Einrichten und Verwenden des GreenBow IPsec VPN Client für die Verbindung mit den Routern RV160 und RV260

Ziel

Ziel dieses Dokuments ist es, den GreenBow IPsec VPN Client für die Verbindung mit den Routern RV160 und RV260 einzurichten und zu verwenden.

Einführung

Über eine VPN-Verbindung (Virtual Private Network) können Benutzer auf ein privates Netzwerk (z. B. das Internet) zugreifen, Daten an ein privates Netzwerk senden und von diesem empfangen. Dabei wird eine sichere Verbindung zu einer zugrunde liegenden Netzwerkinfrastruktur zum Schutz des privaten Netzwerks und seiner Ressourcen sichergestellt.

Ein VPN-Tunnel richtet ein privates Netzwerk ein, das Daten sicher mit Verschlüsselung und Authentifizierung senden kann. Unternehmensbüros verwenden häufig eine VPN-Verbindung, da es sowohl nützlich als auch notwendig ist, Mitarbeitern den Zugriff auf ihr privates Netzwerk zu ermöglichen, selbst wenn sie sich außerhalb des Büros befinden.

Mit dem VPN kann ein Remotehost oder Client so agieren, als ob er sich im selben lokalen Netzwerk befinde. Der RV160-Router unterstützt bis zu 10 VPN-Tunnel und der RV260 bis zu 20. Nachdem der Router für die Internetverbindung konfiguriert wurde, kann zwischen dem Router und einem Endpunkt eine VPN-Verbindung eingerichtet werden. Der VPN-Client ist vollständig von den Einstellungen des VPN-Routers abhängig, um eine Verbindung herstellen zu können. Die Einstellungen müssen genau übereinstimmen, da sie sonst nicht kommunizieren können.

Der GreenBow VPN Client ist eine VPN-Client-Anwendung eines Drittanbieters, mit der ein Hostgerät eine sichere Verbindung für einen Client-to-Site-IPsec-Tunnel mit den Routern der Serien RV160 und RV260 konfigurieren kann.

Vorteile einer VPN-Verbindung

Die Verwendung einer VPN-Verbindung trägt zum Schutz vertraulicher Netzwerkdaten und -ressourcen bei.

Remote-Mitarbeiter und Mitarbeiter im Unternehmen können so problemlos auf die Hauptniederlassung zugreifen, ohne dabei physisch präsent sein zu müssen. Gleichzeitig wird die Sicherheit des privaten Netzwerks und seiner Ressourcen gewahrt.

Die Kommunikation über eine VPN-Verbindung bietet ein höheres Maß an Sicherheit als andere Remote-Kommunikationsmethoden. Ein erweiterter Verschlüsselungsalgorithmus macht dies möglich und schützt das private Netzwerk vor unberechtigtem Zugriff.

Die tatsächlichen geografischen Standorte der Benutzer sind geschützt und nicht mit öffentlichen oder gemeinsam genutzten Netzwerken wie dem Internet verbunden.

Mit einem VPN können neue Benutzer oder eine Benutzergruppe hinzugefügt werden, ohne dass

zusätzliche Komponenten oder eine komplizierte Konfiguration erforderlich sind.

Risiken der Verwendung einer VPN-Verbindung

Aufgrund von Konfigurationsfehlern können Sicherheitsrisiken bestehen. Da das Design und die Implementierung eines VPNs kompliziert sein kann, ist es notwendig, die Konfiguration der Verbindung einem hoch qualifizierten und erfahrenen Experten zu übertragen, um sicherzustellen, dass die Sicherheit des privaten Netzwerks nicht beeinträchtigt wird.

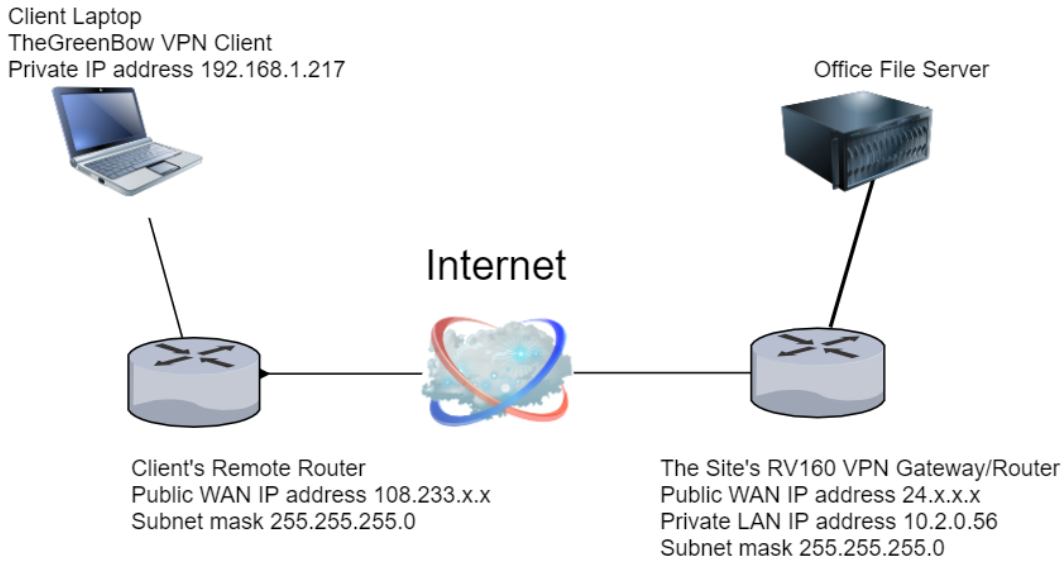
Sie ist möglicherweise weniger zuverlässig. Da eine VPN-Verbindung eine Internetverbindung erfordert, ist es wichtig, dass ein Anbieter mit einer bewährten Reputation einen ausgezeichneten Internetservice anbietet und nur minimale bis keine Ausfallzeiten garantiert.

Wenn eine Situation eintritt, in der eine neue Infrastruktur oder eine neue Gruppe von Konfigurationen hinzugefügt werden muss, können technische Probleme aufgrund der Inkompatibilität entstehen, insbesondere, wenn es sich um andere Produkte oder Anbieter als die handelt, die Sie bereits verwenden.

Es können langsame Verbindungsgeschwindigkeiten auftreten. Wenn Sie einen VPN-Client verwenden, der einen kostenlosen VPN-Service bereitstellt, ist zu erwarten, dass Ihre Verbindung ebenfalls langsam ist, da diese Anbieter die Verbindungsgeschwindigkeiten nicht priorisieren. In diesem Artikel verwenden wir einen bezahlten Dritten, der dieses Problem beseitigen sollte.

Grundlegende Topologie des Client-to-Site-Netzwerks

Dies ist das grundlegende Layout des Netzwerks für die Einrichtung. Die öffentlichen WAN-IP-Adressen wurden teilweise verwischt oder zeigen ein **x** anstelle der tatsächlichen Zahlen an, um das Netzwerk vor Angriffen zu schützen.



In diesem Artikel werden die Schritte zur Konfiguration des RV160- oder RV260-Routers am Standort für Folgendes erläutert:

- Eine Benutzergruppe - **VPN-Benutzer**
- Benutzerkonten (ein oder mehrere Benutzer), die als Client Zugriff erhalten
- Ein IPsec-Profil - **TheGreenBow**
- Ein Client-to-Site-Profil - **Client**

- Sie werden auch angezeigt, wie Sie den VPN-Status auf dem Standort anzeigen, wenn der Client verbunden ist.

Hinweis: Sie können einen beliebigen Namen für die Benutzergruppe, das IPsec-Profil und das Client-to-Site-Profil verwenden. Die Namen sind nur Beispiele.

In diesem Artikel werden auch die Schritte erläutert, die jeder Client zum Konfigurieren von TheGreenBow VPN auf seinem Computer ausführen würde:

- Laden Sie die GreenBow VPN Client-Software herunter und richten Sie sie ein.
- Konfigurieren der Einstellungen für Phase 1 und 2 des Clients
- Starten und Überprüfen einer VPN-Verbindung als Client

Es ist wichtig, dass alle Einstellungen auf dem Router vor Ort mit den Client-Einstellungen übereinstimmen. Wenn Ihre Konfiguration nicht zu einer erfolgreichen VPN-Verbindung führt, überprüfen Sie alle Einstellungen, um sicherzustellen, dass sie übereinstimmen. Das Beispiel in diesem Artikel ist nur eine Möglichkeit, die Verbindung einzurichten.

Inhaltsverzeichnis

Anwendbare Geräte

- RV160
- RV260

Softwareversion

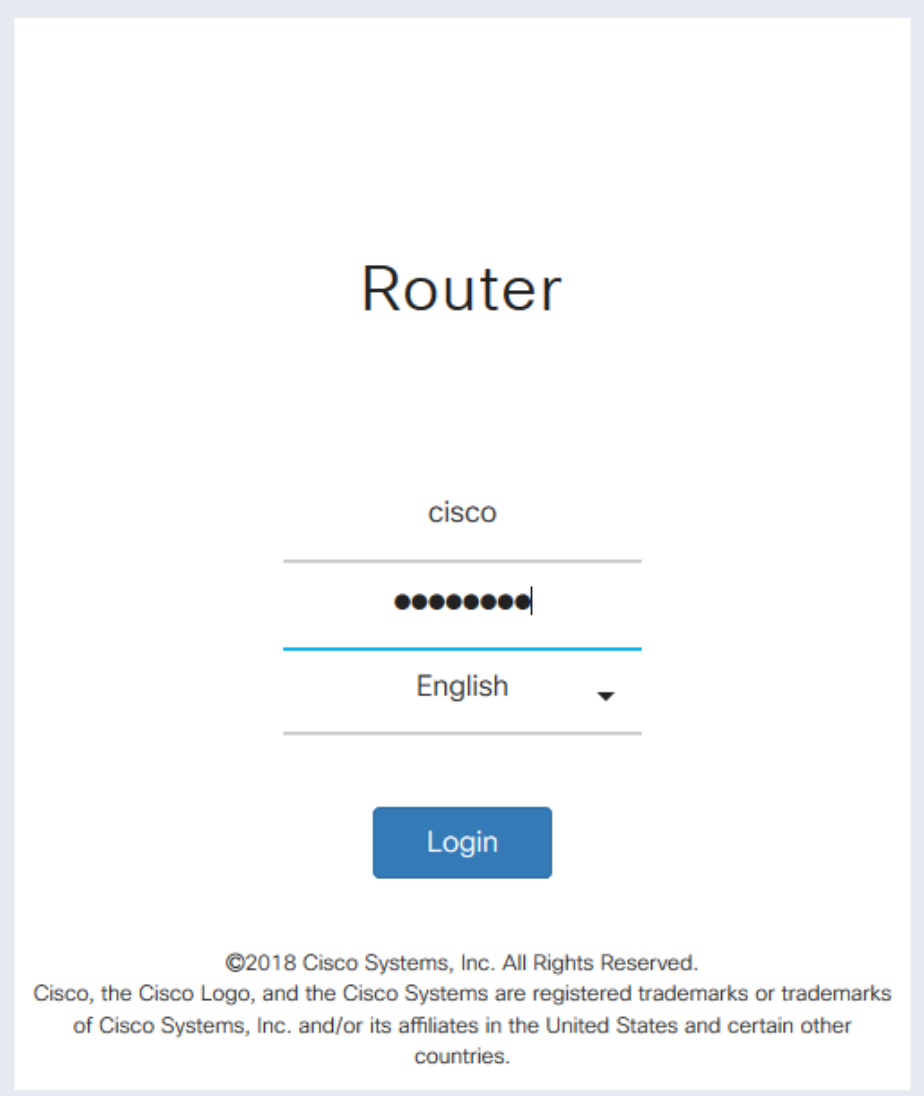
- 1,0 00,15

Konfigurieren des VPN-Clients am Standort des Routers RV160 oder RV260

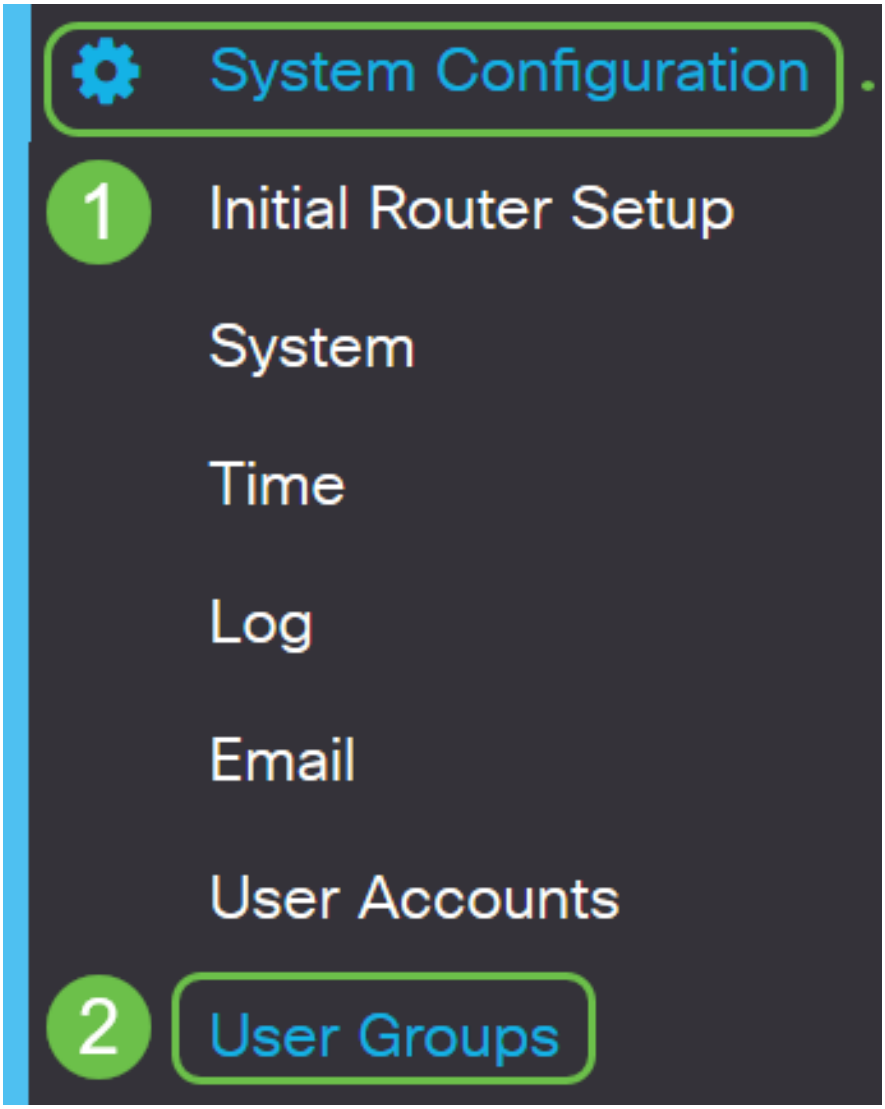
Erstellen einer Benutzergruppe

Wichtiger Hinweis: Bitte lassen Sie das Standard-Admin-Konto in der Admin-Gruppe und erstellen Sie ein neues Benutzerkonto und eine Benutzergruppe für TheGreenBow. Wenn Sie Ihr Admin-Konto in eine andere Gruppe verschieben, können Sie sich nicht beim Router anmelden.

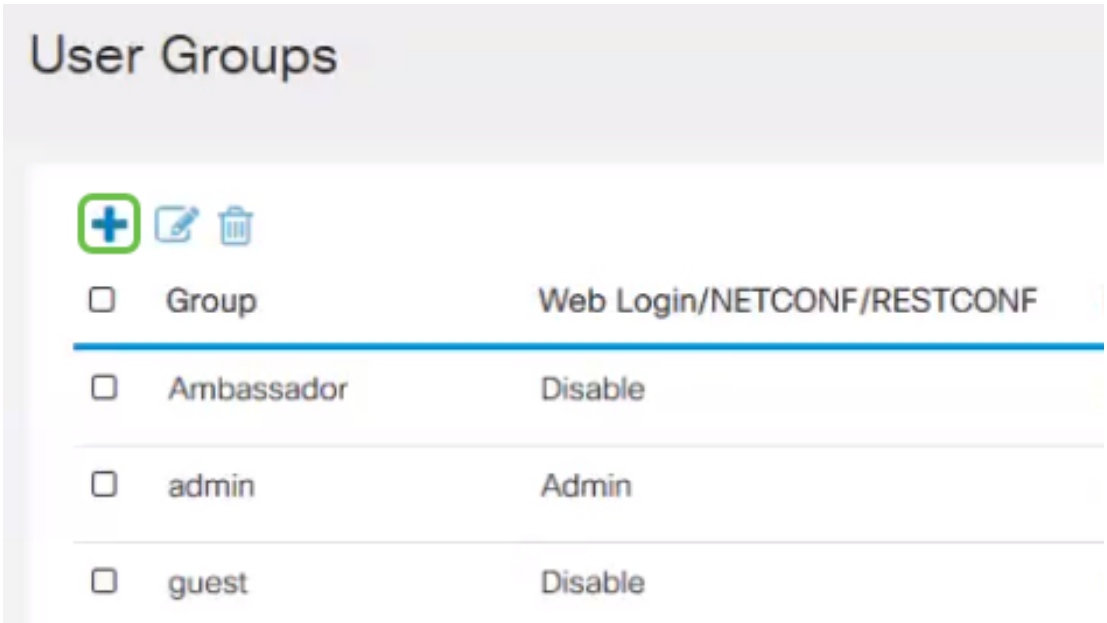
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an.



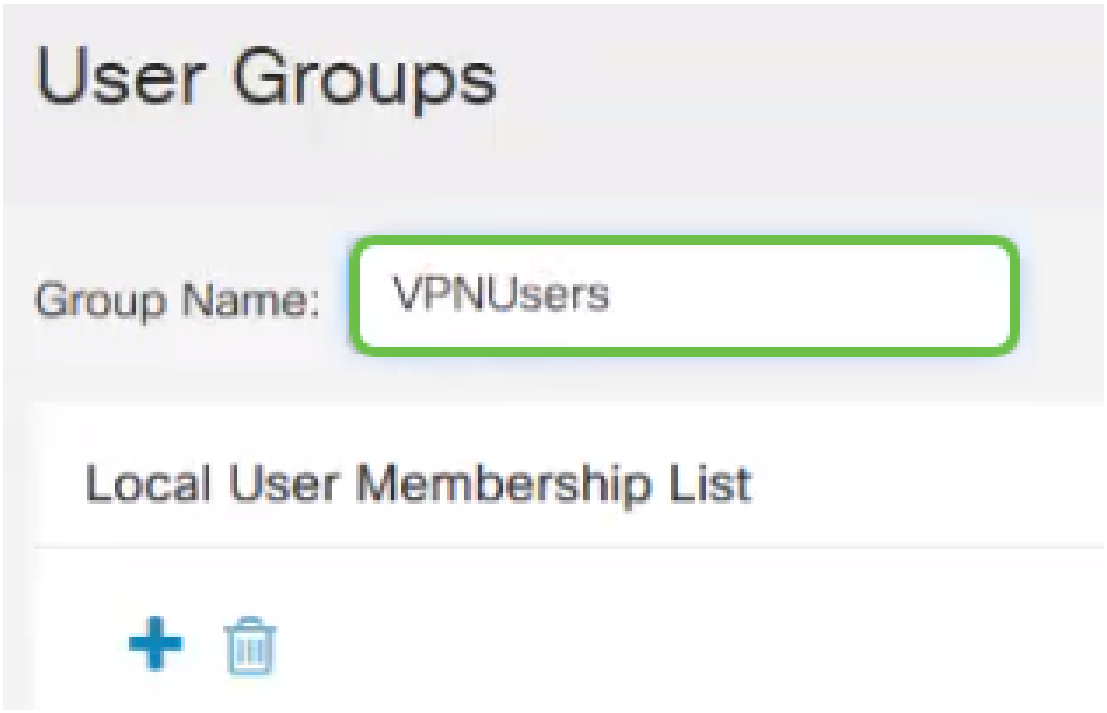
Schritt 2: Wählen Sie **Systemkonfiguration > Benutzergruppen aus**.



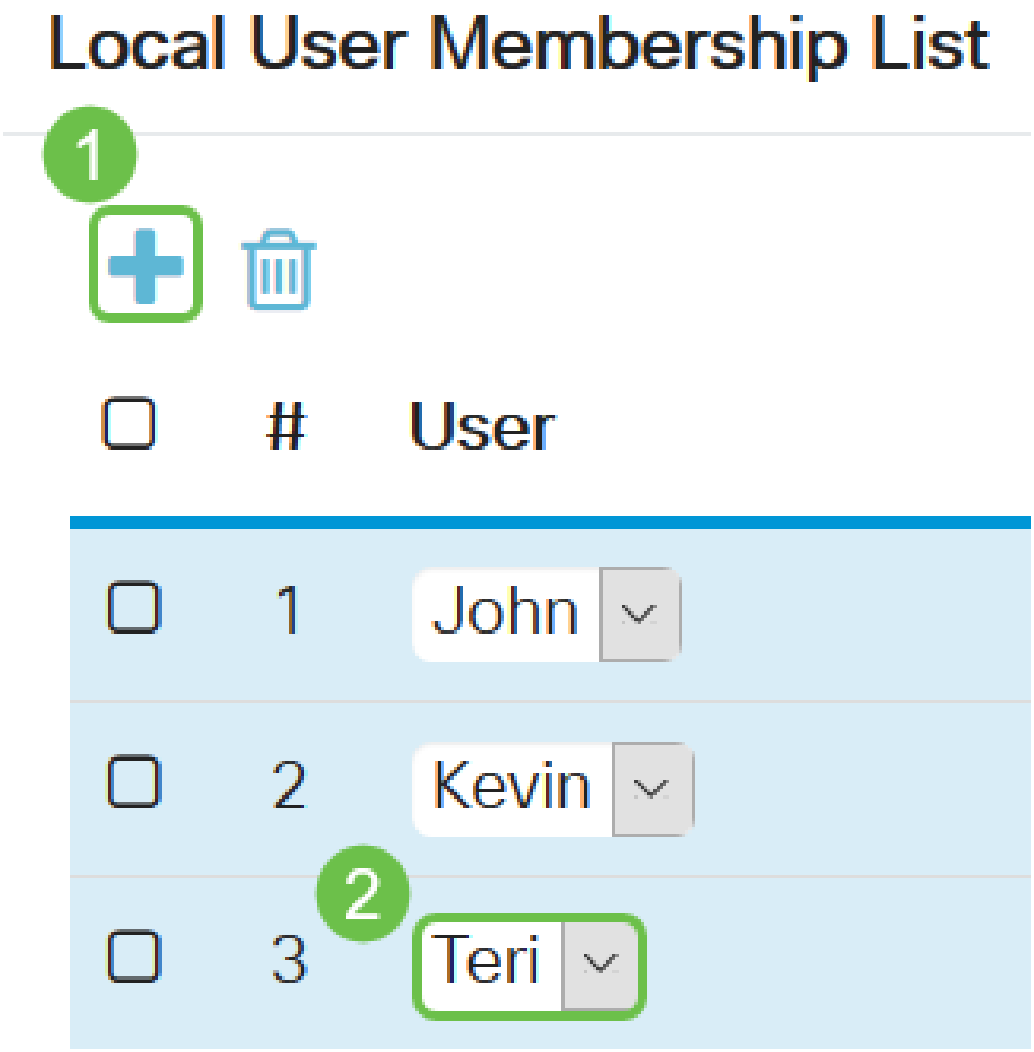
Schritt 3: Klicken Sie auf das **Plus-**Symbol, um eine Benutzergruppe hinzuzufügen.



Schritt 4: Geben Sie im Bereich Übersicht den Namen der Gruppe im Feld *Gruppenname ein*.

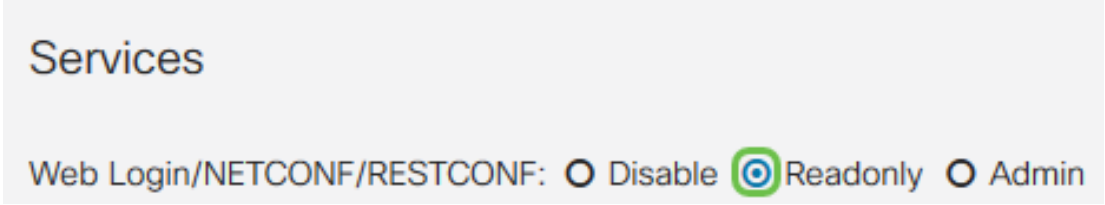


Schritt 5: Klicken Sie unter *Local User Membership List* (*Lokale Benutzermitgliedschaftsliste)* auf das **Plus-**Symbol, und wählen Sie den Benutzer aus der Dropdown-Liste aus. Wenn Sie weitere hinzufügen möchten, drücken Sie erneut das **Plus-**Symbol, und wählen Sie ein anderes Mitglied aus, das hinzugefügt werden soll. Mitglieder können nur Teil einer Gruppe sein. Wenn nicht alle Benutzer bereits eingegeben sind, können Sie im Abschnitt Benutzerkonto erstellen weitere hinzufügen.

