在RV320和RV325 VPN路由器系列上配置單客戶端到網關虛擬專用網路(VPN)

目標

本文檔的目的是向您展示如何在RV32x系列VPN路由器上配置單個客戶端到網關虛擬專用網路(VPN)。

簡介

VPN是通過公共網路虛擬連線遠端使用者的專用網路。其中一種VPN是客戶端到網關VPN。客戶端到網關VPN是遠端使用者與網路之間的連線。使用者端是使用VPN使用者端軟體在使用者裝置上設定的。它允許使用者安全地遠端連線到網路。

適用裝置

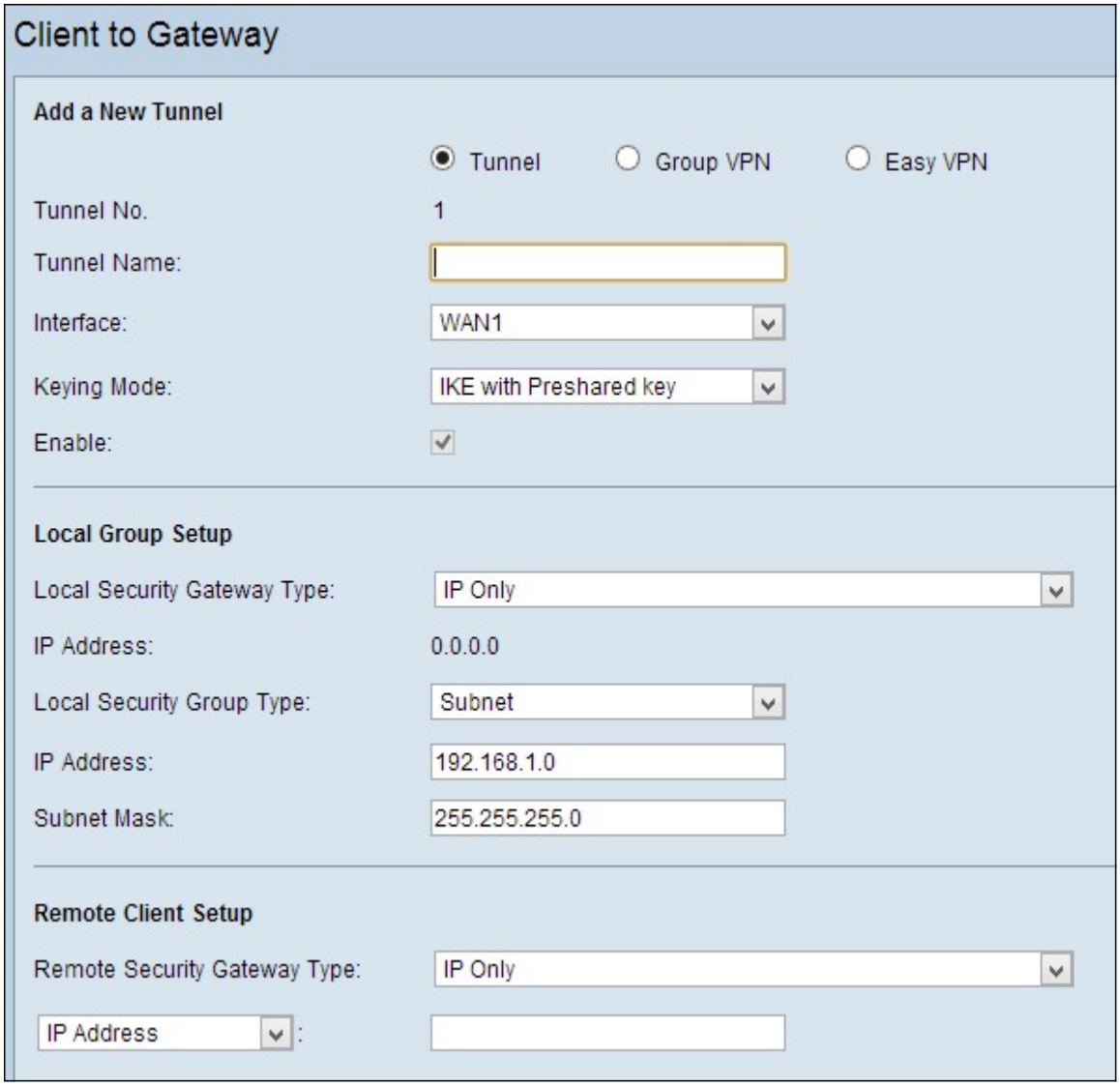
- RV320 Dual WAN VPN路由器
- RV325 Gigabit Dual WAN VPN路由器

軟體版本

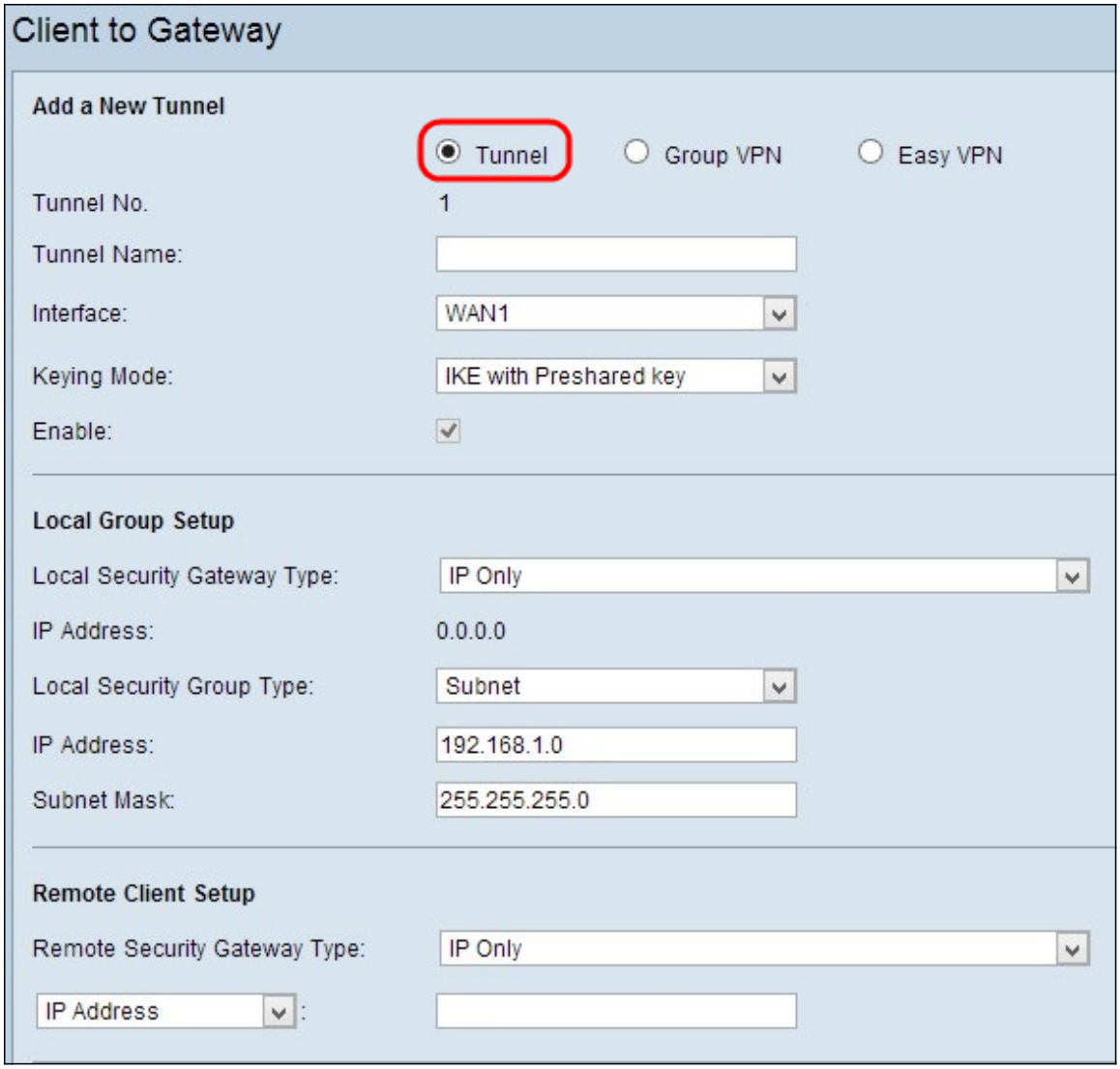
- v1.1.0.09

配置單個客戶端到網關VPN

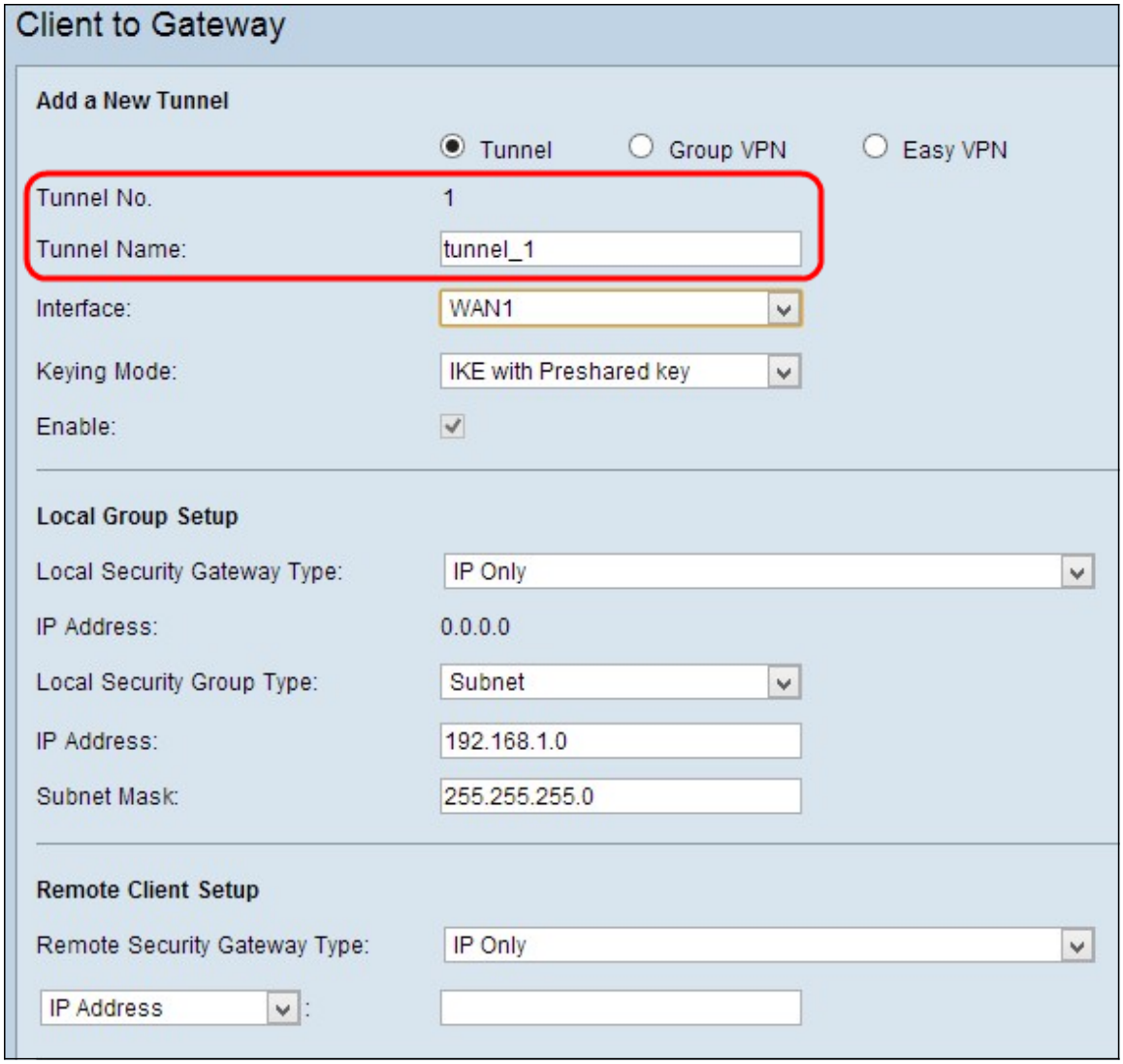
步驟1.登入到Web配置實用程式並選擇**VPN > Client to Gateway**。將開啟*Client to Gateway*頁面：



步驟2.按一下**Tunnel**單選按鈕為客戶端新增一條隧道到網關VPN。


Client to Gateway
Add a New Tunnel
Tunnel
Group VPN
Easy VPN
Tunnel No.
1
Tunnel Name:
Interface:
WAN1
Keying Mode:
IKE with Preshared key
Enable:
Local Group Setup
Local Security Gateway Type:
IP Only
IP Address:
0.0.0.0
Local Security Group Type:
Subnet
IP Address:
192.168.1.0
Subnet Mask:
255.255.255.0
Remote Client Setup
Remote Security Gateway Type:
IP Only
IP Address
:

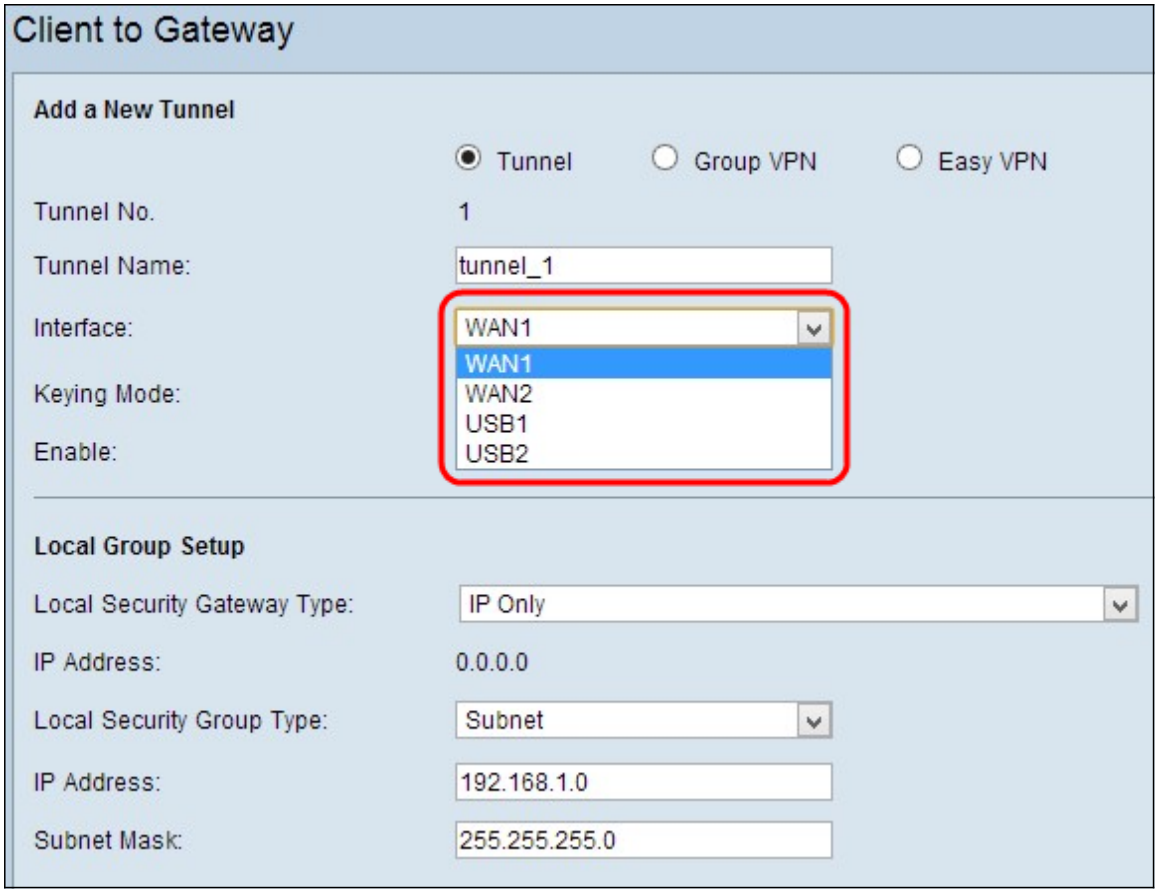
新增新隧道



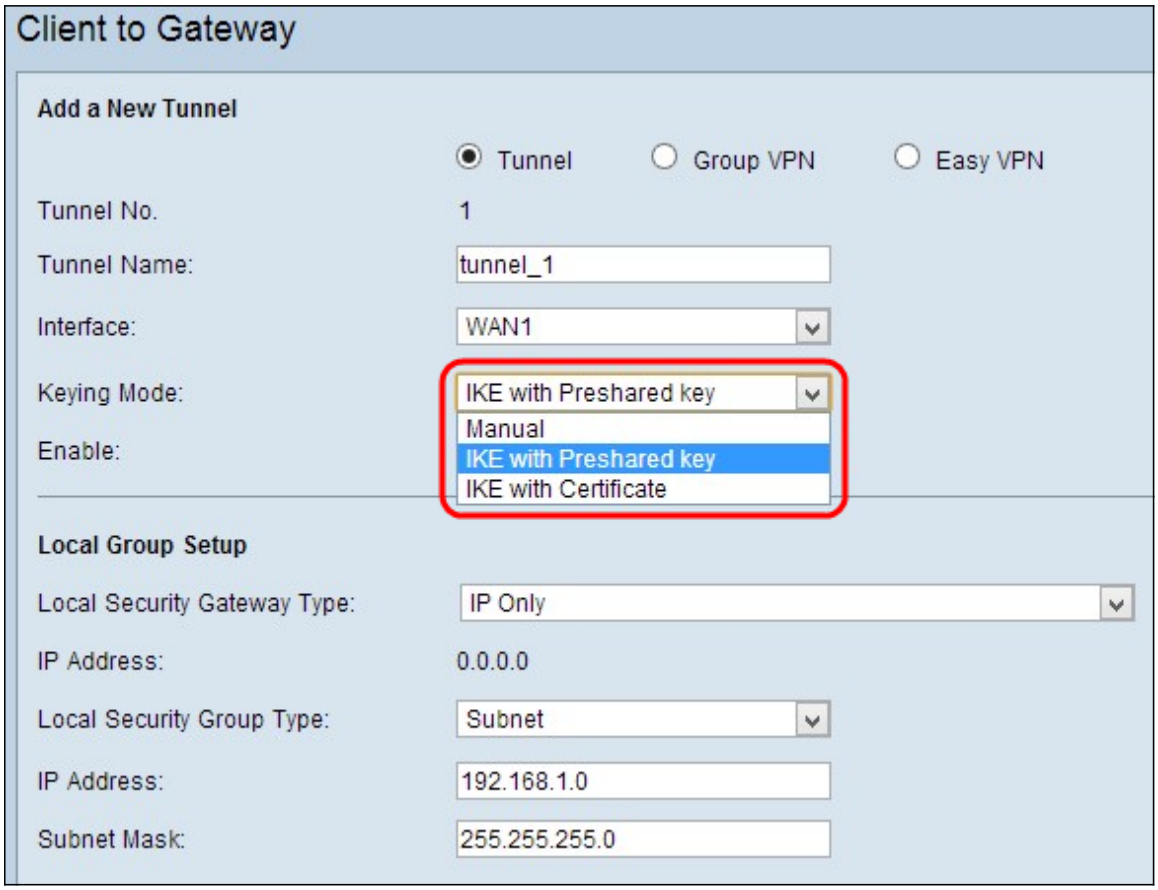
附註：通道編號 — 表示通道編號。此號碼將自動生成。

步驟1.在*Tunnel Name*欄位中輸入隧道的名稱。

步驟2.從*Interface*下拉選單中選擇遠端客戶端訪問VPN所使用的介面。



步驟3.從*Keying Mode*下拉選單中選擇適當的金鑰管理模式以確保安全。預設模式為IKE，使用預共用金鑰。



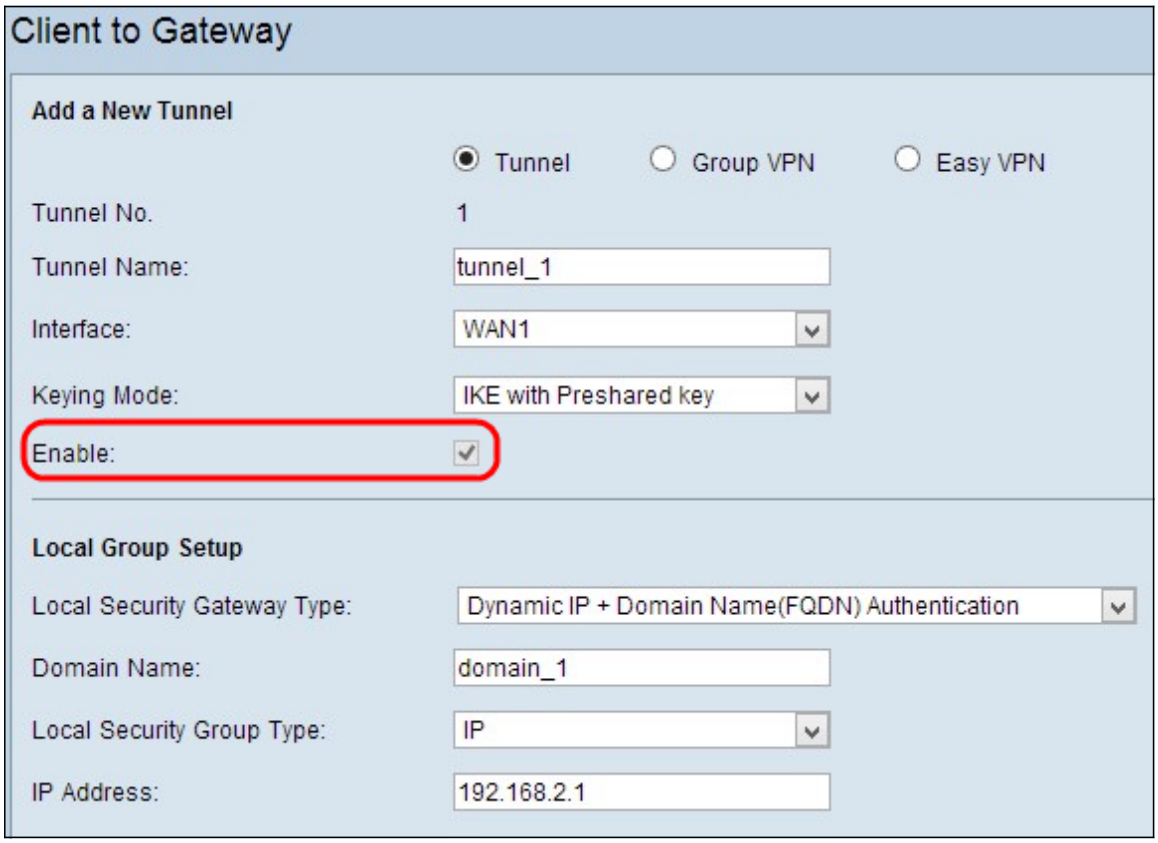
這些選項定義如下：

- 手動 — 自定義安全模式，可自行生成新的安全金鑰，無需與金鑰協商。它最適合在故障排除期

間或小型靜態環境中使用。

- 帶有預共用金鑰的IKE — 網際網路金鑰交換(IKE)協定用於自動生成和交換預共用金鑰以建立隧道的驗證通訊。
- 帶證書的IKE — 帶證書的Internet金鑰交換(IKE)協定是一種更安全的方法，可以自動生成和交換預共用金鑰，為隧道建立更安全的通訊。

步驟4.選中**Enable**覈取方塊以啟用客戶端到網關VPN。預設情況下啟用。



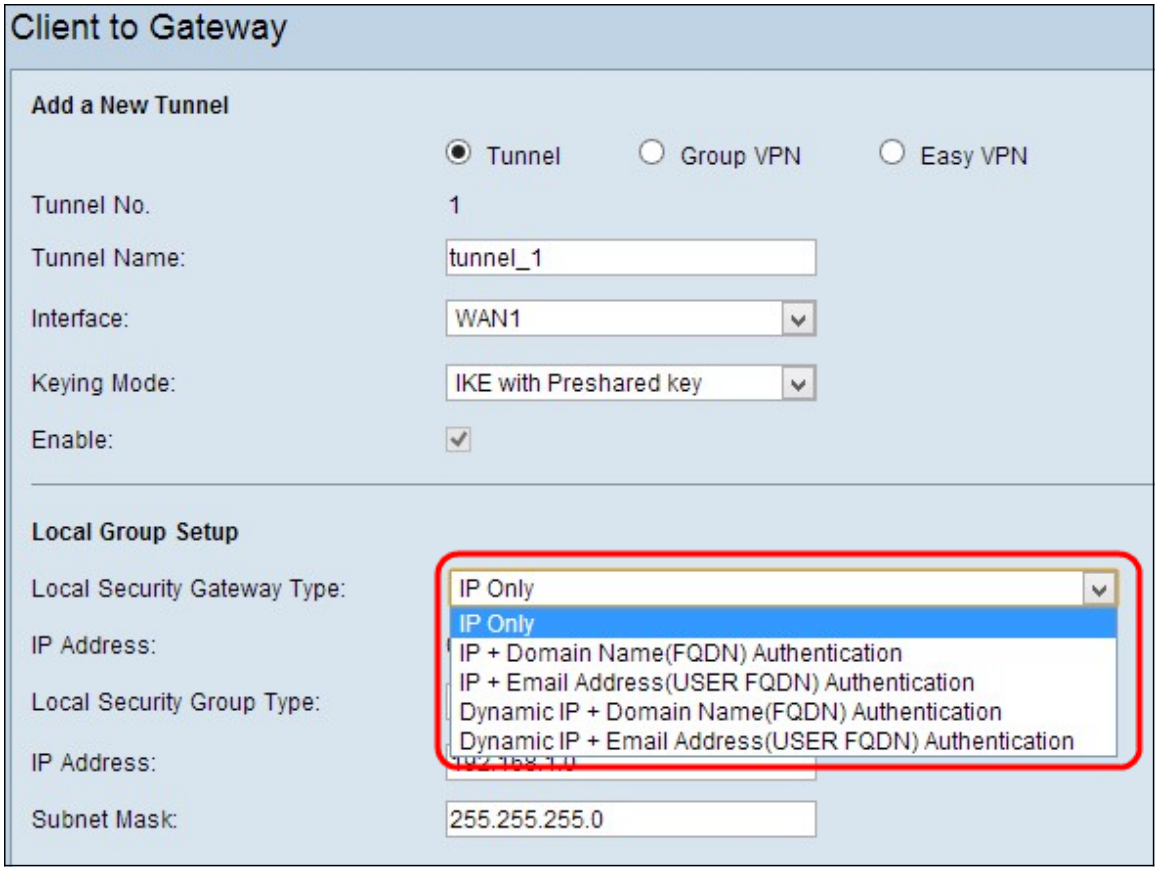
步驟5.如果要儲存目前的設定，請向下滾動，然後按一下**Save**以儲存設定。

