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

目標

虛擬專用網路(VPN)是一種專用網路，用於通過公共網路虛擬連線遠端使用者的裝置以提供安全性。VPN的型別之一是客戶端到網關VPN。通過客戶端到網關，您可以遠端連線公司位於不同地理區域的不同分支機構，以更安全地在這些區域之間傳輸和接收資料。組VPN可簡化配置VPN，因為它無需為每個使用者配置VPN。RV32x VPN路由器系列最多可以支援兩個VPN組。

本文檔的目的是解釋如何在RV32x系列VPN路由器上配置組客戶端到網關VPN。

適用裝置

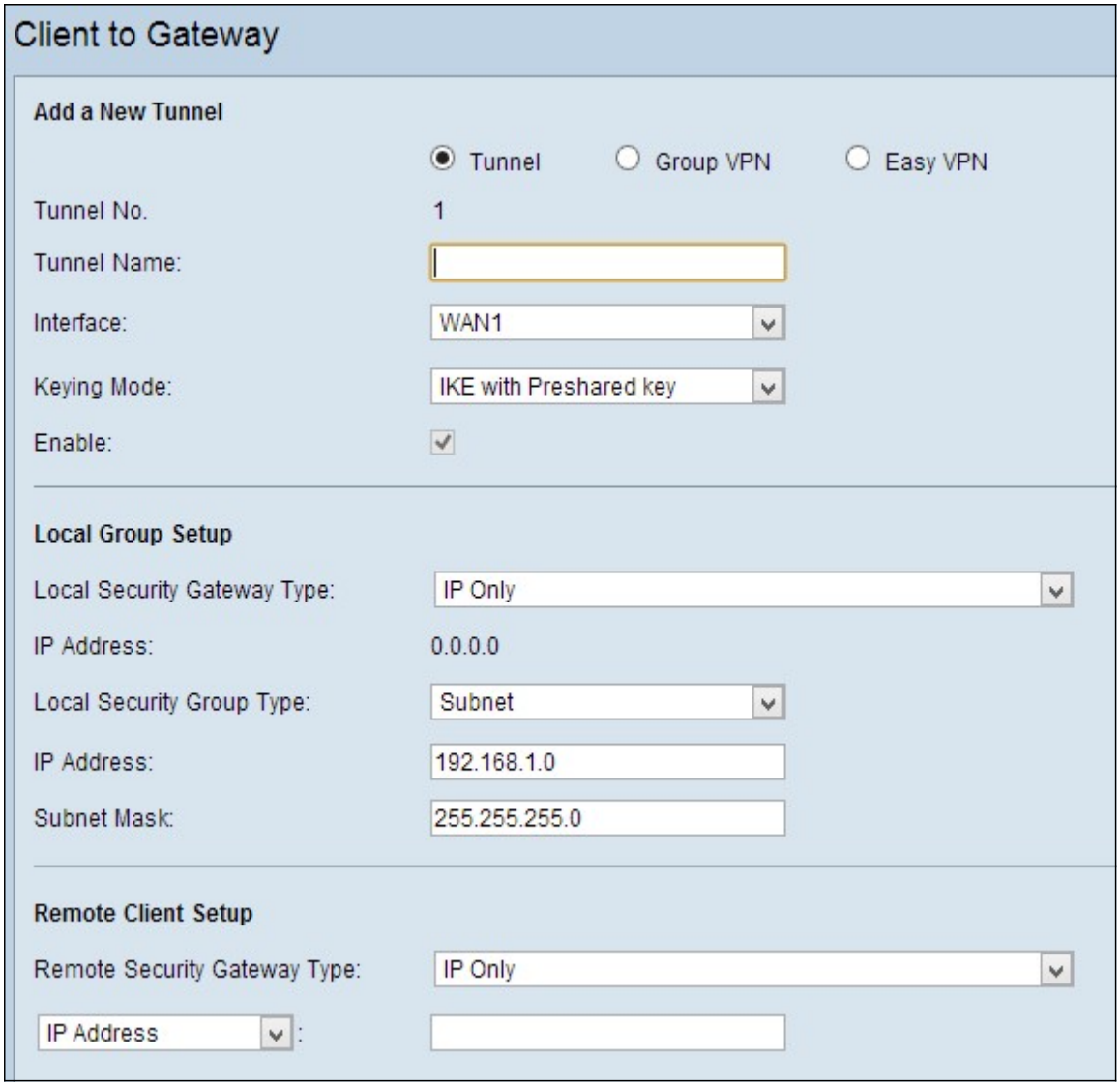
·RV320 Dual WAN VPN路由器
· RV325 Gigabit Dual WAN VPN路由器

