在RV130和RV130W上使用Shrew Soft VPN客戶端連線IPSec VPN伺服器

目標

通過IPSec VPN（虛擬專用網路），您可以通過建立網際網路上的加密隧道來安全地獲取遠端資源。

RV130和RV130W充當IPSec VPN伺服器，並支援Shrew Soft VPN客戶端。

確保下載最新版本的客戶端軟體。

·Shrew軟體(https://www.shrew.net/download/vpn)

附註：要成功設定並配置帶有IPSec VPN伺服器的Shrew Soft VPN客戶端，您需要首先配置IPSec VPN伺服器。有關如何執行此操作的資訊，請參閱*在RV130和RV130W上配置IPSec VPN伺服器。*

本文檔的目的是向您展示如何使用Shrew Soft VPN客戶端連線到RV130和RV130W上的IPSec VPN伺服器。

適用裝置

·RV130W無線 — N VPN防火牆

·RV130 VPN防火牆

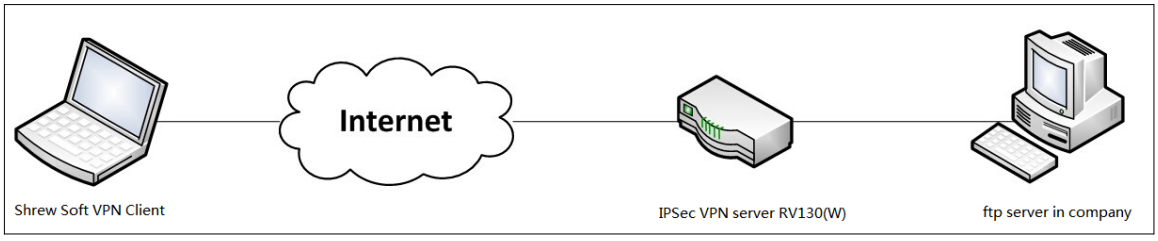
系統要求

·32或64位系統

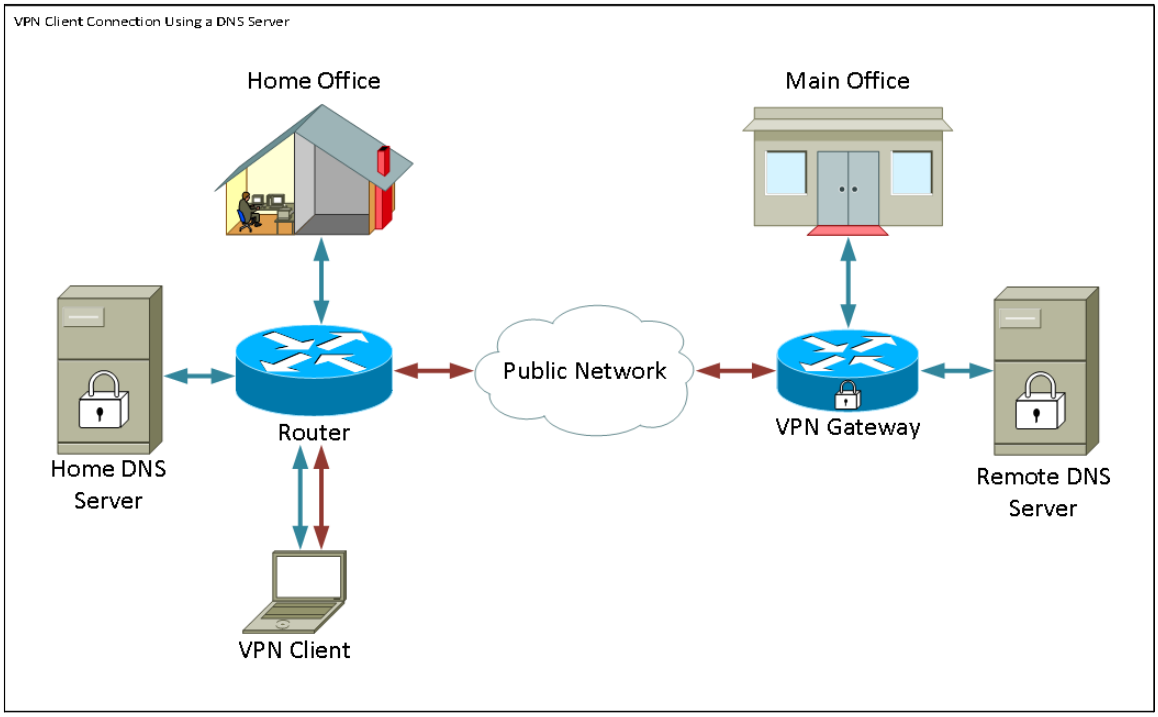
·Windows 2000、XP、Vista或Windows 7/8

拓撲

下面顯示了頂級拓撲，說明Shrewsoft客戶端到站點配置中涉及的裝置。



下面是一個更詳細的流程圖，說明DNS伺服器在小型企業網路環境中的作用。



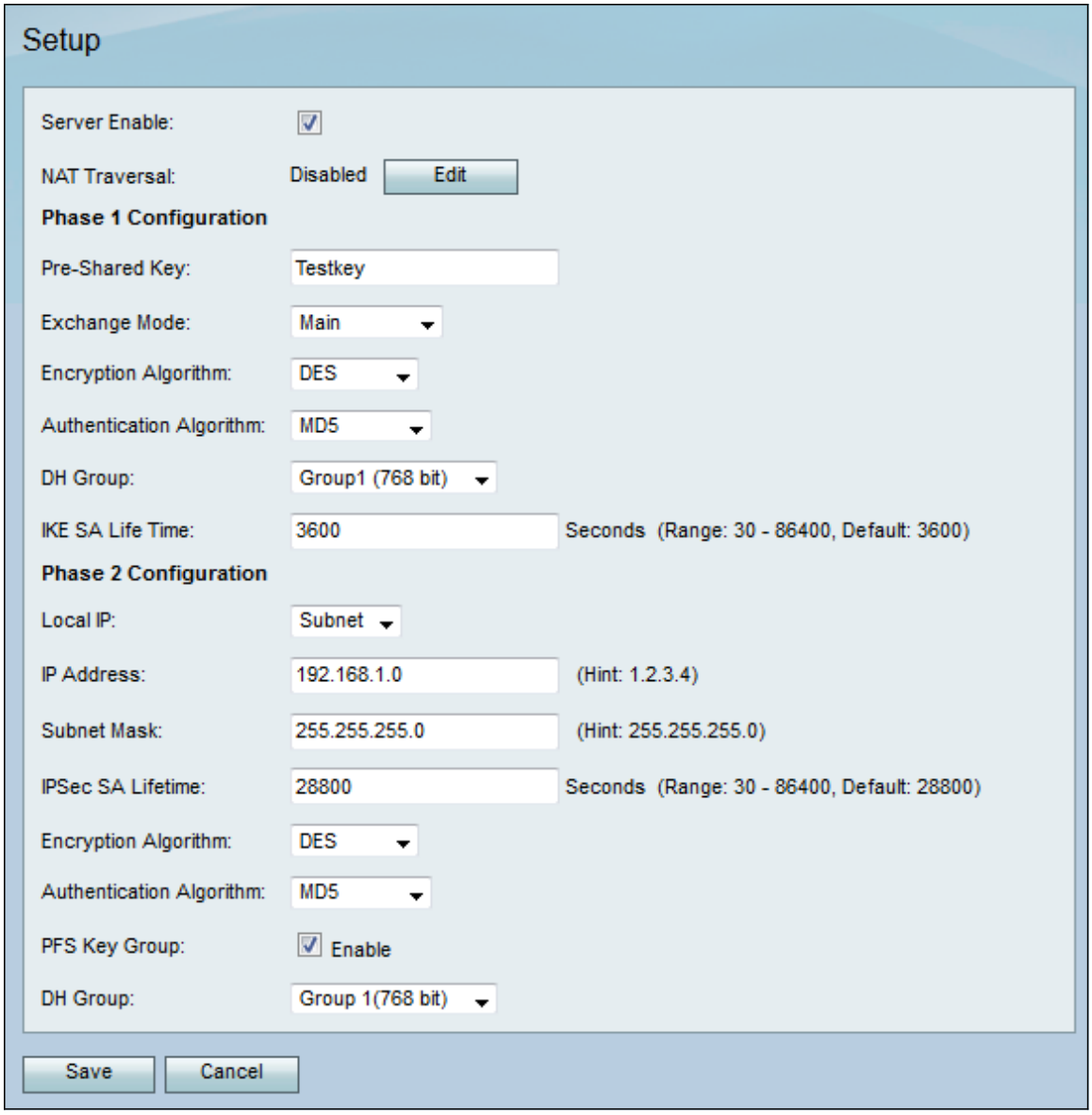
軟體版本

- 1.0.1.3

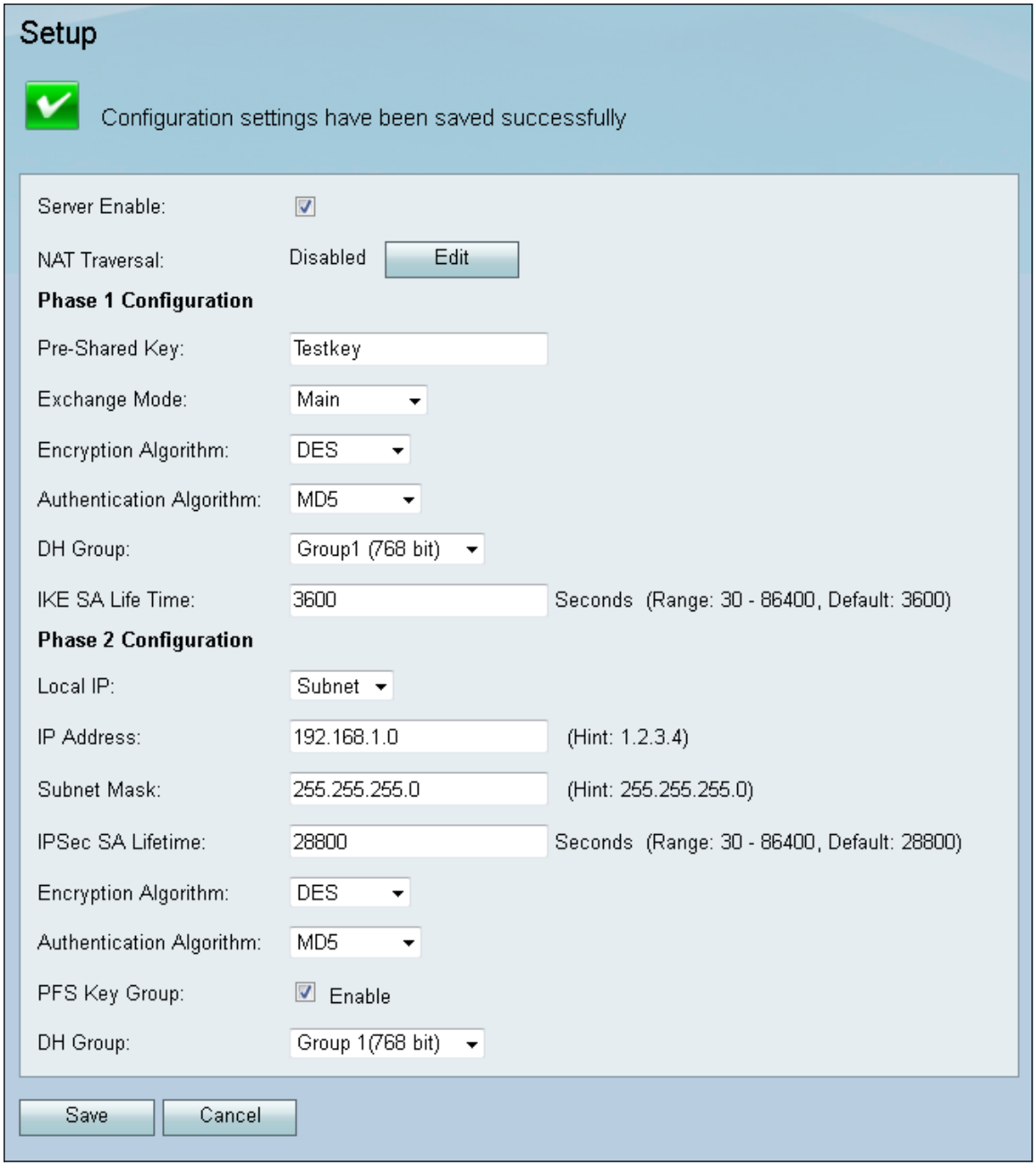
設定顯示軟VPN客戶端

IPSec VPN設定和使用者配置

步驟1.登入到Web配置實用程式並選擇**VPN > IPSec VPN Server > Setup**。將開啟*Setup*頁面。

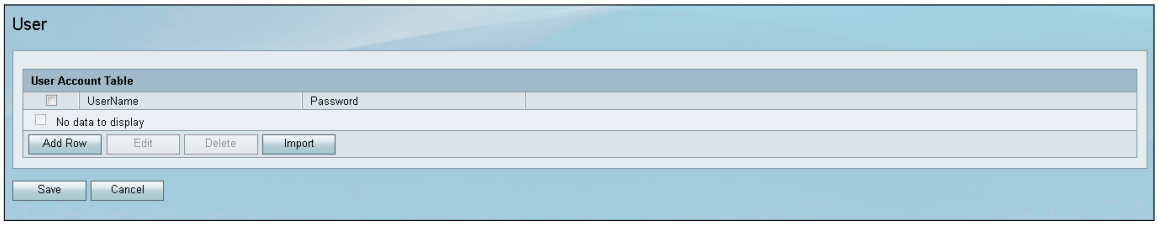


步驟2.驗證是否已正確配置RV130的IPSec VPN伺服器。如果IPSec VPN伺服器未配置或配置錯誤，請參閱*在RV130和RV130W上配置IPSec VPN伺服器*，然後按一下**Save**。

