie nur verwendet werden sollte, wenn es keine besseren Alternativen gibt, da sie immer noch ein marginales, aber akzeptables Sicherheitsniveau bietet. Benutzer sollten diese Daten nur dann verwenden, wenn sie für die Abwärtskompatibilität erforderlich sind, da sie für einige "Block-Kollision"-Angriffe anfällig sind. Advanced Encryption Standard (AES) ist ein Verschlüsselungsalgorithmus, der sicherer ist als DES. AES verwendet eine größere Schlüsselgröße, die sicherstellt, dass der einzige bekannte Ansatz zur Entschlüsselung einer Nachricht darin besteht, dass ein Eindringling jeden möglichen Schlüssel ausprobiert. Es wird empfohlen, AES anstelle von 3DES zu verwenden. In diesem Beispiel verwenden wir **AES-192** als Verschlüsselungsoption.

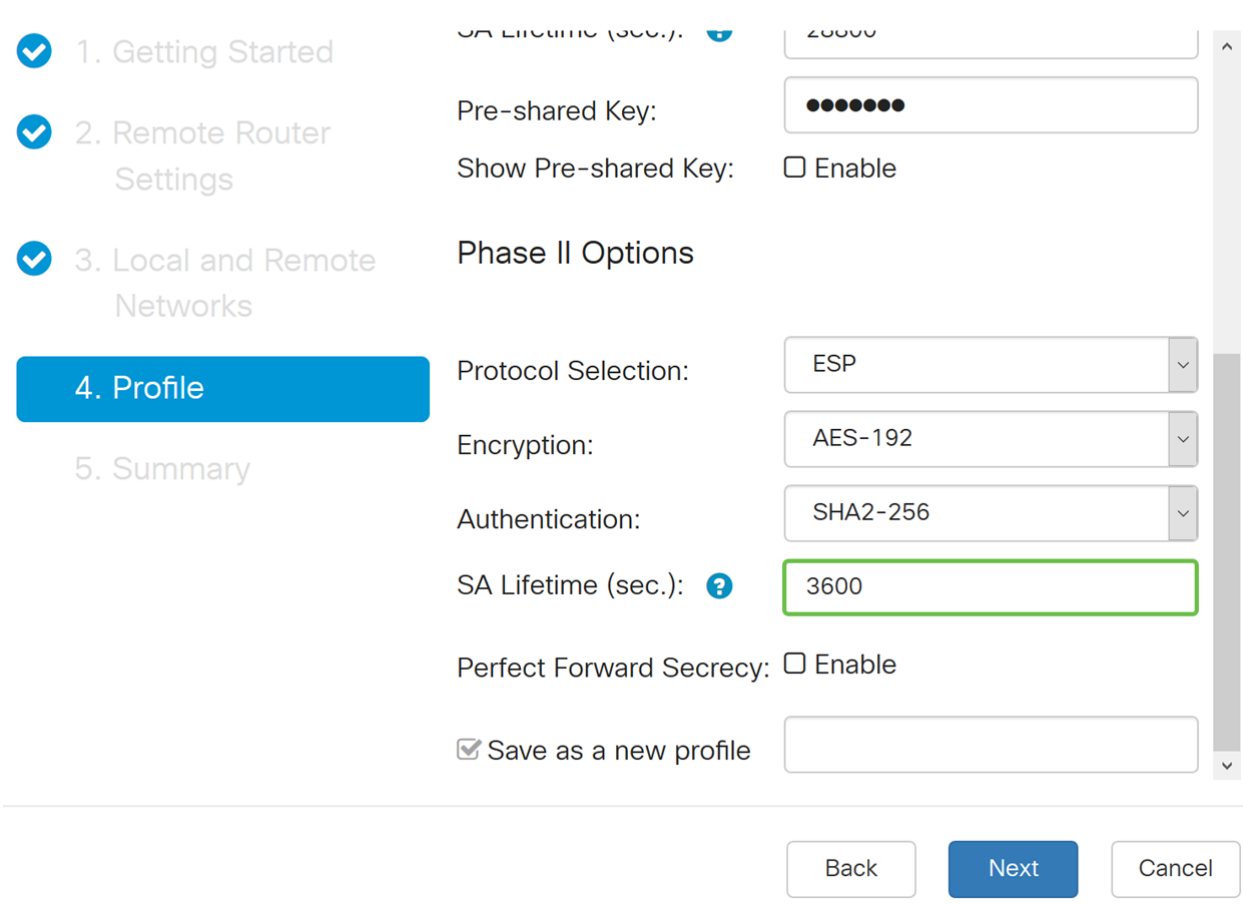
Hinweis: Hier einige weitere Ressourcen, die Ihnen helfen können: Konfigurieren der Sicherheit für VPNs mit IPSec und Verschlüsselung der nächsten Generation.