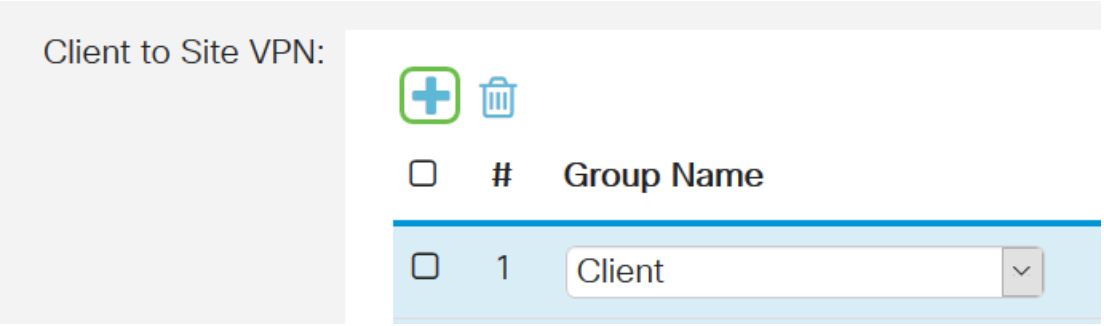


Schritt 6: Wählen Sie unter *Dienste* eine Berechtigung aus, die den Benutzern in der Gruppe erteilt werden soll. Folgende Optionen stehen zur Verfügung:

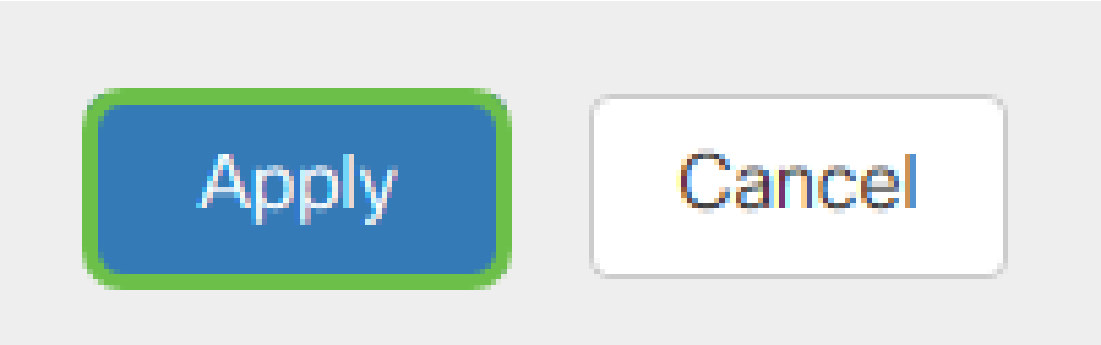
- Disabled (Deaktiviert): Diese Option bedeutet, dass Mitglieder der Gruppe nicht über einen Browser auf das webbasierte Dienstprogramm zugreifen dürfen.
- Readonly (Schreibgeschützt): Diese Option bedeutet, dass die Mitglieder der Gruppe den Status des Systems erst lesen können, nachdem sie sich angemeldet haben. Sie können keine der Einstellungen bearbeiten.
- Admin (Admin): Diese Option gewährt den Mitgliedern der Gruppe Lese- und Schreibberechtigungen und kann den Systemstatus konfigurieren.



Schritt 7: Klicken Sie auf das **Plus-**Symbol, um ein vorhandenes Client-to-Site-VPN hinzuzufügen. Wenn Sie dies nicht konfiguriert haben, finden Sie Informationen in diesem Artikel im Abschnitt Erstellen eines Client-zu-Site-Profils.

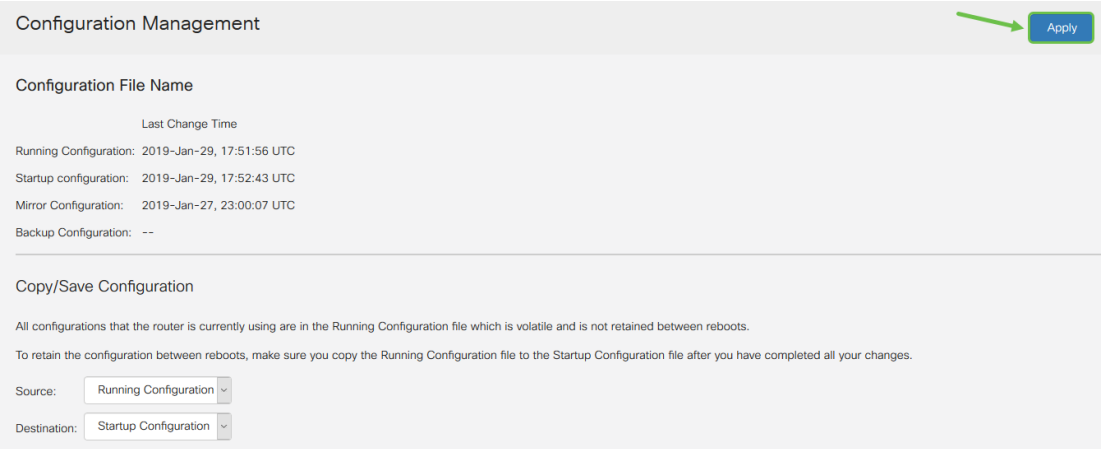


Schritt 8: Klicken Sie auf **Übernehmen**.

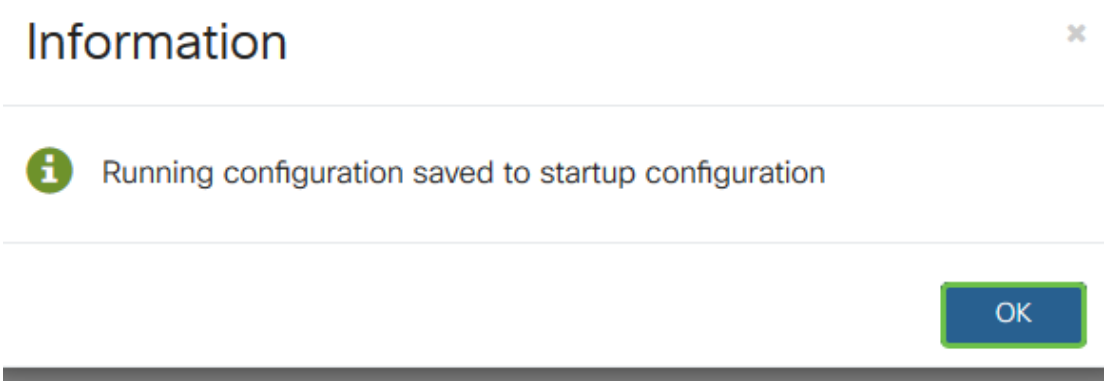


Schritt 9: Klicken Sie auf **Speichern**.

Schritt 10: Klicken Sie erneut auf **Apply**, um die aktuelle Konfiguration in der Startkonfiguration zu speichern.



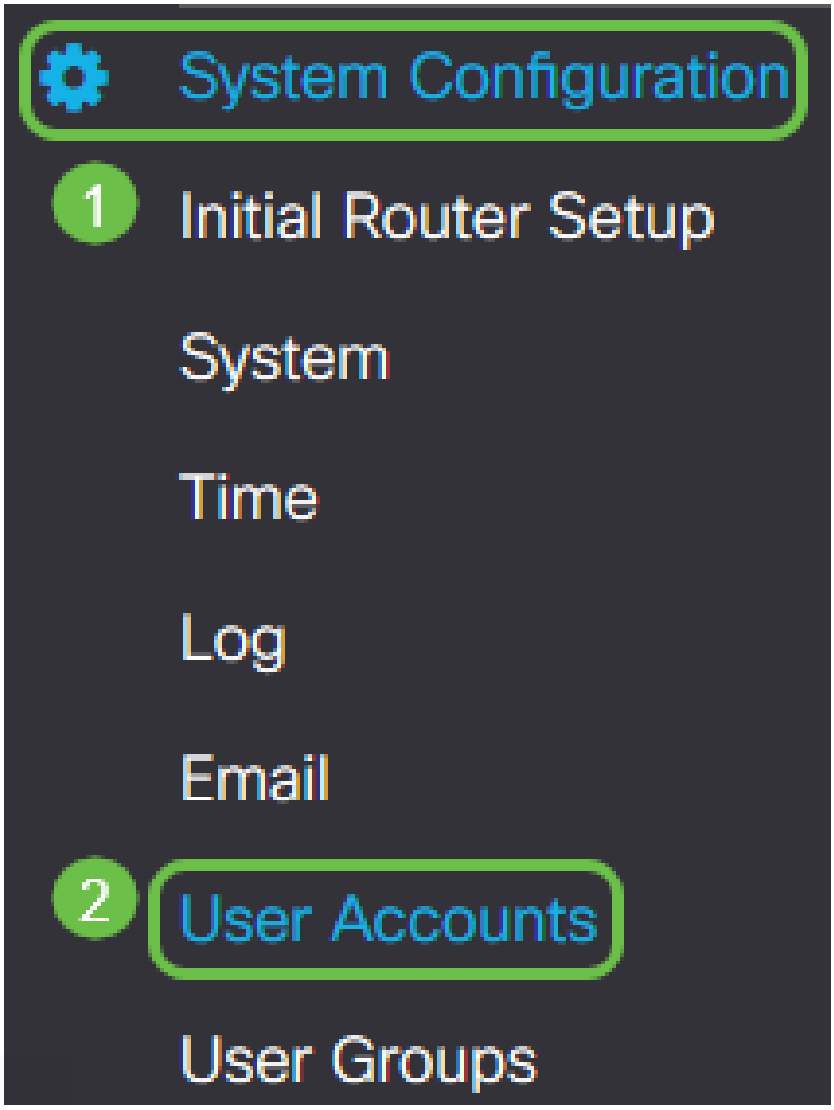
Schritt 11: Wenn Sie die Bestätigung erhalten, klicken Sie auf **OK**.



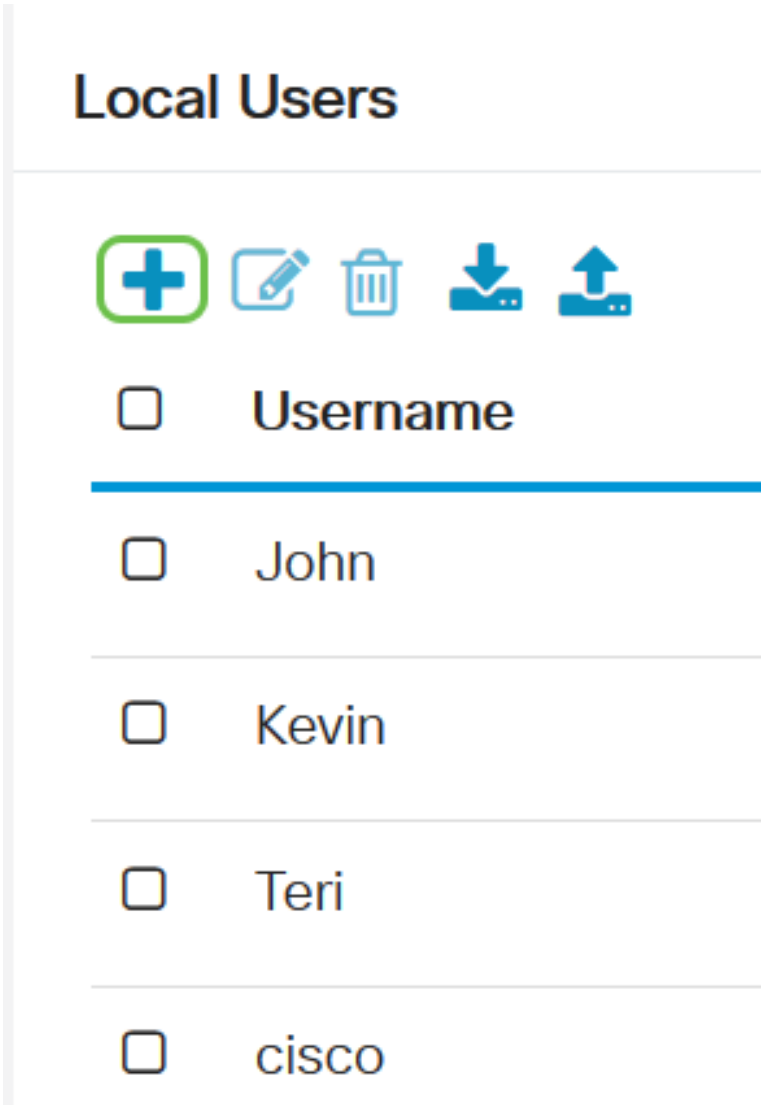
Sie sollten jetzt erfolgreich eine Benutzergruppe auf dem Router der Serie RV160 oder RV260 erstellt haben.

Erstellen eines Benutzerkontos

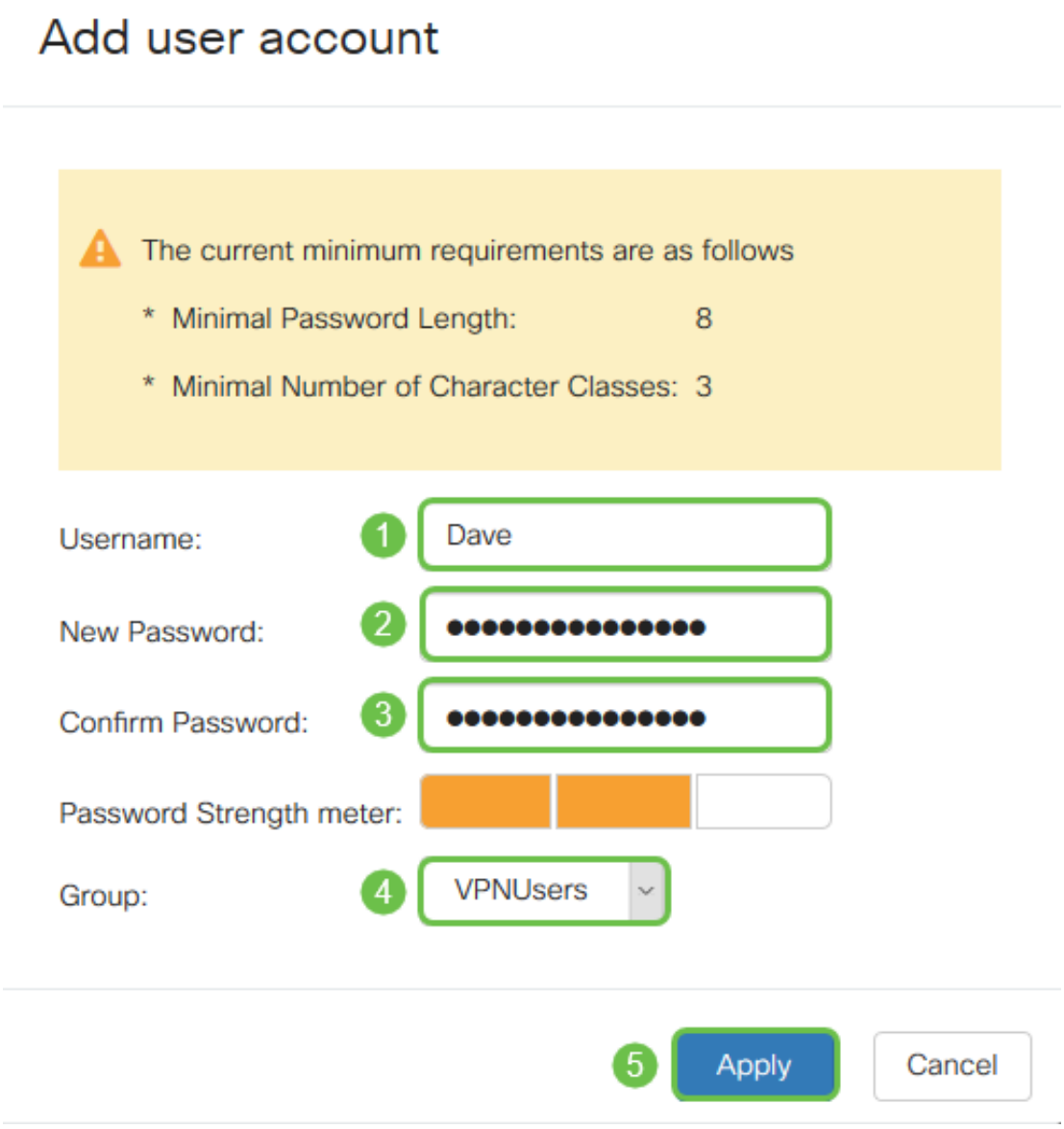
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **Systemkonfiguration > Benutzerkonten aus**.



Schritt 2: Klicken Sie im Bereich *Lokale Benutzer* auf das Symbol **hinzufügen**.



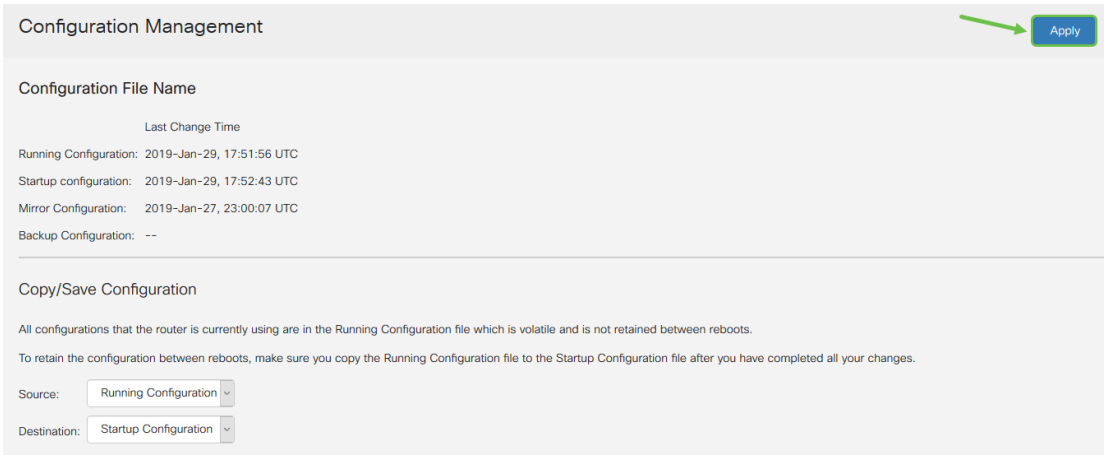
Schritt 3: Geben Sie im Feld *Benutzername*, das Kennwort und die Gruppe ein, der Sie den Benutzer aus dem Dropdown-Menü hinzufügen möchten. Klicken Sie auf **Übernehmen**.



Hinweis: Wenn der Client TheGreenBow Client auf seinem Computer eingerichtet hat, meldet er sich mit demselben Benutzernamen und Kennwort an.

Schritt 4: Klicken Sie auf **Speichern**.

Schritt 5: Klicken Sie erneut auf **Apply**, um die aktuelle Konfiguration in der Startkonfiguration zu speichern.



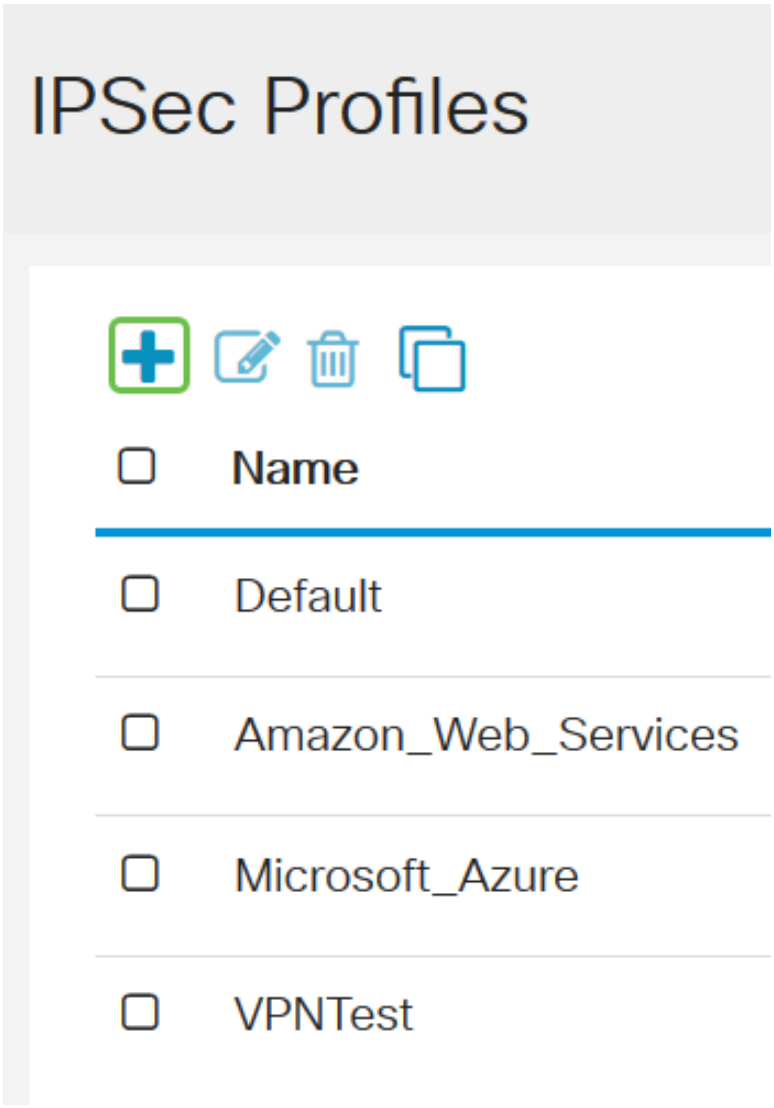
Schritt 6: Wenn Sie die Bestätigung erhalten, klicken Sie auf **OK**.

Sie sollten jetzt ein Benutzerkonto auf Ihrem Router RV160 oder RV260 erstellt haben.

Konfigurieren des IPsec-Profils

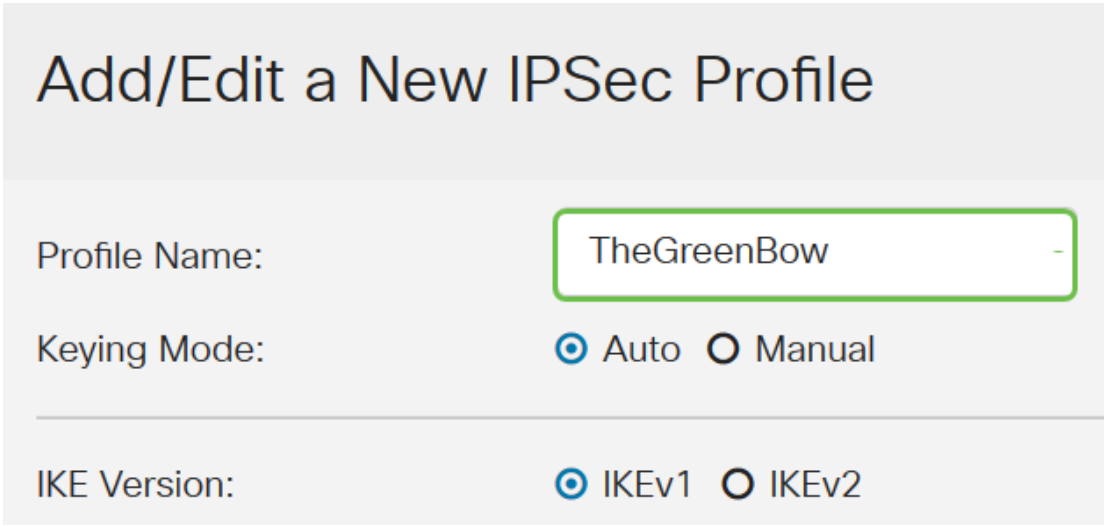
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des RV160- oder RV260-Routers an, und wählen Sie **VPN > IPSec VPN > IPSec-Profile aus**.

Schritt 2: Die IPSec-Profiltabelle zeigt die vorhandenen Profile. Klicken Sie auf das **Pluszeichen**, um ein neues Profil zu erstellen.



Hinweis: Amazon_Web_Services, Default und Microsoft_Azure sind Standardprofile.

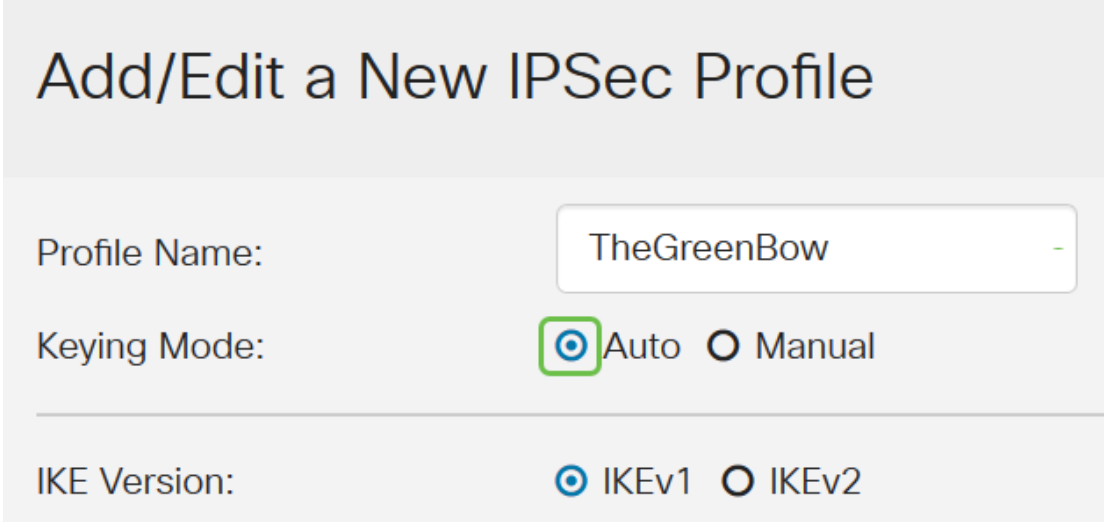
Schritt 3: Erstellen Sie im Feld *Profilname* einen Namen für das Profil. Der Profilname darf nur alphanumerische Zeichen und ein Unterstrich (_) für Sonderzeichen enthalten.



