

Uso del client VPN GreenBow per la connessione con il router serie RV34x

Avviso speciale: Struttura delle licenze: firmware versioni 1.0.3.15 e successive. Inoltre, AnyConnect sarà a pagamento solo per le licenze client.

Per ulteriori informazioni sulle licenze AnyConnect sui router serie RV340, consultare l'articolo [Licenze AnyConnect per i router serie RV340](#).

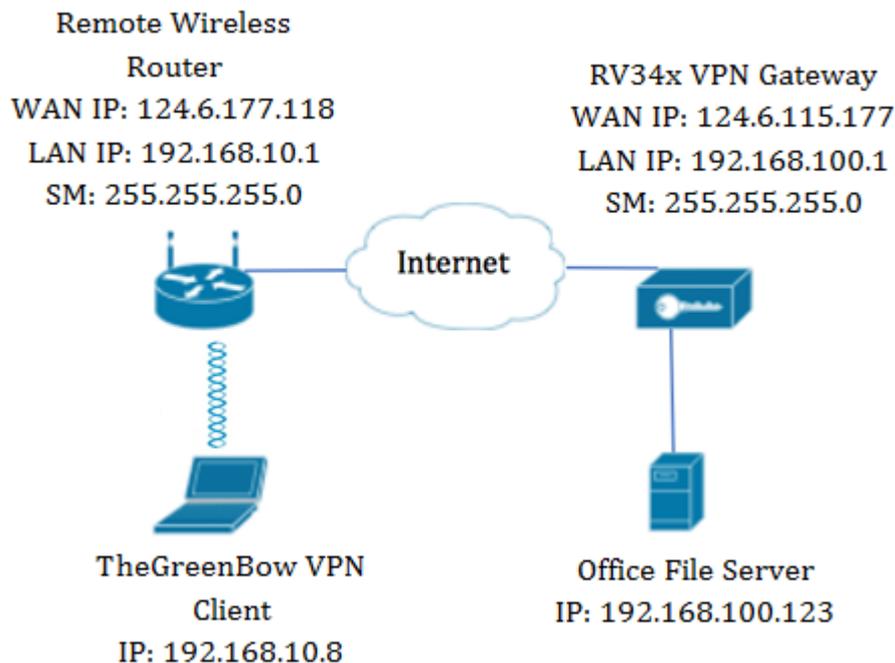
Introduzione

Una connessione VPN (Virtual Private Network) consente agli utenti di accedere, inviare e ricevere dati da e verso una rete privata tramite una rete pubblica o condivisa, ad esempio Internet, ma garantisce comunque una connessione sicura a un'infrastruttura di rete sottostante per proteggere la rete privata e le relative risorse.

Un tunnel VPN stabilisce una rete privata in grado di inviare i dati in modo sicuro utilizzando la crittografia e l'autenticazione. Le filiali utilizzano per lo più connessioni VPN in quanto è utile e necessario consentire ai dipendenti di accedere alla rete privata anche quando si trovano all'esterno dell'ufficio.

La VPN consente a un host remoto di agire come se si trovasse sulla stessa rete locale. Il router supporta fino a 50 tunnel. È possibile configurare una connessione VPN tra il router e un endpoint dopo che il router è stato configurato per la connessione Internet. Il client VPN dipende interamente dalle impostazioni del router VPN per poter stabilire una connessione.

Il client VPN GreenBow è un'applicazione client VPN di terze parti che consente a un dispositivo host di configurare una connessione sicura per il tunnel IPsec da sito a sito con il router serie RV34x.



Nel diagramma il computer si conetterà al file server dell'ufficio al di fuori della rete per accedere alle risorse. A tale scopo, il client VPN GreenBow nel computer sarà configurato in modo tale da estrarre le impostazioni dal gateway VPN RV34x.

Vantaggi dell'utilizzo di una connessione VPN

1. L'utilizzo di una connessione VPN consente di proteggere i dati e le risorse di rete riservati.
2. Offre convenienza e accessibilità per i dipendenti remoti o aziendali, in quanto possono accedere facilmente all'ufficio principale senza dover essere fisicamente presenti e mantenere la sicurezza della rete privata e delle sue risorse.
3. La comunicazione tramite una connessione VPN offre un livello di protezione più elevato rispetto ad altri metodi di comunicazione remota. L'elevato livello di tecnologia rende possibile questa operazione, proteggendo la rete privata da accessi non autorizzati.
4. L'effettiva posizione geografica degli utenti è protetta e non esposta al pubblico o alle reti condivise come Internet.
5. Aggiungere nuovi utenti o gruppi di utenti alla rete è facile poiché le VPN sono facilmente scalabili. È possibile far crescere la rete senza la necessità di componenti aggiuntivi o una configurazione complicata.

Rischi dell'utilizzo di una connessione VPN

1. Rischio per la sicurezza dovuto a una configurazione errata. Poiché la progettazione e l'implementazione di una VPN può essere complicata, è necessario affidare il compito di configurare la connessione a un professionista altamente qualificato ed esperto per assicurarsi che la sicurezza della rete privata non venga compromessa.
2. Affidabilità. Poiché una connessione VPN richiede una connessione a Internet, è importante disporre di un provider con una reputazione collaudata e testata per fornire un servizio Internet eccellente e garantire tempi di inattività minimi o nulli.
3. Scalabilità. In una situazione in cui è necessario aggiungere una nuova infrastruttura o una nuova serie di configurazioni, possono verificarsi problemi tecnici dovuti all'incompatibilità, in particolare se si utilizzano prodotti o fornitori diversi da quelli già in uso.

4. Problemi di sicurezza per i dispositivi mobili. Quando si avvia la connessione VPN su un dispositivo mobile, possono verificarsi problemi di protezione, in particolare quando il dispositivo mobile è connesso alla rete locale in modalità wireless.
5. Velocità di connessione lente. Se si utilizza un client VPN che offre un servizio VPN gratuito, è probabile che anche la connessione risulti lenta poiché questi provider non assegnano la priorità alle velocità di connessione.

Prerequisiti per l'utilizzo del client VPN GreenBow

I seguenti elementi devono prima essere configurati sul router VPN e verranno applicati al client VPN di TheGreenBow facendo clic [qui](#) per stabilire una connessione.

1. [Creare un profilo da client a sito sul gateway VPN](#)
2. [Creare un gruppo di utenti sul gateway VPN](#)
3. [Crea account utente sul gateway VPN](#)
4. [Creare un profilo IPsec sul gateway VPN](#)
5. [Configurare le impostazioni di Fase I e Fase II sul gateway VPN](#)

Dispositivi interessati

- Serie RV34x

Versione del software

- 1.0.01.17

Usa il client VPN GreenBow

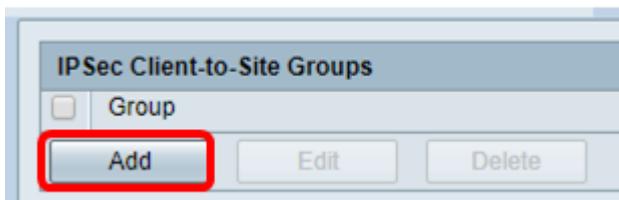
[Creazione di un profilo da client a sito sul router](#)

Passaggio 1. Accedere all'utility basata sul Web del router RV34x e scegliere **VPN > Da client a sito**.



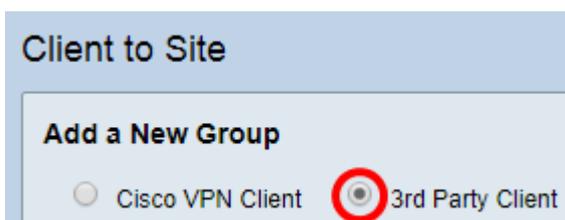
Nota: Le immagini riportate in questo articolo vengono acquisite dal router RV340. Le opzioni possono variare a seconda del modello del dispositivo.

Passaggio 2. Fare clic su **Add**.



Passaggio 3. Fare clic su **Client di terze parti**.

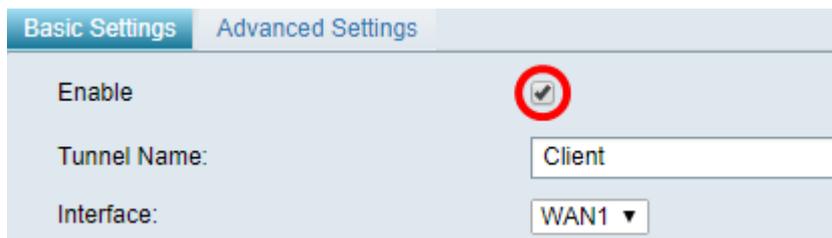
Nota: AnyConnect è un esempio di client VPN Cisco, mentre TheGreenBow VPN Client è un esempio di client VPN di terze parti.



Nota: In questo esempio viene scelto Client di terze parti.

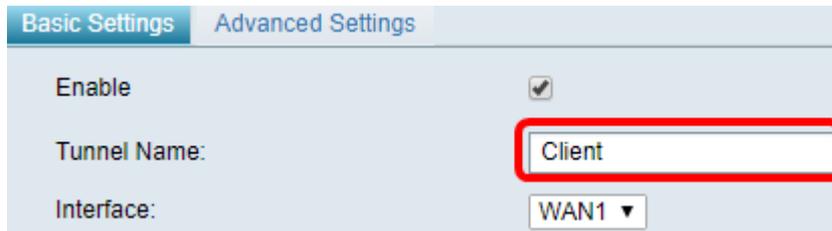
Passaggio 4. Nella scheda Basic Settings, selezionare la casella di controllo **Enable** per

assicurarsi che il profilo VPN sia attivo.



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

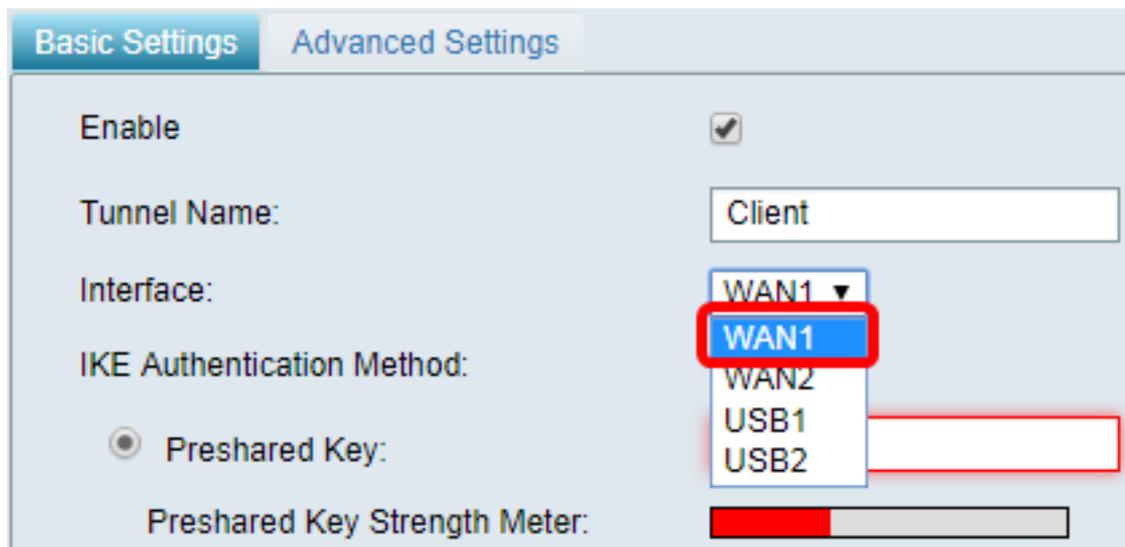
Passaggio 5. Immettere un nome per la connessione VPN nel campo *Nome tunnel*.



The screenshot shows the 'Basic Settings' tab. The 'Tunnel Name' field, which contains 'Client', is highlighted with a red rectangular border. The 'Enable' checkbox is also checked.

Nota: Nell'esempio, viene immesso **Client**.

Passaggio 6. Scegliere l'interfaccia da utilizzare dall'elenco a discesa *Interfaccia*. Le opzioni sono WAN1, WAN2, USB1 e USB2 che utilizzeranno l'interfaccia corrispondente sul router per la connessione VPN.



The screenshot shows the 'Basic Settings' tab with the 'Interface' dropdown menu open. The 'WAN1' option is highlighted with a blue background and a red border. Other options visible in the dropdown are WAN2, USB1, and USB2. The 'Tunnel Name' field contains 'Client' and the 'Enable' checkbox is checked.

Nota: Le opzioni dipendono dal modello di router in uso. Nell'esempio, viene scelta WAN1.

Passaggio 7. Scegliere un metodo di autenticazione IKE. Le opzioni sono:

- Chiave già condivisa — Questa opzione consente di utilizzare una password condivisa per la connessione VPN.
- Certificato - questa opzione utilizza un certificato digitale che contiene informazioni quali il nome, l'indirizzo IP, il numero di serie, la data di scadenza del certificato e una copia della chiave pubblica del titolare del certificato.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Certificate:

Nota: In questo esempio viene scelta Chiave già condivisa.

Passaggio 8. Immettere la password di connessione nel campo *Chiave già condivisa*.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Passaggio 9. (Facoltativo) Per utilizzare una password semplice, deselegionare la casella di controllo **Abilita** complessità minima chiave già condivisa.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Nota: In questo esempio, l'opzione Complessità minima chiave già condivisa è abilitata.

Passaggio 10. (Facoltativo) Selezionare la casella di controllo Mostra testo normale in caso di modifica **Attiva** per visualizzare la password in testo normale.

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

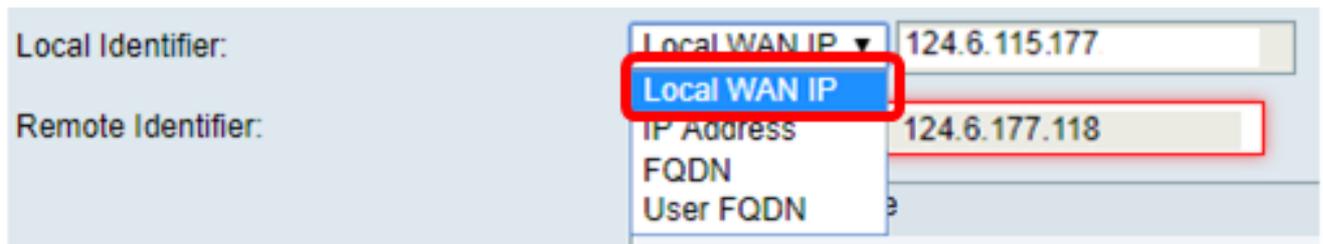
Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Nota: In questo esempio, mostra il testo normale quando la modifica viene lasciata disattivata.

Passaggio 11. Scegliere un identificatore locale dall'elenco a discesa Identificatore locale. Le opzioni sono:

- Local WAN IP: questa opzione utilizza l'indirizzo IP dell'interfaccia WAN (Wide Area Network) del gateway VPN.
- Indirizzo IP - Questa opzione consente di immettere manualmente un indirizzo IP per la connessione VPN.
- FQDN: questa opzione è nota anche come nome di dominio completo (FQDN). Consente di utilizzare un nome di dominio completo per un computer specifico su Internet.
- FQDN utente — questa opzione consente di utilizzare un nome di dominio completo per un utente specifico su 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 value '124.6.115.177' is entered in the adjacent text box. Below it, the 'Remote Identifier' dropdown menu is open, with 'IP Address' selected and highlighted with a red box. The value '124.6.177.118' is entered in the adjacent text box.

Nota: Nell'esempio, viene scelto Local WAN IP. Con questa opzione, l'indirizzo IP della WAN locale viene rilevato automaticamente.

Passaggio 12. (Facoltativo) Scegliere un identificatore per l'host remoto. Le opzioni sono:

- Indirizzo IP - Questa opzione utilizza l'indirizzo IP WAN del client VPN.
- FQDN — questa opzione consente di utilizzare un nome di dominio completo per un computer specifico su Internet.
- FQDN utente — questa opzione consente di utilizzare un nome di dominio completo per un utente specifico su Internet.



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 value '124.6.177.118' is entered in the adjacent text box. The 'Local Identifier' dropdown menu is also visible, with 'Local WAN IP' selected and the value '124.6.115.177' entered.

Nota: Nell'esempio, viene scelto IP Address (Indirizzo IP).

Passaggio 13. Immettere l'identificativo remoto nel campo *Identificativo remoto*.



The screenshot shows the 'Remote Identifier' text box. The value '124.6.177.118' is entered and highlighted with a red box. The 'Local Identifier' dropdown menu is also visible, with 'Local WAN IP' selected and the value '124.6.115.177' entered.

Nota: Nell'esempio, viene immesso 124.6.115.177.

Passaggio 14. (Facoltativo) Selezionare la casella di controllo **Autenticazione estesa** per attivare la funzionalità. Se attivata, questa opzione fornirà un ulteriore livello di autenticazione che richiederà agli utenti remoti di inserire le proprie credenziali prima di ottenere l'accesso alla VPN.

Extended Authentication:

Group Name

Add Delete

Nota: Nell'esempio, l'opzione Autenticazione estesa non è selezionata.

Passaggio 15. In Nome gruppo fare clic su **Aggiungi**.

Extended Authentication:

Group Name

Add Delete

Passaggio 16. Scegliere il gruppo che utilizzerà l'autenticazione estesa dall'elenco a discesa Nome gruppo.