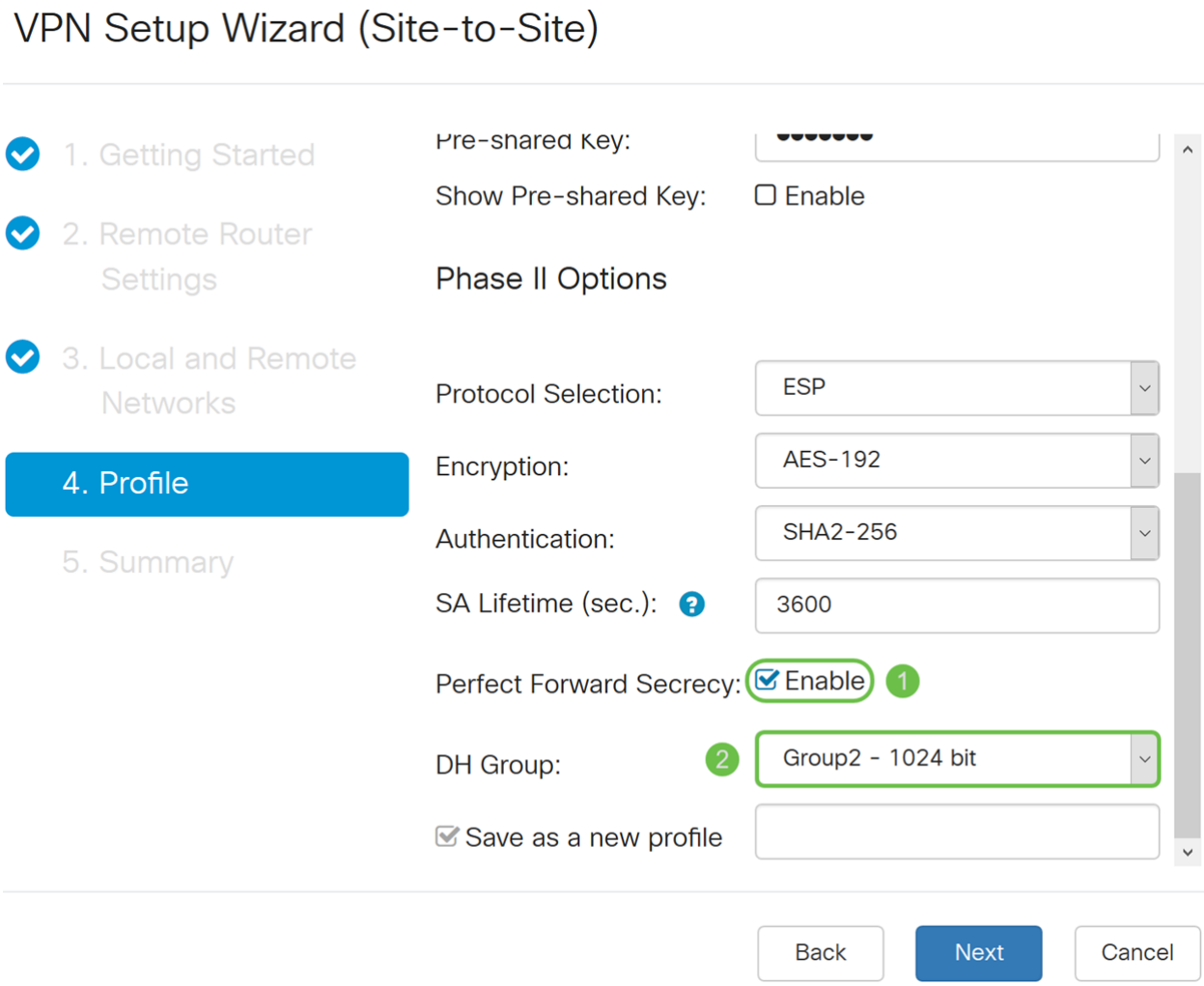
Schritt 17: Die Authentifizierungsmethode legt fest, wie die ESP-Headerpakete (Encapsulating Security Payload Protocol) validiert werden. MD5 ist ein unidirektionaler Hash-Algorithmus, der einen 128-Bit-Digest erzeugt. SHA1 ist ein unidirektionaler Hashing-Algorithmus, der ein 160-Bit-Digest erzeugt, während SHA2-256 ein 256-Bit-Digest erzeugt. SHA2-256 wird empfohlen, da es sicherer ist. Stellen Sie sicher, dass beide Enden des VPN-Tunnels dieselbe Authentifizierungsmethode verwenden. Wählen Sie eine Authentifizierung aus (**MD5, SHA1** oder **SHA2-256**). **Für** dieses Beispiel wurde **SHA2-256** ausgewählt.



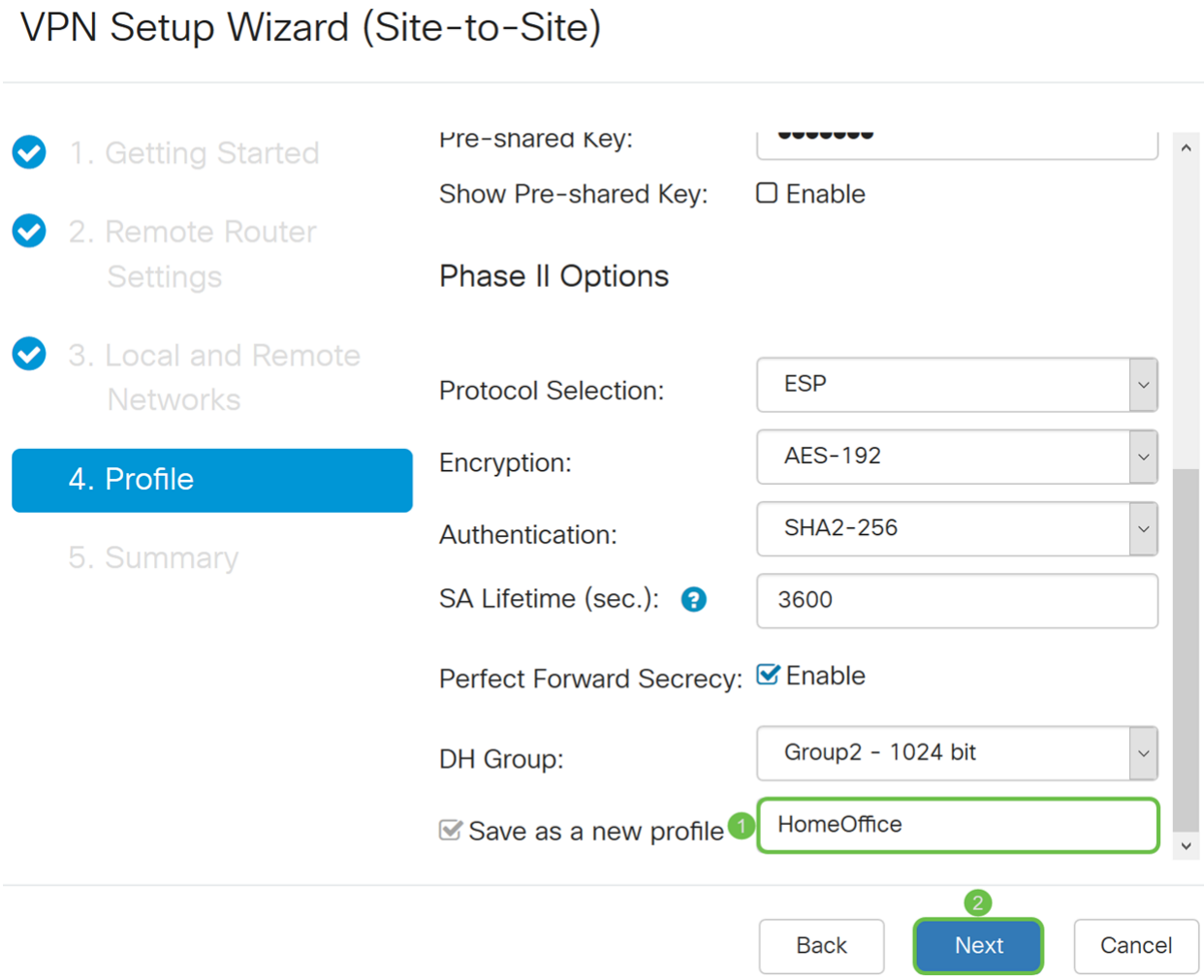
Schritt 18: Geben Sie in die *SA Lifetime (Sec)* ein, d. h. die Zeitdauer in Sekunden, die ein VPN-Tunnel (IPsec SA) in dieser Phase aktiv ist. Der Standardwert für Phase 2 ist 3600 Sekunden.



