Verwenden des GreenBow VPN-Clients für die Verbindung mit dem Router der Serie RV34x

Besonderer Hinweis: Lizenzierungsstruktur - Firmware-Versionen 1.0.3.15 und höher. Für AnyConnect wird künftig nur noch Client-Lizenzen berechnet.

Weitere Informationen zur AnyConnect-Lizenzierung für Router der Serie RV340 finden Sie im Artikel AnyConnect Licensing for the RV340 Series Routers.

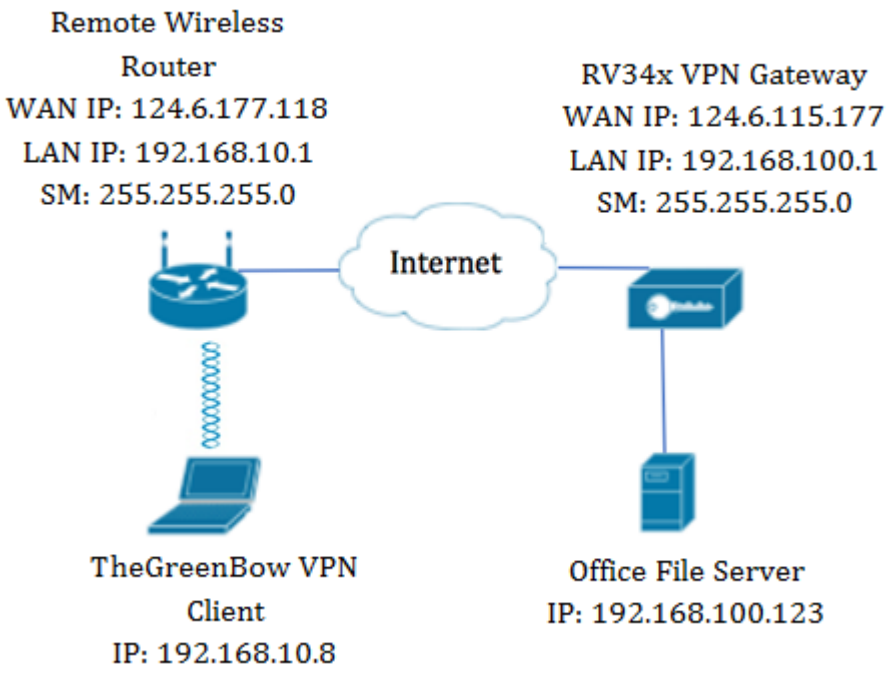
Einführung

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. Die meisten Firmenbüros verwenden eine VPN-Verbindung, da es sowohl nützlich als auch notwendig ist, den Mitarbeitern den Zugriff auf ihr privates Netzwerk zu ermöglichen, selbst wenn sie sich außerhalb des Büros befinden.

Mit dem VPN kann ein Remote-Host so agieren, als ob er sich im selben lokalen Netzwerk befinde. Der Router unterstützt bis zu 50 Tunnel. 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.

Der GreenBow VPN Client ist eine VPN-Client-Anwendung eines Drittanbieters, mit der ein Hostgerät eine sichere Verbindung für einen Site-to-Site-IPSec-Tunnel mit dem Router der Serie RV34x konfigurieren kann.



Im Diagramm stellt der Computer eine Verbindung zum Dateiserver im Büro außerhalb seines Netzwerks her, um auf seine Ressourcen zuzugreifen. Hierzu wird der GreenBow VPN Client im Computer so konfiguriert, dass er die Einstellungen vom RV34x VPN-Gateway abruft.

Vorteile einer VPN-Verbindung

1. Die Verwendung einer VPN-Verbindung trägt zum Schutz vertraulicher Netzwerkdaten und -ressourcen bei.
2. Remote-Mitarbeiter oder Firmenmitarbeiter erhalten damit einfachen Zugriff auf die Hauptniederlassung, ohne dass sie physisch anwesend sein müssen. Gleichzeitig wird die Sicherheit des privaten Netzwerks und seiner Ressourcen gewahrt.
3. Die Kommunikation über eine VPN-Verbindung bietet ein höheres Maß an Sicherheit als andere Remote-Kommunikationsmethoden. Modernste Technologie macht dies heute möglich und schützt damit das private Netzwerk vor unbefugtem Zugriff.
4. Der tatsächliche geografische Standort der Benutzer ist geschützt und nicht öffentlichen oder gemeinsam genutzten Netzwerken wie dem Internet ausgesetzt.
5. Das Hinzufügen neuer Benutzer oder Benutzergruppen zum Netzwerk ist denkbar einfach, da VPNs einfach skalierbar sind. Das Netzwerk kann ohne zusätzliche Komponenten oder komplizierte Konfiguration erweitert werden.

Risiken bei der Verwendung einer VPN-Verbindung

1. Sicherheitsrisiko durch Fehlkonfiguration. 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.
2. Zuverlässigkeit. 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.
3. Skalierbarkeit. Wenn eine neue Infrastruktur oder eine neue Gruppe von Konfigurationen

hinzugefügt werden muss, können technische Probleme aufgrund der Inkompatibilität entstehen, insbesondere wenn es um andere Produkte oder Anbieter als die handelt, die Sie bereits verwenden.
4. Sicherheitsprobleme bei Mobilgeräten. Beim Initiieren der VPN-Verbindung auf einem Mobilgerät können Sicherheitsprobleme auftreten, insbesondere wenn das Mobilgerät drahtlos mit dem lokalen Netzwerk verbunden ist.
5. Langsame Verbindungsgeschwindigkeiten. 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.

Voraussetzungen für die Verwendung desGreenBow VPN-Clients

Die folgenden Elemente müssen zuerst auf dem VPN-Router konfiguriert und auf den TheGreenBow VPN Client angewendet werden, indem Sie hier klicken, um eine Verbindung herzustellen.

1. Erstellen eines Client-to-Site-Profils auf dem VPN-Gateway
2. Erstellen einer Benutzergruppe im VPN-Gateway
3. Benutzerkonto auf dem VPN-Gateway erstellen
4. Erstellen eines IPSec-Profils auf dem VPN-Gateway
5. Konfigurieren der Einstellungen für Phase I und Phase II am VPN-Gateway

Anwendbare Geräte

- Serie RV34x

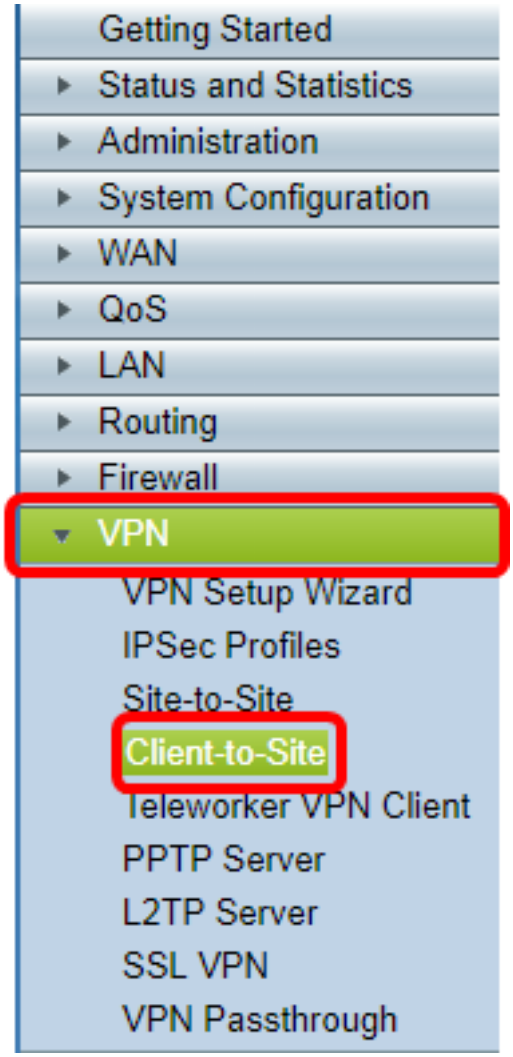
Softwareversion

- 1.0.01.17

Verwenden desGreenBow VPN-Clients

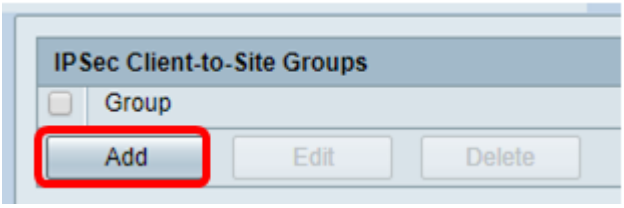
Erstellen eines Client-to-Site-Profils auf dem Router

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des RV34x-Routers an, und wählen Sie **VPN > Client-to-Site aus**.



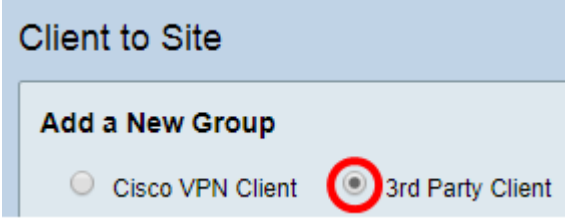
Hinweis: Die Bilder in diesem Artikel stammen vom RV340 Router. Die Optionen können je nach Gerät variieren.

Schritt 2: Klicken Sie auf **Hinzufügen**.



Schritt 3: Klicken Sie auf **Drittanbieter-Client**.

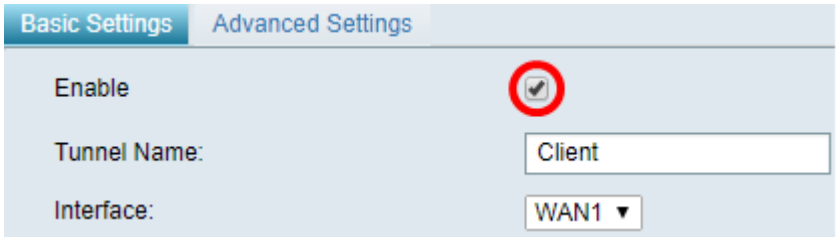
Hinweis: AnyConnect ist ein Beispiel für einen Cisco VPN-Client, während der GreenBow VPN-Client ein Beispiel für einen VPN-Client eines Drittanbieters ist.



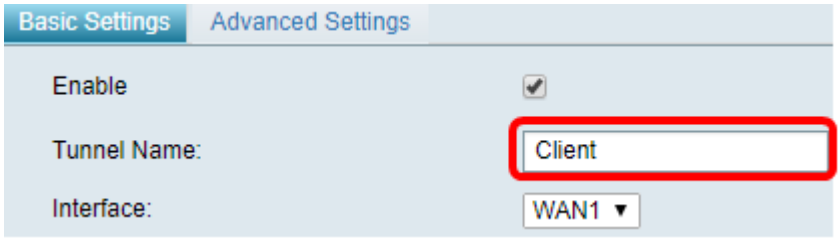
Hinweis: In diesem Beispiel wird Drittanbieter-Client ausgewählt.

Schritt 4: Aktivieren Sie auf der Registerkarte Basiseinstellungen das Kontrollkästchen

Aktivieren, um sicherzustellen, dass das VPN-Profil aktiv ist.

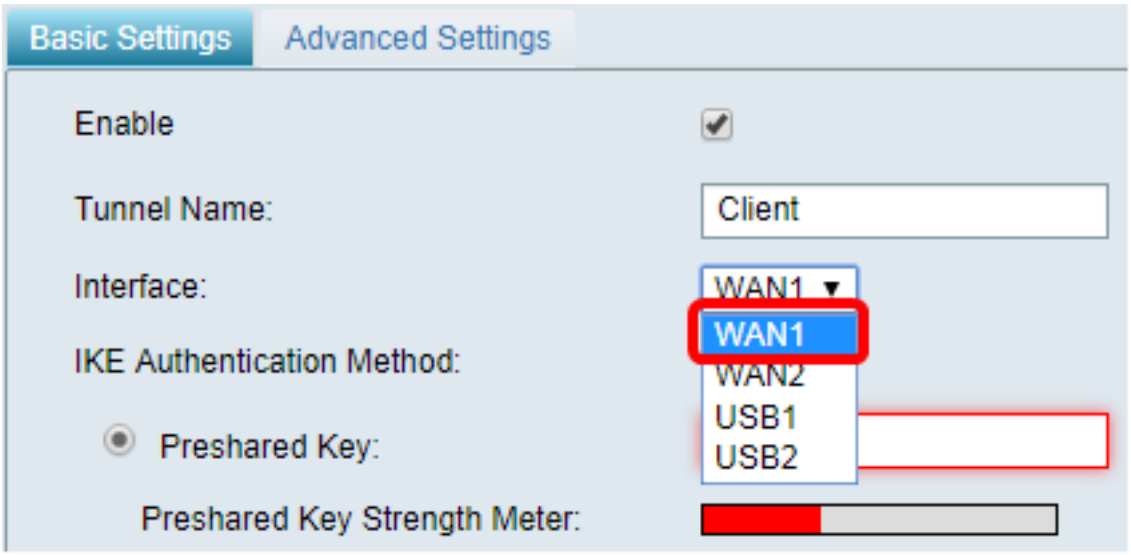


Schritt 5: Geben Sie im Feld *Tunnel Name* einen Namen für die VPN-Verbindung ein.



Hinweis: In diesem Beispiel wird **Client** eingegeben.

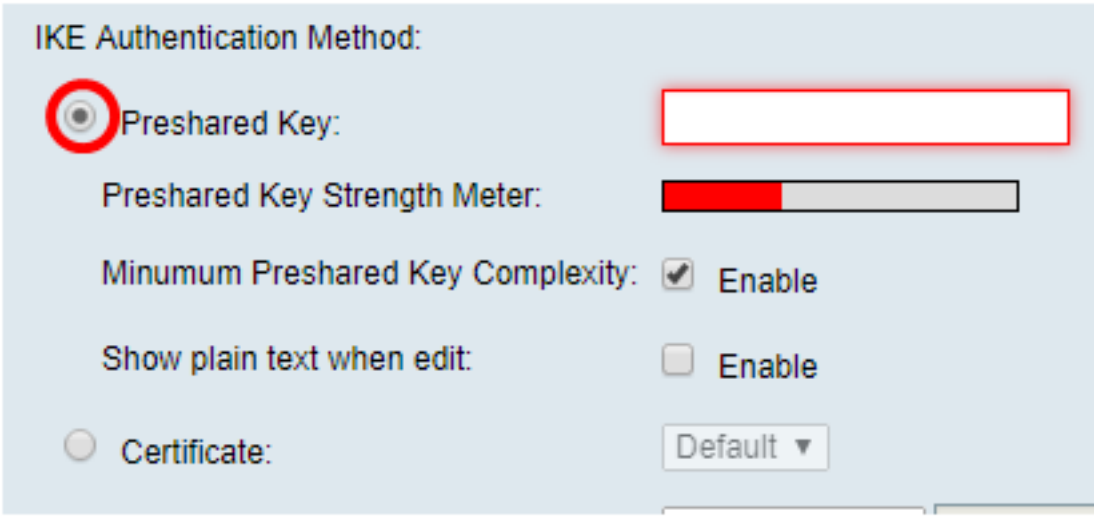
Schritt 6: Wählen Sie in der Dropdown-Liste Interface (Schnittstelle) die zu verwendende Schnittstelle aus. Die Optionen sind WAN1, WAN2, USB1 und USB2, die die entsprechende Schnittstelle auf dem Router für die VPN-Verbindung verwenden.



Hinweis: Die Optionen hängen vom verwendeten Router-Modell ab. In diesem Beispiel wird WAN1 ausgewählt.

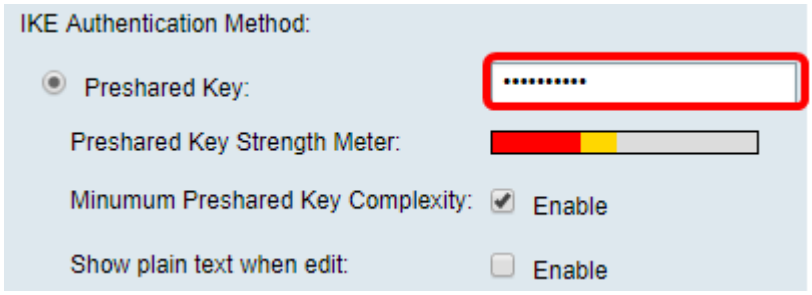
Schritt 7: Wählen Sie eine IKE-Authentifizierungsmethode aus. Folgende Optionen stehen zur Verfügung:

- Preshared 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.

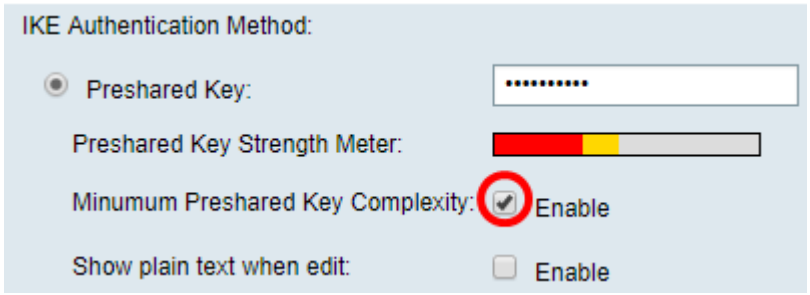


Hinweis: In diesem Beispiel wird der vorinstallierte Schlüssel ausgewählt.

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

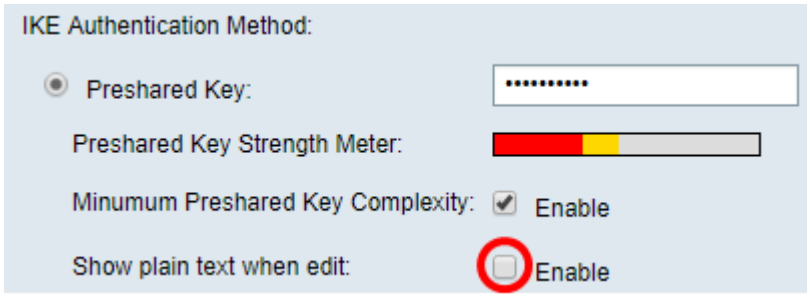


Schritt 9: (Optional) Deaktivieren Sie das Kontrollkästchen Minimum Preshared Key Complexity **Enable** (Minimale **Komplexität des** gemeinsamen Schlüssels aktivieren, um ein einfaches Kennwort verwenden zu können.)



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

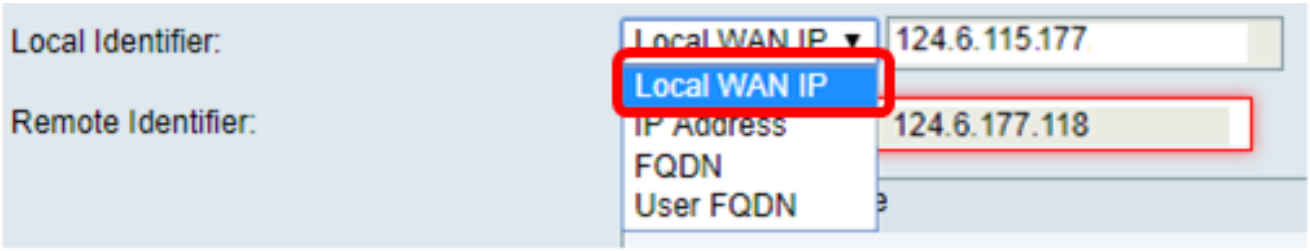
Schritt 10: (Optional) Aktivieren Sie das Kontrollkästchen Nur Text anzeigen, wenn **Aktivieren** bearbeitet wird, um das Kennwort im Klartext anzuzeigen.



Hinweis: In diesem Beispiel zeigen Sie Klartext, wenn die Bearbeitung deaktiviert bleibt.

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

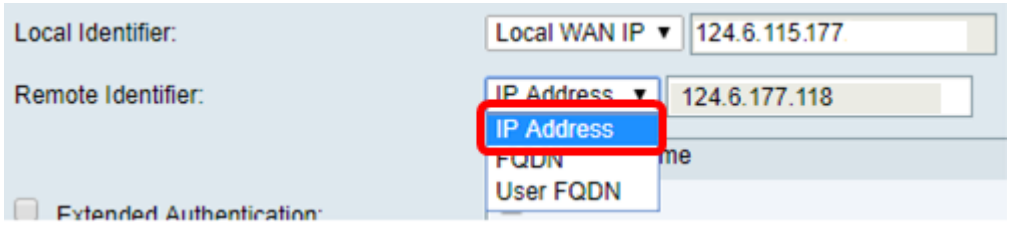
- Local WAN IP (Lokale WAN-IP): Diese Option verwendet die IP-Adresse der WAN-Schnittstelle (Wide Area Network) des VPN-Gateways.
- IP Address (IP-Adresse): Mit dieser Option können Sie manuell eine IP-Adresse für die VPN-Verbindung eingeben.
- FQDN - Diese Option wird auch als Fully Qualified Domain 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 lokale WAN-IP ausgewählt. Bei dieser Option wird die lokale WAN-IP automatisch erkannt.

Schritt 12: (Optional) 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.
- FQDN: 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.



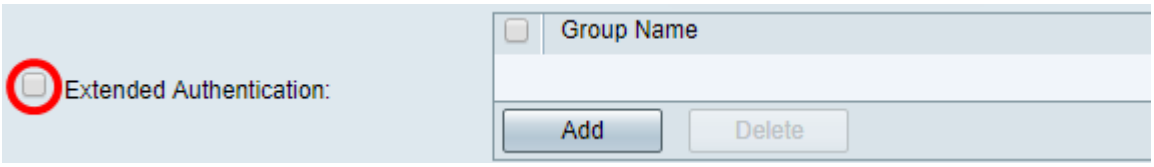
Hinweis: In diesem Beispiel wird die IP-Adresse ausgewählt.

Schritt 13: Geben Sie die Remote-ID im Feld *Remote Identifier (Remote-ID)* ein.

Hinweis: In diesem Beispiel wird 124.6.115.177 eingegeben.

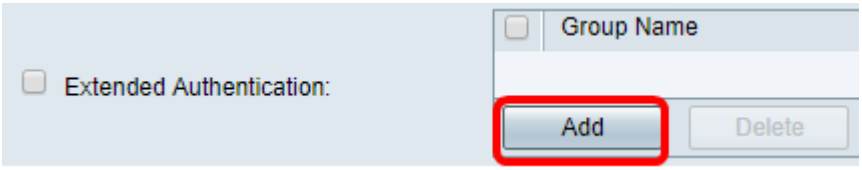
Schritt 14: (Optional) Aktivieren Sie das Kontrollkästchen **Erweiterte Authentifizierung**, um die Funktion zu aktivieren. Wenn diese Option aktiviert ist, wird eine zusätzliche Authentifizierungsstufe bereitgestellt, bei der Remote-Benutzer ihre Anmeldeinformationen

eingeben müssen, bevor sie Zugriff auf das VPN erhalten.

