

Utiliser le client VPN TheGreenBow pour se connecter avec un routeur de la gamme RV34x

Avis spécial : Structure des licences - Firmware versions 1.0.3.15 et ultérieures. À l'avenir, AnyConnect entraînera des frais pour les licences client uniquement.

Pour plus d'informations sur les licences AnyConnect sur les routeurs de la gamme RV340, consultez l'article [Licence AnyConnect pour les routeurs de la gamme RV340](#).

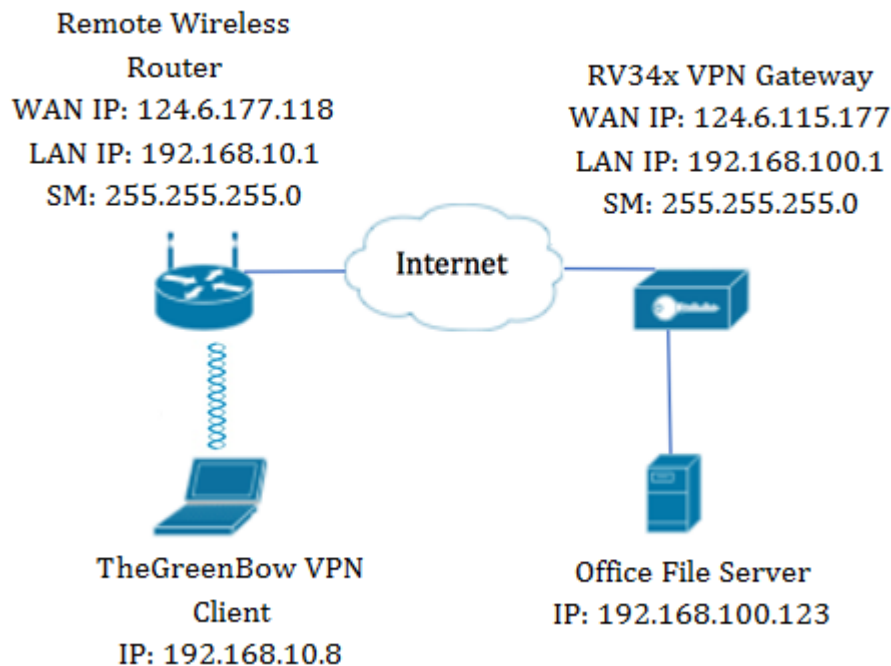
Introduction

Une connexion de réseau privé virtuel (VPN) permet aux utilisateurs d'accéder, d'envoyer et de recevoir des données depuis et vers un réseau privé en passant par un réseau public ou partagé tel qu'Internet, tout en assurant une connexion sécurisée à une infrastructure réseau sous-jacente afin de protéger le réseau privé et ses ressources.

Un tunnel VPN établit un réseau privé qui peut envoyer des données en toute sécurité à l'aide du chiffrement et de l'authentification. Les bureaux d'entreprise utilisent principalement une connexion VPN car il est à la fois utile et nécessaire de permettre à leurs employés d'accéder à leur réseau privé même s'ils se trouvent en dehors du bureau.

Le VPN permet à un hôte distant d'agir comme s'il se trouvait sur le même réseau local. Le routeur prend en charge jusqu'à 50 tunnels. Une connexion VPN peut être configurée entre le routeur et un point d'extrémité une fois que le routeur a été configuré pour la connexion Internet. Le client VPN dépend entièrement des paramètres du routeur VPN pour établir une connexion.

Le client VPN GreenBow est une application cliente VPN tierce qui permet à un périphérique hôte de configurer une connexion sécurisée pour un tunnel IPSec site à site avec le routeur de la gamme RV34x.



Dans le schéma, l'ordinateur se connecte au serveur de fichiers du bureau en dehors de son réseau pour accéder à ses ressources. Pour ce faire, le client VPN TheGreenBow de l'ordinateur sera configuré de manière à extraire les paramètres de la passerelle VPN RV34x.

Avantages de l'utilisation d'une connexion VPN

1. L'utilisation d'une connexion VPN permet de protéger les données et les ressources réseau confidentielles.
2. Elle offre commodité et accessibilité aux travailleurs distants ou aux employés d'entreprise, car ils pourront facilement accéder au bureau central sans avoir à être physiquement présents et, pourtant, maintenir la sécurité du réseau privé et de ses ressources.
3. La communication via une connexion VPN offre un niveau de sécurité plus élevé que les autres méthodes de communication à distance. Un niveau de technologie avancé permet aujourd'hui de protéger le réseau privé contre tout accès non autorisé.
4. L'emplacement géographique réel des utilisateurs est protégé et n'est pas exposé aux réseaux publics ou partagés comme Internet.
5. L'ajout de nouveaux utilisateurs ou de nouveaux groupes d'utilisateurs au réseau est facile car les VPN sont facilement évolutifs. Il est possible de développer le réseau sans avoir besoin de composants supplémentaires ni de configuration compliquée.

Risques d'utilisation d'une connexion VPN

1. Risque de sécurité dû à une mauvaise configuration. Étant donné que la conception et la mise en oeuvre d'un VPN peuvent être compliquées, il est nécessaire de confier la tâche de configuration de la connexion à un professionnel expérimenté et hautement expérimenté afin de s'assurer que la sécurité du réseau privé ne soit pas compromise.
2. Fiabilité. Étant donné qu'une connexion VPN nécessite une connexion Internet, il est important d'avoir un fournisseur ayant une réputation éprouvée et testée pour fournir un excellent service Internet et garantir un temps d'arrêt minimal voire nul.
3. Évolutivité. S'il s'agit d'une situation dans laquelle il est nécessaire d'ajouter une nouvelle

infrastructure ou un nouvel ensemble de configurations, des problèmes techniques peuvent survenir en raison d'incompatibilité, en particulier s'il s'agit de produits ou de fournisseurs différents autres que ceux que vous utilisez déjà.

4. Problèmes de sécurité pour les appareils mobiles. Lors de l'ouverture de la connexion VPN sur un appareil mobile, des problèmes de sécurité peuvent survenir, en particulier lorsque l'appareil mobile est connecté au réseau local sans fil.
5. Vitesses de connexion lentes. Si vous utilisez un client VPN qui fournit un service VPN gratuit, il est probable que votre connexion sera également lente car ces fournisseurs ne donnent pas la priorité aux vitesses de connexion.

Conditions requises pour l'utilisation du client VPN TheGreenBow

Les éléments suivants doivent d'abord être configurés sur le routeur VPN et seront appliqués au client VPN TheGreenBow en cliquant [ici](#) pour établir une connexion.

1. [Créer un profil client-site sur la passerelle VPN](#)
2. [Créer un groupe d'utilisateurs sur la passerelle VPN](#)
3. [Créer un compte d'utilisateur sur la passerelle VPN](#)
4. [Créer un profil IPSec sur la passerelle VPN](#)
5. [configuration des paramètres des phases I et II sur la passerelle VPN](#)

Périphériques pertinents

- Gamme RV34x

Version du logiciel

- 1.0.01.17

Utiliser le client VPN TheGreenBow

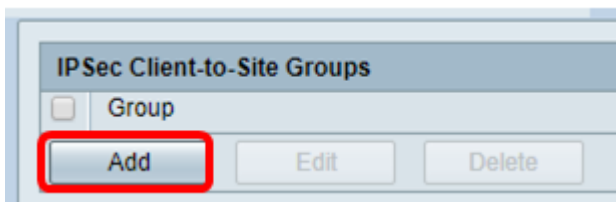
[Créer un profil client-site sur le routeur](#)

Étape 1. Connectez-vous à l'utilitaire Web du routeur RV34x et choisissez **VPN > Client-to-Site**.



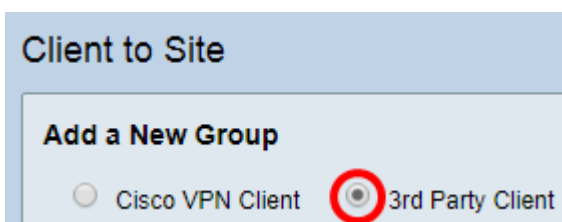
Note: Les images de cet article proviennent du routeur RV340. Les options peuvent varier en fonction du modèle de votre périphérique.

Étape 2. Cliquez sur **Add**.



Étape 3. Cliquez sur **Client tiers**.

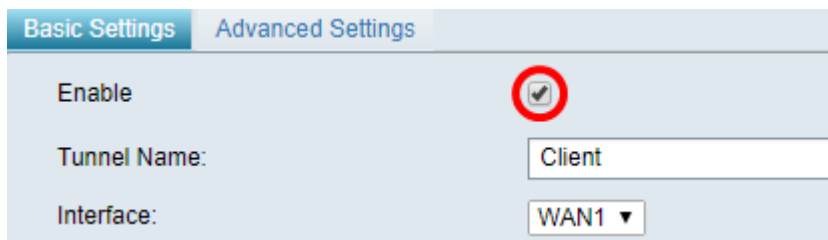
Note: AnyConnect est un exemple de client VPN Cisco, tandis que TheGreenBow VPN Client est un exemple de client VPN tiers.



Note: Dans cet exemple, le client tiers est sélectionné.

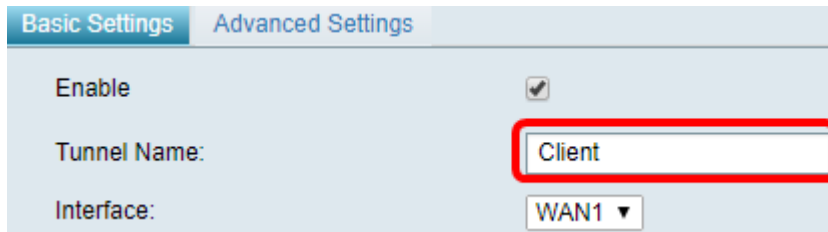
Étape 4. Sous l'onglet Basic Settings (Paramètres de base), cochez la case **Enable (Activer)**

pour vous assurer que le profil VPN est actif.



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'.

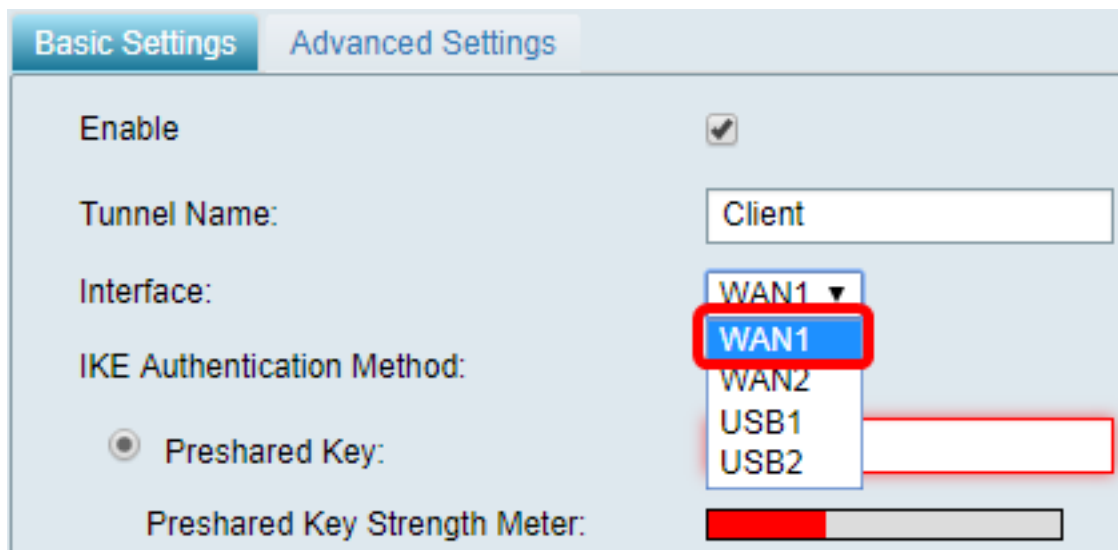
Étape 5. Entrez un nom pour la connexion VPN dans le champ *Tunnel Name*.



This screenshot is similar to the previous one, but the 'Tunnel Name' input field, which contains 'Client', is highlighted with a red rectangular border.

Note: Dans cet exemple, **Client** est saisi.

Étape 6. Sélectionnez l'interface à utiliser dans la liste déroulante Interface. Les options sont WAN1, WAN2, USB1 et USB2 qui utiliseront l'interface correspondante sur le routeur pour la connexion VPN.



The screenshot shows the 'Basic Settings' tab with the 'Interface' dropdown menu open. The menu lists 'WAN1', 'WAN2', 'USB1', and 'USB2'. 'WAN1' is highlighted with a blue background and a red border. The 'Tunnel Name' field contains 'Client'. 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.

Note: Les options dépendent du modèle de routeur que vous utilisez. Dans cet exemple, WAN1 est choisi.

Étape 7. Sélectionnez une méthode d'authentification IKE. Les options sont les suivantes :

- Preshared Key : cette option nous permet d'utiliser un mot de passe partagé pour la connexion VPN.
- Certificate : cette option utilise un certificat numérique qui contient des informations telles que le nom, ou l'adresse IP, le numéro de série, la date d'expiration du certificat et une copie de la clé publique du titulaire du certificat.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Certificate:

Note: Dans cet exemple, la clé prépartagée est choisie.

Étape 8. Entrez le mot de passe de connexion dans le champ *Preshared Key* (Clé prépartagée).

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Étape 9. (Facultatif) Décochez la case Minimum Preshared Key Complexity **Enable** pour pouvoir utiliser un mot de passe simple.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Note: Dans cet exemple, la Complexité de clé prépartagée minimale reste activée.

Étape 10. (Facultatif) Cochez la case Afficher le texte brut lors de la modification **Activer** pour afficher le mot de passe en texte brut.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

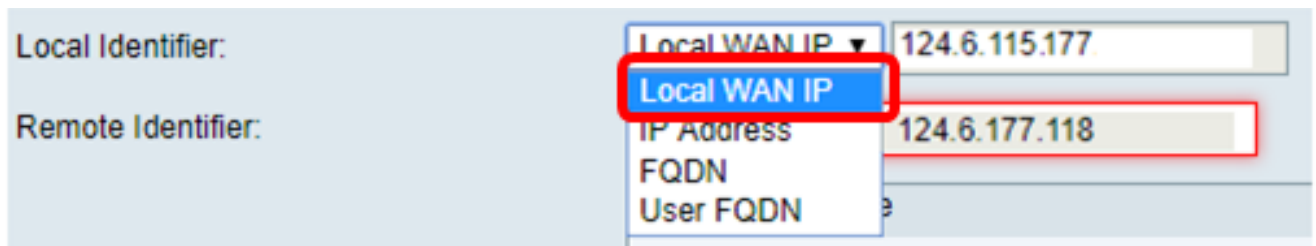
Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Note: Dans cet exemple, affichez le texte brut lorsque la modification est désactivée.

Étape 11. Sélectionnez un identificateur local dans la liste déroulante Local Identifier. Les options sont les suivantes :

- Local WAN IP : cette option utilise l'adresse IP de l'interface WAN (Wide Area Network) de la passerelle VPN.
- IP Address : cette option vous permet de saisir manuellement une adresse IP pour la connexion VPN.
- FQDN : cette option est également appelée FQDN (Fully Qualified Domain Name). Il vous permet d'utiliser un nom de domaine complet pour un ordinateur spécifique sur Internet.
- User FQDN : cette option vous permet d'utiliser un nom de domaine complet pour un utilisateur spécifique sur Internet.

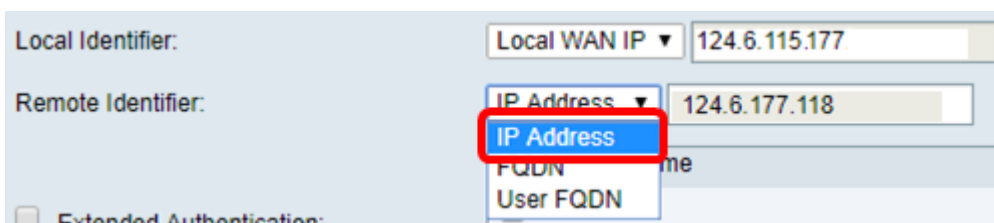


The screenshot shows the 'Local Identifier' dropdown menu. The 'Local WAN IP' option is selected and highlighted with a red box. The text 'Local WAN IP' is also visible in the dropdown list. The IP address '124.6.115.177' is entered in the adjacent text box. Below it, the 'Remote Identifier' section shows the 'IP Address' option selected and highlighted with a red box, with the IP address '124.6.177.118' entered in its text box.

Note: Dans cet exemple, l'adresse IP WAN locale est choisie. Avec cette option, l'adresse IP WAN locale est automatiquement détectée.

Étape 12. (Facultatif) Choisissez un identificateur pour l'hôte distant. Les options sont les suivantes :

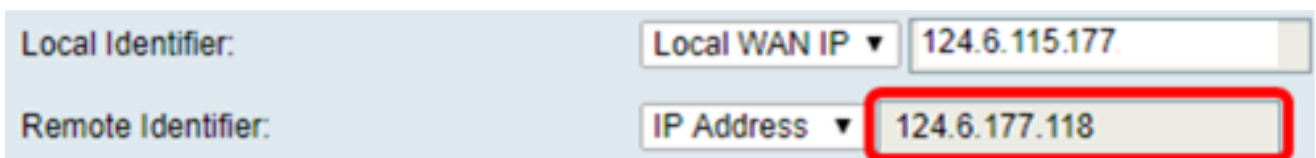
- IP Address : cette option utilise l'adresse IP WAN du client VPN.
- FQDN : cette option vous permet d'utiliser un nom de domaine complet pour un ordinateur spécifique sur Internet.
- User FQDN : cette option vous permet d'utiliser un nom de domaine complet pour un utilisateur spécifique sur Internet.



The screenshot shows the 'Remote Identifier' dropdown menu. The 'IP Address' option is selected and highlighted with a red box. The IP address '124.6.177.118' is entered in the adjacent text box. The 'Local Identifier' section above it shows 'Local WAN IP' selected and the IP address '124.6.115.177' entered. The 'Extended Authentication' checkbox is visible and unchecked.

Note: Dans cet exemple, l'adresse IP est choisie.

Étape 13. Entrez l'identificateur distant dans le champ *Identificateur distant*.



