設定和使用GreenBow IPsec VPN客戶端與RV160和RV260路由器連線

目標

本文檔的目標是設定和使用TheGreenBow IPsec VPN客戶端與RV160和RV260路由器連線。

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。企業辦公室經常使用VPN連線，因為即使員工不在辦公室，允許他們訪問其專用網路也是非常有用和必要的。

VPN允許遠端主機或客戶端像位於同一本地網路一樣工作。RV160路由器支援最多10個VPN隧道，RV260支援最多20個。在路由器配置為網際網路連線後，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。設定必須完全匹配，否則它們無法通訊。

GreenBow VPN客戶端是第三方VPN客戶端應用，使主機裝置能夠配置客戶端到站點IPsec隧道與RV160和RV260系列路由器的安全連線。

使用VPN連線的優點

使用VPN連線有助於保護機密的網路資料和資源。

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，而不必親自到場，同時還可以維護專用網路及其資源的安全。

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。高級加密演算法使這一點成為可能，保護私有網路免受未經授權的訪問。

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（例如Internet）。

VPN允許新增新使用者或使用者組，而無需新增其他元件或複雜的配置。

使用VPN連線的風險

由於配置錯誤，可能存在安全風險。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。

它可能就不那麼可靠了。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）。

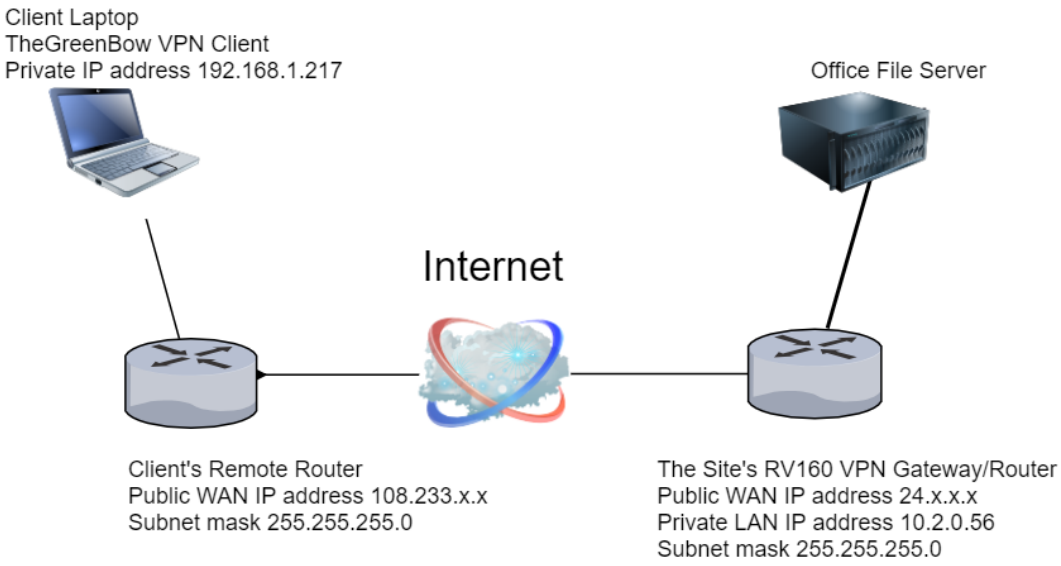
如果出現需要新增新基礎架構或新配置的情況，技術問題可能因不相容而產生，尤其是當所使用產品或供應商不是涉及到時。

可能會出現連線速度慢的情況。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。在本文中，我們將使用應消除此問題的付費第三

方。

客戶端到站點網路的基本拓撲

這是用於設定的網路的基本佈局。公有WAN IP地址已部分模糊，或顯示**x**代替實際數字以保護此網路免受攻擊。



本文將介紹在站點配置RV160或RV260路由器所需的步驟，其中包括：

- 使用者組 — **VPNUsers**
- 允許作為客戶端訪問的使用者帳戶（一個或多個使用者）
- IPsec配置檔案 — **TheGreenBow**
- 客戶端到站點配置檔案 — 客戶**端**
- 還將向您展示如何在客戶端連線後檢視站點的VPN狀態

附註：使用者組、IPsec配置檔案和客戶端到站點配置檔案可以使用任何名稱。所列名字只是例子。

本文還說明了每個客戶端在其電腦上配置TheGreenBow VPN的步驟：

- 下載並設定TheGreenBow VPN客戶端軟體
- 配置客戶端的第1階段和第2階段設定
- 作為客戶端啟動並驗證VPN連線

很重要的一點是，路由器上的所有設定都與客戶端設定匹配。如果您的配置不會導致VPN連線成功，請檢查所有設定以確保它們匹配。本文中所示的示例只是一種設定連線的方法。

目錄

在現場配置RV160或RV260路由器

建立使用者組

建立使用者帳戶

配置IPsec配置檔案

配置階段1和2設定

建立客戶端到站點配置檔案

在客戶端位置配置

配置階段1設定

配置隧道設定

作為客戶端啟動VPN連線

檢查RV160或RV260上的連通性

驗證站點的VPN狀態

適用裝置

- RV160
- RV260

軟體版本

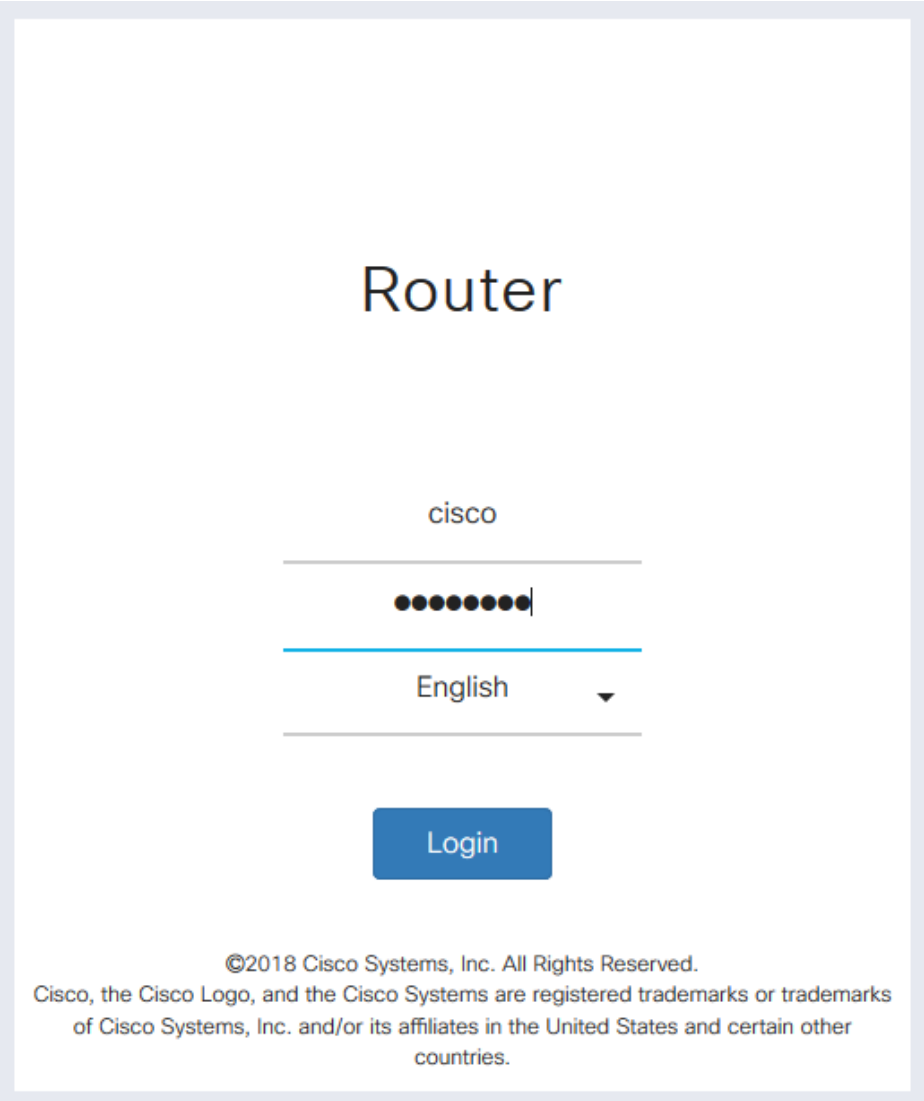
- 1.0.00.15

在RV160或RV260路由器的站點配置VPN客戶端

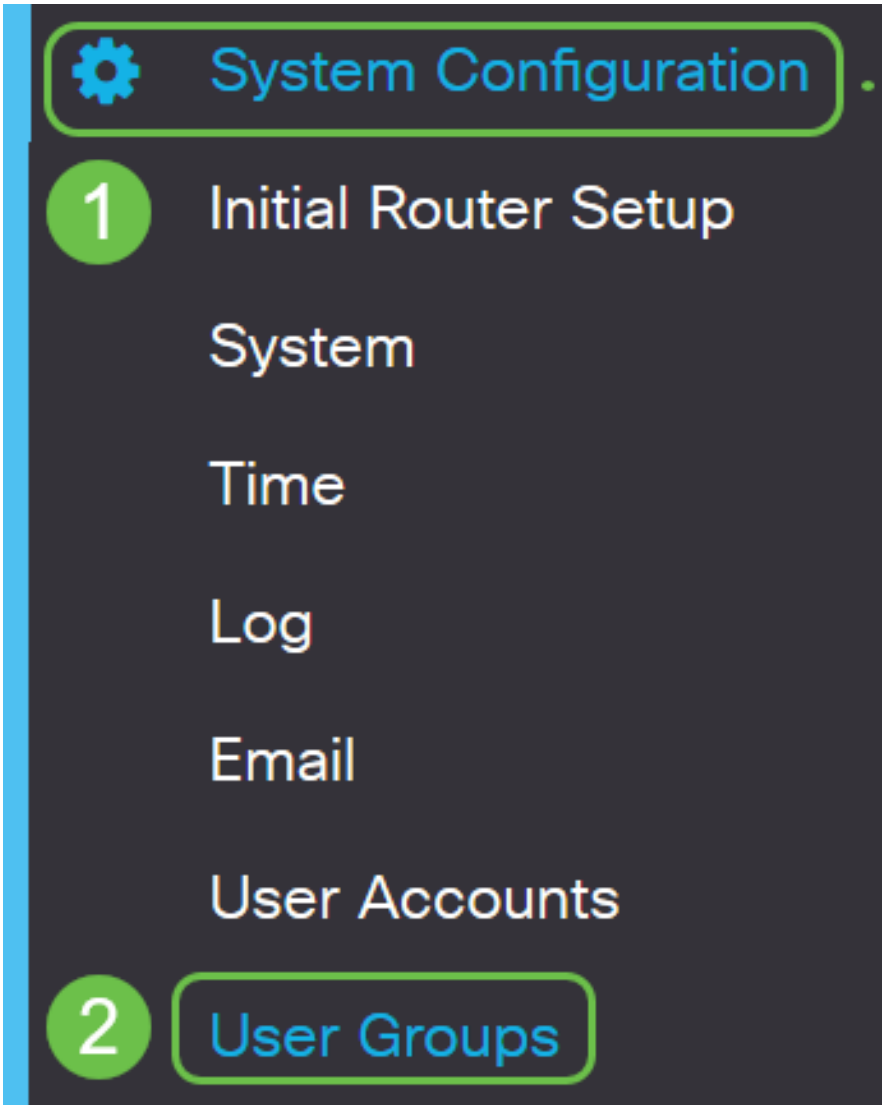
建立使用者組

重要附註：請將預設管理員帳戶保留在管理組中，並為TheGreenBow建立新的使用者帳戶和使用者組。如果將管理員帳戶移動到不同的組，您將阻止自己登入路由器。

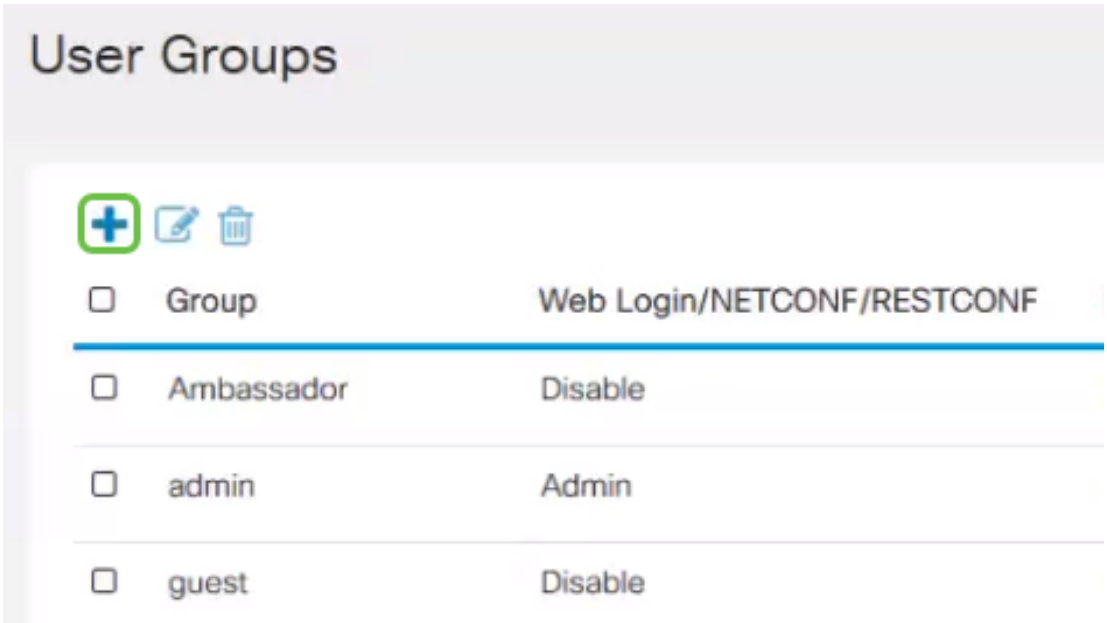
步驟1.登入到路由器的基於Web的實用程式。



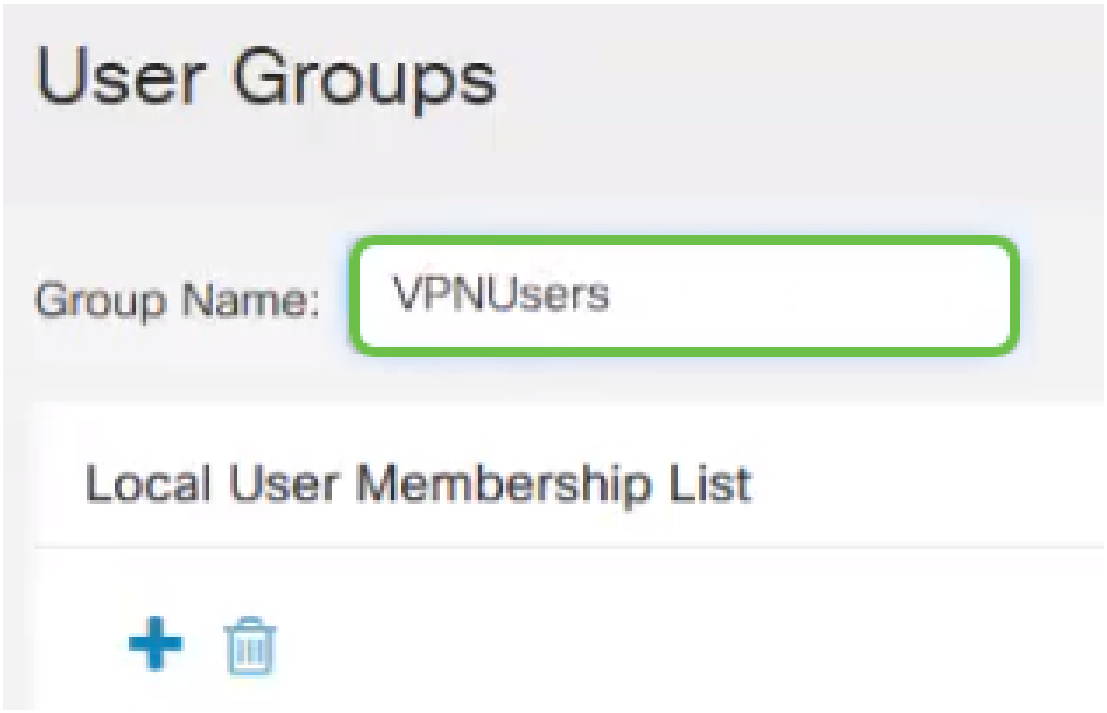
步驟2.選擇System Configuration > User Groups。



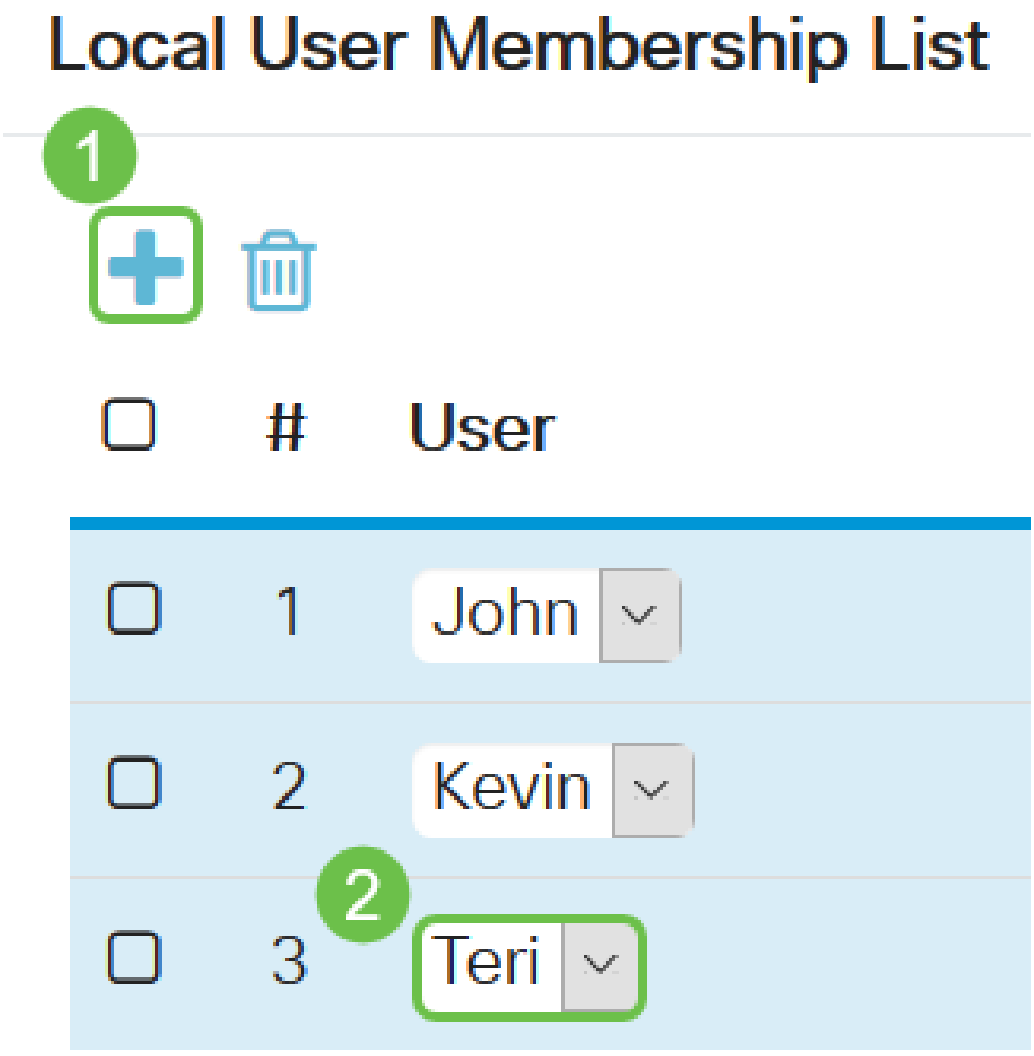
步驟3.按一下**plus**圖示新增使用者組。



步驟4.在「概覽」區域中，在「組名稱」欄位中*輸入組*名。

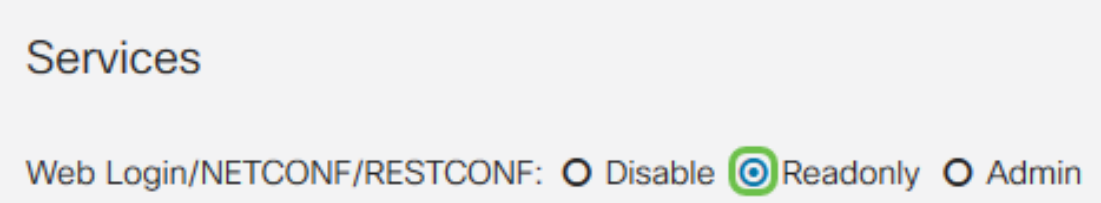


步驟5.在*Local User Membership List*下，按一下**plus**圖示並從下拉選單中選擇使用者。如果要新增更多，請再次按**加號**圖示，然後選擇要新增的其他成員。成員只能是一個組的一部分。如果您尚未輸入所有使用者，則可以在建立使用者帳戶部分中新增更多使用者。

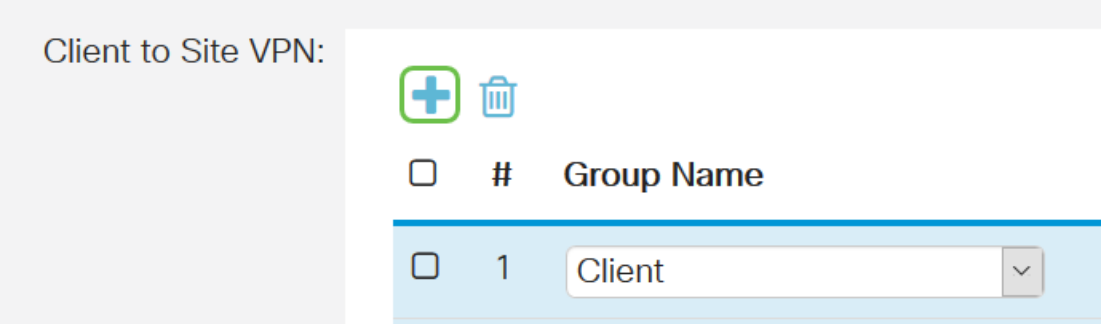


步驟6.在*服務*下，選擇要授予組中的使用者的許可權。選項包括：

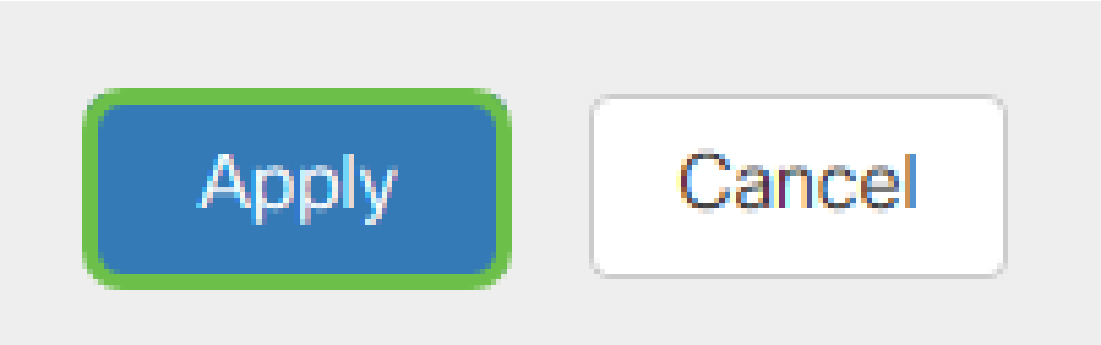
- 已禁用 — 此選項表示不允許組成員通過瀏覽器訪問基於Web的實用程式。
- 只讀 — 此選項表示組的成員只有在登入後才能讀取系統的狀態。它們無法編輯任何設定。
- Admin — 此選項為組的成員提供讀寫許可權，並能夠配置系統狀態。