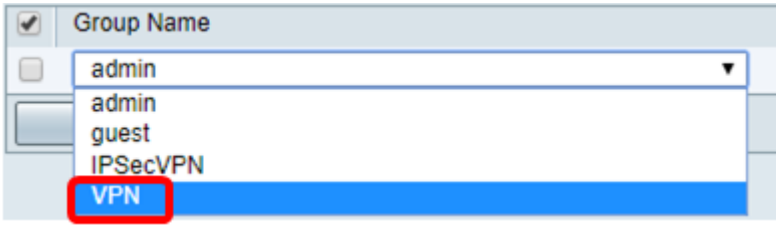


Hinweis: In diesem Beispiel wird die erweiterte Authentifizierung deaktiviert.

Schritt 15: Klicken Sie unter Gruppenname auf **Hinzufügen**.

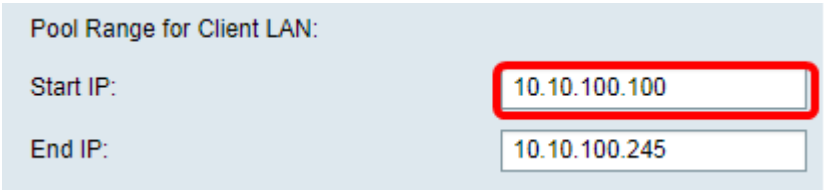


Schritt 16: Wählen Sie aus der Dropdown-Liste Gruppenname die Gruppe aus, die erweiterte Authentifizierung verwendet.



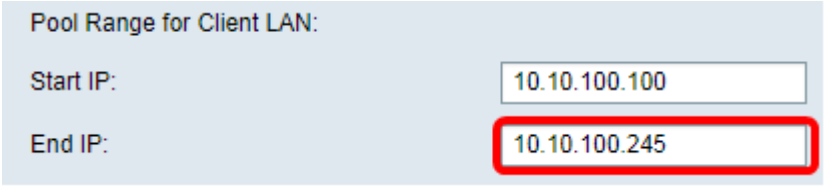
Hinweis: In diesem Beispiel wird VPN ausgewählt.

Schritt 17: Geben Sie unter Pool Range for Client LAN (Pool-Bereich für Client-LAN) die erste IP-Adresse ein, die einem VPN-Client im Feld *Start IP (IP starten)* zugewiesen werden kann.



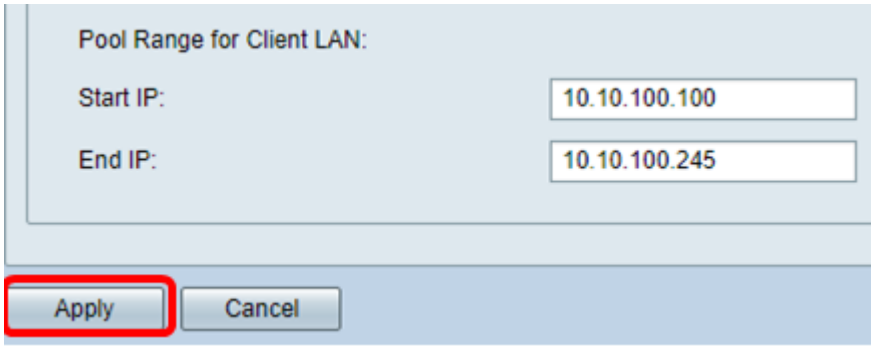
Hinweis: In diesem Beispiel wird 10.10.100.100 eingegeben.

Schritt 18: Geben Sie die letzte IP-Adresse ein, die einem VPN-Client im Feld *End IP* zugewiesen werden kann.

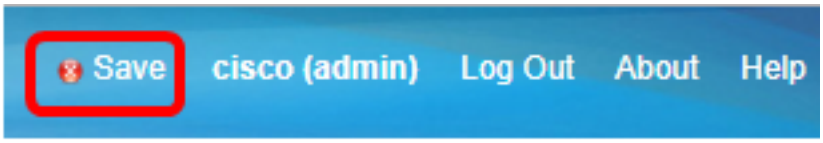


Hinweis: In diesem Beispiel wird 10.10.100.245 eingegeben.

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



Schritt 20: Klicken Sie auf **Speichern**.

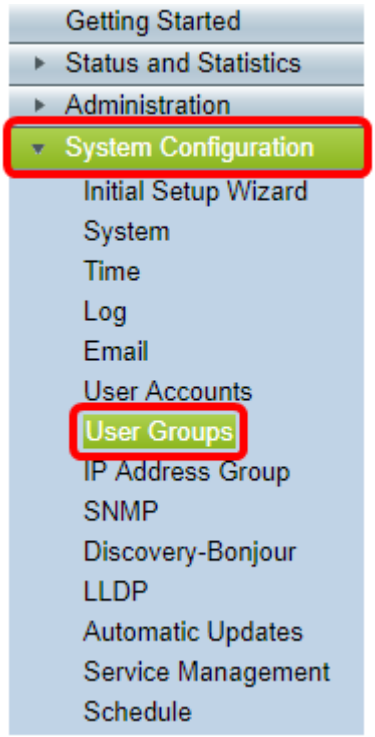


Sie sollten jetzt das Client-to-Site-Profil auf dem Router für den GreenBow VPN Client konfiguriert haben.

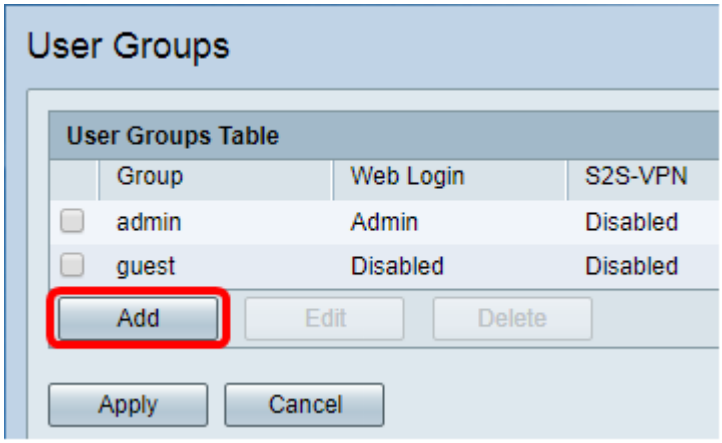
Erstellen einer Benutzergruppe

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

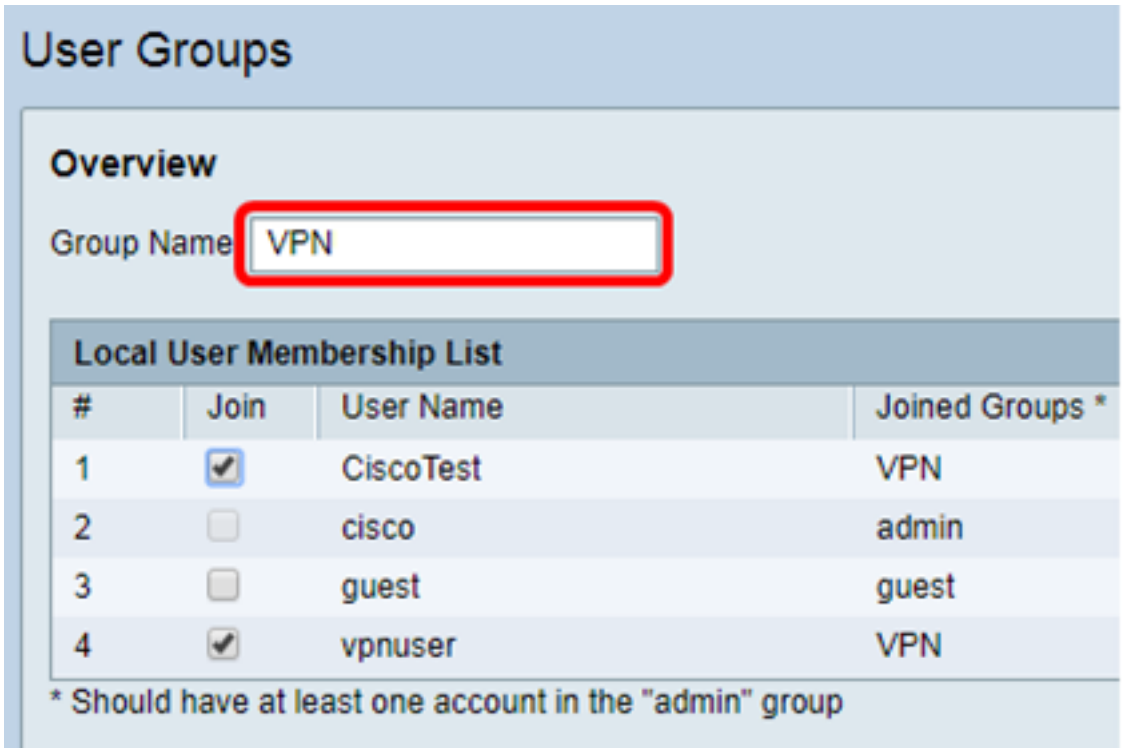
Hinweis: Die Bilder in diesem Artikel stammen von einem RV340 Router. Die Optionen können je nach Modell Ihres Geräts variieren.



Schritt 2: Klicken Sie auf **Hinzufügen**, um eine Benutzergruppe hinzuzufügen.

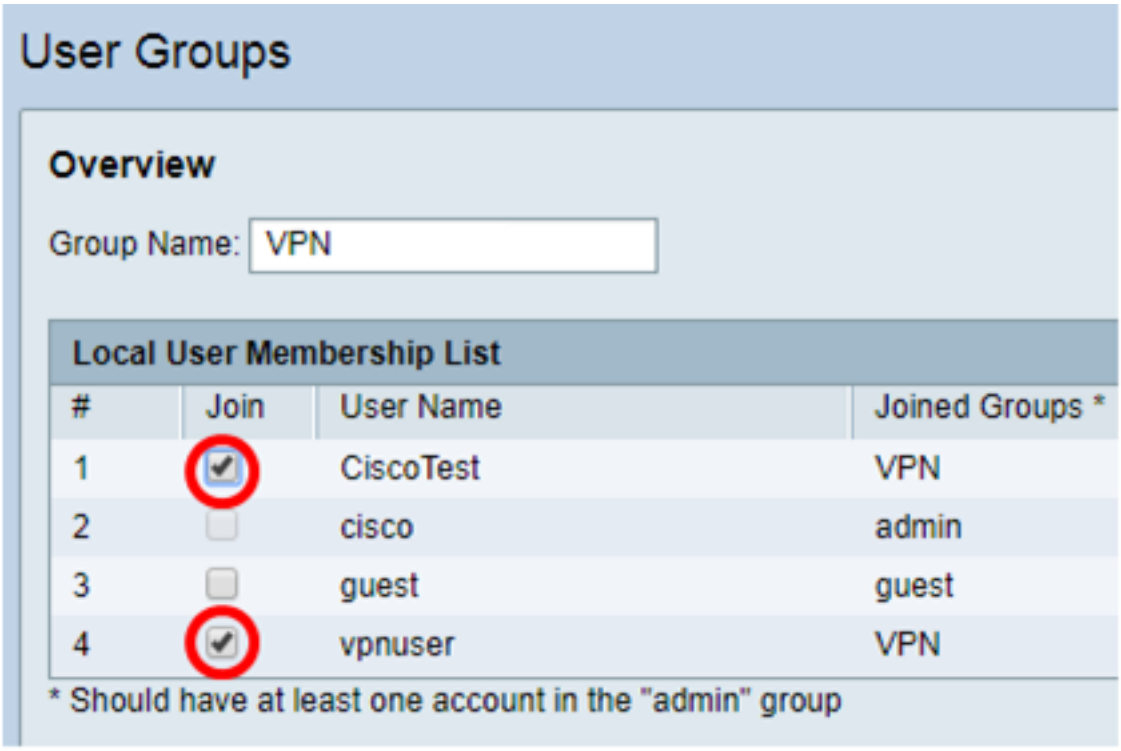


Schritt 3: Geben Sie im Bereich Übersicht im Feld *Gruppenname* den Namen der Gruppe ein.



Hinweis: In diesem Beispiel wird VPN verwendet.

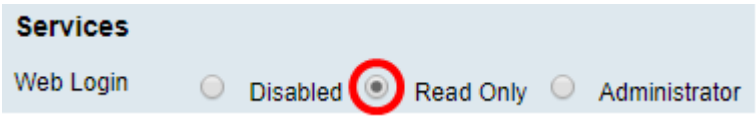
Schritt 4: Aktivieren Sie unter Lokale Mitgliedschaftsliste die Kontrollkästchen der Benutzernamen, die derselben Gruppe angehören sollen.



Hinweis: In diesem Beispiel werden CiscoTest und vpnuser ausgewählt.

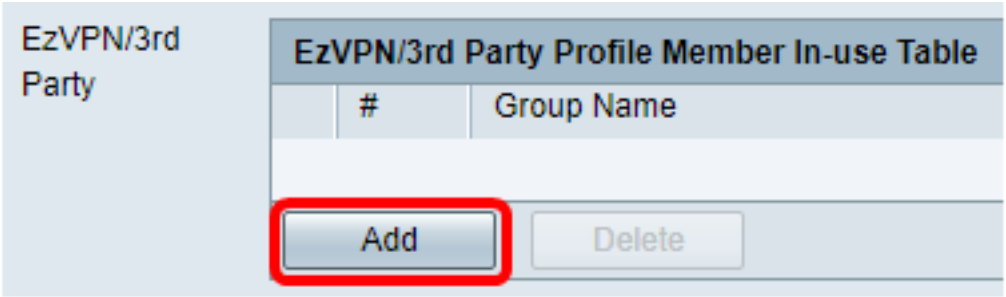
Schritt 5: Wählen Sie unter Dienste eine Berechtigung aus, die den Benutzern in der Gruppe erteilt werden soll. Folgende Optionen stehen zur Verfügung:

- Disabled (Deaktiviert): Diese Option bedeutet, dass Mitglieder der Gruppe nicht über einen Browser auf das webbasierte Dienstprogramm zugreifen dürfen.
- Read Only (Nur Lesen): 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.
- Administrator (Administrator): Diese Option gewährt den Mitgliedern der Gruppe Lese- und Schreibrechte und kann den Systemstatus konfigurieren.

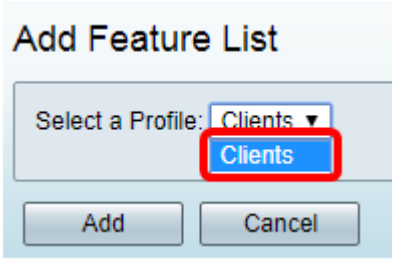


Hinweis: In diesem Beispiel wird Read Only (Nur Lesen) ausgewählt.

Schritt 6: Klicken Sie in der Tabelle "EzVPN/Drittanbieter-Profil-Teilnehmer in Verwendung" auf **Hinzufügen**.

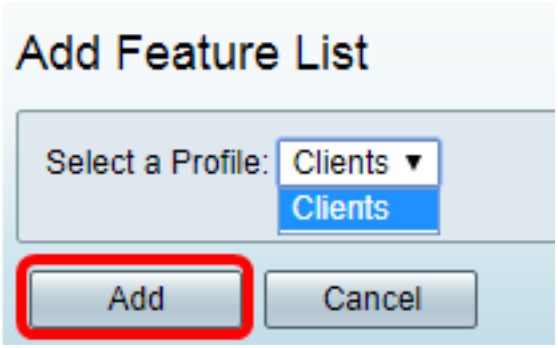


Schritt 7: Wählen Sie aus der Dropdown-Liste Profil auswählen ein Profil aus. Die Optionen können je nach den Profilen variieren, die auf dem VPN-Gateway konfiguriert wurden.

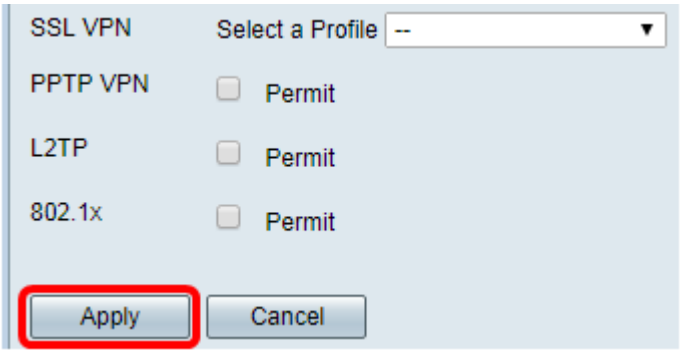


Hinweis: In diesem Beispiel werden Clients ausgewählt.

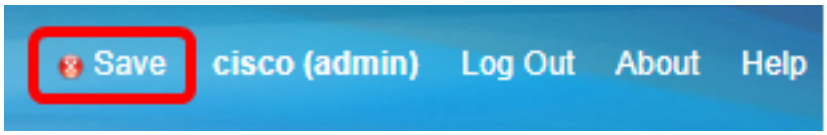
Schritt 8: Klicken Sie auf **Hinzufügen**.



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



Schritt 10: Klicken Sie auf **Speichern**.

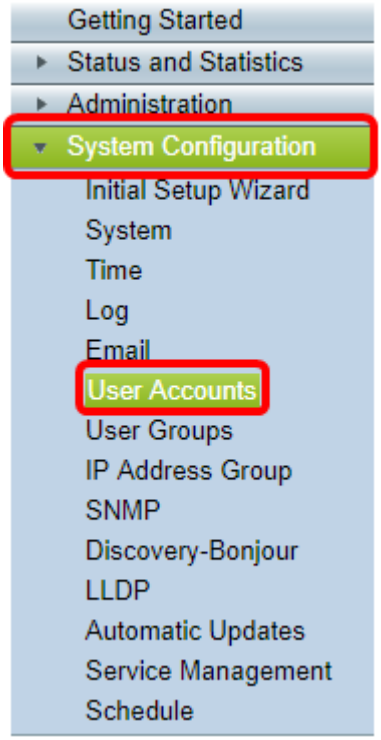


Sie sollten jetzt erfolgreich eine Benutzergruppe auf dem Router der Serie RV34x erstellt haben.

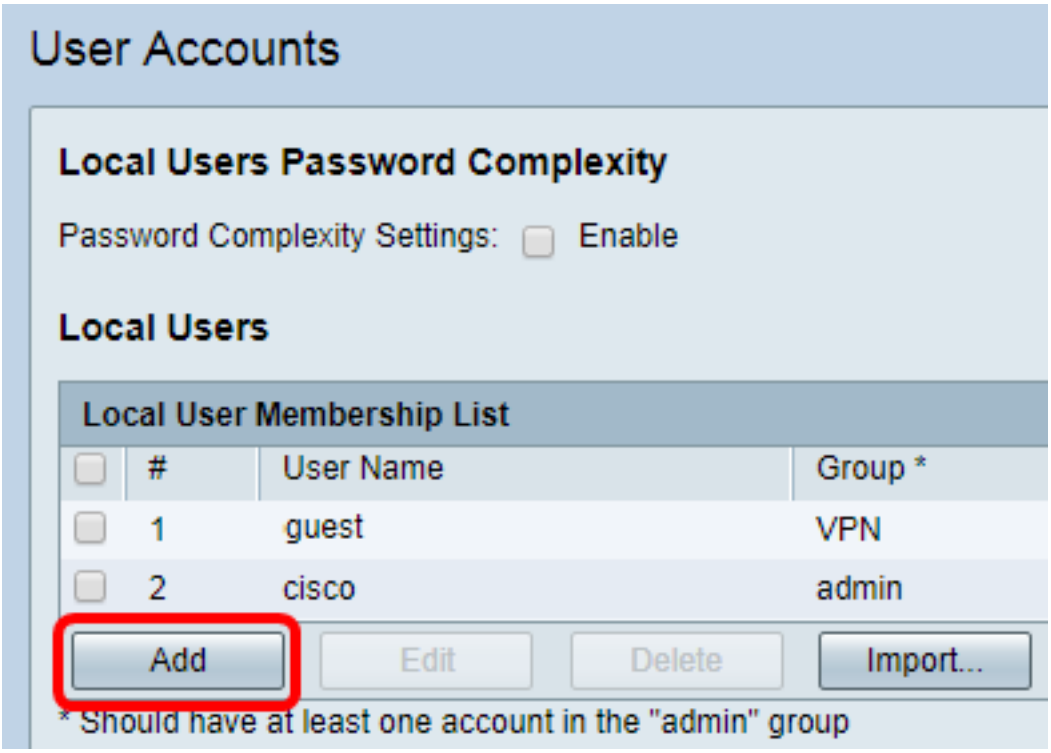
Erstellen eines Benutzerkontos

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

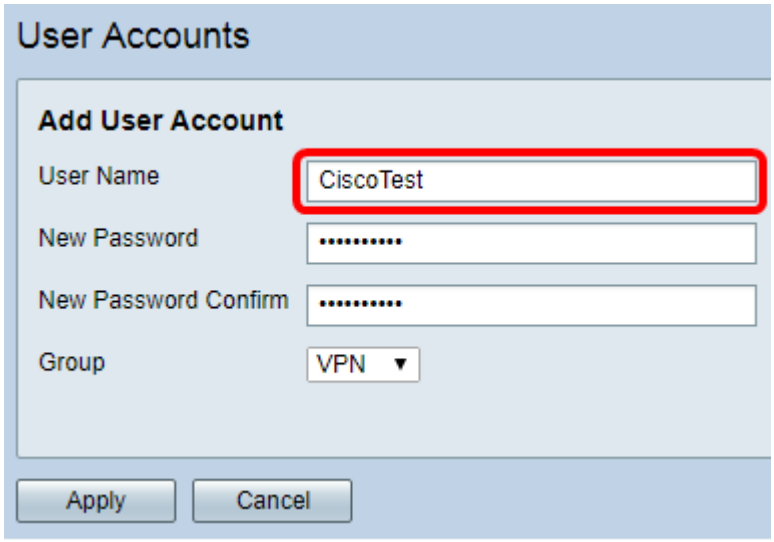
Hinweis: Die Bilder in diesem Artikel stammen von einem RV340 Router. Die Optionen können je nach Modell Ihres Geräts variieren.



Schritt 2: Klicken Sie im Bereich "Liste der lokalen Benutzer" auf **Hinzufügen**.

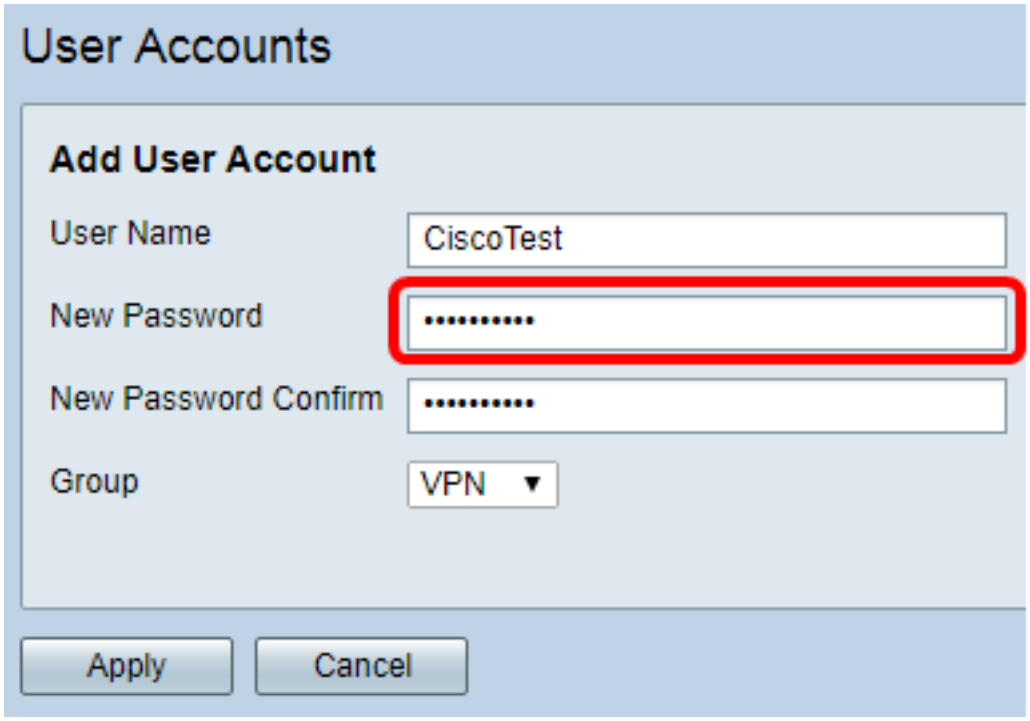


Schritt 3: Geben Sie im Feld *Benutzername* einen Namen für den Benutzer ein.