本地組設定

使用手動設定本地組，或使用預共用金鑰設定IKE

附註：如果您從*新增新隧道*一節的步驟3中的*金鑰模式*下拉選單中選擇Manual或IKE with Preshared key，請按照以下步驟操作。

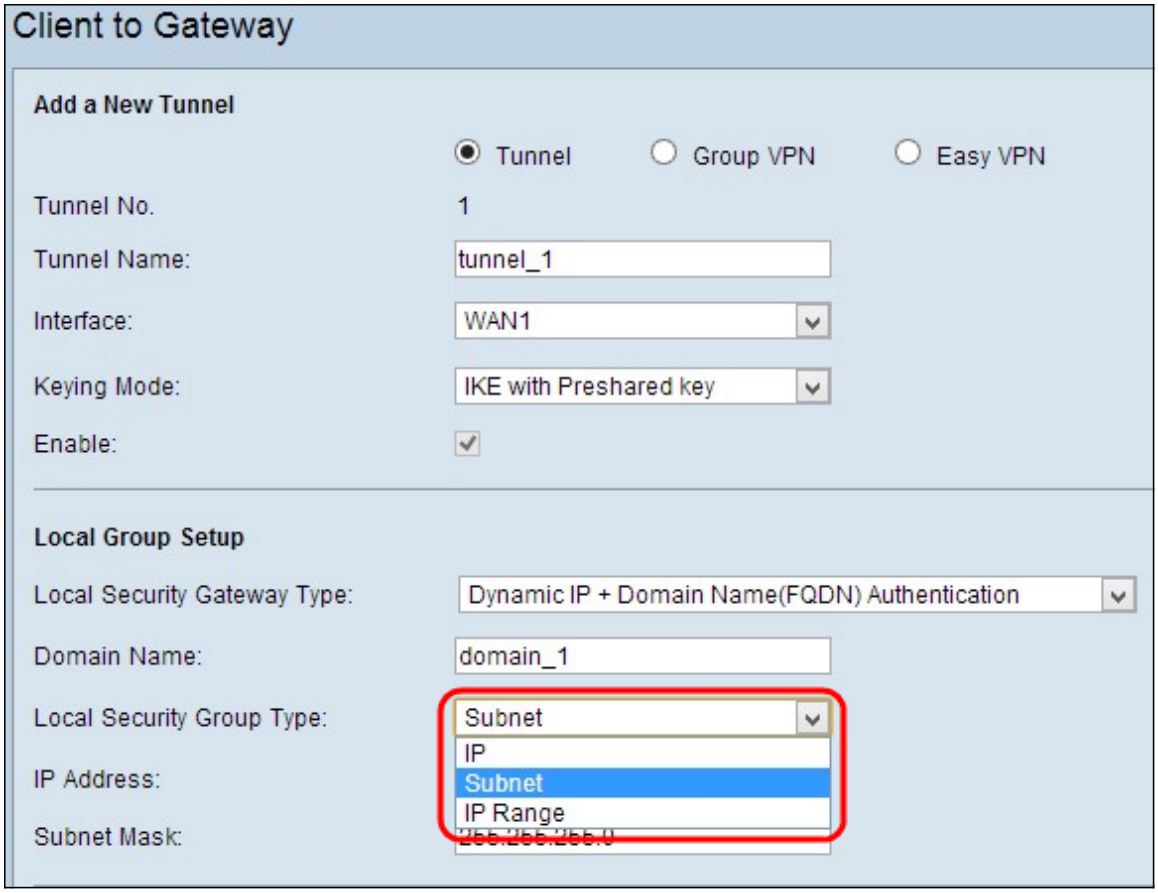
步驟1.從*Local Security Gateway*下拉選單中選擇適當的路由器標識方法以建立VPN隧道。



這些選項定義如下：

- 僅IP — 只能通過靜態WAN IP訪問隧道。如果只有路由器具有任何靜態WAN IP，則可以選擇此選項。靜態WAN IP地址會自動生成。
- IP +域名(FQDN)身份驗證 — 可以通過靜態IP地址和註冊域訪問隧道。如果選擇此選項，請在「域名」欄位中輸入已註冊*域的*名稱。靜態WAN IP地址會自動生成。
- IP +電子郵件地址（使用者FQDN）身份驗證 — 可以通過靜態IP地址和電子郵件地址訪問隧道。如果選擇此選項，請在*Email Address*欄位中輸入電子郵*件地址*。靜態WAN IP地址會自動生成。
- 動態IP +域名(FQDN)身份驗證 — 可以通過動態IP地址和註冊域訪問隧道。如果選擇此選項，請在「域名」欄位中輸入已註冊*域的*名稱。
- 動態IP +電子郵件地址（使用者FQDN）身份驗證 — 可以通過動態IP地址和電子郵件地址訪問隧道。如果選擇此選項，請在*Email Address*欄位中輸入電子郵*件地址*。
- IP地址 — 表示WAN介面的IP地址。它是只讀欄位。

步驟2.從*Local Security Group Type*下拉選單中選擇可以訪問VPN隧道的相應本地LAN使用者或使用者組。預設值為Subnet。

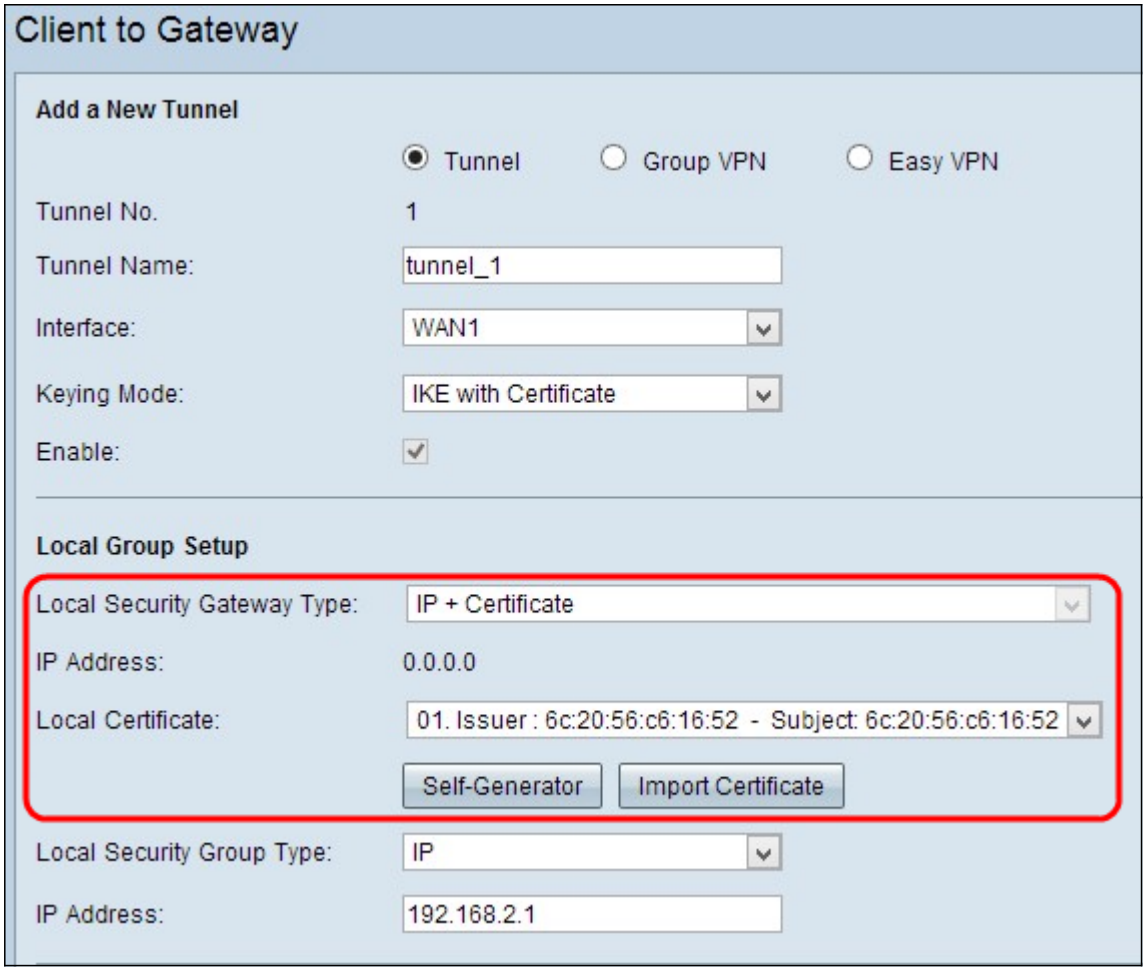


- IP — 只有一個特定的LAN裝置可以存取通道。如果選擇此選項，請在*IP地址*欄位中輸入LAN裝置的IP地址。預設IP是192.168.1.0。
- 子網 — 特定子網上的所有LAN裝置都可以訪問隧道。如果選擇此選項，請在*IP地址*和子網掩碼欄位中分別輸入LAN裝置的IP地址和子網掩碼。預設掩碼為255.255.255.0。
- IP範圍 — 一系列LAN裝置可以存取通道。如果選擇此選項，請在*起始IP*和*結束IP*欄位中分別輸入起始和結束IP地址。預設範圍是從192.168.1.0到192.168.1.254。

步驟3.如果要儲存到目前為止的設定，請向下滾動並按一下**Save**儲存設定。

使用隧道VPN證書的IKE進行本地組設定

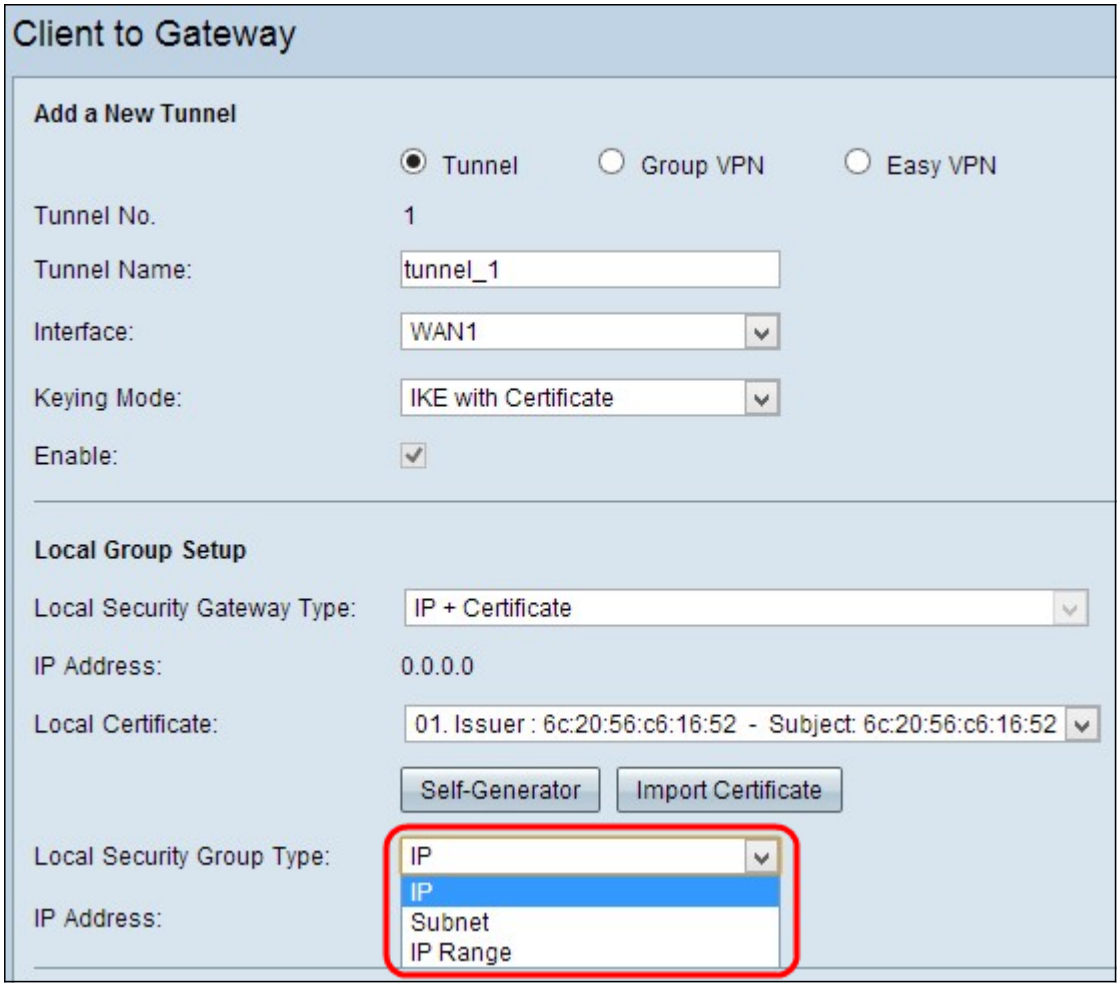
附註：如果您從*新增新隧道*一節的步驟3中的*金鑰模式*下拉選單中選擇IKE with Certificate，請按照以下步驟操作。



- 本地安全閘道型別 — 可以透過具有憑證的IP存取通道。
- IP地址 — 表示WAN介面的IP地址。它是只讀欄位。

步驟1.從*Local Certificate*下拉選單中選擇相應的本地證書以標識路由器。按一下**Self-Generator**以自動生成證書，或按一下**Import Certificate**以匯入新證書。

