# 在RV34x上配置站點到站點VPN

## 目標

本文檔的目標是在RV34x系列路由器上建立站點到站點VPN。

## 簡介

虛擬專用網路(VPN)是將遠端工作人員連線到安全網路的理想方式。VPN允許遠端主機像連線到現場安全網路一樣工作。在站點到站點VPN中，一個位置的本地路由器通過VPN隧道連線到遠端路由器。此隧道通過使用行業標準的加密和身份驗證技術來保護傳送的資料，從而安全地封裝資料。

站點到站點VPN的配置涉及設定IPsec配置檔案以及兩台路由器上的站點到站點VPN的配置。IPsec配置檔案已配置為易於設定站點到站點VPN，即使使用第3方(如AWS或Azure)也如此。IPsec配置檔案包含隧道的所有必要加密。站點到站點VPN是路由器知道要連線到哪個其他站點的配置。如果選擇不使用預配置的IPsec配置檔案，則可以選擇建立其他配置檔案。

配置站點到站點VPN時，隧道兩端的區域網(LAN)子網不能位於同一網路中。例如，如果站點A LAN使用192.168.***1.***x/24子網，則站點B不能使用相同的子網。站點B必須使用不同的子網，如192.168.***2***.x/24。

要正確配置隧道，請在配置兩台路由器時輸入相應的設定（反向本地和遠端）。假設此路由器被識別為路由器A。在「本地組設定」部分輸入其設定，並在「遠端組設定」部分輸入其他路由器（路由器B）的設定。配置另一台路由器（路由器B）時，在本地組設定部分輸入其設定，在遠端組設定部分輸入路由器A設定。

下面是路由器A和路由器B的配置表。以粗體突出顯示的引數是相反路由器的反向引數。所有其他引數配置相同。在本檔案中，我們將配置本地路由器A。

| **欄位** | **本地路由器（路由器A）**<br>WAN IP地址：140.x.x.x<br>專用IP地址（本地）：192.168.2.0/24 | **遠端路由器（路由器B）**<br>WAN IP地址：145.x.x.x<br>專用IP地址（本地）： 10.1.1.0/24 |
|---|---|---|
| 連線名稱 | VPNTest | VPNTestRemote |
| IPsec設定檔 | 測試配置檔案 | 測試配置檔案 |
| 介面 | WAN1 | WAN1 |
| 遠端終端 | 靜態IP | 靜態IP |
| 遠端終端IP地址 | **145.x.x.x** | **140.x.x.x** |
| 預共用金鑰 | CiscoTest123! | CiscoTest123! |
| 本地識別符號型別 | 本地WAN IP | 本地WAN IP |
| 本地識別符號 | **140.x.x.x** | **145.x.x.x** |
| 本地IP型別 | 子網 | 子網 |
| 本地IP地址 | **192.168.2.0** | **10.1.1.0** |
| 本地子網掩碼 | 255.255.255.0 | 255.255.255.0 |
| 遠端識別符號 | 遠端WAN IP | 遠端WAN IP |

| 型別 | | |
|---|---|---|
| 遠端識別符號 | 145.x.x.x | 140.x.x.x |
| 遠端IP型別 | 子網 | 子網 |
| 遠端IP地址 | 10.1.1.0 | 192.168.2.0 |
| 遠端子網掩碼 | 255.255.255.0 | 255.255.255.0 |