Schritt 4: Klicken Sie auf ein Optionsfeld, um die Schlüsselaustauschmethode für die Authentifizierung des Profils festzulegen. Folgende Optionen stehen zur Verfügung:

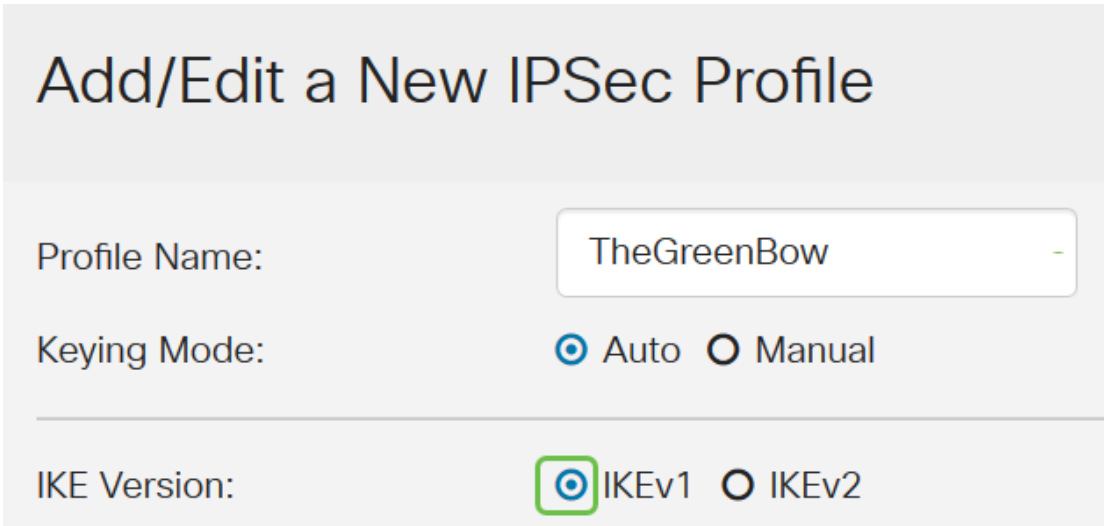
- Auto (Automatisch): Richtlinienparameter werden automatisch festgelegt. Diese Option verwendet eine IKE-Richtlinie (Internet Key Exchange) für Datenintegrität und Verschlüsselungsschlüssel-Austausch. Wenn diese Option ausgewählt ist, sind die

Konfigurationseinstellungen im Bereich Auto Policy Parameters (Parameter für automatische Richtlinie) aktiviert.
- Manual (Manuell): Mit dieser Option können Sie die Schlüssel für Datenverschlüsselung und -integrität für den VPN-Tunnel manuell konfigurieren. Wenn diese Option ausgewählt ist, werden die Konfigurationseinstellungen im Bereich "Manuelle Richtlinienparameter" aktiviert. Dies wird nicht häufig verwendet.



Hinweis: Für dieses Beispiel wurde **Auto** ausgewählt.

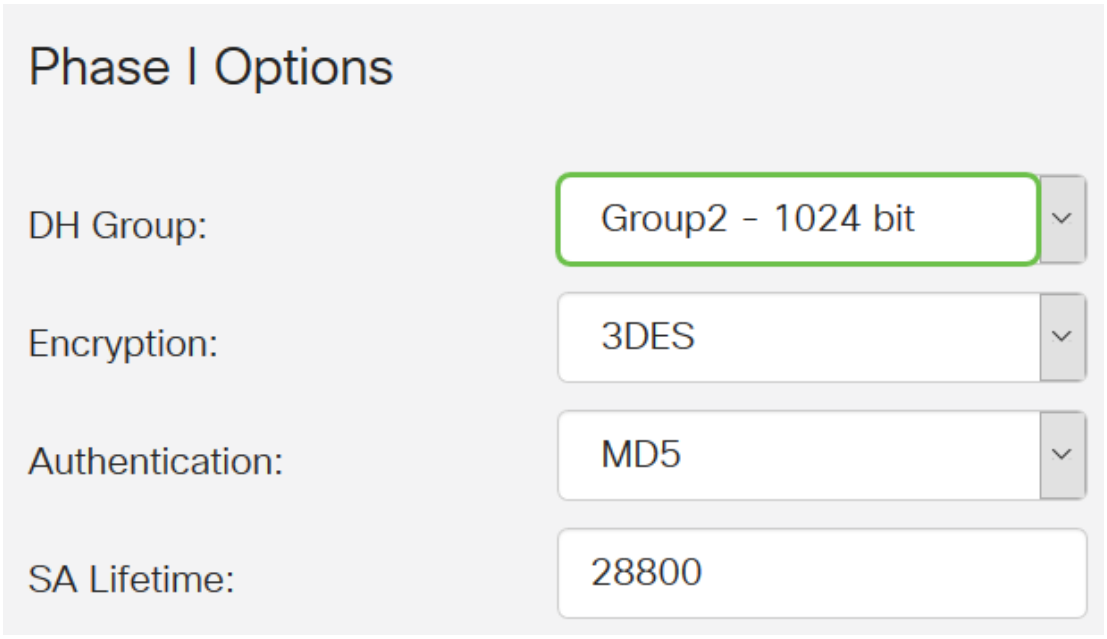
Schritt 5: Wählen Sie die IKE-Version aus. Stellen Sie sicher, dass beim Einrichten von TheGreenBow auf Clientseite dieselbe Version ausgewählt ist.



Konfigurieren der Einstellungen für Phase 1 und 2

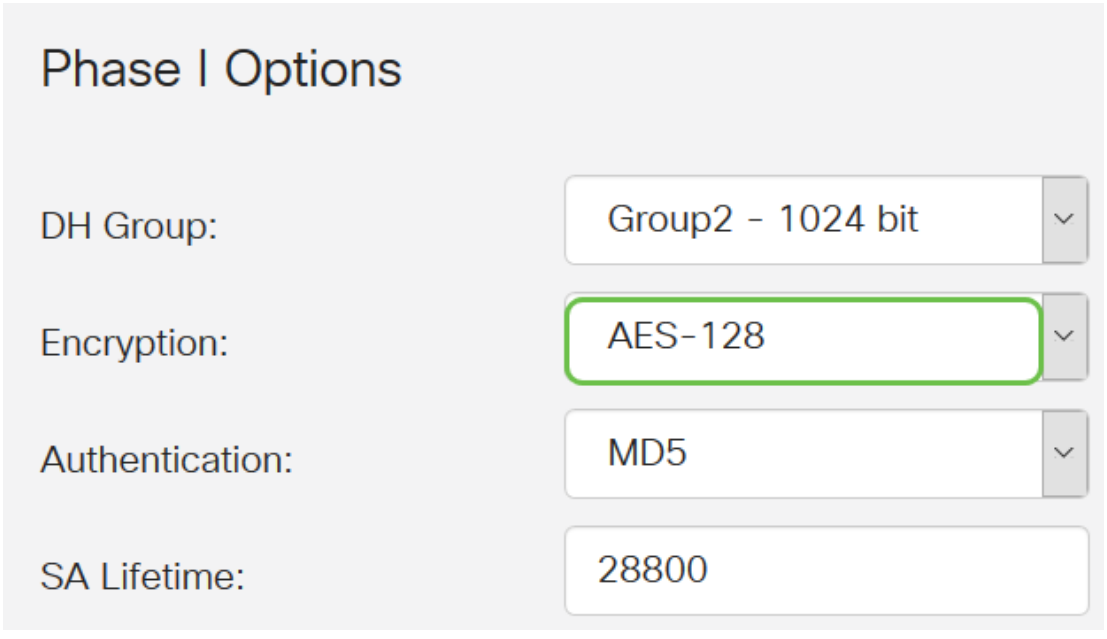
Schritt 1: Wählen Sie im Bereich Phase 1-Optionen die entsprechende Diffie-Hellman-Gruppe (DH) aus der Dropdown-Liste *DH Group* (DH-Gruppe) aus, die mit dem Schlüssel in Phase 1 verwendet werden soll. Diffie-Hellman ist ein kryptografisches Schlüsselaustauschprotokoll, das bei der Verbindung zum Austausch von vorinstallierten Schlüsselsätzen verwendet wird. Die Stärke des Algorithmus wird durch Bits bestimmt. Folgende Optionen stehen zur Verfügung:

- Group2-1024 bit (Gruppe2-1024 Bit): Diese Option berechnet den Schlüssel langsamer, ist aber sicherer als Gruppe 1.
- Group5-1536 bit (Gruppe5-156 Bit): Diese Option berechnet den Schlüssel am langsamsten, aber am sichersten.



Schritt 2: Wählen Sie aus der Dropdown-Liste *Encryption* eine Verschlüsselungsmethode zum Verschlüsseln und Entschlüsseln der Encapsulating Security Payload (ESP) und der Internet Security Association and Key Management Protocol (ISAKMP). Folgende Optionen stehen zur Verfügung:

- 3DES - Triple Data Encryption Standard. Nicht empfohlen. Verwenden Sie sie nur, wenn sie für die Abwärtskompatibilität erforderlich ist, da sie für einige "Block-Kollision"-Angriffe anfällig ist.
- AES-128 - Advanced Encryption Standard verwendet einen 128-Bit-Schlüssel. 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.
- AES-192 - Advanced Encryption Standard verwendet einen 192-Bit-Schlüssel.
- AES-256 - Advanced Encryption Standard verwendet einen 256-Bit-Schlüssel. Dies ist die sicherste Verschlüsselungsoption.

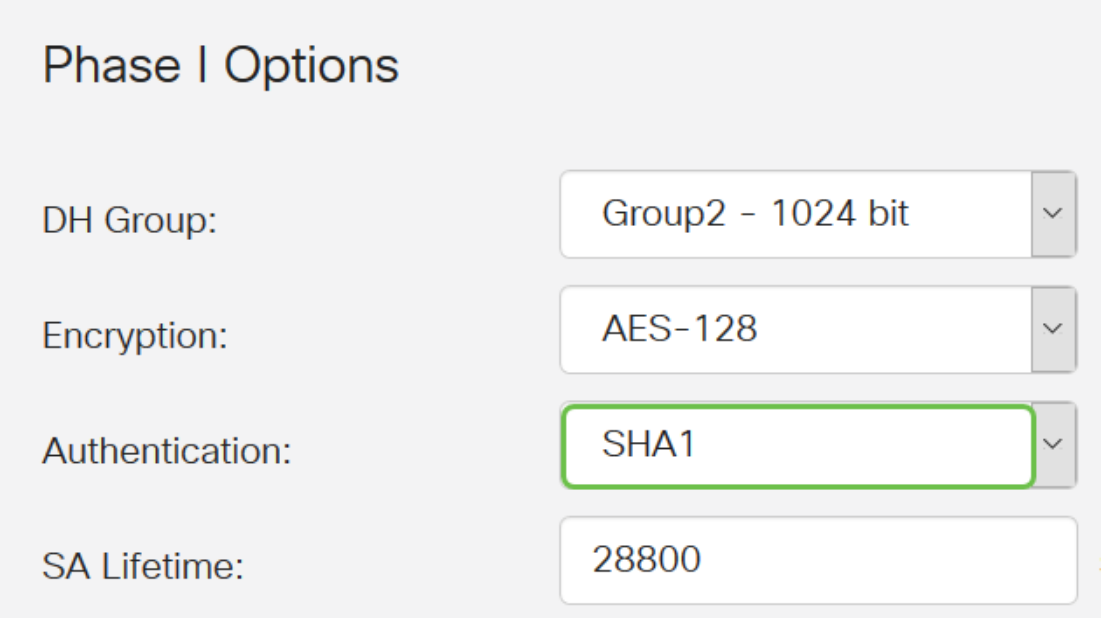


Hinweis: AES ist die Standardmethode zur Verschlüsselung über DES und 3DES für mehr Leistung und Sicherheit. Durch die Verlängerung des AES-Schlüssels wird die Sicherheit mit einem Leistungsabfall erhöht.

Schritt 3: Wählen Sie aus der Dropdown-Liste *Authentication (Authentifizierung)* eine Authentifizierungsmethode aus, die bestimmt, wie ESP und ISAKMP authentifiziert werden. Folgende Optionen stehen zur Verfügung:

- MD5 - Message-Digest Algorithm hat einen 128-Bit-Hashwert.
- SHA-1 - Secure Hash Algorithm hat einen 160-Bit-Hashwert.
- SHA2-256 - Sicherer Hash-Algorithmus mit einem Hashwert von 256 Bit. Dies ist der sicherste und empfohlene Algorithmus.

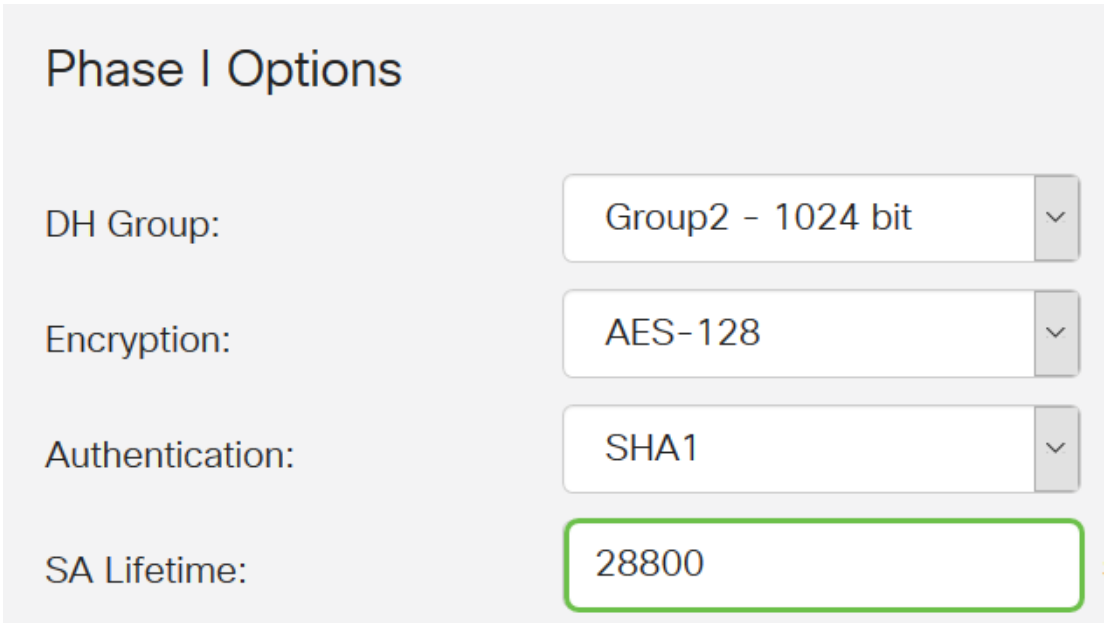
Hinweis: Stellen Sie sicher, dass beide Enden des VPN-Tunnels dieselbe Authentifizierungsmethode verwenden.



Hinweis: MD5 und SHA sind beide kryptografische Hashfunktionen. Sie nehmen Daten, kompilieren sie und erstellen eine eindeutige Hexadezimalausgabe, die normalerweise nicht reproduziert werden kann. In diesem Beispiel wird SHA1 ausgewählt.

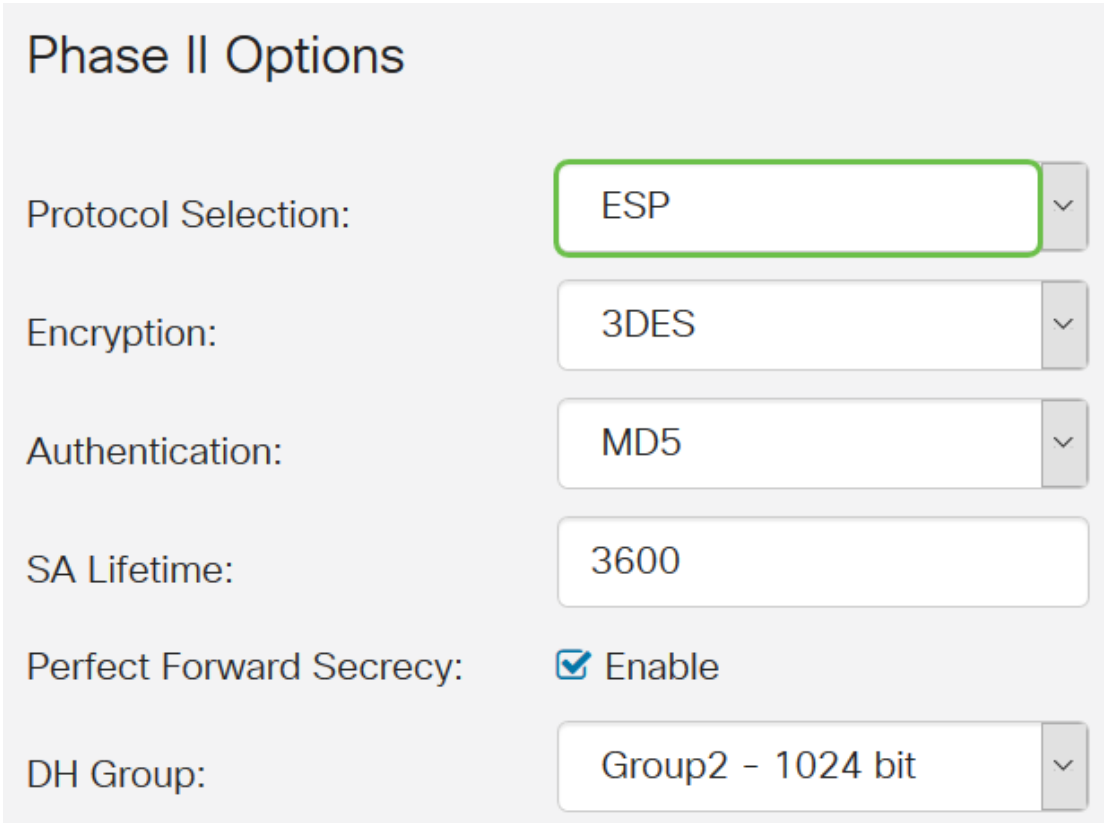
Schritt 4: Geben Sie im Feld *SA Lifetime* (SA-Lebensdauer) einen Wert zwischen 120 und 86400 ein. Der Standardwert ist 28800. Die *SA Lifetime (Sec)* gibt Ihnen die Zeitdauer (in Sekunden) an, die eine IKE SA in dieser Phase aktiv ist. Vor Ablauf der Lebensdauer wird eine neue Security Association (SA) 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 28800 Sekunden als 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.



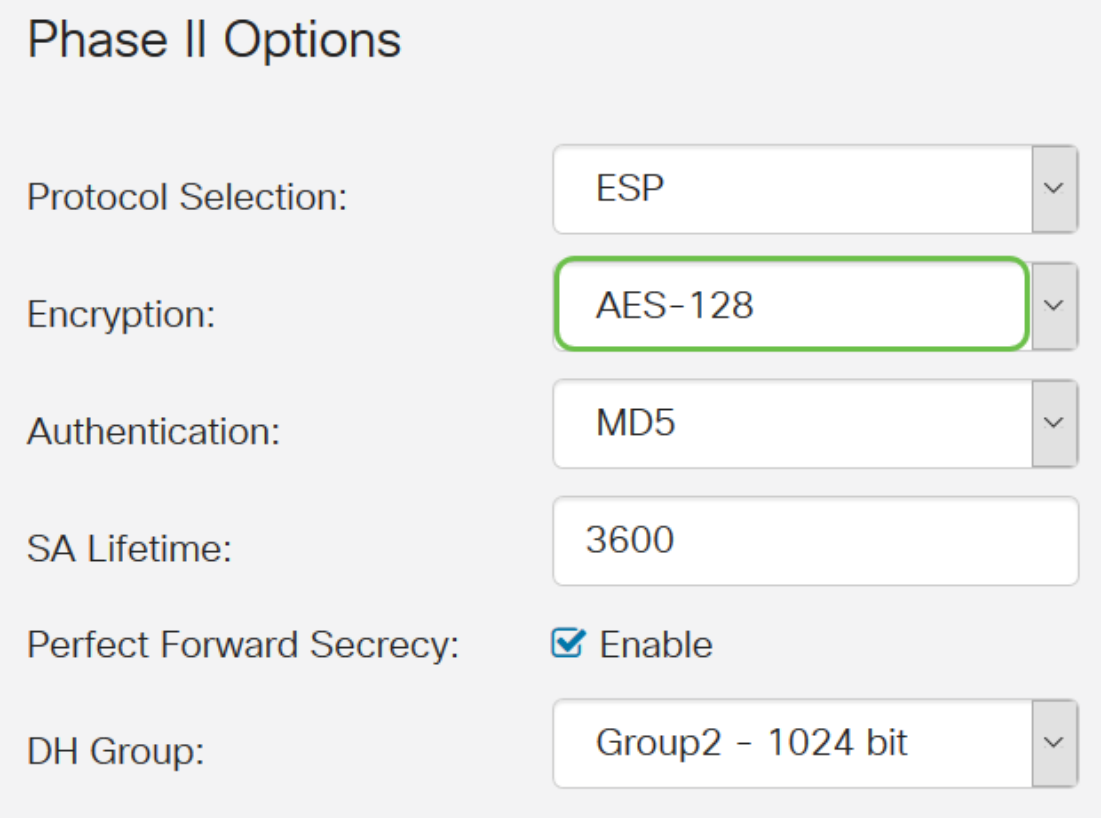
Schritt 5: Wählen Sie aus der Dropdown-Liste *Protocol Selection* (Protokollauswahl) im Bereich Phase II Options (Optionen für Phase II) einen Protokolltyp aus, der auf die zweite Verhandlungsphase angewendet werden soll. Folgende Optionen stehen zur Verfügung:

- ESP - Diese Option wird auch als Encapsulating Security Payload (SicherheitsPayload einkapseln) bezeichnet. Diese Option kapselt die zu schützenden Daten. Wenn diese Option ausgewählt ist, fahren Sie mit Schritt 6 fort, um eine Verschlüsselungsmethode auszuwählen.
- AH - Diese Option wird auch als Authentication Header (AH) bezeichnet. Es ist ein Sicherheitsprotokoll, das Datenauthentifizierung und optionalen Anti-Replay-Dienst bietet. AH ist in das zu schützende IP-Datagramm integriert. Wenn diese Option ausgewählt ist, fahren Sie mit Schritt 7 fort.



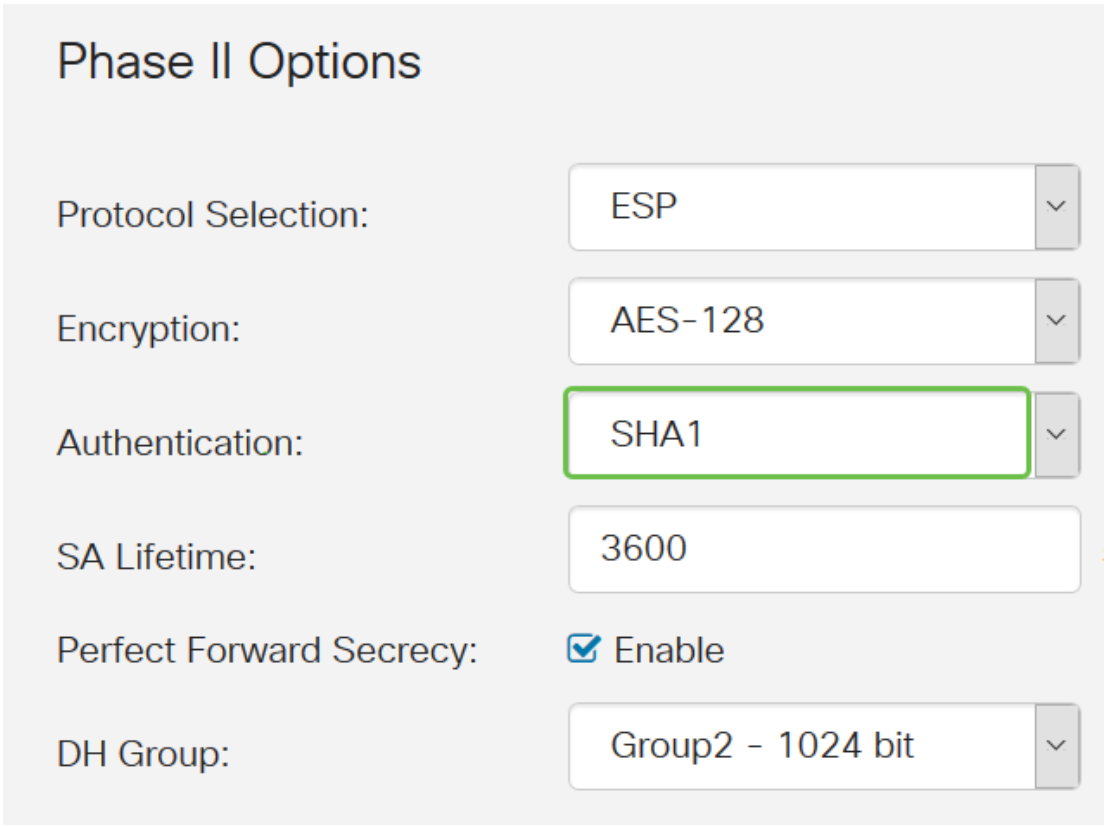
Schritt 6: Wenn in Schritt 6 ESP ausgewählt wurde, wählen Sie eine *Verschlüsselung*. Folgende Optionen stehen zur Verfügung:

- 3DES = Triple Data Encryption Standard
- AES-128 - Advanced Encryption Standard verwendet einen 128-Bit-Schlüssel.
- AES-192 - Advanced Encryption Standard verwendet einen 192-Bit-Schlüssel.
- AES-256 - Advanced Encryption Standard verwendet einen 256-Bit-Schlüssel.