The screenshot shows the 'Remote Identifier' section. The 'IP Address' dropdown is selected, and the IP address '124.6.177.118' is entered in the text box and highlighted with a red box. The 'Local Identifier' section above it shows 'Local WAN IP' selected and the IP address '124.6.115.177' entered.

Note: Dans cet exemple, 124.6.115.177 est entré.

Étape 14. (Facultatif) Cochez la case **Authentification étendue** pour activer la fonction. Lorsqu'elle est activée, cette option fournit un niveau d'authentification supplémentaire qui nécessite que les utilisateurs distants saisissent leurs informations d'identification avant d'obtenir l'accès au VPN.

The screenshot shows a configuration interface. On the left, there is a checkbox labeled 'Extended Authentication:' which is currently unchecked and circled in red. To the right, there is a dropdown menu labeled 'Group Name' with a small square icon to its left. Below the dropdown menu are two buttons: 'Add' and 'Delete'.

Note: Dans cet exemple, l'authentification étendue n'est pas cochée.

Étape 15. Sous Nom du groupe, cliquez sur **Ajouter**.

This screenshot is similar to the previous one, but the 'Add' button is now highlighted with a red rectangular box, indicating it should be clicked.

Étape 16. Sélectionnez le groupe qui utilisera l'authentification étendue dans la liste déroulante Nom du groupe.

The screenshot shows the 'Group Name' dropdown menu open. The list of options includes 'admin', 'admin', 'guest', 'IPSecVPN', and 'VPN'. The 'VPN' option is highlighted in blue and circled in red, indicating it is the selected group.

Note: Dans cet exemple, VPN est choisi.

Étape 17. Sous Pool Range for Client LAN, saisissez la première adresse IP pouvant être attribuée à un client VPN dans le champ *Start IP*.

The screenshot shows the 'Pool Range for Client LAN' section. The 'Start IP:' field contains the value '10.10.100.100', which is circled in red. The 'End IP:' field contains the value '10.10.100.245'.

Note: Dans cet exemple, 10.10.100.100 est entré.

Étape 18. Entrez la dernière adresse IP pouvant être attribuée à un client VPN dans le champ *End IP*.

This screenshot is similar to the previous one, but the 'End IP:' field now contains the value '10.10.100.245', which is circled in red. The 'Start IP:' field still contains '10.10.100.100'.

Note: Dans cet exemple, 10.10.100.245 est entré.

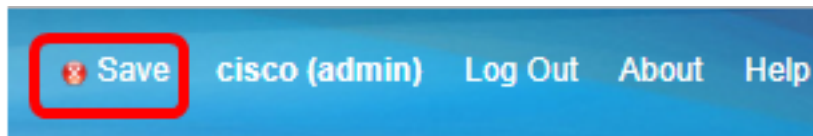
Étape 19. Cliquez sur Apply.

Pool Range for Client LAN:

Start IP:

End IP:

Étape 20. Cliquez sur **Save**.

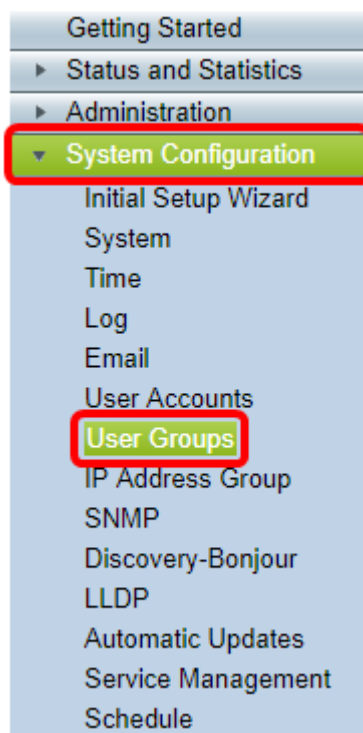


Vous devez maintenant avoir configuré le profil client-site sur le routeur pour le client VPN TheGreenBow.

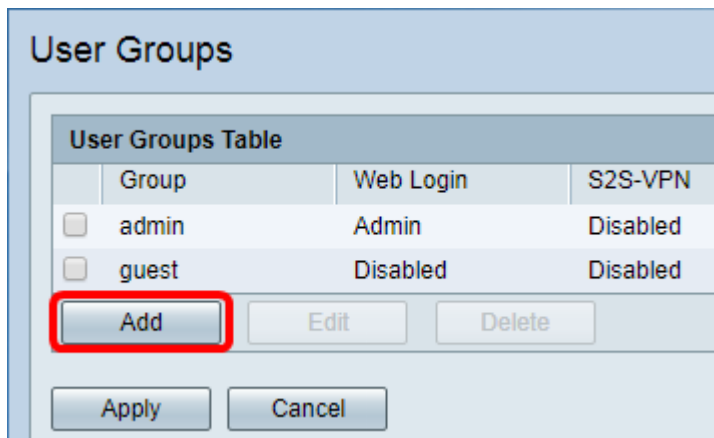
[Créer un groupe d'utilisateurs](#)

Étape 1. Connectez-vous à l'utilitaire Web du routeur et sélectionnez **Configuration système > Groupes d'utilisateurs**.

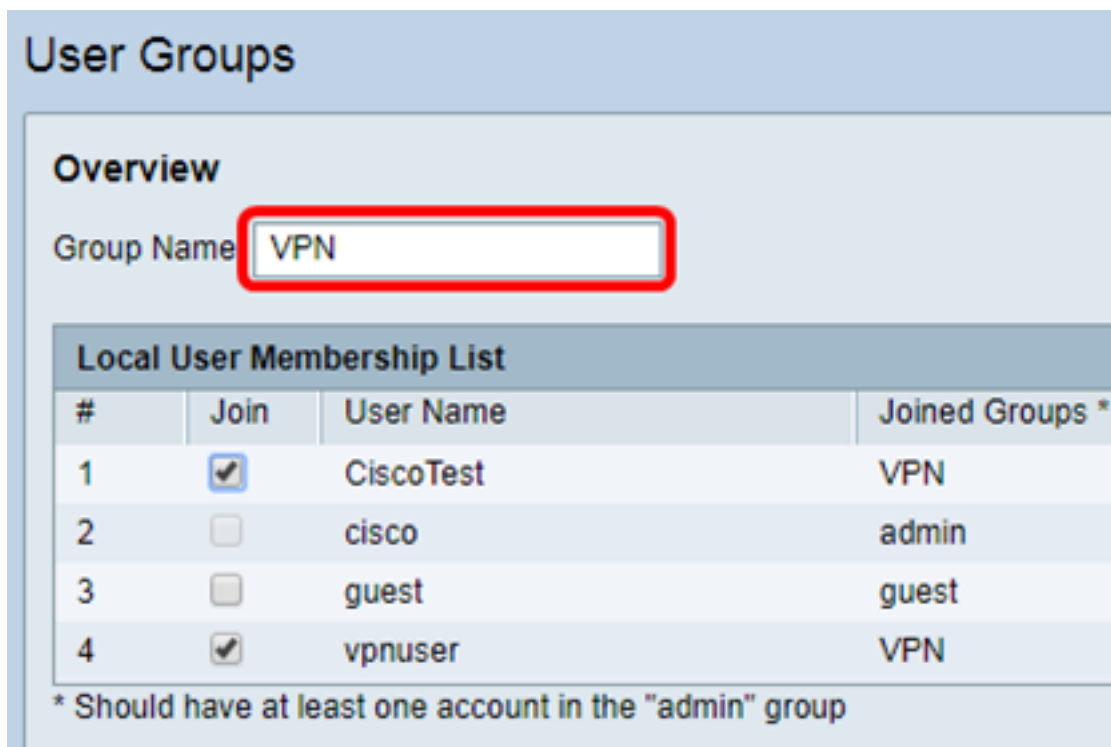
Note: Les images de cet article proviennent d'un routeur RV340. Les options peuvent varier en fonction du modèle de votre périphérique.



Étape 2. Cliquez sur **Ajouter** pour ajouter un groupe d'utilisateurs.



Étape 3. Dans la zone Vue d'ensemble, saisissez le nom du groupe dans le champ *Nom du groupe*.



Note: Dans cet exemple, VPN est utilisé.

Étape 4. Sous Local Membership List, cochez les cases des noms d'utilisateurs qui doivent appartenir au même groupe.

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

Note: Dans cet exemple, CiscoTest et vpnuser sont sélectionnés.

Étape 5. Sous Services, sélectionnez une autorisation à accorder aux utilisateurs du groupe. Les options sont les suivantes :

- Disabled : cette option signifie que les membres du groupe ne sont pas autorisés à accéder à l'utilitaire Web via un navigateur.
- Read Only : cette option signifie que les membres du groupe ne peuvent lire l'état du système qu'après leur connexion. Ils ne peuvent modifier aucun des paramètres.
- Administrateur : cette option donne aux membres du groupe des privilèges de lecture et d'écriture et permet de configurer l'état du système.

Services

Web Login Disabled Read Only Administrator

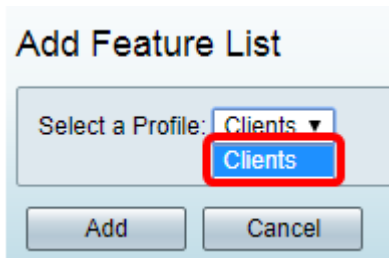
Note: Dans cet exemple, Lecture seule est sélectionnée.

Étape 6. Dans la table In-use des membres de profil EzVPN/tiers, cliquez sur **Add**.

EzVPN/3rd Party

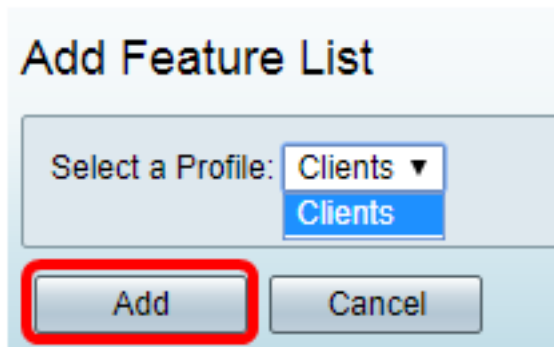
EzVPN/3rd Party Profile Member In-use Table	
#	Group Name

Étape 7. Sélectionnez un profil dans la liste déroulante Sélectionner un profil. Les options peuvent varier en fonction des profils configurés sur la passerelle VPN.

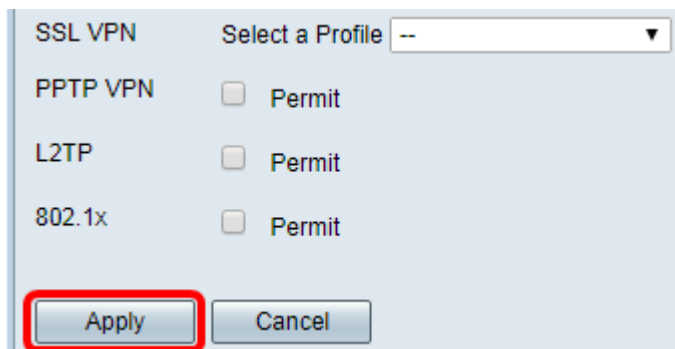


Note: Dans cet exemple, Clients est sélectionné.

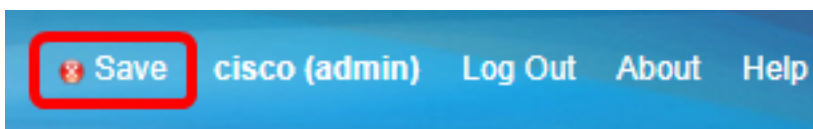
Étape 8. Cliquez sur **Add**.



Étape 9. Cliquez sur **Apply**.



Étape 10. Cliquez sur **Save**.

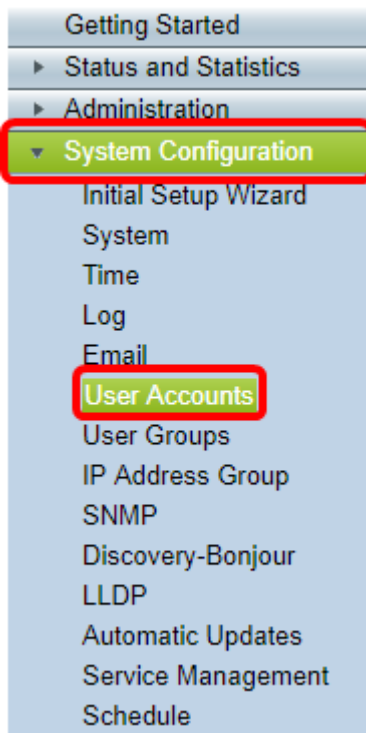


Vous devez maintenant avoir créé un groupe d'utilisateurs sur le routeur de la gamme RV34x.

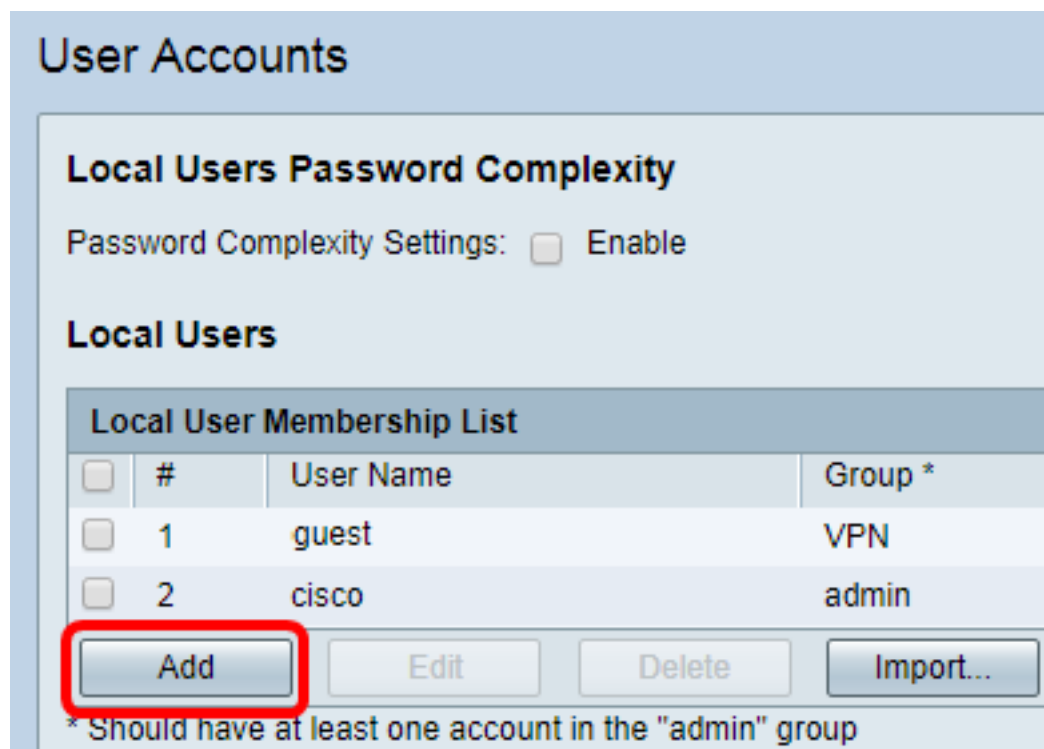
[Créer un compte d'utilisateur](#)

Étape 1. Connectez-vous à l'utilitaire Web du routeur et sélectionnez **Configuration système > Comptes d'utilisateurs**.

Note: Les images de cet article proviennent d'un routeur RV340. Les options peuvent varier en fonction du modèle de votre périphérique.



Étape 2. Dans la zone Liste des membres des utilisateurs locaux, cliquez sur **Ajouter**.



Étape 3. Entrez un nom pour l'utilisateur dans le champ *Nom d'utilisateur*.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Note: Dans cet exemple, CiscoTest est entré.

Étape 4. Entrez le mot de passe utilisateur dans le champ *Nouveau mot de passe*.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Étape 5. Confirmez le mot de passe dans la zone *Nouveau mot de passe Confirmer*.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Étape 6. Sélectionnez un groupe dans la liste déroulante Groupe. Il s'agit du groupe auquel l'utilisateur sera associé.

Group

Note: Dans cet exemple, VPN est choisi.

Étape 7. Cliquez sur Apply.

User Accounts

Add User Account

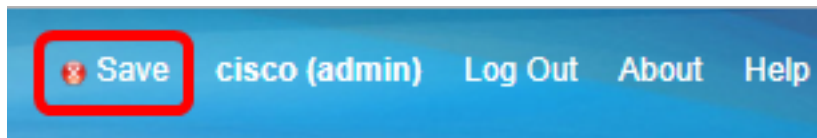
User Name

New Password

New Password Confirm

Group

Étape 8. Cliquez sur **Save**.



Vous devez maintenant avoir créé un compte d'utilisateur sur votre routeur de la gamme RV34x.

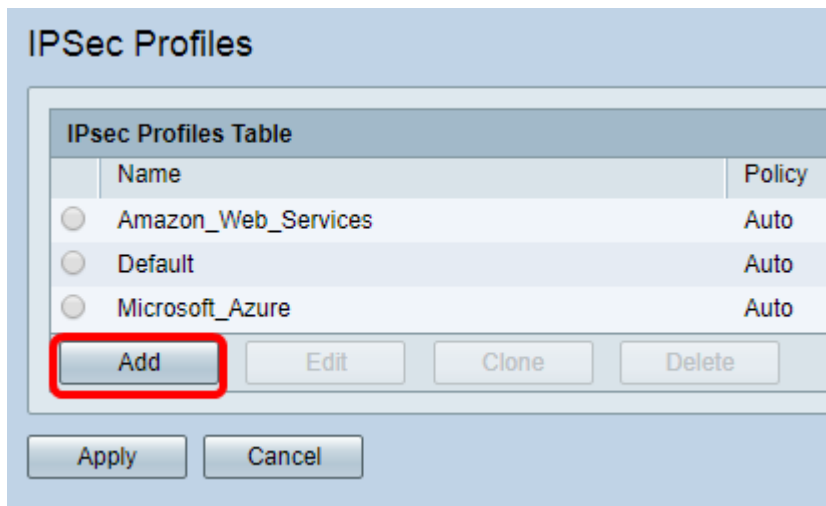
[Configurer le profil IPSec](#)

Étape 1. Connectez-vous à l'utilitaire Web du routeur RV34x et choisissez **VPN > IPSec Profiles**.



