

使用GreenBow VPN客戶端連線RV34x系列路由器

特別宣告：許可結構 — 韌體版本1.0.3.15及更高版本。接下來，AnyConnect將只對客戶端許可證收費。

有關RV340系列路由器上的AnyConnect許可的其他資訊，請檢視[RV340系列路由器的AnyConnect許可](#)一文。

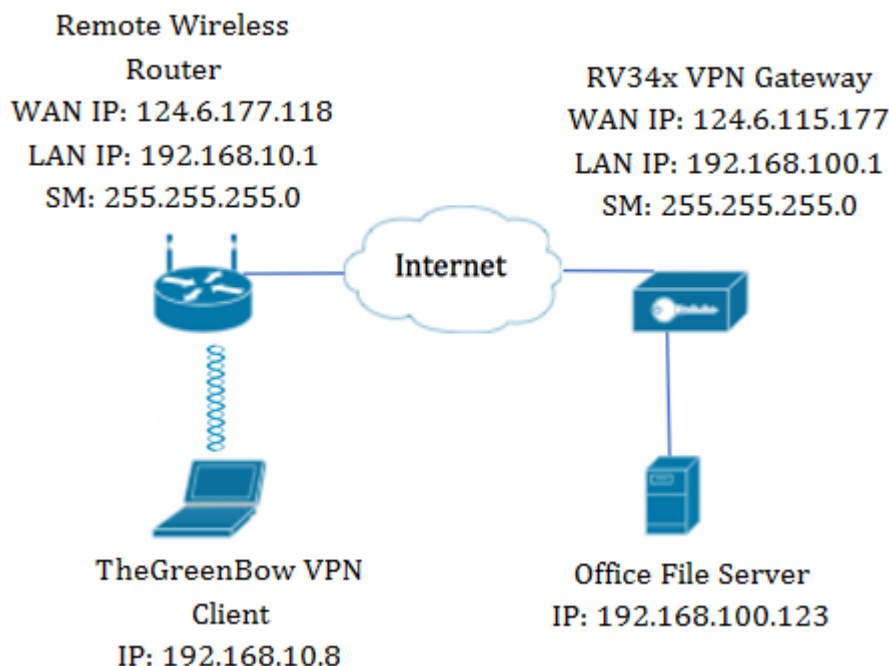
簡介

虛擬專用網路(VPN)連線允許使用者通過公共或共用網路（例如Internet）來訪問、傳送和從專用網路接收資料，但仍確保與底層網路基礎設施的安全連線，以保護專用網路及其資源。

VPN隧道建立私有網路，該私有網路可以使用加密和身份驗證安全地傳送資料。企業辦公室大多使用VPN連線，因為即使員工不在辦公室，也允許他們訪問其專用網路既有用又必要。

VPN允許遠端主機像位於同一本地網路一樣工作。該路由器最多支援50條隧道。在路由器配置用於Internet連線後，可以在路由器和終端之間建立VPN連線。VPN客戶端完全依賴於VPN路由器的設定才能建立連線。

GreenBow VPN客戶端是第三方VPN客戶端應用，使主機裝置能夠通過RV34x系列路由器為站點到站點IPSec隧道配置安全連線。



在圖中，電腦將連線到其網路之外的辦公室的檔案伺服器以訪問其資源。為此，電腦中的GreenBow VPN客戶端將配置為從RV34x VPN網關提取設定。

使用VPN連線的優點

1. 使用VPN連線有助於保護機密的網路資料和資源。
2. 它為遠端工作人員或公司員工提供了便利和可訪問性，因為他們可以輕鬆訪問總部，而無需親自到場，而且仍然維護專用網路及其資源的安全。
3. 與其他遠端通訊方法相比，使用VPN連線的通訊可提供更高級別的安全性。當今的技術水準已經使這一點成為可能，從而保護私有網路免受未經授權的訪問。
4. 使用者的實際地理位置受到保護，不會暴露於公共網路或共用網路（如Internet）。
5. 由於VPN易於擴展，因此向網路中新增新使用者或使用者組非常容易。無需額外的元件或複雜的配置即可使網路擴展。

使用VPN連線的風險

1. 配置錯誤導致安全風險。由於VPN的設計和實施可能很複雜，因此必須將配置連線的任務委託給知識豐富且經驗豐富的專業人員，以確保專用網路的安全不會受到危害。
2. 可靠性。由於VPN連線需要網際網路連線，因此必須有一個經過驗證和測試的信譽的提供商，以提供卓越的網際網路服務，並保證最短（甚至無停機時間）。
3. 可擴充性。如果需要新增新的基礎架構或新的配置集，則可能會由於不相容性而出現技術問題，尤其是當涉及的產品或供應商與您正在使用的產品或供應商不同時。
4. 流動裝置的安全問題。在流動裝置上啟動VPN連線時，可能會出現安全問題，尤其是當流動裝置無線連線到本地網路時。
5. 連線速度慢。如果您使用的是提供免費VPN服務的VPN客戶端，則連線速度可能也會很慢，因為這些提供商不優先選擇連線速度。

使用GreenBow VPN客戶端的先決條件

以下專案必須首先在VPN路由器上配置，並通過按一下此處[建立連線](#)應用於TheGreenBow VPN客戶端。

1. [在VPN網關上建立客戶端到站點配置檔案](#)
2. [在VPN網關上建立使用者組](#)
3. [在VPN網關上建立使用者帳戶](#)
4. [在VPN網關上建立IPSec配置檔案](#)
5. [在VPN網關上配置I階段和II階段設定](#)

適用裝置

- RV34x系列

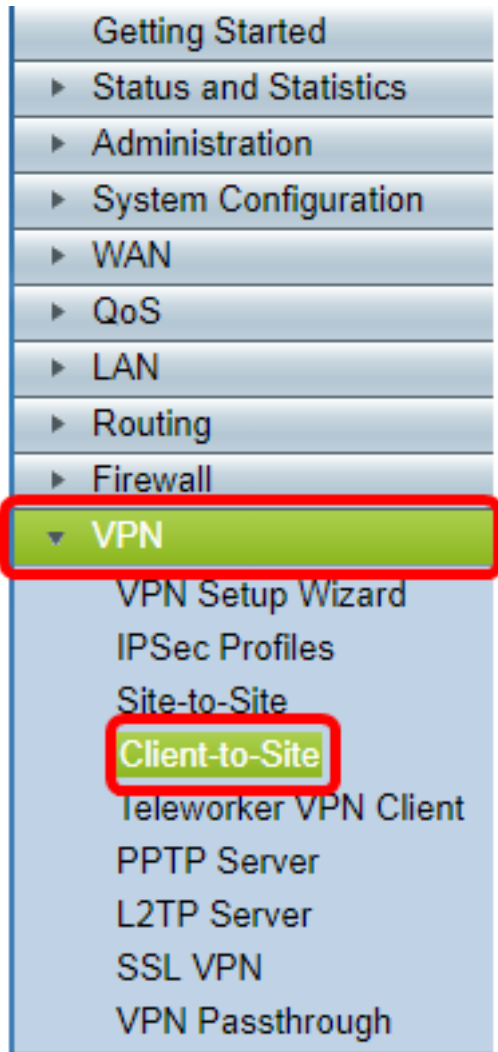
軟體版本

- 1.0.01.17

使用GreenBow VPN客戶端

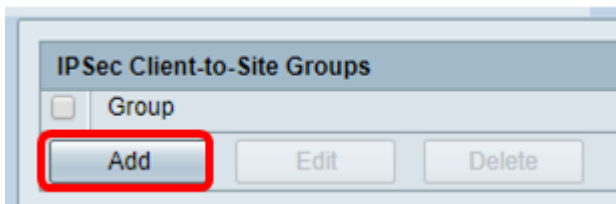
[在路由器上建立客戶端到站點配置檔案](#)

步驟1. 登入到RV34x路由器的基於Web的實用程式，然後選擇VPN > Client-to-Site。



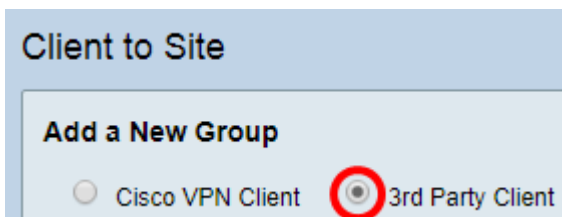
附註：本文中的影象來自RV340路由器。選項可能會有所不同，具體取決於裝置型號。

步驟2.按一下Add。



步驟3.按一下**第三方客戶端**。

附註：AnyConnect是Cisco VPN客戶端的示例，而GreenBow VPN客戶端是第三方VPN客戶端的示例。



附註：在此示例中，選擇**第三方客戶端**。

步驟4.在Basic Settings頁籤下，選中**Enable**覆取方塊以確保VPN配置檔案處於活動狀態。

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

步驟5.在 *Tunnel Name* 欄位中輸入VPN連線的名稱。

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

附註：在此範例中，輸入Client。

步驟6.從Interface下拉選單中選擇要使用的介面。選項包括WAN1、WAN2、USB1和USB2，它們將使用路由器上的相應介面進行VPN連線。

The screenshot shows the 'Interface' dropdown menu open, displaying options: WAN1 (highlighted in blue and circled in red), WAN2, USB1, and USB2. The 'Tunnel Name' is 'Client' and the 'Enable' checkbox is checked. Below the dropdown, there is a 'Preshared Key' section with a radio button selected and an empty text box, and a 'Preshared Key Strength Meter' bar.

附註：這些選項取決於您使用的路由器型號。在本示例中，選擇了WAN1。

步驟7.選擇IKE身份驗證方法。選項包括：

- 預共用金鑰(Preshared Key) — 此選項允許我們為VPN連線使用共用密碼。
- Certificate — 此選項使用的數位證書中包含資訊，例如證書的名稱或IP地址、序列號、到期日以及證書持有者的公鑰的副本。

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Certificate:

附註：在此示例中，選擇預共用金鑰。

步驟8.在預共用金鑰欄位中輸入連線密碼。

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

步驟9. (可選) 取消選中Minimum Preshared Key Complexity **Enable** 覈取方塊以可以使用簡單密碼。

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

附註：在此示例中，保留啟用最小預共用金鑰複雜性。

步驟10. (可選) 選中Show plain text when edit **Enable** 覈取方塊以純文字檔案顯示密碼。

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

附註：在此示例中，禁用編輯時顯示純文字檔案。

步驟11.從Local Identifier下拉選單中選擇本地識別符號。選項包括：

- 本地WAN IP — 此選項使用VPN網關的廣域網(WAN)介面的IP地址。
- IP地址 — 此選項允許您手動輸入VPN連線的IP地址。
- FQDN — 此選項也稱為完全限定域名(FQDN)。它允許您對Internet上的特定電腦使用完整的域名。
- 使用者FQDN — 此選項允許您對Internet上的特定使用者使用完整的域名。

Local Identifier: Local WAN IP 124.6.115.177

Remote Identifier: IP Address 124.6.177.118

FQDN

User FQDN

附註：在本示例中，選擇本地WAN IP。使用此選項，將自動檢測本地WAN IP。

步驟12。(可選)選擇遠端主機的識別符號。選項包括：

- IP地址 — 此選項使用VPN客戶端的WAN IP地址。
- FQDN — 此選項允許您對Internet上的特定電腦使用完整的域名。
- 使用者FQDN — 此選項允許您對Internet上的特定使用者使用完整的域名。

Local Identifier: Local WAN IP 124.6.115.177

Remote Identifier: IP Address 124.6.177.118

FQDN

User FQDN

附註：在本例中，選擇了IP地址。

步驟13.在遠端識別符號欄位中輸入遠端識別符號。

Local Identifier: Local WAN IP 124.6.115.177

Remote Identifier: IP Address 124.6.177.118

附註：在本示例中，輸入了124.6.115.177。

步驟14。(可選)勾選**Extended Authentication**覆取方塊以啟用該功能。啟用後，這將提供額外的身份驗證級別，要求遠端使用者在獲得對VPN的訪問許可權之前輸入其憑據。

Extended Authentication:

Group Name

Add Delete

附註：在本示例中，擴展身份驗證未選中。

步驟15.在「組名」下，按一下**Add**。

Extended Authentication:

Group Name

Add Delete

步驟16.從Group Name下拉選單中選擇將使用擴展身份驗證的組。

Group Name

admin

admin

guest

IPSecVPN

VPN

附註：在此示例中，選擇VPN。

步驟17.在Pool Range for Client LAN下，在Start IP欄位中輸入可分配給VPN客戶端的第一個IP地址。

Pool Range for Client LAN:

Start IP: 10.10.100.100

End IP: 10.10.100.245

附註：在此示例中，輸入了10.10.100.100。

步驟18.在End IP欄位中輸入可分配給VPN客戶端的最後一個IP地址。

Pool Range for Client LAN:

Start IP: 10.10.100.100

End IP: 10.10.100.245

附註：在此示例中，輸入了10.10.100.245。

步驟19.按一下Apply。

Pool Range for Client LAN:

Start IP: 10.10.100.100

End IP: 10.10.100.245

Apply Cancel

步驟20.按一下「Save」。

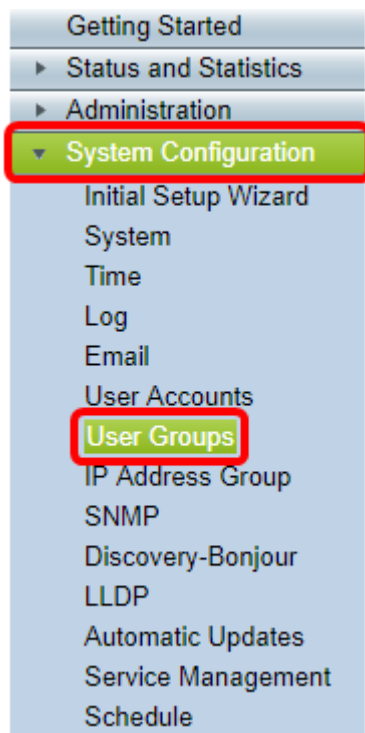
Save cisco (admin) Log Out About Help

現在，您應該在路由器上為TheGreenBow VPN客戶端配置客戶端到站點配置檔案。

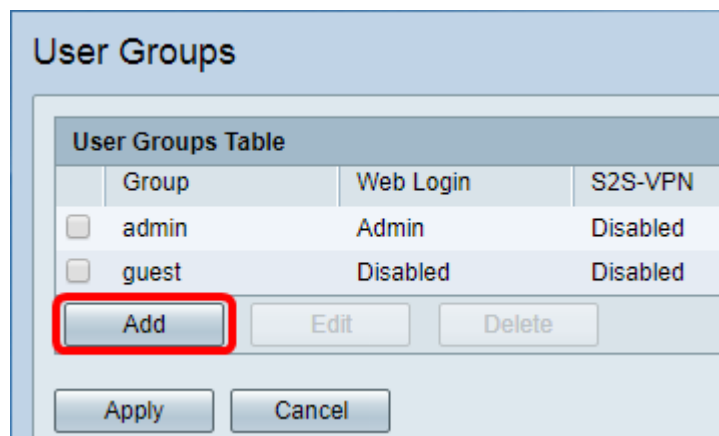
建立使用者組

步驟1.登入到路由器的基於Web的實用程式，然後選擇**System Configuration > User Groups**。

附註：本文中的影象來自RV340路由器。選項可能會因裝置型號而異。



步驟2.按一下**Add**以新增使用者群組。



步驟3.在「概覽」區域的「組名稱」欄位中輸入組名稱。

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

附註：本示例使用VPN。

步驟4.在Local Membership List下，選中需要位於同一組中的使用者名稱的覈取方塊。

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

附註：在本例中，選擇了CiscoTest和vpnuser。

步驟5.在「服務」下，選擇要授予組中的使用者的許可權。選項包括：

- 已禁用 — 此選項表示不允許組成員通過瀏覽器訪問基於Web的實用程式。
- 只讀 — 此選項表示組的成員只有在登入後才能讀取系統的狀態。它們無法編輯任何設定。
- 管理員 — 此選項為組的成員提供讀寫許可權，並能夠配置系統狀態。

Services

Web Login Disabled Read Only Administrator

附註：在此範例中，選擇了「唯讀」。

步驟6.在EzVPN/第三方配置檔案成員使用表中，按一下Add。

EzVPN/3rd Party

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

步驟7.從「選擇配置檔案」下拉選單中選擇配置檔案。選項可能會有所不同，具體取決於VPN網關上配置的配置檔案。

Add Feature List

Select a Profile:

附註：在本例中，選擇了Clients。

步驟8.按一下Add。

Add Feature List

Select a Profile:

步驟9.按一下Apply。

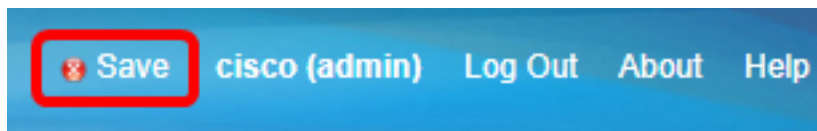
SSL VPN

PPTP VPN Permit

L2TP Permit

802.1x Permit

步驟10.按一下「Save」。

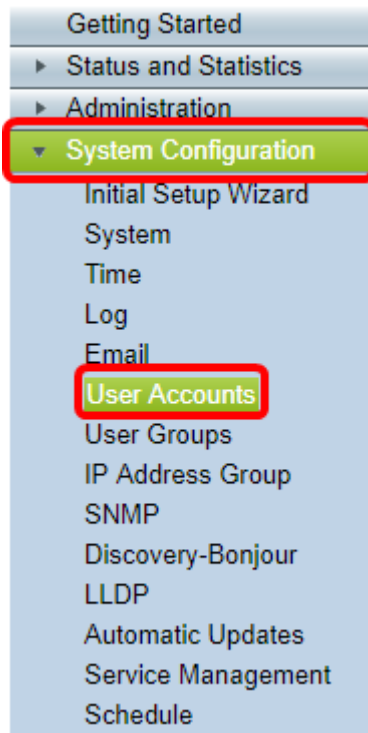


現在，您應該已經在RV34x系列路由器上成功建立了使用者組。

建立使用者帳戶

步驟1. 登入到路由器的基於Web的實用程式，然後選擇**System Configuration > User Accounts**。

附註：本文中的影象來自RV340路由器。選項可能會因裝置型號而異。



步驟2. 在Local User Membership List區域中，按一下**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

步驟3.在 *User Name* 欄位中輸入使用者的名稱。

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group ▼

附註：在此範例中，輸入CiscoTest。

步驟4.在 *New Password* 欄位中輸入使用者密碼。

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

步驟5.在 *New Password Confirm* 框中確認密碼。

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

步驟6.從「組」下拉選單中選擇一個組。這是將與使用者關聯的組。

Group

附註：在此示例中，選擇VPN。

步驟7.按一下Apply。

User Accounts

Add User Account

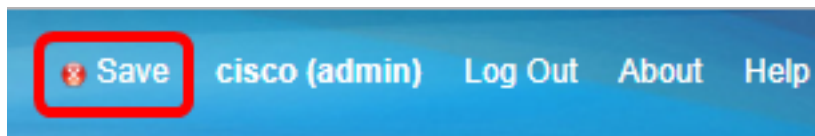
User Name

New Password

New Password Confirm

Group

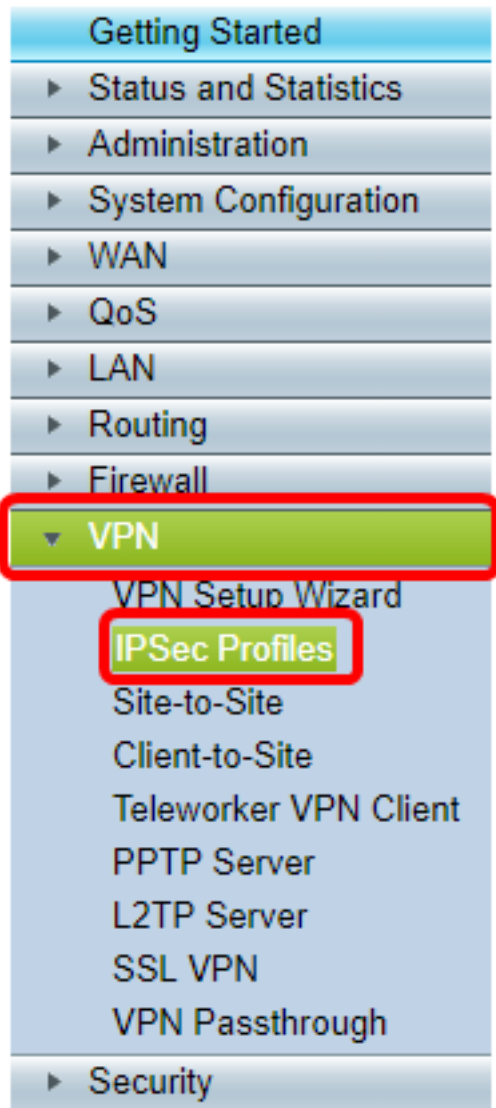
步驟8.按一下「Save」。



您現在應該已經在RV34x系列路由器上建立使用者帳戶。

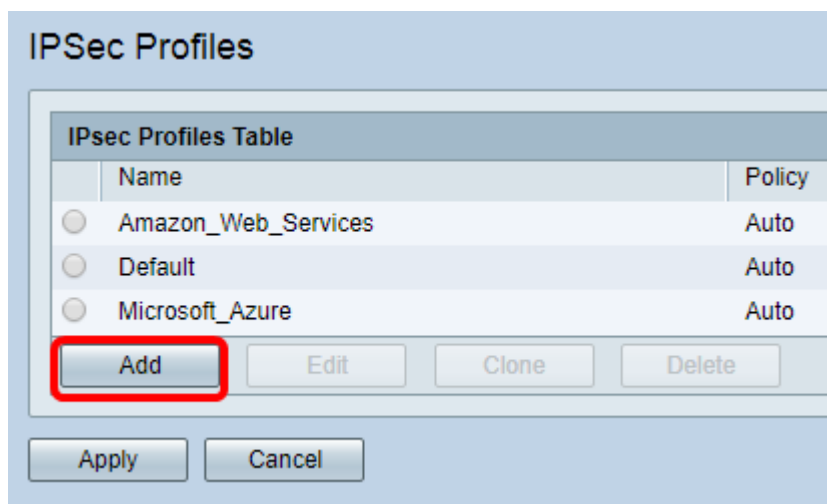
[配置IPSec配置檔案](#)

步驟1.登入到RV34x路由器的基於Web的實用程式，然後選擇VPN > IPSec Profiles。



附註：本文中的影象來自RV340路由器。選項可能會因裝置型號而異。

步驟2. IPSec簡檔表顯示現有簡檔。按一下**Add**建立新配置檔案。



附註：Amazon_Web_Services、Default和Microsoft_Azure是預設配置檔案。

步驟3.在*Profile Name* 欄位中建立檔案的名稱。配置檔名稱只能包含字母數字字元以及特殊字元的下劃線()。

IPSec Profiles

Add a New IP Sec Profile

Profile Name:

Keying Mode Auto Manual

附註：在本示例中，輸入客戶端。

步驟4.按一下單選按鈕以確定配置檔案將用於進行身份驗證的金鑰交換方法。選項包括：

- 自動(Auto) — 自動設定策略引數。此選項使用Internet金鑰交換(IKE)策略進行資料完整性和加密金鑰交換。如果選擇此選項，則啟用Auto Policy Parameters區域下的配置設定。如果選擇此選項，請跳至[配置自動設定](#)。
- 手動(Manual) — 此選項允許您手動配置VPN隧道的資料加密和完整性的金鑰。如果選擇此選項，則啟用Manual Policy Parameters區域下的配置設定。如果選擇此選項，請跳至[配置手動設定](#)。

IPSec Profiles

Add a New IP Sec Profile

Profile Name:

Keying Mode Auto Manual

附註：在本示例中，選擇了Auto。

[配置I階段和II階段設定](#)

步驟1。在Phase 1 Options區域中，從DH Group下拉選單中選擇要與Phase 1中的金鑰一起使用的適當Diffie-Hellman(DH)組。Diffie-Hellman是一種加密金鑰交換協定，用於交換預共用金鑰集。演算法的強度由位決定。選項包括：

- Group2-1024位 — 此選項計算金鑰的速度較慢，但比組1更安全。
- Group5-1536位 — 此選項計算金鑰最慢，但最安全。

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: Group2 - 1024 bit
Group5 - 1536 bit

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

附註：在本例中，選擇了Group5-1536位。

步驟2.從Encryption下拉選單中，選擇一種加密方法以加密和解密封裝安全負載(ESP)和網際網路安全關聯和金鑰管理協定(ISAKMP)。 選項包括：

- 3DES — 三重資料加密標準。
- AES-128 — 高級加密標準使用128位金鑰。
- AES-192 — 高級加密標準使用192位金鑰。
- AES-256 — 高級加密標準使用256位金鑰。

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼
3DES
AES-128
AES-192
AES-256

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

附註：AES是使用DES和3DES進行加密的標準方法，因為它具有更高的效能和安全性。延長AES金鑰將增加安全性，但效能會下降。在此範例中，選擇AES-128。

步驟3.從Authentication下拉選單中，選擇確定ESP和ISAKMP身份驗證方式的身份驗證方法。 選項包括：

- MD5 — 消息摘要演算法具有128位雜湊值。
- SHA-1 — 安全雜湊演算法具有160位雜湊值。
- SHA2-256 — 具有256位雜湊值的安全雜湊演算法。

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼
MD5
SHA1
SHA2-256

SA Lifetime: **SHA1**

Perfect Forward Security: Enable

附註：MD5和SHA都是加密雜湊函式。他們獲取一段資料，將其壓縮，然後建立通常無法再現的唯一的十六進位制輸出。在此範例中，選擇SHA1。

步驟4.在SA Lifetime欄位中，輸入介於120和86400之間的值。這是Internet金鑰交換(IKE)安全關聯(SA)在該階段保持活動狀態的時間長度。預設值為 28800。

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: **86400**

Perfect Forward Security: Enable

附註：在此範例中，86400入錯誤。

步驟5. (可選) 選中**Enable** Perfect Forward Security覈取方塊以生成IPSec流量加密和身份驗證的新金鑰。

Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Security: Enable

附註：在此範例中，已啟用「完全向前保密」。

步驟6.從Phase II Options區域的Protocol Selection下拉選單中，選擇要應用於協商第二階段的協定型別。選項包括：

- ESP — 此選項封裝要保護的資料。如果選擇此選項，請繼續[步驟7](#)以選擇加密方法。
- AH — 此選項也稱為身份驗證報頭(AH)。它是一種安全協定，提供資料身份驗證和可選的反重播服務。AH嵌入到要保護的IP資料包中。如果選擇此選項，請跳至[步驟8](#)。

Phase II Options

Protocol Selection: ESP

Encryption: ESP (highlighted)

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Buttons: Apply, Cancel

附註：在本示例中，選擇了ESP。

[步驟7](#).如果在步驟6中選擇了ESP，請選擇確定ESP和ISAKMP身份驗證方式的身份驗證方法。選項包括：

- 3DES — 三重資料加密標準
- AES-128 — 高級加密標準使用128位金鑰。
- AES-192 — 高級加密標準使用192位金鑰。
- AES-256 — 高級加密標準使用256位金鑰。

Phase II Options

Protocol Selection: ESP

Encryption: AES-128 (highlighted)

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Buttons: Apply, Cancel

附註：在此範例中，選擇AES-128。

[步驟8](#).從Authentication下拉選單中，選擇一種將確定ESP和ISAKMP身份驗證方式的身份驗證方法。選項包括：

- MD5 — 消息摘要演算法具有128位雜湊值。
- SHA-1 — 安全雜湊演算法具有160位雜湊值。
- SHA2-256 — 具有256位雜湊值的安全雜湊演算法。

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

附註：在此範例中，選擇SHA1。

步驟9.在 *SA Lifetime* 欄位中，輸入介於120和28800之間的值。這是IKE SA在此階段保持活動狀態的時間長度。預設值為 3600。

步驟10.從DH組下拉選單中，選擇要與階段2中的金鑰一起使用的DH組。選項包括：

- Group2-1024位 — 此選項計算金鑰的速度較慢，但比Group1更安全。
- Group5-1536位 — 此選項計算金鑰最慢，但最安全。

Phase II Options

Protocol Selection: ESP

Encryption: AES-128

Authentication: SHA1

SA Lifetime: 3600

DH Group: Group5 - 1536 bit

Apply Cancel

附註：在此範例中輸入3600。

步驟11.按一下**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:

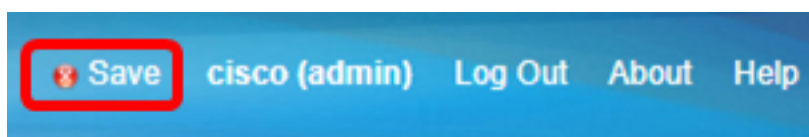
Encryption:

Authentication:

SA Lifetime:

DH Group:

步驟12.按一下**Save**以永久儲存組態。



現在，您應該已經在RV34x系列路由器上成功配置了Automatic IPSec Profile。

配置手動設定

步驟1.在*SPI-Incoming*欄位中，為VPN連線上的傳入流量的安全引數索引(SPI)標籤輸入從100到FFFFFFF的十六進位制值。SPI標籤用於區分一個會話的流量和其他會話的流量。

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

附註：在此示例中，輸入0xabcd。

步驟2.在 *SPI-Outgoing* 欄位中，為VPN連線上的傳出流量的SPI標籤輸入從100到FFFFFFF的十六進位制值。

The screenshot shows a configuration window titled "Manual Policy Parameters". It contains two input fields: "SPI-Incoming:" with the value "0xABCD" and "SPI-Outgoing:" with the value "0x1234". The "SPI-Outgoing:" field is highlighted with a red rectangular border.

附註：在此示例中，輸入0x1234。

步驟3.從下拉選單中選擇加密值。選項包括：

- 3DES — 三重資料加密標準
- AES-128 — 高級加密標準使用128位金鑰。
- AES-192 — 高級加密標準使用192位金鑰。

The screenshot shows a configuration window with fields for "SPI Incoming:", "SPI Outgoing:", and "Encryption:". A dropdown menu is open over the "Encryption:" field, showing options: "3DES", "AES-128", "AES-192", and "AES-256". The "AES-256" option is selected and highlighted with a blue background and a checkmark, and the entire dropdown area is enclosed in a red border.

附註：在此範例中，選擇AES-256。

步驟4.在 *Key-In* 欄位中輸入入站策略的金鑰。金鑰的長度取決於步驟3中選擇的演算法。

The screenshot shows a configuration window with two input fields: "Key-In:" containing the value "123456789123456789123" and "Key-Out:" containing the value "1a1a1a1a1a1a1a1a1212121". Both input fields are enclosed in red rectangular borders.

附註：在此示例中123456789123456789123輸入.....。

步驟5.在 *Key-Out* 欄位中輸入傳出策略的金鑰。金鑰的長度取決於步驟3中選擇的演算法。

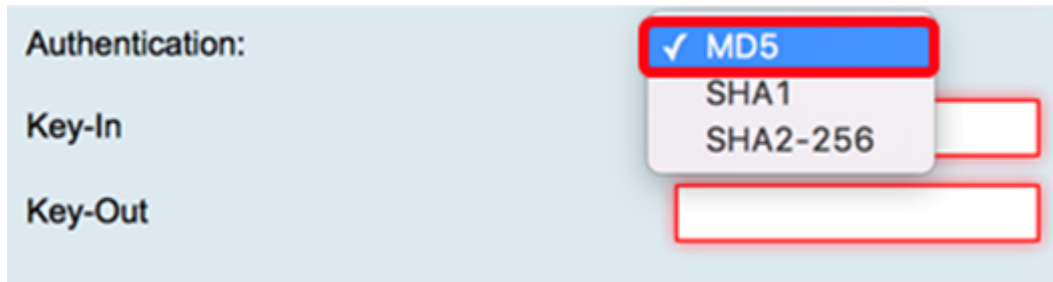
The screenshot shows a configuration window with two input fields: "Key-In:" containing the value "123456789123456789123" and "Key-Out:" containing the value "1a1a1a1a1a1a1a1a1212121". Both input fields are enclosed in red rectangular borders.