軟體版本

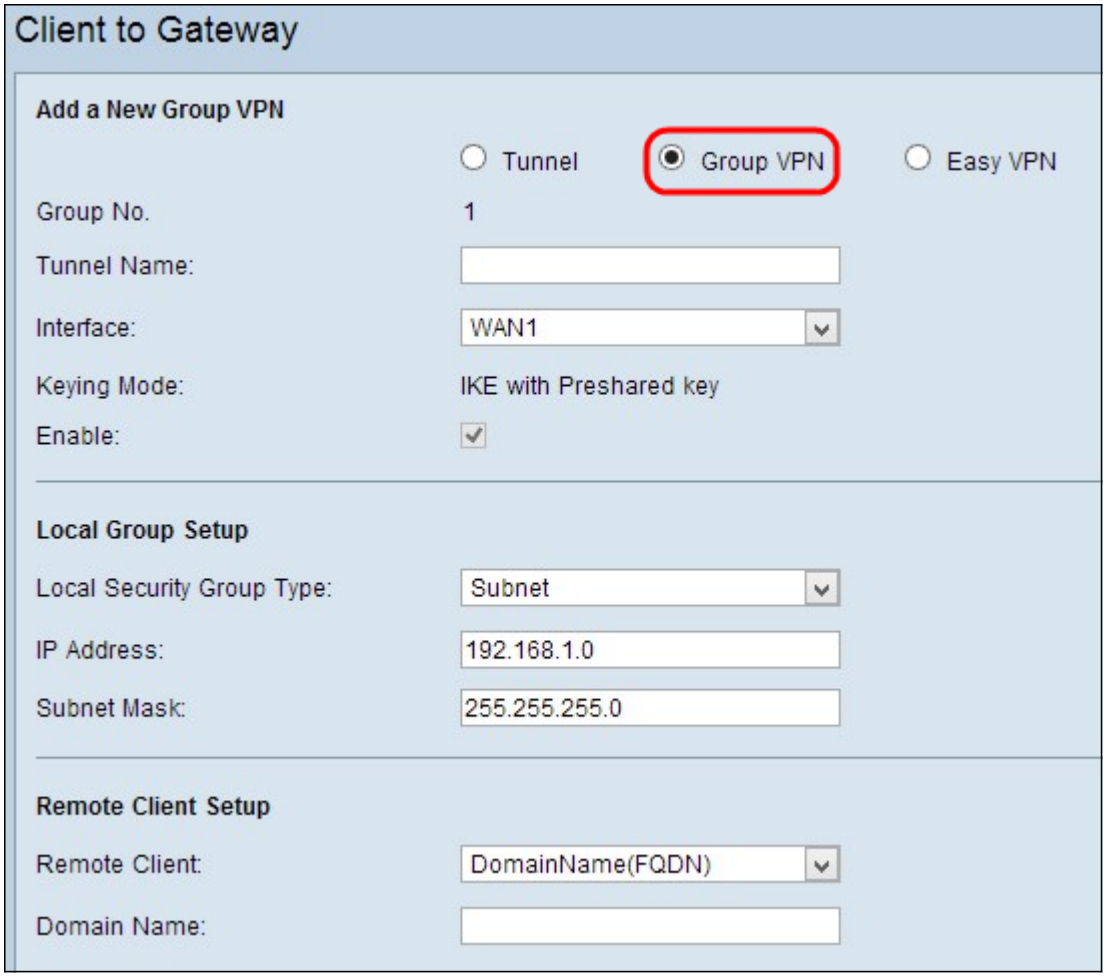
·v1.1.0.09

配置組客戶端到網關VPN

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

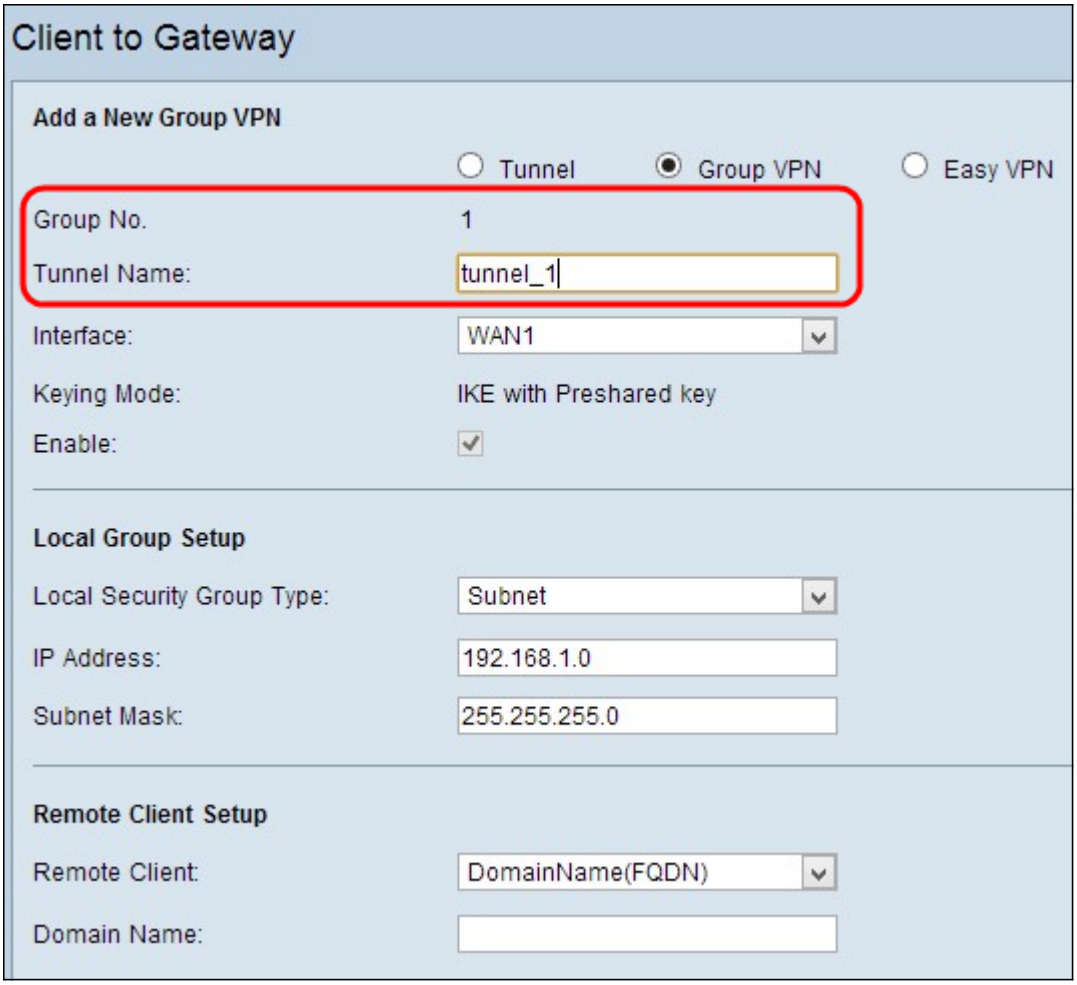


步驟2.按一下**Group VPN**單選按鈕新增組客戶端到網關VPN。



