Instellen en gebruiken de client voor GreenBow IPsec VPN om verbinding te maken met RV160- en RV260-routers

Doel

Het doel van dit document is het instellen en gebruiken van de client voor GreenBow IPsec VPN om verbinding te maken met de routers RV160 en RV260.

Inleiding

Een Virtual Private Network (VPN)-verbinding stelt gebruikers in staat om toegang te krijgen tot, gegevens te verzenden en te ontvangen van en naar een privaat netwerk door middel van een openbaar of gedeeld netwerk zoals het internet, maar toch een beveiligde verbinding met een onderliggende netwerkinfrastructuur te waarborgen om het particuliere netwerk en de bijbehorende bronnen te beschermen.

Een VPN-tunnel stelt een privaat netwerk in dat gegevens veilig kan verzenden met behulp van encryptie en verificatie. Bedrijven maken gebruik vaak van een VPN-verbinding omdat het zowel nuttig als noodzakelijk is om hun werknemers toegang te geven tot hun privénetwerk, zelfs als ze zich niet binnen het kantoor bevinden.

VPN staat een externe host of client toe te handelen alsof ze zich op hetzelfde lokale netwerk bevonden. De RV160-router ondersteunt tot 10 VPN-tunnels en RV260 ondersteunt tot 20.0 Een VPN-verbinding kan worden ingesteld tussen de router en een eindpunt nadat de router is geconfigureerd voor internetverbinding. De VPN-client is volledig afhankelijk van de instellingen van de VPN-router om een verbinding op te zetten. De instellingen moeten exact overeenkomen of ze kunnen niet communiceren.

De GreenBow VPN-client is een client-applicatie van derden die het voor een host-apparaat mogelijk maakt om een beveiligde verbinding te configureren voor de client-naar-site IPsec-tunnel met de RV160- en RV260-Series routers.

Voordelen van het gebruik van een VPN-verbinding

Gebruik van een VPN-verbinding om vertrouwelijke netwerkgegevens en -bronnen te beschermen.

Het zorgt voor gemak en toegankelijkheid voor externe werknemers of bedrijfsmedewerkers, aangezien zij gemakkelijk toegang zullen hebben tot het hoofdbureau zonder dat zij fysiek aanwezig moeten zijn en toch de beveiliging van het particuliere netwerk en zijn middelen in stand moeten houden.

Communicatie via een VPN-verbinding biedt een hoger beveiligingsniveau dan andere methoden voor communicatie op afstand. Een geavanceerd encryptie algoritme maakt dit mogelijk, om het privé netwerk tegen onbevoegde toegang te beschermen.

De werkelijke geografische locaties van de gebruikers worden beschermd en niet blootgesteld aan het publiek of gedeelde netwerken zoals het internet.

Een VPN kan nieuwe gebruikers of een groep gebruikers toevoegen zonder dat u extra onderdelen of een gecompliceerde configuratie nodig hebt.

Risico's van het gebruik van een VPN-verbinding

Er kunnen veiligheidsrisico's zijn door verkeerde configuratie. Aangezien het ontwerp en de implementatie van een VPN gecompliceerd kunnen zijn, is het nodig de taak toe te vertrouwen om de verbinding te configureren naar een zeer deskundig en ervaren professional, om er zeker van te zijn dat de beveiliging van het privénetwerk niet in gevaar zou worden gebracht.

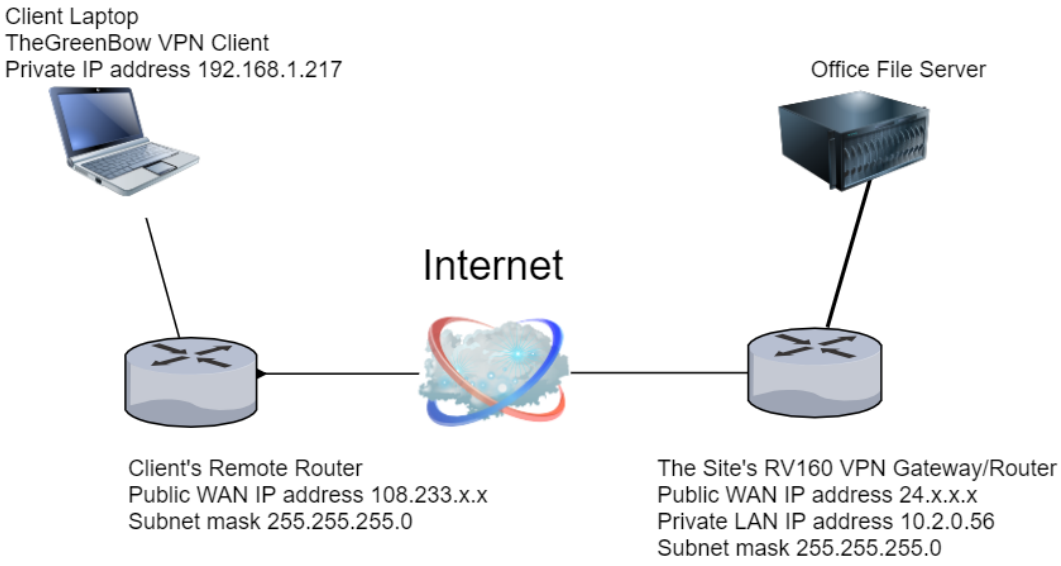
Het kan minder betrouwbaar zijn. Aangezien een VPN-verbinding een internetverbinding vereist, is het belangrijk dat u een provider hebt met een beproefde reputatie en een beproefde reputatie die u een uitstekende internetservice kunt bieden en die minimaal is aan een downtime.

Als er een situatie is waarin er een nieuwe infrastructuur of een nieuwe reeks configuraties moet worden toegevoegd, kunnen technische problemen ontstaan door onverenigbaarheid, vooral als er andere producten of verkopers bij betrokken zijn dan de producten die u al gebruikt.

U kunt lange verbindingssnelheden verwachten. Als u een VPN-client gebruikt die gratis VPN-service biedt, kan er verwacht worden dat uw verbinding ook langzaam verloopt omdat deze providers geen prioriteit geven aan verbindingssnelheden. In dit artikel zullen wij een betaalde derde gebruiken die deze kwestie moet oplossen.

Basistopologie van het client-naar-site netwerk

Dit is de basislay-out van het netwerk voor installatie. De openbare WAN IP-adressen zijn gedeeltelijk vervormd of tonen een **x** in plaats van de eigenlijke getallen om dit netwerk tegen aanvallen te beschermen.



Dit artikel zal door de stappen lopen die nodig zijn om de RV160 of RV260 router op de site te configureren voor het volgende:

- Een gebruikersgroep — **VPN's**
- Gebruikersrekeningen (één of meer gebruikers) die als cliënt toegang zullen krijgen
- Een IPsec-profiel — **TheGreenBow**
- Een client-naar-site profiel — **client**

- U wordt ook getoond hoe de VPN-status op de site wordt weergegeven wanneer de client is aangesloten

Opmerking: U kunt elke naam gebruiken voor de gebruikersgroep, IPsec-profiel en client-naar-site profiel. De namen in de lijst zijn slechts voorbeelden.

Dit artikel beschrijft ook de stappen die elke client zou ondernemen om The GreenBow VPN op hun computer te configureren:

- De GroeneBoE VPN-clientsoftware downloaden en instellen
- Instellingen fase 1 en fase 2 voor de client configureren
- Start en controleer VPN-verbinding als client

Het is van essentieel belang dat elke instelling op de router op site overeenkomt met de clientinstellingen. Als uw configuratie niet leidt tot een succesvolle VPN-verbinding, controleert u alle instellingen om te zorgen dat ze overeenkomen. Het voorbeeld in dit artikel is slechts één manier om de verbinding in te stellen.

Inhoud

Toepasselijke apparaten

- RV160
- RV260

Softwareversie

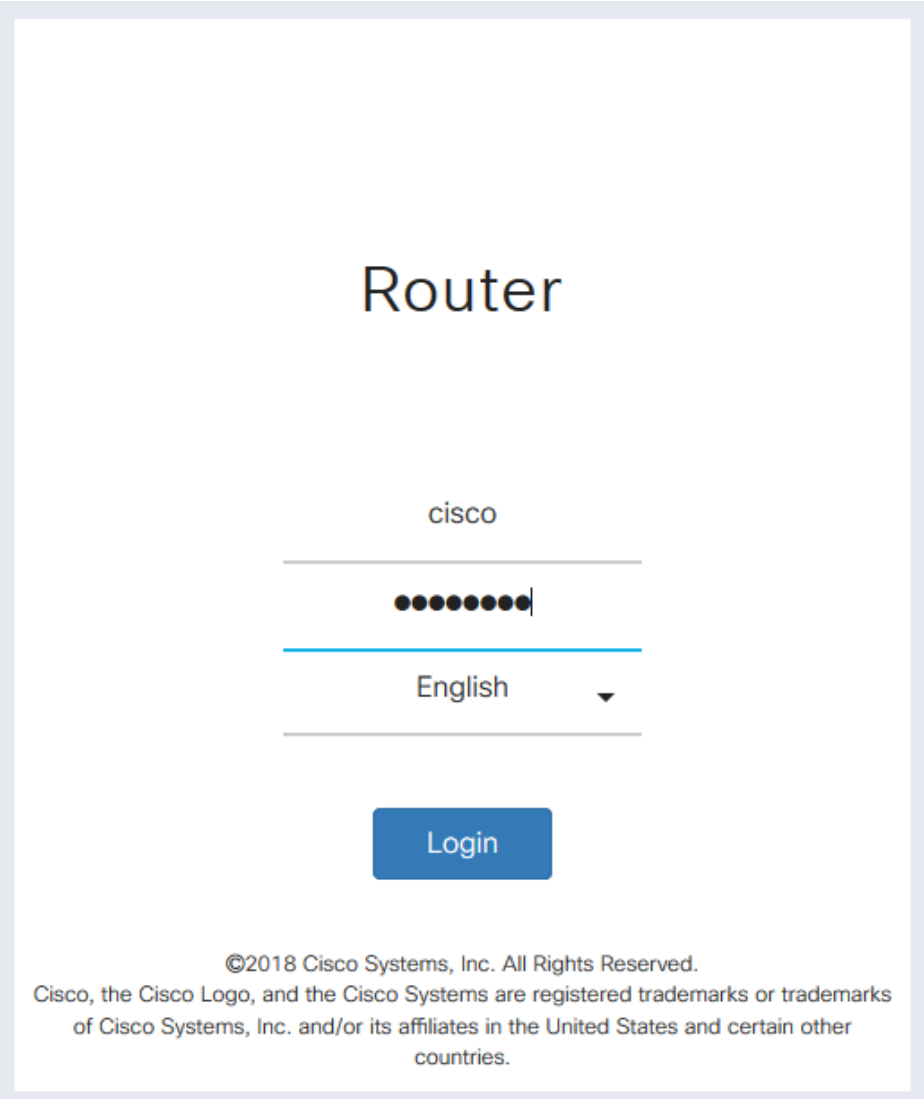
- 1.0.00.15

VPN-client configureren op de site op de RV160- of RV260-router

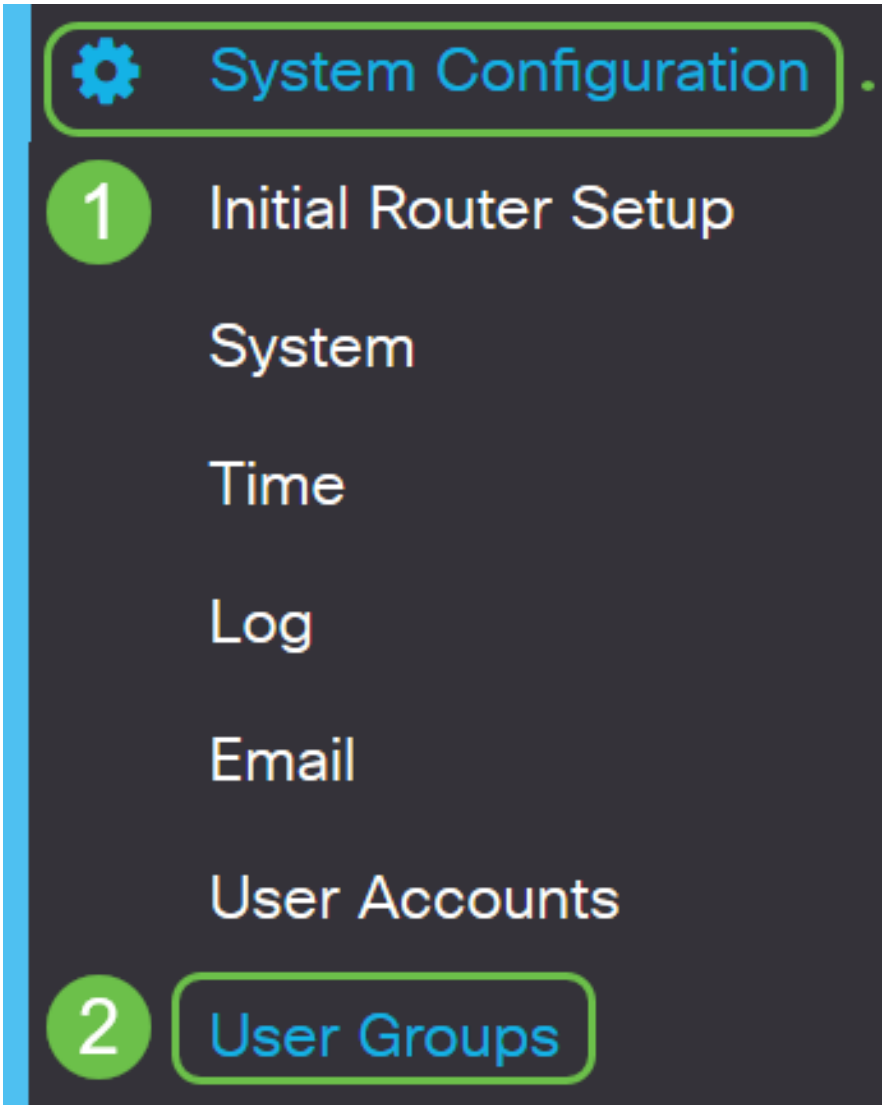
Een gebruikersgroep maken

Belangrijke opmerking: Laat de standaard-admin-account in de admin-groep achter en maak een nieuwe gebruikersaccount en gebruikersgroep voor TheGreenBow. Als u uw Admin-account naar een andere groep verplaatst, voorkomt u dat u zich in de router registreert.

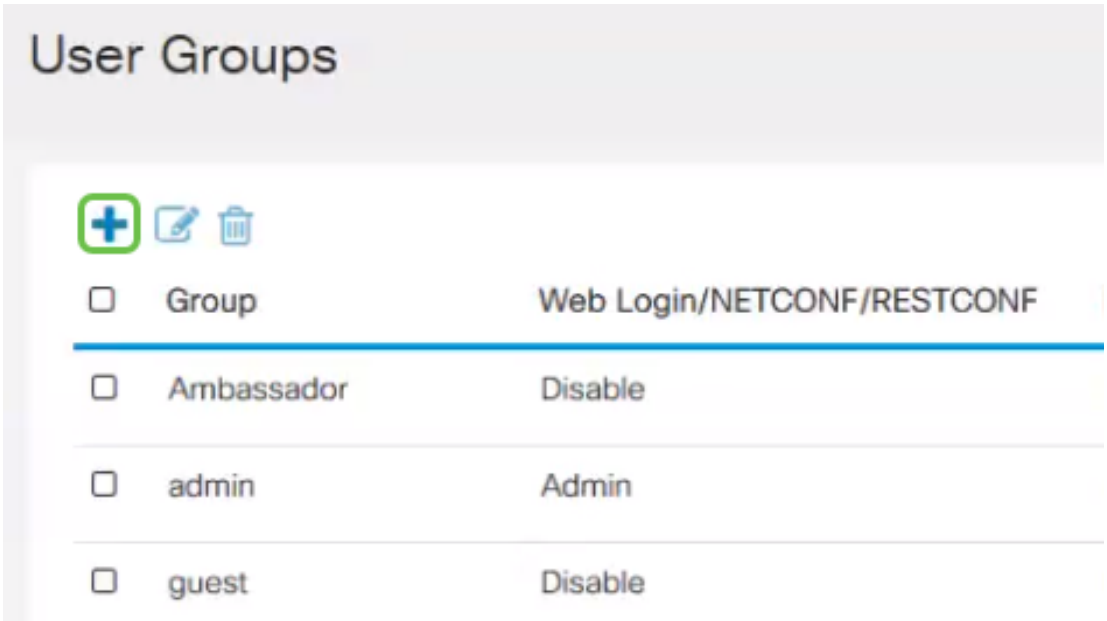
Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van de router.



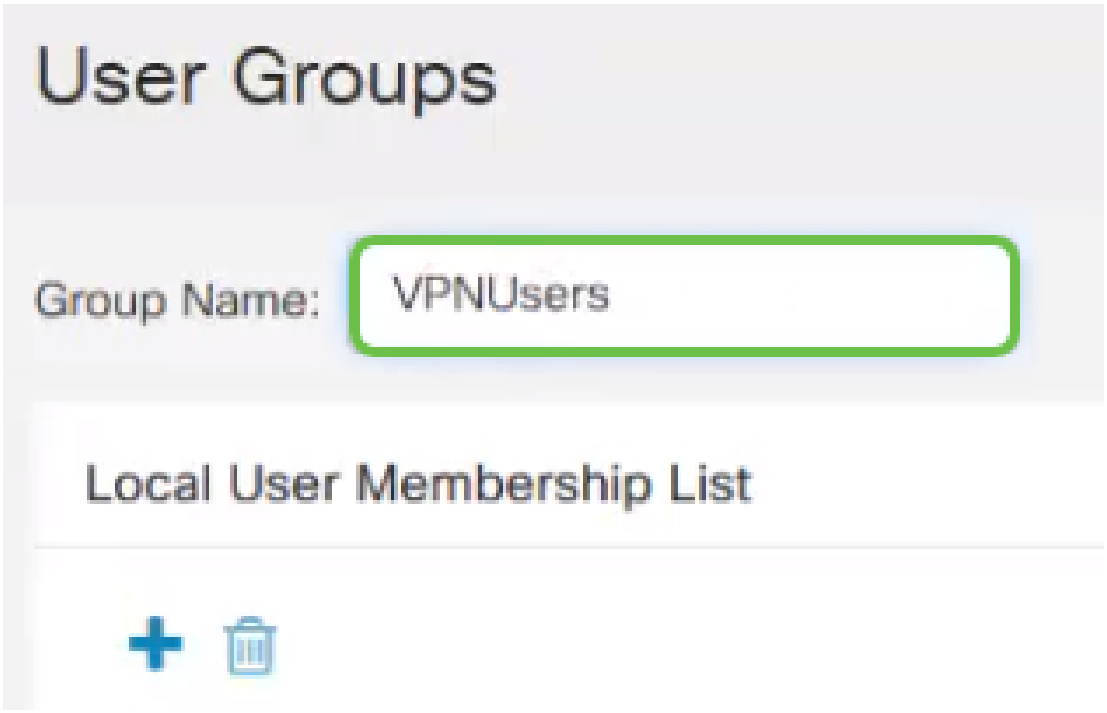
Stap 2. Selecteer **systeemconfiguratie** > **Gebruikersgroepen**.



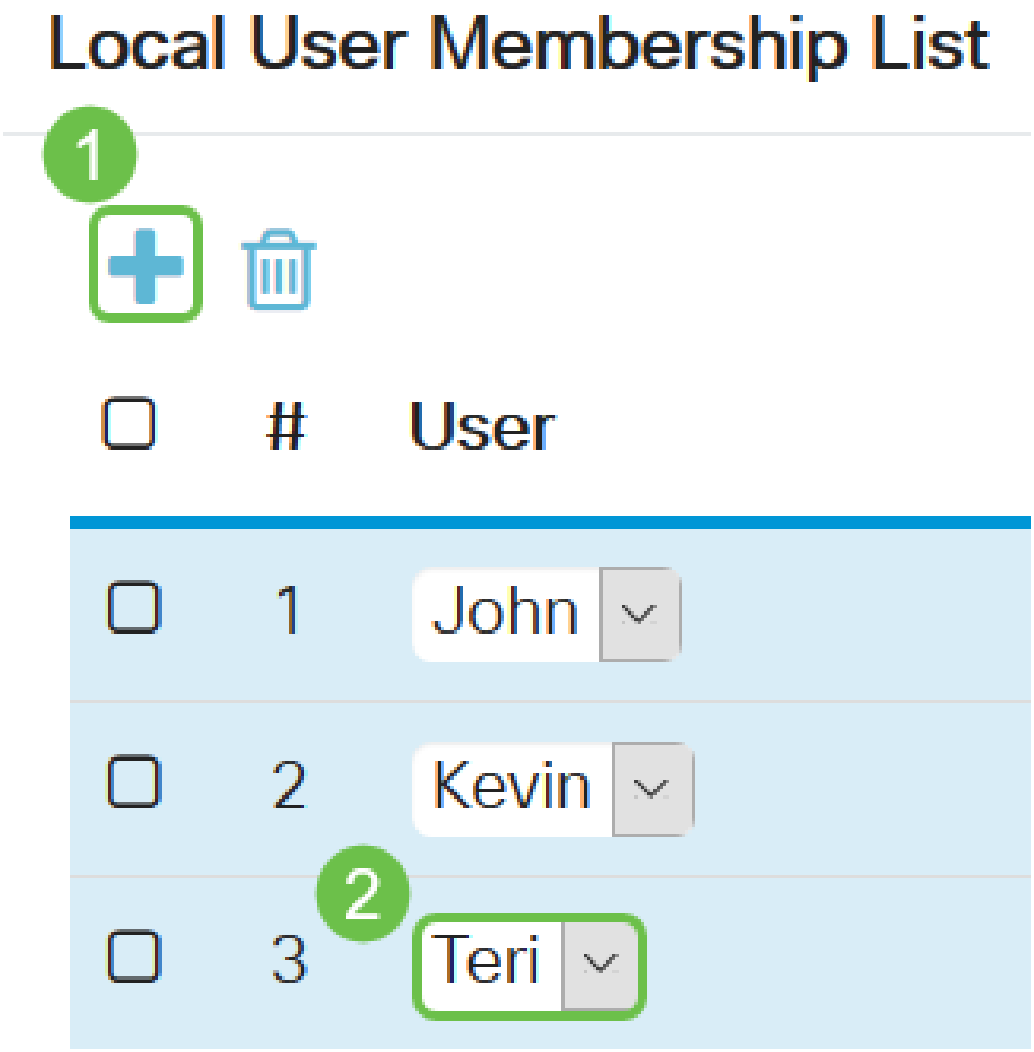
Stap 3. Klik op het pictogram **plus** om een gebruikersgroep toe te voegen.



Stap 4. Voer in het gedeelte Overzicht de naam van de groep in het veld *groepsnaam in*.

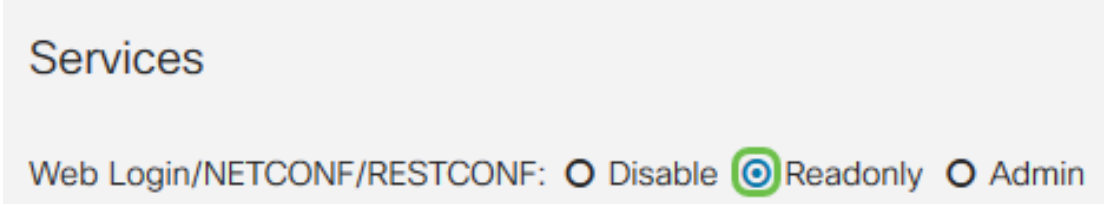


Stap 5. Onder *Local User Membership List* , klikt u op het **plus-**pictogram en vervolgens selecteert u de gebruiker in de vervolgkeuzelijst. Als u meer wilt toevoegen, drukt u nogmaals op het pictogram **plus** en selecteert u een ander toegevoegd lid. De leden kunnen slechts deel uitmaken van één groep. Als niet alle ingevoerde gebruikers al zijn ingevoerd, kunt u meer toevoegen in het gedeelte Een gebruikersaccount maken.