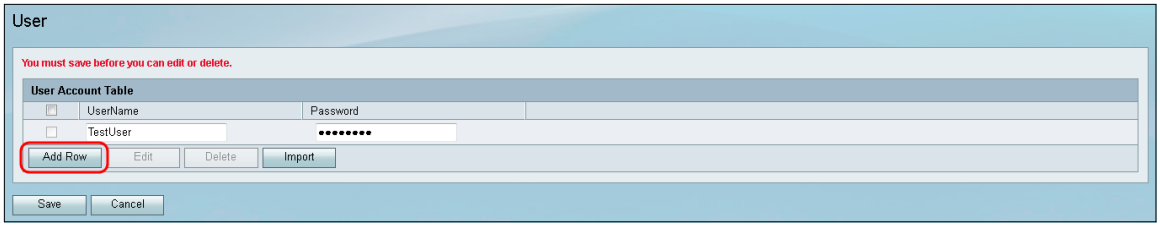


附註：以上設定是RV130/RV130W IPSec VPN伺服器配置的示例。這些設定基於*RV130和RV130W上的IPSec VPN伺服器配置*文檔，將在後續步驟中參考。

步驟3.導航到**VPN > IPSec VPN Server > User**。系統將顯示*User*頁面。



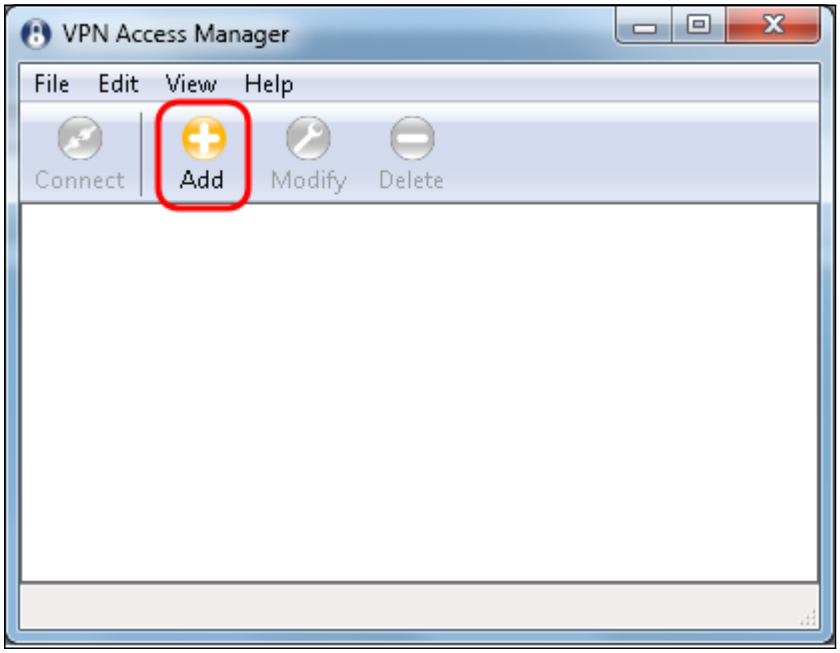
步驟4.單擊**Add Row**以新增使用者帳戶，用於對VPN客戶端進行身份驗證（擴展身份驗證），並在提供的欄位中輸入所需的使用者名稱和密碼。



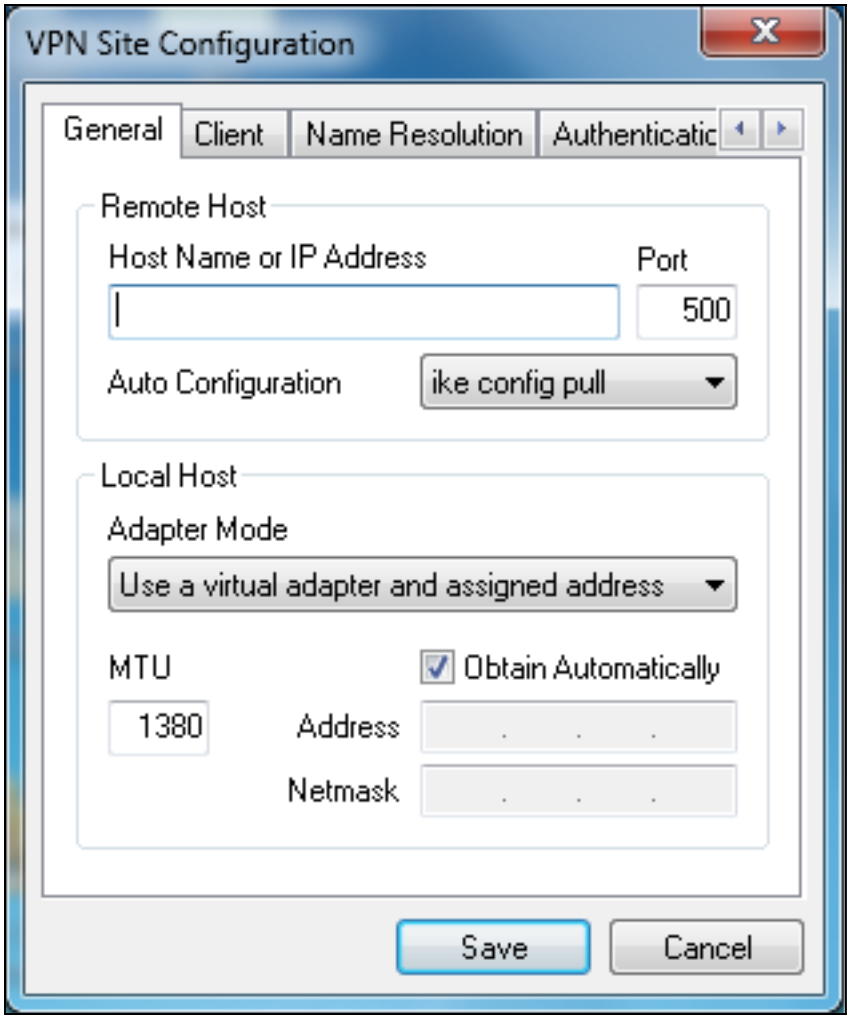
步驟5.按一下**Save**以儲存設定。

VPN客戶端配置

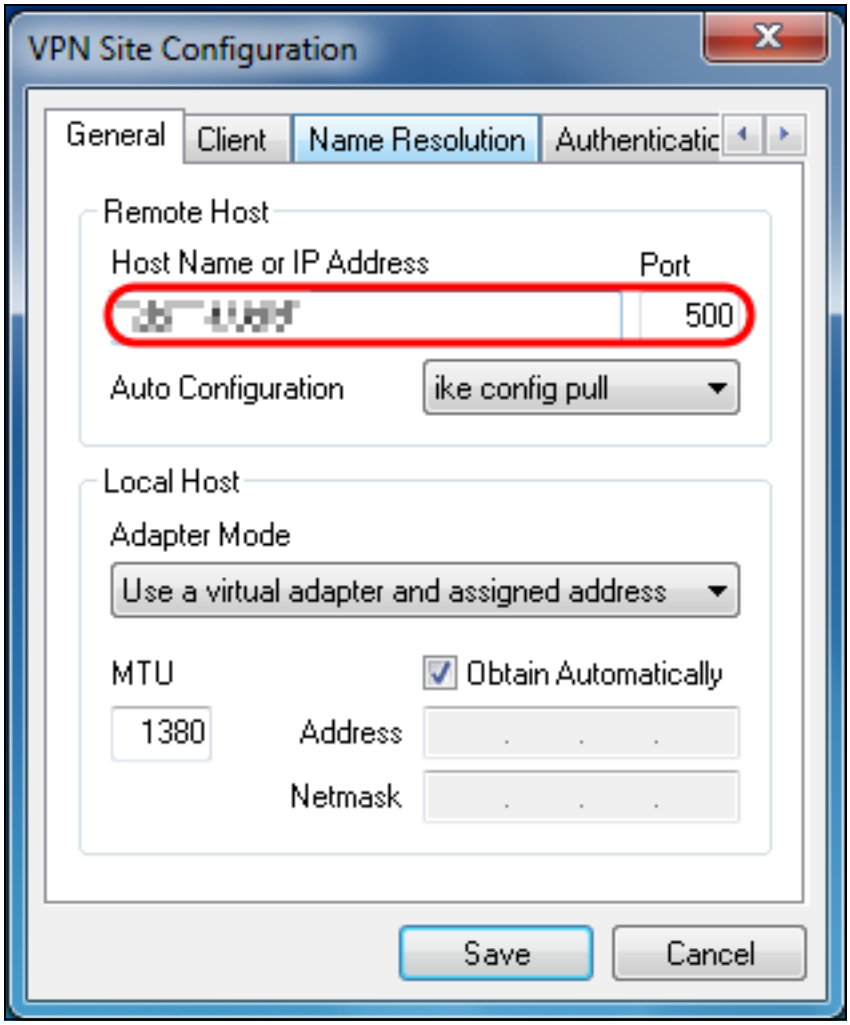
步驟1.開啟Shrew VPN Access Manager並按一下**Add**新增配置檔案。