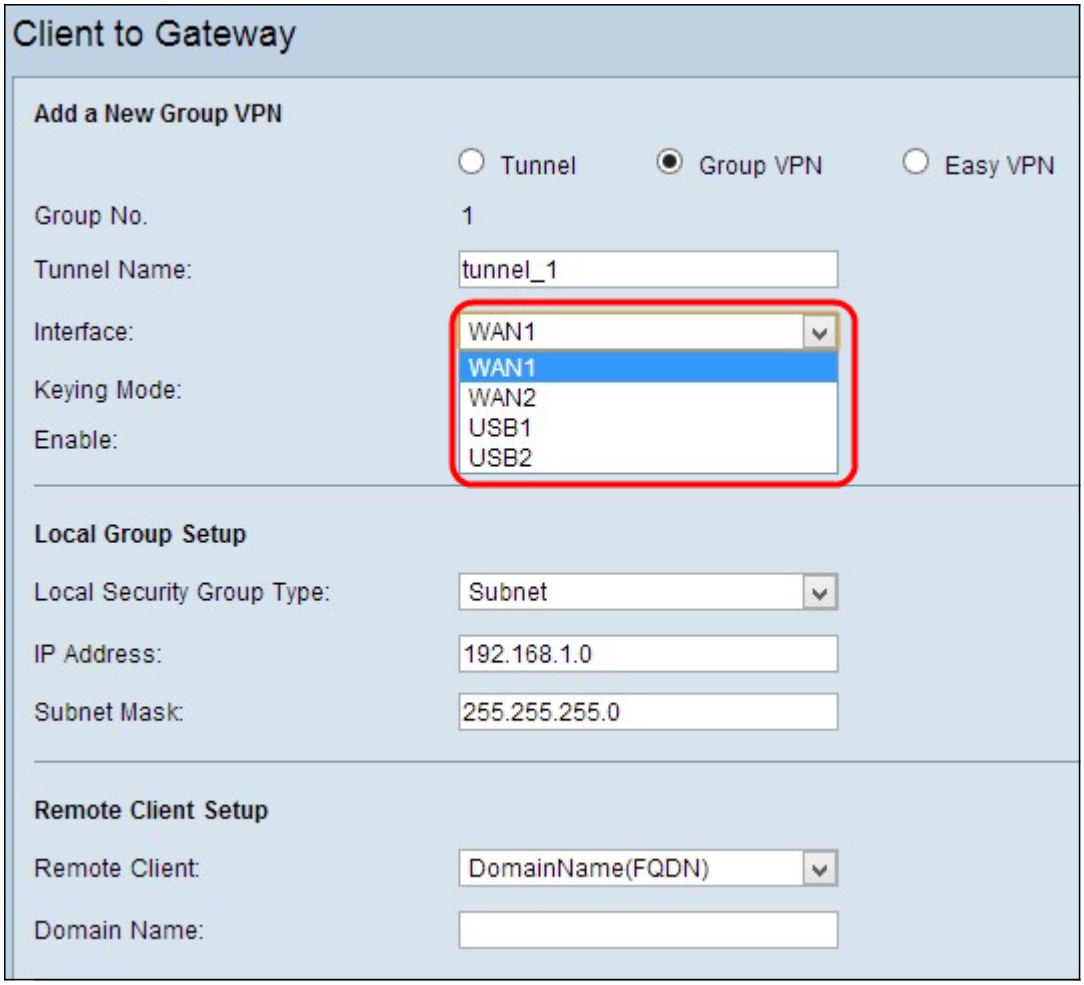
新增新隧道

步驟1.在*Tunnel Name*欄位中輸入隧道的名稱。

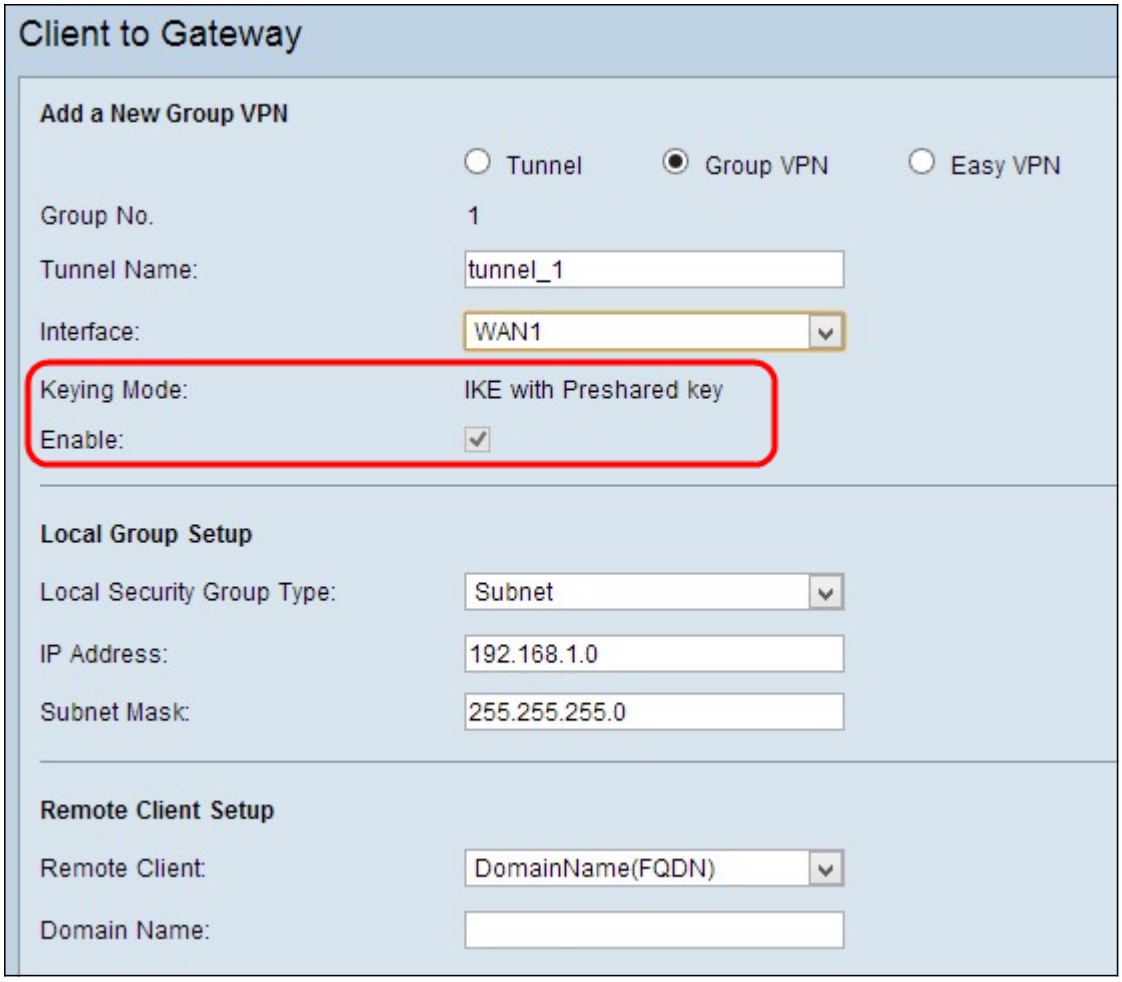


附註：組編號 — 表示組的編號。這是一個自動生成的欄位。

步驟2.從*Interface*下拉選單選擇VPN組通過哪個介面與網關連線。



