使用RV160和RV260配置Shrew Soft VPN客戶端

目標

本文檔的目的是向您展示如何配置通過RV160或RV260系列路由器連線Shrew Soft VPN客戶端所需的設定。

VPN基本知識簡介

虛擬專用網路(VPN)是將遠端使用者連線到安全網路的理想方式。它通過較不安全的網路（如Internet）建立加密連線。

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，因為允許員工訪問其內部資源不僅有用，而且必要，即使員工不在辦公室。

RV160路由器最多支援10個VPN隧道，RV260最多支援20個。

本文將引導您完成配置RV160/RV260路由器和軟體VPN客戶端所需的步驟。您將學習如何建立使用者組、使用者帳戶、IPsec配置檔案和客戶端到站點配置檔案。在Show Soft VPN client上，您將學習如何配置General、Client、Name Resolution、Authentication、Phase 1和Phase 2頁籤。

如果我想使用VPN，優缺點是什麼？

VPN可解決許多行業和業務型別共有的實際使用案例情況。下表顯示了使用VPN的一些優缺點。

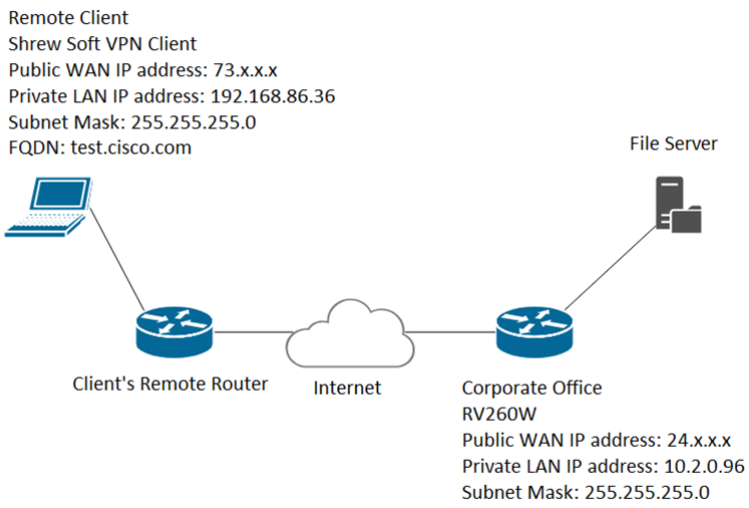
優點	缺點
通過為個人使用者（如員工、承包商或合作夥伴）定製的訪問權，提供安全的通訊、便利性和可訪問性。	可能會出現連線速度慢的情況。更強的加密需要時間和資源來確保匿名性和安全性。加密網路流量通常需要更多開銷。您可能可以找到兩個VPN提供商，它們可以在保持匿名性和安全性的同時保持良好的連線速度，但是它們通常是付費服務。
通過擴展公司網路和應用提高工作效率。	配置錯誤帶來的潛在安全風險。設計和實施VPN可能非常複雜。必須委託有經驗的專業人員來配置您的VPN，以確保您的網路不會受到危害。
降低通訊成本並提高靈活性。	如果出現需要新增新基礎架構或新配置的情況，技術問題可能因不相容而產生，尤其是當所使用產品或供應商不是涉及到時。
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）。	
保護機密的網路資料和資源。	
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。	

拓撲

這是一個簡單的網路拓撲。

附註：公有WAN IP地址已模糊。



適用裝置

- RV160
- RV260

軟體版本

- 1.0.0.xx（RV160和RV260）

•議2.2.1，因為2.2.2可能與我們的路由器存在連線問題(Shrew Soft VPN Client Download)

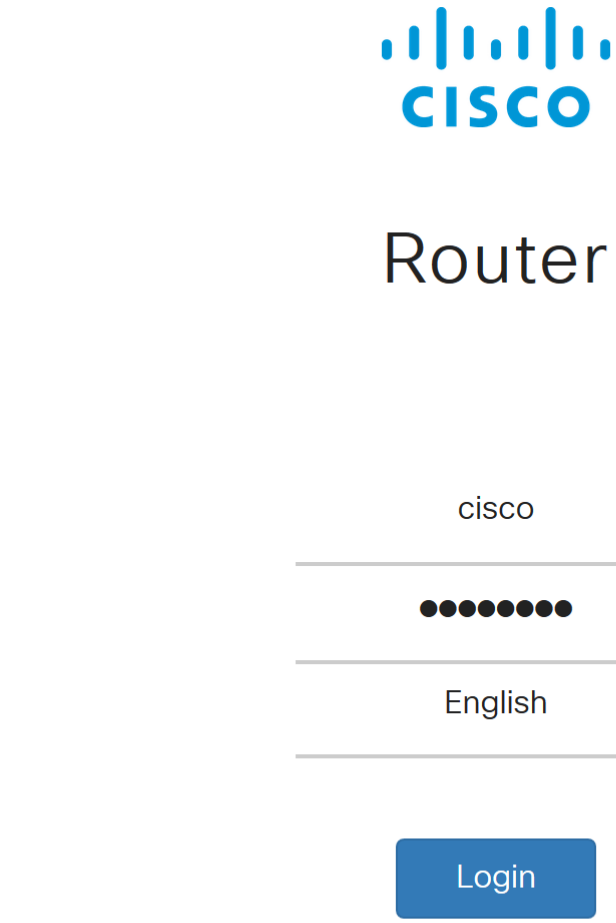
目錄

5. 配置軟體VPN客戶端
6. 顯示軟VPN客戶端：常規頁籤
7. 顯示軟VPN客戶端：客戶端頁籤
8. 顯示軟VPN客戶端：名稱解析頁籤
9. 顯示軟VPN客戶端：Authentication頁籤
10. 顯示軟VPN客戶端：階段1頁籤
11. 顯示軟VPN客戶端：階段2頁籤
12. 顯示軟VPN客戶端：正在連線
13. VPN連線故障排除提示
14. 驗證
15. 結論

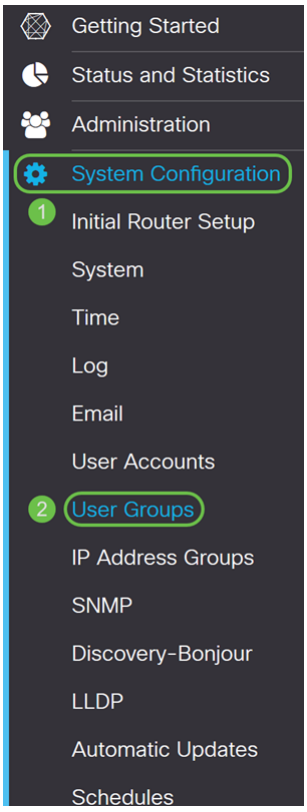
建立使用者組

重要附註：請將預設管理員帳戶保留在管理組中，並為Shrew Soft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。

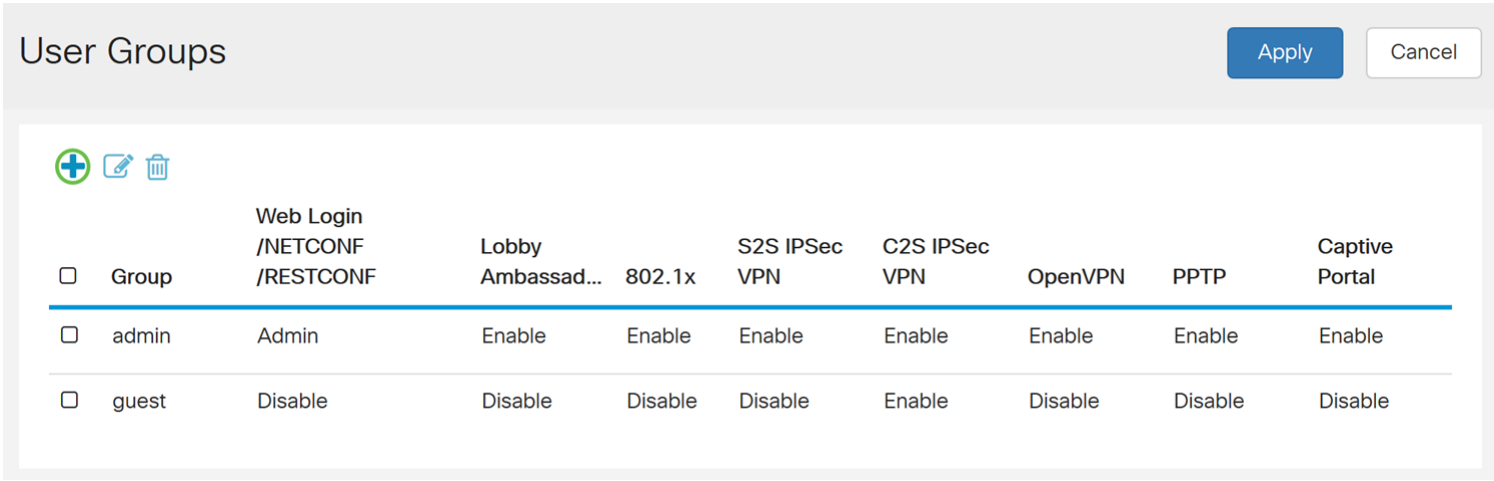
步驟1.登入Web組態頁面。



步驟2.導覽至System Configuration > User Groups。



步驟3.按一下**plus**圖示新增新使用者組。



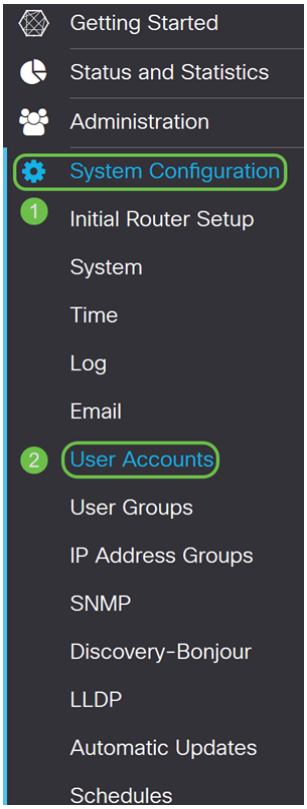
步驟4.在「組名稱」欄位中輸入*組名*稱。

我們將使用**ShrewSoftGroup**作為示例。

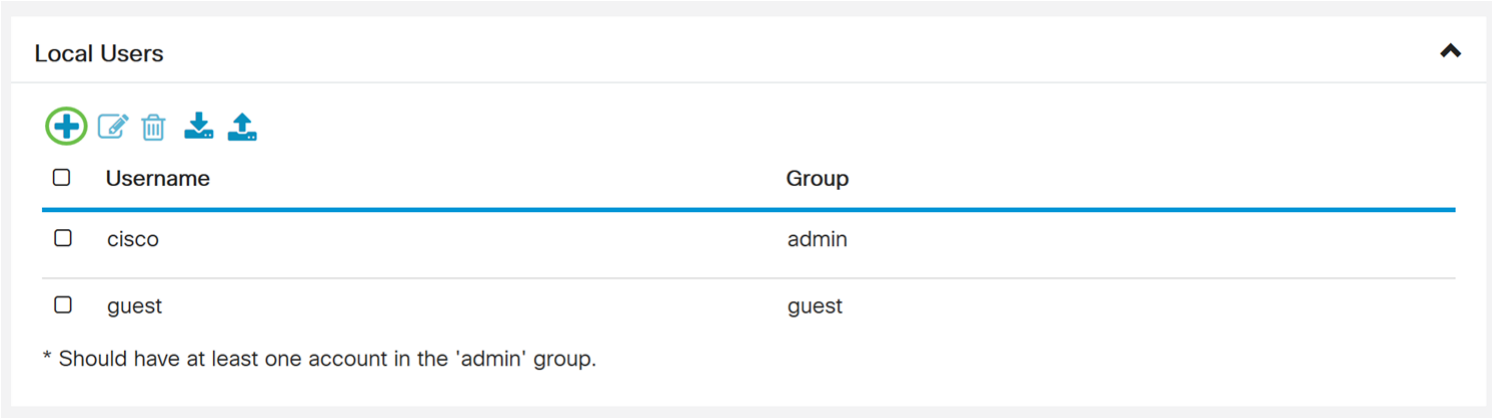
步驟5.按**Apply** 建立新組。

建立使用者帳戶

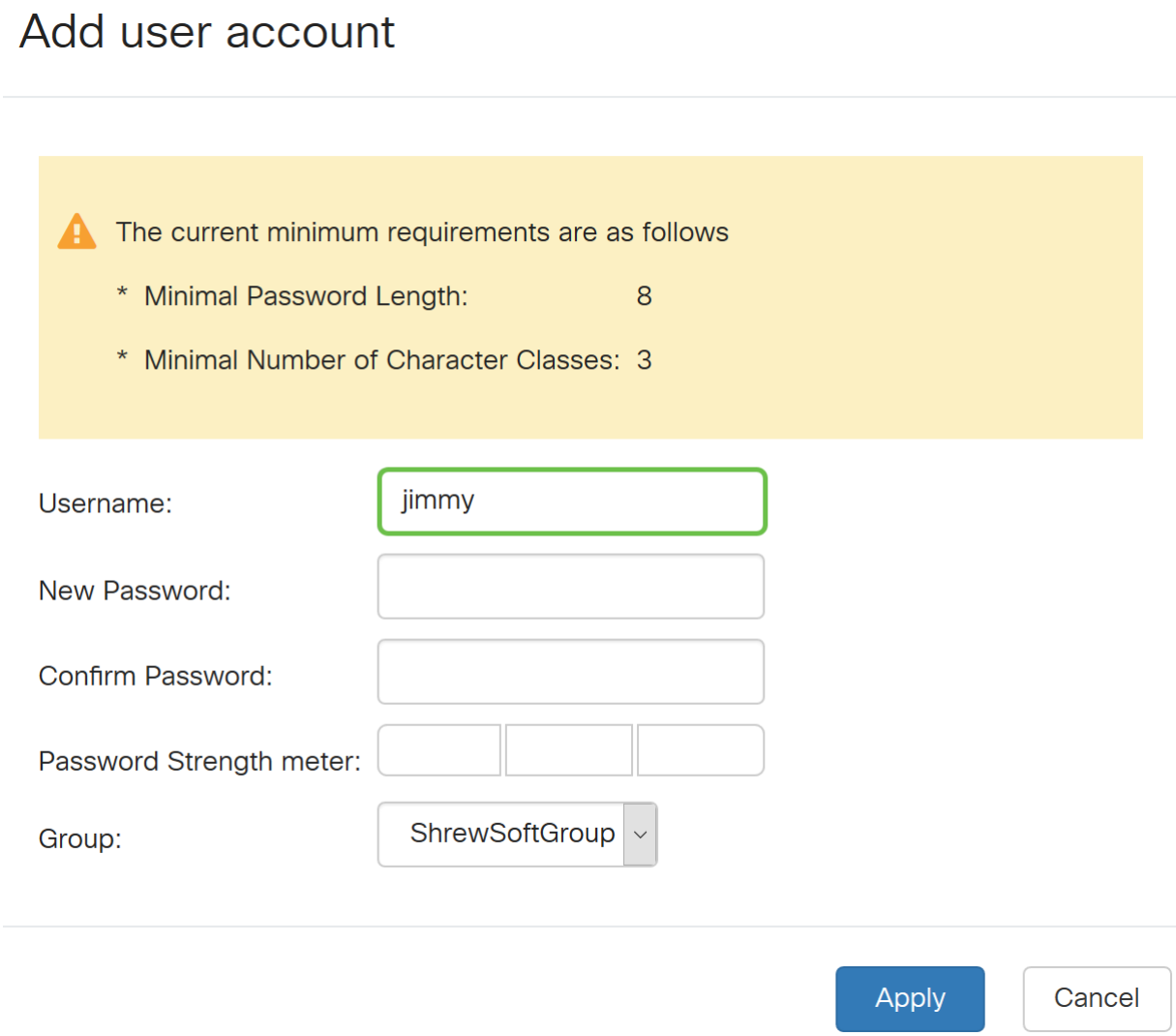
步驟1.導覽至**System Configuration > User Accounts**。



