

Gebruik de GreenBow VPN-client voor een verbinding met RV34x Series router

Bijzondere opmerking: Licentiestructuur - Firmware versies 1.0.3.15 en hoger. AnyConnect wordt in voorwaartse richting gebruikt voor alleen licenties op klanten.

Ga voor extra informatie over AnyConnect-licenties op de RV340-Series routers naar het artikel [AnyConnect-licenties voor de RV340 Series routers](#).

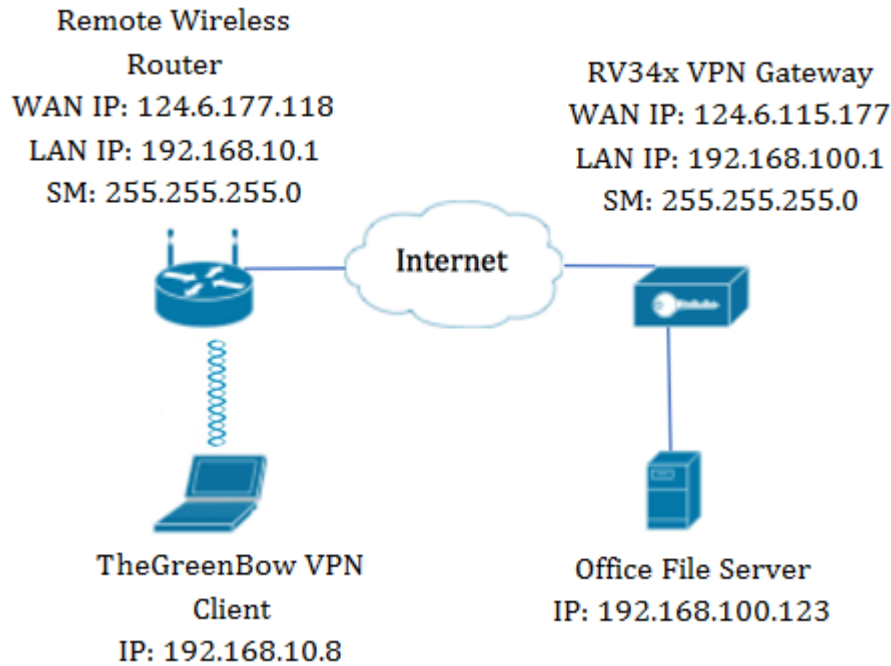
Inleiding

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 vooral van 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 toe te handelen alsof ze zich op hetzelfde lokale netwerk bevonden. De router ondersteunt maximaal 50 tunnels. Een VPN-verbinding kan tussen de router en een eindpunt worden ingesteld nadat de router voor internetverbinding is geconfigureerd. De VPN-client is volledig afhankelijk van de instellingen van de VPN-router om een verbinding op te zetten.

De client voor GreenBow VPN is een client-applicatie van derden die het voor een host-apparaat mogelijk maakt om een beveiligde verbinding te configureren voor een site-to-site IPSec-tunnel met de RV34x Series router.



In het diagram zal de computer verbinding maken met de bestandserver in het kantoor buiten het netwerk om toegang te krijgen tot de bronnen. Om dit te doen zal de GreenBow VPN-client in de computer zo worden geconfigureerd dat deze de instellingen haalt uit de RV34x VPN-gateway.

Voordelen van het gebruik van een VPN-verbinding

1. Gebruik van een VPN-verbinding om vertrouwelijke netwerkgegevens en -bronnen te beschermen.
2. Het zorgt voor gemak en toegankelijkheid voor externe werknemers of bedrijfsmedewerkers, aangezien zij gemakkelijk toegang zullen hebben tot het hoofdbureau zonder fysiek aanwezig te moeten zijn en toch de beveiliging van het particuliere netwerk en de bijbehorende middelen behouden.
3. Communicatie via een VPN-verbinding biedt een hoger beveiligingsniveau dan andere methoden voor communicatie op afstand. Dankzij de geavanceerde technologie kan dit nu ook, en dus tegen ongeoorloofde toegang, het particuliere netwerk worden beschermd.
4. De werkelijke geografische locatie van de gebruikers wordt beschermd en niet blootgesteld aan het publiek of gedeelde netwerken zoals het internet.
5. Het toevoegen van nieuwe gebruikers of groepen gebruikers aan het netwerk is gemakkelijk aangezien VPN's gemakkelijk schaalbaar zijn. Het is mogelijk om het netwerk te laten groeien zonder de behoefte aan extra componenten of gecompliceerde configuratie.

Risico's van het gebruik van een VPN-verbinding

1. Beveiligingsrisico 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.
2. Betrouwbaarheid. 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.

3. schaalbaarheid. In een situatie waarin er 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.
4. Beveiligingsproblemen voor mobiele apparaten. Wanneer het van start gaat van de VPN-verbinding op een mobiel apparaat, kunnen zich beveiligingsproblemen voordoen, vooral wanneer het mobiele apparaat draadloos is aangesloten op het lokale netwerk.
5. Lage verbindingssnelheden. 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.

Voorwaarden voor het gebruik van de GreenBow VPN-client

De volgende items moeten eerst op de VPN-router worden geconfigureerd en zullen worden toegepast op de Groene VPN-client door [hier](#) te klikken om een verbinding tot stand te brengen.

1. [Een client-naar-site profiel maken via de VPN-gateway](#)
2. [Een gebruikersgroep maken in de VPN-gateway](#)
3. [Gebruikersaccount maken via de VPN-gateway](#)
4. [Een IPSec-profiel maken op de VPN-gateway](#)
5. [Configureer de instellingen van fase I en fase II op de VPN-gateway](#)

Toepasselijke apparaten

- RV34x Series

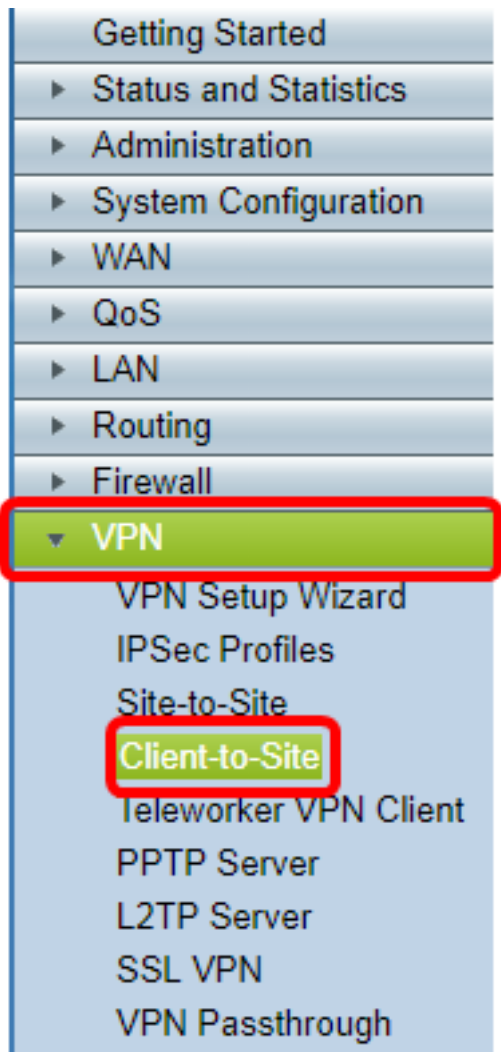
Softwareversie

- 1.0.01.17

De GroeneBoog VPN-client gebruiken

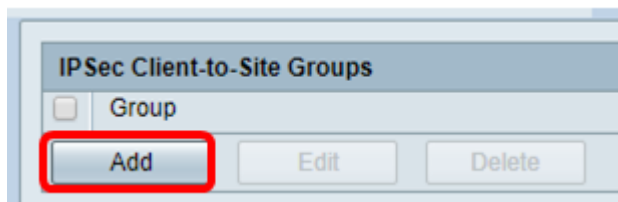
[Een client-naar-site profiel op de router maken](#)

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van de RV34x-router en kies **VPN > Client-to-Site**.



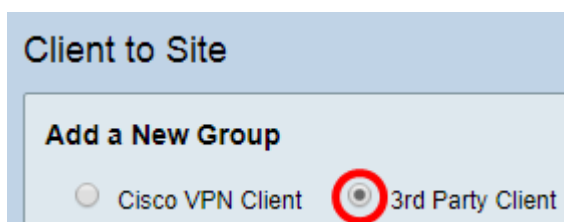
Opmerking: De beelden in dit artikel worden genomen van de RV340 router. De opties kunnen variëren, afhankelijk van het model van het apparaat.

Stap 2. Klik op **Add**.



Stap 3. Klik op **client van derden**.

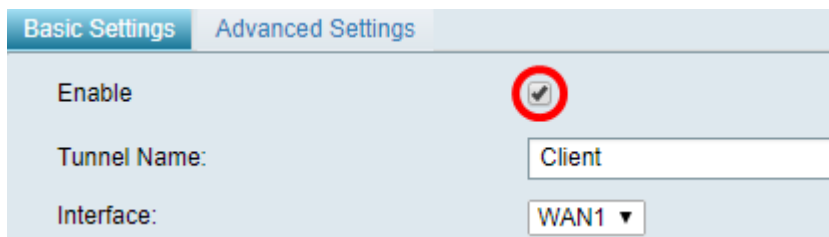
Opmerking: AnyConnect is een voorbeeld van een Cisco VPN-client, terwijl de GreenBow VPN-client een voorbeeld is van een VPN-client van derden.



Opmerking: In dit voorbeeld wordt de client van de derde partij gekozen.

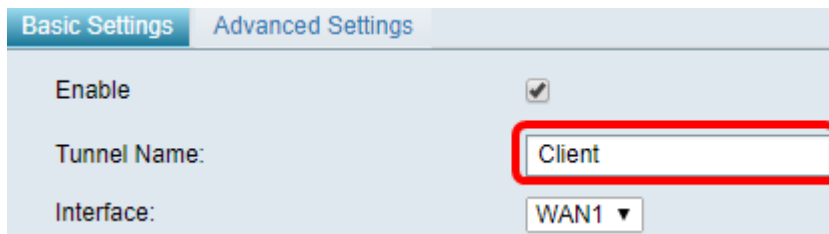
Stap 4. Onder het tabblad Basis-instellingen, controleert u het vakje **Enable** om er zeker van

te zijn dat het VPN-profiel actief is.



The screenshot shows the 'Basic Settings' tab for a VPN configuration. The 'Enable' checkbox is checked and circled in red. The 'Tunnel Name' field contains the text 'Client'. The 'Interface' dropdown menu is set to 'WAN1'.

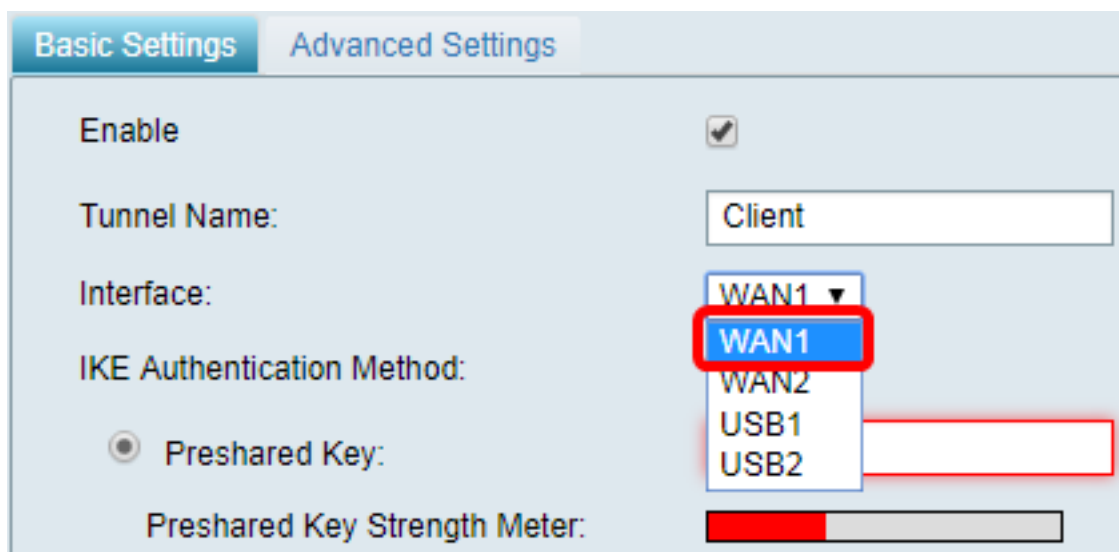
Stap 5. Voer een naam in voor de VPN-verbinding in het veld *Tunnelnaam*.



The screenshot shows the 'Basic Settings' tab. The 'Enable' checkbox is checked. The 'Tunnel Name' text input field, containing 'Client', is highlighted with a red rectangular border. The 'Interface' dropdown menu is set to 'WAN1'.

Opmerking: In dit voorbeeld wordt **Client** ingevoerd.

Stap 6. Kies de te gebruiken interface in de vervolgkeuzelijst Interfacegebied. De opties zijn WAN1, WAN2, USB1 en USB2, die de corresponderende interface op de router voor de VPN-verbinding zullen gebruiken.



The screenshot shows the 'Basic Settings' tab. The 'Enable' checkbox is checked. The 'Tunnel Name' field contains 'Client'. The 'Interface' dropdown menu is open, showing options: WAN1 (highlighted with a blue background and a red border), WAN2, USB1, and USB2. The 'IKE Authentication Method' section shows 'Preshared Key' selected with a radio button. Below it is a 'Preshared Key Strength Meter' with a red bar indicating strength.

Opmerking: De opties hangen af van het model van de router die u gebruikt. In dit voorbeeld wordt WAN1 geselecteerd.

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

- Voorgedeelde 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.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Certificate:

Opmerking: In dit voorbeeld wordt PreShared Key gekozen.

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

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

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

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Opmerking: In dit voorbeeld, wordt de Minimale Gedeelde Belangrijkste Complexiteit links ingeschakeld.

Stap 10. (Optioneel) Controleer de onbewerkte tekst tonen wanneer u het vakje Inschakelen bewerkt om het wachtwoord in onbewerkte tekst weer te geven.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

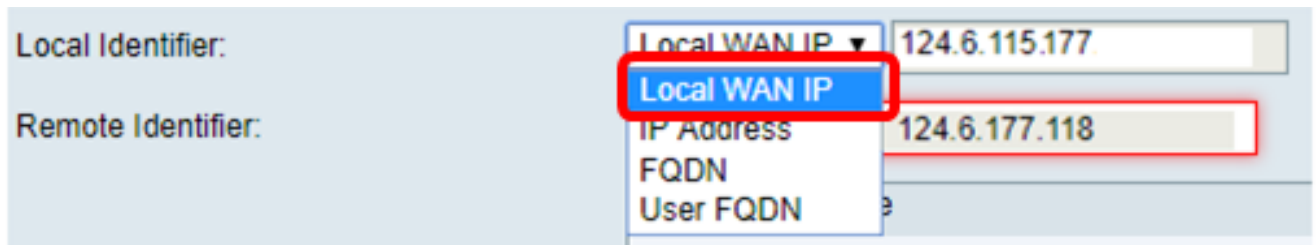
Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Opmerking: In dit voorbeeld, toon onbewerkte tekst wanneer de bewerking is 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.
- 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.

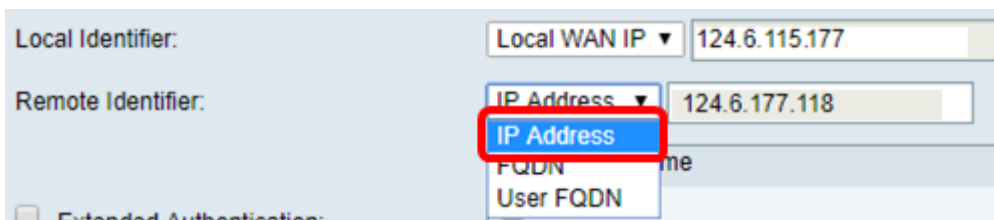


The screenshot shows the 'Local Identifier' dropdown menu. The 'Local WAN IP' option is selected and highlighted with a red box. The text 'Local WAN IP' is also visible in the dropdown list. The text '124.6.115.177' is visible in the input field next to the dropdown. The text 'Remote Identifier:' is visible below the dropdown. The text 'IP Address' and '124.6.177.118' are visible in the input field next to the dropdown. The text 'FQDN' and 'User FQDN' are visible in the dropdown list.

Opmerking: In dit voorbeeld wordt IP van lokaal WAN geselecteerd. Met deze optie wordt de lokale WAN IP automatisch gedetecteerd.

Stap 12. (Optioneel) Kies een identificator voor de externe host. De opties zijn:

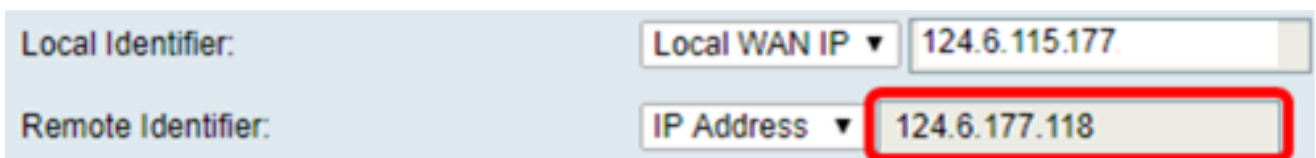
- IP-adres - Deze optie gebruikt het WAN IP-adres van de VPN-client.
- FQDN - Met deze optie kunt u een volledige domeinnaam voor een specifieke computer op het internet gebruiken.
- Gebruiker FQDN - Met deze optie kunt u een volledige domeinnaam voor een specifieke gebruiker op het internet gebruiken.