附註：在此範例中，輸入1a1a1a1a1a1a1a1a1212121...。

步驟6.從Authentication下拉選單中選擇身份驗證方法。選項包括：

- MD5 — 消息摘要演算法具有128位雜湊值。
- SHA-1 — 安全雜湊演算法具有160位雜湊值。

- SHA2-256 — 具有256位雜湊值的安全雜湊演算法。



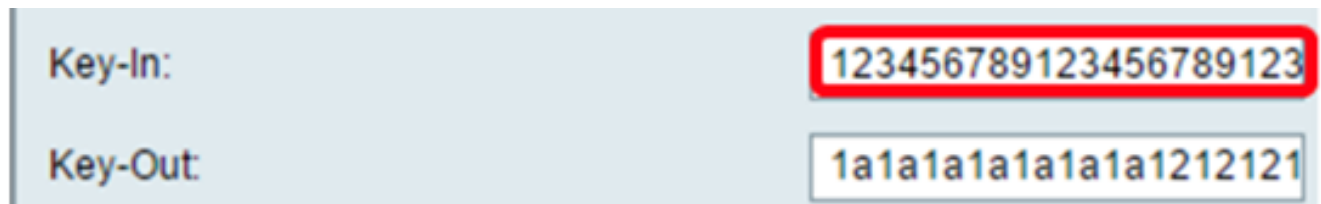
Authentication: MD5
 SHA1
 SHA2-256

Key-In

Key-Out

附註：在本例中，選擇了MD5。

步驟7.在 *Key-In* 欄位中輸入入站策略的金鑰。金鑰的長度取決於步驟6中選擇的演算法。

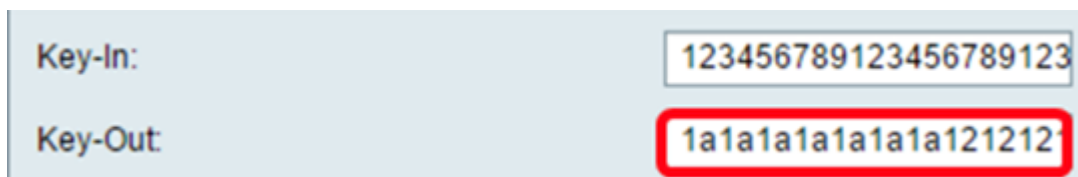


Key-In: 123456789123456789123

Key-Out: 1a1a1a1a1a1a1a1a1212121

附註：在此示例中123456789123456789123輸入.....。

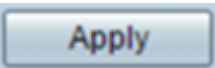
步驟8.在 *Key-Out* 欄位中輸入傳出策略的金鑰。金鑰的長度取決於步驟6中選擇的演算法。



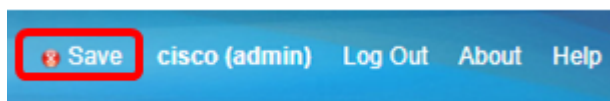
Key-In: 123456789123456789123

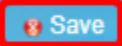
Key-Out: 1a1a1a1a1a1a1a1a1212121

附註：在此範例中，輸入1a1a1a1a1a1a1a1a1212121...。

步驟9.單  擊。

步驟10.按一下 **Save** 以永久儲存組態。



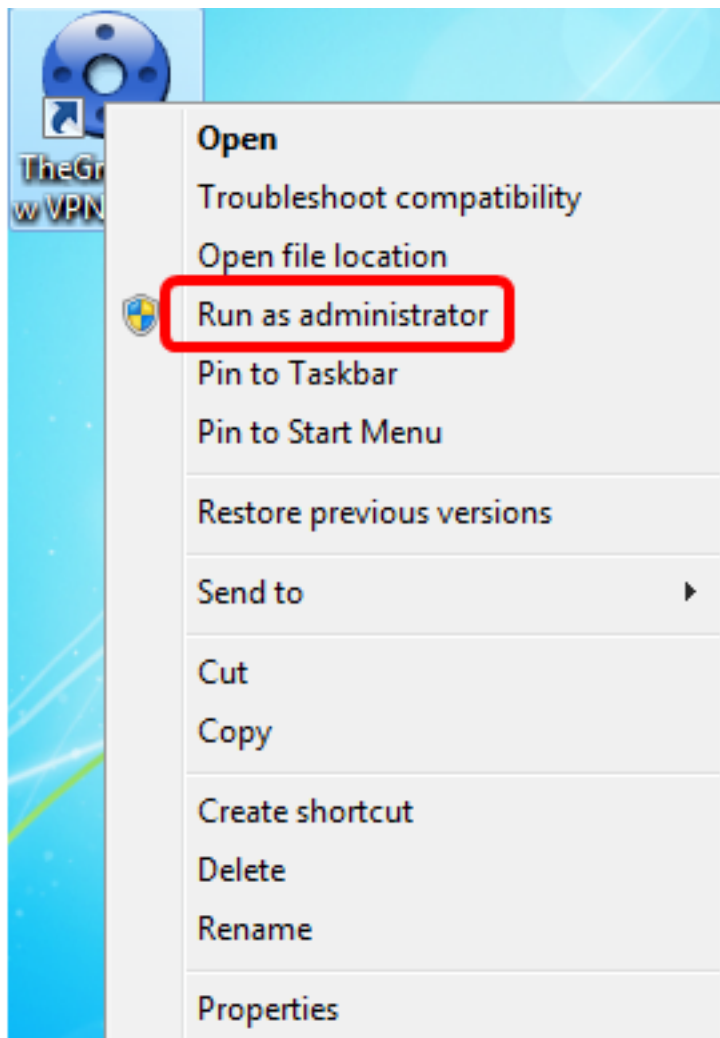
 Save cisco (admin) Log Out About Help

現在，您應該已經在RV34x系列路由器上成功配置手動IPSec配置檔案。

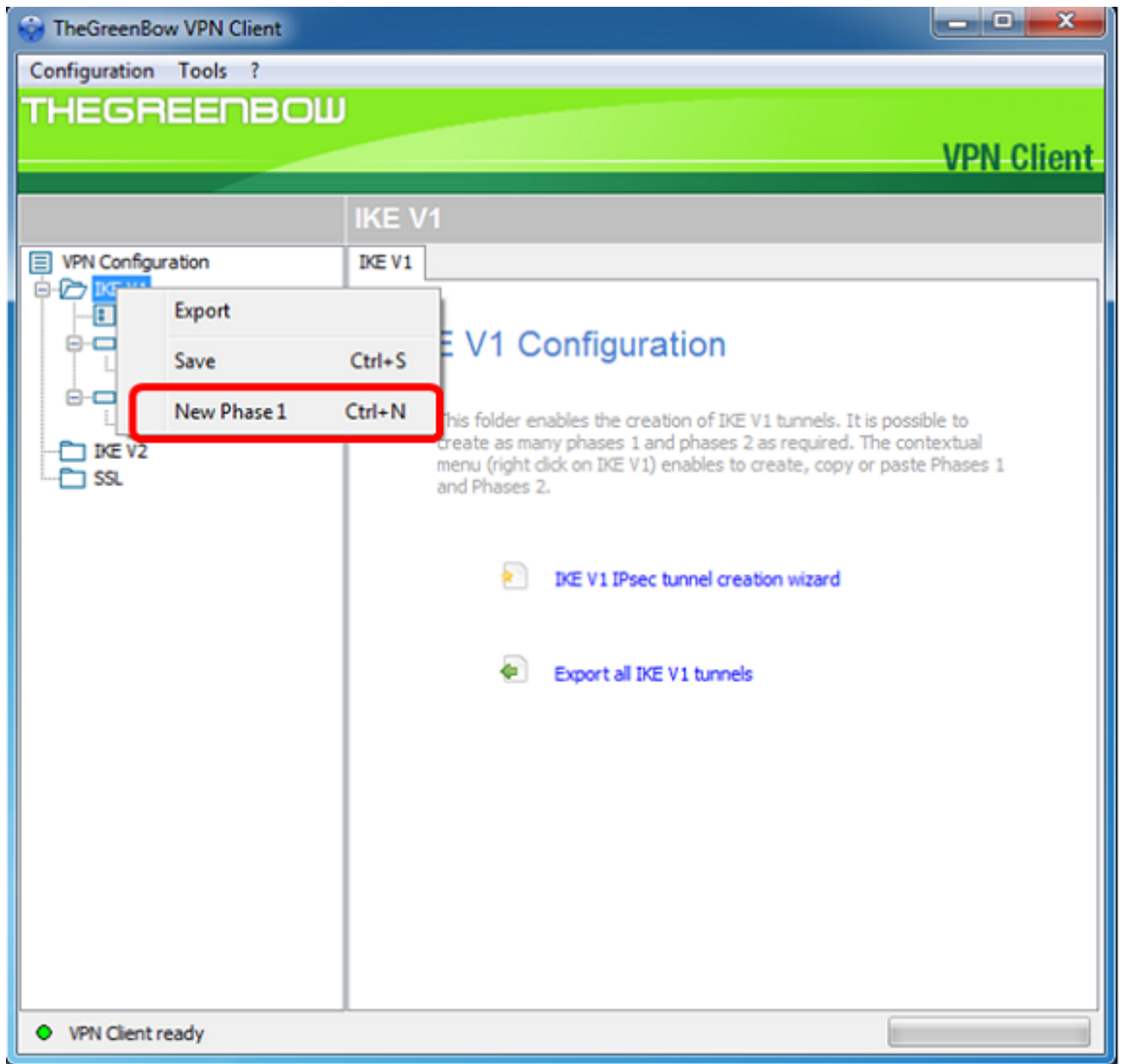
配置GreenBow VPN客戶端軟體

配置階段1設定

步驟1.按一下右鍵GreenBow VPN Client圖示並選擇Run as administrator。

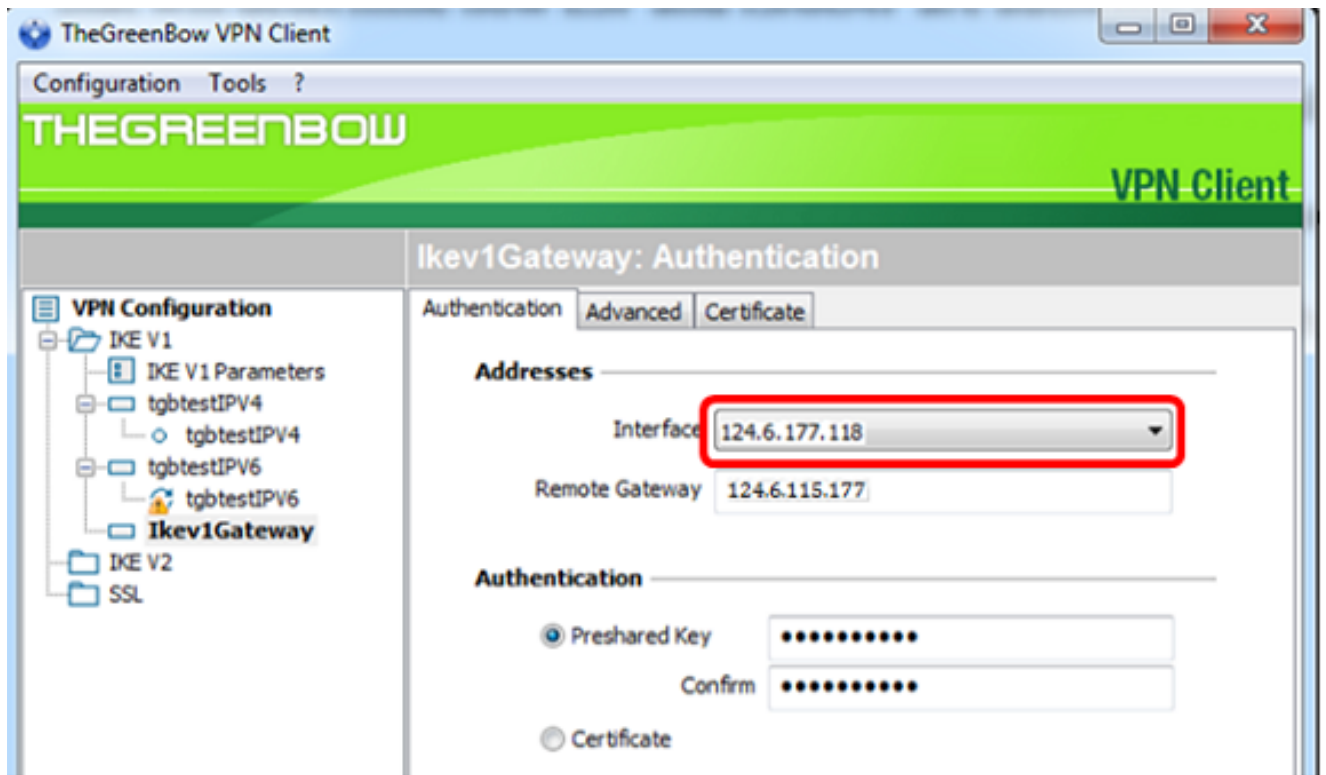


步驟2.在VPN配置下的左窗格中，按一下右鍵IKE V1，然後選擇New Phase 1。



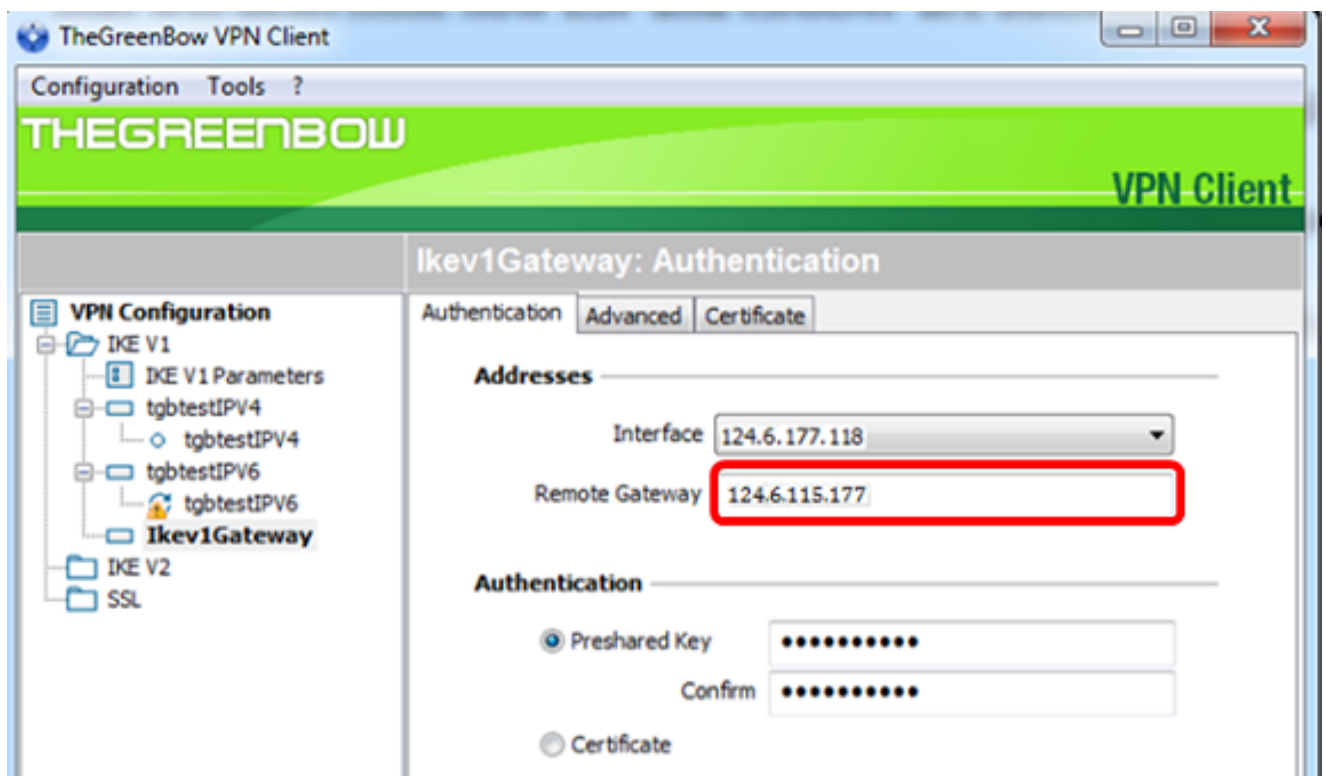
步驟3.在Addresses下的Authentication頁籤中，驗證Interface區域中的IP地址與安裝了GreenBow VPN客戶端的電腦的WAN IP地址相同。