步驟2.向下滾動到*Local Users*表，然後按**plus**圖示新增新使用者。

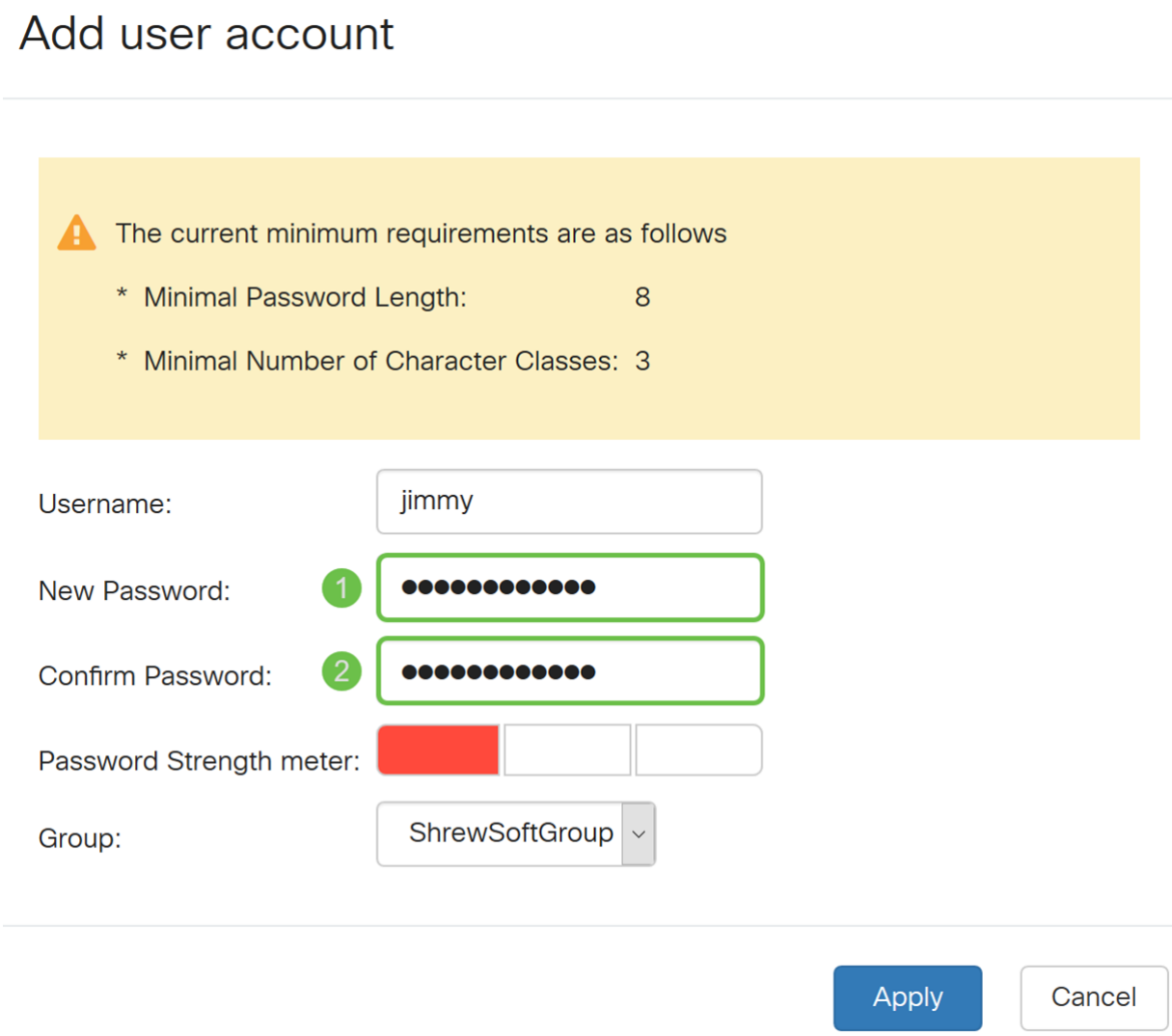


步驟3.將打*開「新增使用者*帳戶」頁。輸入使用者的使用者名稱。

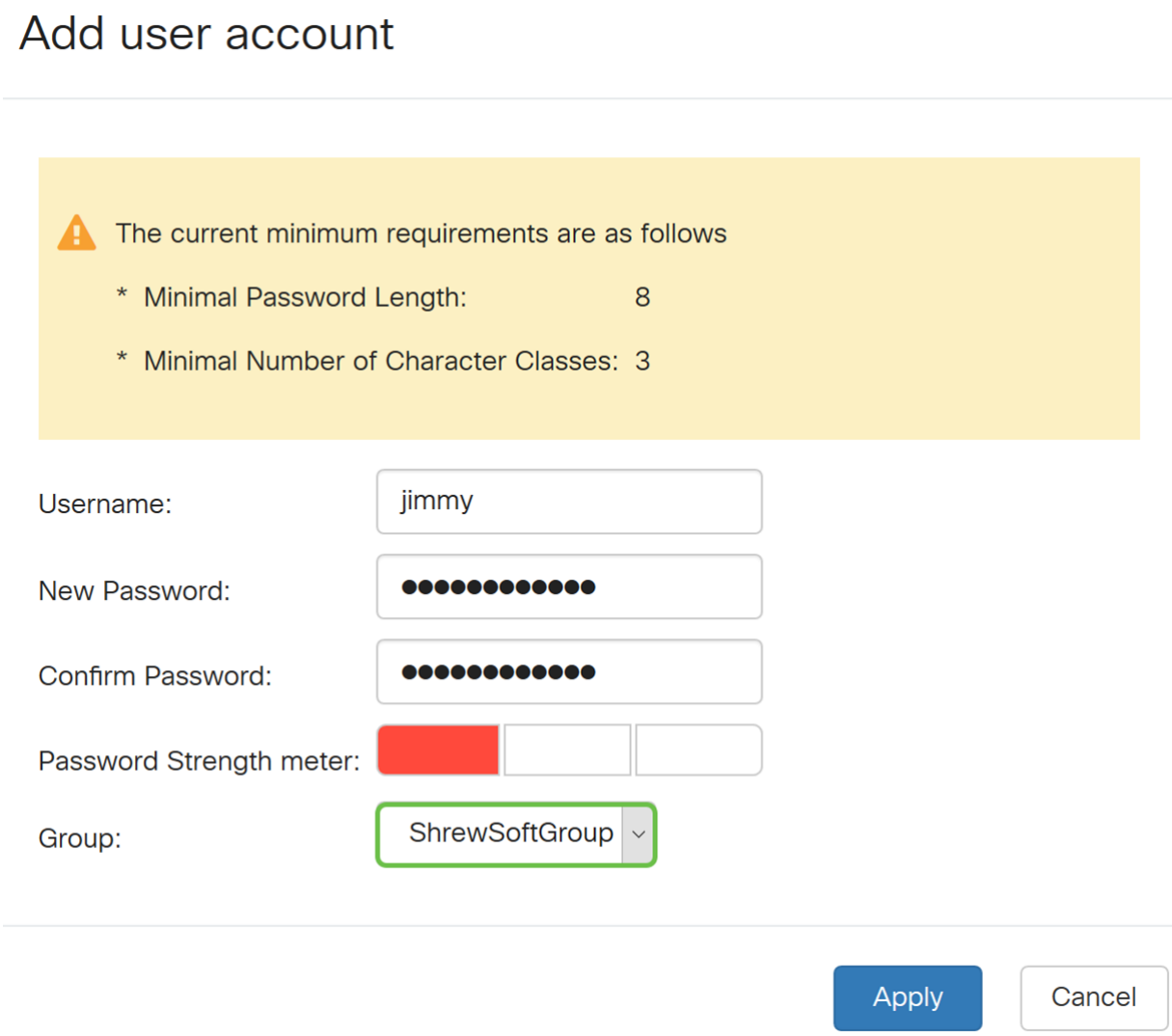


步驟4.在*New Password*(新密*碼)欄位中輸*入密碼。在*Confirm Password*欄位中重新輸入相同的密碼。在本例中，我們將使用**CiscoTest123**作為密碼。

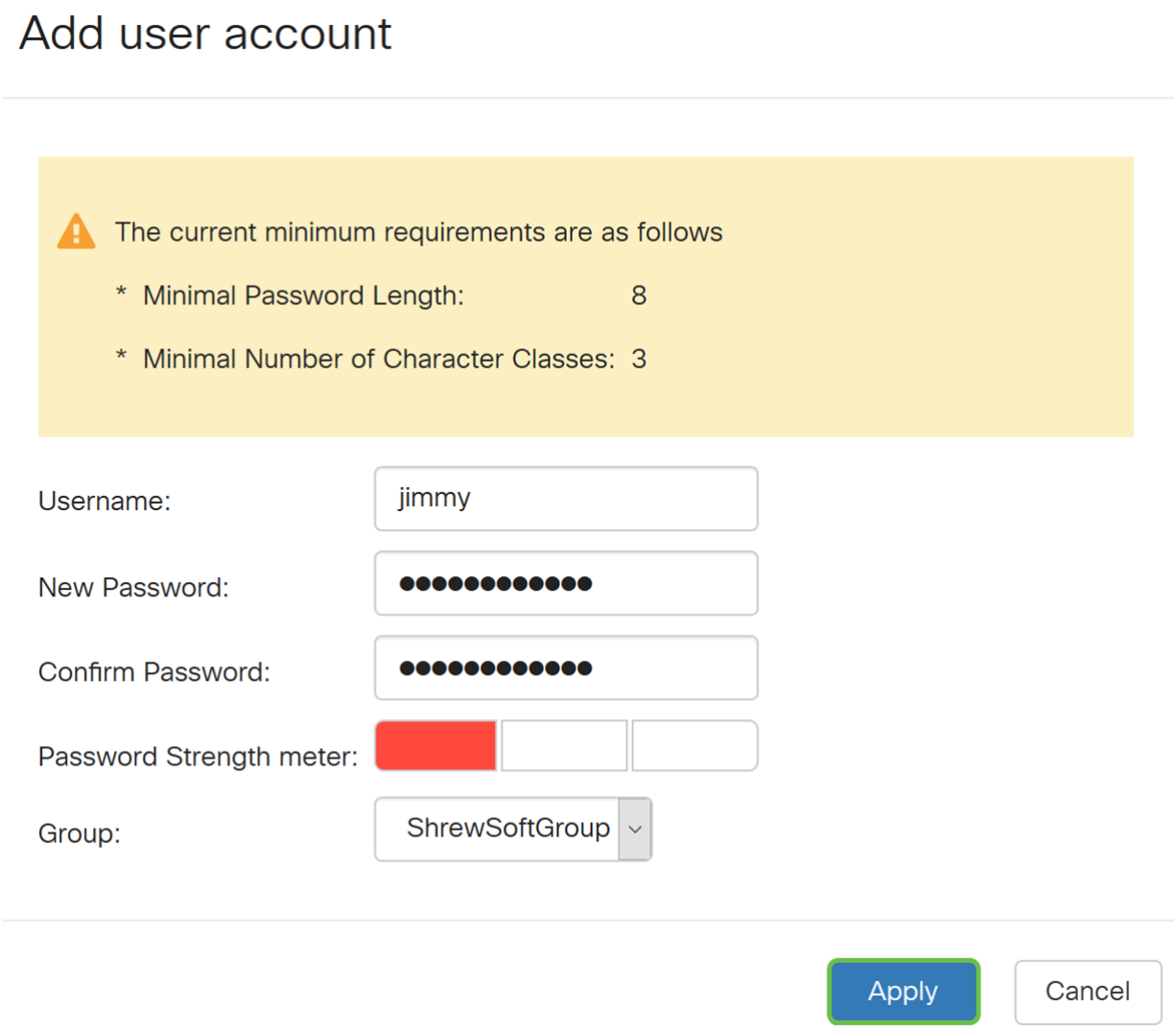
附註：此處使用的密碼就是一個示例。建議使您的密碼更複雜。



步驟5.在*Group*下拉選單中，選擇希望使用者所在的組。

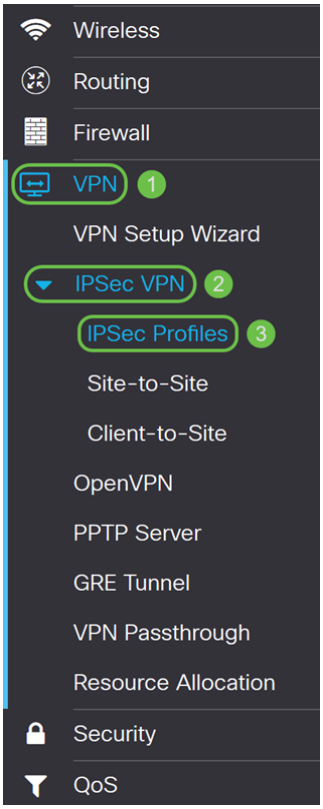


步驟6.按**Apply**建立新使用者帳戶。



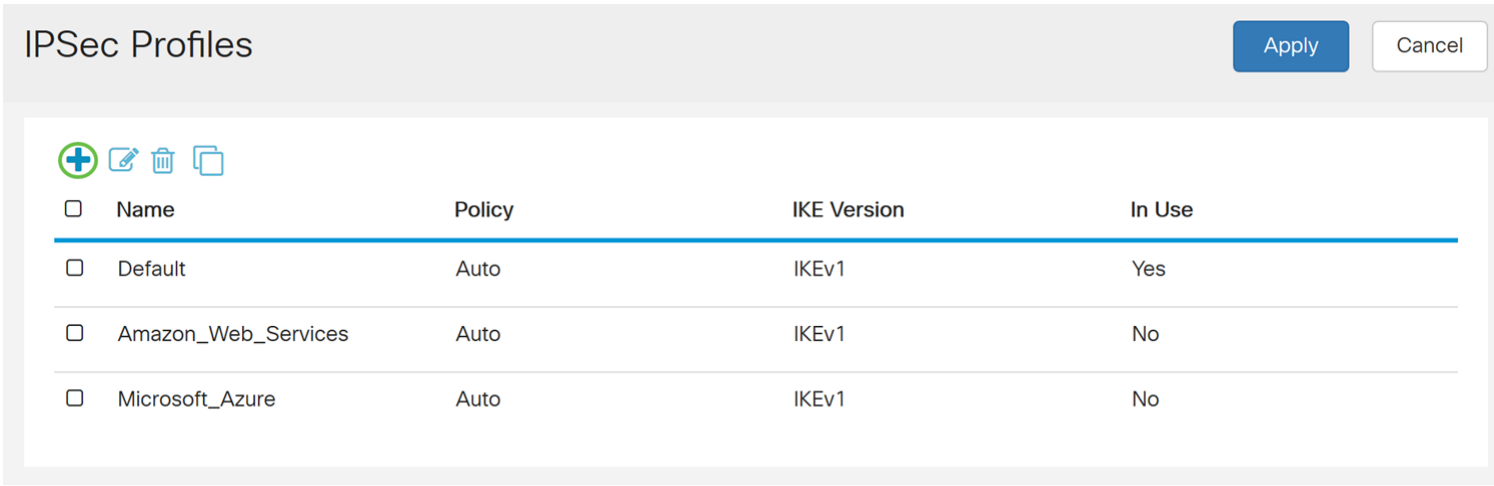
配置IPsec配置檔案

步驟1.導航到VPN > IPSec VPN > IPSec Profiles。

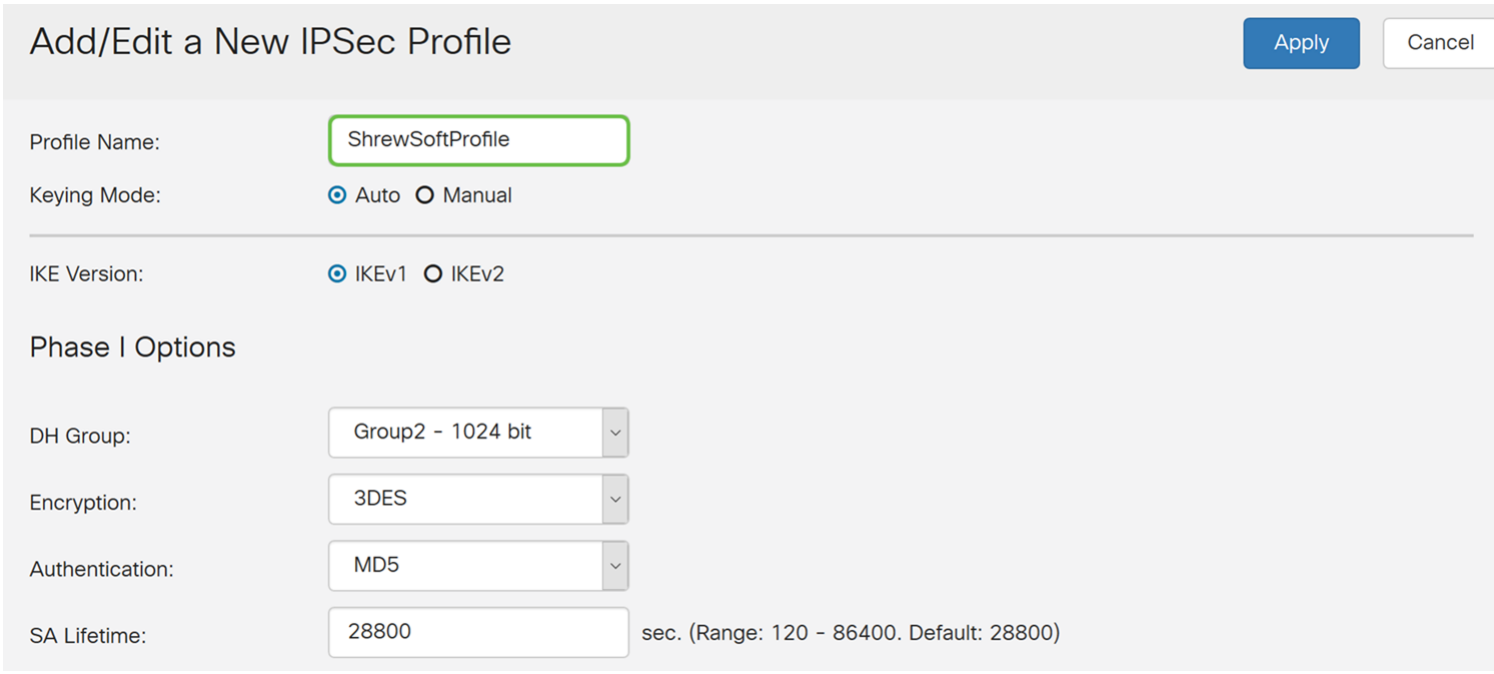


附註：有關如何配置IPsec配置檔案的詳細說明，請按一下該連結檢視以下文章：[在RV160和RV260上配置IPsec配置檔案（自動金鑰模式）]