步驟3.選中**Enable** 覈取方塊以啟用網關到網關VPN。預設情況下，該選項處於啟用狀態。

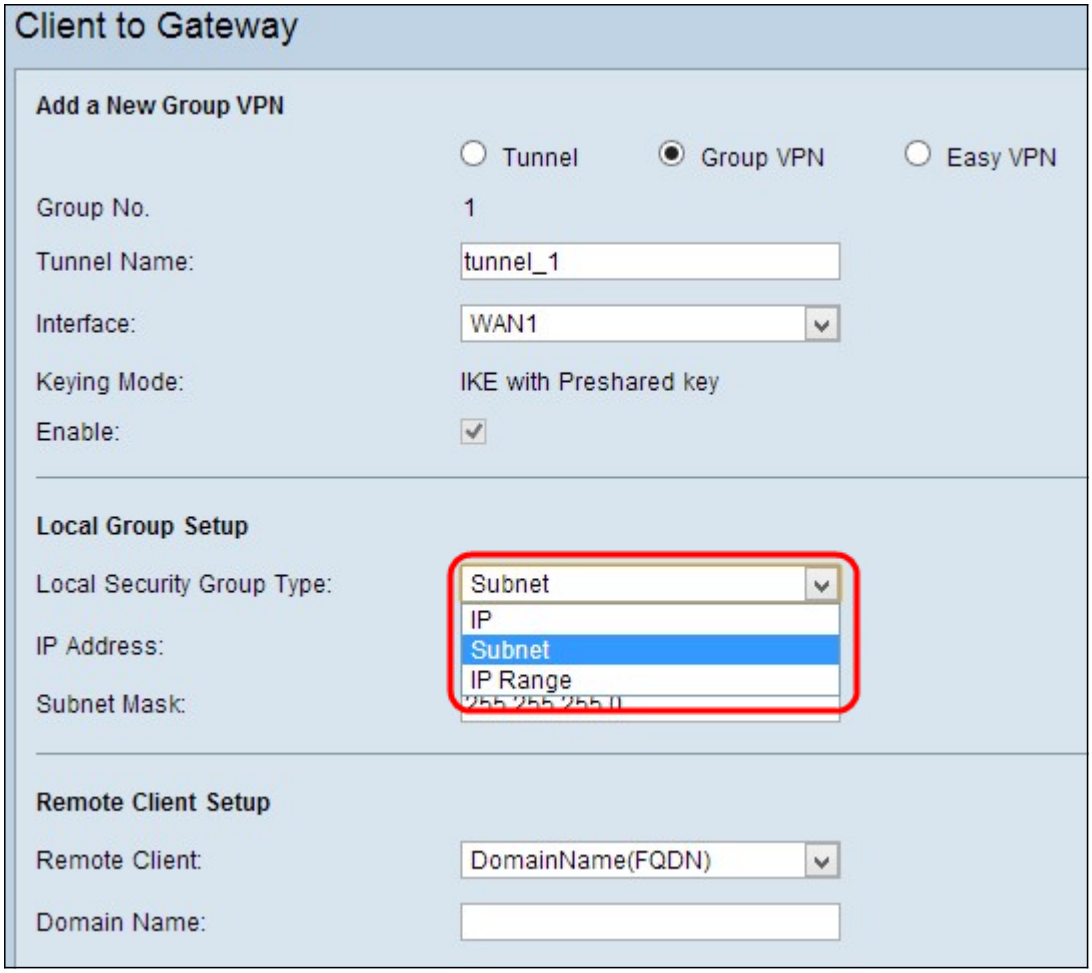


附註：Keying Mode — 顯示使用的身份驗證模式。具有預共用金鑰的IKE是唯一的選項，這意味著網際網路金鑰交換(IKE)協定用於自動生成和交換預共用金鑰，以建立隧道的認證通訊。