注意：要詳細瞭解如何自動生成證書，請參閱*在RV320路由器上生成證書*，**要瞭解如何匯入證書，請參閱***在RV320路由器上配置我的證書*。



步驟2.從*Local Security Group Type*下拉選單中選擇可訪問VPN隧道的適當型別的本地LAN使用者或使用者組。預設值為Subnet。

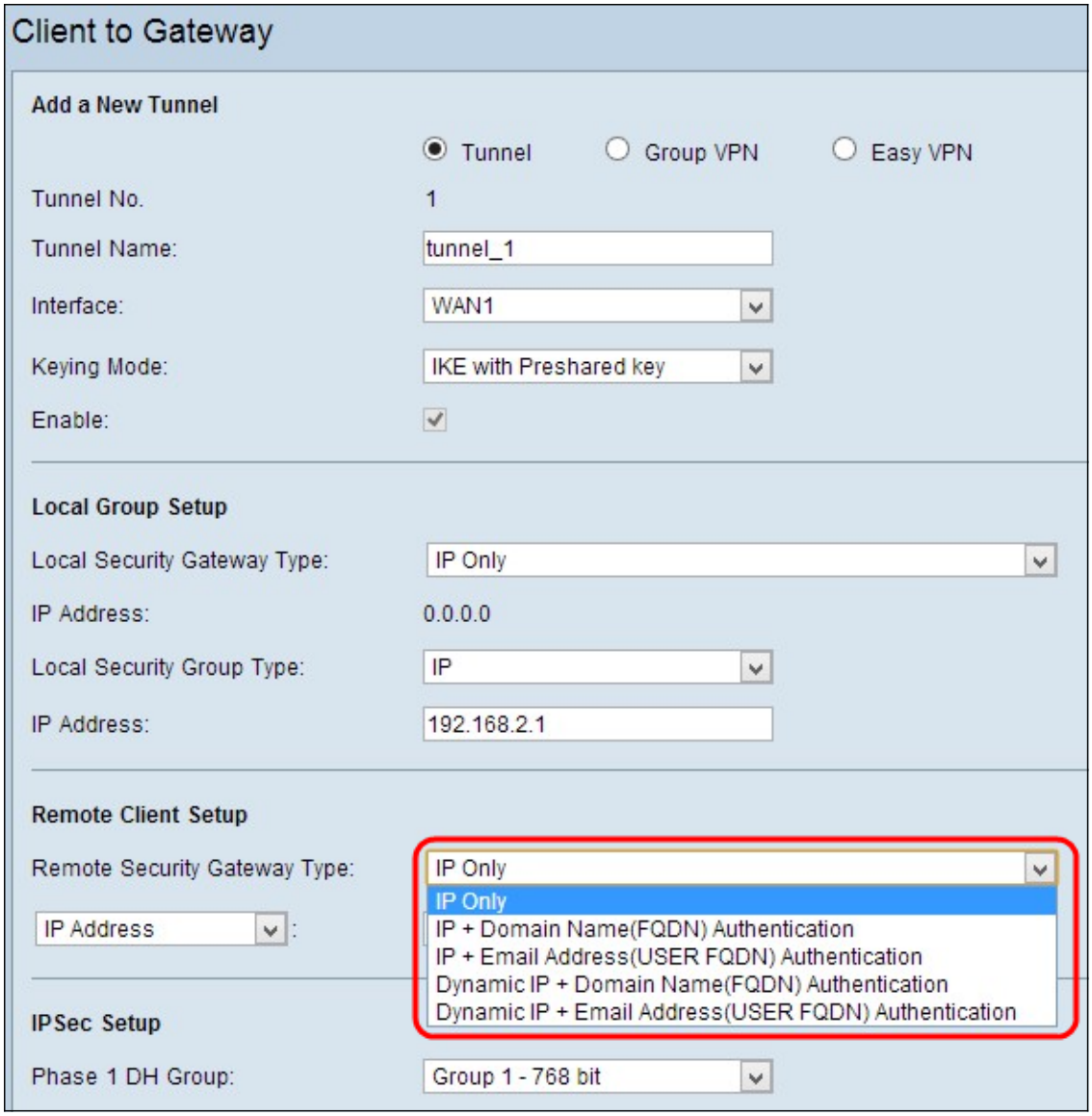
- IP — 只有一個特定的LAN裝置可以存取通道。如果選擇此選項，請在「IP地址」欄位中輸入LAN裝置的IP地址。預設IP是192.168.1.0。
- 子網 — 特定子網上的所有LAN裝置均可訪問隧道。如果選擇此選項，請分別在IP地址和子網掩碼欄位中輸入LAN裝置的IP地址和子網掩碼。預設掩碼為255.255.255.0。
- IP範圍 — 一系列LAN裝置可以存取通道。如果選擇此選項，請在起始IP和結束IP欄位中分別輸入起始和結束IP地址。預設範圍是從192.168.1.0到192.168.1.254。

步驟3.如果要儲存到目前為止的設定，請向下滾動並按一下**Save**儲存設定。

遠端客戶端設定

使用手動設定遠端客戶端或使用預共用金鑰設定IKE

注意：如果您在「*新增新隧道」一節的步驟3中的Keying Mode*下拉選單中選擇Manual或IKE with Preshared Key，請執行以下步驟。



步驟1.從*Remote Security Gateway*下拉選單中選擇相應的客戶端標識方法以建立VPN隧道。預設值為IP Only。

- 僅IP — 只能通過客戶端的靜態WAN IP訪問隧道。只有知道客戶端的靜態WAN IP或域名時，才能選擇此選項。從下拉選單中選擇IP地址並在相鄰欄位中輸入客戶端的靜態IP，或從下拉選單中選擇IP by DNS Resolved並在相鄰欄位中輸入該IP地址的域名。路由器可以通過IP地址的本地DNS伺服器自動檢索IP地址。

  附註：如果在Add a New Tunnel Through Tunnel or Group VPN一節的步驟3中的*Keying Mode*下拉選單中選擇Manual，這將是唯一可用的選項。

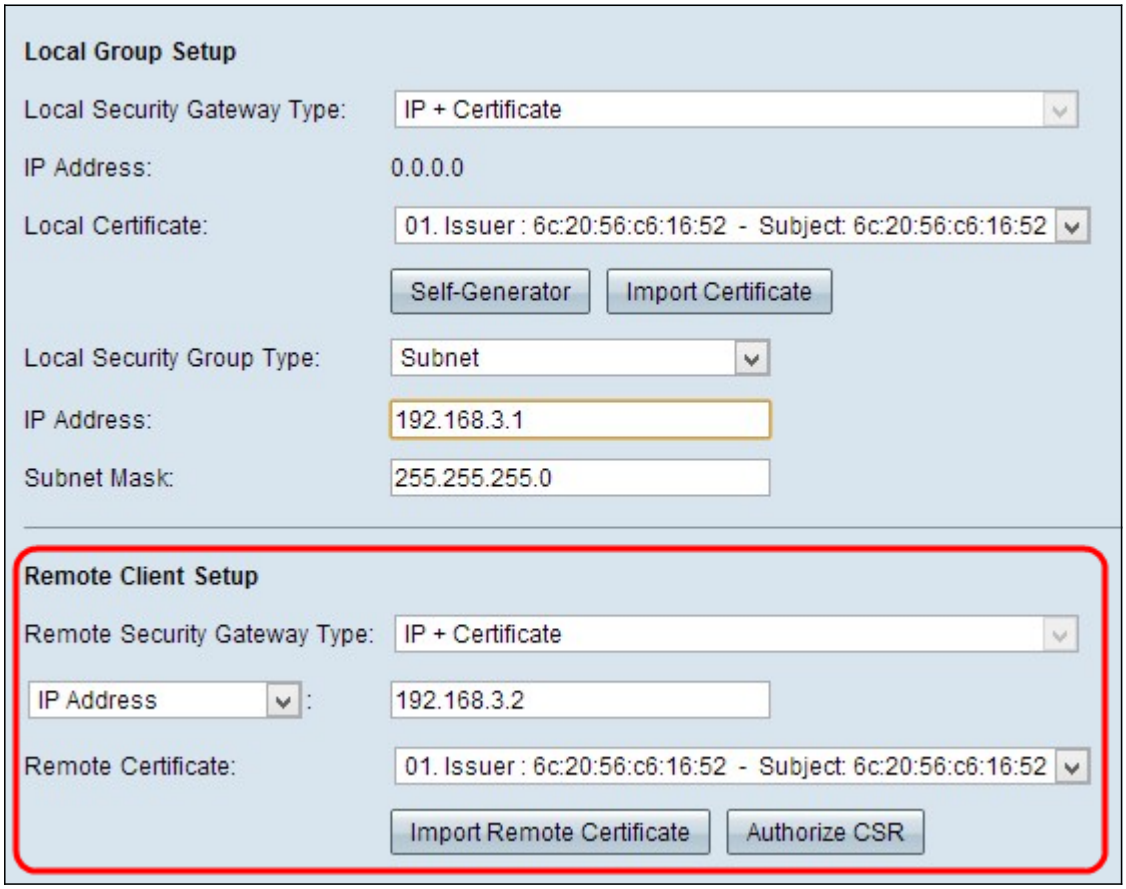
- IP +域名(FQDN)身份驗證 — 可以通過客戶端的靜態IP地址和註冊的域訪問隧道。如果選擇此選項，請在「域名」欄位中輸入已註冊域的名稱。從下拉選單中選擇IP地址並在相鄰欄位中輸入客戶端的靜態IP，或從下拉選單中選擇IP by DNS Resolved並在相鄰欄位中輸入該IP地址的域名。路由器可以通過IP地址的本地DNS伺服器自動檢索IP地址。
- IP +電子郵件地址（使用者FQDN）身份驗證 — 可以通過客戶端的靜態IP地址和電子郵件地址訪問隧道。如果選擇此選項，請在「電子郵件地址」欄位中輸入電子郵件地址。從下拉選單中選擇「IP地址」並在相鄰欄位中輸入客戶端的靜態IP，或從下拉選單中選擇「通過DNS解析IP」，然後在相鄰欄位中輸入IP地址的域名。路由器可以通過IP地址的本地DNS伺服器自動檢索IP地址。

- 動態IP +域名(FQDN)身份驗證 — 可以通過客戶端和註冊域的動態IP地址訪問隧道。如果選擇此選項，請在「域名」欄位中輸入已註冊域的名稱。
- 動態IP +電子郵件地址（使用者FQDN）身份驗證 — 可以通過客戶端的動態IP地址和電子郵件地址訪問隧道。如果選擇此選項，請在「電子郵件地址」欄位中輸入電子郵件地址。

步驟2.如果要儲存目前所用的設定，請向下滾動並按一下**Save**儲存設定。

使用IKE和證書的遠端組設定

注意：如果您在「*新增新隧道」一節的步驟3中的Keying Mode*下拉選單中選擇IKE with Certificate，請執行以下步驟。



- 遠端安全網關型別 — 可以通過具有證書的IP來建立VPN連線。

步驟1.從下拉選單中選擇**IP Address**或**IP by DNS Resolved**。

- IP地址 — 只能通過客戶端的靜態WAN IP訪問隧道。只有知道客戶端的靜態WAN IP時，才能選擇此選項。在*IP address*欄位中輸入客戶端的靜態IP。
- IP By DNS Resolved — 如果您不知道客戶端的IP地址，但知道該IP地址的域，則非常有用。輸入IP地址的域名。路由器可以通過IP地址的本地DNS伺服器自動檢索IP地址。

步驟2.從*Remote Certificate*下拉選單中選擇適當的遠端證書。按一下**Import Remote Certificate**以匯入新證書，或按一下**Authorize CSR**以使用數位簽章請求標識證書。

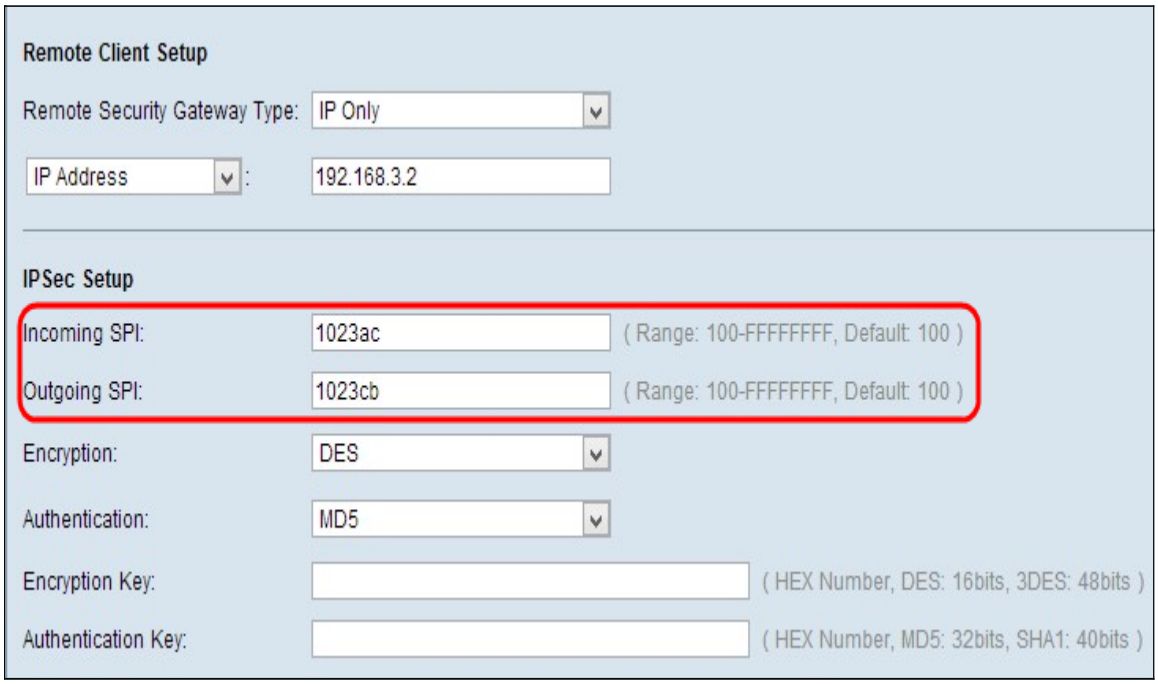
附註：如果您想知道有關如何匯入新證書的更多資訊，請參閱*檢視/新增RV320路由器上的受信任SSL證書*，要瞭解有關授權CSR的更多資訊，請參閱*RV320路由器上的證書簽名請求(CSR)*。