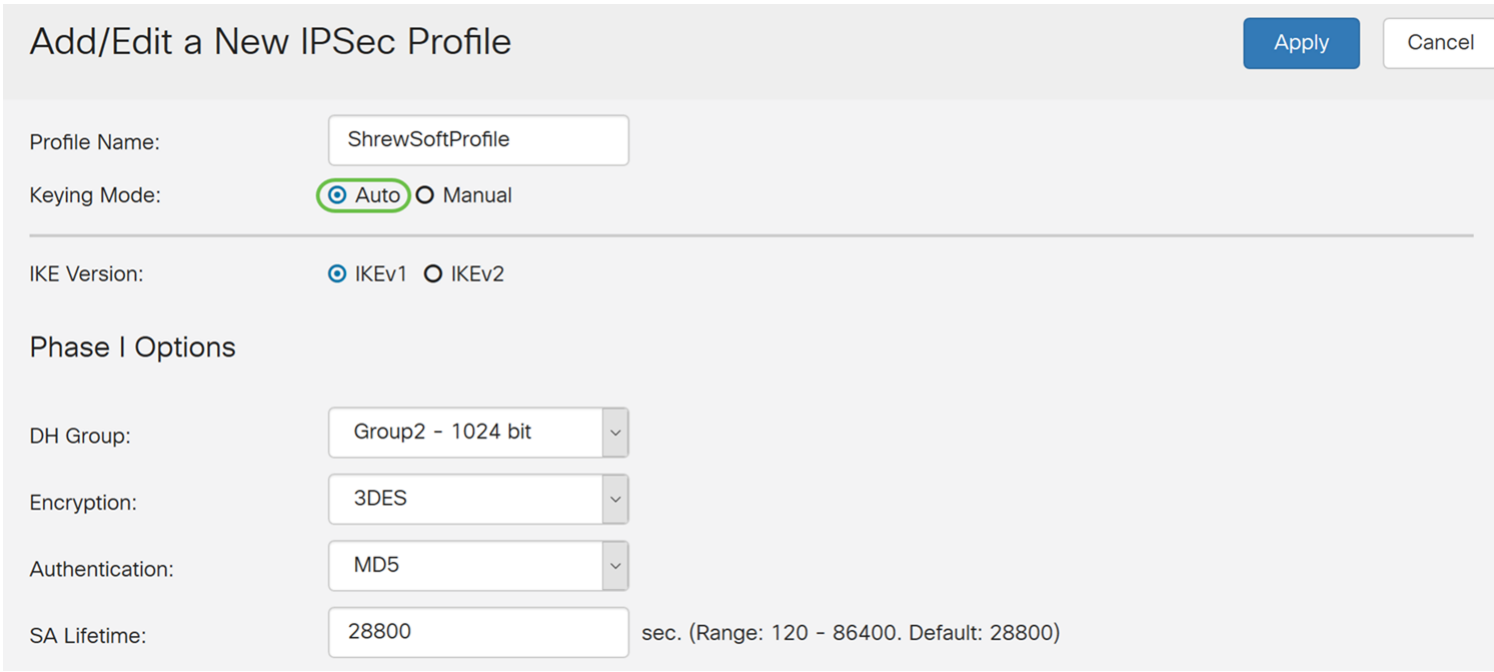
步驟2.按一下**plus**圖示新增新的IPsec配置檔案。



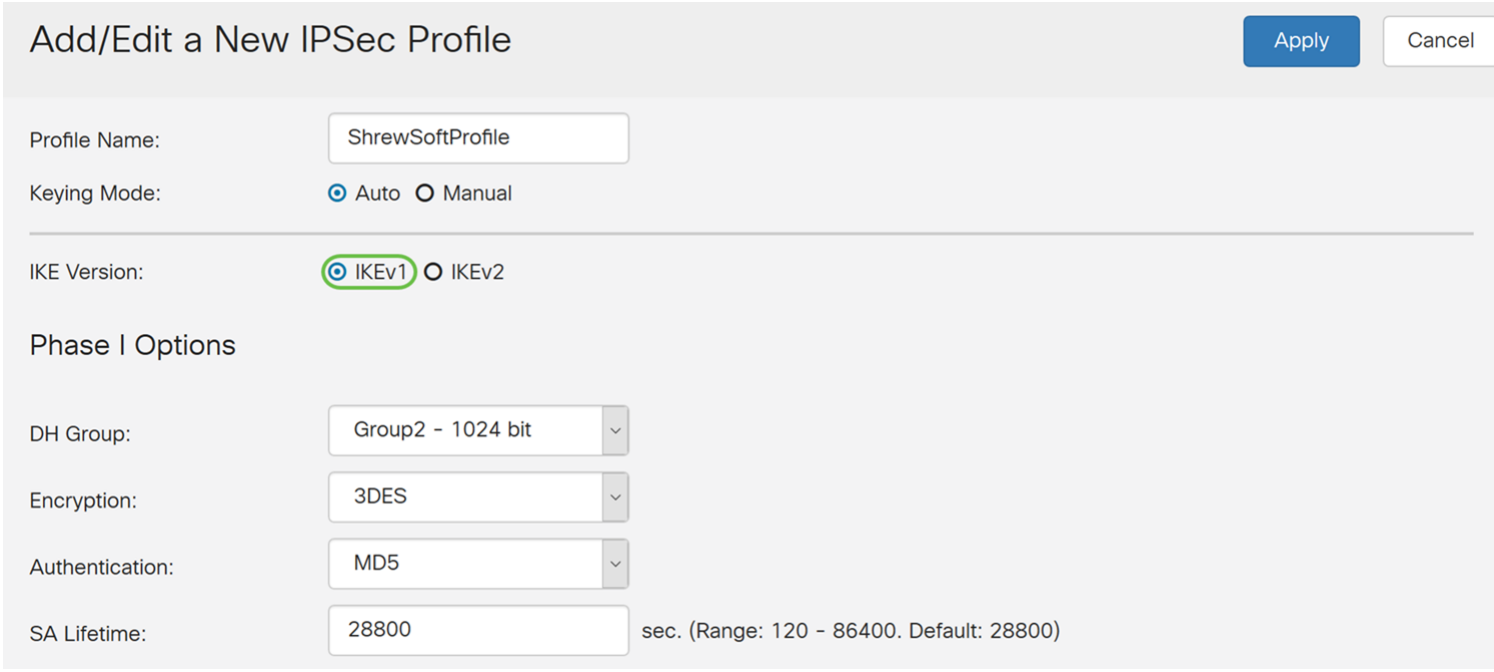
步驟3.在*配置檔名稱*欄位中輸入配置檔名稱。我們將輸入**ShrewSoftProfile**作為配置檔名稱。



步驟4.選擇**Auto**作為*Keying Mode*。



步驟5.選擇**IKEv1**或**IKEv2**作為*IKE版本*。在本示例中，選擇了IKEv1。



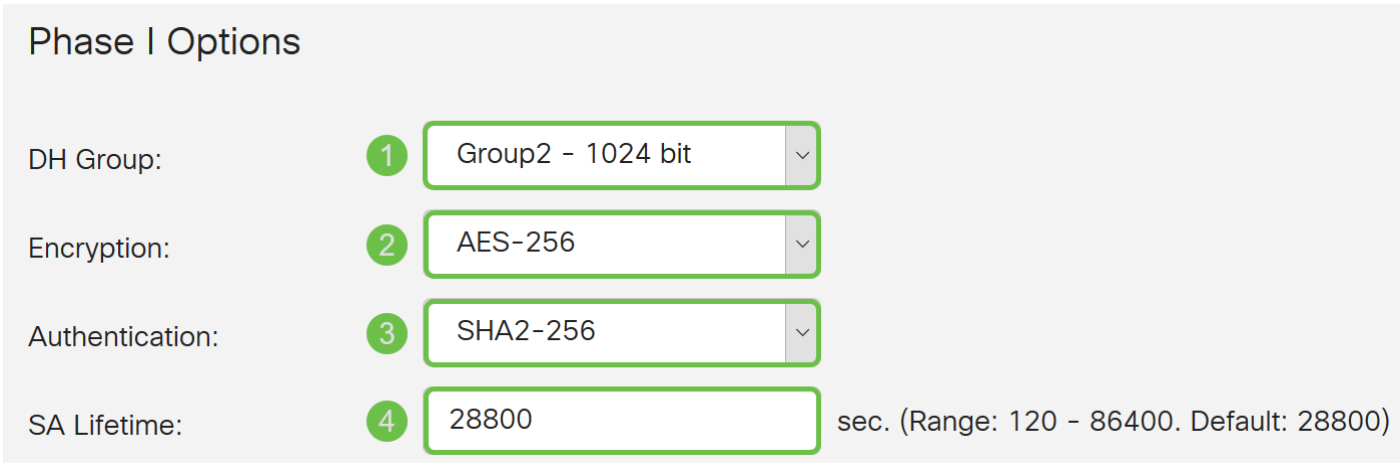
步驟6.在「*Phase I Options*」部分下，這是我們已經為本文配置的選項。

DH組：**Group2 - 1024位**

加密：**AES-256**

驗證:**SHA2-256**

SA生存期：**28800**



第7步.在*Phase II Options*下，這是我們已經為本文配置的選項。

協定選擇：**ESP**

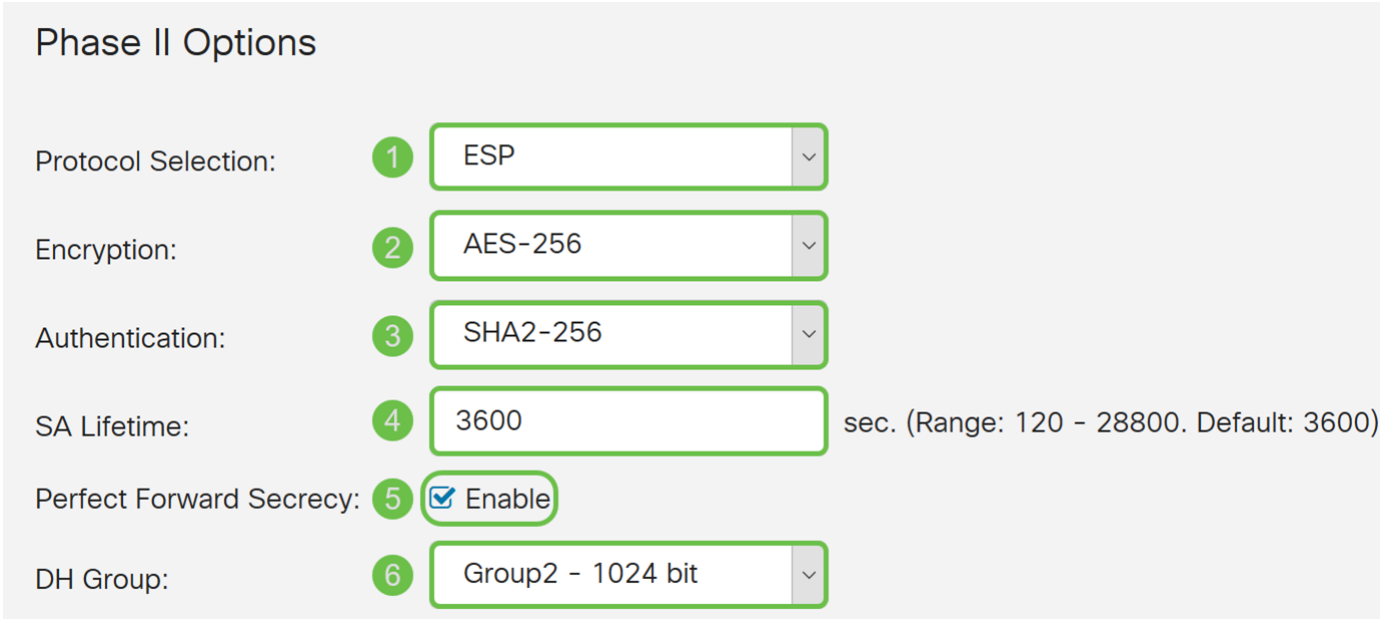
加密：**AES-256**

驗證:**SHA2-256**

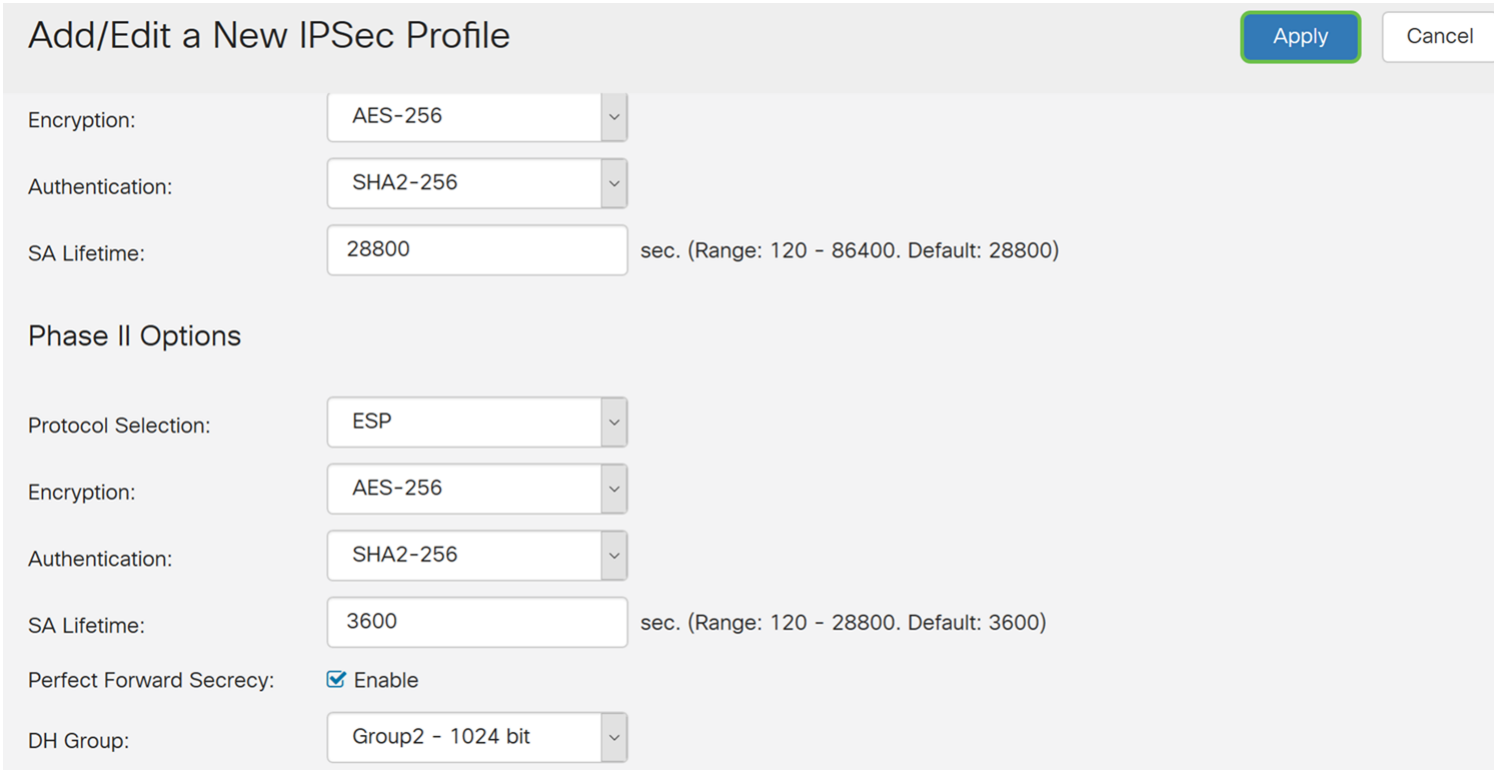
SA生存期：**3600**

完全向前保密：**已啟用**

DH組：**Group2 - 1024位**

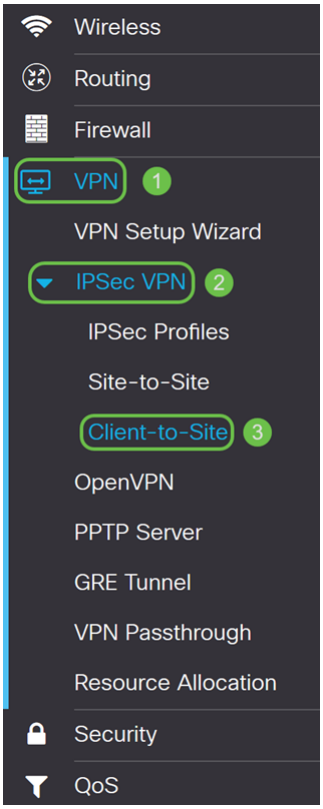


步驟8.按一下**Apply**建立新的IPsec配置檔案。

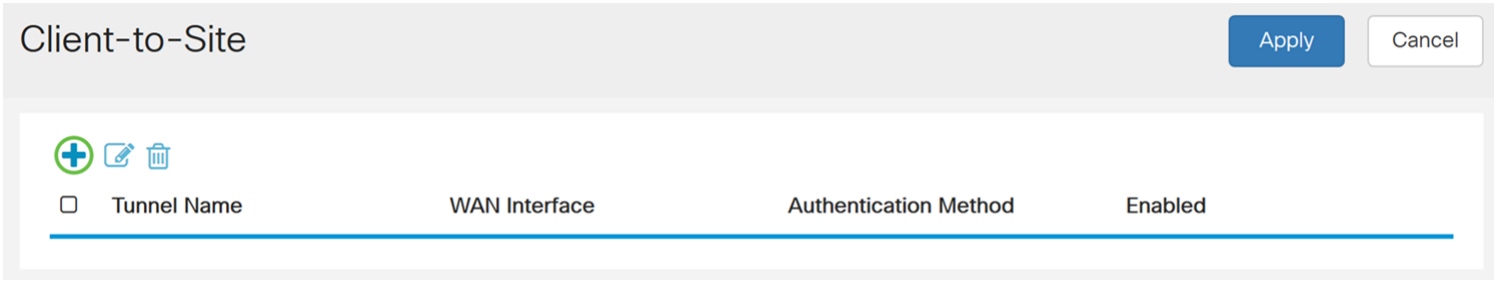


配置客戶端到站點

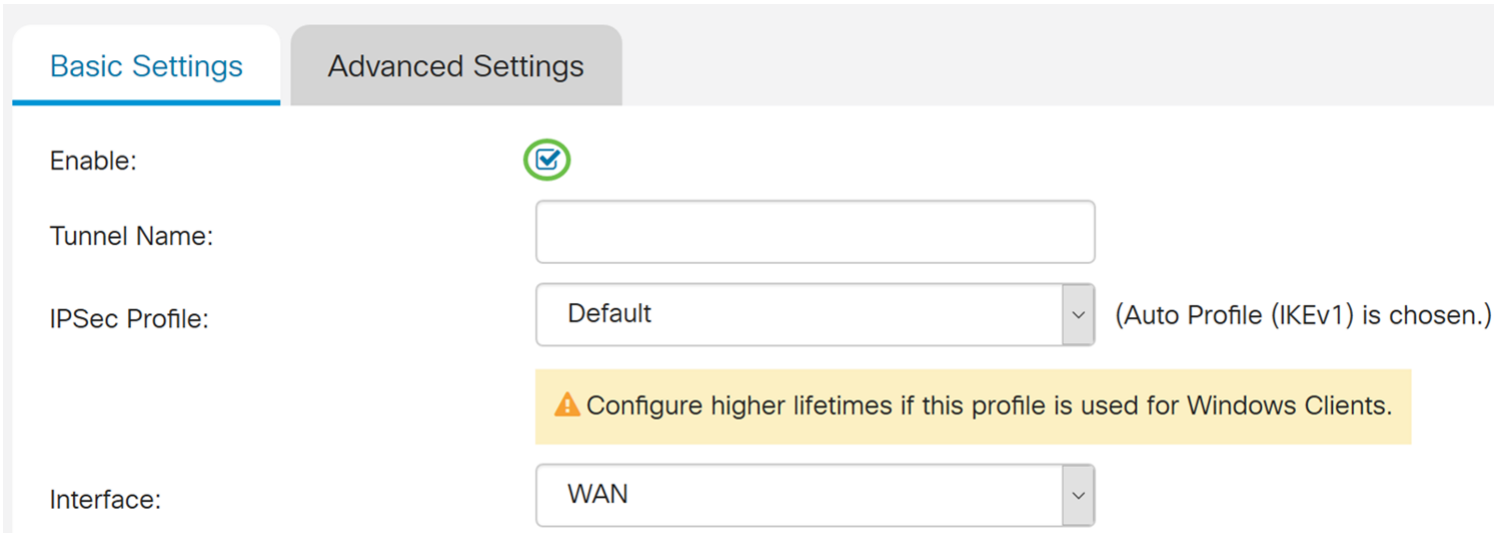
步驟1.導航到**VPN > IPSec VPN > Client-to-Site**。