步驟4.要儲存您到目前為止的設定並將其餘設定保留為預設值，請向下滾動並按一下**Save**儲存設定。

本地組設定

步驟1.從*Local Security Group Type*下拉選單中選擇可訪問VPN隧道的相應本地LAN使用者或使用者組。預設值為Subnet。



可用選項定義如下：

·IP — 只有一台特定LAN裝置可以訪問隧道。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。

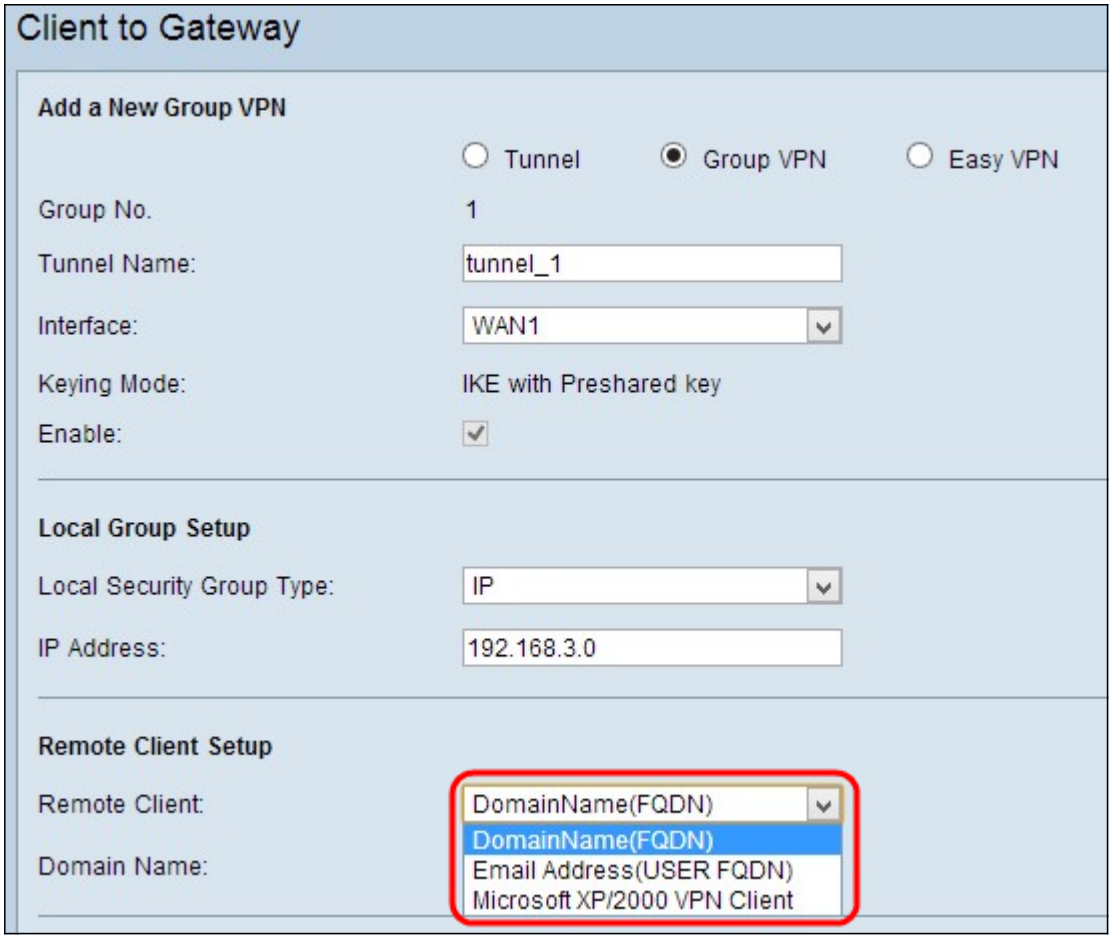
·子網 — 特定子網上的所有LAN裝置都可以訪問隧道。如果選擇此選項，請在*IP地址*和子網掩碼欄位中分別輸入LAN裝置的IP地址和子網掩碼。預設掩碼為255.255.255.0。

·IP範圍 — 一系列LAN裝置可以訪問隧道。如果選擇此選項，請在*起始IP*和*結束IP*欄位中分別輸入範圍的第一個和最後一個IP地址。預設範圍是從192.168.1.0到192.168.1.254。