# 適用裝置

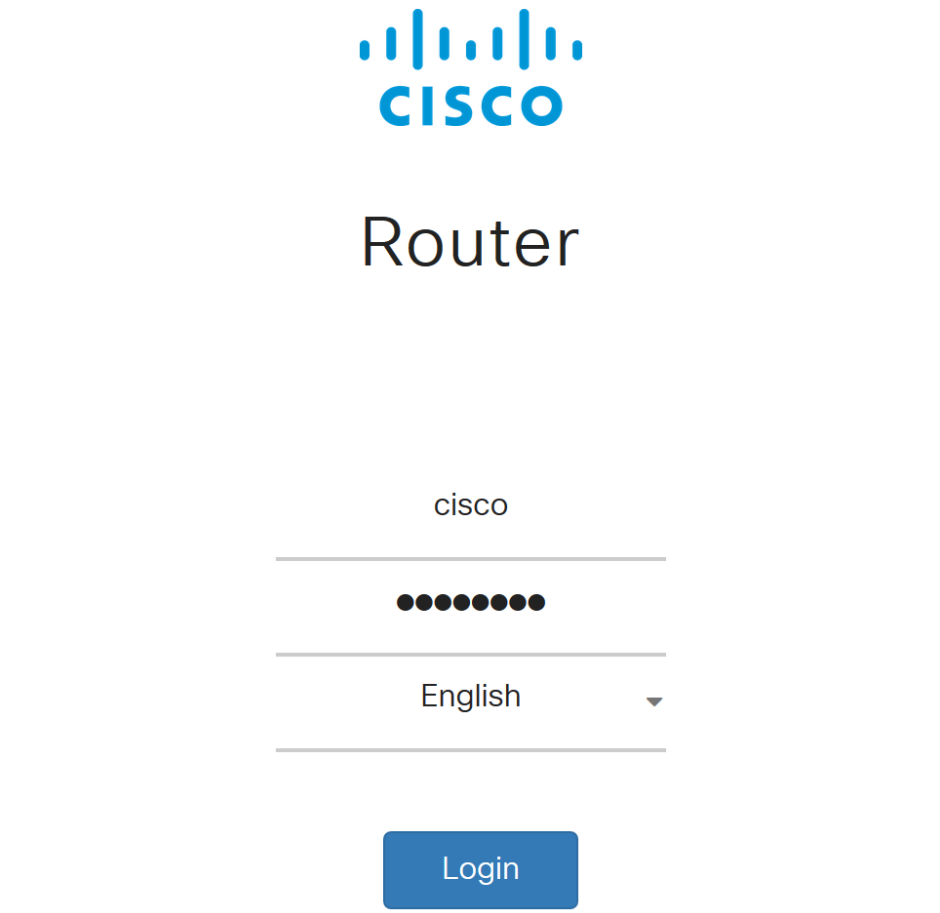
- RV34x

# 軟體版本

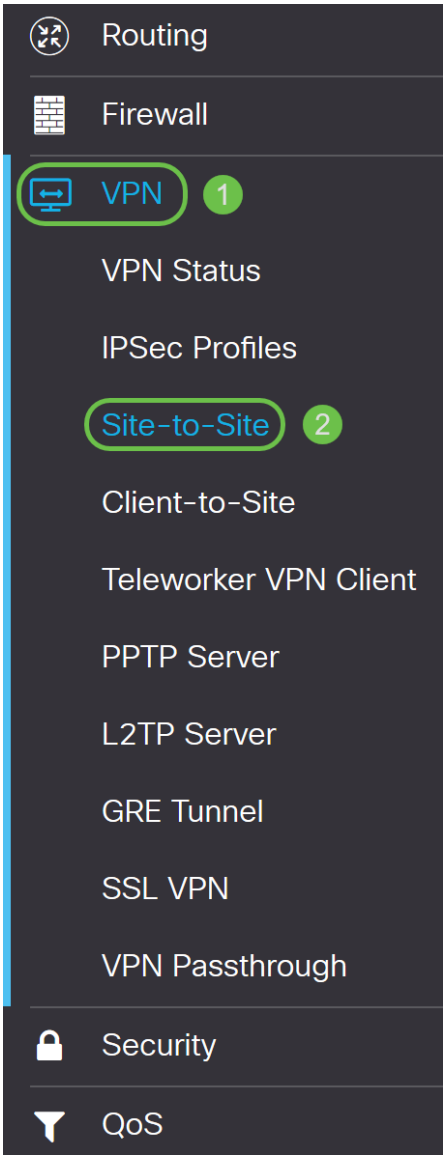
- 1.0.02.16

# 配置站點到站點VPN連線

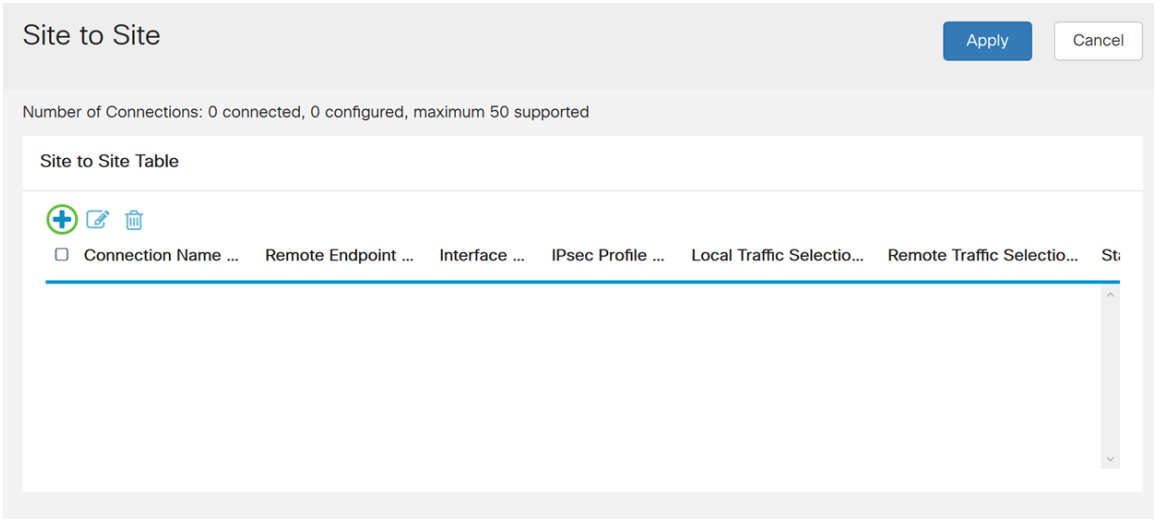
步驟1.登入到路由器的Web配置頁。



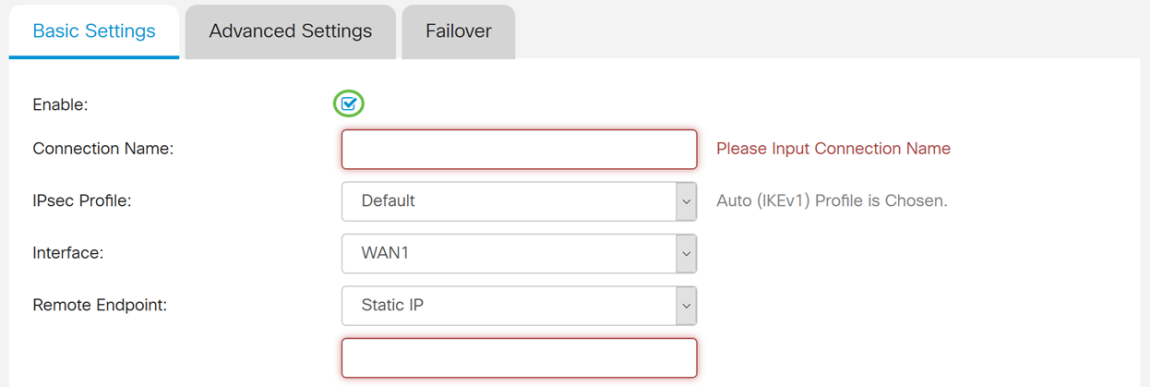

步驟2.導覽至VPN > Site-to-Site。




步驟3.按一下**add**按鈕新增新的站點到站點VPN連線。

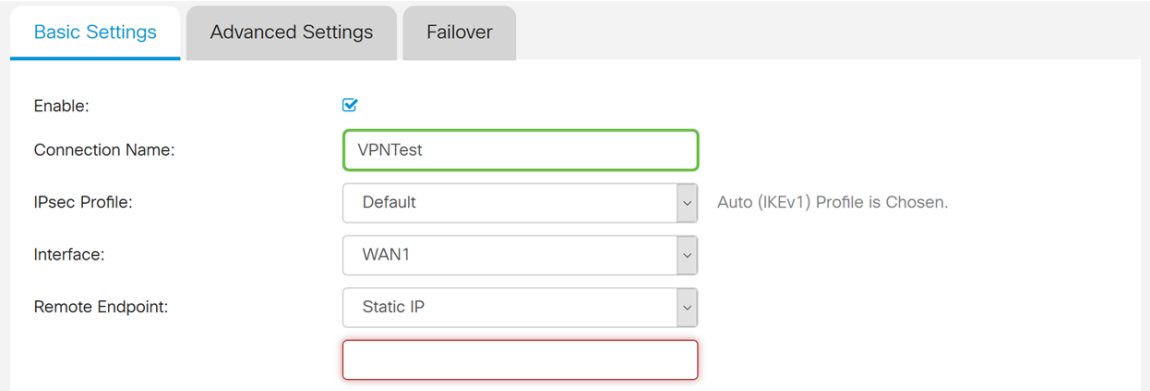