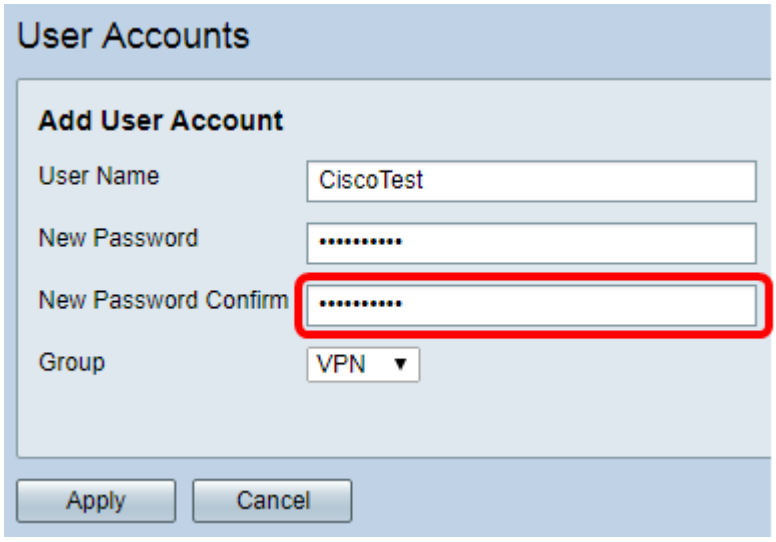


Hinweis: In diesem Beispiel wird CiscoTest eingegeben.

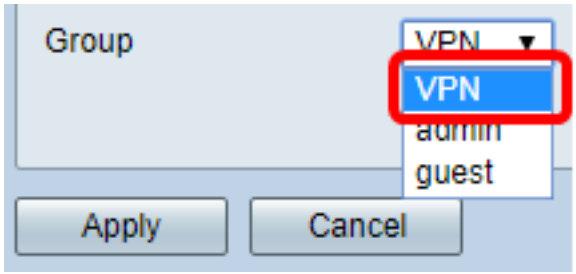
Schritt 4: Geben Sie das Benutzerkennwort in das Feld *Neues Kennwort ein*.



Schritt 5: Bestätigen Sie das Kennwort im Feld *Neue Kennwortbestätigung*.

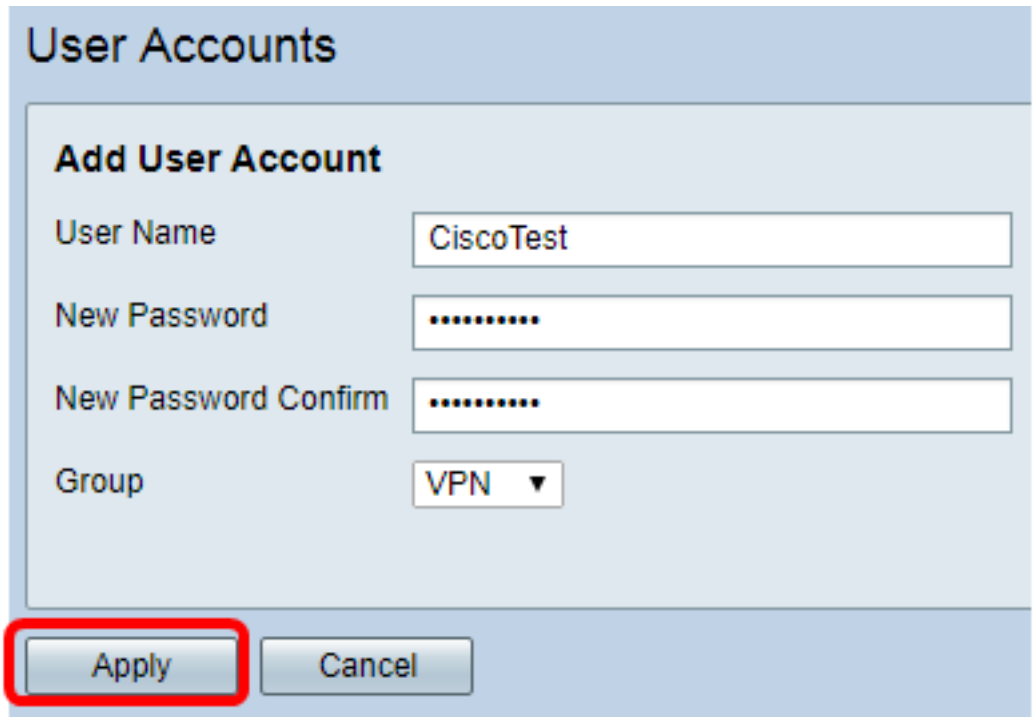


Schritt 6: Wählen Sie aus der Dropdown-Liste Gruppe eine Gruppe aus. Dies ist die Gruppe, der der Benutzer zugeordnet wird.

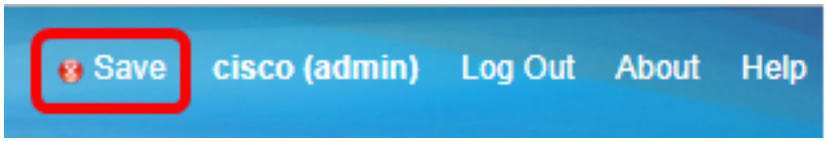


Hinweis: In diesem Beispiel wird VPN ausgewählt.

Schritt 7: Klicken Sie auf **Übernehmen**.



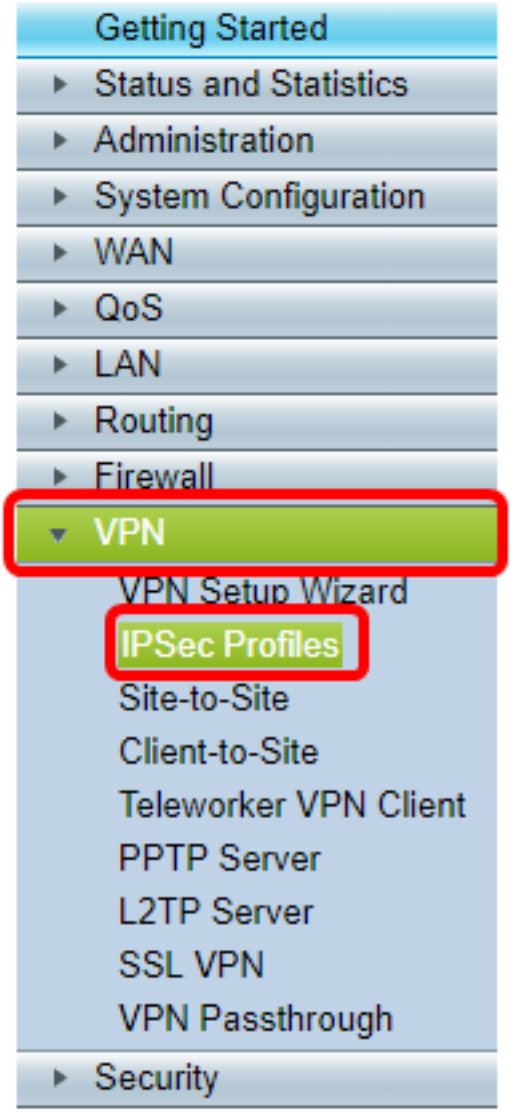
Schritt 8: Klicken Sie auf **Speichern**.



Sie sollten jetzt ein Benutzerkonto auf Ihrem Router der Serie RV34x erstellt haben.

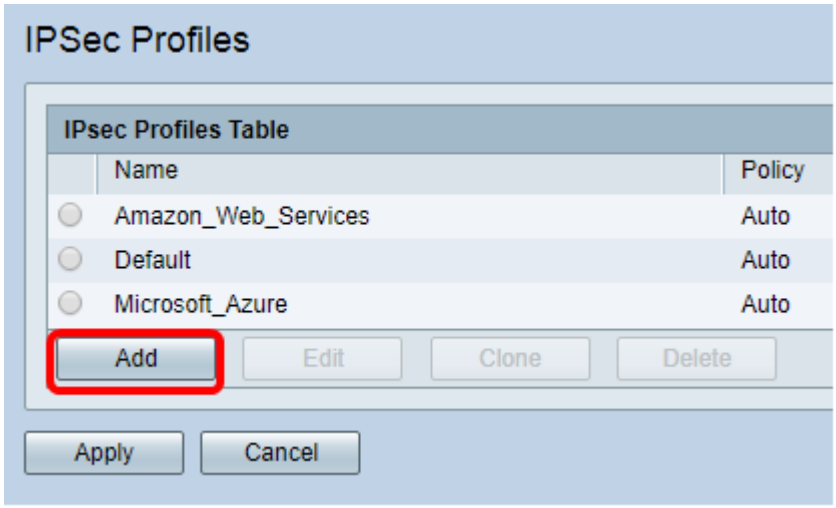
Konfigurieren des IPSec-Profils

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des RV34x-Routers an, und wählen Sie **VPN > IPSec Profiles aus**.



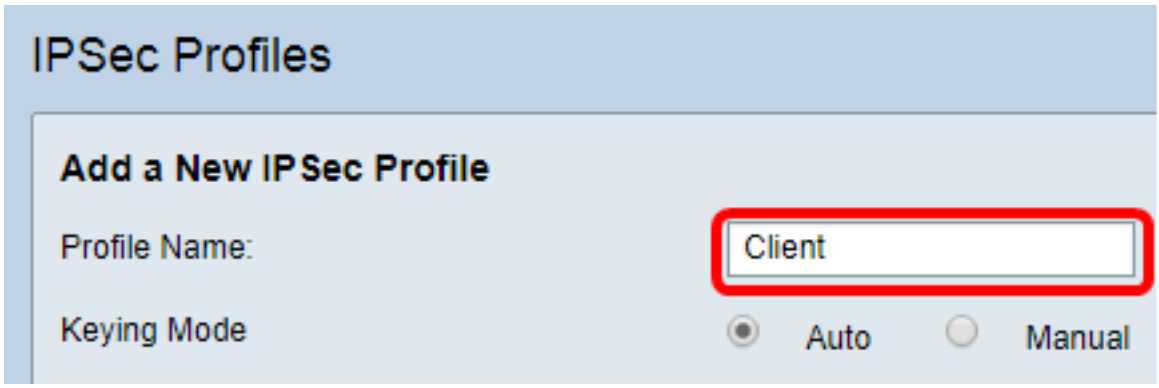
Hinweis: Die Bilder in diesem Artikel stammen vom RV340 Router. Die Optionen können je nach Modell Ihres Geräts variieren.

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



Hinweis: Amazon_Web_Services, Default und Microsoft_Azure sind Standardprofile.

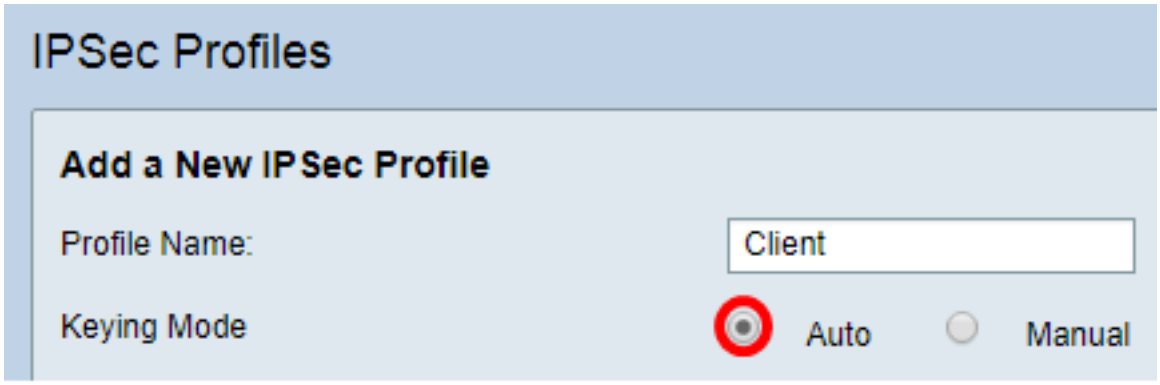
Schritt 3: Erstellen Sie im Feld *Profilname* einen Namen für das Profil. Der Profilname darf nur alphanumerische Zeichen und ein Unterstrich (_) für Sonderzeichen enthalten.



Hinweis: In diesem Beispiel wird Client eingegeben.

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. Wenn diese Option aktiviert ist, fahren Sie mit Auto Settings konfigurieren fort.
- 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. Wenn diese Option ausgewählt ist, fahren Sie mit Manuelle Einstellungen konfigurieren fort.



Hinweis: Für dieses Beispiel wurde Auto ausgewählt.

[Konfigurieren der Einstellungen für Phase I und Phase II]

Schritt 1: Wählen Sie im Bereich Phase 1-Optionen die entsprechende Diffie-Hellman (DH)-Gruppe 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.

Hinweis: In diesem Beispiel wird das Bit Group5-1536 ausgewählt.

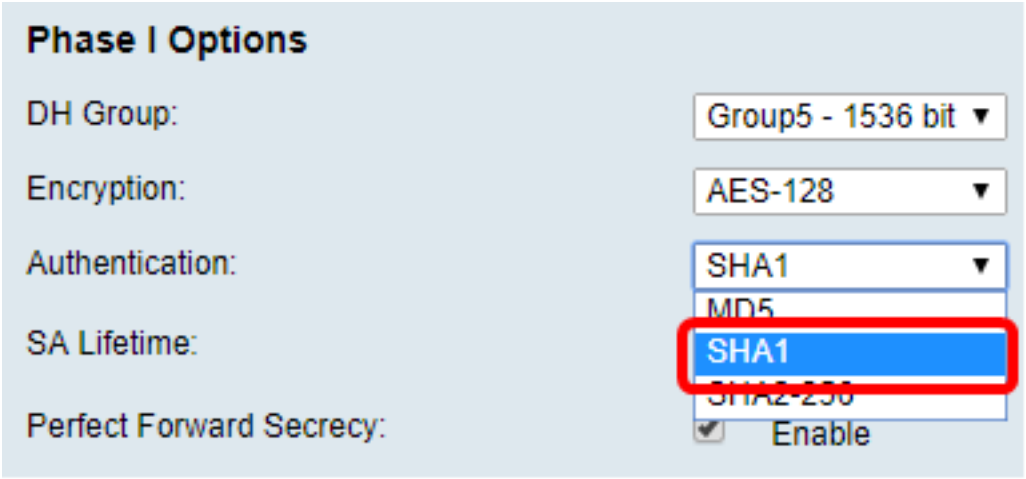
Schritt 2: Wählen Sie in der Dropdown-Liste Verschlüsselung eine Verschlüsselungsmethode zum Verschlüsseln und Entschlüsseln der Encapsulating Security Payload (ESP) und des Internet Security Association and Key Management Protocol (ISAKMP) aus. Folgende Optionen stehen zur Verfügung:

- 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.

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. In diesem Beispiel wird AES-128 ausgewählt.

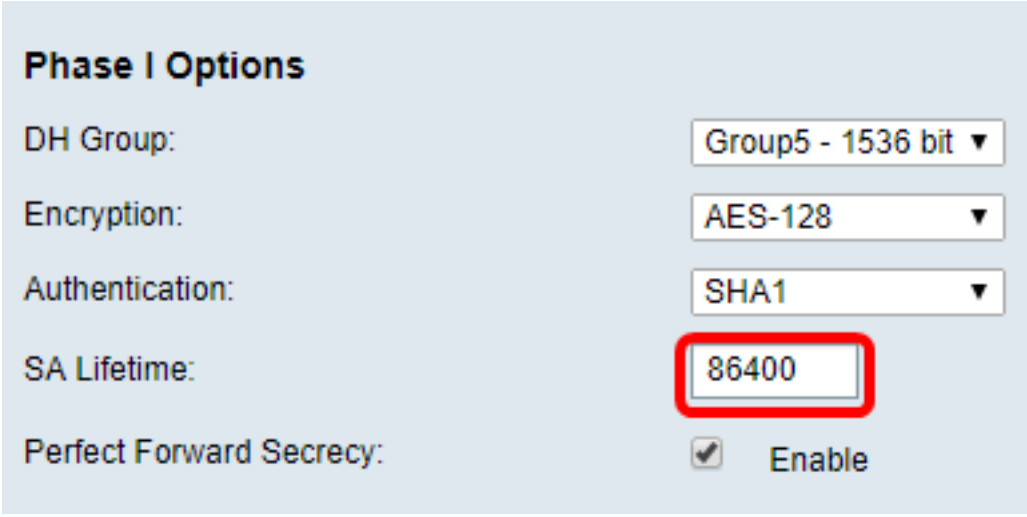
Schritt 3: Wählen Sie in der Dropdown-Liste Authentication (Authentifizierung) eine Authentifizierungsmethode aus, die bestimmt, wie ESP und ISAKMP authentifiziert werden. Folgende Optionen stehen zur Verfügung:

- 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.



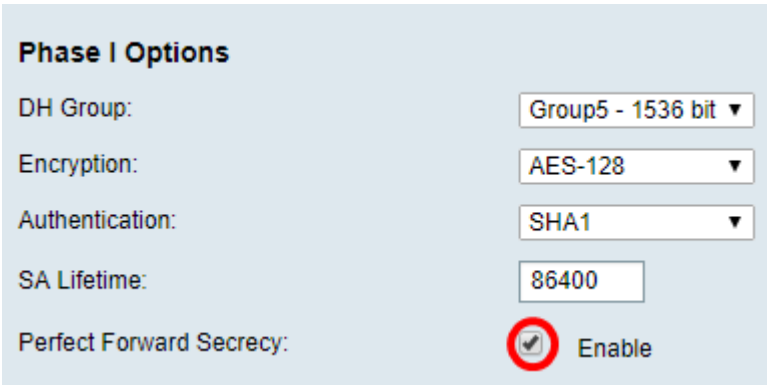
Hinweis: MD5 und SHA sind beide kryptografische Hashfunktionen. Sie nehmen Daten, kompilieren sie und erstellen eine eindeutige Hexadezimalausgabe, die normalerweise nicht reproduziert werden kann. In diesem Beispiel wird SHA1 ausgewählt.

Schritt 4: Geben Sie im Feld *SA Lifetime* (SA-Lebensdauer) einen Wert zwischen 120 und 86400 ein. Dabei handelt es sich um die Dauer, die die Internet Key Exchange (IKE) Security Association (SA) in der Phase aktiv bleiben wird. Der Standardwert ist 28800.



Hinweis: In diesem Beispiel wird 86400 eingegeben.

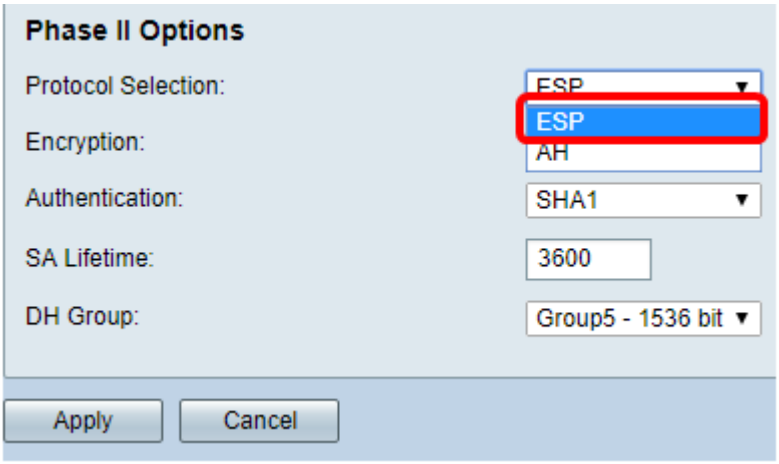
Schritt 5: (Optional) Aktivieren Sie das Kontrollkästchen **Enable Perfect Forward Secrecy** (Perfektes Weiterleitungsgeheimnis aktivieren), um einen neuen Schlüssel für die Verschlüsselung und Authentifizierung des IPSec-Datenverkehrs zu generieren.



Hinweis: In diesem Beispiel ist Perfect Forward Secrecy aktiviert.

Schritt 6: Wählen Sie in 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:

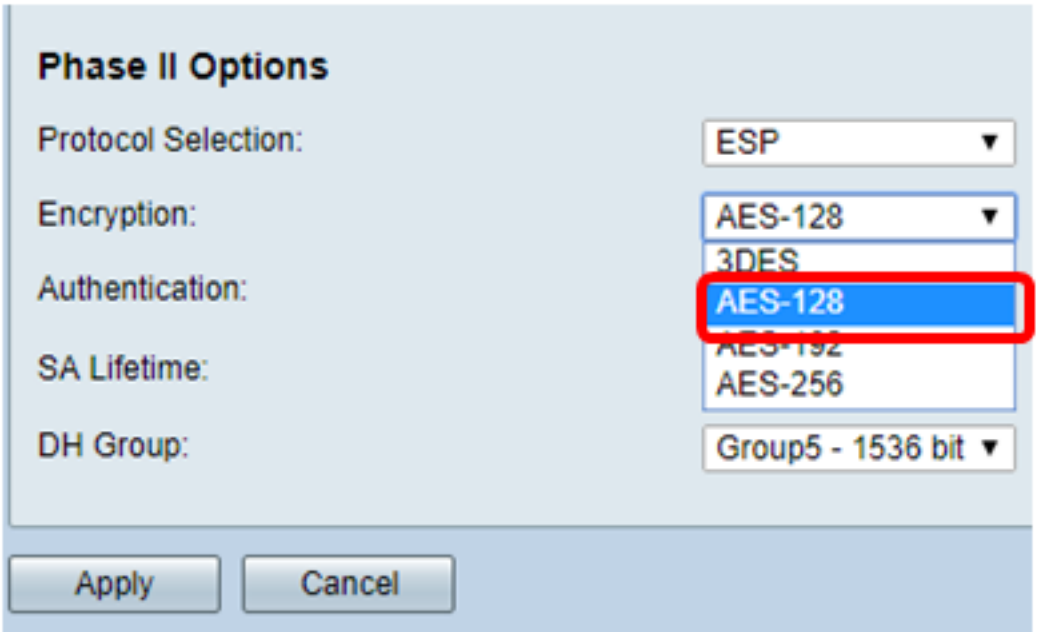
- ESP - Diese Option kapselt die zu schützenden Daten. Wenn diese Option aktiviert ist, fahren Sie mit Schritt 7 fort, um eine Verschlüsselungsmethode auszuwählen.
- AH - Diese Option wird auch als Authentication Header (AH) bezeichnet. Es ist ein Sicherheitsprotokoll, das Datenauthentifizierung und optionalen Anti-Replay-Dienst bietet. AH ist in das zu schützende IP-Datagramm integriert. Wenn diese Option ausgewählt ist, fahren Sie mit Schritt 8 fort.