Group Name

admin

admin

guest

IPSecVPN

VPN

Nota: Nell'esempio, viene scelta VPN.

Passaggio 17. In Intervallo pool per LAN client, immettere il primo indirizzo IP che può essere assegnato a un client VPN nel campo *IP iniziale*.

Pool Range for Client LAN:

Start IP: 10.10.100.100

End IP: 10.10.100.245

Nota: nell'esempio, viene immesso 10.10.100.100.

Passaggio 18. Immettere l'ultimo indirizzo IP che può essere assegnato a un client VPN nel campo *End IP*.

Pool Range for Client LAN:

Start IP: 10.10.100.100

End IP: 10.10.100.245

Nota: nell'esempio, viene immesso 10.10.100.245.

Passaggio 19. Fare clic su **Applica**.

Pool Range for Client LAN:

Start IP:

End IP:

Passaggio 20. Fare clic su **Salva**.

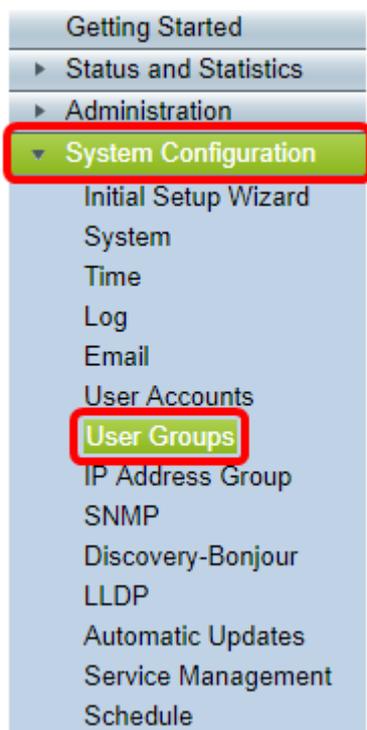


A questo punto, è necessario configurare il profilo client-sito sul router per il client VPN TheGreenBow.

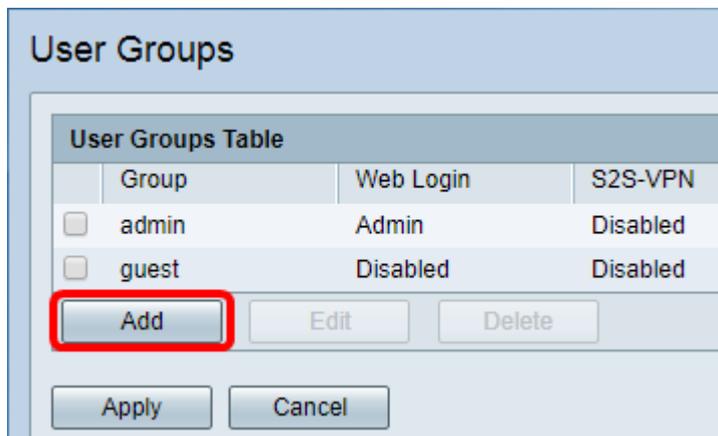
[Crea un gruppo di utenti](#)

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **Configurazione di sistema > Gruppi di utenti**.

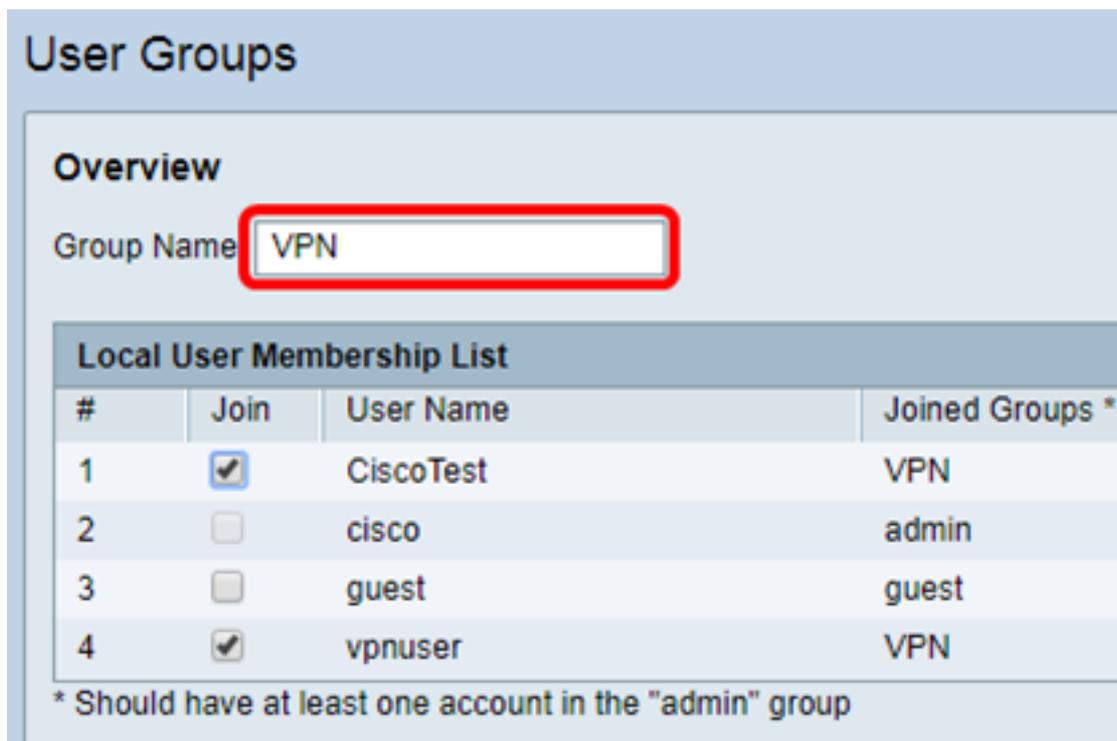
Nota: Le immagini in questo articolo fanno riferimento a un router RV340. Le opzioni possono variare a seconda del modello del dispositivo.



Passaggio 2. Fare clic su **Add** per aggiungere un gruppo di utenti.



Passaggio 3. Nell'area Panoramica, inserire il nome del gruppo nel campo *Nome gruppo*.



Nota: Nell'esempio, viene usata la VPN.

Passaggio 4. In Elenco appartenenza locale selezionare le caselle di controllo dei nomi utente che devono essere inclusi nello stesso gruppo.

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

Nota: Nell'esempio, vengono scelti CiscoTest e vpnuser.

Passaggio 5. In Servizi scegliere un'autorizzazione da concedere agli utenti del gruppo. Le opzioni sono:

- Disattivata - Questa opzione indica che ai membri del gruppo non è consentito accedere all'utility basata sul Web tramite un browser.
- Sola lettura — questa opzione indica che i membri del gruppo possono leggere lo stato del sistema solo dopo aver eseguito l'accesso. Non possono modificare nessuna delle impostazioni.
- Amministratore: questa opzione fornisce ai membri del gruppo i privilegi di lettura e scrittura e consente di configurare lo stato del sistema.

Services

Web Login Disabled Read Only Administrator

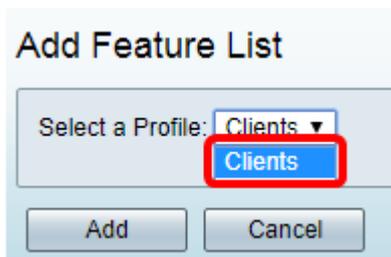
Nota: In questo esempio, è selezionato Sola lettura.

Passaggio 6. Nella tabella EzVPN/Membro in uso del profilo di terze parti, fare clic su **Aggiungi**.

EzVPN/3rd Party

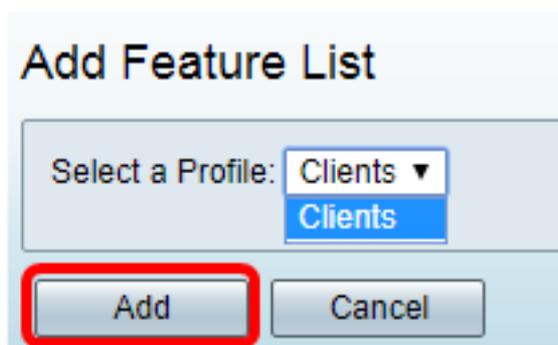
EzVPN/3rd Party Profile Member In-use Table	
#	Group Name

Passaggio 7. Scegliere un profilo dall'elenco a discesa Selezionare un profilo. Le opzioni possono variare a seconda dei profili configurati sul gateway VPN.

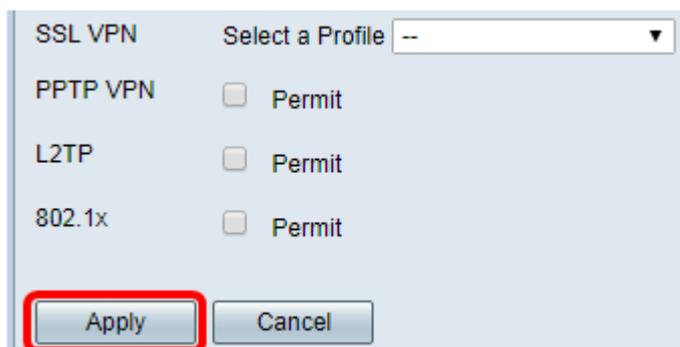


Nota: In questo esempio viene scelto Client.

Passaggio 8. Fare clic su **Add**.



Passaggio 9. Fare clic su **Applica**.



Passaggio 10. Fare clic su **Salva**.

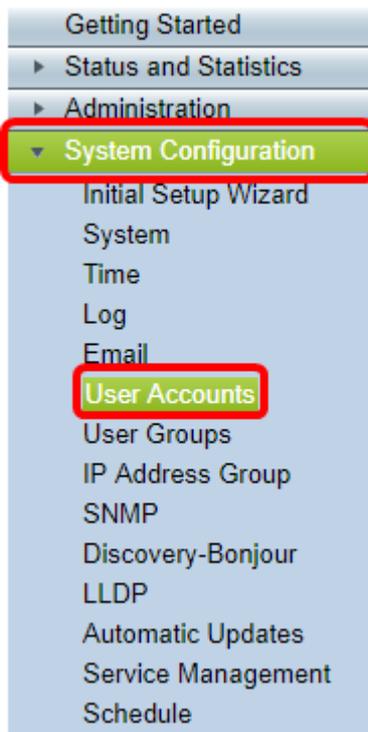


A questo punto, è necessario creare un gruppo di utenti sul router serie RV34x.

[Crea un account utente](#)

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **Configurazione di sistema > Account utente**.

Nota: Le immagini riportate in questo articolo fanno riferimento a un router RV340. Le opzioni possono variare a seconda del modello del dispositivo.



Passaggio 2. Nell'area Elenco appartenenze utente locale fare clic su **Aggiungi**.



Passaggio 3. Inserire un nome per l'utente nel campo *Nome utente*.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Nota: Nell'esempio, viene immesso CiscoTest.

Passaggio 4. Immettere la password utente nel campo *Nuova password*.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Passaggio 5. Confermare la password nella casella *Conferma nuova password*.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Passaggio 6. Scegliere un gruppo dall'elenco a discesa Gruppo. Gruppo a cui verrà associato l'utente.

Group

- VPN
- admin
- guest

Nota: Nell'esempio, viene scelta VPN.

Passaggio 7. Fare clic su **Applica**.

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

Passaggio 8. Fare clic su **Salva**.



A questo punto, è necessario creare un account utente sul router serie RV34x.

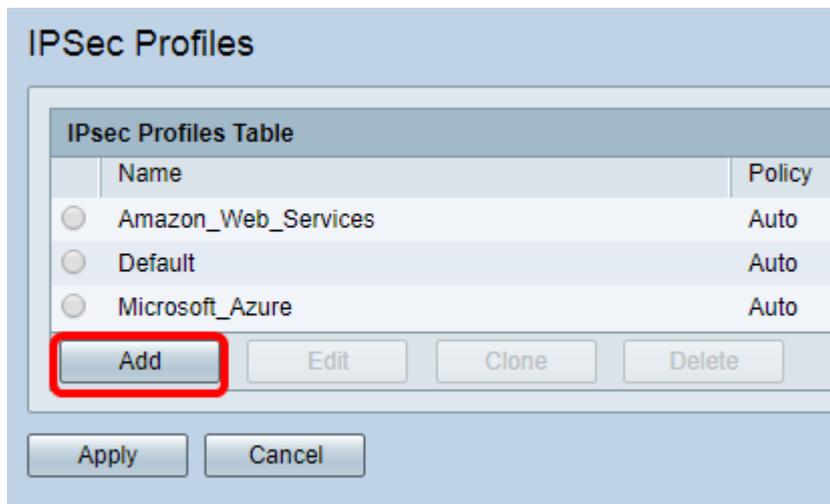
[Configura profilo IPsec](#)

Passaggio 1. Accedere all'utility basata sul Web del router RV34x e scegliere **VPN > Profili IPsec**.



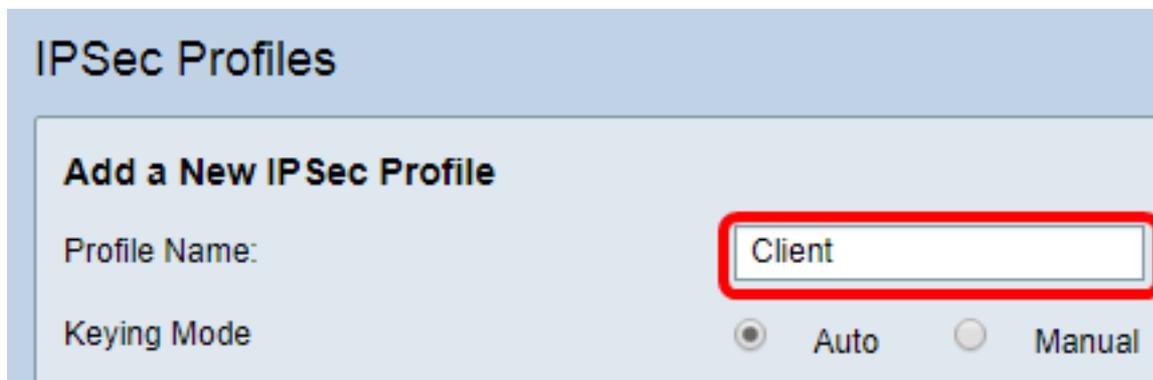
Nota: Le immagini riportate in questo articolo vengono acquisite dal router RV340. Le opzioni possono variare a seconda del modello del dispositivo.

Passaggio 2. Nella tabella Profili IPsec vengono visualizzati i profili esistenti. Fare clic su **Aggiungi** per creare un nuovo profilo.



Nota: Amazon_Web_Services, Default e Microsoft_Azure sono profili predefiniti.

Passaggio 3. Creare un nome per il profilo nel campo *Nome profilo*. Il nome del profilo deve contenere solo caratteri alfanumerici e un carattere di sottolineatura (_) per i caratteri speciali.



Nota: Nell'esempio, viene immesso Client.

Passaggio 4. Fare clic su un pulsante di opzione per determinare il metodo di scambio delle chiavi che verrà utilizzato dal profilo per l'autenticazione. Le opzioni sono:

- Auto — i parametri dei criteri vengono impostati automaticamente. Questa opzione utilizza un criterio IKE (Internet Key Exchange) per l'integrità dei dati e gli scambi di chiavi di crittografia. Se questa opzione è selezionata, le impostazioni di configurazione nell'area Parametri criteri automatici sono attivate. Se questa opzione è selezionata, saltare a [Configura impostazioni automatiche](#).
- Manuale: questa opzione consente di configurare manualmente le chiavi per la crittografia dei dati e l'integrità del tunnel VPN. Se questa opzione è selezionata, le impostazioni di configurazione nell'area Parametri criteri manuali sono attivate. Se si sceglie questa opzione, passare alla sezione [Configurazione delle impostazioni manuali](#).

IPSec Profiles

Add a New IPSec Profile

Profile Name:

Keying Mode Auto Manual

Nota: Per questo esempio è stato scelto Auto.

[Configurazione delle impostazioni di Fase I e Fase II](#)

Passaggio 1. Nell'area Opzioni fase 1, scegliere il gruppo Diffie-Hellman (DH) appropriato da utilizzare con la chiave nella fase 1 dall'elenco a discesa Gruppo DH. Diffie-Hellman è un protocollo di scambio chiave crittografica utilizzato nella connessione per lo scambio di set di chiavi già condivisi. La forza dell'algoritmo è determinata dai bit. Le opzioni sono:

- Group2-1024 bit: questa opzione calcola la chiave più lentamente, ma è più sicura di Group 1.
- Gruppo5-1536 bit — questa opzione calcola la chiave più lentamente, ma è la più sicura.

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime:

Perfect Forward Secrecy: Enable

Nota: Nell'esempio, viene scelto Group5-1536 bit.

Passaggio 2. Dall'elenco a discesa Crittografia, scegliere un metodo di crittografia per crittografare e decrittografare Encapsulating Security Payload (ESP) e Internet Security Association and Key Management Protocol (ISAKMP). Le opzioni sono:

- 3DES: standard per la crittografia tripla dei dati.
- AES-128 — Advanced Encryption Standard utilizza una chiave a 128 bit.
- AES-192 — Advanced Encryption Standard utilizza una chiave a 192 bit.
- AES-256 — Advanced Encryption Standard utilizza una chiave a 256 bit.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: AES-128

SA Lifetime: AES-192
AES-256

Perfect Forward Secrecy: Enable

Nota: AES è il metodo standard di crittografia su DES e 3DES per prestazioni e sicurezza più elevate. L'aumento della lunghezza della chiave AES aumenta la sicurezza con un calo delle prestazioni. Nell'esempio, viene scelto AES-128.