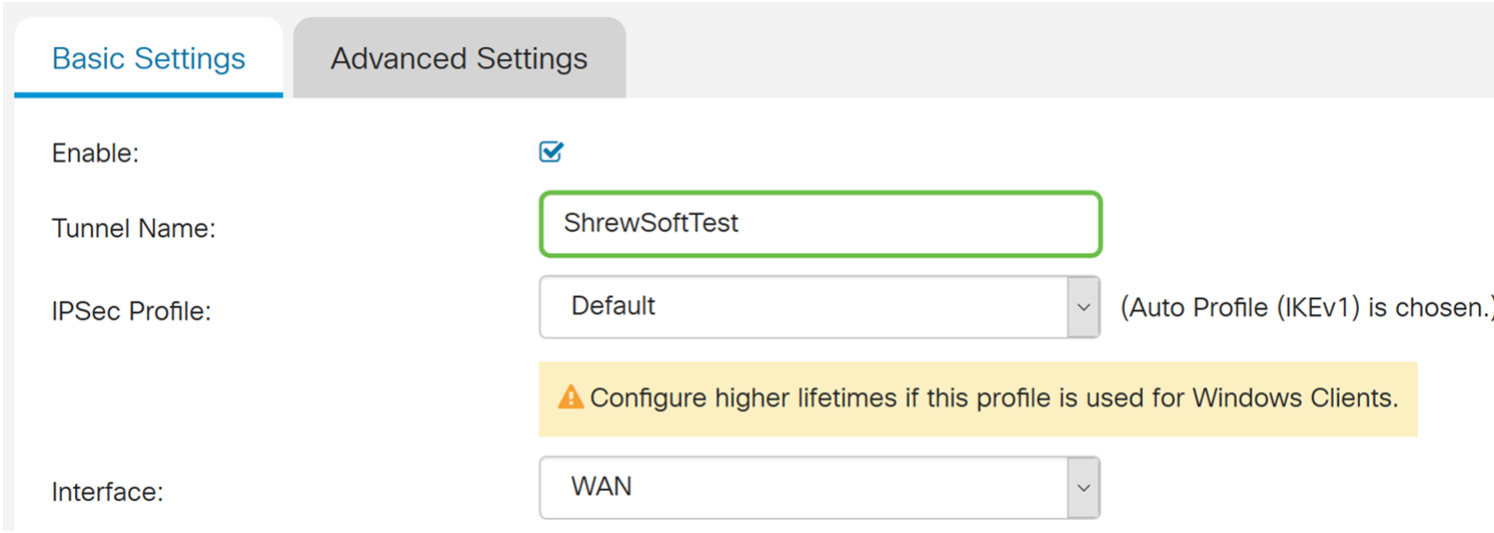
步驟2.按一下**plus**圖示新增通道。



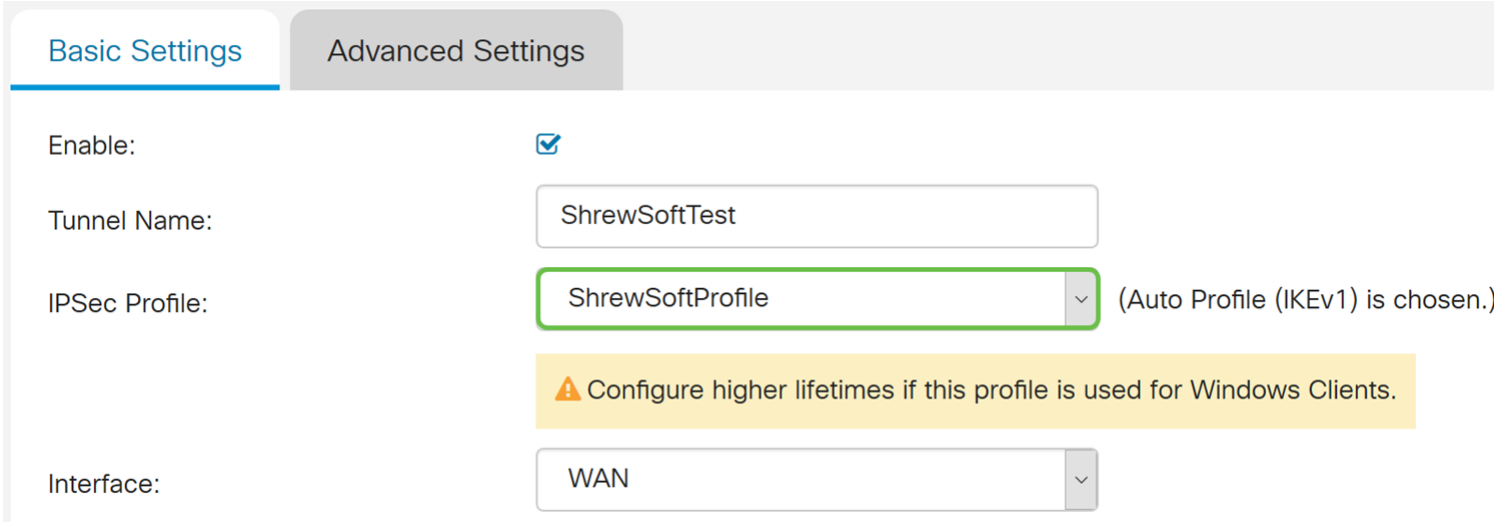
步驟3.勾選**Enable**覈取方塊以啟用通道。



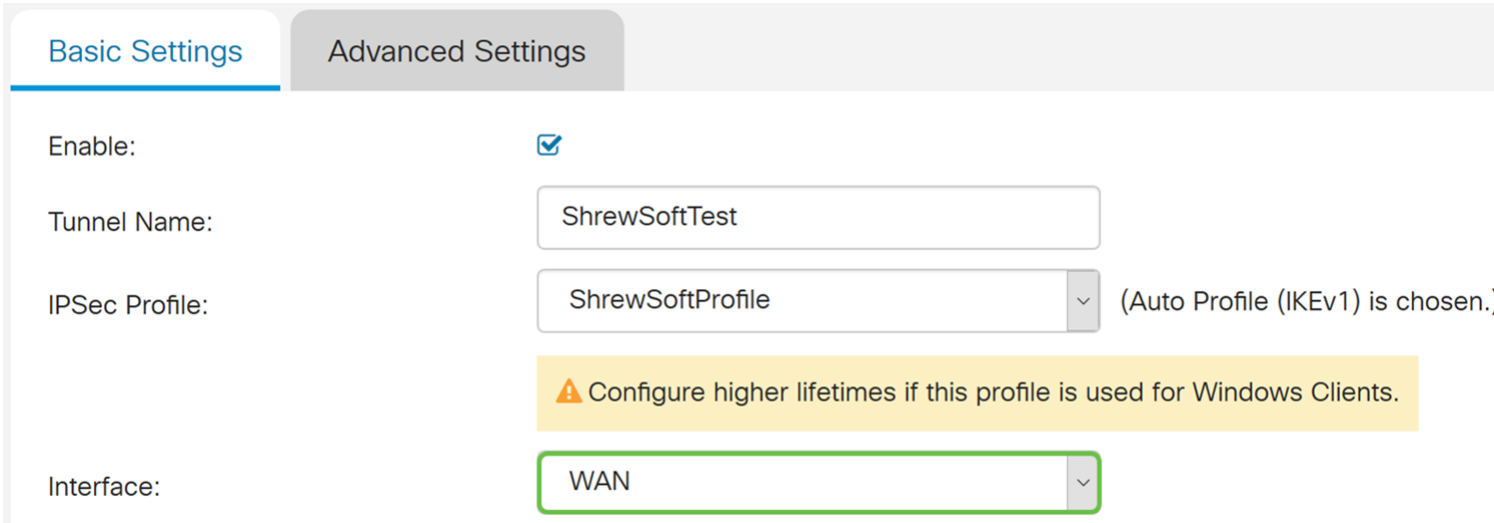
步驟4.在*Tunnel Name*欄位中輸入通道的名稱。



步驟5.在*IPSec Profile*下拉選單中，選擇要使用的配置檔案。我們將選擇在上一節中建立的ShrewSoftProfile:配置IPsec配置檔案。



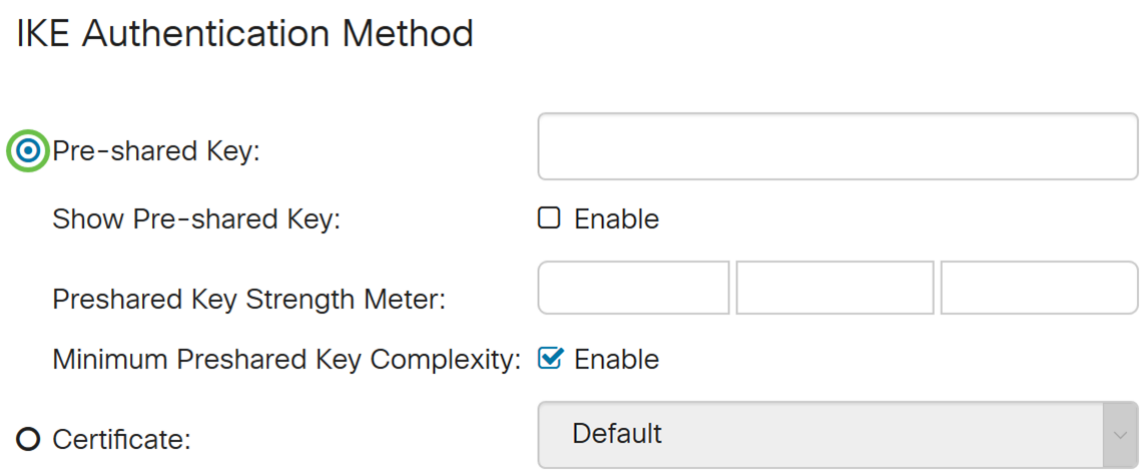
步驟6.從*Interface*下拉選單中，選擇要使用的介面。我們將使用**WAN**作為連線隧道的介面。



步驟7.在*IKE Authentication Method*部分下，選擇*Pre-shared Key*或*Certificate*。我們將使用**預共用金鑰**作為IKE身份驗證方法。

附註：IKE對等體通過計算和傳送包含預共用金鑰的資料的金鑰雜湊來相互進行身份驗證。如果接收對等體能夠使用其預共用金鑰獨立建立相同的雜湊，則它知道兩個對等體必須共用相同的金鑰，從而驗證另一個對等體。預共用金鑰不能很好地擴展，因為每個IPsec對等體必須使用與其建立會話的其他每個對等體的預共用金鑰進行配置。

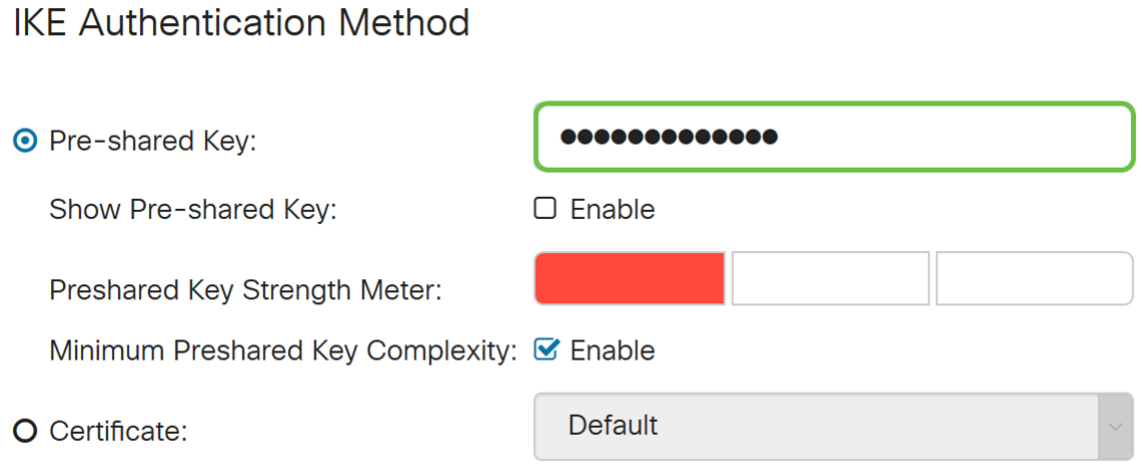
證書使用包含諸如證書的名稱或IP地址、序列號、到期日期以及證書持有者的公鑰副本等資訊的數位證書。



步驟8.輸入要用於驗證的預共用金鑰。預共用金鑰可以是您想要的任何內容。配置時，在Shrew Soft VPN客戶端上配置的預共用金鑰必須與此處相同。

在本例中，我們將使用**CiscoTest123!**作為預共用金鑰。

附註：此處輸入的預共用金鑰就是一個示例。建議輸入更複雜的預共用金鑰。

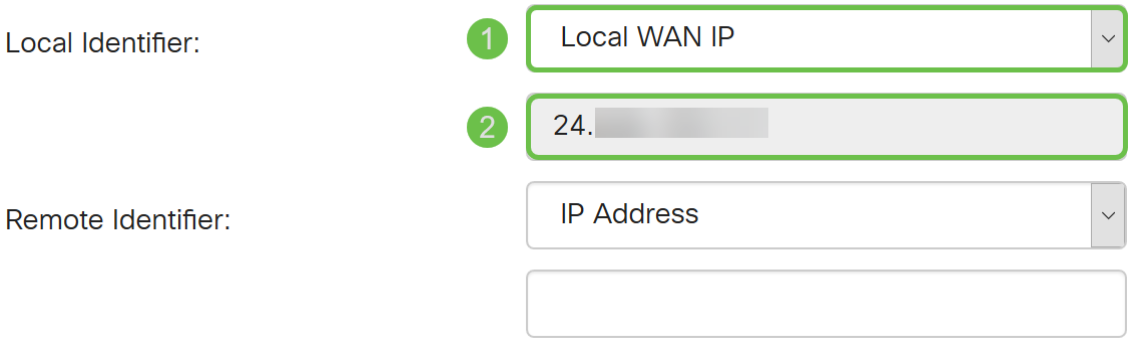


步驟9.從下拉選單中選擇*Local Identifier*。以下選項定義為：

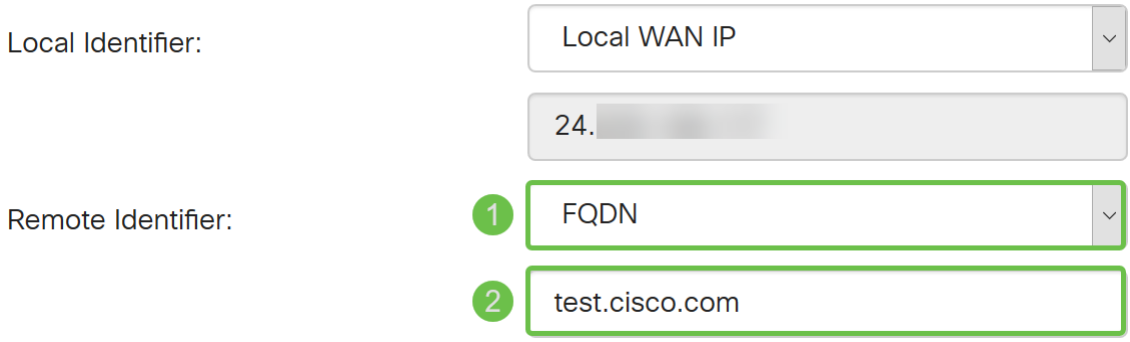
- 本地WAN IP — 此選項使用VPN網關的廣域網(WAN)介面的IP地址
- IP地址 — 此選項允許您手動輸入VPN連線的IP地址。您需要在站點（辦公室）輸入路由器的WAN IP地址。
- FQDN — 建立VPN連線時，此選項將使用路由器的完全限定域名(FQDN)。
- 使用者FQDN — 此選項可讓您為Internet上的特定使用者使用完整的域名。