Hinweis: In diesem Beispiel wird ESP ausgewählt.

Schritt 7: Wenn in Schritt 6 ESP ausgewählt wurde, wählen Sie eine Authentifizierungsmethode aus, die bestimmt, wie ESP und ISAKMP authentifiziert werden. Folgende Optionen stehen zur Verfügung:

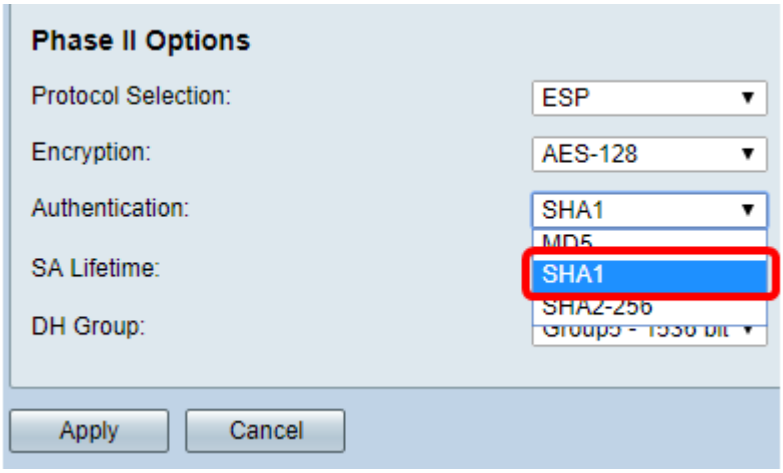
- 3DES = Triple Data Encryption Standard
- AES-128 - Advanced Encryption Standard verwendet einen 128-Bit-Schlüssel.
- AES-192 - Advanced Encryption Standard verwendet einen 192-Bit-Schlüssel.
- AES-256 - Advanced Encryption Standard verwendet einen 256-Bit-Schlüssel.



Hinweis: In diesem Beispiel wird AES-128 ausgewählt.

Schritt 8: Wählen Sie in 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.

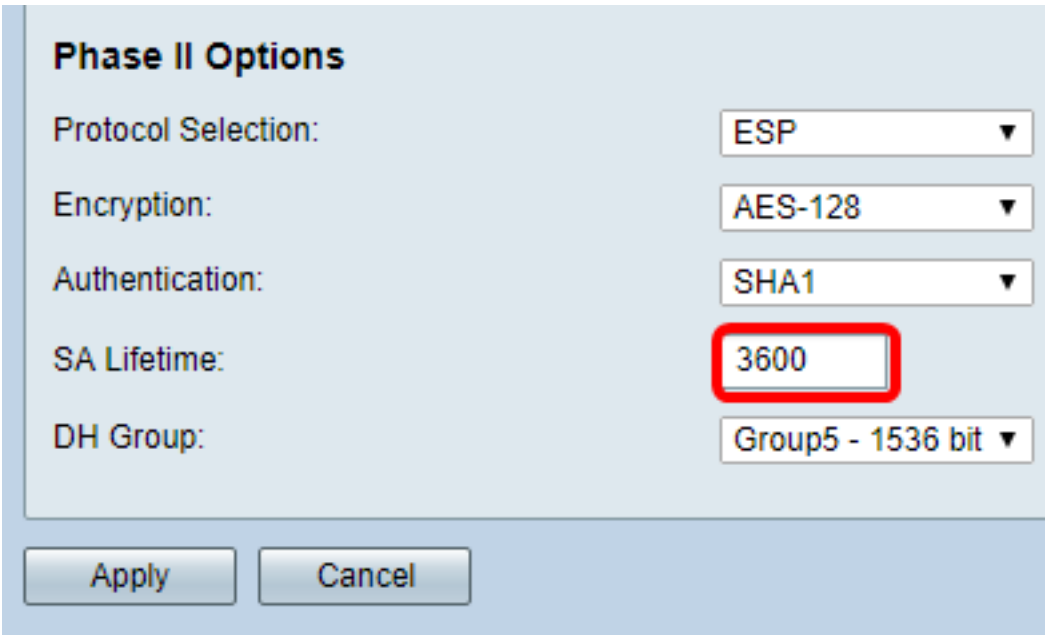


Hinweis: In diesem Beispiel wird SHA1 ausgewählt.

Schritt 9: 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.

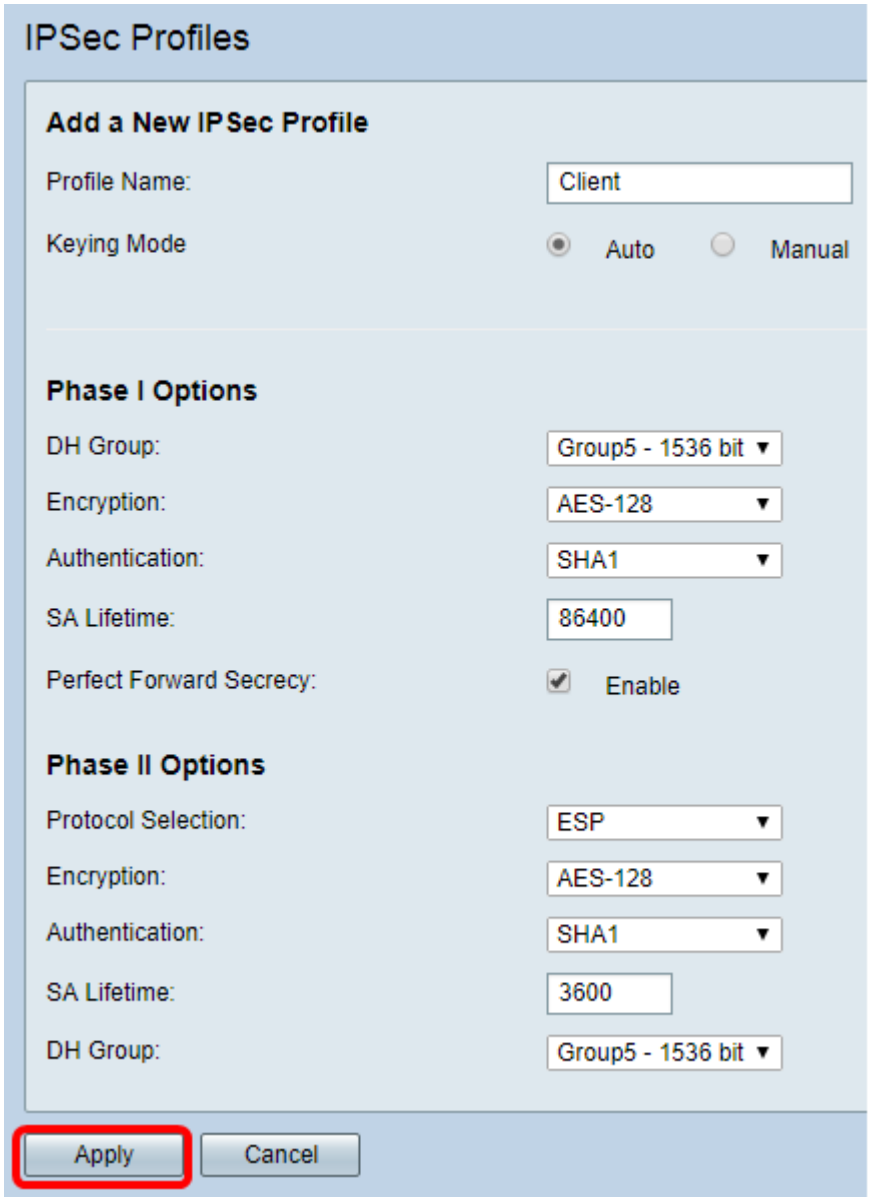
Schritt 10: Wählen Sie in der Dropdown-Liste "DH Group" (DH-Gruppe) eine DH-Gruppe aus, die mit dem Schlüssel in Phase 2 verwendet werden soll. Folgende Optionen stehen zur Verfügung:

- Group2-1024 bit (Gruppe2-1024 Bit): Diese Option berechnet den Schlüssel langsamer, ist jedoch sicherer als Group1.
- Group5-1536 bit (Gruppe5-156 Bit): Diese Option berechnet den Schlüssel am langsamsten, aber am sichersten.

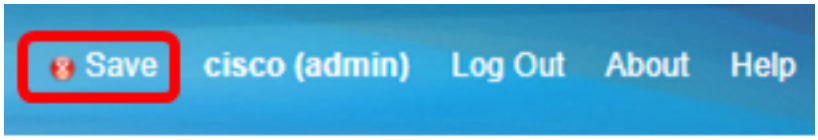


Hinweis: In diesem Beispiel wird 3600 eingegeben.

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



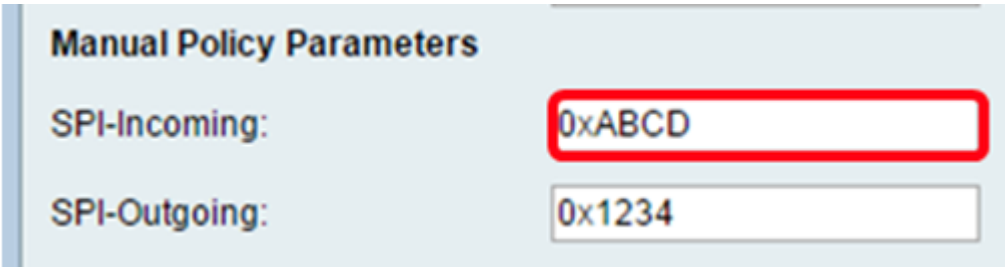
Schritt 12: Klicken Sie auf **Speichern**, um die Konfiguration dauerhaft zu speichern.



Sie sollten jetzt ein automatisches IPSec-Profil auf Ihrem Router der Serie RV34x erfolgreich konfiguriert haben.

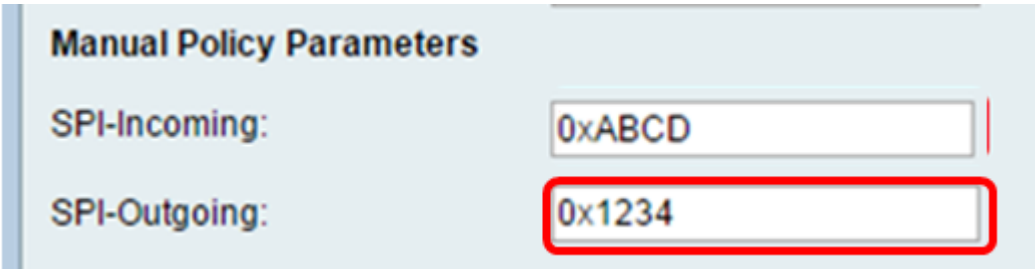
Konfigurieren der manuellen Einstellungen

Schritt 1: Geben Sie im Feld *SPI-Incoming* (SPI-Incoming) einen Hexadezimalwert von 100 bis FFFFFFF für das SPI-Tag (Security Parameter Index) für eingehenden Datenverkehr an der VPN-Verbindung ein. Der SPI-Tag wird verwendet, um den Datenverkehr einer Sitzung vom Datenverkehr anderer Sitzungen zu unterscheiden.



Hinweis: In diesem Beispiel wird 0xABCD eingegeben.

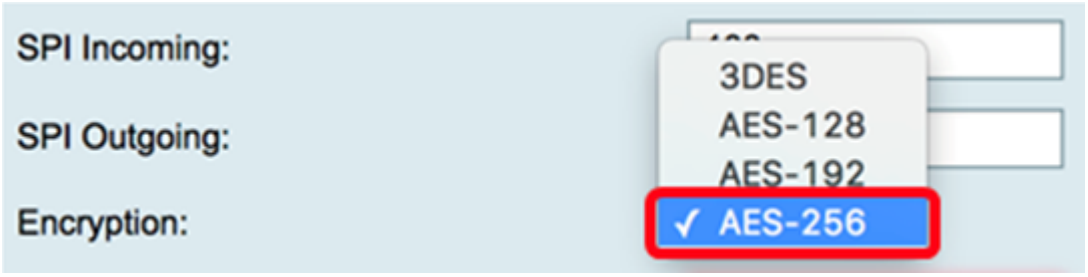
Schritt 2: Geben Sie im Feld *SPI-Outgoing* (*SPI-Ausgang*) einen Hexadezimalwert zwischen 100 und FFFFFFF für das SPI-Tag für ausgehenden Datenverkehr an der VPN-Verbindung ein.



Hinweis: In diesem Beispiel wird 0x1234 eingegeben.

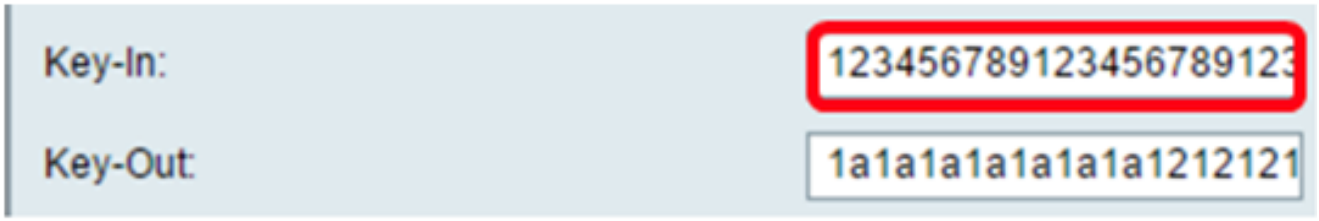
Schritt 3: Wählen Sie aus der Dropdown-Liste einen Verschlüsselungswert aus. Folgende Optionen stehen zur Verfügung:

- 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.



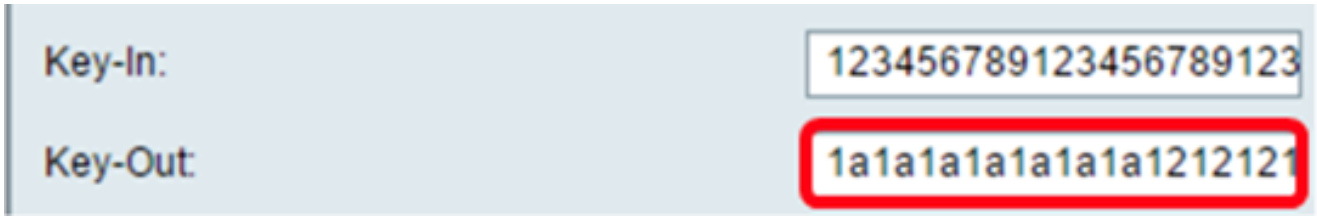
Hinweis: In diesem Beispiel wird AES-256 ausgewählt.

Schritt 4: Geben Sie im Feld *Key-In* (Schlüssel für eingehende Richtlinie) einen Schlüssel ein. Die Länge des Schlüssels hängt von dem in Schritt 3 gewählten Algorithmus ab.



Hinweis: In diesem Beispiel wird 123456789123456789123... eingegeben.

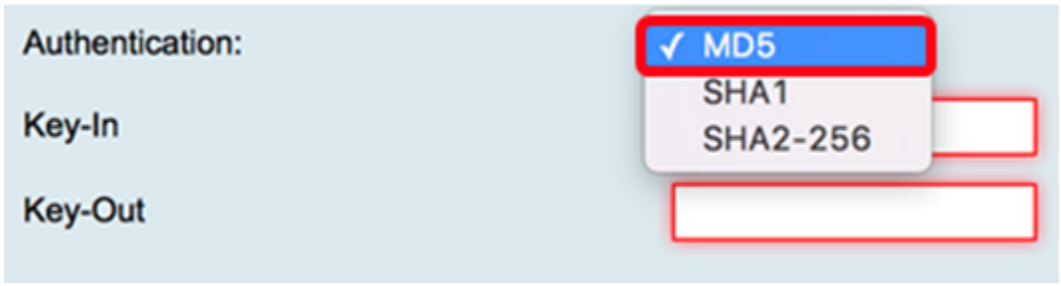
Schritt 5: Geben Sie im Feld *Key-Out* (*Tastenbelegung*) einen Schlüssel für die ausgehende Richtlinie ein. Die Länge des Schlüssels hängt von dem in Schritt 3 gewählten Algorithmus ab.



Hinweis: In diesem Beispiel wird 1a1a1a1a1a1a1a1a121212.. eingegeben.

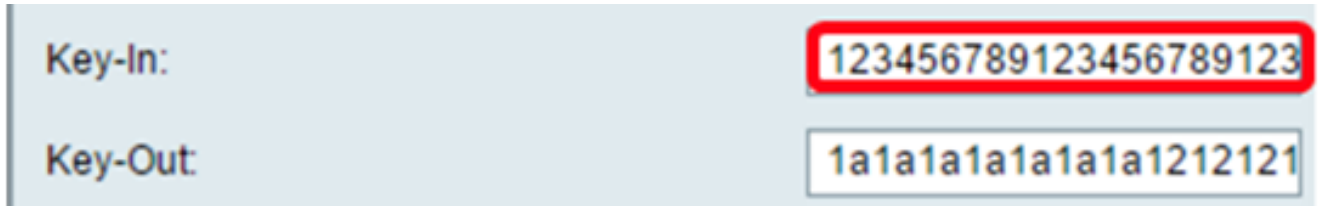
Schritt 6: Wählen Sie aus der Dropdown-Liste Authentifizierung eine Authentifizierungsmethode aus. Folgende Optionen stehen zur Verfügung:

- 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.



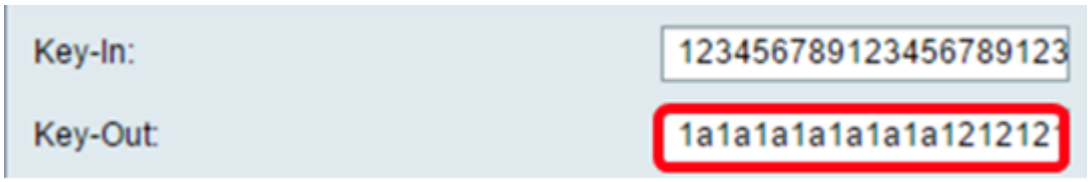
Hinweis: In diesem Beispiel wird MD5 gewählt.

Schritt 7: Geben Sie im Feld *Key-In* (Schlüssel für eingehende Richtlinie) einen Schlüssel ein. Die Länge des Schlüssels hängt von dem in Schritt 6 gewählten Algorithmus ab.

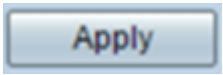


Hinweis: In diesem Beispiel wird 123456789123456789123... eingegeben.

Schritt 8: Geben Sie im Feld *Key-Out* (*Tastenbelegung*) einen Schlüssel für die ausgehende Richtlinie ein. Die Länge des Schlüssels hängt von dem in Schritt 6 gewählten Algorithmus ab.

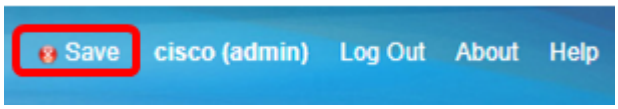


Hinweis: In diesem Beispiel wird 1a1a1a1a1a1a1a1a121212.. eingegeben.

Schritt 9: Klicken Sie auf 

.

Schritt 10: Klicken Sie auf **Speichern**, um die Konfiguration dauerhaft zu speichern.

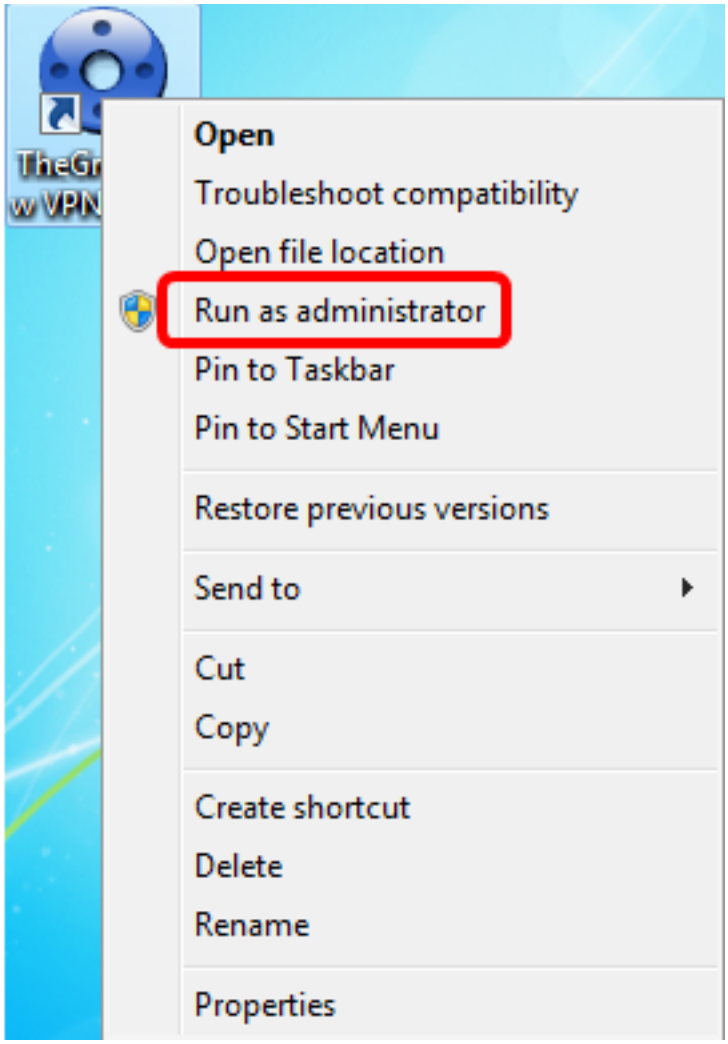


Sie sollten jetzt ein manuelles IPSec-Profil auf einem Router der Serie RV34x erfolgreich konfiguriert haben.