Passaggio 3. Dall'elenco a discesa Autenticazione, scegliere un metodo di autenticazione che determinerà la modalità di autenticazione di ESP e ISAKMP. Le opzioni sono:

- MD5 — Message-Digest Algorithm ha un valore hash a 128 bit.
- SHA-1: l'algoritmo hash sicuro ha un valore hash a 160 bit.
- SHA2-256 — algoritmo hash sicuro con un valore hash a 256 bit.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: MD5
SHA1
SHA2-256

Perfect Forward Secrecy: Enable

Nota: MD5 e SHA sono entrambe funzioni hash crittografiche. Prendono un dato, lo compattano e creano un output esadecimale unico che in genere non può essere riprodotto. Nell'esempio viene scelto SHA1.

Passaggio 4. Nel campo *Durata SA*, immettere un valore compreso tra 120 e 86400. Si tratta dell'intervallo di tempo durante il quale l'associazione di sicurezza IKE (Internet Key Exchange) rimarrà attiva. Il valore predefinito è 28800.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

Nota: nell'esempio, viene immesso 86400.

Passaggio 5. (Facoltativo) Selezionare la casella di controllo **Abilita** Perfect Forward Secrecy per generare una nuova chiave per la crittografia e l'autenticazione del traffico IPSec.

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

Nota: Nell'esempio, la funzione Perfect Forward Secrecy è abilitata.

Passaggio 6. Dall'elenco a discesa Selezione protocollo nell'area Opzioni fase II, scegliere un tipo di protocollo da applicare alla seconda fase della negoziazione. Le opzioni sono:

- ESP — questa opzione incapsula i dati da proteggere. Se si sceglie questa opzione, andare al [Passaggio 7](#) per scegliere un metodo di crittografia.
- AH — questa opzione è nota anche come AH (Authentication Header). Si tratta di un protocollo di sicurezza che fornisce l'autenticazione dei dati e il servizio anti-replay opzionale. AH è incorporato nel datagramma IP da proteggere. Se si sceglie questa opzione, andare al [passaggio 8](#).

Phase II Options

Protocol Selection: ESP

Encryption: ESP

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

Nota: Nell'esempio viene scelto ESP.

[Passaggio 7](#). Se nel passaggio 6 è stato scelto ESP, scegliere un metodo di autenticazione che determinerà la modalità di autenticazione di ESP e ISAKMP. Le opzioni sono:

- 3DES: standard Triple Data Encryption
- AES-128 — Advanced Encryption Standard utilizza una chiave a 128 bit.
- AES-192 — Advanced Encryption Standard utilizza una chiave a 192 bit.
- AES-256 — Advanced Encryption Standard utilizza una chiave a 256 bit.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: AES-128

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

Nota: Nell'esempio, viene scelto AES-128.

[Passaggio 8](#). Dall'elenco a discesa Autenticazione scegliere un metodo di autenticazione che determinerà la modalità di autenticazione di ESP e ISAKMP. Le opzioni sono:

- MD5 — Message-Digest Algorithm ha un valore hash a 128 bit.
- SHA-1: l'algorithmo hash sicuro ha un valore hash a 160 bit.
- SHA2-256 — algorithmo hash sicuro con un valore hash a 256 bit.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime:

DH Group:

Apply Cancel

Nota: Nell'esempio viene scelto SHA1.

Passaggio 9. Nel campo *Durata associazione di protezione* immettere un valore compreso tra 120 e 2800. Questo valore indica il periodo di tempo durante il quale l'associazione di protezione IKE rimarrà attiva in questa fase. Il valore predefinito è 3600.

Passaggio 10. Dall'elenco a discesa Gruppo DH, scegliere un gruppo DH da utilizzare con la chiave nella fase 2. Le opzioni sono:

- Group2-1024 bit: questa opzione calcola la chiave più lentamente, ma è più sicura di Group1.
- Gruppo5-1536 bit — questa opzione calcola la chiave più lentamente, ma è la più sicura.

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

Nota: nell'esempio, viene immesso 3600.

Passaggio 11. Fare clic su **Applica**.

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:

Passaggio 12. Fare clic su **Save** per salvare la configurazione in modo permanente.



A questo punto, è necessario configurare correttamente un profilo IPSec automatico sul router serie RV34x.

[Configurazione delle impostazioni manuali](#)

Passaggio 1. Nel campo *SPI-Incoming*, immettere un valore esadecimale da 100 a FFFF per il tag SPI (Security Parameter Index) per il traffico in entrata sulla connessione VPN. Il tag SPI viene utilizzato per distinguere il traffico di una sessione dal traffico di altre sessioni.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Nota: Nell'esempio, viene immesso 0xABCD.

Passaggio 2. Nel campo *SPI-Outgoing*, immettere un valore esadecimale da 100 a FFFF per il tag SPI per il traffico in uscita sulla connessione VPN.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Nota: Nell'esempio, viene immesso 0x1234.

Passaggio 3. Scegliere un valore di cifratura dall'elenco a discesa. Le opzioni sono:

- 3DES: standard Triple Data Encryption
- AES-128 — Advanced Encryption Standard utilizza una chiave a 128 bit.
- AES-192 — Advanced Encryption Standard utilizza una chiave a 192 bit.

SPI Incoming:

SPI Outgoing:

Encryption:

- 3DES
- AES-128
- AES-192
- ✓ AES-256

Nota: Nell'esempio, viene scelto AES-256.

Passaggio 4. Nel campo *Chiave in ingresso*, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 3.

Key-In:

Key-Out:

Nota: In questo esempio, viene immesso 123456789123456789123...

Passaggio 5. Nel campo *Key-Out*, immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 3.

Key-In:	123456789123456789123
Key-Out	1a1a1a1a1a1a1a1a1212121

Nota: In questo esempio, viene immesso 1a1a1a1a1a1a1a1a12121212....

Passaggio 6. Scegliere un metodo di autenticazione dall'elenco a discesa Autenticazione. Le opzioni sono:

- MD5 — Message-Digest Algorithm ha un valore hash a 128 bit.
- SHA-1: l'algoritmo hash sicuro ha un valore hash a 160 bit.
- SHA2-256 — algoritmo hash sicuro con un valore hash a 256 bit.

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

Nota: In questo esempio, viene scelto MD5.

Passaggio 7. Nel campo *Chiave in ingresso*, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 6.

Key-In:	123456789123456789123
Key-Out	1a1a1a1a1a1a1a1a1212121

Nota: In questo esempio, viene immesso 123456789123456789123...

Passaggio 8. Nel campo *Key-Out*, immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 6.

Key-In:	123456789123456789123
Key-Out	1a1a1a1a1a1a1a1a1212121

Nota: In questo esempio, viene immesso 1a1a1a1a1a1a1a1a12121212....

Passaggio 9. Fare clic su .

Passaggio 10. Fare clic su **Save** per salvare la configurazione in modo permanente.

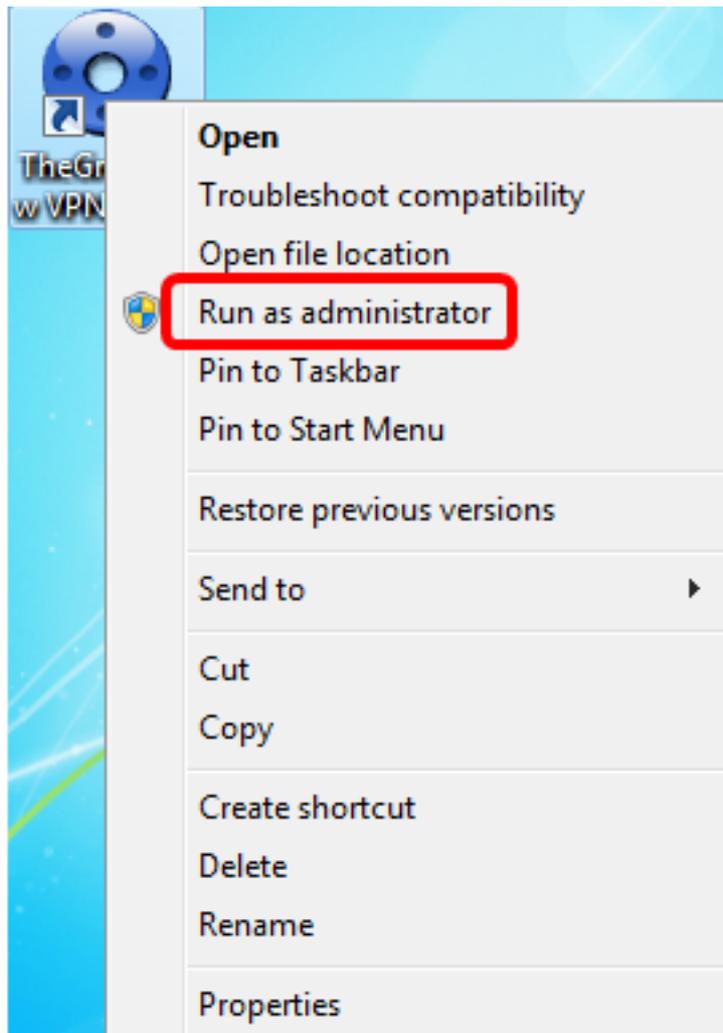


A questo punto, è necessario configurare un profilo IPsec manuale su un router serie RV34x.

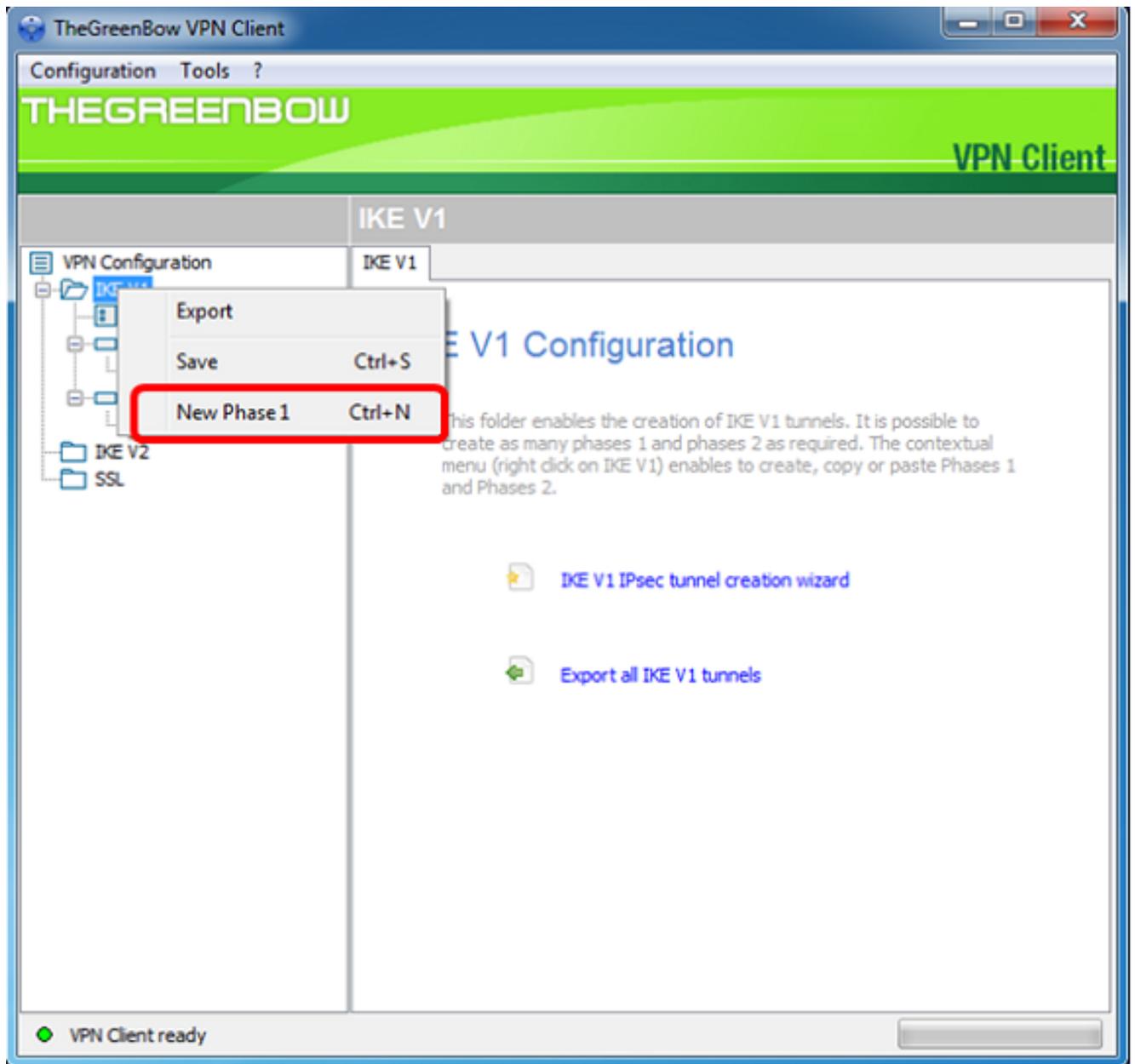
Configurazione del software client VPN GreenBow

Configurazione delle impostazioni della fase 1

Passaggio 1. Fare clic con il pulsante destro del mouse sull'icona di GreenBow VPN Client e scegliere **Esegui come amministratore**.

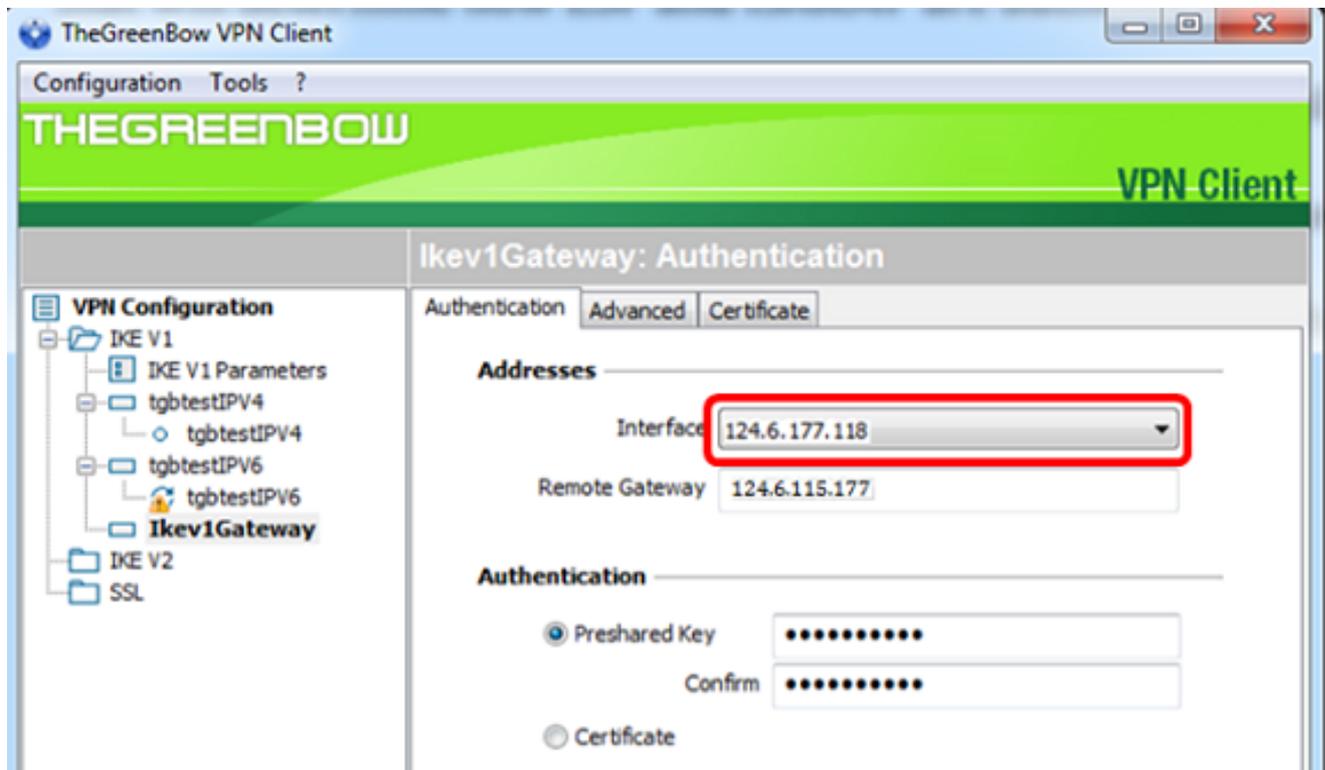


Passaggio 2. Nel riquadro sinistro in Configurazione VPN, fare clic con il pulsante destro del mouse su IKE V1 e scegliere **Nuova fase 1**.