在本例中，我們將選擇**本地WAN IP**作為我們的本地識別符號。

附註：將自動填寫路由器的本地WAN IP。



步驟10.在「*Remote Identifier*」下拉選單中，選擇**IP Address**、**FQDN**或**User FQDN**。然後輸入您選擇的相應響應。在本例中，我們將選擇**FQDN**並輸入**test.cisco.com**。



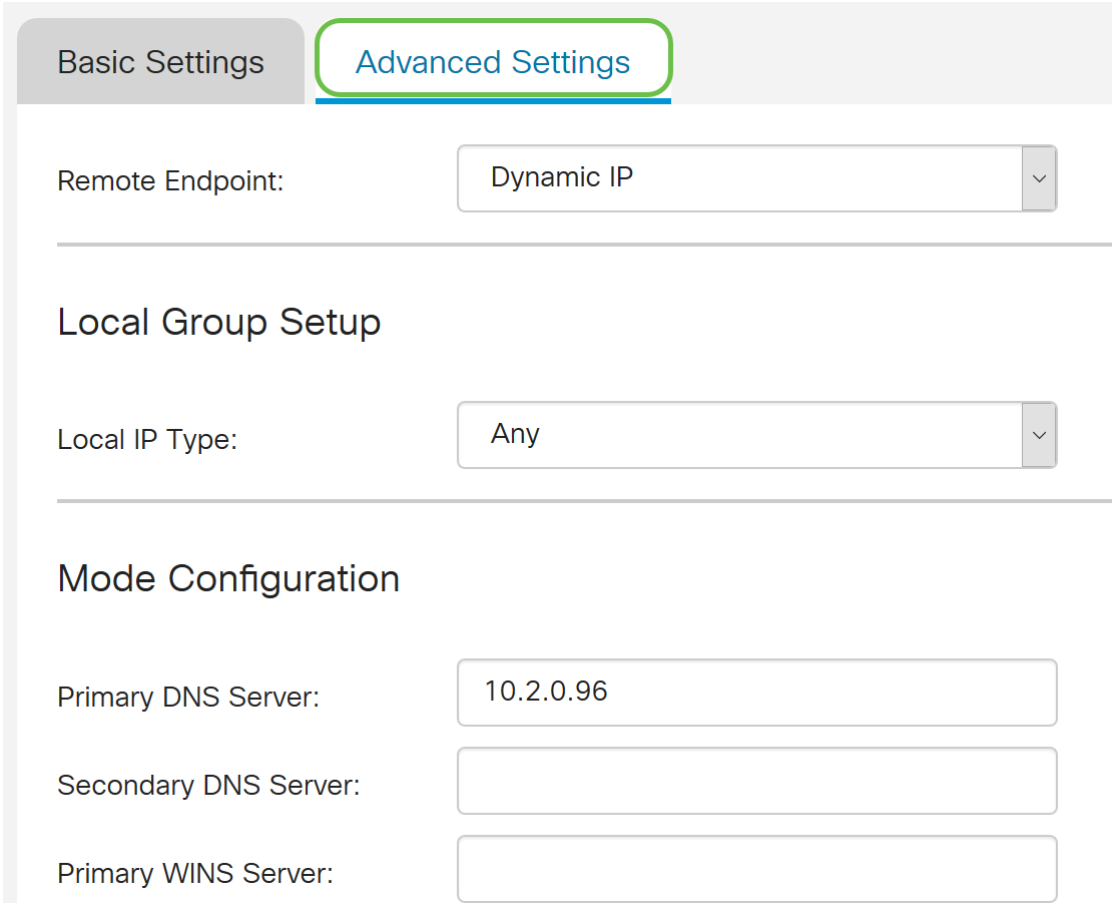
步驟11.勾選「**Extended Authentication**」覈取方塊以啟用。這將提供額外的身份驗證級別，要求遠端使用者在獲得對VPN的訪問許可權之前輸入其憑據。

如果您已啟用*Extended Authentication*，請點選plus 圖示以新增使用者組。從下拉選單中選擇要用於擴展身份驗證的組。我們將選擇**ShrewSoftGroup**作為組。

步驟12.在*Pool Range for Client LAN*中，在*Start IP*和*End IP*欄位中輸入可以分配給VPN客戶端的IP地址範圍。這需要一個與站點地址不重疊的地址池。

我們將輸入**10.2.1.1**作為*Start IP*，輸入**10.2.1.254**作為*End IP*。

步驟13。（可選）按一下**Advanced Settings**索引標籤。



步驟14。（可選）您可以在此處指定遠端終端IP地址。在本指南中，我們將使用**動態IP**，因為最終客戶端的IP地址不是固定的。

您還可以指定哪些內部資源在*本地組設定*下可用。

如果選擇**Any**，則所有內部資源都可用。

您還可以選擇使用內部DNS和WINS伺服器。為此，您需要在*模式配置*下指定它們。

您還可以使用全隧道或拆分隧道以及拆分DNS。

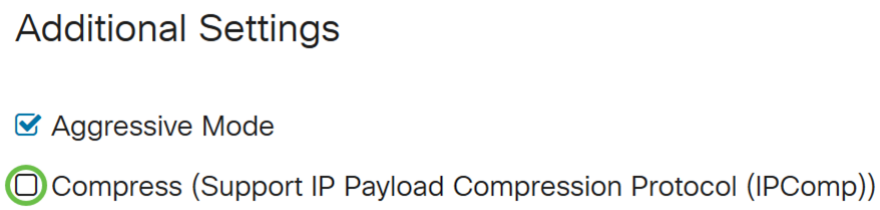
向下滾動至*Additional Settings*。選中**Aggressive Mode**覈取方塊以啟用Aggressive模式。主動模式是IKE SA的協商被壓縮為三個資料包，所有SA所需資料由發起方傳遞。談判速度更快，但他們存在以明文形式交換身份的漏洞。

附註：有關主模式與主動模式的其他資訊，請參閱：主模式與主動模式

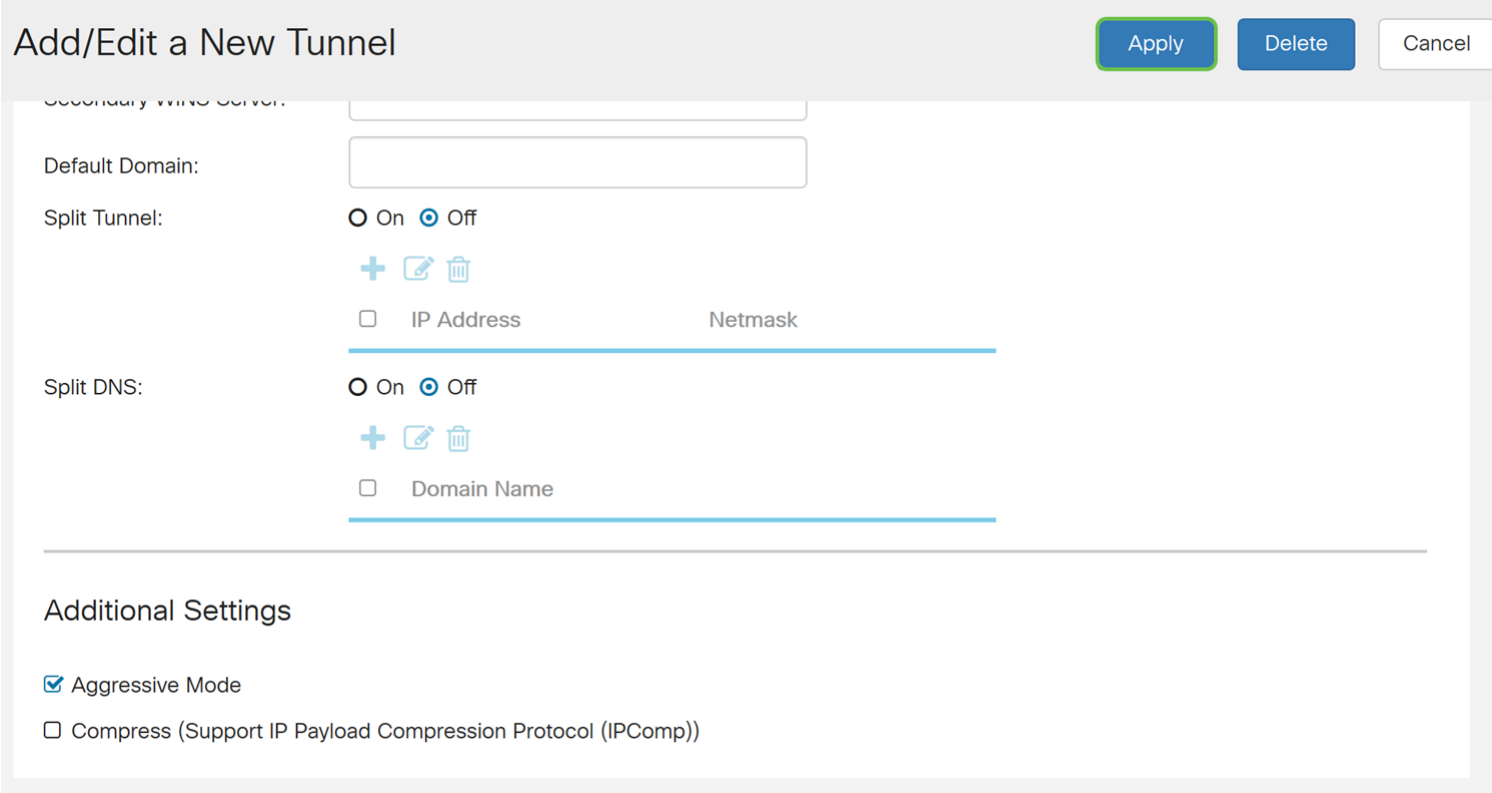
在本例中，我們將啟用**Aggressive Mode**。

步驟15。（可選）選中**Compress(支援IP負載壓縮協定(IPComp))**覈取方塊，使路由器能夠在啟動連線時建議壓縮。這是一種降低IP資料包大小的通訊協定。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。

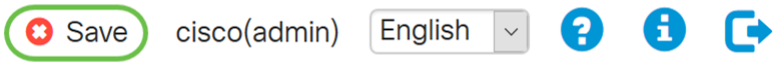
我們將取消對*Compress*的檢查。



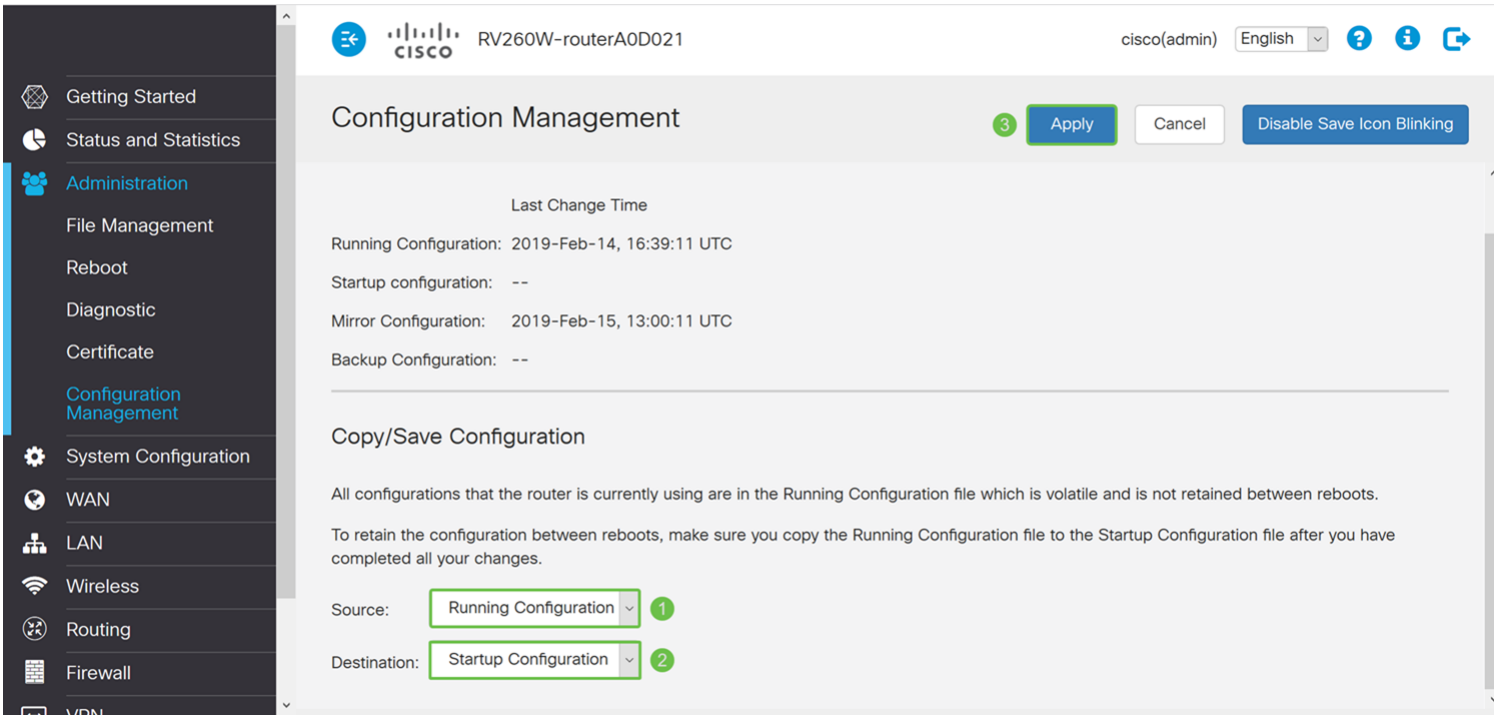
步驟16.按一下**Apply**以新增通道。



步驟17.按一下Web組態頁面頂端快閃的**Save**圖示。



步驟18.將開啟*Configuration Management*頁面。在「複製/儲存配置」部分，確保*Source* 欄位具有**Running Configuration** ，而*Destination* 欄位具有Startup Configuration。然後按下**Apply**。路由器當前使用的所有配置都位於運行配置檔案中，該檔案是易失性檔案，在重新啟動後不會保留。將運行配置檔案複製到啟動配置檔案會在重新啟動後保留您的配置。

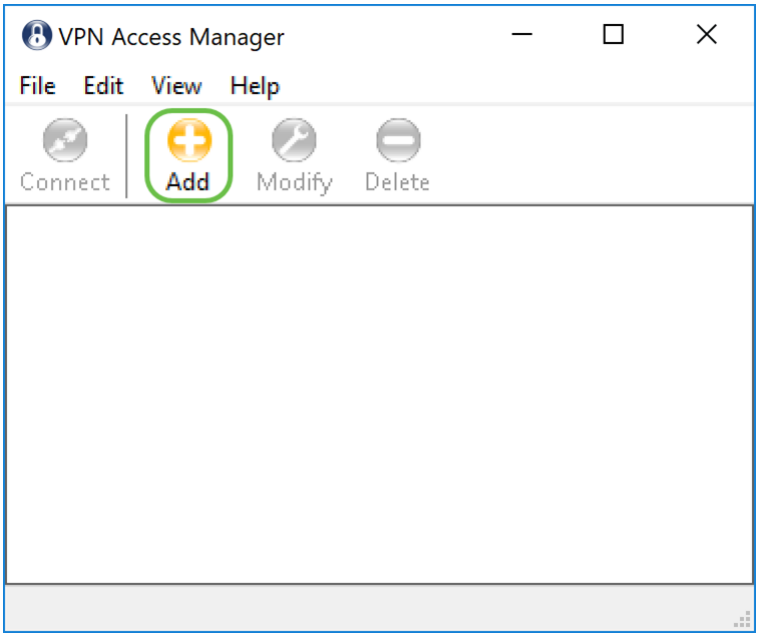


配置軟體VPN客戶端

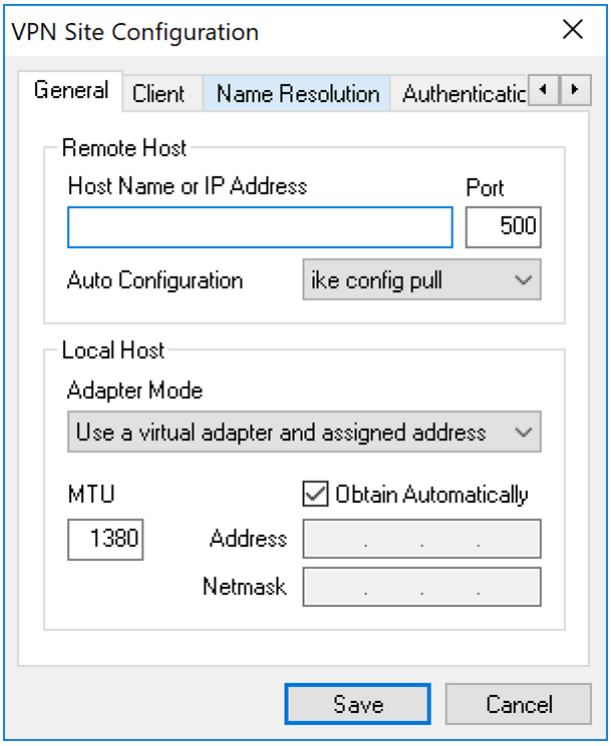
如果您尚未下載Shrew Soft VPN客戶端，請點選以下連結免費下載該客戶端：顯示Windows軟體VPN使用者端。我們將使用標準版。如果您已經下載了Shrew Soft VPN客戶端，請隨意進入第一步。