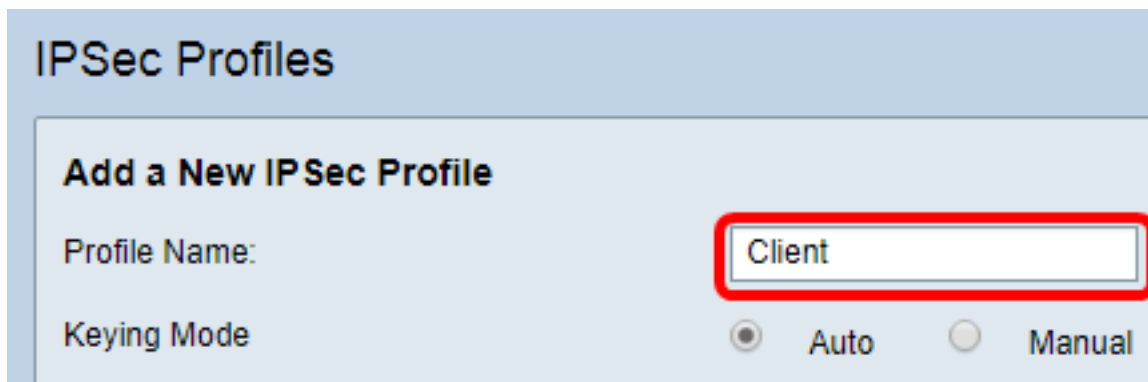
Note: Les images de cet article proviennent du routeur RV340. Les options peuvent varier en fonction du modèle de votre périphérique.

Étape 2. Le tableau Profils IPSec affiche les profils existants. Cliquez sur **Ajouter** pour créer un nouveau profil.



Note: Amazon_Web_Services, Default et Microsoft_Azure sont des profils par défaut.

Étape 3. Créez un nom pour le profil dans le champ *Nom du profil*. Le nom du profil ne doit contenir que des caractères alphanumériques et un trait de soulignement (_) pour les caractères spéciaux.



Note: Dans cet exemple, Client est saisi.

Étape 4. Cliquez sur une case d'option pour déterminer la méthode d'échange de clés que le profil utilisera pour s'authentifier. Les options sont les suivantes :

- Auto : les paramètres de stratégie sont définis automatiquement. Cette option utilise une stratégie IKE (Internet Key Exchange) pour l'intégrité des données et les échanges de clés de chiffrement. Si cette option est sélectionnée, les paramètres de configuration de la zone Paramètres de stratégie automatique sont activés. Si cette option est sélectionnée, passez à [Configurer les paramètres automatiques](#).
- Manual : cette option vous permet de configurer manuellement les clés pour le chiffrement des données et l'intégrité du tunnel VPN. Si cette option est sélectionnée, les paramètres de configuration de la zone Manual Policy Parameters sont activés. Si cette option est sélectionnée, passez à [Configurer les paramètres manuels](#).

IPSec Profiles

Add a New IPSec Profile

Profile Name:

Keying Mode Auto Manual

Note: Dans cet exemple, Auto a été sélectionné.

[Configurer les paramètres des phases I et II](#)

Étape 1. Dans la zone Options de phase 1, sélectionnez le groupe Diffie-Hellman (DH) approprié à utiliser avec la clé de phase 1 dans la liste déroulante Groupe DH. Diffie-Hellman est un protocole d'échange de clés cryptographiques utilisé dans la connexion pour échanger des ensembles de clés pré-partagés. La force de l'algorithme est déterminée par des bits. Les options sont les suivantes :

- Group2-1024 bit : cette option calcule la clé plus lentement, mais elle est plus sécurisée que le groupe 1.
- Group5-1536 bit : cette option calcule la clé la plus lente, mais la plus sécurisée.

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime:

Perfect Forward Secrecy: Enable

Note: Dans cet exemple, le bit Group5-1536 est choisi.

Étape 2. Dans la liste déroulante Encryption (Cryptage), choisissez une méthode de cryptage pour chiffrer et déchiffrer les données utiles ESP (Encapsulating Security Payload) et ISAKMP (Internet Security Association and Key Management Protocol). Les options sont les suivantes :

- 3DES - Triple Data Encryption Standard.
- AES-128 — Advanced Encryption Standard utilise une clé de 128 bits.
- AES-192 — Advanced Encryption Standard utilise une clé 192 bits.
- AES-256 — Advanced Encryption Standard utilise une clé de 256 bits.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: AES-128

SA Lifetime: AES-192
AES-256

Perfect Forward Secrecy: Enable

Note: AES est la méthode standard de cryptage sur DES et 3DES pour ses performances et sa sécurité accrues. Le renforcement de la clé AES augmentera la sécurité en réduisant les performances. Dans cet exemple, AES-128 est choisi.

Étape 3. Dans la liste déroulante Authentification, sélectionnez une méthode d'authentification qui déterminera comment ESP et ISAKMP sont authentifiés. Les options sont les suivantes :

- MD5 — L'algorithme Message-Digest a une valeur de hachage de 128 bits.
- SHA-1 — L'algorithme de hachage sécurisé a une valeur de hachage de 160 bits.
- SHA2-256 — Algorithme de hachage sécurisé avec une valeur de hachage de 256 bits.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: MD5
SHA1
SHA2-256

Perfect Forward Secrecy: Enable

Note: MD5 et SHA sont deux fonctions de hachage cryptographique. Ils prennent une donnée, la compactent et créent une sortie hexadécimale unique qui ne peut généralement pas être reproduite. Dans cet exemple, SHA1 est sélectionné.

Étape 4. Dans le champ *Durée de vie de la SA*, saisissez une valeur comprise entre 120 et 86 400. Il s'agit de la durée pendant laquelle l'association de sécurité IKE (Internet Key Exchange) restera active dans la phase. La valeur par défaut est 28800.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

Note: Dans cet exemple, 86400 est entré.

Étape 5. (Facultatif) Cochez la case **Activer** Perfect Forward Secrecy pour générer une nouvelle clé pour le chiffrement et l'authentification du trafic IPSec.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

Note: Dans cet exemple, Perfect Forward Secrecy est activé.

Étape 6. Dans la liste déroulante Sélection de protocole de la zone Options de phase II, sélectionnez un type de protocole à appliquer à la deuxième phase de la négociation. Les options sont les suivantes :

- ESP : cette option encapsule les données à protéger. Si cette option est sélectionnée, passez à l'[étape 7](#) pour choisir une méthode de cryptage.
- AH : cette option est également appelée en-tête d'authentification (AH). Il s'agit d'un protocole de sécurité qui fournit une authentification des données et un service anti-relecture en option. AH est incorporé dans le datagramme IP à protéger. Si cette option est sélectionnée, passez à l'[étape 8](#).

Phase II Options

Protocol Selection: ESP

Encryption: ESP

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

Note: Dans cet exemple, ESP est choisi.

Étape 7. Si ESP a été choisi à l'étape 6, choisissez une méthode d'authentification qui déterminera comment ESP et ISAKMP sont authentifiés. Les options sont les suivantes :

- 3DES - Triple Data Encryption Standard
- AES-128 — Advanced Encryption Standard utilise une clé de 128 bits.
- AES-192 — Advanced Encryption Standard utilise une clé 192 bits.
- AES-256 — Advanced Encryption Standard utilise une clé de 256 bits.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: AES-128

SA Lifetime:

DH Group: Group5 - 1536 bit

Apply Cancel

Note: Dans cet exemple, AES-128 est choisi.

Étape 8. Dans la liste déroulante Authentification, sélectionnez une méthode d'authentification qui déterminera comment ESP et ISAKMP sont authentifiés. Les options sont les suivantes :

- MD5 — L'algorithme Message-Digest a une valeur de hachage de 128 bits.
- SHA-1 — L'algorithme de hachage sécurisé a une valeur de hachage de 160 bits.
- SHA2-256 — Algorithme de hachage sécurisé avec une valeur de hachage de 256 bits.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime:

DH Group:

Apply Cancel

Note: Dans cet exemple, SHA1 est sélectionné.

Étape 9. Dans le champ *Durée de vie de la SA*, saisissez une valeur comprise entre 120 et 28 800. Il s'agit de la durée pendant laquelle l'association de sécurité IKE restera active dans cette phase. La valeur par défaut est 3600.

Étape 10. Dans la liste déroulante Groupe DH, sélectionnez un groupe DH à utiliser avec la clé dans la phase 2. Les options sont les suivantes :

- Group2-1024 bit : cette option calcule la clé plus lentement, mais elle est plus sécurisée que Group1.
- Group5-1536 bit : cette option calcule la clé la plus lente, mais la plus sécurisée.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

Note: Dans cet exemple, 3600 est entré.

Étape 11. Cliquez sur Apply.

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:

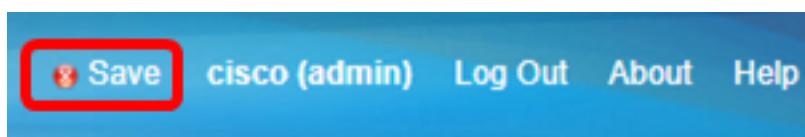
Encryption:

Authentication:

SA Lifetime:

DH Group:

Étape 12. Cliquez sur **Enregistrer** pour enregistrer la configuration de manière permanente.



Vous devez maintenant avoir correctement configuré un profil IPSec automatique sur votre routeur de la gamme RV34x.

[Configuration des paramètres manuels](#)

Étape 1. Dans le champ *SPI-Incoming*, saisissez une valeur hexadécimale comprise entre 100 et FFFFFFF pour la balise SPI (Security Parameter Index) pour le trafic entrant sur la connexion VPN. La balise SPI est utilisée pour distinguer le trafic d'une session du trafic d'autres sessions.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Note: Dans cet exemple, 0xABCD est entré.

Étape 2. Dans le champ *SPI-Outgoing*, saisissez une valeur hexadécimale comprise entre 100 et FFFFFFF pour la balise SPI du trafic sortant sur la connexion VPN.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Note: Dans cet exemple, 0x1234 est entré.

Étape 3. Sélectionnez une valeur de chiffrement dans la liste déroulante. Les options sont les suivantes :

- 3DES - Triple Data Encryption Standard
- AES-128 — Advanced Encryption Standard utilise une clé de 128 bits.
- AES-192 — Advanced Encryption Standard utilise une clé 192 bits.

SPI Incoming:

SPI Outgoing:

Encryption:

3DES

AES-128

AES-192

✓ AES-256

Note: Dans cet exemple, AES-256 est choisi.

Étape 4. Dans le champ *Key-In*, saisissez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'étape 3.

Key-In:

Key-Out:

Note: Dans cet exemple, 123456789123456789123... est entré.

Étape 5. Dans le champ *Clé de sortie*, saisissez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'étape 3.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

Note: Dans cet exemple, 1a1a1a1a1a1a1a1a12121212... est entré.

Étape 6. Sélectionnez une méthode d'authentification dans la liste déroulante Authentication. Les options sont les suivantes :

- MD5 — L'algorithme Message-Digest a une valeur de hachage de 128 bits.
- SHA-1 — L'algorithme de hachage sécurisé a une valeur de hachage de 160 bits.
- SHA2-256 — Algorithme de hachage sécurisé avec une valeur de hachage de 256 bits.

Authentication:	✓ MD5
Key-In	SHA1
Key-Out	SHA2-256

Note: Dans cet exemple, MD5 est sélectionné.

Étape 7. Dans le champ *Key-In*, saisissez une clé pour la stratégie entrante. La longueur de la clé dépend de l'algorithme choisi à l'étape 6.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

Note: Dans cet exemple, 123456789123456789123... est entré.

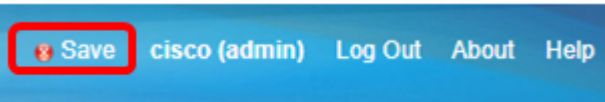
Étape 8. Dans le champ *Clé de sortie*, saisissez une clé pour la stratégie sortante. La longueur de la clé dépend de l'algorithme choisi à l'étape 6.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

Note: Dans cet exemple, 1a1a1a1a1a1a1a1a12121212... est entré.

Étape 9. Cliquez sur .

Étape 10. Cliquez sur **Enregistrer** pour enregistrer la configuration de manière permanente.

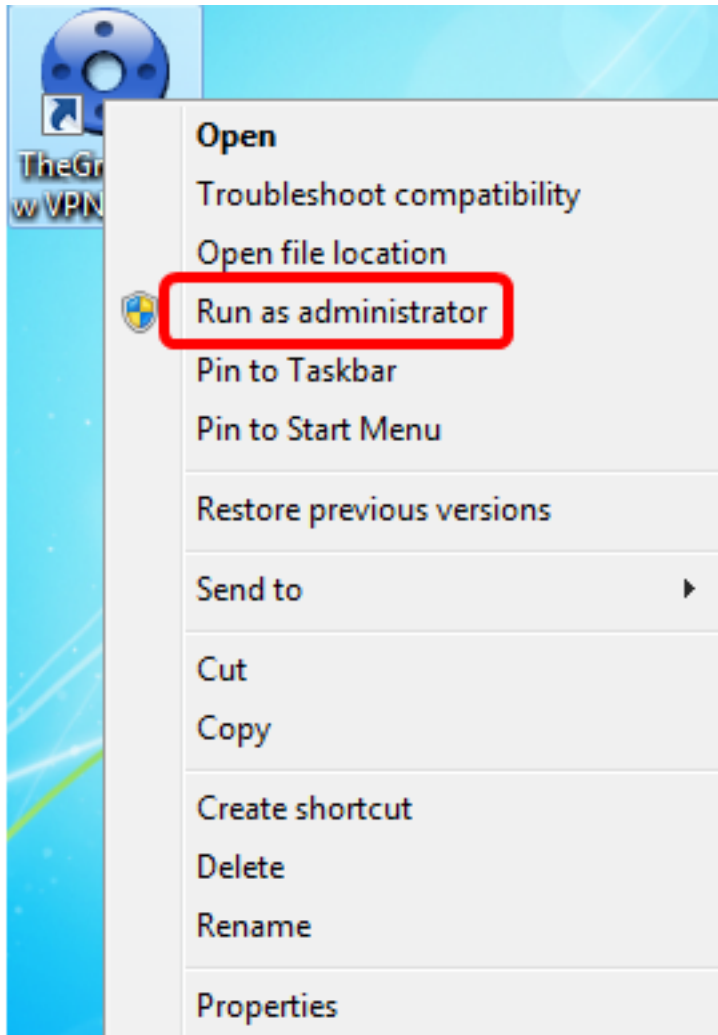


Vous devez maintenant avoir correctement configuré un profil IPsec manuel sur un routeur de la gamme RV34x.

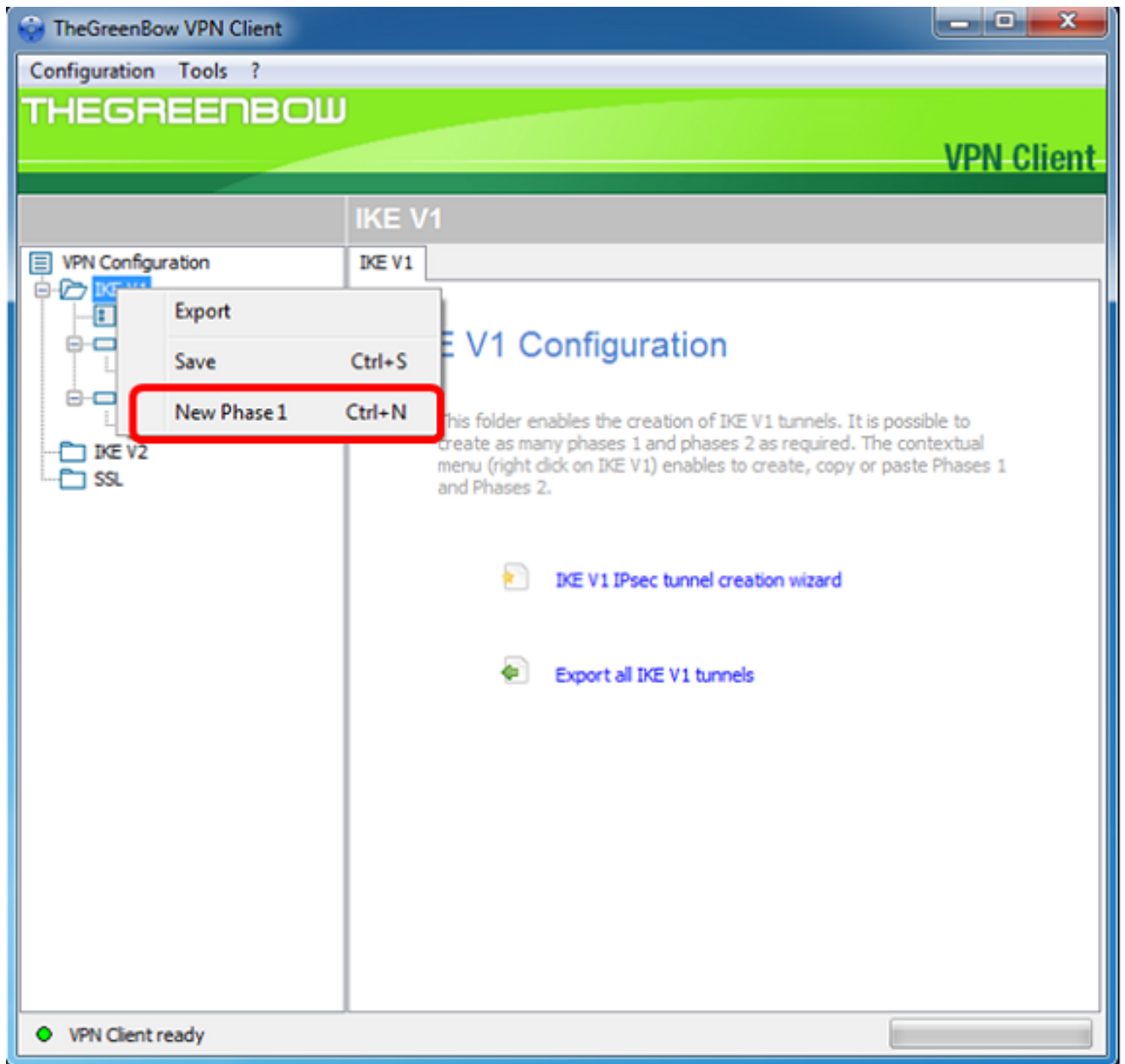
Configuration du logiciel client VPN TheGreenBow

Configuration des paramètres de phase 1

Étape 1. Cliquez avec le bouton droit sur l'icône Client VPN TheGreenBow et sélectionnez **Exécuter en tant qu'administrateur**.