步驟7.按一下**plus**圖示新增現有的客戶端到站點VPN。如果尚未配置此配置檔案，可在[建立客戶端到站點配置檔案](#)部分找到本文中的資訊。

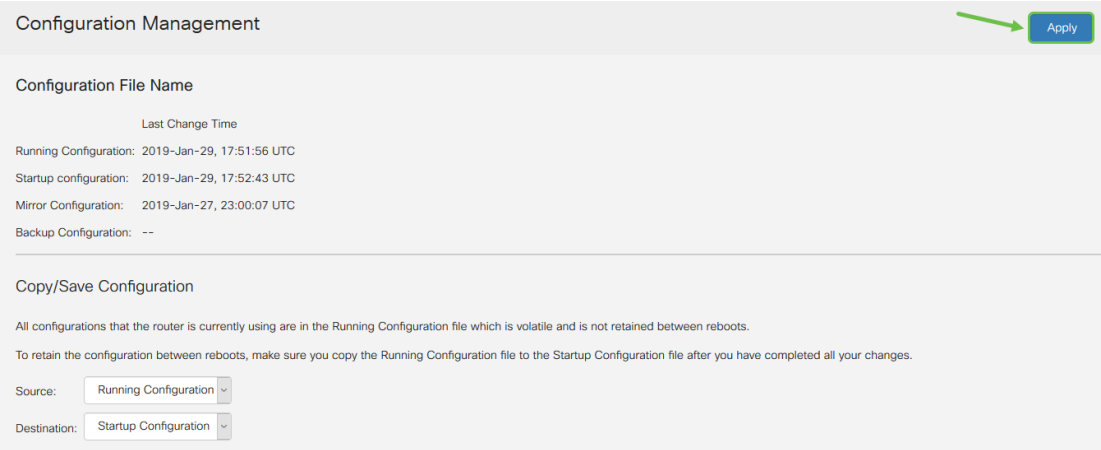


步驟8.按一下**Apply**。

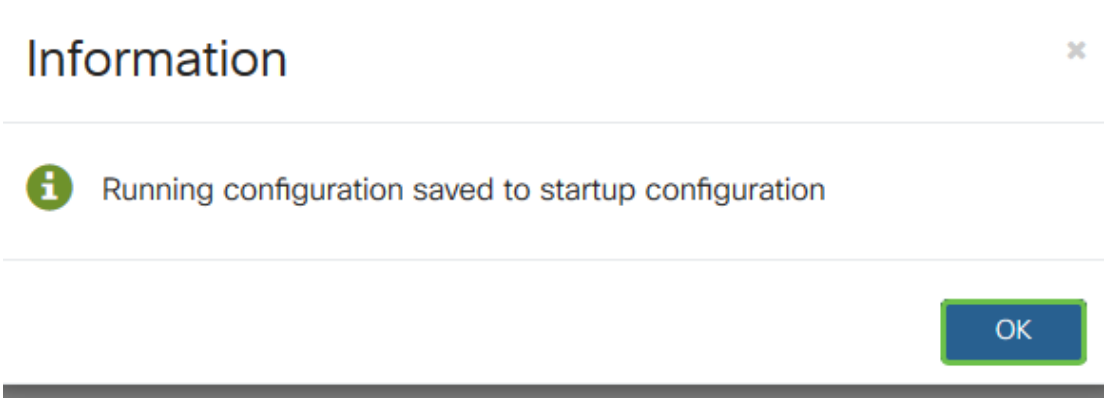


步驟9.按一下「**Save**」。

步驟10.再次按一下**Apply**，將執行組態儲存到啟動組態。



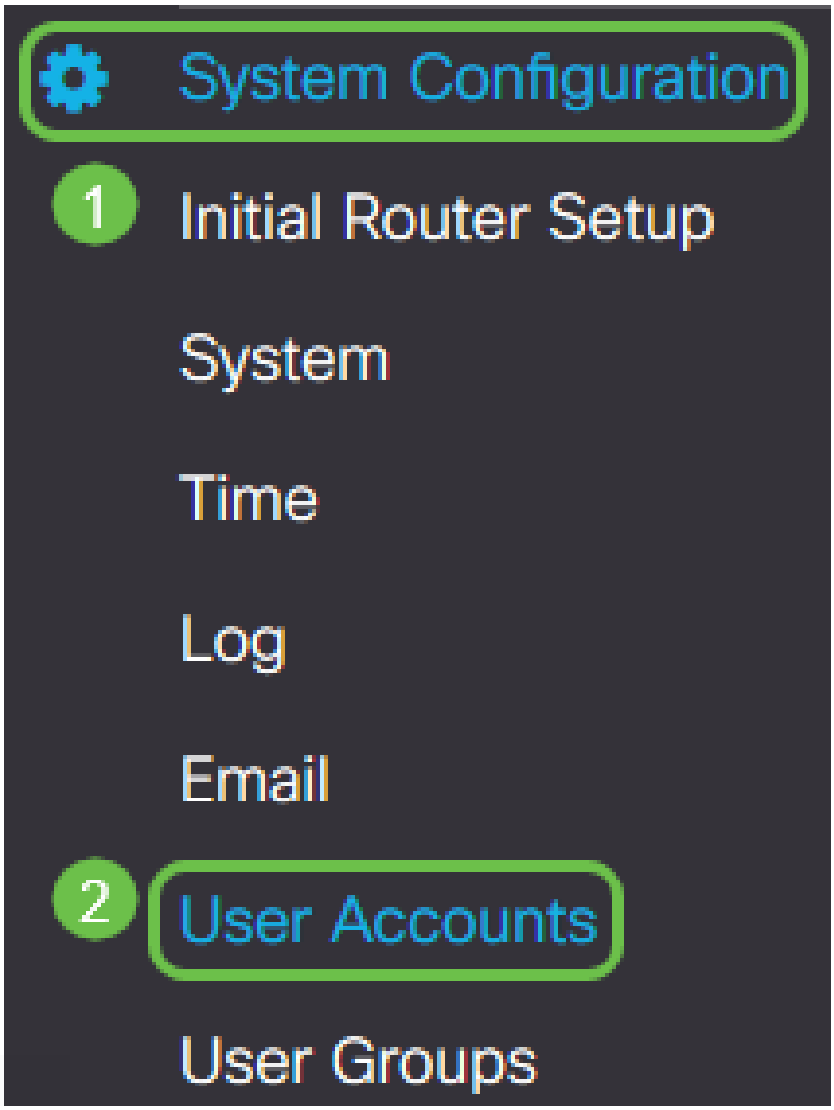
步驟11.收到確認資訊後，按一下**OK**。



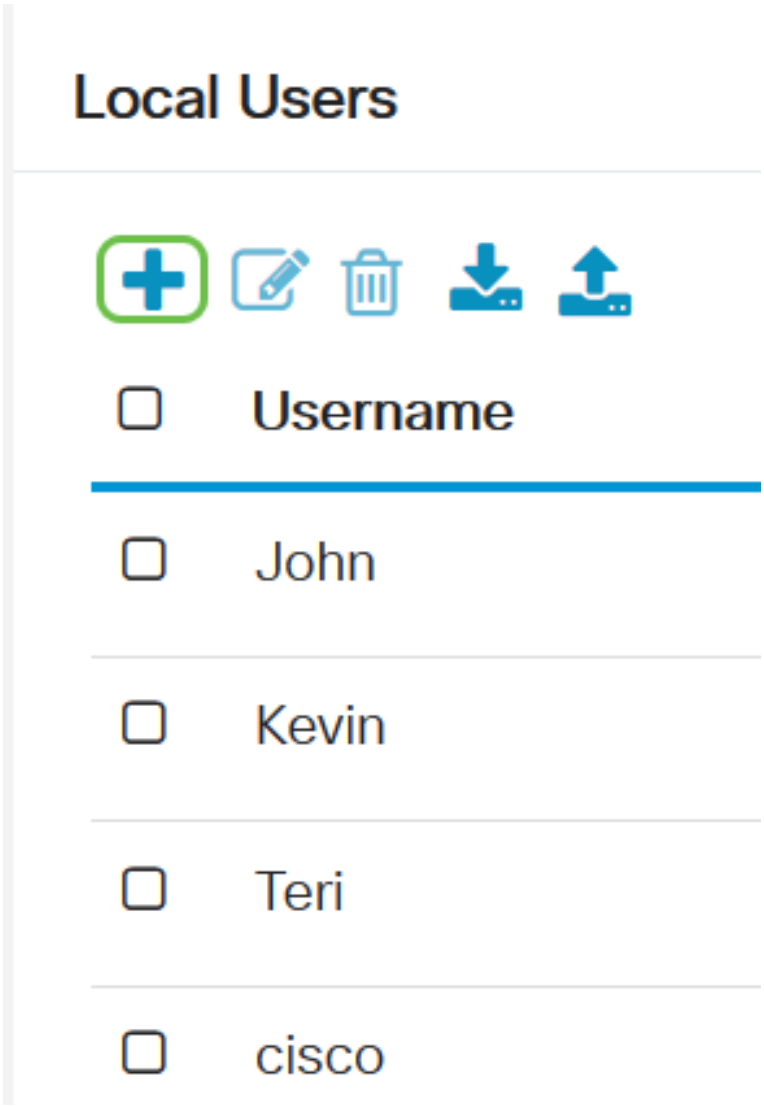
您現在應該已經在RV160或RV260系列路由器上成功建立使用者組。

建立使用者帳戶

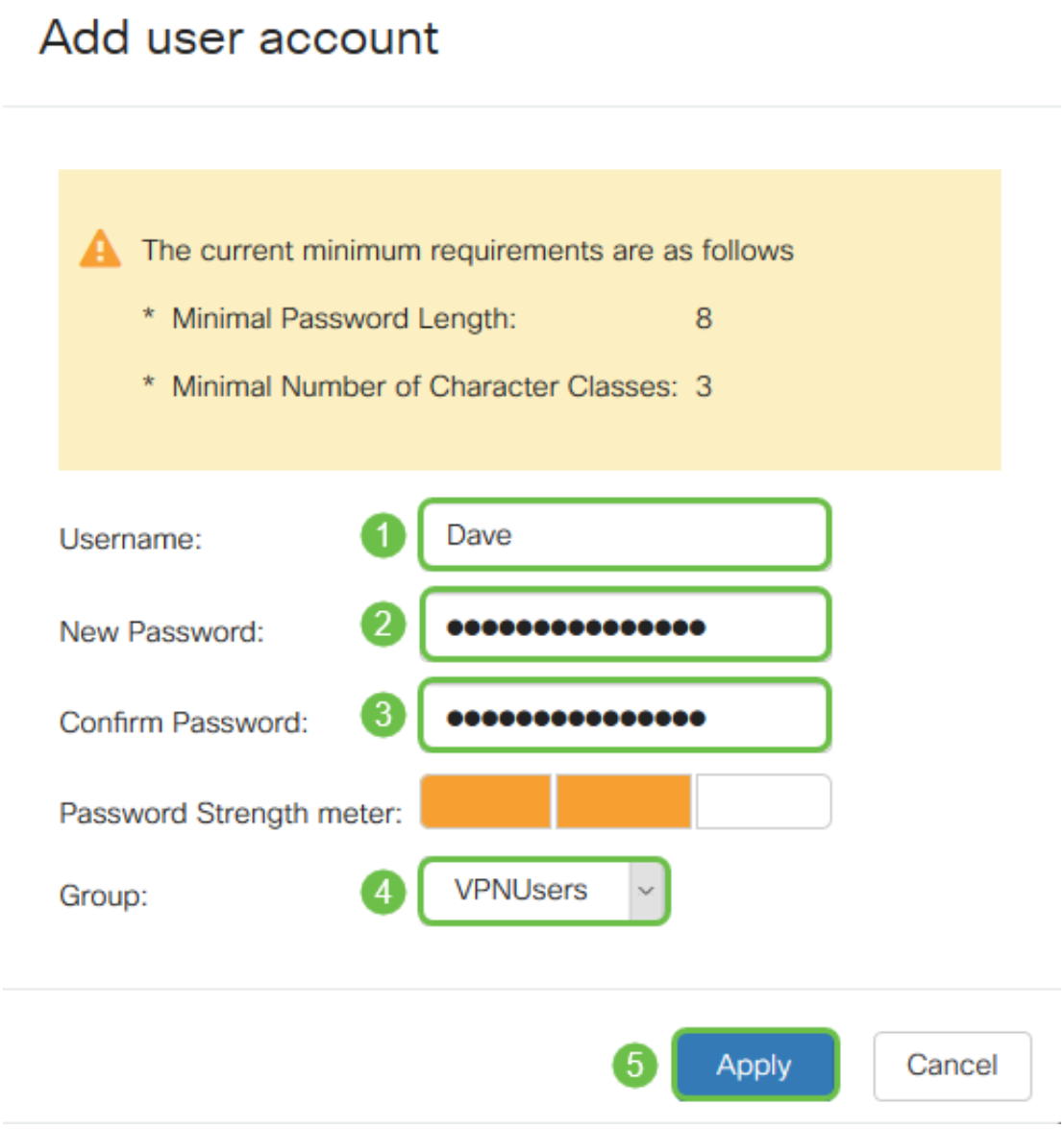
步驟1.登入到路由器的基於Web的實用程式，然後選擇**System Configuration > User Accounts**。



步驟2.在*Local Users*區域中，按一下**add**圖示。



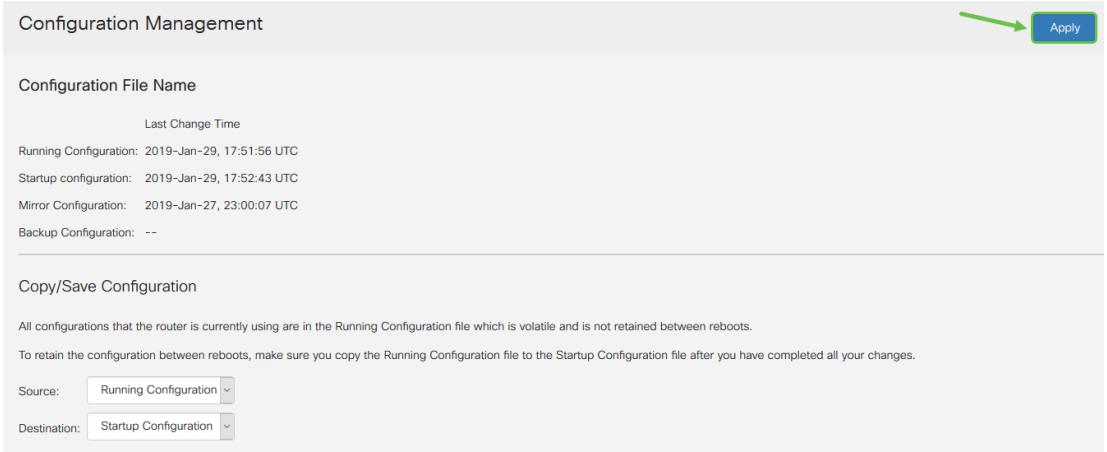
步驟3.在*Username*欄位中輸入使用者的名稱、密碼以及您要從下拉選單將使用者新增到其中的組。按一下「**Apply**」。



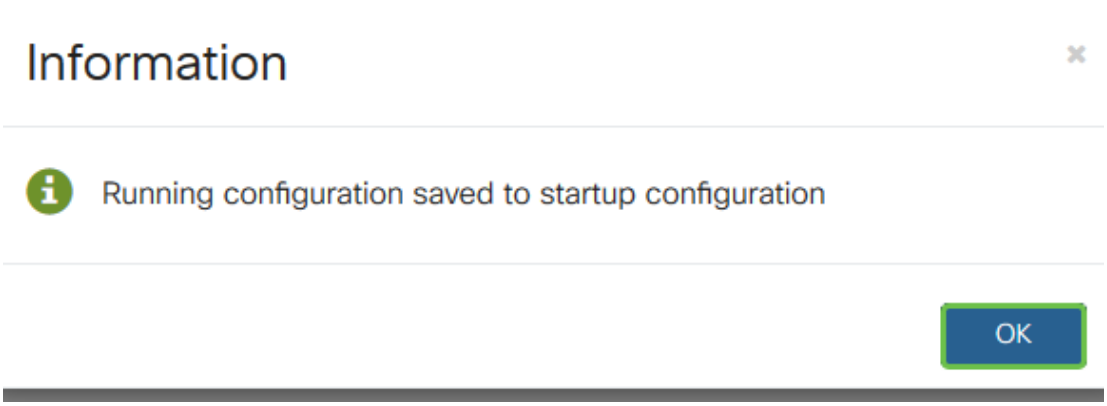
附註：當客戶端在其電腦上設定TheGreenBow Client時，它們將使用相同的使用者名稱和密碼登入。

步驟4.按一下「**Save**」。

步驟5.再次按一下**Apply**，將執行中的組態儲存到啟動組態中。



步驟6.收到確認資訊後，按一下**OK**。

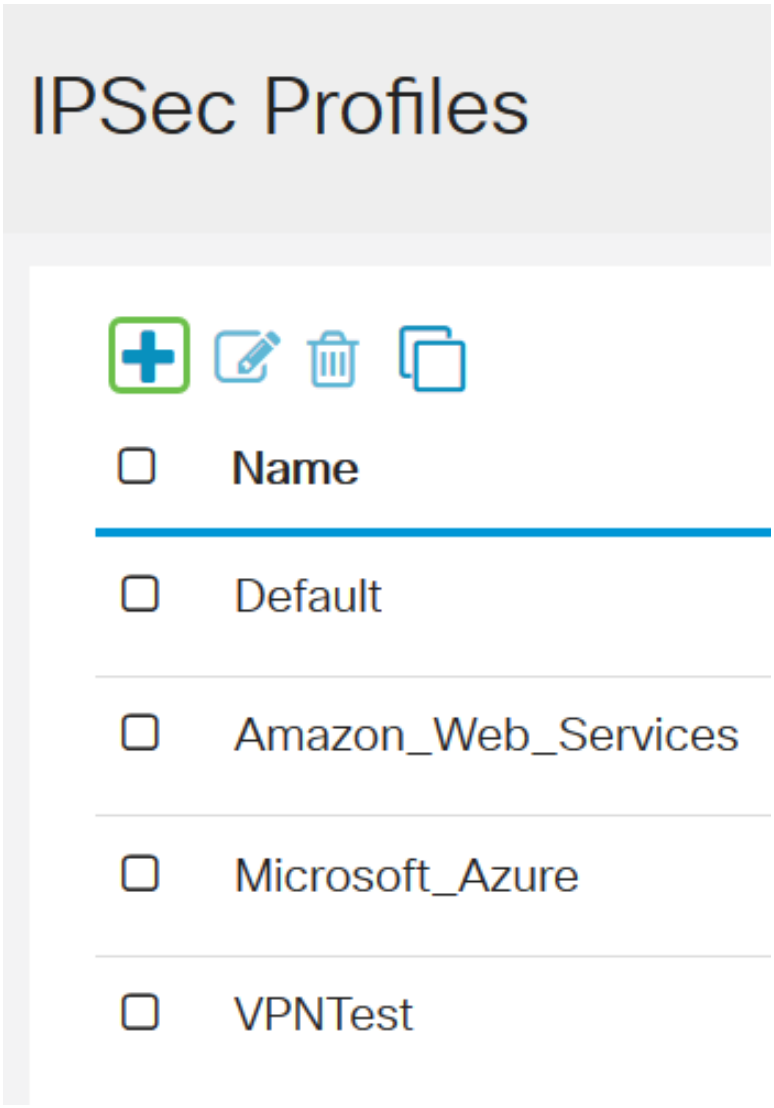


您現在應該已經在RV160或RV260路由器上建立使用者帳戶。

配置IPsec配置檔案

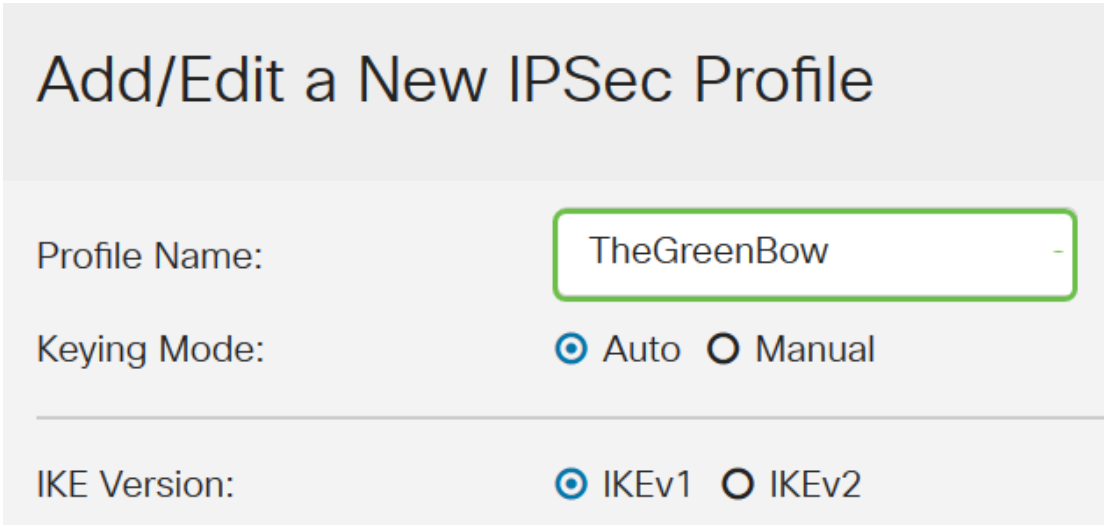
步驟1.登入到RV160或RV260路由器的基於Web的實用程式，然後選擇**VPN > IPSec VPN > IPSec Profiles**。