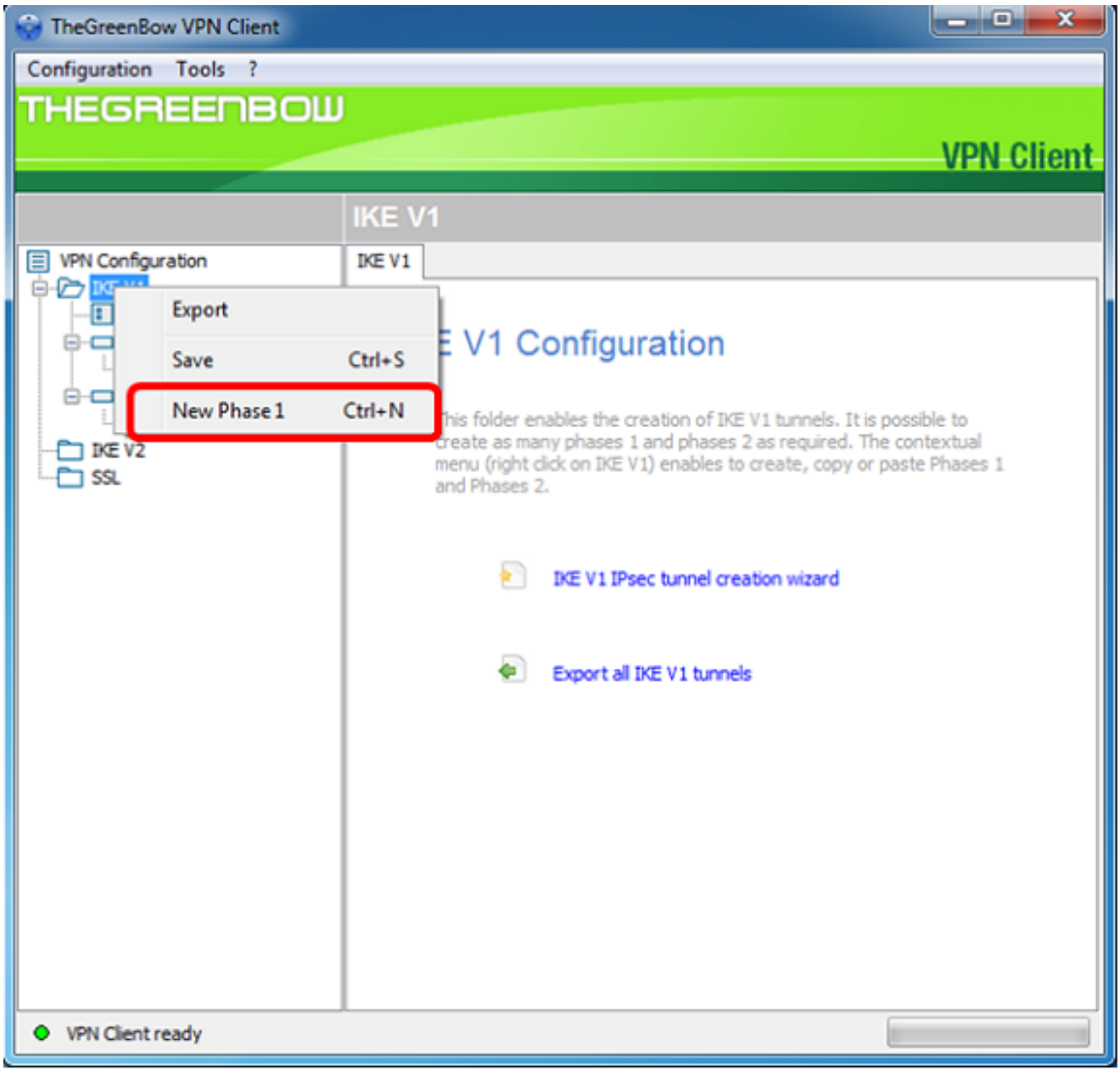
Konfigurieren derGreenBow VPN Client-Software

Konfigurieren der Einstellungen für Phase 1

Schritt 1: Klicken Sie mit der rechten Maustaste auf das Symbol The GreenBow VPN Client, und wählen Sie **Als Administrator ausführen aus**.

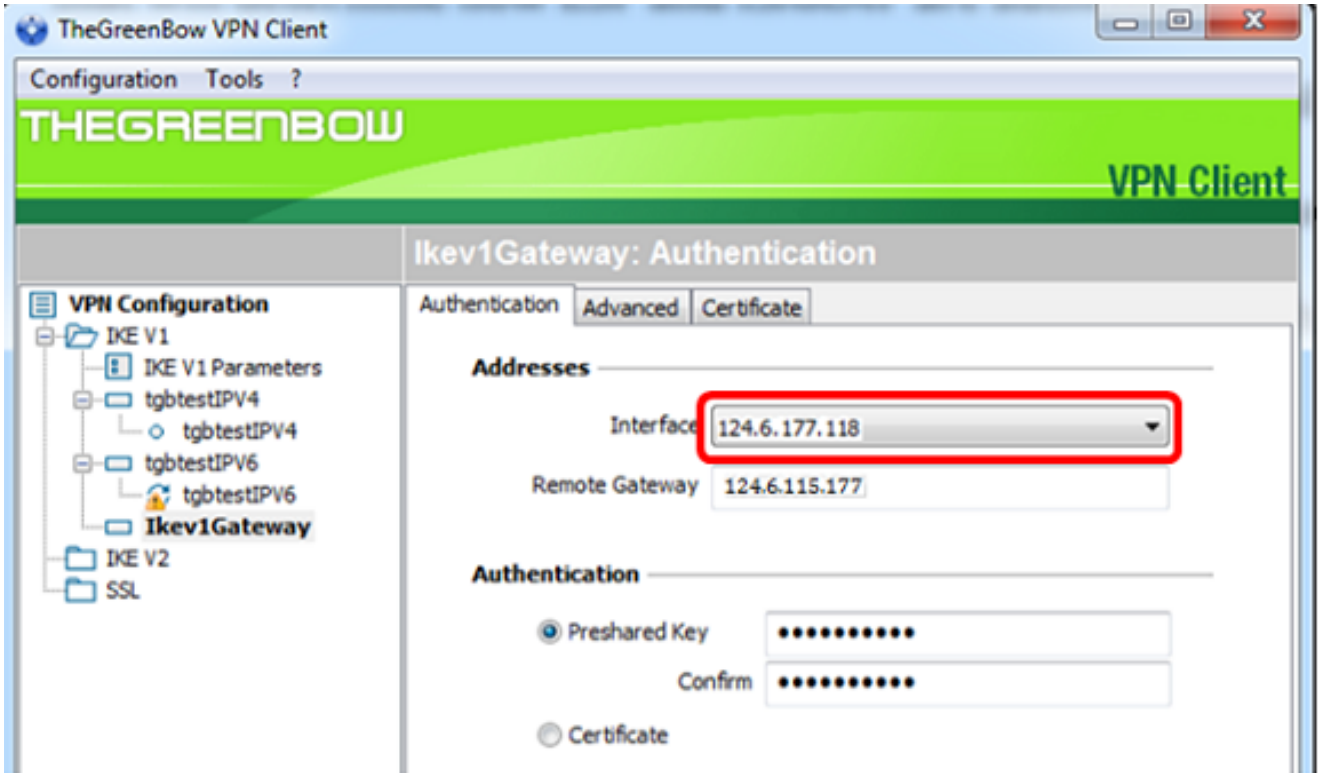


Schritt 2: Klicken Sie im linken Teilfenster unter VPN-Konfiguration mit der rechten Maustaste auf **IKE V1,** und wählen Sie **Neue Phase 1**.



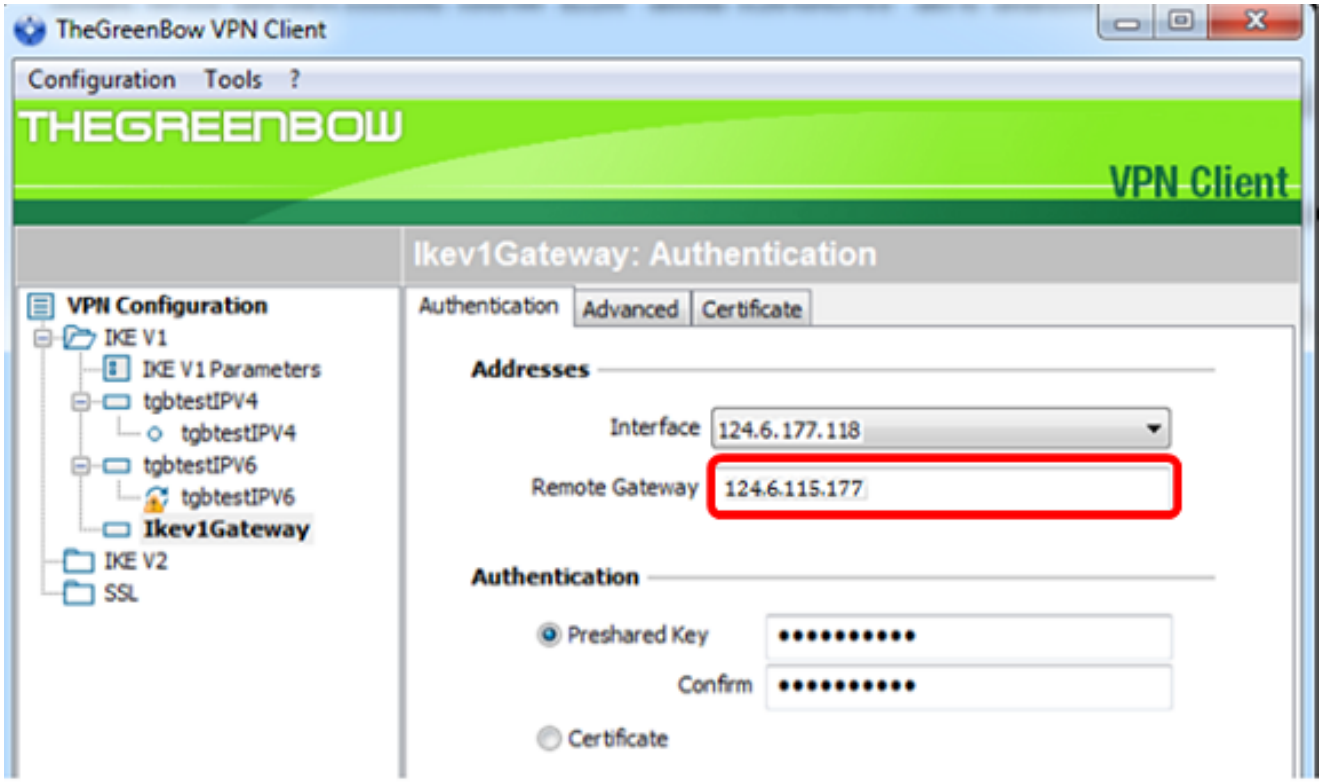
Schritt 3: Überprüfen Sie auf der Registerkarte Authentifizierung unter Adressen, ob die IP-Adresse im Schnittstellenbereich mit der WAN-IP-Adresse des Computers übereinstimmt, auf dem der GreenBow VPN Client installiert ist.

Hinweis: In diesem Beispiel lautet die IP-Adresse 124.6.177.118.



Schritt 4: Geben Sie die Adresse des Remote-Gateways in das Feld *Remote Gateway* ein.

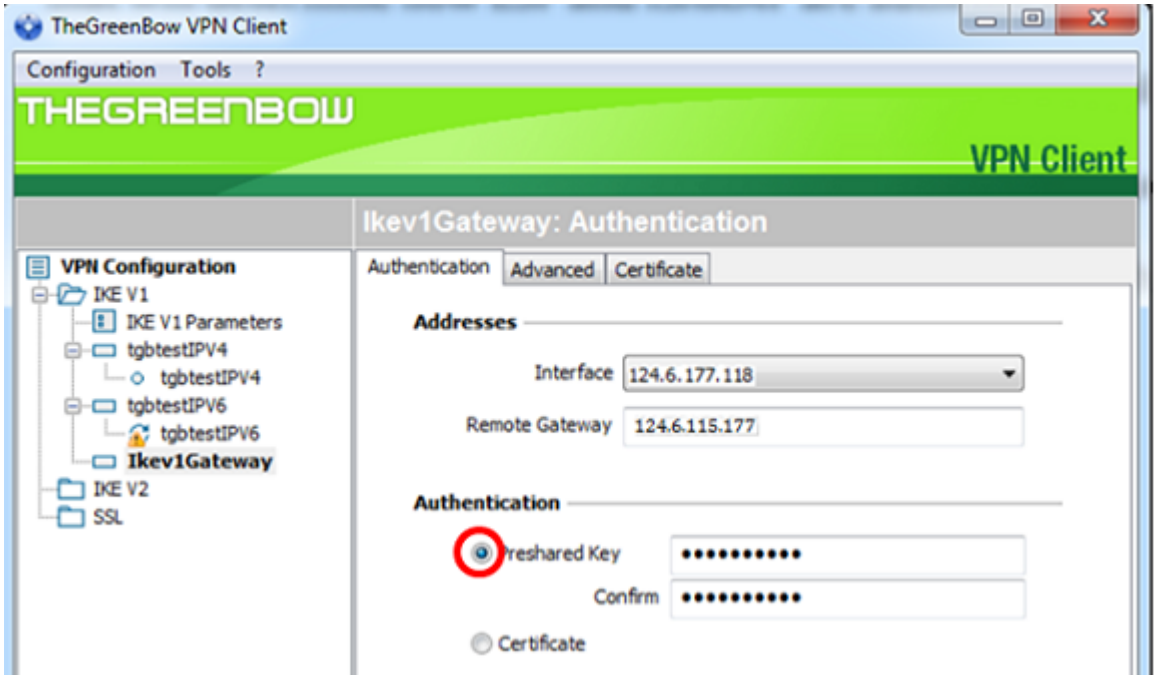
Hinweis: In diesem Beispiel lautet die IP-Adresse des Remote-Routers RV34x 124.6.115.177.



Schritt 5: Wählen Sie unter Authentication (Authentifizierung) den Authentifizierungstyp aus. Folgende Optionen stehen zur Verfügung:

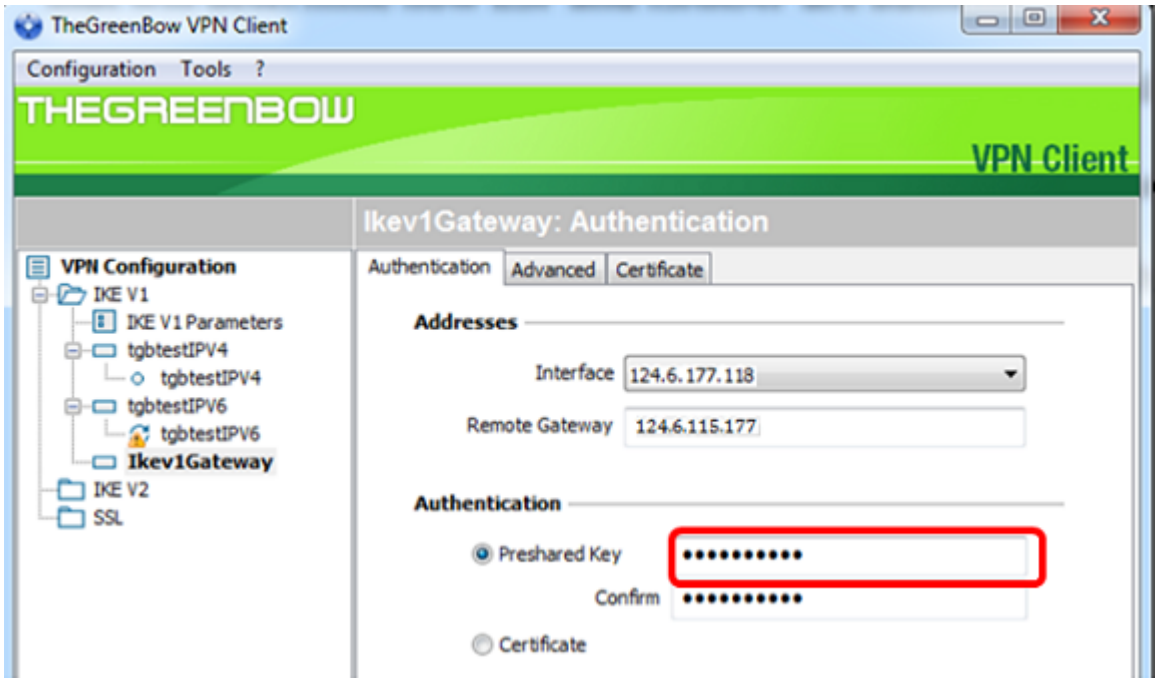
- Preshared Key (Vorinstallierter Schlüssel): Mit dieser Option kann der Benutzer ein Kennwort verwenden, das auf dem VPN-Gateway konfiguriert wurde. Das Kennwort muss vom Benutzer abgeglichen werden, um einen VPN-Tunnel einrichten zu können.

- Zertifikat: Diese Option verwendet ein Zertifikat, um den Handshake zwischen dem VPN-Client und dem VPN-Gateway abzuschließen.

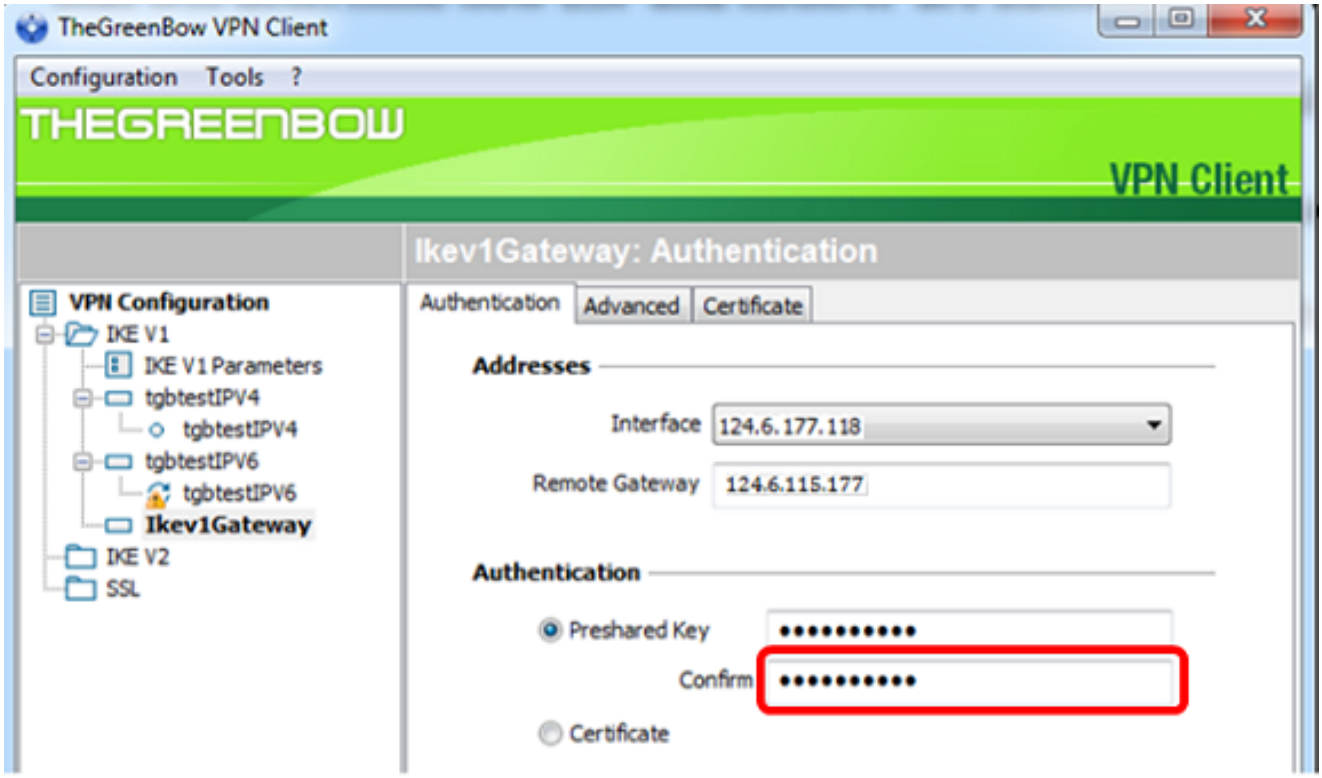


Hinweis: In diesem Beispiel wird der vorinstallierte Schlüssel so gewählt, dass er mit der Konfiguration des RV34x VPN-Gateways übereinstimmt.

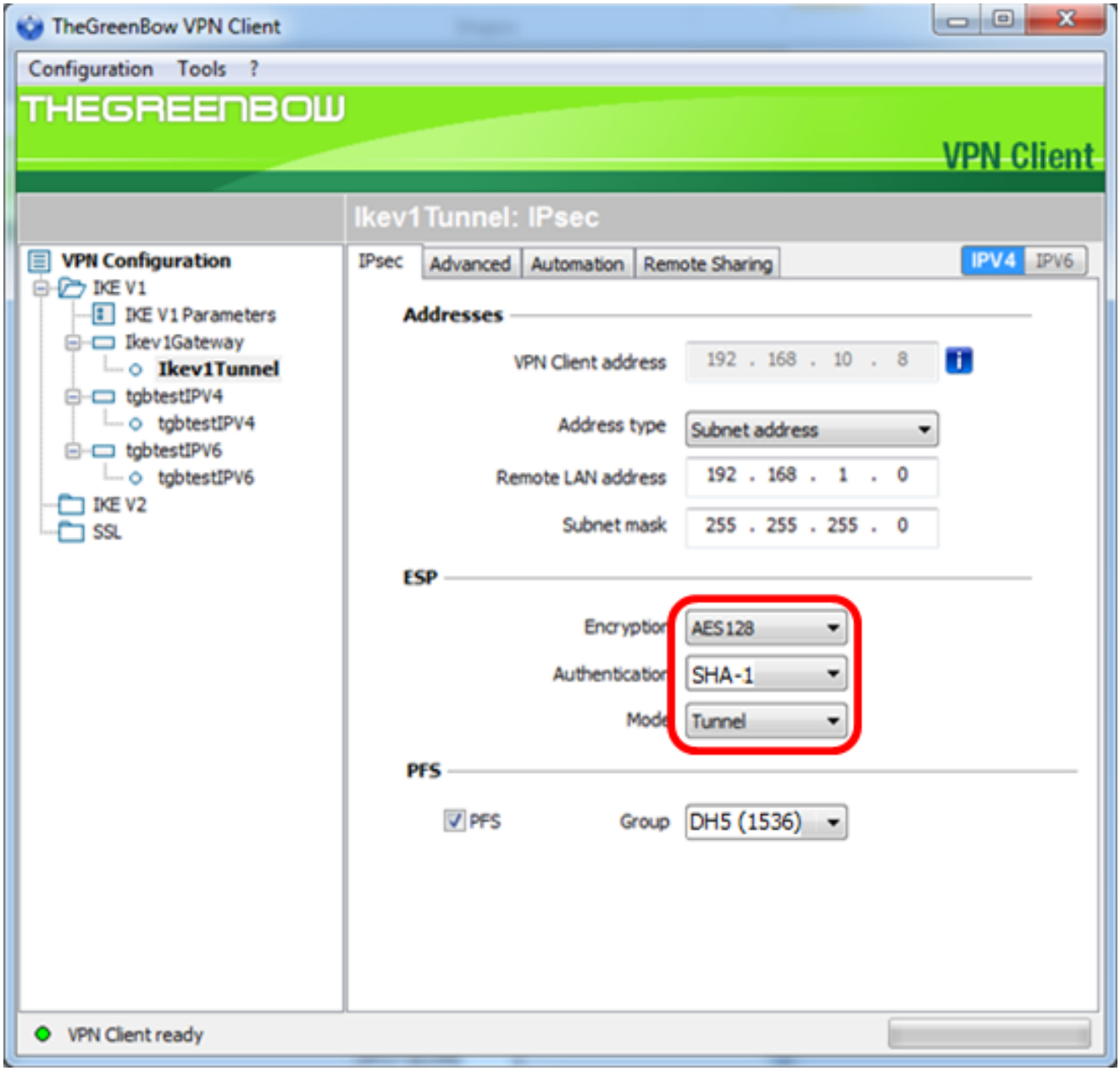
Schritt 6: Geben Sie den im Router konfigurierten vorinstallierten Schlüssel ein.