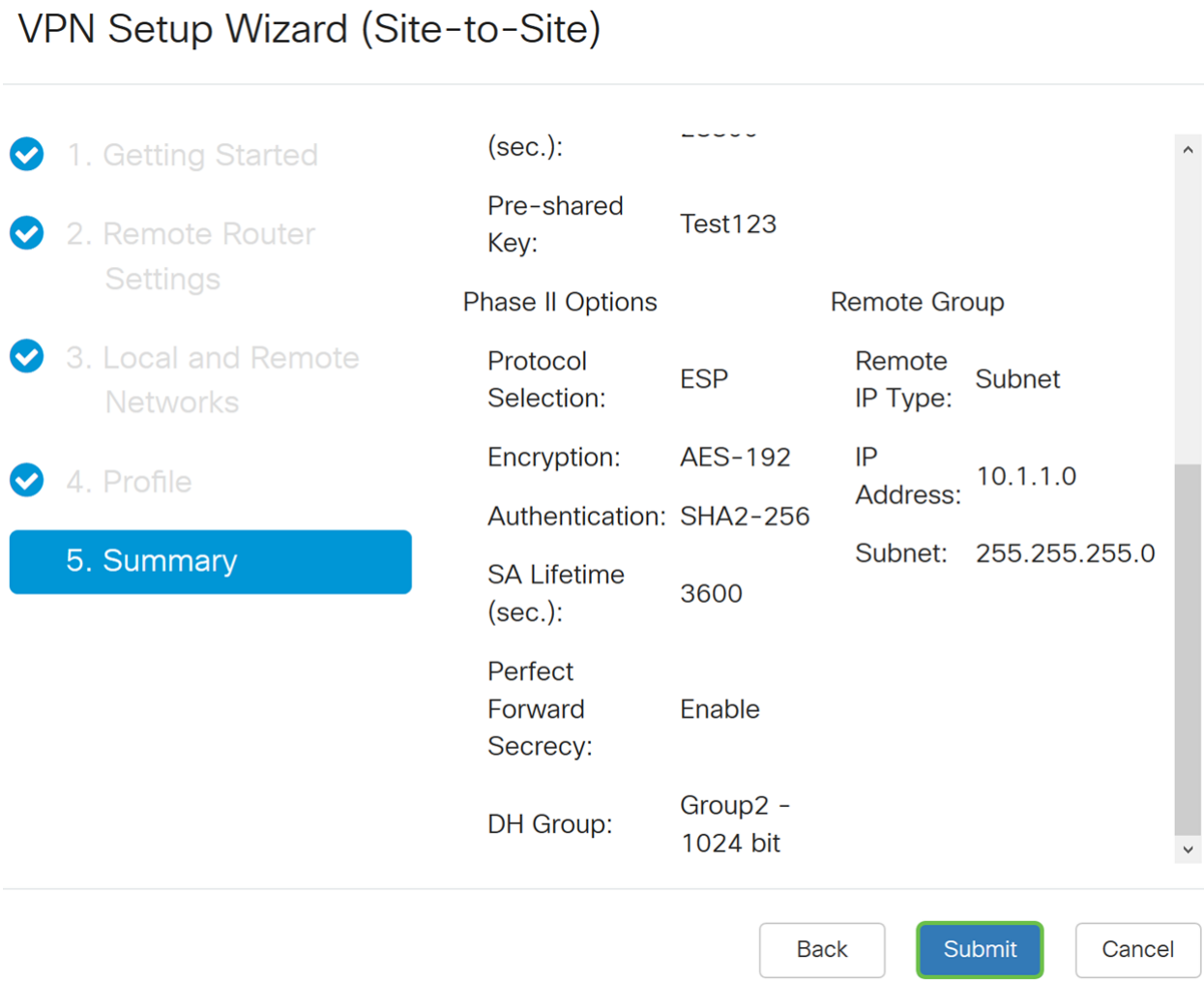
Schritt 19: Wenn Perfect Forward Secrecy (PFS) aktiviert ist, generiert die IKE Phase 2-Aushandlung neues Schlüsselmaterial für die Verschlüsselung und Authentifizierung des IPsec-Datenverkehrs. Perfect Forward Secrecy wird verwendet, um die Sicherheit der Kommunikation, die über das Internet mit Public-Key-Verschlüsselung übertragen wird, zu verbessern. Aktivieren Sie das Kontrollkästchen, um diese Funktion zu aktivieren, oder deaktivieren Sie das Kontrollkästchen, um diese Funktion zu deaktivieren. Diese Funktion wird empfohlen. Wenn aktiviert, wählen Sie eine *DH Group (DH-Gruppe)*. In diesem Beispiel wird **Group2 - 1024 Bit** verwendet.