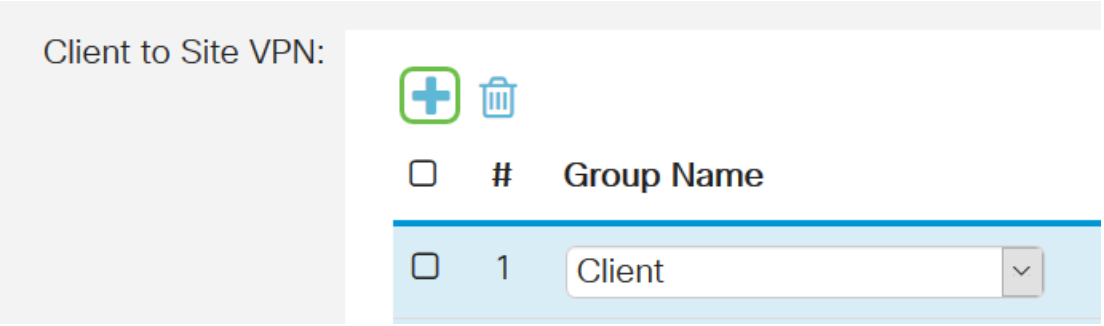


Stap 6. Kies onder *Services* een toestemming om aan de gebruikers in de groep te verlenen. De opties zijn:

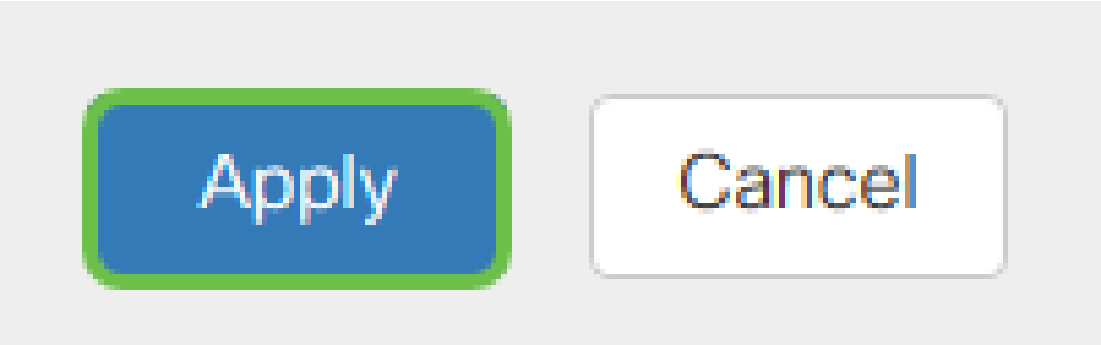
- Uitgeschakeld — Deze optie betekent dat leden van de groep geen toegang hebben tot het web-gebaseerde hulpprogramma via een browser.
- Alleen lezen — Deze optie betekent dat de leden van de groep de status van het systeem pas kunnen lezen nadat ze zijn aangemeld. Ze kunnen geen van de instellingen bewerken.
- Admin — Deze optie geeft de leden van de groep lees- en schrijfrechten en kan de systeemstatus configureren.



Stap 7. Klik op het pictogram **plus** om een bestaand client-naar-site VPN toe te voegen. Als u dit niet hebt ingesteld, kunt u informatie in dit artikel vinden onder de sectie Een client-naar-site profiel maken.

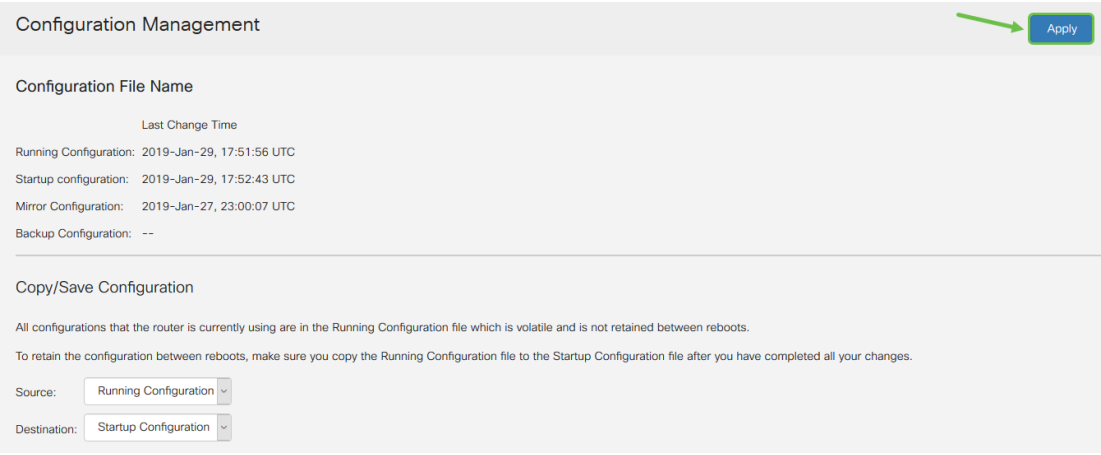


Stap 8. Klik op **Toepassen**.

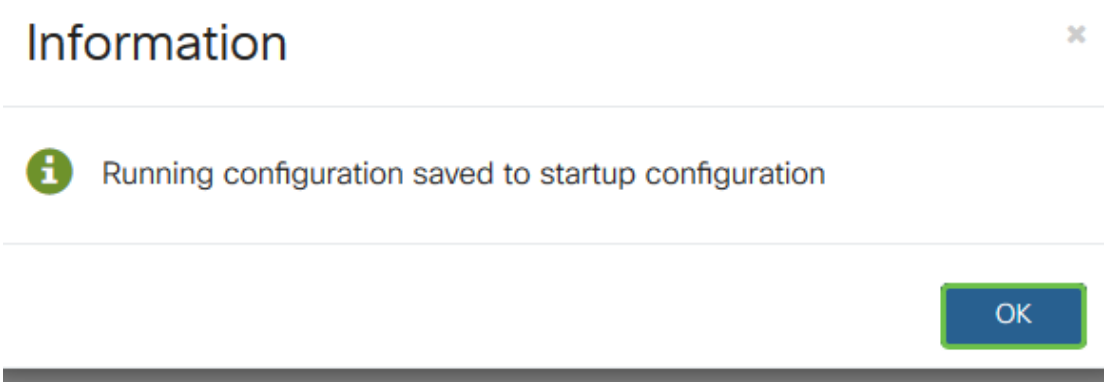


Stap 5. Klik op **Opslaan**.

Stap 10. Klik nogmaals op **Toepassen** om de actieve configuratie op te slaan in het opstartbeeld.



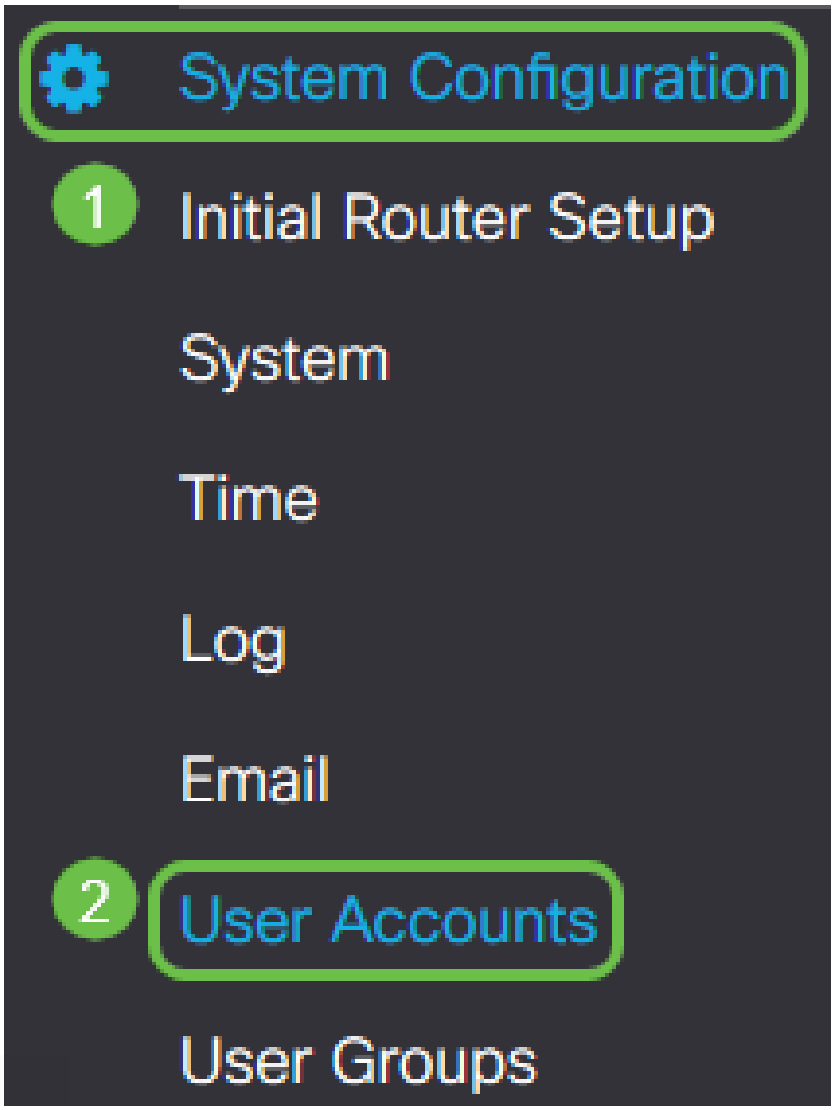
Stap 1. Wanneer u de bevestiging ontvangt, klikt u op **OK**.



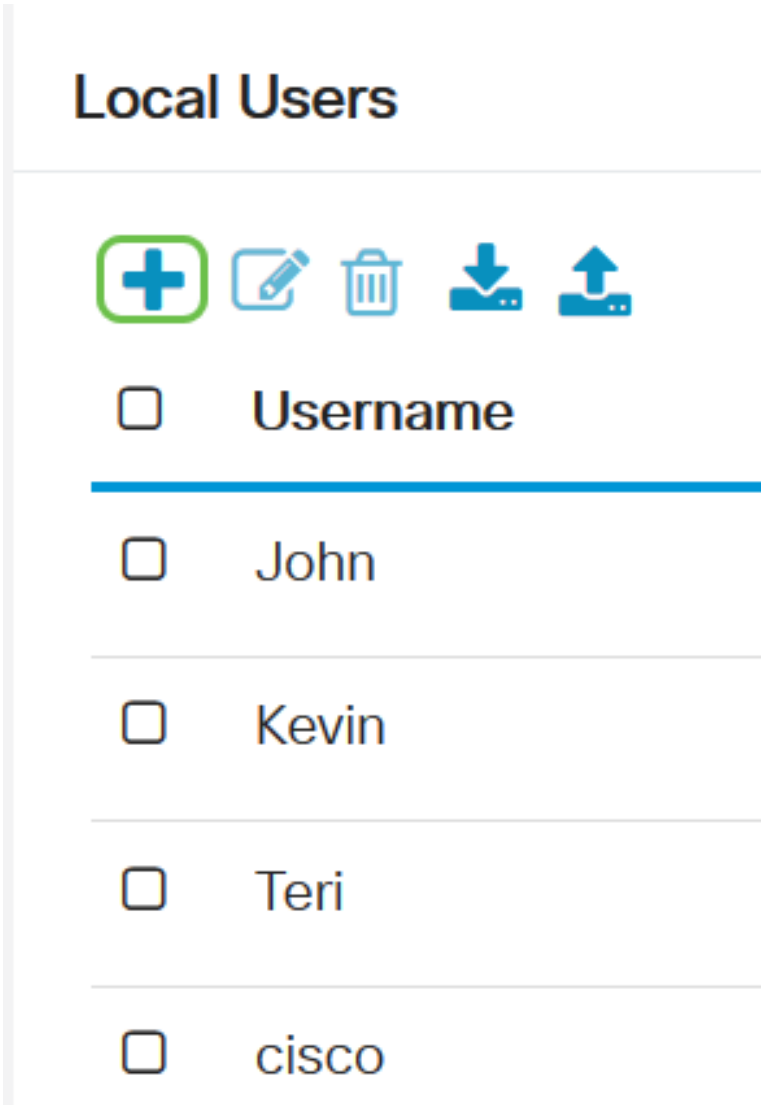
U dient nu met succes een gebruikersgroep op de RV160- of RV260-Series router te hebben gemaakt.

Een gebruikersaccount maken

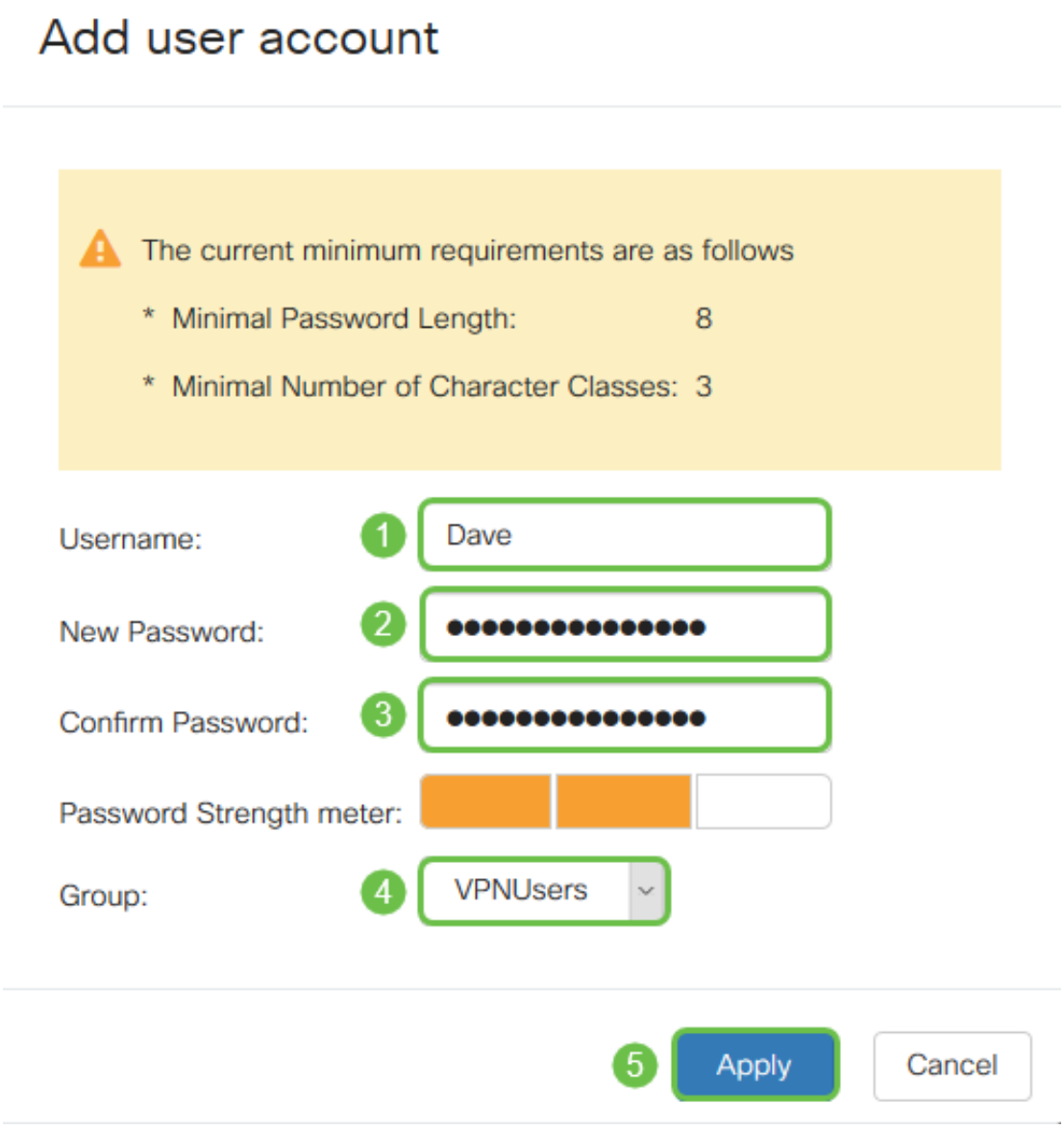
Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van de router en kies **Systeemconfiguratie** > **Gebruikersrekeningen**.



Stap 2. Klik in het gebied *Local Gebruikers* op het **pictogram Add**.



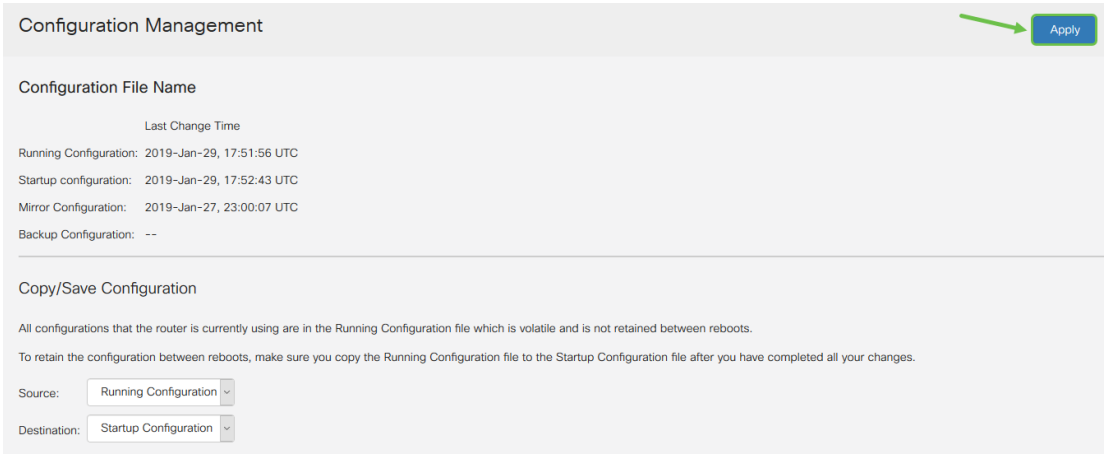
Stap 3. Voer een naam in voor de gebruiker in het veld *Gebruikersnaam*, het wachtwoord en de groep waaraan u de gebruiker wilt toevoegen in het vervolgkeuzemenu. Klik op **Toepassen**.



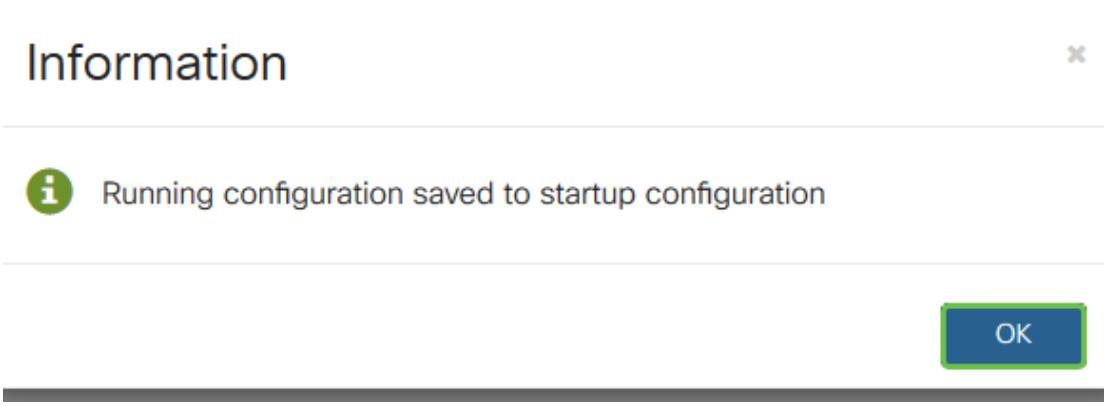
Opmerking: Wanneer de client TheGreenBow Client op hun computer instelt, zouden ze inloggen met dezelfde gebruikersnaam en hetzelfde wachtwoord.

Stap 4. Klik op **Opslaan**.

Stap 5. Klik nogmaals op **Toepassen** om de draaiende configuratie op te slaan.



Stap 6. Wanneer u de bevestiging ontvangt, klikt u op **OK**.

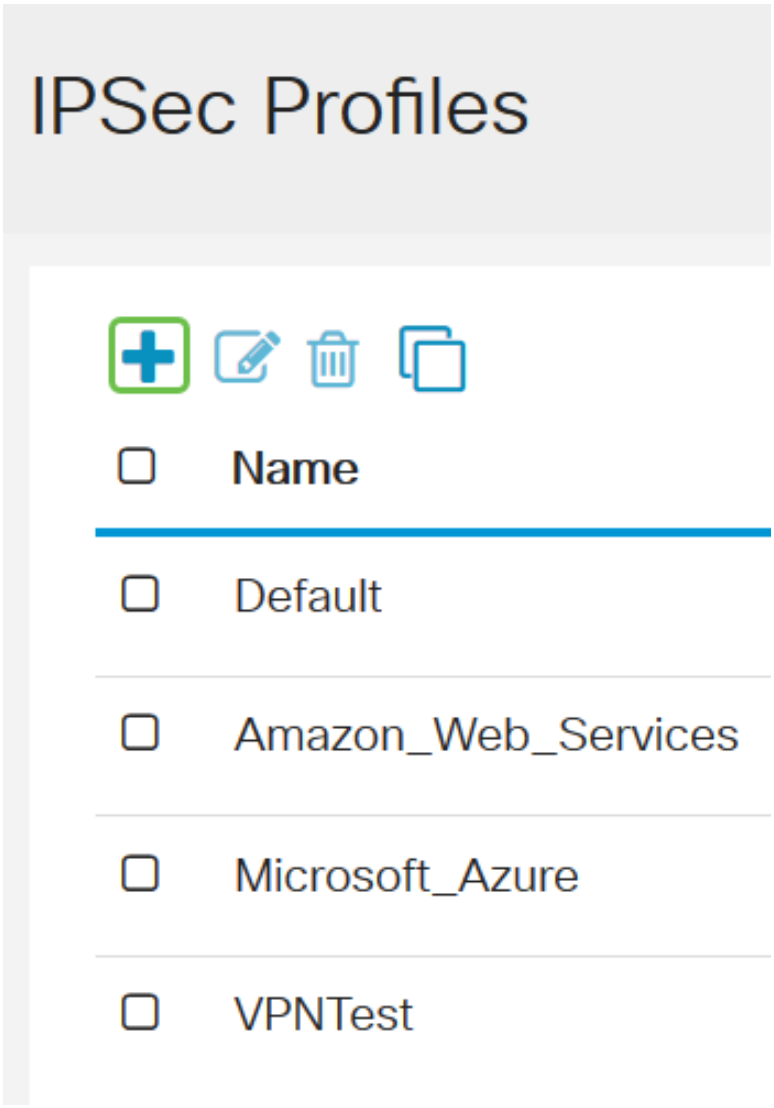


U moet nu een gebruikersaccount op uw RV160- of RV260-router hebben gemaakt.

IPsec-profiel configureren

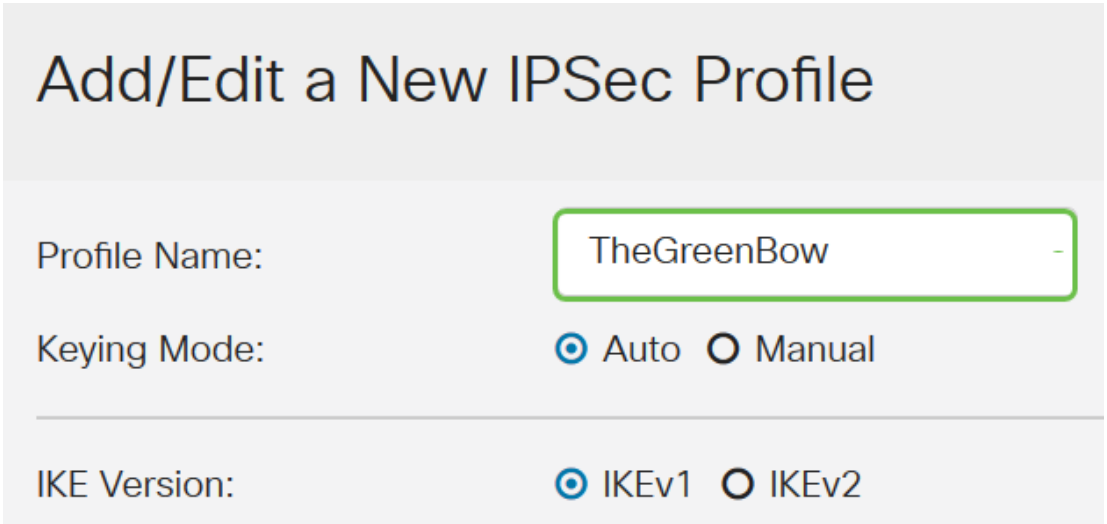
Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van de RV160- of RV260-router en kies **VPN > IPSec VPN > IPSec-profielen**.