步驟4.勾選**Enable**以啟用組態。預設情況下啟用。




步驟5.輸入VPN隧道的連線名稱。此說明僅供參考，無需與通道另一端使用的名稱相符。

在本例中，我們將輸入**VPNTest**作為連線名稱。

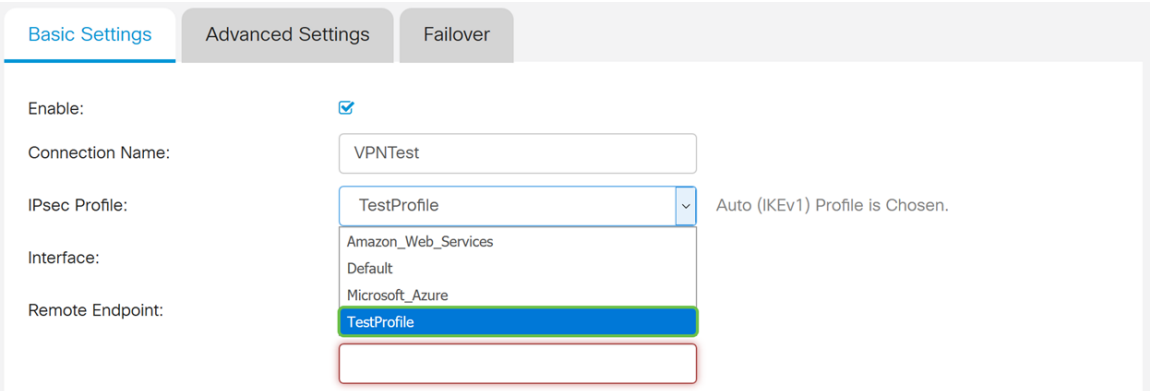



步驟6.選擇要用於VPN的IPsec配置檔案。IPsec設定檔是IPsec中的中央組態，其定義用於第I階段和第II階段交涉的演算法(例如加密、驗證和Diffie-Hellman(DH)群組)。

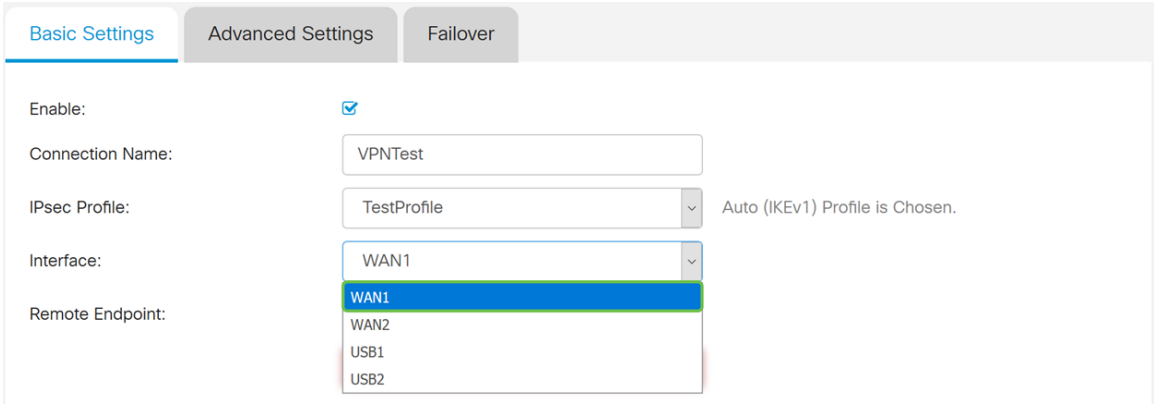
要瞭解如何使用IKEv2配置IPsec配置檔案，請按一下連結：[在RV34x上使用IKEv2配置IPsec配置檔案]。