出現「*VPN Site Configuration*」視窗。

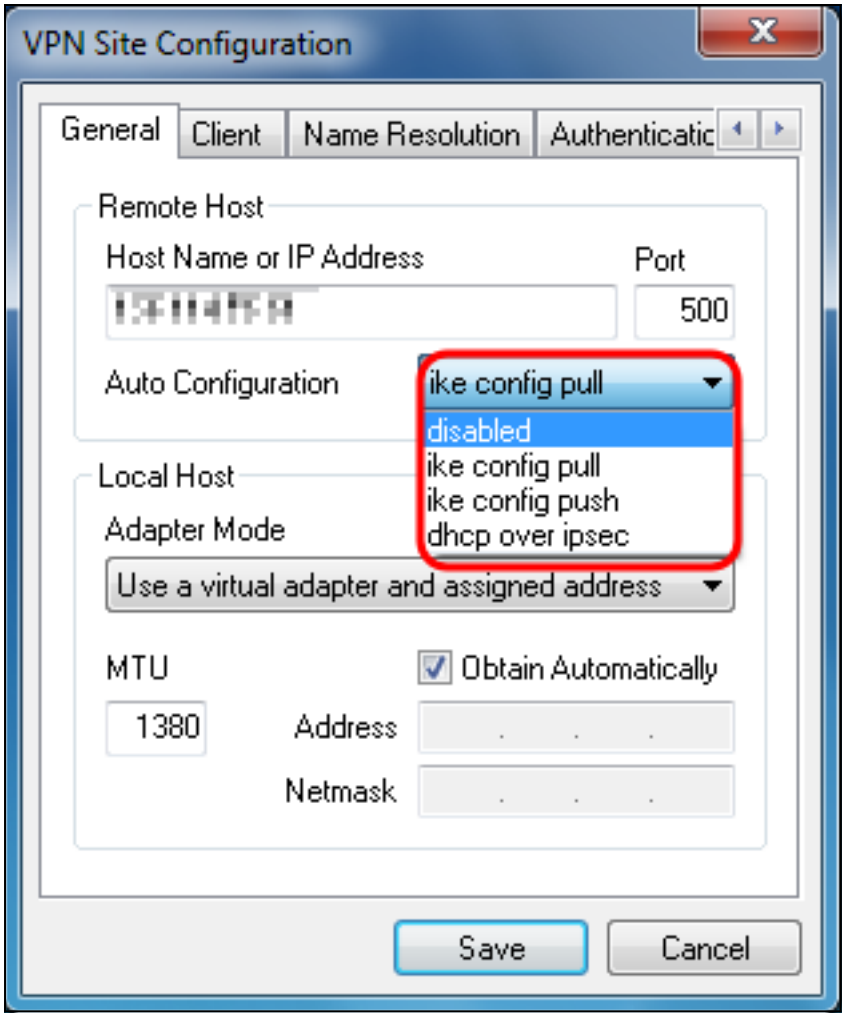


步驟2.在*General* 索引標籤下的*Remote Host*區段中，輸入您嘗試連線的網路的公用主機名或IP地址。



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，該埠應設定為允許在防火牆上轉發ISAKMP流量。

步驟3.在*Auto Configuration*下拉式清單中選擇**disabled**。



可用選項定義如下：

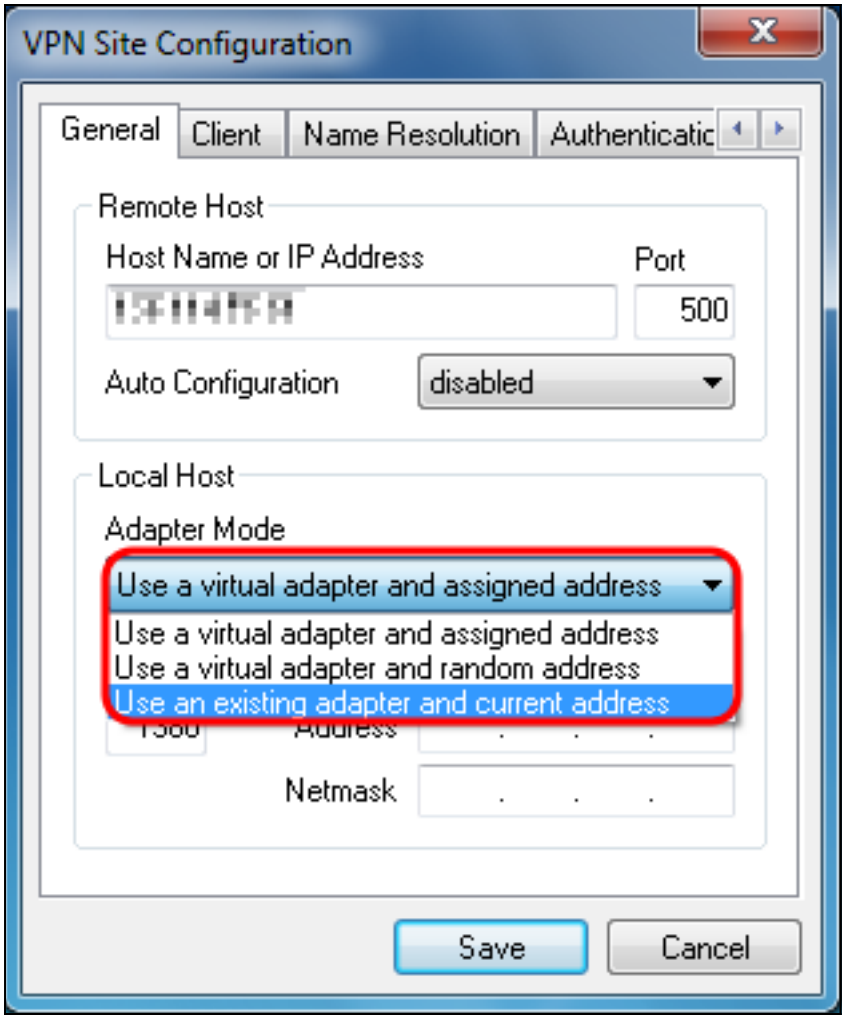
·禁用 — 禁用任何自動客戶端配置。

·IKE Config Pull — 允許客戶端從電腦設定請求。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 — 使電腦有機會通過配置過程向客戶端提供設定。在電腦支援Push方法的情況下，請求將返回客戶端支援的設定清單。

·DHCP Over IPSec — 使客戶端有機會通過DHCP over IPSec從電腦請求設定。

步驟4.在*Local Host*部分，在**Adapter Mode**下拉選單中選擇**Use an existing adapter and current address**。



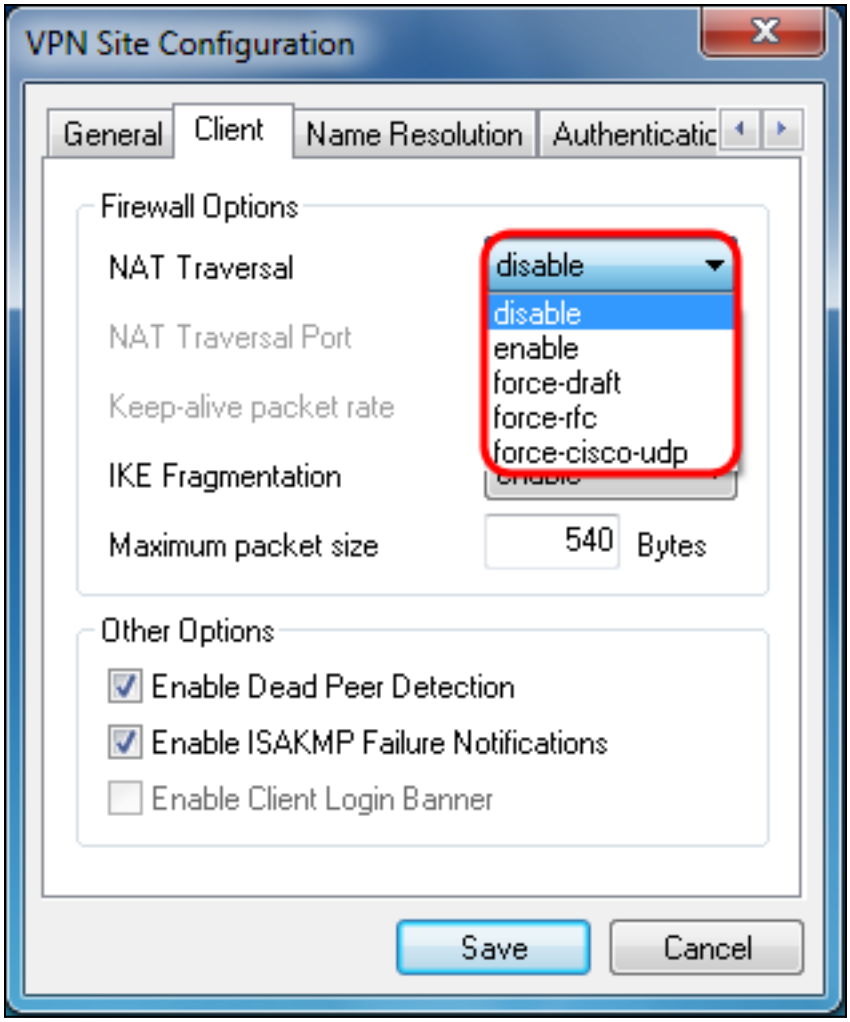
可用選項定義如下：

·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（其當前地址作為其IPsec通訊的源）。

步驟5.按一下*Client* 索引標籤。在「*NAT Traversal*」下拉選單中，選擇在RV130/RV130W上為NAT Traversal配置的相同設定，請參閱*在RV130和RV130W上配置IPSec VPN伺服器。*



可用的Network Address Translation Traversal(NATT)選單選項定義如下：

·禁用 — 將不使用NATT協定擴展。

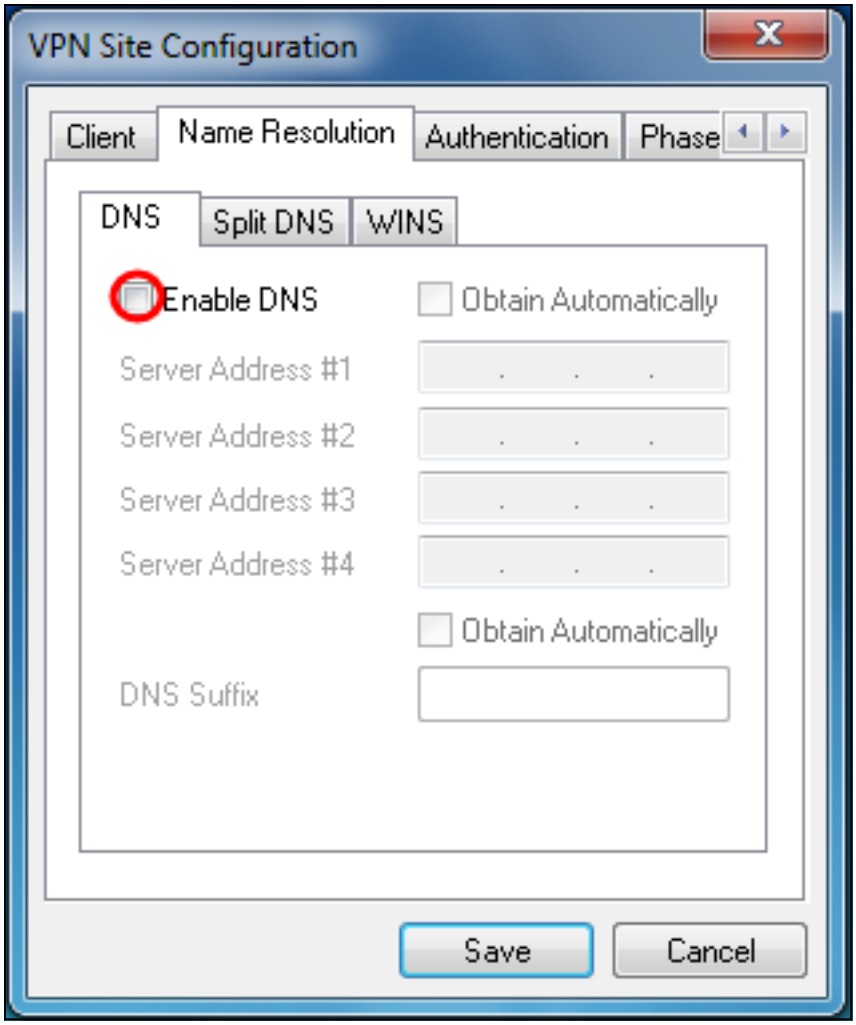
·啟用 — 僅當VPN網關在協商期間指示支援並且檢測到NAT時，才會使用NAT協定擴展。