The screenshot shows the 'Remote Identifier' dropdown menu. The 'IP Address' option is selected and highlighted with a red box. The text 'IP Address' is also visible in the dropdown list. The text '124.6.177.118' is visible in the input field next to the dropdown. The text 'Local Identifier:' is visible above the dropdown. The text 'Local WAN IP' and '124.6.115.177' are visible in the input field next to the dropdown. The text 'FQDN' and 'User FQDN' are visible in the dropdown list. The text 'Extended Authentication:' is visible below the dropdown.

Opmerking: In dit voorbeeld, wordt het IP Adres gekozen.

Stap 13. Voer de externe identificator in het veld *Remote Identifier* in.



The screenshot shows the 'Remote Identifier' input field. The text '124.6.177.118' is entered in the input field and highlighted with a red box. The text 'Local Identifier:' is visible above the input field. The text 'Local WAN IP' and '124.6.115.177' are visible in the input field next to the dropdown. The text 'IP Address' is visible in the dropdown list. The text 'FQDN' and 'User FQDN' are visible in the dropdown list. The text 'Extended Authentication:' is visible below the input field.

Opmerking: In dit voorbeeld wordt 124.6.115.177 opgenomen.

Stap 14. (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.

Extended Authentication:

Group Name

Add Delete

Opmerking: In dit voorbeeld blijft uitgebreide verificatie onbeperkt.

Stap 15. Onder groepsnaam klikt u op **Toevoegen**.

Extended Authentication:

Group Name

Add Delete

Stap 16. Kies de groep die uitgebreide verificatie gebruikt in de vervolgkeuzelijst Naam van de groep.

Group Name

admin

admin

guest

IPSecVPN

VPN

Opmerking: In dit voorbeeld wordt VPN geselecteerd.

Stap 17. Onder Pool Range voor Client LAN, Voer het eerste IP-adres in dat aan een VPN-client kan worden toegewezen in het veld *Start IP*.

Pool Range for Client LAN:

Start IP: 10.10.100.100

End IP: 10.10.100.245

Opmerking: In dit voorbeeld wordt 10.10.100.100 ingevoerd.

Stap 18. Voer het laatste IP-adres in dat aan een VPN-client kan worden toegewezen in het veld *End IP*.

Pool Range for Client LAN:

Start IP: 10.10.100.100

End IP: 10.10.100.245

Opmerking: In dit voorbeeld wordt 10.10.100.245 opgenomen.

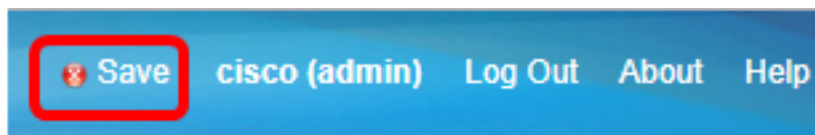
Stap 19. Klik op **Toepassen**.

Pool Range for Client LAN:

Start IP:

End IP:

Stap 20. Klik op **Opslaan**.

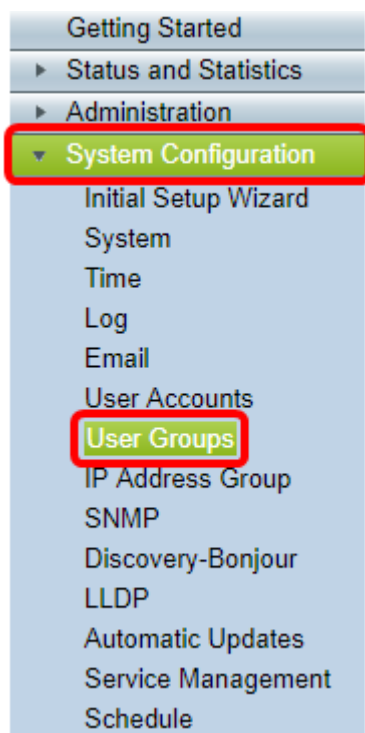


U had nu het Client-to-Site Profile op de router voor The GreenBow VPN-client moeten configureren.

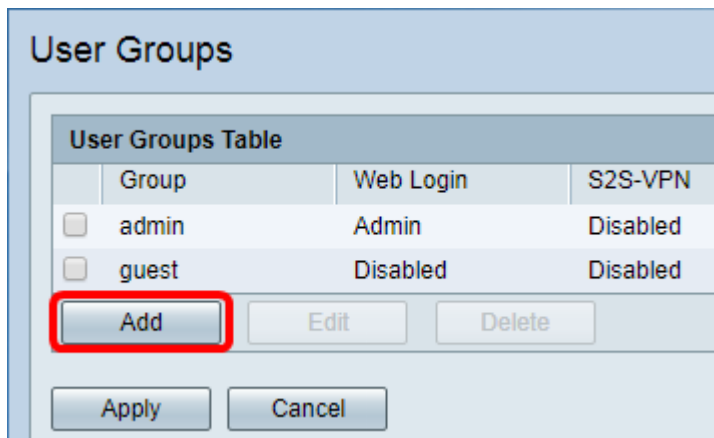
[Een gebruikersgroep maken](#)

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van de router en kies **Systeemconfiguratie > Gebruikersgroepen**.

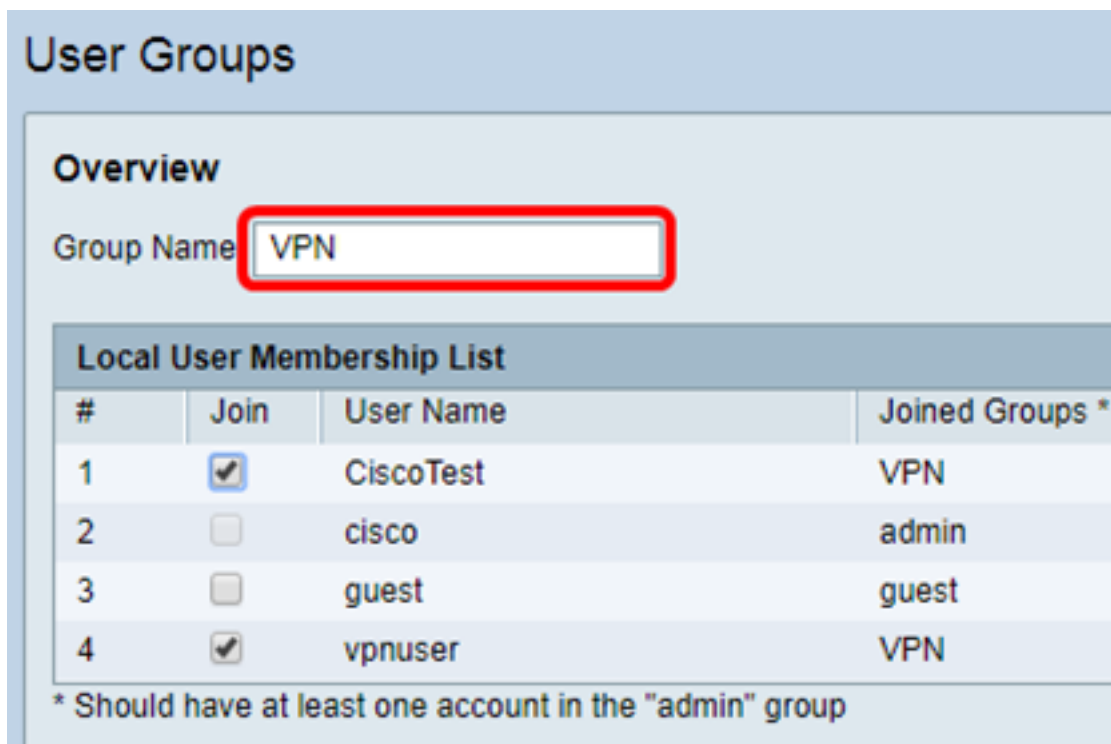
Opmerking: De beelden in dit artikel zijn van een RV340 router. De opties kunnen afhankelijk van het model van het apparaat verschillen.



Stap 2. Klik op **Add** om een gebruikersgroep toe te voegen.



Stap 3. Voer in het gedeelte Overzicht de naam van de groep in het veld *groepsnaam in*.



Opmerking: In dit voorbeeld wordt VPN gebruikt.

Stap 4. Controleer onder de lijst Lokaal lidmaatschap de vinkjes van de gebruikersnamen die in dezelfde groep moeten voorkomen.

User Groups

Overview

Group Name:

Local User Membership List

#	Join	User Name	Joined Groups *
1	<input checked="" type="checkbox"/>	CiscoTest	VPN
2	<input type="checkbox"/>	cisco	admin
3	<input type="checkbox"/>	guest	guest
4	<input checked="" type="checkbox"/>	vpnuser	VPN

* Should have at least one account in the "admin" group

Opmerking: In dit voorbeeld worden CiscoTest en VPN geselecteerd.

Stap 5. Kies onder Services een toestemming die aan de gebruikers in de groep moet worden verleend. 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 alleen kunnen lezen nadat ze zijn aangemeld. Ze kunnen geen van de instellingen bewerken.
- Administrator — Deze optie geeft de leden van de groep lees- en schrijfrechten en kan de systeemstatus configureren.

Services

Web Login Disabled Read Only Administrator

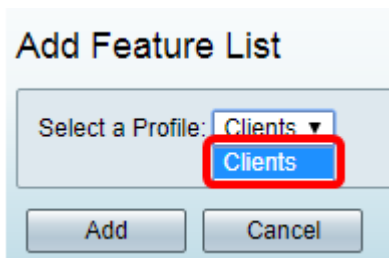
Opmerking: In dit voorbeeld wordt alleen lezen geselecteerd.

Stap 6. Klik in de lijst Lid in gebruik van het profiel van EzVPN/3th Party op **Add**.

EzVPN/3rd Party

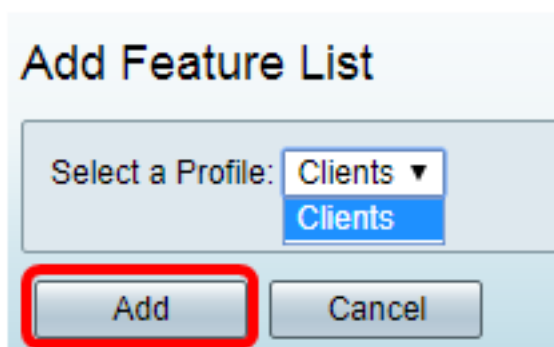
EzVPN/3rd Party Profile Member In-use Table	
#	Group Name

Stap 7. Kies een profiel uit de vervolgkeuzelijst Profiel selecteren. De opties kunnen variëren, afhankelijk van de profielen die op de VPN-gateway zijn geconfigureerd.

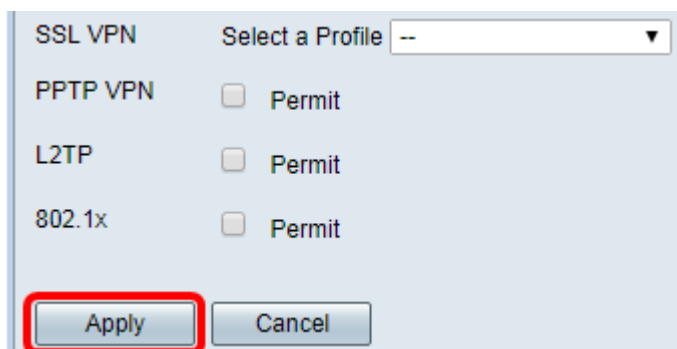


Opmerking: In dit voorbeeld worden de Clients geselecteerd.

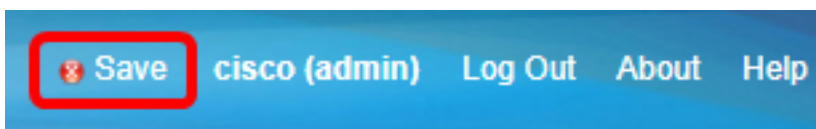
Stap 8. Klik op **Add**.



Stap 9. Klik op **Toepassen**.



Stap 10. Klik op **Opslaan**.

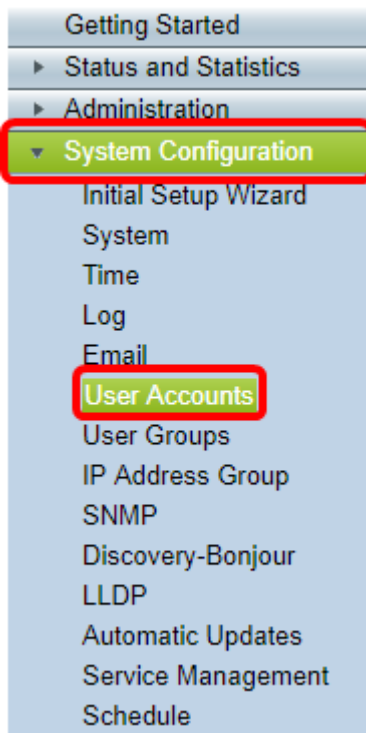


U kunt nu met succes een gebruikersgroep maken op de RV34x Series router.

[Een gebruikersaccount maken](#)

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

Opmerking: De beelden in dit artikel worden genomen van een RV340 router. De opties kunnen afhankelijk van het model van het apparaat verschillen.



Stap 2. Klik in het gedeelte Local User Membership List op **Add**.

User Accounts

Local Users Password Complexity
Password Complexity Settings: Enable

Local Users

Local User Membership List			
<input type="checkbox"/>	#	User Name	Group *
<input type="checkbox"/>	1	guest	VPN
<input type="checkbox"/>	2	cisco	admin

* Should have at least one account in the "admin" group

Stap 3. Voer een naam voor de gebruiker in het veld *Gebruikersnaam in*.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Opmerking: In dit voorbeeld, wordt CiscoTest ingevoerd.

Stap 4. Voer het gebruikerswachtwoord in het veld *Nieuw wachtwoord* in.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Stap 5. Bevestig het wachtwoord in het vakje *Nieuw wachtwoord*.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Stap 6. Kies een groep uit de vervolgkeuzelijst Groep. Dit is de groep waaraan de gebruiker zal worden gekoppeld.

Group

Opmerking: In dit voorbeeld wordt VPN geselecteerd.

Stap 7. Klik op Toepassen.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Stap 8. Klik op Opslaan.



U hebt nu een gebruikersaccount aangemaakt op uw RV34x Series router.

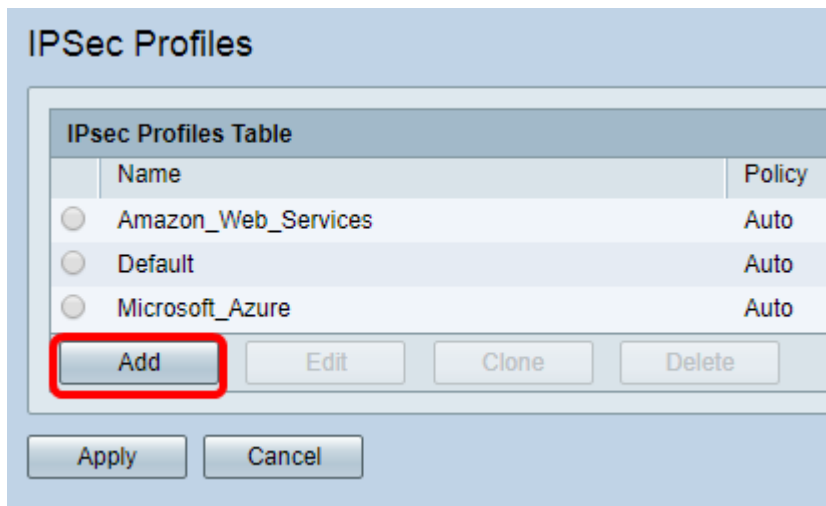
[IPsec-profiel configureren](#)

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van de RV34x-router en kies **VPN > IPSec-profielen**.



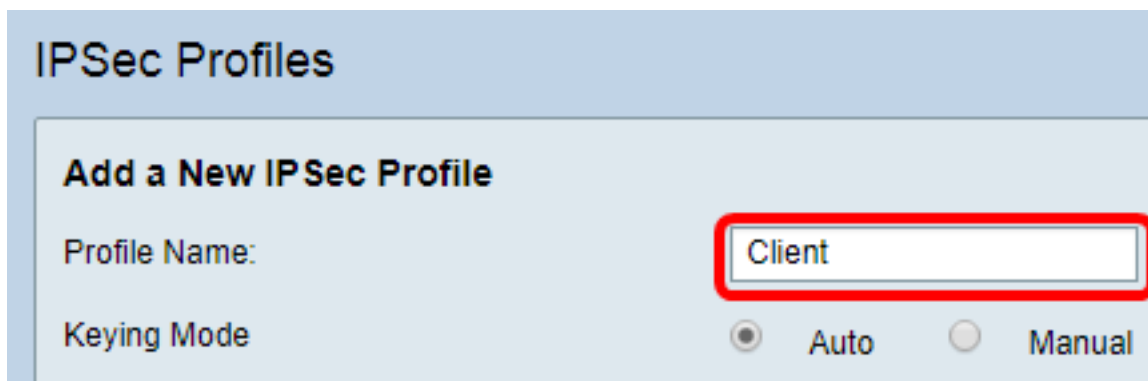
Opmerking: De beelden in dit artikel worden genomen van de RV340 router. De opties kunnen afhankelijk van het model van het apparaat verschillen.