步驟2.要儲存您到目前為止的設定並將其餘設定保留為預設值，請向下滾動並按一下**Save**儲存設定。

遠端客戶端設定

步驟1.從*遠端安全組型別*下拉選單中選擇可以訪問VPN隧道的適當遠端LAN使用者或使用者組。



可用選項定義如下：

·域名(FQDN)身份驗證 — 可以通過已註冊的域訪問隧道。如果選擇此選項，請在「域名」欄位中輸入已註冊*域的*名稱。

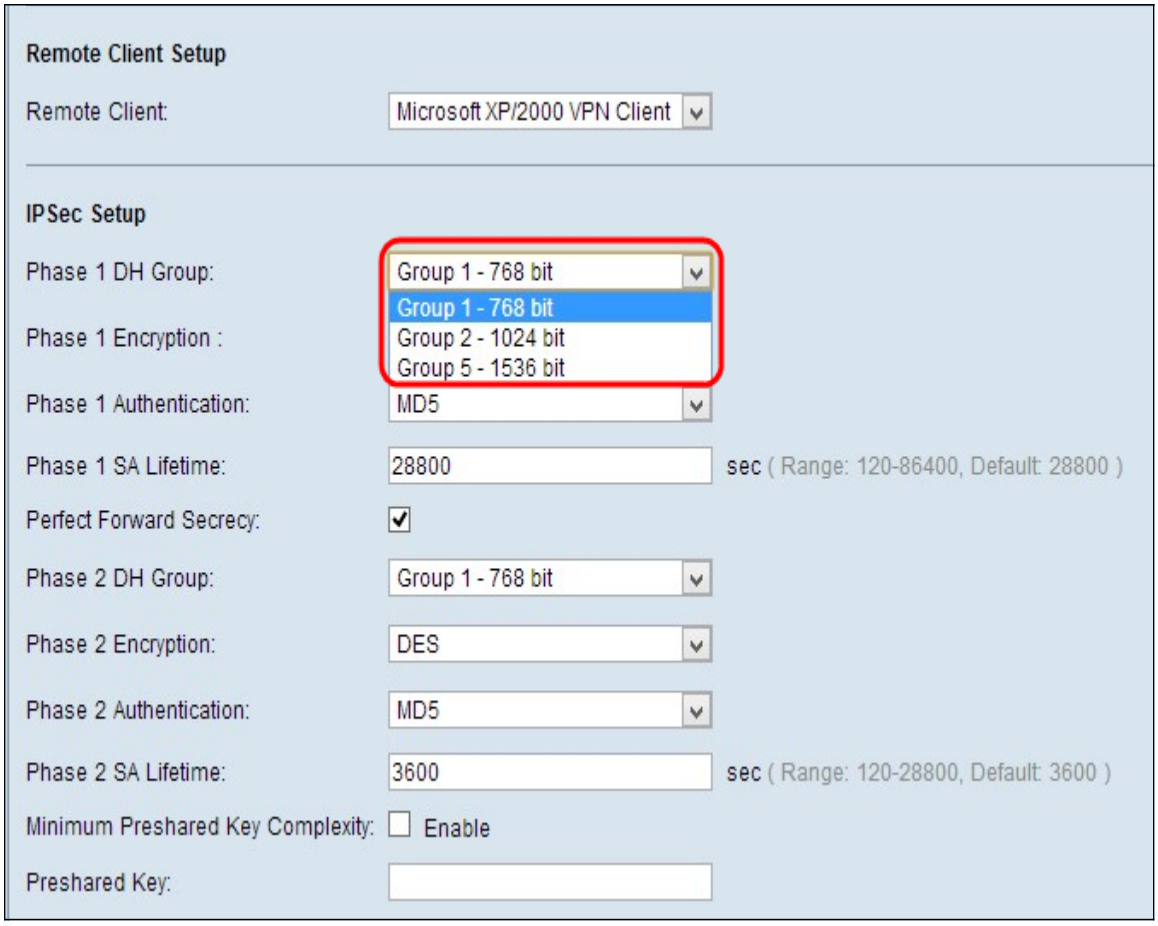
·電子郵件地址（使用者FQDN）身份驗證 — 可以通過電子郵件地址訪問隧道。如果選擇此選項，請在*Email Address*欄位中輸入電子郵*件地址*。

·Microsoft XP/2000 VPN客戶端 — 可通過客戶端軟體（內建Microsoft XP或2000 VPN客戶端軟體）訪問隧道。

步驟2.要儲存您到目前為止的設定並將其餘設定保留為預設值，請向下滾動並按一下**Save**儲存設定。

IPSec設定

步驟1.從*Phase 1 DH Group*下拉式清單中選擇適當的Diffie-Hellman(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是一種加密金鑰交換協定，用於第1階段連線以共用金鑰來驗證通訊。