·Force-Draft — 將使用NATT協定擴展的Draft版本，而不管在協商期間是否顯示VPN網關支援，或是否檢測到NAT。

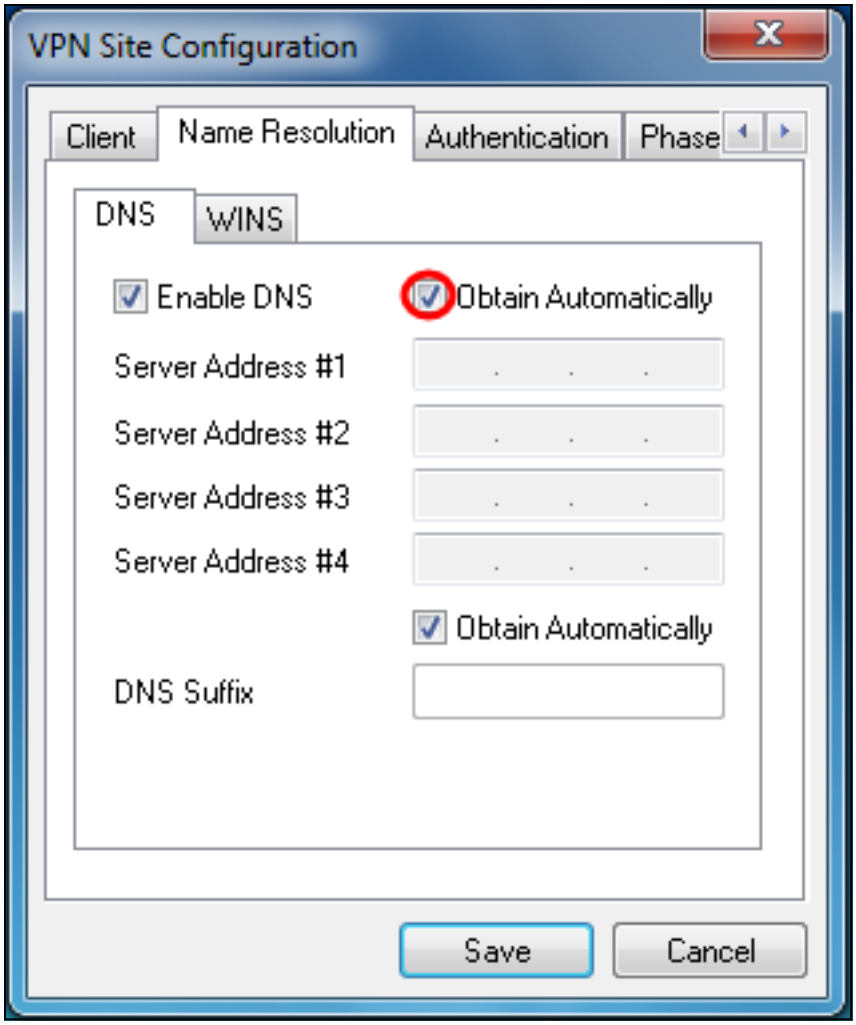
·Force-RFC — 將使用NAT協定的RFC版本，而不管協商期間是否顯示VPN網關支援，或是否檢測到NAT。

·強制 — Cisco-UDP — 對沒有NAT的VPN客戶端強制UDP封裝。

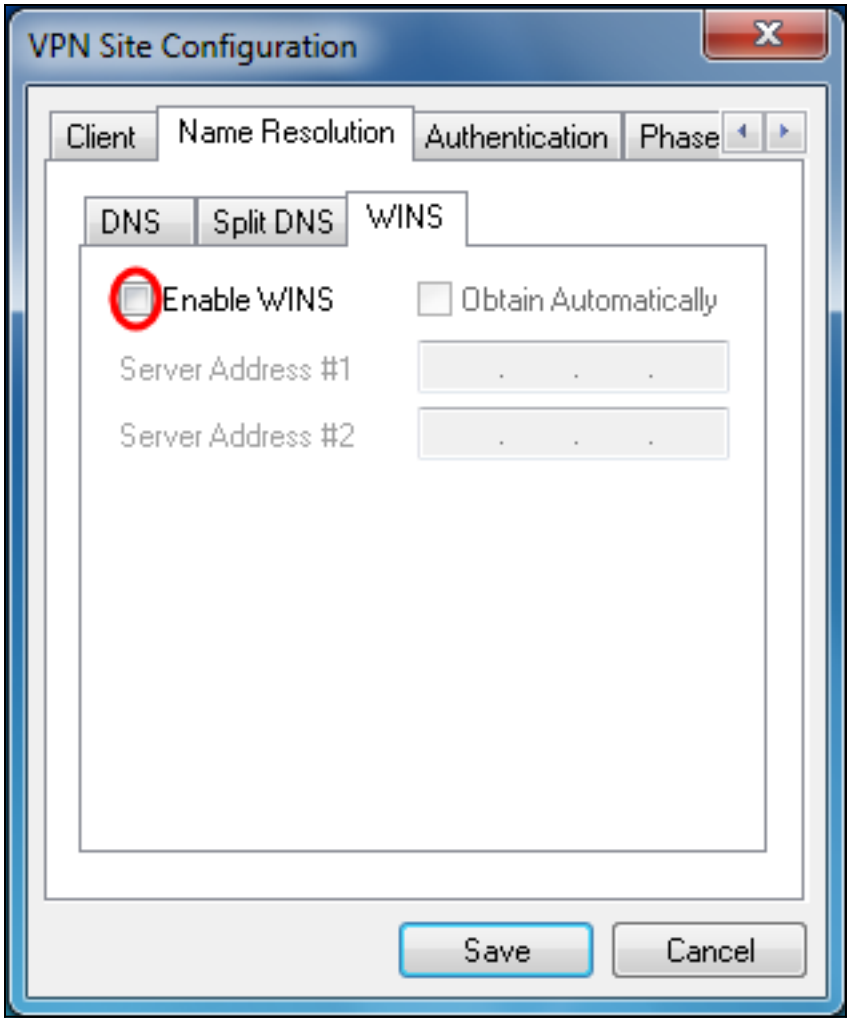
步驟6.按一下*Name Resolution*頁籤，如果要啟用DNS，請選中**Enable DNS**覈取方塊。如果您的站點配置不需要特定DNS設定，請取消選中**Enable DNS**覈取方塊。



步驟7.（可選）如果將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**覈取方塊是否已選中，並手動輸入有效的DNS伺服器地址。

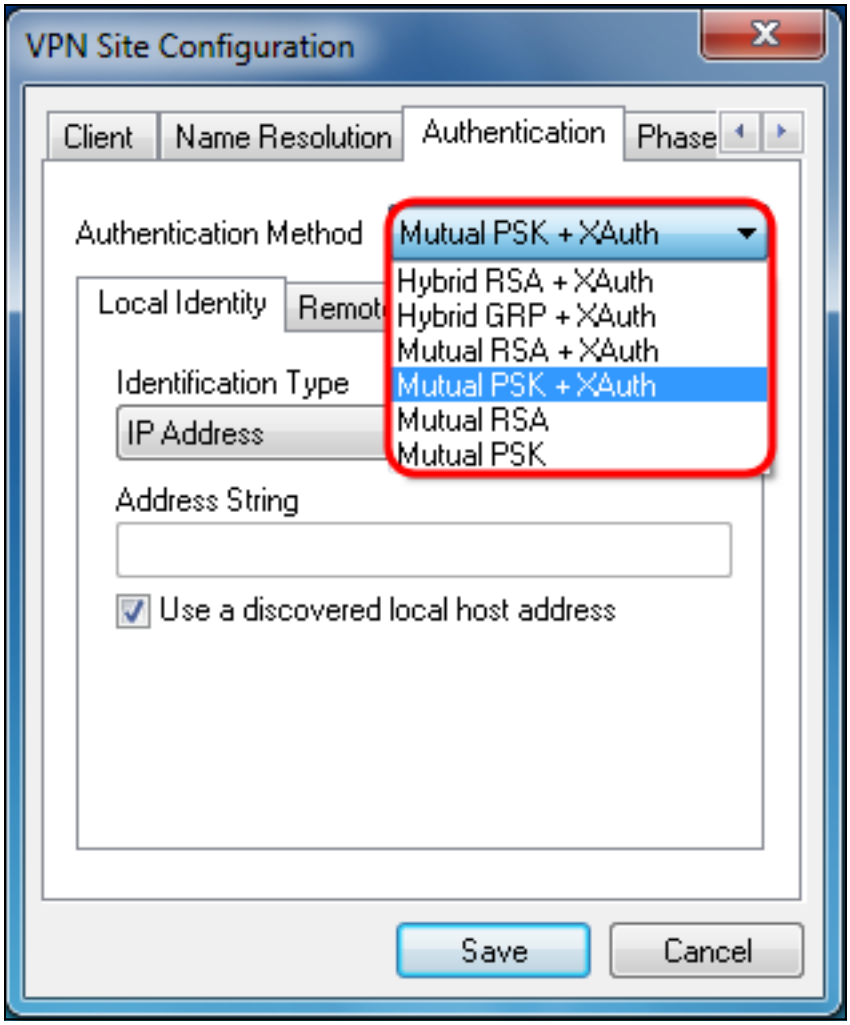


步驟8.（可選）如果要啟用Windows Internet名稱伺服器(WINS)，請按一下*Name Resolution*頁籤，選中**Enable WINS**覈取方塊。 如果您的遠端網關配置為支援配置交換，則該網關能夠自動提供WINS設定。如果未選中，請驗證**Obtain Automatically**覈取方塊是否未選中，並手動輸入有效的WINS伺服器地址。



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。

步驟9.按一下*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 — 不需要客戶端憑據。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 — 不需要客戶端憑據。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。

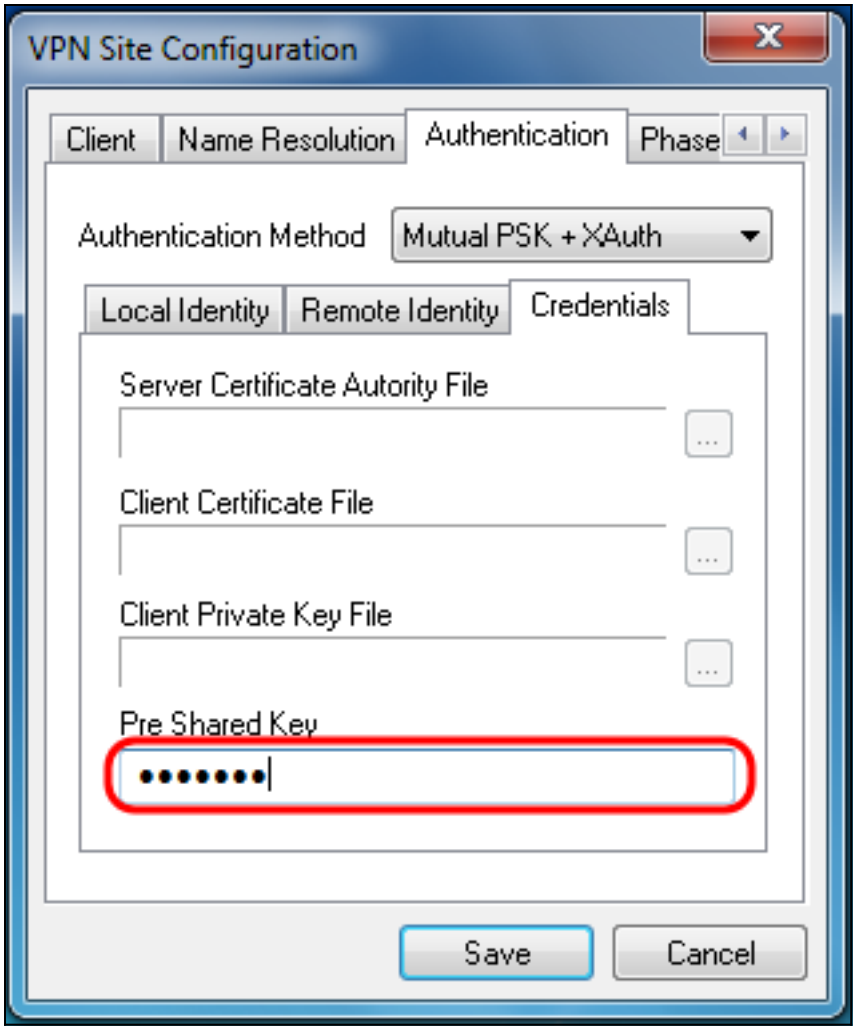
·雙方RSA +擴展驗證 — 客戶端和網關都需要憑證進行身份驗證。憑證將採用PEM或PKCS12證書檔案或金鑰型別的形式。