Stap 2. De tabel met IPSec-profielen toont de bestaande profielen. Klik op **Add** 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.



Opmerking: In dit voorbeeld wordt Client ingevoerd.

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. Als deze optie geselecteerd is, slaat u de [auto-instellingen](#) over om [instellingen te configureren](#).
- 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. Als deze optie geselecteerd is, slaat u de [instructies](#) over om [Handmatige instellingen te configureren](#).

IPSec Profiles

Add a New IPSec Profile

Profile Name:

Keying Mode Auto Manual

Opmerking: Auto is bijvoorbeeld geselecteerd.

Instellen fase I en fase II

Stap 1. Selecteer 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.

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime:

Perfect Forward Secrecy: Enable

Opmerking: In dit voorbeeld wordt het bit Group5-1536 gekozen.

Stap 2. Kies een coderingsmethode in de vervolgkeuzelijst Encryptie om de versleuteling en decryptie van 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.
- 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.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: AES-128

SA Lifetime: AES-192
AES-256

Perfect Forward Secrecy: Enable

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. In dit voorbeeld wordt AES-128 gekozen.

Stap 3. Kies in de vervolgkeuzelijst Verificatie een verificatiemethode die bepaalt hoe ESP en ISAKMP worden geauthentificeerd. 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.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: MD5
SHA1

Perfect Forward Secrecy: Enable

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. In het veld *SA Lifetime* voert u een waarde in tussen 120 en 86400. Dit is de duur van de tijd dat de Internet Key Exchange (IKE) Security Association (SA) actief blijft in de fase. De standaardwaarde is 28800.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

Opmerking: In dit voorbeeld wordt 86400 ingevoerd.

Stap 5. (Optioneel) Controleer het aanvinkvakje Perfect Forward SecRITY om een nieuwe sleutel voor IPSec traffic encryptie en verificatie te genereren.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

Opmerking: In dit voorbeeld wordt Perfect Forward SecRITY ingeschakeld.

Stap 6. Kies in de vervolgkeuzelijst Protocol Selectie 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 bevat de gegevens die moeten worden beschermd. Als deze optie is geselecteerd, gaat u naar [Stap 7](#) 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 8](#).

The screenshot shows a dialog box titled "Phase II Options". It contains several configuration fields: "Protocol Selection" is set to "ESP" (highlighted with a red box), "Encryption" is set to "AH", "Authentication" is set to "SHA1", "SA Lifetime" is set to "3600", and "DH Group" is set to "Group5 - 1536 bit". At the bottom, there are "Apply" and "Cancel" buttons.

Opmerking: In dit voorbeeld wordt ESP gekozen.

[Stap 7](#) . Als ESP in stap 6 is geselecteerd, kiest u een verificatiemethode die bepaalt hoe ESP en ISAKMP worden geauthenticeerd. 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.

The screenshot shows the same "Phase II Options" dialog box. The "Protocol Selection" is still "ESP". The "Encryption" dropdown is open, showing "AES-128" (highlighted with a red box), "3DES", "AES-192", and "AES-256". The "Authentication" field is empty. The "SA Lifetime" is "3600" and "DH Group" is "Group5 - 1536 bit". "Apply" and "Cancel" buttons are at the bottom.

Opmerking: In dit voorbeeld wordt AES-128 gekozen.

[Stap 8](#) . Kies een verificatiemethode in de vervolgkeuzelijst Verificatie die bepaalt hoe ESP en ISAKMP worden gewaarmerkt. 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.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

Opmerking: In dit voorbeeld wordt SHA1 gekozen.

Stap 9. In het veld *SA Lifetime* voert u een waarde in tussen 120 en 2800. Dit is de duur van de tijd dat de IKE SA actief zal blijven in deze fase. De standaardwaarde is 3600.

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 trager, maar is veiliger dan Group1.
- Groep5-1536 bit - Deze optie compileert de toets het traagste, maar is de best beveiligde.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

Opmerking: In dit voorbeeld wordt 3600 ingevoerd.

Stap 1. Klik op **Toepassen**.

IPSec Profiles

Add a New IP Sec Profile

Profile Name:

Keying Mode Auto Manual

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime:

Perfect Forward Secrecy: Enable

Phase II Options

Protocol Selection:

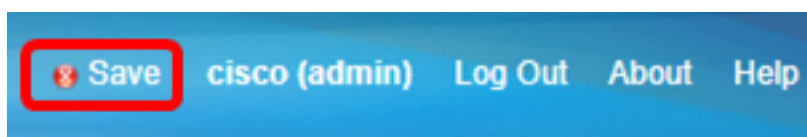
Encryption:

Authentication:

SA Lifetime:

DH Group:

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



U hebt nu een automatisch IPSec profiel op uw RV34x Series router ingesteld.

[De handmatige instellingen configureren](#)

Stap 1. Voer in het veld *SPI-inkomende* veld een hexadecimale waarde in van 100 naar FFFF voor de tag Security Parameter Index (SPI) voor inkomend verkeer op de VPN-verbinding. De SPI-tag wordt gebruikt om het verkeer van de ene sessie te onderscheiden van het verkeer van andere sessies.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Opmerking: In dit voorbeeld wordt 0xABCD ingevoerd.

Stap 2. Voer in het veld *SPI-Uitgaande* een hexadecimale waarde in van 100 naar FFFFFFFF voor de SPI-tag voor uitgaande verkeer op de VPN-verbinding.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Opmerking: In dit voorbeeld wordt 0x1234 ingevoerd.

Stap 3. Kies een coderingswaarde in de vervolgkeuzelijst. 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.

SPI Incoming:

SPI Outgoing:

Encryption:

3DES

AES-128

AES-192

✓ AES-256

Opmerking: In dit voorbeeld wordt AES-256 gekozen.

Stap 4. Voer in het veld *Key-In* een sleutel in voor het inkomende beleid. De lengte van de toets zal afhangen van het algoritme dat in Stap 3 is geselecteerd.

Key-In:

Key-Out:

Opmerking: In dit voorbeeld wordt 123456789123456789123.. opgenomen.

Stap 5. Voer in het veld *Key-Out* een sleutel in voor het uitgaande beleid. De lengte van de toets zal afhangen van het algoritme dat in Stap 3 is geselecteerd.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

Opmerking: In dit voorbeeld, 1a1a1a1a1a1a1a1a1a1a12121212... wordt ingevoerd.

Stap 6. Kies een verificatiemethode in de vervolgkeuzelijst Verificatie. 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.

Authentication:	<input checked="" type="checkbox"/> MD5
Key-In	<input type="checkbox"/> SHA1
Key-Out	<input type="checkbox"/> SHA2-256

Opmerking: In dit voorbeeld wordt MD5 geselecteerd.

Stap 7. Voer in het veld *Key-In* een sleutel in voor het inkomende beleid. De lengte van de toets zal afhangen van het algoritme dat in Stap 6 is geselecteerd.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

Opmerking: In dit voorbeeld wordt 123456789123456789123.. opgenomen.

Stap 8. Voer in het veld *Key-Out* een sleutel in voor het uitgaande beleid. De lengte van de toets zal afhangen van het algoritme dat in Stap 6 is geselecteerd.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

Opmerking: In dit voorbeeld, 1a1a1a1a1a1a1a1a1a1a12121212... wordt ingevoerd.

Stap 9. Klik op .

Stap 10. Klik op **Opslaan** om de configuratie permanent op te slaan.

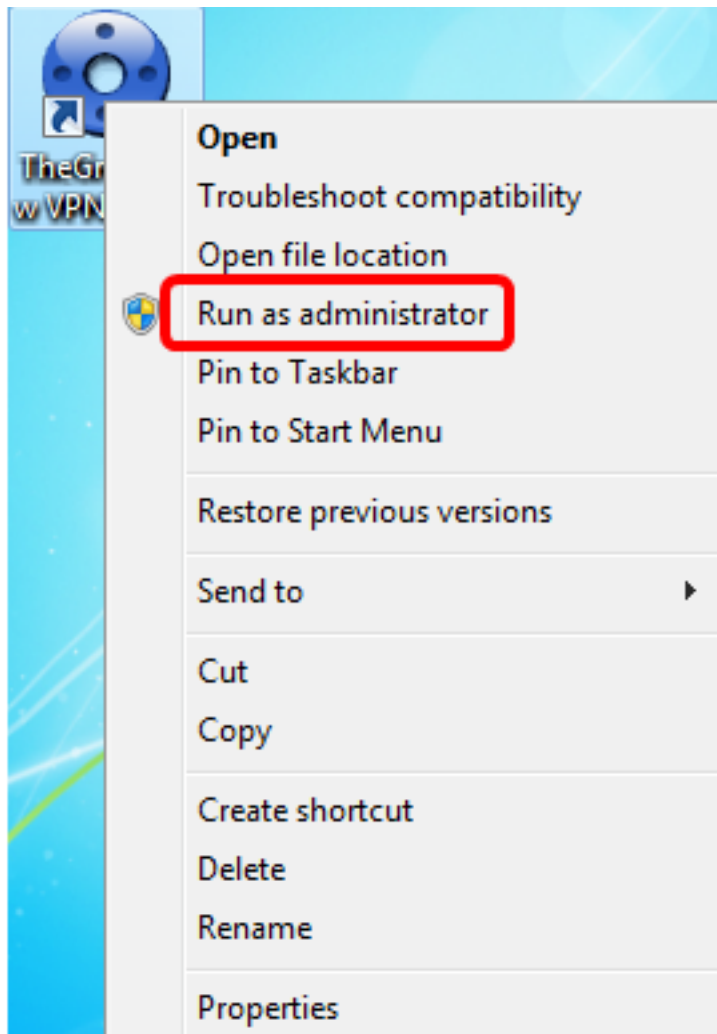
<input checked="" type="button" value="Save"/>	cisco (admin)	Log Out	About	Help
--	-------------------------------	-------------------------	-----------------------	----------------------

U dient nu een handmatig IPSec profiel op een RV34x Series router te hebben ingesteld.

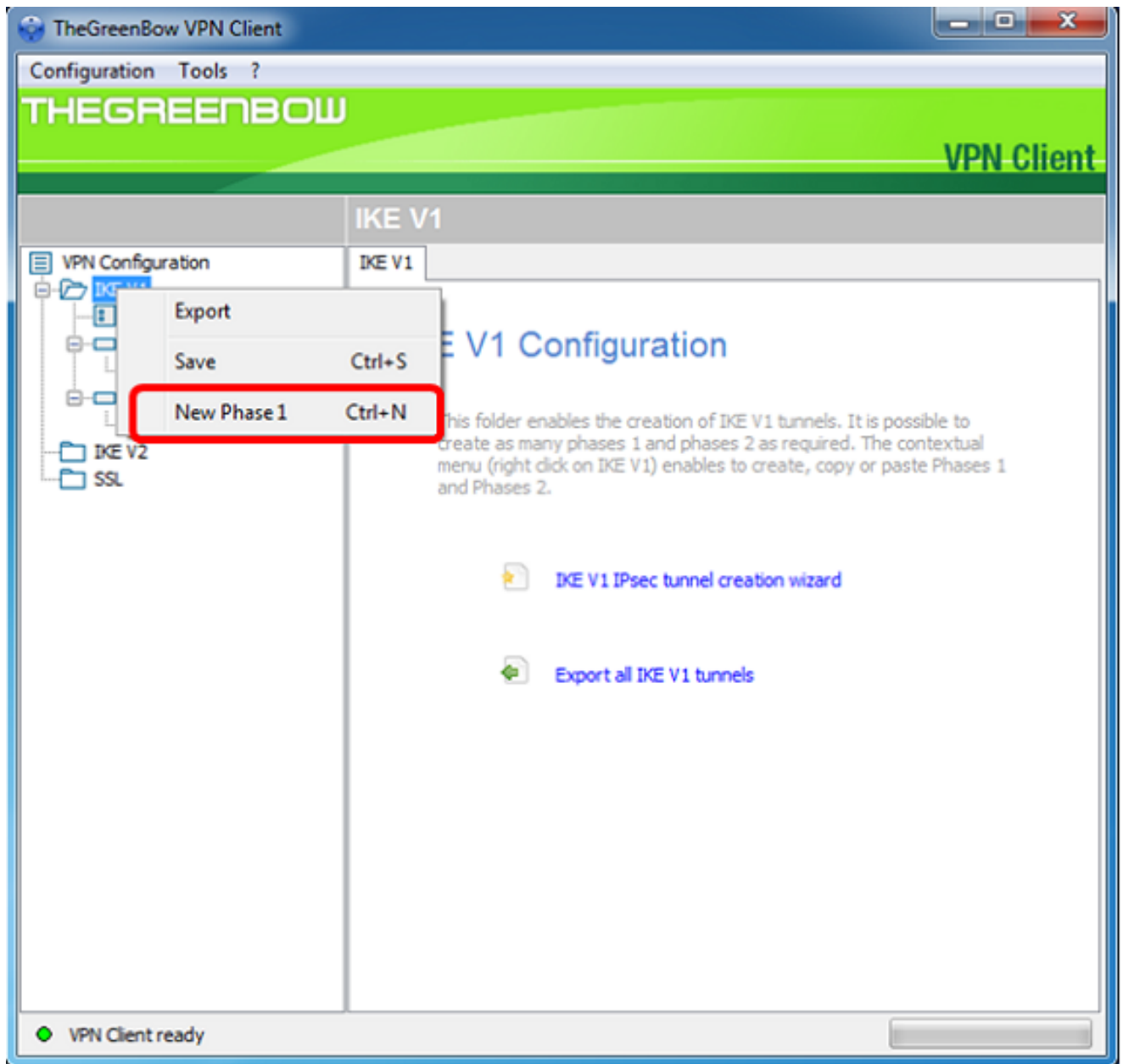
De GroeneBW VPN-clientsoftware configureren

Instellingen fase 1

Stap 1. Klik met de rechtermuisknop op het pictogram GreenBow VPN Client en kies **Run als beheerder**.

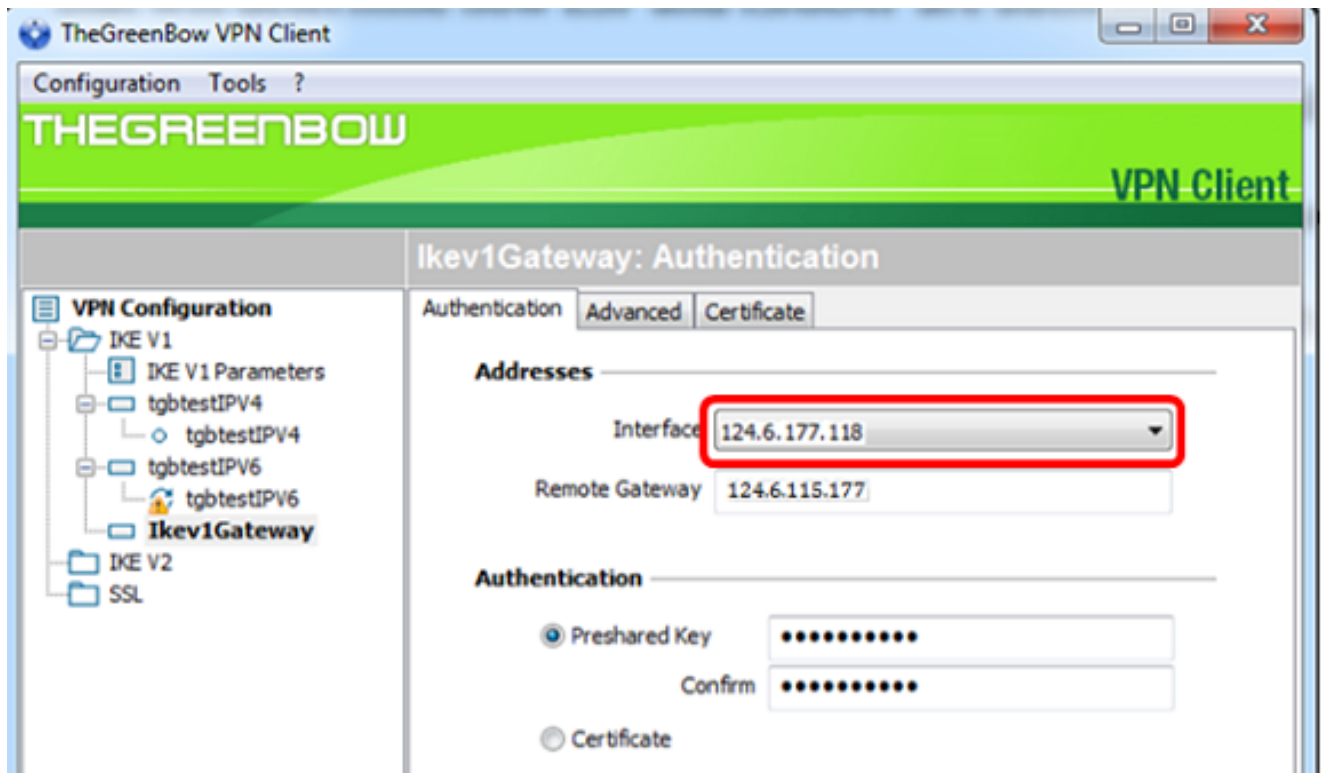


Stap 2. Klik in het linker deelvenster onder VPN-configuratie met de rechtermuisknop op **IKE V1** en kies **Nieuwe fase 1**.