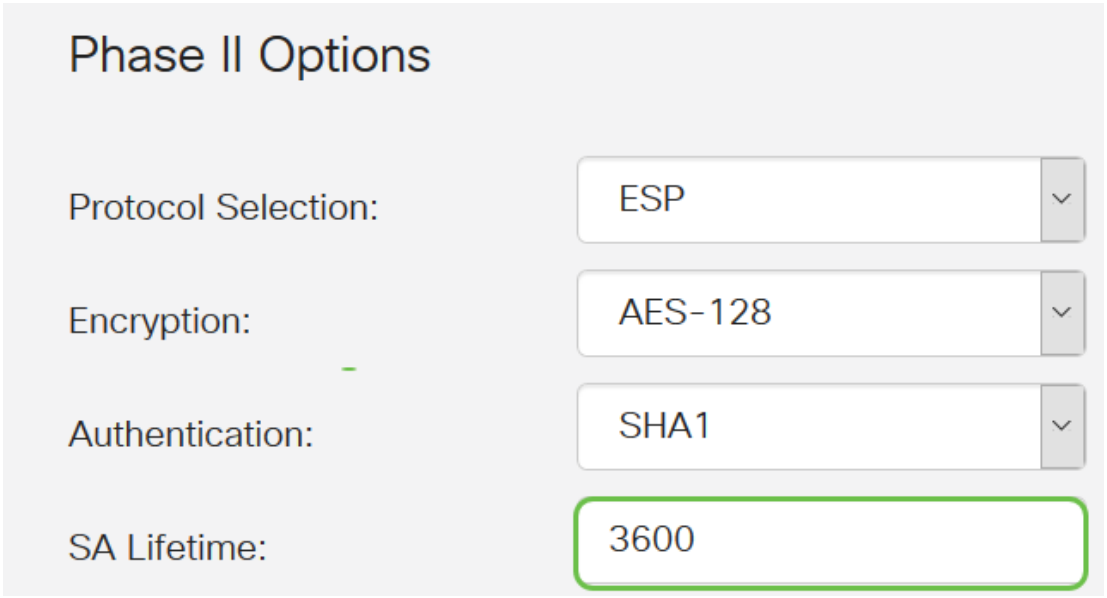


Schritt 7: Wählen Sie aus der Dropdown-Liste *Authentication (Authentifizierung)* eine Authentifizierungsmethode aus, die bestimmt, wie ESP und ISAKMP authentifiziert werden. Folgende Optionen stehen zur Verfügung:

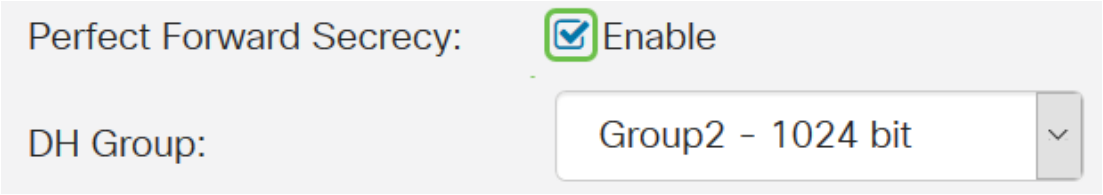
- MD5 - Message-Digest Algorithm hat einen 128-Bit-Hashwert.
- SHA-1 - Secure Hash Algorithm hat einen 160-Bit-Hashwert.
- SHA2-256 - Sicherer Hash-Algorithmus mit einem Hashwert von 256 Bit.



Schritt 8: Geben Sie im Feld *SA Lifetime* (SA-Lebensdauer) einen Wert zwischen 120 und 28800 ein. Dies ist die Dauer, die die IKE SA in dieser Phase aktiv bleiben wird. Der Standardwert ist 3600.

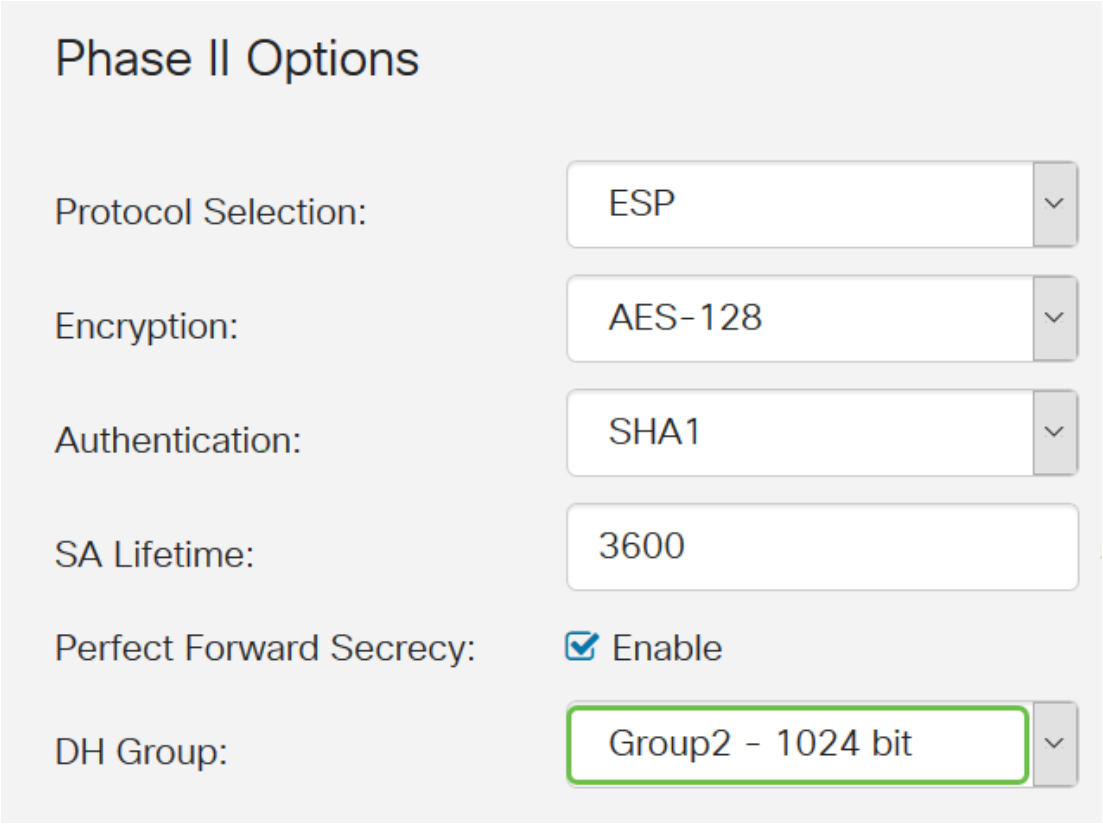


Schritt 9: (Optional) Aktivieren Sie das Kontrollkästchen **Enable** Perfect Forward Secrecy (Perfektes Weiterleitungsgeheimnis **aktivieren**), um einen neuen Schlüssel für die Verschlüsselung und Authentifizierung des IPsec-Datenverkehrs zu generieren. Perfect Forward Secrecy wird verwendet, um die 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.

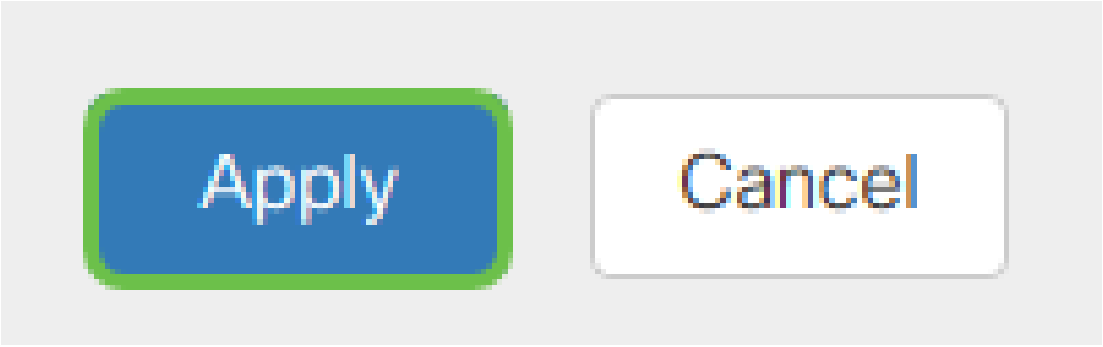


Schritt 10: Wählen Sie aus der Dropdown-Liste *DH Group* (DH-Gruppe) eine DH-Gruppe aus, die mit dem Schlüssel in Phase 2 verwendet werden soll. Folgende Optionen stehen zur Verfügung:

- Group2-1024 Bit: Diese Option berechnet den Schlüssel schneller, aber weniger sicher.
- Group5-1536 bit (Gruppe5-156 Bit): Diese Option berechnet den Schlüssel am langsamsten, aber am sichersten.

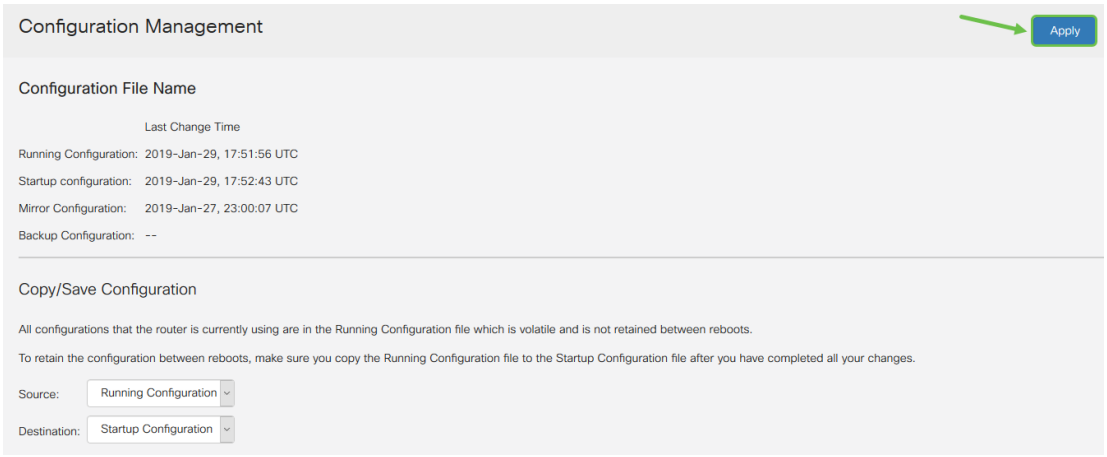


Schritt 11: Klicken Sie auf **Übernehmen**.

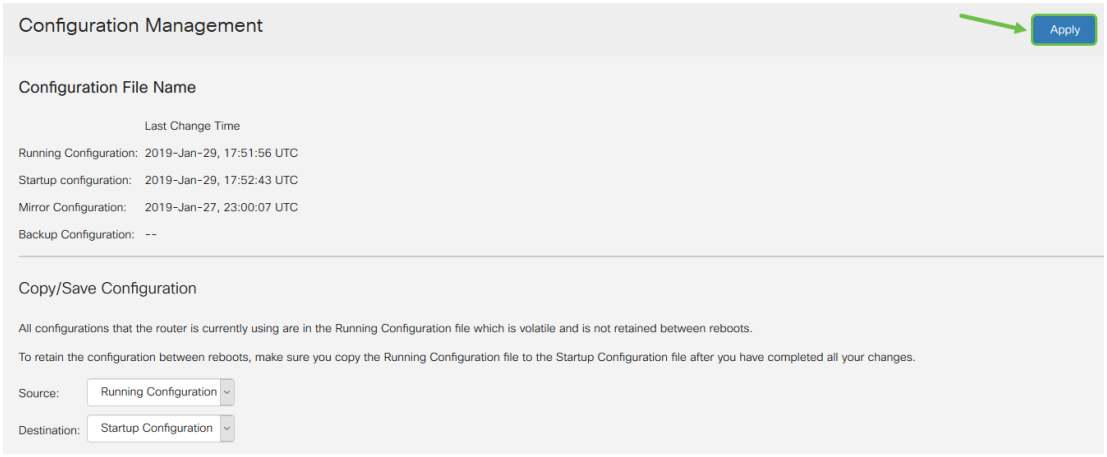


Schritt 12: Klicken Sie auf **Speichern**, um die Konfiguration dauerhaft zu speichern.

Schritt 13: Klicken Sie erneut auf **Apply**, um die aktuelle Konfiguration in der Startkonfiguration zu speichern.



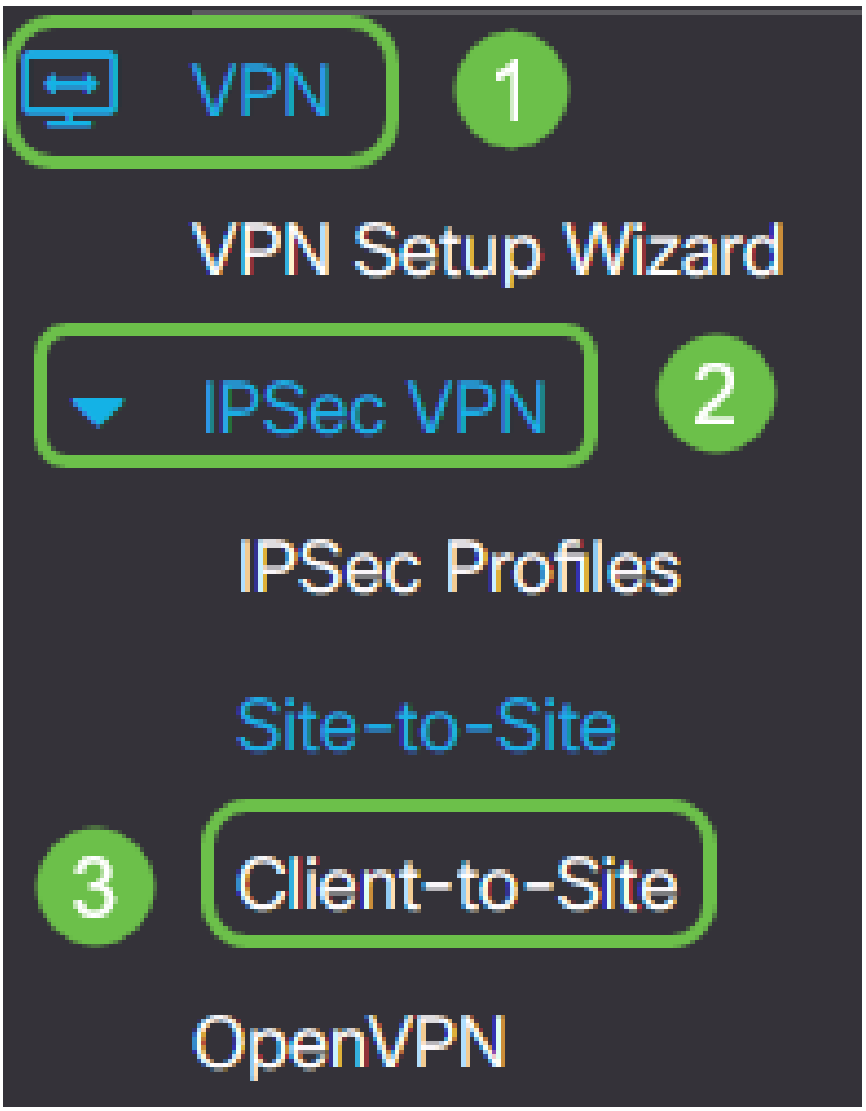
Schritt 14: Wenn Sie die Bestätigung erhalten, klicken Sie auf **OK**.



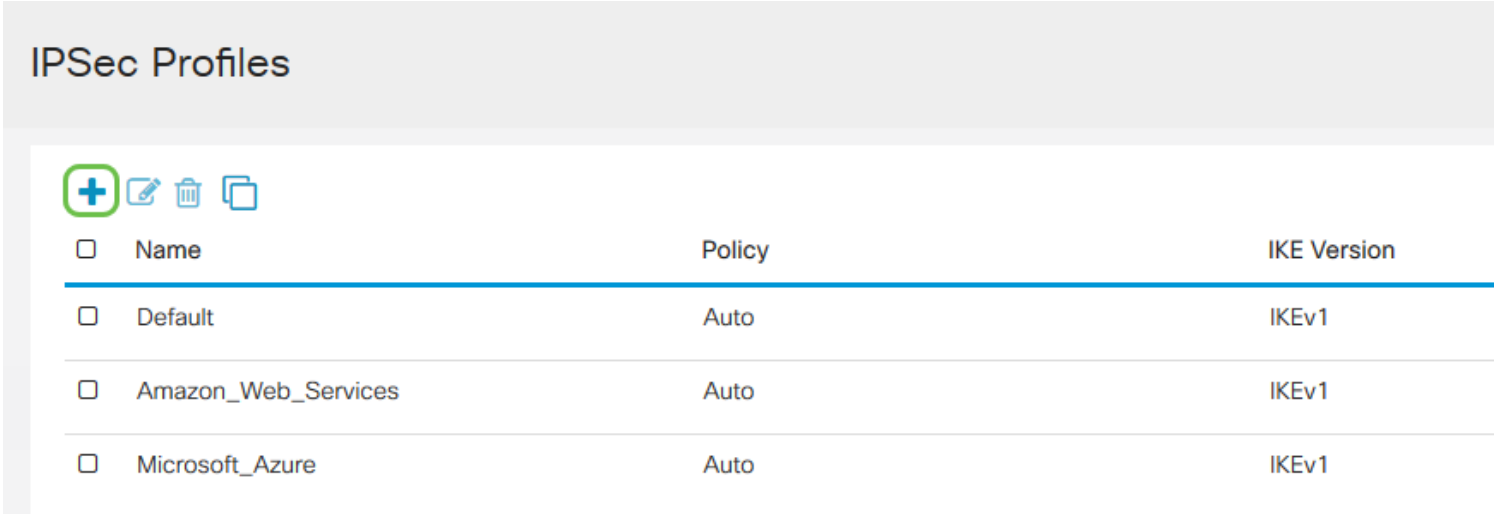
Sie sollten jetzt ein IPsec-Profil auf Ihrem RV160- oder RV260-Router erfolgreich konfiguriert haben.

Erstellen eines Client-to-Site-Profils

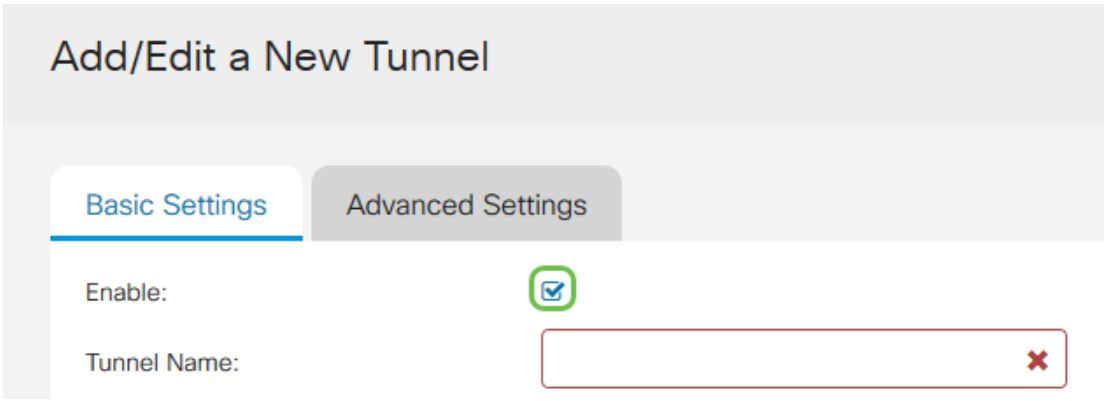
Schritt 1: Wählen Sie **VPN > IPSec VPN > Client-to-Site aus**.



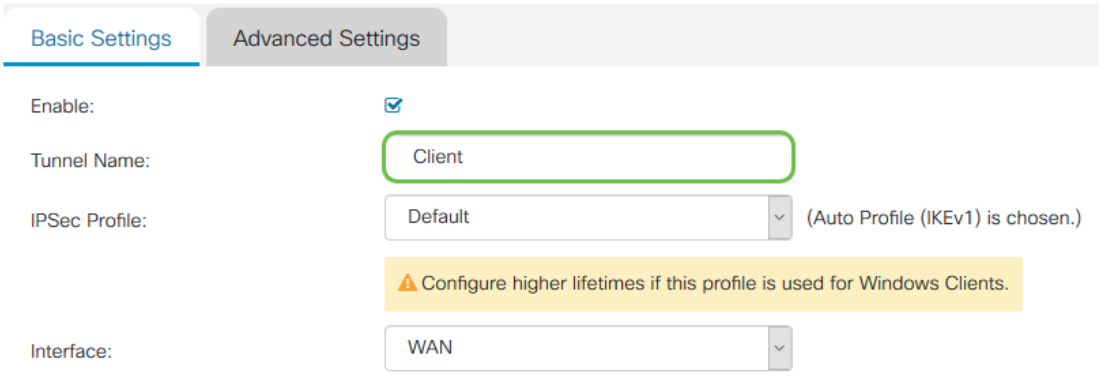
Schritt 2: Klicken Sie auf das **Pluszeichen**.



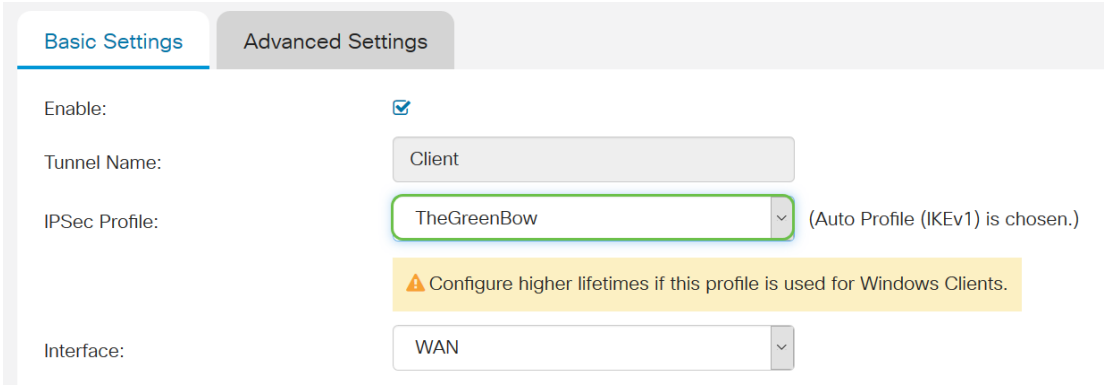
Schritt 3: Aktivieren Sie auf der Registerkarte Basiseinstellungen das Kontrollkästchen **Aktivieren**, um sicherzustellen, dass das VPN-Profil aktiv ist.



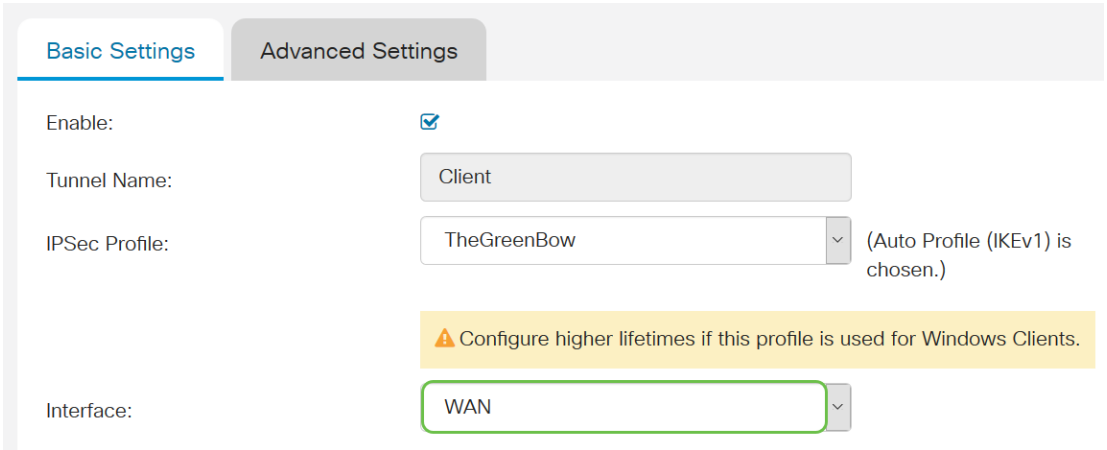
Schritt 4: Geben Sie im Feld *Tunnel Name* einen Namen für die VPN-Verbindung ein.