Stap 2. De tabel met IPSec-profielen toont de bestaande profielen. Klik op het pictogram **plus** om een nieuw profiel te maken.



Opmerking: Amazon_Webex_Services, Default, en Microsoft_karwei zijn standaardprofielen.

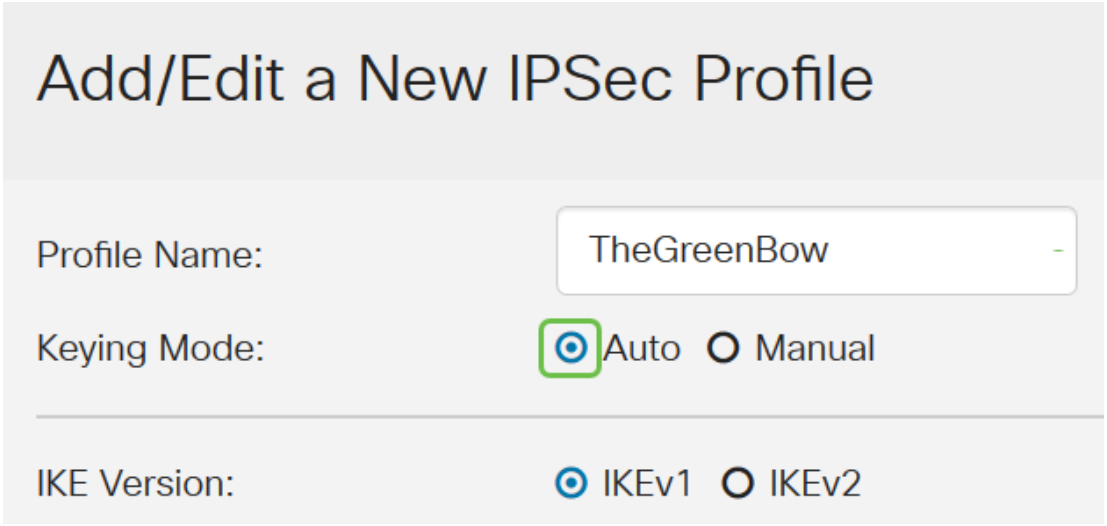
Stap 3. Maak een naam voor het profiel in het veld *Profile Name*. De profielnaam mag alleen alfanumerieke tekens en een underscore (_) voor speciale tekens bevatten.



Stap 4. Klik op een radioknop om de belangrijkste uitwisselingsmethode te bepalen het profiel zal gebruiken om authentiek te verklaren. De opties zijn:

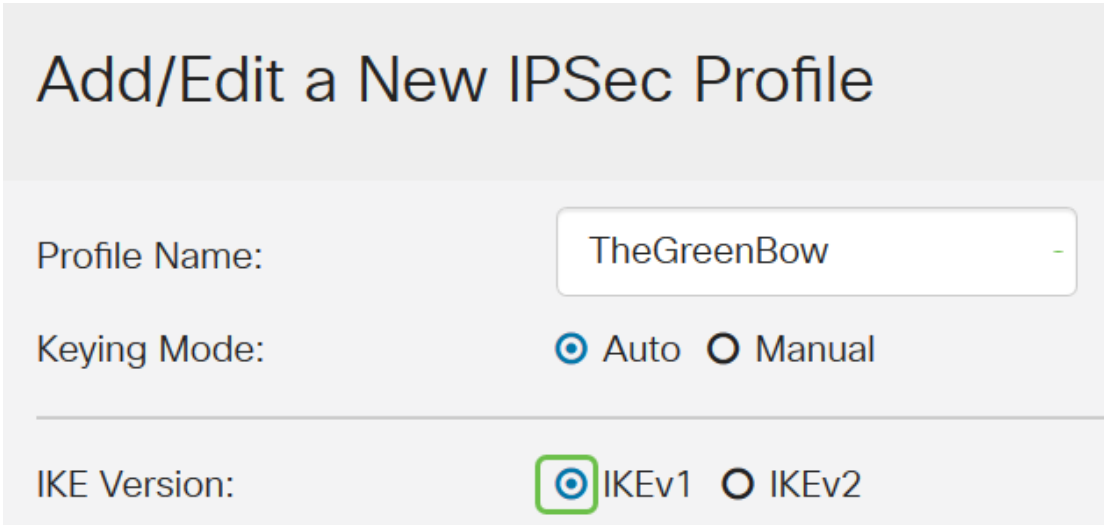
- Auto — Beleidsparameters worden automatisch ingesteld. Deze optie gebruikt een beleid voor de uitwisseling van gegevens (Internet Key Exchange, IKE) en de uitwisseling van encryptiesleutels. Als dit geselecteerd is, worden de configuratie

instellingen onder het gebied Auto Policy parameters ingeschakeld.
- Handmatig - Met deze optie kunt u de toetsen voor gegevensencryptie en integriteit voor de VPN-tunnel handmatig configureren. Als dit wordt geselecteerd, worden de configuratie instellingen onder het gebied Handmatige beleidsparameters ingeschakeld. Dit wordt niet veel gebruikt.



Opmerking: In dit voorbeeld werd **Auto** gekozen.

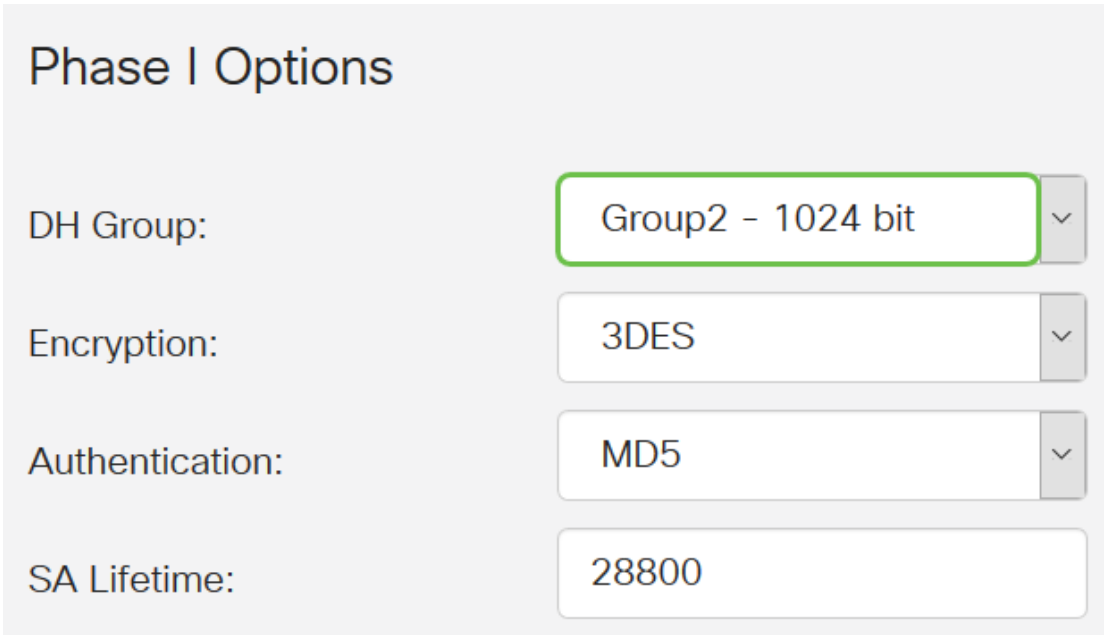
Stap 5. Selecteer de IKE-versie. Zorg ervoor dat wanneer u The GreenBow op de clientzijde instelt, dezelfde versie is geselecteerd.



Instellingen fase 1 en fase 2 configureren

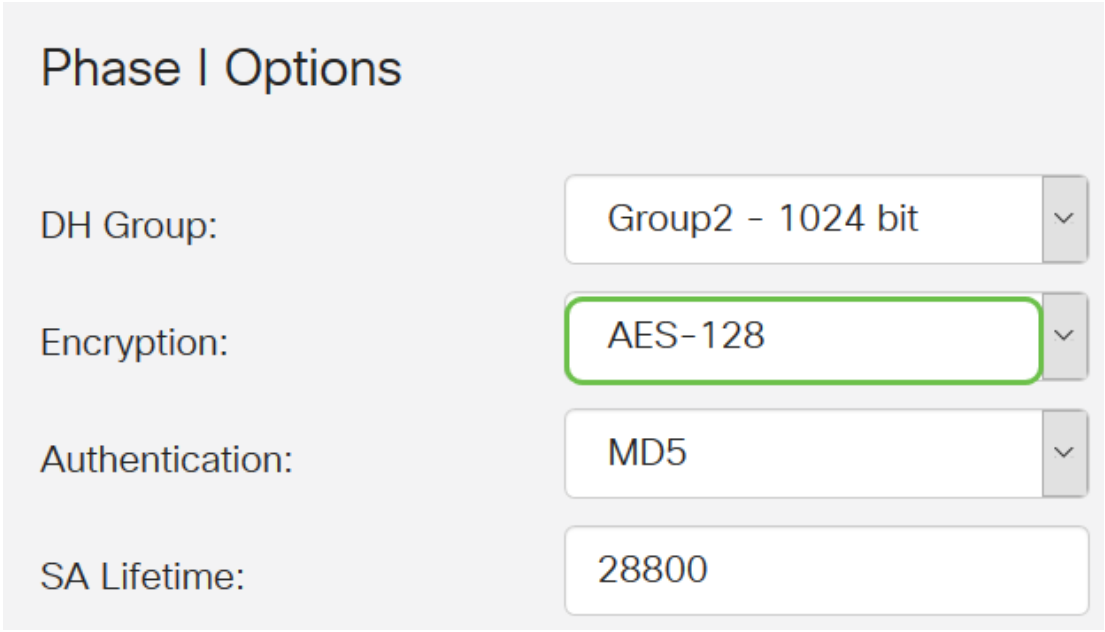
Stap 1. Kies in het gebied Fase 1 Opties de juiste Diffie-Hellman (DH) groep die met de toets in Fase 1 moet worden gebruikt in de vervolgkeuzelijst *DH Group*. Diffie-Hellman is een cryptografisch sleuteluitwisselingsprotocol dat wordt gebruikt in de verbinding om vooraf gedeelde sleutelgroepen uit te wisselen. De sterkte van het algoritme wordt bepaald door bits. De opties zijn:

- Group2-1024 bit - Deze optie compileert de toets trager, maar is veiliger dan Groep 1.
- Groep5-1536 bit - Deze optie compileert de toets het traagste, maar is de best beveiligde.



Stap 2. Kies in de vervolgkeuzelijst *Encryption* een encryptie-methode om de Encapsulation Security Payload (ESP) en Internet Security Association en Key Management Protocol (ISAKMP) te versleutelen en decrypteren. De opties zijn:

- 3DES — Triple Data Encryption Standard. Niet aanbevolen. Gebruik het enkel als het vereist is voor achterwaartse compatibiliteit aangezien het kwetsbaar is voor sommige "blokbotsingen" aanvallen.
- AES-128 — Advanced Encryption Standard gebruikt een 128-bits toets. Advanced Encryption Standard (AES) is een cryptografisch algoritme dat ontworpen is om veiliger te zijn dan DES. AES gebruikt een grotere key size die ervoor zorgt dat de enige bekende benadering om een bericht te decrypteren voor een indringer is om elke mogelijke sleutel te proberen.
- AES-192 — Advanced Encryption Standard gebruikt een 192-bits toets.
- AES-256 — Advanced Encryption Standard gebruikt een 256-bits toets. Dit is de best beveiligde encryptie optie.

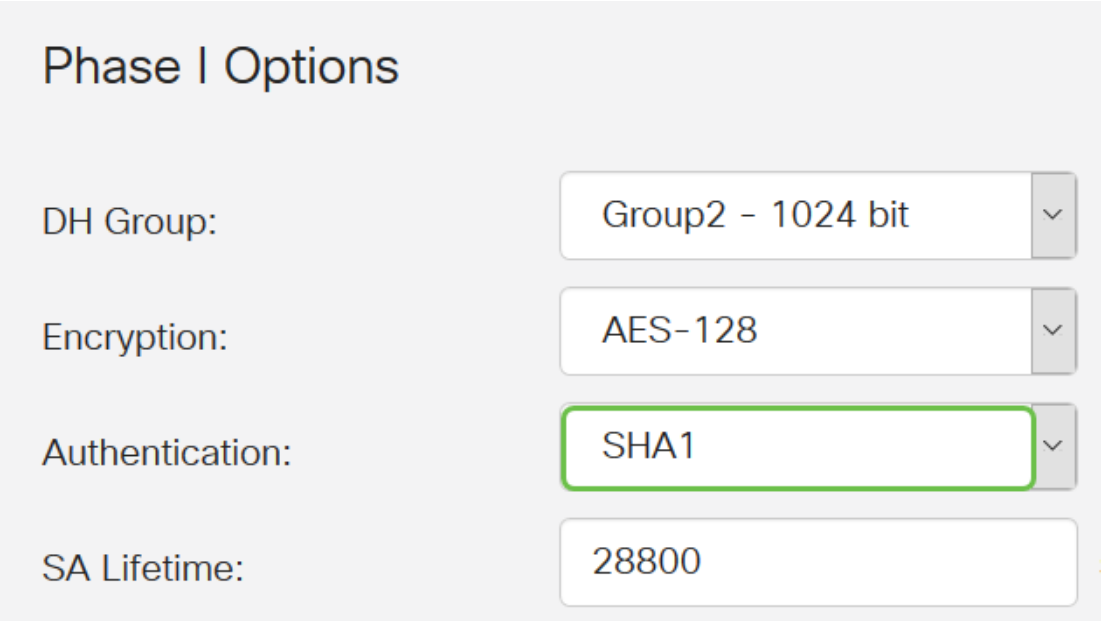


Opmerking: AES is de standaardmethode voor codering via DES en 3DES voor betere prestaties en beveiliging. Door de AES-toets te verlengen, wordt de beveiliging verhoogd met een daling in prestaties.

Stap 3. *Kies* in de vervolgkeuzelijst *Verificatie* een authenticatiemethode die bepaalt hoe ESP en ISAKMP geauthentiseerd zijn. De opties zijn:

- MD5 — Message-Digest-algoritme heeft een hashwaarde van 128 bits.
- SHA-1 — Secure Hash Algorithm heeft een 160-bits hashwaarde.
- SHA2-256 — Secure Hash Algorithm met een hashwaarde van 256 bits. Dit is het best beveiligde en aanbevolen algoritme.

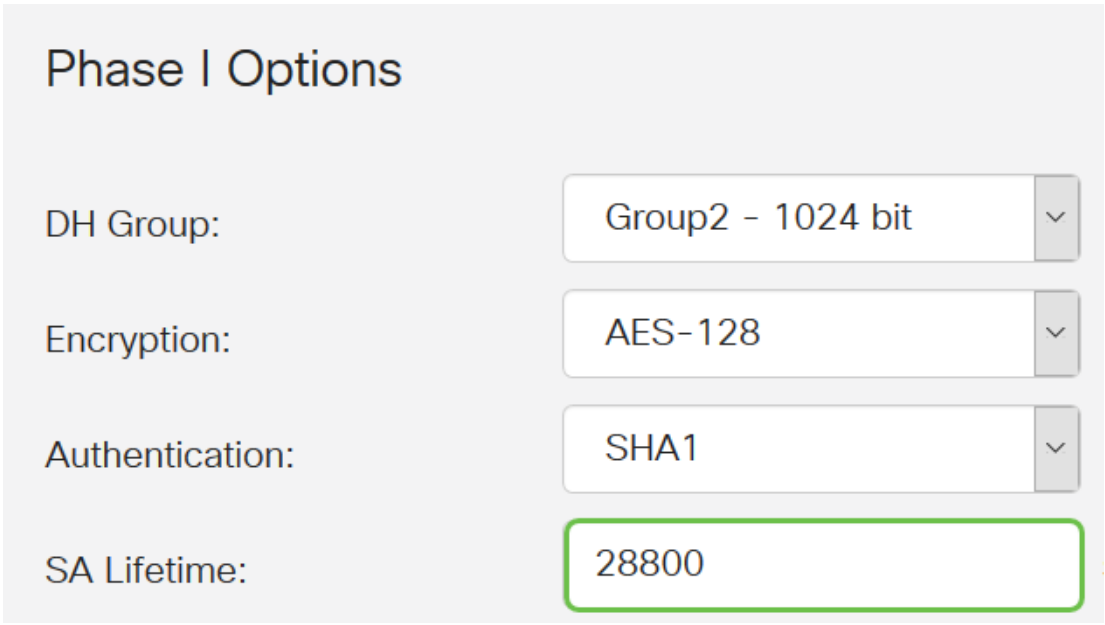
Opmerking: Zorg ervoor dat beide uiteinden van de VPN-tunnel dezelfde authenticatiemethode gebruiken.



Opmerking: MD5 en SHA zijn beide cryptografische hashfuncties. Ze nemen een stuk gegevens, compacte ze en maken een unieke hexadecimale output die normaal niet kan worden gereproduceerd. In dit voorbeeld wordt SHA1 gekozen.

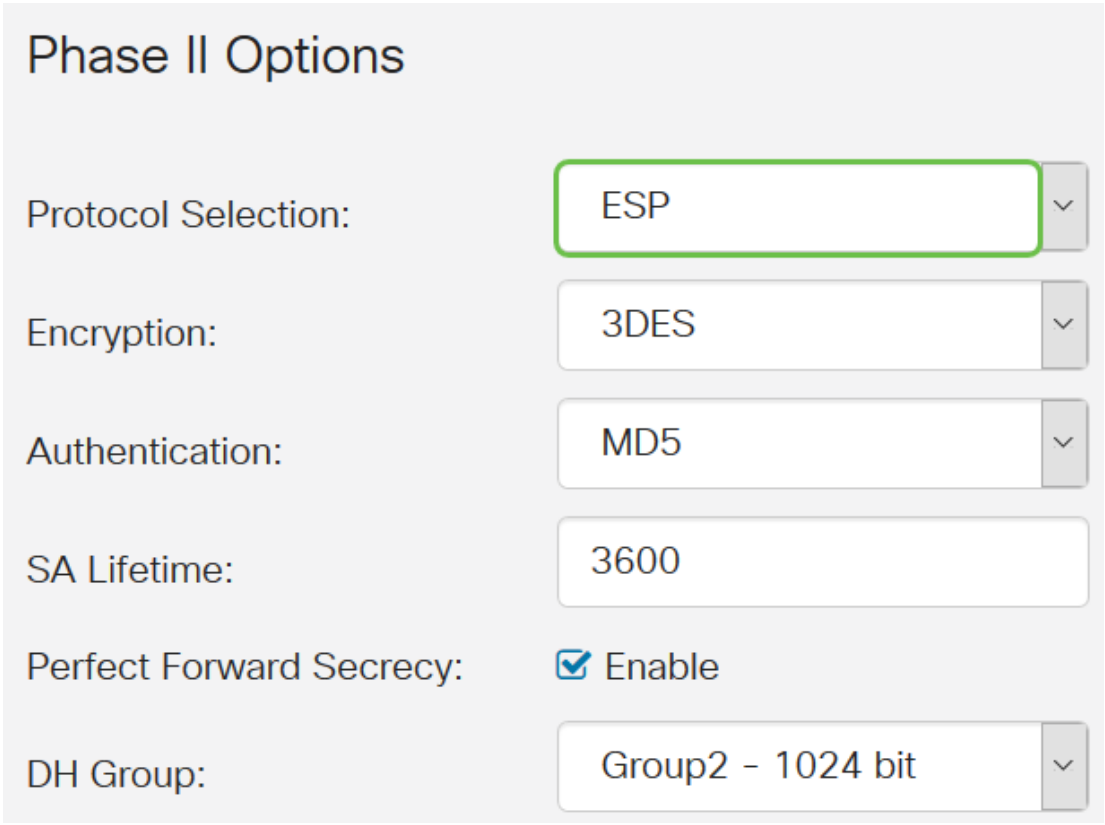
Stap 4. Voer in het veld *SA Lifetime* een waarde in tussen 120 en 86400. De standaardwaarde is 28800. De *SA Lifetime (SEC)* vertelt u de hoeveelheid tijd, in seconden, is een IKE SA actief in deze fase. Er is onderhandeld over een nieuwe Security Association (SA) voordat de levensduur verstrijkt om te verzekeren dat een nieuwe SA klaar is om te worden gebruikt als de oude verstrijkt. Het standaard is 28800 en het bereik loopt van 120 tot 86400. We gebruiken 28800 seconden als onze SA-levensduur voor fase I.

Opmerking: Aanbevolen wordt dat uw SA-levensduur in fase I langer is dan uw fase II SA-levensduur. Als je fase I korter maakt dan fase II, dan moet je regelmatig opnieuw onderhandelen over de tunnel dan vaak in tegenstelling tot de datunnel. Gegevenstunnel is wat meer veiligheid nodig heeft, zodat het beter is om de levensduur in fase II korter te hebben dan fase I.



Stap 5. Kies in de vervolgkeuzelijst *Protocolselectie* in het gebied Fase II Opties een protocoltype dat moet worden toegepast op de tweede fase van de onderhandelingen. De opties zijn:

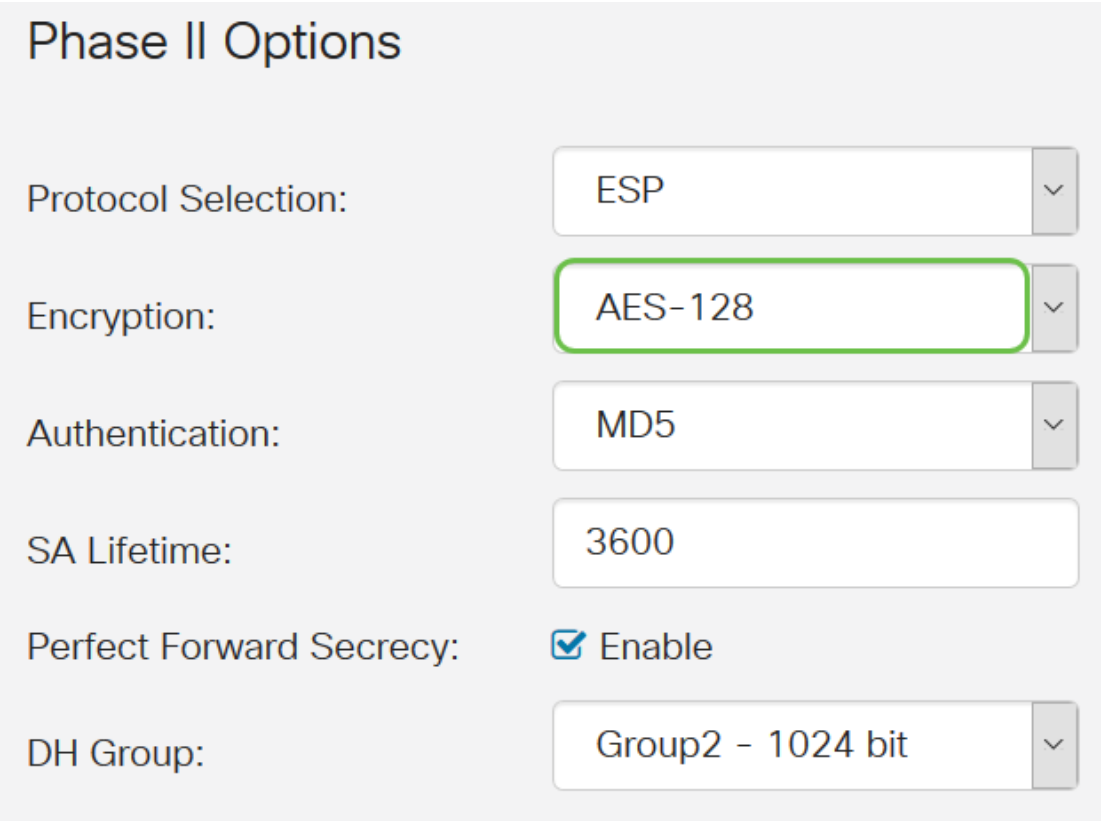
- ESP — Deze optie is ook wel bekend als Inkapselende Security payload. Met deze optie worden de te beschermen gegevens opgenomen. Als deze optie is geselecteerd, gaat u naar Stap 6 om een coderingsmethode te kiezen.
- AH — Deze optie is ook bekend als Verificatieheader (AH). Het is een veiligheidsprotocol dat gegevensverificatie en optionele anti-replay service biedt. AH is ingesloten in het IP-datagram dat moet worden beschermd. Als deze optie is geselecteerd, slaat u over naar Stap 7.