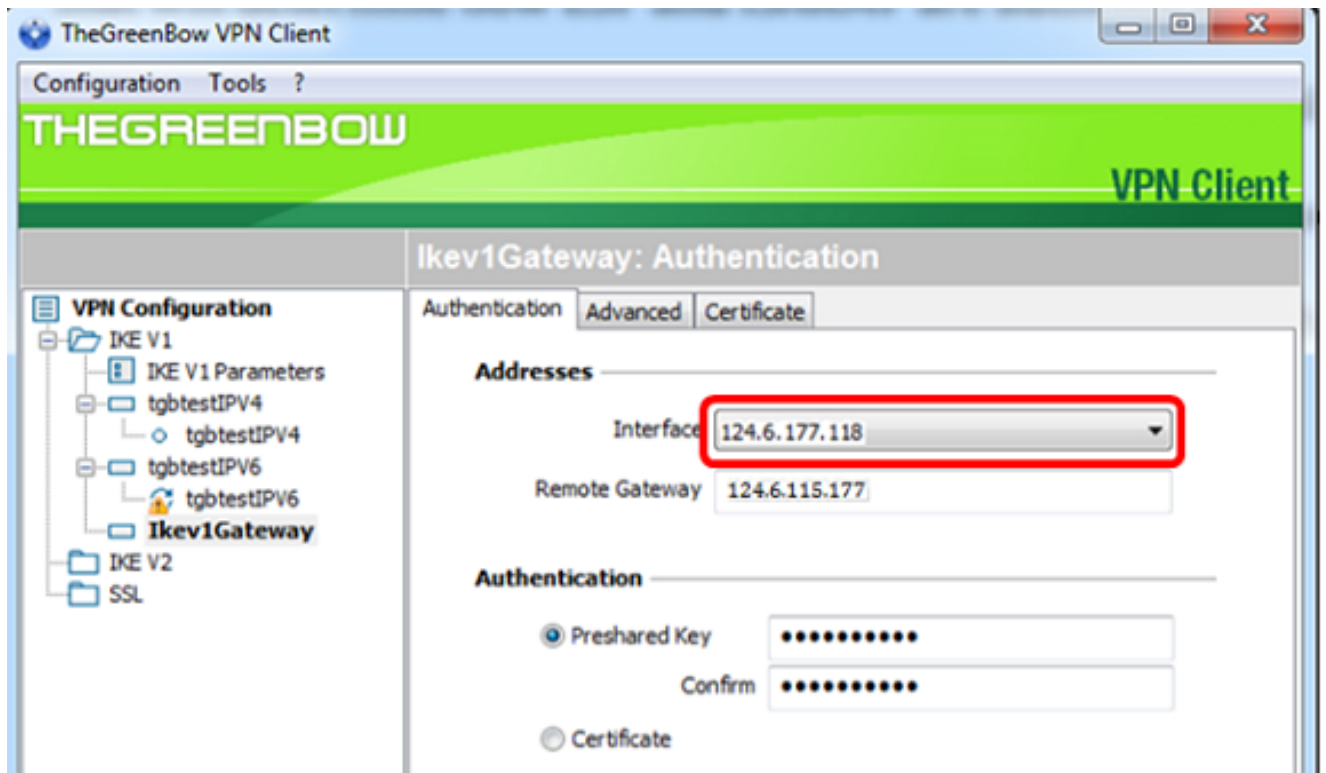


Étape 2. Dans le volet gauche sous Configuration VPN, cliquez avec le bouton droit sur **IKE V1** et choisissez **Nouvelle phase 1**.



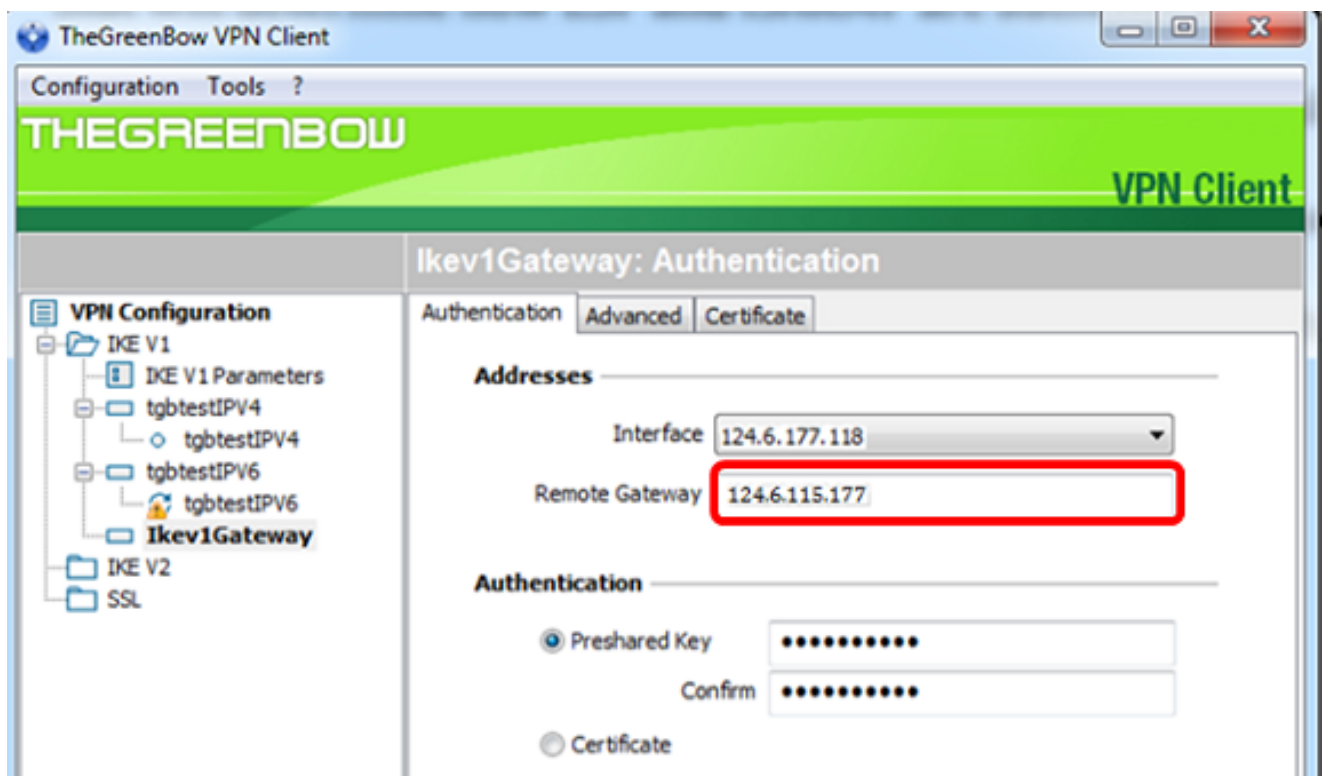
Étape 3. Dans l'onglet Authentification sous Adresses, vérifiez que l'adresse IP dans la zone Interface est identique à l'adresse IP WAN de l'ordinateur sur lequel le client VPN TheGreenBow est installé.

Note: Dans cet exemple, l'adresse IP est 124.6.177.118.



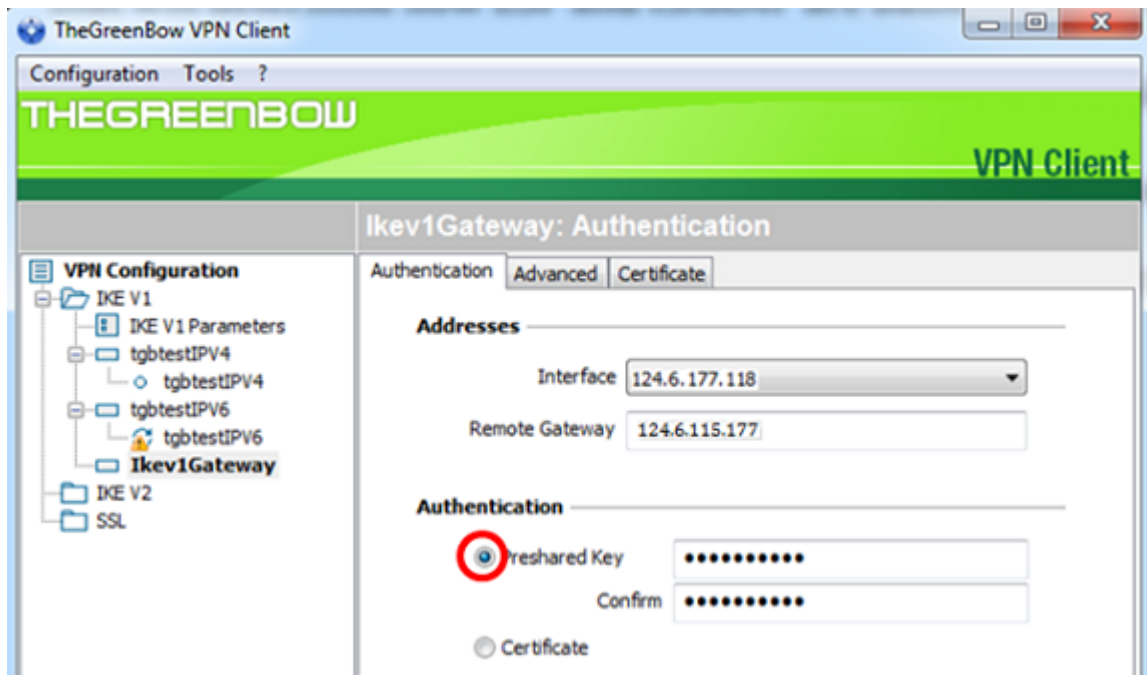
Étape 4. Entrez l'adresse de la passerelle distante dans le champ *Remote Gateway*.

Note: Dans cet exemple, l'adresse IP du routeur RV34x distant est 124.6.115.177.



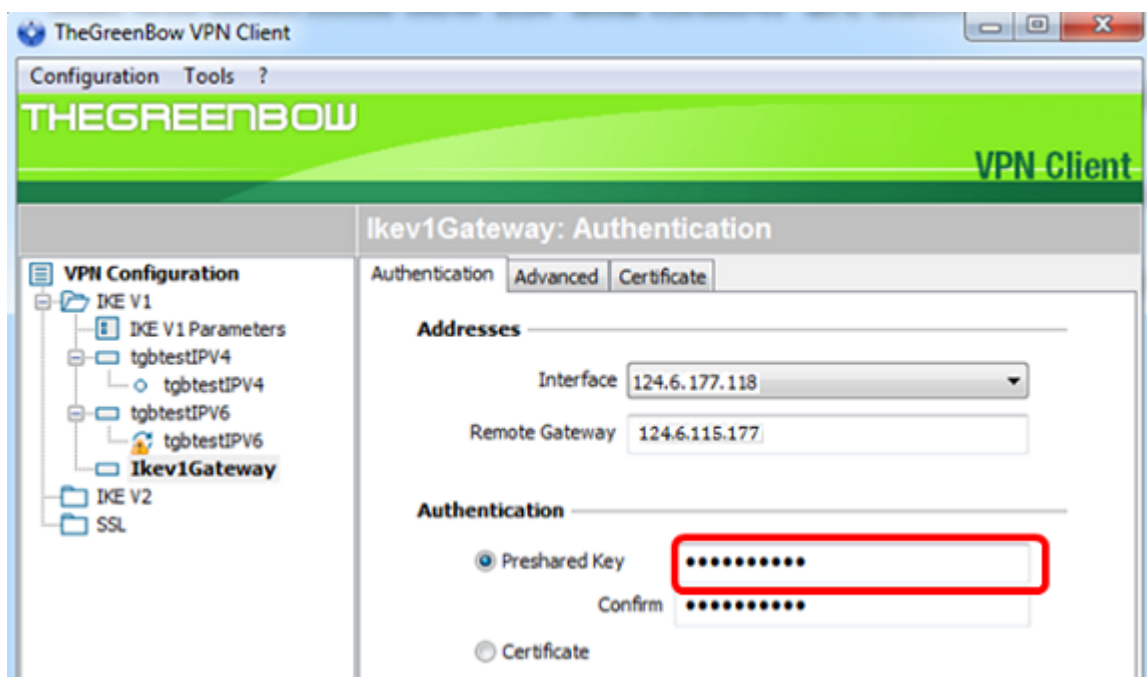
Étape 5. Sous Authentication, sélectionnez le type d'authentification. Les options sont les suivantes :

- Preshared Key : cette option permet à l'utilisateur d'utiliser un mot de passe configuré sur la passerelle VPN. Le mot de passe doit correspondre à celui de l'utilisateur pour pouvoir établir un tunnel VPN.
- Certificate : cette option utilise un certificat pour terminer la connexion entre le client VPN et la passerelle VPN.

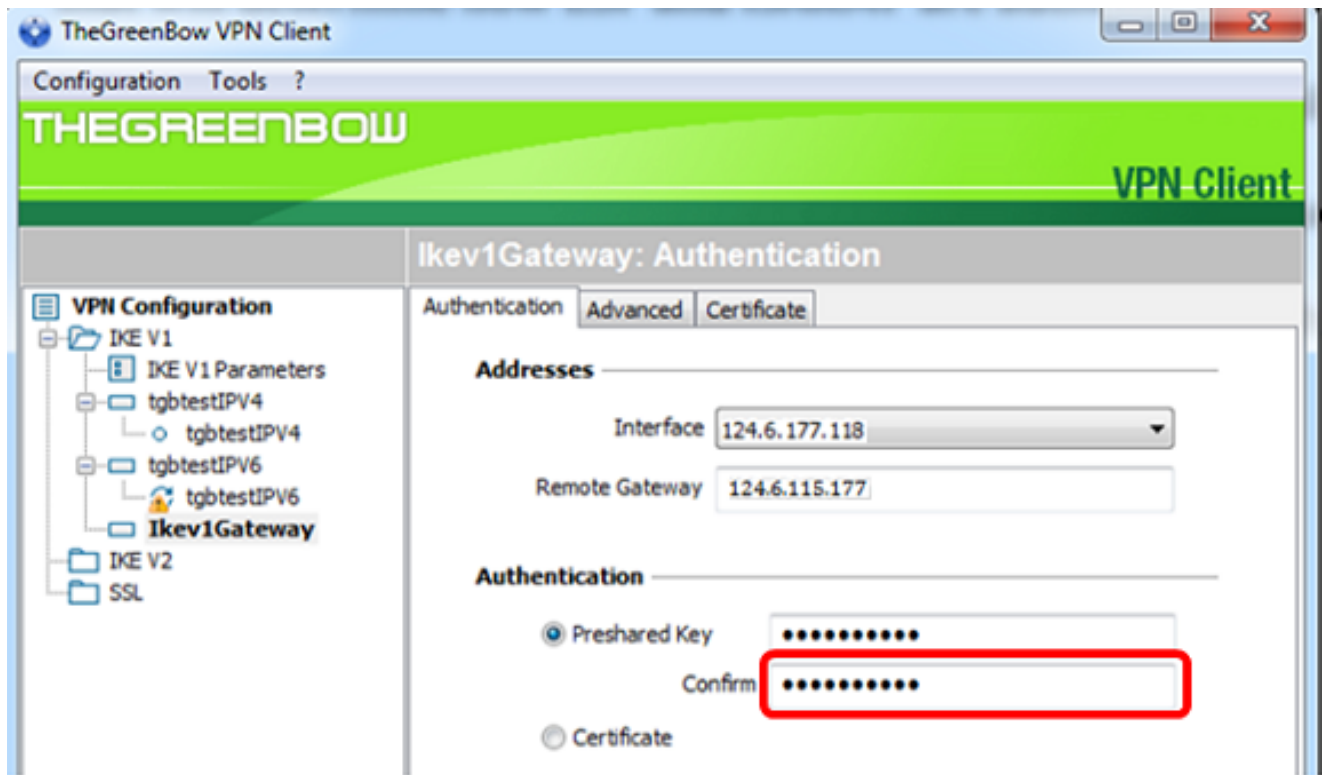


Note: Dans cet exemple, la clé pré-partagée est choisie pour correspondre à la configuration de la passerelle VPN RV34x.