Schritt 20: Geben Sie im *Profil Als neues Profil speichern* einen Namen für das neue Profil ein, das Sie gerade erstellt haben. Klicken Sie auf **Weiter**, um die Zusammenfassung Ihrer VPN-Konfiguration anzuzeigen.



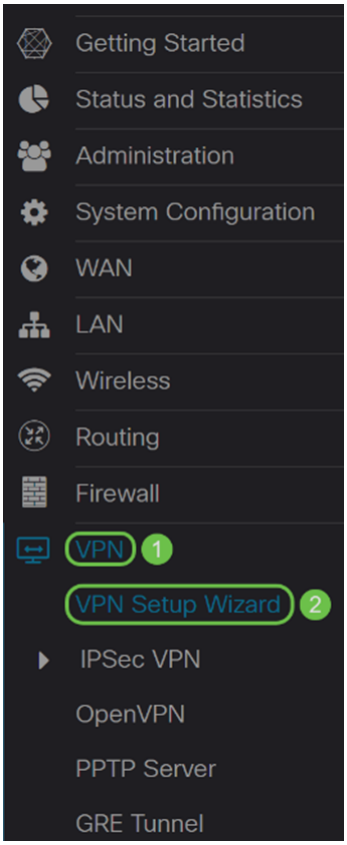
Schritt 21: Überprüfen Sie die Informationen, und klicken Sie dann auf **Senden**.



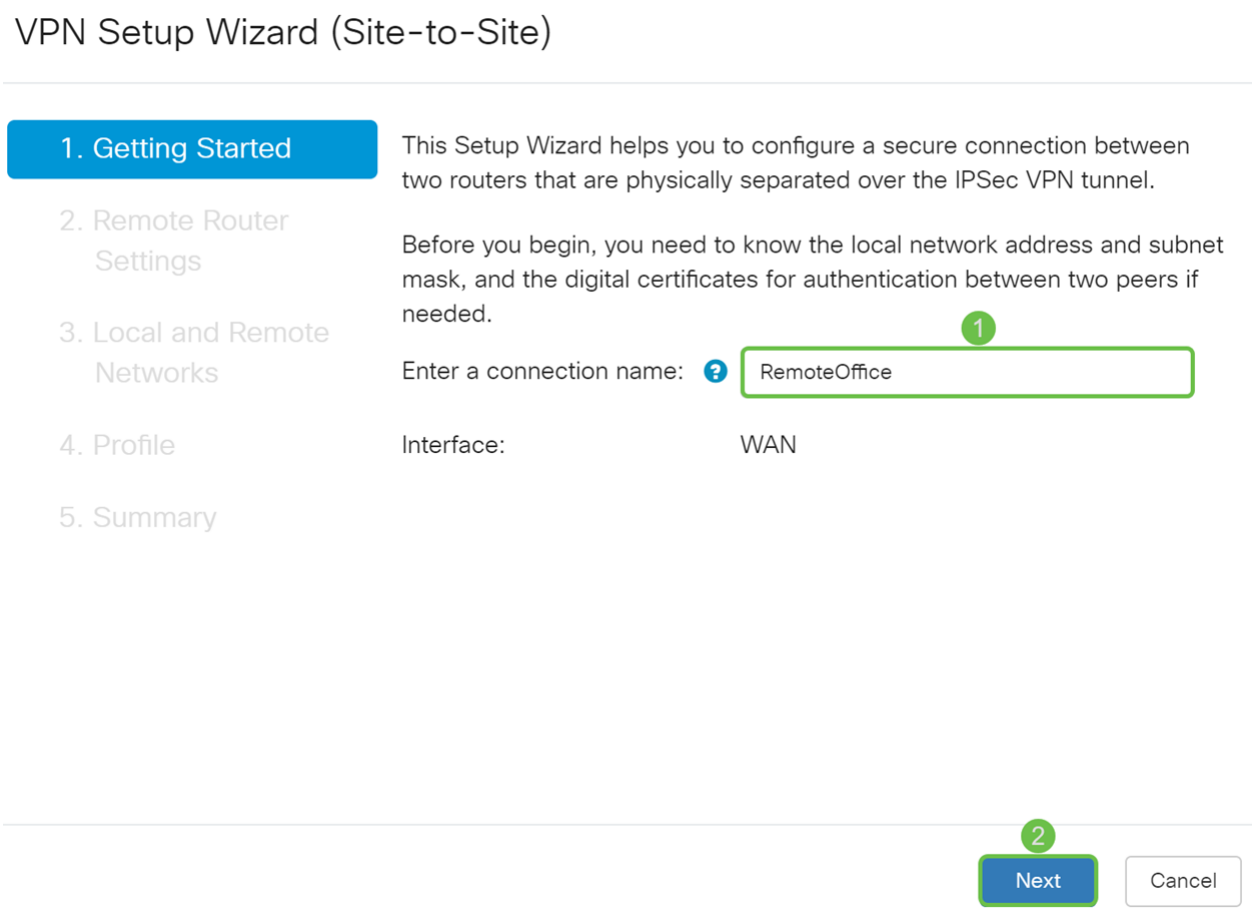
Konfiguration des VPN-Einrichtungsassistenten für den Remote-Router

Auf dem Remote-Router müssen Sie die gleichen Sicherheitseinstellungen wie der lokale Router konfigurieren, aber die IP-Adresse des lokalen Routers als Remote-Datenverkehr verwenden.