步驟3.如果要儲存到目前為止的設定，請向下滾動並按一下**Save**儲存設定。

IPSec設定

使用手動金鑰設定IPSec

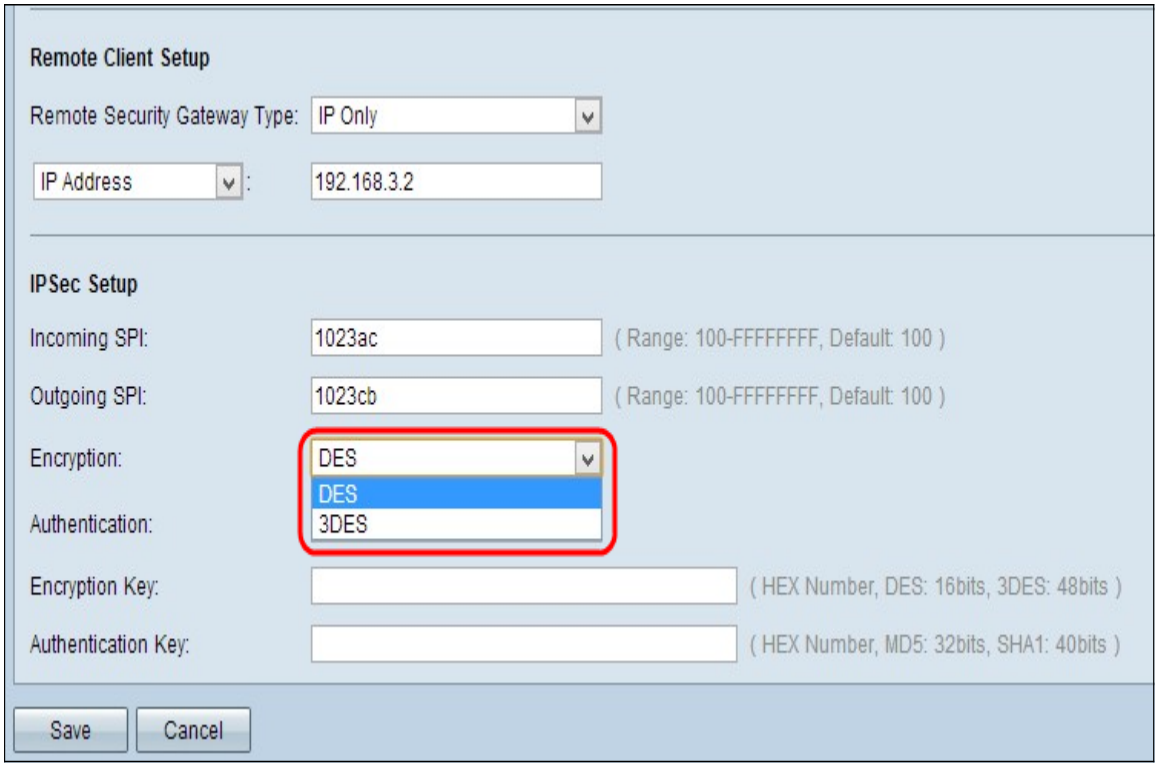
注意：如果您從*Add a New Tunnel一節的步驟3中的Keying Mode*下拉選單中選擇Manual（手動），請執行以下步驟。



步驟1.在*傳入SPI*欄位中輸入傳入的安全引數索引(SPI)的唯一十六進位制值。SPI承載在封裝安全負載協定(ESP)報頭中，該報頭共同確定傳入資料包的安全關聯(SA)。範圍為100到ffffffff，預設值為100。

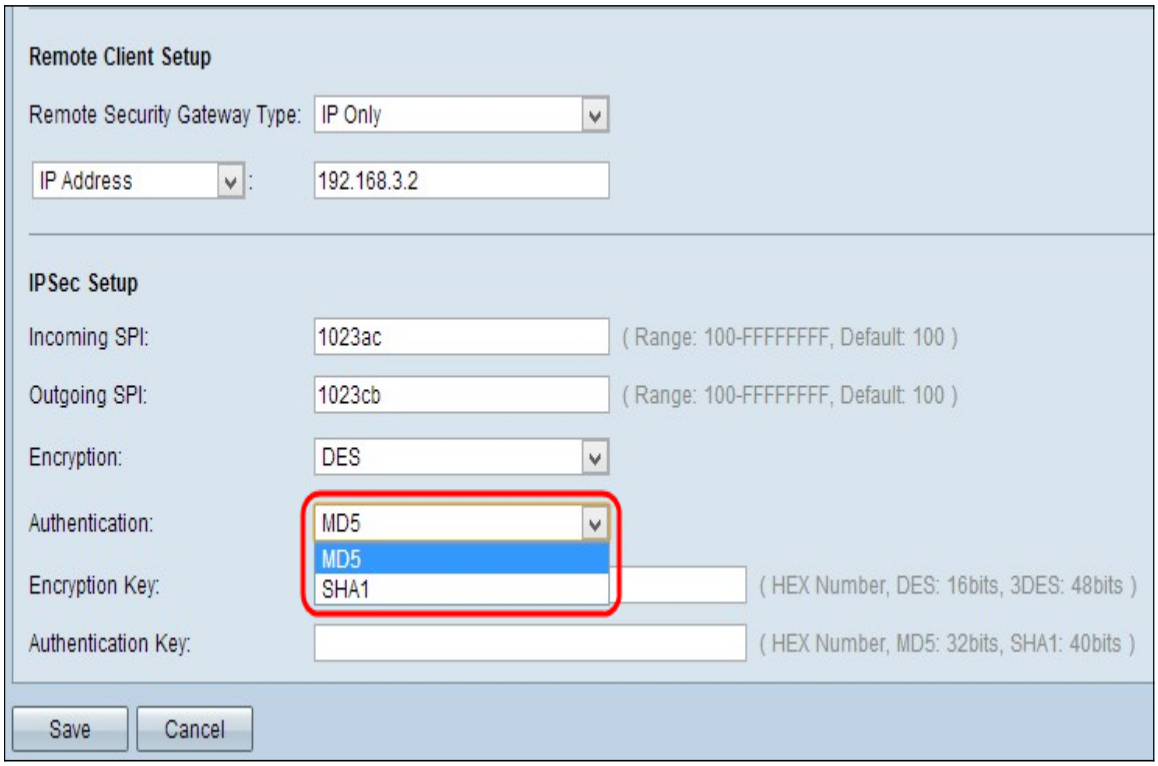
步驟2.在*Outgoing SPI*（傳出SPI）欄位中輸入傳出安全引數索引(SPI)的唯一*十六進位制*值。SPI在封裝安全負載協定(ESP)報頭中攜帶，ESP報頭共同確定傳出資料包的安全關聯(SA)。範圍為100到ffffffff，預設值為100。

附註：連線裝置的傳入SPI和通道另一端的傳出SPI應相互匹配以建立通道。



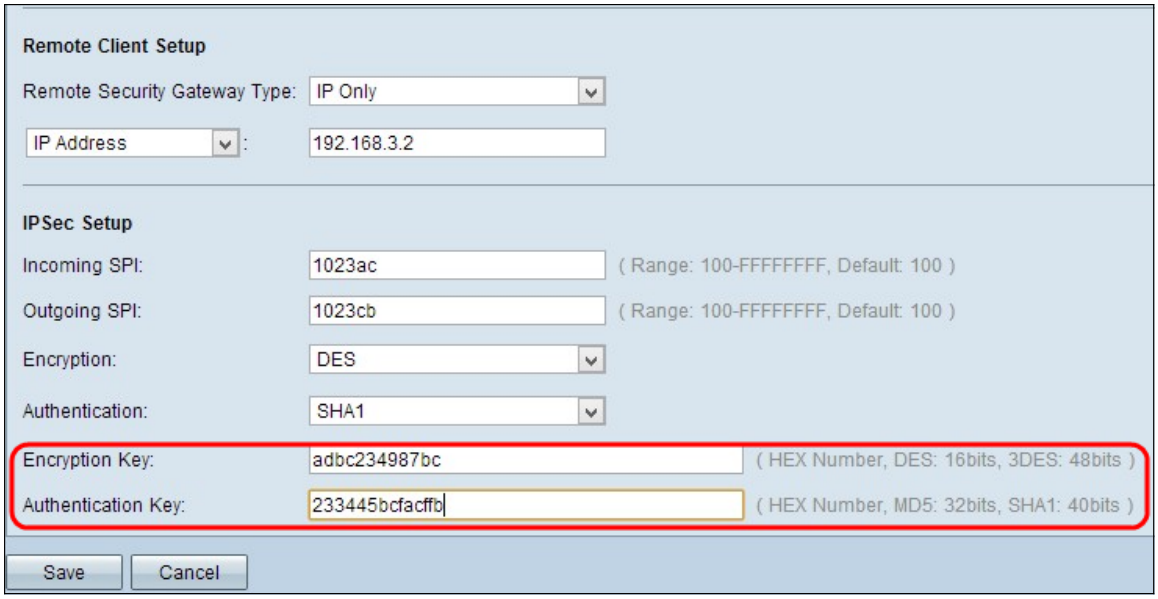
步驟3.從*Encryption*下拉式清單中選擇適當的加密方法。推薦的加密是3DES。VPN通道的兩端需要使用相同的加密方法。

- DES — 資料加密標準(DES)是一種56位、較舊、向後相容的加密方法，安全性較低。
- 3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法，通過對資料進行三次加密來增加金鑰大小，比DES具有更高的安全性。



步驟4.從*Authentication*下拉選單中選擇相應的身份驗證方法。推薦的身份驗證是SHA1。VPN隧道的兩端需要使用相同的身份驗證方法。

- MD5 - Message Digest Algorithm-5(MD5)表示32位十六進位制雜湊函式，通過校驗和計算為資料提供保護，使其免受惡意攻擊。
- SHA1 — 安全雜湊演算法版本1(SHA1)是160位元的雜湊函式，比MD5更安全。



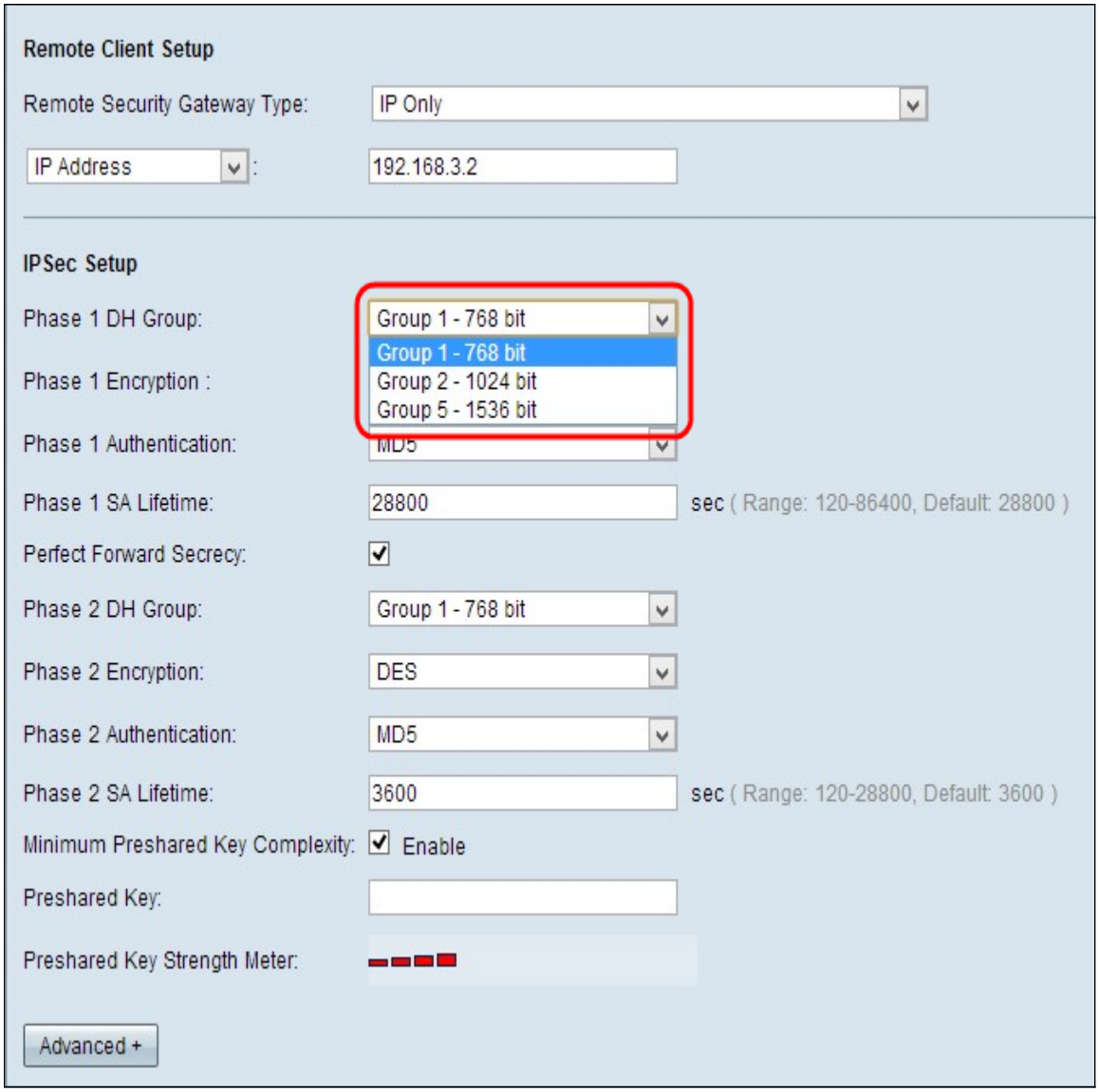
步驟5.在*Encryption Key*欄位中輸入要加密和解密資料的金鑰。如果在步驟3中選擇了DES作為加密方法，請輸入一個16位的十六進位制值。如果在步驟3中選擇了3DES作為加密方法，請輸入一個40位的十六進位制值。

步驟6.在*Authentication Key*欄位中輸入預共用金鑰以驗證流量。如果在步驟4中選擇MD5作為身份驗證方法，請輸入32位十六進位制值。如果您在步驟4中選擇SHA作為驗證方法，請輸入40位十六進位制值。VPN隧道的兩端需要使用相同的預共用金鑰。