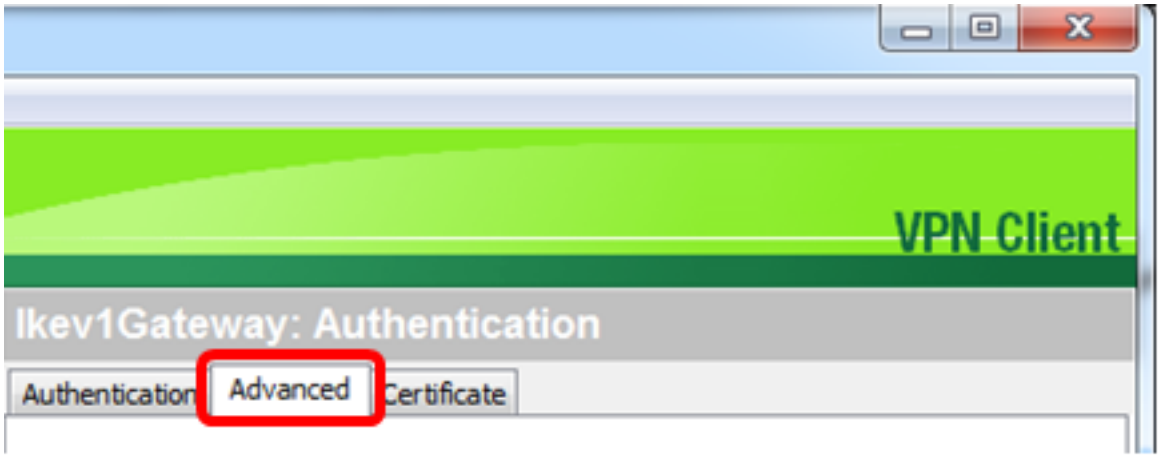
Schritt 7: Geben Sie im Feld *Bestätigen* denselben vorinstallierten Schlüssel ein.



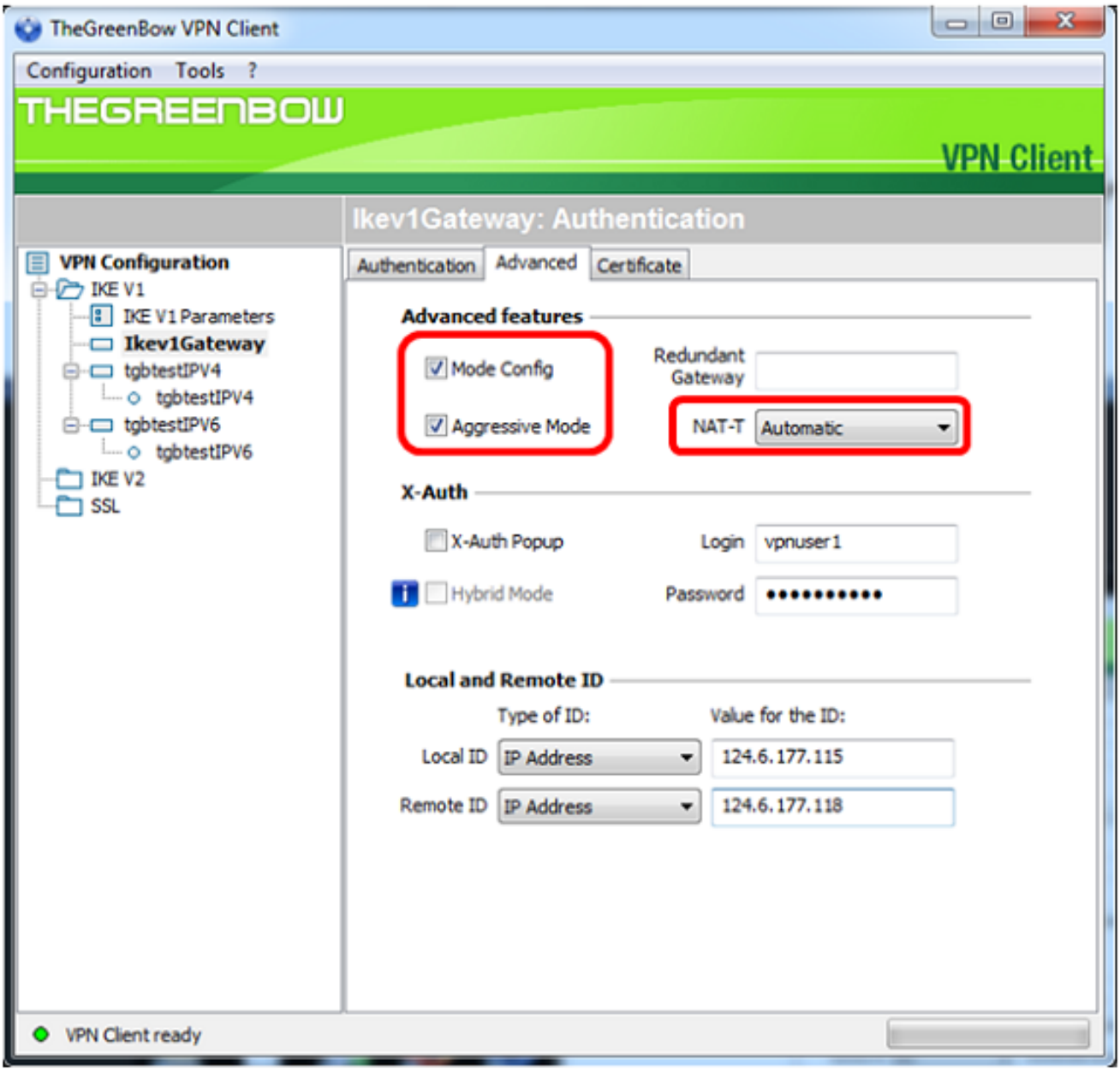
Schritt 8: Legen Sie unter IKE die Einstellungen für Verschlüsselung, Authentifizierung und Schlüsselgruppe so fest, dass sie mit der Konfiguration des Routers übereinstimmen.



Schritt 9: Klicken Sie auf die Registerkarte **Erweitert**.

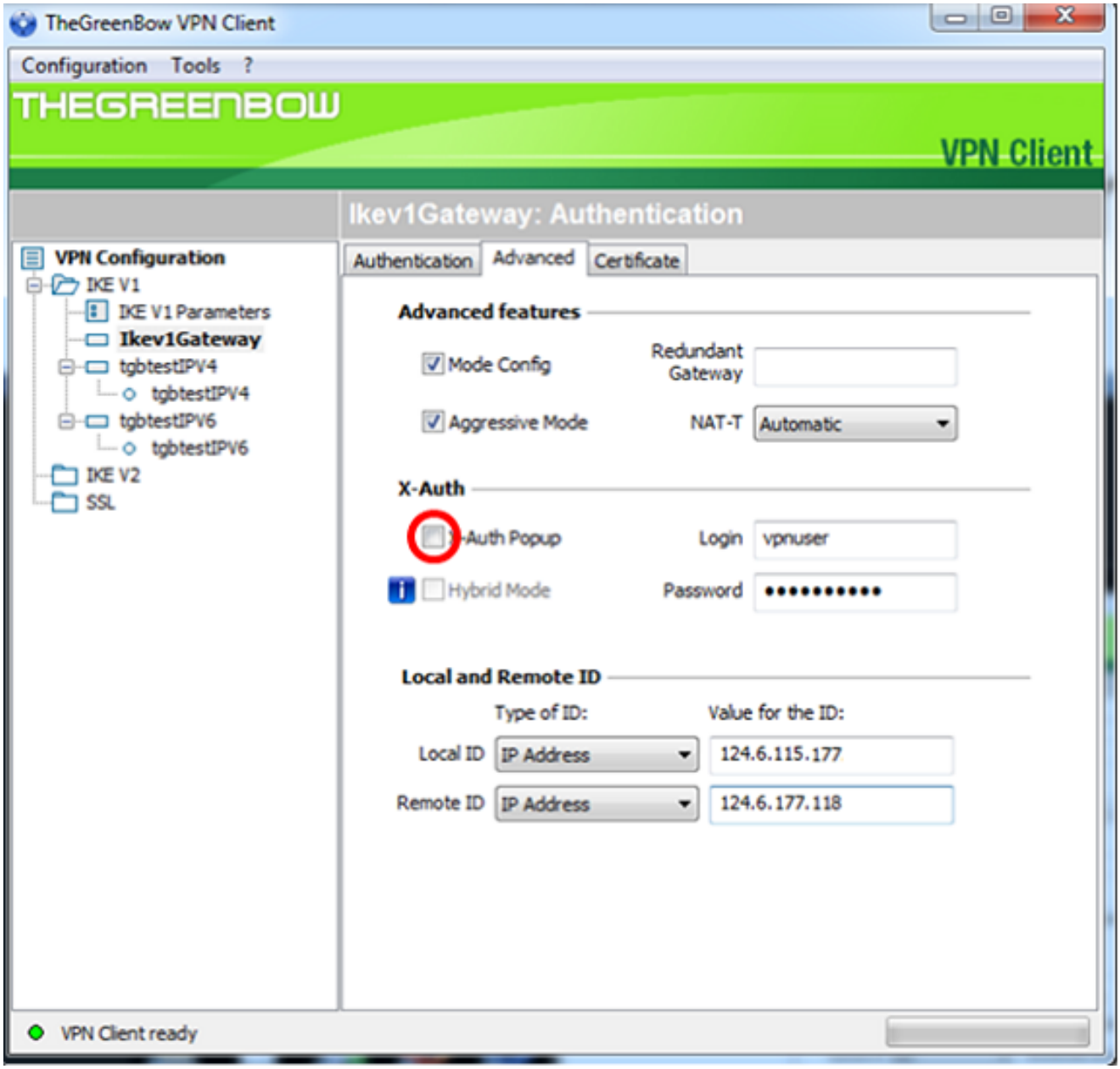


Schritt 10: (Optional) Aktivieren Sie unter Erweiterte Funktionen die Kontrollkästchen **Mode Config** and **Aggressive Mode (Modus-Konfiguration** und aggressiver Modus), und legen Sie die NAT-T-Einstellung auf Automatic (Automatisch) fest.



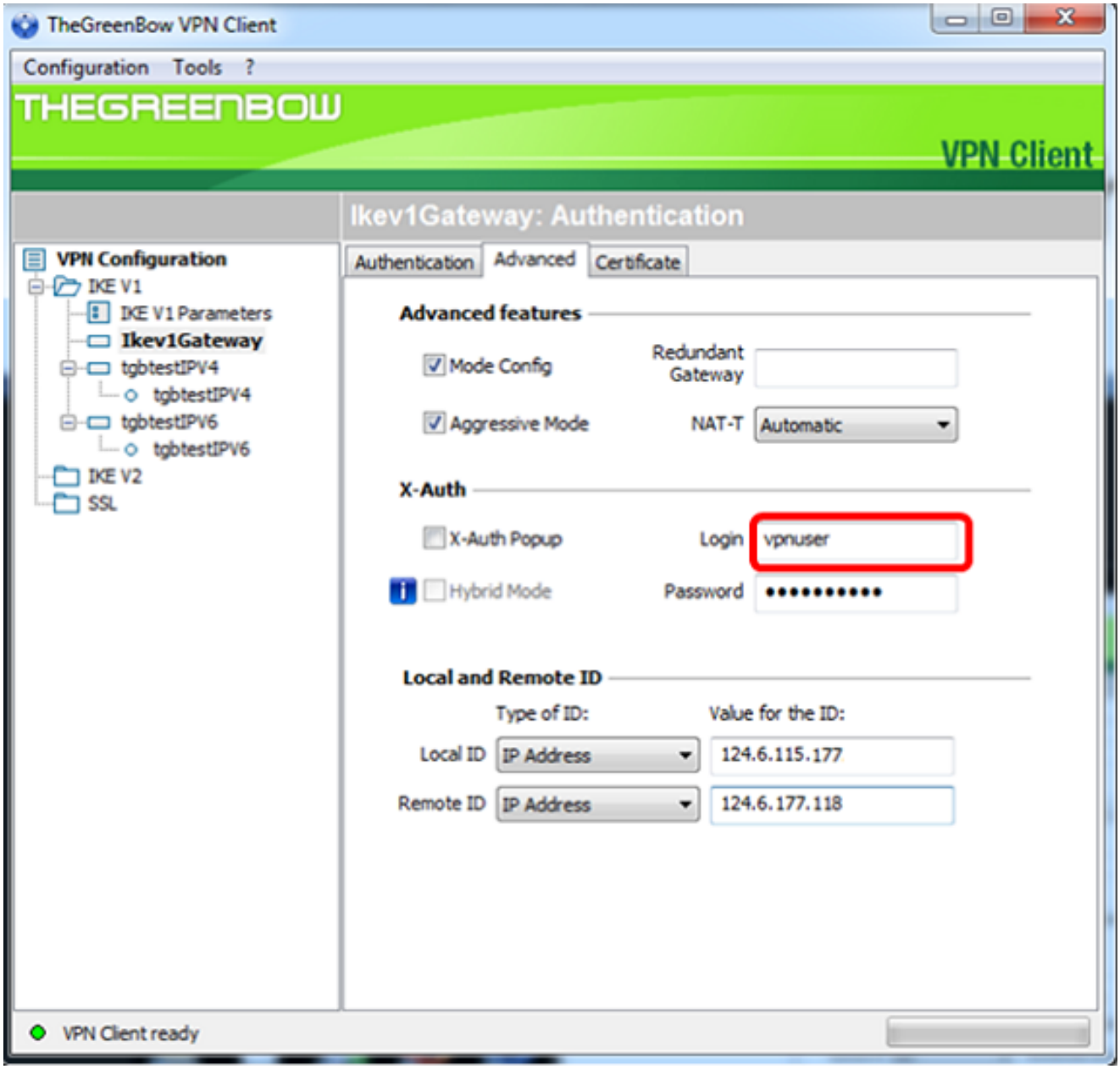
Hinweis: Bei aktivierter Moduskonfiguration ruft der GreenBow VPN Client Einstellungen vom VPN-Gateway ab, um einen Tunnel einzurichten und gleichzeitig den aggressiven Modus zu aktivieren. Mit NAT-T wird der Verbindungsaufbau beschleunigt.

Schritt 11: (Optional) Aktivieren Sie unter X-Auth das Kontrollkästchen **X-Auth Popup**, um das Anmeldungsfenster beim Starten einer Verbindung automatisch aufzurufen. Im Anmeldefenster gibt der Benutzer seine Anmeldeinformationen ein, um den Tunnel abzuschließen.

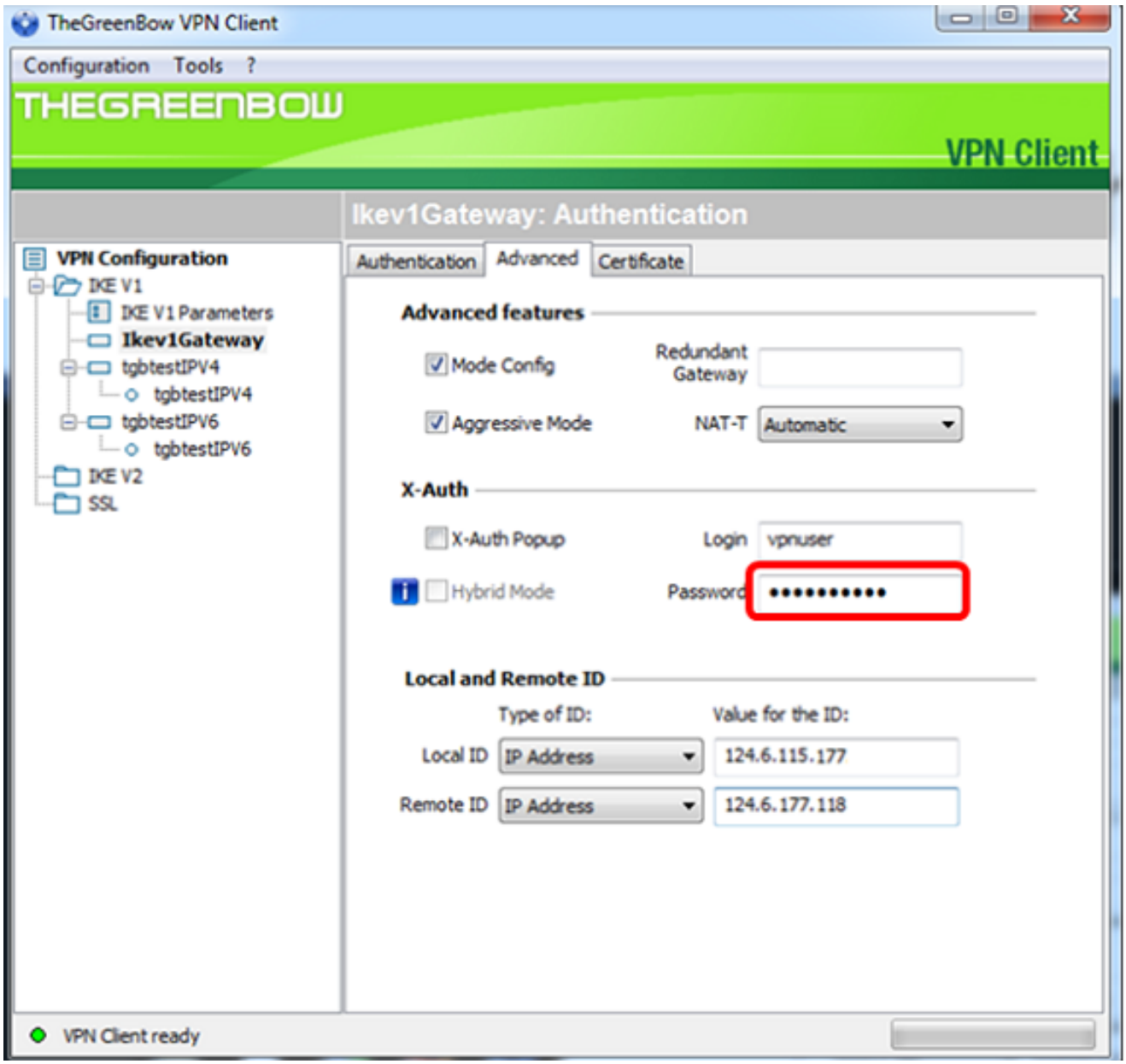


Hinweis: In diesem Beispiel ist X-Auth Popup nicht aktiviert.

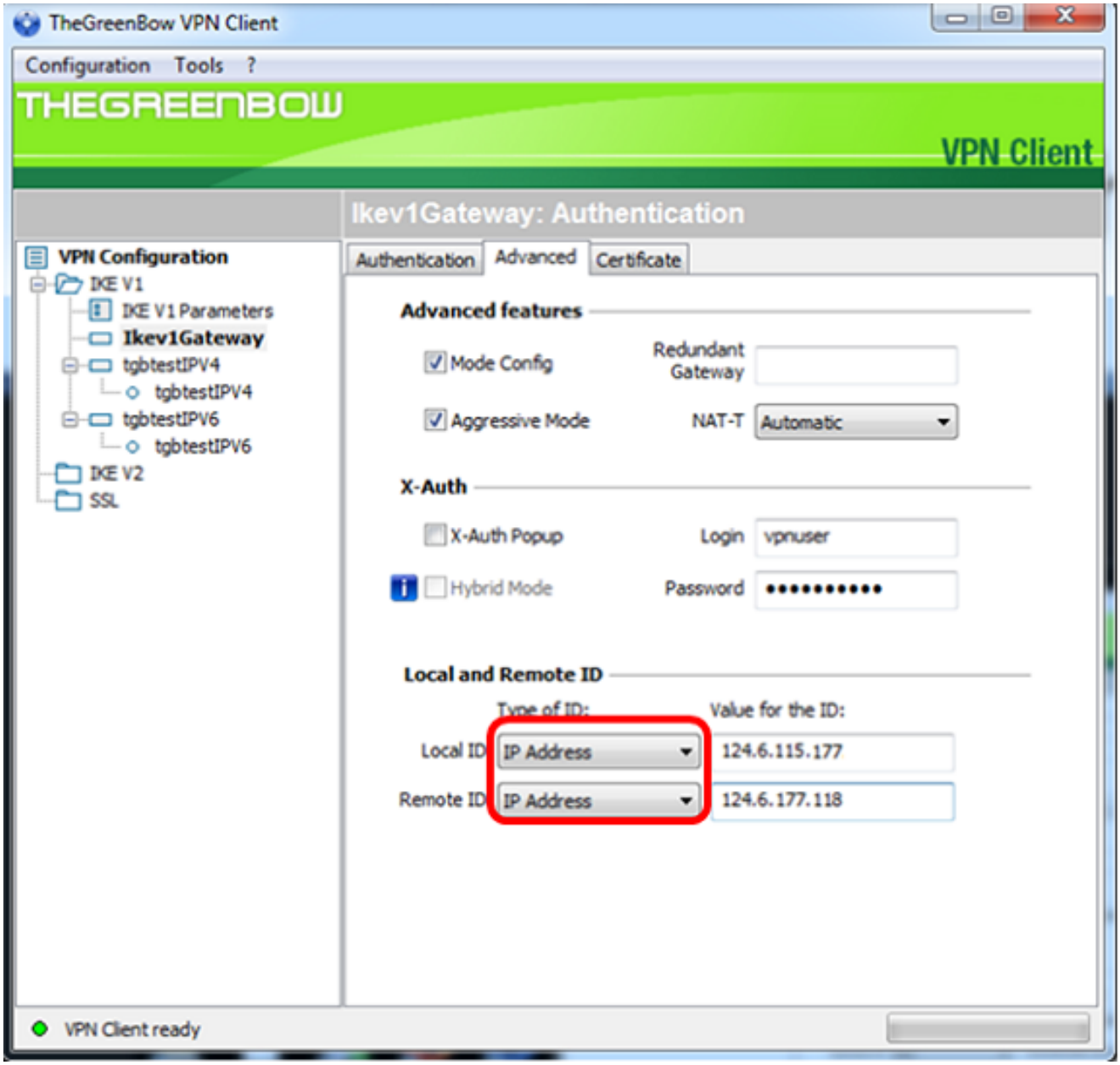
Schritt 12: Geben Sie Ihren Benutzernamen in das Feld *Anmelden ein*. Dies ist der für das Erstellen einer Benutzergruppe im VPN-Gateway konfigurierte Benutzername.



Schritt 13: Geben Sie Ihr Kennwort in das Feld *Kennwort ein*.