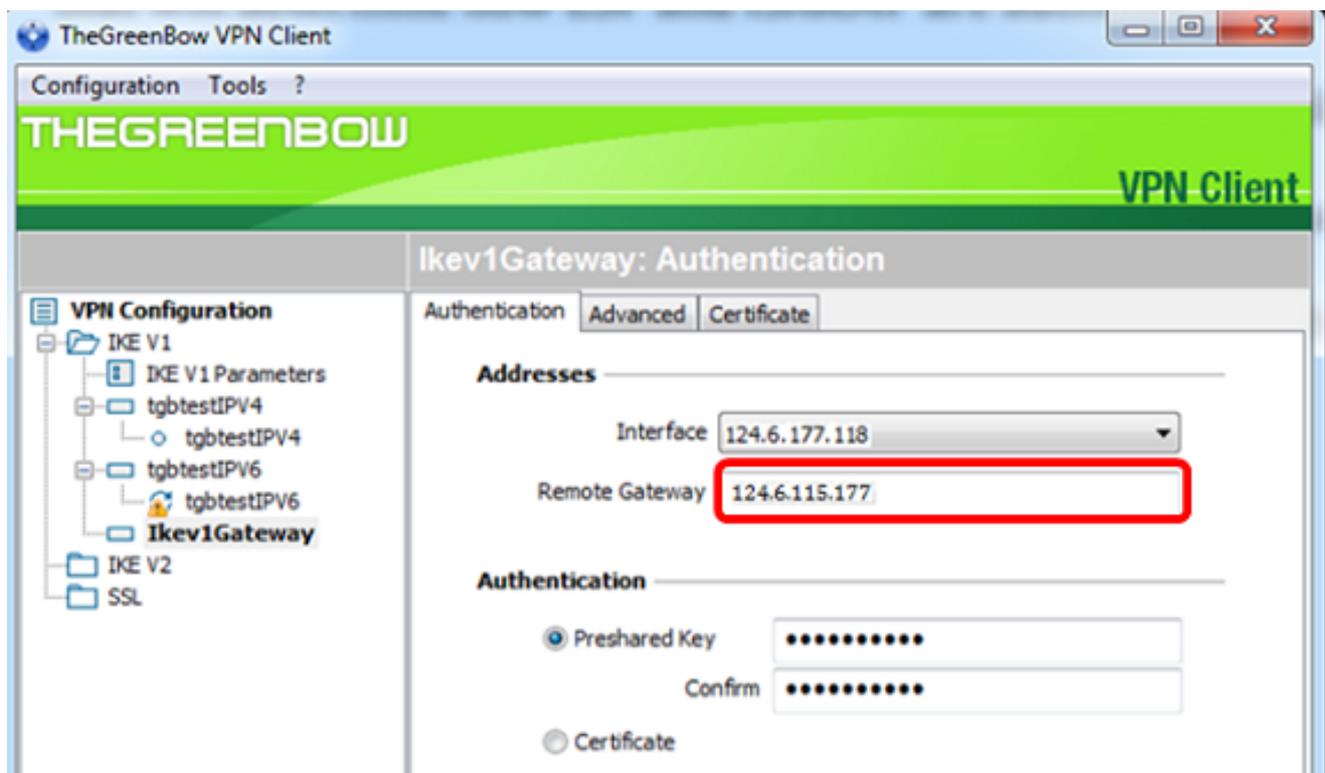
Passaggio 3. Nella scheda Autenticazione sotto Indirizzi, verificare che l'indirizzo IP nell'area Interfaccia sia lo stesso dell'indirizzo IP WAN del computer in cui è installato il client VPN GreenBow.

Nota: Nell'esempio, l'indirizzo IP è 124.6.177.118.



Passaggio 4. Immettere l'indirizzo del gateway remoto nel campo *Gateway remoto*.

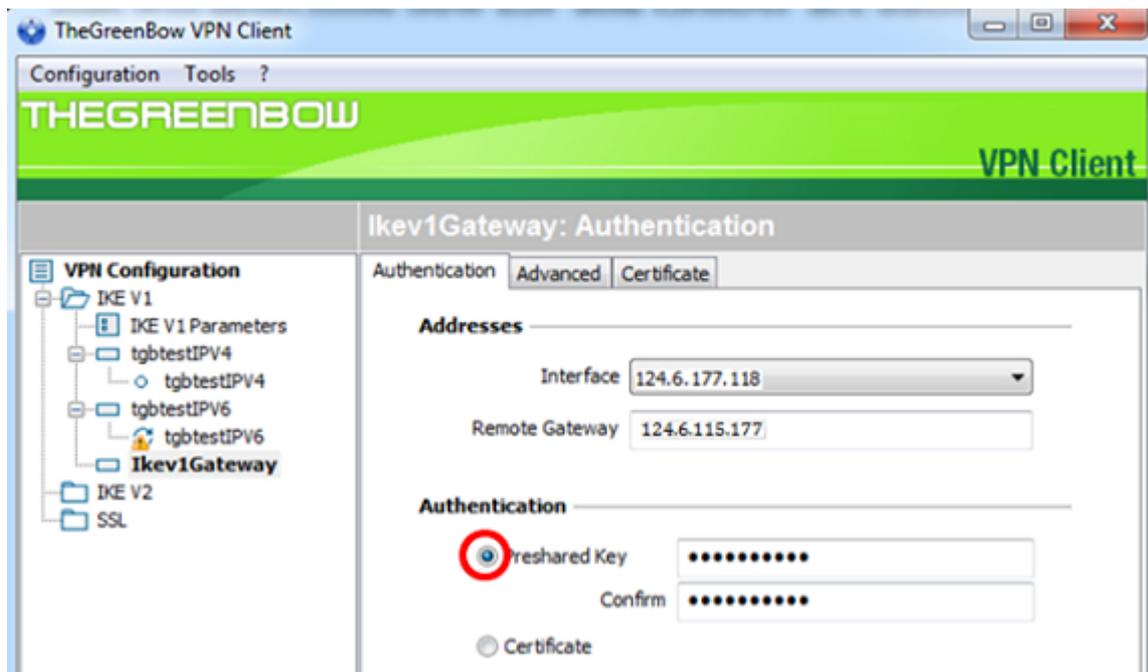
Nota: Nell'esempio, l'indirizzo IP del router RV34x remoto è 124.6.15.177.



Passaggio 5. In Autenticazione scegliere il tipo di autenticazione. Le opzioni sono:

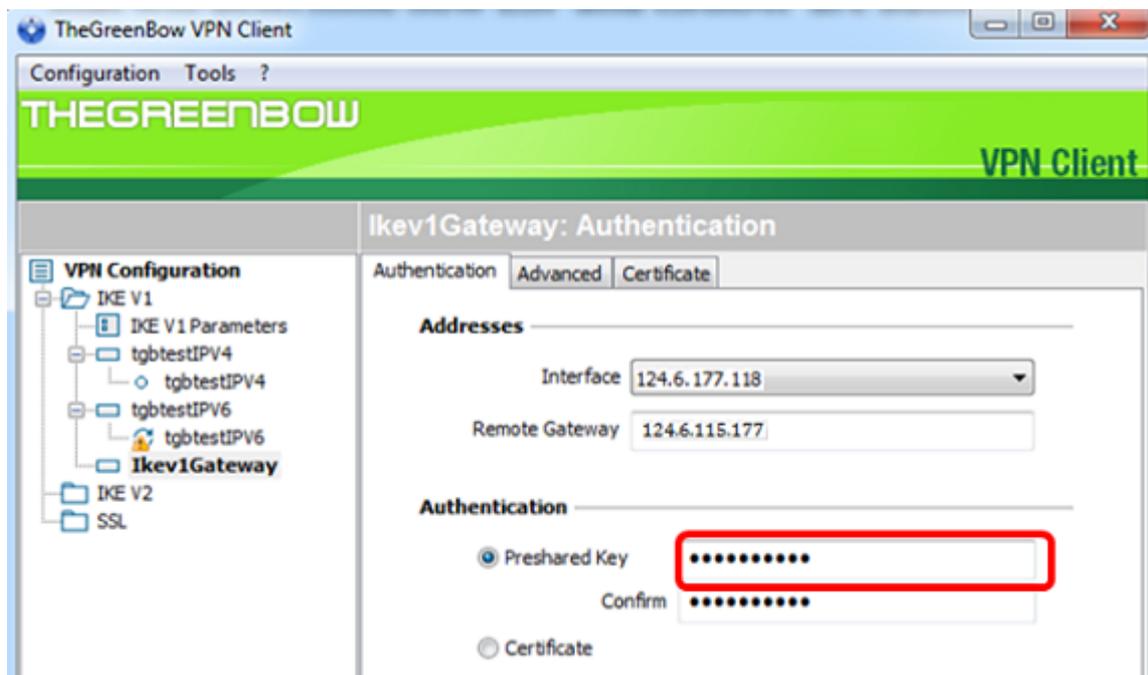
- Chiave già condivisa — questa opzione consente all'utente di utilizzare una password configurata sul gateway VPN. Per poter stabilire un tunnel VPN, l'utente deve associare la password.
- Certificato — questa opzione utilizza un certificato per completare l'handshake tra il client

VPN e il gateway VPN.

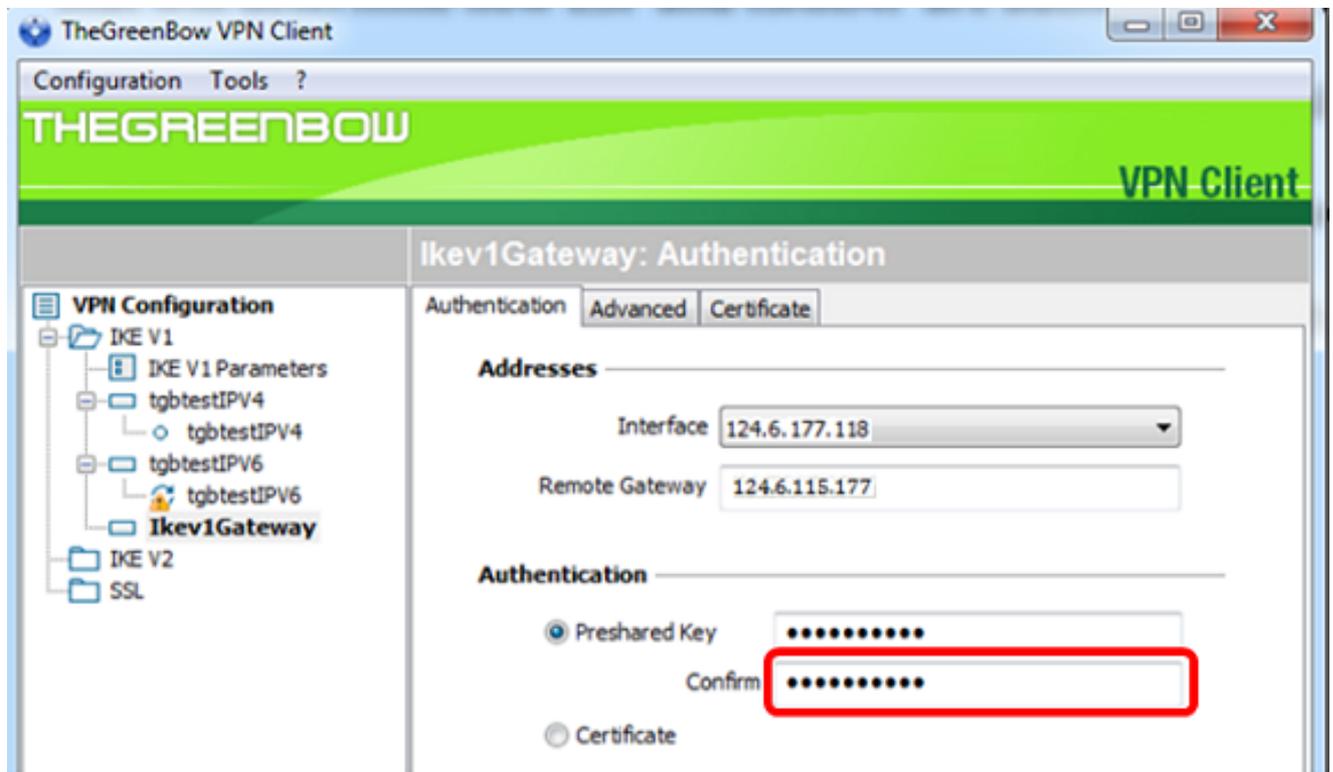


Nota: Nell'esempio, la chiave già condivisa è scelta per corrispondere alla configurazione del gateway VPN RV34x.

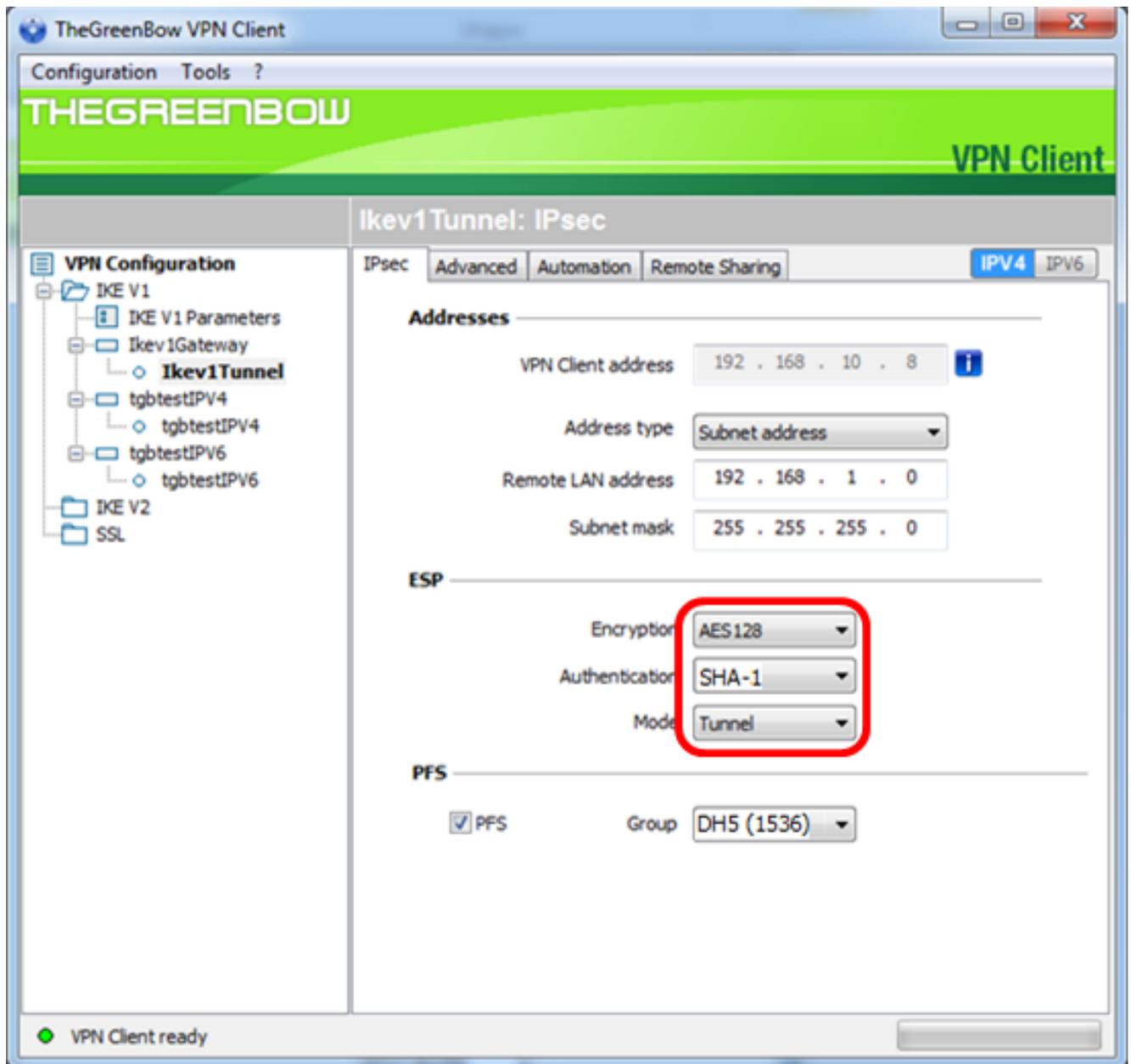
Passaggio 6. Immettere la chiave già condivisa configurata nel router.



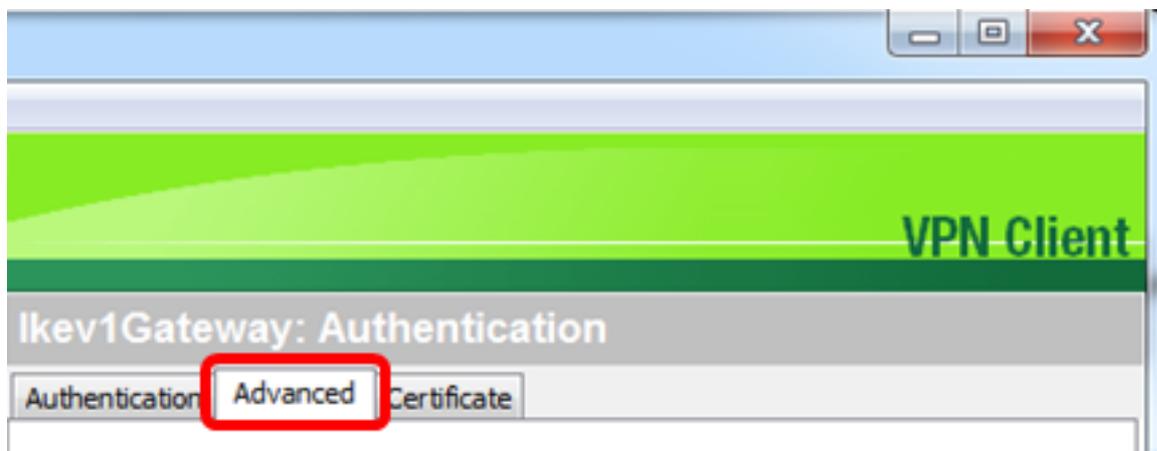
Passaggio 7. Inserire la stessa chiave già condivisa nel campo *Conferma*.