·雙方PSK +擴展驗證 — 客戶端和網關都需要憑證進行身份驗證。憑據將採用共用金鑰字串的形式。

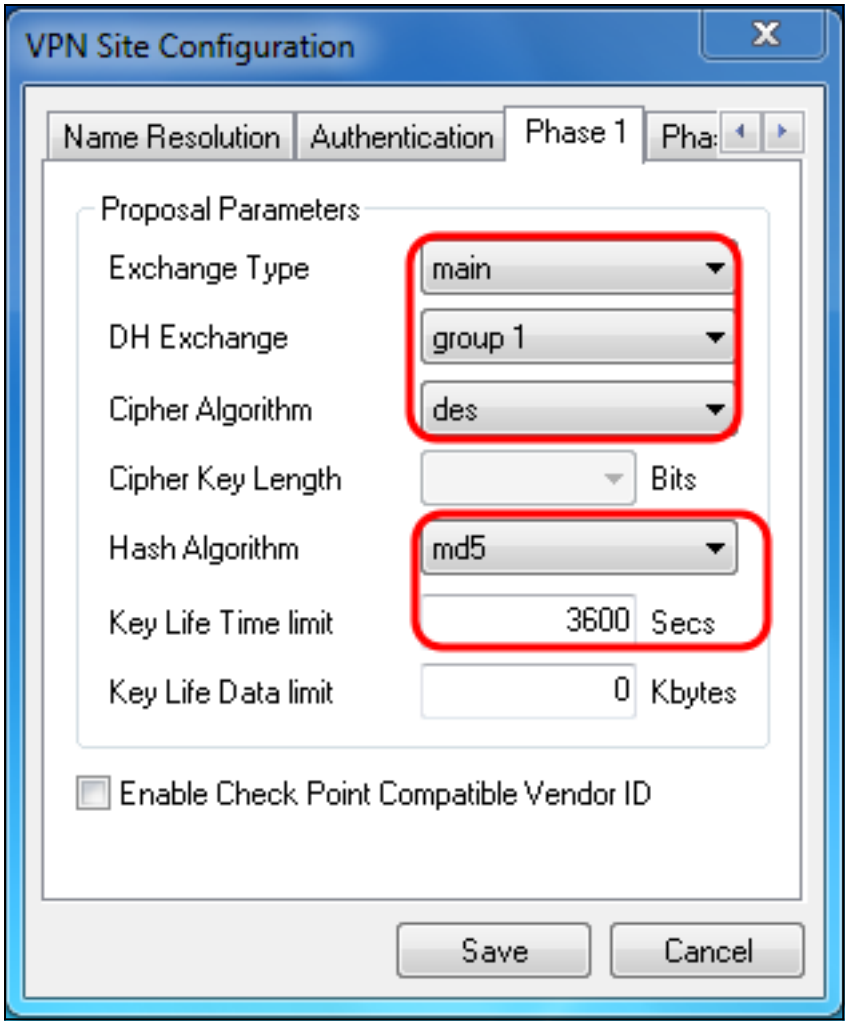
·雙方RSA — 客戶端和網關都需要憑證進行身份驗證。憑證將採用PEM或PKCS12證書檔案或金鑰型別的形式。

·雙向PSK — 客戶端和網關都需要憑證進行身份驗證。憑據將採用共用金鑰字串的形式。

步驟10.在*Authentication*部分，按一下*Credentials*子頁籤，然後在*Pre Shared Key*欄位中輸入在*IPsec VPN伺服器設定*頁上配置的相同預共用金鑰。



步驟11.按一下*Phase 1*選項卡。配置以下引數，使其與本文檔的*IPSec VPN伺服器使用者配置第2步中為*RV130/RV130W配置的設定相同。



Shrew Soft中的引數應匹配階段1中的RV130/RV130W配置，如下所示：

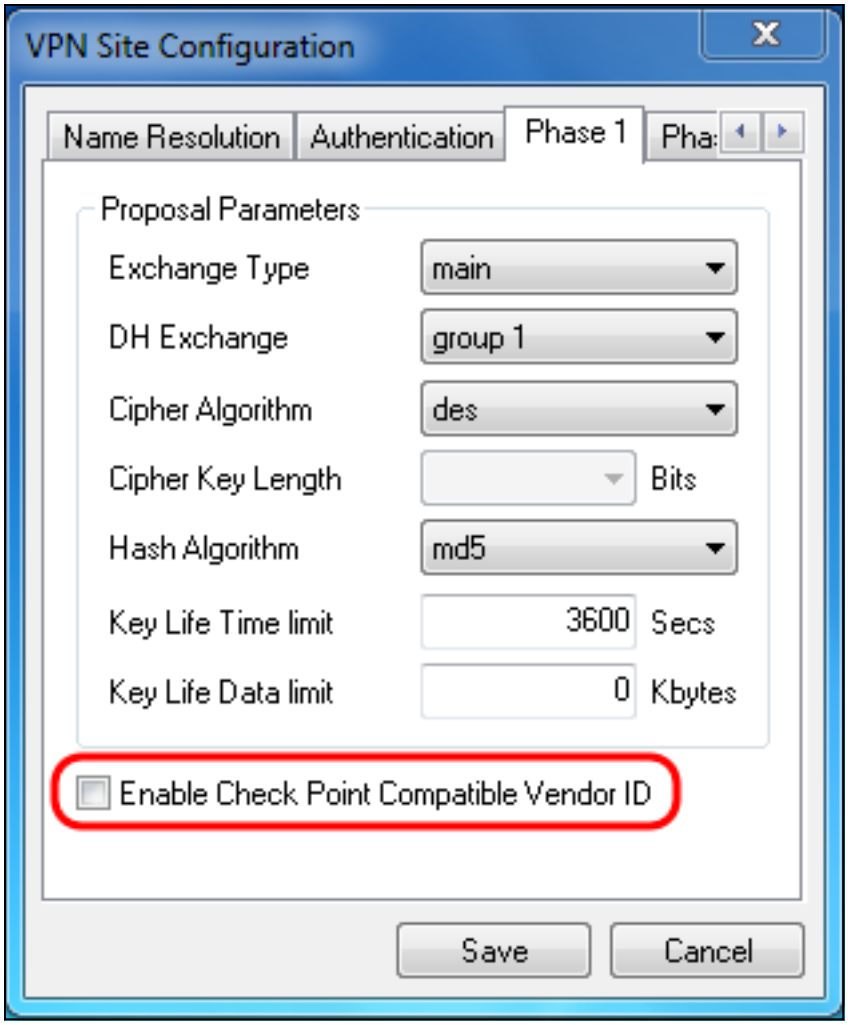
·「Exchange Type」應與「Exchange Mode」匹配。

·「DH交換」應與「DH組」匹配。

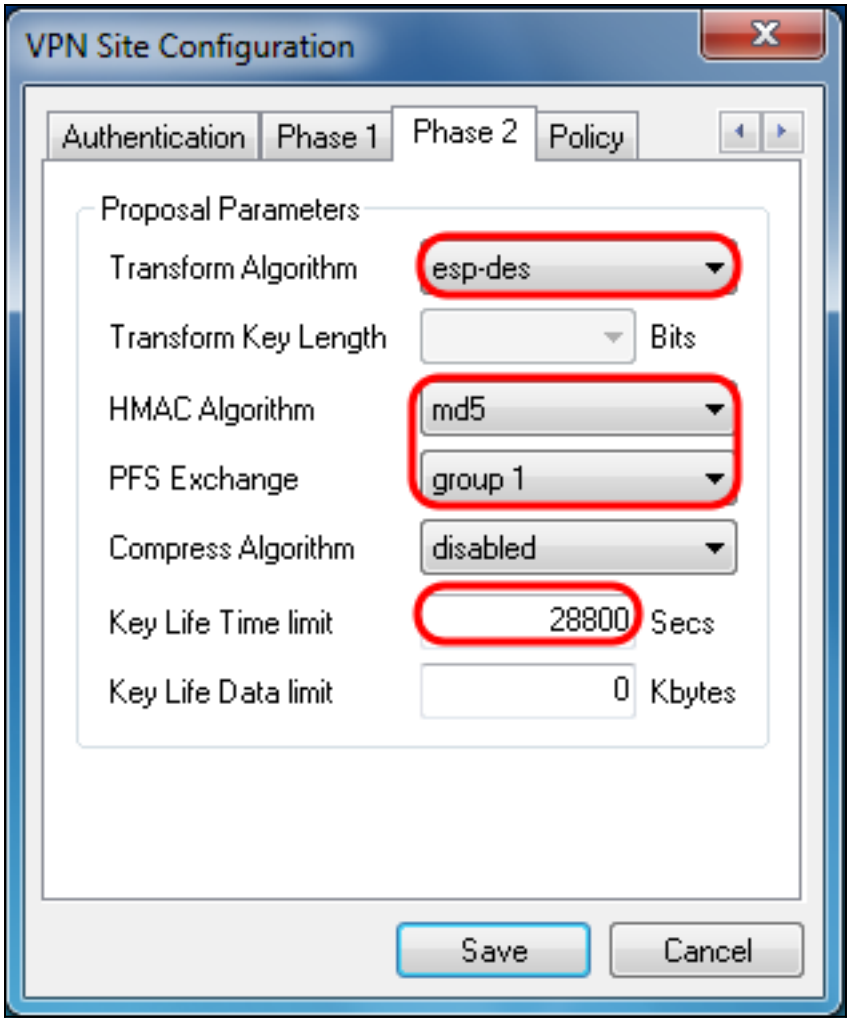
·「密碼演算法」應與「加密演算法」匹配。

·「雜湊演算法」應與「身份驗證演算法」匹配。

步驟12。（可選）如果網關在階段1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。如果網關未選中或您不確定，請取消選中該覈取方塊。



步驟13.按一下*Phase 2*選項卡。配置以下引數，使其與本文檔的*IPSec VPN伺服器使用者配置*第2步中為RV130/RV130W配置的設定相同。



Shrew Soft中的引數應匹配第2階段中的RV130/RV130W配置，如下所示：

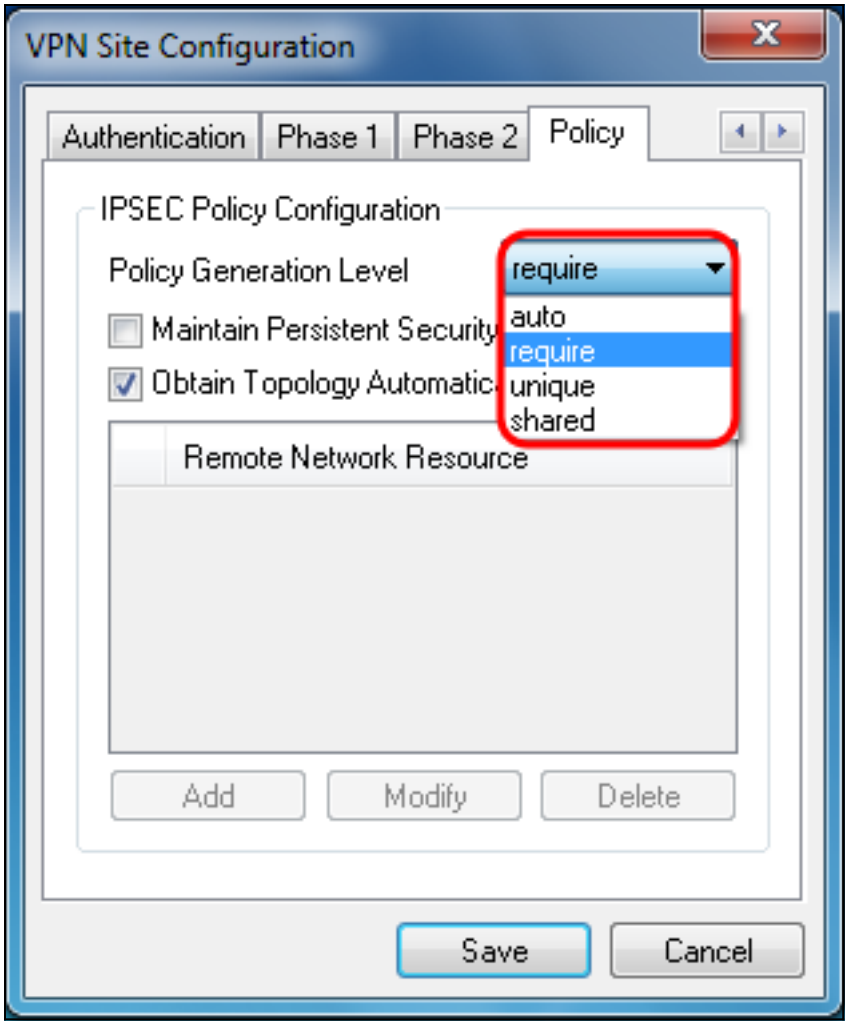
·「轉換演算法」應與「加密演算法」匹配。

·「HMAC演算法」應與「身份驗證演算法」匹配。

·如果在RV130/RV130W上啟用了PFS金鑰組，則PFS Exchange應匹配「DH組」。否則，請選擇**disabled**。

·「金鑰有效期限制」應與「IPSec SA生存期」匹配。

步驟14.按一下*Policy*頁籤，然後在**Policy Generation Level**下拉選單中選擇**require**。*Policy Generation Level*選項修改生成IPsec策略的級別。下拉選單中提供的不同級別對映到由不同供應商實施實施的IPSec SA協商行為。