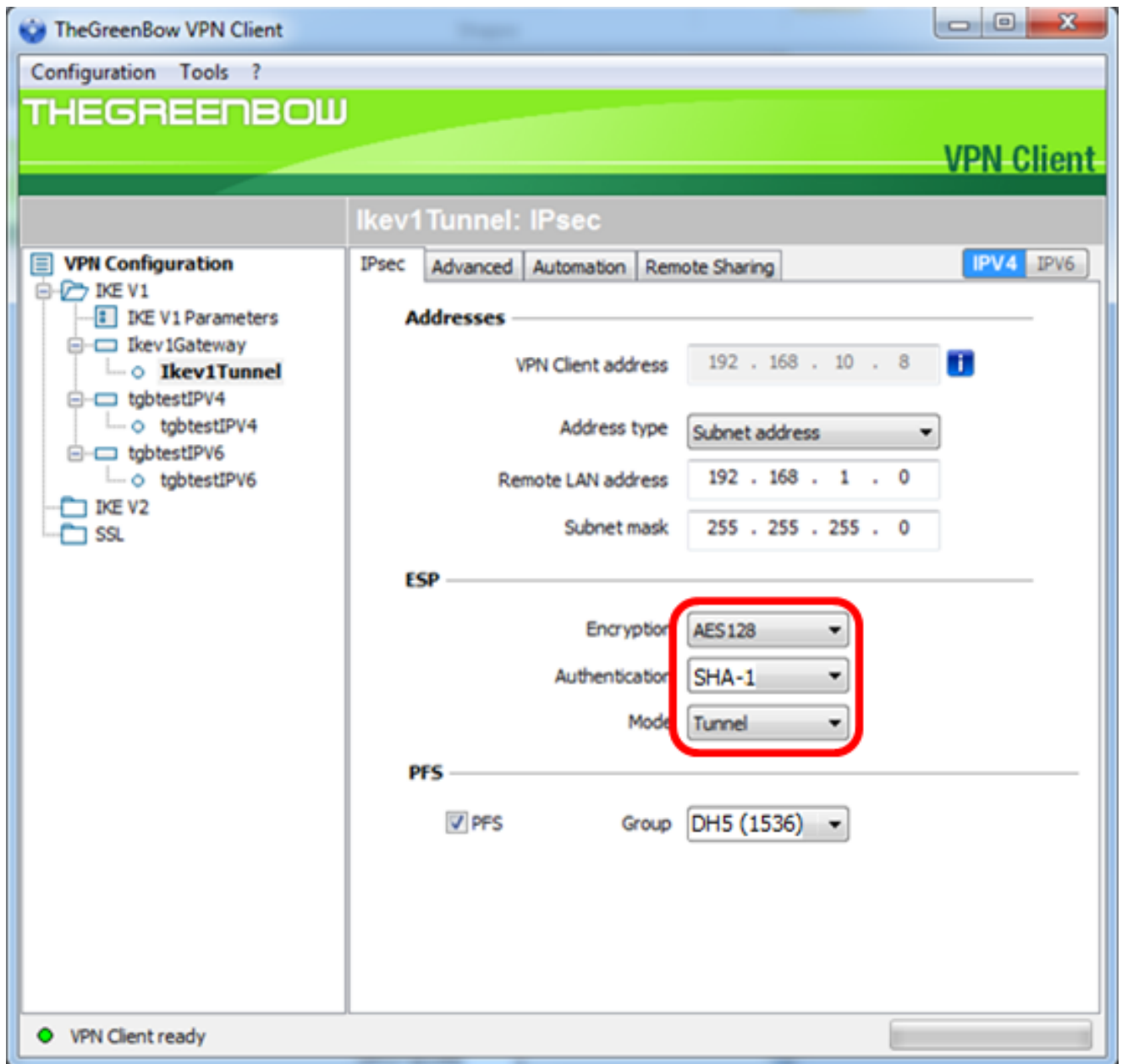
Étape 6. Saisissez la clé pré-partagée configurée dans le routeur.



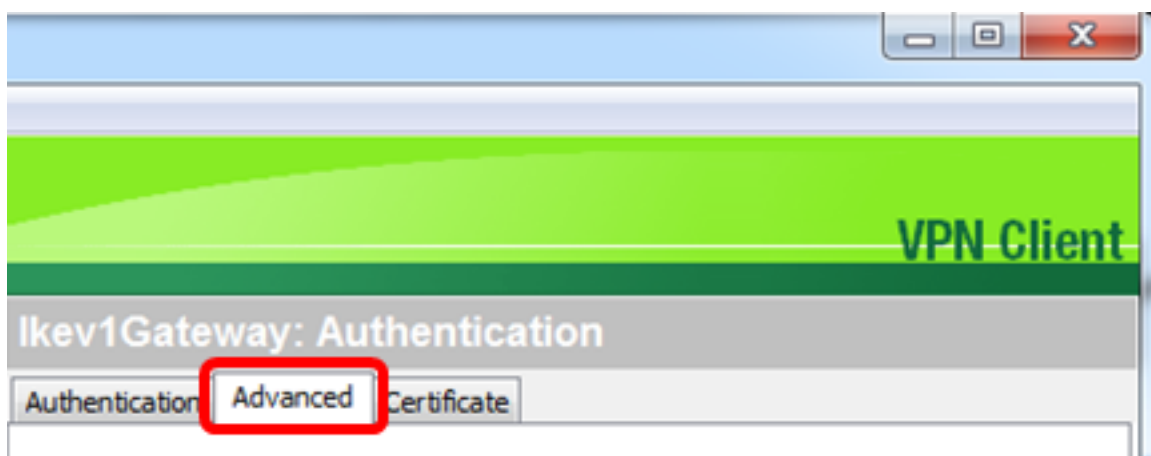
Étape 7. Entrez la même clé pré-partagée dans le champ *Confirmer*.



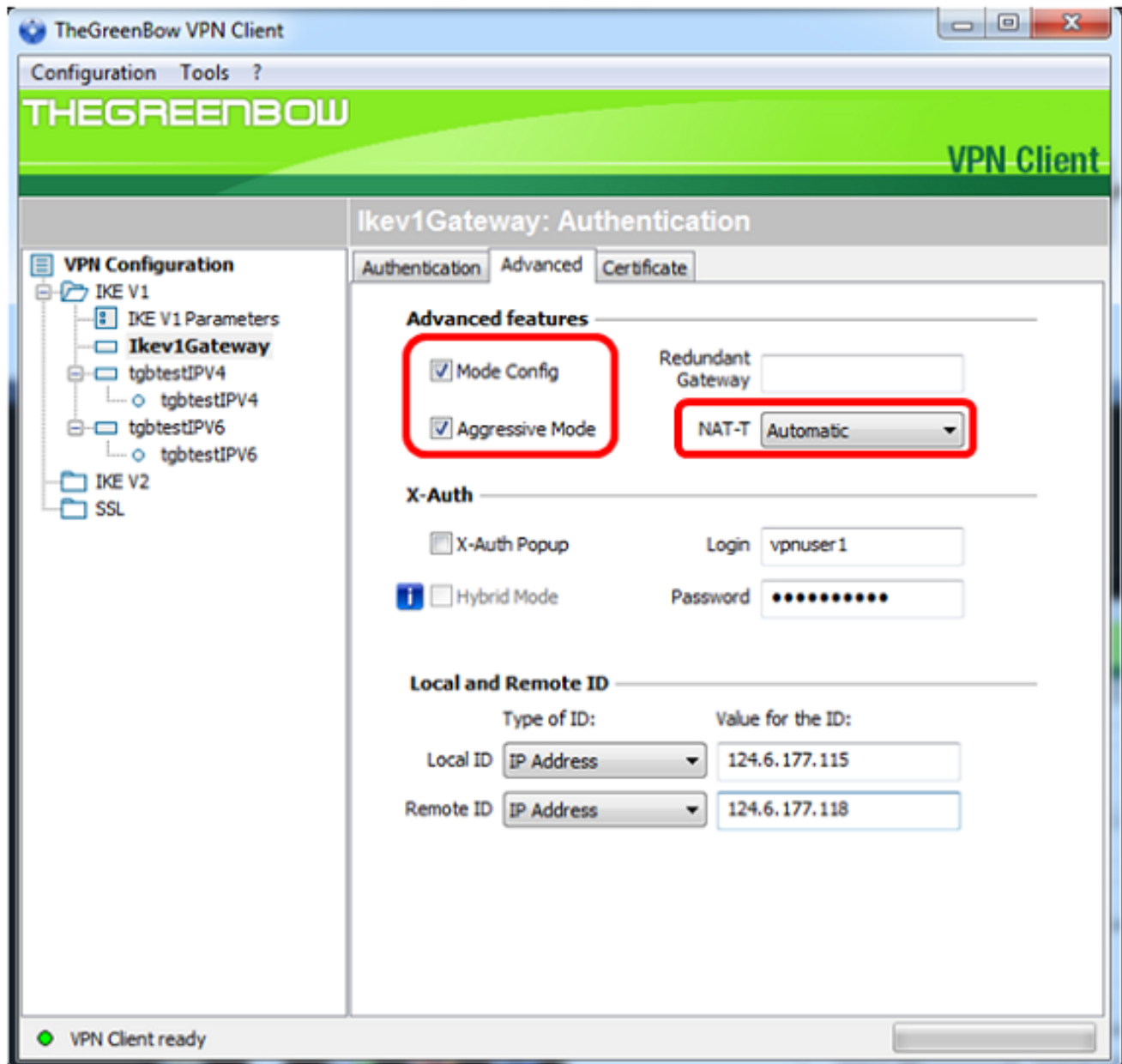
Étape 8. Sous IKE, définissez les paramètres Encryption, Authentication et Key Group pour qu'ils correspondent à la configuration du routeur.



Étape 9. Cliquez sur l'onglet **Advanced**.

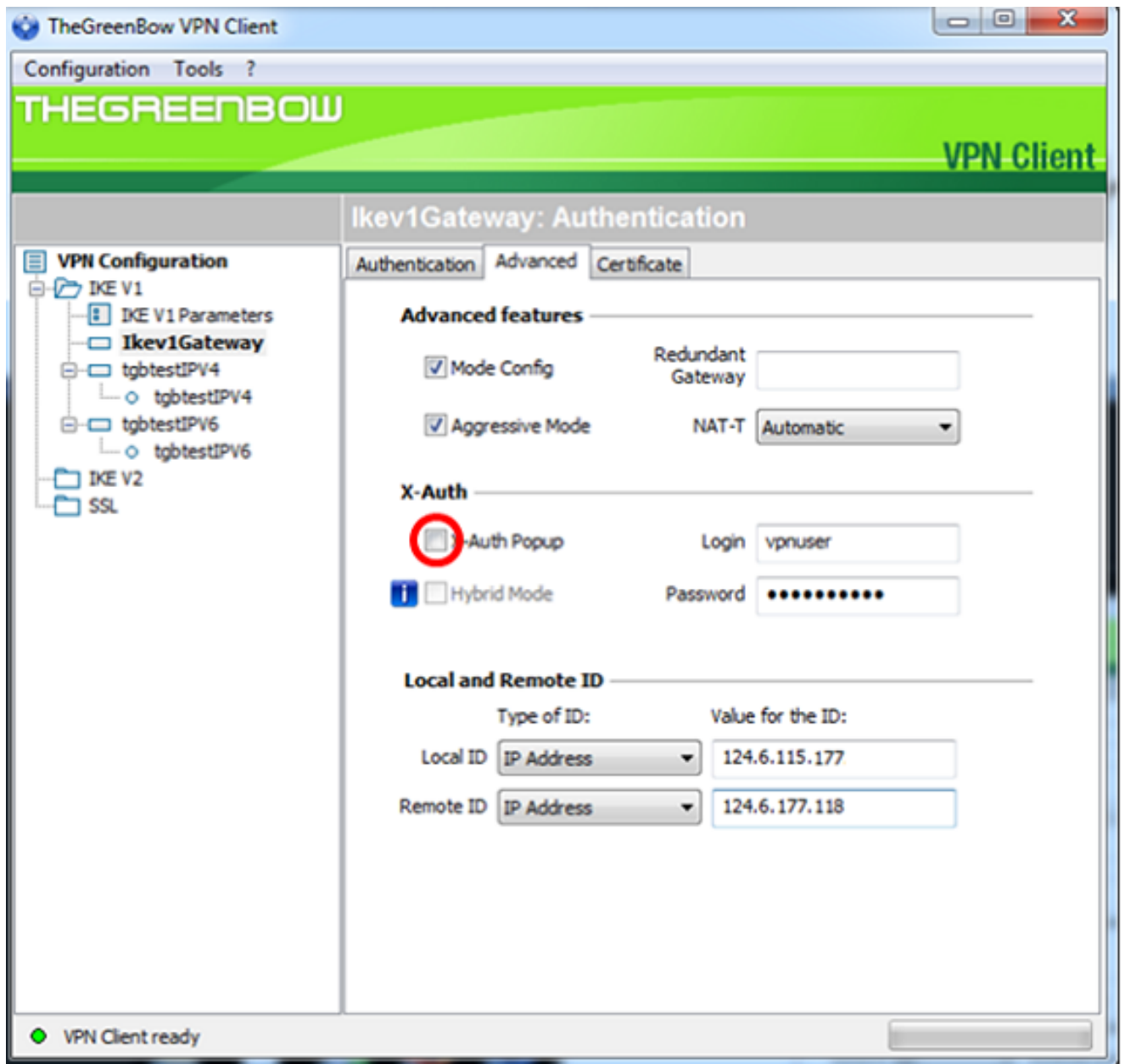


Étape 10. (Facultatif) Sous Fonctionnalités avancées, cochez les cases **Mode Config** et **Mode agressif** et définissez le paramètre NAT-T sur Automatique.



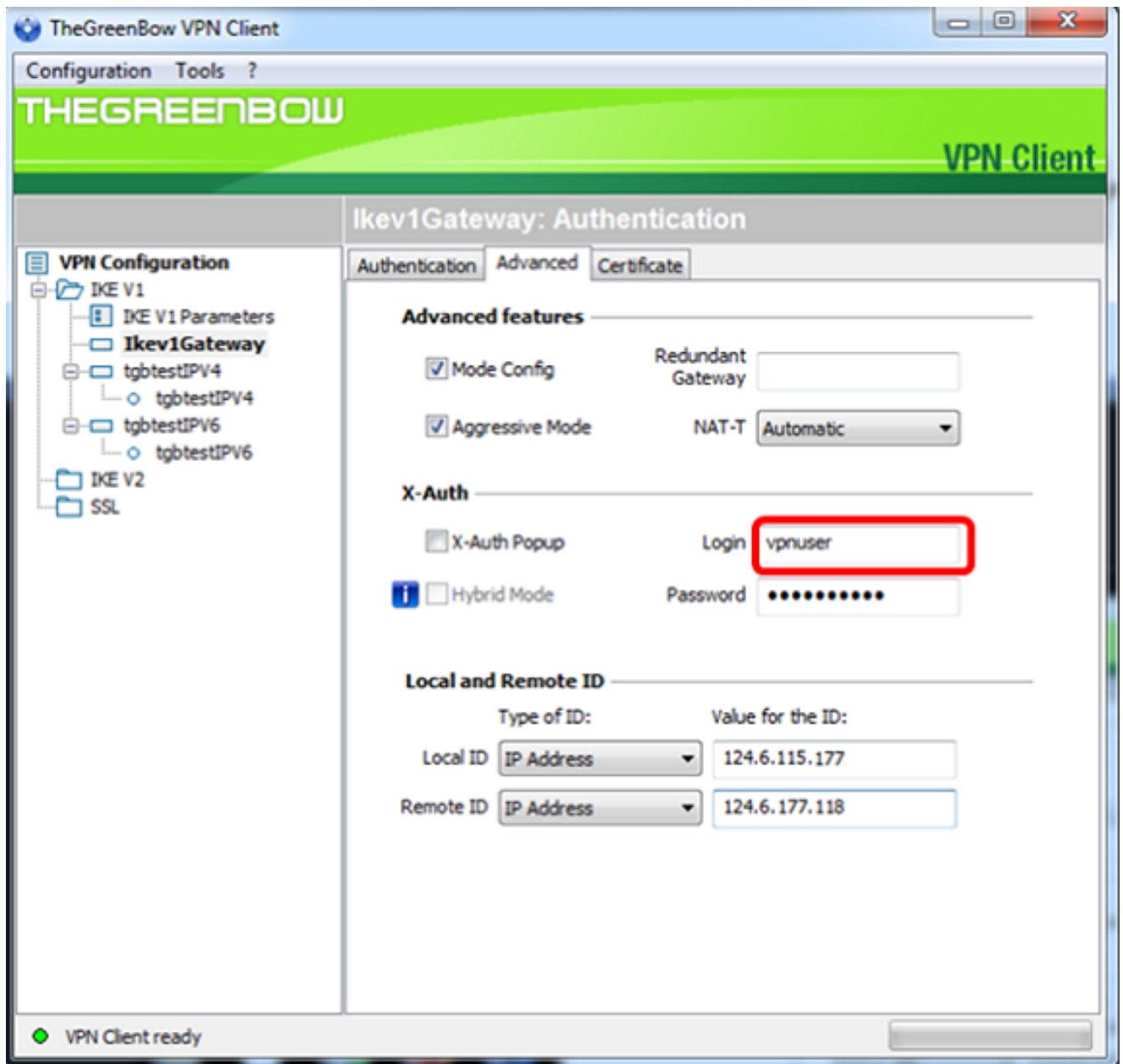
Note: Lorsque la configuration du mode est activée, le client VPN TheGreenBow extrait les paramètres de la passerelle VPN pour tenter d'établir un tunnel tout en activant Aggressive Mode et NAT-T pour accélérer l'établissement d'une connexion.

Étape 11. (Facultatif) Sous X-Auth, cochez la case **X-Auth Popup** pour afficher automatiquement la fenêtre de connexion lors du démarrage d'une connexion. La fenêtre de connexion permet à l'utilisateur de saisir ses informations d'identification pour pouvoir terminer le tunnel.

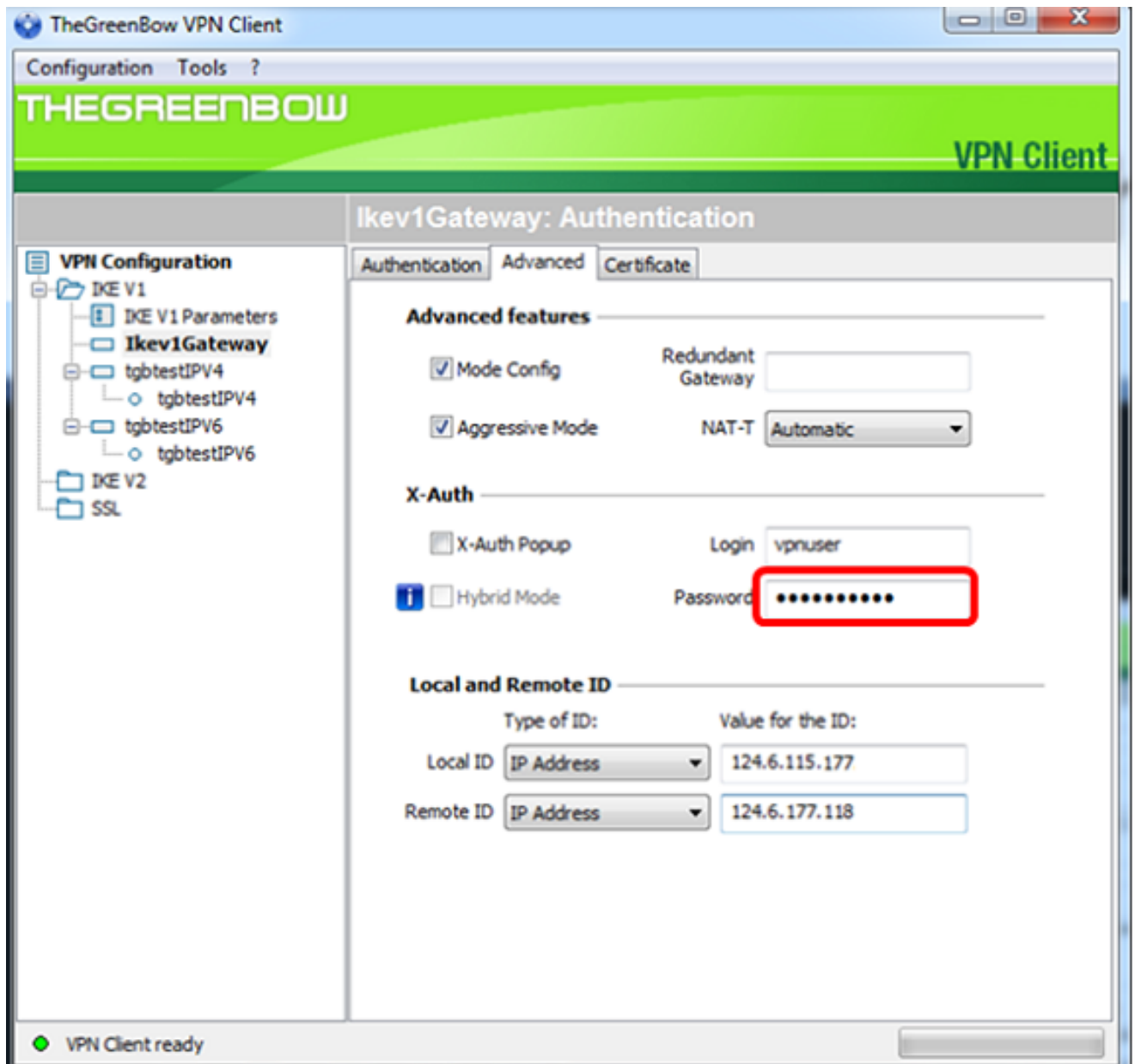


Note: Dans cet exemple, X-Auth Popup n'est pas coché.