Schritt 5: Wählen Sie aus der Dropdown-Liste *IPsec* Profile (IPsec-Profil) aus, das verwendet werden soll.



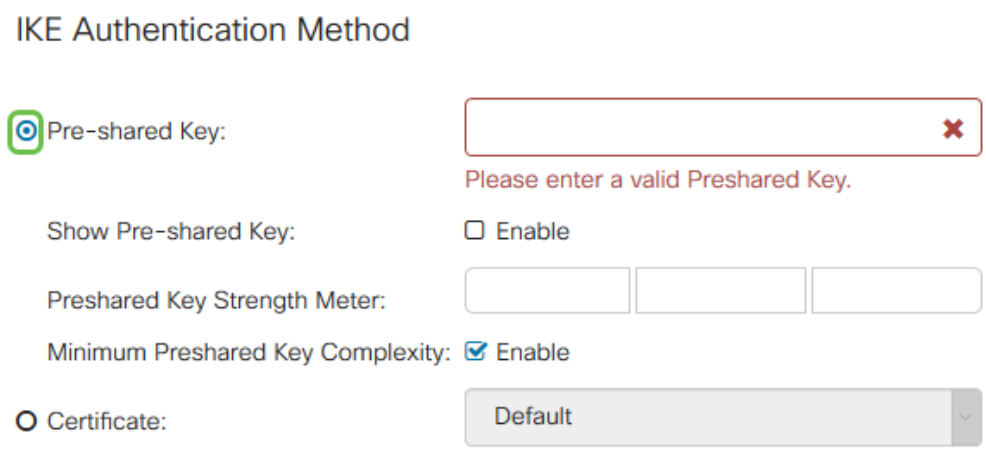
Schritt 6: Wählen Sie die Schnittstelle aus der Dropdown-Liste *Interface (Schnittstelle*) aus.



Hinweis: Die Optionen hängen vom verwendeten Router-Modell ab. In diesem Beispiel wird WAN ausgewählt.

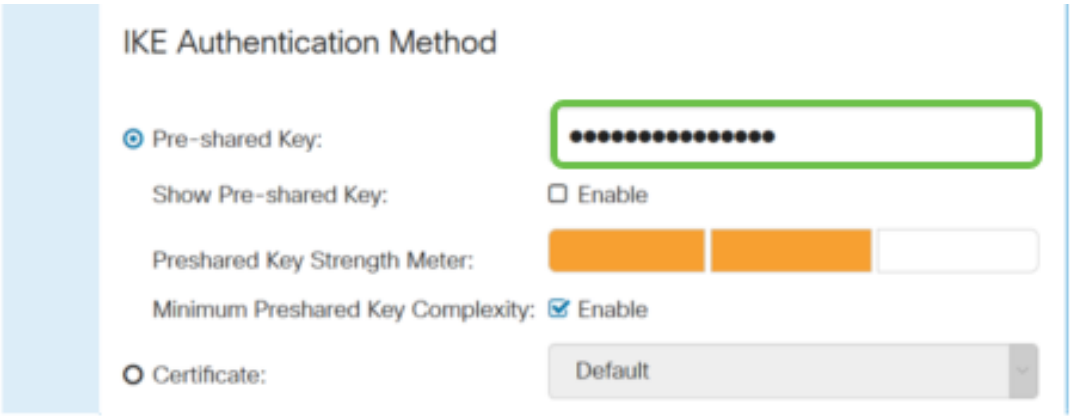
Schritt 7: Wählen Sie eine IKE-Authentifizierungsmethode aus. Folgende Optionen stehen zur Verfügung:

- Pre-shared Key (Vorinstallierter Schlüssel): Mit dieser Option können wir ein freigegebenes Kennwort für die VPN-Verbindung verwenden.
- Zertifikat: Diese Option verwendet ein digitales Zertifikat, das Informationen wie den Namen oder die IP-Adresse, die Seriennummer, das Ablaufdatum des Zertifikats und eine Kopie des öffentlichen Schlüssels des Inhabers des Zertifikats enthält.

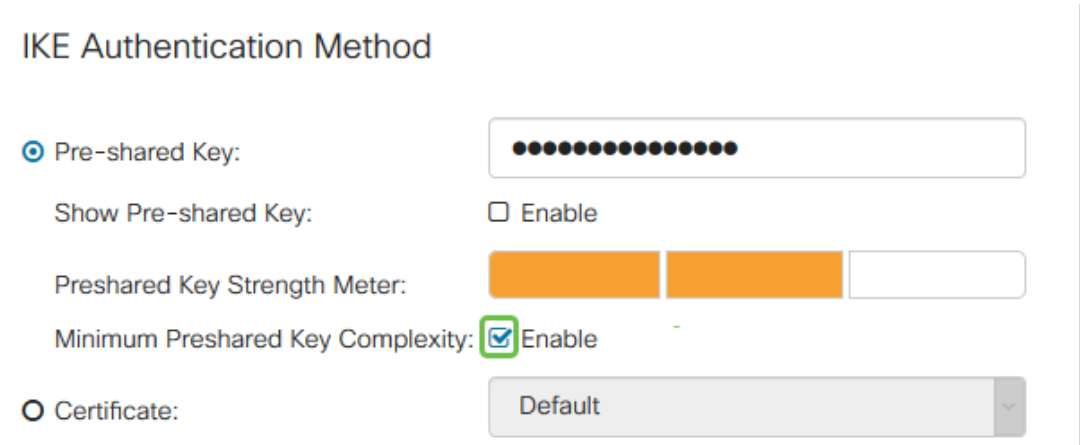


Hinweis: Ein Pre-Shared Key kann sein, was Sie wollen, es muss nur auf der Website und mit dem Client, wenn sie die Einrichtung von TheGreenBow Client auf ihrem Computer.

Schritt 8: Geben Sie das Verbindungskennwort in das Feld *Vorinstallierter Schlüssel ein*.

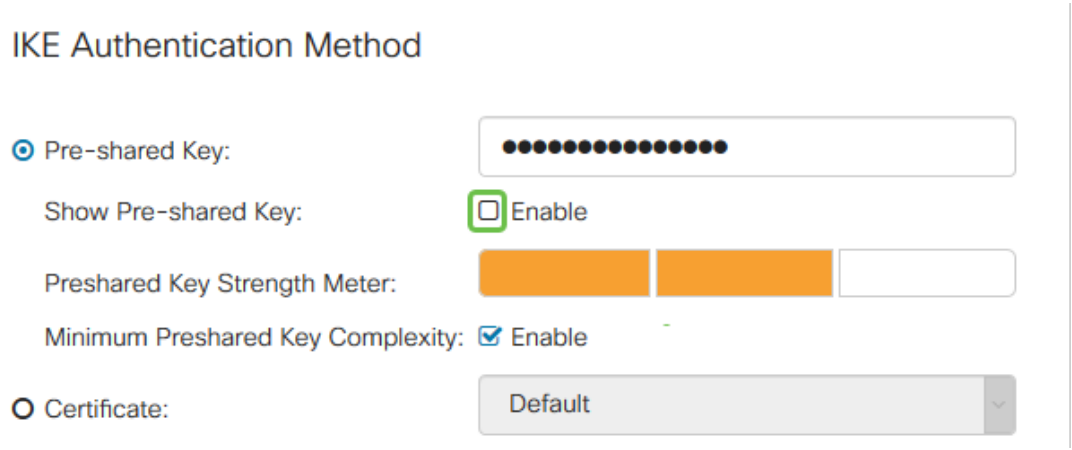


Schritt 9: (Optional) Deaktivieren Sie das Kontrollkästchen *Minimale Komplexität des vorinstallierten Schlüssels* **Aktivieren**, um ein einfaches Kennwort verwenden zu können.



Hinweis: In diesem Beispiel bleibt die minimale Komplexität des vorinstallierten Schlüssels aktiviert.

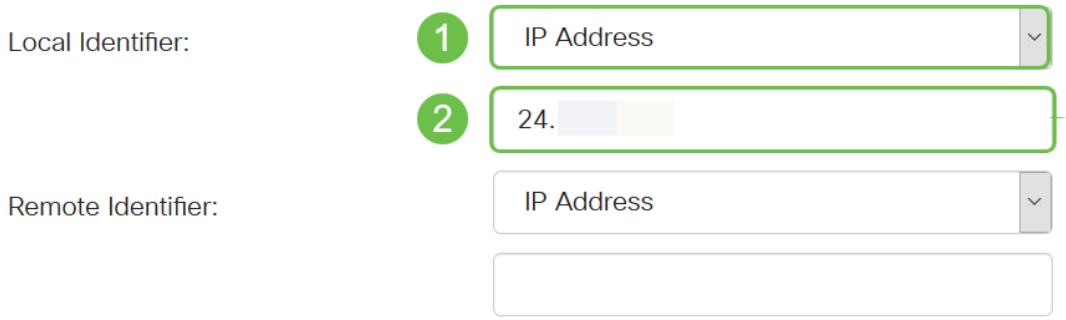
Schritt 10: (Optional) Aktivieren Sie das Kontrollkästchen *Vorinstallierten Schlüssel* **aktivieren** *anzeigen*, um das Kennwort im Klartext anzuzeigen.



Hinweis: In diesem Beispiel wird "Vorinstallierter Schlüssel anzeigen" deaktiviert.

Schritt 11: Wählen Sie eine lokale ID aus der Dropdown-Liste *Local Identifier* aus. Folgende Optionen stehen zur Verfügung:

- Local WAN IP (Lokale WAN-IP): Diese Option verwendet die IP-Adresse der WAN-Schnittstelle (Wide Area Network) des VPN-Gateways.
- IP Address (IP-Adresse): Mit dieser Option können Sie manuell eine IP-Adresse für die VPN-Verbindung eingeben. Dies ist die WAN-IP-Adresse des Routers am Standort (Büro).
- FQDN - Diese Option wird auch als Fully Qualified Domain Name (FQDN) bezeichnet. Sie können einen vollständigen Domänennamen für einen bestimmten Computer im Internet verwenden.
- User FQDN (Benutzer-FQDN): Mit dieser Option können Sie einen vollständigen Domänennamen für einen bestimmten Benutzer im Internet verwenden.

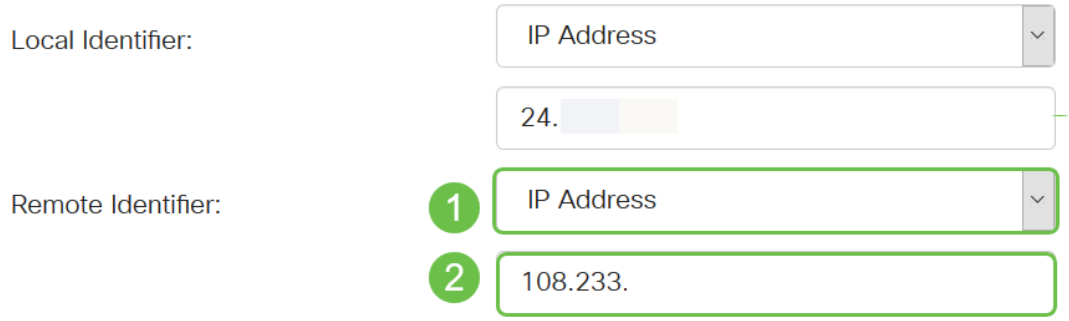


Hinweis: In diesem Beispiel wird die IP-Adresse ausgewählt und die WAN-IP-Adresse des Routers am Standort eingegeben. In diesem Beispiel wurde 24.x.x.x eingegeben. Die vollständige Adresse wurde aus Datenschutzgründen verschwommen.

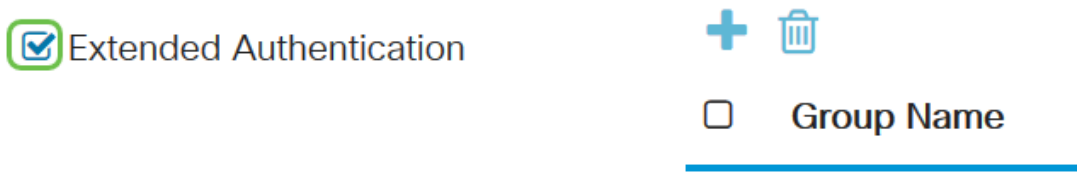
Schritt 12: Wählen Sie eine Kennung für den Remotehost aus. Folgende Optionen stehen zur Verfügung:

- IP Address (IP-Adresse): Diese Option verwendet die WAN-IP-Adresse des VPN-Clients. Um die WAN-IP-Adresse zu erfahren, können Sie "What is my IP" (Was ist meine IP) in Ihren Webbrowser eingeben. Dies ist die Client-IP-Adresse.
- FQDN - Vollqualifizierter Domänenname. Mit dieser Option können Sie einen vollständigen Domänennamen für einen bestimmten Computer im Internet verwenden.
- User FQDN (Benutzer-FQDN): Mit dieser Option können Sie einen vollständigen Domänennamen für einen bestimmten Benutzer im Internet verwenden.

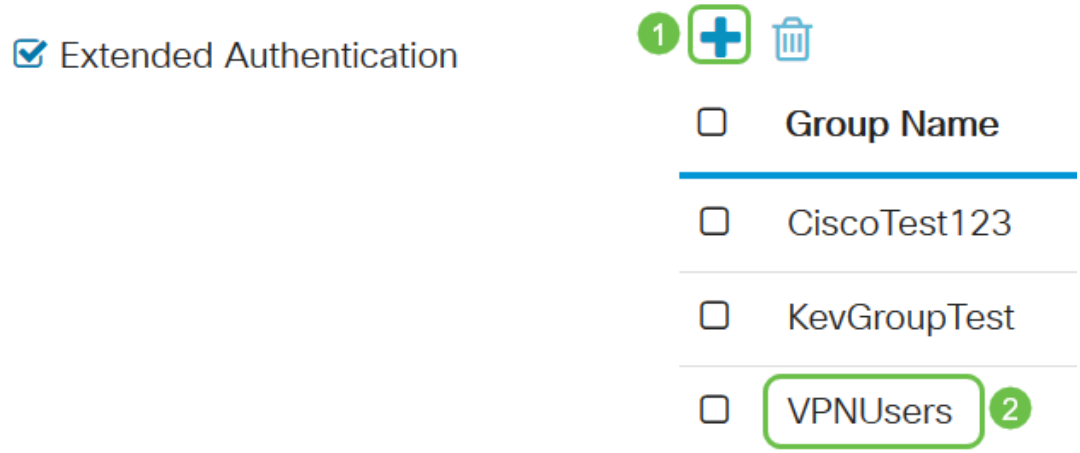
Hinweis: In diesem Beispiel wird die IP-Adresse ausgewählt und die aktuelle IPv4-Adresse des Routers am Standort des Clients eingegeben. Dies lässt sich durch die Suche nach "What's my IP address" (Meine IP-Adresse) in Ihrem Webbrowser feststellen. Diese Adresse kann sich ändern. Wenn Sie nach einer erfolgreichen Konfiguration Probleme bei der Verbindung haben, kann dies sowohl auf dem Client als auch am Standort überprüft und geändert werden.



Schritt 13: (Optional) Aktivieren Sie das Kontrollkästchen **Erweiterte Authentifizierung**, um die Funktion zu aktivieren. Wenn diese Option aktiviert ist, wird eine zusätzliche Authentifizierungsstufe bereitgestellt, bei der Remote-Benutzer ihre Anmeldeinformationen eingeben müssen, bevor sie Zugriff auf das VPN erhalten.



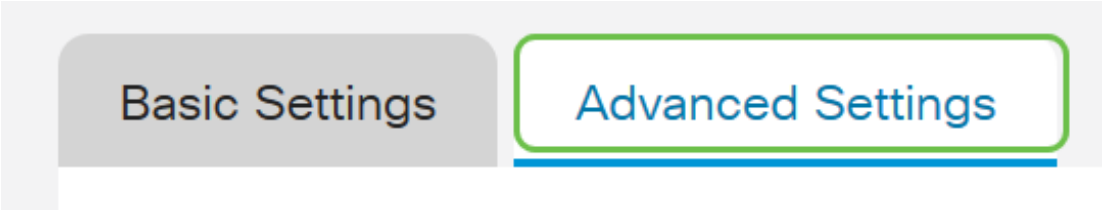
Schritt 14: (Optional) Wählen Sie die Gruppe aus, die die erweiterte Authentifizierung verwendet, indem Sie auf das **Plus-**Symbol klicken und den Benutzer aus der Dropdown-Liste auswählen.



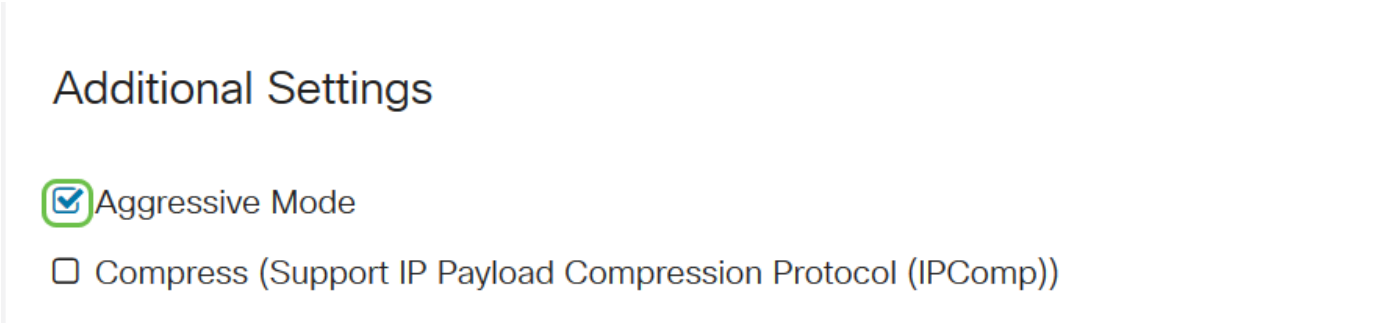
Hinweis: In diesem Beispiel werden **VPNUsers** ausgewählt.

Schritt 15: Geben Sie unter *Pool Range for Client LAN* (Pool-Bereich für Client-LAN) die erste IP- und End-IP-Adresse ein, die einem VPN-Client zugewiesen werden kann. Dabei muss es sich um einen Adresspool handeln, der sich nicht mit den Standortadressen überschneidet. Diese können auch als virtuelle Schnittstellen bezeichnet werden. Wenn Sie eine Meldung erhalten, dass eine virtuelle Schnittstelle geändert werden muss, können Sie dies beheben.

Schritt 16: Wählen Sie die Registerkarte **Erweiterte Einstellungen**.

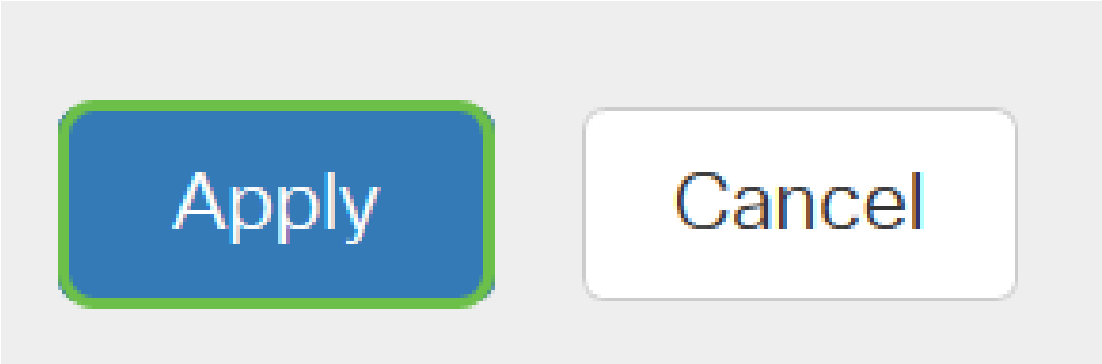


Schritt 17: (Optional) Blättern Sie nach unten zur Seite, und wählen Sie **Aggressive Mode (aggressiver Modus)** aus. Mithilfe der Funktion Aggressive Mode (Aggressiver Modus) können Sie RADIUS-Tunnelattribute für einen IP Security (IPsec)-Peer festlegen und eine IKE-Aggressive Mode-Aushandlung (Internet Key Exchange) mit dem Tunnel initiieren. Weitere Informationen zum aggressiven Modus und zum Hauptmodus finden Sie hier.

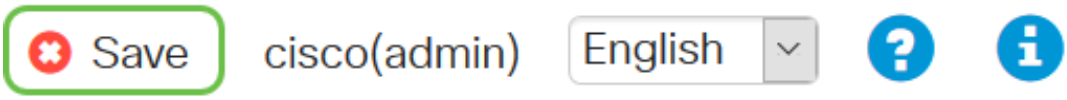


Hinweis: Das Kontrollkästchen Compress (Komprimieren) ermöglicht es dem Router, Komprimierung vorzuschlagen, wenn eine Verbindung gestartet wird. Dieses Protokoll reduziert die Größe von IP-Datagrammen. Wenn der Befrager dieses Angebot ablehnt, implementiert der Router keine Komprimierung. Wenn der Router der Responder ist, akzeptiert er Komprimierung, auch wenn die Komprimierung nicht aktiviert ist. Wenn Sie diese Funktion für diesen Router aktivieren, müssen Sie sie auf dem Remote-Router aktivieren (am anderen Ende des Tunnels). In diesem Beispiel wurde *Compress* deaktiviert.

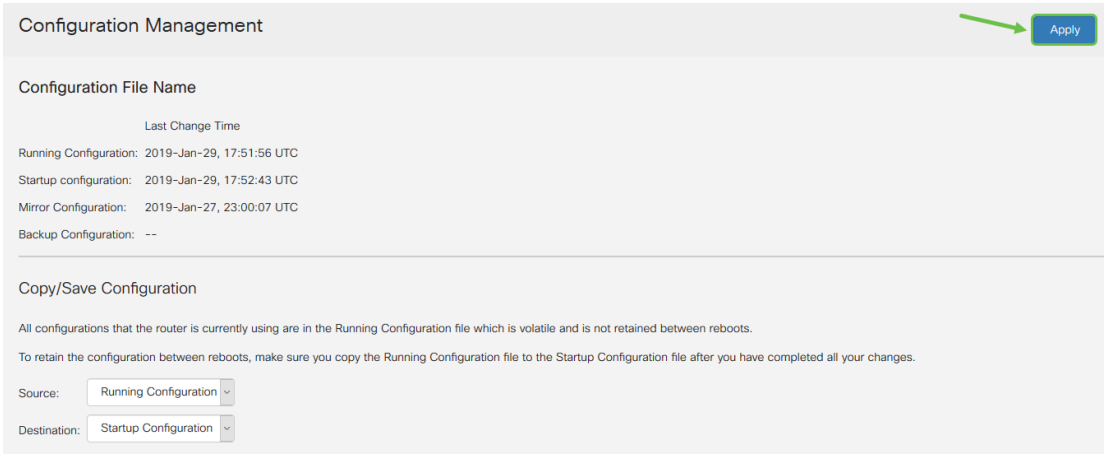
Schritt 18: Klicken Sie auf **Übernehmen**.



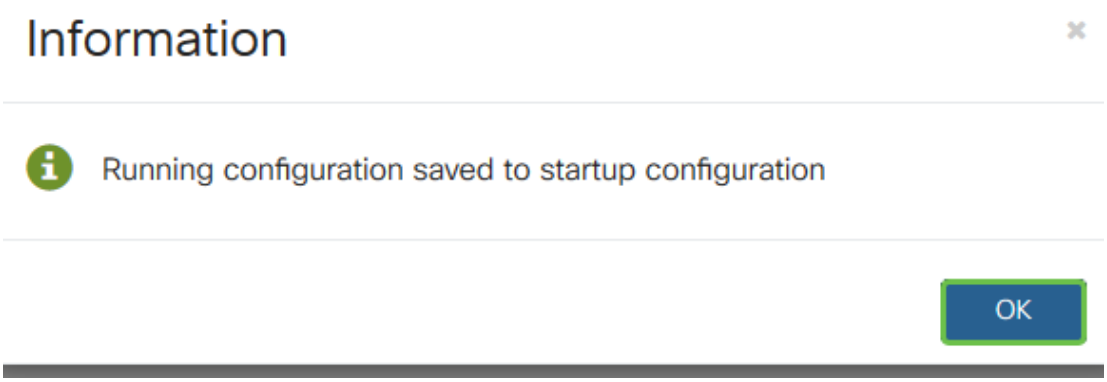
Schritt 19: Klicken Sie auf **Speichern**.



Schritt 20: Klicken Sie erneut auf **Apply**, um die aktuelle Konfiguration in der Startkonfiguration zu speichern.



Schritt 21: Wenn Sie die Bestätigung erhalten, klicken Sie auf **OK**.



Sie sollten jetzt den Client-to-Site-Tunnel auf dem Router für den GreenBow VPN-Client konfiguriert haben.