Stap 6. Als u in Stap 6 voor ESP hebt gekozen, kiest u een *encryptie*. De opties zijn:

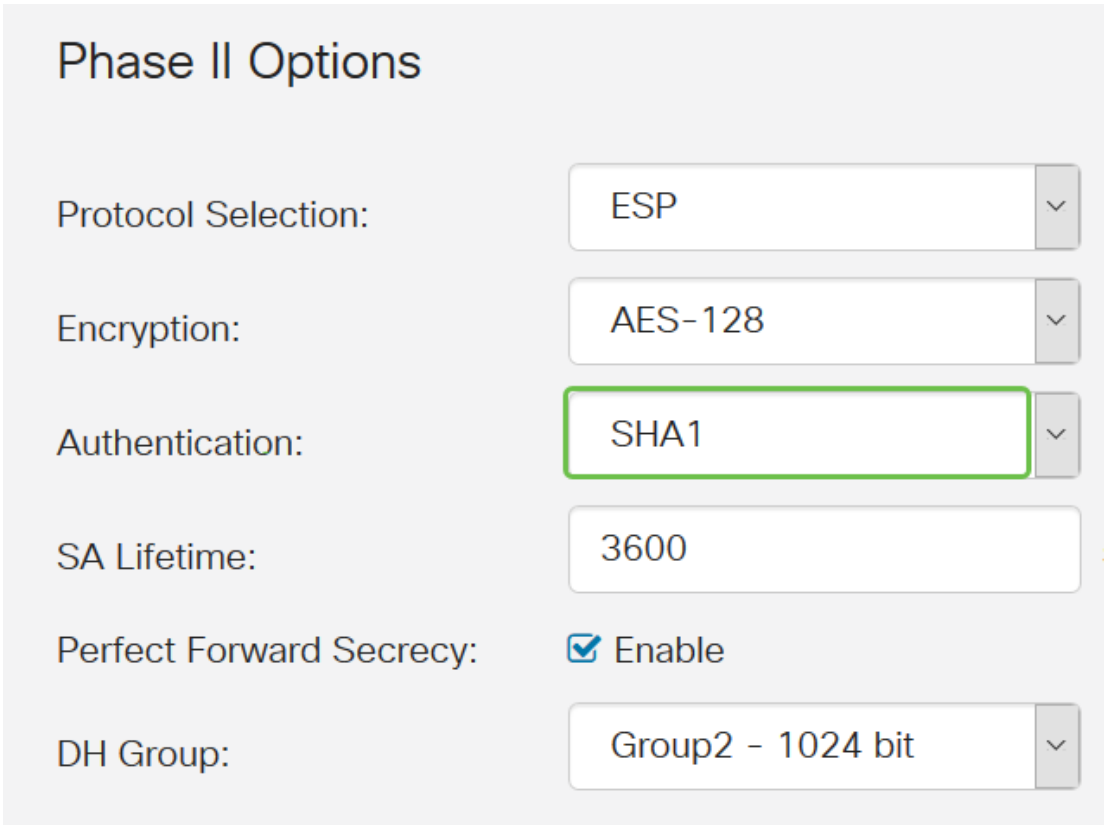
- 3DES — Standaard met drie gegevensencryptie
- AES-128 — Advanced Encryption Standard gebruikt een 128-bits toets.

- AES-192 — Advanced Encryption Standard gebruikt een 192-bits toets.
- AES-256 — Advanced Encryption Standard gebruikt een 256-bits toets.

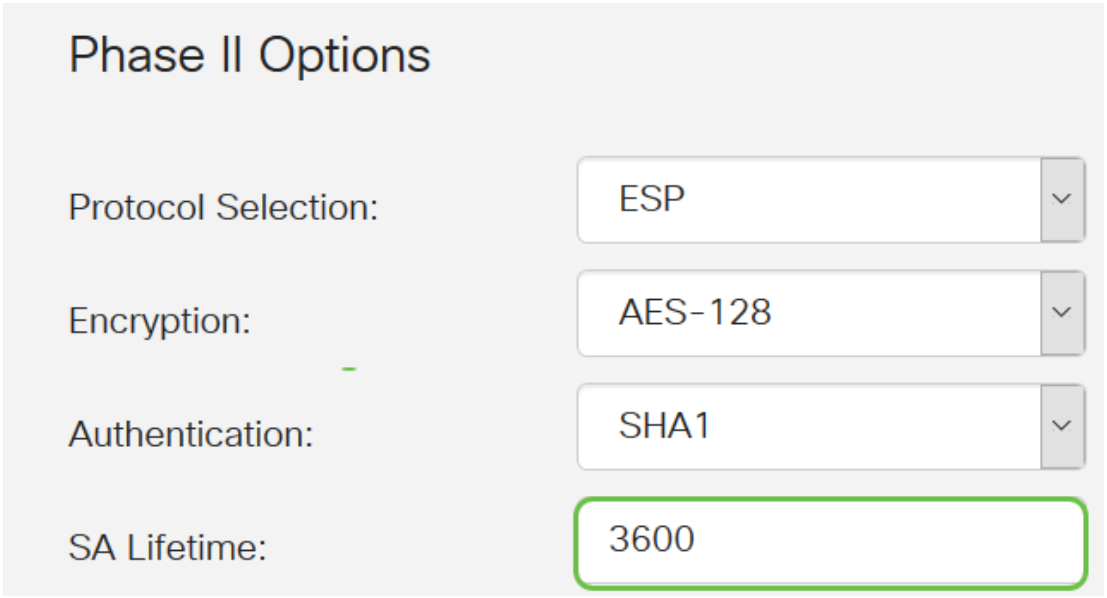


Stap 7. *Kies* in de vervolgkeuzelijst *Verificatie* een authenticatiemethode die bepaalt hoe ESP en ISAKMP geauthentiseerd zijn. De opties zijn:

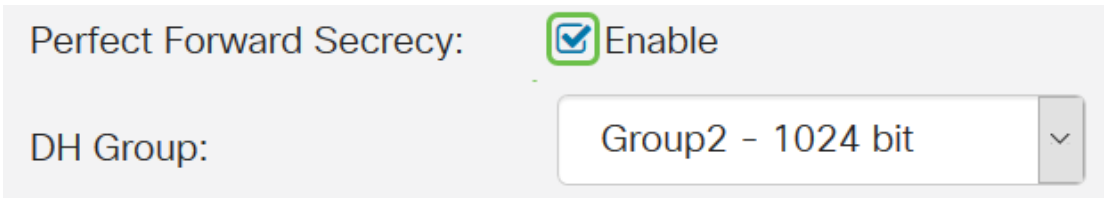
- MD5 — Message-Digest-algoritme heeft een hashwaarde van 128 bits.
- SHA-1 — Secure Hash Algorithm heeft een 160-bits hashwaarde.
- SHA2-256 — Secure Hash Algorithm met een hashwaarde van 256 bits.



Stap 8. Voer in het veld *SA Liftime* een waarde in tussen 120 en 2800. Dit is de tijdsduur van de IKE SA actief in deze fase. De standaardwaarde is 3600.

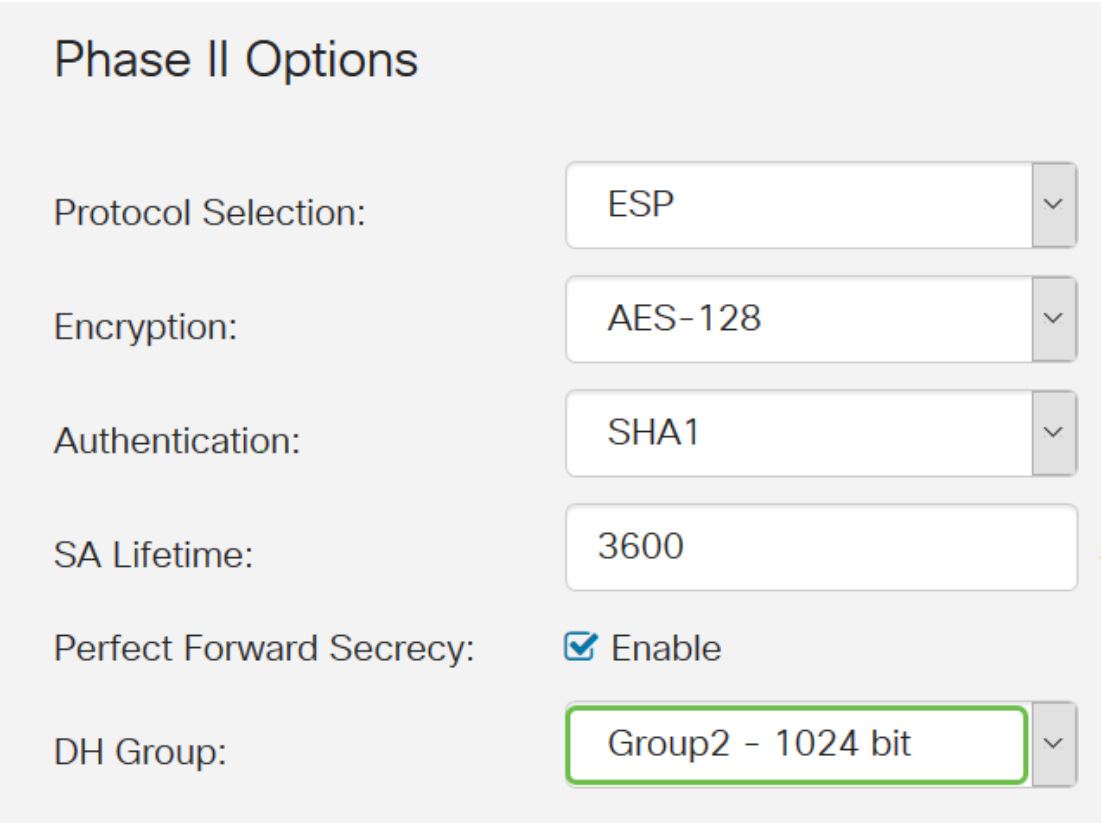


Stap 9. (Optioneel) Controleer het aanvinkvakje Perfect Forward Security **inschakelen** om een nieuwe toets voor IPsec-verkeersencryptie en verificatie te genereren. Perfect voorwaartse geheimhouding wordt gebruikt om de beveiliging van communicatie via het internet te verbeteren door middel van openbare sleutelcryptografie. Schakel dit vakje in om deze optie in te schakelen, of trek het vakje uit om deze optie uit te schakelen. Deze optie wordt aanbevolen.

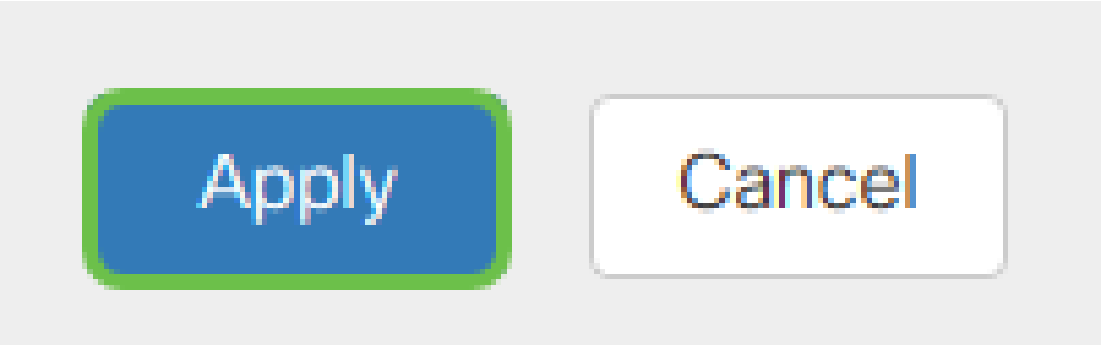


Stap 10. Kies in de vervolgkeuzelijst *DH Group* een DH-groep die met de toets in fase 2 moet worden gebruikt. De opties zijn:

- Group2-1024 bit - Deze optie compileert de toets sneller, maar is minder veilig.
- Groep5-1536 bit - Deze optie compileert de toets het traagste, maar is de best beveiligde.

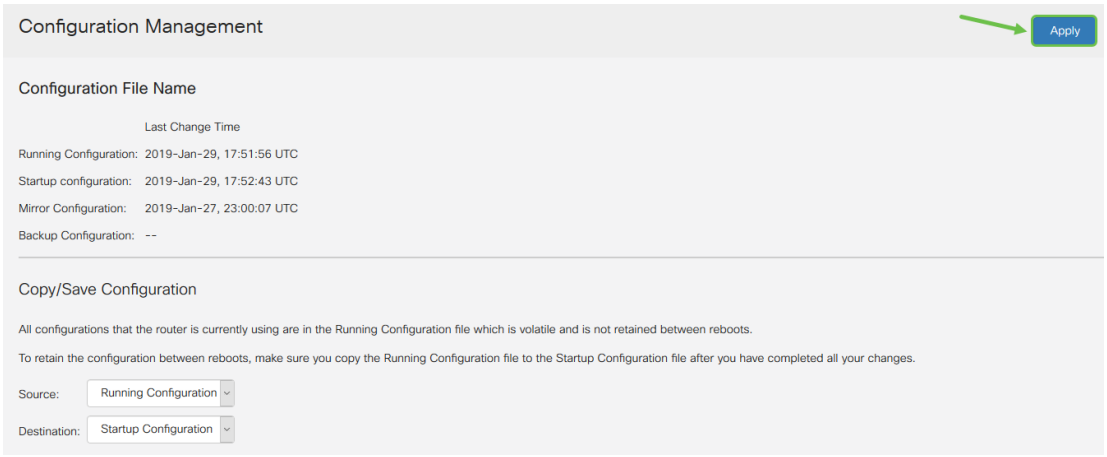


Stap 1. Klik op **Toepassen**.

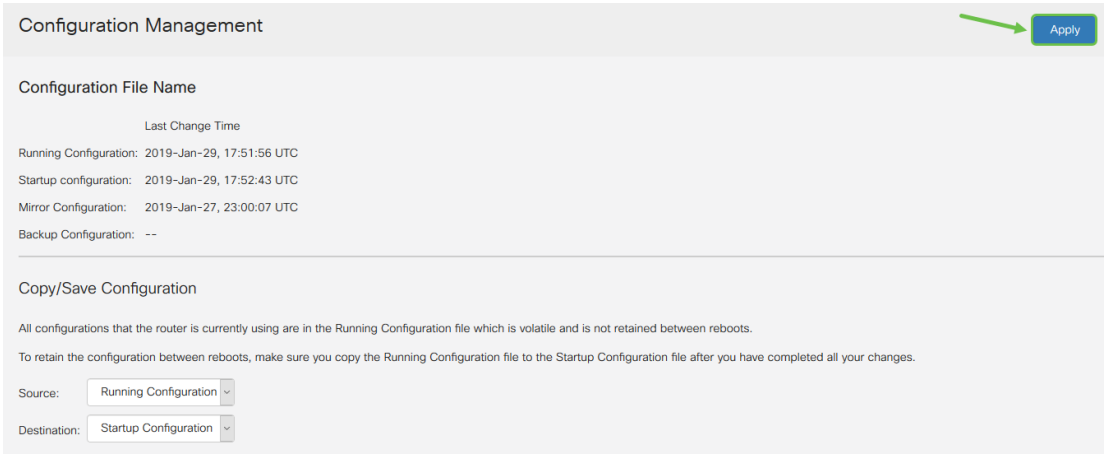


Stap 12. Klik op **Save** om de configuratie permanent op te slaan.

Stap 13. Klik nogmaals op **Toepassen** om de actieve configuratie op te slaan als u het opstartbeeld wilt configureren.



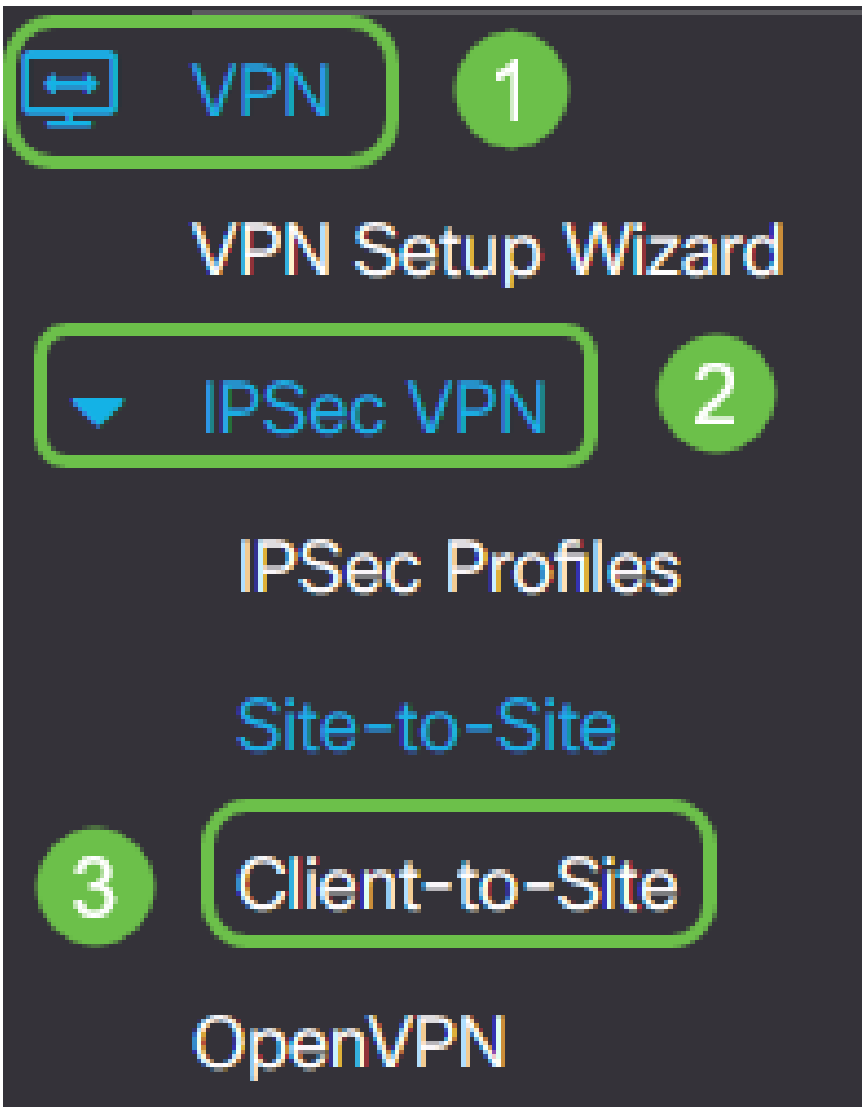
Stap 14. Wanneer u de bevestiging ontvangt, klikt u op **OK**.



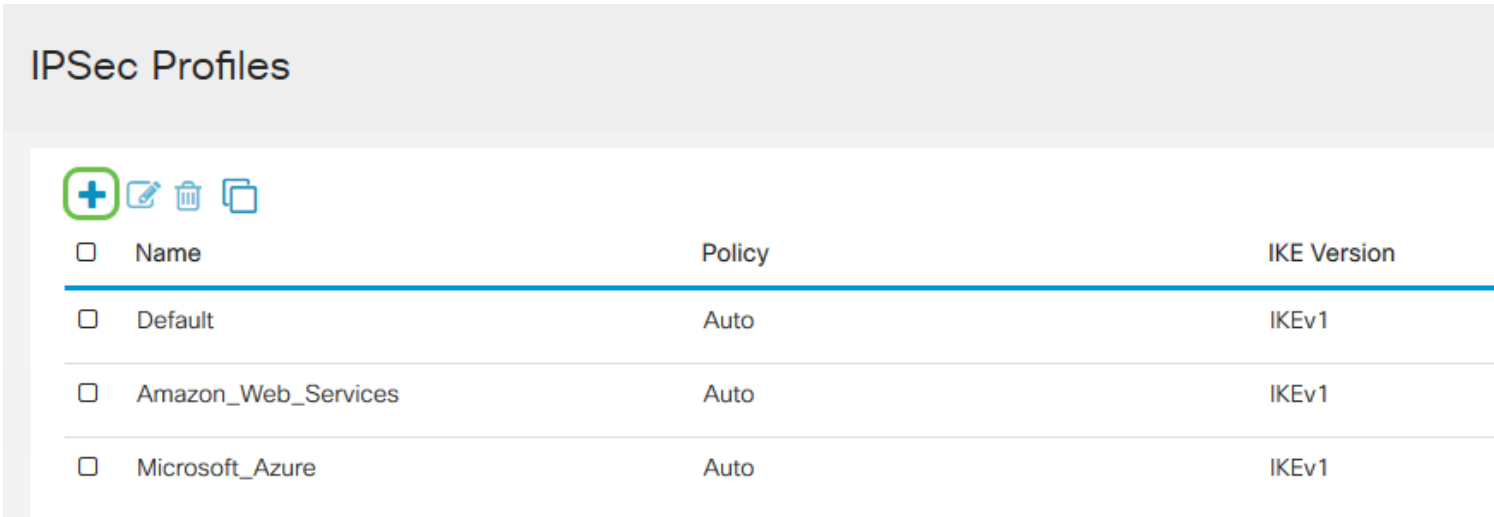
U moet nu met succes een IPsec-profiel op uw RV160- of RV260-router hebben geconfigureerd.

Een client-naar-site profiel maken

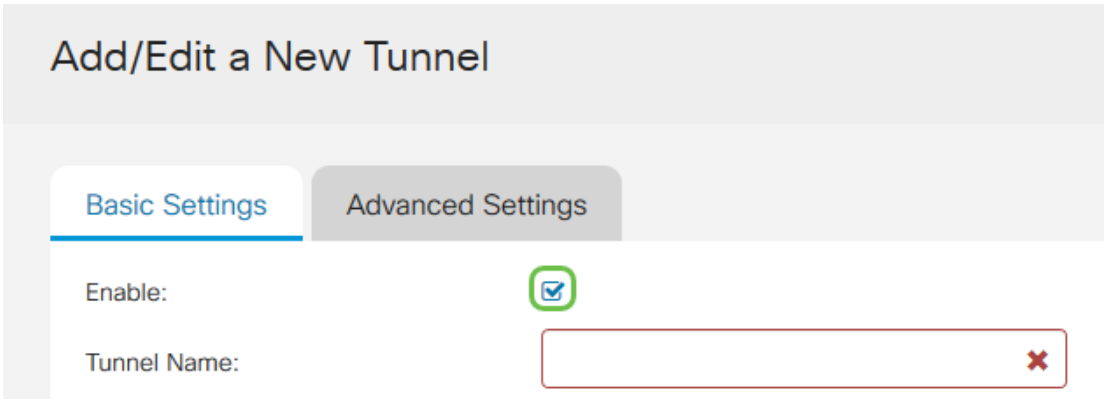
Stap 1. Kies **VPN > IPSec VPN > Client-to-Site**.



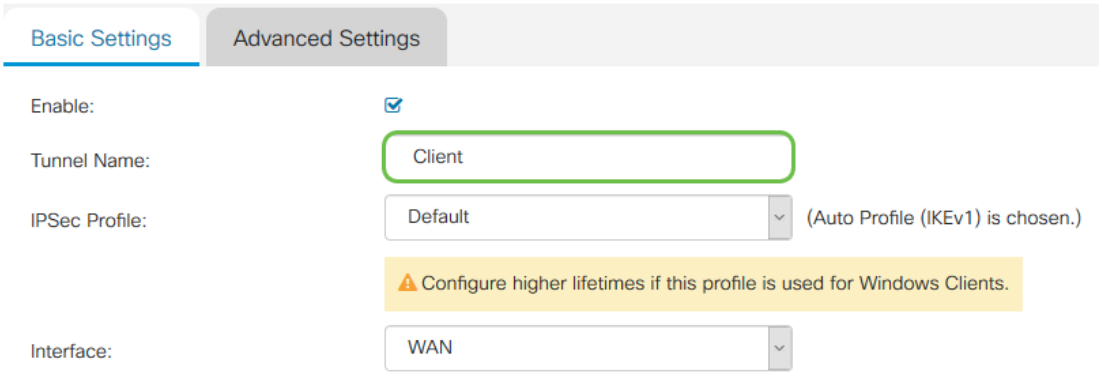
Stap 2. Klik op het pictogram **plus**.