附註：在本例中，IP地址為124.6.177.118。



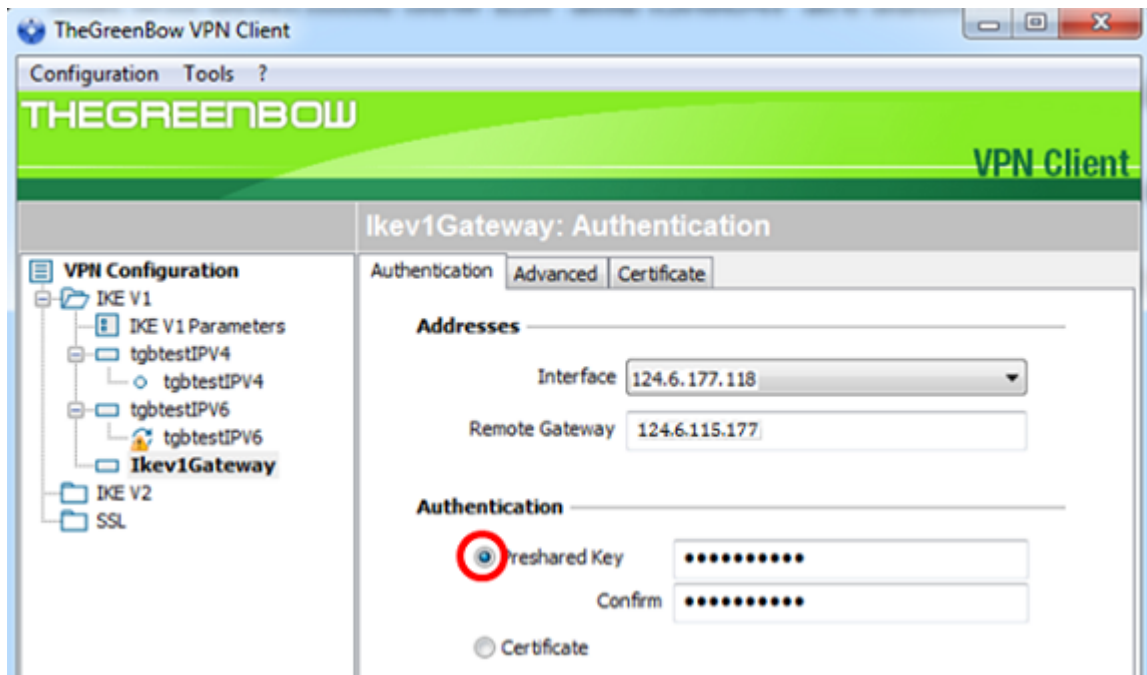
步驟4.在*Remote Gateway*欄位中輸入遠端網關的地址。

附註：在本示例中，遠端RV34x路由器的IP地址為124.6.115.177。



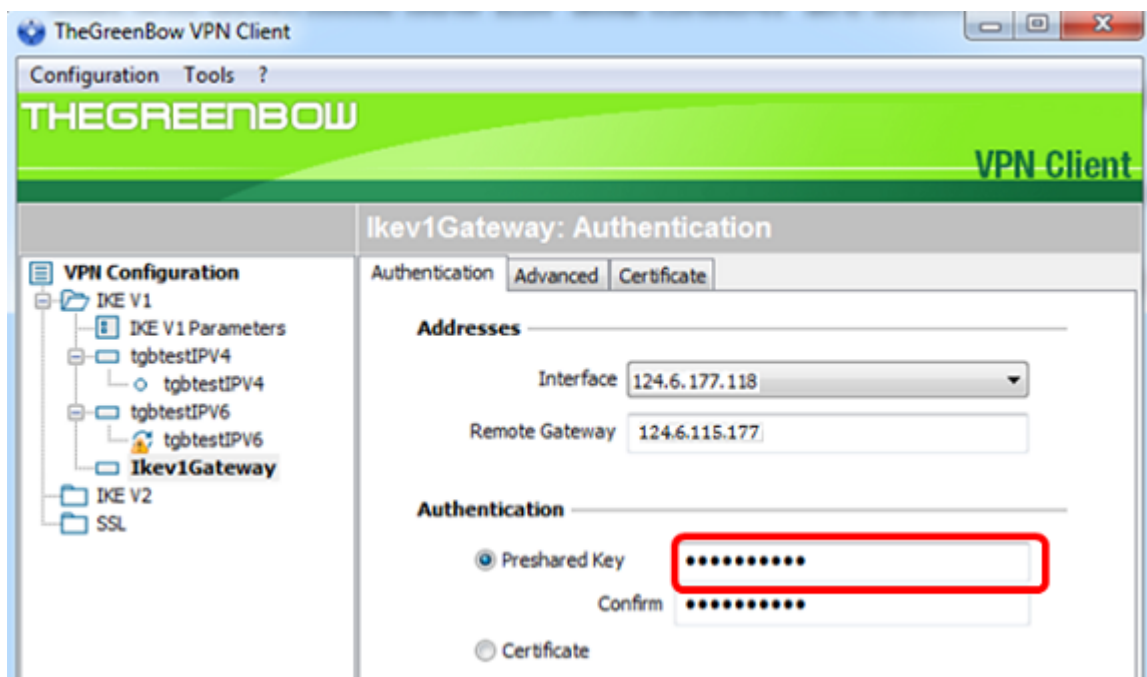
步驟5.在Authentication下，選擇身份驗證型別。選項包括：

- 預共用金鑰(Preshared Key) — 此選項允許使用者使用已在VPN網關上配置的密碼。使用者必須匹配密碼才能建立VPN隧道。
- 證書(Certificate) — 此選項將使用證書來完成VPN客戶端和VPN網關之間的握手。