Schritt 1: Melden Sie sich auf der Webkonfigurationsseite Ihres Remote-Routers (Router B) an, und navigieren Sie zu **VPN > VPN Setup Wizard (VPN > VPN-Einrichtungsassistent)**.

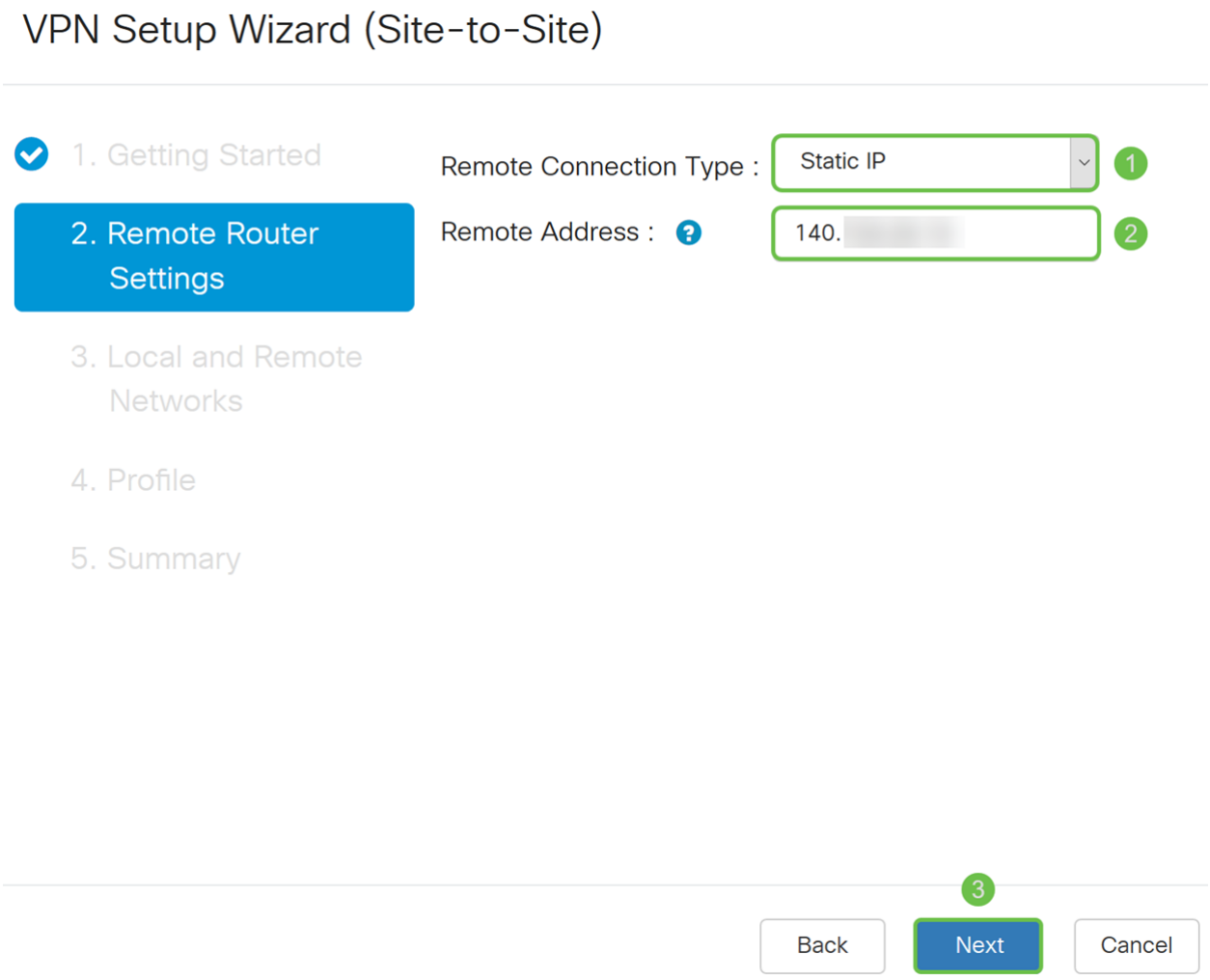


Schritt 2: Geben Sie einen Verbindungsnamen ein, und wählen Sie die Schnittstelle aus, die für das VPN verwendet wird, wenn Sie einen RV260 verwenden. Der RV160 verfügt nur über einen WAN-Link. Daher können Sie im Dropdown-Menü keine Schnittstelle auswählen. Klicken Sie anschließend auf **Weiter**, um fortzufahren.