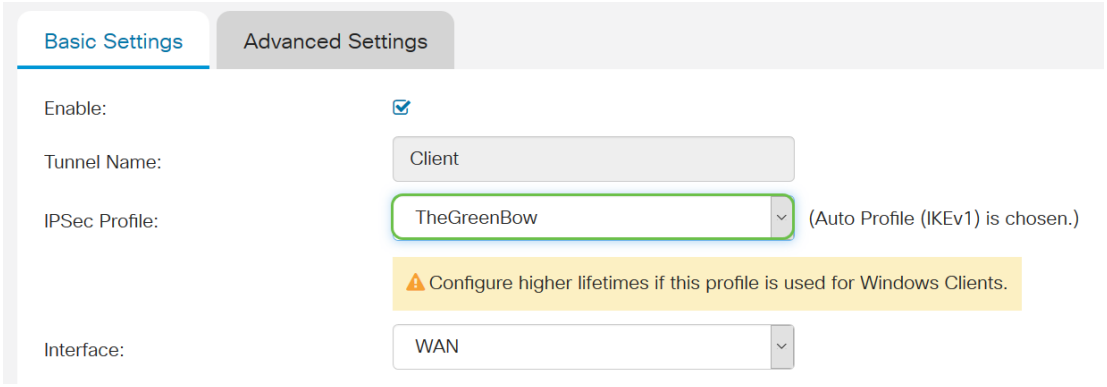
Stap 3. Onder het tabblad Basis-instellingen, controleert u het vakje **Enable** om er zeker van te zijn dat het VPN-profiel actief is.



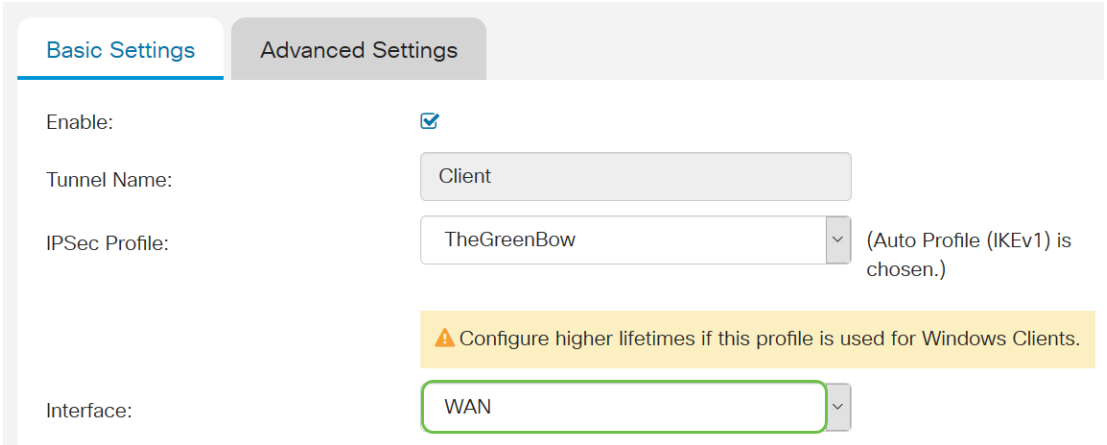
Stap 4. Voer een naam in voor de VPN-verbinding in het veld *Tunnelnaam*.



Stap 5. Kies het IPsec-profiel dat in de vervolgkeuzelijst *IPsec* moet worden gebruikt.



Stap 6. Kies de interface in de vervolgkeuzelijst *Interface*.



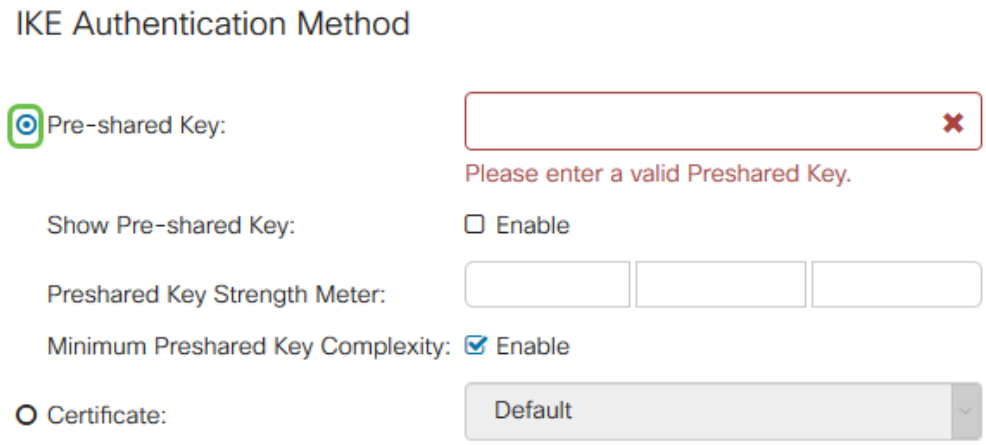
Opmerking: De opties hangen af van het model van de router die u gebruikt. In dit voorbeeld wordt WAN geselecteerd.

Stap 7. Kies een IKE-verificatiemethode. De opties zijn:

- Vooraf gedeelde sleutel — Deze optie laat ons een gedeeld wachtwoord gebruiken voor

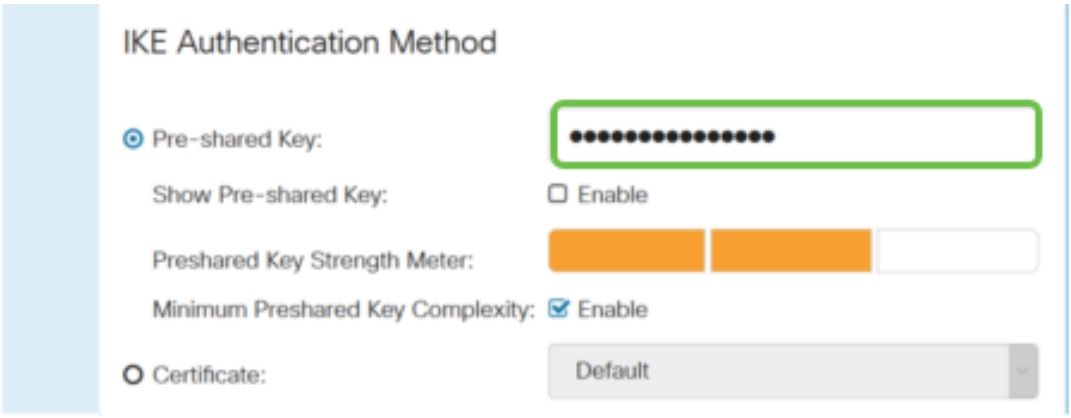
de VPN-verbinding.

- Certificaat — Deze optie gebruikt een digitaal certificaat met informatie als de naam, het IP-adres, het serienummer, de vervaldatum van het certificaat en een kopie van de openbare sleutel van de houder van het certificaat.

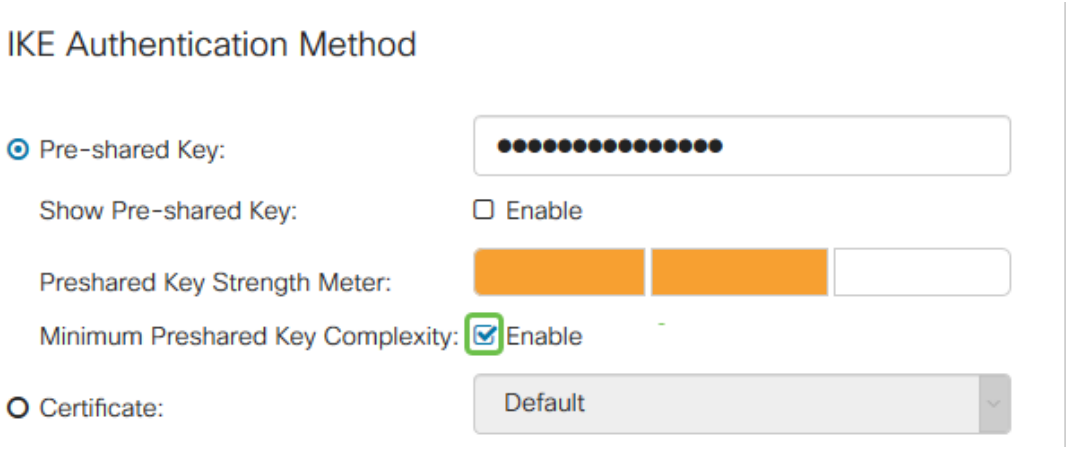


Opmerking: Een Pre-Shared Key kan zijn wat je maar wilt, hij moet alleen op de site en met de klant passen wanneer ze The GreenBow Client op hun computer opzetten.

Stap 8. Voer het verbindingswachtwoord in in het veld *Voorgedeelde sleutel*.

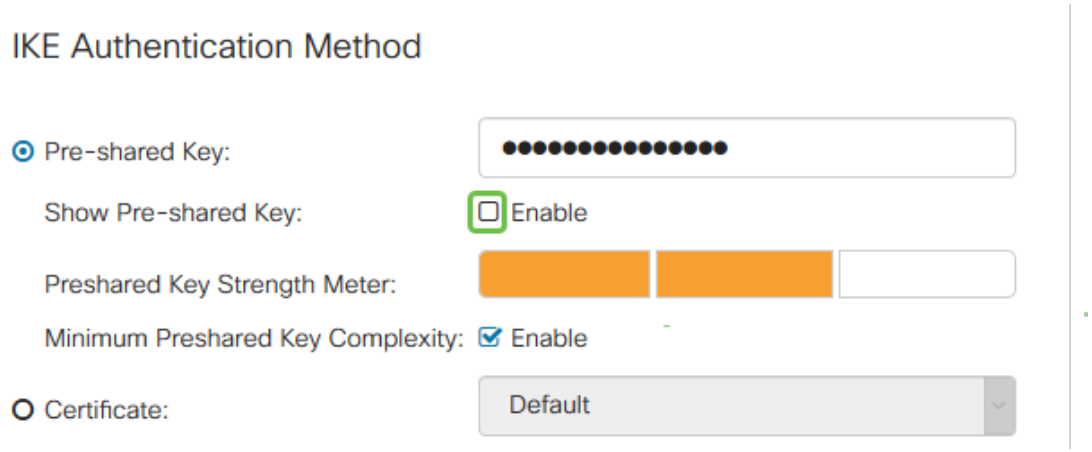


Stap 9. (optioneel) Schakel het *vakje Minimale voorgedeelde sleutel* uit. Schakel in om een eenvoudig wachtwoord te kunnen gebruiken.



Opmerking: In dit voorbeeld, wordt de Minimale Pre-Shared Key Complexity links ingeschakeld.

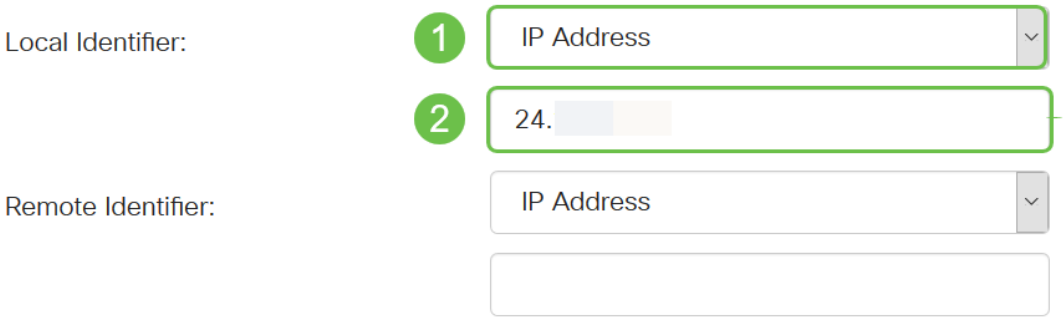
Stap 10. (Optioneel) Controleer de *Voorgedeeld sleutel* voor *weergave* van het wachtwoord in onbewerkte tekst.



Opmerking: In dit voorbeeld wordt de voorgedeelde toets tonen uitgeschakeld.

Stap 11. Kies een lokaal identificatienummer in de vervolgkeuzelijst *Local Identifier*. De opties zijn:

- Lokale WAN IP — Deze optie gebruikt het IP-adres van de WAN-interface (Wide Area Network) van de VPN-gateway.
- IP-adres - Met deze optie kunt u handmatig een IP-adres voor de VPN-verbinding invoeren. Dit is het WAN IP-adres van de router op de site (Office).
- FQDN - Deze optie is ook bekend als Full Qualified Domain Name (FQDN). Het laat u een volledige domeinnaam voor een specifieke computer op het internet gebruiken.
- Gebruiker FQDN - Met deze optie kunt u een volledige domeinnaam voor een specifieke gebruiker op het internet gebruiken.

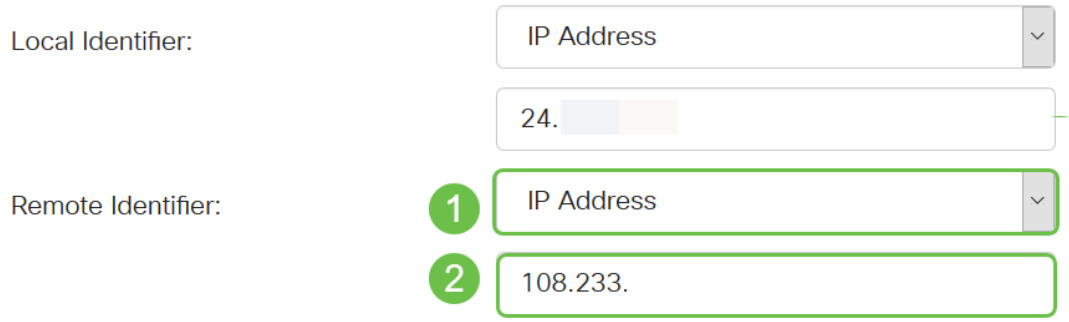


Opmerking: In dit voorbeeld, wordt het IP Adres gekozen en het WAN IP Adres van de router op de plaats binnendringen. In dit voorbeeld is 24.x.x.x ingevoerd. Het volledige adres is verstoord voor privacydoeleinden.

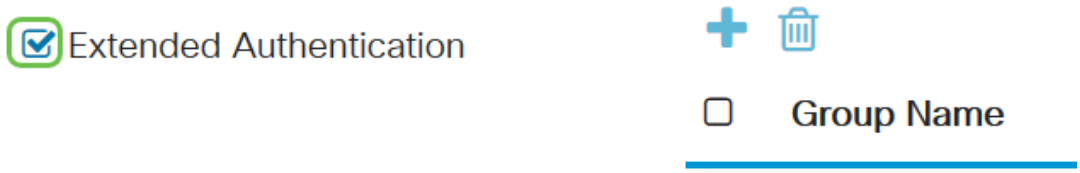
Stap 12. Kies een identificatie voor de externe host. De opties zijn:

- IP-adres - Deze optie gebruikt het WAN IP-adres van de VPN-client. Om het WAN IP-adres te vinden kunt u in uw webbrowser "wat is mijn IP" invoeren. Dit is het client-IP-adres.
- FQDN - volledig gekwalificeerde domeinnaam. Met deze optie kunt u een volledige domeinnaam voor een specifieke computer op het internet gebruiken.
- Gebruiker FQDN - Met deze optie kunt u een volledige domeinnaam voor een specifieke gebruiker op het internet gebruiken.

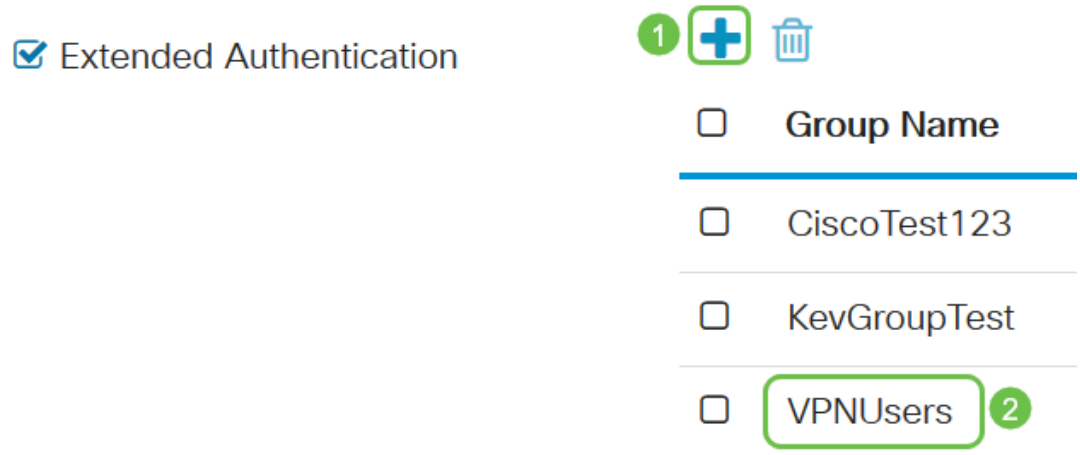
Opmerking: In dit voorbeeld, wordt het IP Adres gekozen en het huidige IPv4 adres van de router op de plaats van de klant is ingevoerd. Dit kan worden bepaald door te zoeken naar "Wat is mijn IP adres" in uw webbrowser. Dit adres kan zo veranderen als u problemen hebt met het verbinden na een succesvolle configuratie, kan dit een gebied zijn om op zowel de client als op de site te controleren en te wijzigen.



Stap 13. (Optioneel) Controleer het vakje **Extended Verificatie** om de functie te activeren. Indien geactiveerd, zal dit een extra niveau van authenticatie opleveren dat van externe gebruikers vereist is om in hun aanmeldingsgegevens te klikken voordat ze toegang tot VPN krijgen.



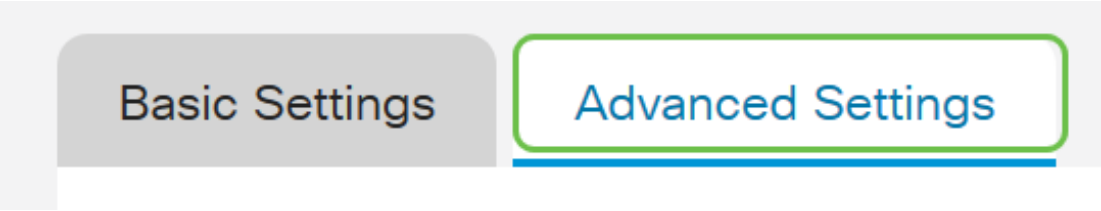
Stap 14. (Optioneel) Kies de groep die uitgebreide authenticatie zal gebruiken door op het pictogram **plus** te klikken en selecteer de gebruiker in de vervolgkeuzelijst.



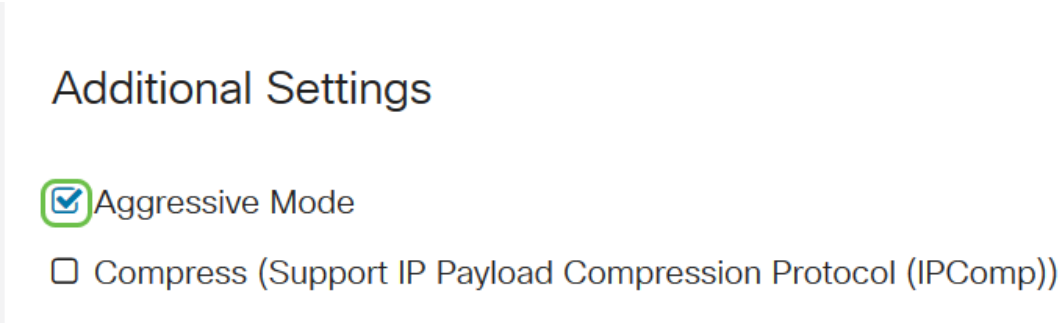
Opmerking: In dit voorbeeld wordt **VPNU** geselecteerd.

Stap 15. Onder *Pool Range voor Client LAN*, Voer het eerste IP- en eindadres in dat aan een VPN-client kan worden toegewezen. Dit moet een pool van adressen zijn die niet met de site adressen overlapt. Deze kunnen virtuele interfaces worden genoemd. Als u een bericht ontvangt dat een virtuele interface moet worden gewijzigd, dan kunt u dat repareren.

Stap 16. Selecteer het tabblad **Geavanceerde instellingen**.

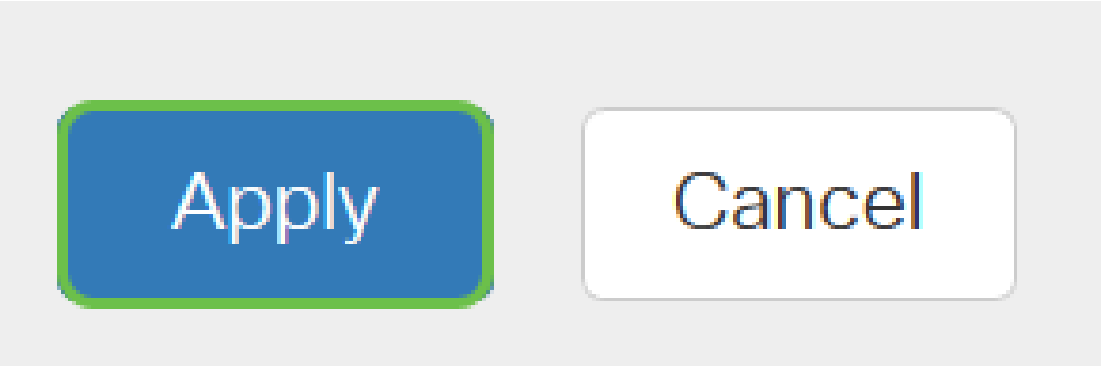


Stap 17. (Optioneel) Scrolt naar de onderkant van de pagina en selecteer **Aggressive Mode**. Met de optie Aggressive Mode kunt u RADIUS-tunneleigenschappen specificeren voor een IP security (IPsec) peer en een Internet Key Exchange (IKE)-agressieve mode-onderhandeling met de tunnel openen. Klik hier voor meer informatie over Aggressive Mode vs. Main Mode.



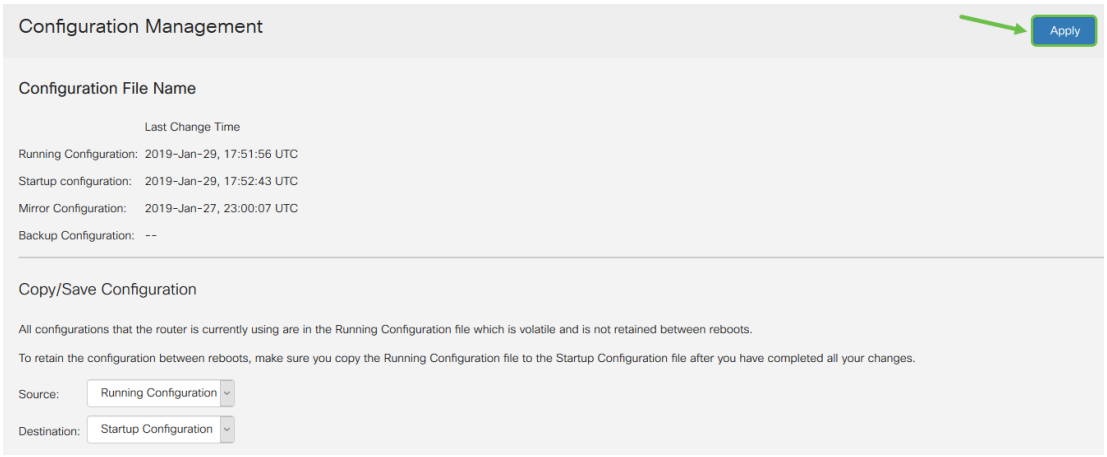
Opmerking: Het vakje Compress check stelt de router in staat om compressie voor te stellen wanneer het een verbinding begint. Dit protocol beperkt de omvang van IP-datagrammen. Als de responder dit voorstel afwijst, dan voert de router geen compressie uit. Wanneer de router de responder is, accepteert het compressie, zelfs als compressie niet ingeschakeld is. Als u deze eigenschap voor deze router toelaat, zou u het op de verre router (het andere eind van de tunnel) moeten toelaten. In dit voorbeeld bleef *Compress* ongecontroleerd.

Stap 18. Klik op **Toepassen**.



Stap 19. Klik op **Opslaan**.

Stap 20. Klik nogmaals op **Toepassen** om de actieve configuratie op te slaan in het opstartbeeld.



Stap 21. Wanneer u de bevestiging ontvangt, klikt u op **OK**.

U had nu de client-to-Site Tunnel op de router voor The GreenBow VPN-client moeten configureren.