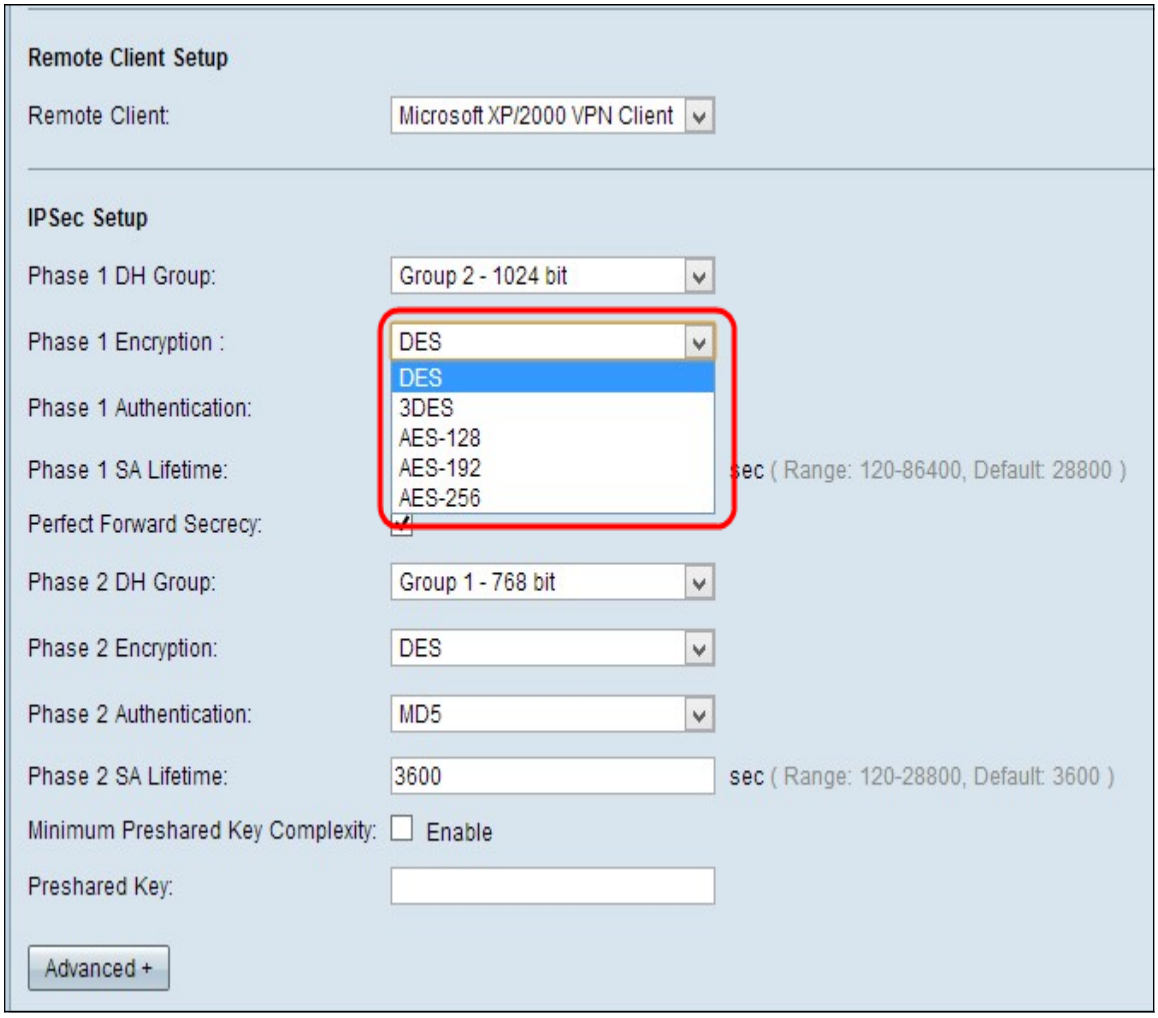
可用選項定義如下：

·組1（768位）— 以最快的速度計算金鑰，但最不安全。

·Group2（1024位）— 計算金鑰的速度較慢，但比Group1更安全。

·組5（1536位）— 計算金鑰最慢，但最安全。

步驟2.從*Phase 1 Encryption* 下拉式清單中選擇適當的加密方法來加密金鑰。建議使用AES-128來實現其高安全性和快速效能。VPN隧道的兩端需要使用相同的加密方法。



可用選項定義如下：

·DES — 資料加密標準(DES)是一種56位舊加密方法，它不是非常安全的加密方法，但為了向後相容，可能需要這種加密方法。

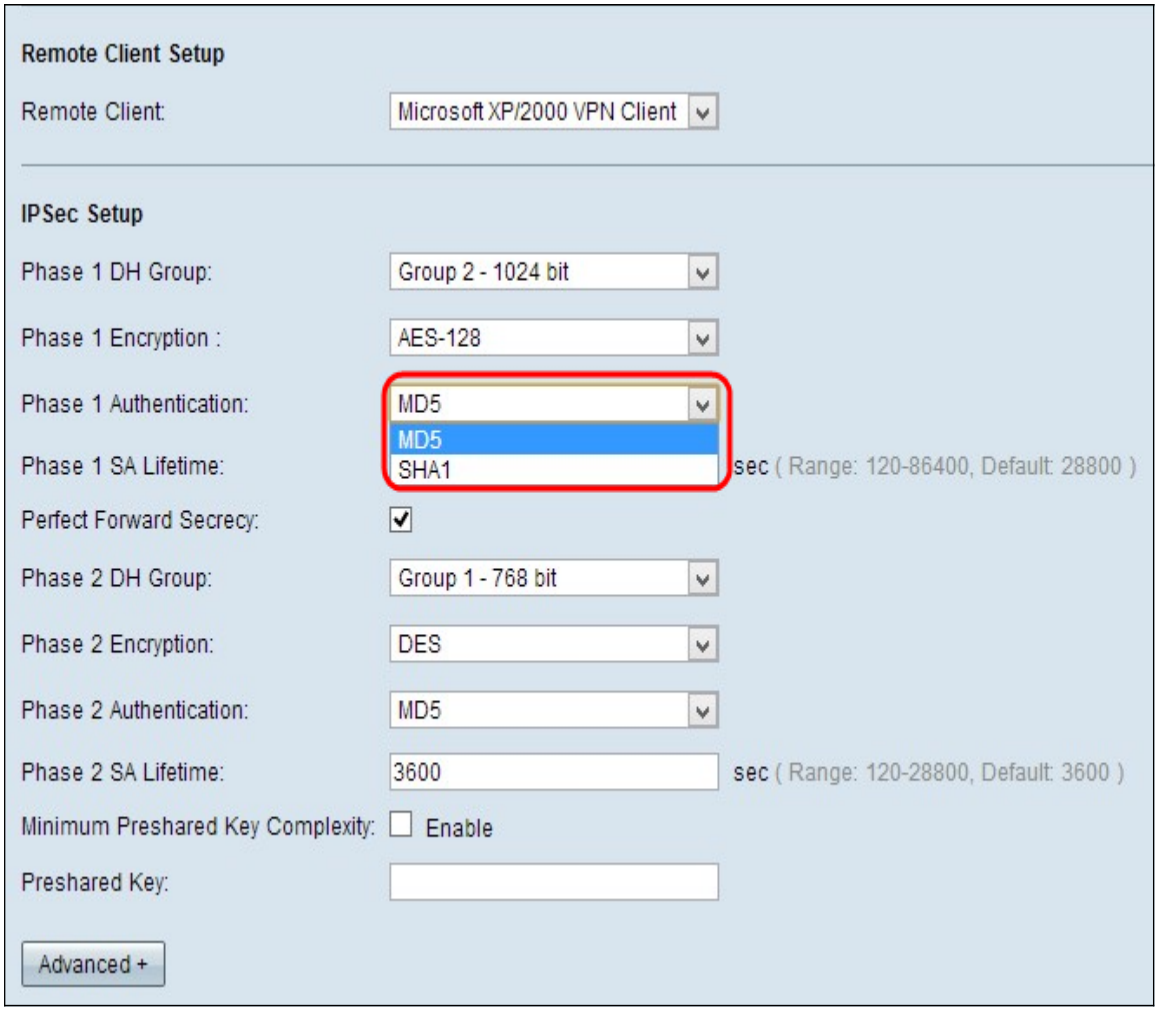
·3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法，用於增加金鑰大小，因為它將資料加密三次。這比DES提供了更高的安全性，但比AES提供的安全性更低。