顯示軟VPN客戶端：常規頁籤

步驟1.開啟Shrew VPN Access Manager並按一下**Add**新增新配置檔案。

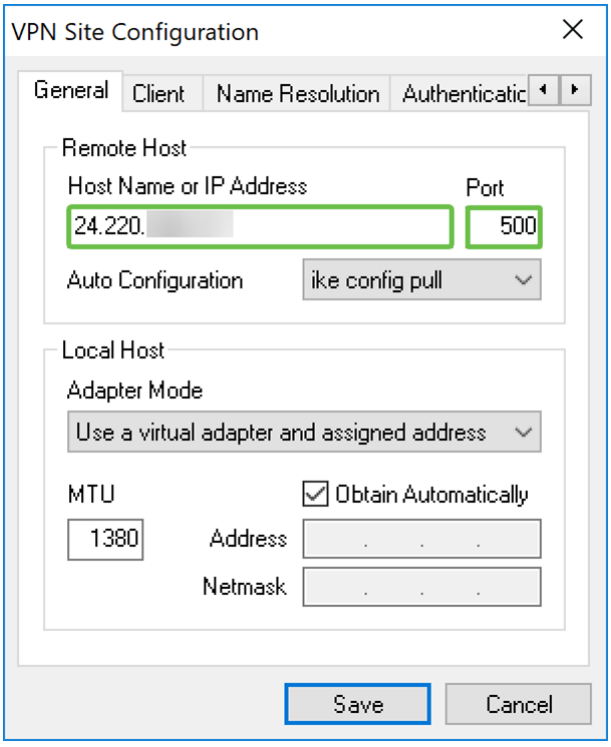


出現「*VPN Site Configuration*」視窗。



步驟2.在*General* 索引標籤下的*Remote Host* 區段中，輸入您嘗試連線的網路的公用主機名或IP地址。在本例中，我們將輸入現場的RV160/RV260的WAN IP地址以設定連線。

附註：確保埠號設定為預設值500。為使VPN正常工作，隧道使用UDP埠500，該埠應設定為允許通過防火牆轉發ISAKMP流量。



步驟3.在*Auto Configuration*下拉式清單中選擇一個選項。可用選項定義如下：

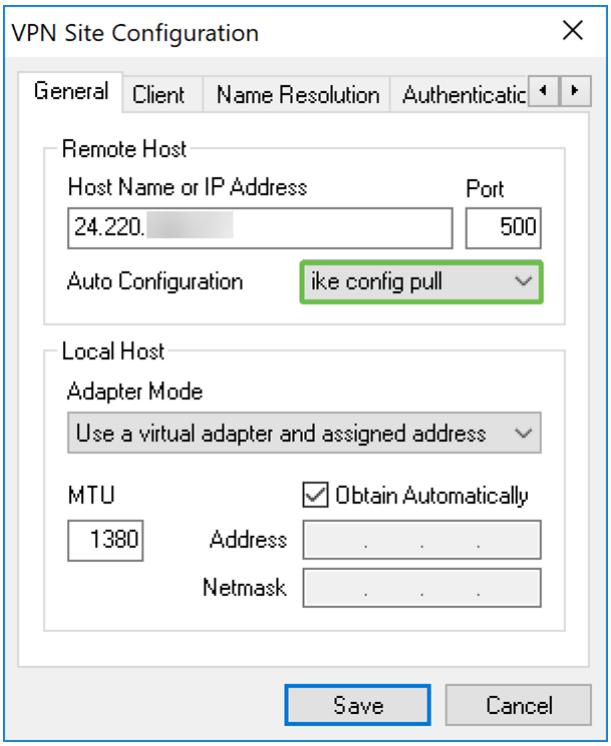
·**Disabled**

·**Ike Config Pull** 在電腦支援pull方法的情況下，請求將返回客戶端支援的設定清單。

·**Ike Config Push** 在電腦支援推送方法的情況下，請求將返回客戶端支援的設定清單。

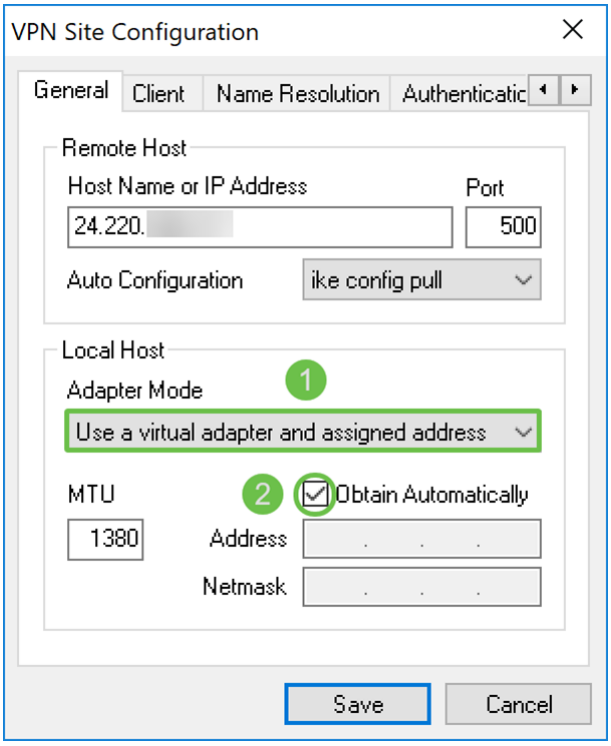
·**DHCP Over IPsec** ΔΗΧΠ οωερ ΙΠσεχ

在本例中，我們將選擇**ike config pull**。



步驟4.在*Local Host*部分中，在**Adapter Mode**下拉選單中選擇**Use a virtual adapter and assigned address**，然後選中**Obtain Automatically**覈取方塊。可用選項定義如下：

- **使用虛擬介面卡和分配的地址** — 允許客戶端使用具有指定地址的虛擬介面卡作為其IPsec通訊的源。
- **使用虛擬介面卡和隨機地址** — 允許客戶端使用具有隨機地址的虛擬介面卡作為其IPsec通訊的源。
- **使用現有介面卡和當前地址** — 允許客戶端僅使用其現有物理介面卡（當前地址為源）進行IPsec通訊。



顯示軟VPN客戶端：客戶端頁籤

步驟1。按一下*Client*索引標籤。在「*NAT Traversal*」下拉選單中，選擇在RV160/RV260上為NAT Traversal配置的相同設定。可用的Network Address Traversal(NATT)選單選項定義如下：

·**Disabled** NATT

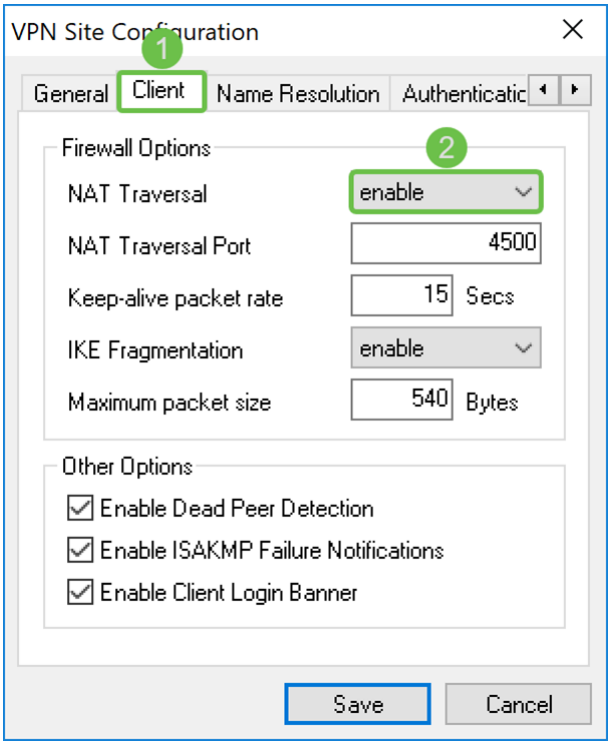
·**Enabled** çΠINNATNAT

·**Force-Draft** NATTΔραφτçΠINNAT

·**Force-RFC** NATPΦXçΠINNAT

• **Force-Cisco-UDP** NATçΠINYΔΠ

在本文檔中，我們將選擇**enable** for NAT Traversal，並保留*NAT Traversal Port*和*Keep-alive packet rate*作為預設值。



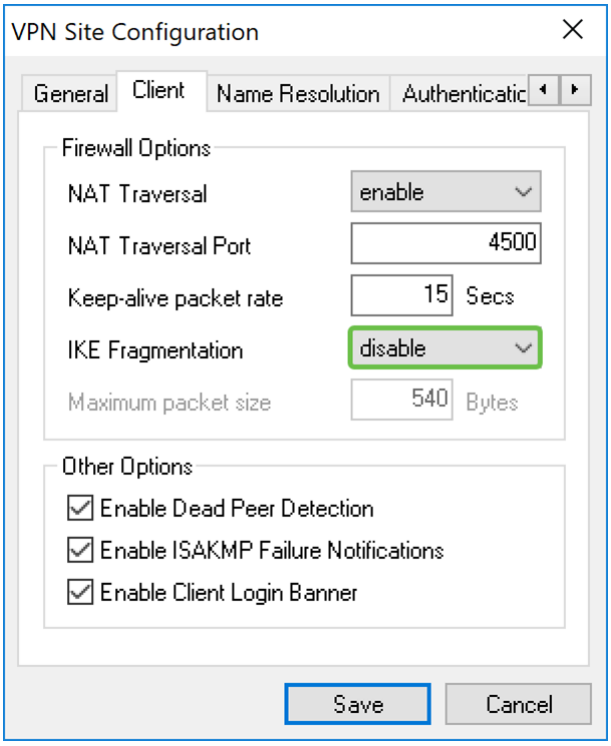
步驟2.在*IKE Fragmentation*下拉式清單中選擇**Disable**、**Enable**或**Force**。這些選項定義如下：

·**Disable** IKE

·**Enable** çΠINIKE

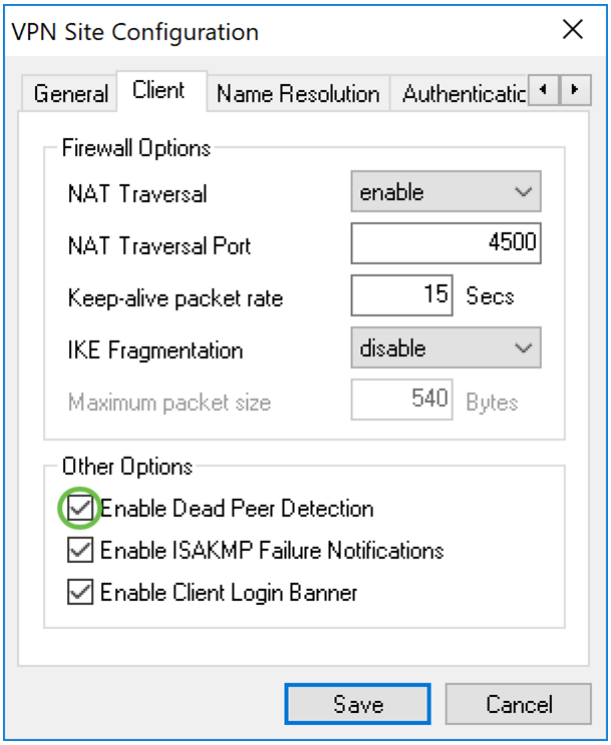
·**Force** IKEçΠN

我們選擇了**disable**進行*IKE分段*。



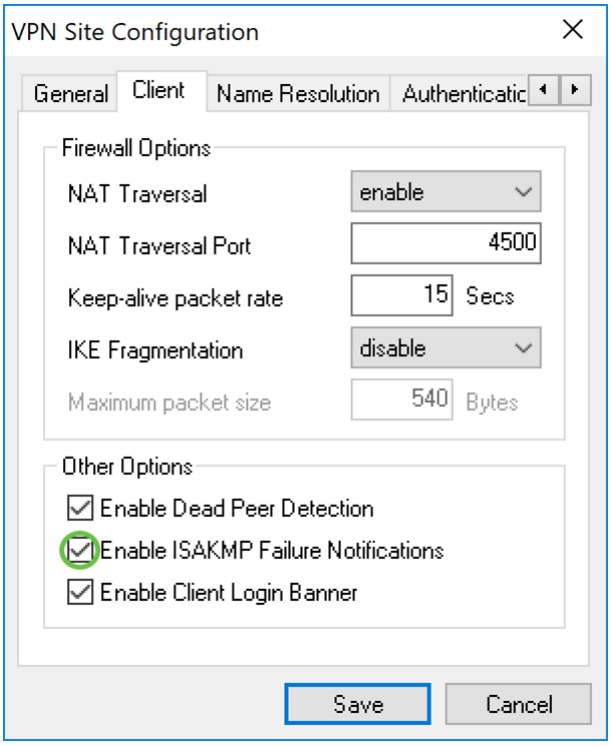
步驟3.選中**Enable Dead Peer Detection**覈取方塊以啟用Dead Peer Detection協定。如果啟用此選項，則只有在路由器支援時才使用它。這允許使用者端和路由器檢查通道的狀態，以偵測到哪一端不再能夠回應。預設情況下啟用此選項。

在本例中，我們將保持選中Dead Peer Detection。



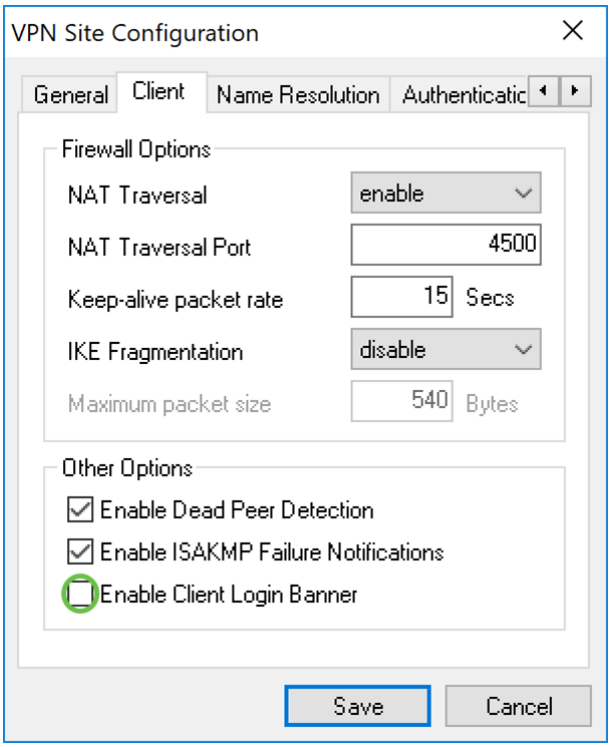
步驟4.選中**Enable ISAKMP Failure Notification**覈取方塊以從VPN客戶端IPsec守護程式啟用ISAKMP故障通知。預設情況下啟用。

在本示例中，我們將保持選中ISAKMP故障通知的狀態。



步驟5.取消選中**Enable Client Login Banner** 以禁用。這將在與路由器建立隧道後顯示登入標語。路由器必須支援事務交換，並配置為將登入標語轉發給客戶端。預設情況下啟用此值。

我們將取消選中客戶端登入橫幅。

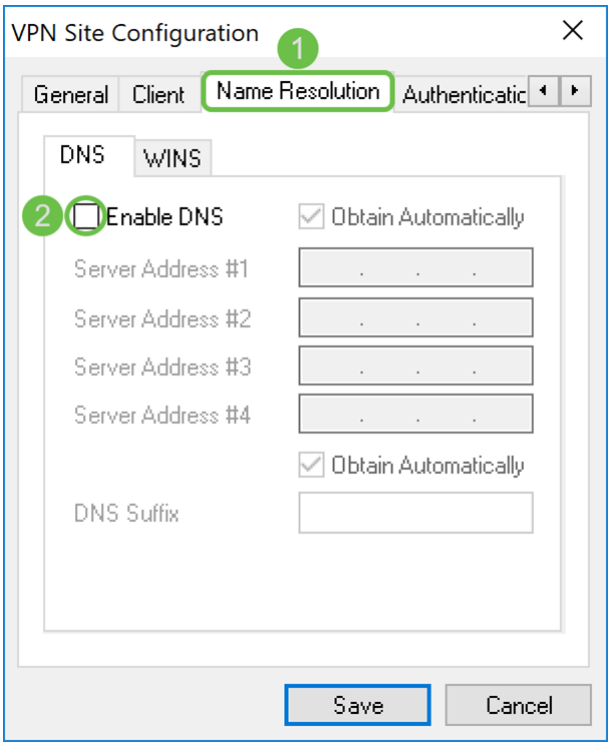


顯示軟VPN客戶端：名稱解析頁籤

步驟1.按一下*名稱解析*標籤，如果要啟用DNS，請選中**啟用DNS**覈取方塊。如果您的站點配置不需要特定DNS設定，請取消選中**Enable DNS**覈取方塊。

如果選中*Enable DNS*，並且遠端網關配置為支援配置交換，則網關能夠自動提供DNS設定。如果未選中，請驗證**Obtain Automatically**覈取方塊是否已取消選中，並手動輸入有效的DNS伺服器地址。