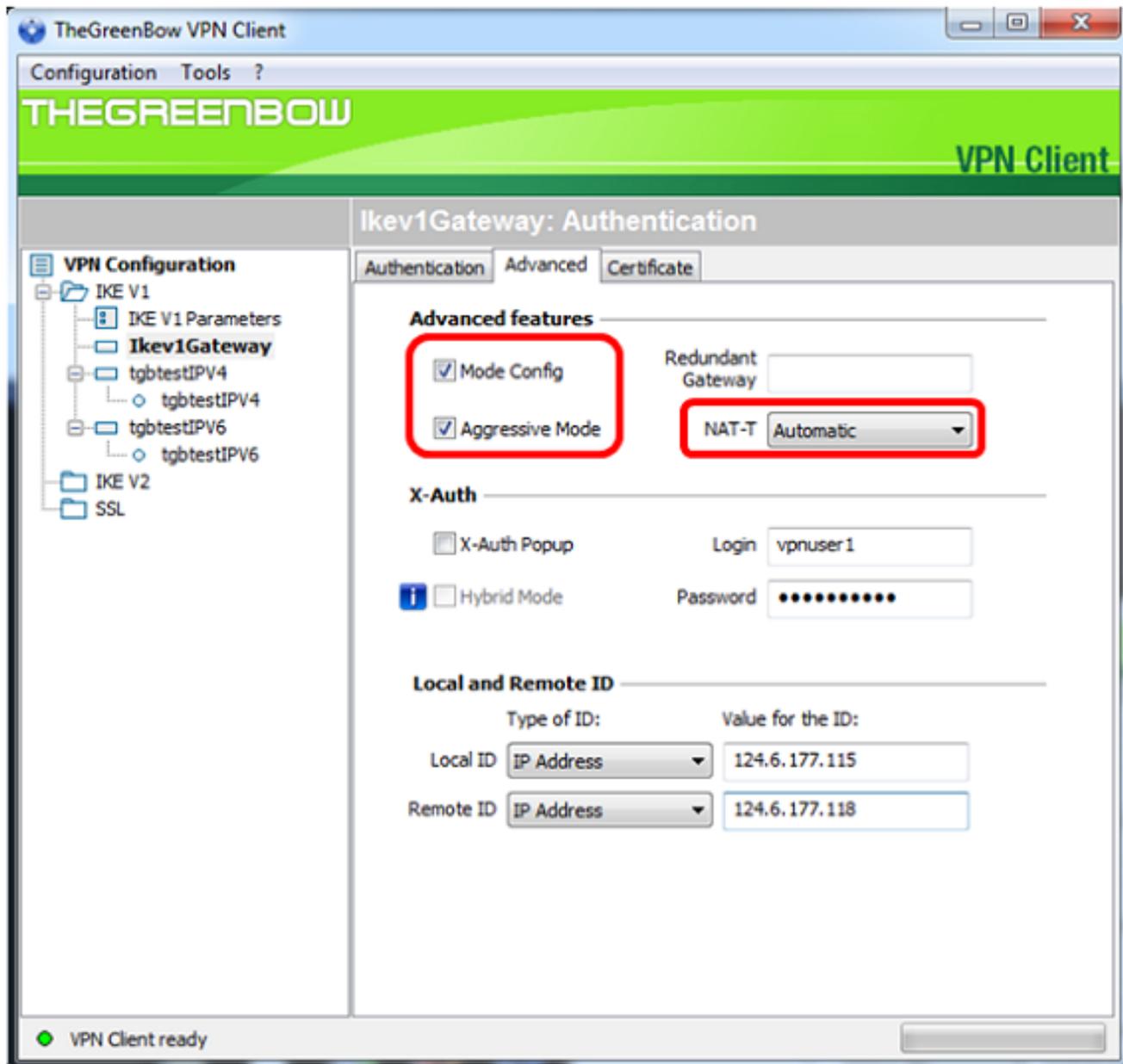
Passaggio 8. In IKE, impostare le impostazioni di crittografia, autenticazione e gruppo di chiavi in modo che corrispondano alla configurazione del router.



Passaggio 9. Fare clic sulla scheda **Avanzate**.

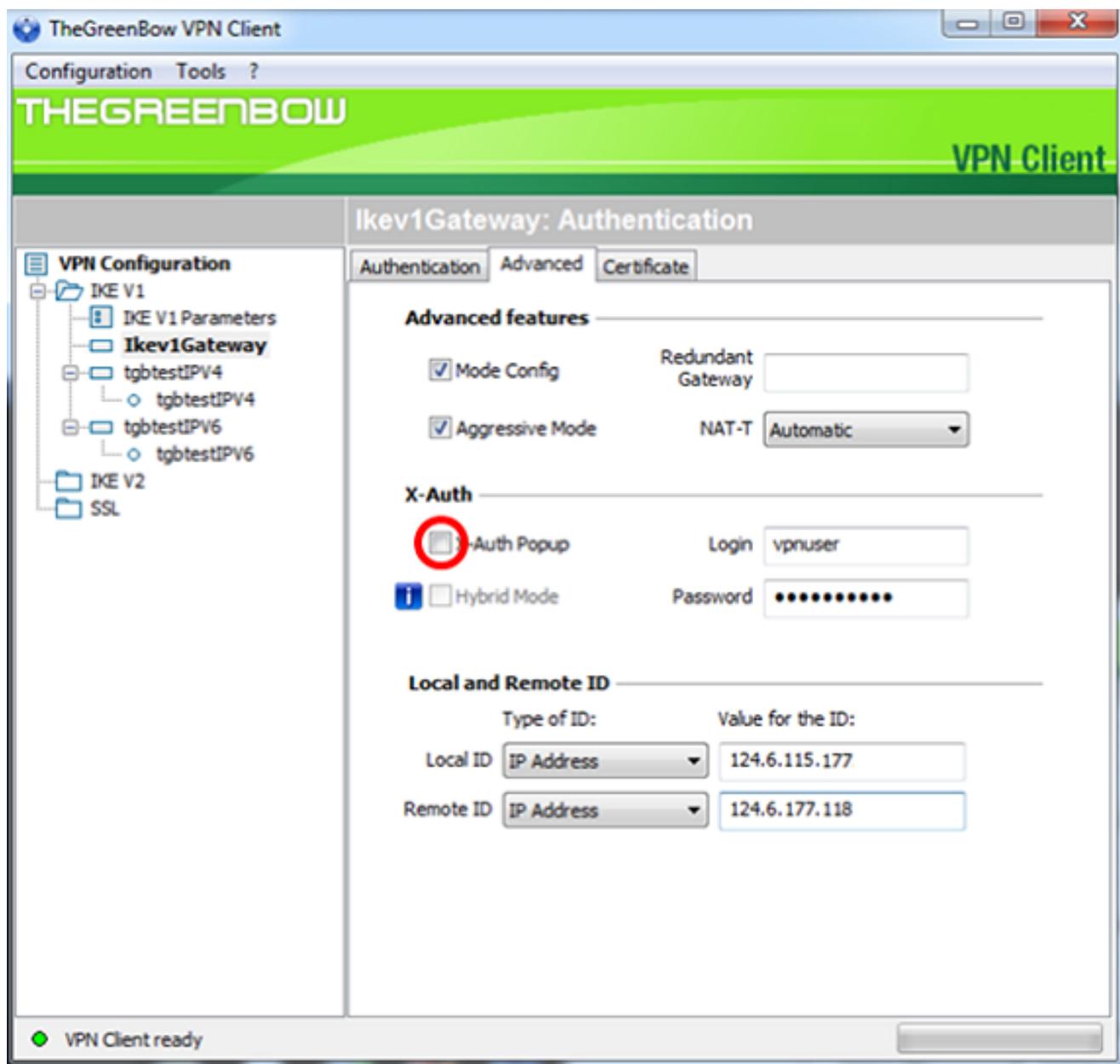


Passaggio 10. (Facoltativo) In Funzioni avanzate, selezionare le caselle di controllo **Mode Config** e **Aggressive Mode** e impostare NAT-T su Automatic.



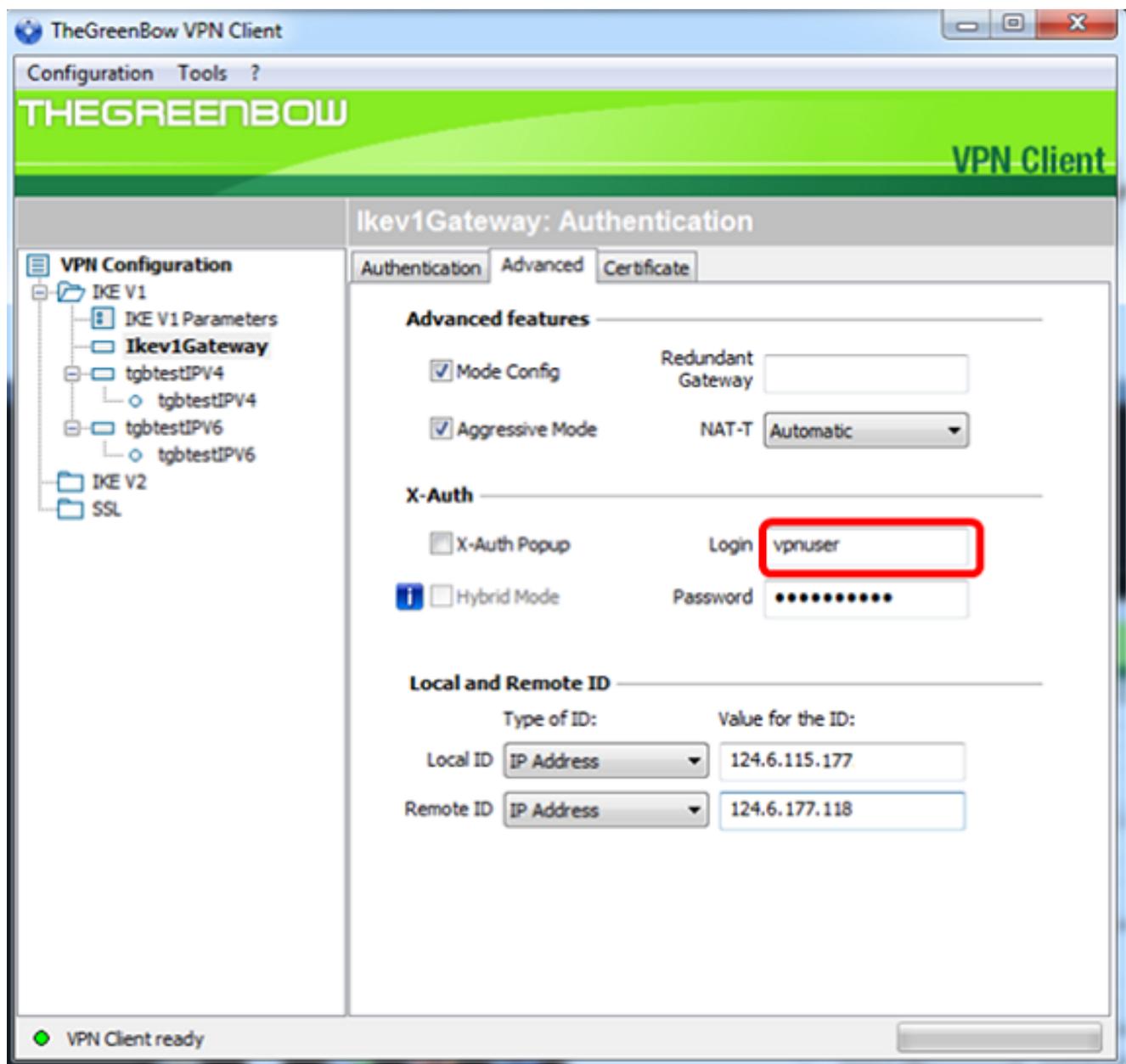
Nota: Con la configurazione della modalità abilitata, il client VPN GreenBow estrae le impostazioni dal gateway VPN per tentare di stabilire un tunnel, abilitando la modalità aggressiva e NAT-T per stabilire una connessione più rapidamente.

Passaggio 11. (Facoltativo) In X-Auth, selezionare la **casella di controllo X-Auth Popup** per richiamare automaticamente la finestra di accesso quando si avvia una connessione. Nella finestra di accesso l'utente immette le proprie credenziali per completare il tunnel.

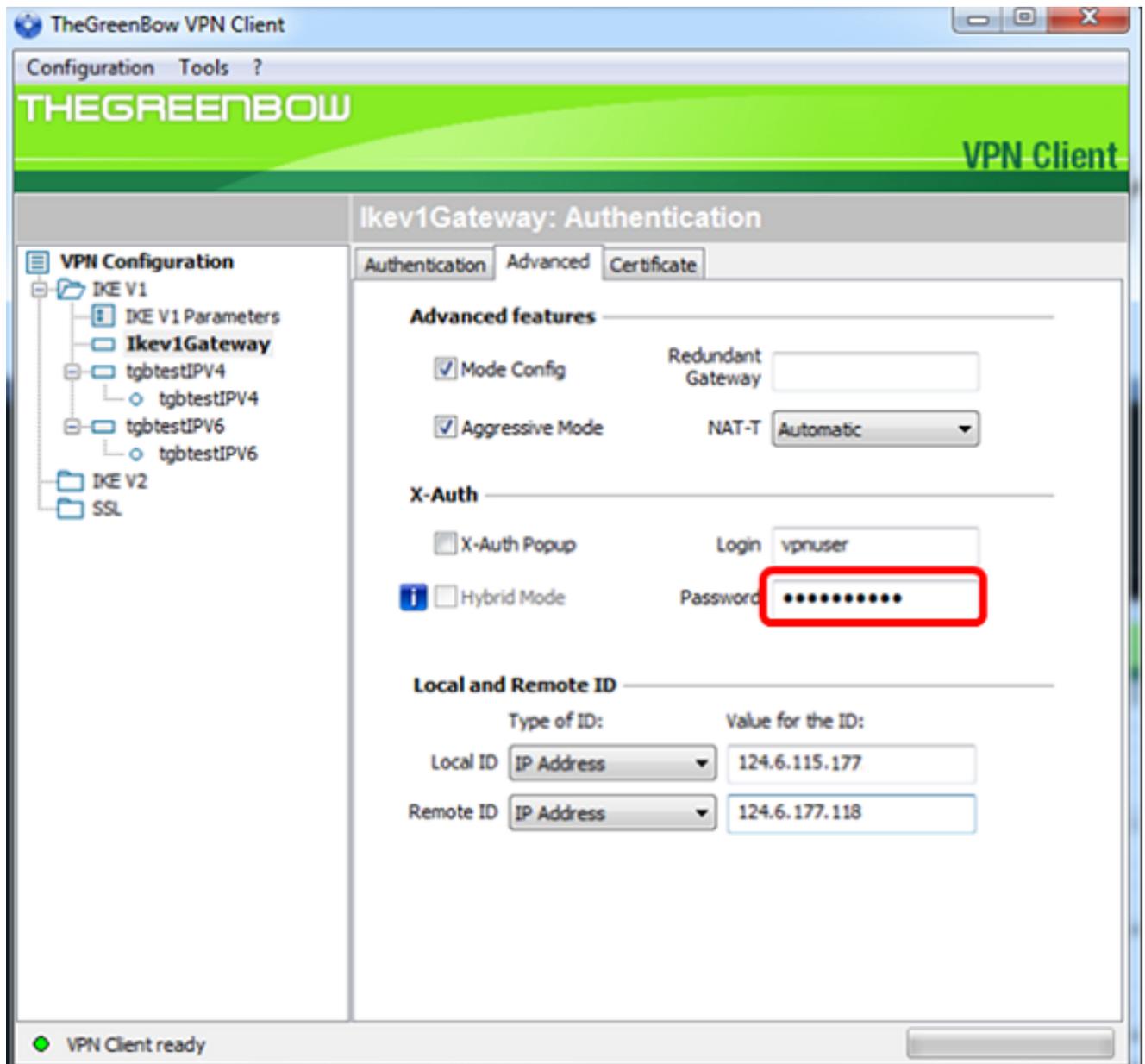


Nota: In questo esempio, Popup X-Auth non è selezionato.