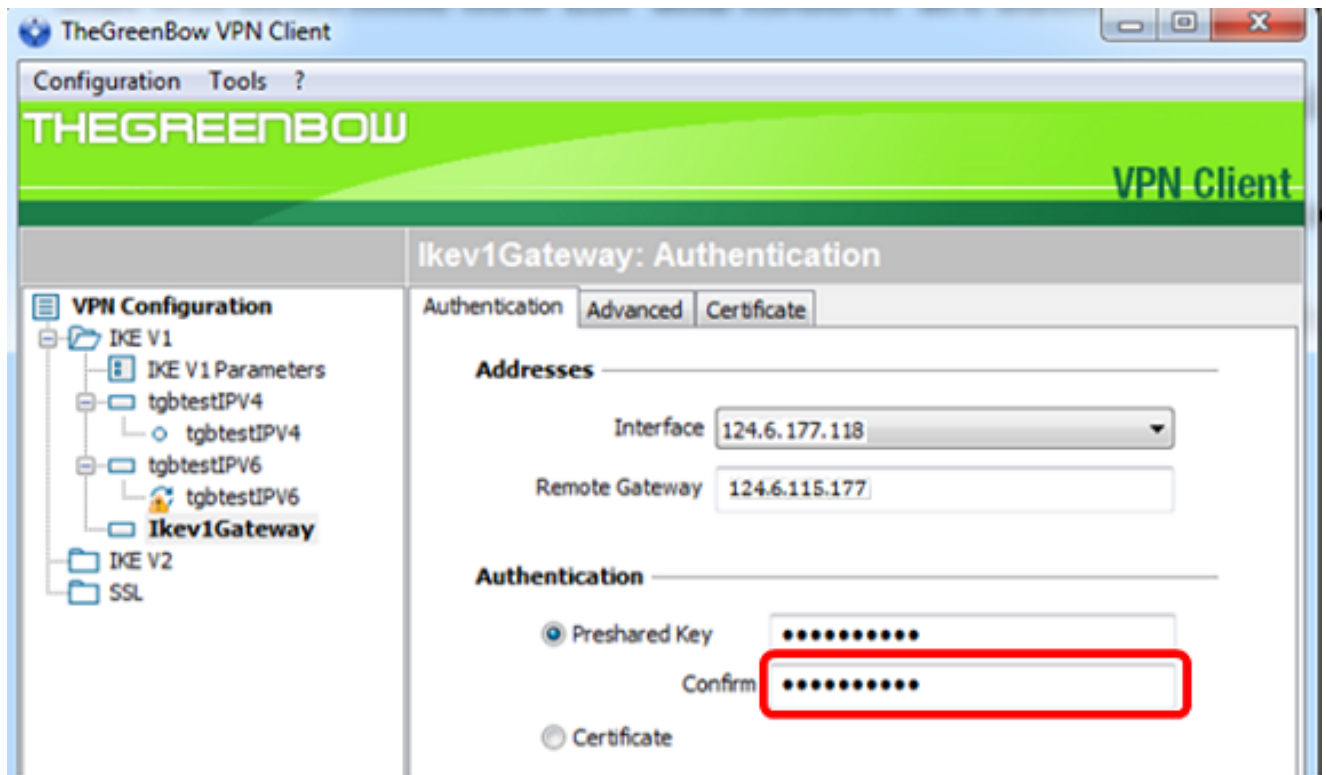


附註：在本示例中，選擇預共用金鑰以匹配RV34x VPN網關的配置。

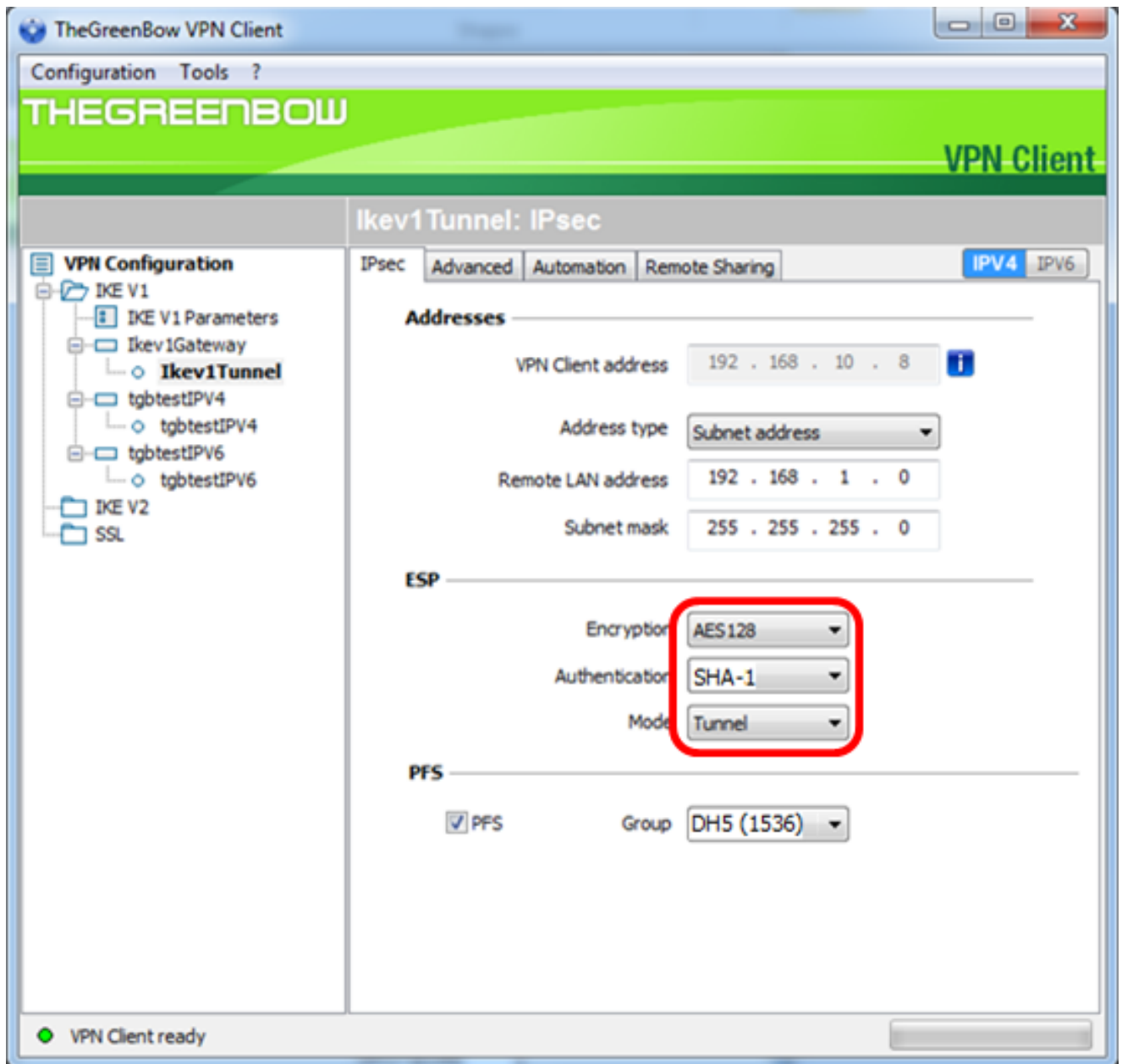
步驟6.輸入在路由器中配置的預共用金鑰。



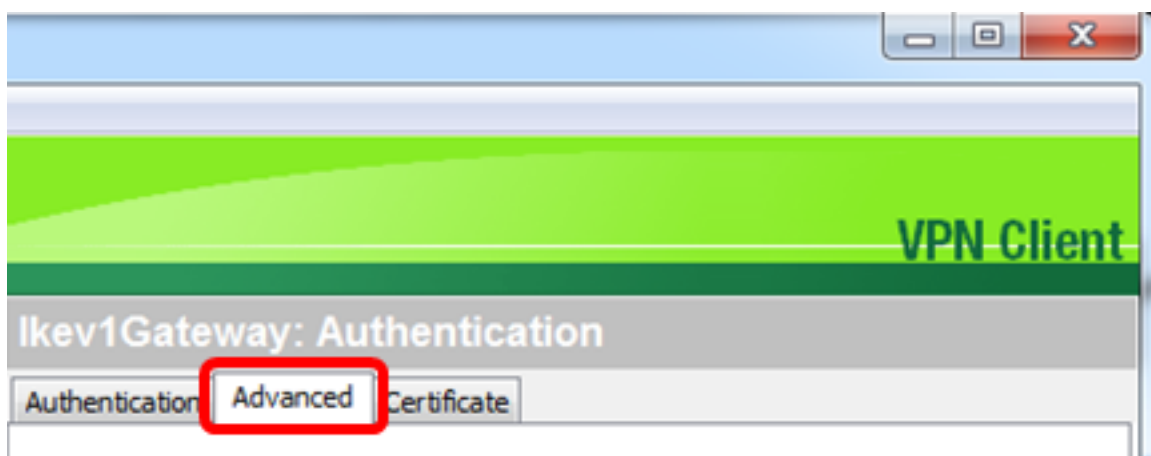
步驟7.在 *Confirm* 欄位中輸入相同的預共用金鑰。



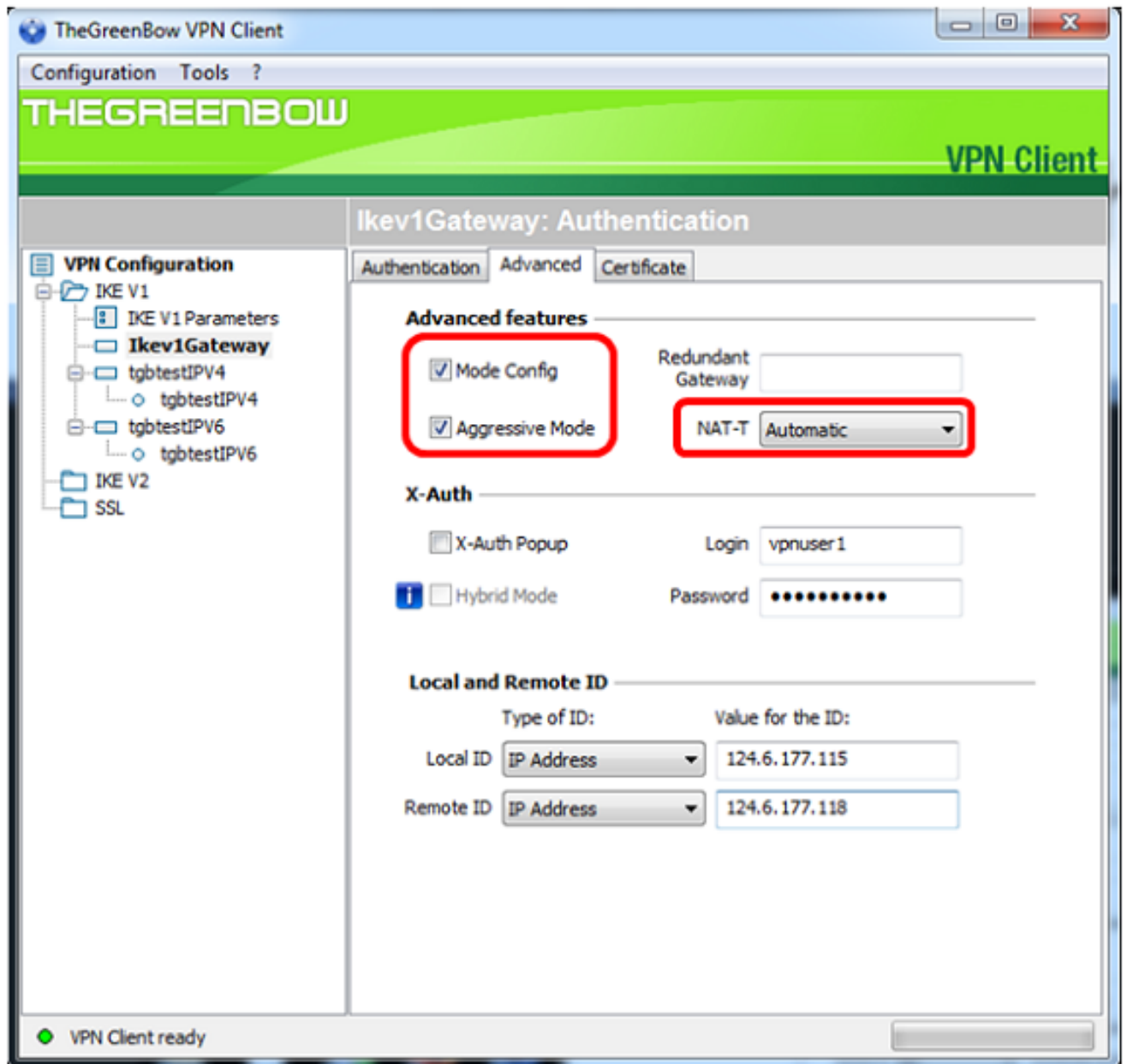
步驟8.在IKE下，設定加密、身份驗證和金鑰組設定以匹配路由器的配置。



步驟9.按一下Advanced索引標籤。

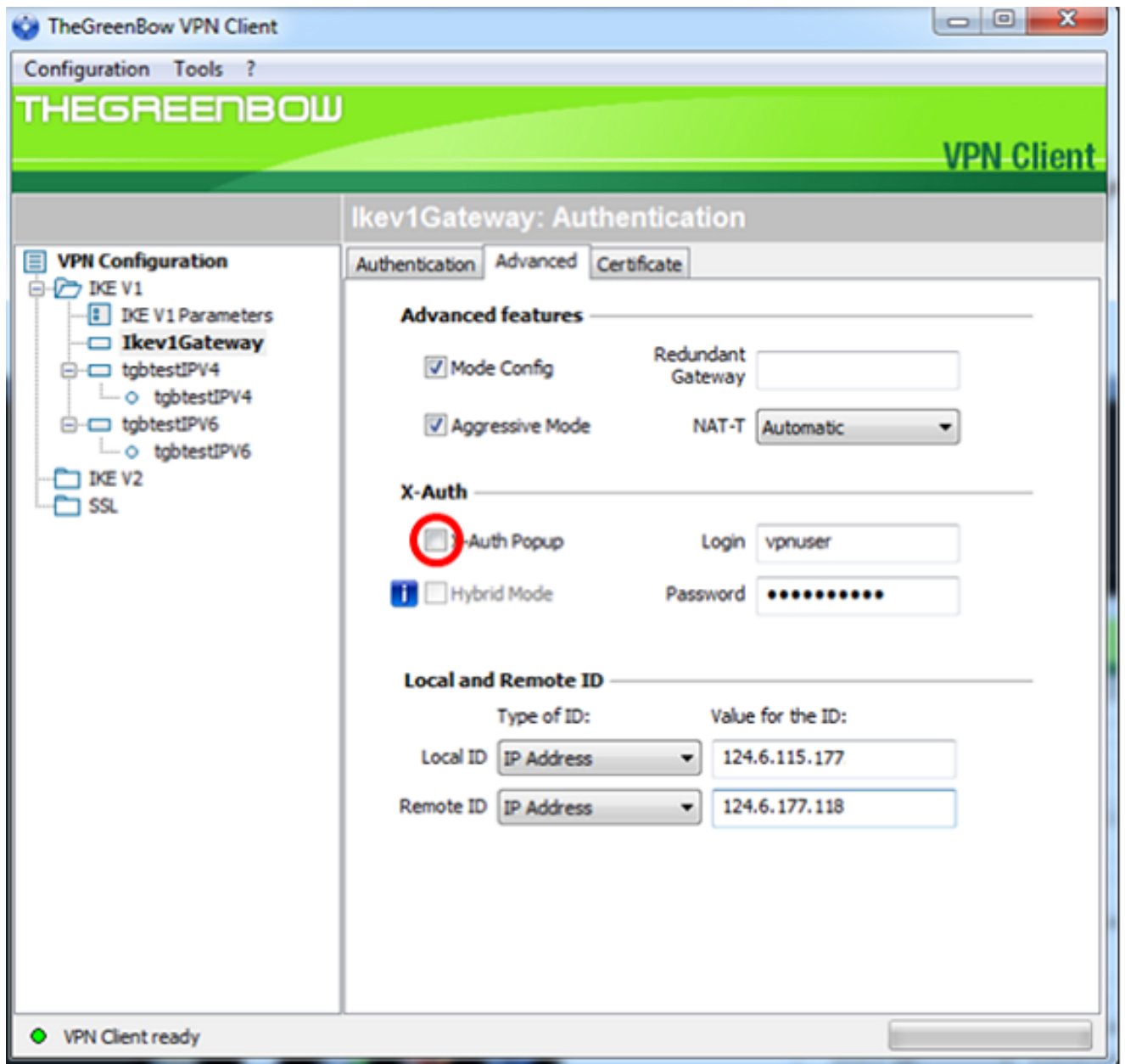