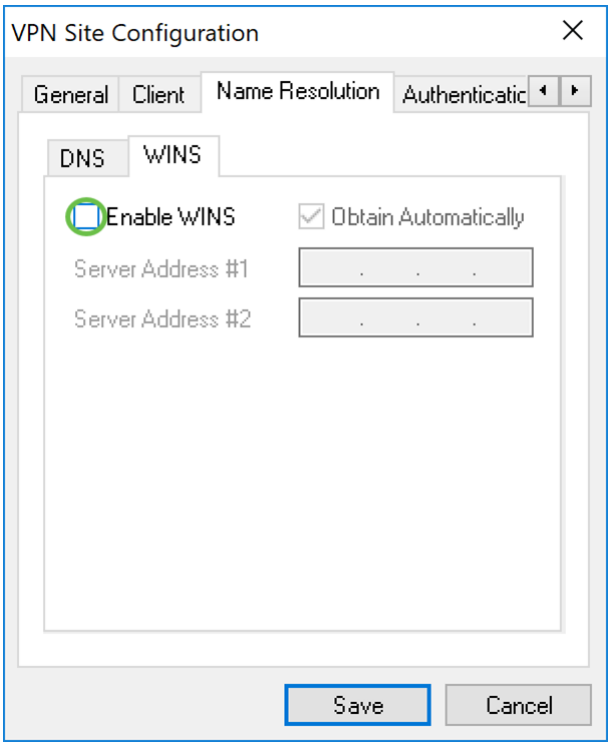
在本例中， **Enable DNS** 未選中。



步驟2.如果要啟用Windows Internet Name Server(WINS)，請選中**Enable WINS**覈取方塊。如果您的遠端網關配置為支援配置交換，則該網關能夠自動提供WINS設定。如果未選中，請確認**Obtain Automatically**覈取方塊未選中並手動輸入有效的WINS伺服器地址。

附註：通過提供WINS配置資訊，客戶端將能夠使用位於遠端專用網路中的伺服器解析WINS名稱。這在嘗試使用統一命名約定路徑名訪問遠端Windows網路資源時很有用。WINS伺服器通常屬於Windows域控制器或Samba伺服器。

在本例中， **Enable WINS**未選中。



顯示軟VPN客戶端：Authentication頁籤

步驟1。點選*Authentication*頁籤，然後在**Authentication Method**下拉選單中選擇**Mutual PSK + XAuth**。可用選項定義如下：

·**混合RSA +擴展驗證** 使用者端會驗證閘道。憑據將採用PEM或PKCS12證書檔案或金鑰檔案型別的形式。

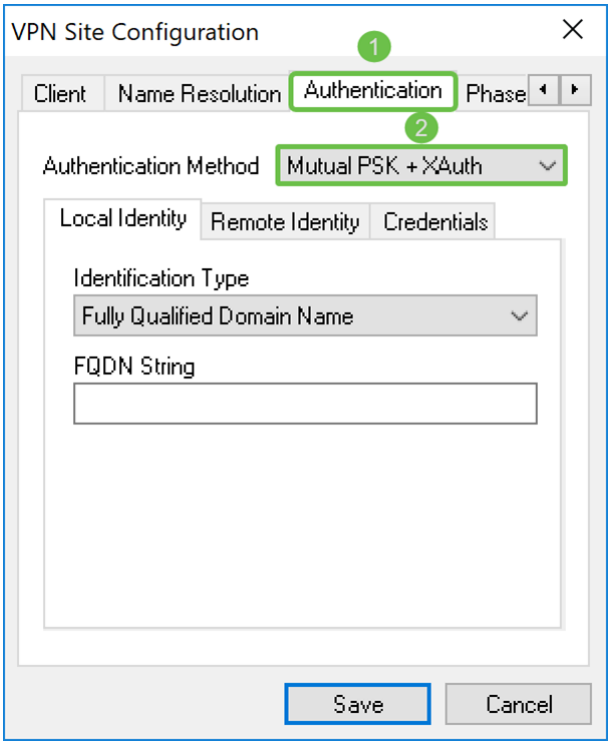
·**混合GRP +擴展驗證** 使用者端會驗證閘道。憑證將採用PEM或PKCS12證書檔案和共用金鑰字串的形式。

·**Mutual RSA + XAuth** 憑證將採用PEM或PKCS12證書檔案或金鑰型別的形式。

·**Mutual PSK + XAuth** 憑據將採用共用金鑰字串的形式。

·**Mutual RSA** 憑證將採用PEM或PKCS12證書檔案或金鑰型別的形式。

·**雙向PSK** 憑據將採用共用金鑰字串的形式。



步驟2.在*Local Identity*頁籤中，選擇標識型別，然後在空欄位中輸入相應的字串。以下選項定義為：

·**Any** 客戶端將接受任何ID型別和值。應謹慎使用此方法，因為它會繞過IKE第1階段識別過程的一部分。

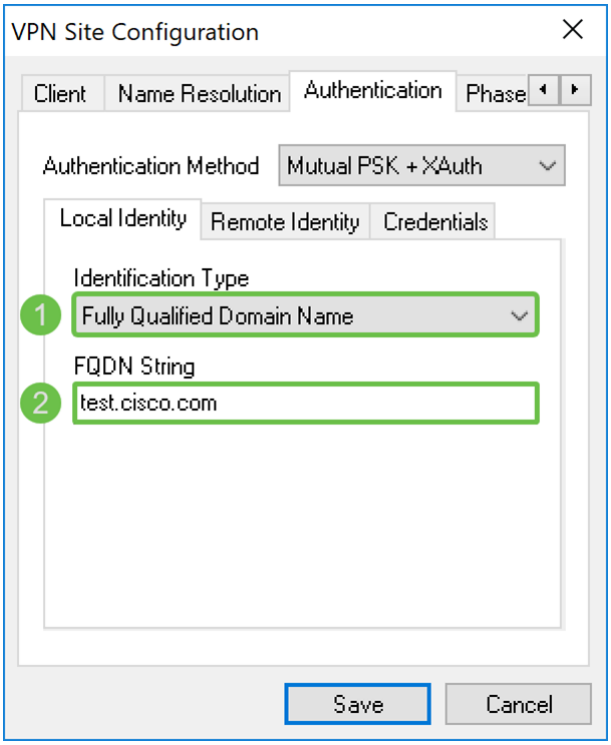
• **完全限定域名** — 此選項必須提供DNS域字串形式的FQDN字串。例如，「cisco.com」將是可接受的值。如果使用PSK身份驗證模式，客戶端將只允許選擇此選項。

• **使用者完全限定域名** — 必須以user@domain字串的形式提供使用者FQDN字串。例如，"dave@cisco.com"是一個可接受的值。如果使用PSK身份驗證模式，客戶端將只允許選擇此選項。

·**IP Address** ш*Use a discovered local host address*這意味著將自動確定該值。如果要使用除用於與客戶端網關通訊的介面卡地址以外的地址，請取消選中該覈取方塊。然後，輸入特定地址字串。如果使用PSK身份驗證模式，客戶端將只允許選擇此選項。

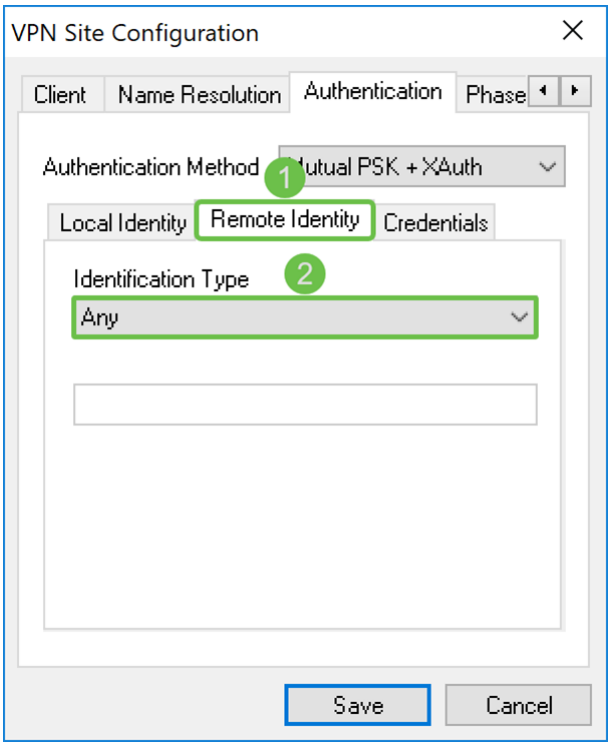
·**Key Identifier**

在本例中，我們將選擇**完全限定域名**，並在**FQDN字串**欄位中輸入**test.cisco.com**。



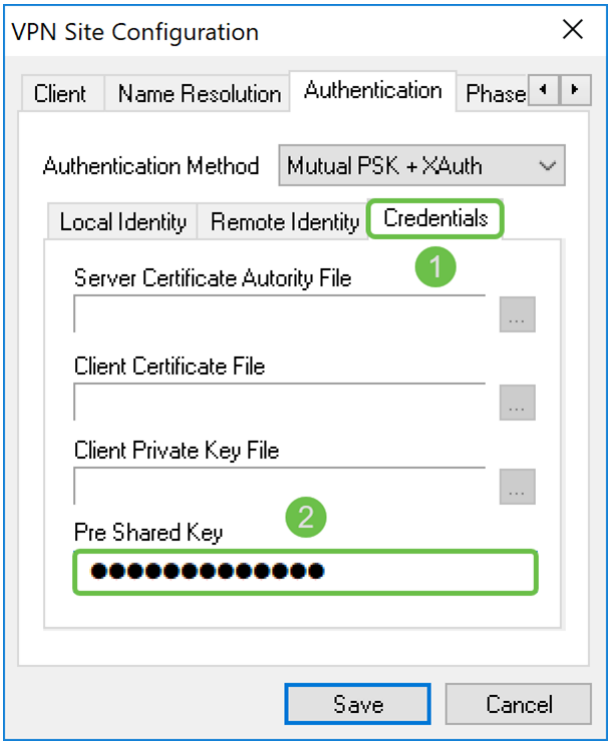
步驟3.按一下*Remote Identity*頁籤並選擇標識型別。選項包括：任何完全限定域名、使用者完全限定域名、IP地址或金鑰識別符號。

在本檔案中，我們將使用**Any**作為我們的標識型別。



步驟4.按一下*Credentials*頁籤，並輸入在RV160/RV260上配置的相同預共用金鑰。

我們將進入**CiscoTest123!**在*Pre Shared Key*欄位中。

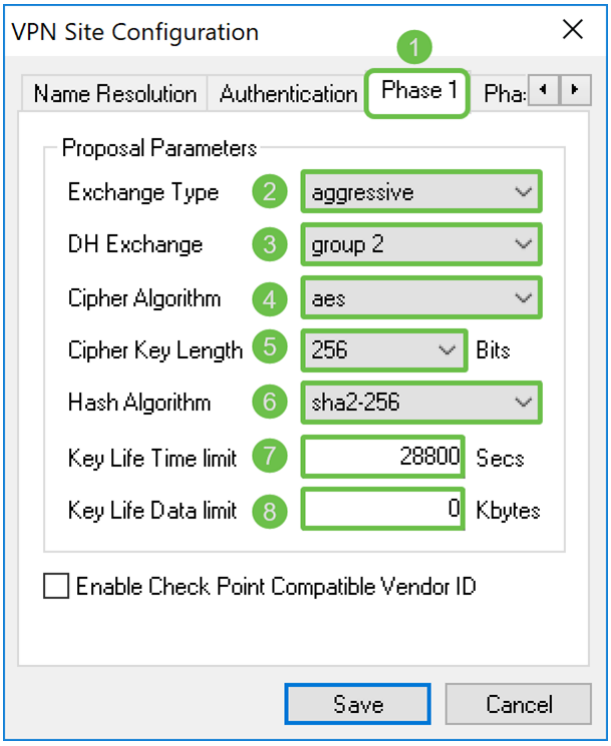


顯示軟VPN客戶端：階段1頁籤

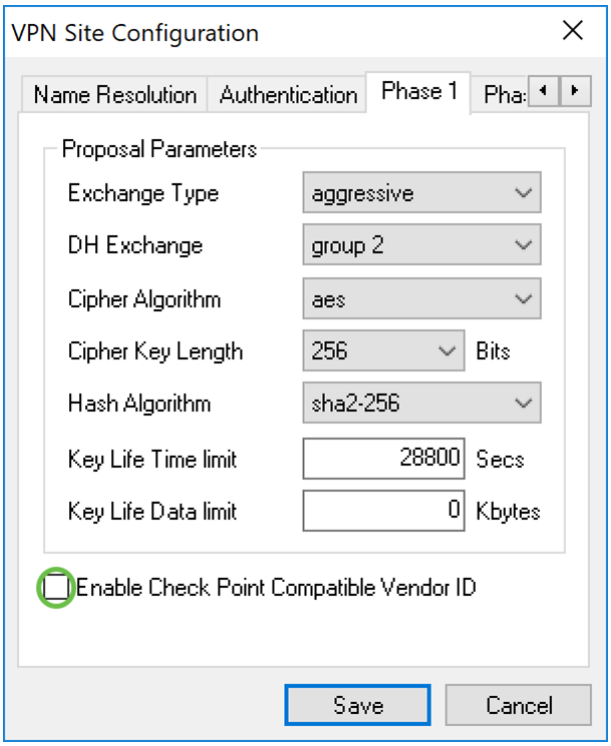
步驟1。按一下*Phase 1* 索引標籤。配置以下引數，使其與為RV160/RV260配置的設定相同。

Shrew Soft中的引數應匹配您在階段1中選擇的RV160/RV260配置。在本文檔中，Shrew Soft中的引數將設定為：

- Exchange型別：**攻擊性**
- DH交換：**組2**
- 密碼演算法：**aes**
- 金鑰長度：**256**
- 雜湊演算法：**sha2-256**
- 主要使用期限：**28800**
- 關鍵壽命資料限制：**0**



步驟2.（可選）如果您的網關在第1階段協商期間提供思科相容供應商ID，請選中**Enable Check Point Compatible Vendor ID**覈取方塊。如果網關不提供思科相容的供應商ID，或者如果您不確定，請取消選中覈取方塊。我們將取消選中該覈取方塊。



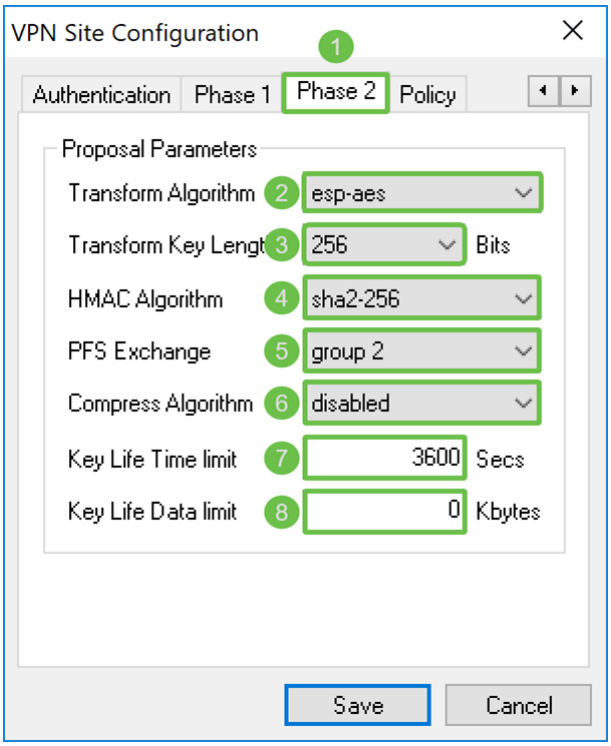
顯示軟VPN客戶端：階段2頁籤

步驟1。按一下*Phase 2* 索引標籤。配置以下引數，使其與為RV160/RV260配置的設定相同。

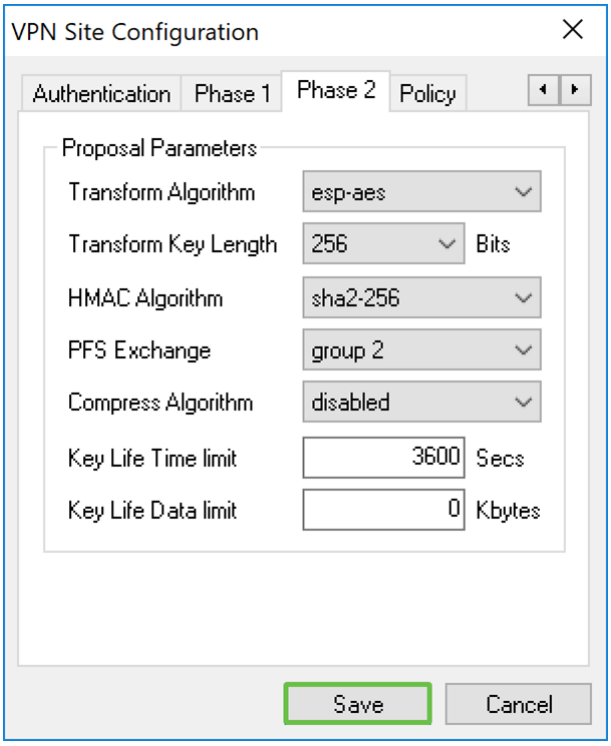
引數應與第2階段中的RV160/260配置匹配，如下所示：

- 轉換演算法：**esp-aes**
- 轉換金鑰長度：**256**

- HMAC演算法：**sha2-256**
- PFS Exchange:**組2**
- **壓縮演算法：已禁用**
- **主要使用期限：3600**
- **關鍵壽命資料限制：0**