步驟2. IPSec簡檔表顯示現有簡檔。按一下**plus**圖示以建立新的配置檔案。



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

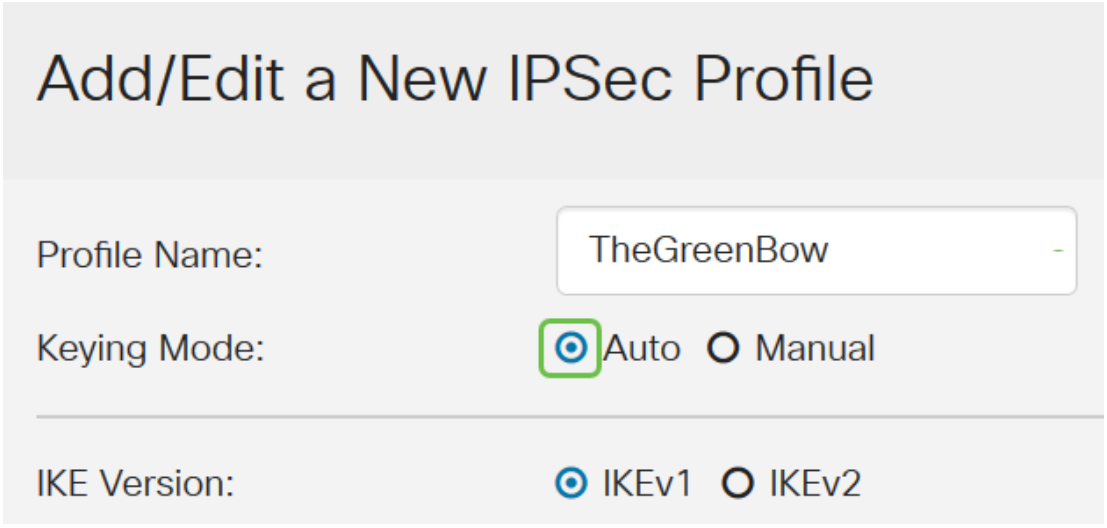
步驟3.在「配置檔名稱」欄位中為配*置檔案*建立名稱。配置檔名稱只能包含字母數字字元以及特殊字元的下劃線(_)。



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：

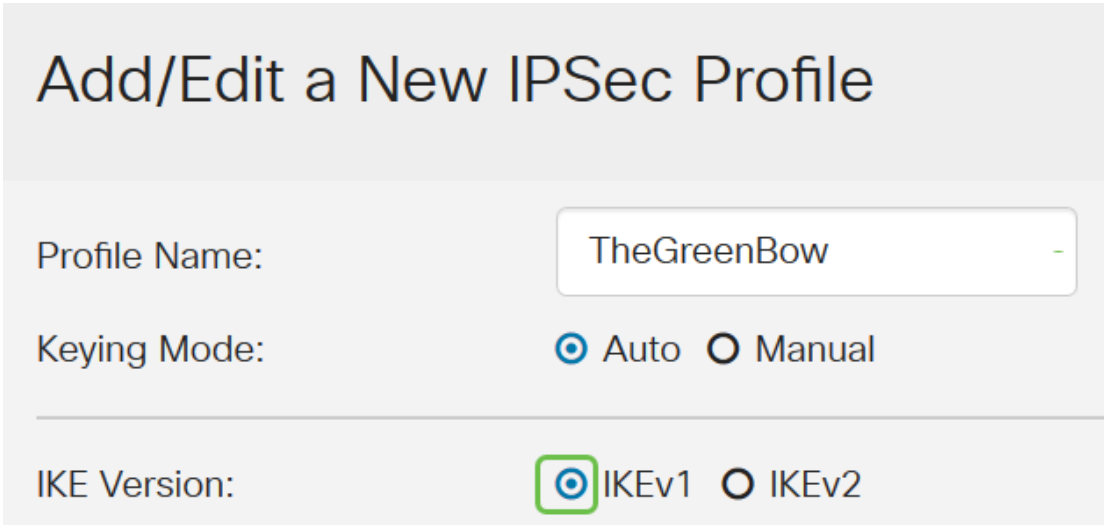
- 自動(Auto) — 自動設定策略引數。此選項使用Internet金鑰交換(IKE)策略進行資料完整性和加密金鑰交換。如果選擇此選項，則啟用Auto Policy Parameters區域下的配置設定。
- 手動(Manual) — 此選項允許您手動配置VPN隧道的資料加密和完整性的金鑰。如果選擇

此選項，則啟用Manual Policy Parameters區域下的配置設定。這並未得到廣泛使用。



附註：在本例中，選擇了**Auto**。

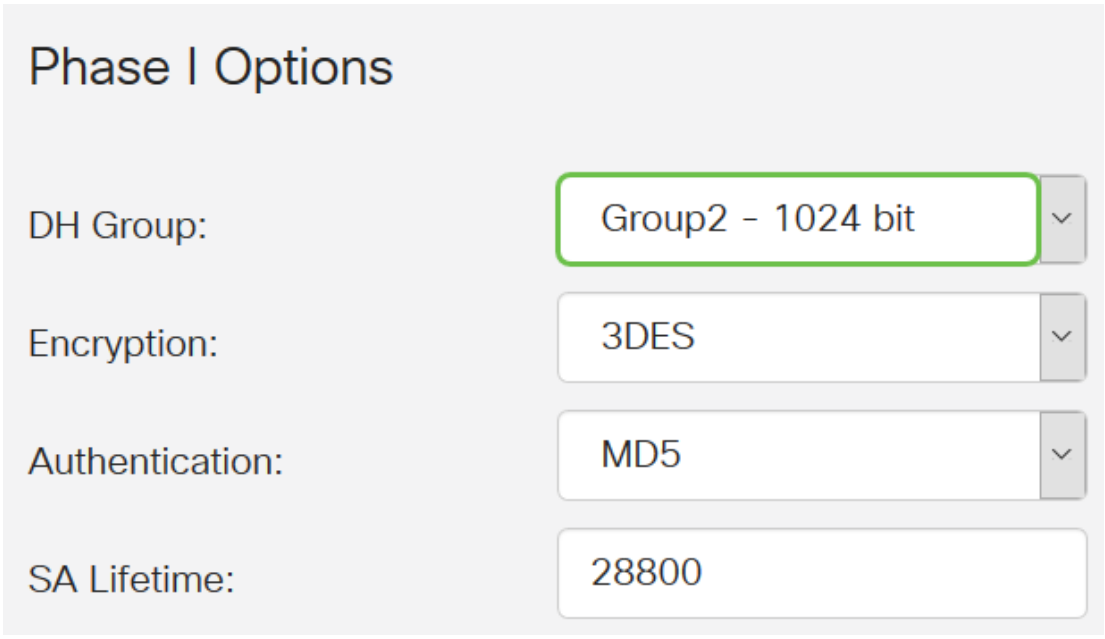
步驟5.選擇IKE版本。確保在客戶端設定TheGreenBow時，選擇相同的版本。



配置階段1和2設定

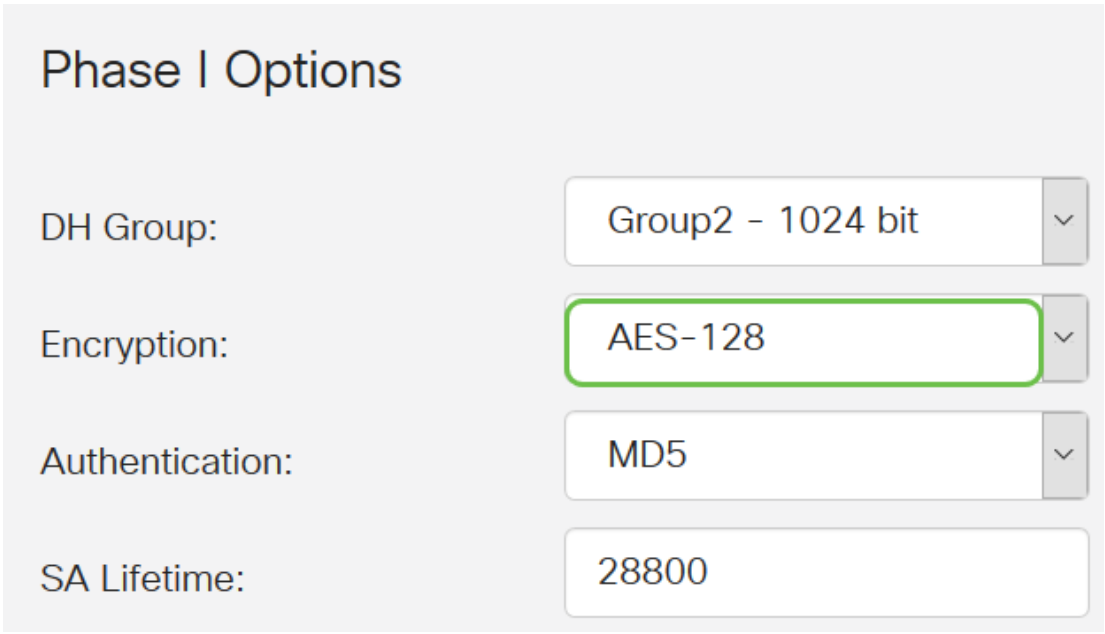
步驟1。在Phase 1 Options區域中，從*DH Group*下拉選單中選擇要與Phase 1中的金鑰一起使用的適當Diffie-Hellman(DH)組。Diffie-Hellman是一種加密金鑰交換協定，用於交換預共用金鑰集。演算法的強度由位決定。選項包括：

- 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。



步驟2.從*Encryption*下拉式清單中選擇一種加密方法以加密和解密封裝安全性裝載(ESP)和網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)。 選項包括：

- 3DES — 三重資料加密標準。不推薦。只有在需要向後相容性時才能使用它，因為它容易受到某些「塊衝突」攻擊。
- AES-128 — 高級加密標準使用128位金鑰。高級加密標準(AES)是一種加密演算法，旨在比DES更安全。AES使用較大的金鑰大小，確保唯一已知解密消息的方法是讓入侵者嘗試所有可能的金鑰。
- 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。這是最安全的加密選項。



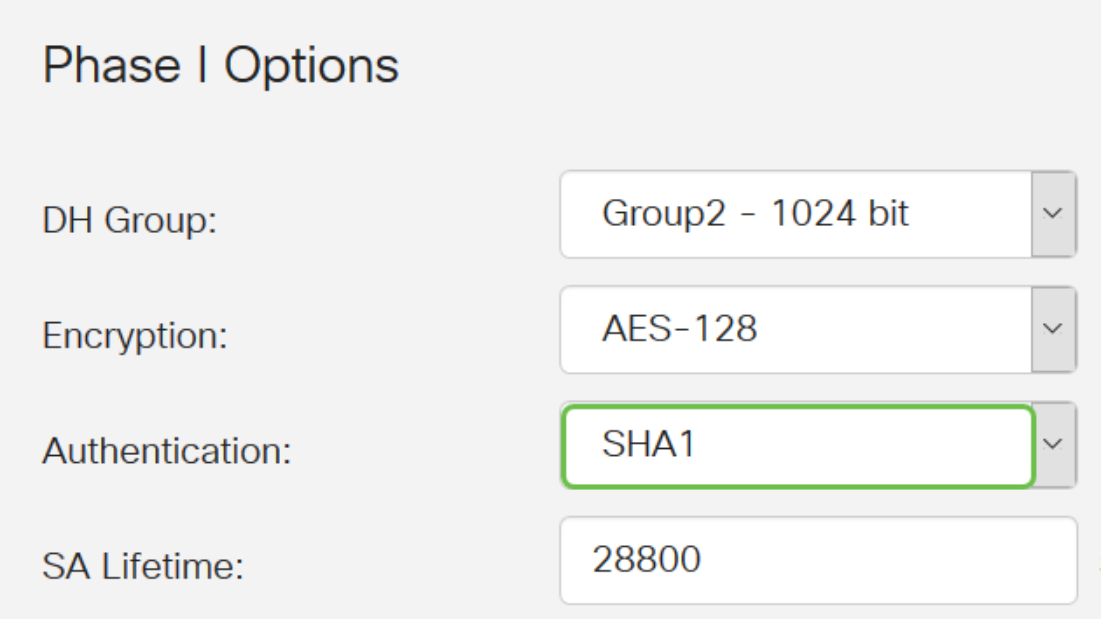
附註：AES是使用DES和3DES進行加密的標準方法，因為它具有更高的效能和安全性。延長AES金鑰將增加安全性，但效能會下降。

步驟3.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。這是最安全和推薦的演算法。

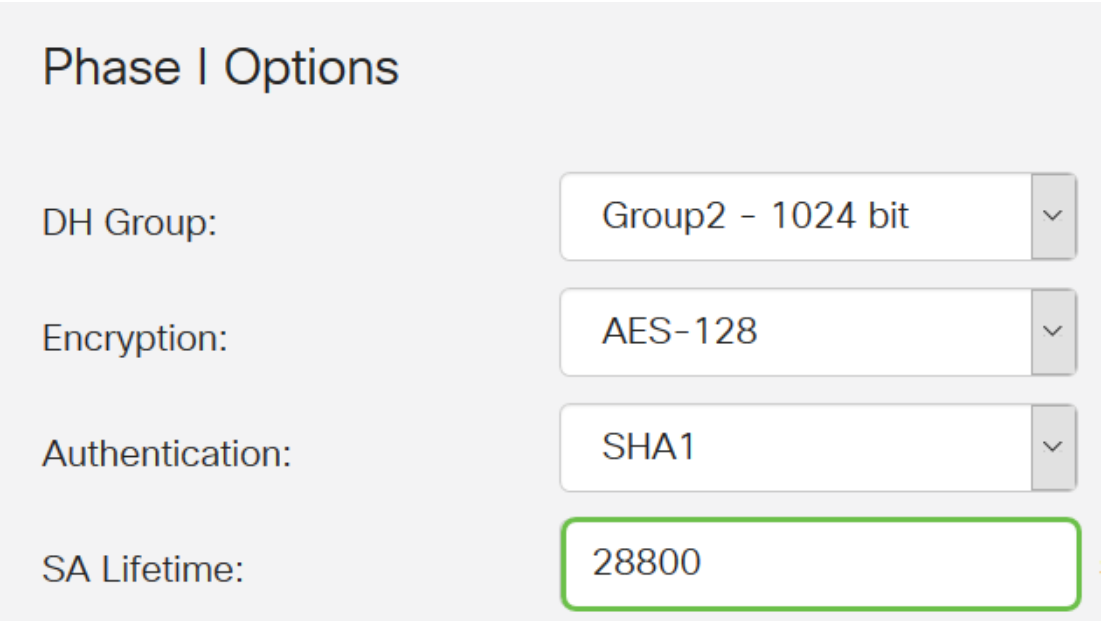
附註：確保VPN隧道的兩端使用相同的身份驗證方法。



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。預設值為28800。*SA Lifetime(Sec)*會告訴您在此階段中IKE SA處於活動狀態的時間量（以秒為單位）。在生存期到期之前協商新的安全關聯(SA)，以確保在舊的SA到期時可以使用新的SA。預設值為28800，範圍為120到86400。我們將使用28800秒作為階段I的SA生存期。

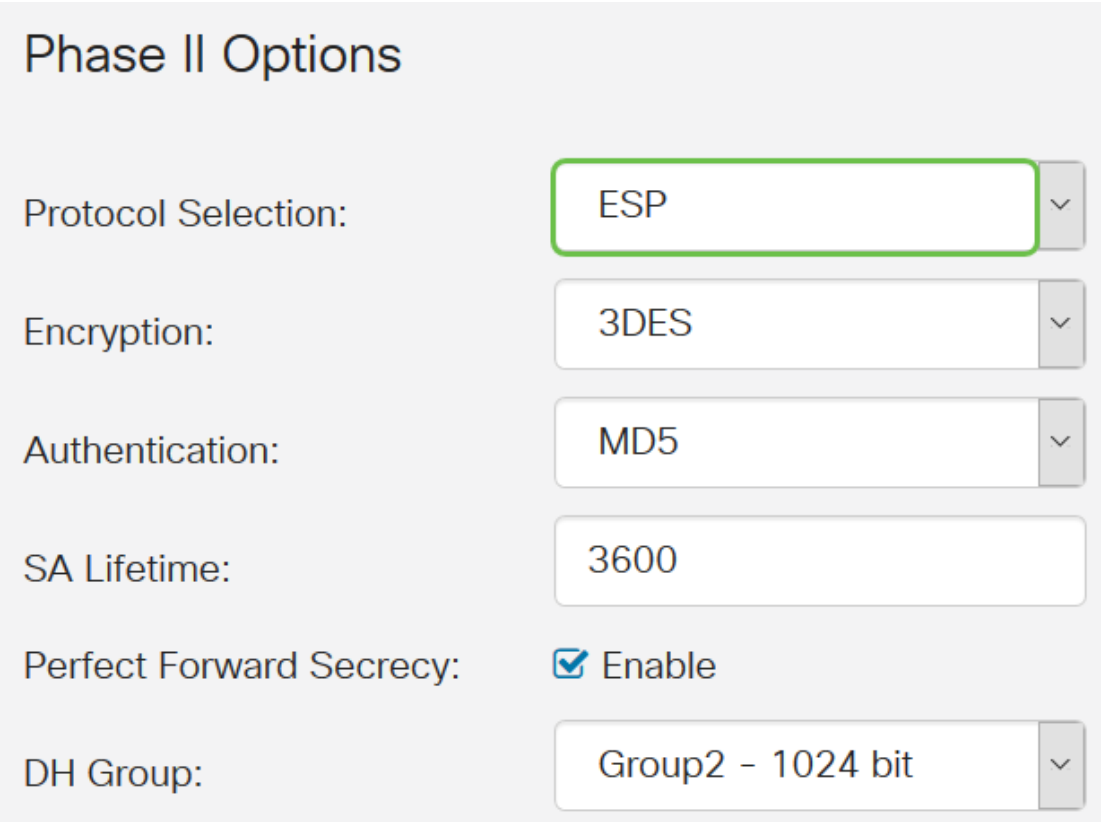
附註：建議您在階段I的SA生存時間長於階段II SA生存時間。如果您使第I階段比第II階段短，那麼您將不得不頻繁地來回重新協商隧道，而不是資料隧道。資料隧道需要更高的安全性，因此最好在II階段具有比I階段更短的生存期。



步驟5.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：

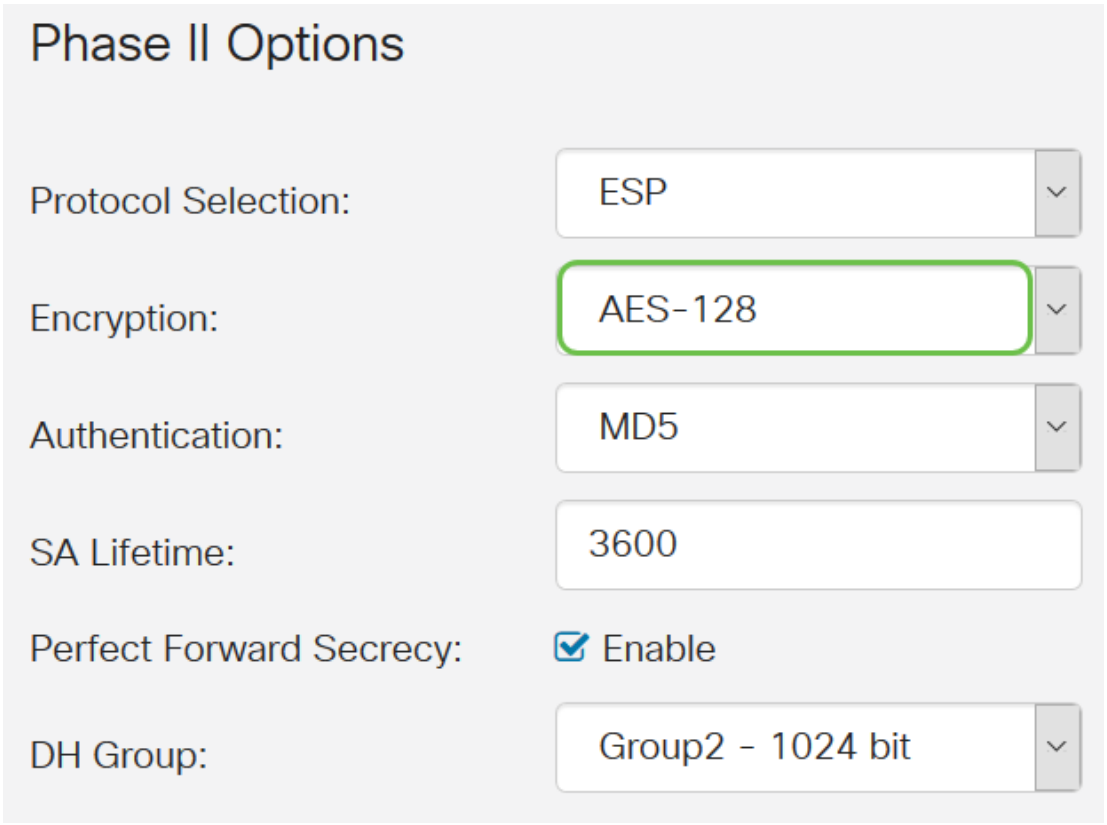
- ESP — 此選項也稱為封裝安全負載。此選項封裝要保護的資料。如果選擇此選項，請繼續執行步驟6以選擇加密方法。