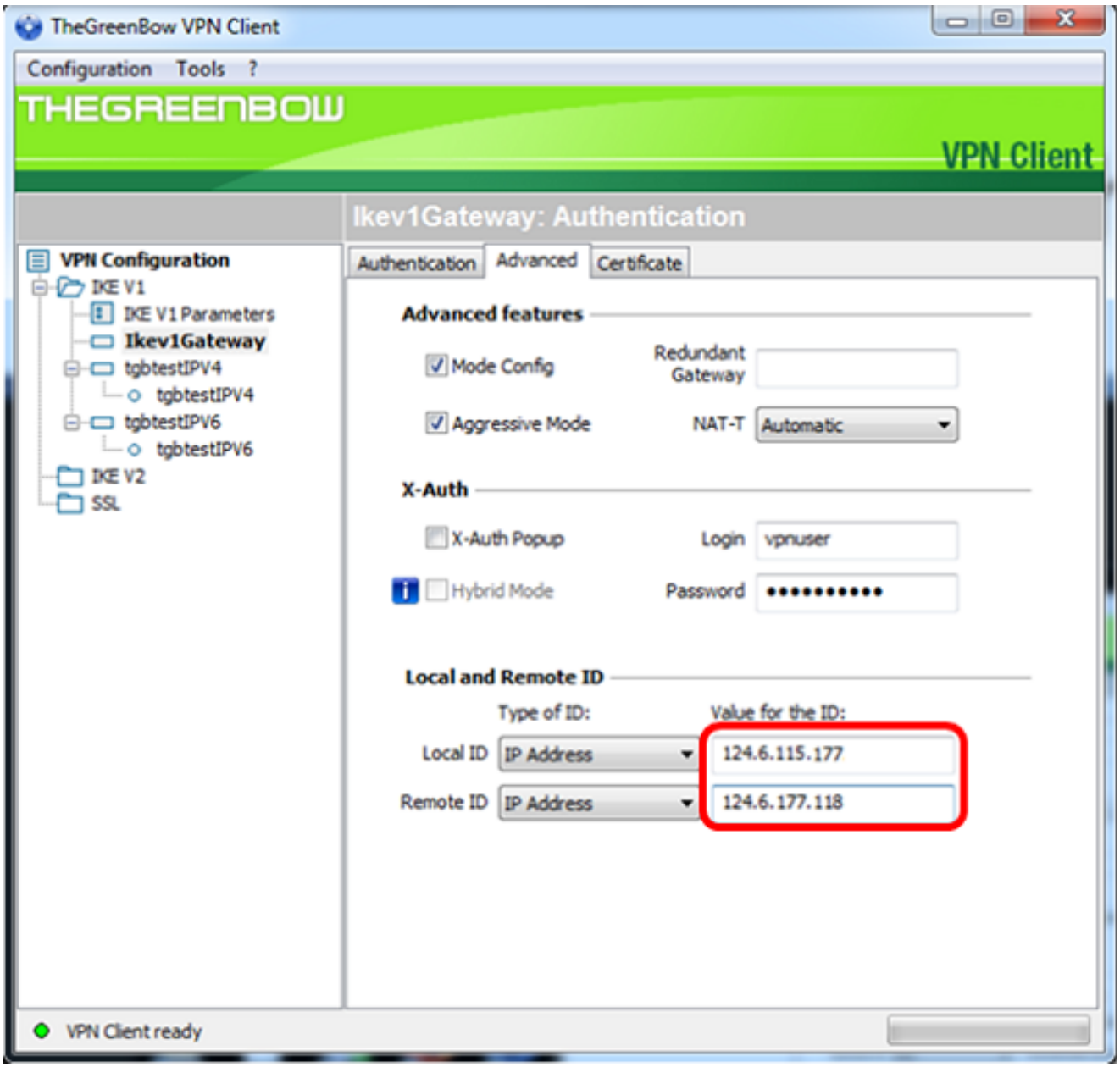


Schritt 14: Legen Sie unter "Lokale und Remote-ID" die Lokale ID und die Remote-ID so fest, dass sie mit den Einstellungen des VPN-Gateways übereinstimmen.

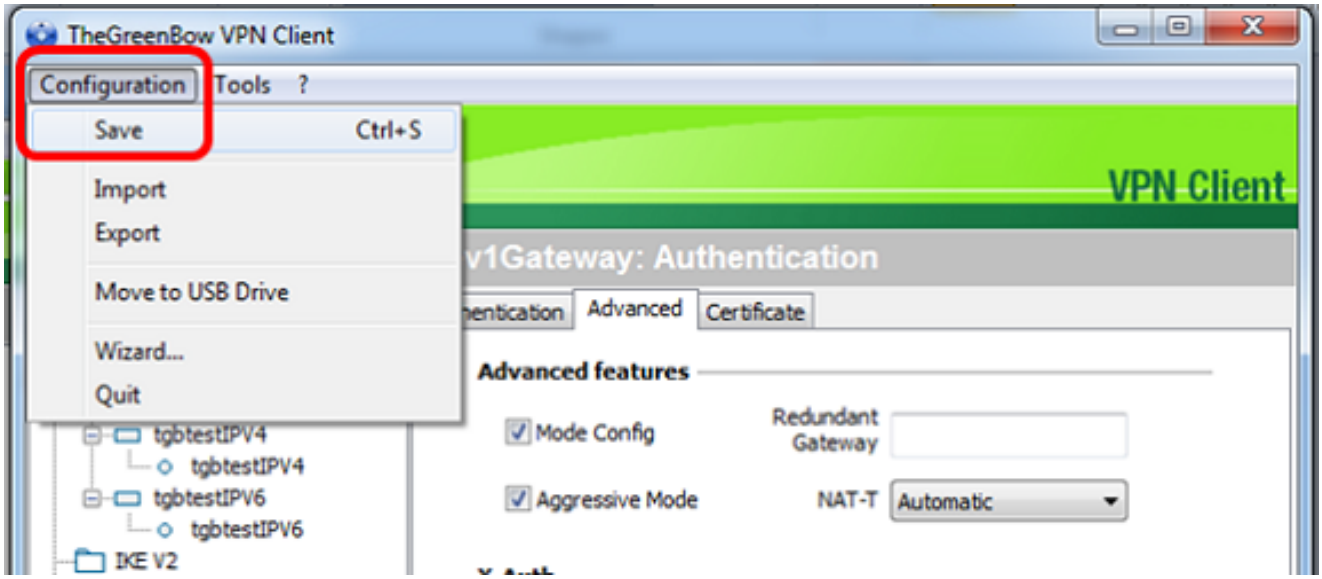


Hinweis: In diesem Beispiel werden sowohl die lokale ID als auch die Remote-ID auf die IP-Adresse eingestellt, um die Einstellungen des RV34x-VPN-Gateways zu erfüllen.

Schritt 15: Geben Sie unter Wert für die ID die lokale ID und Remote-ID in die entsprechenden Felder ein.

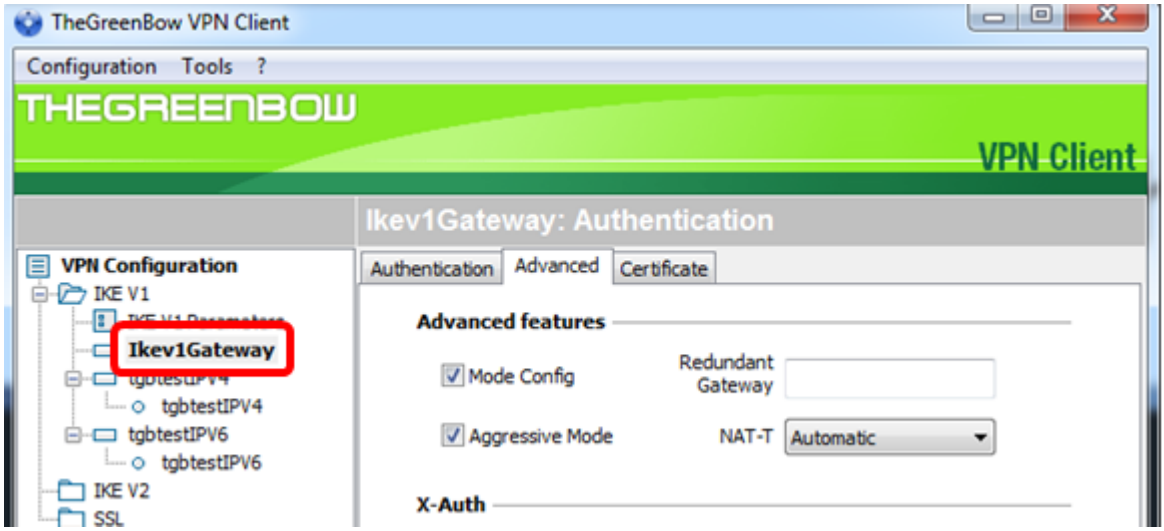


Schritt 16: Klicken Sie auf **Konfiguration > Speichern**, um die Einstellungen zu speichern.

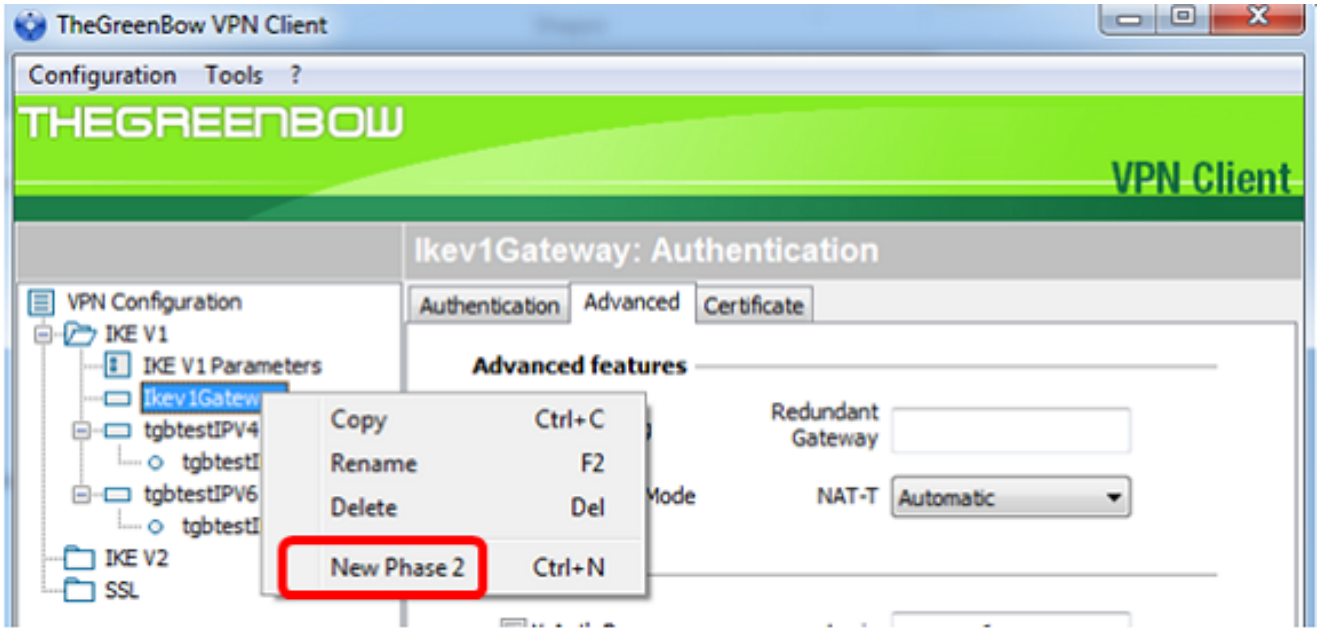


Konfigurieren der Einstellungen für Phase 2

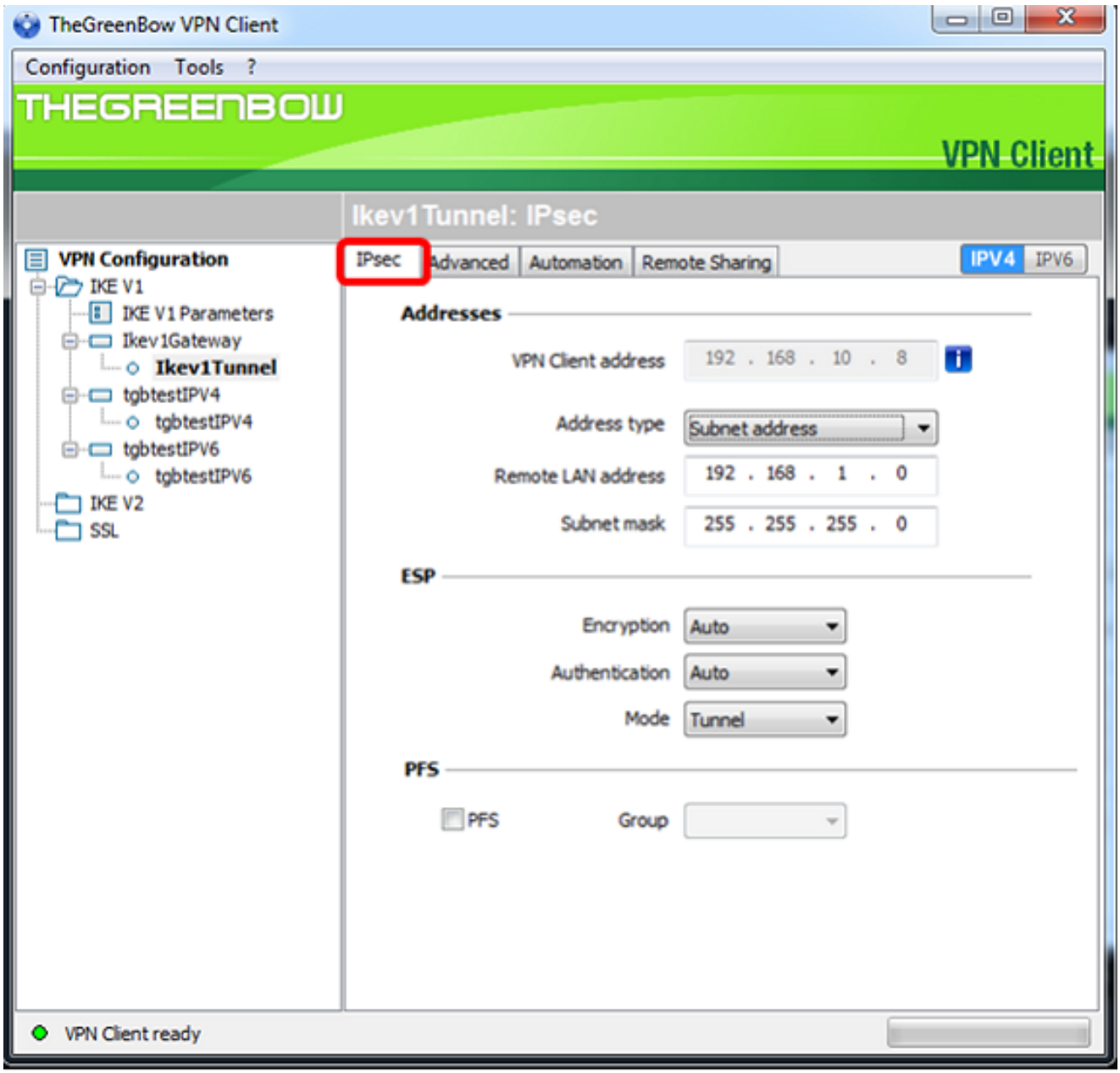
Schritt 1: Klicken Sie mit der rechten Maustaste auf **Ikev1-Gateway**.



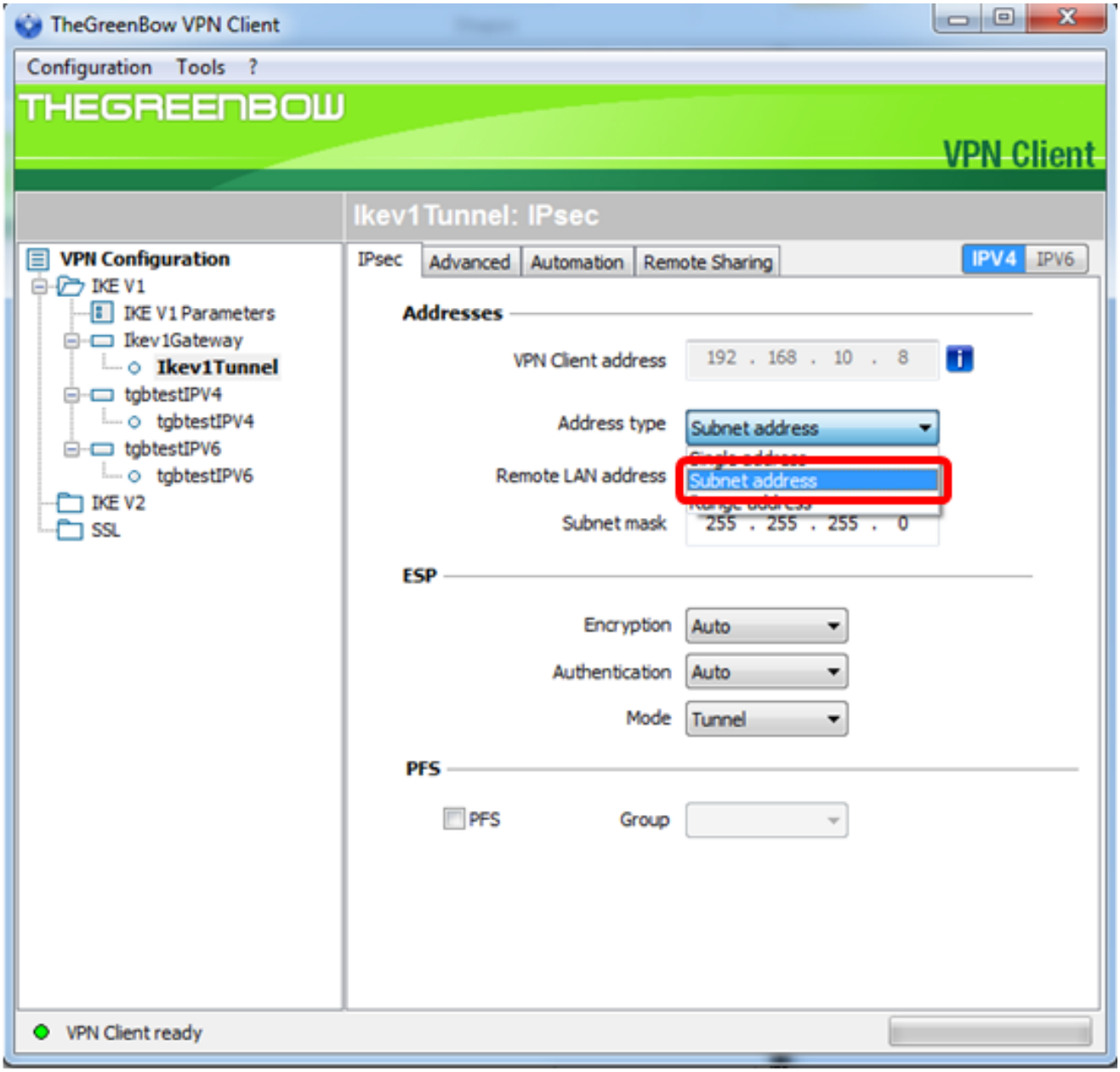
Schritt 2: Wählen Sie **Neue Phase 2 aus**.



Schritt 3: Klicken Sie auf die Registerkarte **IPsec**.

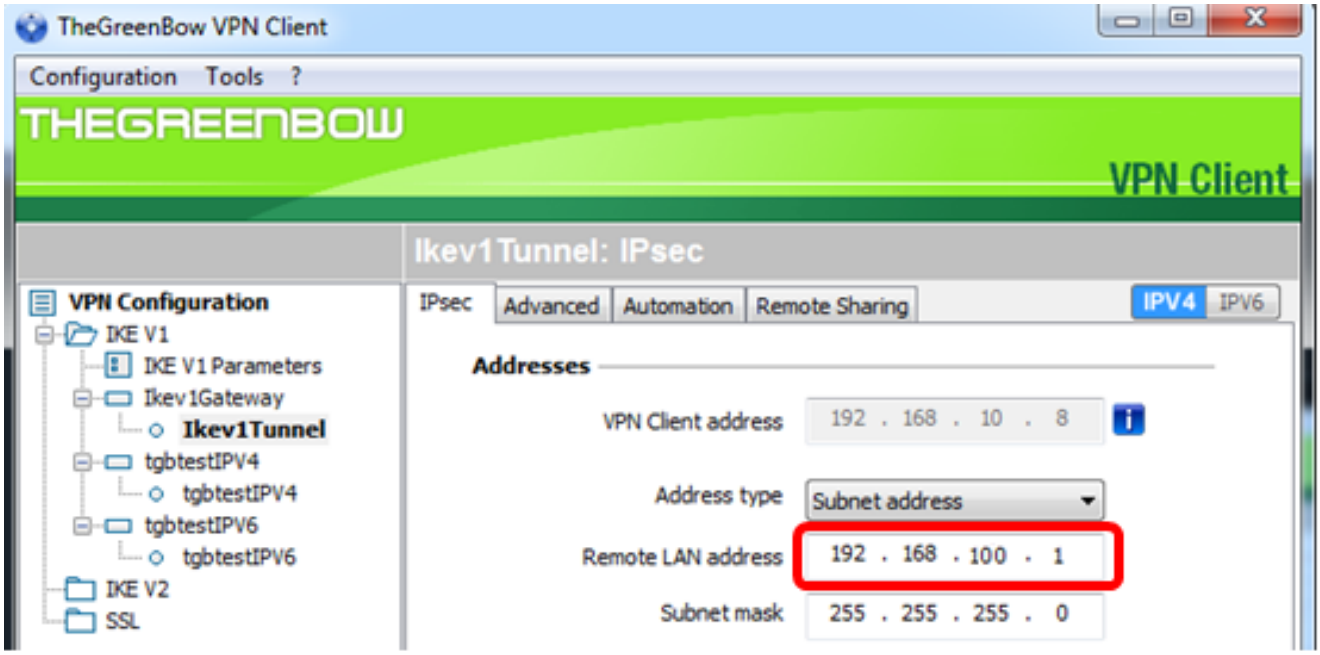


Schritt 4: Wählen Sie aus der Dropdown-Liste Adresstyp den Adresstyp aus, auf den der VPN-Client zugreifen kann.



Hinweis: In diesem Beispiel wird die Subnetzadresse ausgewählt.

Schritt 5: Geben Sie die Netzwerkadresse ein, auf die der VPN-Tunnel im Feld *Remote LAN-Adresse* zugreifen soll.