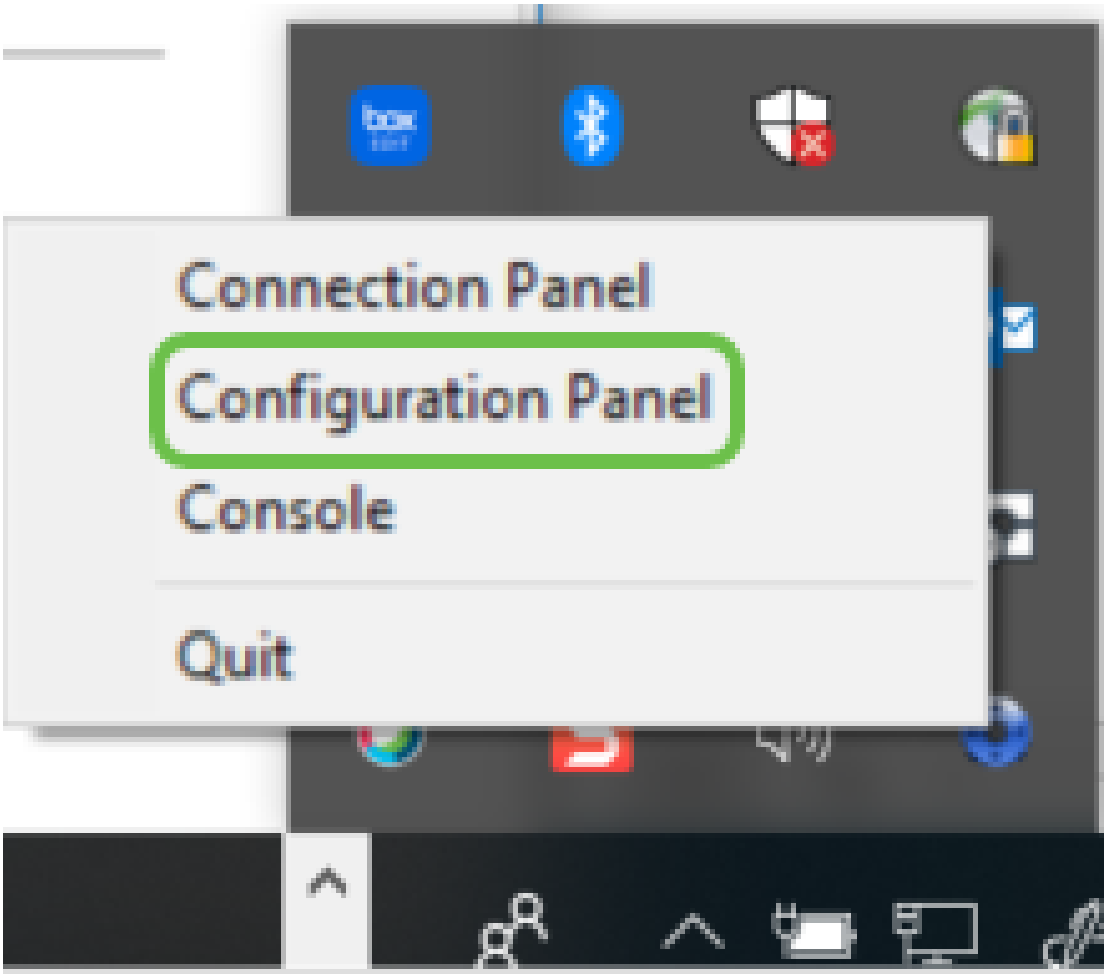
Konfigurieren des GreenBow VPN-Clients auf dem Computer des Remote-Mitarbeiters

Konfigurieren der Einstellungen für Phase 1

Klicken Sie hier, um die neueste Version von TheGreenBow IPsec VPN Client Software herunterzuladen.

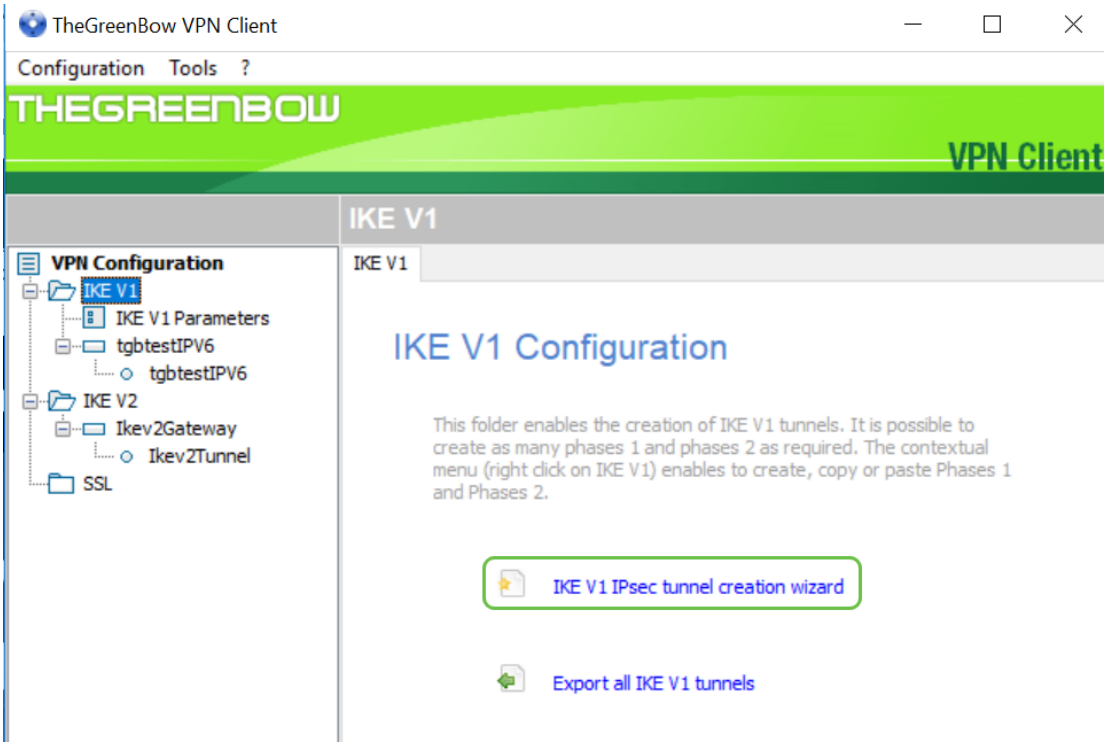
Schritt 1: Klicken Sie mit der rechten Maustaste auf das Symbol The GreenBow VPN Client. Diese befindet sich in der unteren rechten Ecke der Taskleiste.

Schritt 2: Wählen Sie **Konfigurationsleiste aus**.



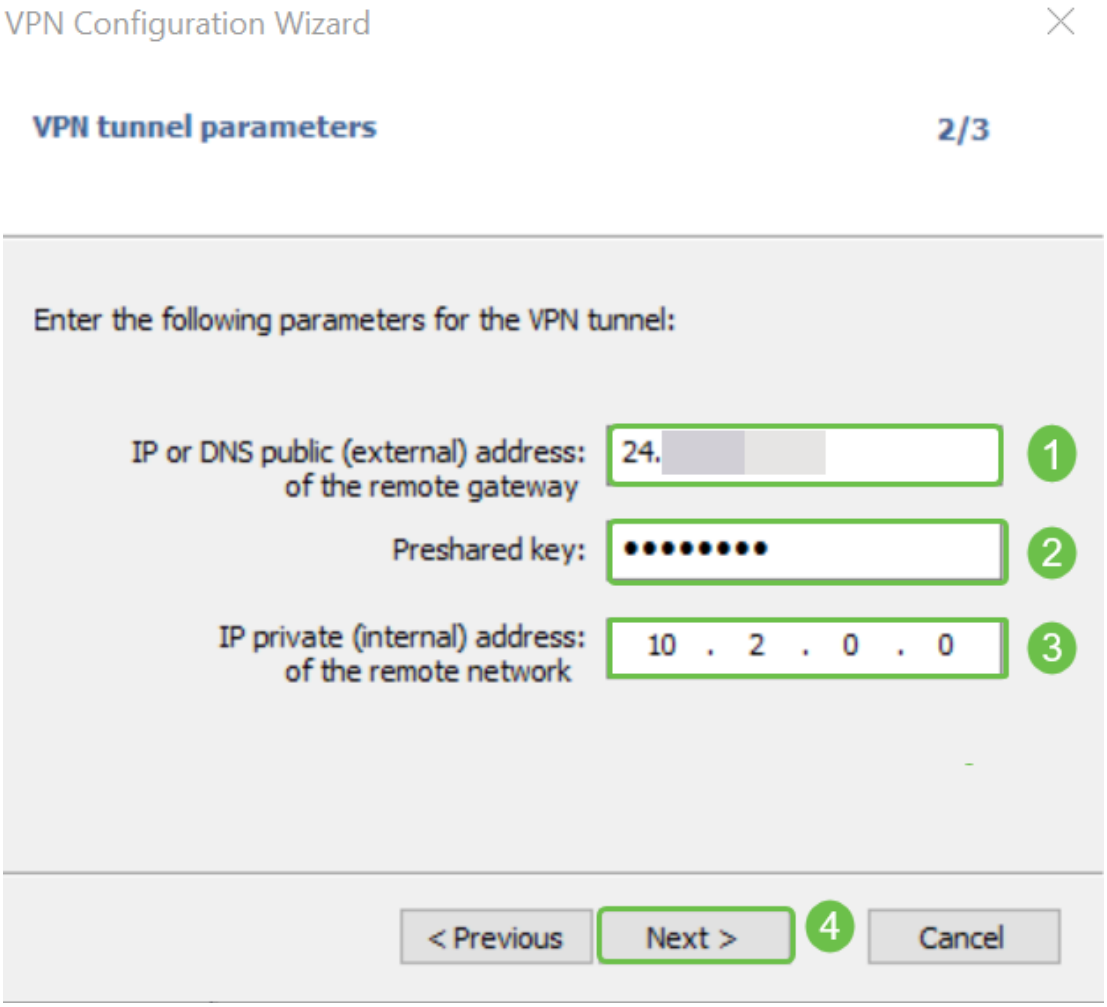
Hinweis: Dies ist ein Beispiel auf einem Windows-Computer. Dies kann je nach Software variieren.

Schritt 3: Wählen Sie **den IKE V1 IPsec-Tunnelerstellungsassistenten aus**.

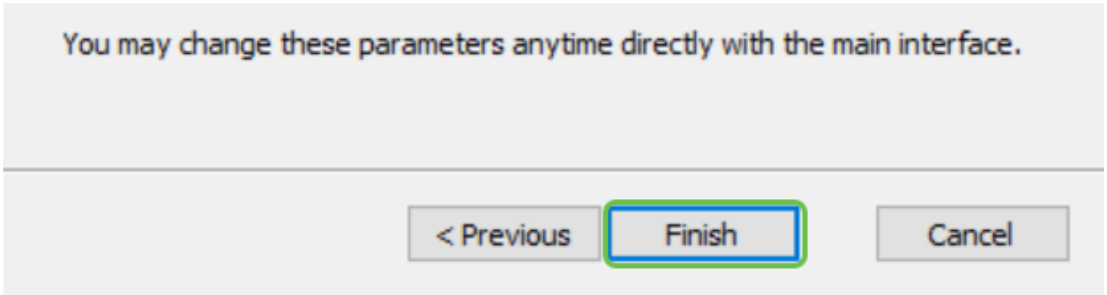


Hinweis: In diesem Beispiel wird IKE-Version 1 konfiguriert. Wenn Sie IKE Version 2 konfigurieren möchten, gehen Sie wie folgt vor, klicken Sie jedoch mit der rechten Maustaste auf den Ordner IKE V2. Sie müssen außerdem IKEv2 für das IPsec-Profil auf dem Router am Standort auswählen.

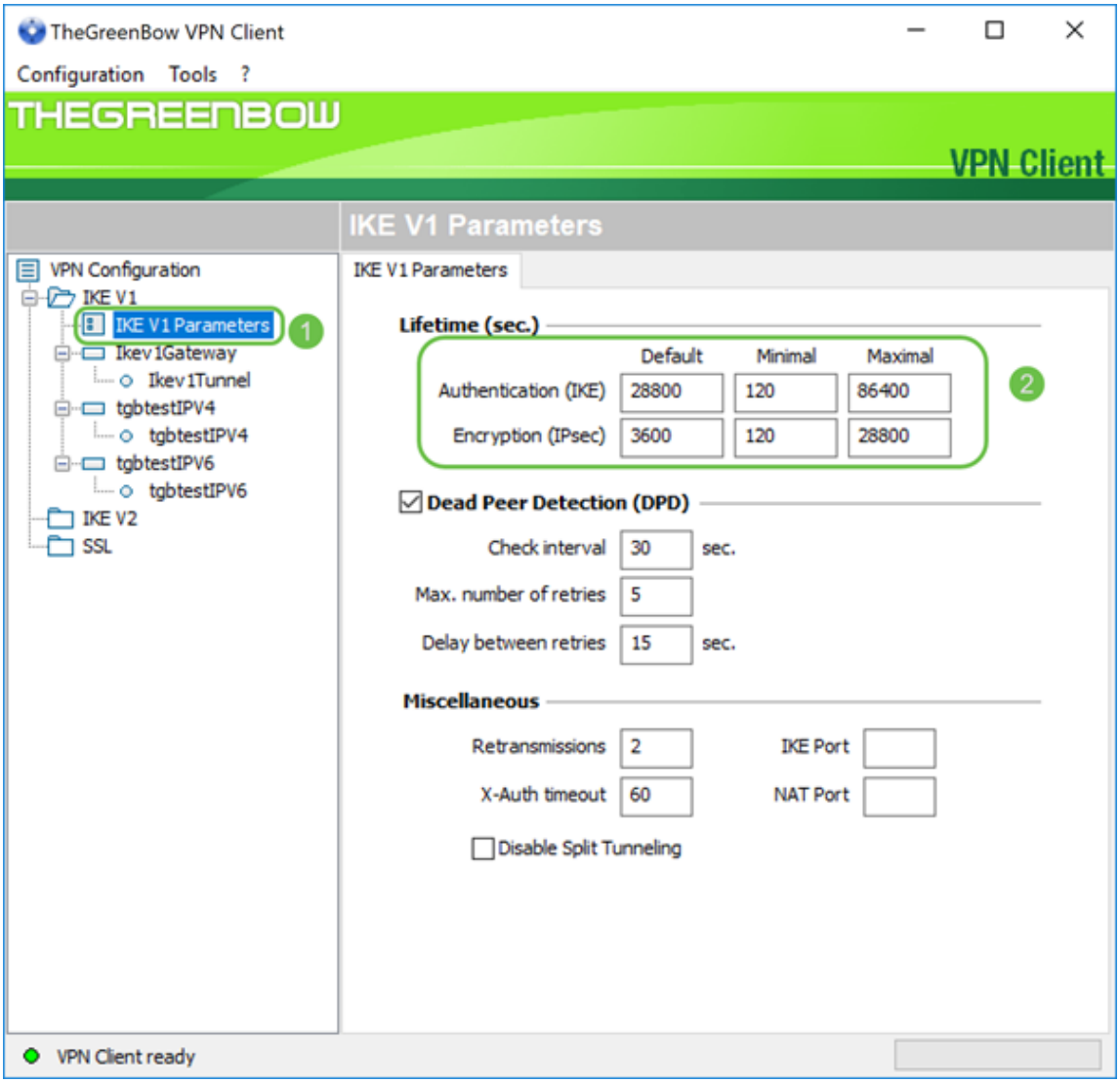
Schritt 4: Geben Sie die öffentliche WAN-IP-Adresse des Routers an der Stelle (im Büro) ein, an der sich der Dateiserver befindet, den vorinstallierten Schlüssel und die private interne Adresse des Remote-Netzwerks vor Ort. Klicken Sie auf **Weiter**. In diesem Beispiel ist die Site 24.x.x.x. Die letzten drei Oktette (Zahlensätze in dieser IP-Adresse) wurden durch ein x ersetzt, um dieses Netzwerk zu schützen. Geben Sie die vollständige IP-Adresse ein.



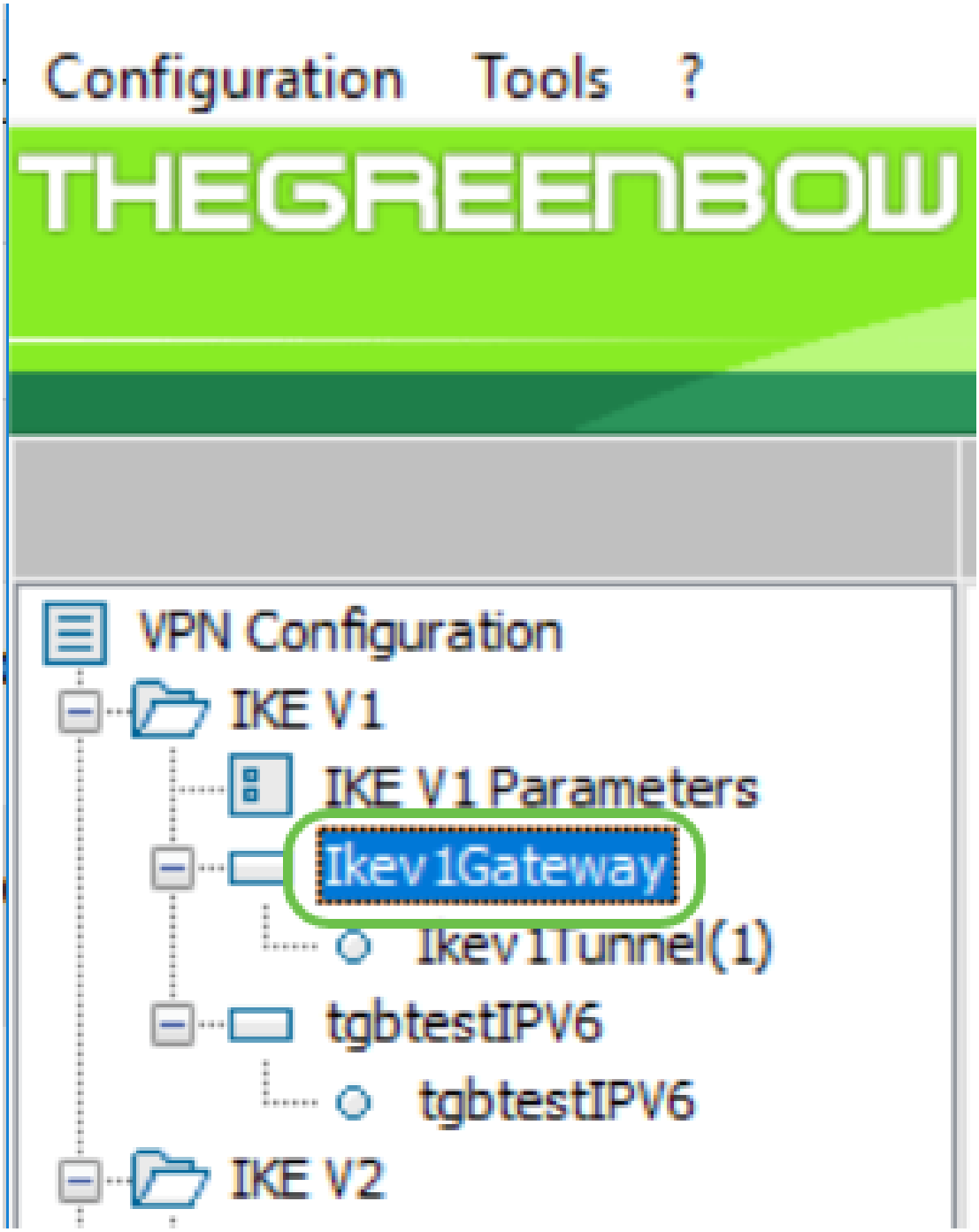
Schritt 5: Klicken Sie auf **Fertig stellen**.



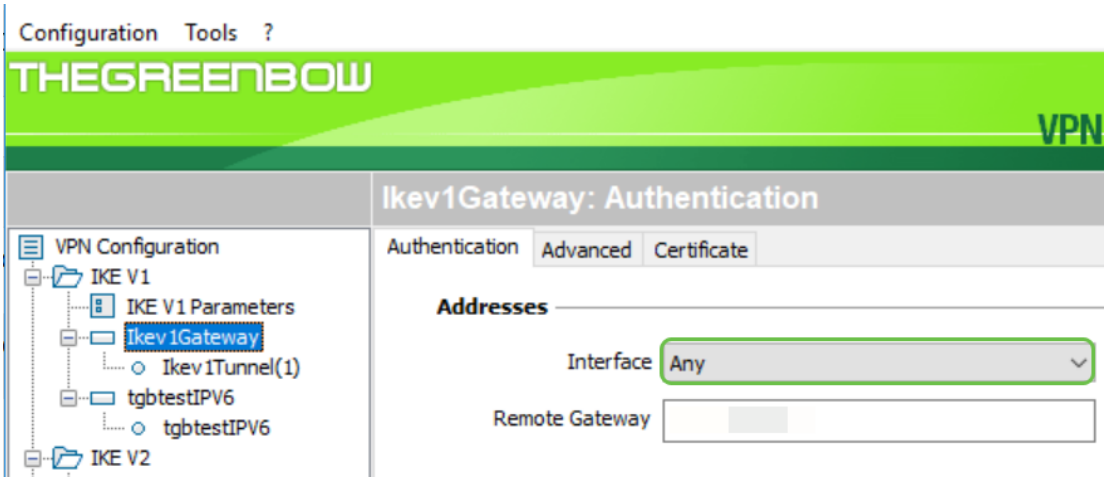
Schritt 6 (Optional) Sie können die IKE V1-Parameter ändern. Die WerteGreenBow Default, Minimal und Maximum für die Lebensdauer können angepasst werden. An diesem Speicherort können Sie den Bereich der Lebensdauer eingeben, der vom Router akzeptiert wird.



Schritt 7: Klicken Sie auf das von Ihnen erstellte Gateway.

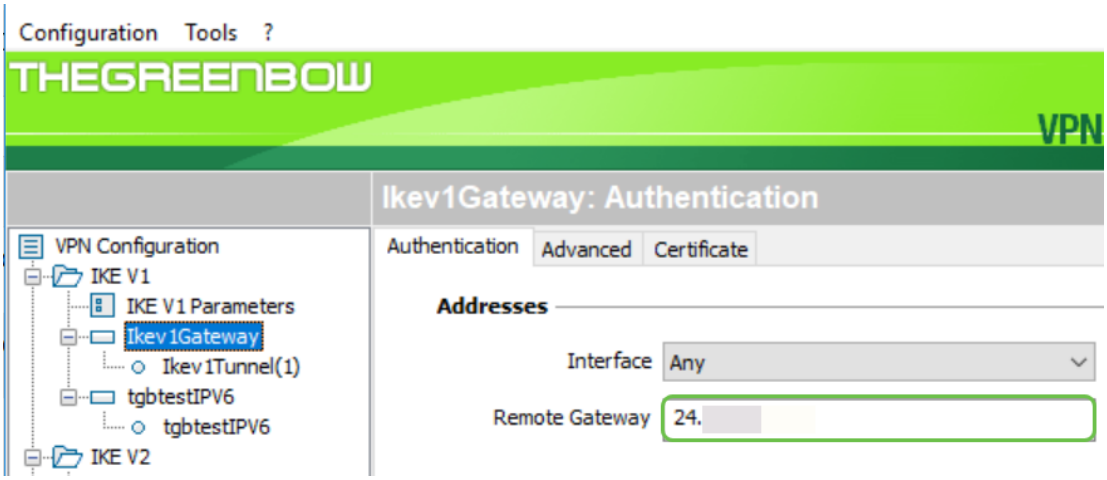


Schritt 8: Auf der Registerkarte *Authentifizierung* unter *Adressen* wird eine Dropdown-Liste mit lokalen Adressen angezeigt. Sie können eine Option auswählen oder **Any** auswählen (siehe unten).



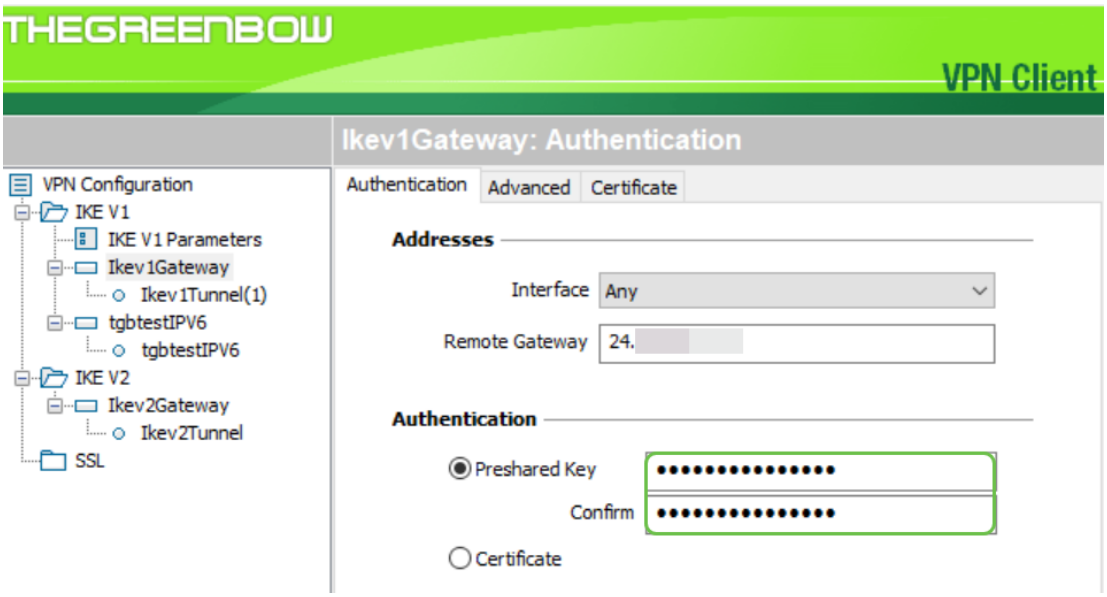
Schritt 9: Geben Sie die Adresse des Remote-Gateways in das Feld *Remote Gateway* ein. Dabei

kann es sich um eine IP-Adresse oder einen DNS-Namen handeln. Dies ist die Adresse der öffentlichen IP-Adresse für den Router am Standort (Büro).