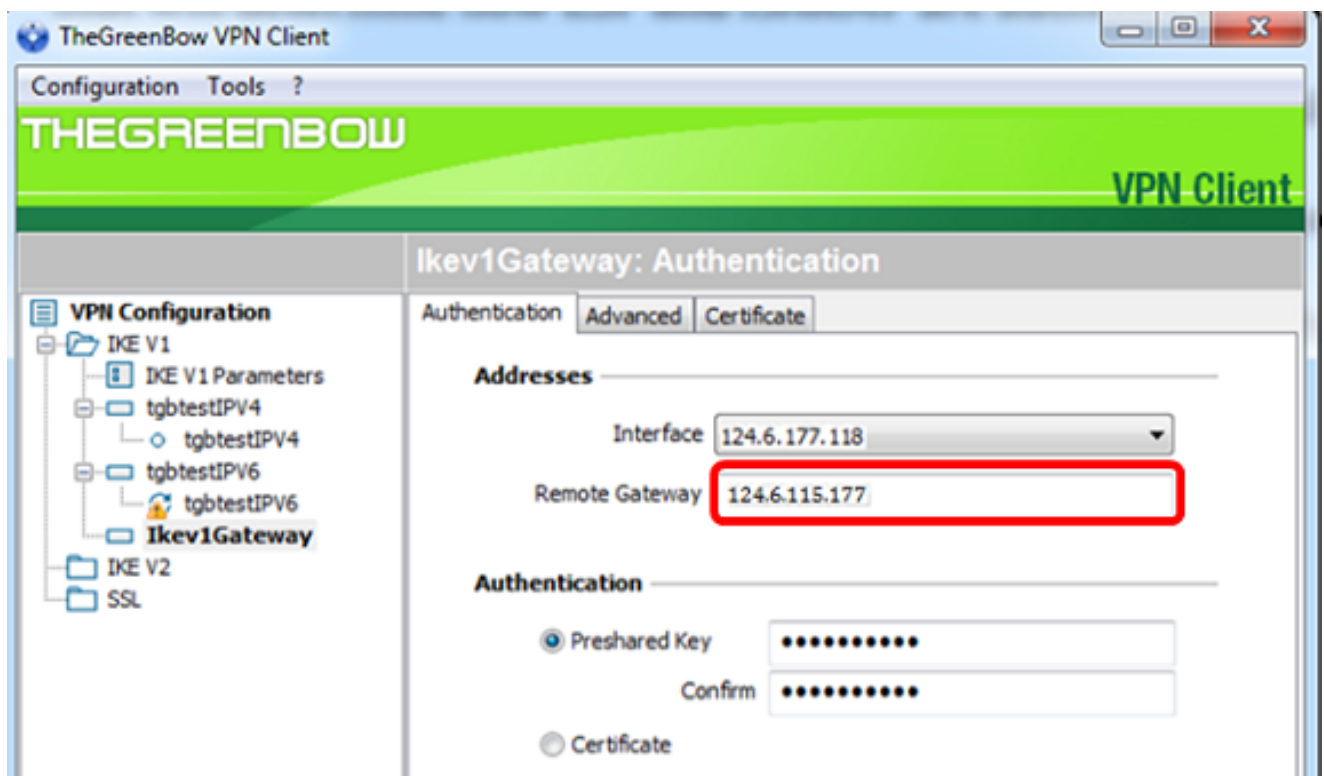
Stap 3. In het tabblad Verificatie onder Adressen controleert u of het IP-adres in het interfacegebied hetzelfde is als het WAN IP-adres van de computer waarop De GreenBow VPN-client is geïnstalleerd.

Opmerking: In dit voorbeeld is het IP-adres 124.6.177.118.



Stap 4. Voer het adres van de externe gateway in het veld *Remote Gateway* in.

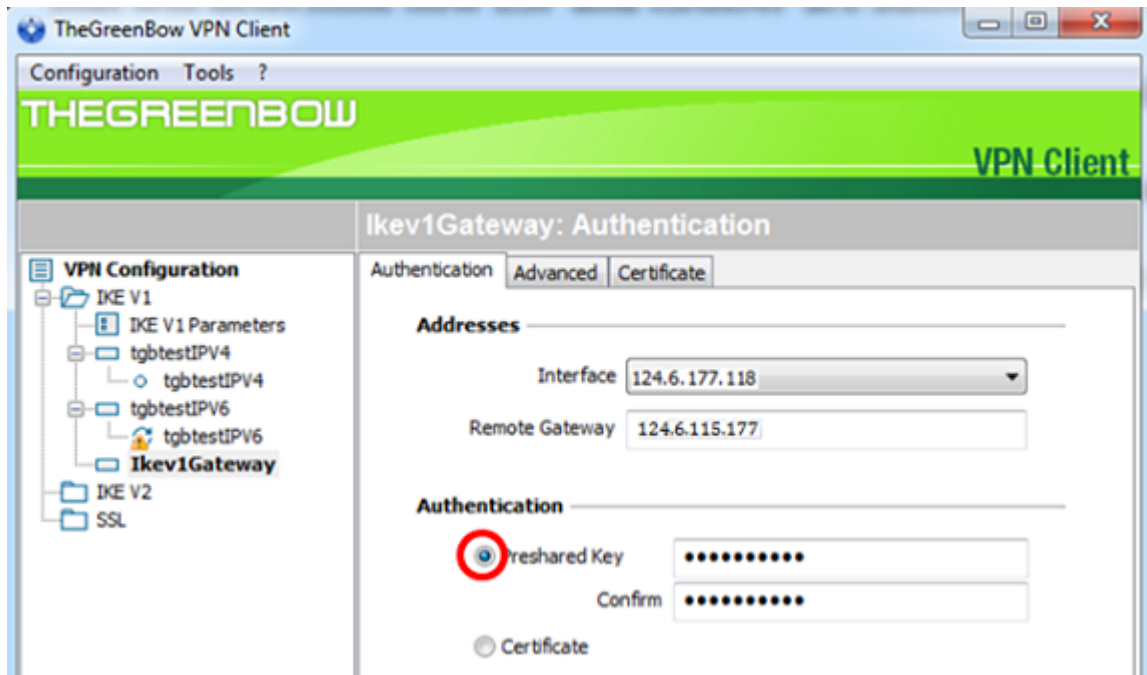
Opmerking: In dit voorbeeld is het IP-adres van de externe RV34x-router 124.6.115.177.



Stap 5. Kies onder Verificatie het verificatietype. De opties zijn:

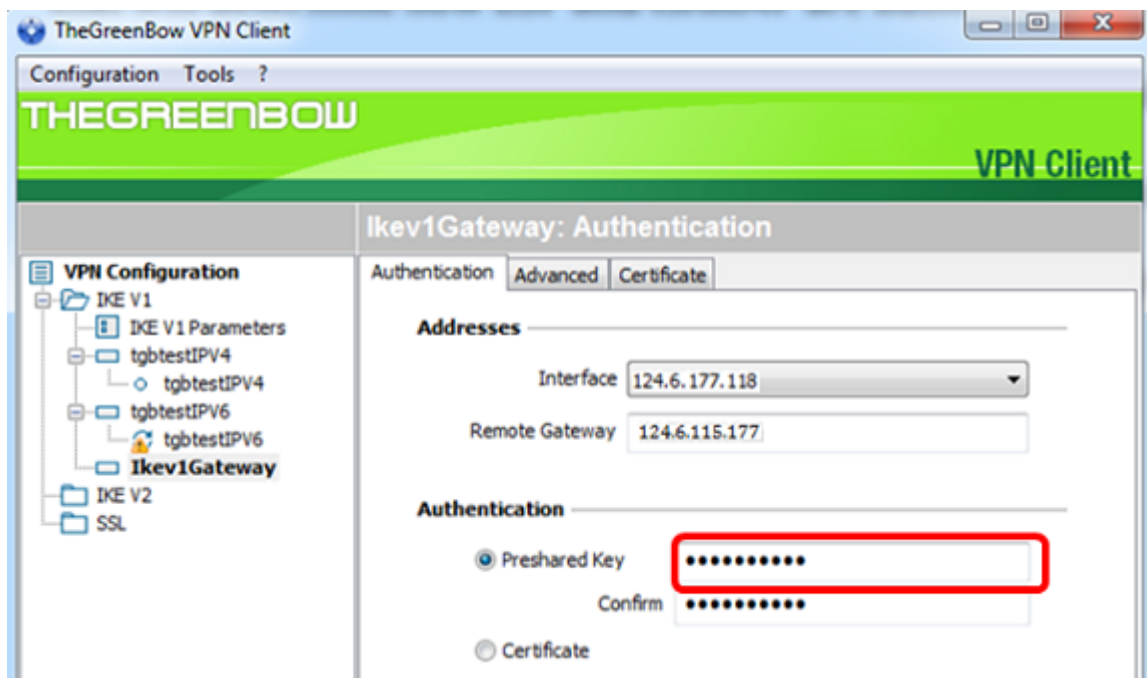
- Voorgedeelde sleutel — Deze optie laat de gebruiker een wachtwoord gebruiken dat is ingesteld op de VPN-poort. Het wachtwoord moet door de gebruiker worden aangepast om een VPN-tunnel te kunnen maken.
- Certificaat - Deze optie zal een certificaat gebruiken om de handdruk tussen de VPN-client en

de VPN-gateway te voltooien.

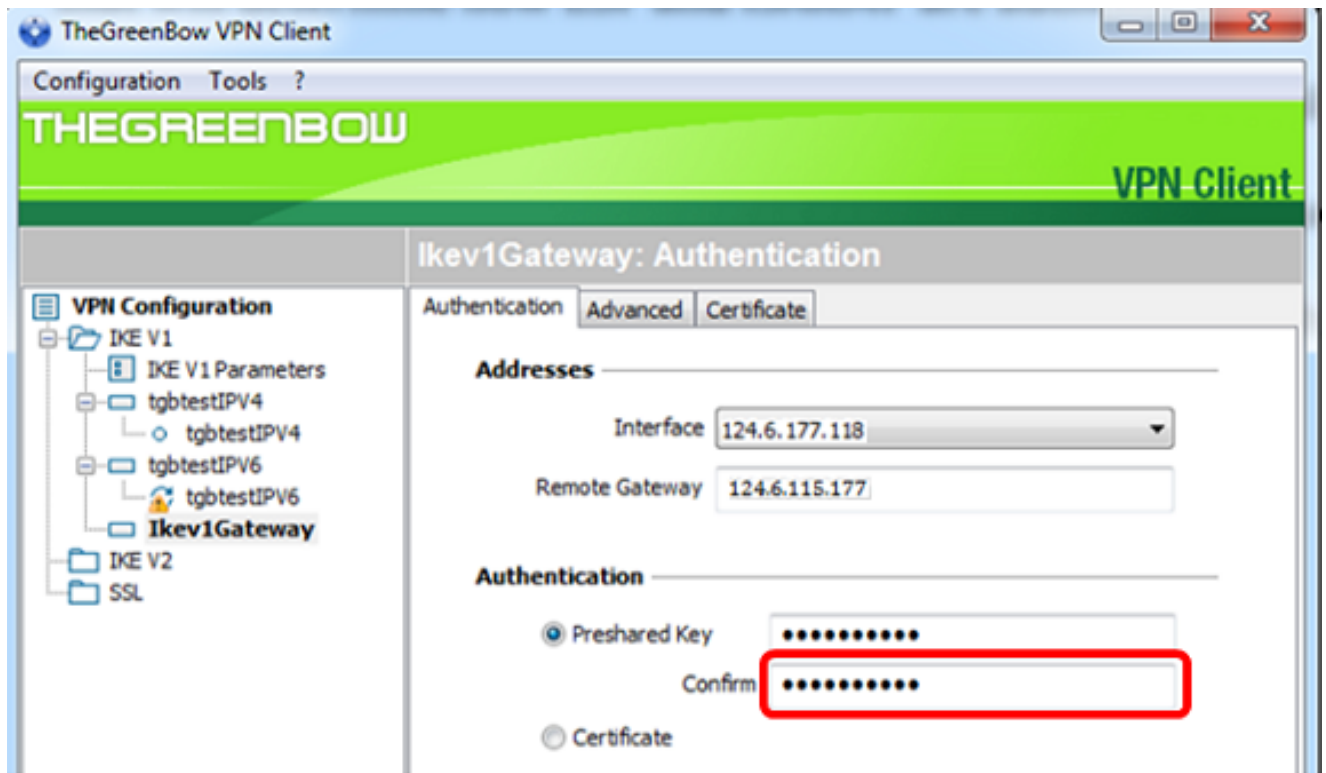


Opmerking: In dit voorbeeld wordt PreShared Key gekozen om de configuratie van de RV34x VPN-gateway aan te passen.

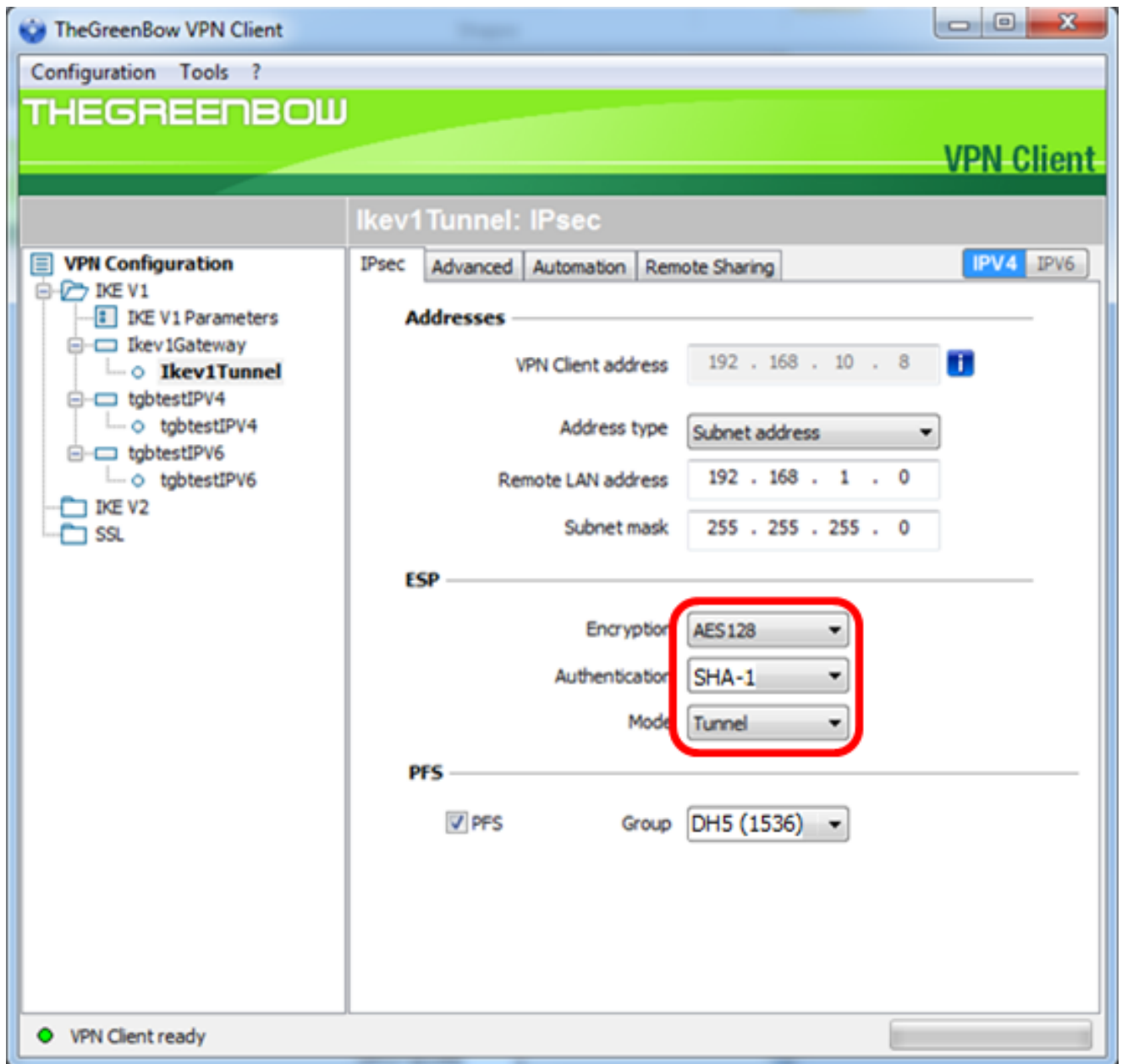
Stap 6. Voer de vooraf gedeelde sleutel in die in de router is ingesteld.