**附註：**可以選擇使用第三方（Amazon Web Services或Microsoft Azure）for IPsec配置檔案。此IPsec配置檔案已配置有需要為Amazon Web Services或Microsoft Azure配置的所有必要選擇，因此您無需對其進行配置。如果您嘗試在站點的AWS或Azure之間配置站點到站點VPN，則您需要使用AWS或Azure在站點一側提供的資訊，並在在此側配置站點到站點VPN時使用預配置的IPsec配置檔案。

在本示例中，我們將選擇**TestProfile**作為我們的IPsec配置檔案。

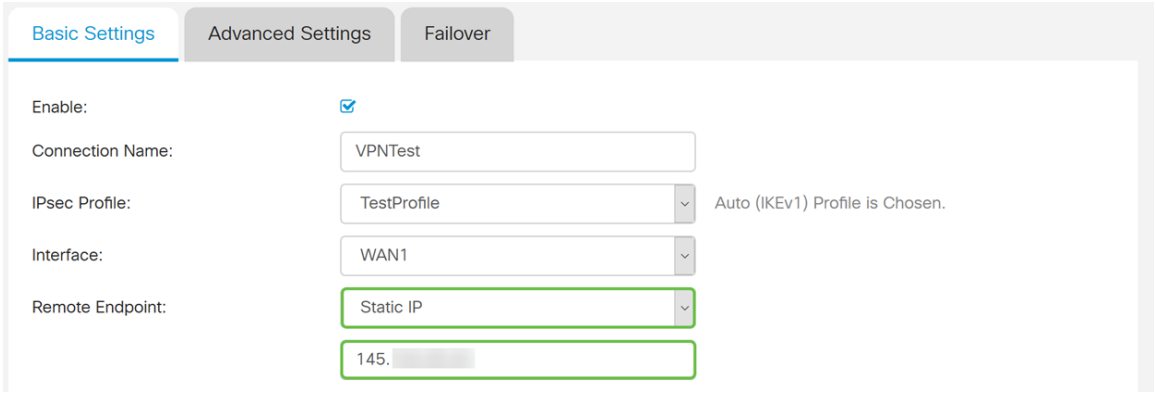



步驟7.在*Interface*欄位中，選擇用於通道的介面。在本例中，我們將使用**WAN1**作為我們的介面。




步驟8.為遠端終端選擇**靜態IP**、**完全限定域名(FQDN)**或**動態IP**。根據您的選擇輸入遠端終端的IP地址或FQDN。

我們選擇了**Static IP**，並輸入了遠端終端IP地址。



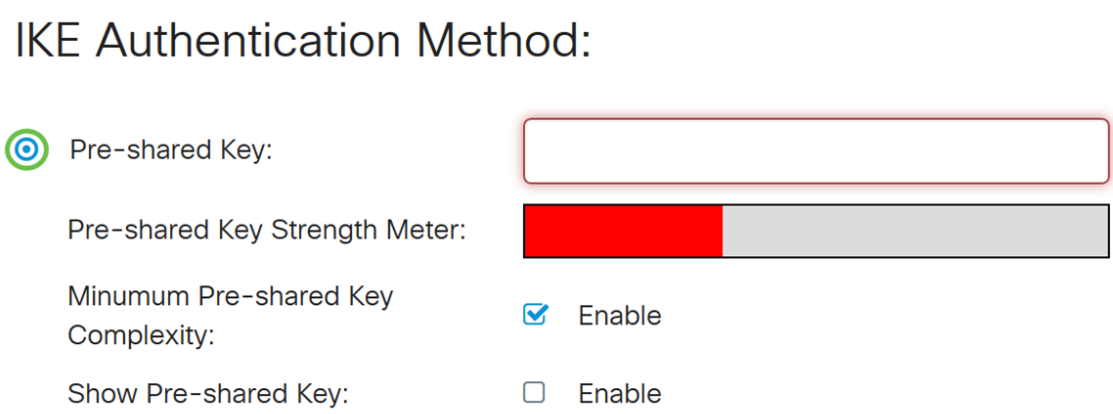

# 配置IKE身份驗證方法

步驟1。選擇**Pre-shared Key**或**Certificate**。

預共用金鑰：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驗證。兩個對等體必須共用同一個金鑰。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，則它會對另一個對等體進行身份驗證。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對等體的預共用金鑰進行配置。