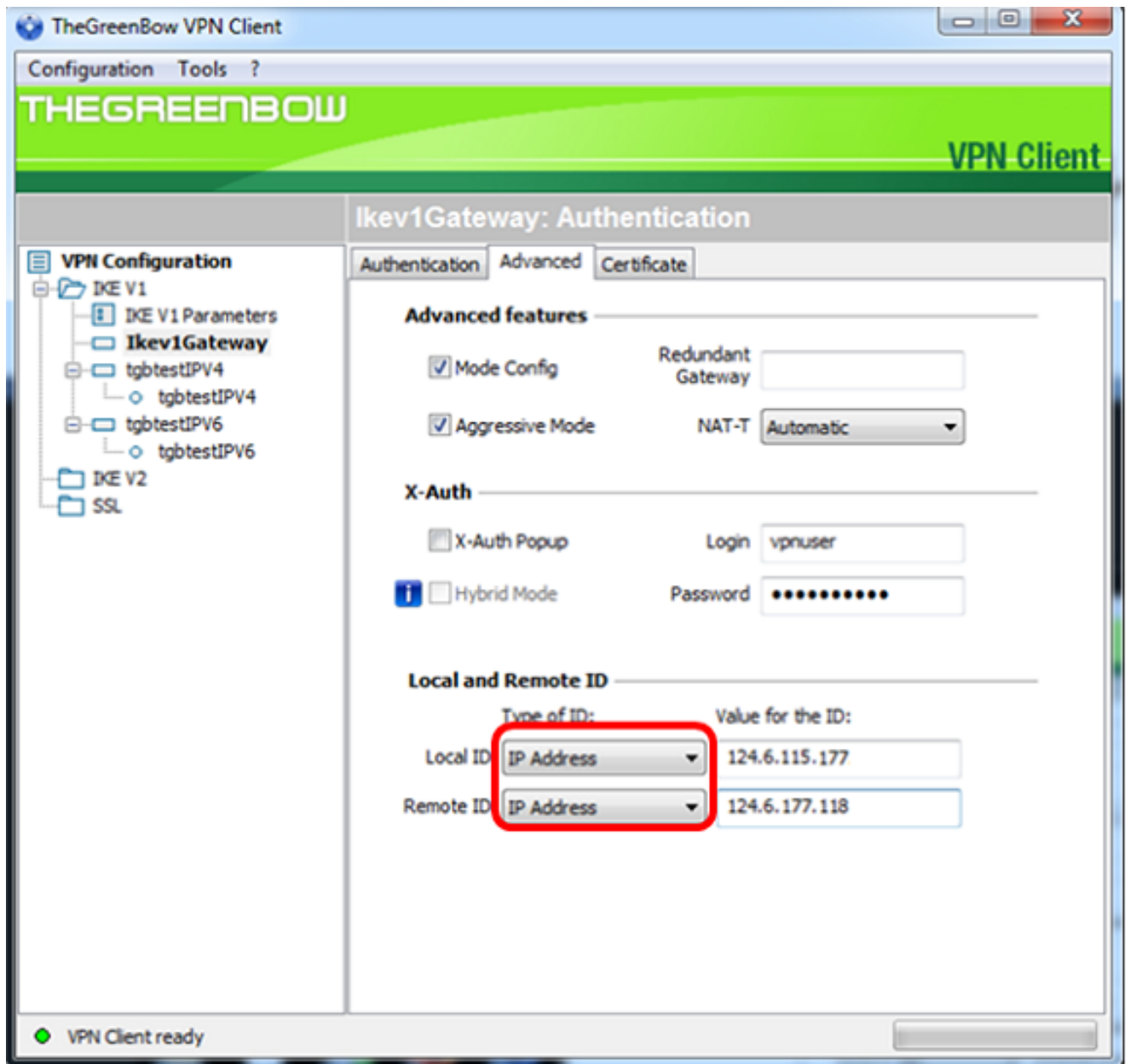
Étape 12. Entrez votre nom d'utilisateur dans le champ *Connexion*. Il s'agit du nom d'utilisateur configuré pour la création d'un groupe d'utilisateurs dans la passerelle VPN.



Étape 13. Entrez votre mot de passe dans le champ *Mot de passe*.

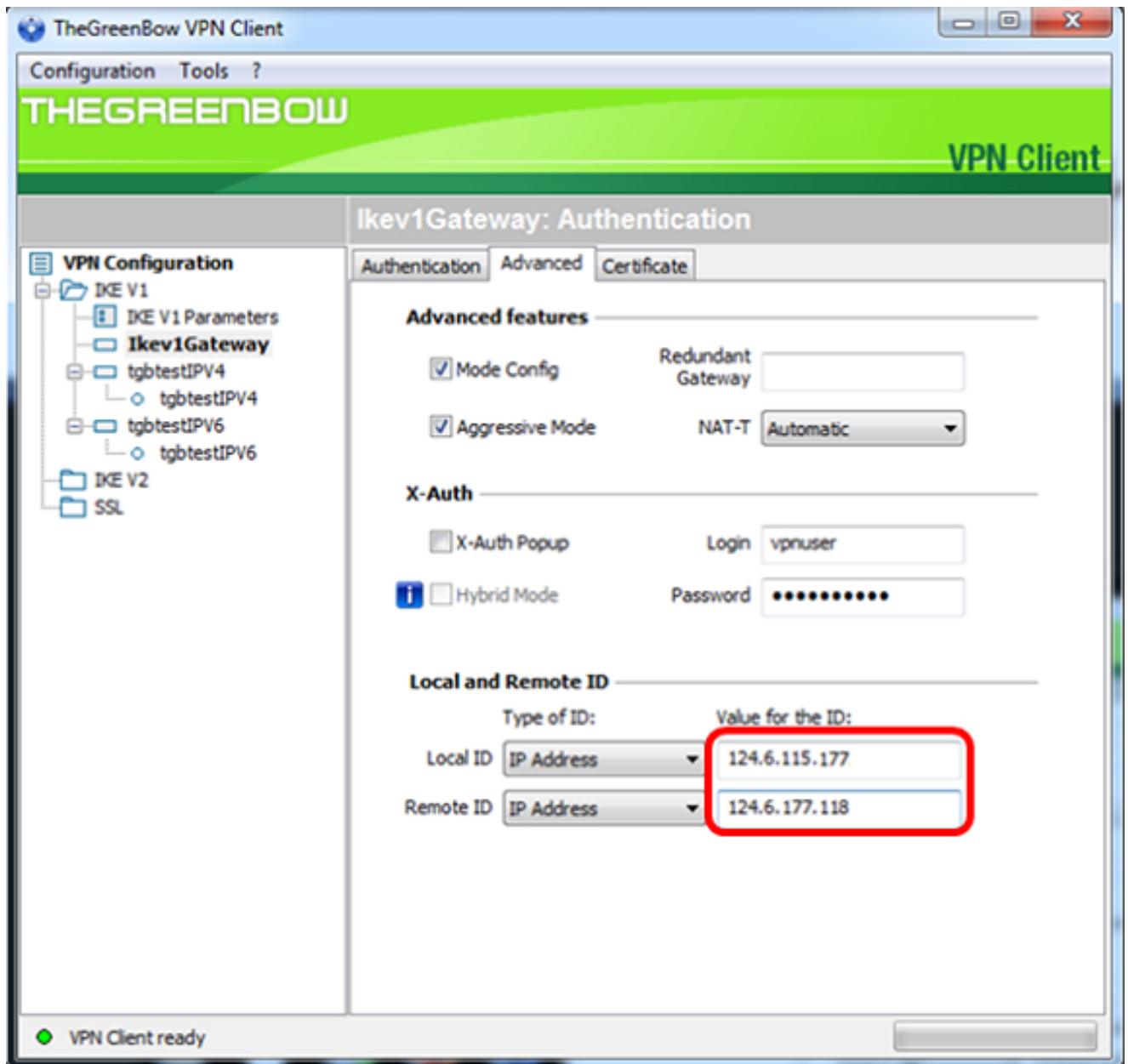


Étape 14. Sous Local and Remote ID, définissez l'ID local et l'ID distant pour qu'ils correspondent aux paramètres de la passerelle VPN.

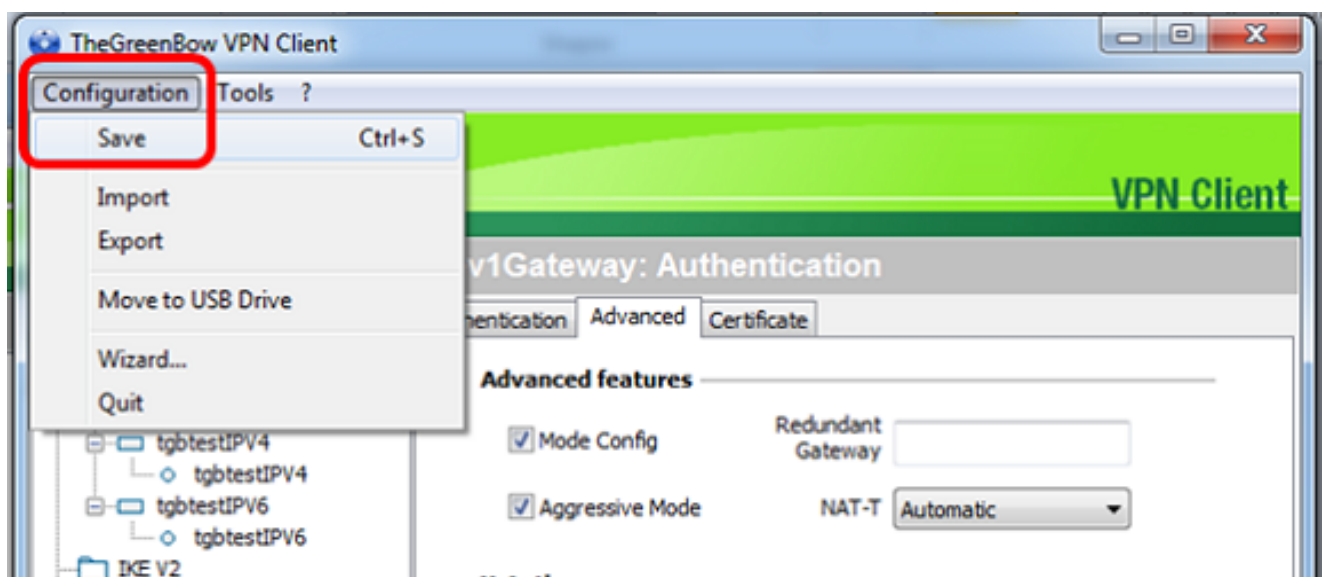


Note: Dans cet exemple, l'ID local et l'ID distant sont tous deux définis sur Adresse IP pour correspondre aux paramètres de la passerelle VPN RV34x.

Étape 15. Sous Valeur de l'ID, saisissez l'ID local et l'ID distant dans leurs champs respectifs.

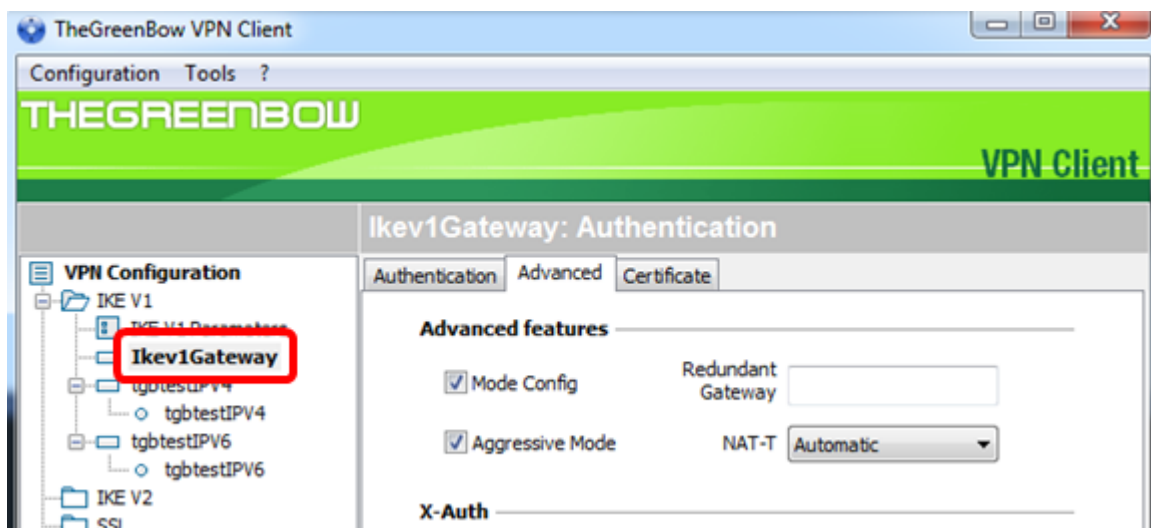


Étape 16. Cliquez sur **Configuration** > **Save** pour enregistrer les paramètres.