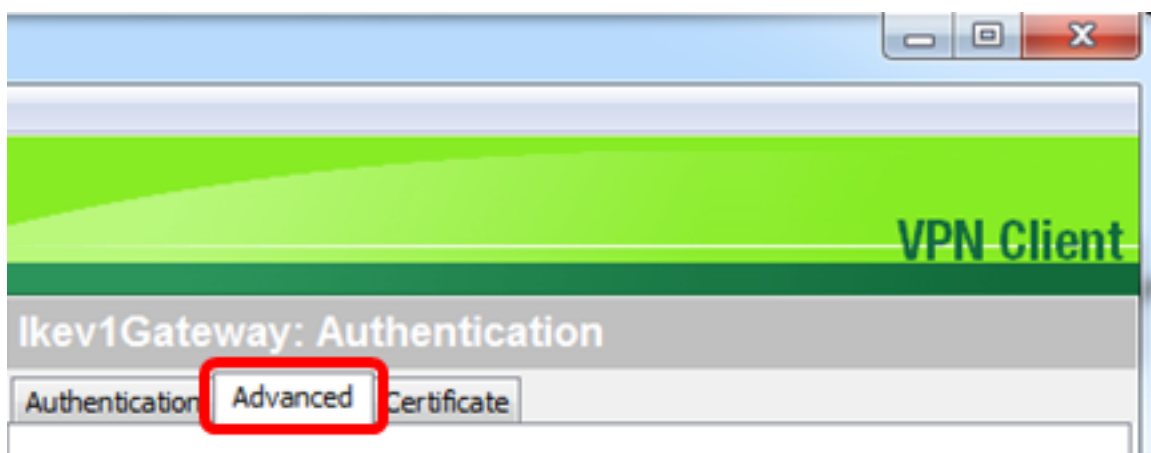
Stap 7. Voer dezelfde gedeelde sleutel in in het veld *Bevestiging*.



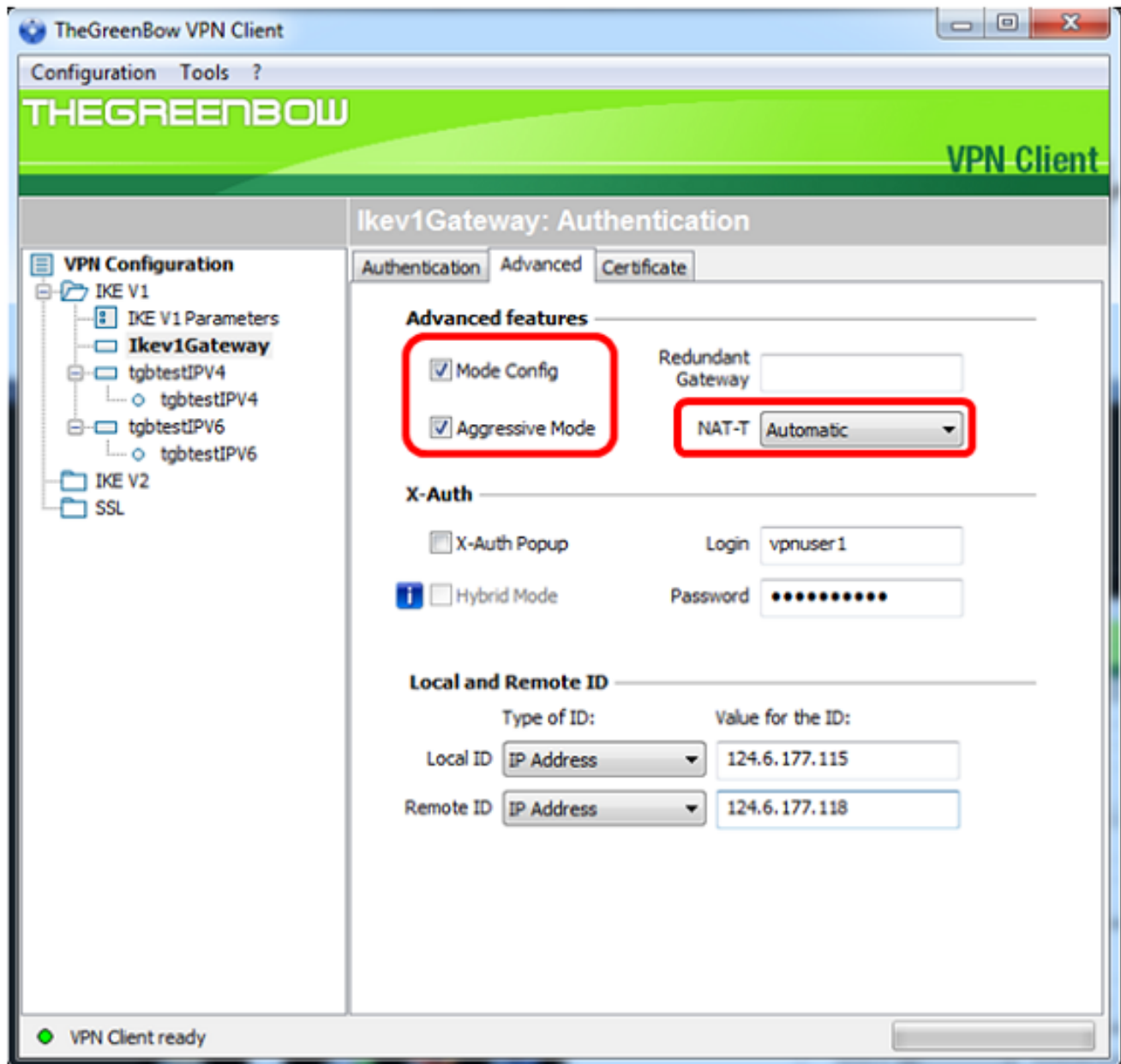
Stap 8. Onder IKE, stel de instellingen Encryptie, verificatie en Key Group in om de configuratie van de router aan te passen.



Stap 9. Klik op het tabblad **Geavanceerd**.

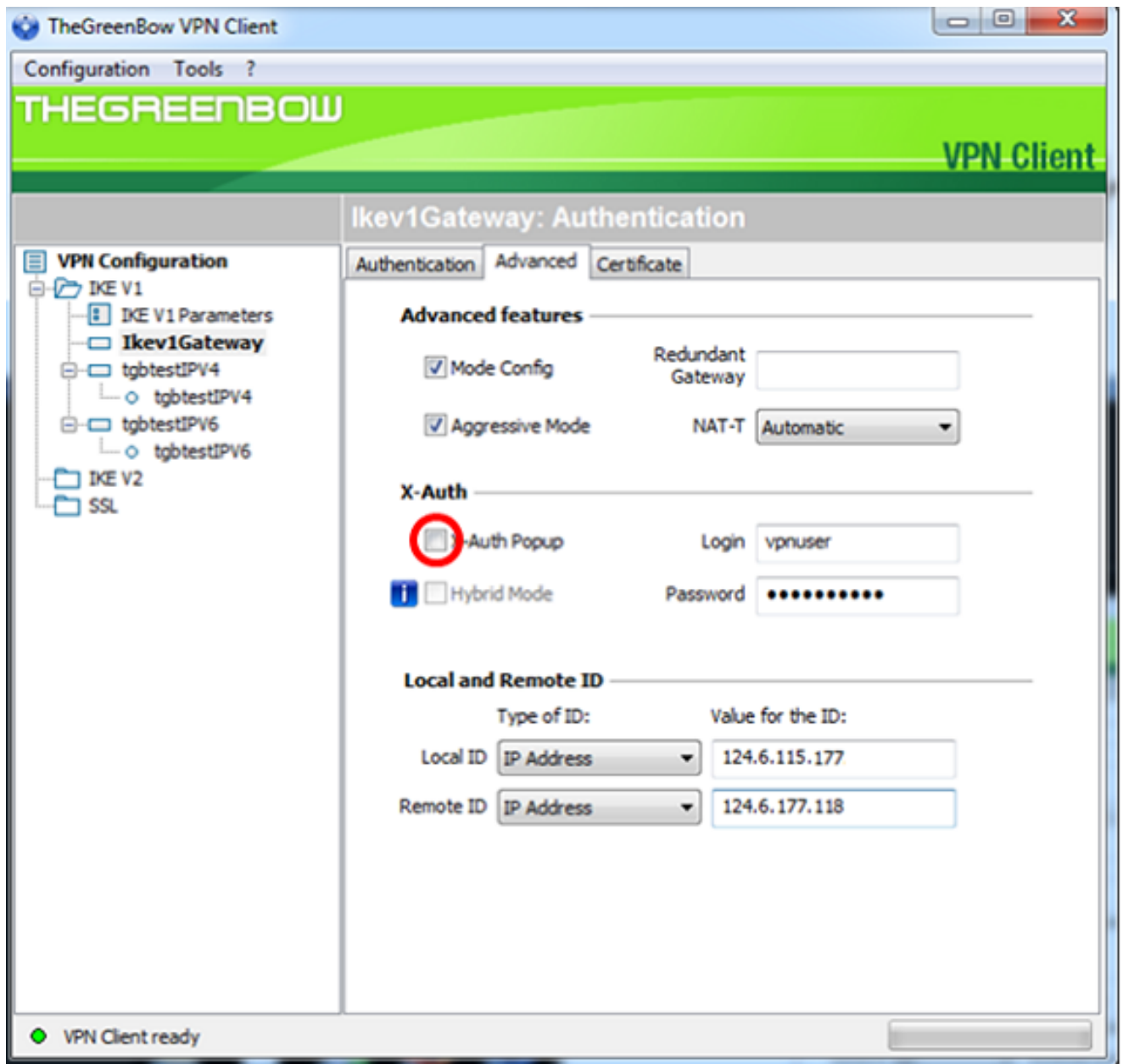


Stap 10. (Optioneel) Controleer onder Geavanceerde functies de vinkjes **Modus Config** en **Aggressief Mode** en stel de NAT-T instelling in op Automatisch.



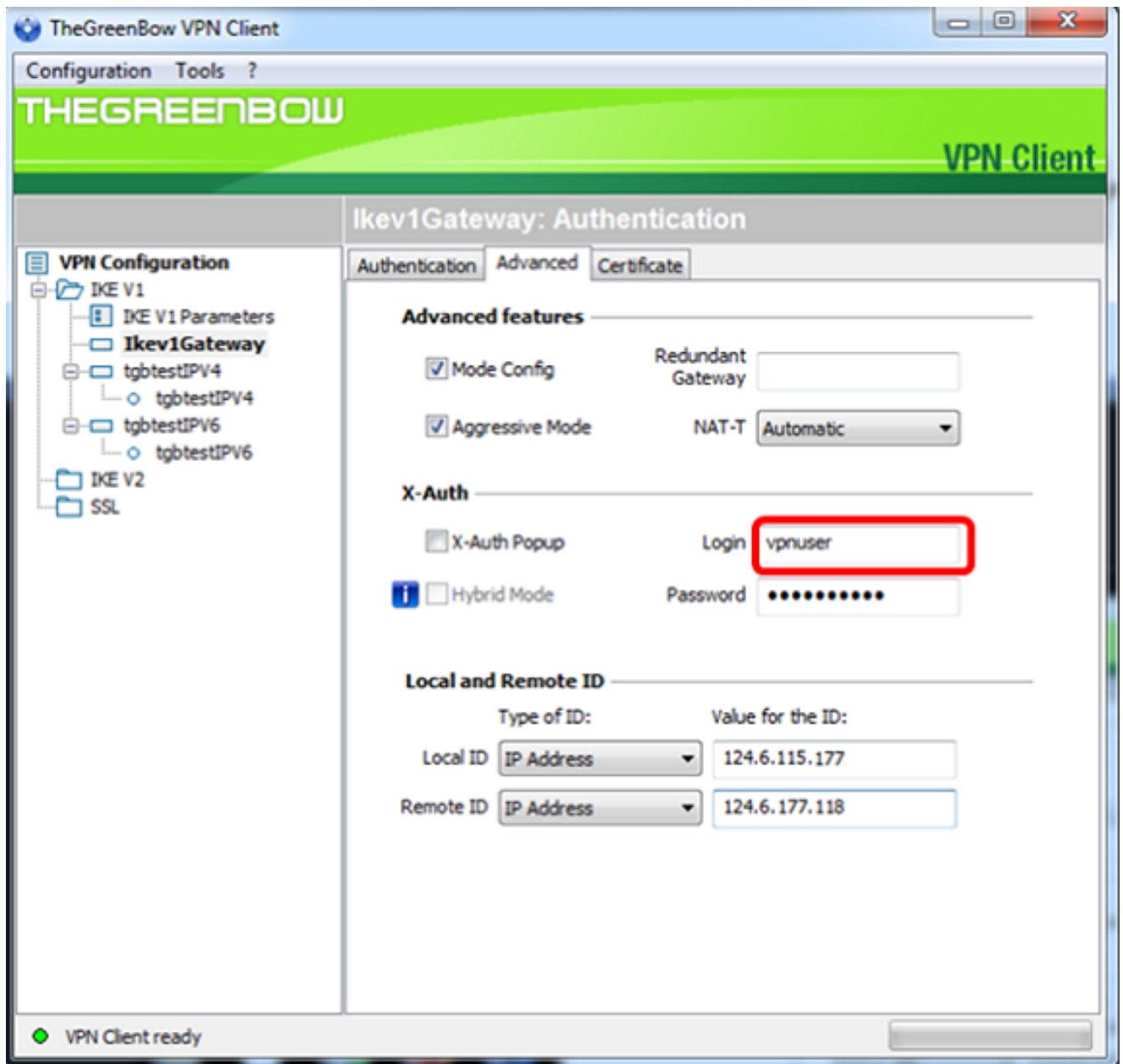
Opmerking: Als Mode Config ingeschakeld is, zal de client voor GreenBow VPN de instellingen van de VPN-gateway ophalen om te proberen een tunnel in te stellen terwijl Aggressief Mode en NAT-T de verbinding sneller maken.

Stap 1. (Optioneel) Onder X-Auth controleert u het vakje **X-Auth Popup** om automatisch het inlogvenster op te trekken wanneer u een verbinding start. In het inlogvenster verschijnen de inloggegevens van de gebruiker om de tunnel te kunnen voltooien.

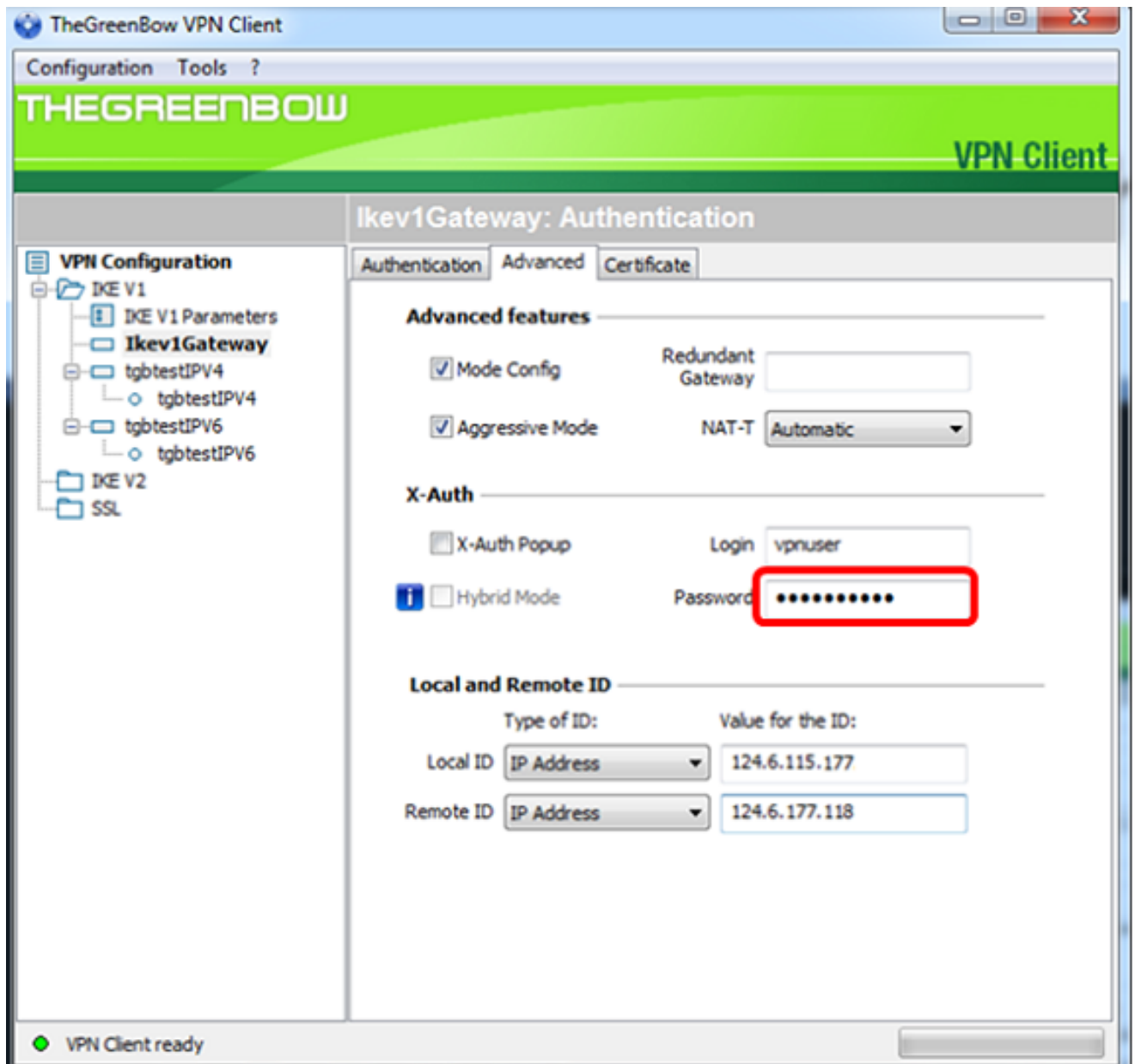


Opmerking: In dit voorbeeld, wordt X-Auth Popup niet gecontroleerd.