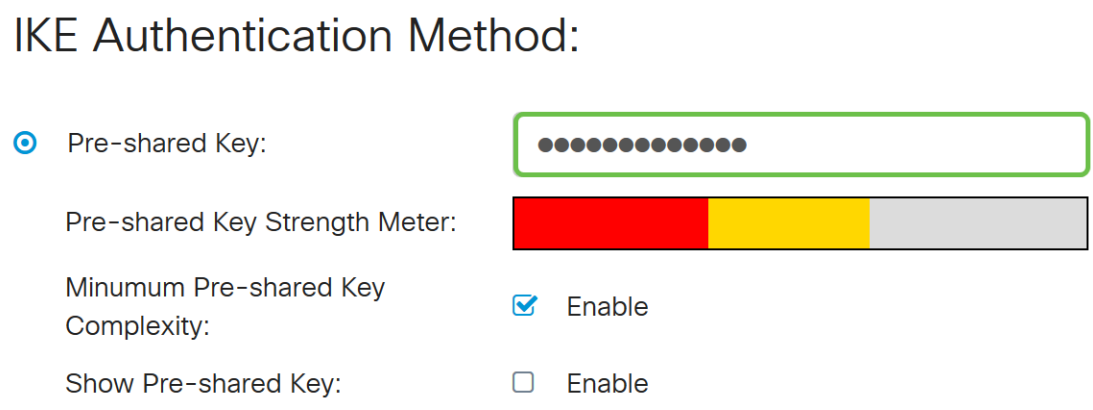
證書：數位證書是一個包，其中包含諸如證書持有者的身份資訊，包括名稱或IP地址、證書的序列號、證書的到期日期，以及證書持有者的公鑰的副本。標準數位證書格式在X.509規範中定義。X.509版本3定義了憑證的資料結構。如果您已選擇**Certificate**，請確保在**Administration > Certificate**中匯入了您的簽名證書。從下拉選單中選擇本地和遠端證書。

在本演示中，我們將選擇**Pre-shared key**作為我們的IKE身份驗證方法。

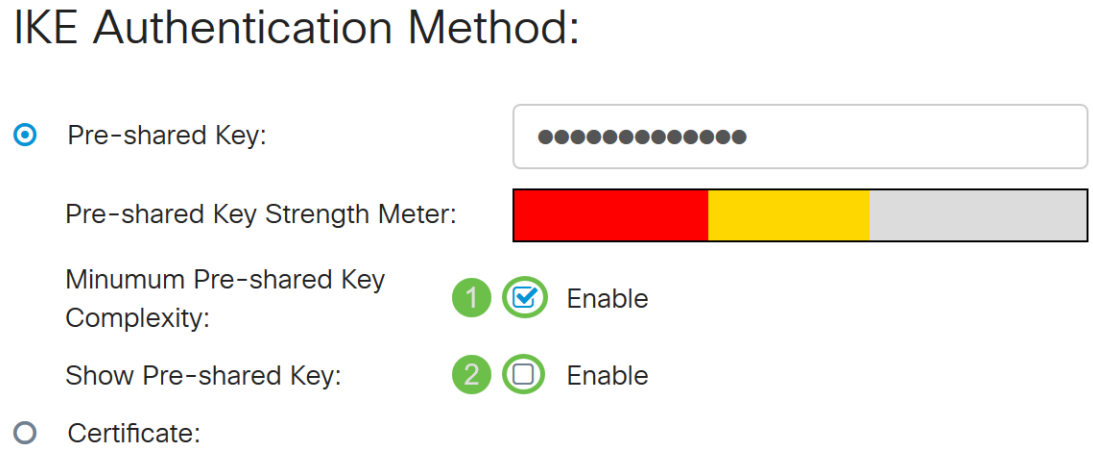



步驟2.在*Pre-shared Key*欄位中，輸入預共用金鑰。

**附註：**確保遠端路由器使用相同的預共用金鑰。

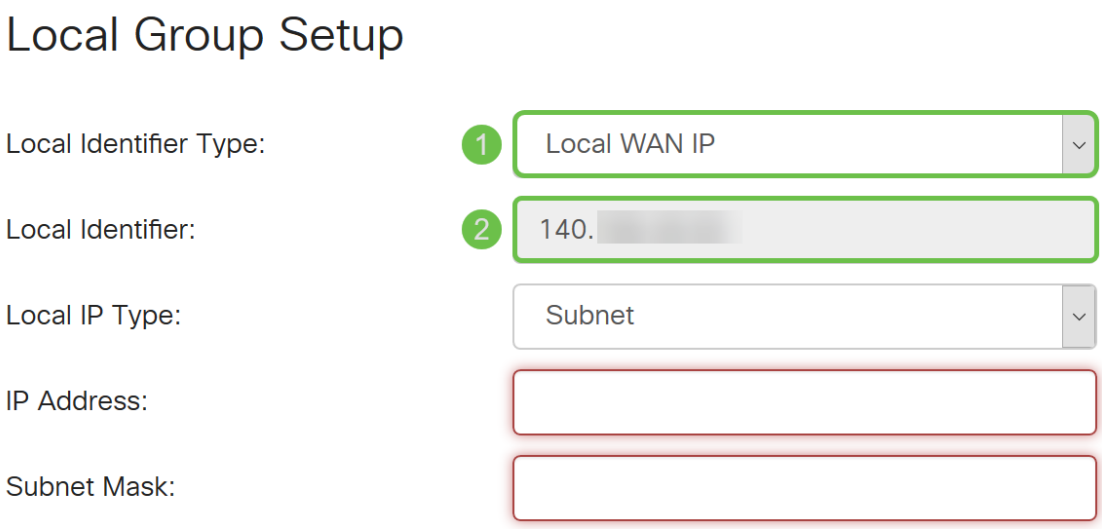



步驟3. *預共用金鑰強度表*通過彩色條顯示預共用金鑰的強度。選中**Enable**以啟用最低預共用金鑰複雜性。預設情況下會檢查預共用金鑰的複雜性。如果要顯示預共用金鑰，請選中**Enable**覈取方塊。