步驟7.如果要儲存目前所用的設定，請向下滾動並按一下**Save**儲存設定。

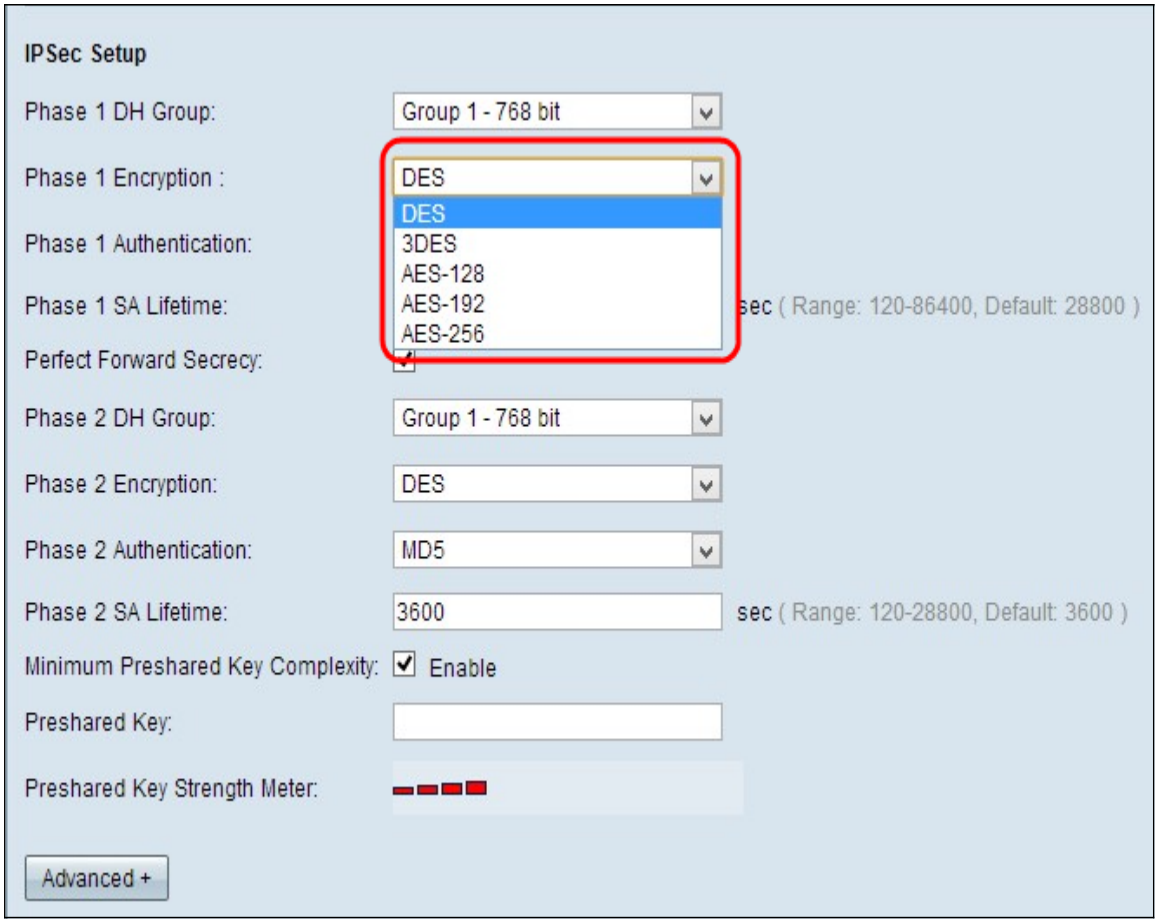
使用預共用金鑰的IKE或使用證書的IKE的IPSec設定

注意：如果您在「*新增新隧道」一節的步驟3的「金鑰模式」下拉選單中選擇「帶預共用金鑰的IKE*」或「帶證書的IKE」，請執行以下步驟。



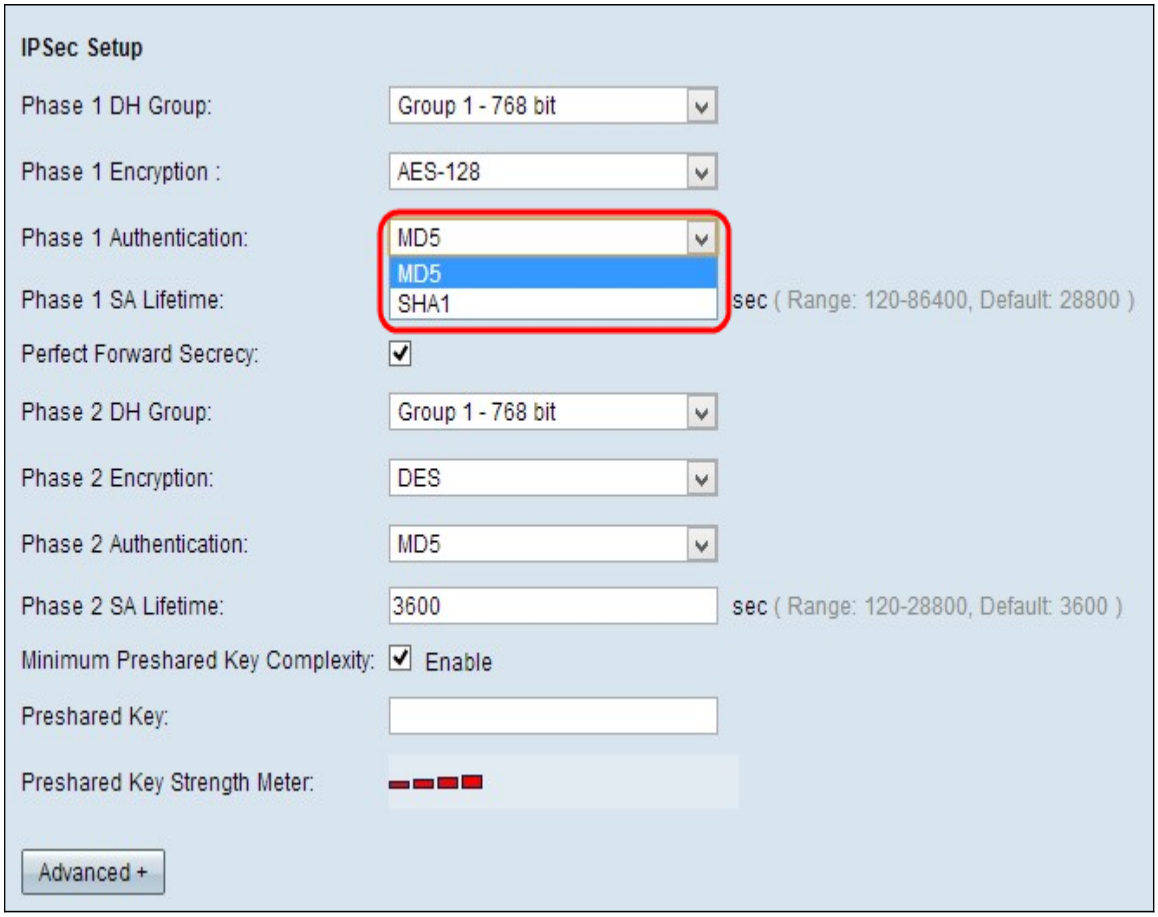
步驟1.從*Phase 1 DH* Group下拉選單中*選擇適當*的第1階段DH組。階段1用於在隧道兩端之間建立單純的邏輯安全關聯(SA)，以支援安全的真實通訊。Diffie-hellman(DH)是在階段1連線期間用於共用金鑰以驗證通訊的金鑰交換協定。

- 組1 - 768位 — 表示強度最低的金鑰和最不安全的身份驗證組。但計算IKE金鑰所需的時間更少。如果網路速度低，則優先使用。
- 組2 - 1024位 — 表示強度更高的金鑰和更安全的身份驗證組。但需要一些時間來計算IKE金鑰。
- 組5 - 1536位 — 表示強度最高的金鑰和最安全的身份驗證組。它需要更多時間計算IKE金鑰。如果網路速度高，則優先使用。



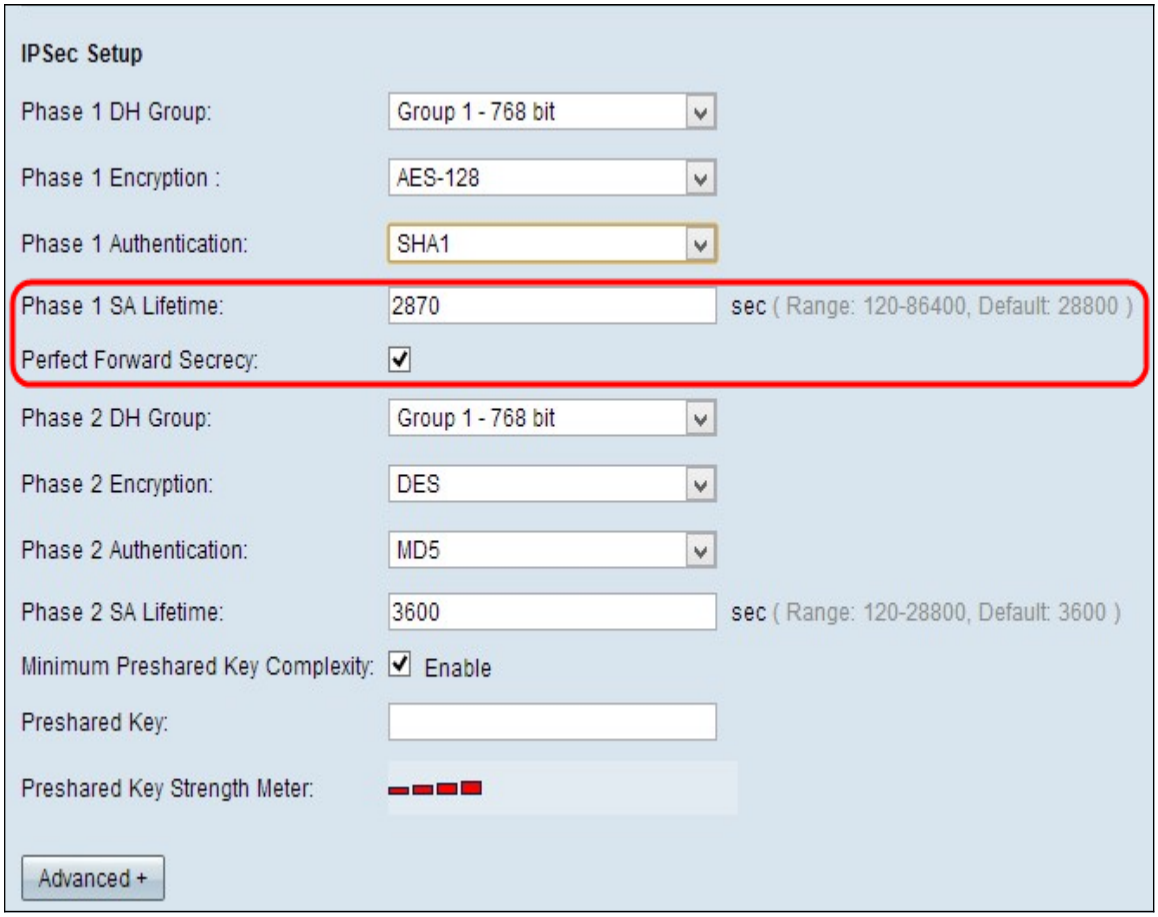
步驟2.從*Phase 1 Encryption*下拉式清單中選擇適當的階段1加密以加密金鑰。建議使用AES-256，因為它是最安全的加密方法。VPN通道的兩端需要使用相同的加密方法。

- DES — 資料加密標準(DES)是56位的，舊加密方法，並不是非常安全的加密方法。
- 3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法，通過對資料進行三次加密來增加金鑰大小，比DES具有更高的安全性。
- AES-128 — 高級加密標準(AES)是128位元加密方法，它通過10個週期的重複將純文字檔案轉換為密文。
- AES-192 — 高級加密標準(AES)是一種通過12個循環重複將純文字檔案轉換為密文的192位加密方法。
- AES-256 — 高級加密標準(AES)是256位加密方法，它通過14個週期的重複將純文字檔案轉換為密文。



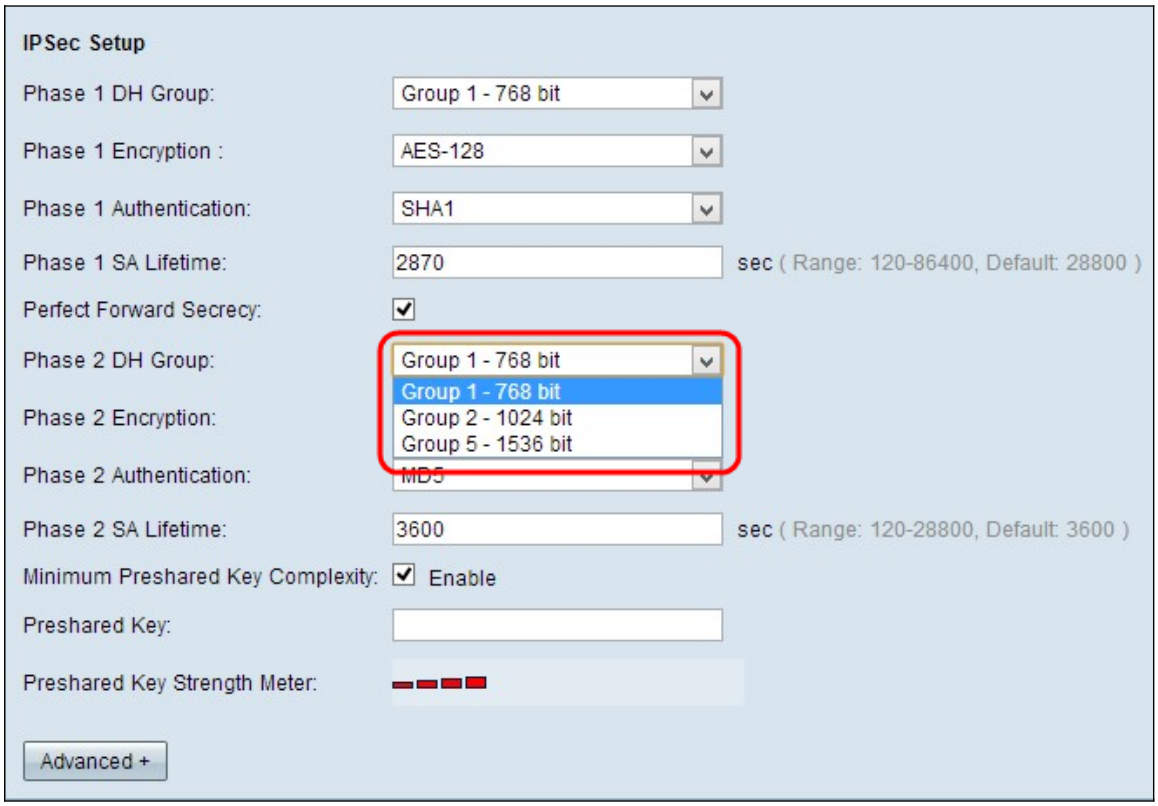
步驟3.從*Phase 1 Authentication*下拉選單中選擇相應的身份驗證方法。VPN隧道的兩端需要使用相同的身份驗證方法。