- 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7。



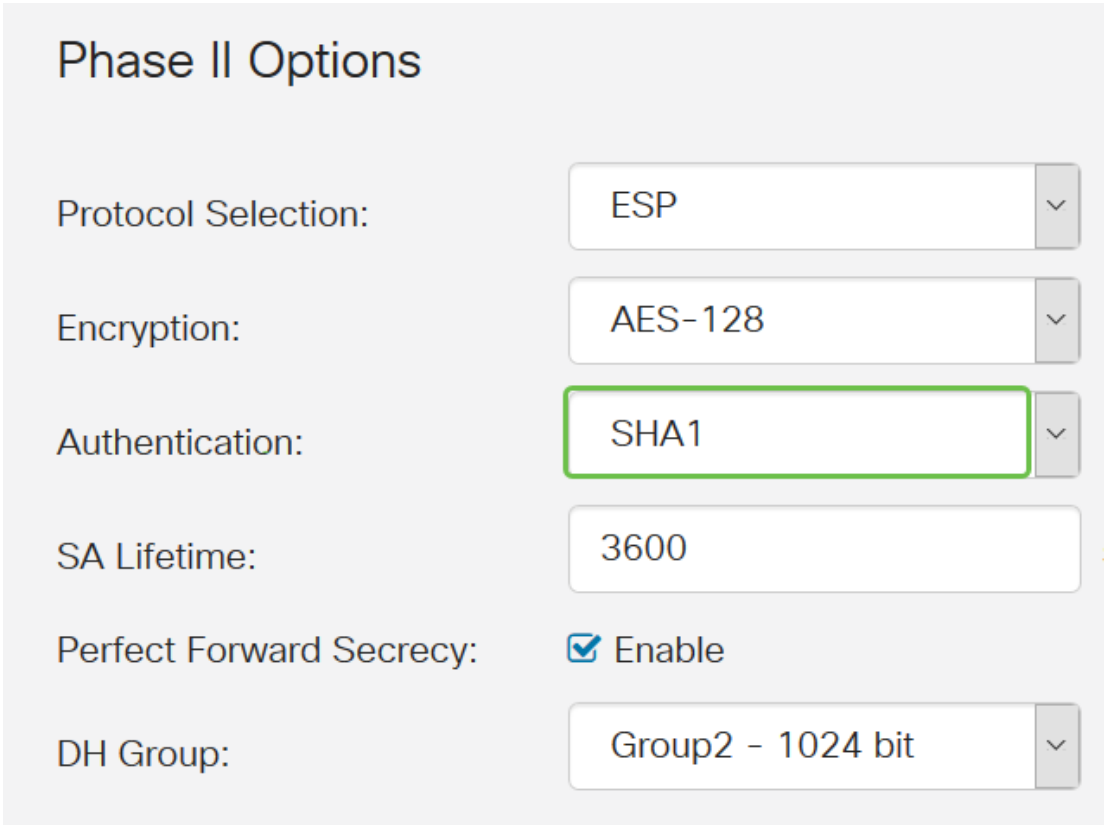
步驟6.如果在步驟6中選擇了ESP，請選擇*Encryption*。選項包括：

- 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。

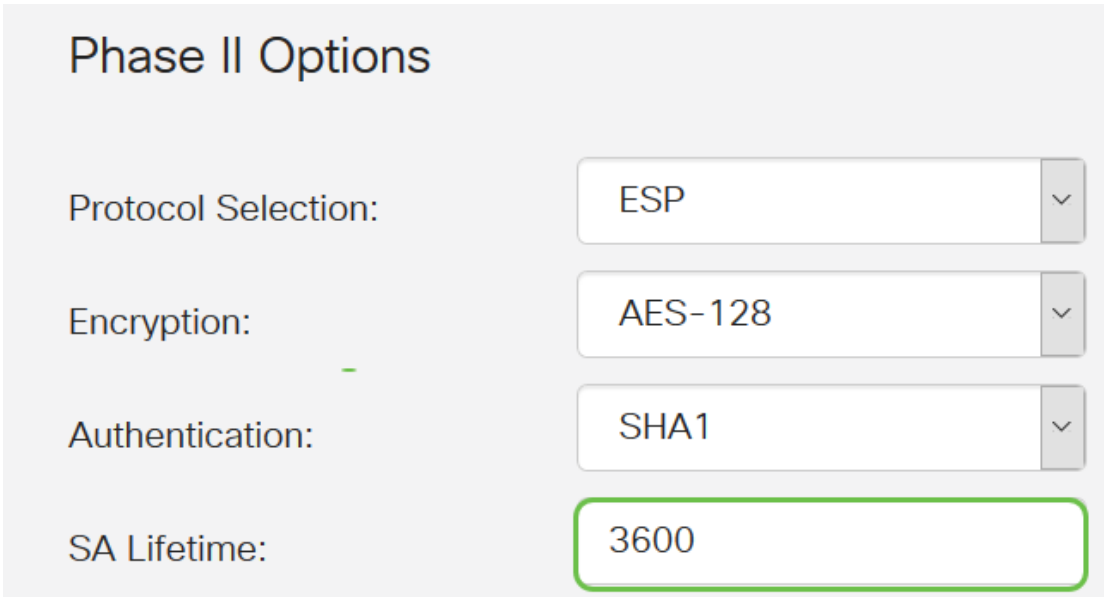


步驟7.從*Authentication*下拉選單中，選擇一種將確定ESP和ISAKMP身份驗證方式的身份驗證方法。選項包括：

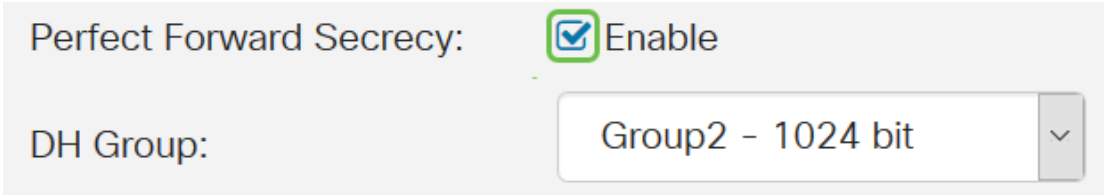
- MD5 — 消息摘要演算法具有128位雜湊值。
- SHA-1 — 安全雜湊演算法具有160位雜湊值。
- SHA2-256 — 具有256位雜湊值的安全雜湊演算法。



步驟8.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。

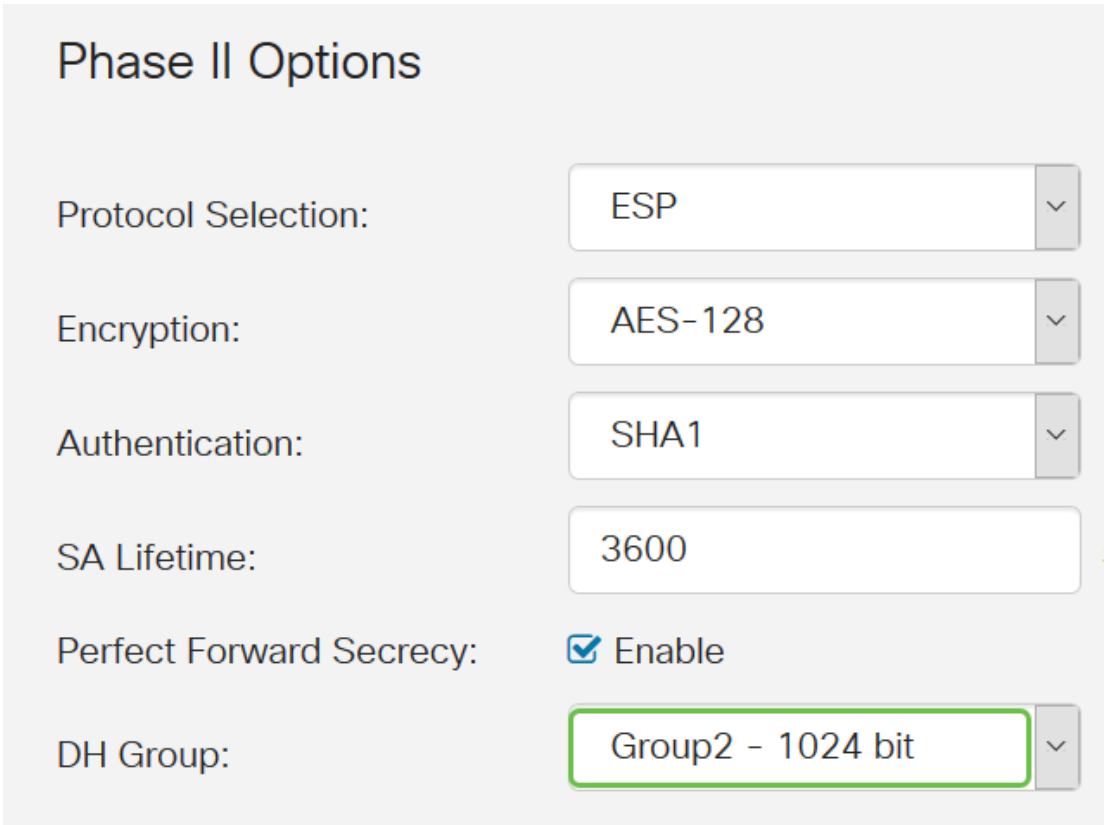


步驟9.（可選）選中**Enable** Perfect Forward Secrecy覈取方塊以生成IPsec流量加密和身份驗證的新金鑰。完全轉發保密技術用於使用公鑰密碼技術提高通過網際網路傳輸的通訊的安全性。選中此框以啟用此功能，或取消選中此框以禁用此功能。建議使用此功能。

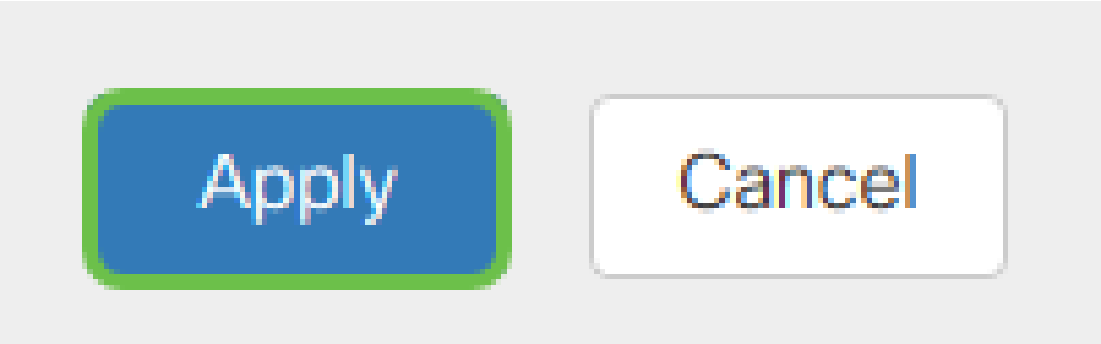


步驟10.從*DH Group*下拉選單中，選擇要與階段2中的金鑰一起使用的DH組。選項包括：

- Group2-1024位 — 此選項計算金鑰更快，但安全性較低。
- Group5-1536位 — 此選項計算金鑰最慢，但最安全。

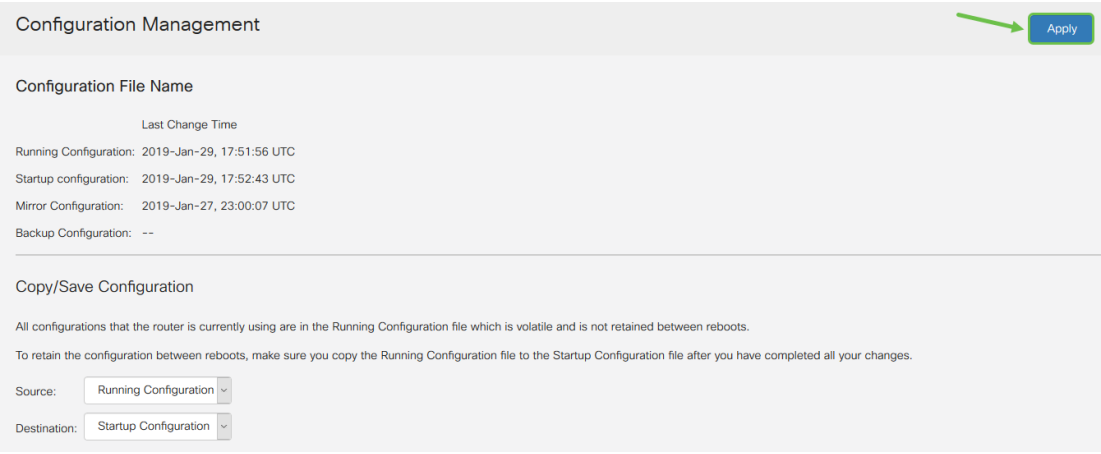


步驟11.按一下**Apply**。

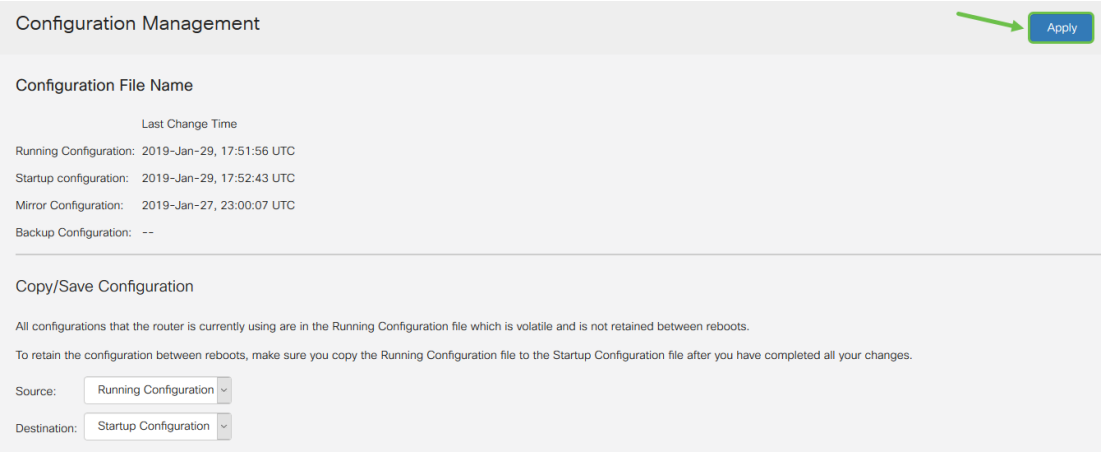


步驟12.按一下**Save**以永久儲存組態。

步驟13.再次按一下**Apply**，將執行組態儲存到啟動組態。



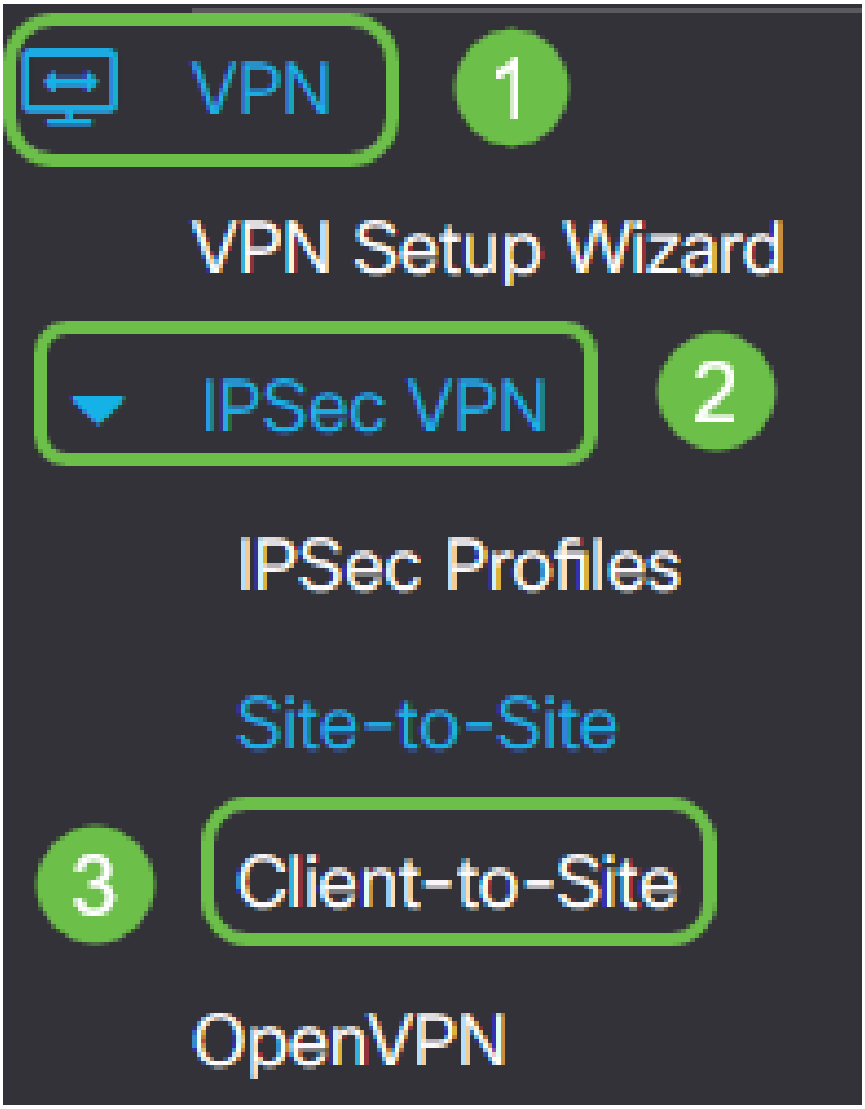
步驟14.收到確認資訊後，按一下**OK**。



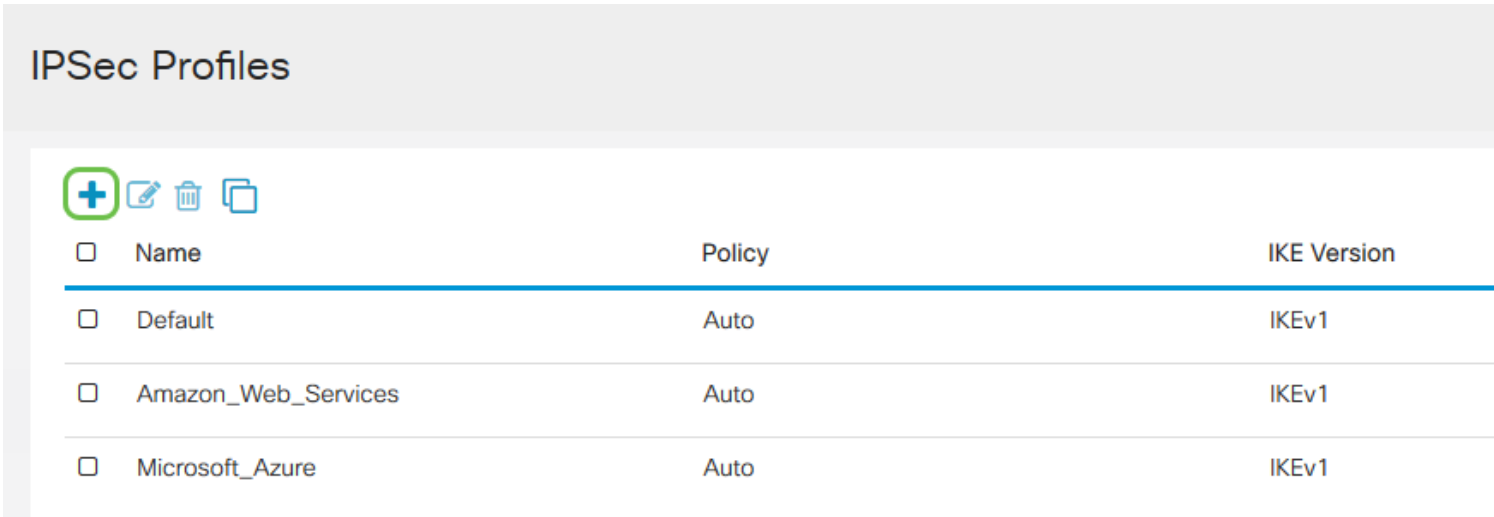
現在，您應該已經在RV160或RV260路由器上成功配置了IPsec配置檔案。

建立客戶端到站點配置檔案

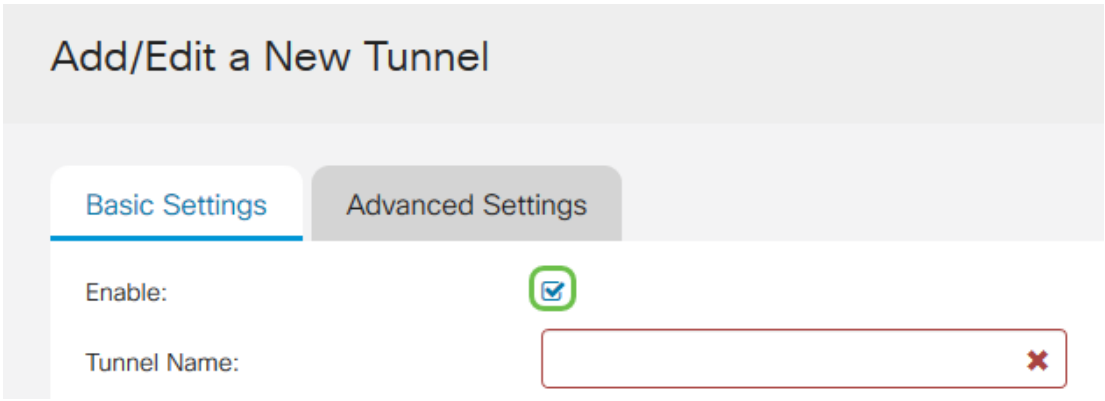
步驟1.選擇**VPN > IPSec VPN > Client-to-Site**。



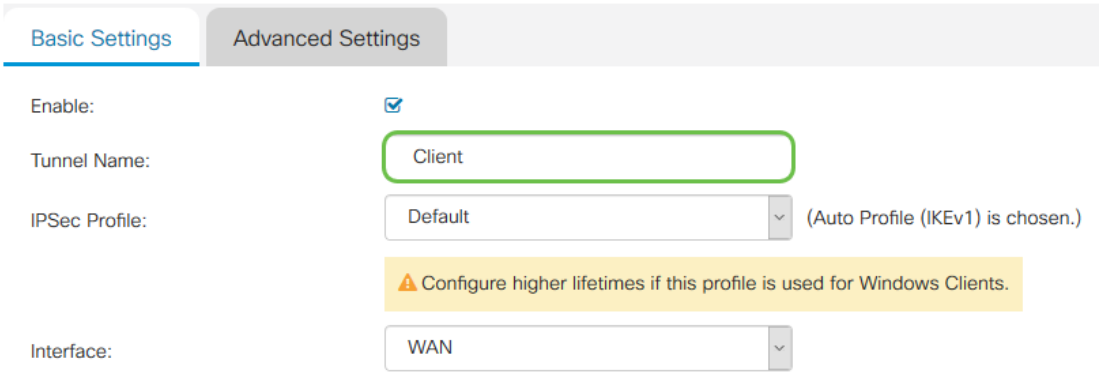
步驟2.按一下**plus**圖示。



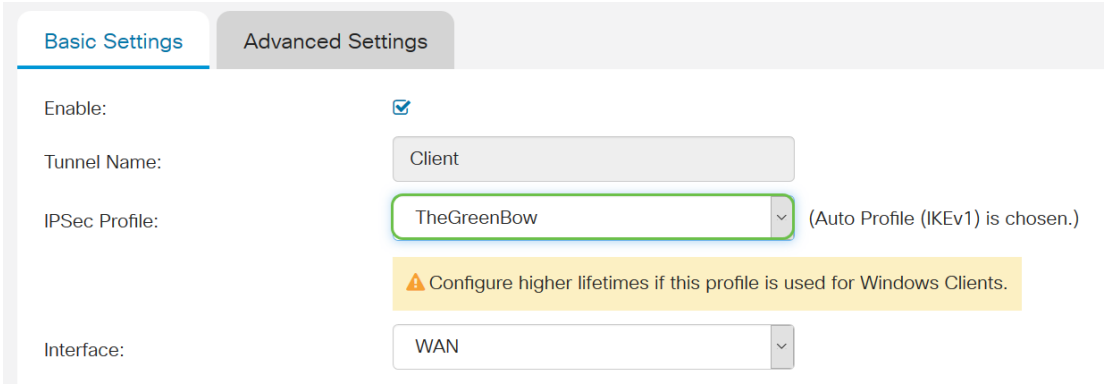
步驟3.在Basic Settings頁籤下，選中**Enable**覈取方塊以確保VPN配置檔案處於活動狀態。