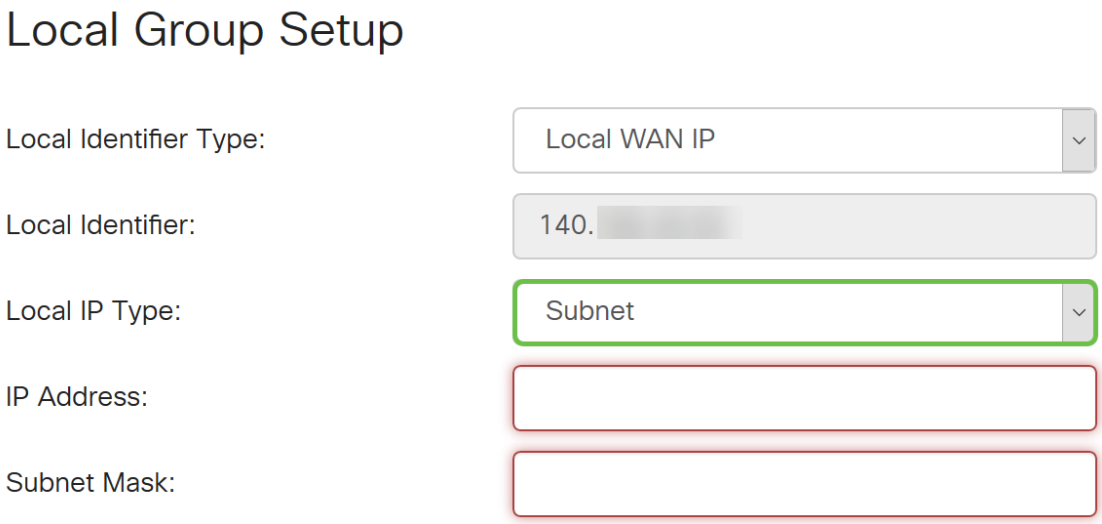

# 本地組設定

步驟1.從下拉選單中選擇**本地WAN IP**、**IP地址**、**本地FQDN**或**本地使用者FQDN**。根據您的選擇輸入識別符號名稱或IP地址。如果您已選擇**本地WAN IP**，則應自動輸入路由器的WAN IP地址。



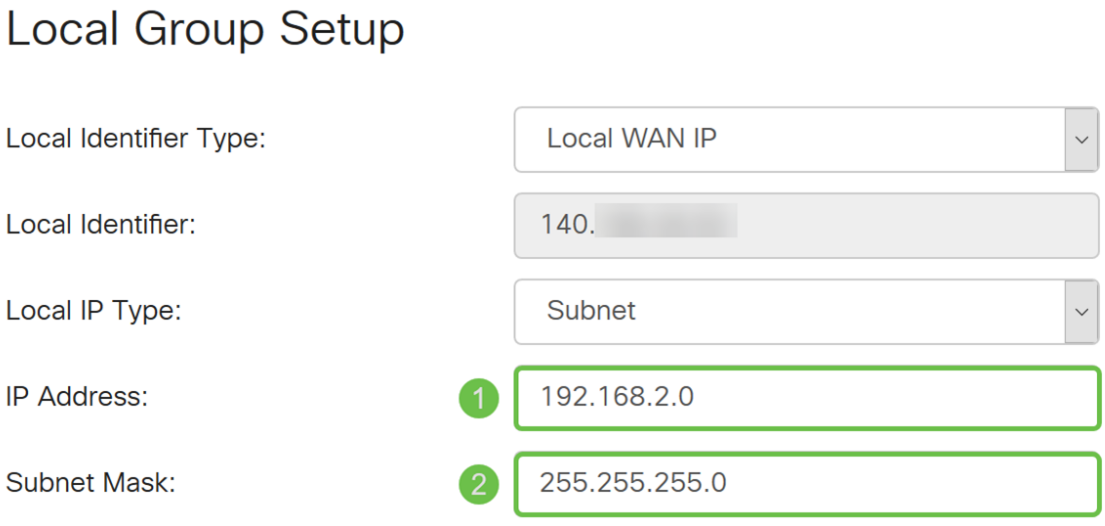

步驟2.對於本地IP型別，從下拉選單中選擇Subnet、Single、**Any**、**IP Group**或GRE Interface。

在本例中，選擇了**Subnet**。




步驟3.輸入可使用此隧道的裝置的IP地址。然後輸入子網掩碼。

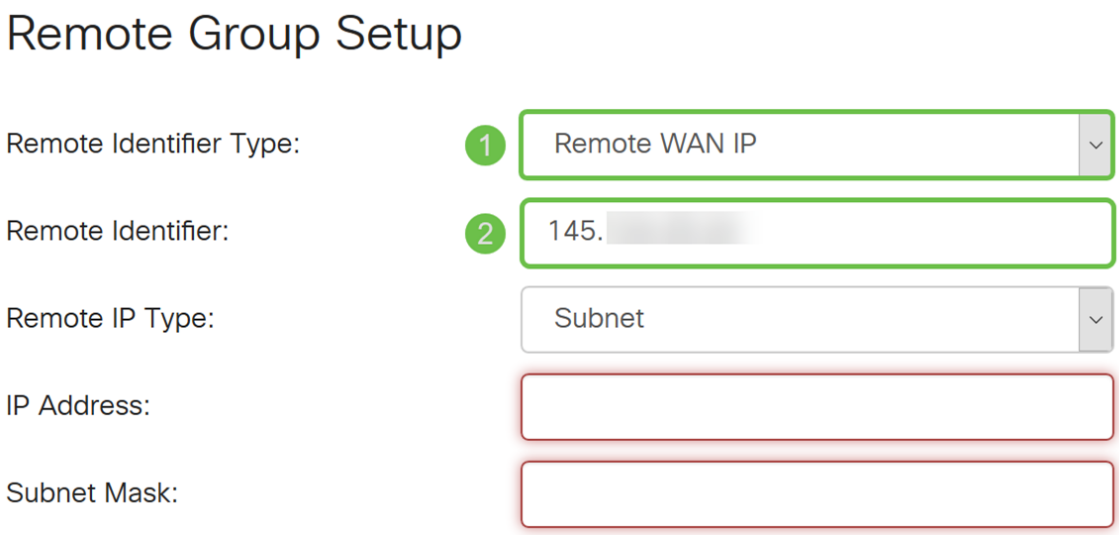
在本演示中，我們將輸入**192.168.2.0**作為本地IP地址，輸入**255.255.255.0**作為子網掩碼。