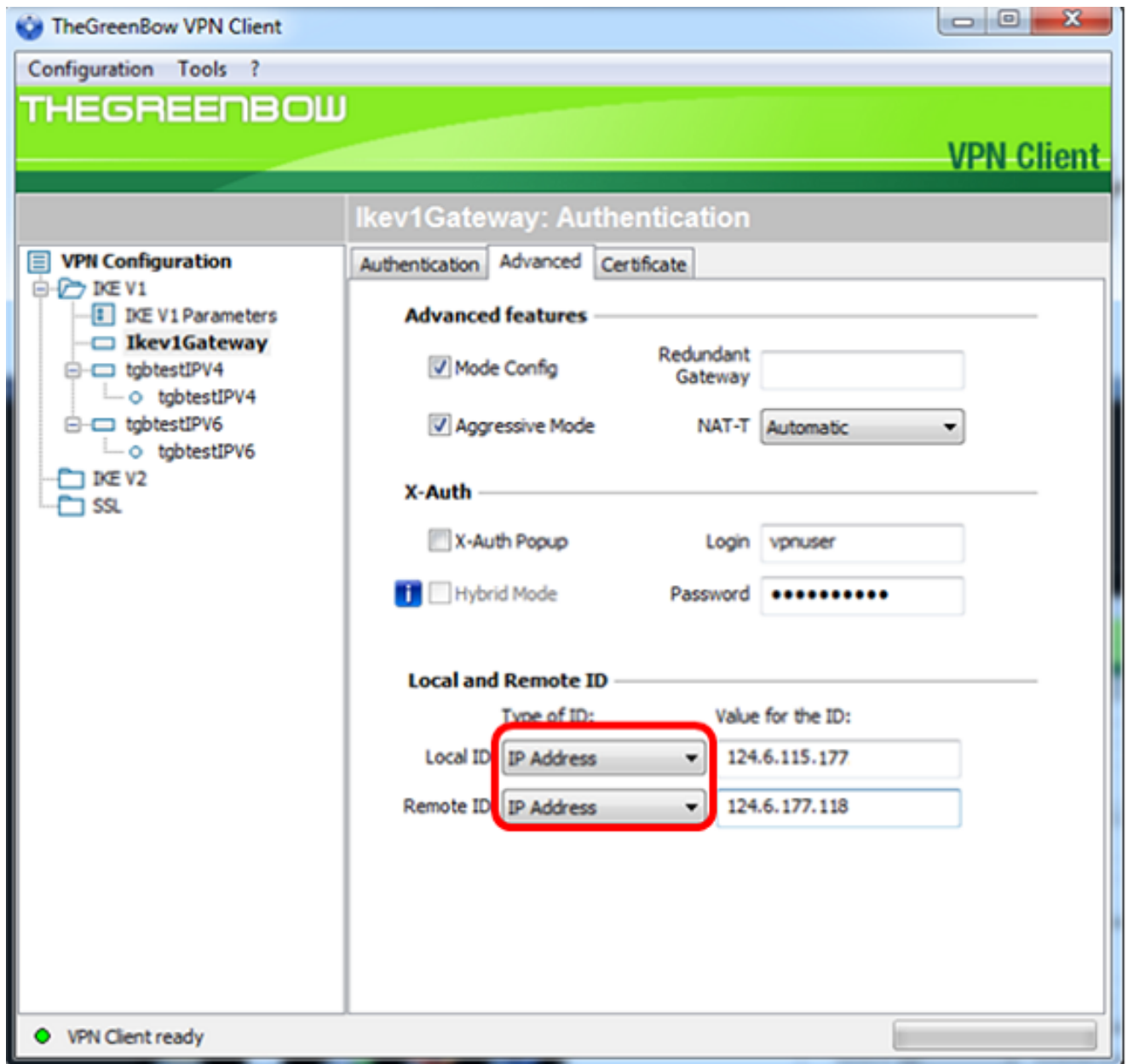
Stap 12. Voer uw gebruikersnaam in het veld *Aanmelden*. Dit is de gebruikersnaam die is ingesteld voor het maken van een gebruikersgroep in de VPN-poort.



Stap 13. Voer uw wachtwoord in het veld *Wachtwoord in*.

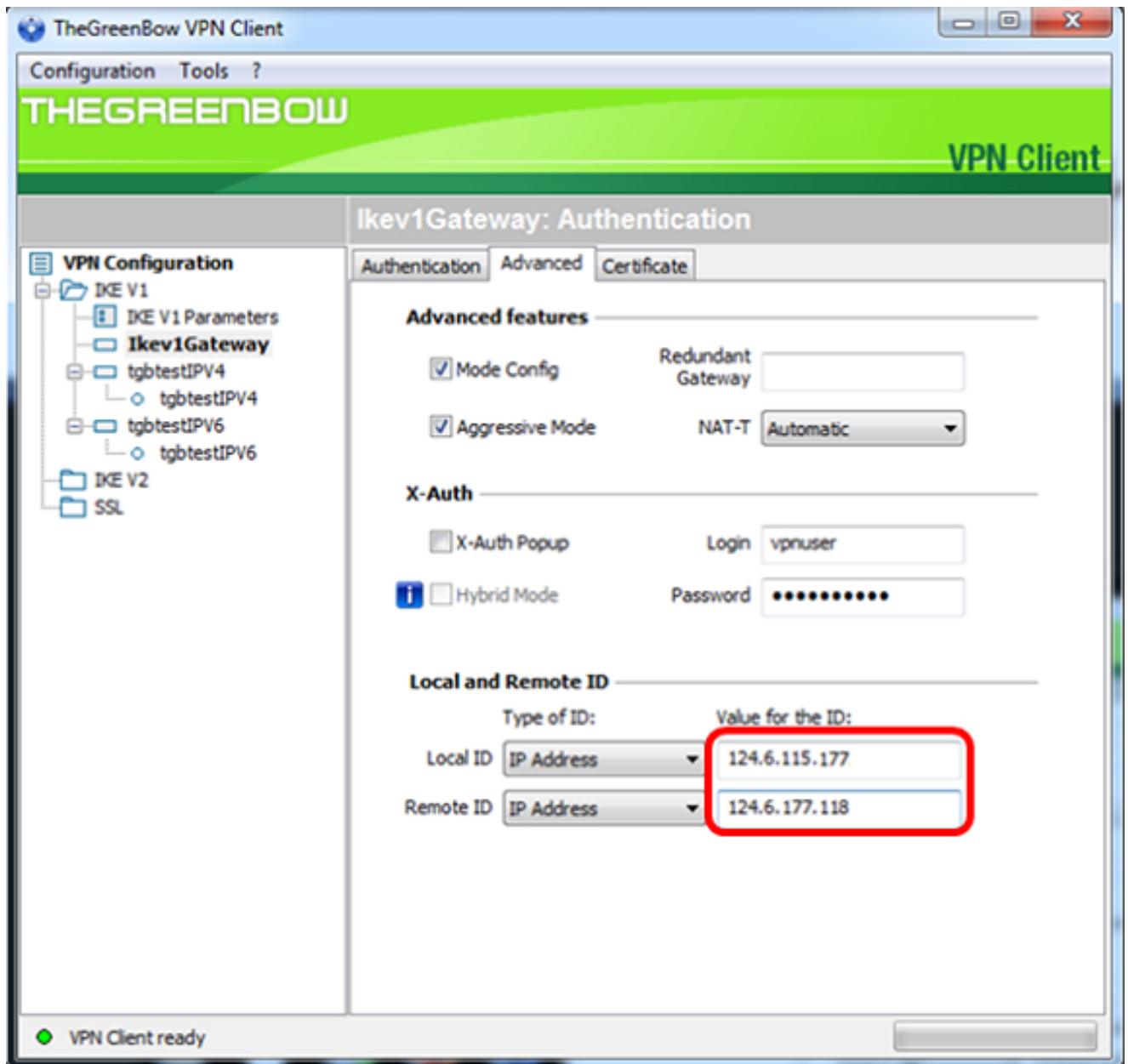


Stap 14. Stel onder Lokale en Remote-ID de lokale ID en de Remote-ID in om de instellingen van de VPN-gateway aan te passen.

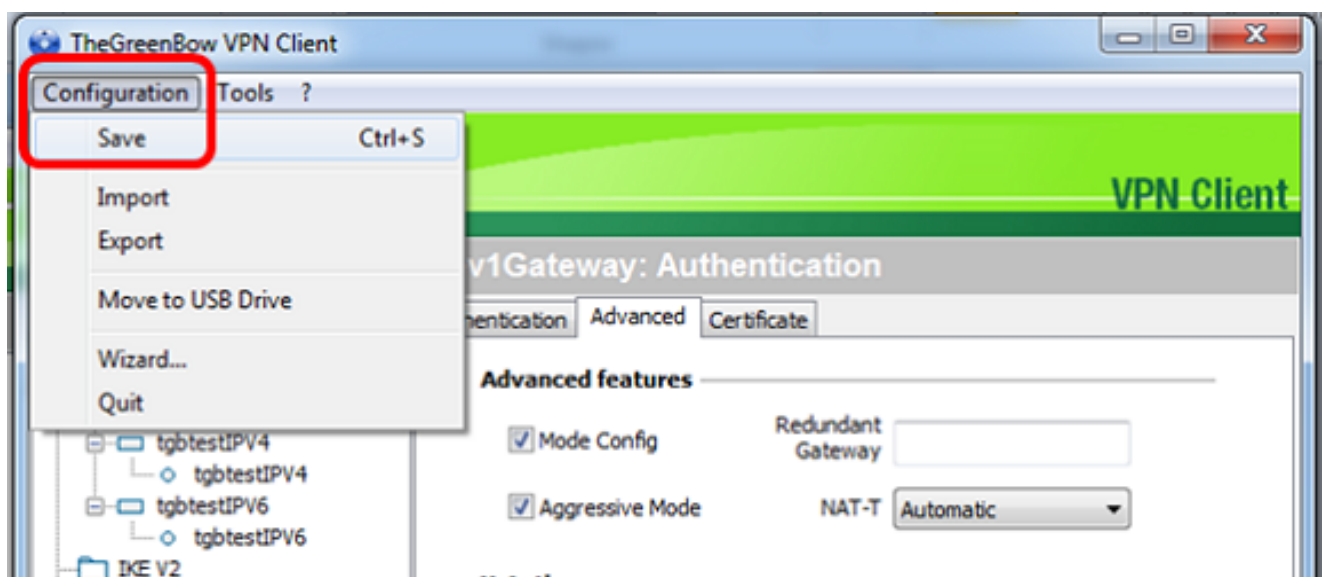


Opmerking: In dit voorbeeld, worden zowel Lokale ID als Remote-ID ingesteld op IP-adres om de instellingen van de RV34x VPN-gateway aan te passen.

Stap 15. Onder Waarde voor de ID, voer de lokale ID en de externe ID in hun respectievelijke velden in.

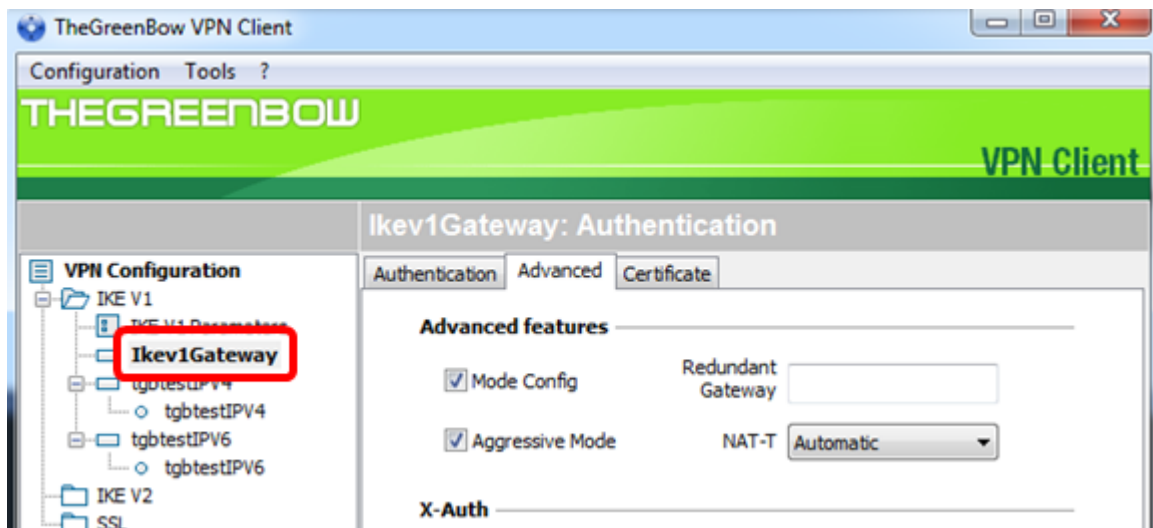


Stap 16. Klik op Configuration > Save om de instellingen op te slaan.