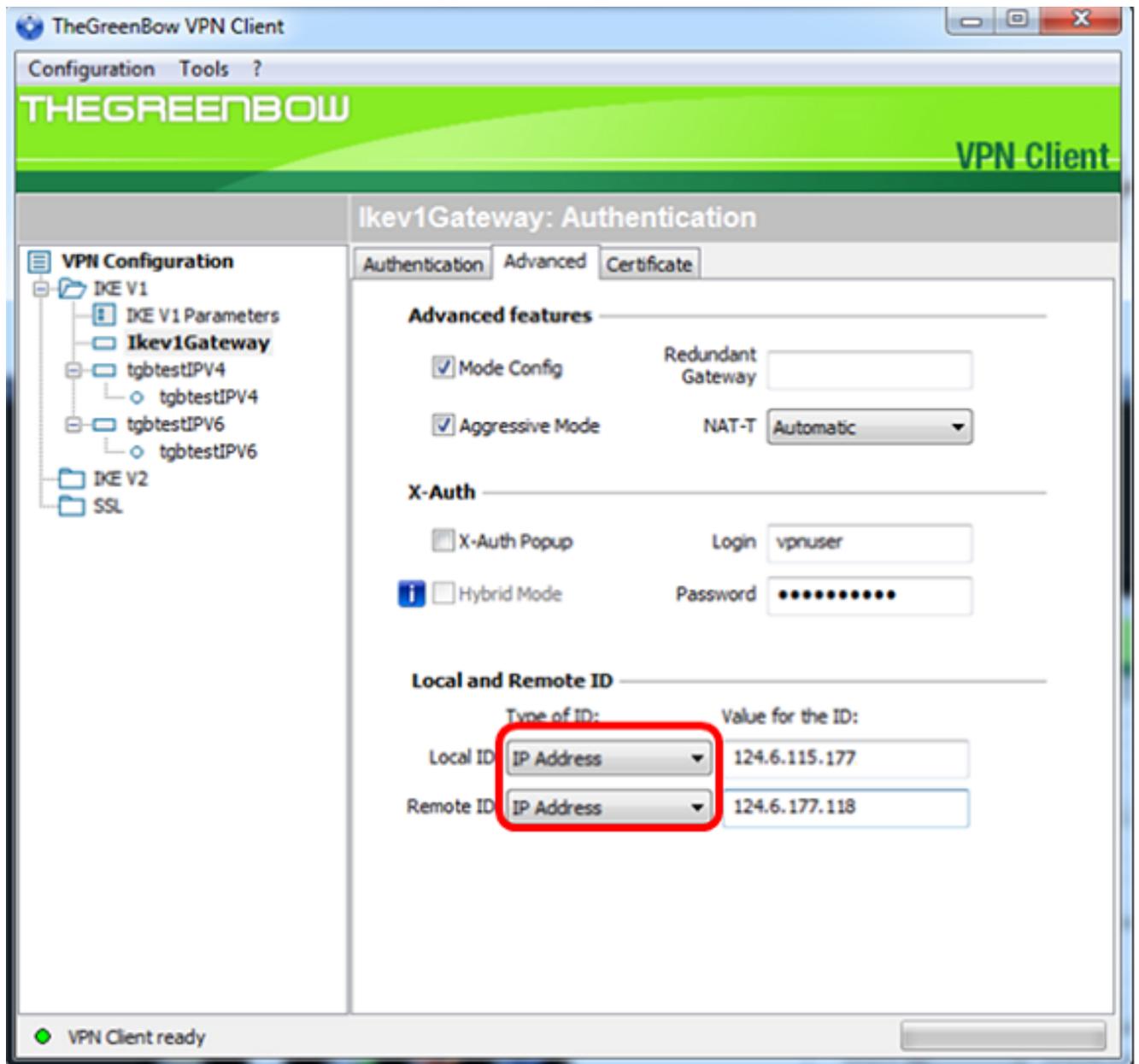
Passaggio 12. Inserire il nome utente nel campo *Login*. Nome utente configurato per la creazione di un gruppo di utenti nel gateway VPN.



Passaggio 13. Immettere la password nel campo *Password*.

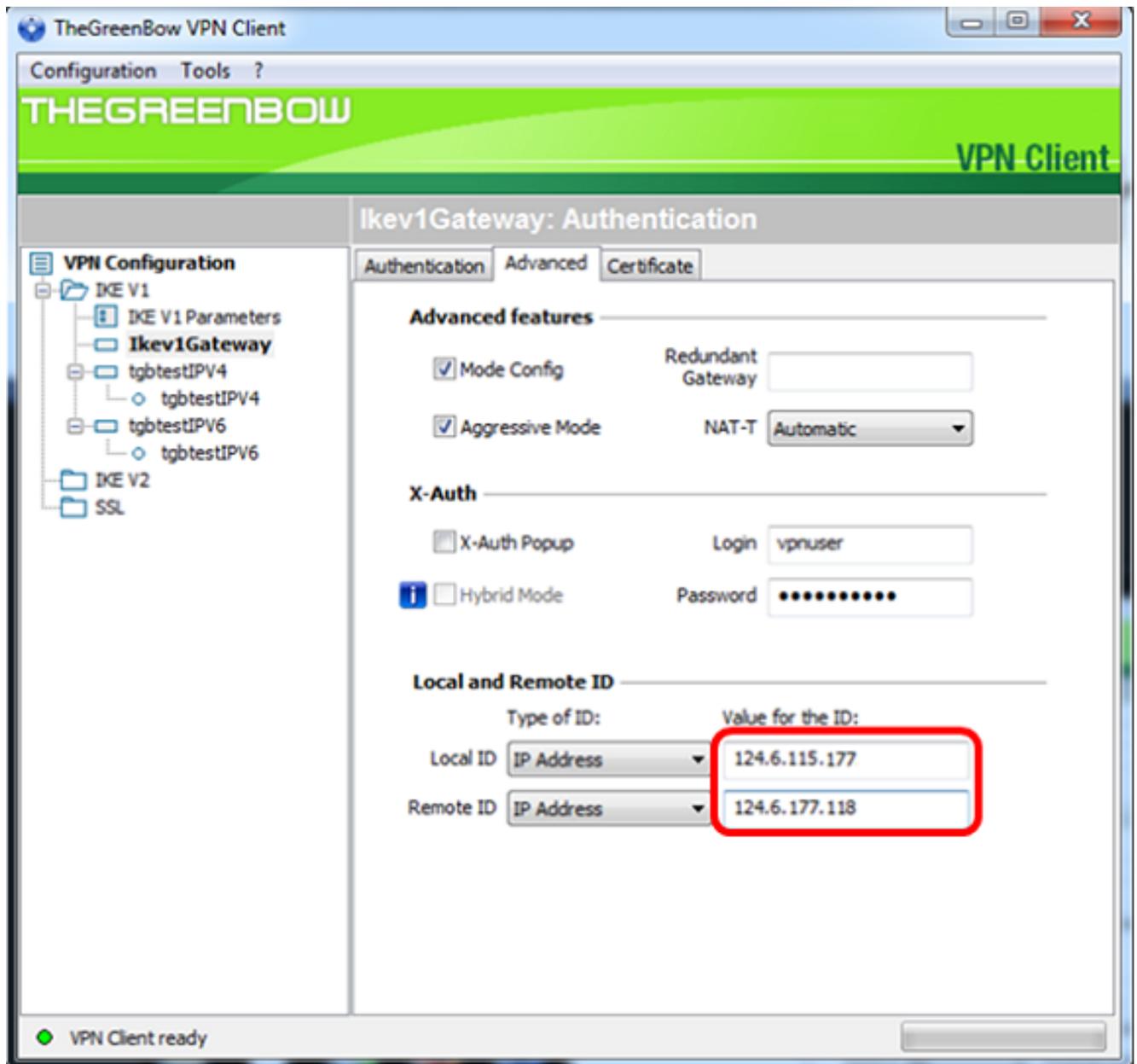


Passaggio 14. In ID locale e remoto impostare l'ID locale e l'ID remoto in modo che corrispondano alle impostazioni del gateway VPN.

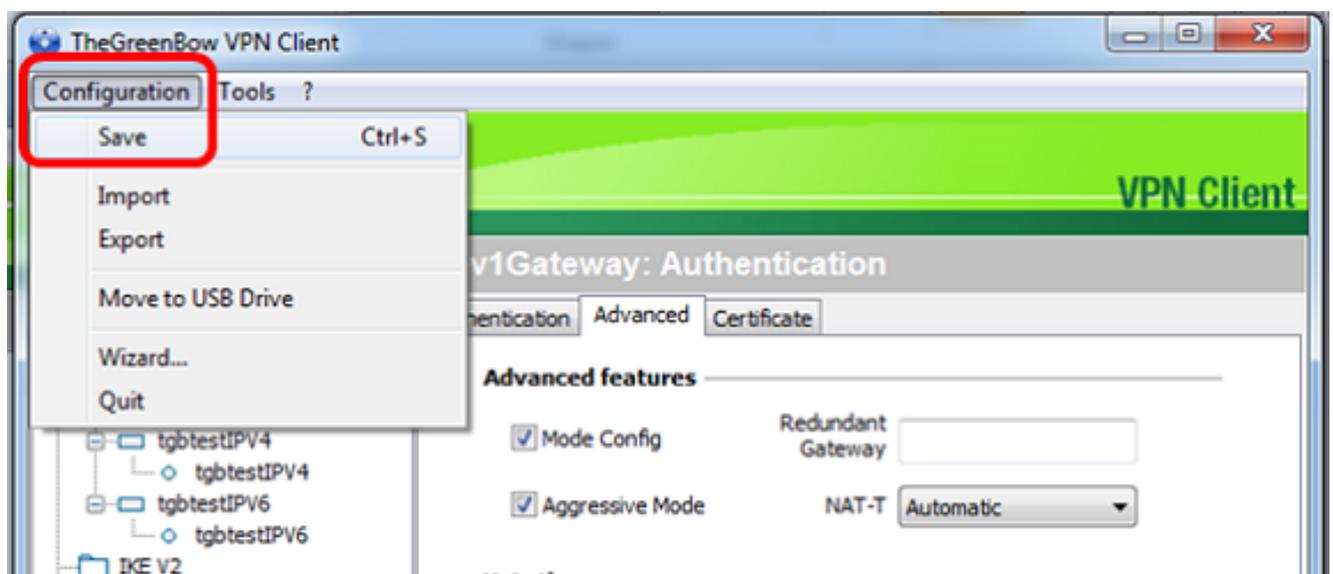


Nota: Nell'esempio, sia l'ID locale che l'ID remoto sono impostati su Indirizzo IP in modo da corrispondere alle impostazioni del gateway VPN RV34x.

Passaggio 15. In Valore per l'ID, immettere l'ID locale e l'ID remoto nei rispettivi campi.

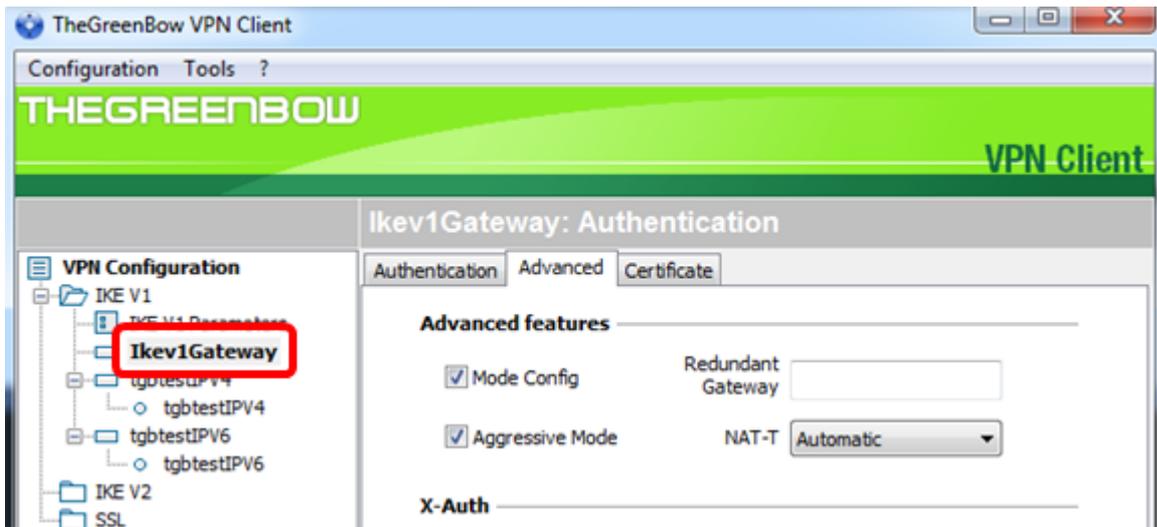


Passaggio 16. Fare clic su **Configuration** > **Save** per salvare le impostazioni.

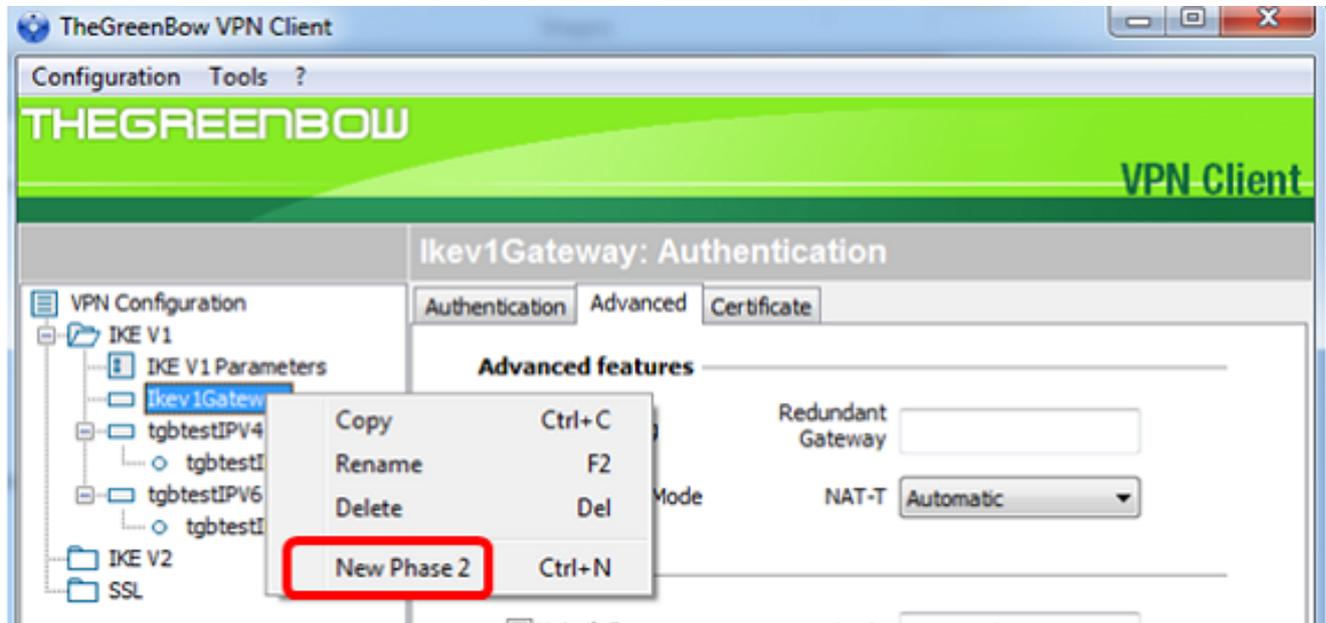


Configurazione delle impostazioni della fase 2

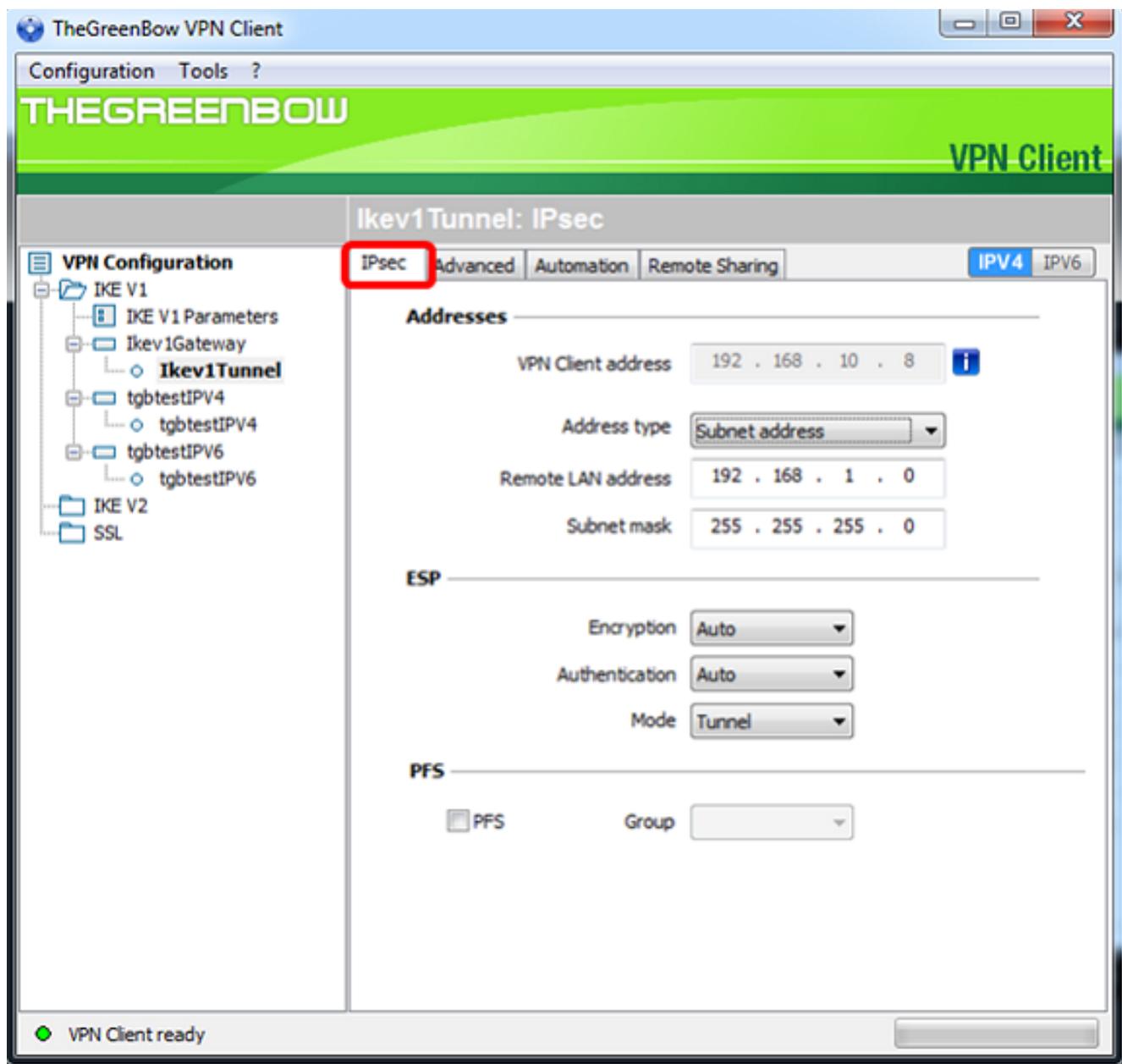
Passaggio 1. Fare clic con il pulsante destro del mouse su **Ikev1Gateway**.