## 遠端組設定

步驟1.從下拉選單中選擇**遠端WAN IP**、**遠端FQDN**或**遠端使用者FQDN**。根據您的選擇輸入識別符號名稱或IP地址。

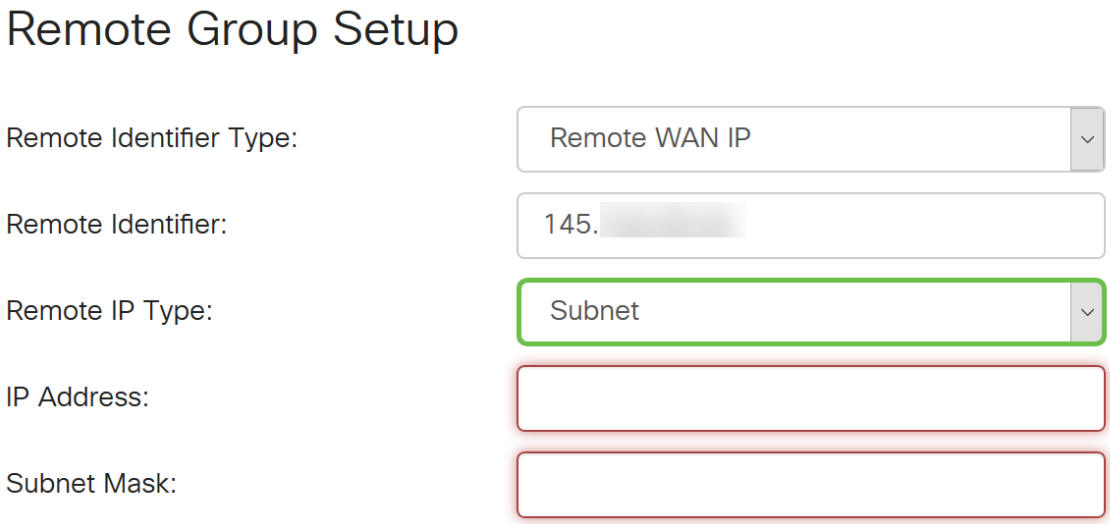
我們已選擇**遠端WAN IP**作為*遠端識別符號型別*，並已輸入遠端路由器的IP地址。