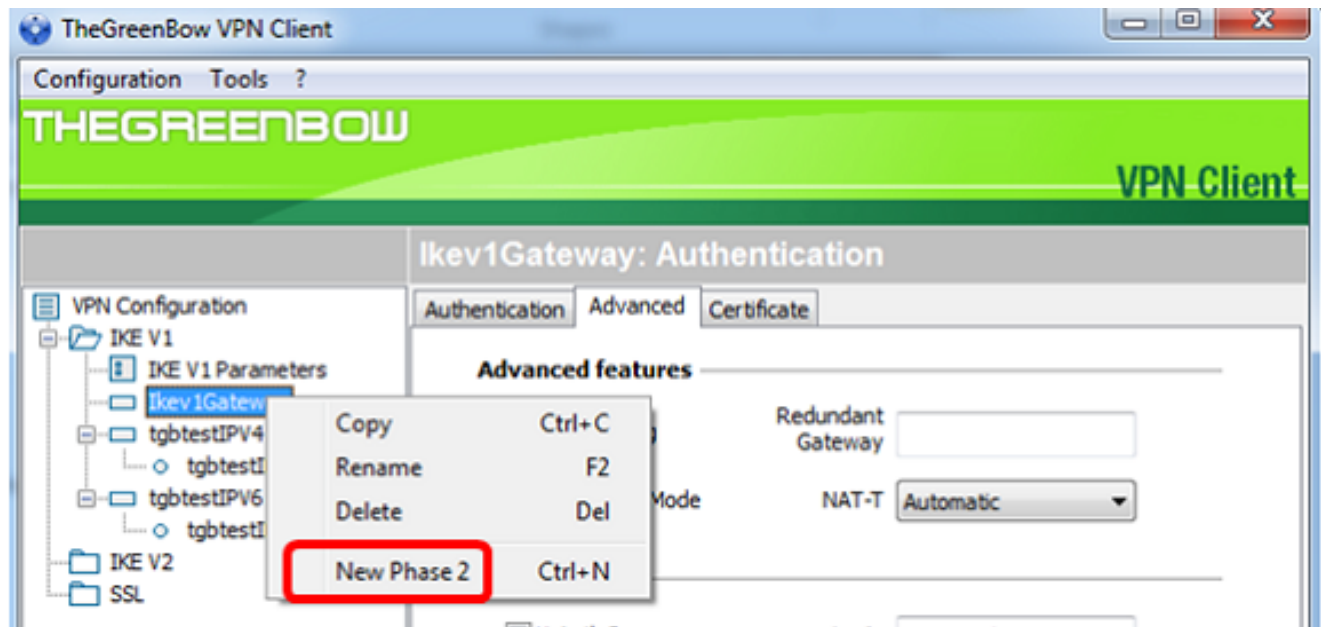


Instellingen fase 2 instellen

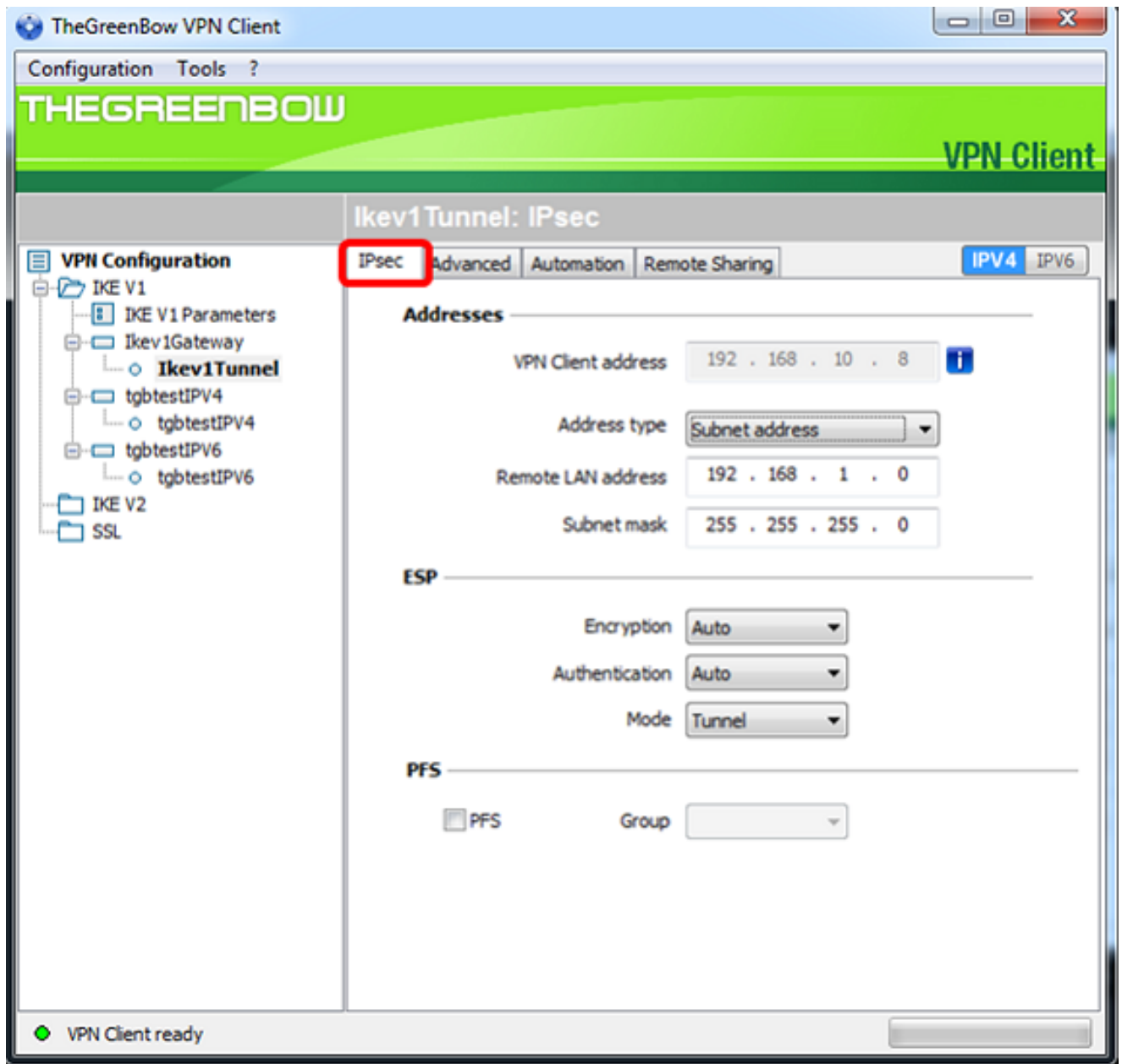
Stap 1. Klik met de rechtermuisknop op Ikev1-gateway.



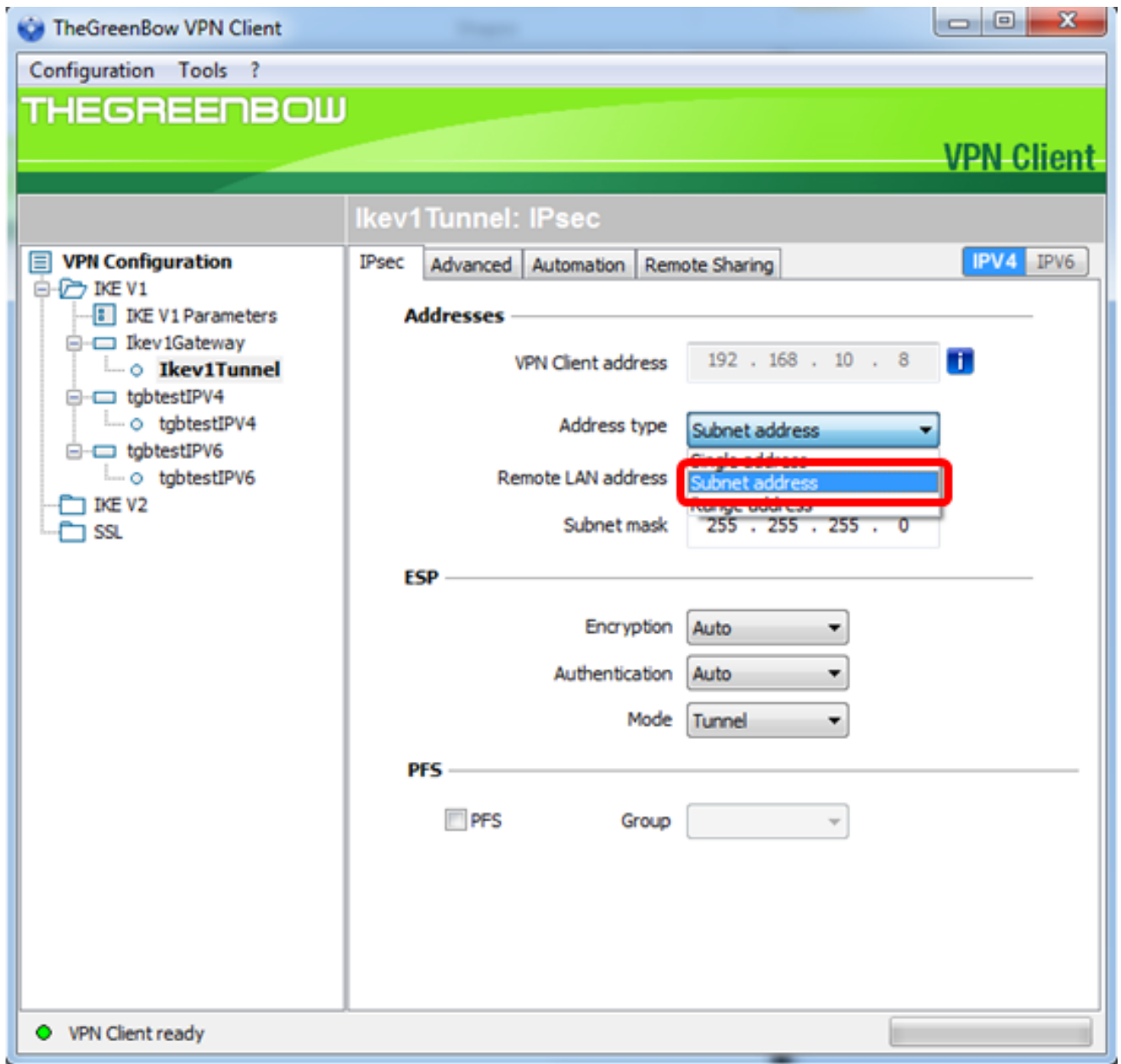
Stap 2. Kies nieuwe fase 2.



Stap 3. Klik op het tabblad IPsec.

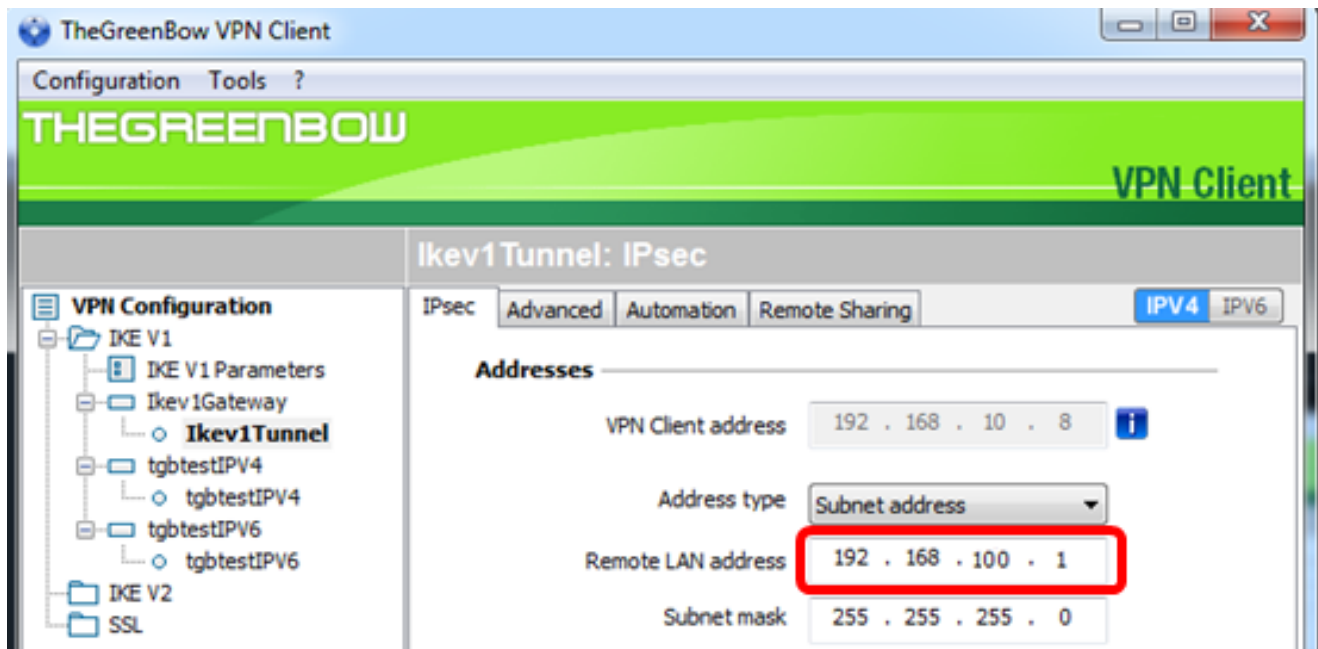


Stap 4. Kies het adrestype dat de VPN-client toegang kan hebben van de vervolgkeuzelijst Adres.



Opmerking: In dit voorbeeld wordt het Subnet adres gekozen.

Stap 5. Voer het netwerkadres in dat door de VPN-tunnel toegankelijk moet zijn in het veld *Remote LAN-adres*.



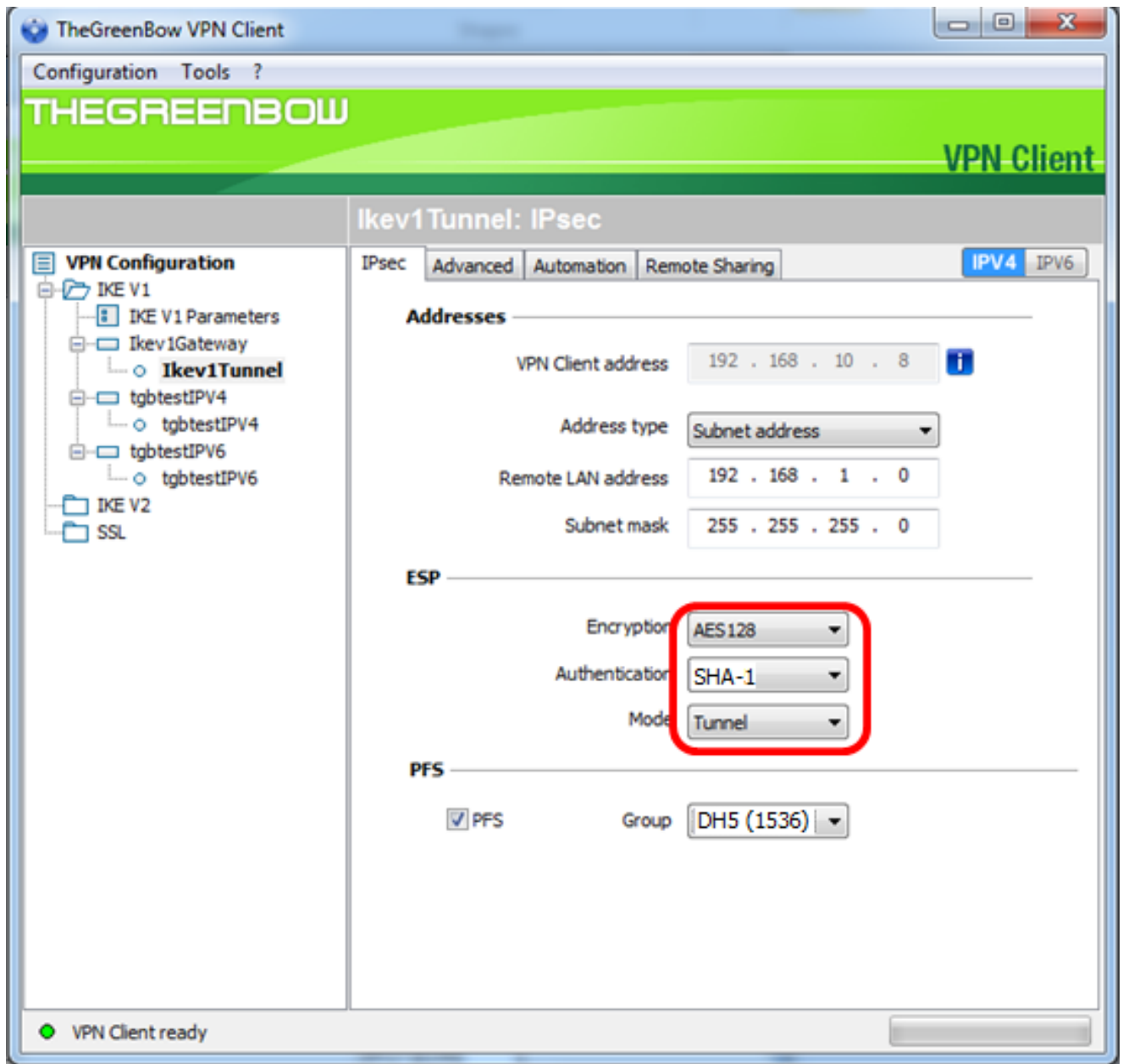
Opmerking: In dit voorbeeld wordt 192.168.100.1 opgenomen.

Stap 6. Voer het subnetmasker van het externe netwerk in het veld *Subnetmasker* in.

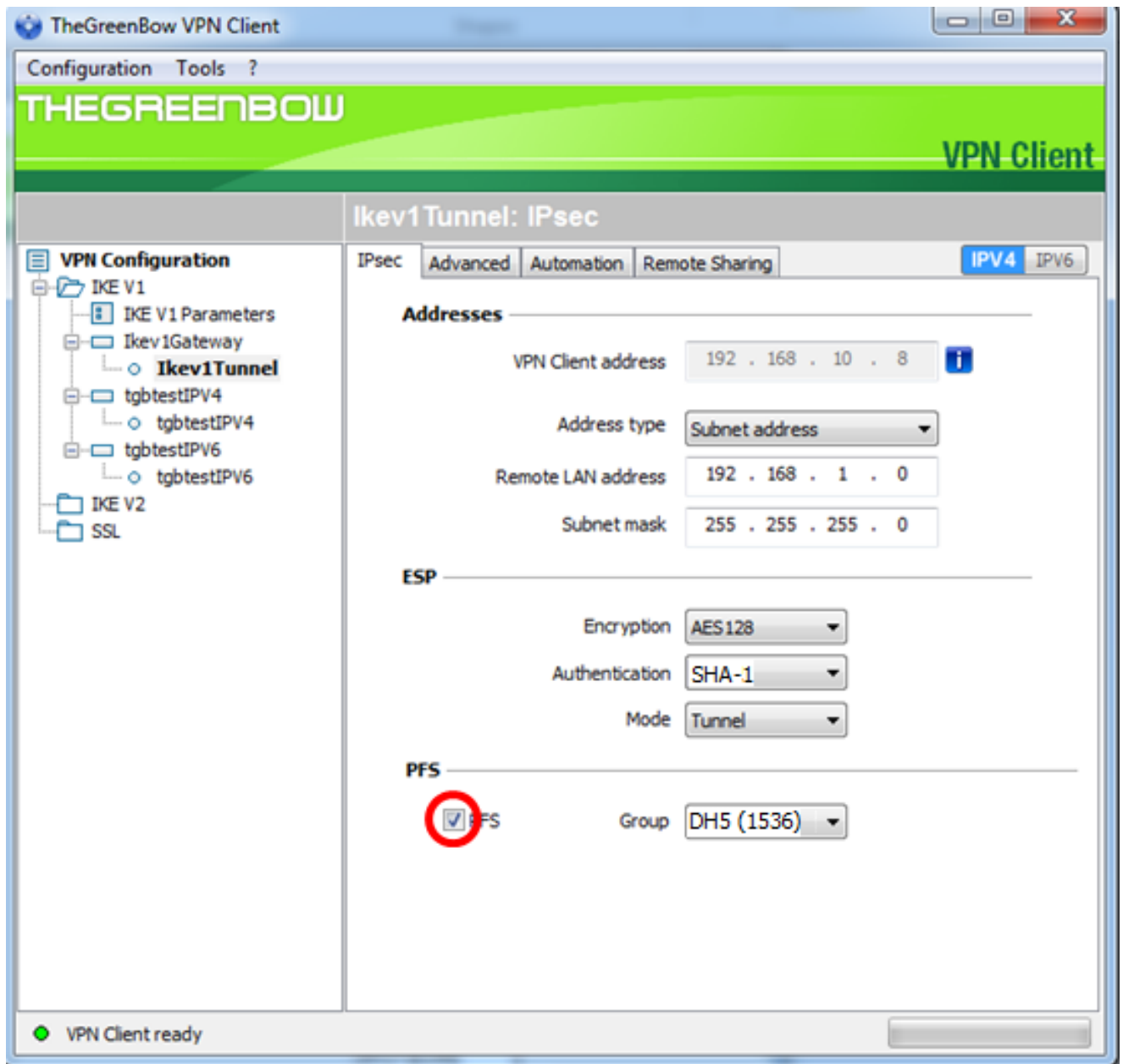
Opmerking: In dit voorbeeld wordt 255.255.255.0 ingevoerd.