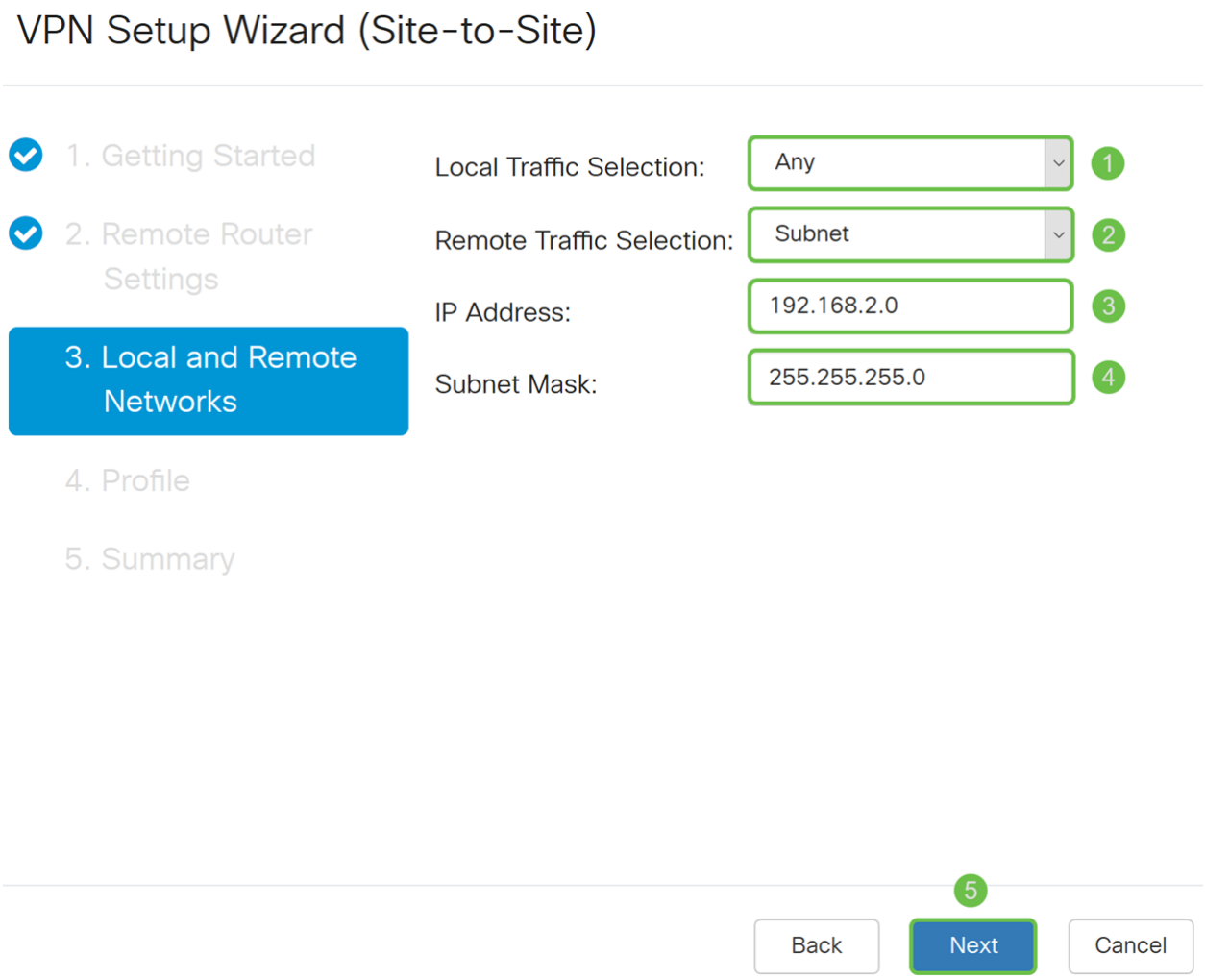


Schritt 3: Wählen Sie in den *Remote Router Settings* den *Remote Connection Type*

(Verbindungstyp für *Remote-Router)* aus, und geben Sie dann die WAN-IP-Adresse von Router A ein. Klicken Sie anschließend auf **Weiter**, um mit dem nächsten Abschnitt fortzufahren.