步驟2.從Remote IP Type下拉選單中選擇Subnet、Single、**Any**、IP Group。

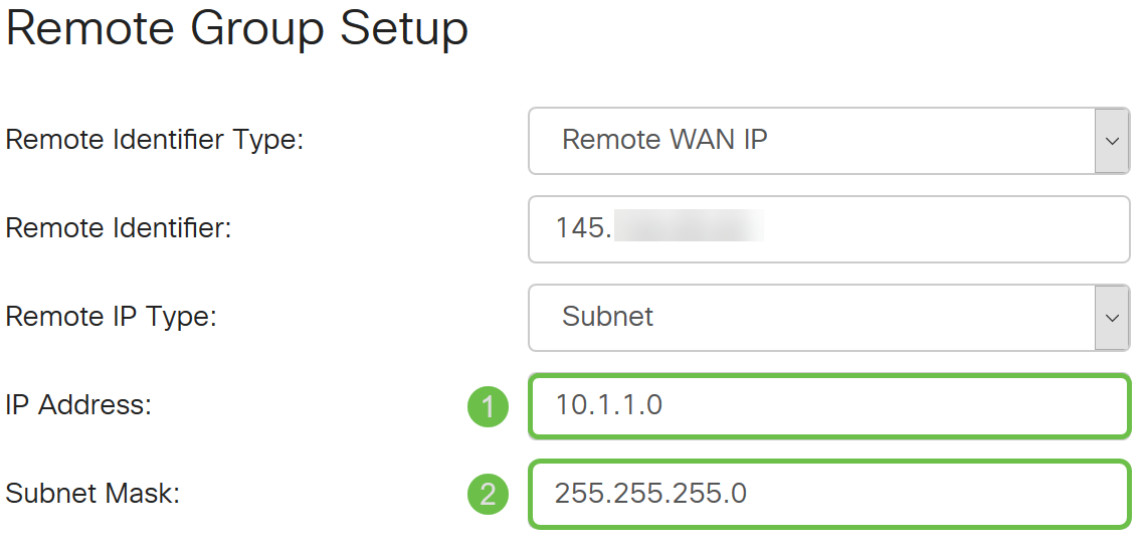
在本例中，我們將選擇**Subnet**。

**附註：**如果已選擇IP組作為遠端IP型別，則會出現一個彈出視窗，用於建立新的IP組。

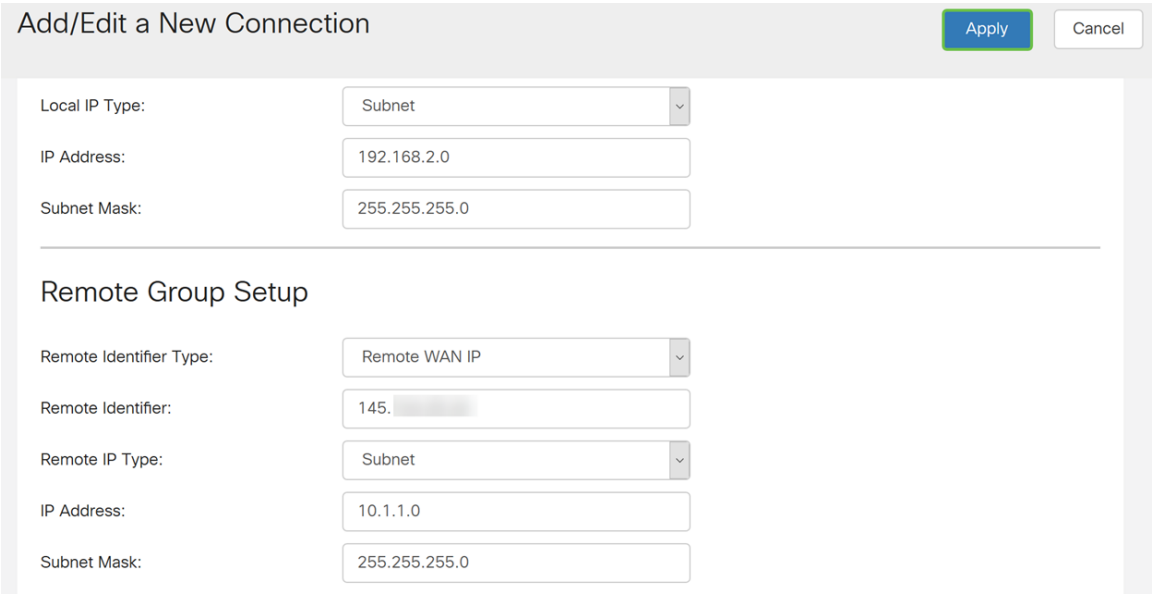



步驟3.輸入可使用此隧道的裝置的IP地址和子網掩碼。

我們已輸入**10.1.1.0**作為可使用此通道的遠端本地IP位址，以及子網路遮罩**255.255.255.0**。



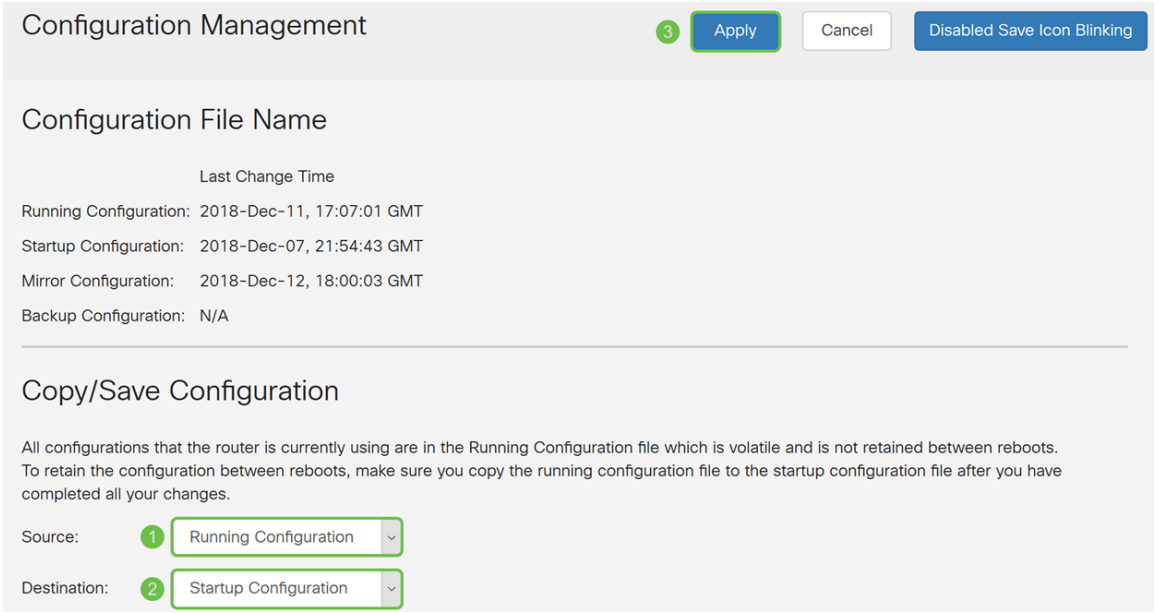

步驟4.按一下**Apply** 建立新的站點到站點VPN連線。




您在路由器上輸入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。

步驟5.在頁面頂部，按一下**Save**按鈕導航到*Configuration Management*，將運行配置儲存到啟動配置。這是要在重新開機後保留組態。


步驟6.在組態管理中，請確認*來源*是**執行組態**，而*目的地*是**啟動組態**。然後按下**Apply**將運行配置儲存到啟動配置。重新啟動後，啟動配置檔案將保留所有配置。




# 結論

現在，您應該已經成功為您的本地路由器新增了新的站點到站點VPN連線。您需要使用相反的資訊配置遠端路由器（路由器B）。