可用選項定義如下：

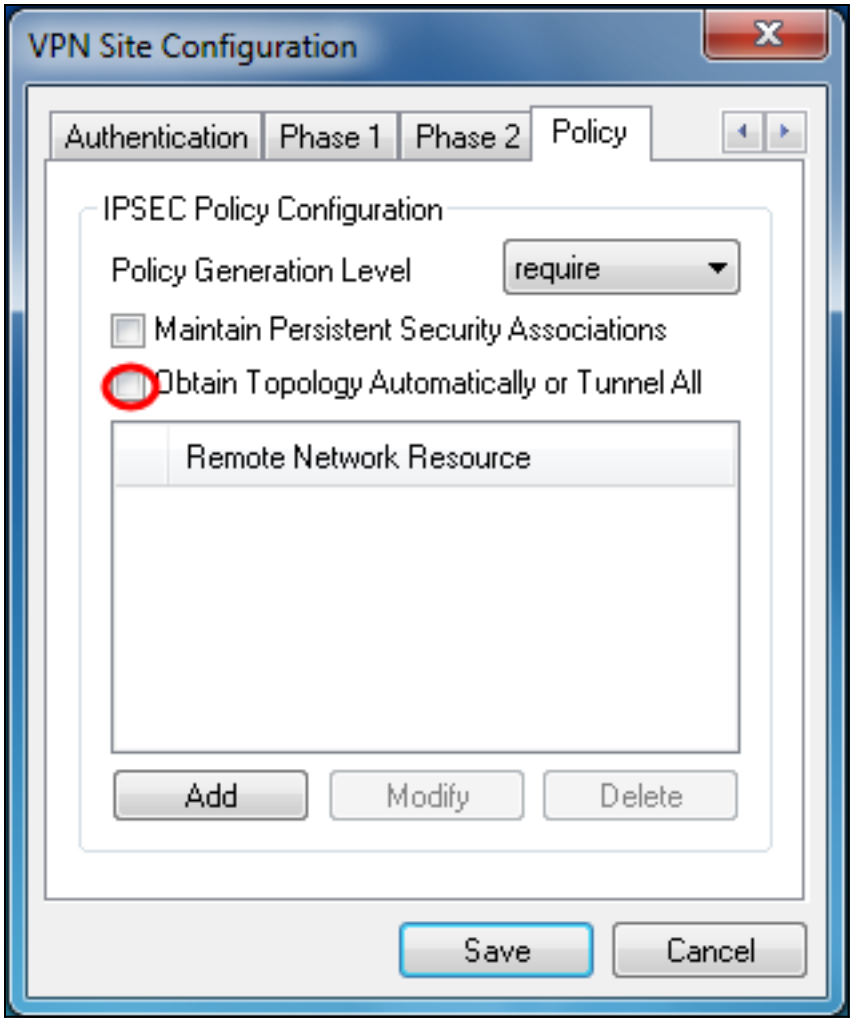
·自動 — 客戶端將自動確定適當的IPSec策略級別。

·要求 — 客戶端不會為每個策略協商唯一的安全關聯(SA)。使用本地公有地址作為本地策略ID，使用遠端網路資源作為遠端策略ID來生成策略。階段2建議將在協商期間使用策略ID。

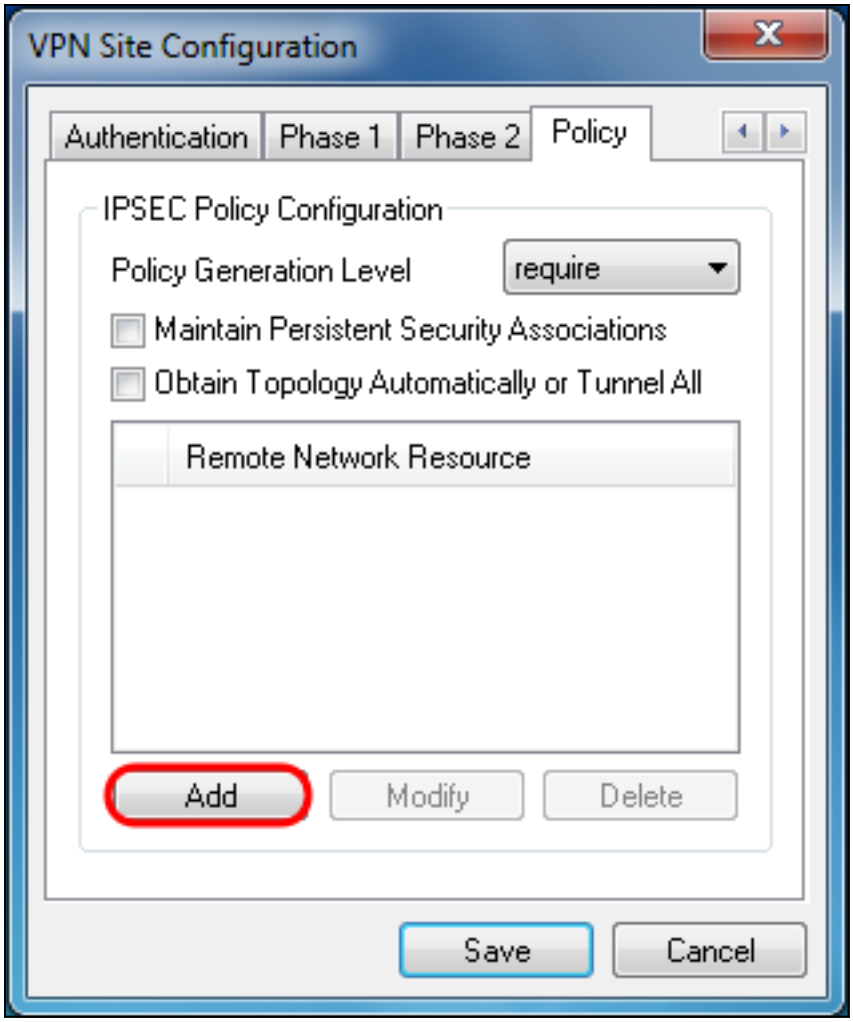
·唯一 — 客戶端將為每個策略協商一個唯一的SA。

·共用 — 在所需級別生成策略。階段2建議將在協商期間使用本地策略ID作為本地ID，使用Any(0.0.0.0/0)作為遠端ID。

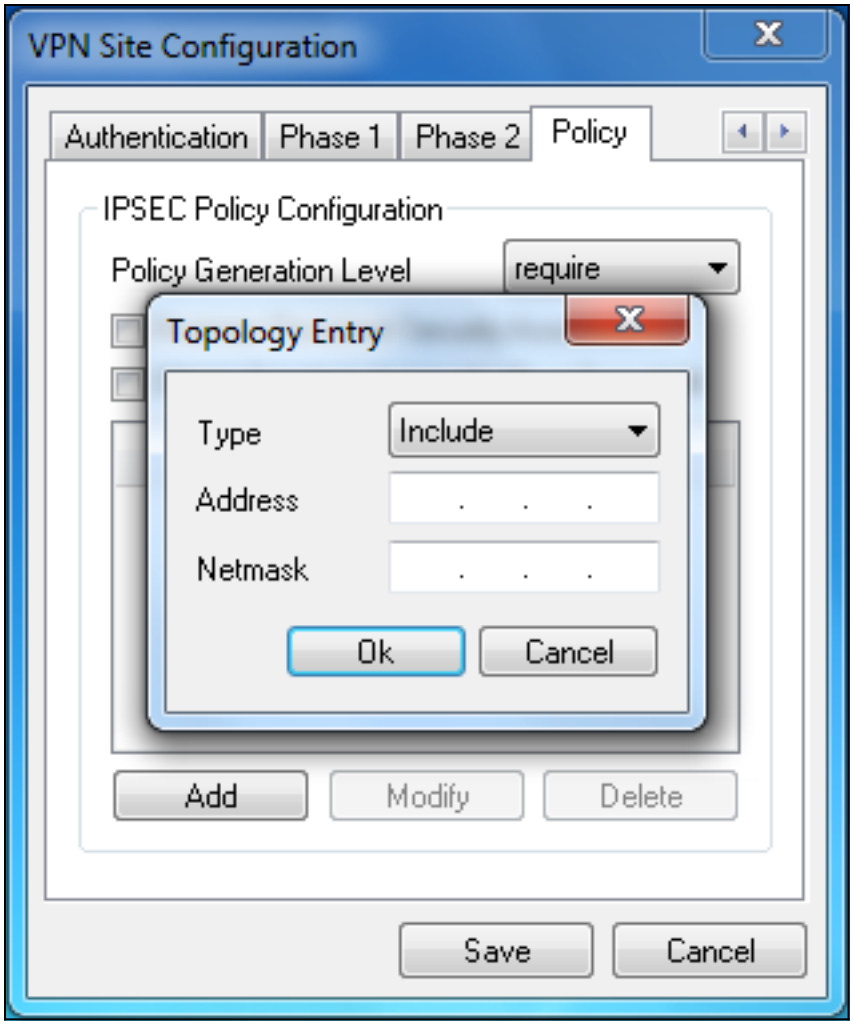
步驟15.取消選中**Obtain Topology Automatically or Tunnel All**覈取方塊。此選項修改為連線配置安全策略的方式。禁用時，必須執行手動配置。啟用時，會執行自動配置。



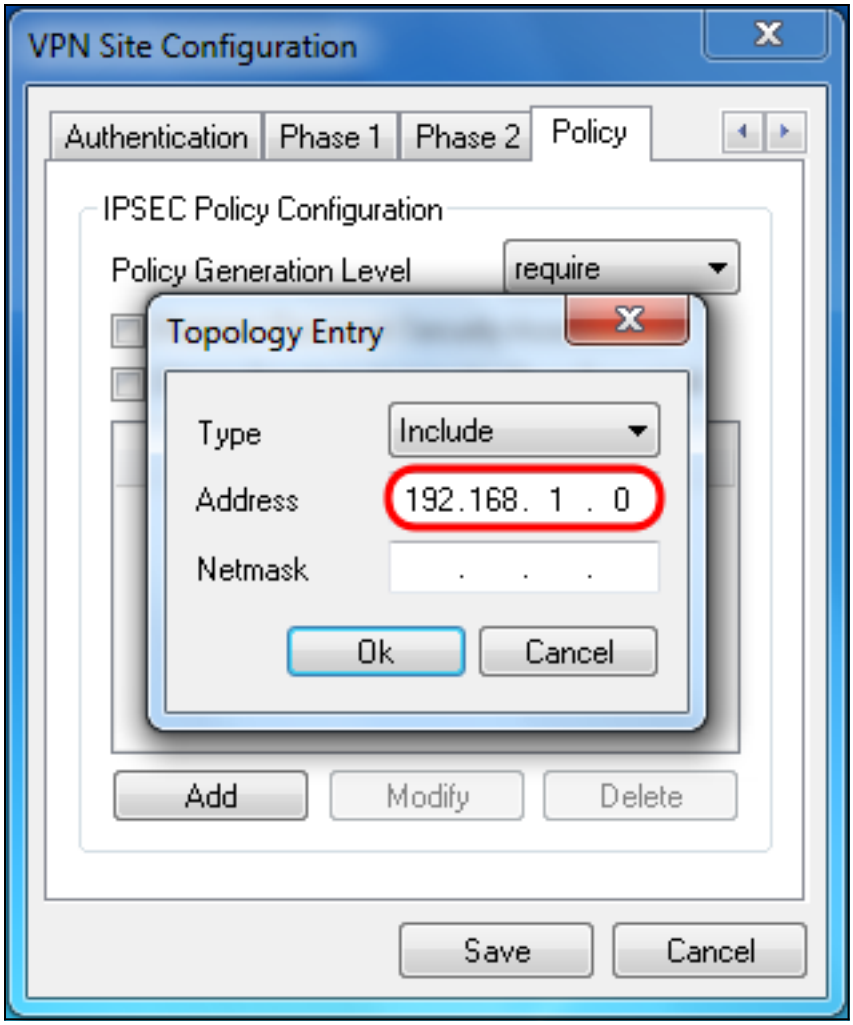
步驟16.按一下**Add**以新增您要連線的遠端網路資源。遠端網路資源包括遠端案頭訪問、部門資源、網路驅動器和安全電子郵件。