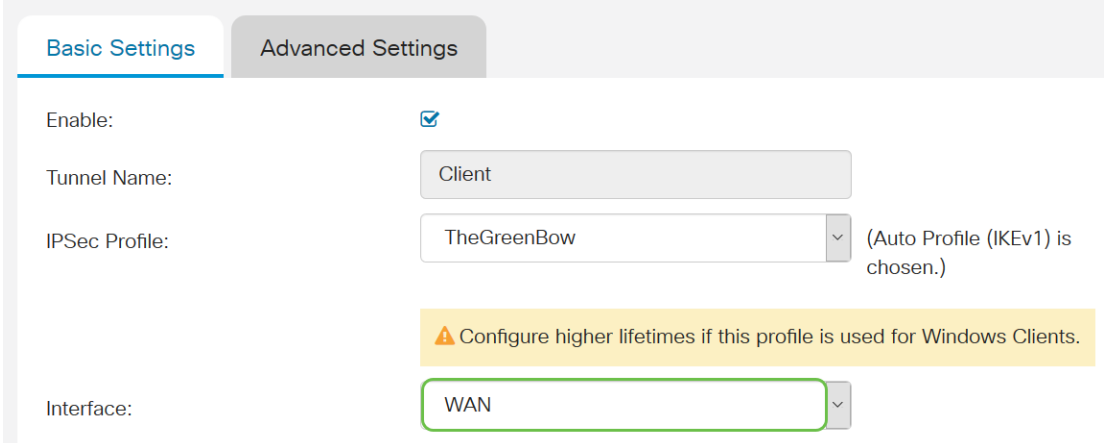
步驟4.在*Tunnel Name*欄位中輸入VPN連線的名稱。



步驟5.從*IPsec*下拉選單選擇要使用的IPsec配置檔案。



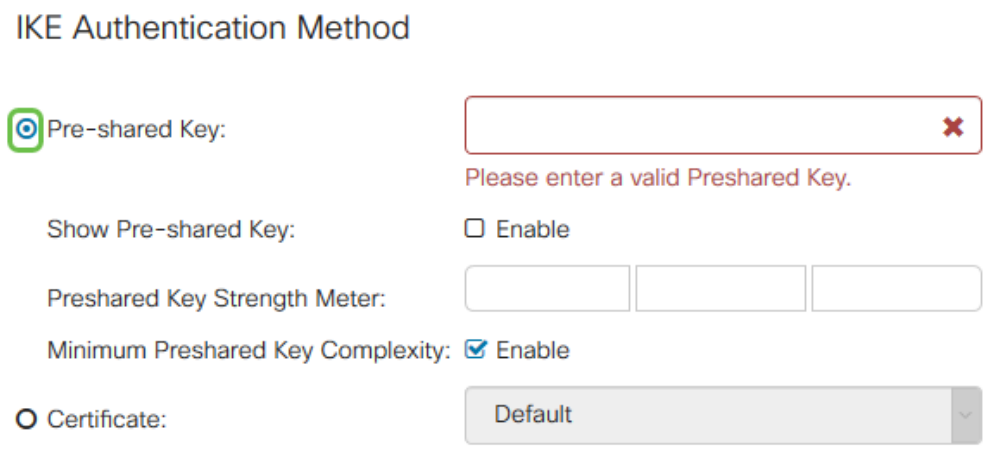
步驟6.從*Interface*下拉式清單中選擇Interface。



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WAN。

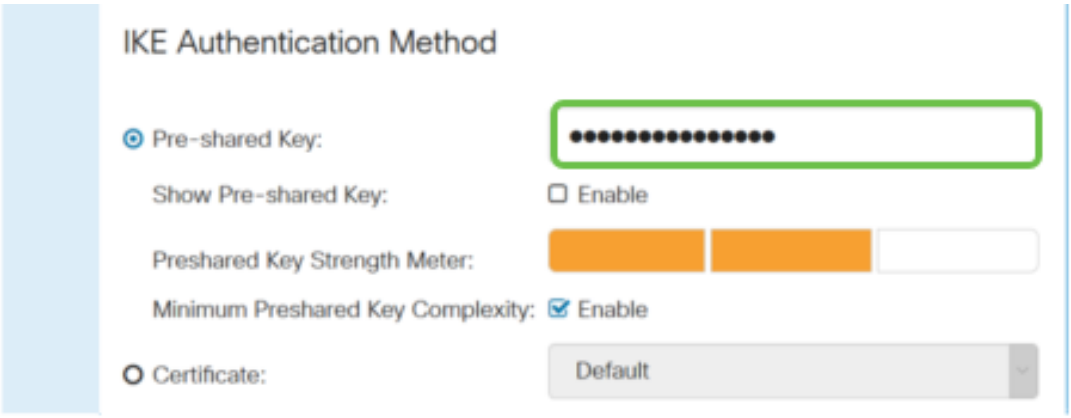
步驟7.選擇IKE身份驗證方法。選項包括：

- Pre-shared 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。

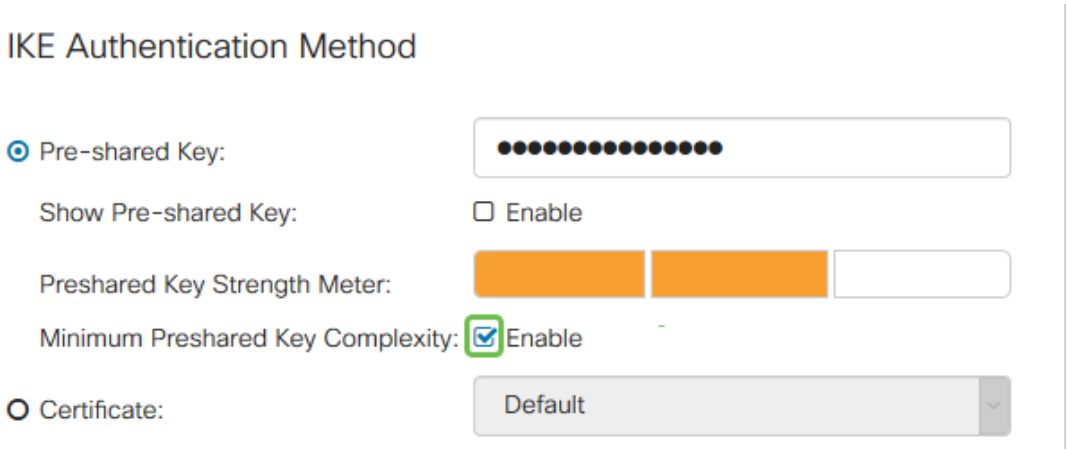


附註：預共用金鑰可以是任何您想要的金鑰，只要在站點和客戶端在其電腦上設定TheGreenBow客戶端時匹配即可。

步驟8.在*Pre-shared Key*欄位中輸入連線密碼。

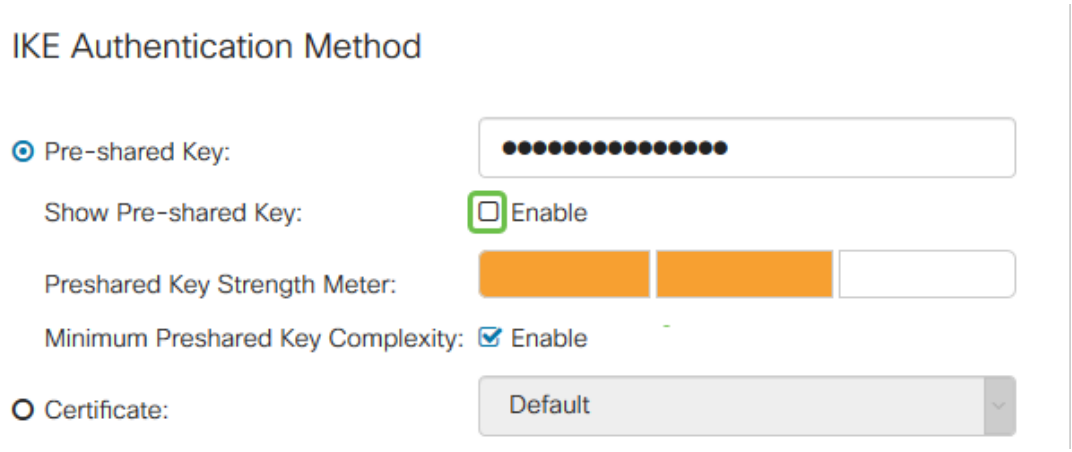


步驟9.（可選）取消選中*Minimum Pre-shared Key Complexity* **Enable**覈取方塊以能夠使用簡單密碼。



附註：在此示例中，保留啟用最小預共用金鑰複雜性。

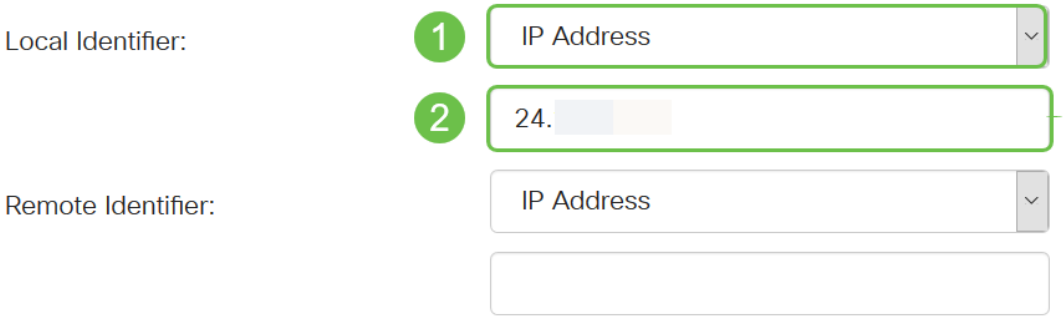
步驟10。（可選）選中*Show Pre-shared Key* **Enable**覈取方塊以純文字檔案顯示密碼。



附註：在此示例中，Show Pre-shared key處於禁用狀態。

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。這是站點（辦公室）的路由器的WAN 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。

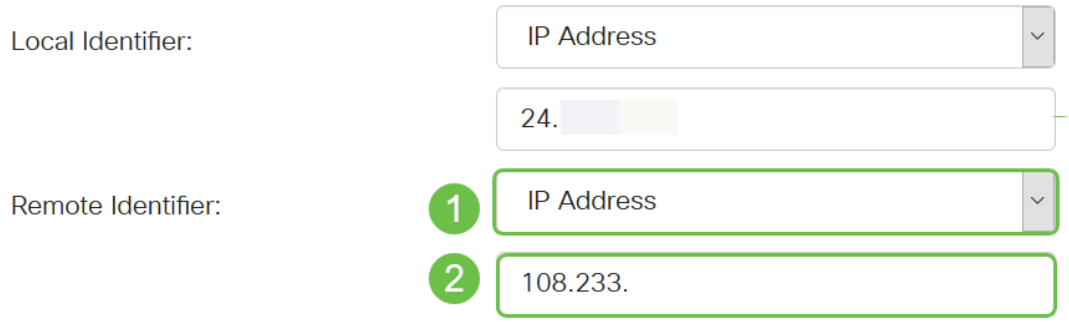


附註：在本示例中，選擇IP地址並輸入站點路由器的WAN IP地址。在本示例中，已輸入24.x.x.x。出於隱私目的，完整地址已模糊。

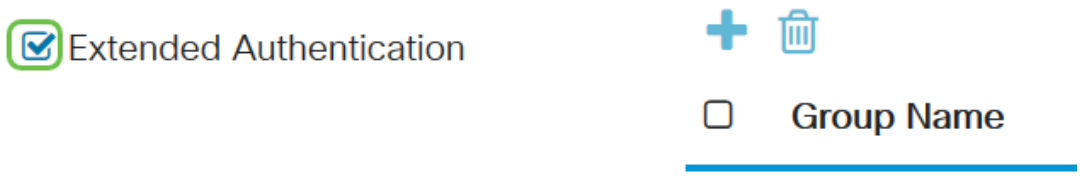
步驟12.選擇遠端主機的識別符號。選項包括：

- IP地址 — 此選項使用VPN客戶端的WAN IP地址。要查詢WAN IP地址，您可以在網路瀏覽器中輸入「我的IP是什麼」。這是客戶端IP地址。
- FQDN — 完全限定的域名。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。

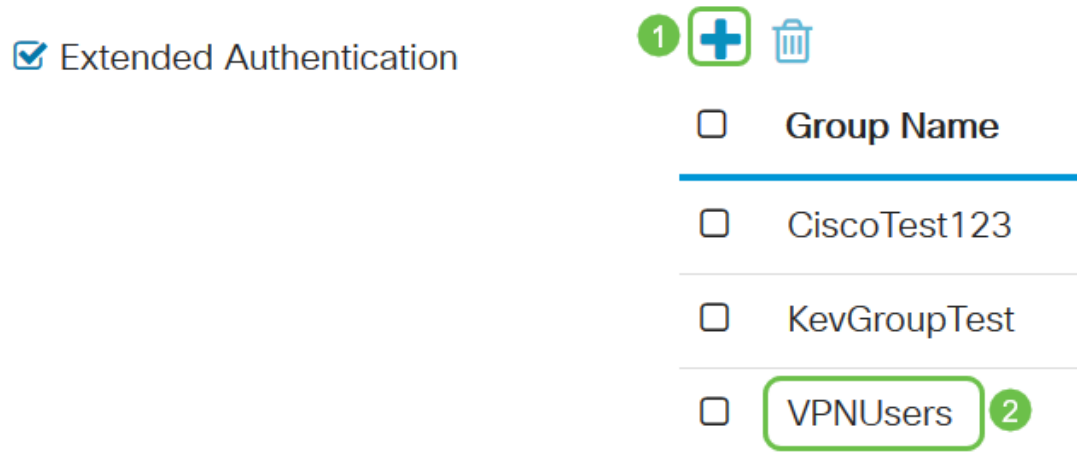
附註：在本例中，選擇IP地址，並輸入客戶端所在位置的路由器的當前IPv4地址。這可以通過在Web瀏覽器中搜尋「我的IP地址是什麼」來確定。此地址可以更改，因此，如果在配置成功後連線時出現問題，則此區域可以在客戶端和站點上檢查並更改。



步驟13。（可選）勾選**Extended Authentication**覈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。



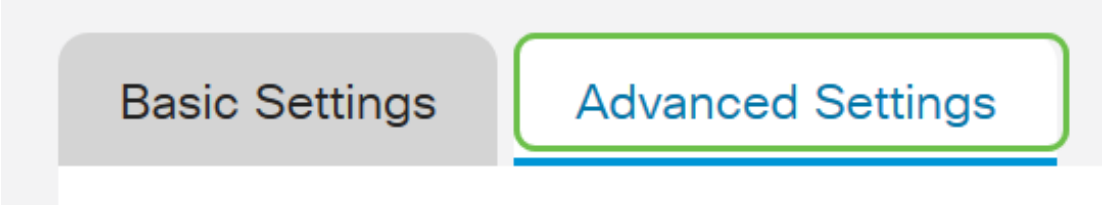
步驟14。（可選）通過按一下**plus**圖示並從下拉選單中選擇使用者，選擇將使用擴展身份驗證的組。



附註：在本示例中，選擇了**VPNUsers**。

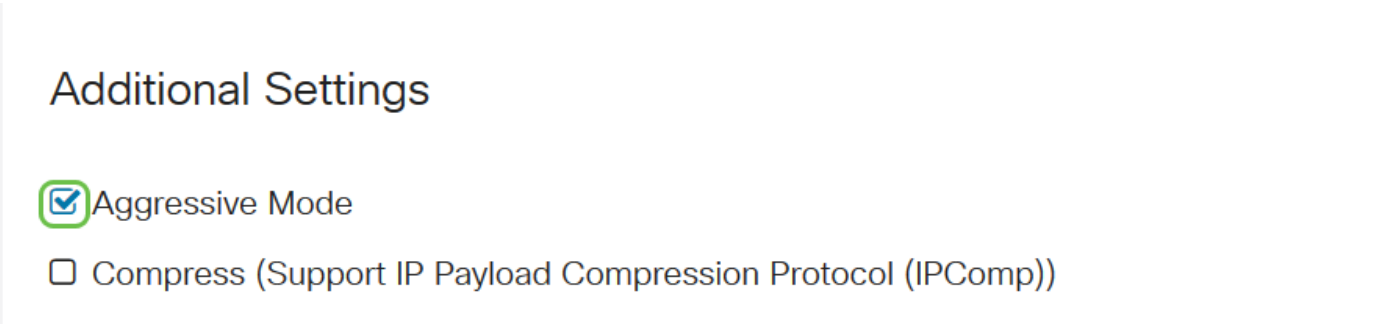
步驟15.在*Pool Range for Client LAN*下，輸入可以分配給VPN客戶端的第一個IP地址和結束IP地址。這需要一個與站點地址不重疊的地址池。這些介面可稱為虛擬介面。如果您收到需要更改虛擬介面的消息，則可以在此進行修復。

步驟16.選擇**Advanced Settings選項**卡。



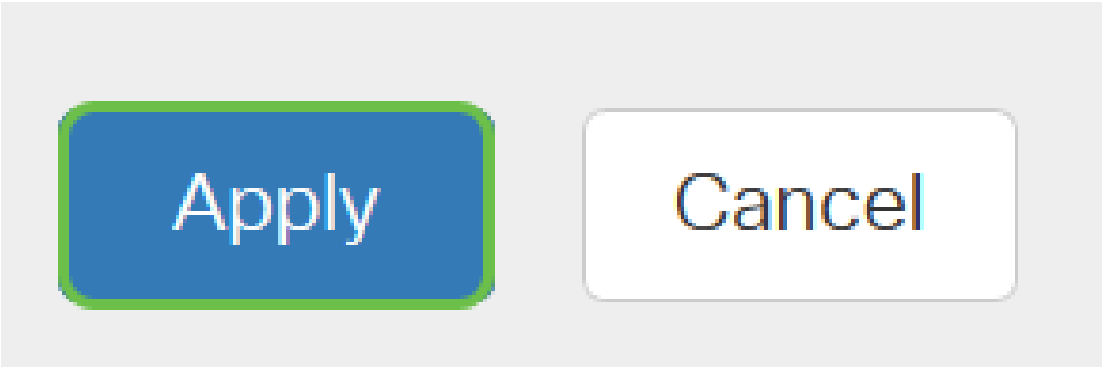
步驟17。（可選）向下滾動到頁面底部，然後選擇**Aggressive Mode**。主動模式功能可讓您指定

IP安全(IPsec)對等路由器的RADIUS通道屬性，並發起與通道的網際網路金鑰交換(IKE)主動模式協商。有關主動模式與主模式的詳細資訊，請單擊此處。



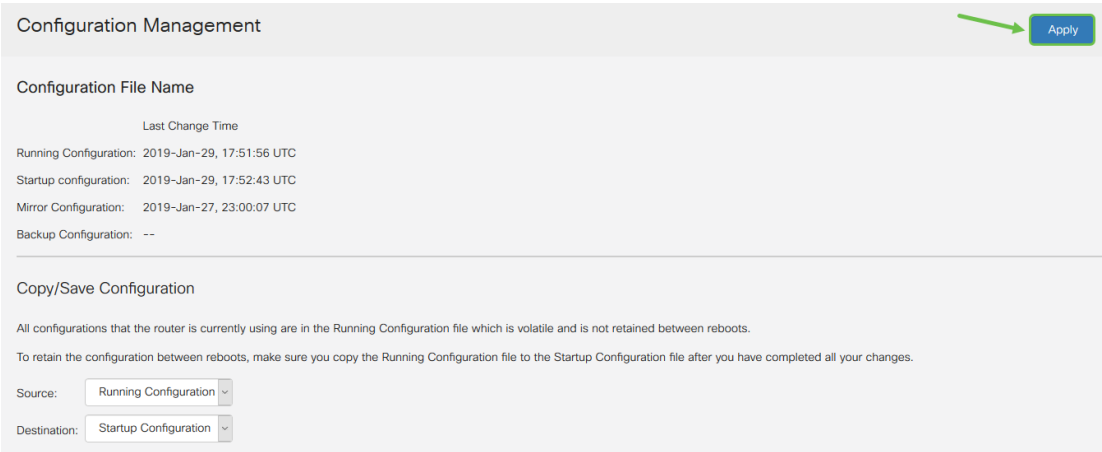
附註：Compress覈取方塊使路由器能夠在啟動連線時提議壓縮。此通訊協定降低IP資料包的大小。如果響應方拒絕此提議，則路由器不會實施壓縮。當路由器是響應方時，它接受壓縮，即使未啟用壓縮。如果為此路由器啟用此功能，則需要在遠端路由器（隧道的另一端）上啟用它。 在本示例中，未選中*Compress*。