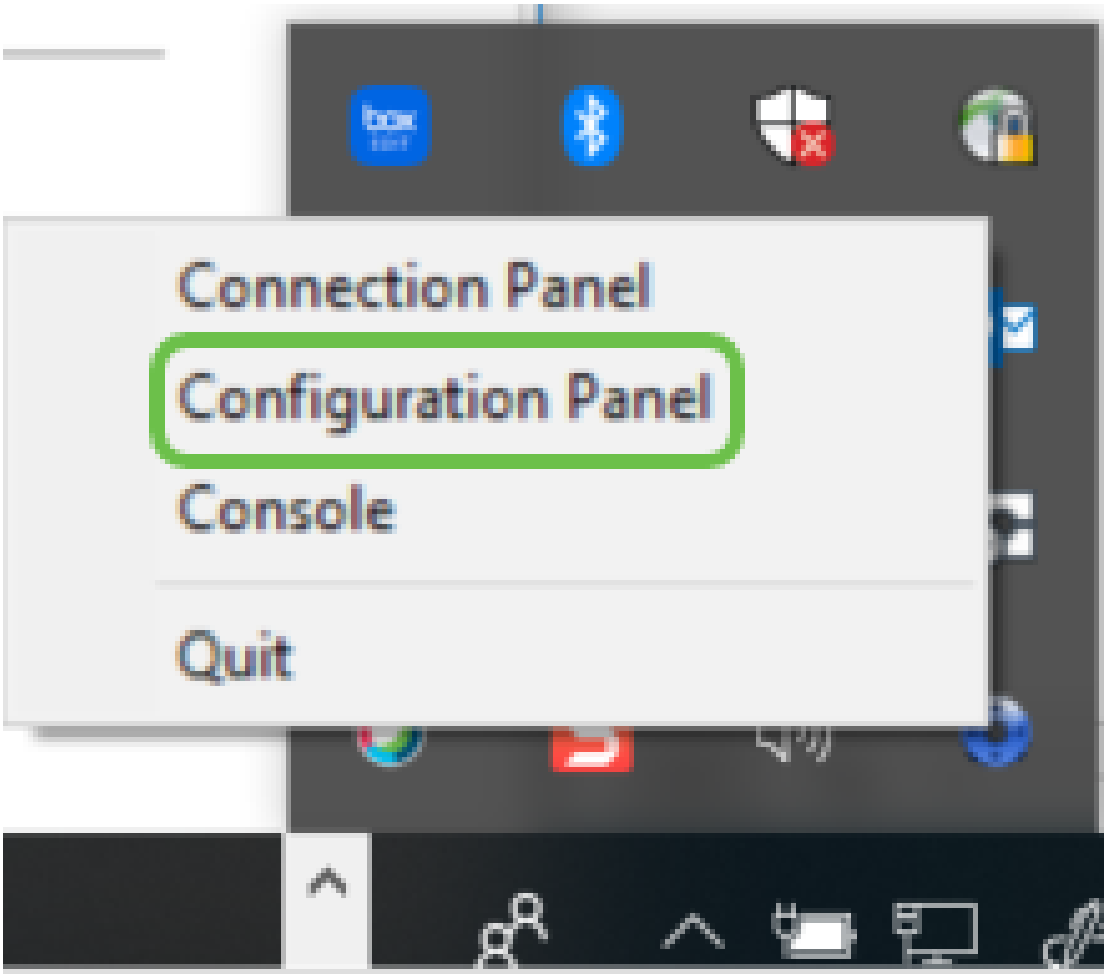
De GroeneBow VPN-client configureren op de computer van de afstandsbediening

Instellingen fase 1

Klik hier om de nieuwste release van de clientsoftware van de GreenBow IPsec VPN te downloaden.

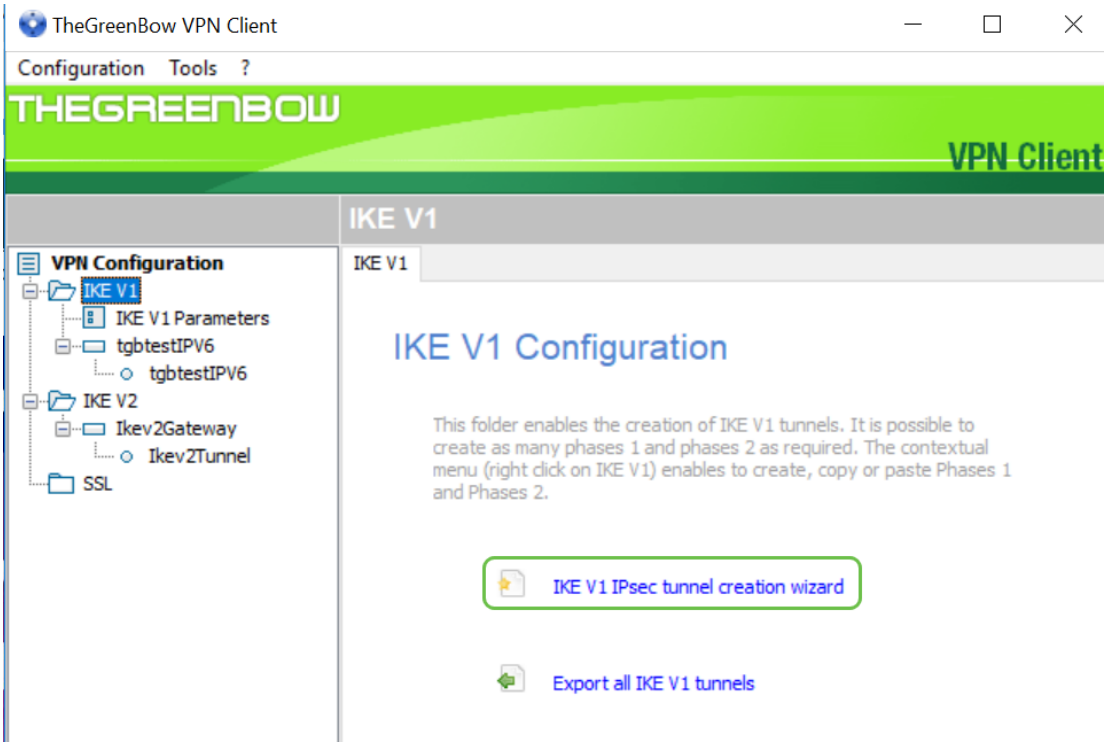
Stap 1. Klik met de rechtermuisknop op het pictogram GreenBow VPN-client. Dit bevindt zich in de rechterbenedenhoek van de taakbalk.

Stap 2. Selecteer **het Configuratiescherm**.



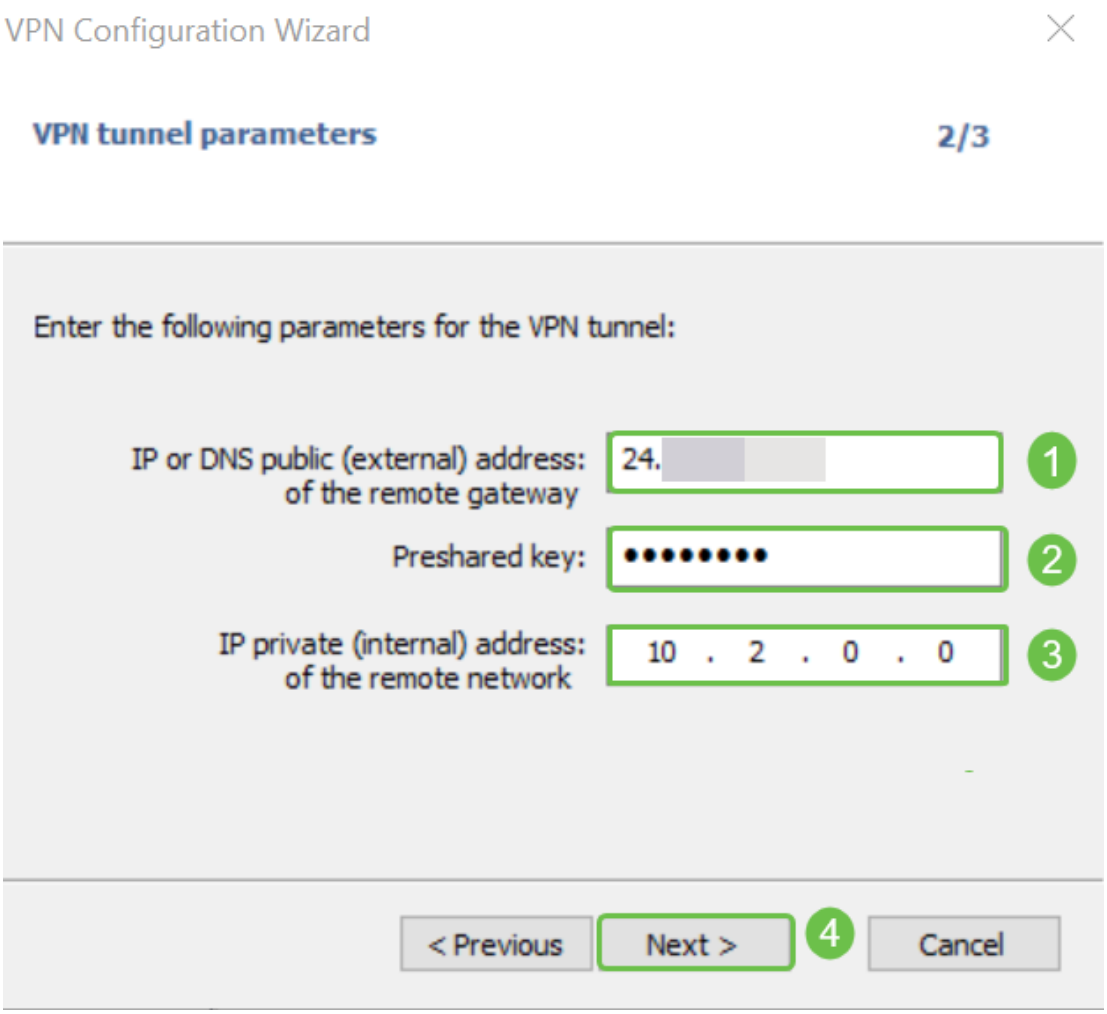
Opmerking: Dit is een voorbeeld op een Windows-computer. Dit kan variëren afhankelijk van de software die u gebruikt.

Stap 3. Selecteer **de wizard IKE V1 IPsec-tunnelvorming**.

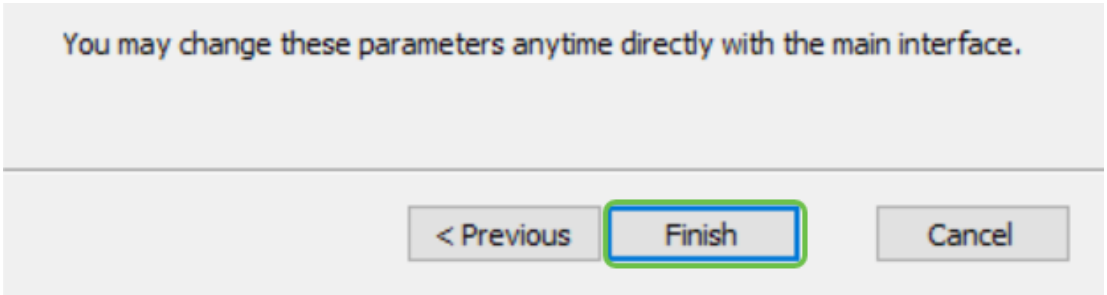


Opmerking: In dit voorbeeld wordt IKE, versie 1, ingesteld. Als u IKE versie 2 wilt configureren volgt u dezelfde stappen maar klikt u met de rechtermuisknop op de IKE V2-map. U moet ook IKEv2 voor het IPsec-profiel op de router op de site selecteren.

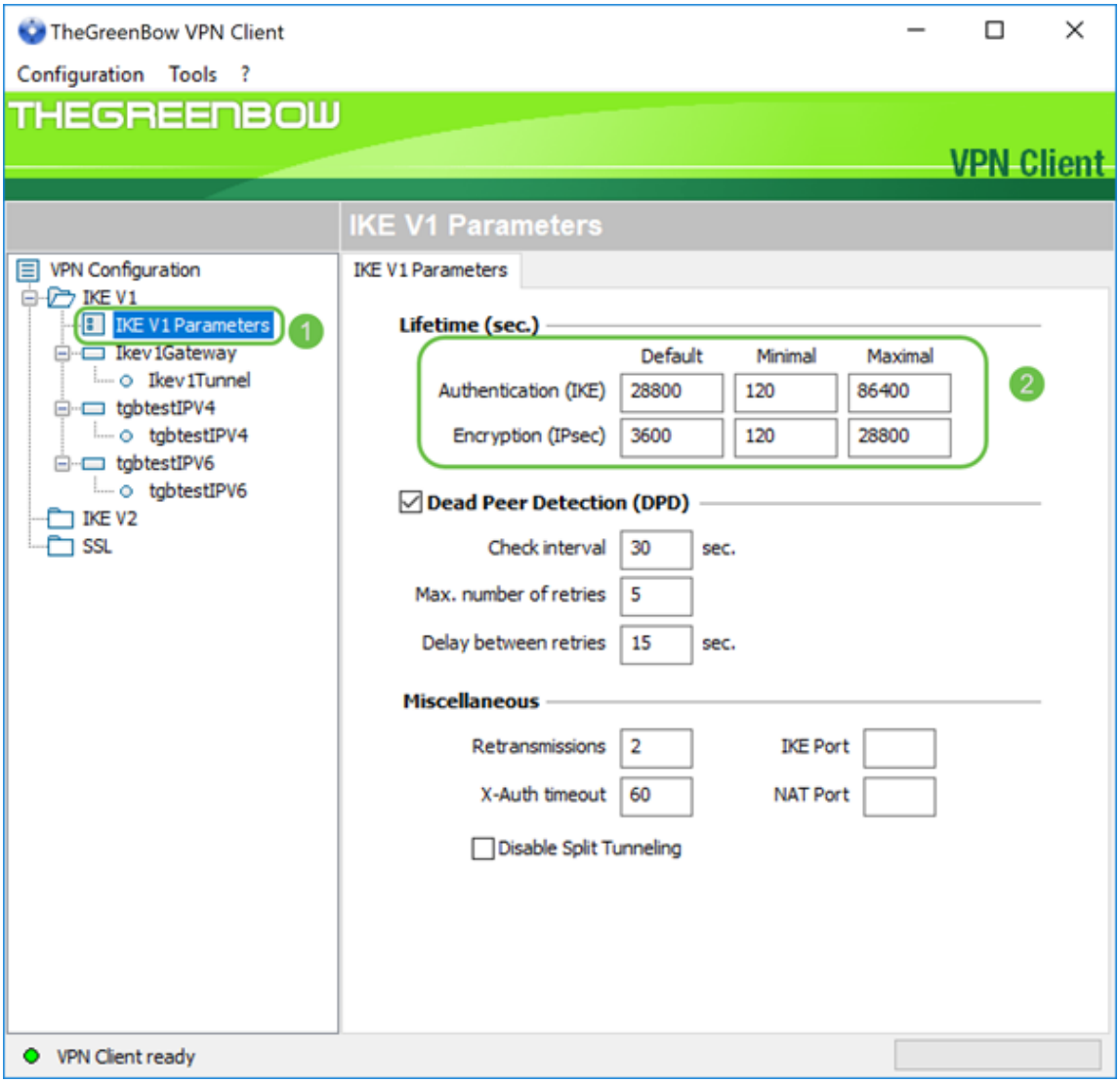
Stap 4. Vul het openbare WAN IP-adres van de router in op de locatie (kantoor) waar de bestandsserver zich bevindt, op de gedeelde sleutel en op het particuliere interne adres van het externe netwerk op de site. Klik op **Volgende**. In dit voorbeeld is de site 24.x.x.x. De laatste drie octetten (reeksen getallen in dit IP adres) zijn vervangen door een x om dit netwerk te beschermen. U voert het volledige IP-adres in.



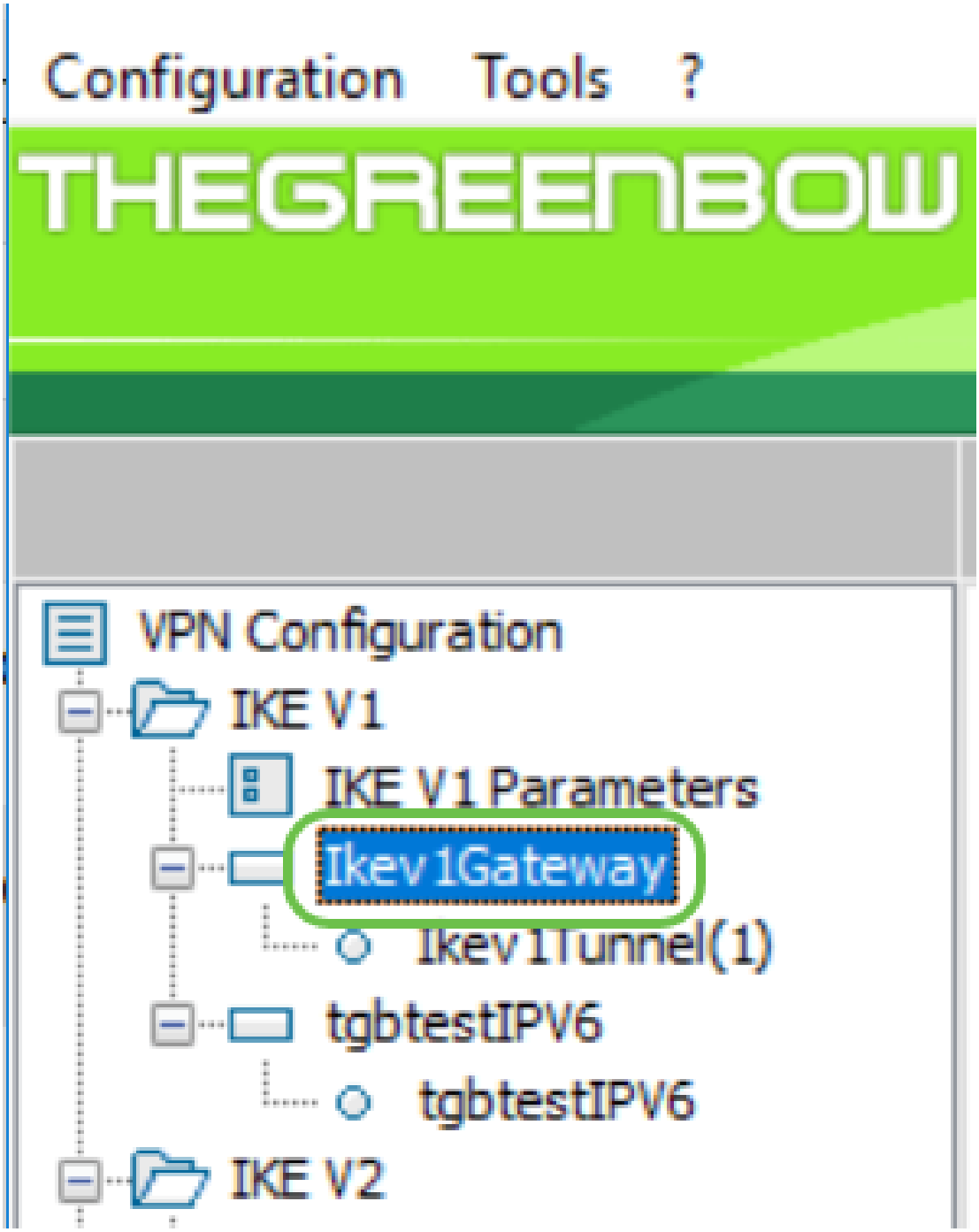
Stap 5. Klik op **Voltooien**.



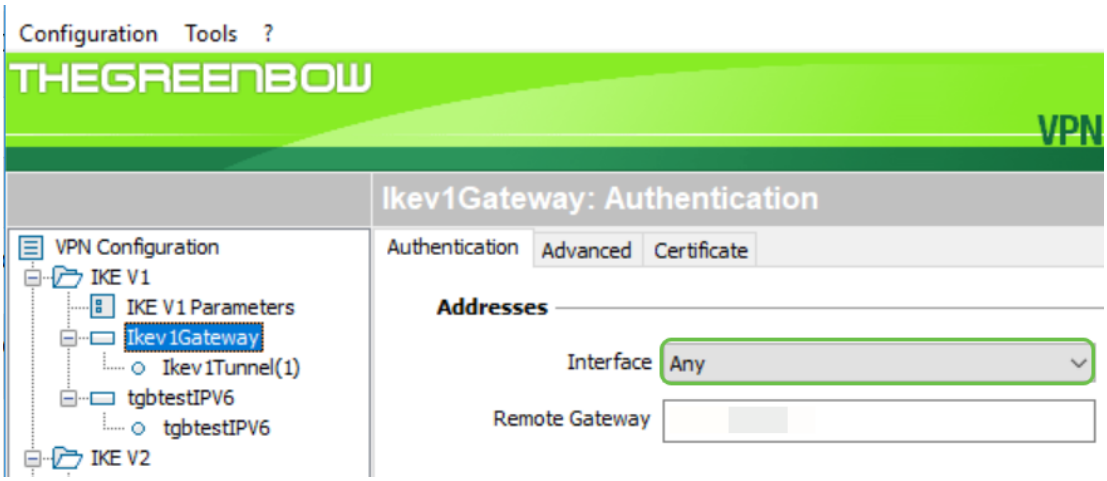
Stap 6 (optioneel) U kunt de IKE V1-parameters wijzigen. De standaardinstelling, minimalisering en maximale levensduur van GreenBow kunnen worden aangepast. In deze plaats kunt u elk bereik van het leven invoeren dat de router accepteert.



Stap 7. Klik op de door u gemaakte poort.

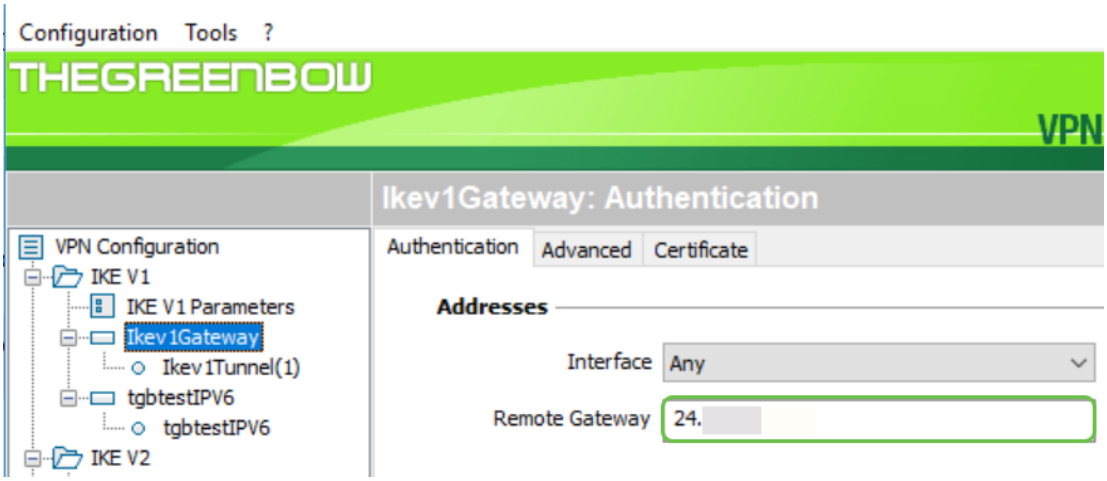


Stap 8. In het tabblad *Verificatie* onder *Adressen* ziet u een vervolgkeuzelijst met lokale adressen. U kunt één of **andere** selecteren, zoals hieronder wordt getoond.