步驟10。(可選)在Advanced features下，選中Mode Config和Aggressive Mode覆取方塊，並將NAT-T設定設定為Automatic。



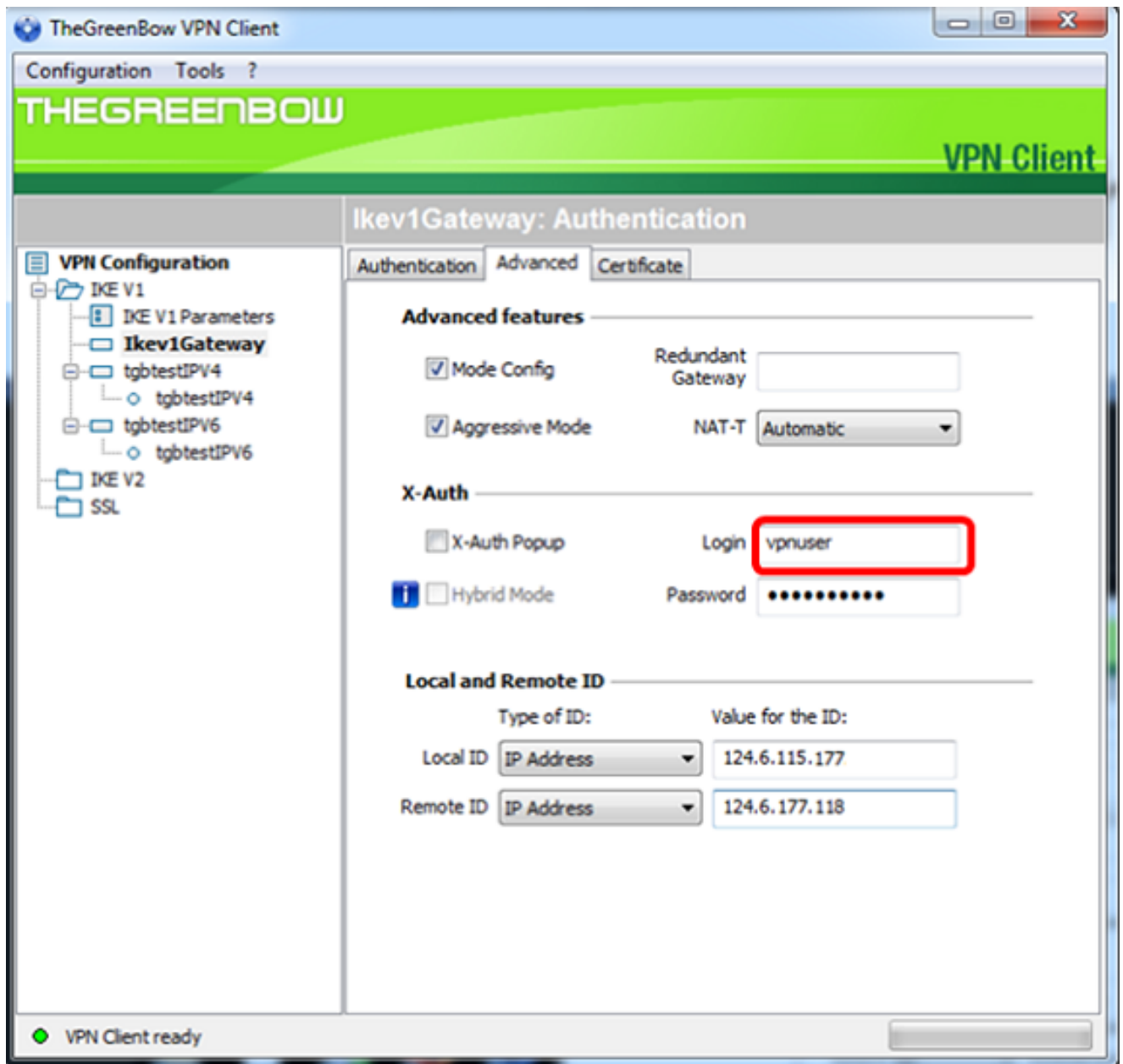
附註：啟用模式配置後，GreenBow VPN客戶端將從VPN網關提取設定以嘗試建立隧道，同時啟用主動模式和NAT-T使建立連線更快。

步驟11。（可選）在X-Auth下，勾選X-Auth Popup覈取方塊以在啟動連線時自動拉出登入視窗。使用者可在登入視窗輸入其憑證以完成隧道。

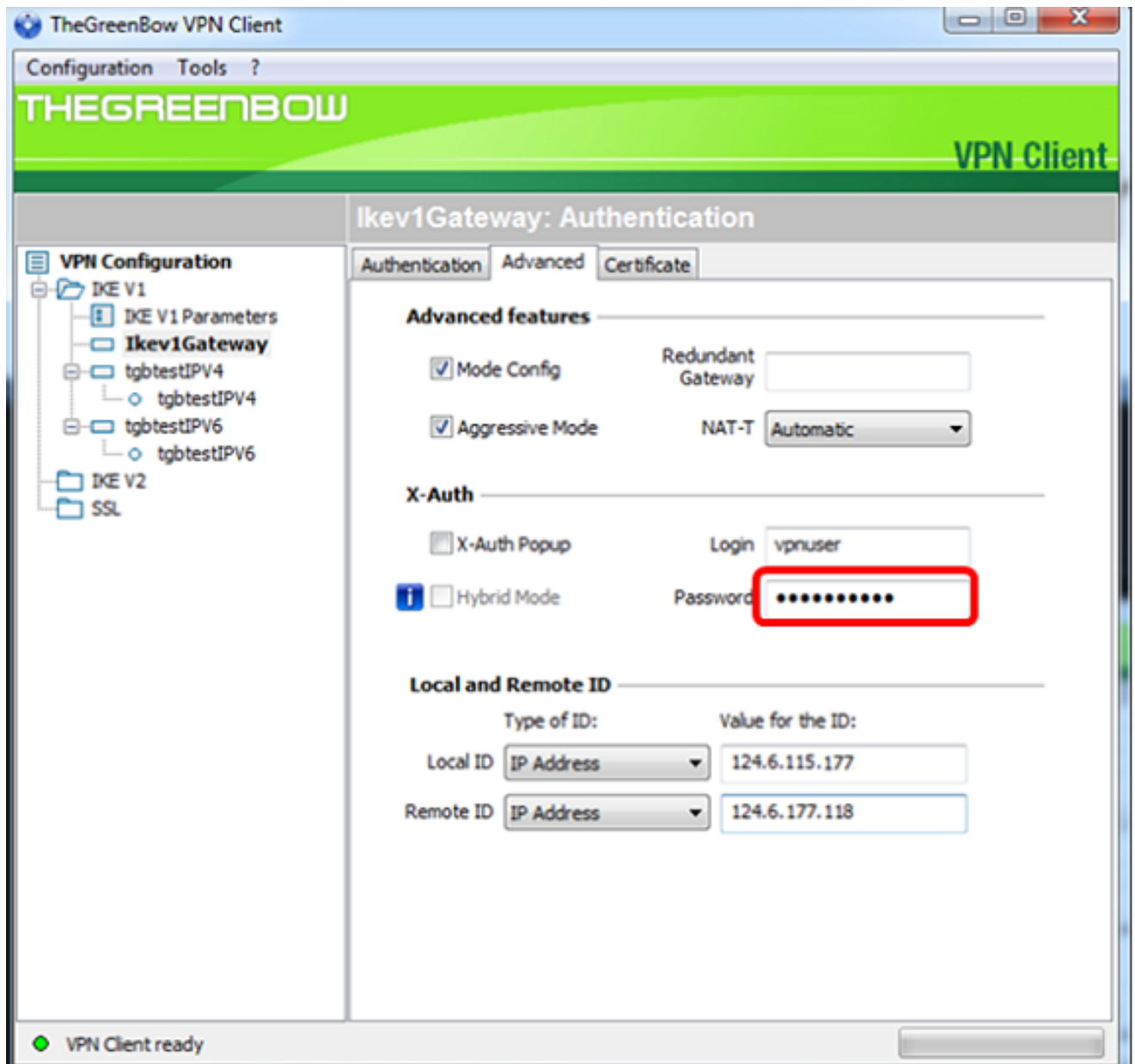


附註：在本示例中，未選中X-Auth Popup。

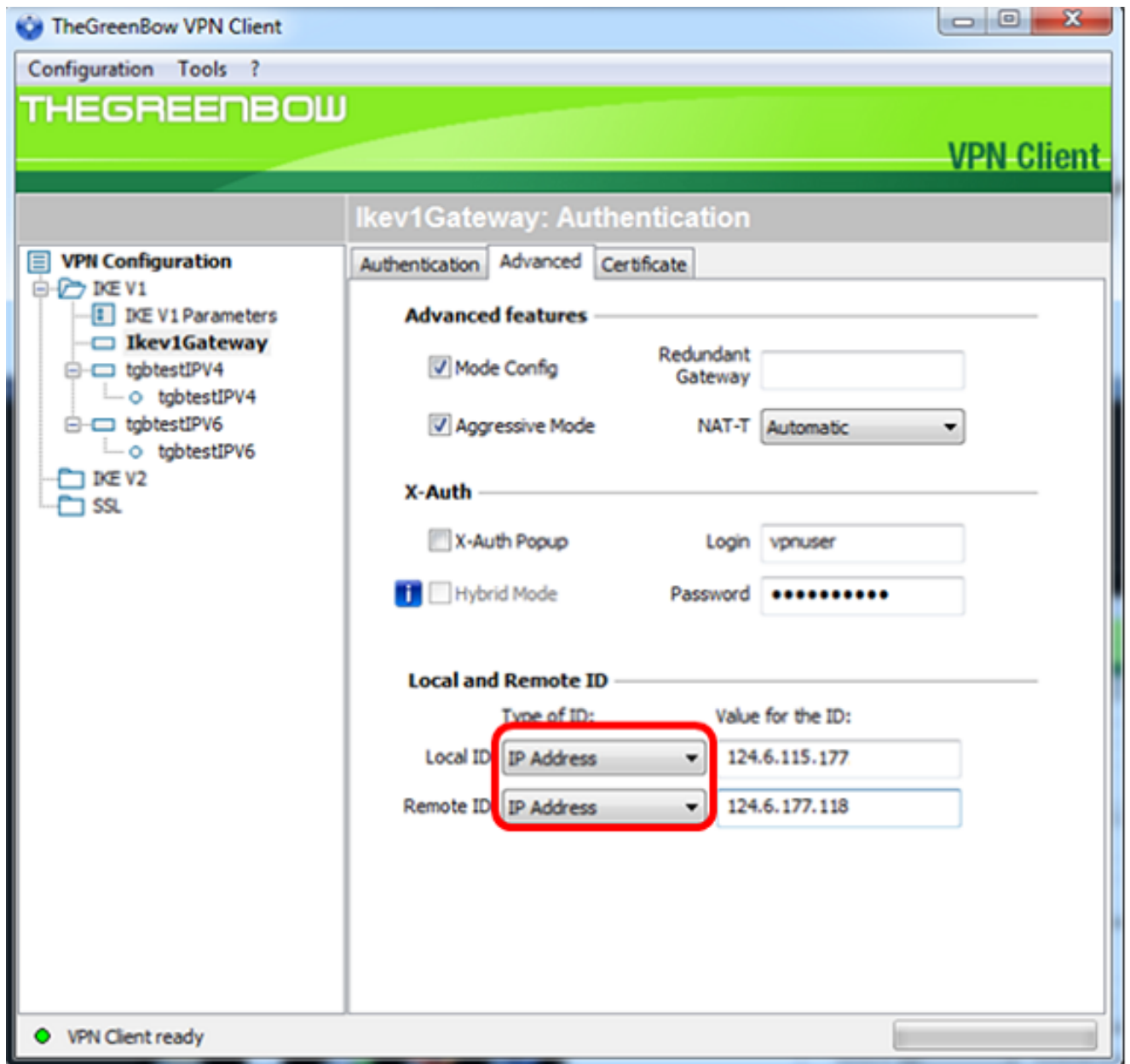
步驟12.在Login欄位中輸入您的使用者名稱。這是為在VPN網關中建立使用者組而配置的使用者名稱。