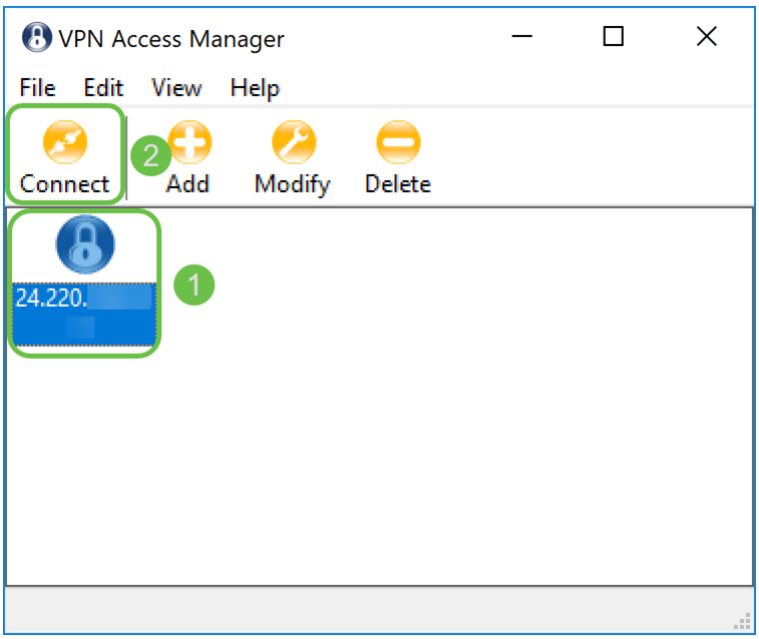
步驟2.按頁面底部的**Save**按鈕以儲存配置。



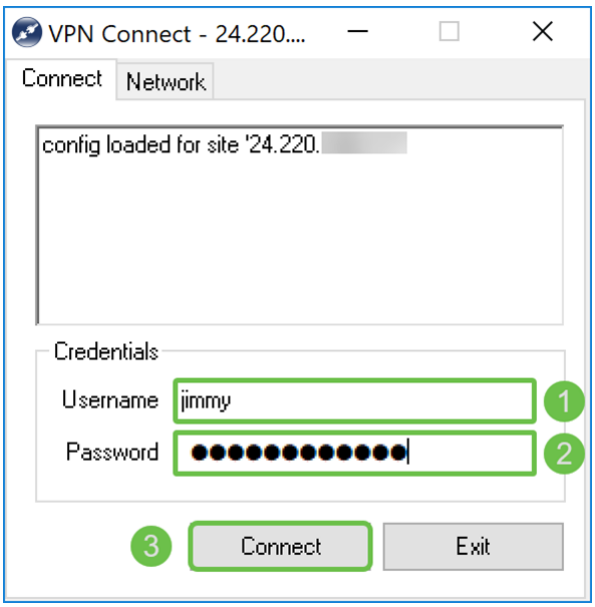
顯示軟VPN客戶端：正在連線

步驟1.在*VPN訪問管理器*中，選擇您剛剛建立的VPN配置檔案。然後按下**Connect**。

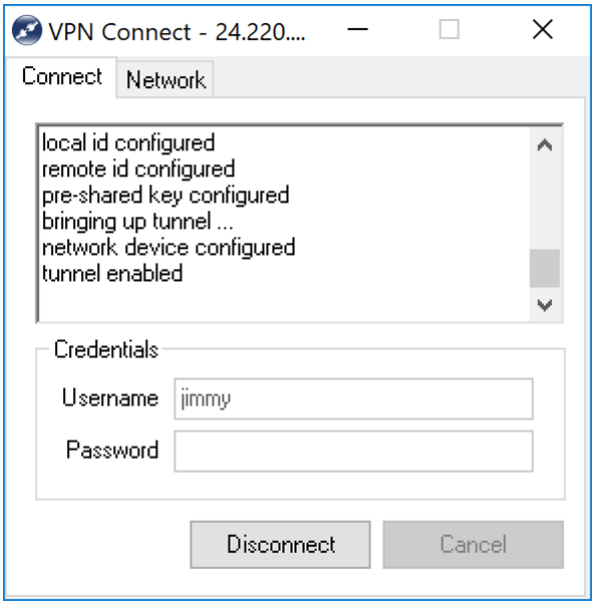
附註：如果要重新命名VPN配置檔案，請按一下右鍵該配置檔案並選擇**Rename**。配置檔案中的部分IP地址被模糊以保護該網路。



步驟2.出現*VPN Connect*視窗。輸入在*建立使用者帳戶*部分建立的使用者名稱和密碼。然後按下**Connect**。

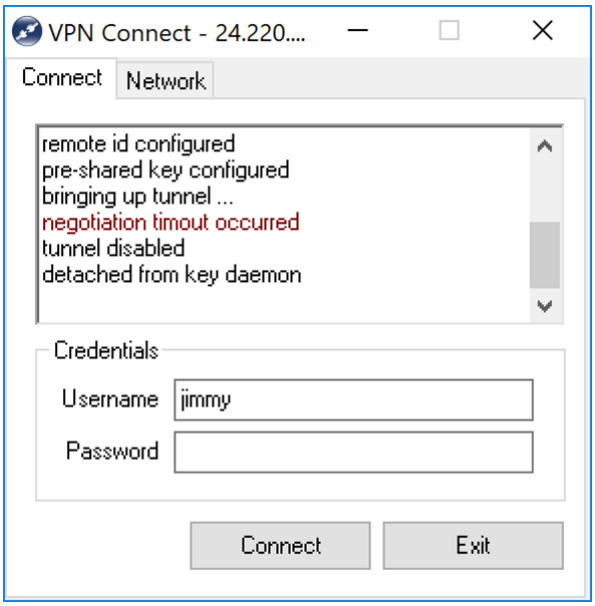


步驟3.按*Connect*後，配置資訊會隨請求通訊一起傳遞到IKE守護程式。連線狀態的不同消息顯示在輸出視窗中。如果連線成功，您將收到一條消息「network device configured」和「tunnel enabled」。*Connection*按鈕將更改為*Disconnect*按鈕。

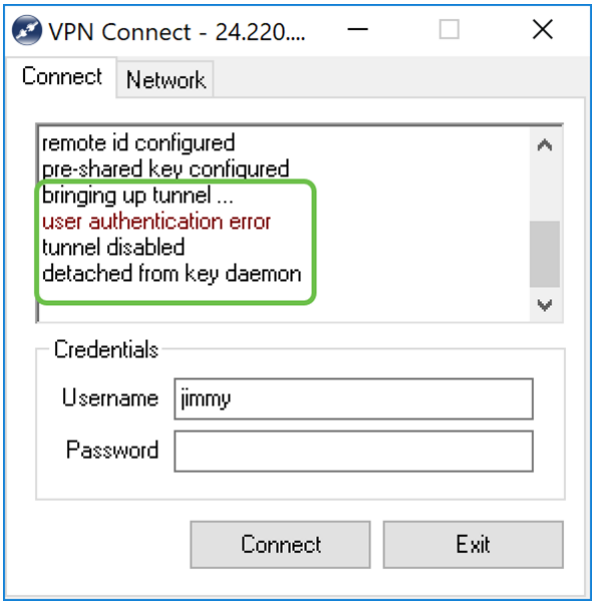


VPN連線故障排除提示

如果您收到錯誤消息「協商超時」、「隧道已禁用」和「與金鑰守護程式分離」。您可能需要仔細檢查路由器和顯示軟VPN客戶端上的配置，以確保它們匹配。

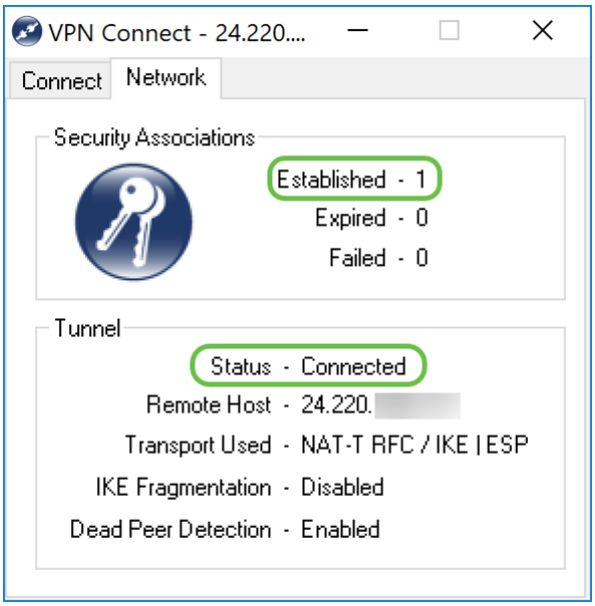


如果您收到錯誤消息顯示「user authentication error」，則表示您輸入了錯誤的使用者名稱密碼。請仔細檢查使用者憑據，並確保已正確配置和輸入該憑據。

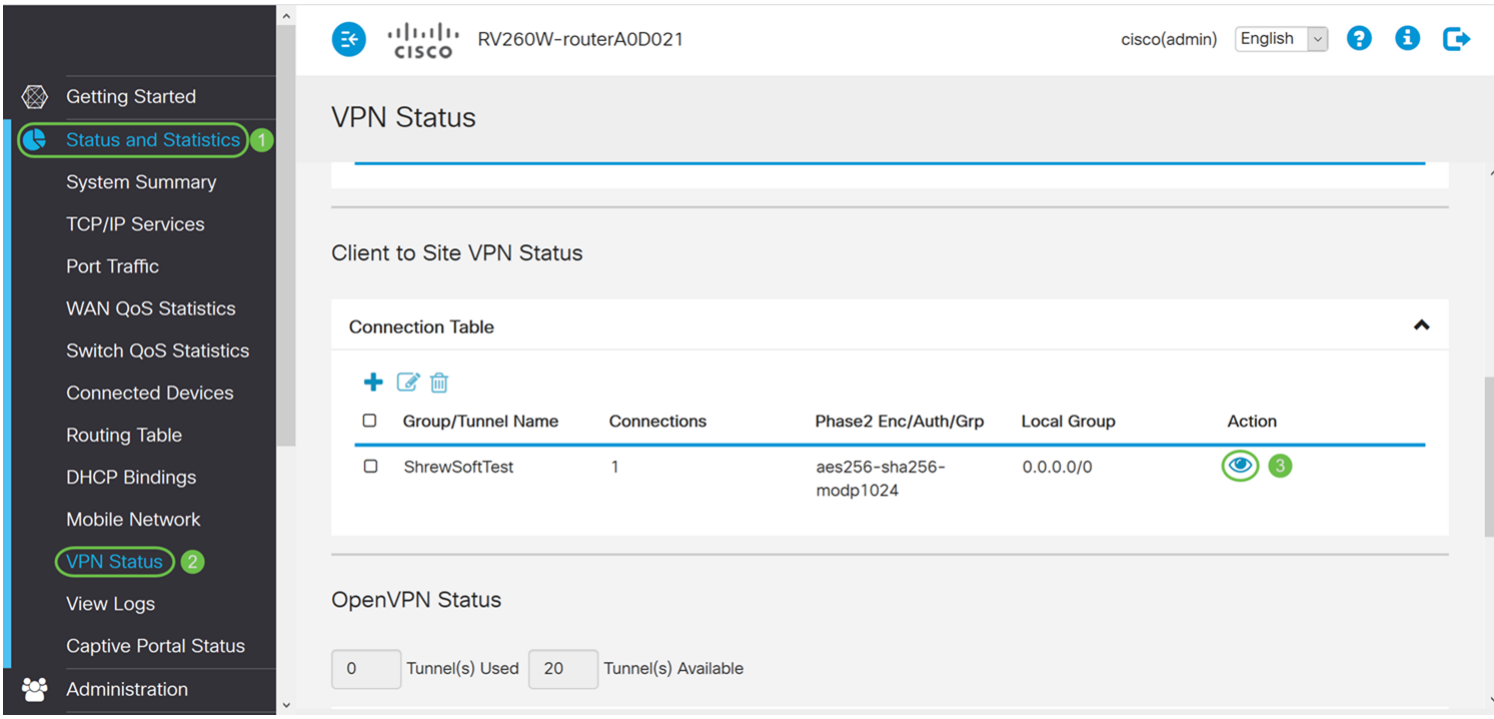


驗證

步驟1.在*VPN connect*視窗中按一下*Network*頁籤。在此頁籤中，您應該能夠檢視連線的當前網路統計資訊。在*Tunnel*部分中，您應該看到*Connected*作為狀態。

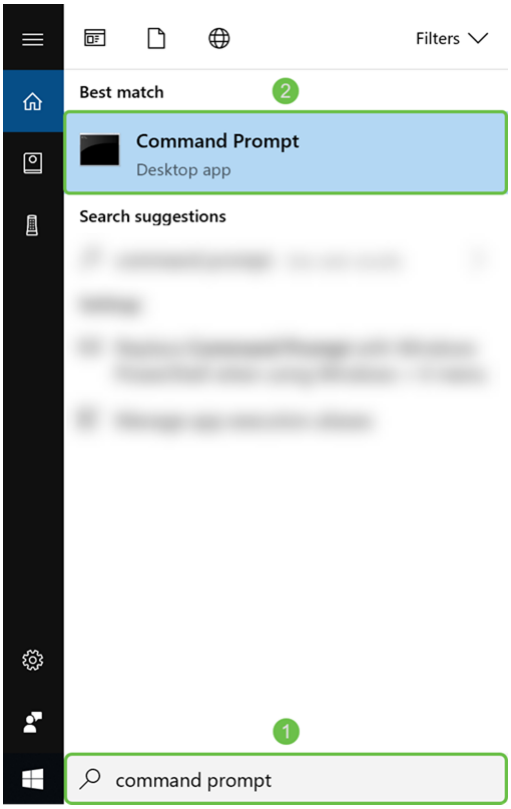


步驟2.在路由器上，導航到**Status and Statistics > VPN Status**。在*VPN Status*頁面中，向下滾動至*Client to Site VPN Status*部分。在此部分中，可以檢視所有客戶端到站點的連線。按一下**眼睛**圖示檢視更多詳細資訊。



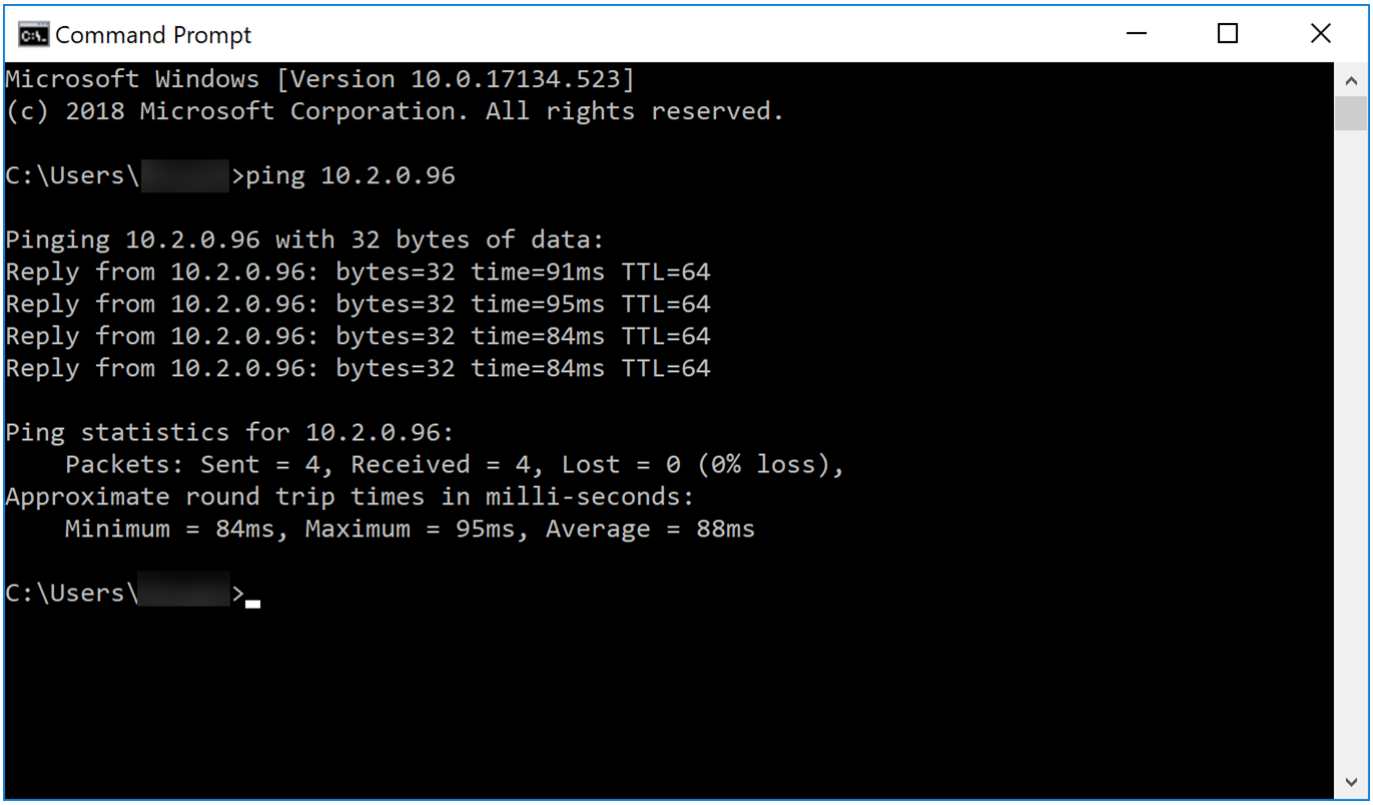
步驟3.導航到工作列上的搜尋欄，然後搜尋**命令提示**。

附註：以下說明用於Windows 10作業系統。具體取決於您使用的作業系統。



步驟4.鍵入不帶引號的命令「**ping [路由器的專用IP地址]**」，但輸入的是專用IP地址，而不是單詞。您應該能夠成功ping通路由器的私有IP地址。

在本例中，我們將鍵入**ping 10.2.0.96**。10.2.0.96是路由器的專用IP地址。



結論

現在，您應該已經成功地將您的軟體VPN客戶端連線到RV160或RV260。