- MD5 - Message Digest Algorithm-5(MD5)表示32位十六進位制雜湊函式，通過校驗和計算為資料提供保護，使其免受惡意攻擊。
- SHA1 — 安全雜湊演算法版本1(SHA1)是160位元的雜湊函式，比MD5更安全。



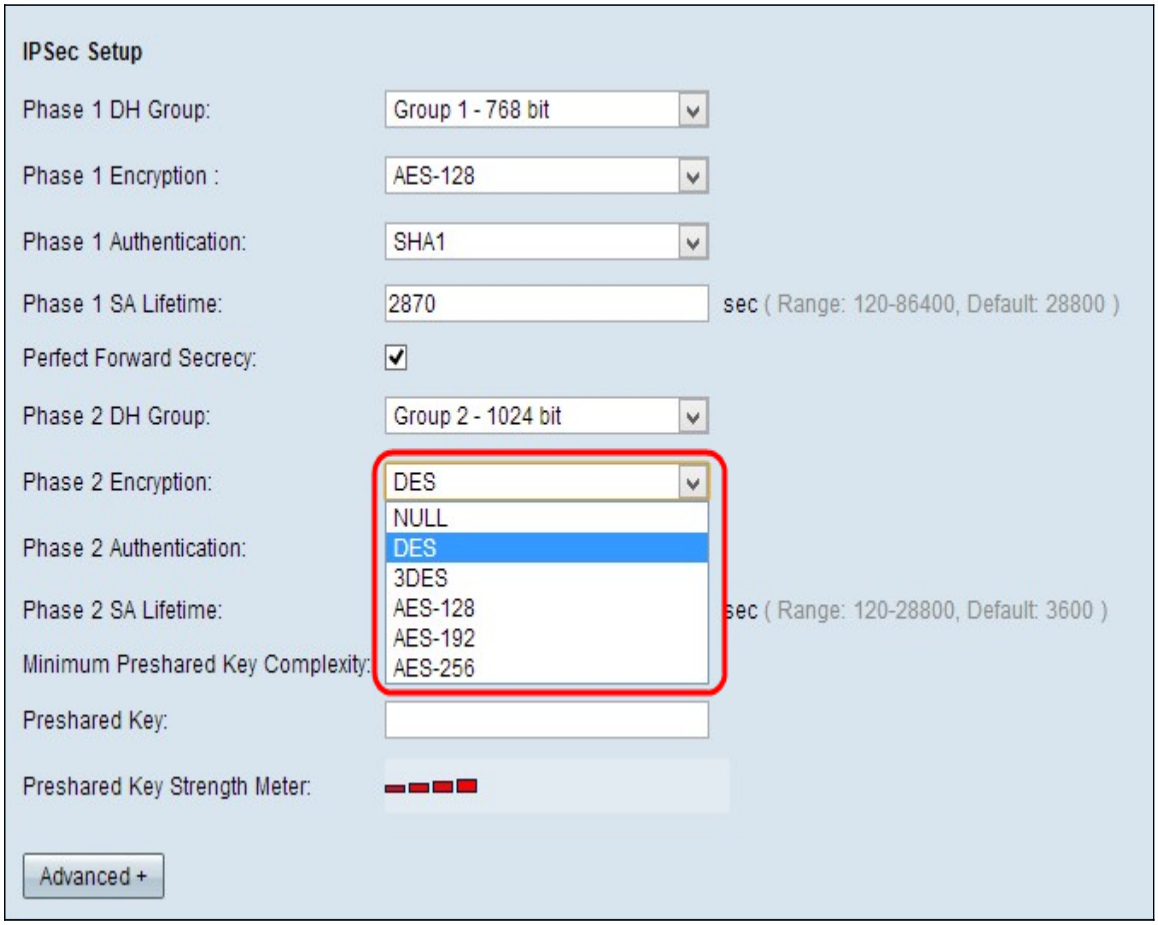
步驟4.在*Phase 1 SA Lifetime欄位中輸入*VPN隧道保持活動狀態的時間量（以秒為單位），在階段1中,*VPN隧道保持活*動狀態。 預設時間為28800秒。

步驟5.選中**Perfect Forward Secrecy**覈取方塊以對金鑰提供更多保護。此選項允許在任何金鑰受到危害時生成新金鑰。加密資料僅通過被洩露的金鑰被洩露。因此，當通過金鑰洩露保護其他金鑰時，它可提供更安全的身份驗證通訊。這是推薦的操作，因為它提供了更高的安全性。



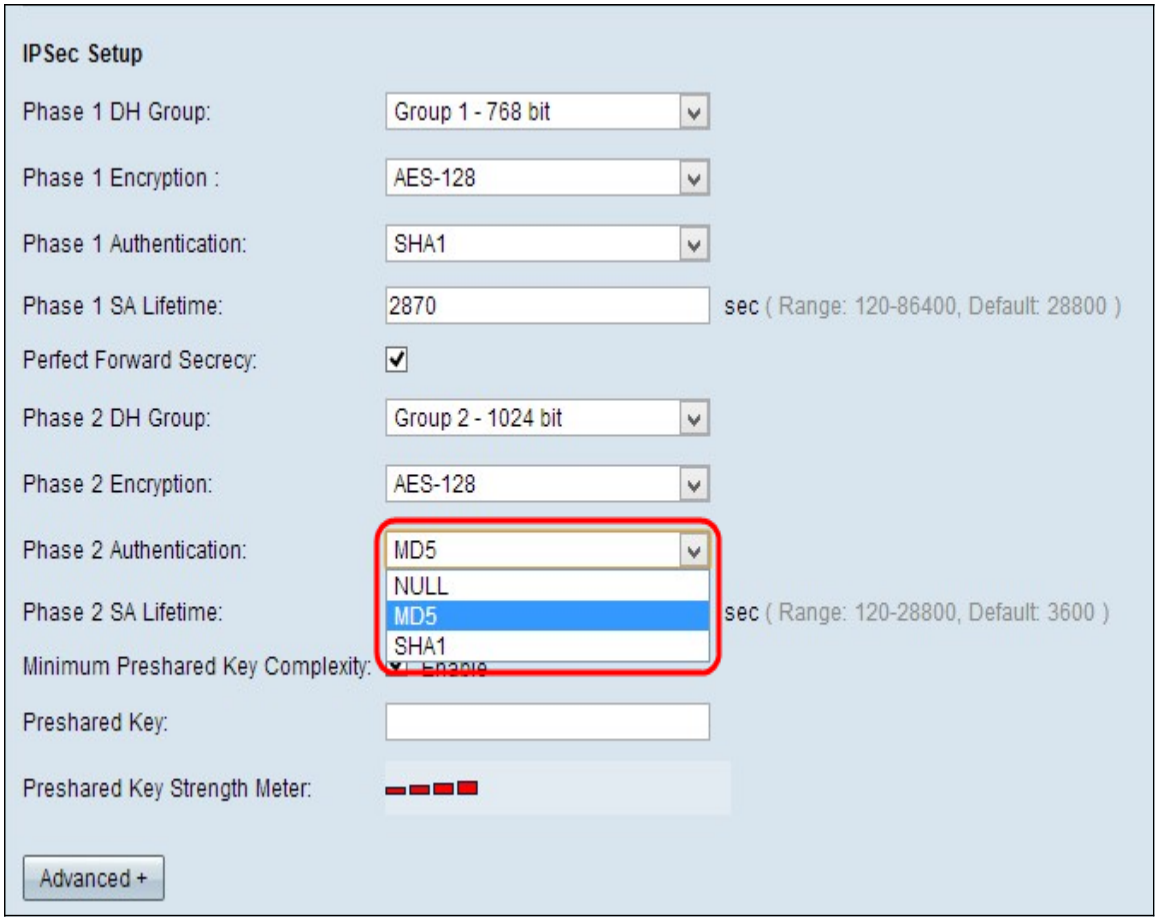
步驟6.從*Phase 2 DH Group*（第2階段DH組）下*拉清單中選擇相*應的第2階段DH組。階段1用於在隧道兩端之間建立單純的邏輯安全關聯(SA)，以支援安全身份驗證通訊。Diffie-hellman(DH)是在階段1連線期間用於共用金鑰以驗證通訊的金鑰交換協定。

- 組1 - 768位 — 表示強度最低的金鑰和最不安全的身份驗證組。但計算IKE金鑰所需的時間更少。如果網路速度低，則優先使用。
- 組2 - 1024位 — 表示強度更高的金鑰和更安全的身份驗證組。但需要一些時間來計算IKE金鑰。
- 組5 - 1536位 — 表示強度最高的金鑰和最安全的身份驗證組。它需要更多時間計算IKE金鑰。如果網路速度高，則優先使用。



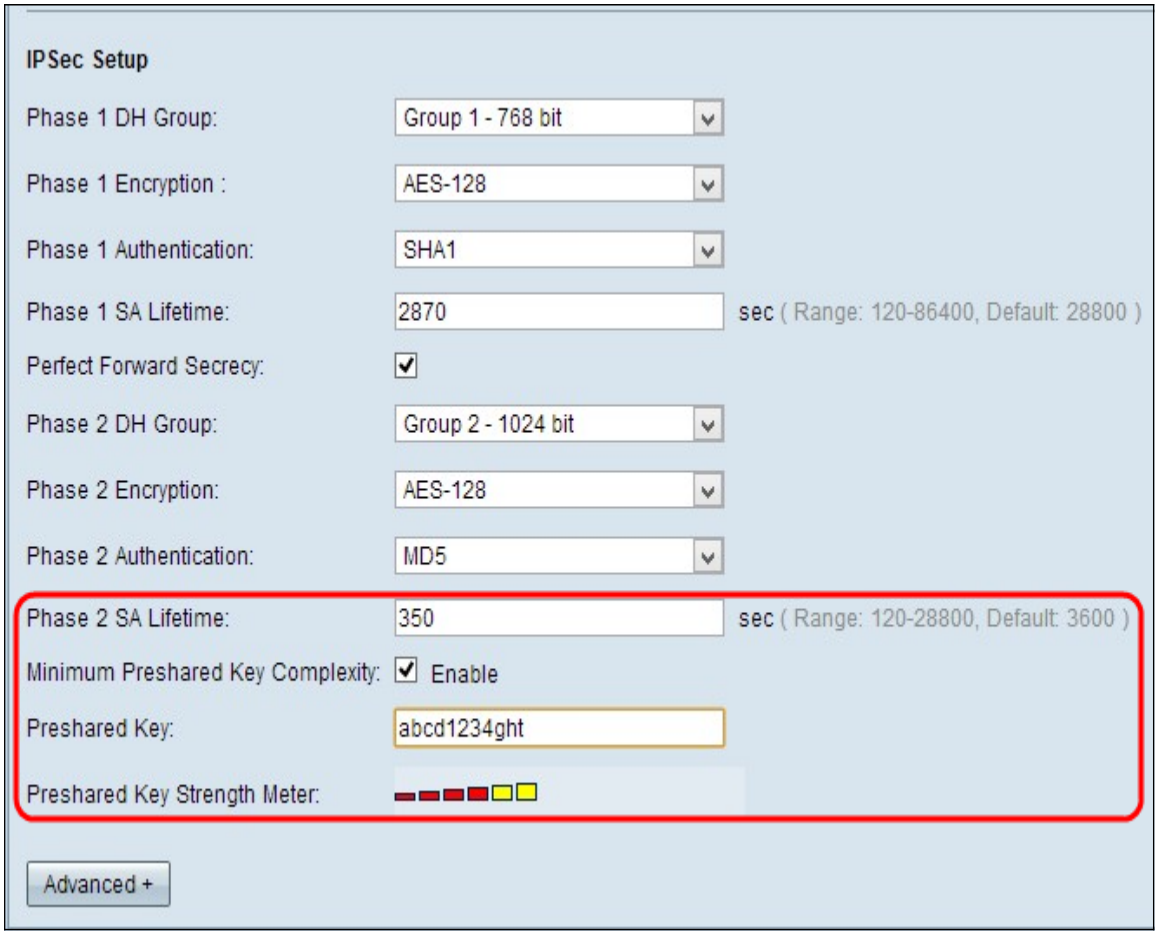
步驟7.從*Phase 2 Encryption* 下拉式清單中選擇適當的階段2加密以加密金鑰。建議使用AES-256，因為它是最安全的加密方法。VPN通道的兩端需要使用相同的加密方法。

- DES — 資料加密標準(DES)是56位的，舊加密方法，並不是非常安全的加密方法。
- 3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法，通過對資料進行三次加密來增加金鑰大小，比DES具有更高的安全性。
- AES-128 — 進階加密標準(AES)是128位元加密方法，它透過10個週期的重複將純文字轉換為密碼文字。
- AES-192 — 進階加密標準(AES)是192位元加密方法，透過12個循環重複將純文字轉換為密碼文字。
- AES-256 — 進階加密標準(AES)是256位元加密方法，它透過14個週期重複將純文字轉換為密碼文字。