Stap 7. Stel onder ESP de optie Encryptie, verificatie en modus in om de instellingen van de VPN-gateway aan te passen.

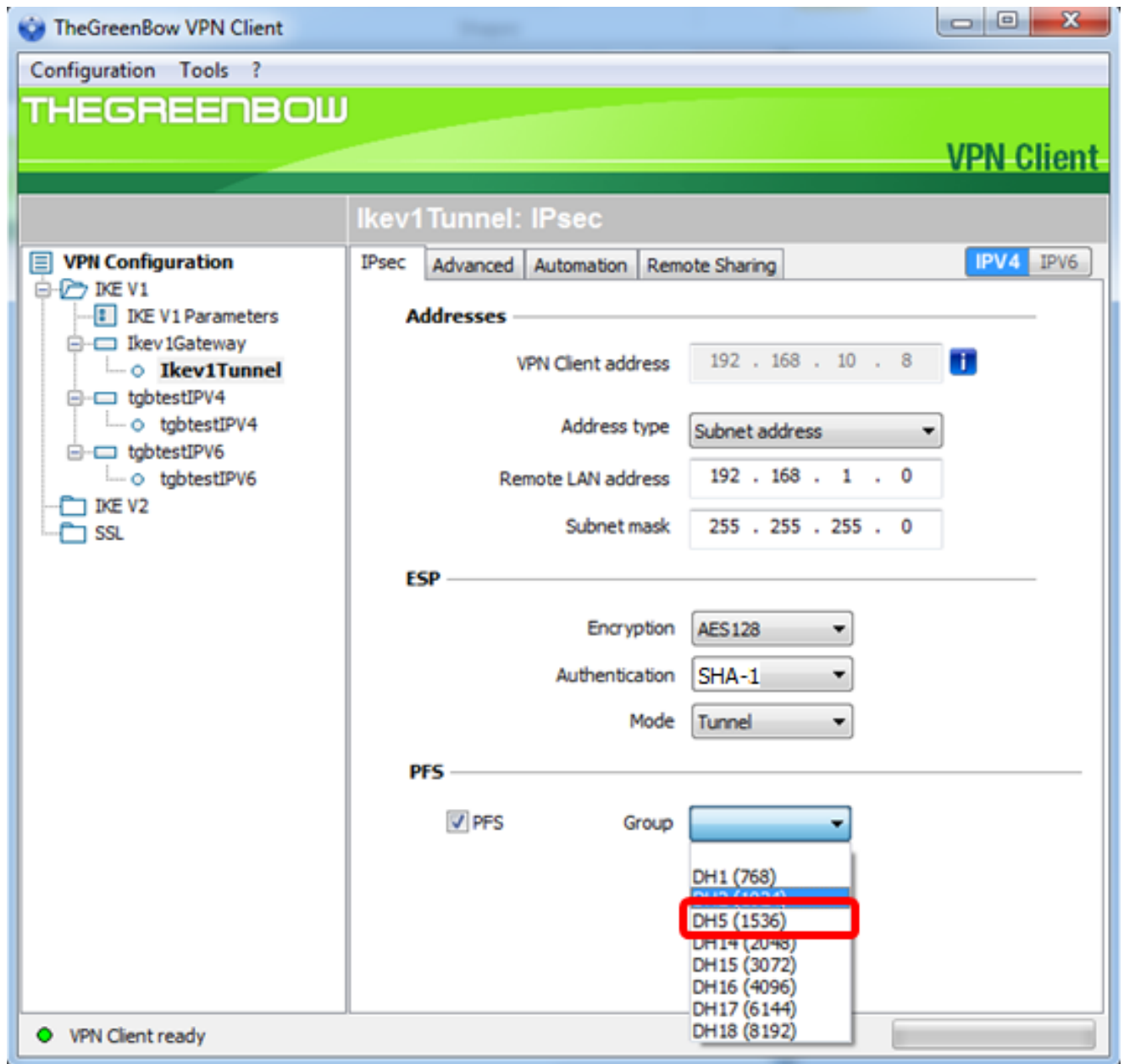


Stap 8. (Optioneel) Onder PFS, vinkt u het aankruisvakje **PFS** aan om Perfect Forward Security (PFS) mogelijk te maken. PFS genereert willekeurige toetsen om de sessie te versleutelen.

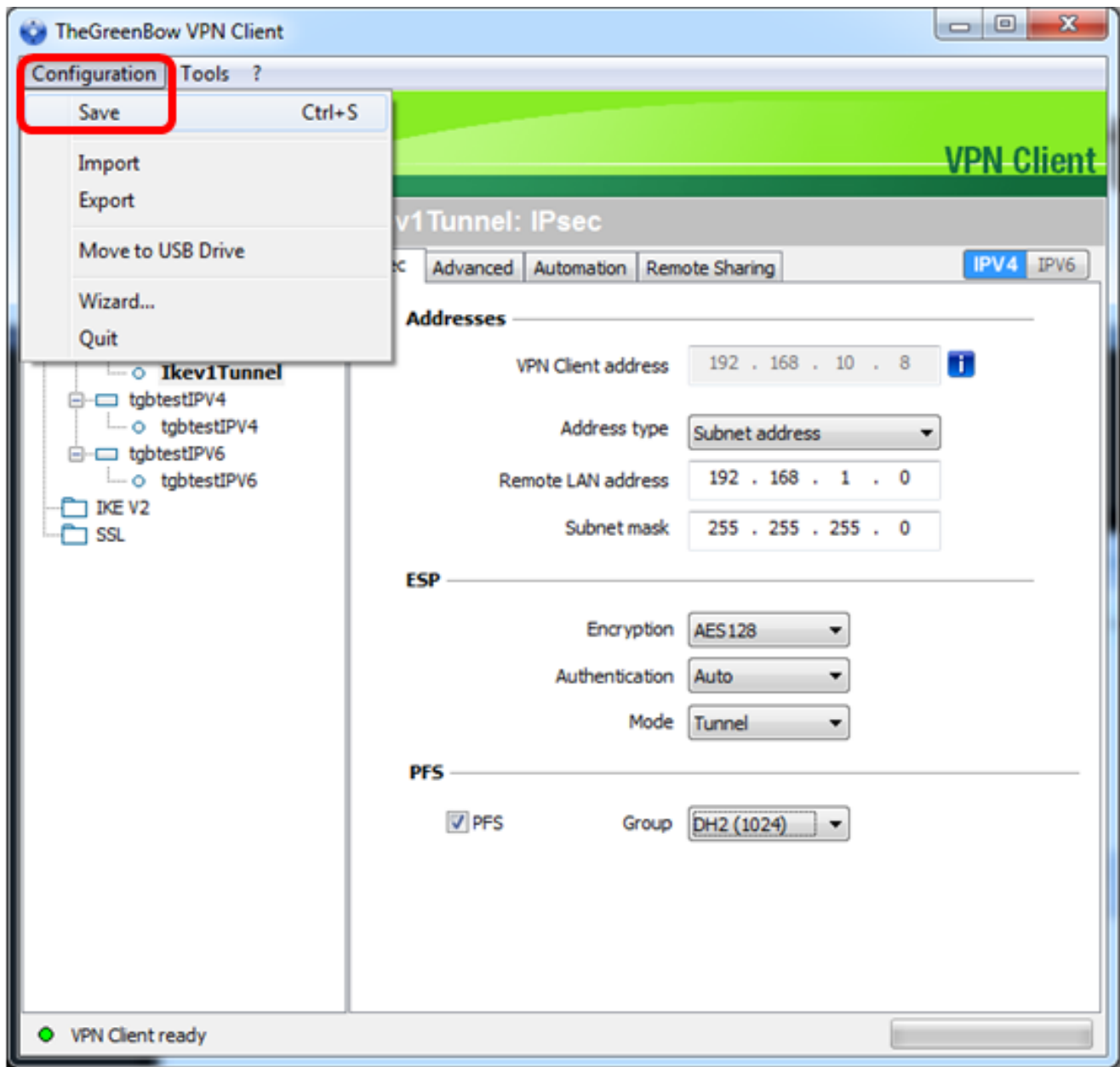


Stap 9. Kies een PFS-groepsinstelling in de vervolgkeuzelijst Groep.

Opmerking: In dit voorbeeld wordt DH5 (1536) geselecteerd om de instelling van de DH Group van de router aan te passen.



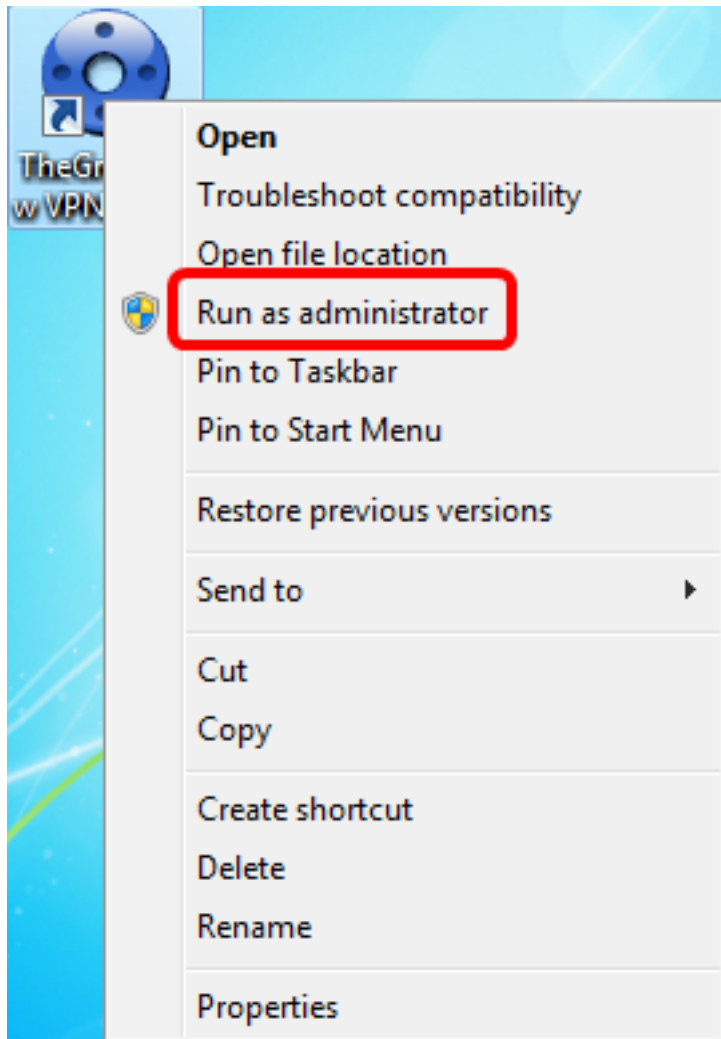
Stap 10. Klik met de rechtermuisknop op **Configuration** en kies Opslaan.



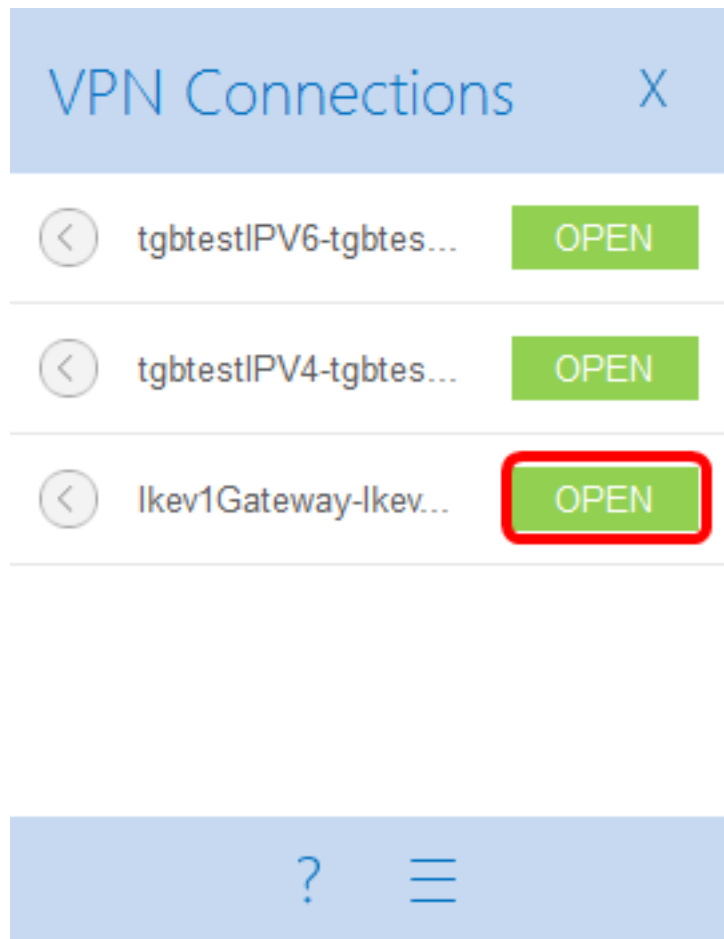
U dient nu met succes de GreenBow VPN-client te configureren om verbinding te maken met de RV34x Series router via VPN.

Een VPN-verbinding starten

Stap 1. Klik met de rechtermuisknop op de Groene VPN-client en kies **Uitvoeren als beheerder**.



Stap 2. Kies de VPN-verbinding die u moet gebruiken en klik vervolgens op **Openen**. De VPN-verbinding moet automatisch worden gestart.

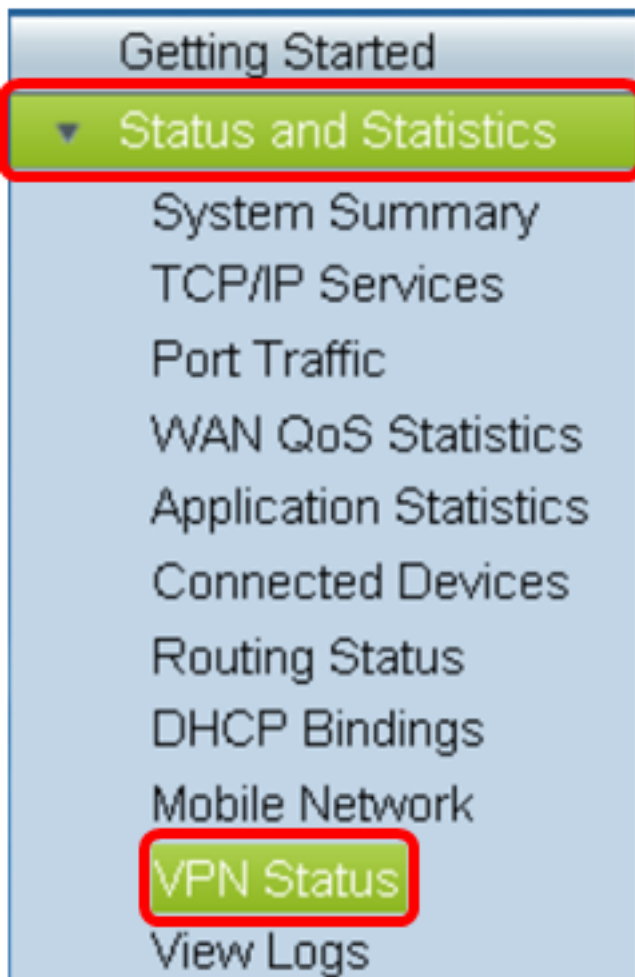


Opmerking: In dit voorbeeld werd de geconfigureerde Ikev1Gateway geselecteerd.

Controleer de VPN-status

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van de VPN-gateway.

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



Stap 3. Controleer onder Client-to-Site Tunnel Status de kolom Connections in de verbindingstabel.

Opmerking: In dit voorbeeld, is één VPN verbinding gevestigd.

Connections
1

U dient nu met succes de VPN-verbindingstatus op de RV34x Series router te hebben geverifieerd. De GreenBow VPN-client is nu geconfigureerd voor verbinding met de router door VPN.