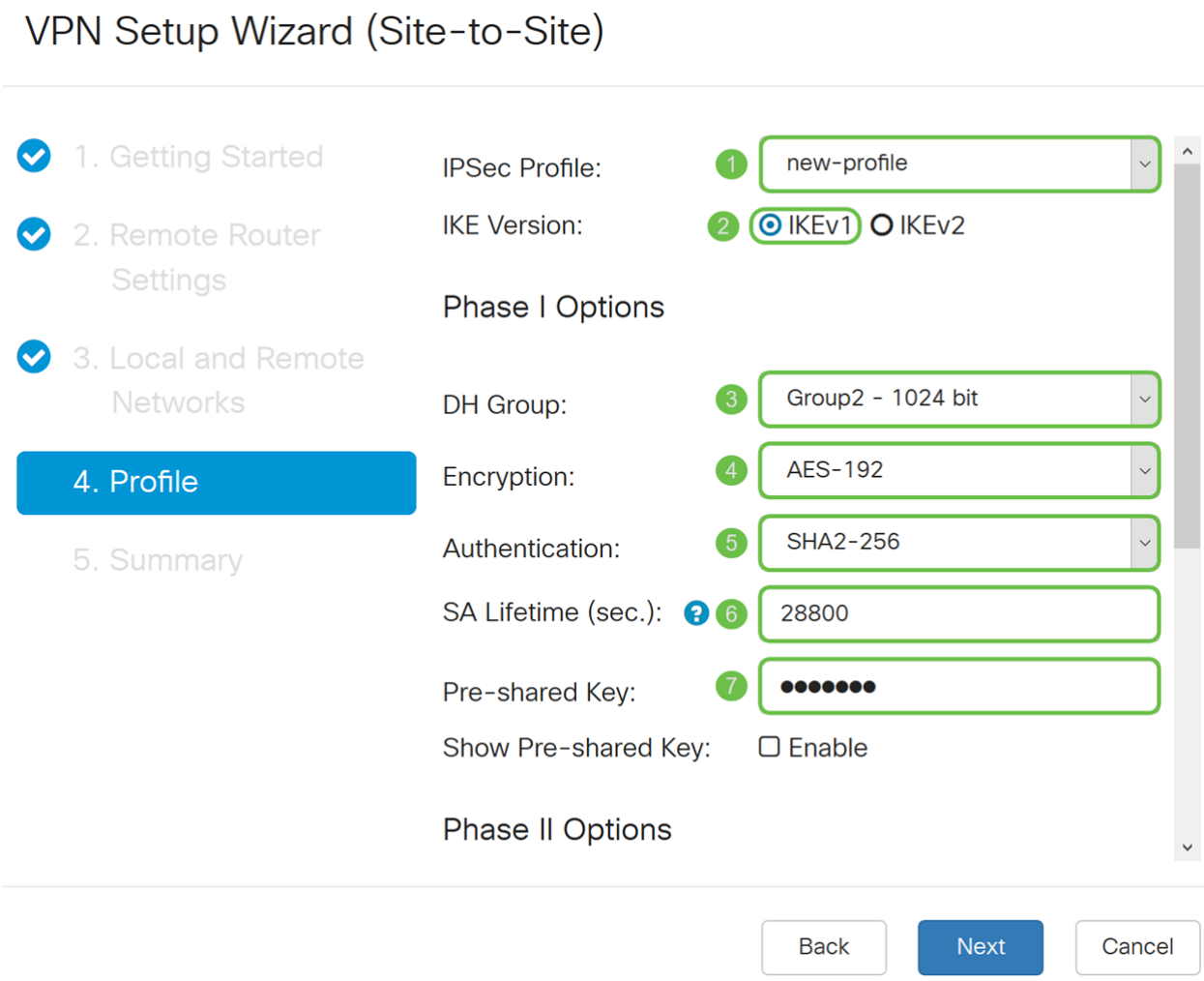


Schritt 4: Wählen Sie den lokalen und den Remote-Datenverkehr aus. Wenn Sie **Subnetz** im Feld *Remote Traffic Selection* (*Remote-Datenverkehrsauswahl*) ausgewählt haben, geben Sie das Subnetz der privaten IP-Adresse von Router A ein. Klicken Sie anschließend auf **Weiter**, um den Abschnitt *"Profil"* zu konfigurieren.

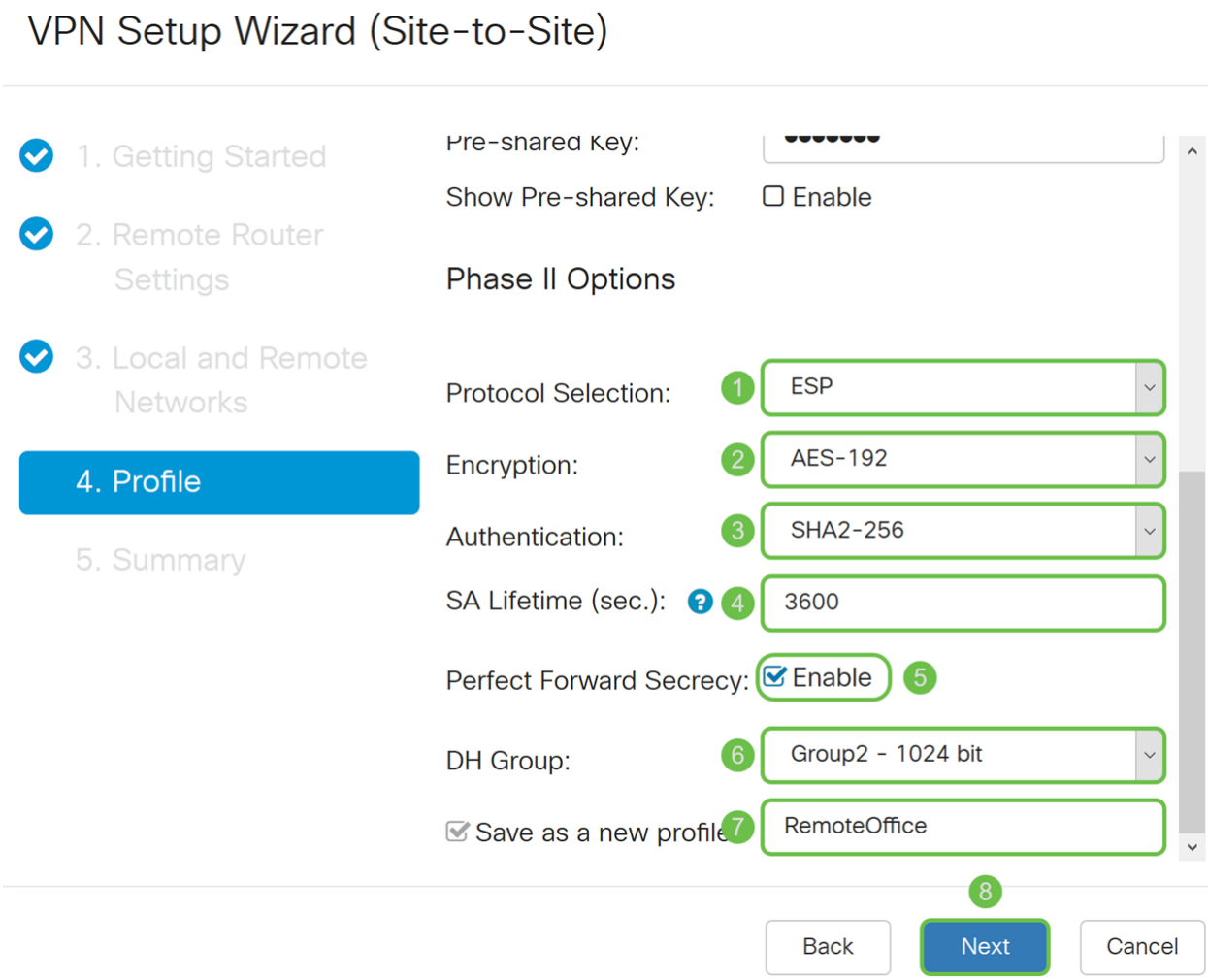


Schritt 5: Wählen Sie im Abschnitt *"Profil"* die gleichen Sicherheitseinstellungen wie Router A aus. Außerdem haben wir denselben vorinstallierten Schlüssel wie Router A eingegeben. Klicken Sie anschließend auf **Weiter**, um zur Seite *Zusammenfassung* zu gelangen.