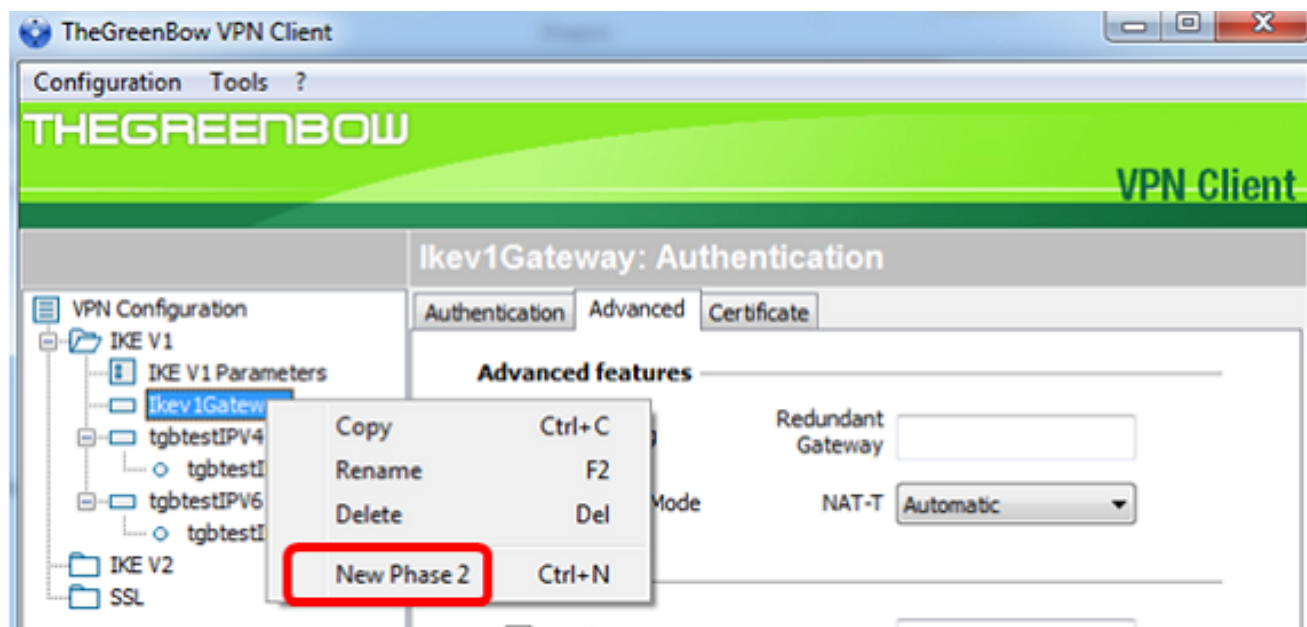


Configuration des paramètres de phase 2

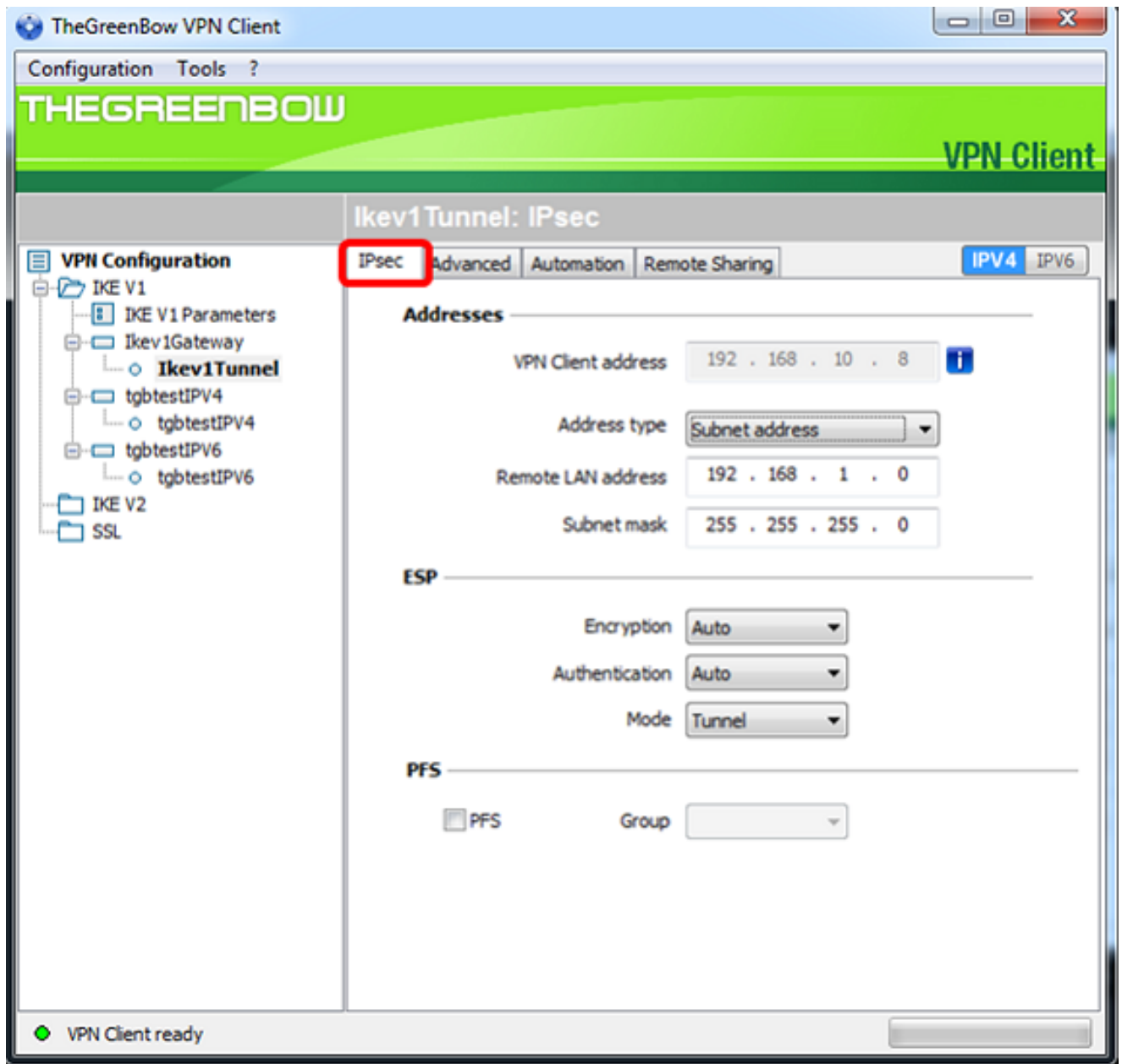
Étape 1. Cliquez avec le bouton droit sur **Ikev1 Gateway**.



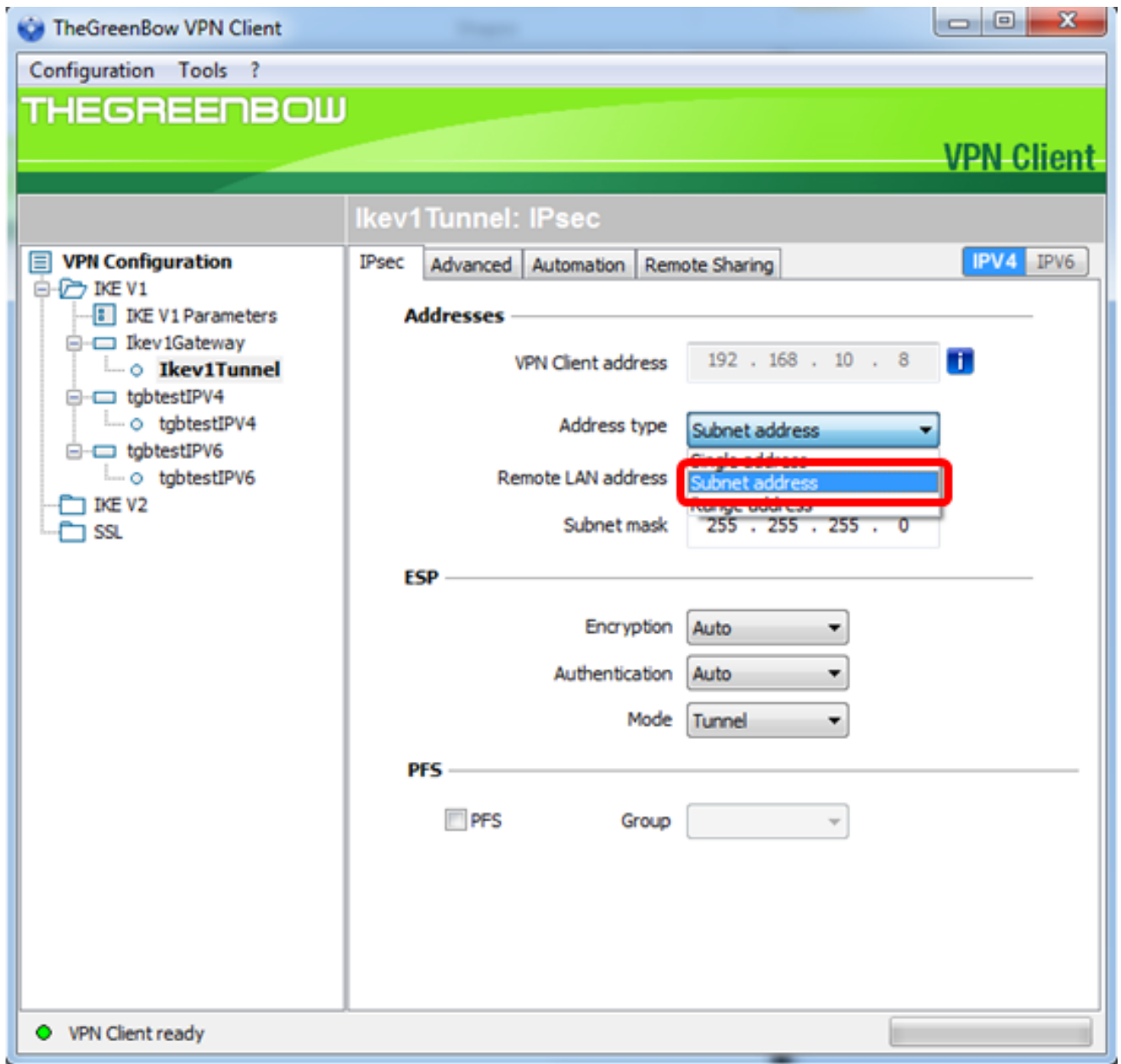
Étape 2. Sélectionnez **Nouvelle phase 2**.



Étape 3. Cliquez sur l'onglet **IPsec**.

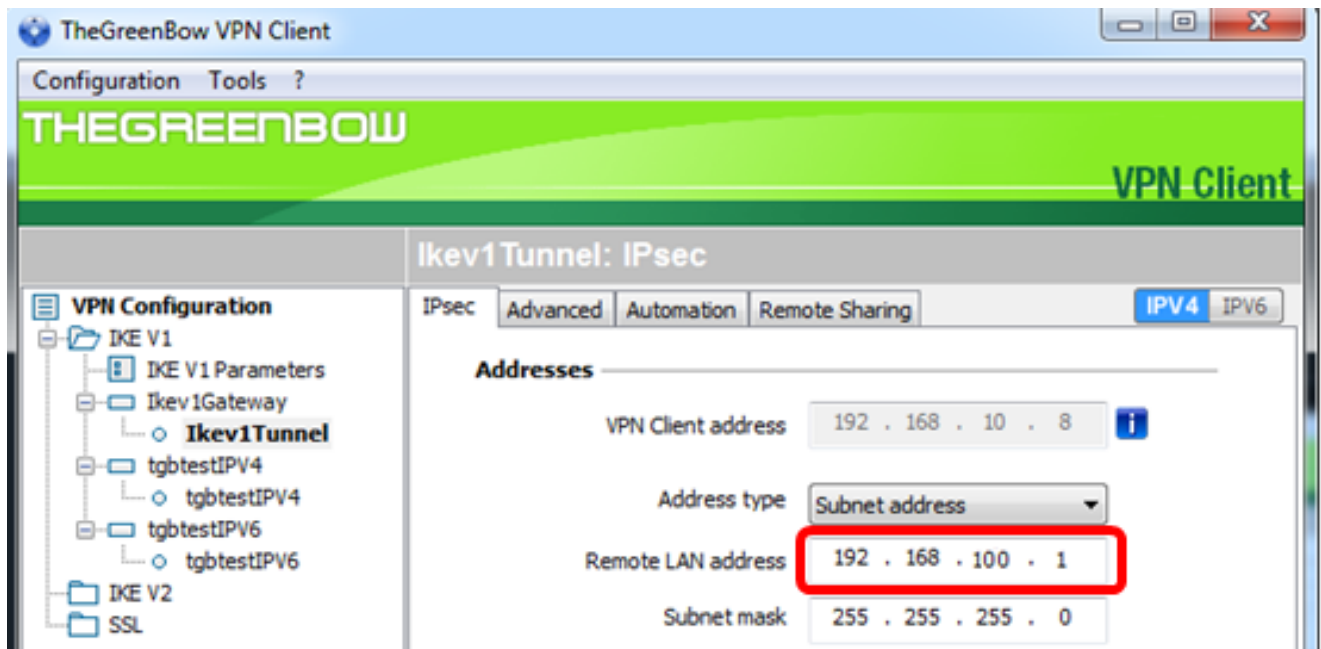


Étape 4. Sélectionnez le type d'adresse auquel le client VPN peut accéder dans la liste déroulante Type d'adresse.



Note: Dans cet exemple, l'adresse de sous-réseau est choisie.

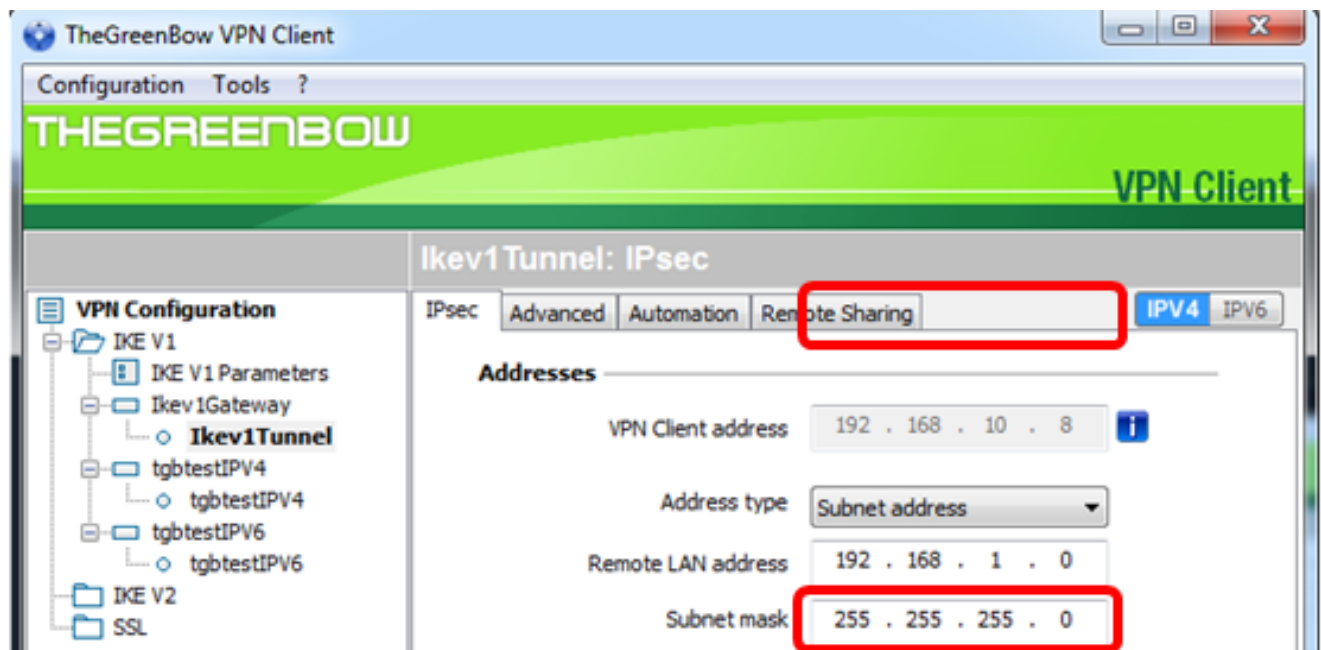
Étape 5. Entrez l'adresse réseau à laquelle le tunnel VPN doit accéder dans le champ *Adresse LAN distante*.



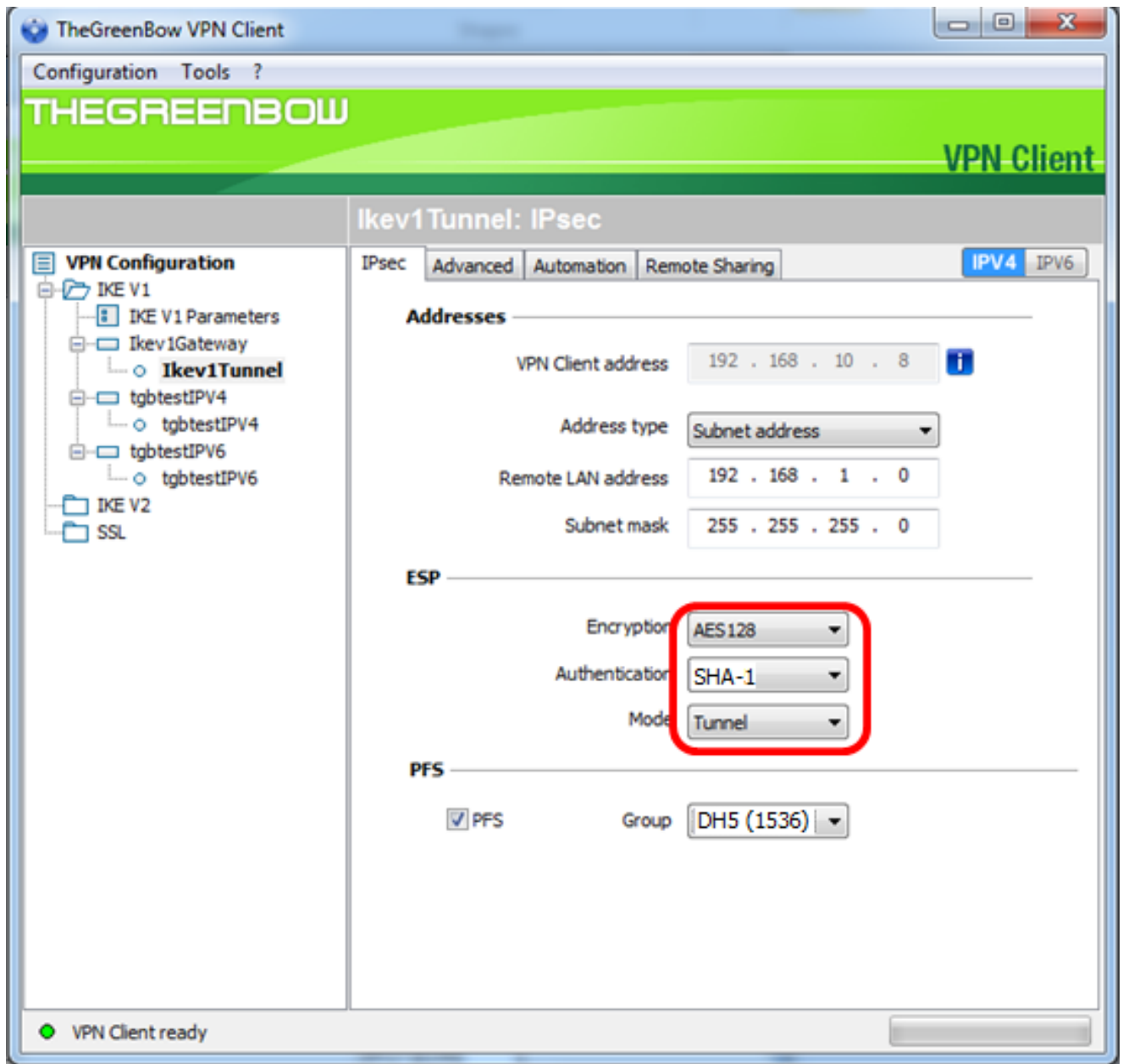
Note: Dans cet exemple, 192.168.100.1 est entré.

Étape 6. Entrez le masque de sous-réseau du réseau distant dans le champ *Masque de sous-réseau*.