步驟8.從*Phase 2 Authentication*下拉選單中選擇相應的身份驗證方法。VPN隧道的兩端需要使用相同的身份驗證方法。

- MD5 - Message Digest Algorithm-5(MD5)表示32位十六進位制雜湊函式，通過校驗和計算為資料提供保護，使其免受惡意攻擊。
- SHA1 — 安全雜湊演算法版本1(SHA1)是160位元的雜湊函式，比MD5更安全。
- 空 — 不使用身份驗證方法。



步驟9.在*Phase 2 SA Lifetime欄位中輸入*VPN隧道保持活動狀態的時間量（以秒為單位），在Phase 2 *SA Lifetime欄位中輸入*。 預設時間為3600秒。

步驟10.如果要啟用預共用金鑰的強度計，請選中**Minimum Preshared Key Complexity**覈取方塊。

步驟11.在*Preshared Key*欄位中輸入之前在IKE對等體之間共用的金鑰。最多30個字母數字字元可用作預共用金鑰。VPN隧道的兩端需要使用相同的預共用金鑰。

附註：強烈建議頻繁更改IKE對等體之間的預共用金鑰，以便VPN保持安全。

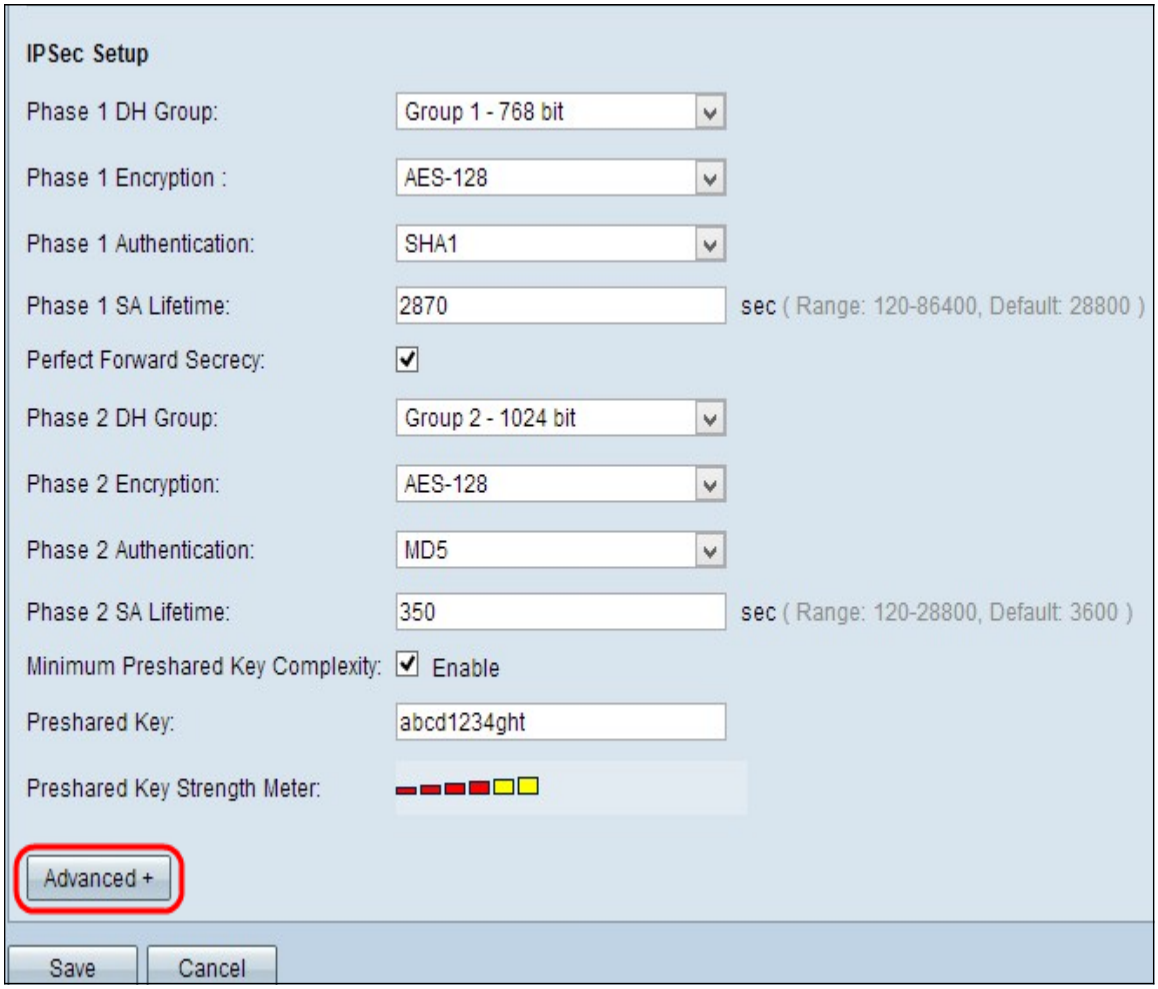
- 預共用金鑰強度計 — 這通過彩色條顯示預共用金鑰的強度。紅色表示弱強度，黃色表示可接受強度，綠色表示強強度。如果在IPSec設定部分的步驟10中選中**Minimum Preshared Key Complexity**覈取方塊，則僅顯示Preshared Key Strength Meter。

附註：如果從*Add a New Tunnel* 部分的*Keying Mode*下拉選單中選擇IKE with Preshared Key，則只有您能夠選擇配置步驟10、步驟11並檢視Preshared Key Strength Meter。

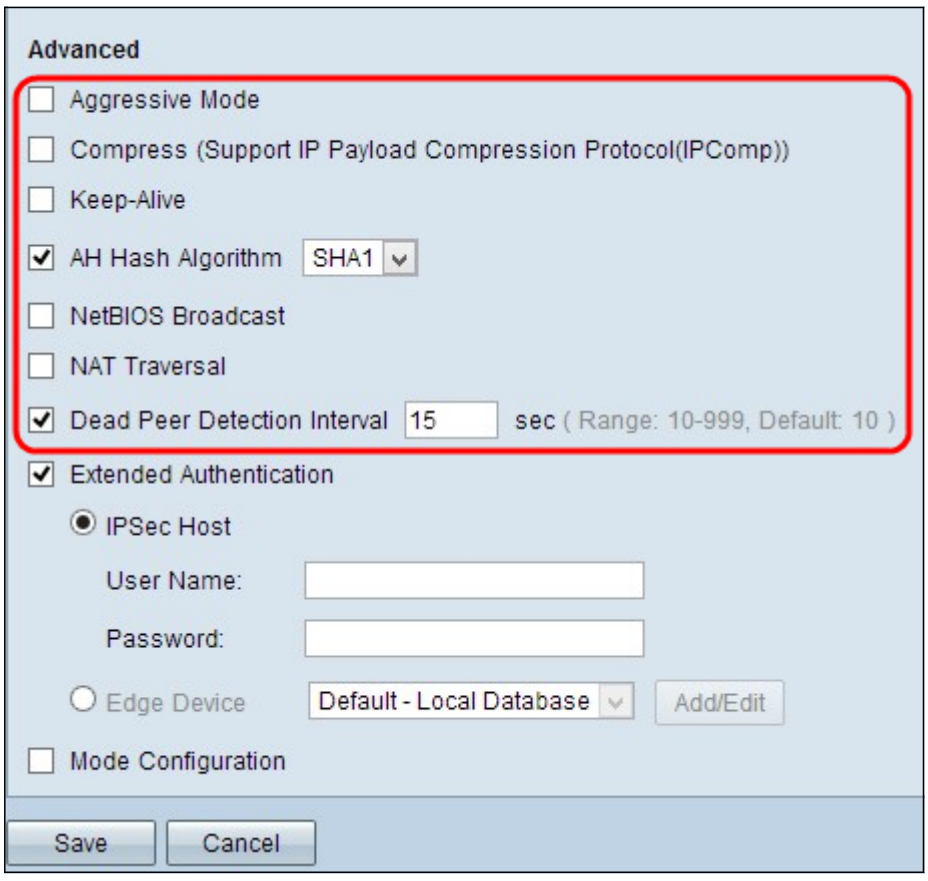
步驟12.如果要儲存目前所做的設定，請向下滾動並按一下**Save**以儲存設定。

使用預共用金鑰的IKE或使用證書的IKE進行高級設定

高級設定只能用於具有預共用金鑰的IKE和具有證書金鑰的IKE。手動金鑰設定沒有任何高級設定。



步驟1.按一下**Advanced**獲取預共用金鑰的IKE的高級設定。



步驟2.如果網路速度低，請勾選**Aggressive Mode**覈取方塊。在SA連線期間，它以明文形式交

換隧道端點的ID，這要求交換時間較短，但安全性較低。

步驟3.如果要壓縮IP資料包的大小，請勾選**Compress(Support IP Payload Compression Protocol(IPComp))**覈取方塊。IPComp是一種IP壓縮協定，用於壓縮IP資料包的大小，如果網路速度低且使用者希望快速傳輸資料而不丟失慢速網路。

步驟4.如果您始終希望VPN隧道的連線保持活動狀態，請選中**Keep-Alive**覈取方塊。它有助於在任何連線變為非活動狀態時立即重新建立連線。

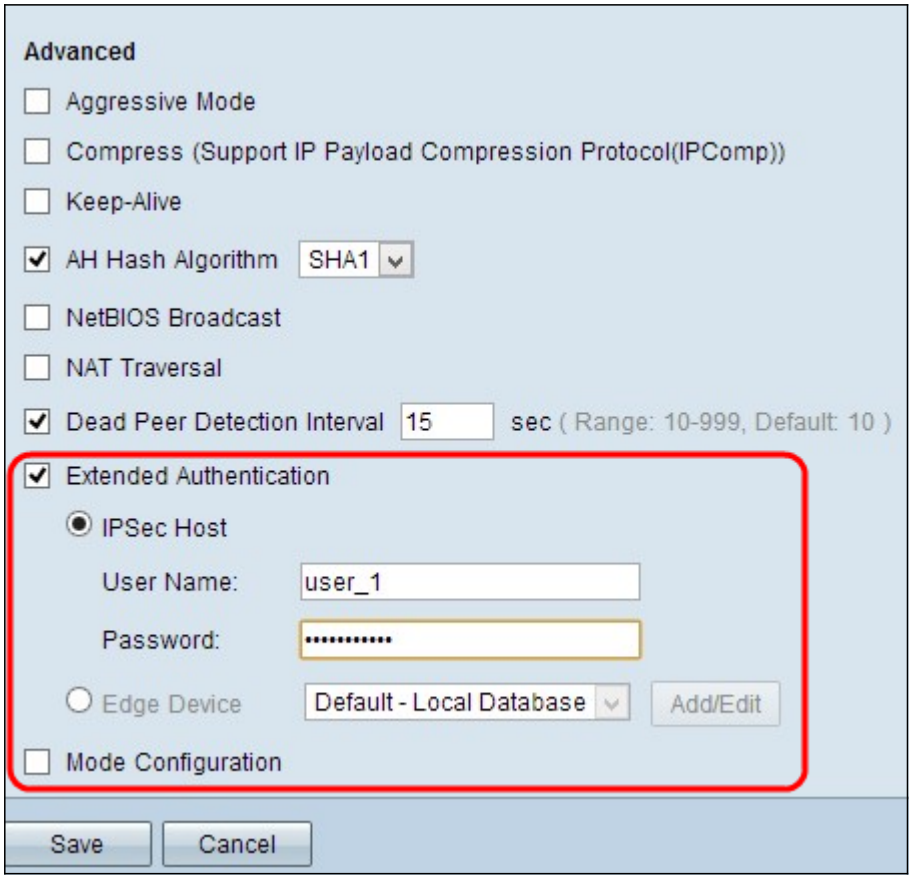
步驟5.如果要驗證驗證標頭(AH)，請選中**AH Hash Algorithm**覈取方塊。AH為資料來源提供身份驗證，通過校驗和資料完整性檢查，並將保護擴展到IP報頭。通道的兩端應使用相同的演算法。

- MD5 - Message Digest Algorithm-5(MD5)表示128位十六進位制雜湊函式，通過校驗和計算為資料提供保護，使其免受惡意攻擊。
- SHA1 — 安全雜湊演算法版本1(SHA1)是160位元的雜湊函式，比MD5更安全。

步驟6.如果要允許不可路由的流量通過VPN隧道，請檢查**NetBIOS廣播**。預設設定為未選中。NetBIOS用於通過一些軟體應用程式和Windows功能（如Network Neighborhood）檢測網路中的網路資源（如印表機、電腦等）。

步驟7.如果要通過公共IP地址從專用LAN訪問Internet，請選中**NAT穿越**覈取方塊。NAT遍歷用於將內部系統的私有IP地址顯示為公有IP地址，以保護私有IP地址免受任何惡意攻擊或發現。

步驟8.檢查**Dead Peer Detection Interval**，通過呼叫或ACK定期檢查VPN隧道的活躍度。如果選中此覈取方塊，請輸入所需的hello消息的持續時間或時間間隔。



步驟9.檢查**Extended Authentication**，為VPN連線提供更多安全性和身份驗證。點選適當的單選按鈕以擴展VPN連線的身份驗證。

- IPSec主機 — 通過IPSec主機的擴展身份驗證。如果選擇此選項，請在User Name欄位中輸入IPSec主機的使用者名稱，並在Password欄位中輸入密碼。
- 邊緣裝置 — 通過邊緣裝置的擴展身份驗證。如果選擇此選項，請從下拉選單中選擇包含邊緣裝置的資料庫。如果要新增或編輯資料庫，請按一下**新增/編輯**。

附註：要詳細瞭解如何新增或編輯本地資料庫，請參閱*RV320路由器上的使用者和域管理配置*。

步驟10 。檢查**模式配置**，為傳入隧道請求方提供IP地址。

附註：第9步到第11步可用於隧道VPN的IKE預共用金鑰模式。

步驟11.按一下**Save**以儲存設定。

結論

現在，您已瞭解在RV32x系列VPN路由器上配置單個客戶端到網關VPN的步驟

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