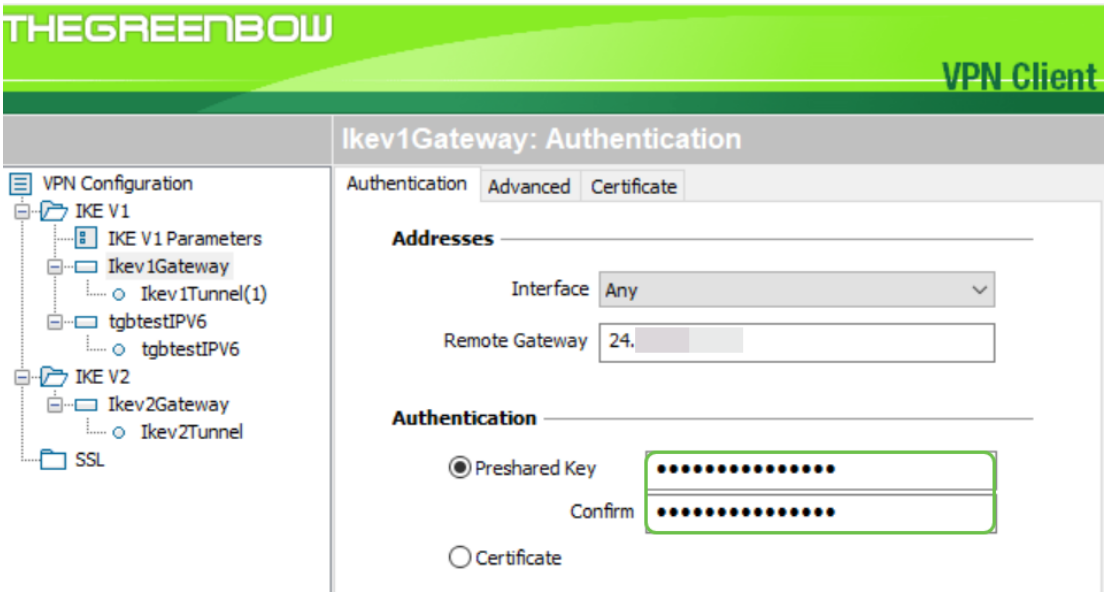
Stap 9. Voer het adres van de externe gateway in het veld *Remote Gateway in*. Dit kan een IP-adres of een DNS-naam zijn. Dit is het adres van het openbare IP-adres voor router op de site

(kantoor).



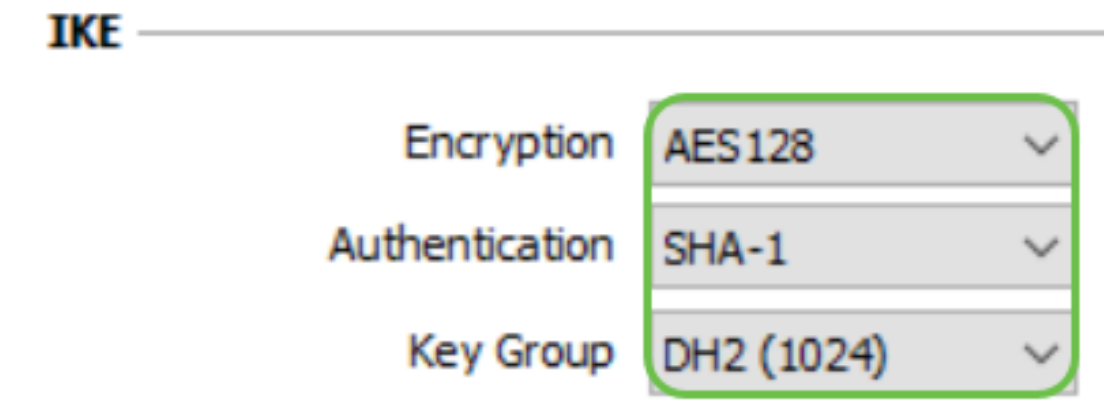
Stap 10. Onder *Verificatie* kiest u het verificatietype. De opties zijn:

- Voorgedeelde sleutel — Deze optie laat de gebruiker een wachtwoord gebruiken dat is ingesteld op de VPN-poort. Het wachtwoord moet door de gebruiker worden aangepast om een VPN-tunnel te kunnen maken.
- Certificaat - Deze optie zal een certificaat gebruiken om de handdruk tussen de VPN-client en de VPN-gateway te voltooien.

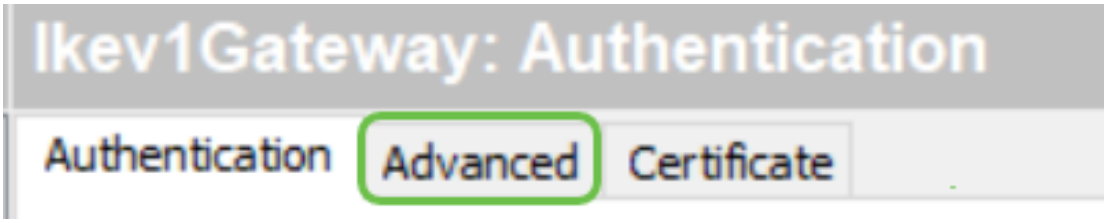


Opmerking: In dit voorbeeld, werd de Pre-Shared Key ingevoerd die op de router was geconfigureerd en bevestigd.

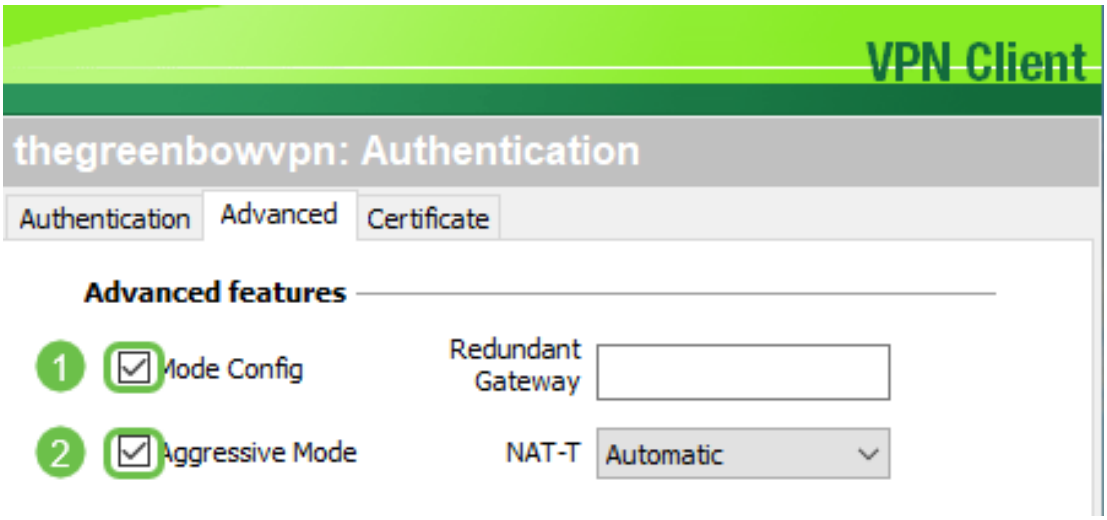
Stap 1. Onder *IKE*, stelt u de instellingen Encryptie, verificatie en sleutelgroep in om de configuratie van de router aan te passen.



Stap 12. Klik op het tabblad **Geavanceerd**.

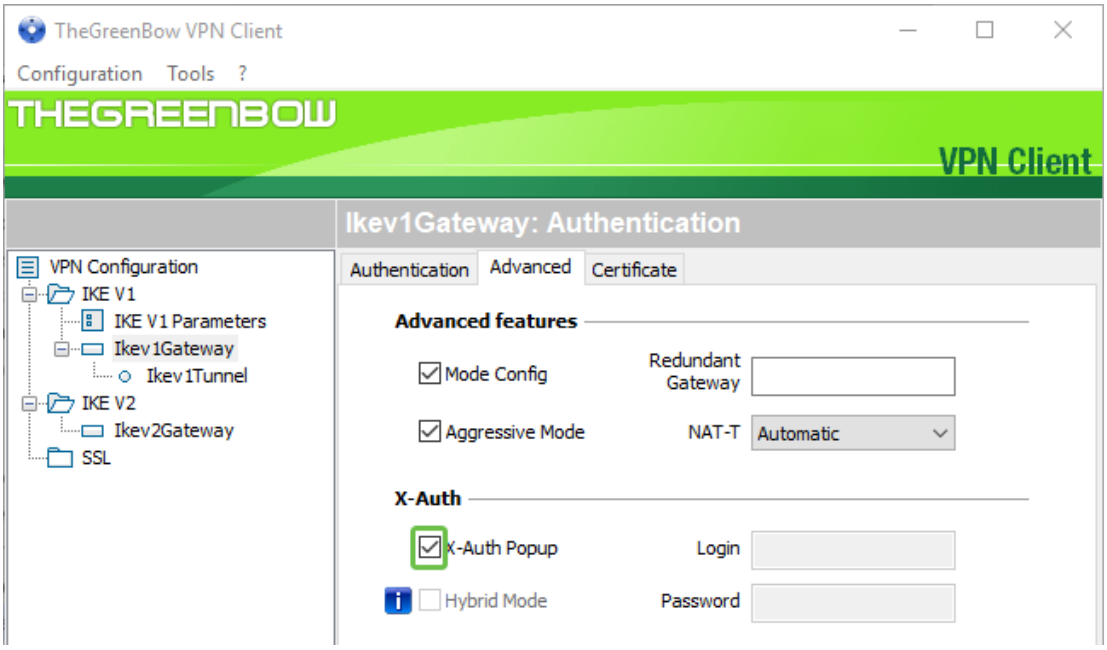


Stap 13. Controleer onder Geavanceerde functies het vakje **Mode Config** en de **Aggressief Mode**. De agressieve modus werd op de RV160 geselecteerd in het client-to-site profiel van dit voorbeeld. Laat de NAT-T-instelling automatisch instellen.

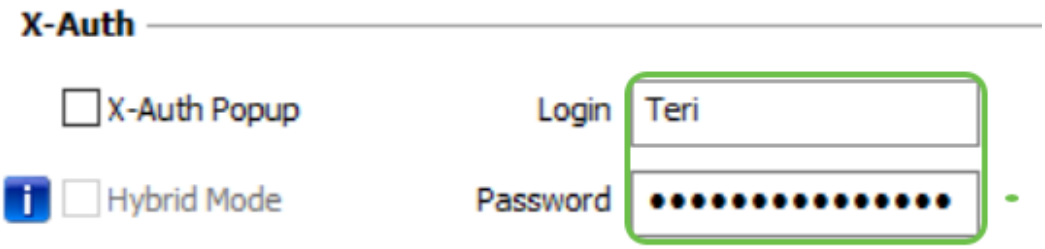


Opmerking: Als Mode Config ingeschakeld is, trekt de client voor GreenBow VPN instellingen uit de VPN-gateway om te proberen een tunnel op te zetten. NAT-T maakt het sneller opzetten van een verbinding.

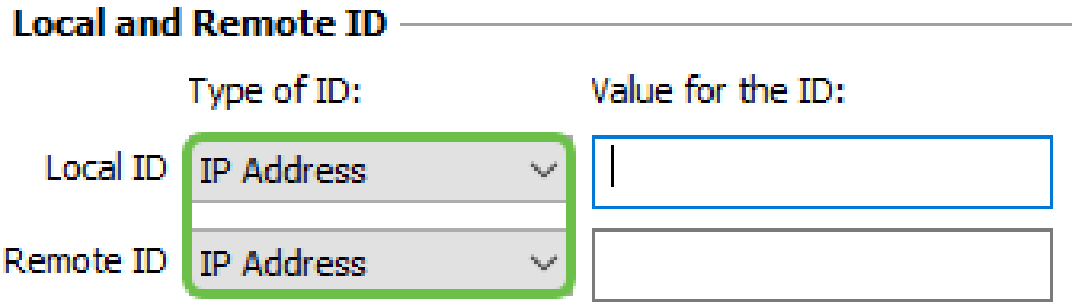
Stap 14. (Optioneel) Onder *X-Auth* kunt u het aanvinkvakje **X-Auth Popup** aanvinken om automatisch het inlogvenster op te trekken wanneer u een verbinding start. In het inlogvenster gaat de gebruiker hun aanmeldingsgegevens in om de tunnel te kunnen voltooien.



Stap 15. (Optioneel) Als u *X-Auth Popup* niet selecteert, specificeert u uw gebruikersnaam in het veld *Aanmelden*. Dit is de gebruikersnaam die is ingevoerd toen een gebruikersaccount is aangemaakt in de VPN-gateway en het wachtwoord op de site.

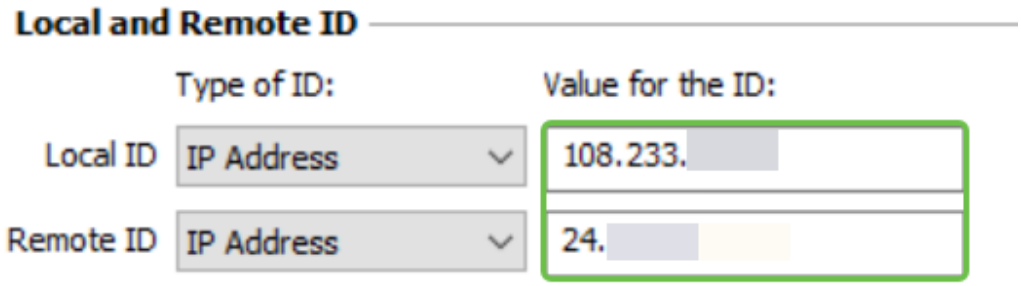


Stap 16. Onder *Local en Remote ID* stelt u de lokale ID en de Remote-ID in om de instellingen van de VPN-gateway aan te passen.

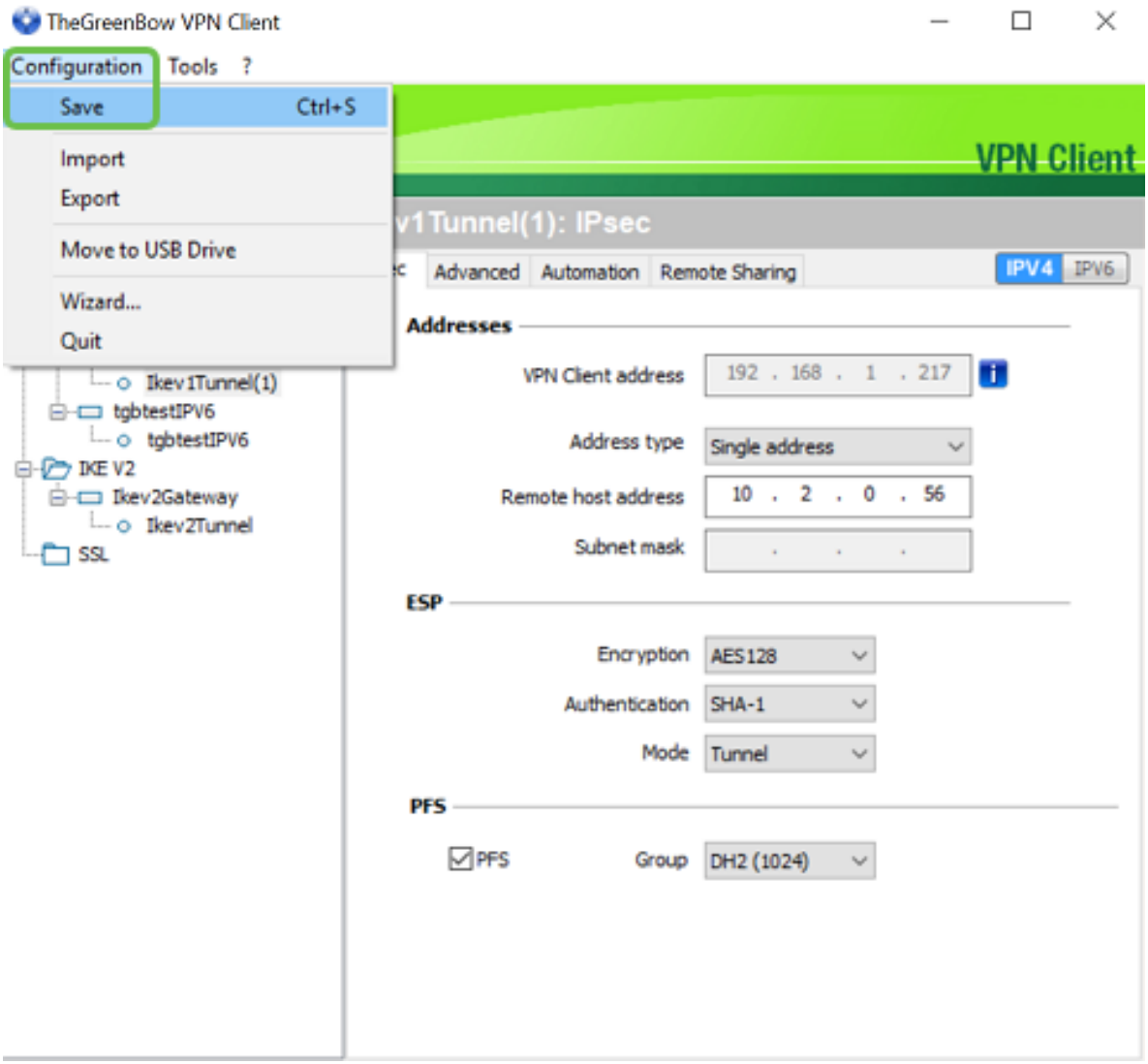


Opmerking: In dit voorbeeld, worden zowel Lokale ID als Remote-ID ingesteld op IP-adres om de instellingen van de RV160- of RV260 VPN-poort aan te passen.

Stap 17. Onder *Waarde voor de ID*, voer de lokale ID en de externe ID in hun respectieve velden in. De lokale ID is het WAN IP-adres voor de client. Dit is te vinden door op internet te zoeken naar "Wat is mijn IP". De externe ID is het WAN IP-adres van de router op de site.

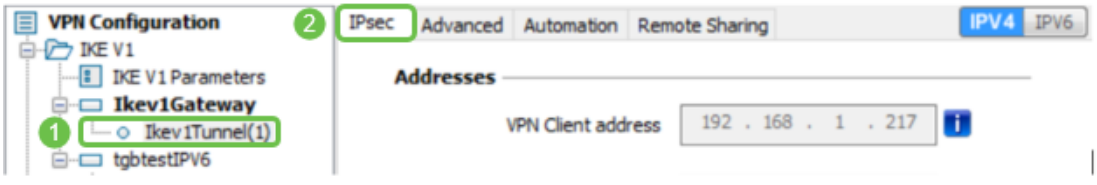


Stap 18. Klik op **Configuration** en kies **Opslaan**.



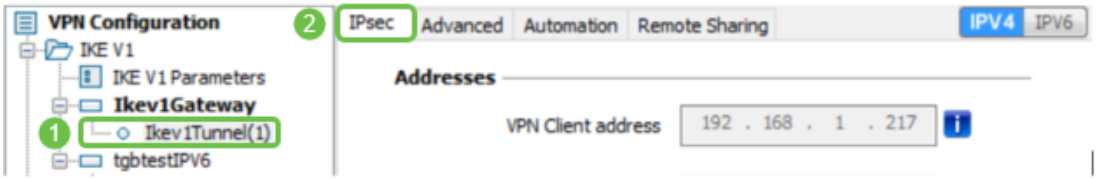
Tunnelinstellingen configureren

Stap 1. Klik op het **IKev1Tunnel(1)** (uw naam kan een andere naam hebben) en het **IPsec** tabblad. Het VPN-clientadres wordt automatisch ingevuld als u Modus Config in de geavanceerde instellingen van Ikev1Gateway hebt geselecteerd. Dit toont het lokale IP adres van de computer/laptop op de verre plaats.



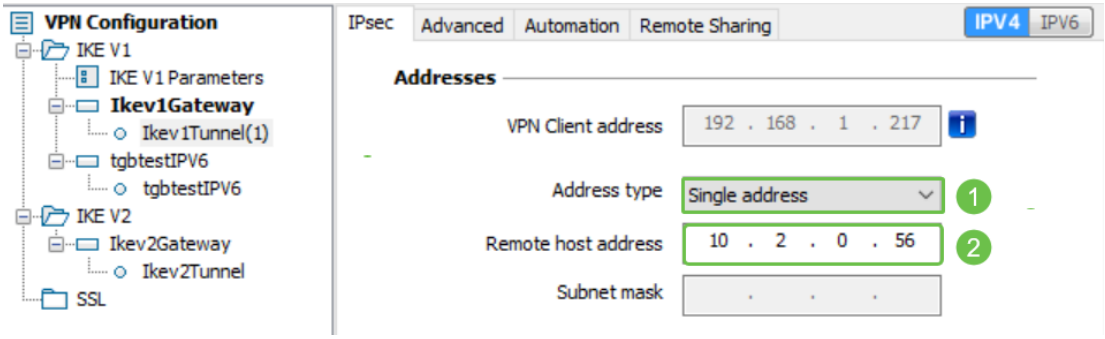
Stap 2. Kies het adrestype dat de VPN-client toegang kan hebben van de vervolgkeuzelijst *Adres*

type. Dit kan een enkel adres, bereik van adressen of een Subnet adres zijn. Het standaard-, subnetadres, bevat automatisch het VPN-clientadres (het lokale IP-adres van de computer), het Remote LAN-adres en het subnetmasker. Als één adres of bereik van adressen is geselecteerd, moeten deze velden handmatig worden ingevuld. Voer het netwerkadres in dat door de VPN-tunnel benaderd moet worden in het veld *Remote LAN-adres* en het subnetmasker van het externe netwerk in het veld *Subnet-masker*.

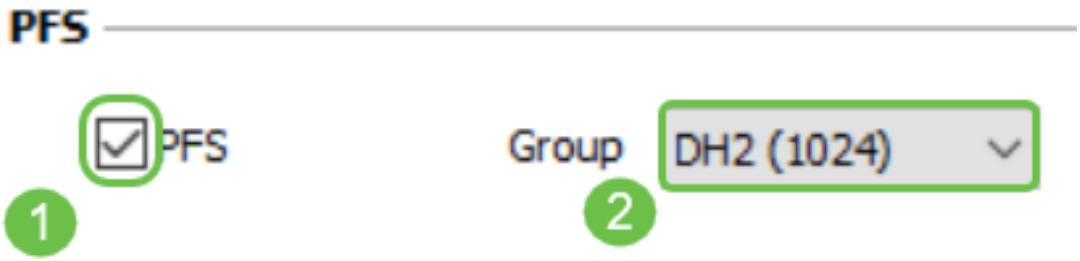


Opmerking: In dit voorbeeld, werd het Enkele adres geselecteerd en het lokale IP adres van de router op de plaats binnendringen.

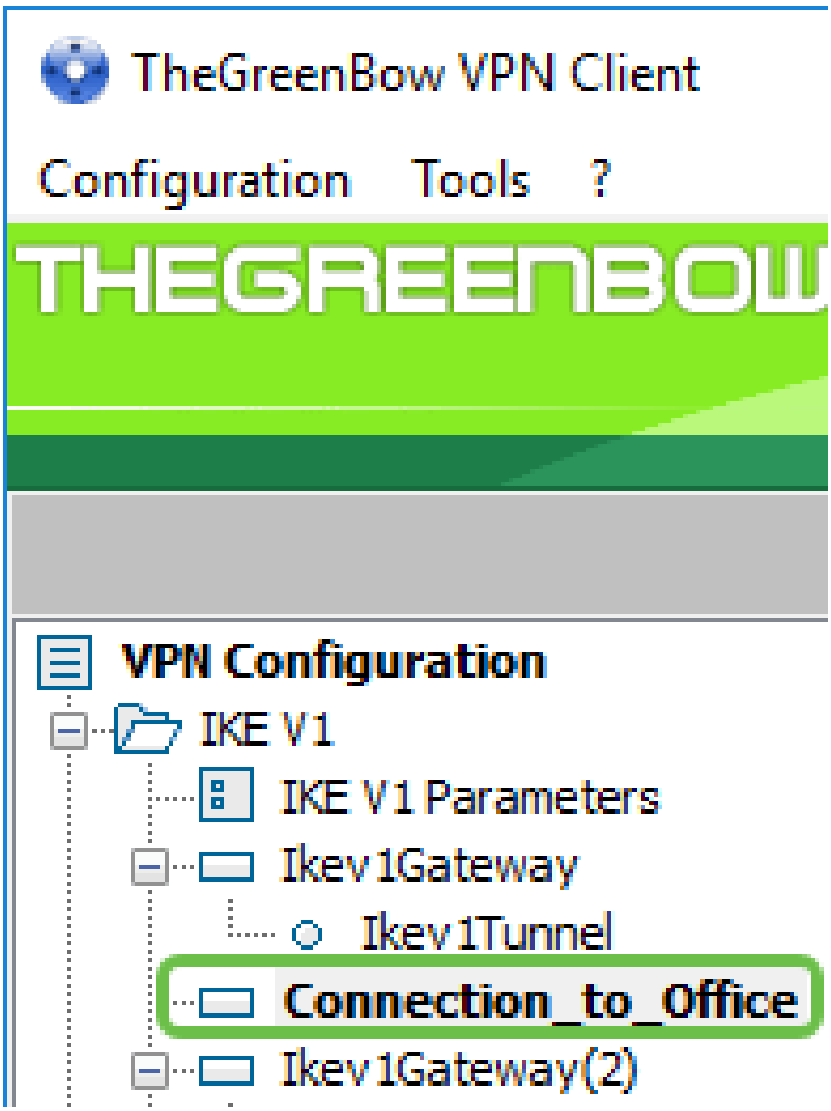
Stap 3. Onder *ESP*, stelt u de encryptie, verificatie en modus in om de instellingen van de VPN-gateway op de site (Office) aan te passen.