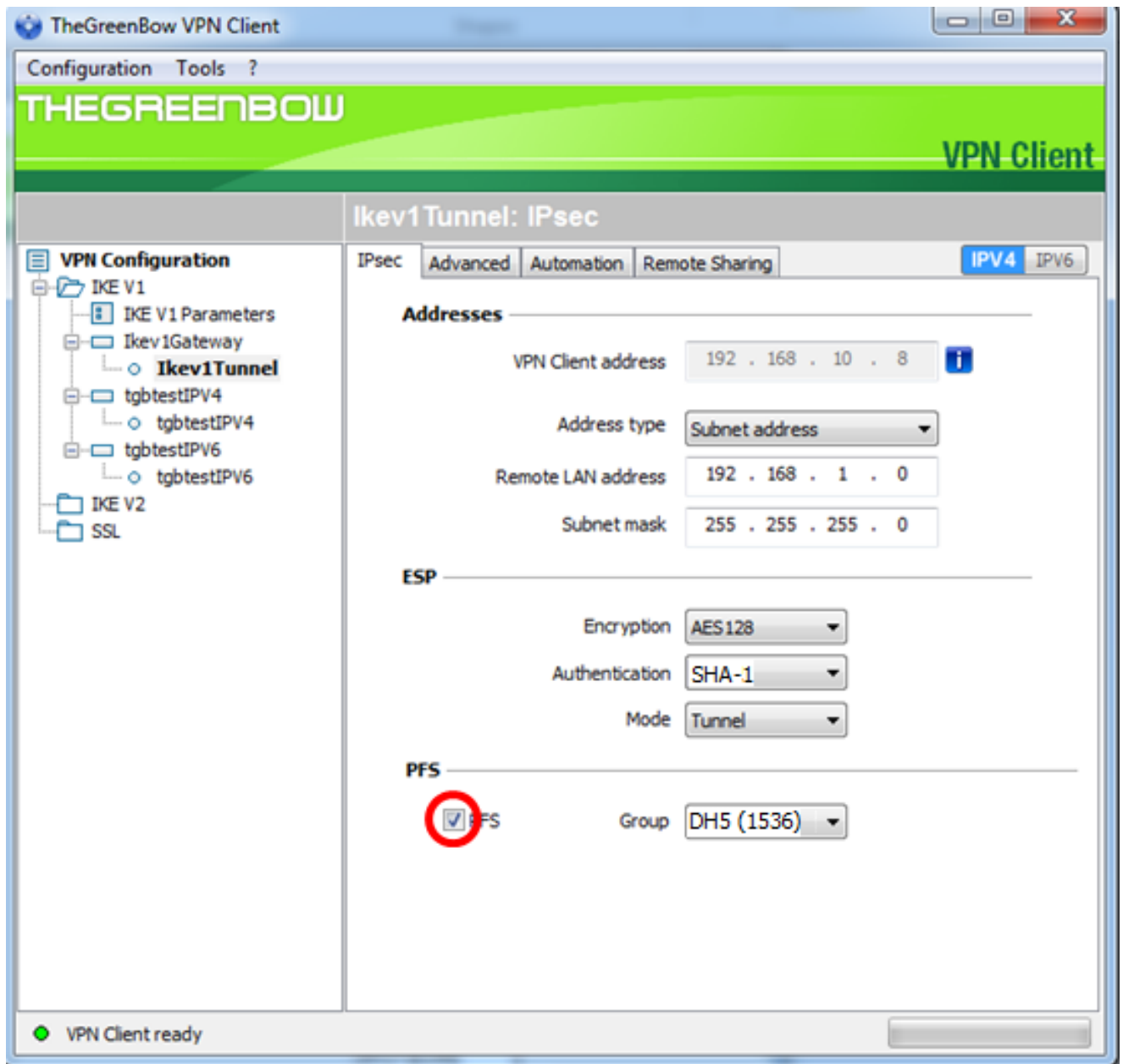
Note: Dans cet exemple, 255.255.255.0 est entré.



Étape 7. Sous ESP, définissez le chiffrement, l'authentification et le mode pour qu'ils correspondent aux paramètres de la passerelle VPN.

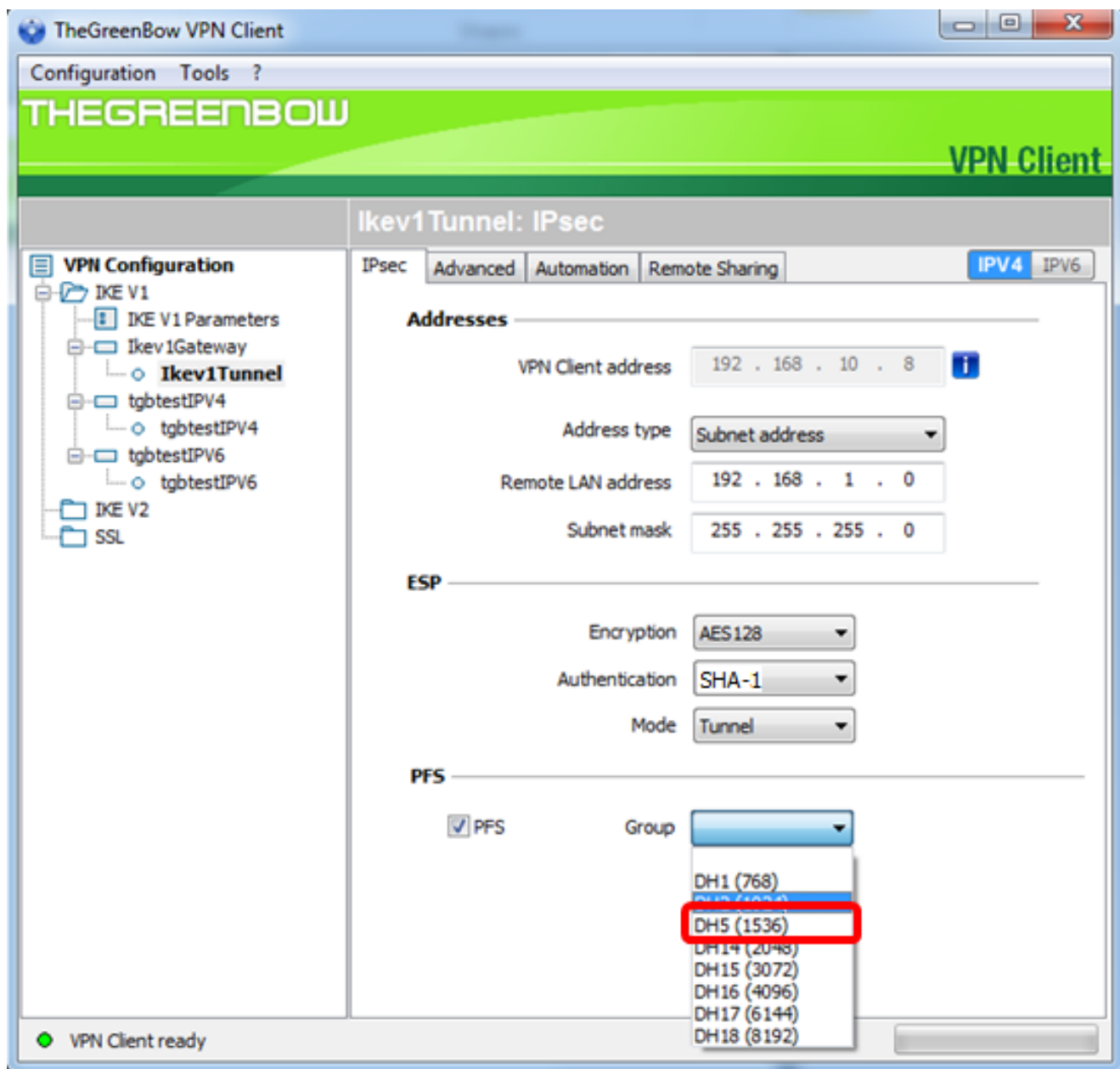


Étape 8. (Facultatif) Sous PFS, cochez la case **PFS** pour activer Perfect Forward Secrecy (PFS). PFS génère des clés aléatoires pour chiffrer la session.

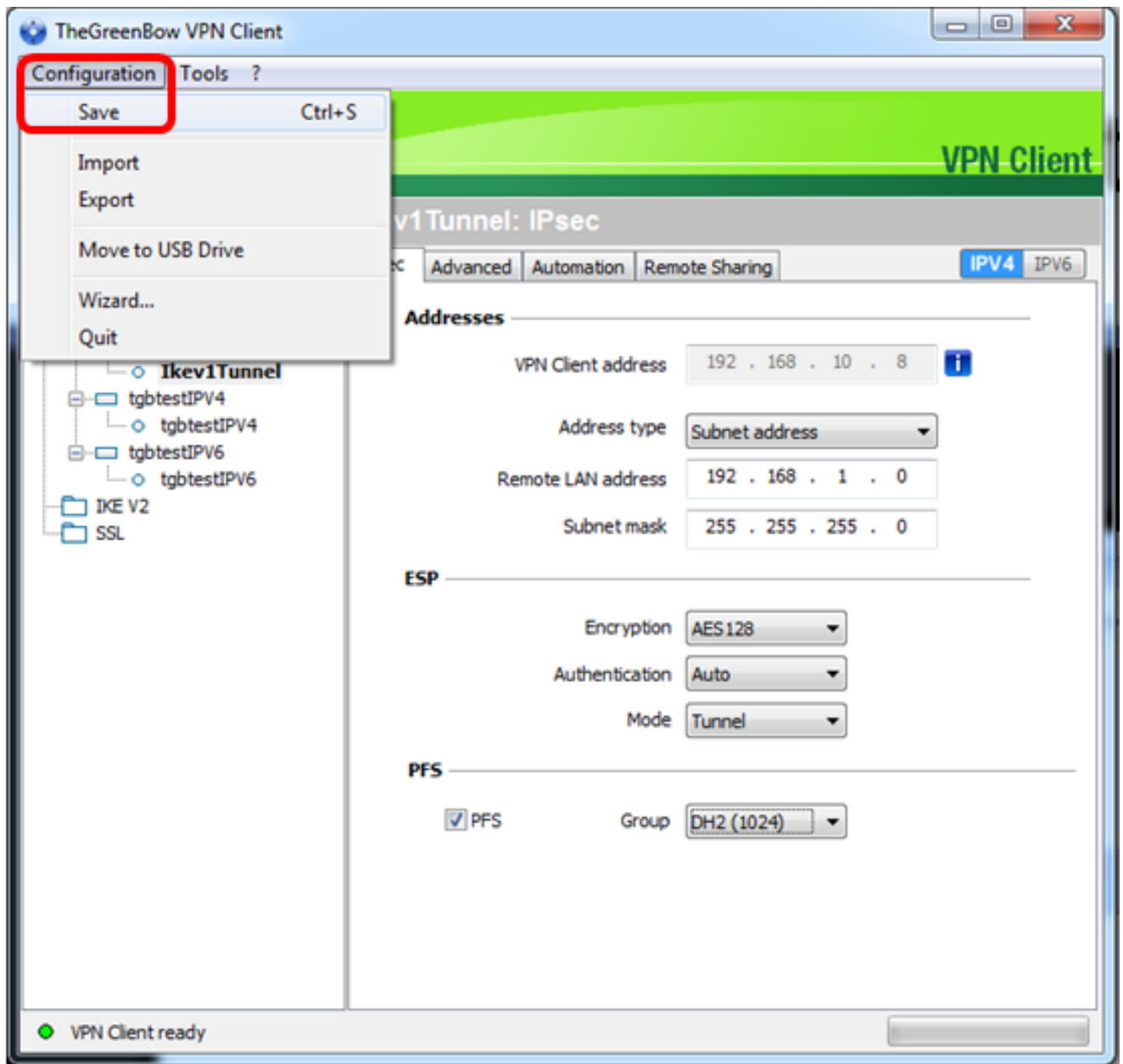


Étape 9. Sélectionnez un paramètre de groupe PFS dans la liste déroulante Groupe.

Note: Dans cet exemple, DH5 (1536) est choisi pour correspondre au paramètre du groupe DH du routeur.



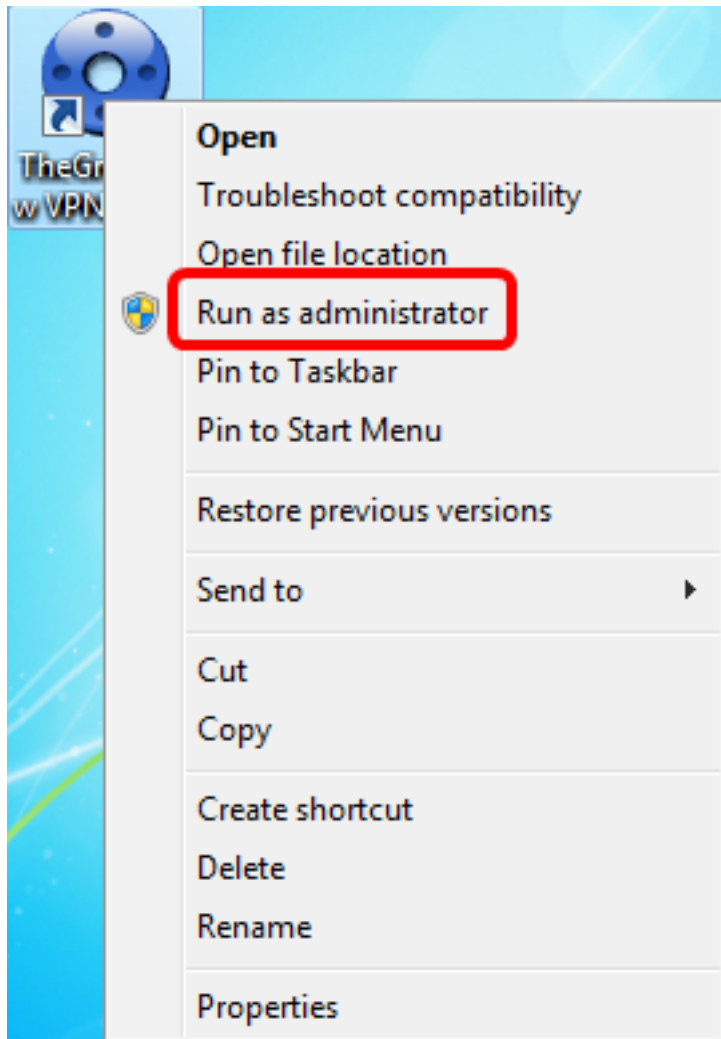
Étape 10. Cliquez avec le bouton droit sur **Configuration** et choisissez Enregistrer.



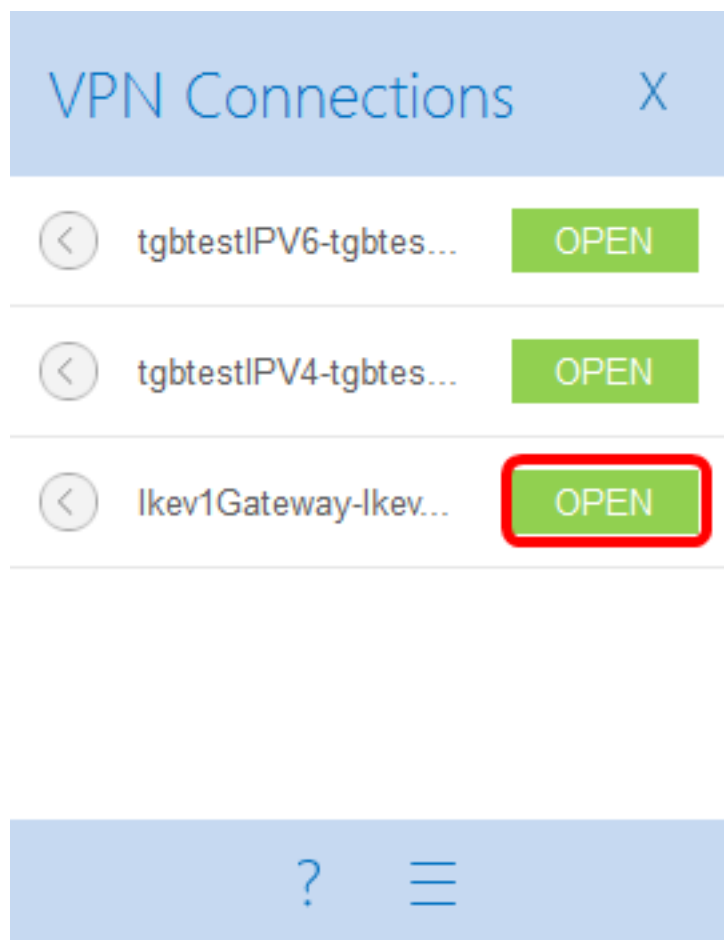
Vous devez maintenant avoir correctement configuré le client VPN TheGreenBow pour vous connecter au routeur de la gamme RV34x via VPN.

Démarrer une connexion VPN

Étape 1. Cliquez avec le bouton droit sur TheGreenBow VPN Client et sélectionnez **Exécuter en tant qu'administrateur**.



Étape 2. Choisissez la connexion VPN à utiliser, puis cliquez sur **OPEN**. La connexion VPN doit démarrer automatiquement.

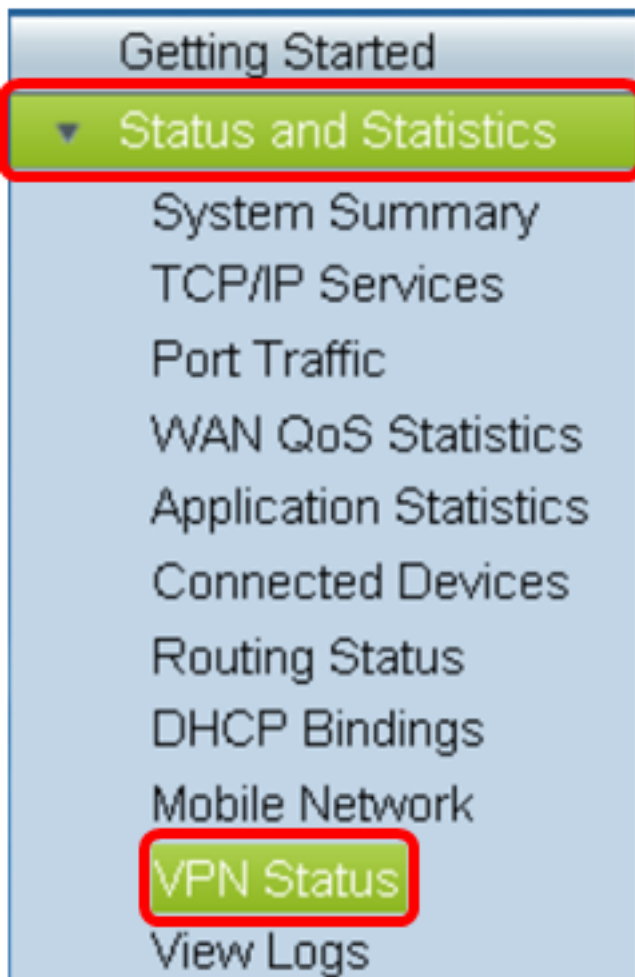


Note: Dans cet exemple, la passerelle Ikev1 configurée a été choisie.

Vérifier l'état du VPN

Étape 1. Connectez-vous à l'utilitaire Web de la passerelle VPN.

Étape 2. Choisissez **Status and Statistics > VPN Status**.



Étape 3. Sous Client-to-Site Tunnel Status, cochez la colonne Connections de la table Connection.

Note: Dans cet exemple, une connexion VPN a été établie.

Connections
1

Vous devez maintenant avoir vérifié l'état de la connexion VPN sur le routeur de la gamme RV34x. Le client VPN GreenBow est maintenant configuré pour se connecter au routeur via VPN.