步驟18.按一下**Apply**。



步驟19.按一下「**Save**」。

步驟20.再次按一下**Apply**，將執行組態儲存到啟動組態。



步驟21.收到確認資訊後，按一下**OK**。

現在，您應該已經在路由器上為TheGreenBow VPN客戶端配置了客戶端到站點隧道。

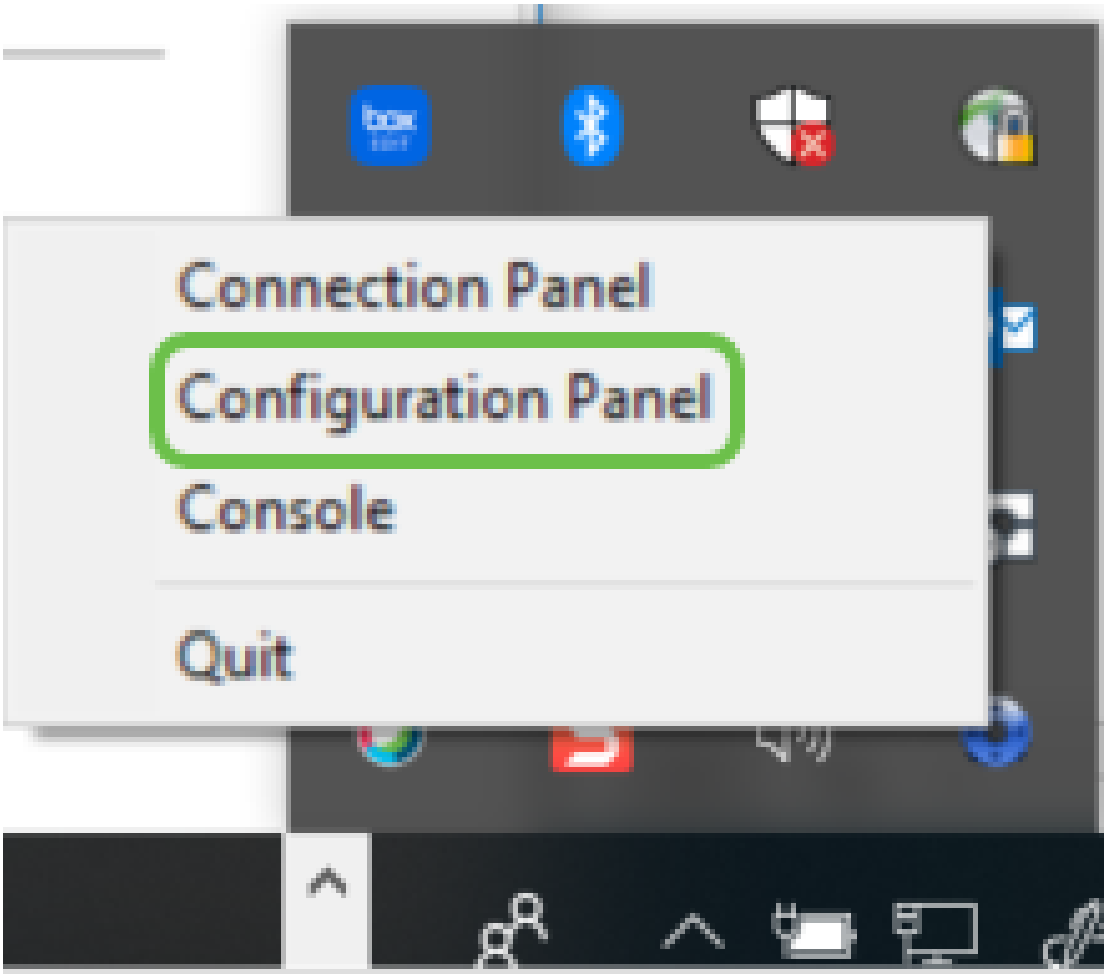
在遠端工作人員的電腦上配置GreenBow VPN客戶端

配置階段1設定

要下載最新版本的TheGreenBow IPsec VPN客戶端軟體，請按一下此處。

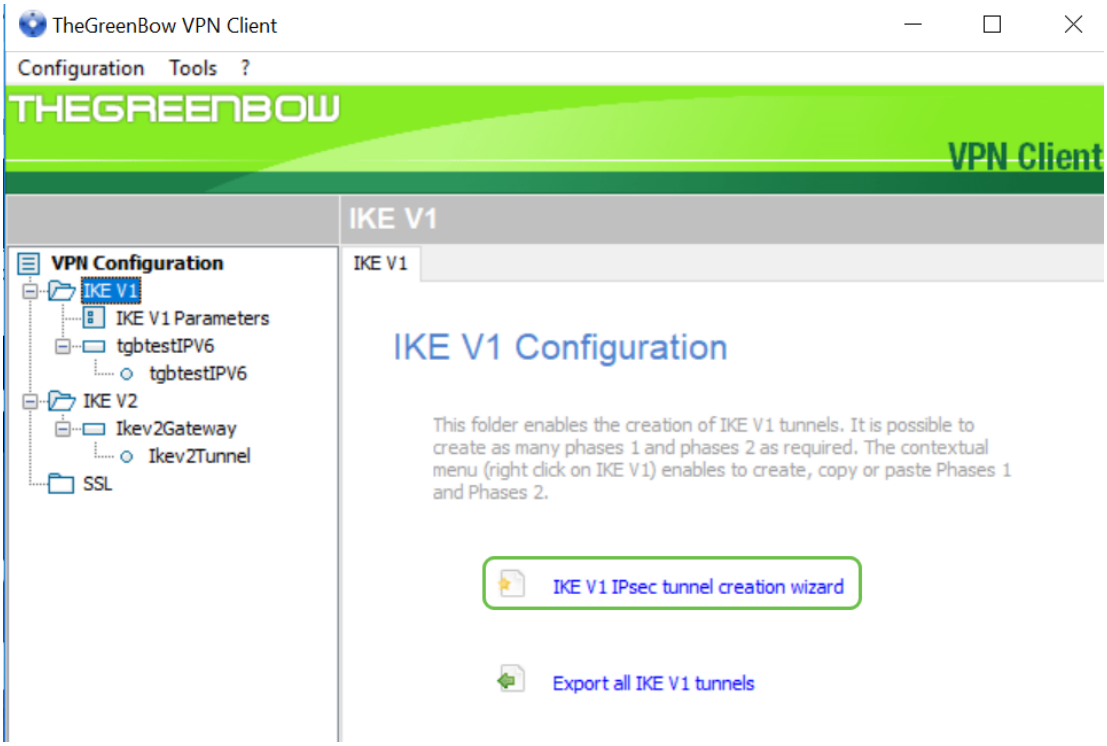
步驟1.按一下右鍵GreenBow VPN客戶端圖示。位於工作列的右下角。

步驟2.選擇Configuration Panel。



附註：以下是Windows電腦上的示例。視您使用的軟體而定。

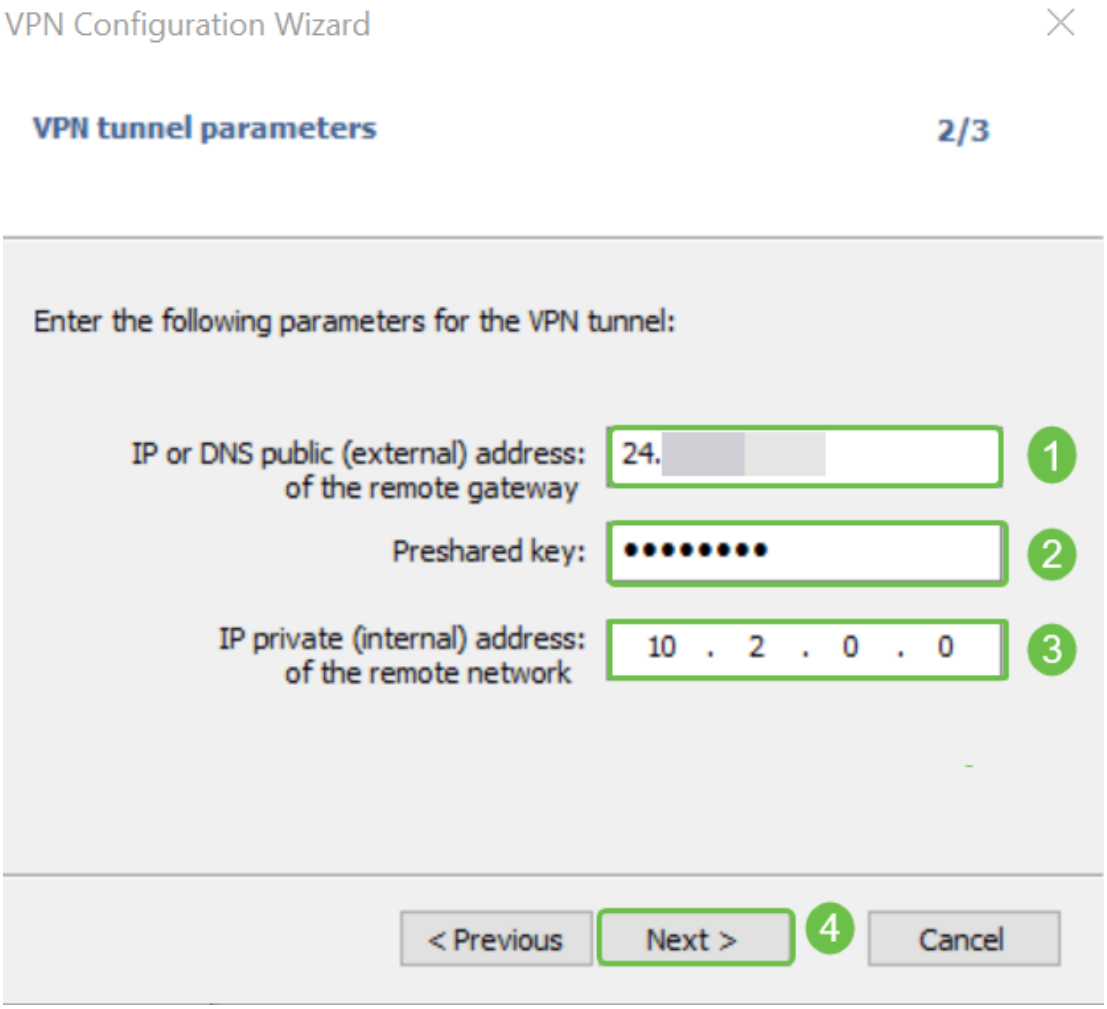
步驟3.選擇**IKE V1 IPsec隧道建立嚮導**。



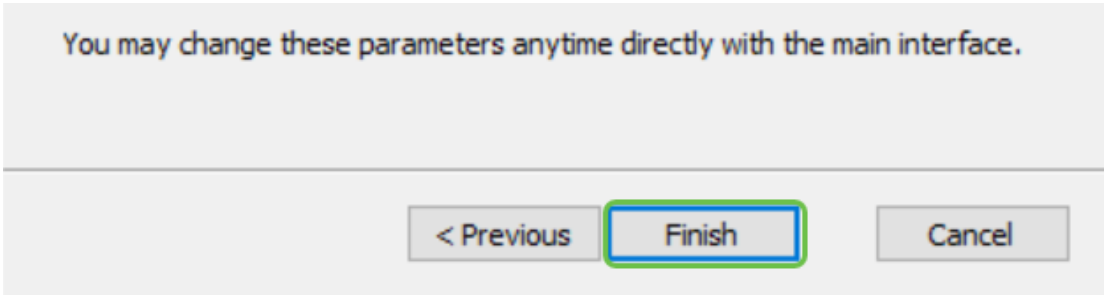
附註：在此示例中，正在配置IKE版本1。如果要配置IKE版本2，請按照相同的步驟操作，但按一下右鍵IKE V2資料夾。您還需要為站點路由器上的IPsec配置檔案選擇IKEv2。

步驟4.填寫檔案伺服器所在站點（辦公室）的路由器的公用WAN IP地址、預共用金鑰以及站點上遠端網路的專用內部地址。按「**Next**」（下一步）。在本示例中，站點為24.x.x.x。為保護此網路，最

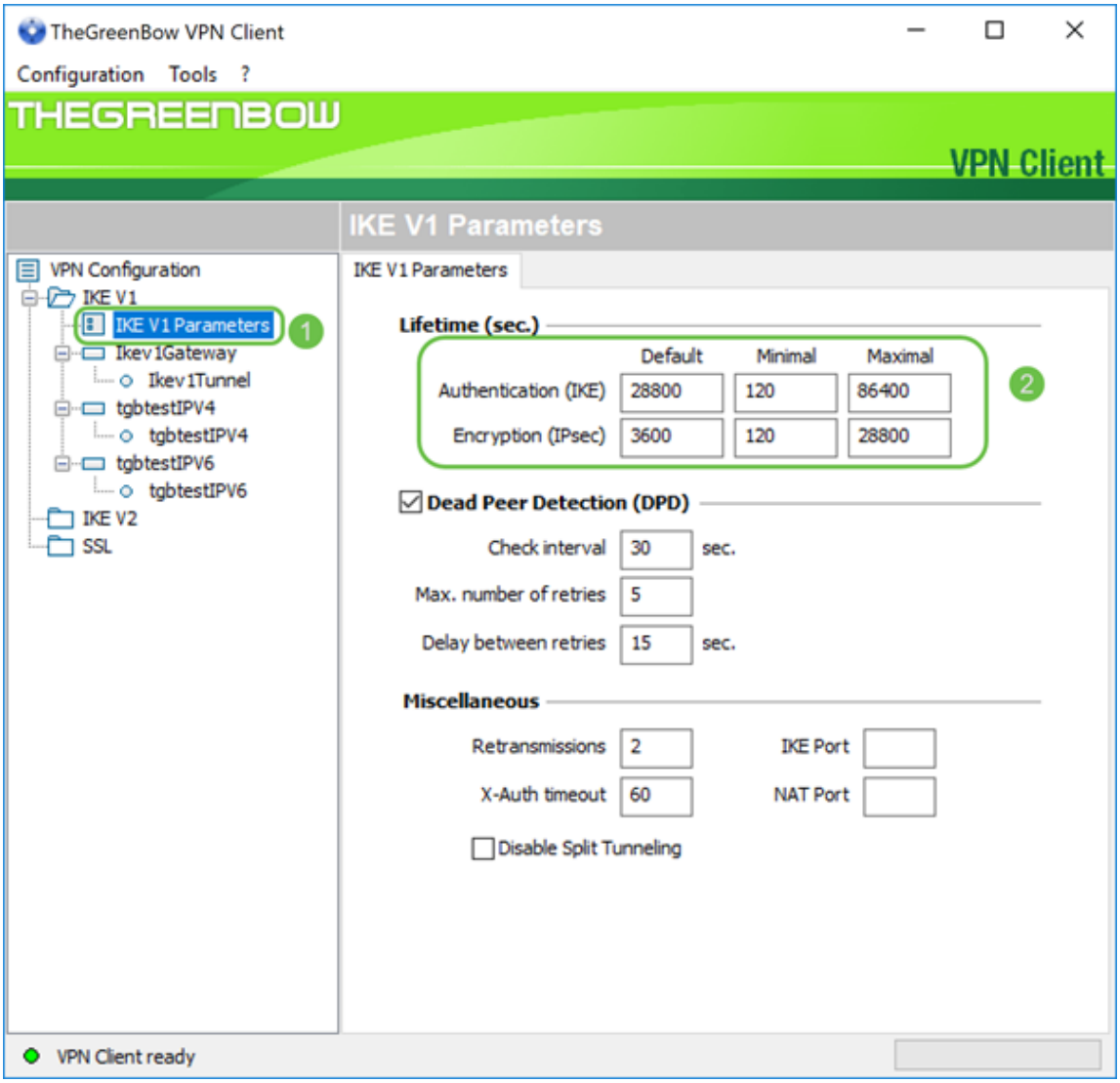
後三個八位組（此IP地址中的一組數字）已替換為x。輸入完整的IP地址。



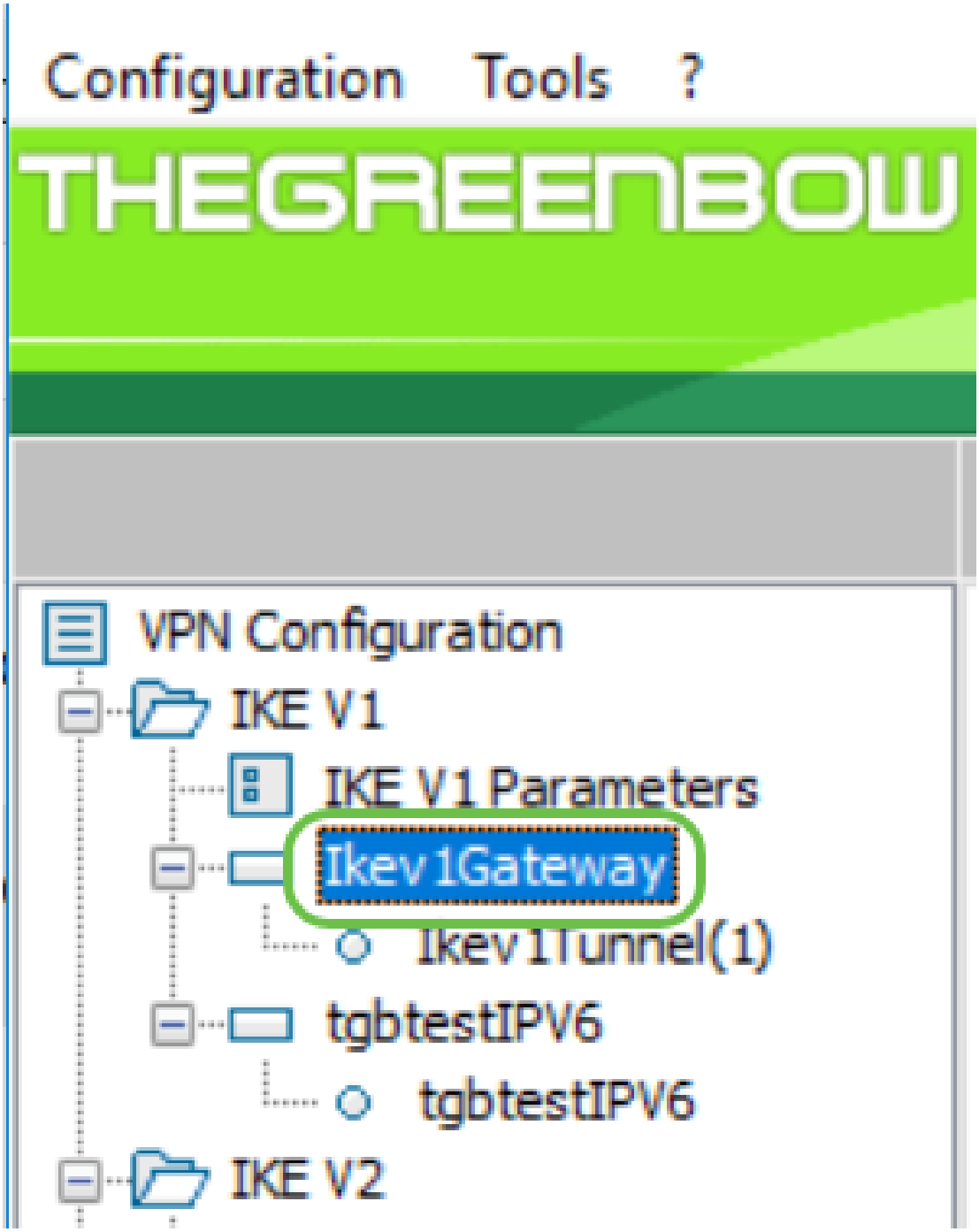
步驟5.按一下「Finish」。



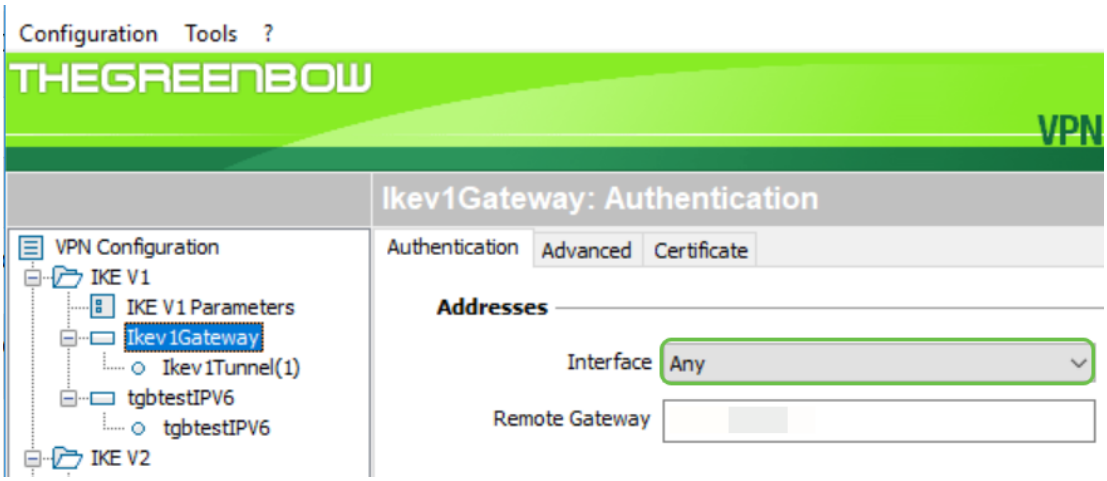
第6步（可選）您可以更改IKE V1引數。可以調整GreenBow預設值、最小和最大壽命。在此位置，您可以輸入路由器接受的壽命範圍。