步驟13.在 *Password* 欄位中輸入密碼。

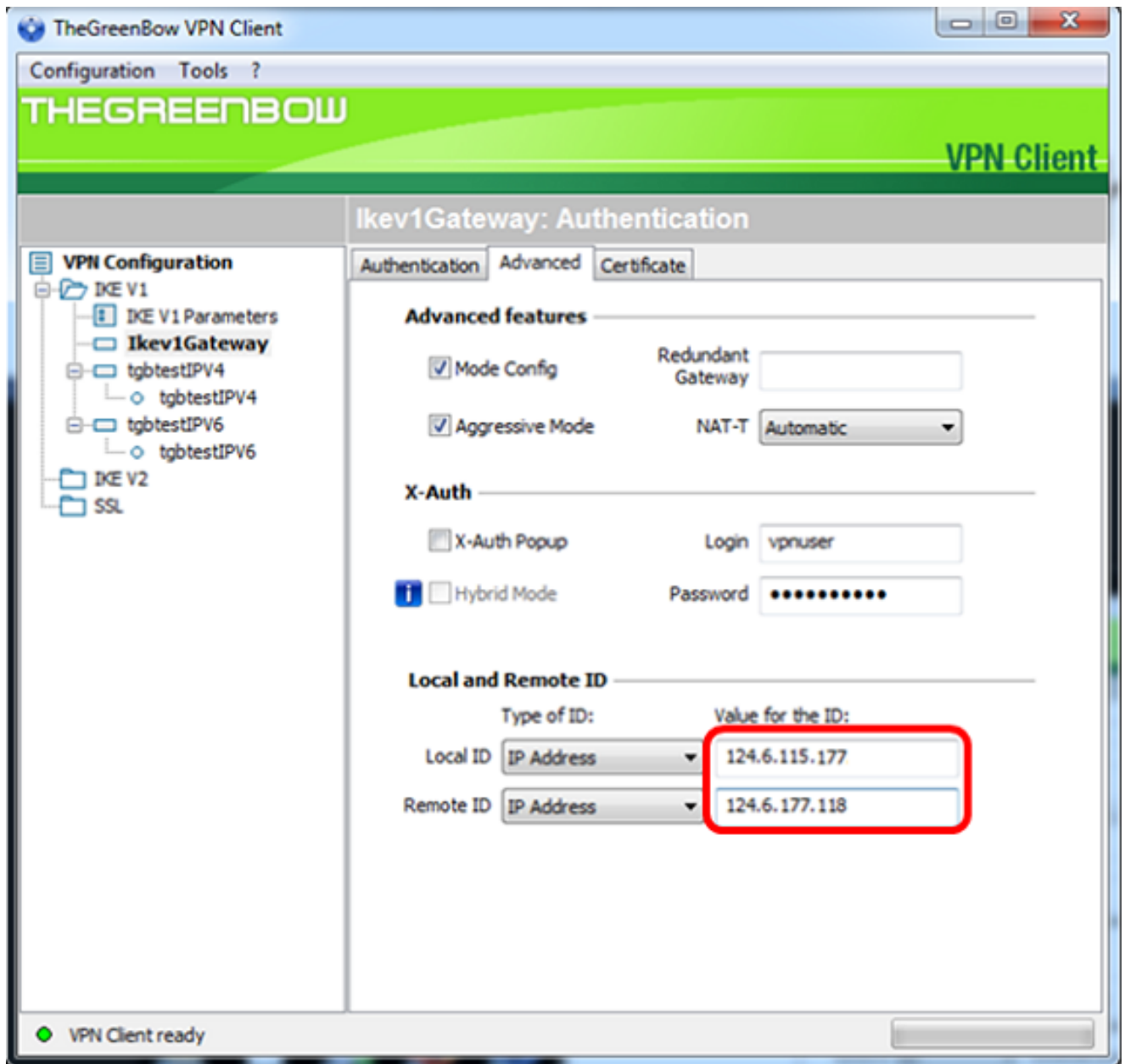


步驟14.在Local和Remote ID下，設定Local ID和Remote ID以匹配VPN網關的設定。

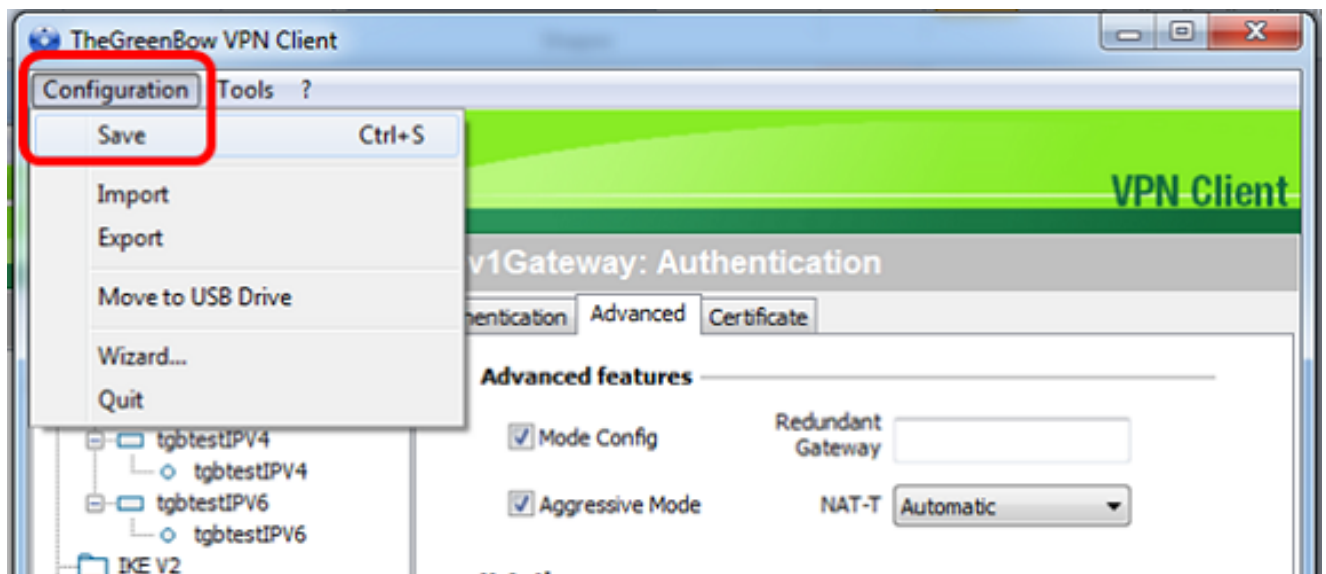


附註：在本示例中，本地ID和遠端ID都設定為IP地址以匹配RV34x VPN網關的設定。

步驟15.在ID的值下，在各自的欄位中輸入本地ID和遠端ID。

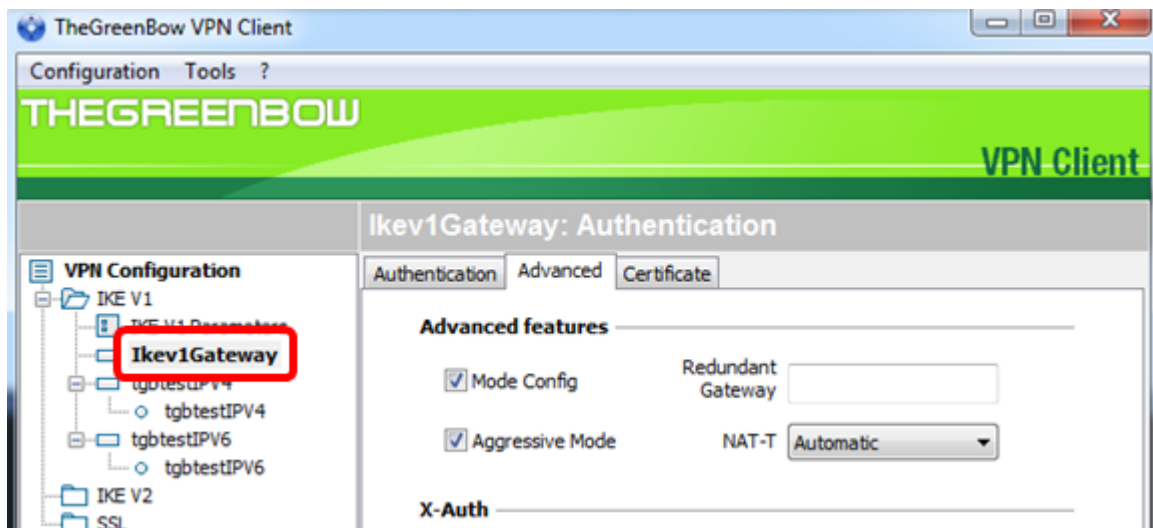


步驟16. 按一下Configuration > Save以儲存設定。

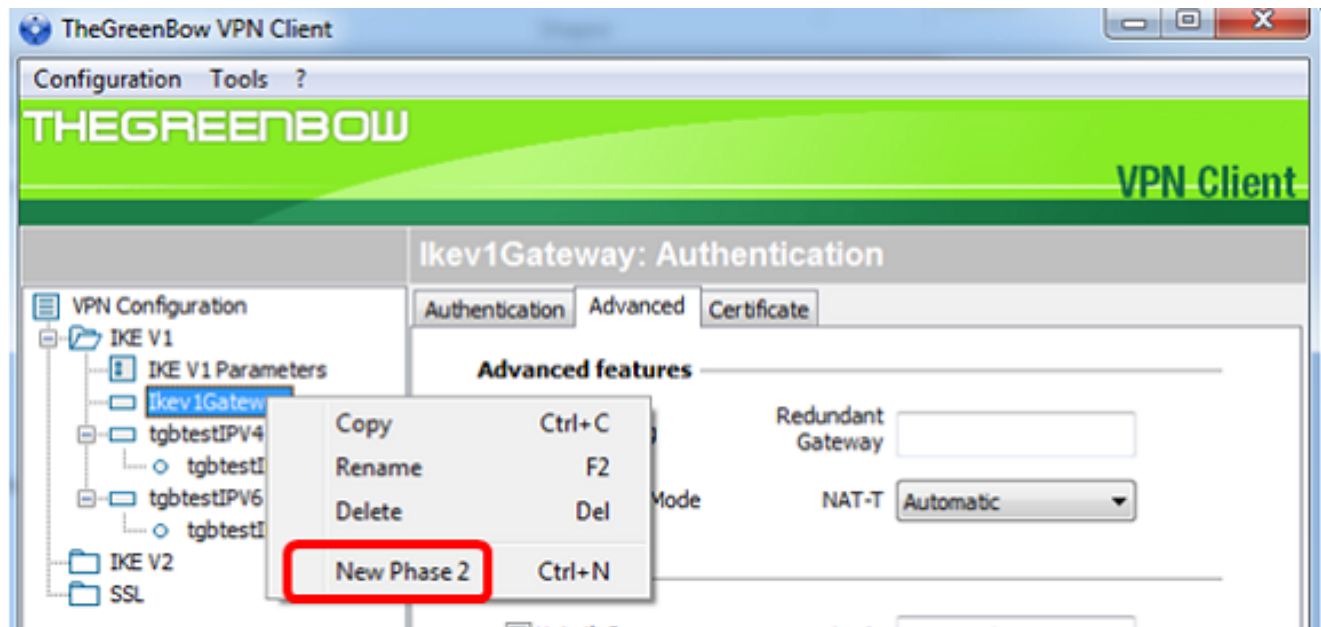


配置階段2設定

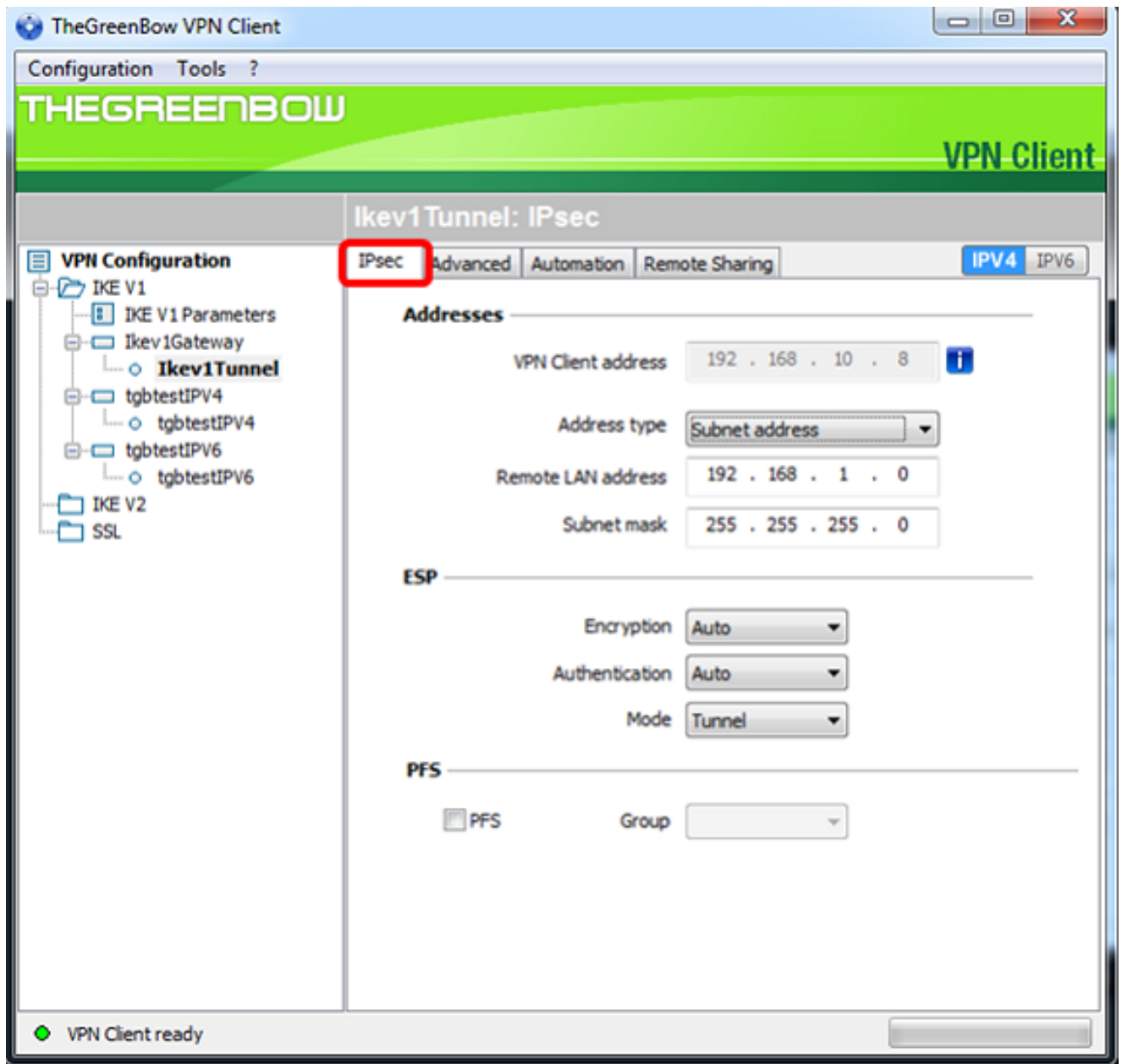
步驟1.按一下右鍵Ikev1Gateway。



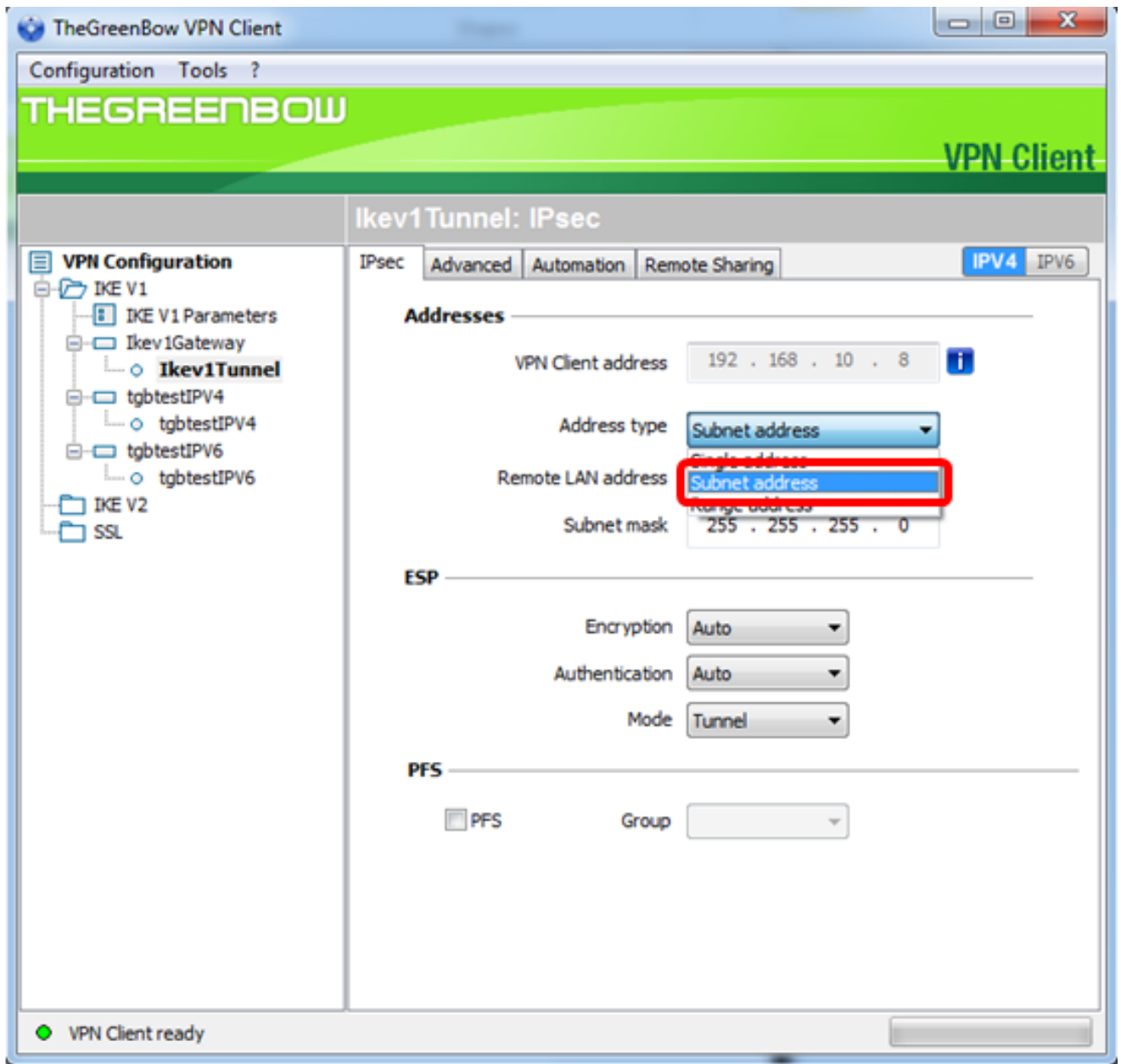
步驟2.選擇新階段2。



步驟3.按一下IPsec選項卡。

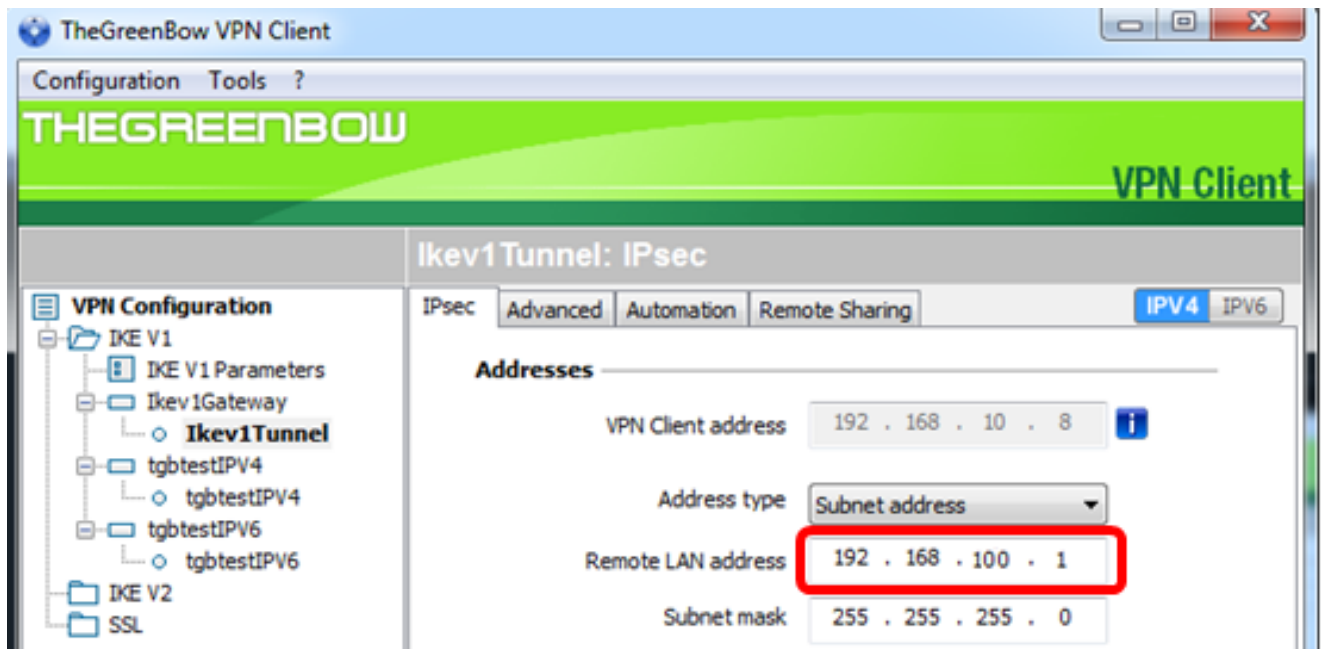


步驟4.從Address type下拉選單中選擇VPN客戶端可以訪問的地址型別。



附註：在本例中，選擇了子網地址。

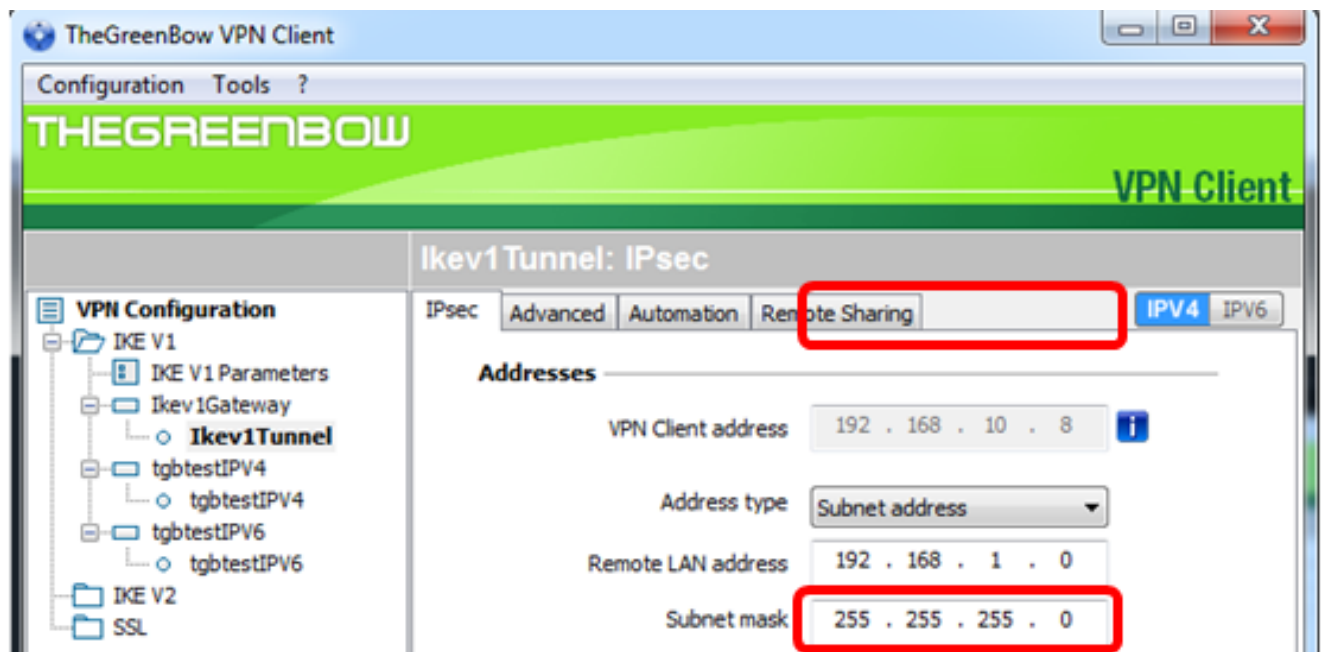
步驟5.在 *Remote LAN address* 欄位中輸入應由VPN隧道訪問的網路地址。