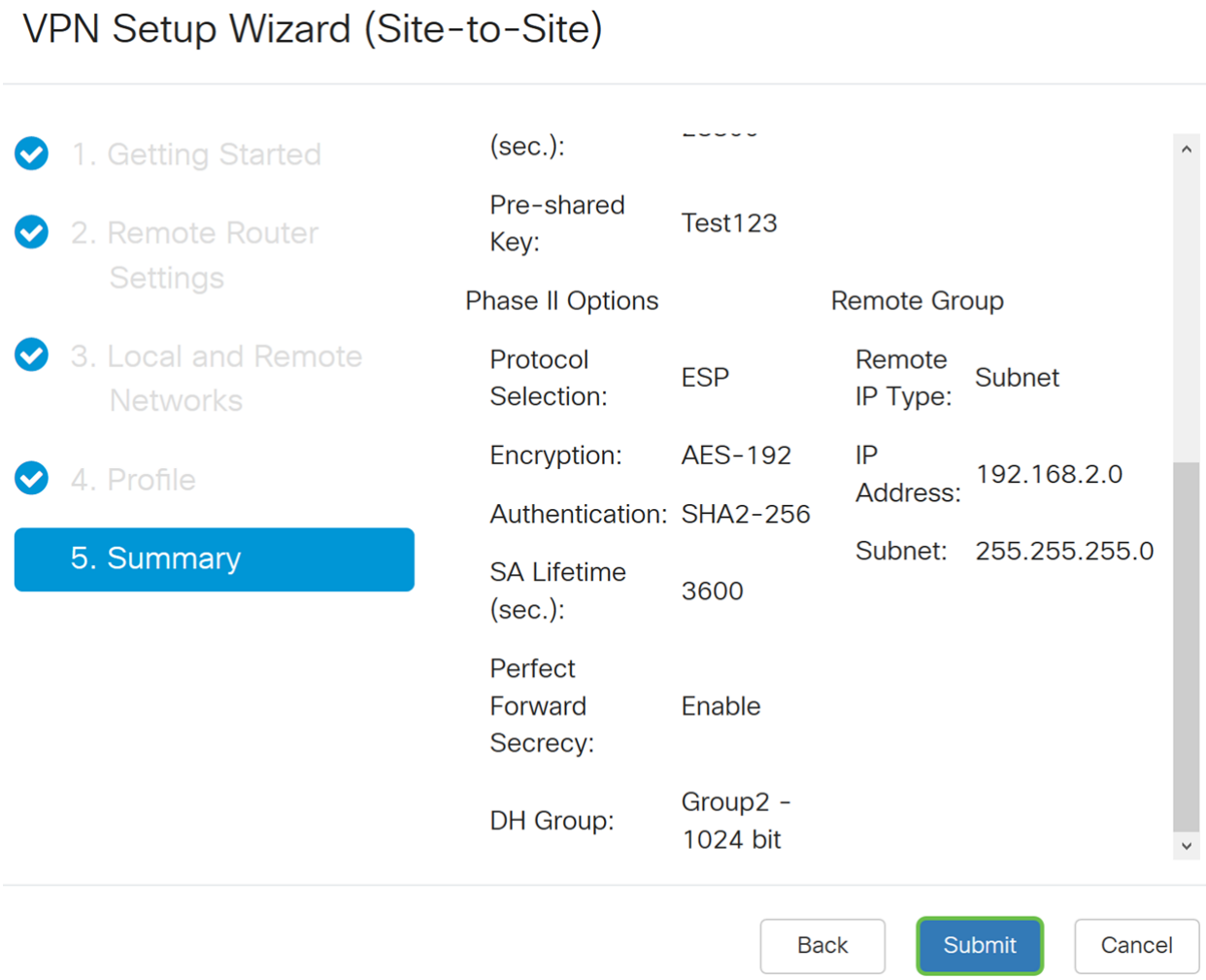
Optionen aus Phase I:



Optionen aus Phase II:



Schritt 6: Überprüfen Sie auf der Seite *Zusammenfassung*, ob die soeben konfigurierten Informationen korrekt sind. Klicken Sie anschließend auf **Senden**, um ein Site-to-Site-VPN zu erstellen.

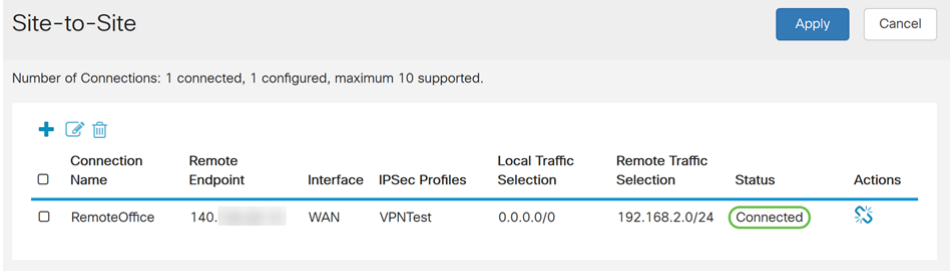


Hinweis: Alle Konfigurationen, die der Router derzeit verwendet, befinden sich in der Running Configuration-Datei, die flüchtig ist und zwischen Neustarts nicht beibehalten wird. Um die Konfiguration zwischen Neustarts beizubehalten, kopieren Sie die Konfigurationsdatei Running in die Startkonfigurationsdatei, nachdem Sie alle Änderungen vorgenommen haben. Klicken Sie dazu auf die Schaltfläche **Speichern**, die oben auf der Seite angezeigt wird, oder navigieren Sie zu **Administration > Configuration Management**. Vergewissern Sie sich anschließend, dass die *Quelle* **Konfiguration ausführen** und das *Ziel* **Startkonfiguration** ist. Klicken Sie auf **Übernehmen**.

Schlussfolgerung

Sie sollten mithilfe des VPN-Einrichtungsassistenten erfolgreich ein Site-to-Site-VPN konfiguriert haben. Führen Sie die unten aufgeführten Schritte aus, um zu überprüfen, ob Ihr Site-to-Site-VPN verbunden ist.

Schritt 1: Um zu überprüfen, ob die Verbindung hergestellt wurde, sollte der Status *Verbunden* angezeigt werden, wenn Sie zu **VPN > IPSec VPN > Site-to-Site** navigieren.



Schritt 2: Navigieren Sie zu **Status und Statistik > VPN Status** und stellen Sie sicher, dass

der Site-to-Site-Tunnel *aktiviert* und *aktiviert* ist.