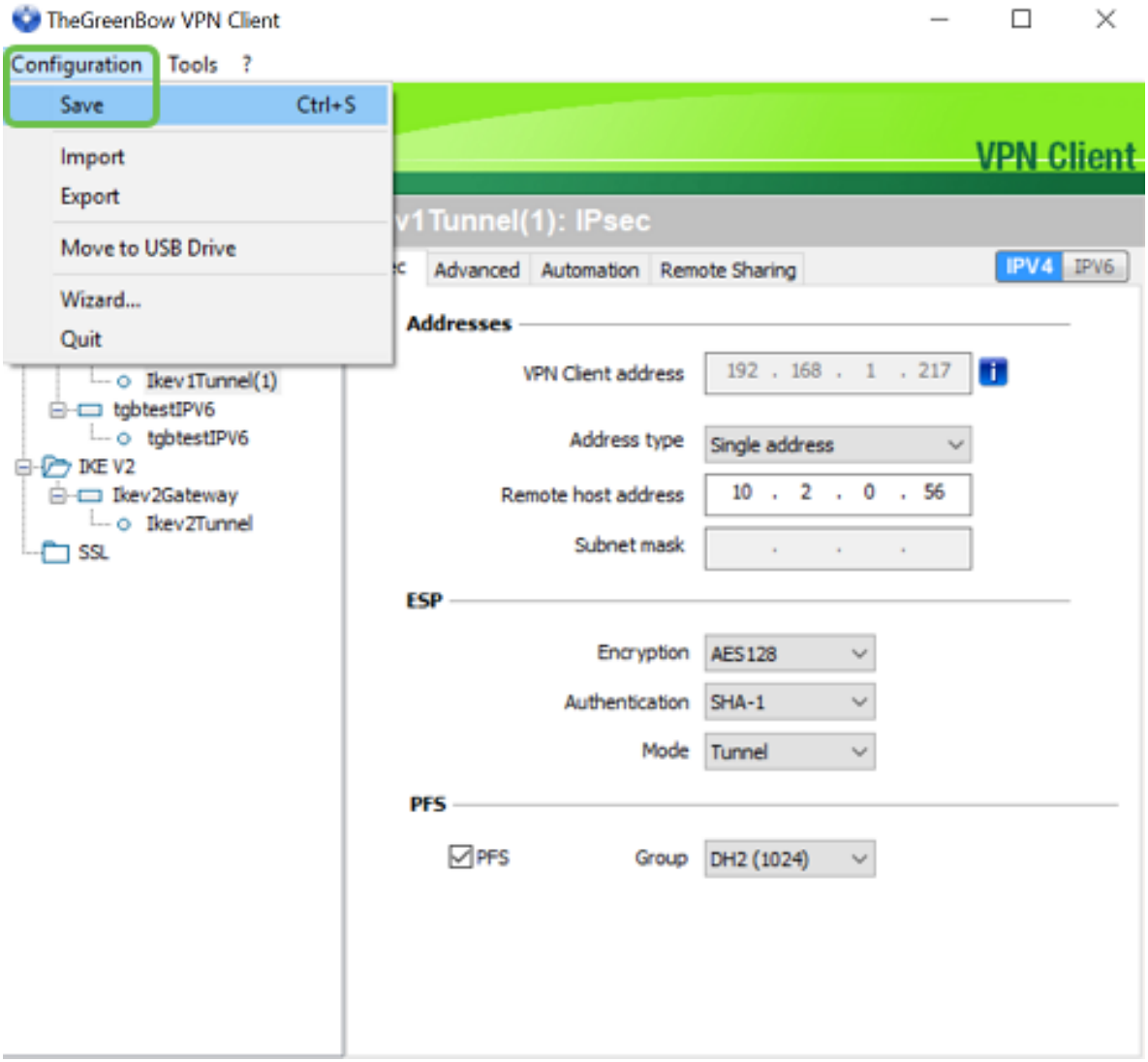
Stap 4. (Optioneel) Onder *PFS*, vinkt u het aankruisvakje **PFS** aan om Perfect Forward Security (PFS) mogelijk te maken. PFS genereert willekeurige toetsen om de sessie te versleutelen. Selecteer een PFS-groepsinstelling in de vervolgkeuzelijst *Groep*. Als deze op de router was ingeschakeld, zou deze ook hier kunnen worden ingeschakeld.



Stap 5. (Optioneel) Klik met de rechtermuisknop op de naam van de Ikev1Gateway en klik op de sectie Hernoemen als u het wilt hernoemen.



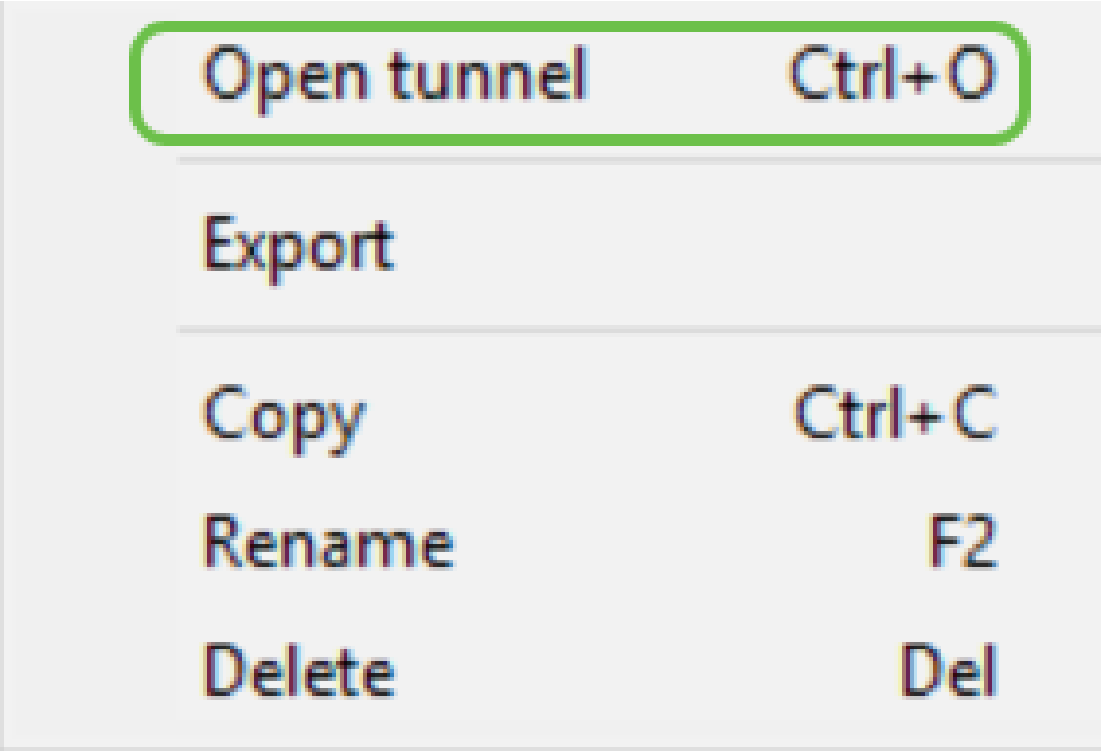
Stap 6. Klik op **Configuration** en kies **Opslaan**.



U had nu met succes de GreenBow VPN-client moeten configureren om verbinding te maken met de RV160- of RV260-router door VPN.

Een VPN-verbinding als client starten

Stap 1. Aangezien u The GreenBow open hebt, kunt u met de rechtermuisknop op de tunnel klikken en **Open Tunnel** selecteren **om met een verbinding te beginnen**.

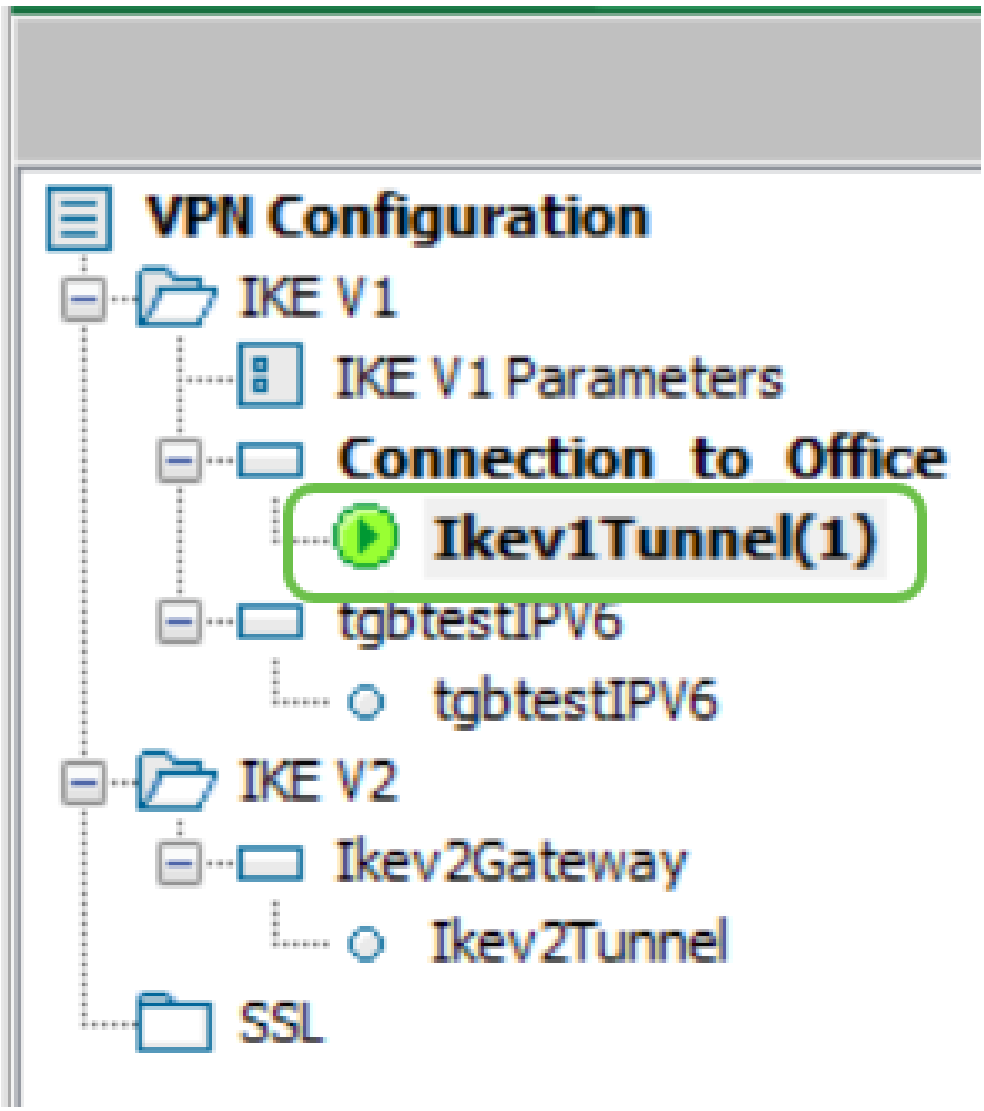


Opmerking: Je kunt ook een tunnel openen door te dubbelklikken op de tunnel.

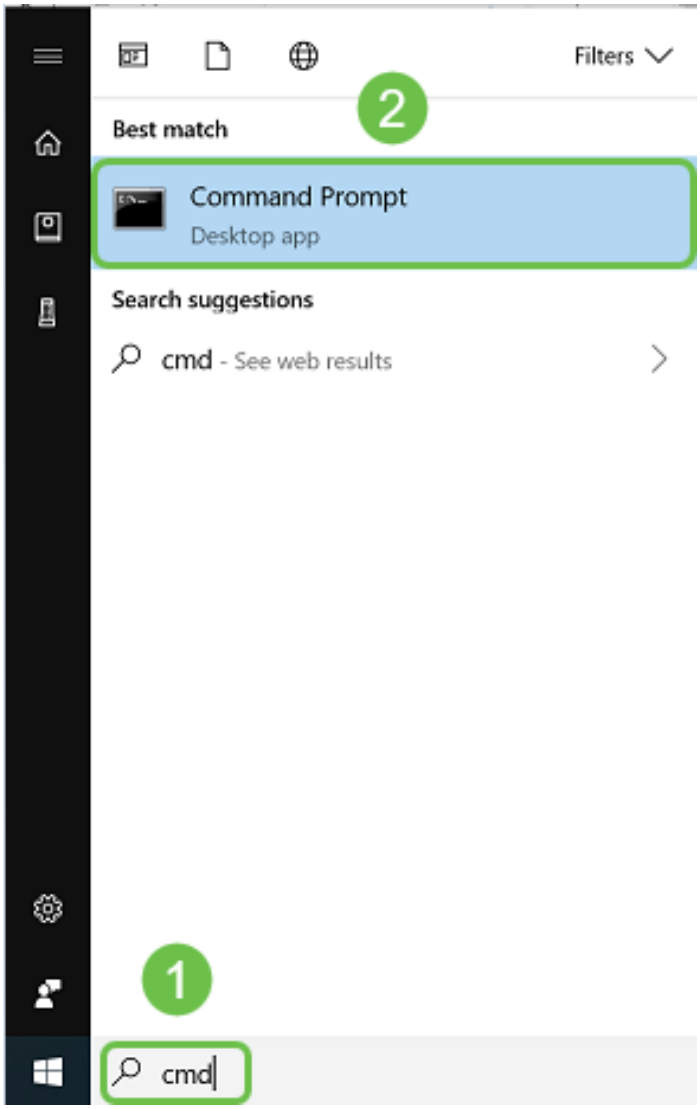
Stap 2. (Optioneel) Als u een nieuwe sessie start en The GreenBow hebt gesloten, klikt u op **het** pictogram **GreenBow VPN**-client aan de rechterkant van het scherm.

Stap 3. (Optioneel) Deze stap is alleen nodig als u een nieuwe sessie installeert en Stap 2 volgt. Kies de VPN-verbinding die u moet gebruiken en klik op **OPEN**. De VPN-verbinding moet automatisch worden gestart.

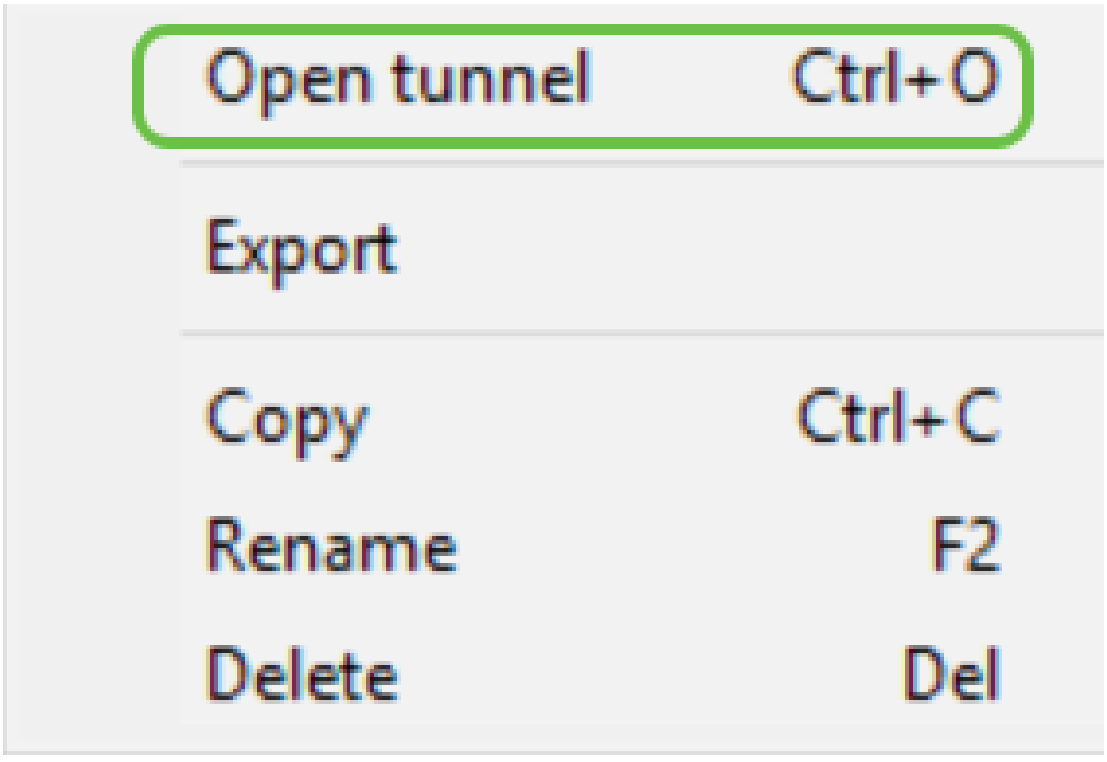
Stap 4. Wanneer de tunnel is aangesloten, verschijnt er een groene cirkel naast de tunnel. Als u een uitroepteken ziet, kunt u erop klikken om de fout te vinden.



Stap 5. (Optioneel) Om te controleren of u aangesloten bent, krijgt u toegang tot de opdrachtmelding vanaf de clientcomputer.



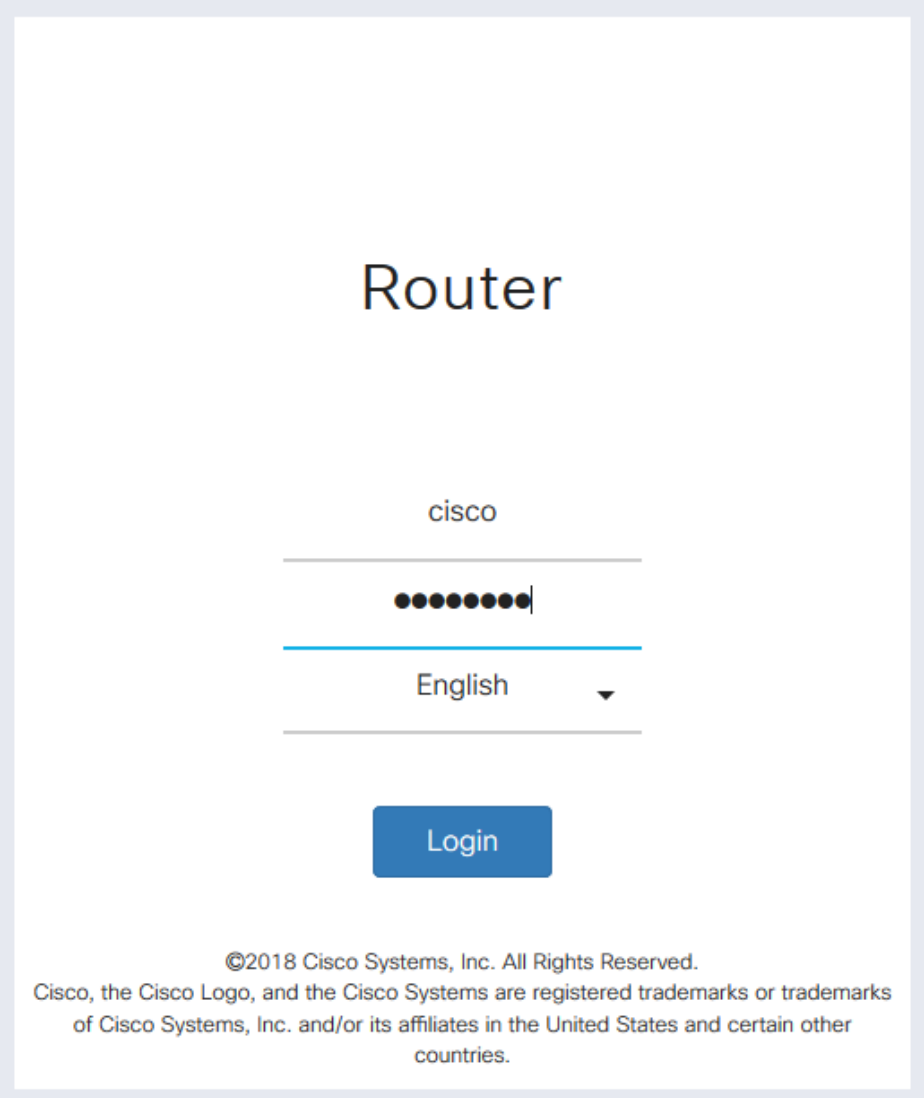
Stap 6. (Optioneel) Voer ping in en selecteer vervolgens het particuliere LAN-adres van de router op de site. Als u antwoorden ontvangt, bent u verbonden.



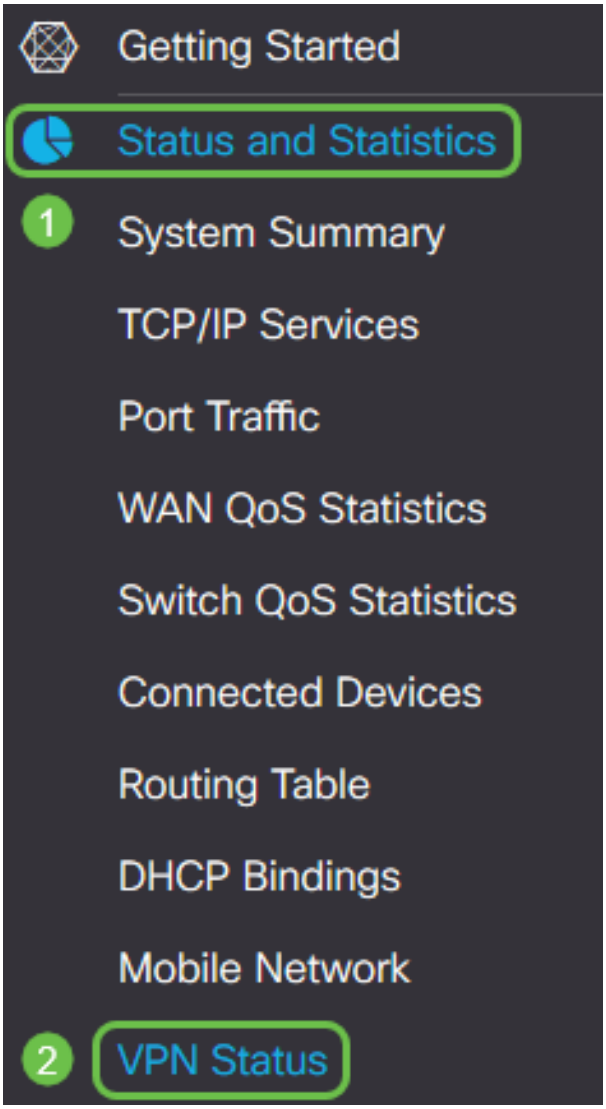
Controleer VPN-status

Controleer de VPN-status op de site

Stap 1. Meld u aan bij het webgebaseerde gebruik van de VPN-gateway van de RV160 of RV260.



Stap 2. Kies **Status en Statistieken > VPN-status**.

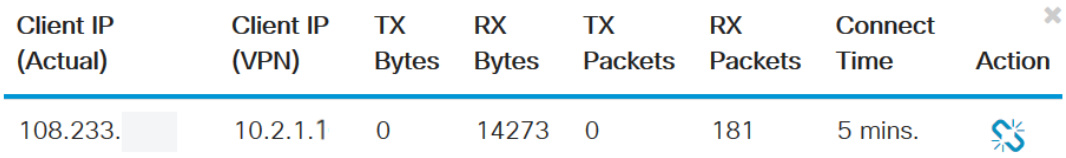


Stap 3. *Controleer* onder *de status Client-to-Site Tunnel* de kolom *Connections* van de *verbindingstabel*. De VPN-verbinding moet worden bevestigd.

Stap 4. Klik op het pictogram in het **oog** om meer informatie te zien.

Stap 5. De details van de client-naar-site VPN-status worden hier weergegeven. U zal het WAN IP-adres van de client waarnemen, het lokale IP-adres dat is toegewezen in de pool van adressen die bij een instelling zijn ingesteld. Het toont ook bytes en pakketten die worden verzonden en

ontvangen evenals de verbindingstijd. Als u de client wilt loskoppelen, klikt u onder *Actie* op het blauwe **gebroken kettingpictogram**. Klik in de rechterbovenhoek op **x** om na inspectie te sluiten.



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.	

Conclusie

U moet nu met succes de VPN-verbinding op de RV160- of RV260-router hebben ingesteld en geverifieerd en de GreenBow VPN-client is geconfigureerd voor verbinding met de router door VPN.