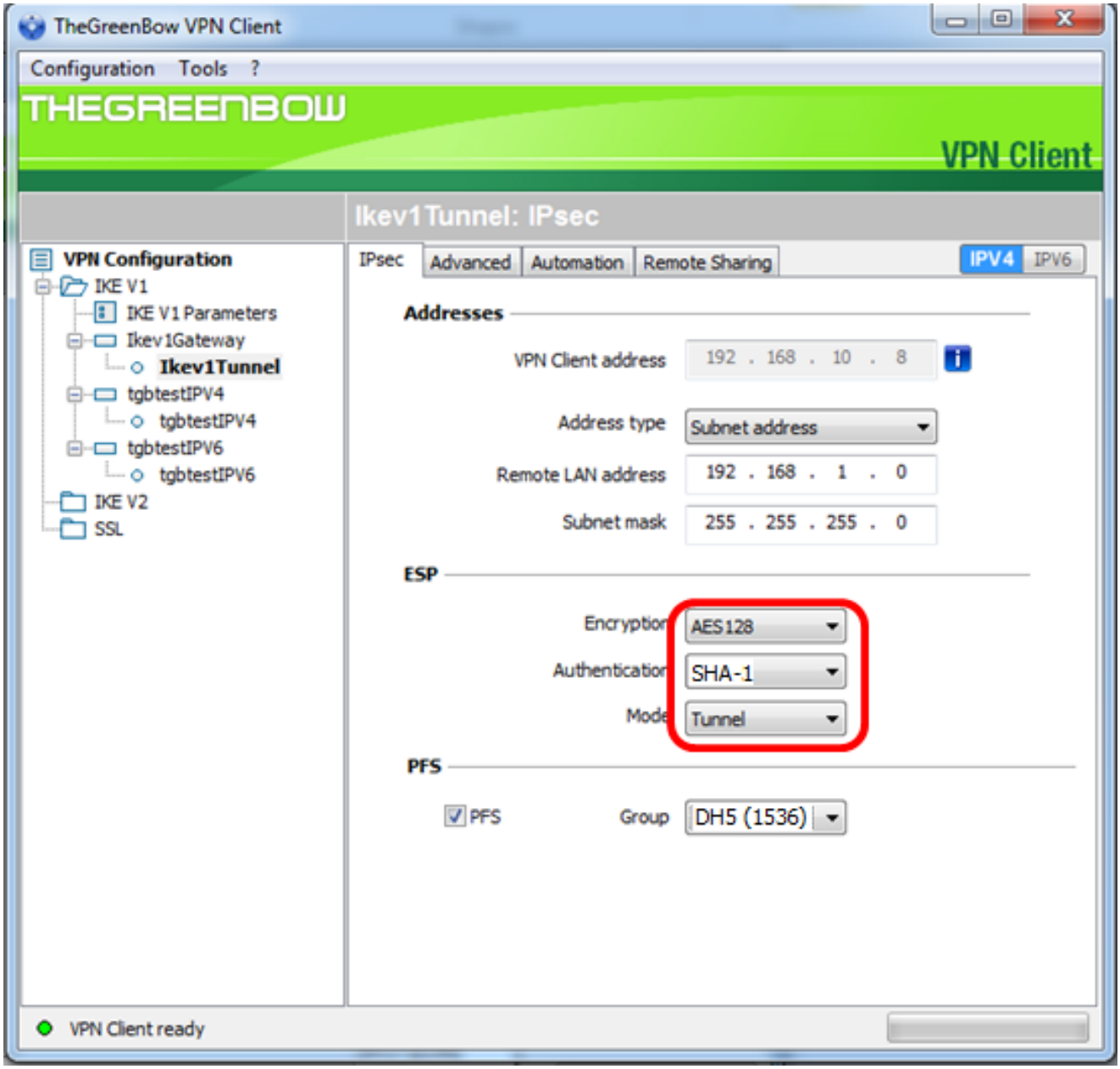


Hinweis: In diesem Beispiel wird 192.168.100.1 eingegeben.

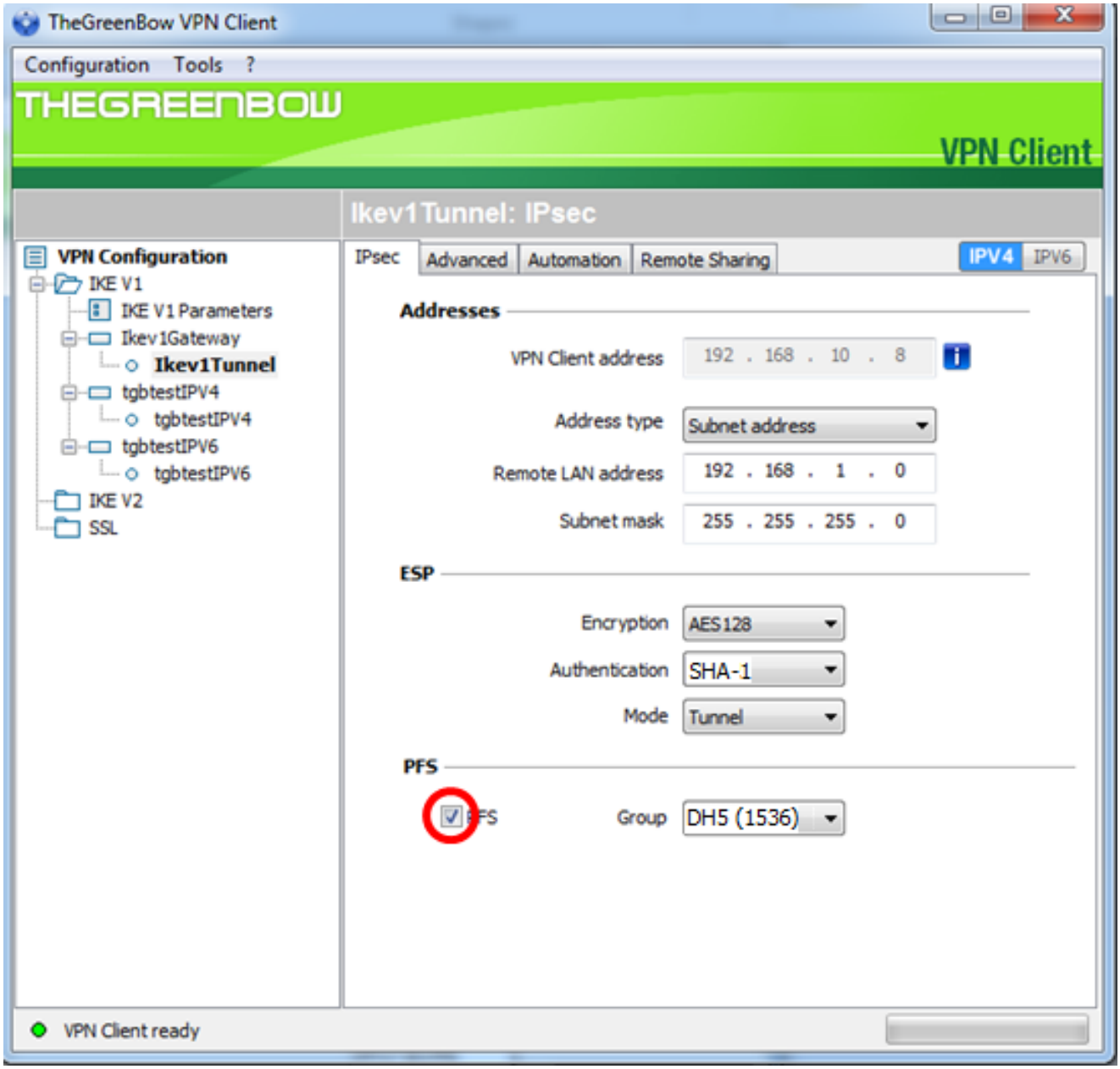
Schritt 6: Geben Sie die Subnetzmaske des Remote-Netzwerks in das Feld *Subnetzmaske ein*.

Hinweis: In diesem Beispiel wird 255.255.255.0 eingegeben.

Schritt 7: Legen Sie unter ESP die Einstellungen für Verschlüsselung, Authentifizierung und Modus so fest, dass sie mit den Einstellungen des VPN-Gateways übereinstimmen.

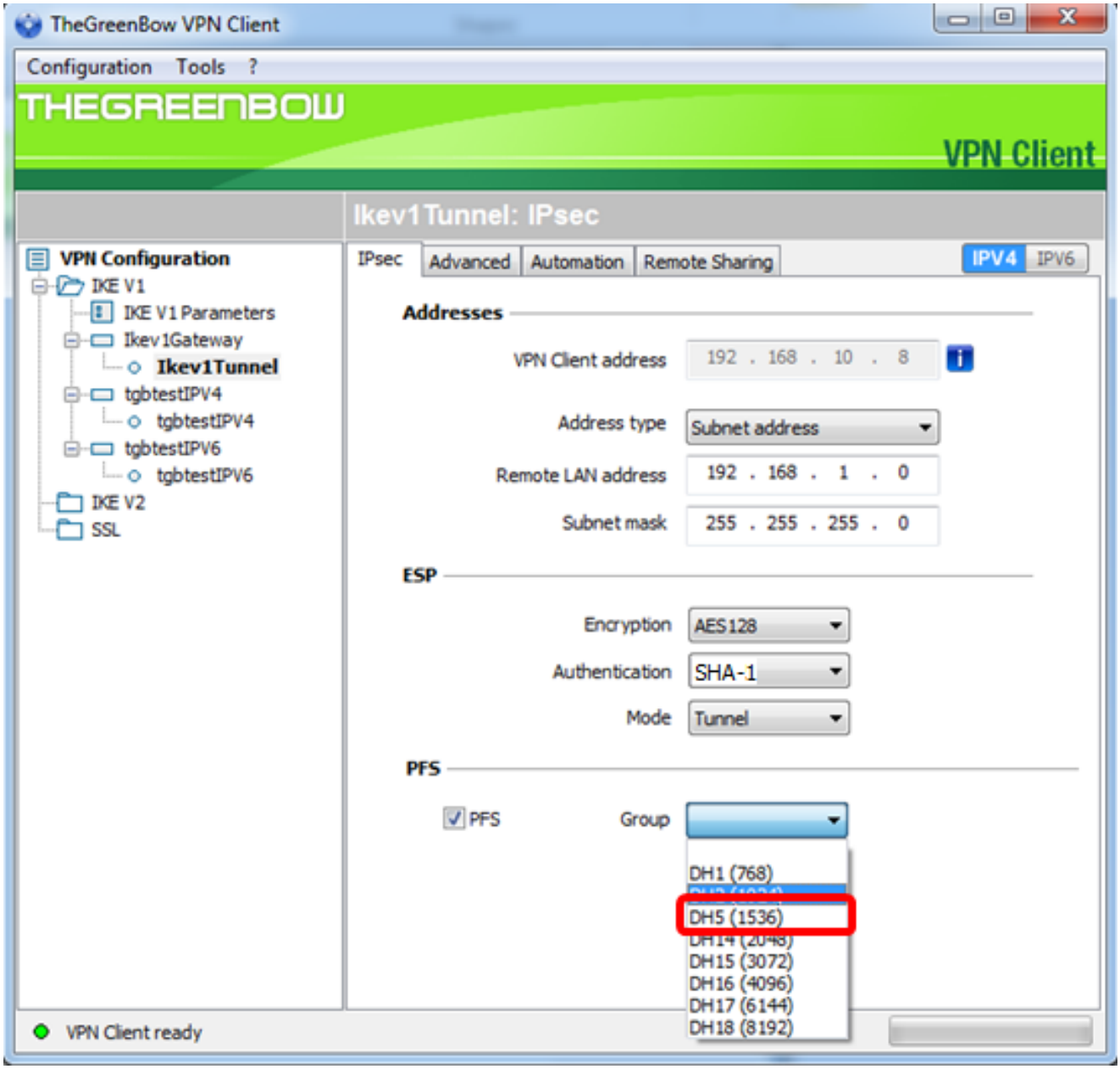


Schritt 8: (Optional) Aktivieren Sie unter PFS das Kontrollkästchen **PFS**, um Perfect Forward Secrecy (PFS) zu aktivieren. PFS generiert zufällige Schlüssel zur Verschlüsselung der Sitzung.

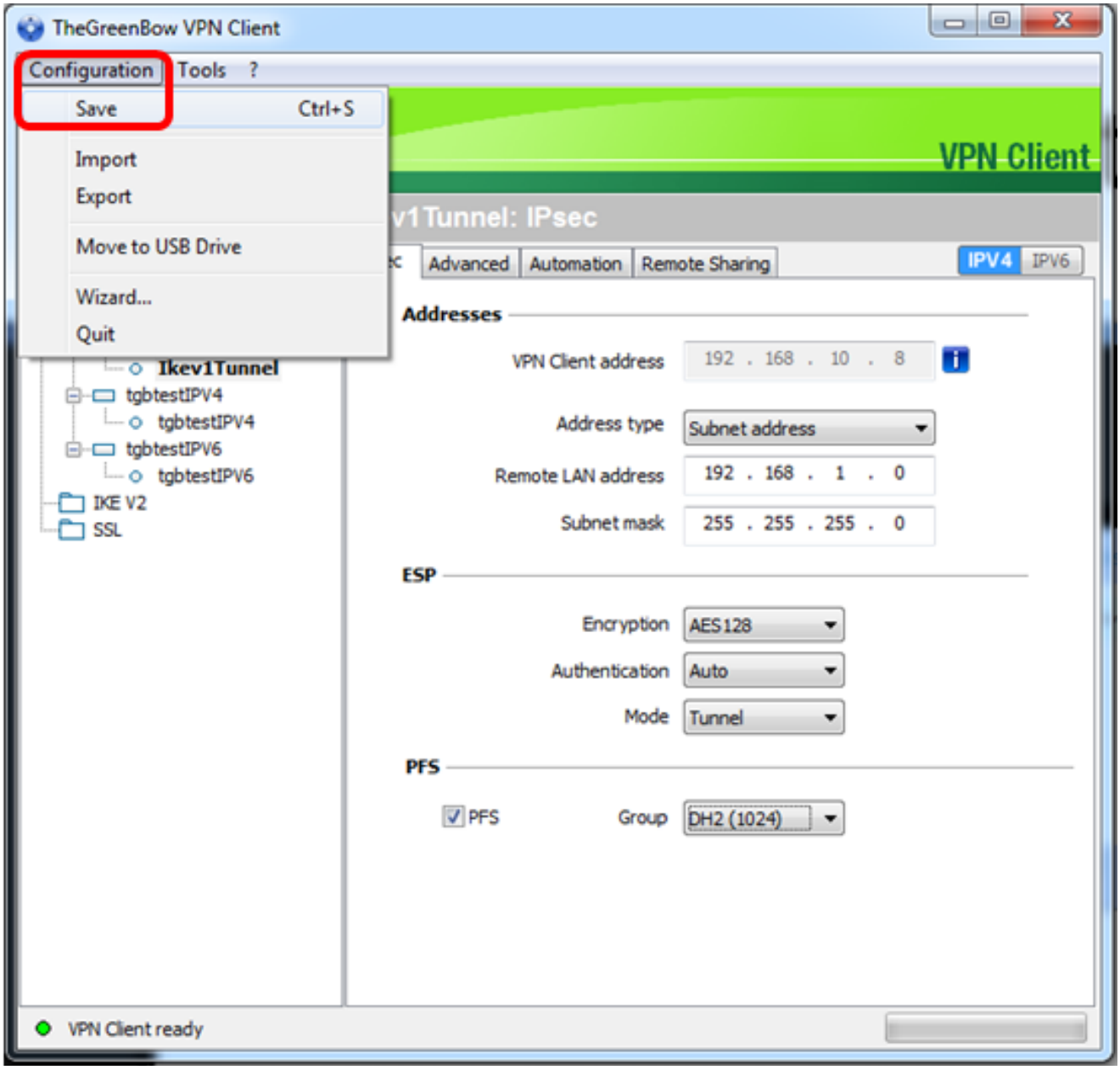


Schritt 9: Wählen Sie aus der Dropdown-Liste "Gruppe" eine PFS-Gruppeneinstellung aus.

Hinweis: In diesem Beispiel wird DH5 (1536) so gewählt, dass es mit der DH-Gruppeneinstellung des Routers übereinstimmt.



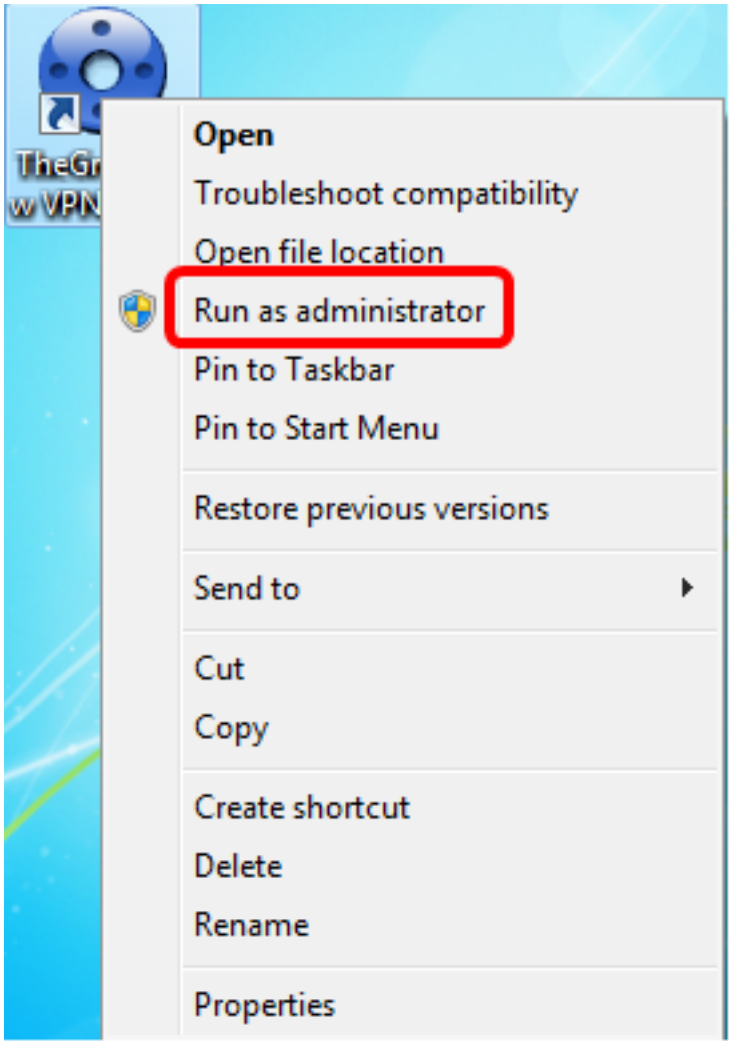
Schritt 10: Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie Speichern aus.



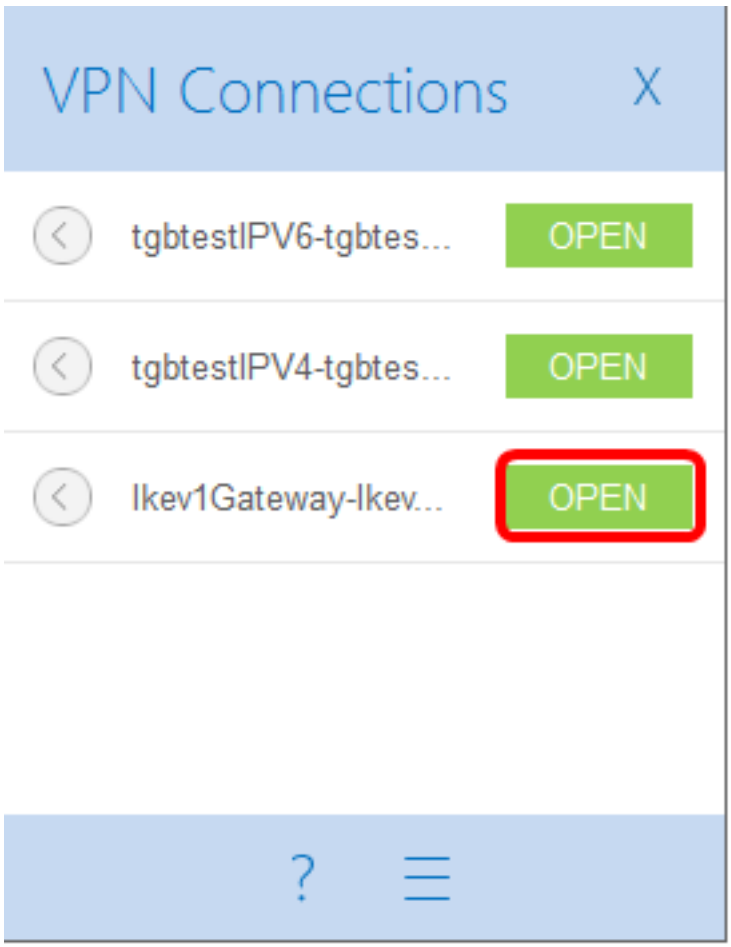
Sie sollten jetzt den GreenBow VPN Client für die Verbindung mit dem Router der Serie RV34x über VPN erfolgreich konfiguriert haben.

VPN-Verbindung starten

Schritt 1: Klicken Sie mit der rechten Maustaste auf TheGreenBow VPN Client, und wählen Sie **Als Administrator ausführen aus**.



Schritt 2: Wählen Sie die zu verwendende VPN-Verbindung aus, und klicken Sie dann auf **ÖFFNEN**. Die VPN-Verbindung sollte automatisch gestartet werden.

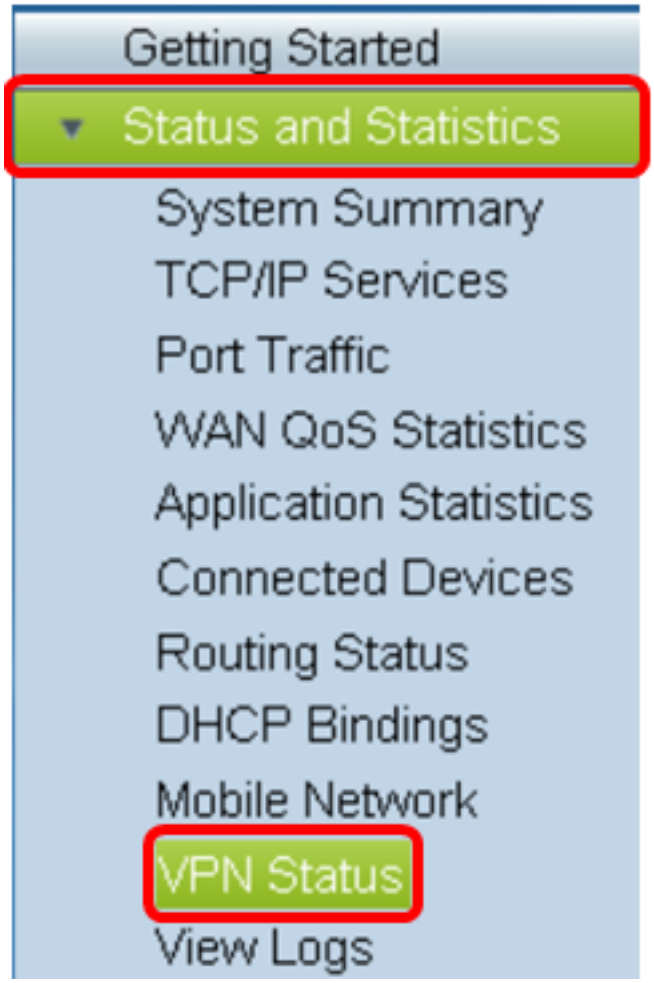


Hinweis: In diesem Beispiel wurde das konfigurierte Ikev1Gateway ausgewählt.

Überprüfen des VPN-Status

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

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



Schritt 3: Überprüfen Sie unter Client-to-Site-Tunnelstatus die Spalte Verbindungen der Verbindungstabelle.

Hinweis: In diesem Beispiel wurde eine VPN-Verbindung hergestellt.

Sie sollten jetzt den VPN-Verbindungsstatus auf dem Router der Serie RV34x erfolgreich überprüft haben. Der GreenBow VPN-Client ist jetzt so konfiguriert, dass er über VPN eine Verbindung zum Router herstellt.