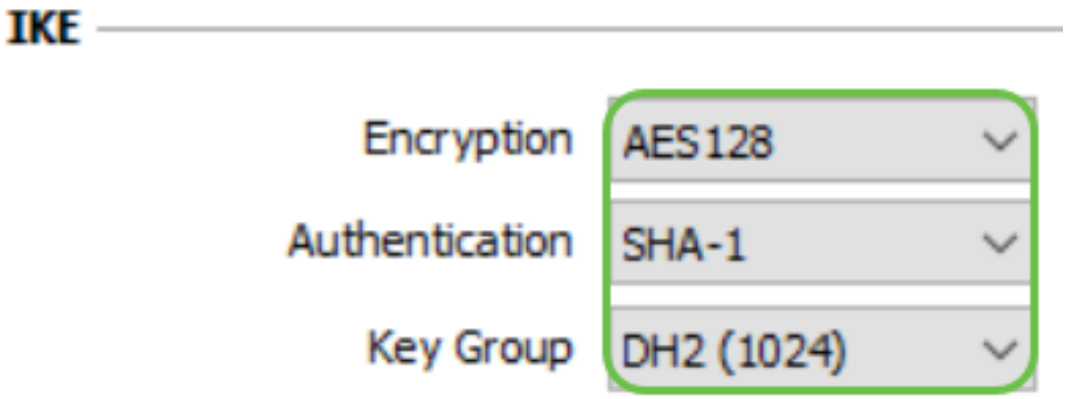
Schritt 10: Wählen Sie unter *Authentication* (Authentifizierung) den Authentifizierungstyp aus. Folgende Optionen stehen zur Verfügung:

- Preshared Key (Vorinstallierter Schlüssel): Mit dieser Option kann der Benutzer ein Kennwort verwenden, das auf dem VPN-Gateway konfiguriert wurde. Das Kennwort muss vom Benutzer abgeglichen werden, um einen VPN-Tunnel einrichten zu können.
- Zertifikat: Diese Option verwendet ein Zertifikat, um den Handshake zwischen dem VPN-Client und dem VPN-Gateway abzuschließen.

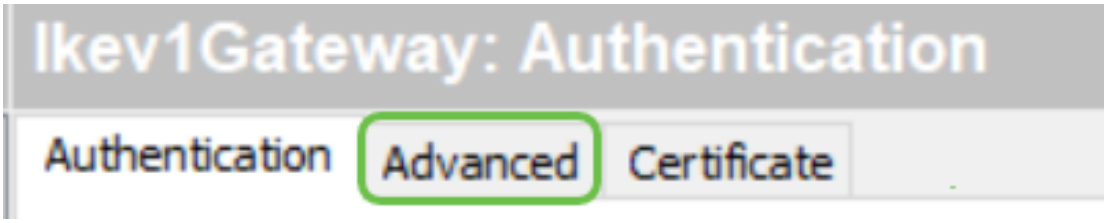


Hinweis: In diesem Beispiel wurde der auf dem Router konfigurierte Pre-shared Key eingegeben und bestätigt.

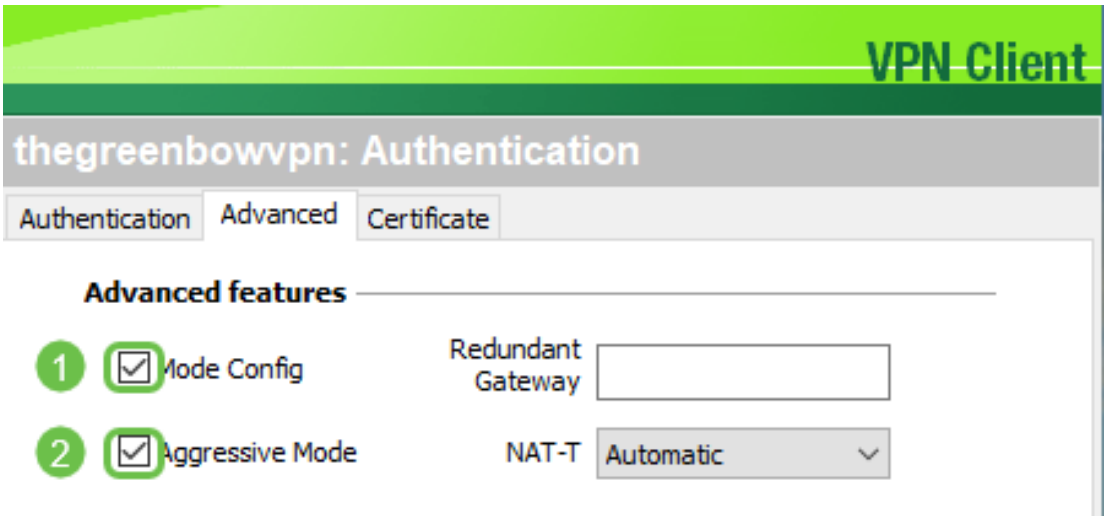
Schritt 11: Legen Sie unter *IKE* die Einstellungen für Verschlüsselung, Authentifizierung und Schlüsselgruppe so fest, dass sie mit der Konfiguration des Routers übereinstimmen.



Schritt 12: Klicken Sie auf die Registerkarte **Erweitert**.

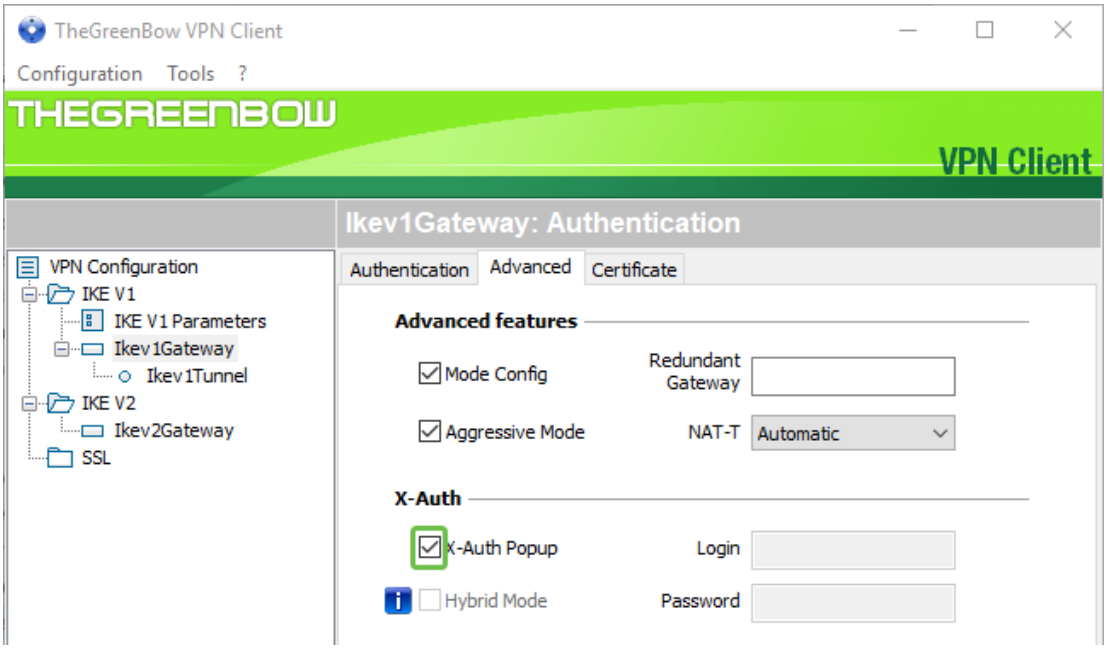


Schritt 13: Aktivieren Sie unter Erweiterte Funktionen das Kontrollkästchen **Moduskonfiguration** und **aggressiver Modus**. Der aggressive Modus wurde für den RV160 im Client-to-Site-Profil dieses Beispiels ausgewählt. Belassen Sie die NAT-T-Einstellung auf Automatisch.

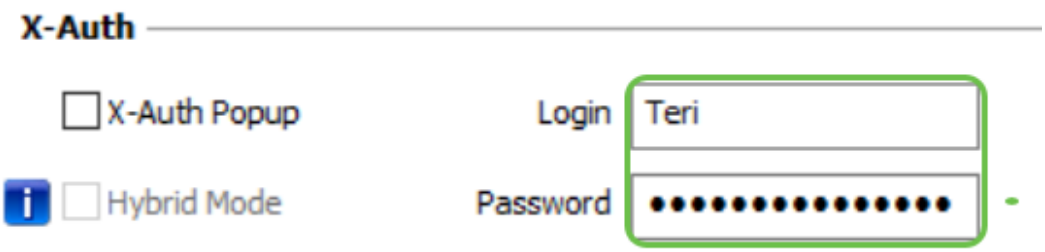


Hinweis: Bei aktivierter Moduskonfiguration ruft der GreenBow VPN Client Einstellungen vom VPN-Gateway ab, um einen Tunnel einzurichten. NAT-T beschleunigt den Verbindungsaufbau.

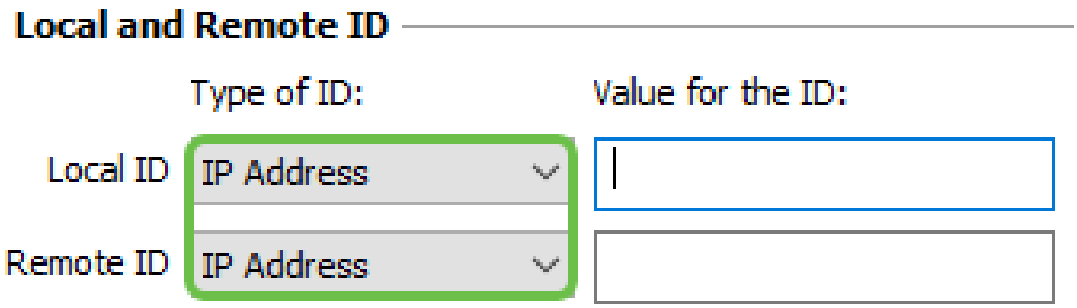
Schritt 14: (Optional) Unter *X-Auth* können Sie das **Kontrollkästchen X-Auth Popup** aktivieren, um beim Starten einer Verbindung automatisch das Anmeldungsfenster aufzurufen. Im Anmeldefenster gibt der Benutzer seine Anmeldeinformationen ein, um den Tunnel abzuschließen.



Schritt 15: (Optional) Wenn Sie *X-Auth Popup* nicht auswählen, geben Sie Ihren Benutzernamen in das Feld *Anmelden* ein. Dies ist der Benutzername, der eingegeben wurde, als ein Benutzerkonto im VPN-Gateway erstellt wurde, und das Kennwort am Standort.

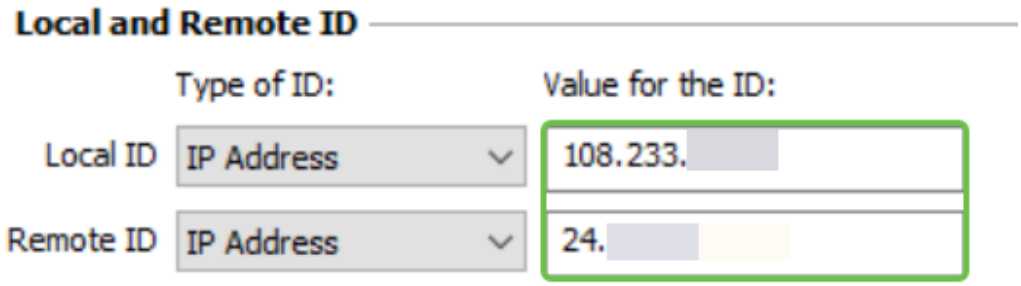


Schritt 16: Legen Sie unter *Lokale und Remote-ID* die lokale ID und die Remote-ID so fest, dass sie mit den Einstellungen des VPN-Gateways übereinstimmen.

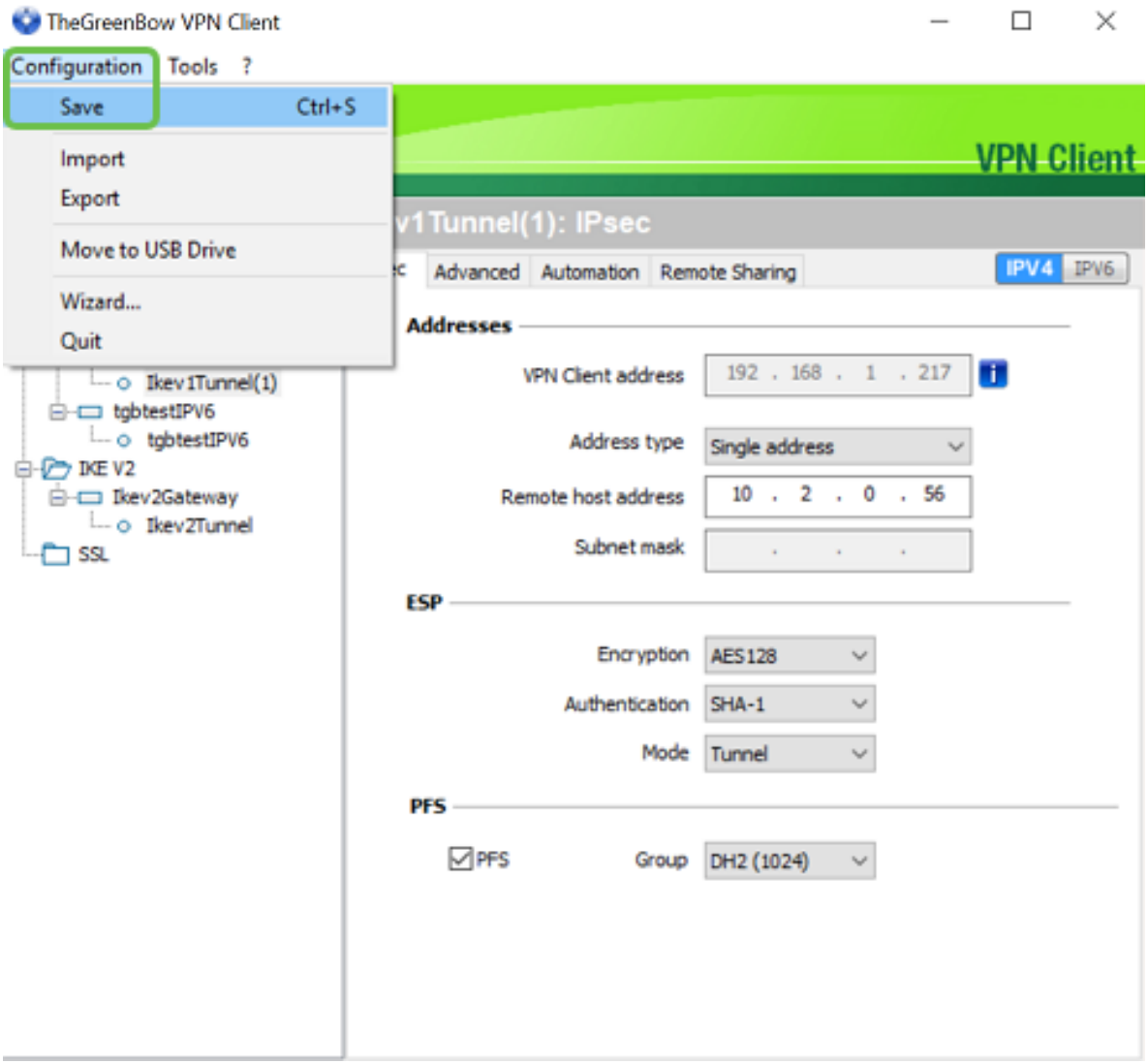


Hinweis: In diesem Beispiel werden sowohl die lokale ID als auch die Remote-ID auf die IP-Adresse eingestellt, um die Einstellungen des RV160- oder RV260-VPN-Gateways zu erfüllen.

Schritt 17: Geben Sie unter *Wert für die ID* die lokale ID und Remote-ID in die entsprechenden Felder ein. Die lokale ID ist die WAN-IP-Adresse für den Client. Sie finden diese Informationen im Internet nach "What's my IP" (Was ist meine IP-Adresse). Die Remote-ID ist die WAN-IP-Adresse des Routers am Standort.

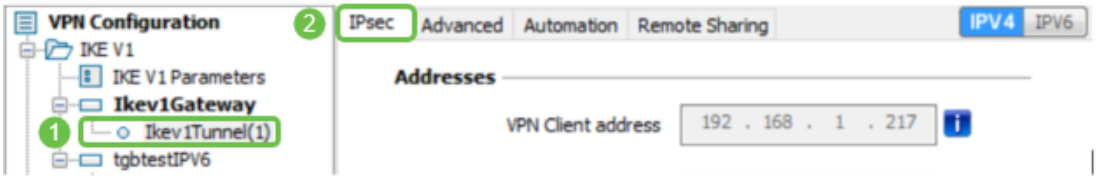


Schritt 18: Klicken Sie auf **Konfiguration** und wählen Sie **Speichern**.

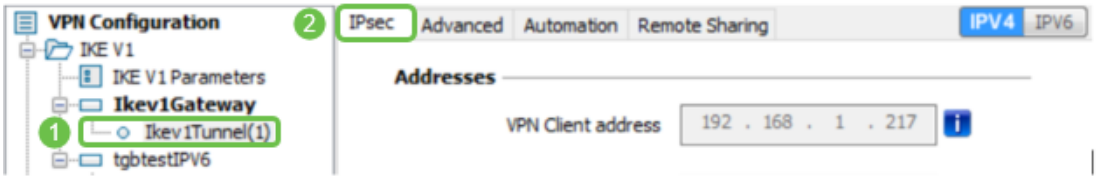


Tunnel-Einstellungen konfigurieren

Schritt 1: Klicken Sie auf die Registerkarte **IKev1Tunnel(1)** (der eigene Tunnel hat möglicherweise einen anderen Namen) und auf die Registerkarte **IPsec**. Die Adresse des VPN-Clients wird automatisch eingetragen, wenn Sie in den erweiterten Einstellungen des Ikev1Gateway die Option "Mode Config" (Moduskonfiguration) ausgewählt haben. Es wird die lokale IP-Adresse des Computers/Laptops am Remote-Standort angezeigt.

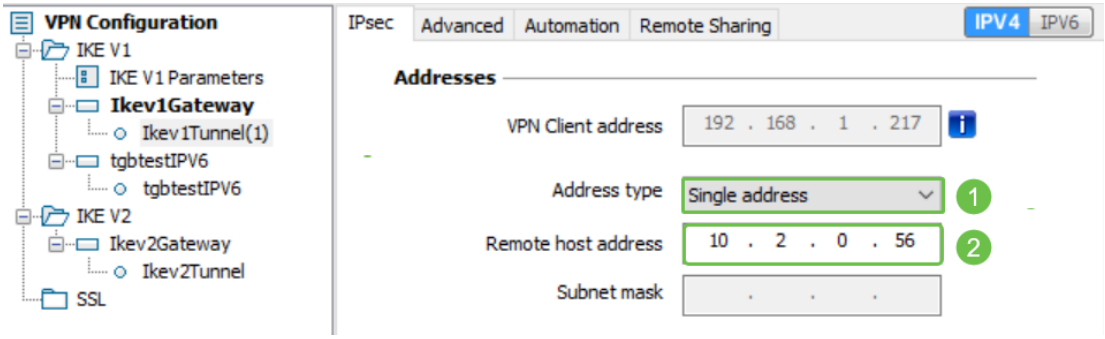


Schritt 2: Wählen Sie aus der Dropdown-Liste *Adresstyp* den Adresstyp aus, auf den der VPN-Client zugreifen kann. Dabei kann es sich um eine einzelne Adresse, einen Adressbereich oder eine Subnetzadresse handeln. Der Standardwert, Subnetzadresse, enthält automatisch die VPN-Client-Adresse (die lokale IP-Adresse des Computers), die Remote-LAN-Adresse und die Subnetzmaske. Wenn Sie Single Address (Eine Adresse) oder Range of Adressen (Adressenbereich) auswählen, müssen diese Felder manuell ausgefüllt werden. Geben Sie die Netzwerkadresse ein, auf die der VPN-Tunnel zugreifen soll, im Feld *Remote LAN-Adresse* und die Subnetzmaske des Remote-Netzwerks im Feld *Subnetzmaske*.

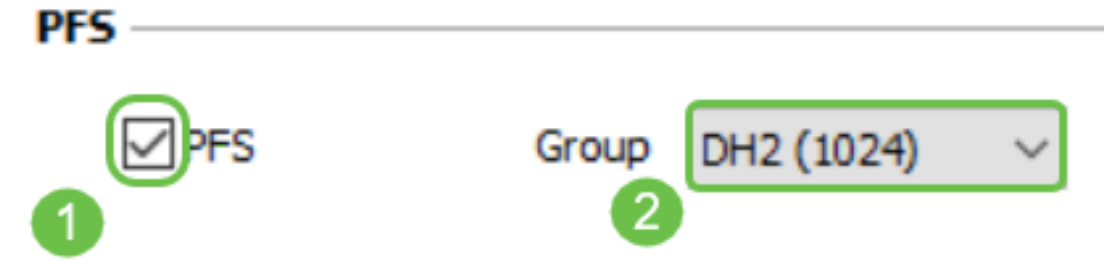


Hinweis: In diesem Beispiel wurde eine einzige Adresse ausgewählt und die lokale IP-Adresse des Routers am Standort eingegeben.

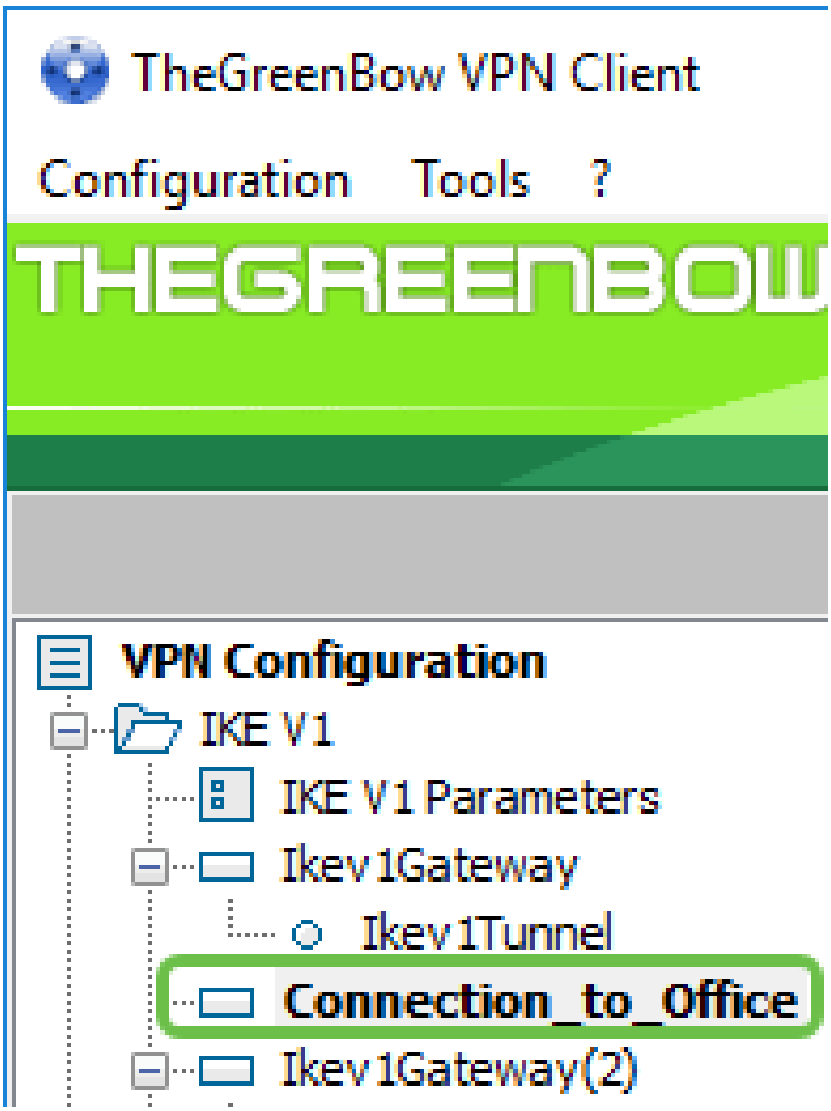
Schritt 3: Legen Sie unter *ESP* die Einstellungen für Verschlüsselung, Authentifizierung und Modus so fest, dass sie mit den Einstellungen des VPN-Gateways am Standort (im Büro) übereinstimmen.