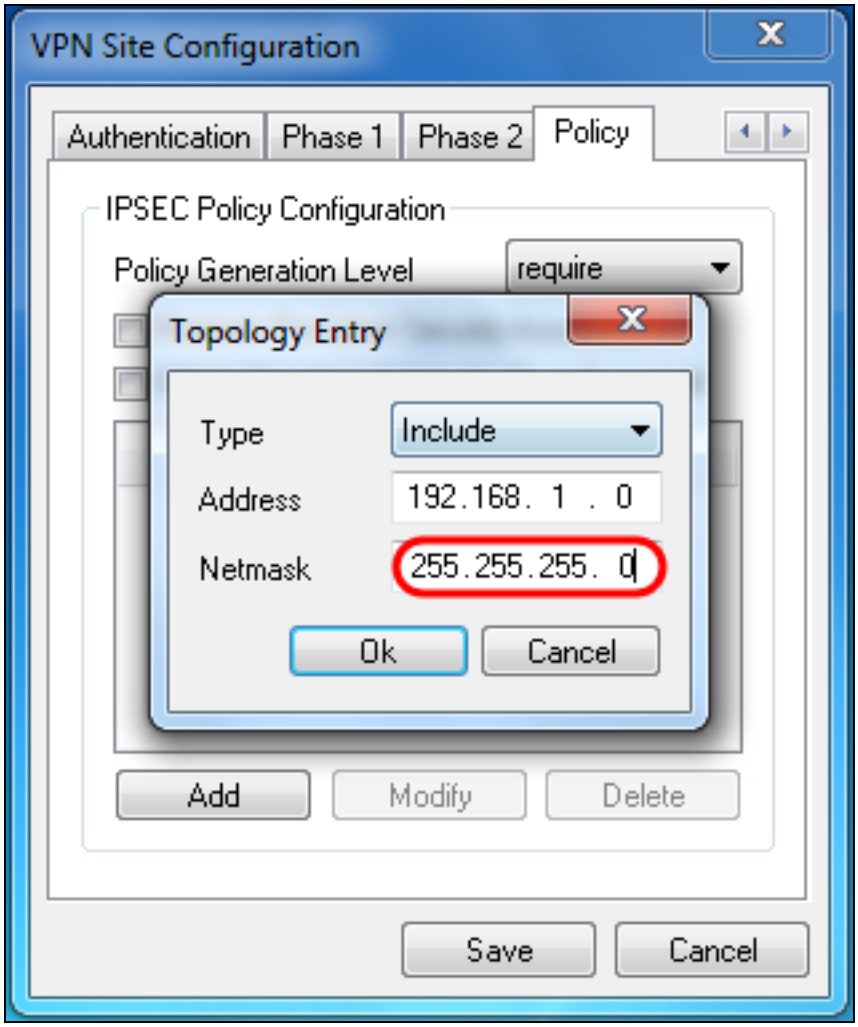
出現*Topology Entry*視窗：



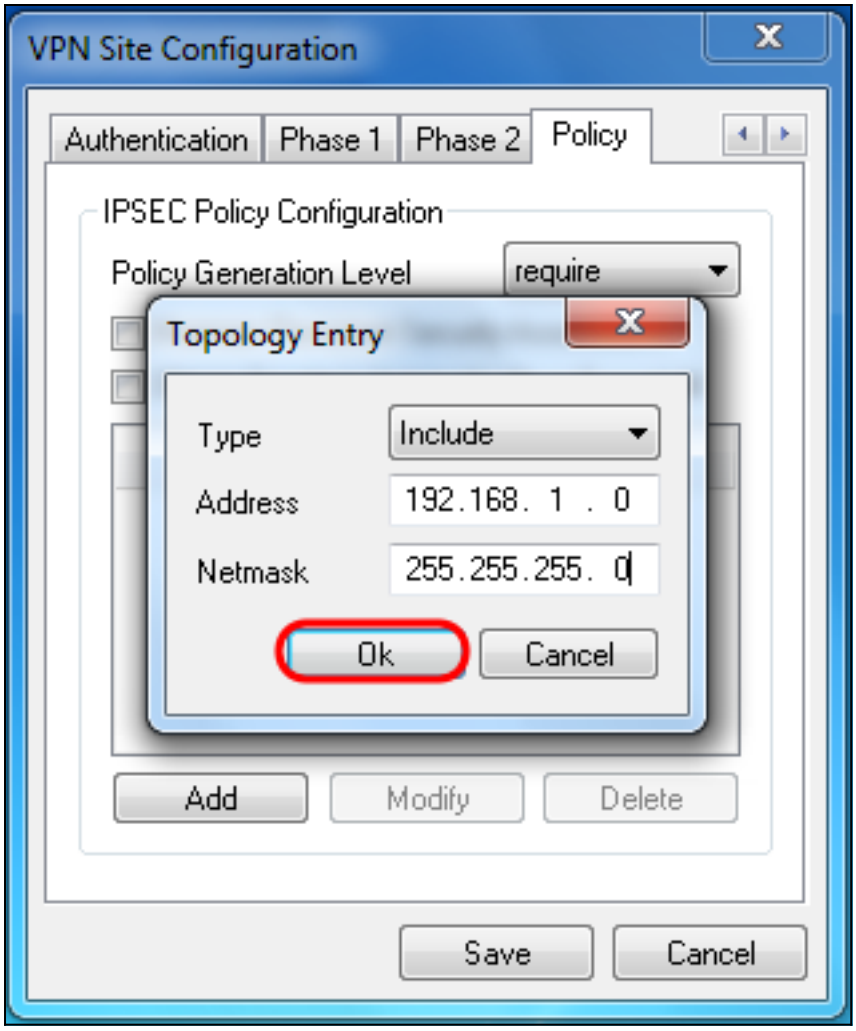
步驟17.在*地址*欄位中，輸入RV130/RV130W的子網ID。此地址應與本文檔的*IPSec VPN Server Setup and User Configuration*部分的步驟2中的*IP Address*欄位匹配。



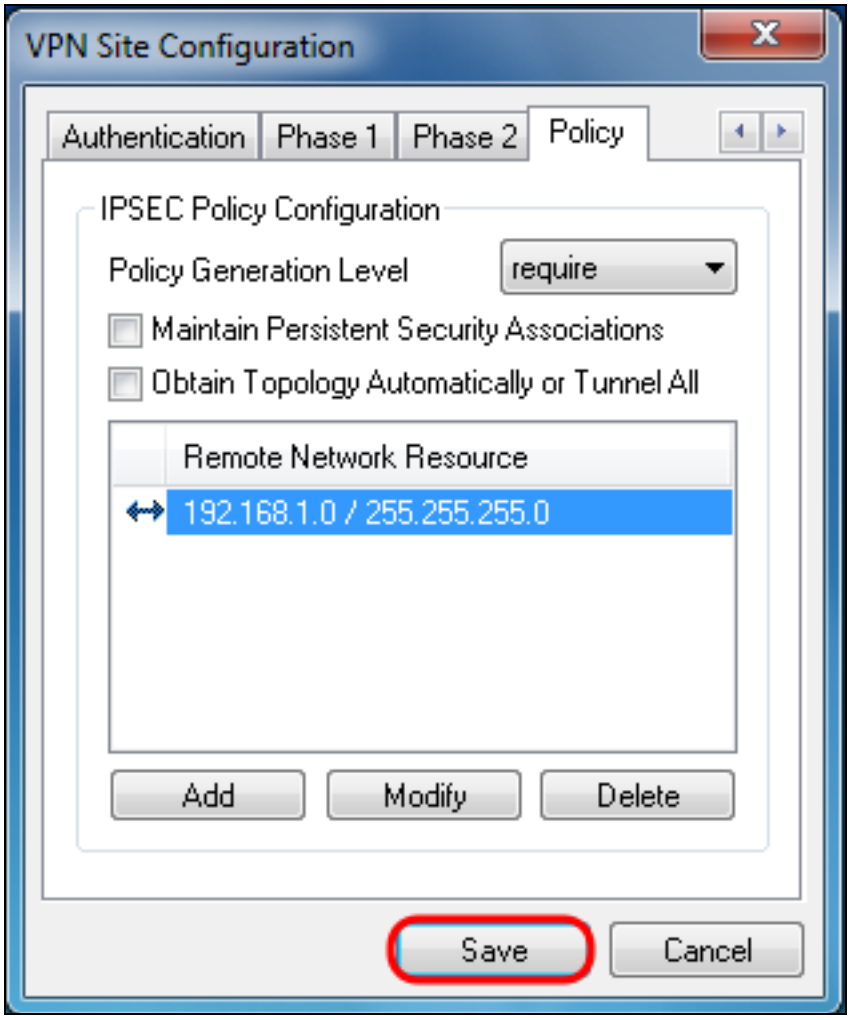
步驟18.在*Netmask*欄位中，輸入RV130/RV130W本地網路的子網掩碼。網路掩碼應與本文檔的*IPSec VPN伺服器使用者配置*部分的步驟2中的*子網掩碼*欄位匹配。