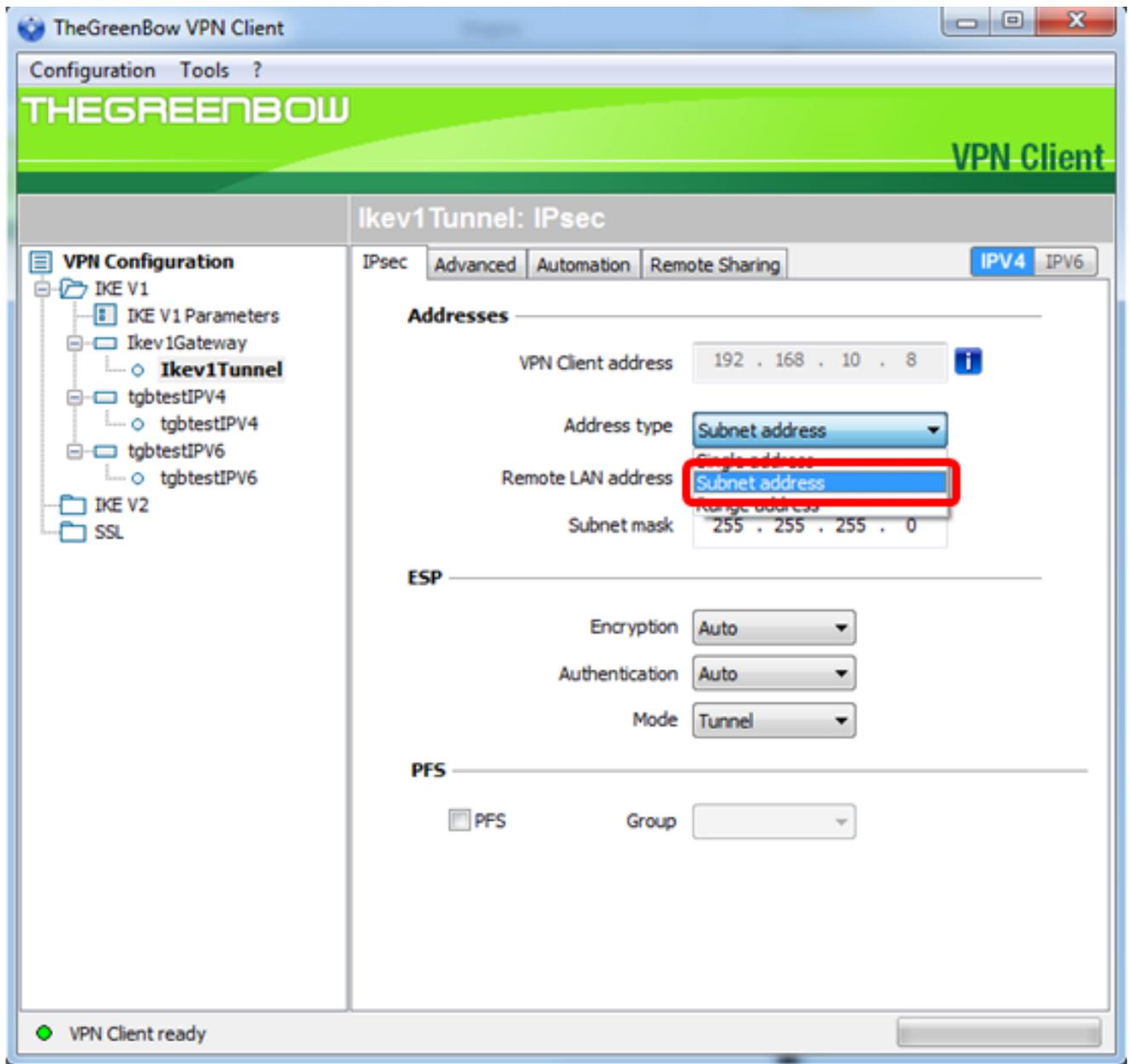
Passaggio 2. Scegliere **Nuova fase 2**.



Passaggio 3. Fare clic sulla scheda **IPSec**.

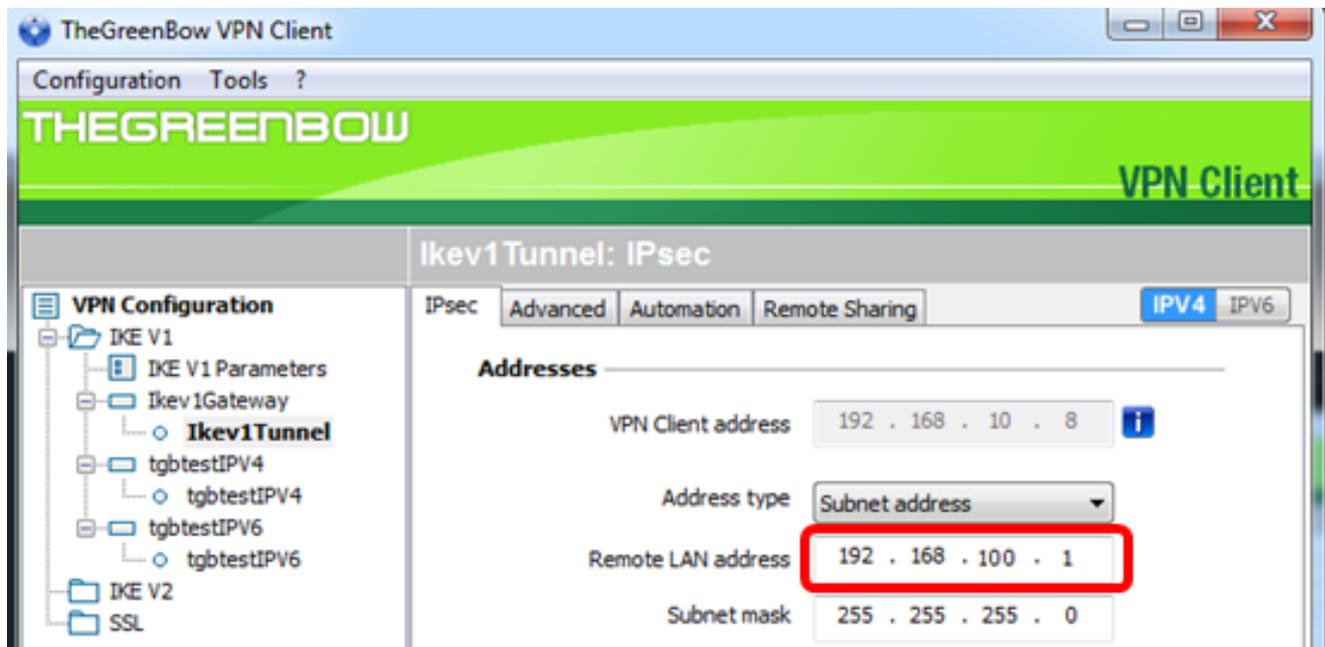


Passaggio 4. Scegliere il tipo di indirizzo a cui il client VPN può accedere dall'elenco a discesa Tipo di indirizzo.



Nota: Nell'esempio riportato di seguito, viene scelto l'indirizzo di subnet.

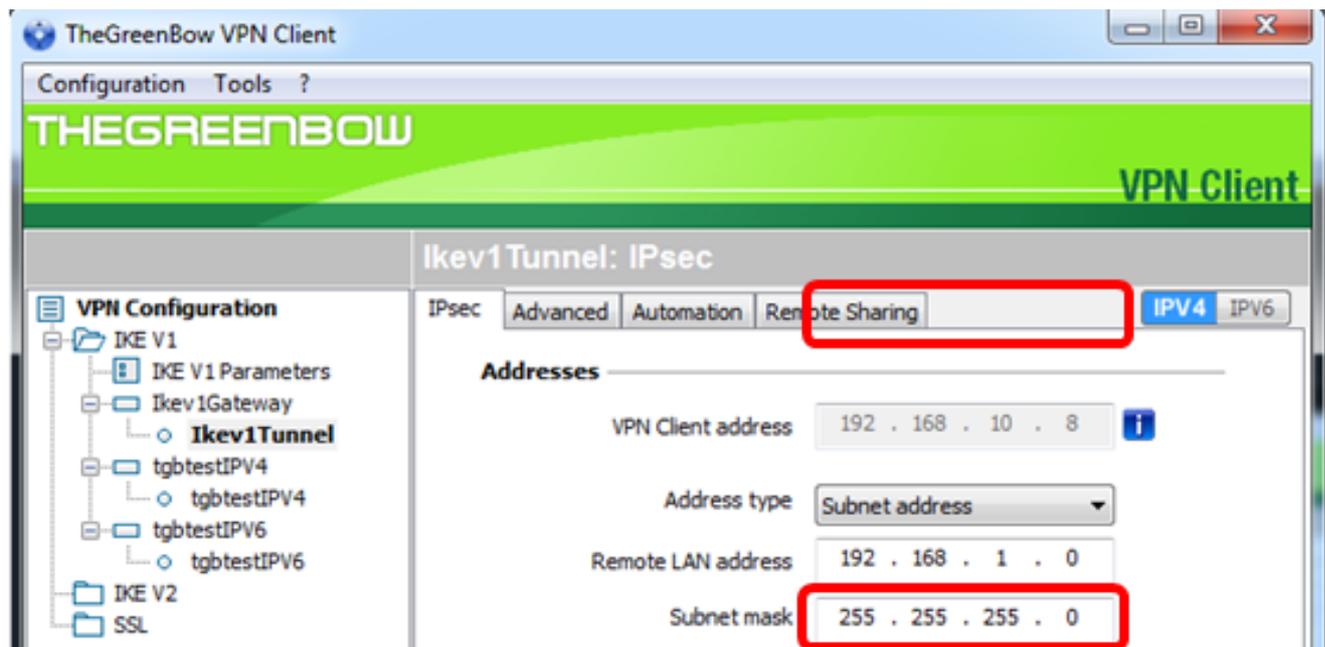
Passaggio 5. Immettere l'indirizzo di rete a cui il tunnel VPN deve accedere nel campo *Indirizzo LAN remoto*.



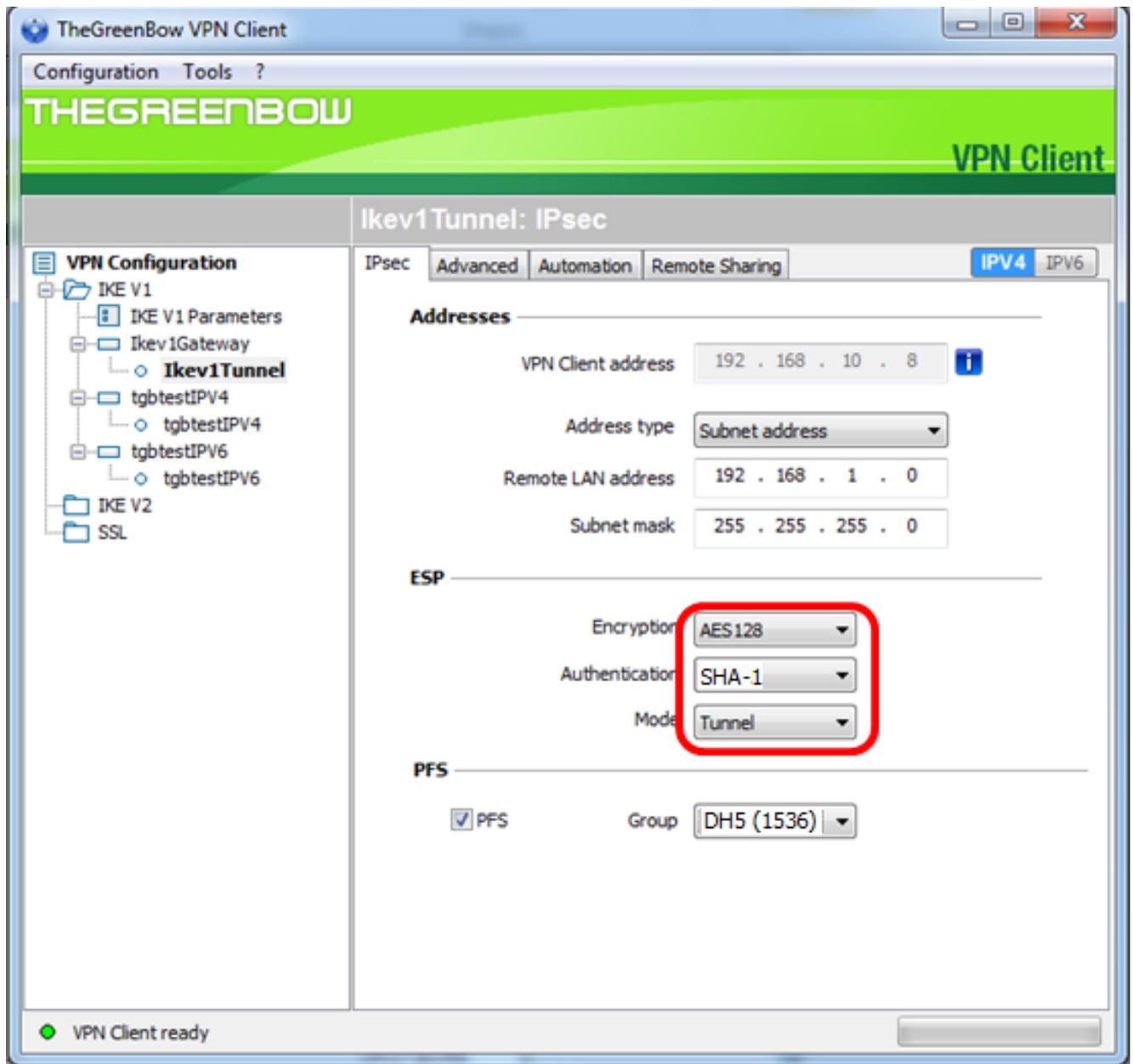
Nota: Nell'esempio, viene immesso 192.168.100.1.

Passaggio 6. Immettere la subnet mask della rete remota nel campo *Subnet mask*.

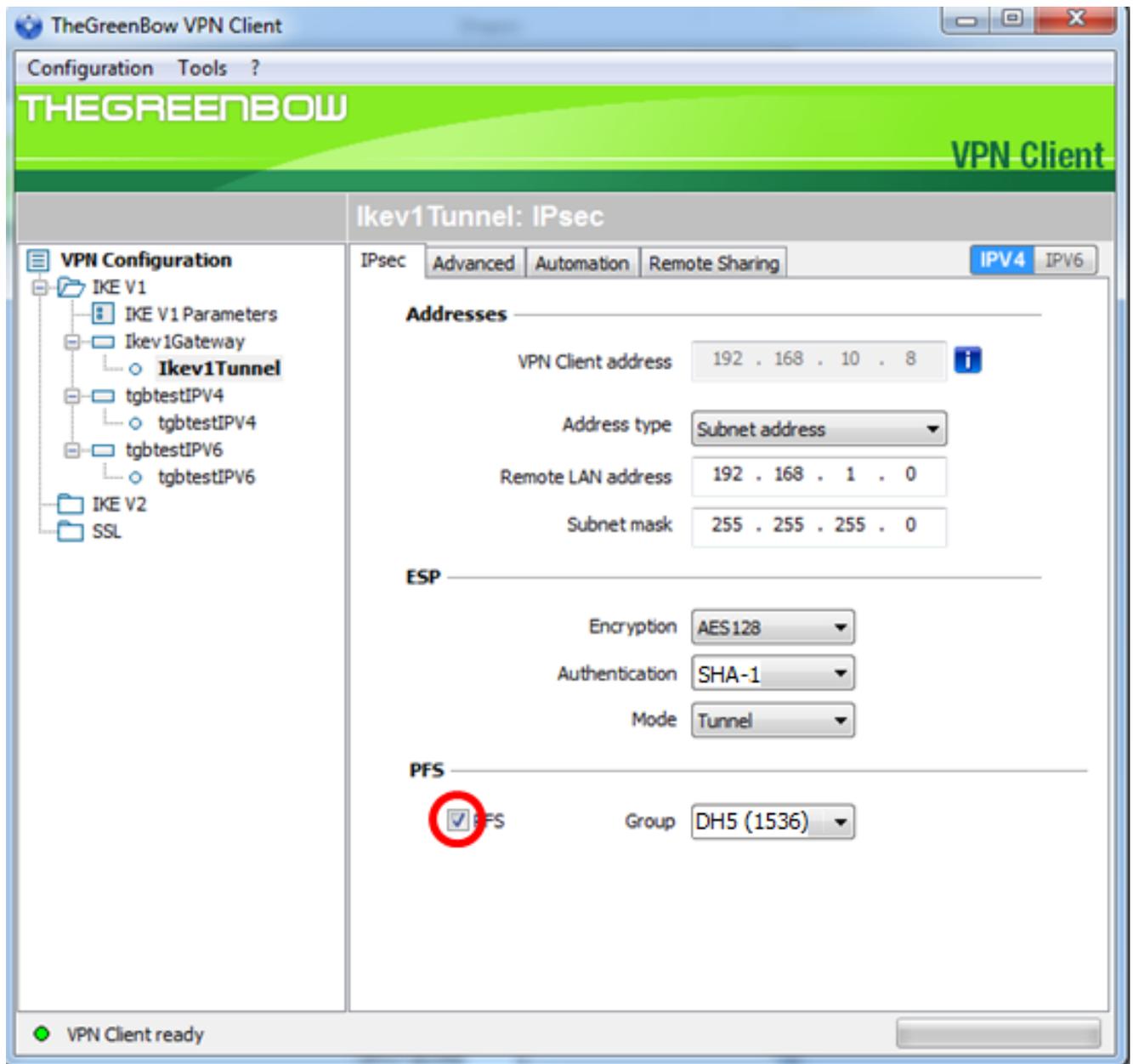
Nota: Nell'esempio, viene immesso 255.255.255.0.