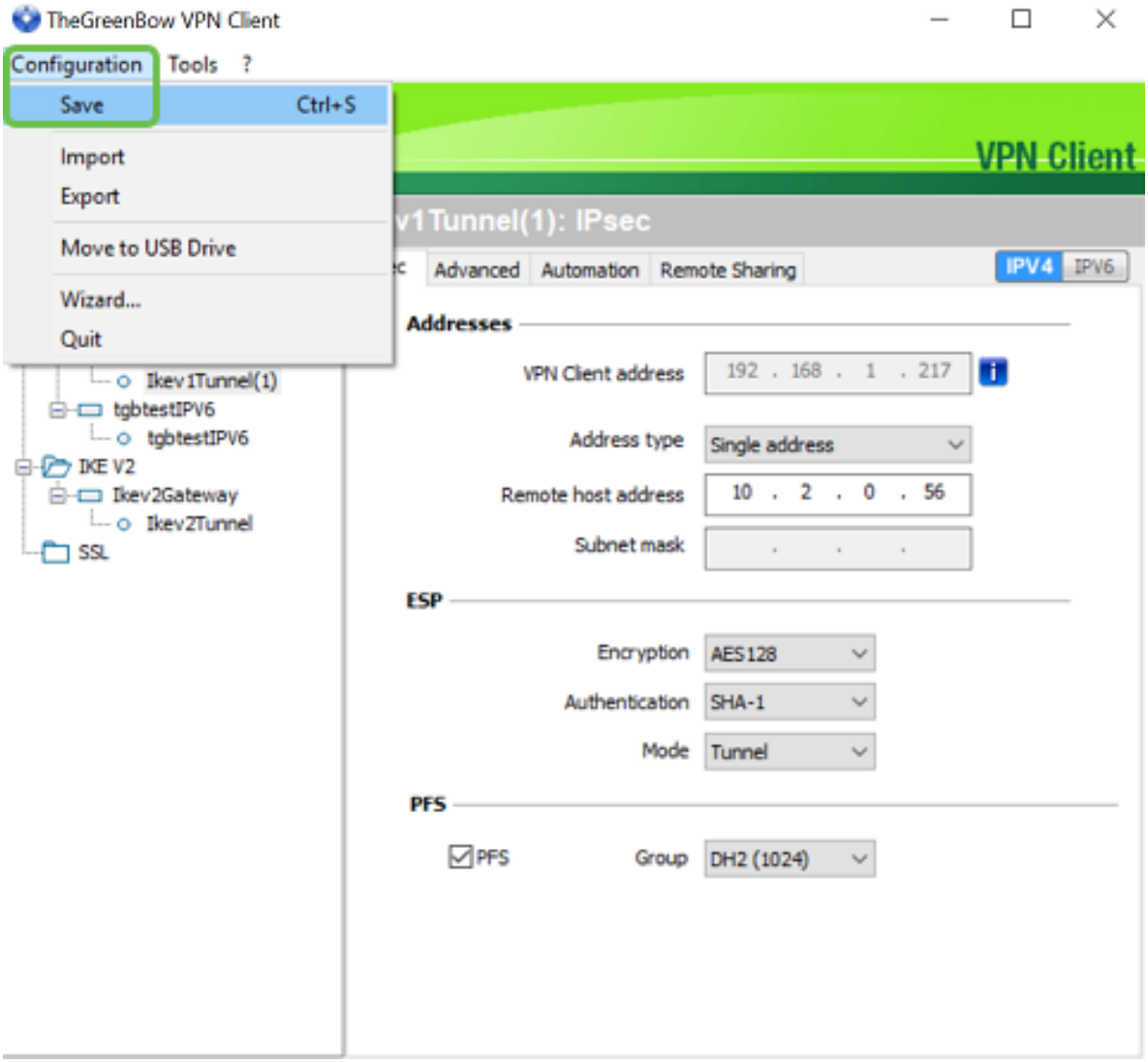
Schritt 4: (Optional) Aktivieren Sie unter *PFS* das **PFS**-Kontrollkästchen, um Perfect Forward Secrecy (PFS) zu aktivieren. PFS generiert zufällige Schlüssel zur Verschlüsselung der Sitzung. Wählen Sie aus der Dropdown-Liste *Gruppe* eine PFS-Gruppeneinstellung aus. Wenn sie auf dem Router aktiviert wurde, sollte sie auch hier aktiviert sein.



Schritt 5: (Optional) Klicken Sie mit der rechten Maustaste auf den Namen des Ikev1Gateway und klicken Sie auf den Abschnitt Umbenennen, wenn Sie ihn umbenennen möchten.



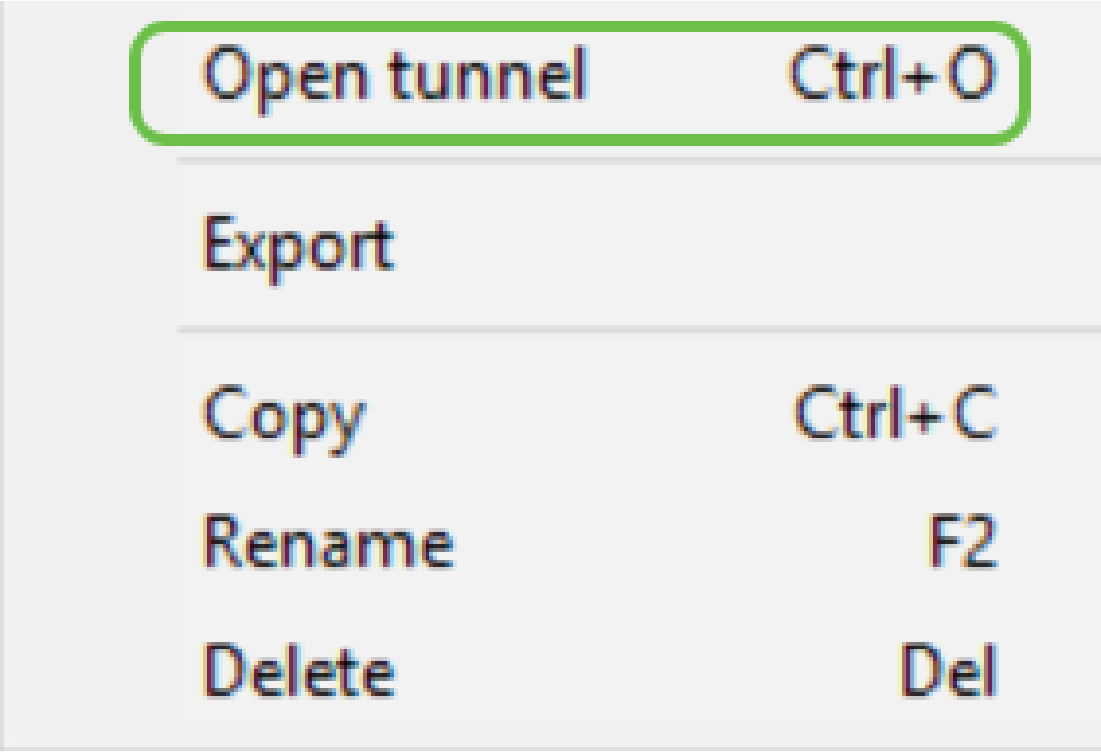
Schritt 6: Klicken Sie auf **Konfiguration** und wählen Sie **Speichern**.



Sie sollten den GreenBow VPN Client jetzt erfolgreich für die Verbindung mit dem RV160- oder RV260-Router über VPN konfiguriert haben.

VPN-Verbindung als Client starten

Schritt 1: Da Sie TheGreenBow geöffnet haben, können Sie mit der rechten Maustaste auf den Tunnel klicken und **Tunnel öffnen** auswählen**, um eine Verbindung herzustellen**.

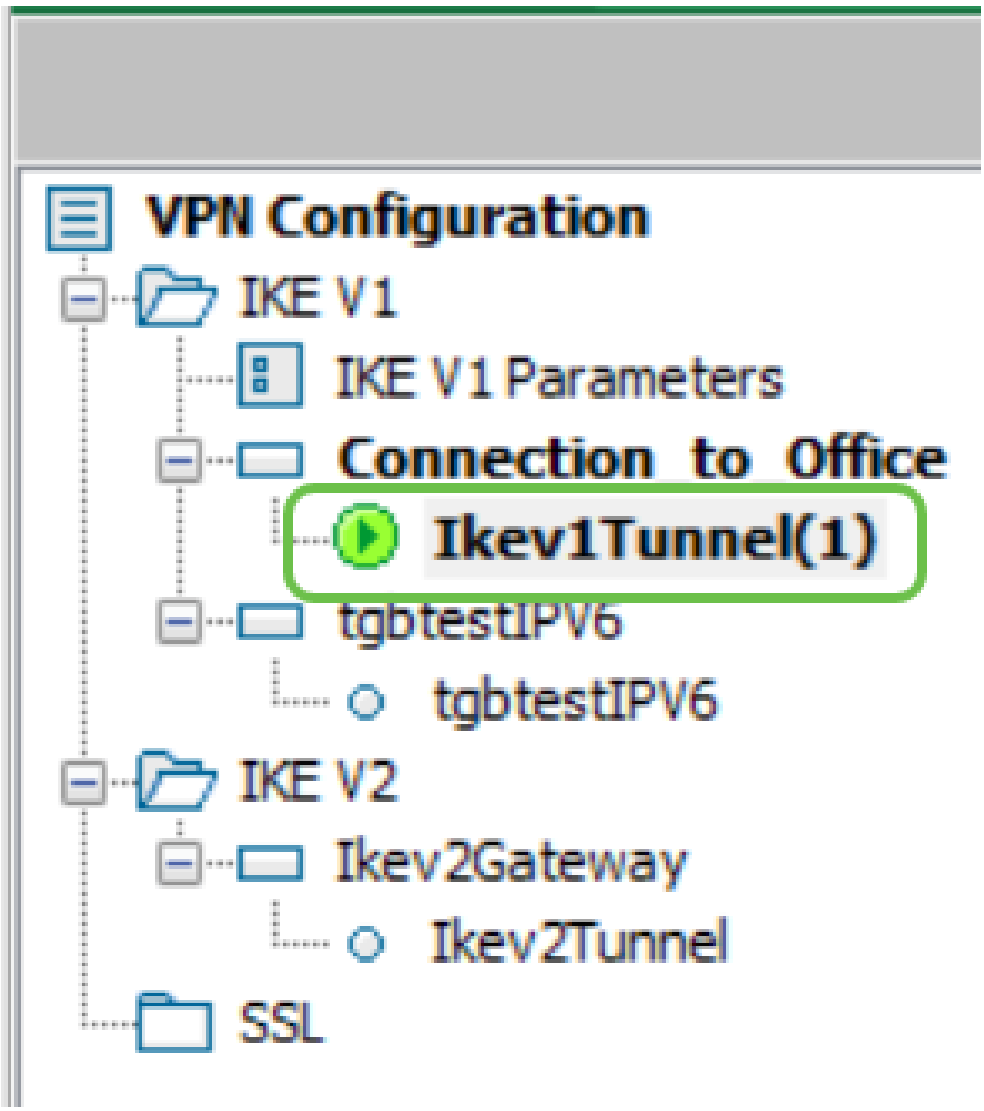


Hinweis: Sie können auch einen Tunnel öffnen, indem Sie auf den Tunnel doppelklicken.

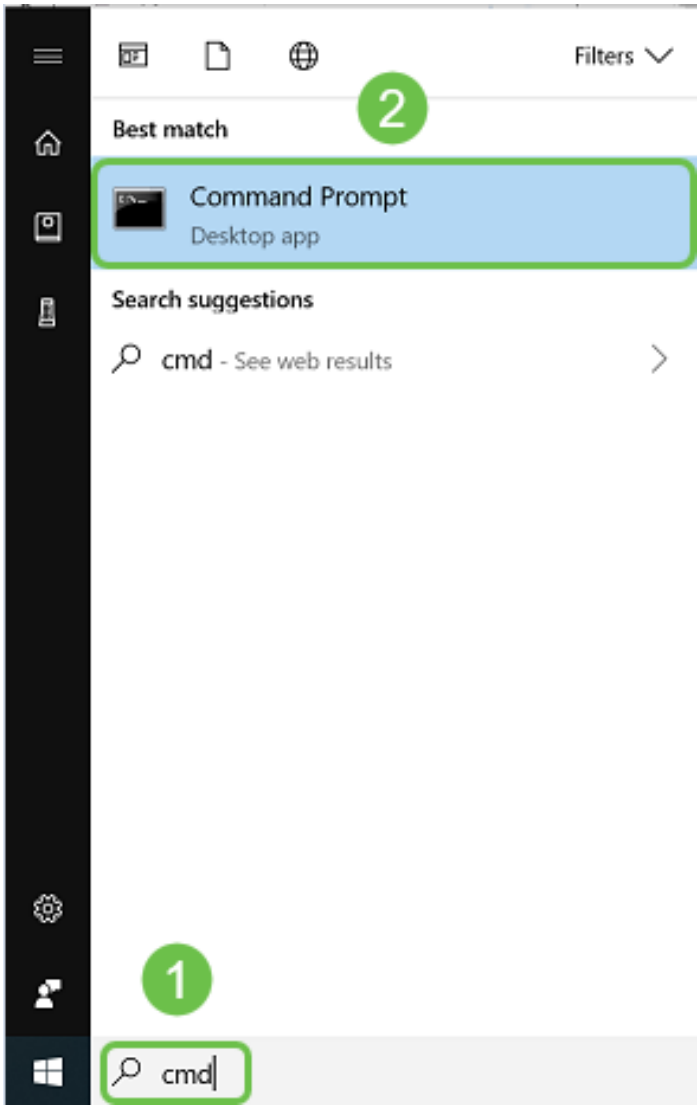
Schritt 2: (Optional) Wenn Sie eine neue Sitzung starten und TheGreenBow geschlossen haben, klicken Sie auf **das** Symbol **TheGreenBow VPN Client** auf der rechten Seite des Bildschirms.

Schritt 3: (Optional) Dieser Schritt ist nur erforderlich, wenn Sie eine neue Sitzung einrichten und Schritt 2 befolgt haben. Wählen Sie die zu verwendende VPN-Verbindung aus, und klicken Sie dann auf **ÖFFNEN**. Die VPN-Verbindung sollte automatisch gestartet werden.

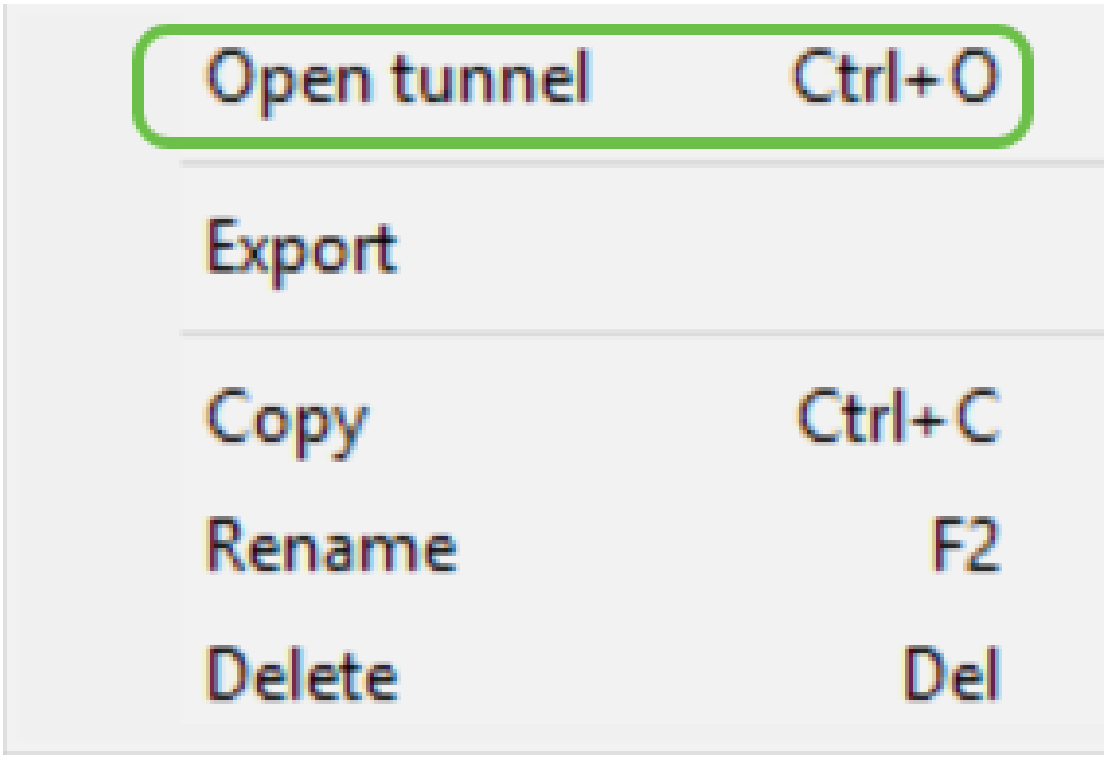
Schritt 4: Wenn der Tunnel angeschlossen ist, wird neben dem Tunnel ein grüner Kreis angezeigt. Wenn Sie ein Ausrufezeichen sehen, können Sie auf dieses klicken, um den Fehler zu finden.



Schritt 5: (Optional) Um zu überprüfen, ob Sie verbunden sind, greifen Sie über den Client-Computer auf die Eingabeaufforderung zu.



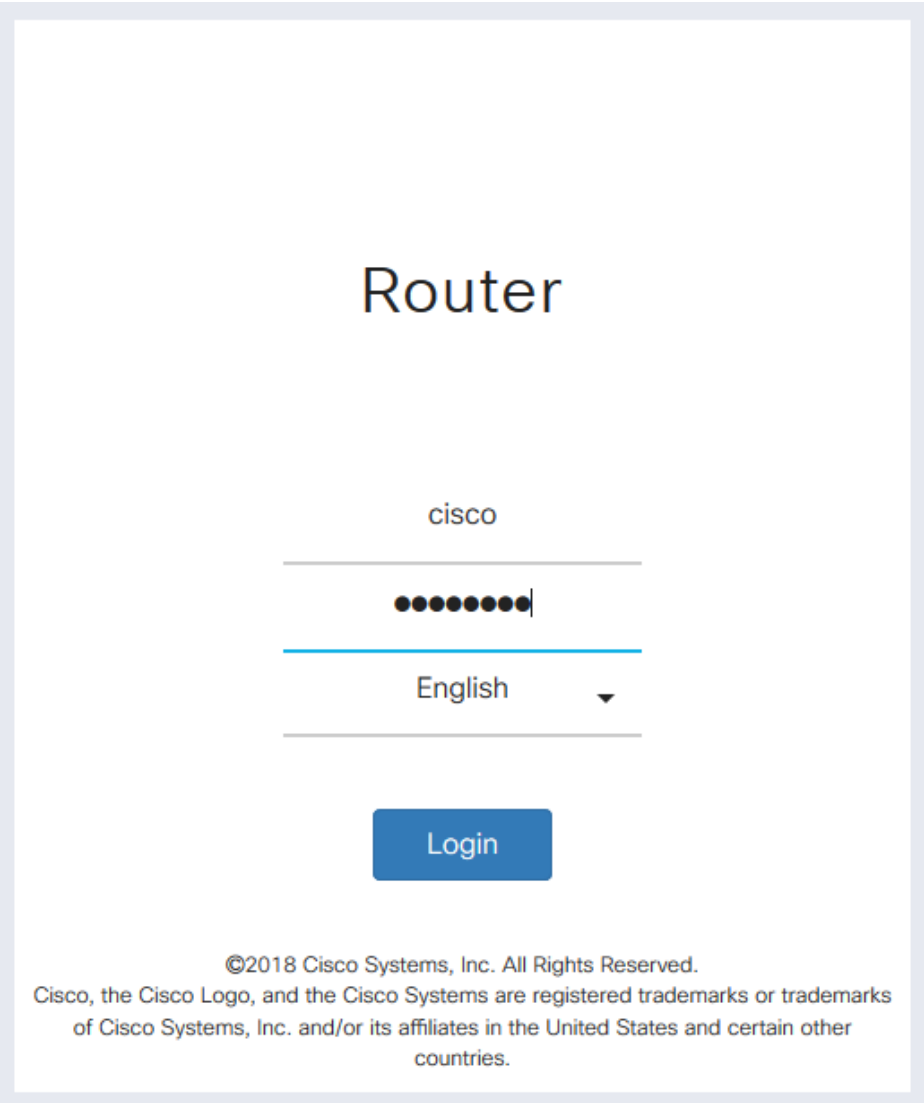
Schritt 6: (Optional) Geben Sie ping und anschließend die private LAN-IP-Adresse des Routers am Standort ein. Wenn Sie Antworten erhalten, sind Sie verbunden.



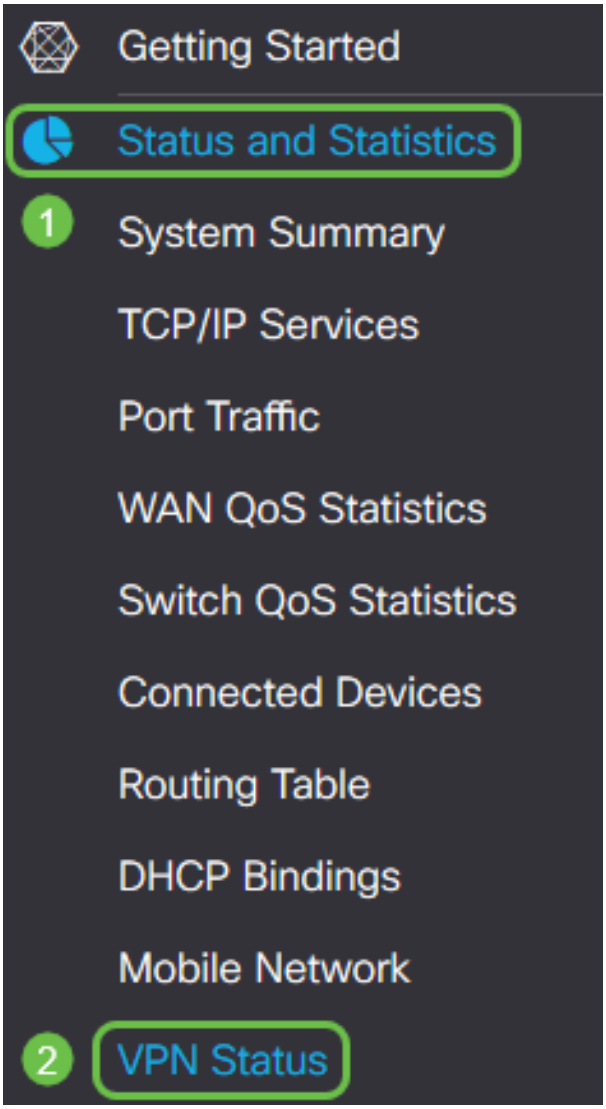
VPN-Status überprüfen

Überprüfen Sie den VPN-Status am Standort.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des VPN-Gateways des RV160 oder RV260 an.



Schritt 2: Wählen Sie **Status und Statistik > VPN Status aus**.

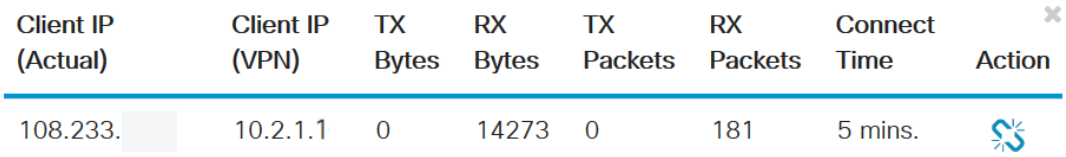


Schritt 3: Überprüfen Sie unter *Client-to-Site-Tunnelstatus* die Spalte *Verbindungen* in der *Verbindungstabelle*. Die VPN-Verbindung sollte bestätigt werden.

Schritt 4: Klicken Sie auf das **Augen**-Symbol, um weitere Details anzuzeigen.

Schritt 5: Die Details zum Client-to-Site VPN-Status finden Sie hier. Sie sehen die WAN-IP-Adresse des Clients, die lokale IP-Adresse, die aus dem bei der Einrichtung konfigurierten Adresspool zugewiesen wurde. Außerdem werden Bytes und Pakete angezeigt, die gesendet und

empfangen wurden, sowie die Verbindungszeit. Wenn Sie den Client trennen möchten, klicken Sie unter *Aktion* auf das blaue **defekte Kettensymbol**. Klicken Sie auf das **x** in der oberen rechten Ecke, um nach der Überprüfung zu schließen.



Client IP (Actual)	Client IP (VPN)	TX Bytes	RX Bytes	TX Packets	RX Packets	Connect Time	Action
108.233.	10.2.1.1	0	14273	0	181	5 mins.	

Schlussfolgerung

Sie sollten jetzt die VPN-Verbindung auf dem Router RV160 oder RV260 erfolgreich eingerichtet und verifiziert haben. Außerdem sollte der VPN-Client GreenBow so konfiguriert sein, dass er auch über VPN eine Verbindung zum Router herstellt.