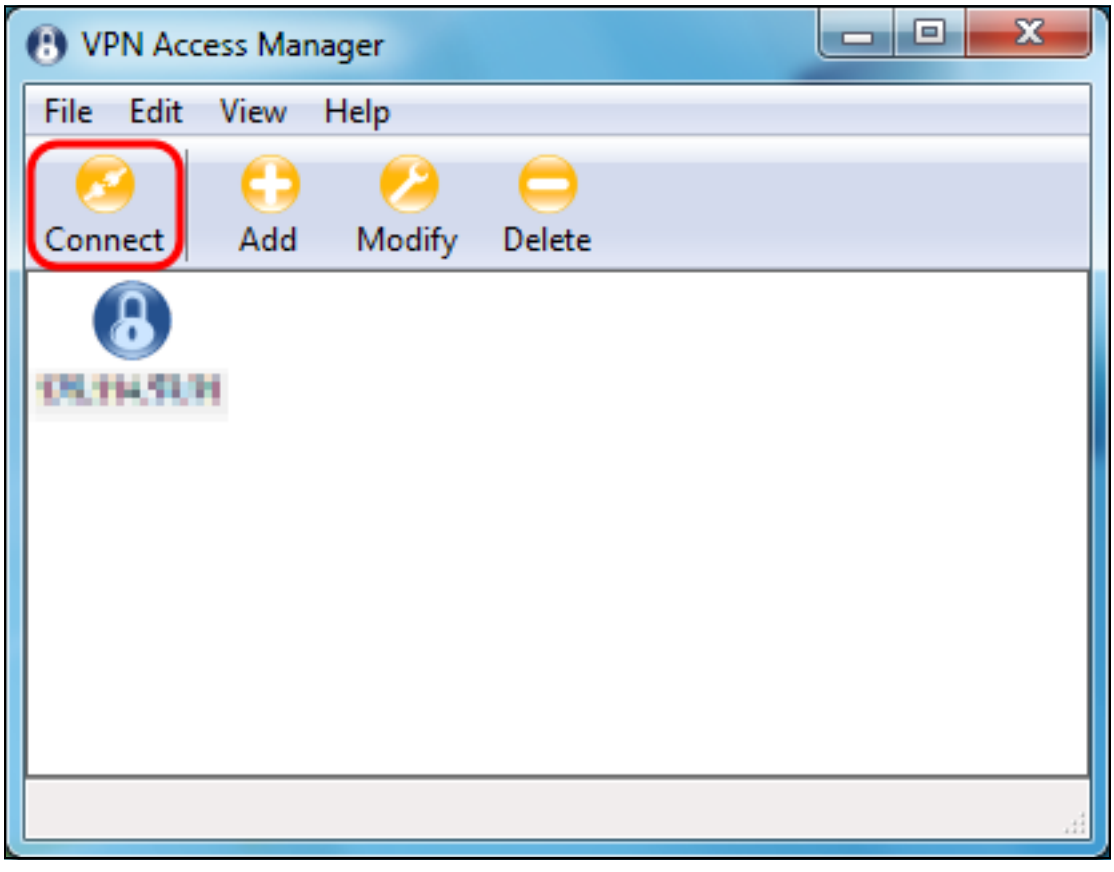
步驟19.按一下**Ok**完成新增遠端網路資源。



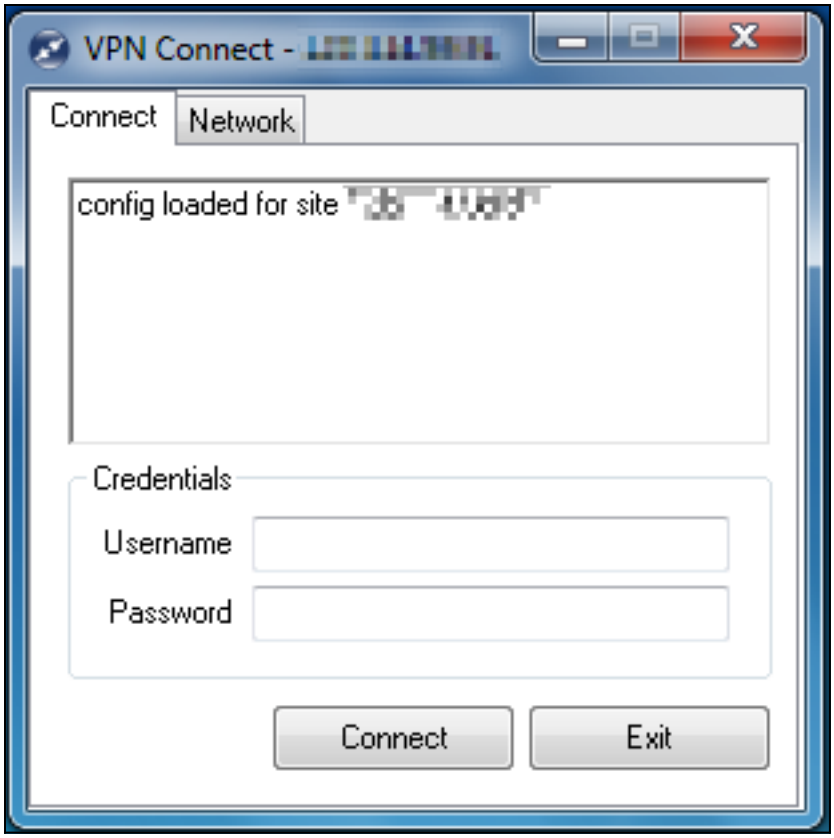
步驟20.按一下**Save**儲存要連線到VPN站點的配置。



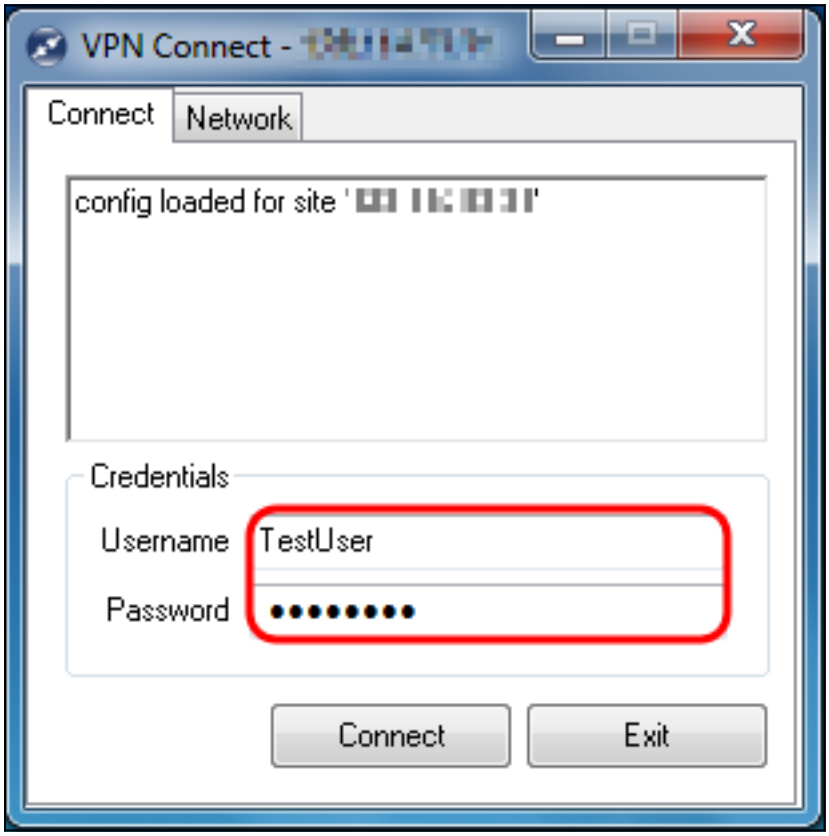
步驟21.返回*VPN Access Manager*視窗以選擇配置的VPN站點，然後按一下**Connect**按鈕。



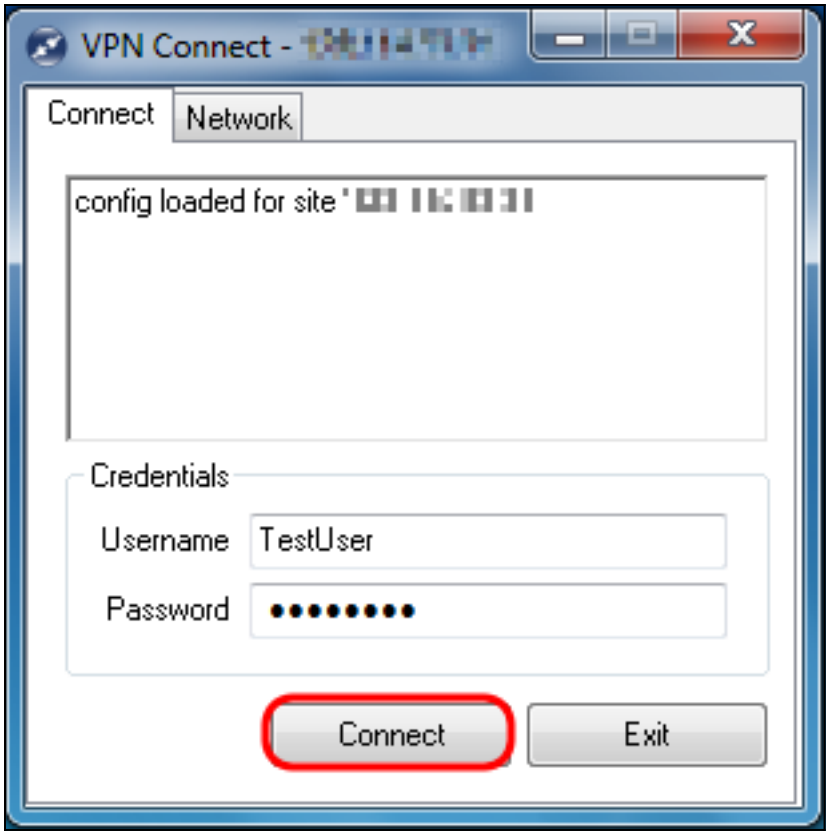
出現*VPN Connect*視窗。



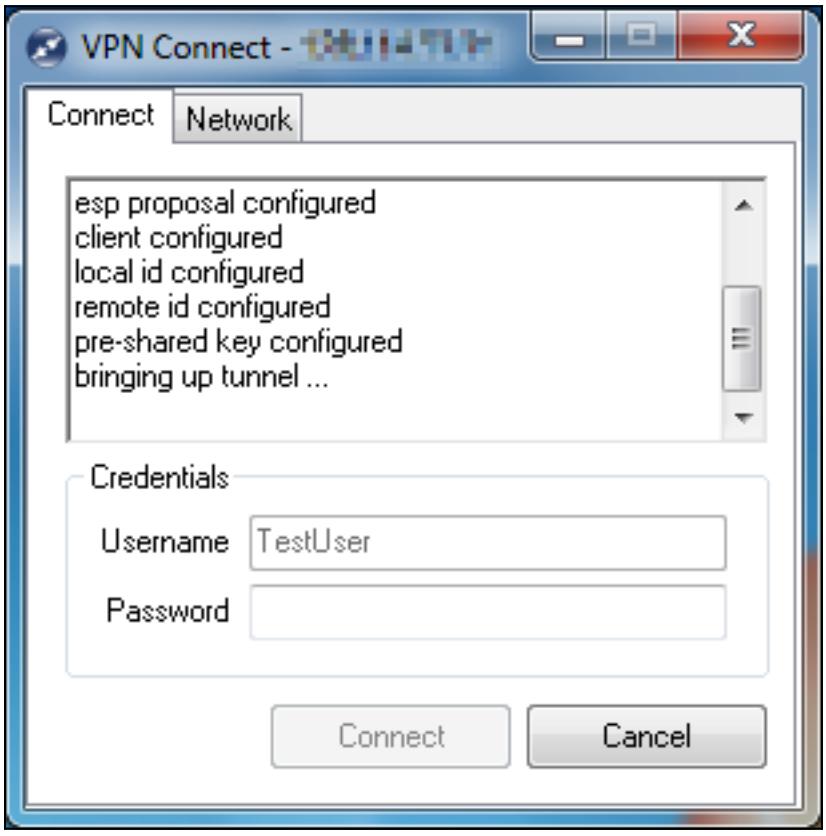
步驟22.在*Credentials*部分中，輸入您在本文檔的*IPSec VPN伺服器使用者配置*部分的步驟4中設定的帳戶的使用者名稱和密碼。

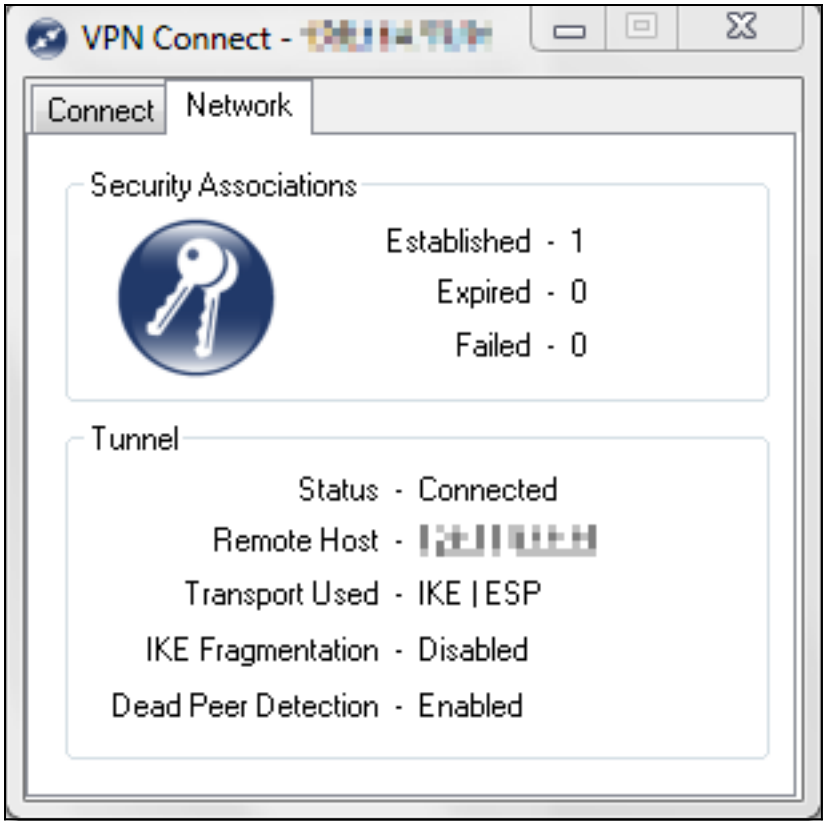


步驟23.按一下**Connect** to VPN into the RV130/RV130W。



IPSec VPN隧道已建立，VPN客戶端可以訪問RV130/RV130W LAN後面的資源。





檢視與本文相關的影片……

按一下此處檢視思科的其他技術對話

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。