Passaggio 7. In ESP, impostare Encryption, Authentication e Mode (Crittografia, autenticazione e modalità) in modo che corrispondano alle impostazioni del gateway VPN.

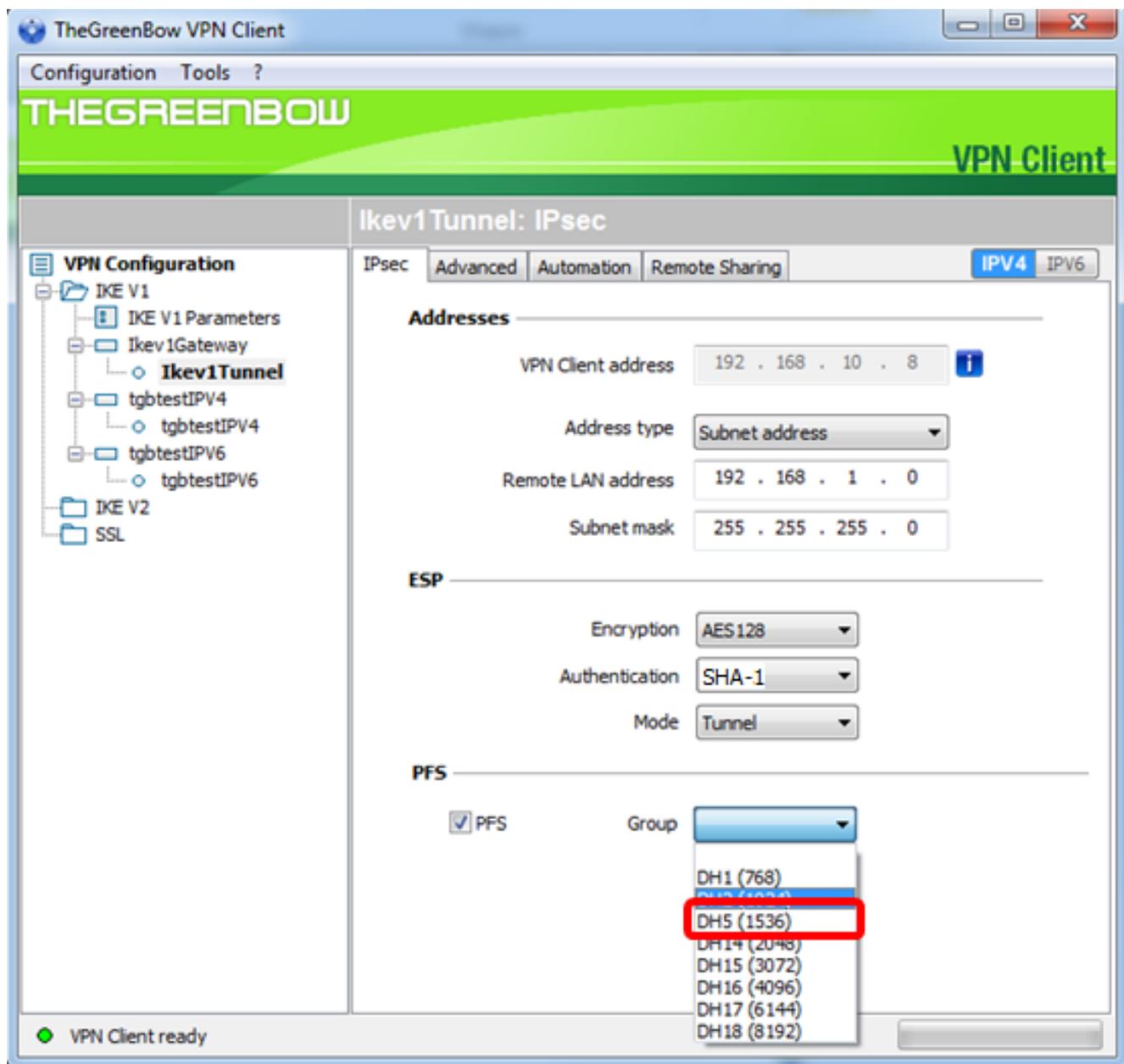


Passaggio 8. (Facoltativo) In PFS selezionare la casella di controllo **PFS** per attivare PFS (Perfect Forward Secrecy). PFS genera chiavi casuali per la crittografia della sessione.

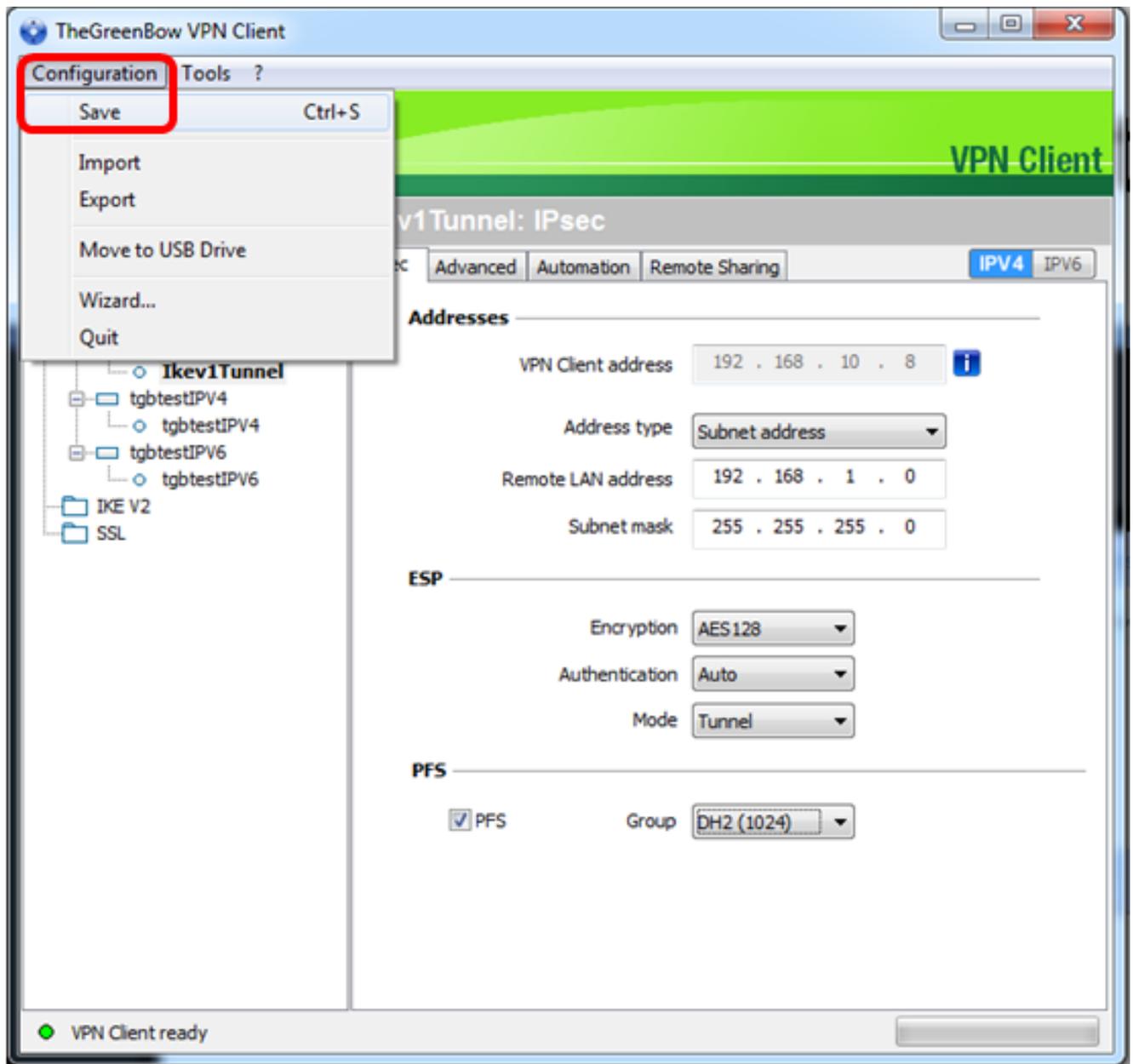


Passaggio 9. Scegliere un'impostazione di gruppo PFS dall'elenco a discesa Gruppo.

Nota: Nell'esempio, viene scelto DH5 (1536) in modo che corrisponda all'impostazione del gruppo DH del router.



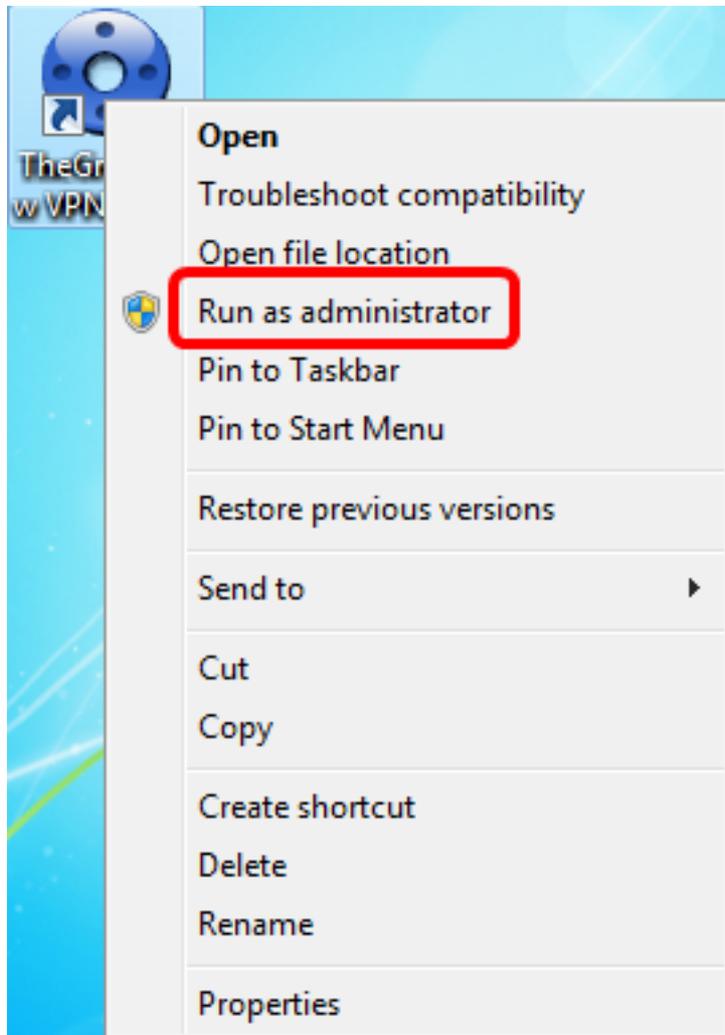
Passaggio 10. Fare clic con il pulsante destro del mouse su **Configuration** (Configurazione) e scegliere **Save** (Salva).



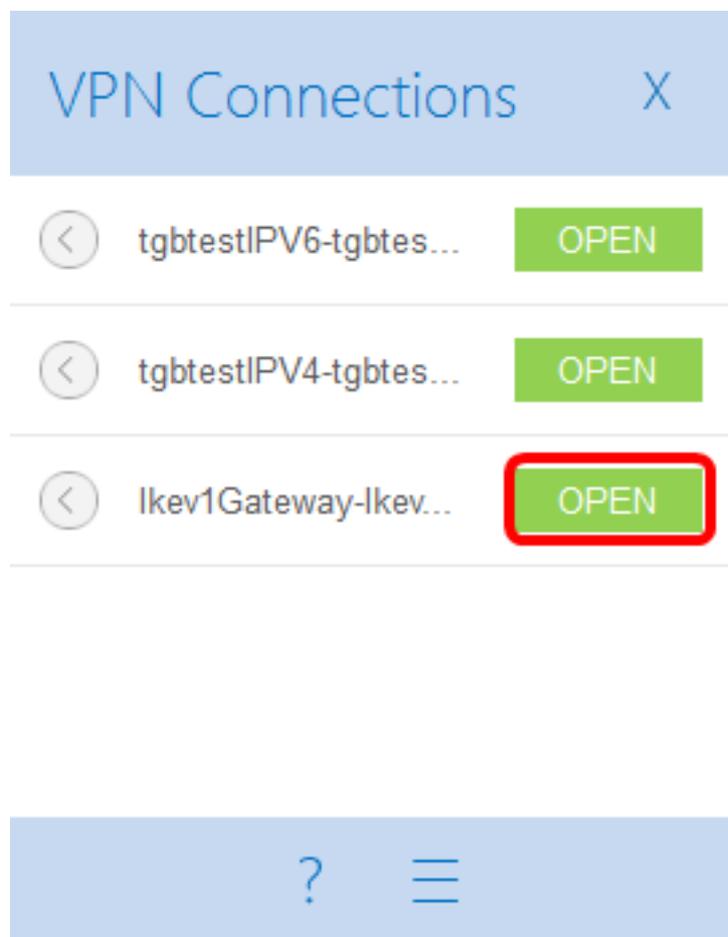
A questo punto, è necessario configurare correttamente il client VPN GreenBow per la connessione al router serie RV34x tramite VPN.

Avvia connessione VPN

Passaggio 1. Fare clic con il pulsante destro del mouse su TheGreenBow VPN Client e scegliere **Esegui come amministratore**.



Passaggio 2. Scegliere la connessione VPN da utilizzare e quindi fare clic su **APRI**. La connessione VPN dovrebbe avviarsi automaticamente.

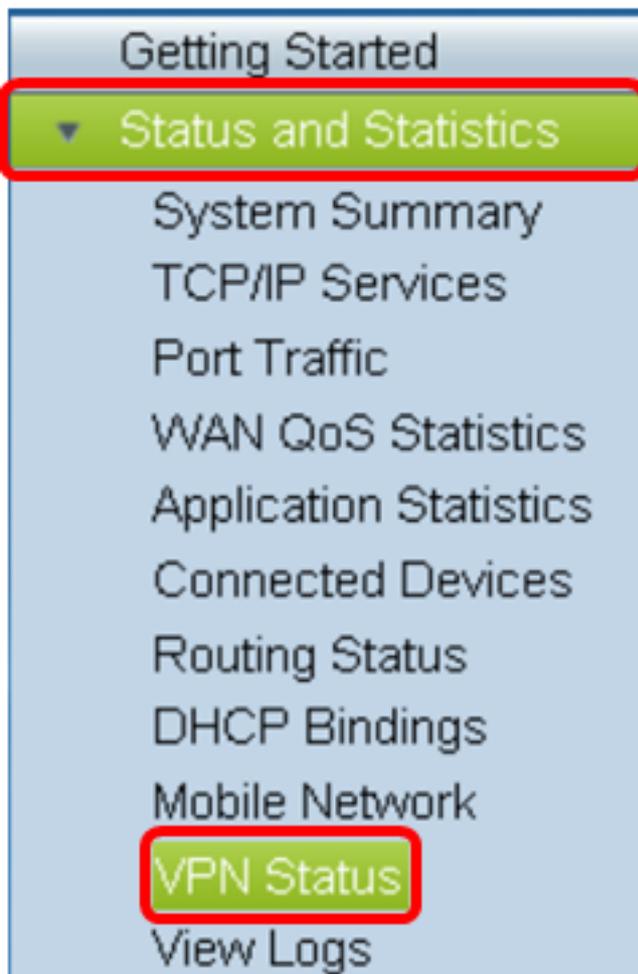


Nota: Nell'esempio è stato scelto il gateway lkev1 configurato.

Verifica dello stato della VPN

Passaggio 1. Accedere all'utility basata sul Web del gateway VPN.

Passaggio 2. Scegliere **Stato e Statistiche > Stato VPN**.



Passaggio 3. In Stato tunnel da client a sito controllare la colonna Connessioni della tabella di connessione.

Nota: In questo esempio è stata stabilita una connessione VPN.

Connections
1

A questo punto, è necessario verificare lo stato della connessione VPN sul router serie RV34x. Il client VPN GreenBow è ora configurato per connettersi al router tramite VPN.