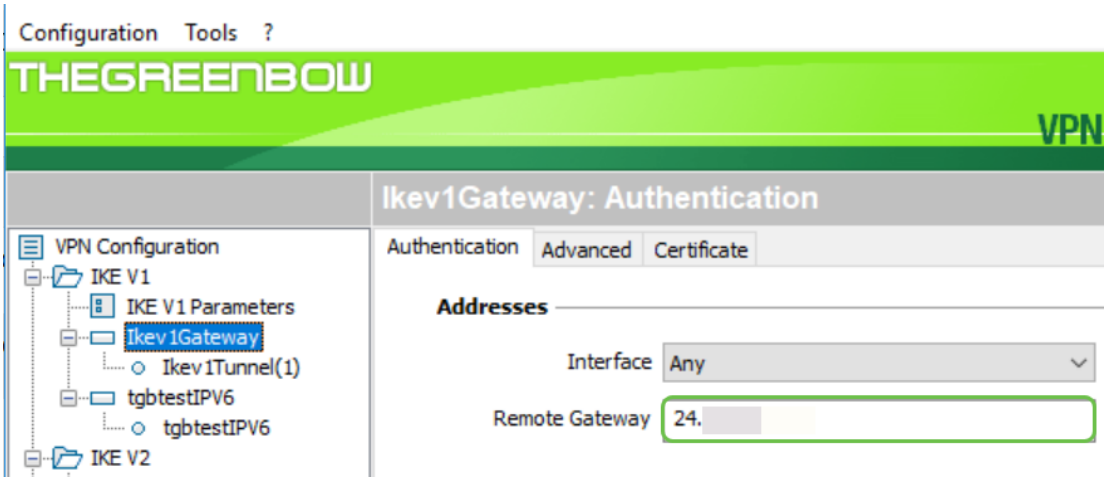
步驟7.按一下您建立的網關。



步驟8.在*Addresses*下的*Authentication*頁籤中，您將看到本地地址的下拉選單。您可以選擇一個或選擇**Any**，如下所示。

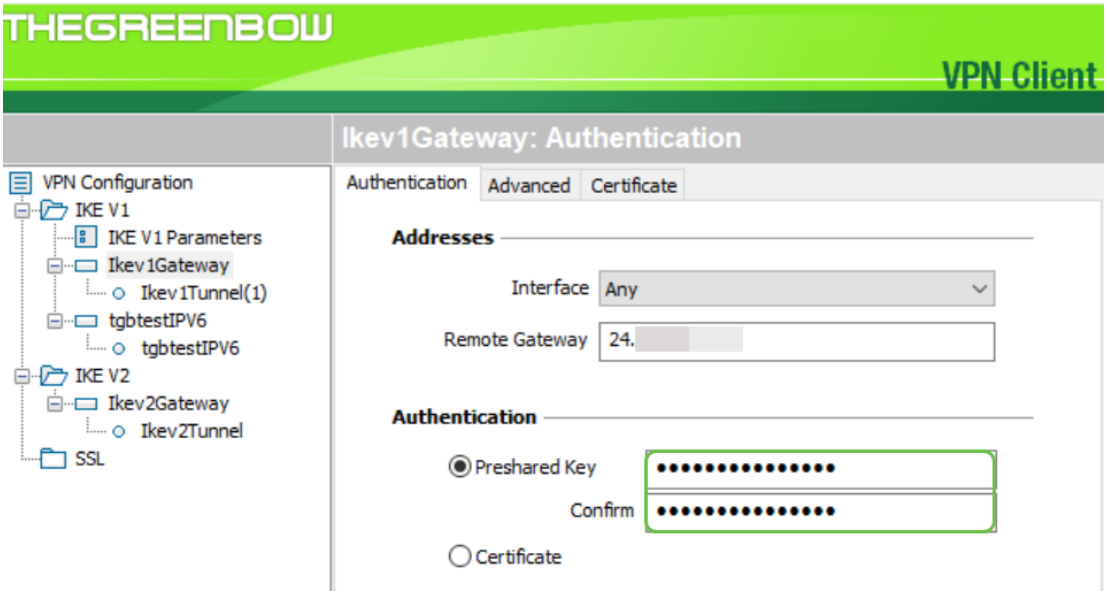


步驟9.在*Remote Gateway*欄位中輸入遠端網關的地址。可以是IP地址或DNS名稱。這是站點（辦公室）上路由器的公用IP地址。



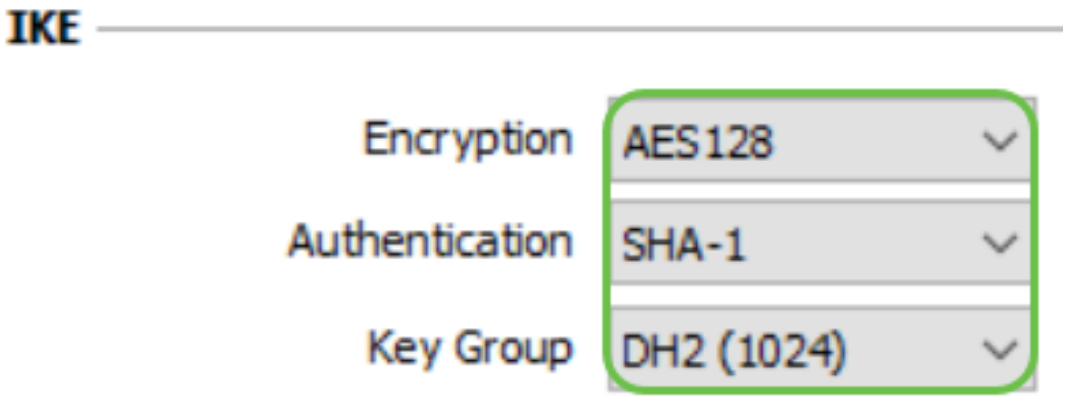
步驟10.在*Authentication*下，選擇身份驗證型別。選項包括：

- 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。

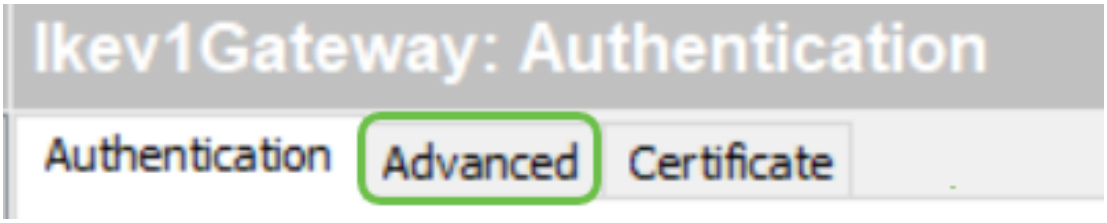


附註：在本示例中，輸入並確認了在路由器上配置的預共用金鑰。

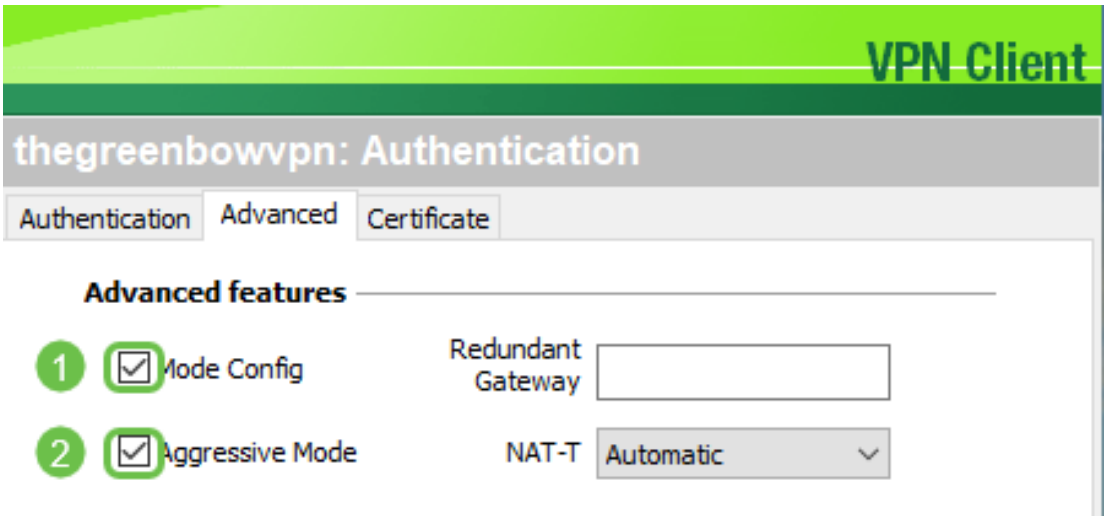
步驟11.在*IKE*下，設定加密、身份驗證和金鑰組設定以匹配路由器的配置。



步驟12.按一下**Advanced**索引標籤。

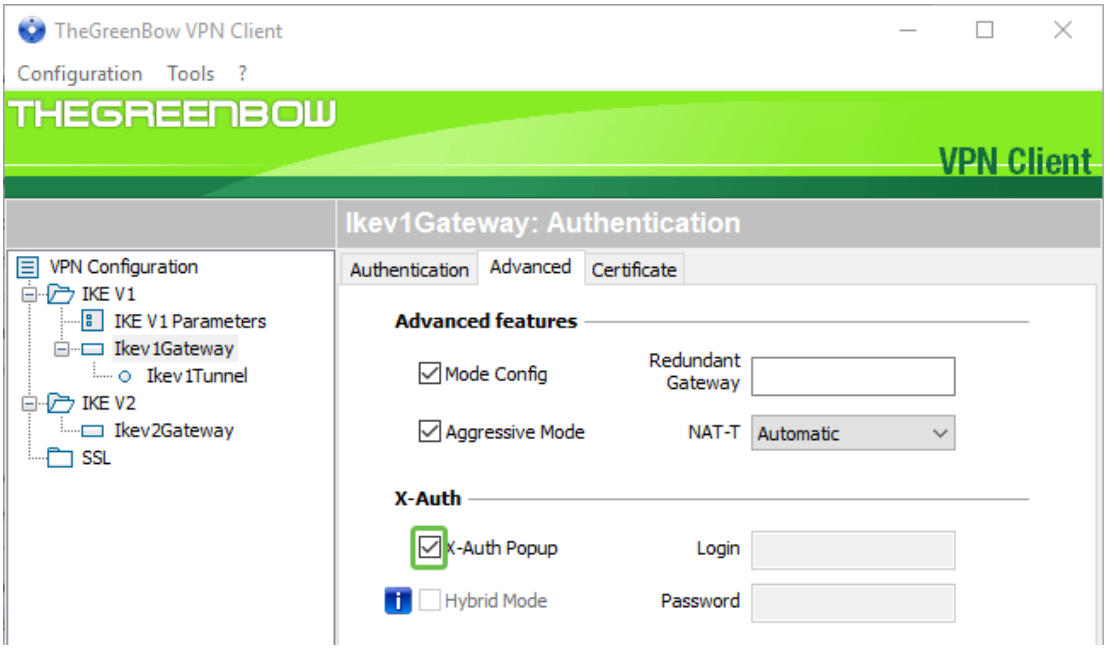


步驟13.在Advanced features下，勾選**Mode Config**和**Aggressive Mode**覈取方塊。在本示例的「客戶端到站點」配置檔案中，在RV160上選擇了「主動模式」。將NAT-T設定保留為「自動」。

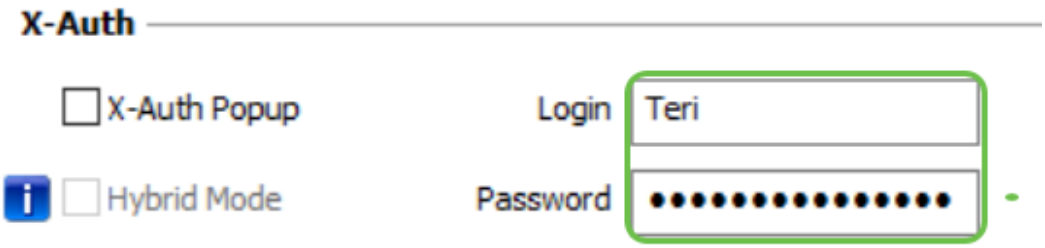


附註：啟用模式配置後，GreenBow VPN客戶端將從VPN網關提取設定以嘗試建立隧道。NAT-T使建立連線更快。

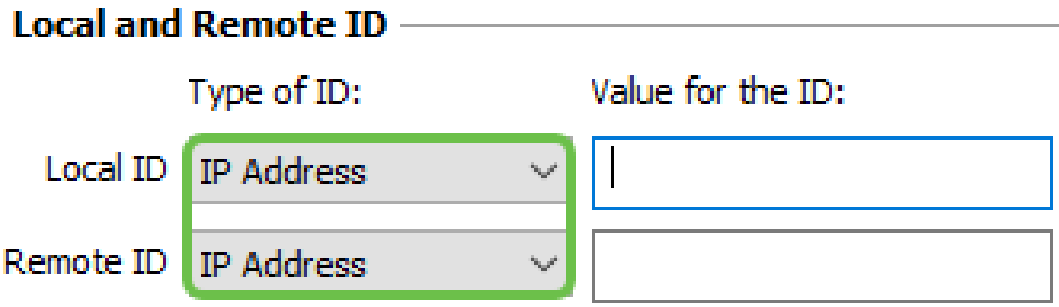
步驟14。（可選）在*X-Auth*下，您可以選中**X-Auth Popup**覈取方塊，以便在啟動連線時自動拉出登入視窗。使用者可在登入視窗輸入其憑證以完成隧道。



步驟15。（可選）如果沒有選擇*X-Auth Popup*，請在*Login*欄位中輸入使用者名稱。這是在VPN網關中建立使用者帳戶時輸入的使用者名稱和站點的密碼。

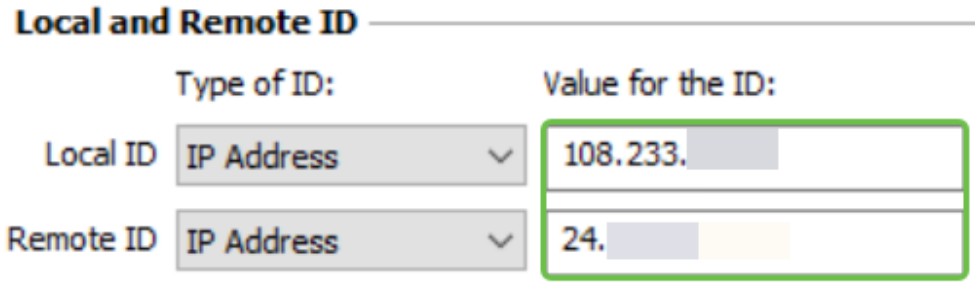


步驟16.在*本地和遠端ID*下，設定本地ID和遠端ID以匹配VPN網關的設定。

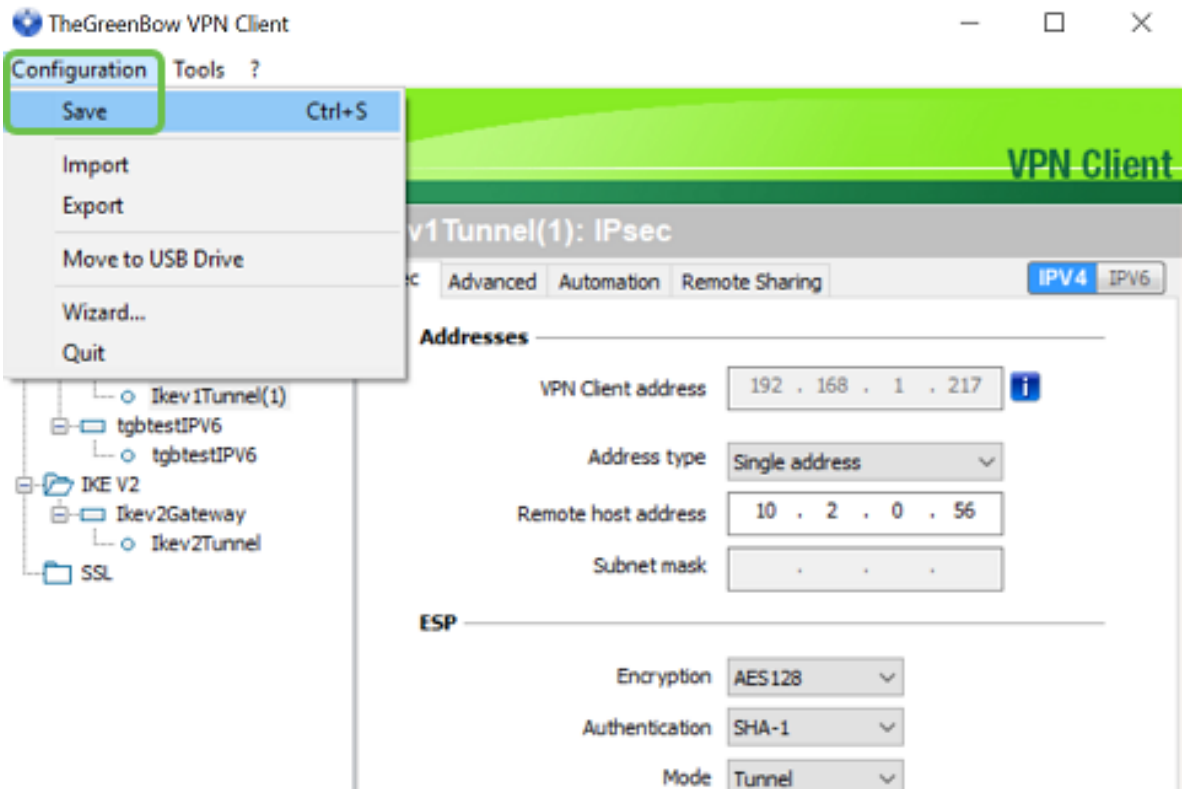


附註：在本示例中，本地ID和遠端ID都設定為IP地址以匹配RV160或RV260 VPN網關的設定。

步驟17.在ID的*值下*，在各自的欄位中輸入本地ID和遠端ID。本地ID是客戶端的WAN IP地址。可通過在Web上搜尋「What's my IP」（我的IP是什麼）來找到此項。遠端ID是站點上路由器的WAN IP地址。

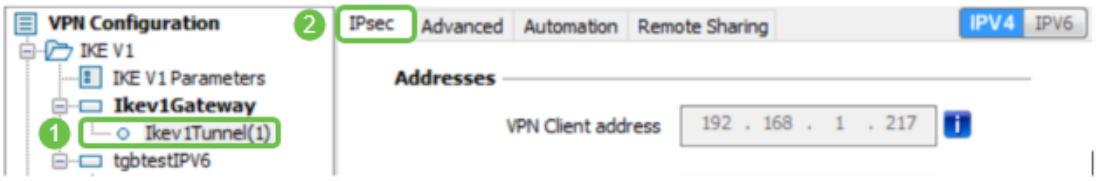


步驟18.按一下**Configuration**，然後選擇**Save**。

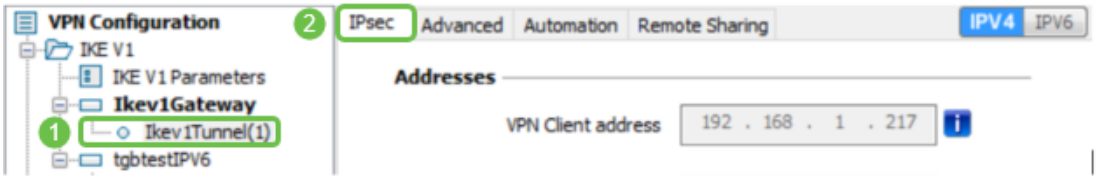


配置隧道設定

步驟1.按一下**IKev1Tunnel(1)**（您的可能有不同名稱）和**IPsec**索引標籤。如果在Ikev1Gateway高級設定中選擇了Mode Config，則會自動填充VPN客戶端地址。這將顯示遠端位置電腦/筆記型電腦的本地IP地址。

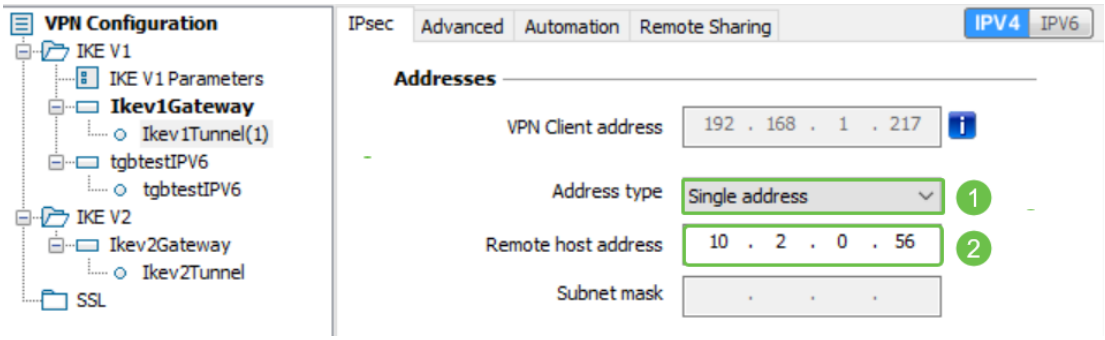


步驟2.從*Address type*下拉選單中選擇VPN客戶端可以訪問的地址型別。可以是單個地址、地址範圍或子網地址。預設子網地址自動包括VPN客戶端地址（電腦的本地IP地址）、遠端LAN地址和子網掩碼。如果選擇單一地址或地址範圍，則需要手動填寫這些欄位。在*Remote LAN address*欄位中輸入應由VPN隧道訪問的網路地址，並在*Subnet mask欄位中輸入遠端網路的子*掩碼。

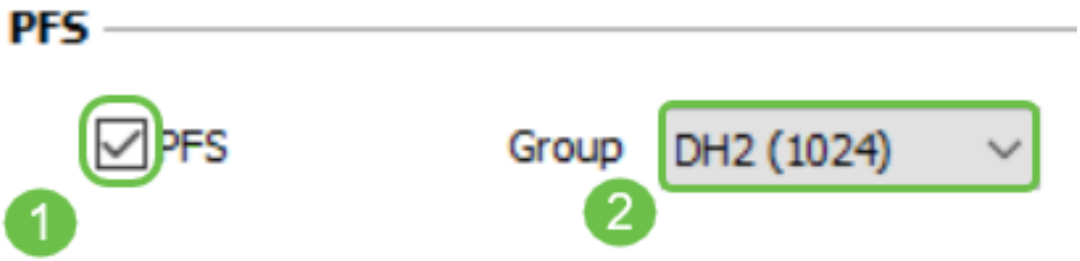


附註：在本例中，選擇了單個地址並輸入了站點路由器的本地IP地址。

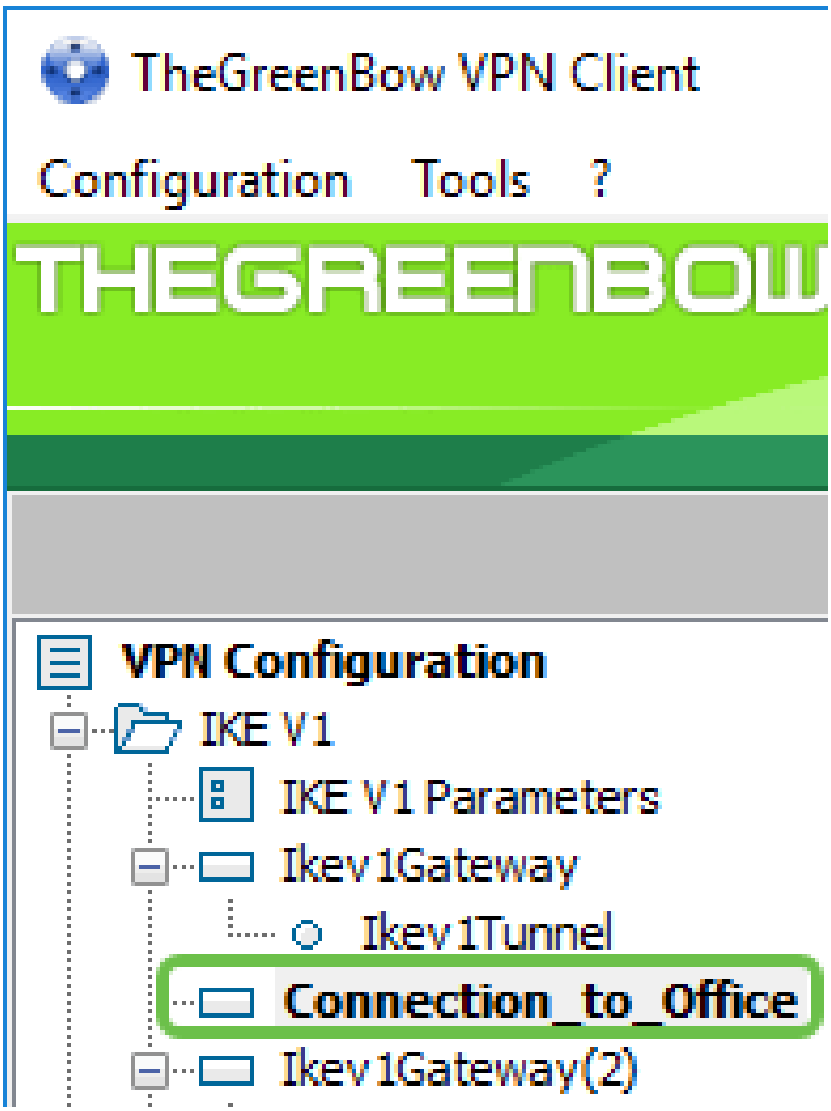
步驟3.在*ESP*下，將Encryption、Authentication和Mode設定為與站點（辦公室）的VPN網關設定相匹配。