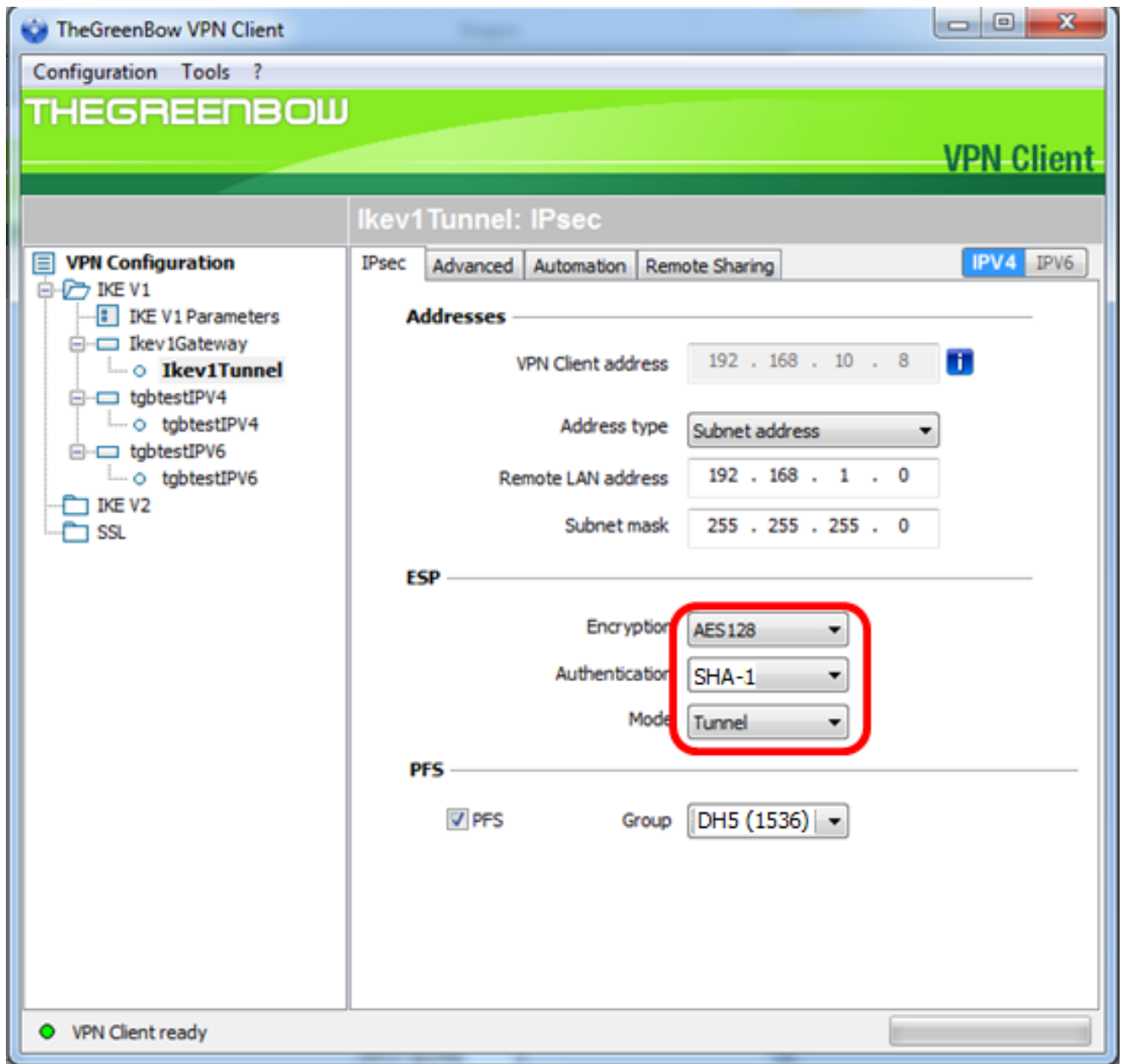
附註：在本示例中，輸入了192.168.100.1。

步驟6.在Subnet mask欄位中輸入遠端網路的子網掩碼。

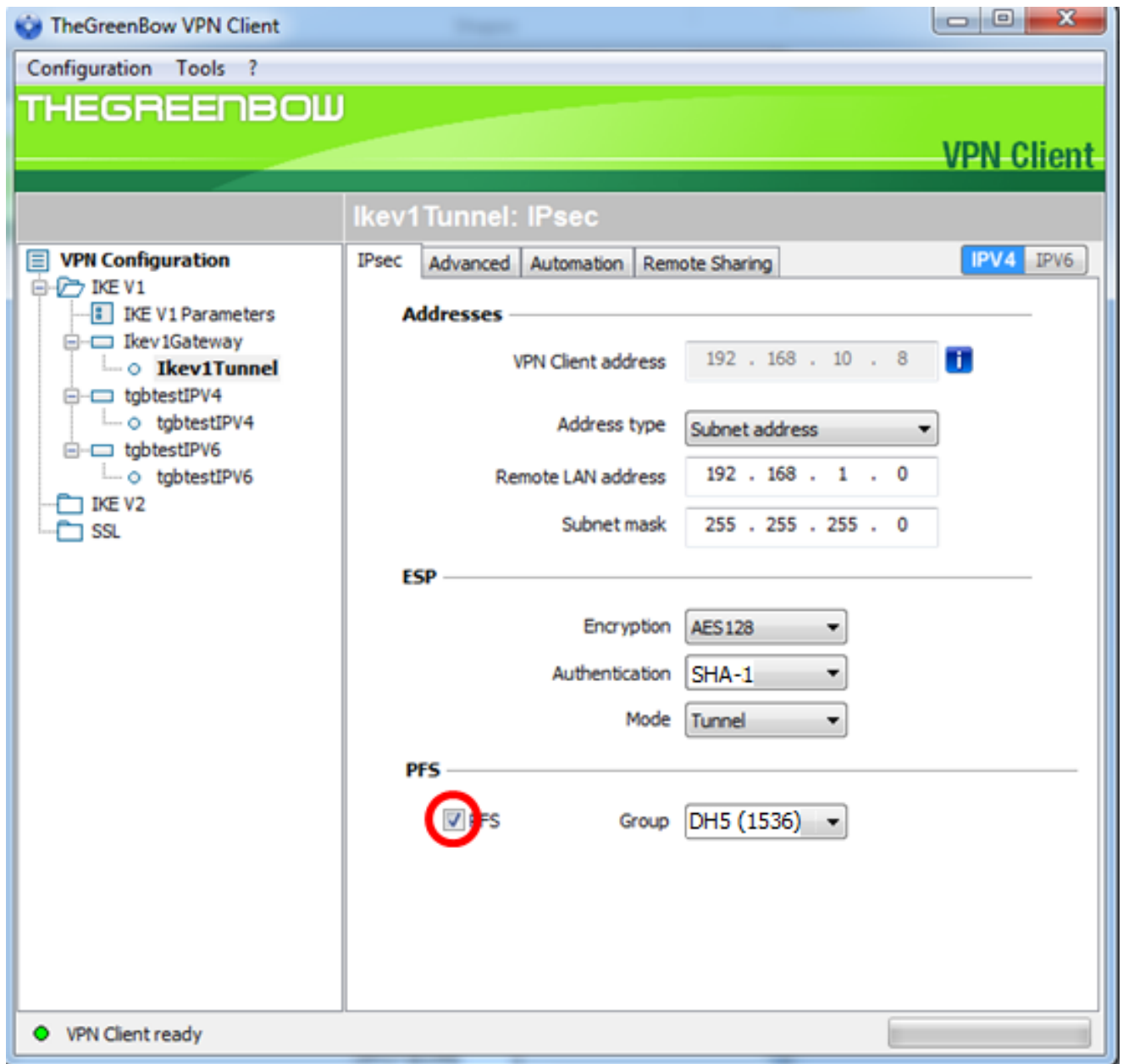
附註：在本例中，輸入了255.255.255.0。



步驟7.在ESP下，設定加密、身份驗證和模式以匹配VPN網關的設定。

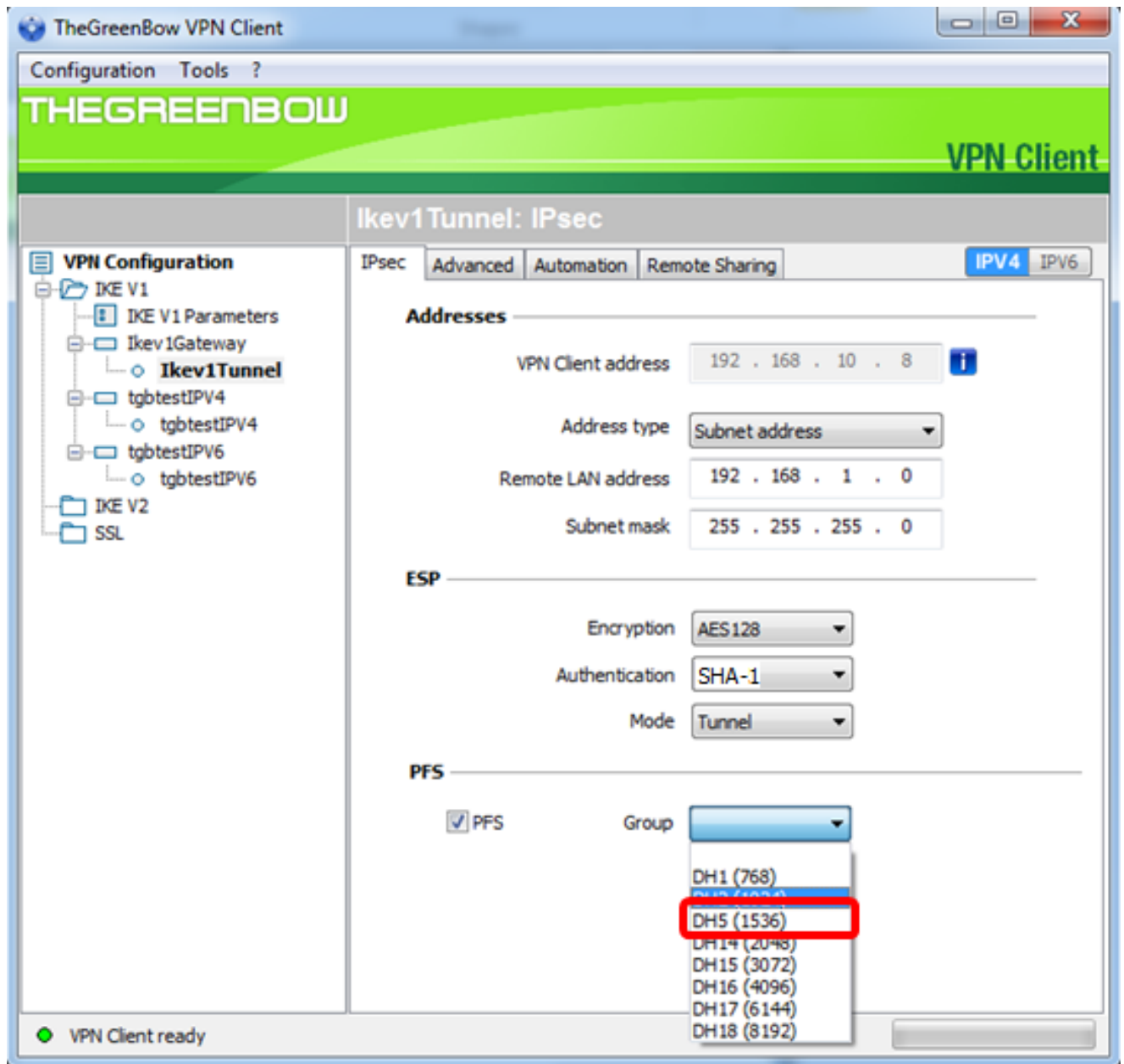


步驟8. (可選) 在PFS下，勾選PFS覈取方塊以啟用完全向前保密(PFS)。PFS生成用於加密會話的隨機金鑰。

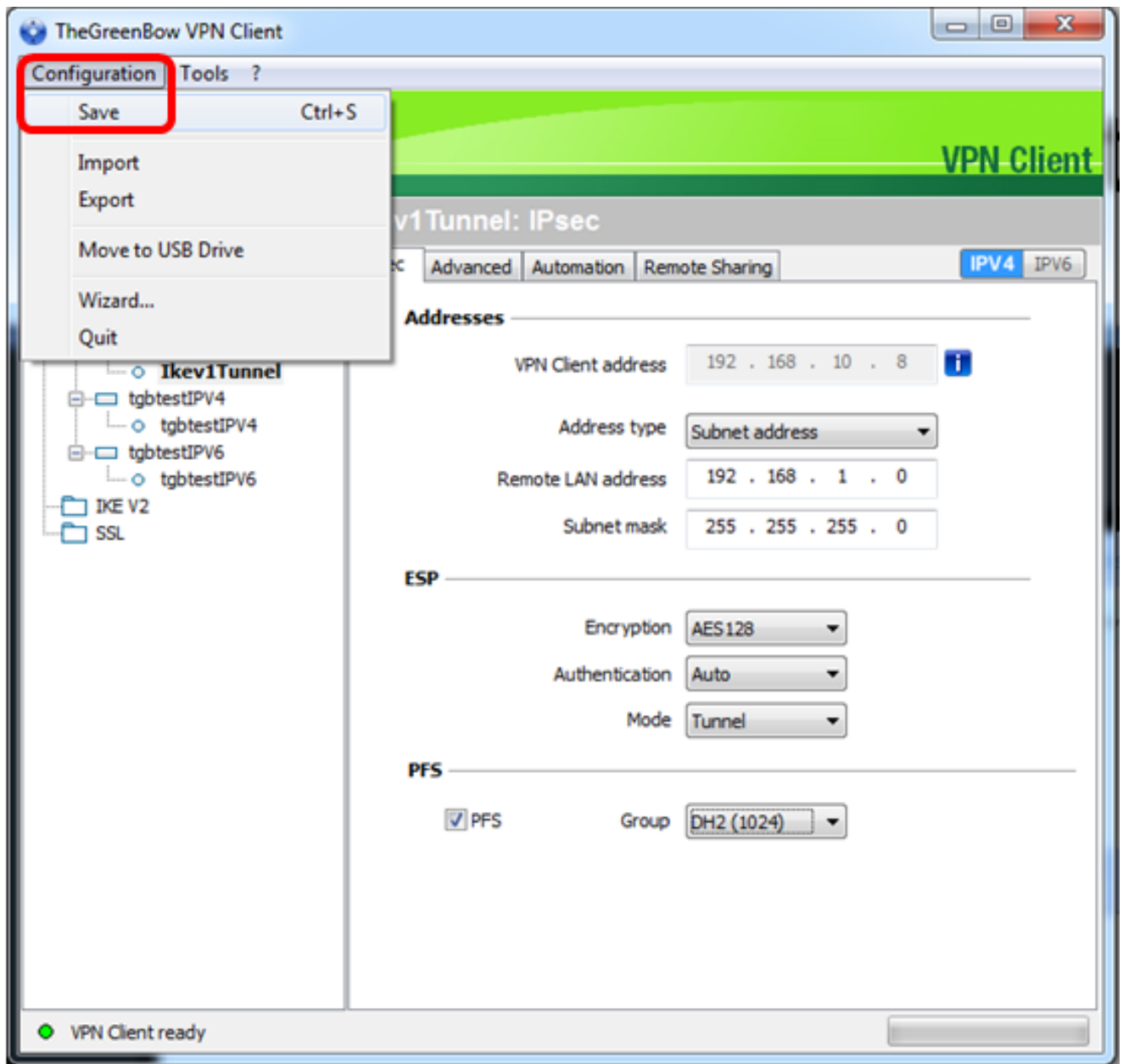


步驟9.從Group下拉選單中選擇PFS組設定。

附註：在本例中，選擇DH5(1536)以匹配路由器的DH組設定。



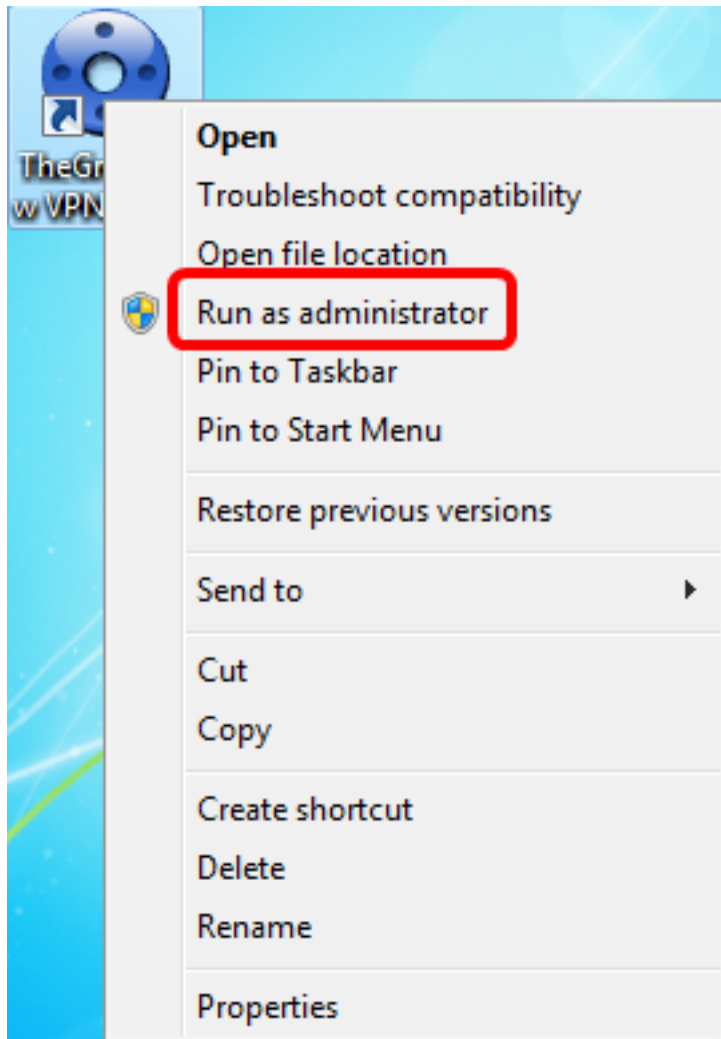
步驟10.按一下右鍵Configuration並選擇「儲存」。



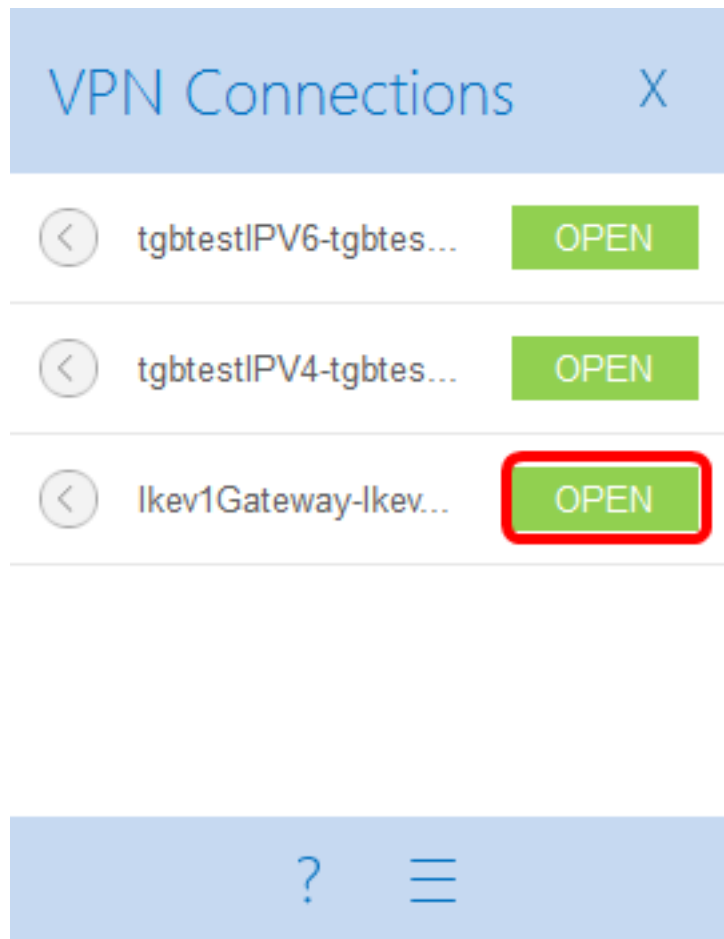
您現在應該已經成功配置TheGreenBow VPN客戶端，通過VPN連線到RV34x系列路由器。

啟動VPN連線

步驟1. 按一下右鍵TheGreenBow VPN Client並選擇Run as administrator。



步驟2.選擇您需要使用的VPN連線，然後按一下**OPEN**。VPN連線應自動啟動。

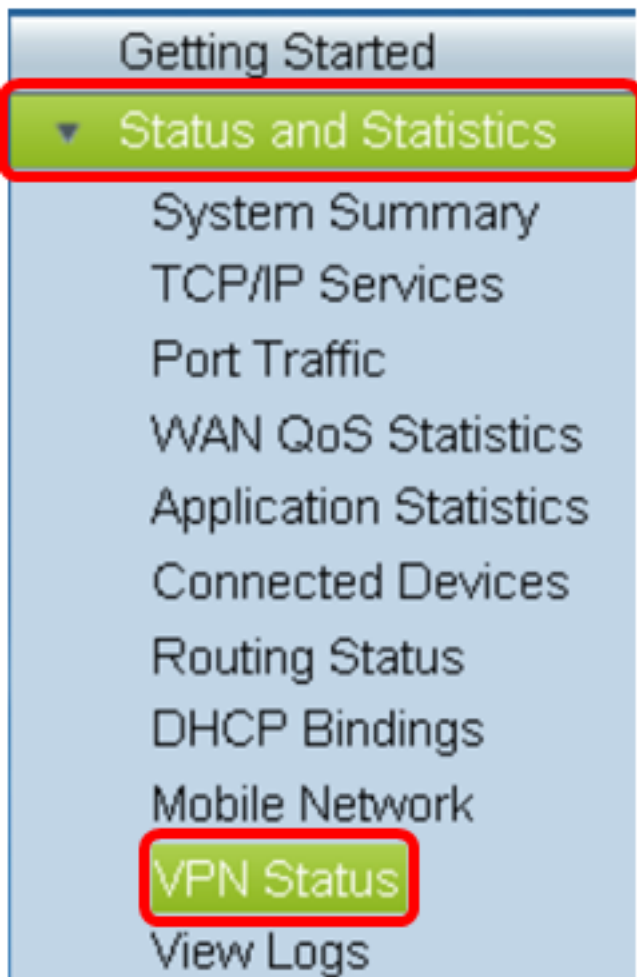


附註：在本示例中，選擇了配置的Ikev1Gateway。

驗證VPN狀態

步驟1.登入到VPN網關的基於Web的實用程式。

步驟2.選擇Status and Statistics > VPN Status。



步驟3.在Client-to-Site Tunnel Status下，檢查Connection表的Connections列。

附註：在本示例中，已建立了一個VPN連線。

Connections
1

現在，您應該已經成功驗證了RV34x系列路由器上的VPN連線狀態。GreenBow VPN客戶端現在配置為通過VPN連線到路由器。