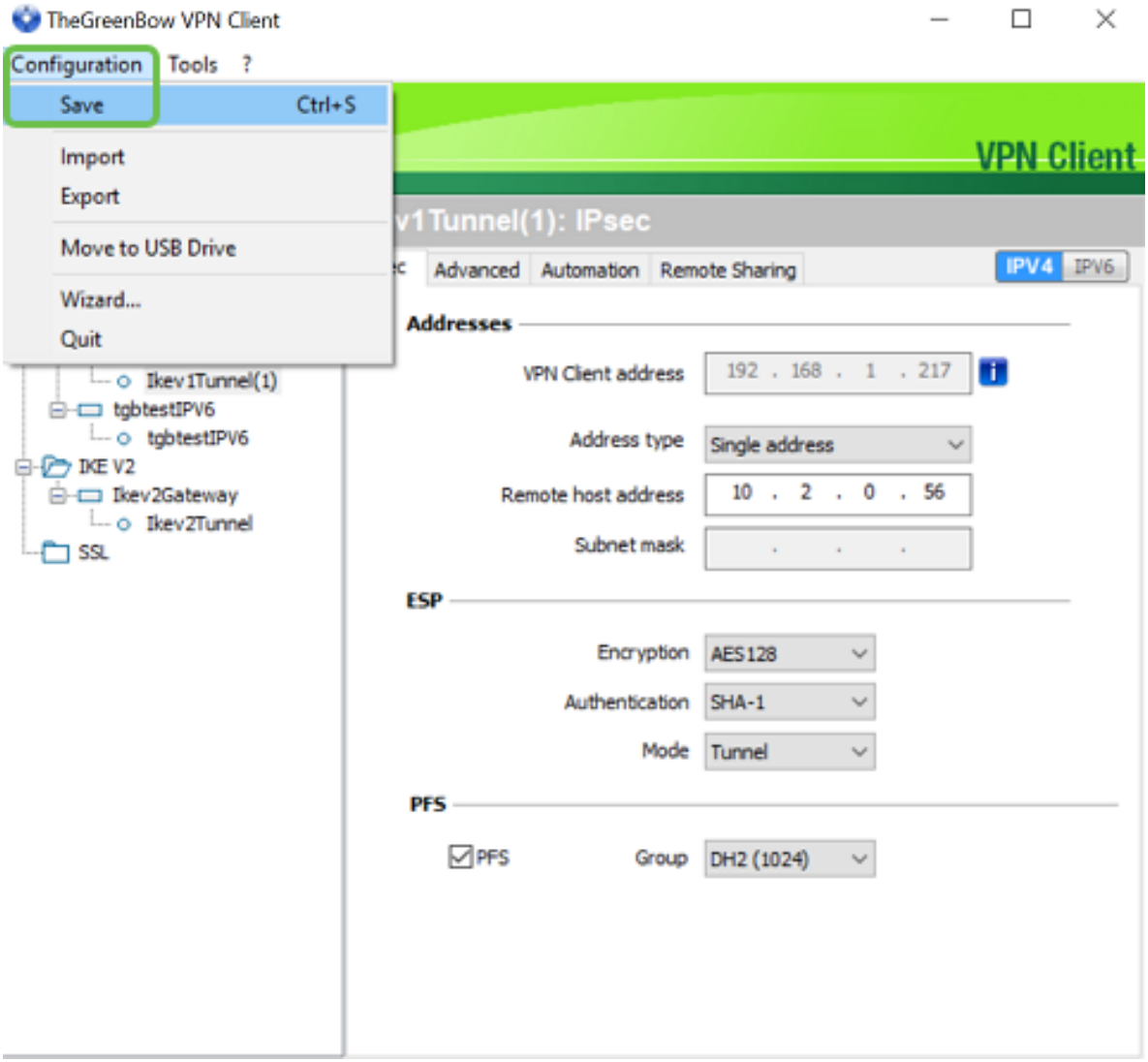
步驟4.（可選）在*PFS*下，勾選**PFS**覈取方塊以啟用完全向前保密(PFS)。PFS生成用於加密會話的隨機金鑰。從*Group*下拉選單中選擇PFS組設定。如果在路由器上啟用該選項，則也應在此處啟用該選項。



步驟5.（可選）按一下右鍵Ikev1Gateway的名稱，然後按一下重新命名部分（如果要對其進行重新命名）。



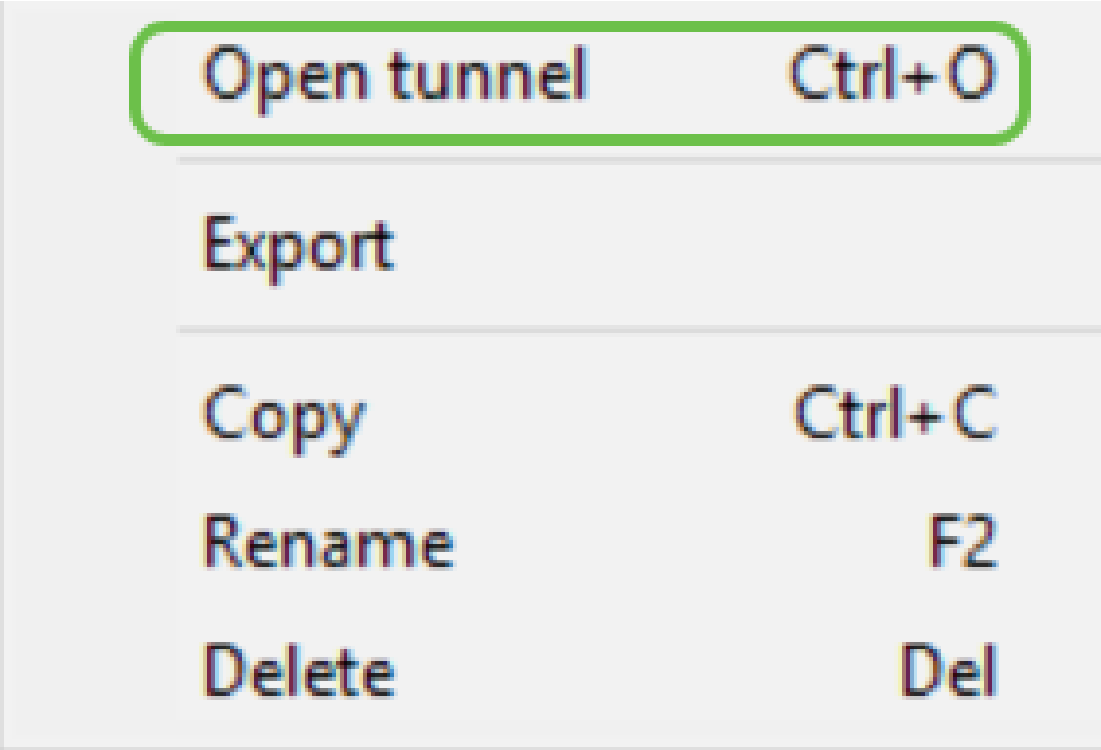
步驟6.按一下**Configuration**，然後選擇**Save**。



您現在應該已經成功配置TheGreenBow VPN客戶端，通過VPN連線到RV160或RV260路由器。

作為客戶端啟動VPN連線

步驟1。由於TheGreenBow已開啟，因此您可以按一下右鍵隧道並選擇**開啟隧道以開始連線**。

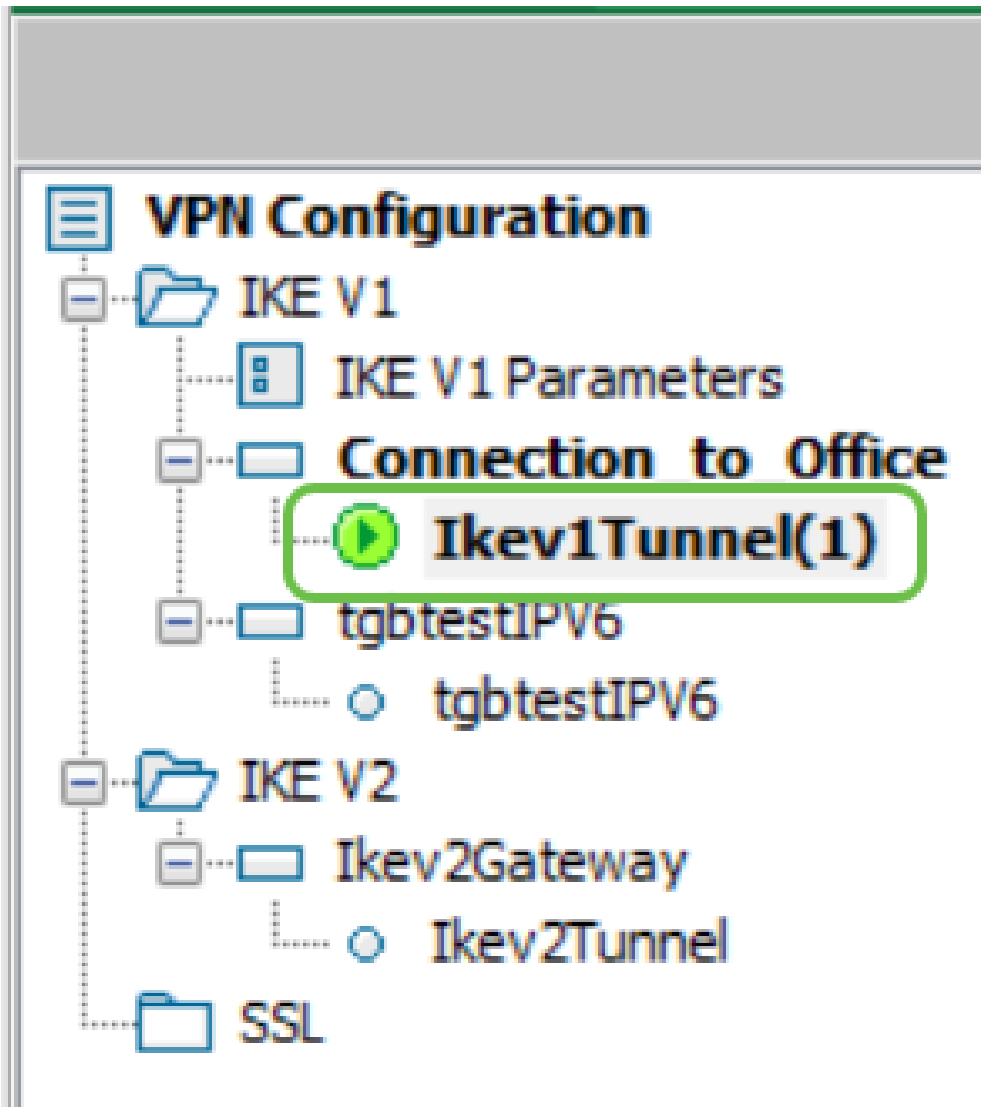


附註：您也可以通過按兩下隧道來開啟隧道。

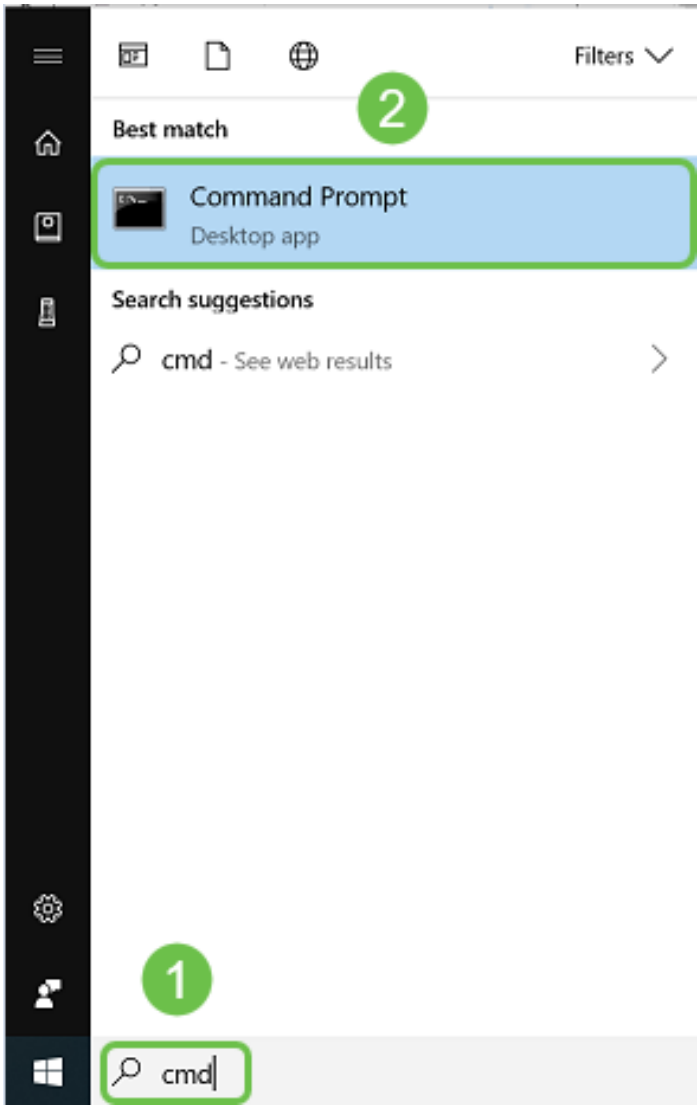
步驟2.（可選）如果您正在開始新會話並已關閉TheGreenBow，請按一下螢幕右側的**TheGreenBow VPN Client**圖示。

步驟3.（可選）只有在您正在設定新會話並且遵循步驟2時，才需要執行此步驟。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。

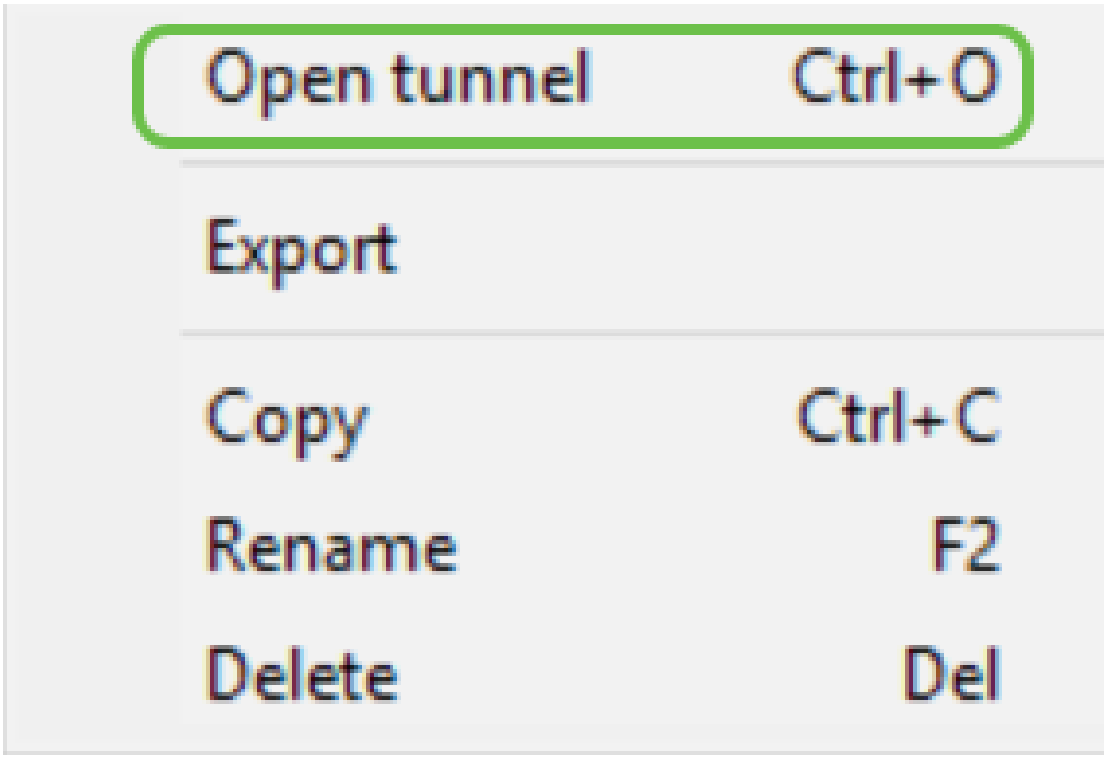
步驟4.連線通道後，通道旁會顯示一個綠色圓圈。如果您看到感歎號，可以按一下它來查詢錯誤。



步驟5.（可選）若要確認是否已連線，請從客戶端電腦訪問命令提示符。



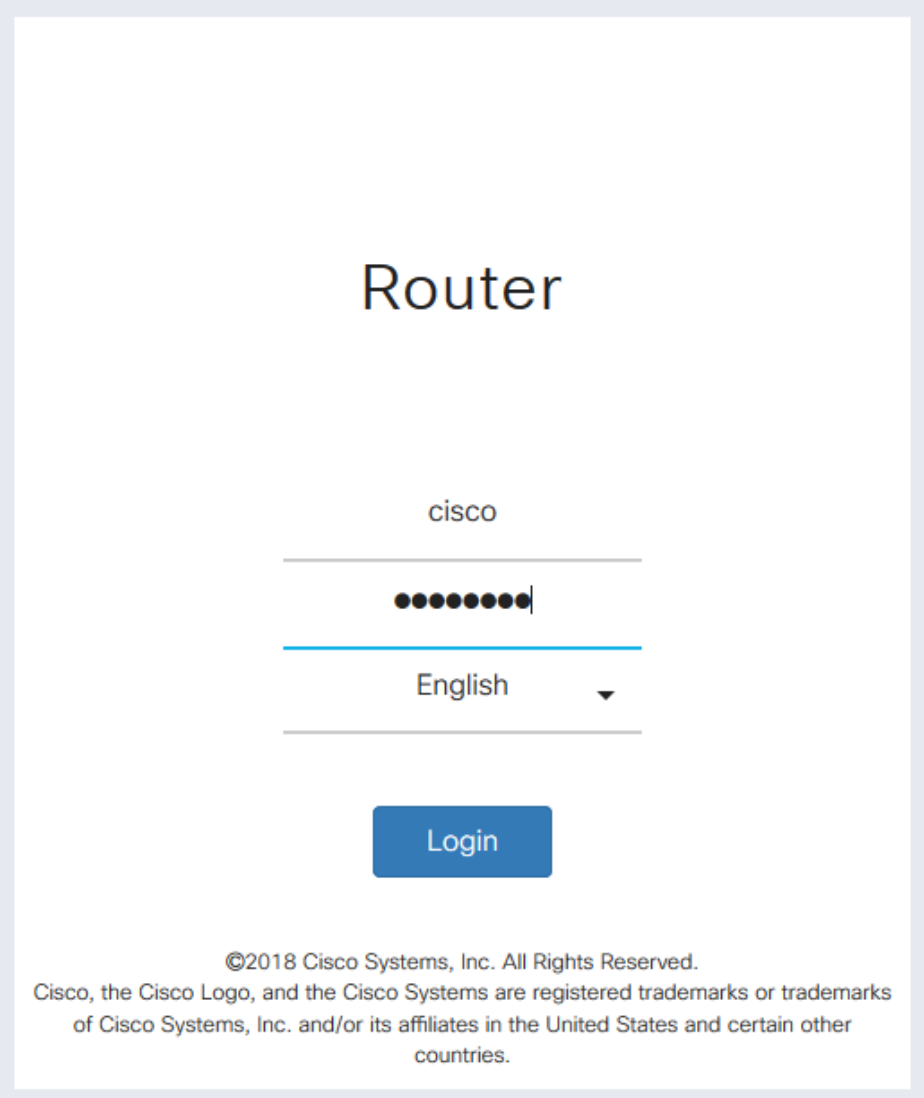
步驟6.（可選）輸入ping，然後輸入站點上路由器的專用LAN IP地址。如果您收到回覆，則表明您已連線。



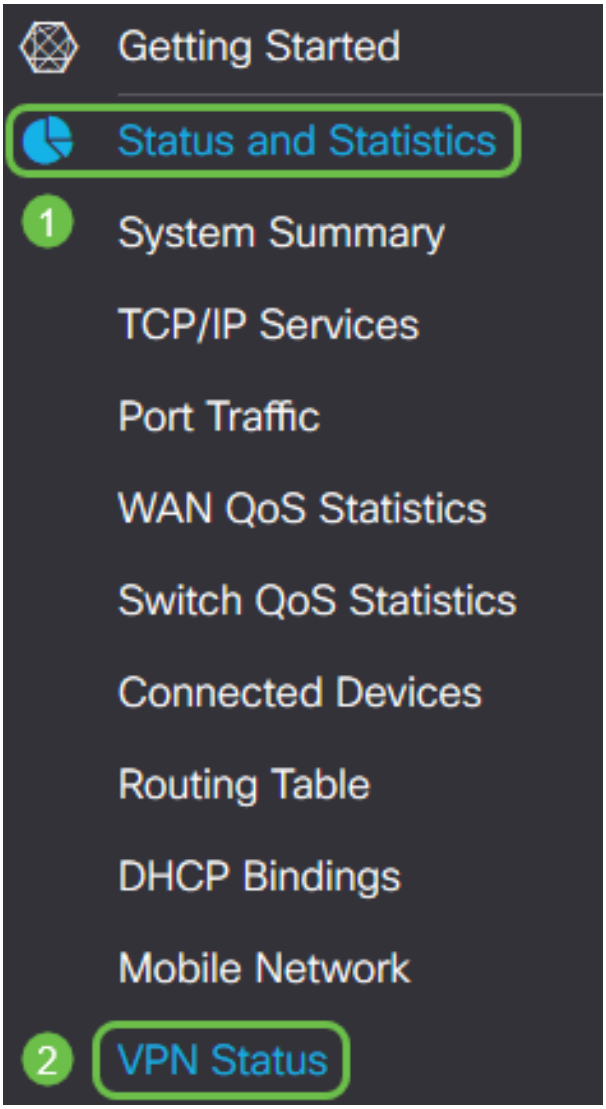
驗證VPN狀態

驗證站點的VPN狀態

步驟1.登入到RV160或RV260的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。您應該看到VPN連線已確認。

步驟4.點選**眼睛**圖示以檢視更多詳細資訊。

步驟5.此處顯示客戶端到站點VPN狀態的詳細資訊。您會注意到客戶端的WAN IP地址，即從設定時配置的地址池中分配的本地IP地址。它還顯示傳送和接收的位元組和資料包以及連線時間。如果要斷開客戶端的連線，請按一下*操作*下的**藍色斷**開鏈圖示。檢查後，按一下右上角的**x**關閉。

Client IP (Actual)	Client IP (VPN)	TX Bytes	RX Bytes	TX Packets	RX Packets	Connect Time	Action
108.233.	10.2.1.1	0	14273	0	181	5 mins.	

結論

現在，您應該已經成功在RV160或RV260路由器上設定和驗證了VPN連線，並且已配置GreenBow VPN客戶端以通過VPN連線到路由器。