·AES-128 — 具有128位金鑰的高級加密標準(AES-128)使用128位金鑰進行AES加密。AES比DES更快、更安全。一般來說，AES也比3DES更快和更安全。AES-128比AES-192和AES-256更快，但安全性較低。

·AES-192 — AES-192使用192位金鑰進行AES加密。AES-192比AES-128速度較慢但更安全，比AES-256速度更快但安全性較低。

·AES-256 — AES-256使用256位金鑰進行AES加密。AES-256比AES-128和AES-192慢，但更安全。

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。

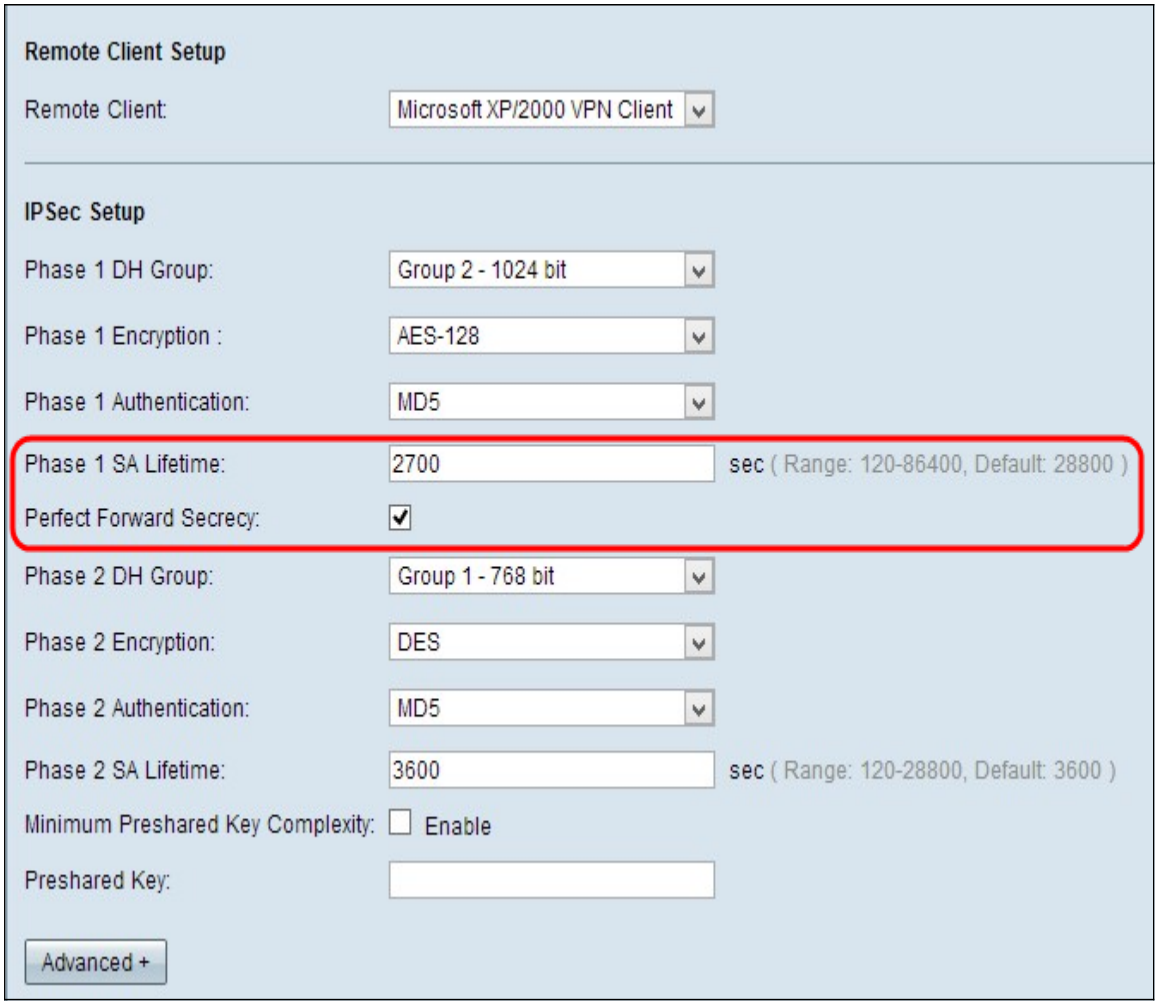


可用選項定義如下：

·MD5 — 消息摘要演算法5(MD5)表示一個128位雜湊函式，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)是一個160位雜湊函式，比MD5更安全。

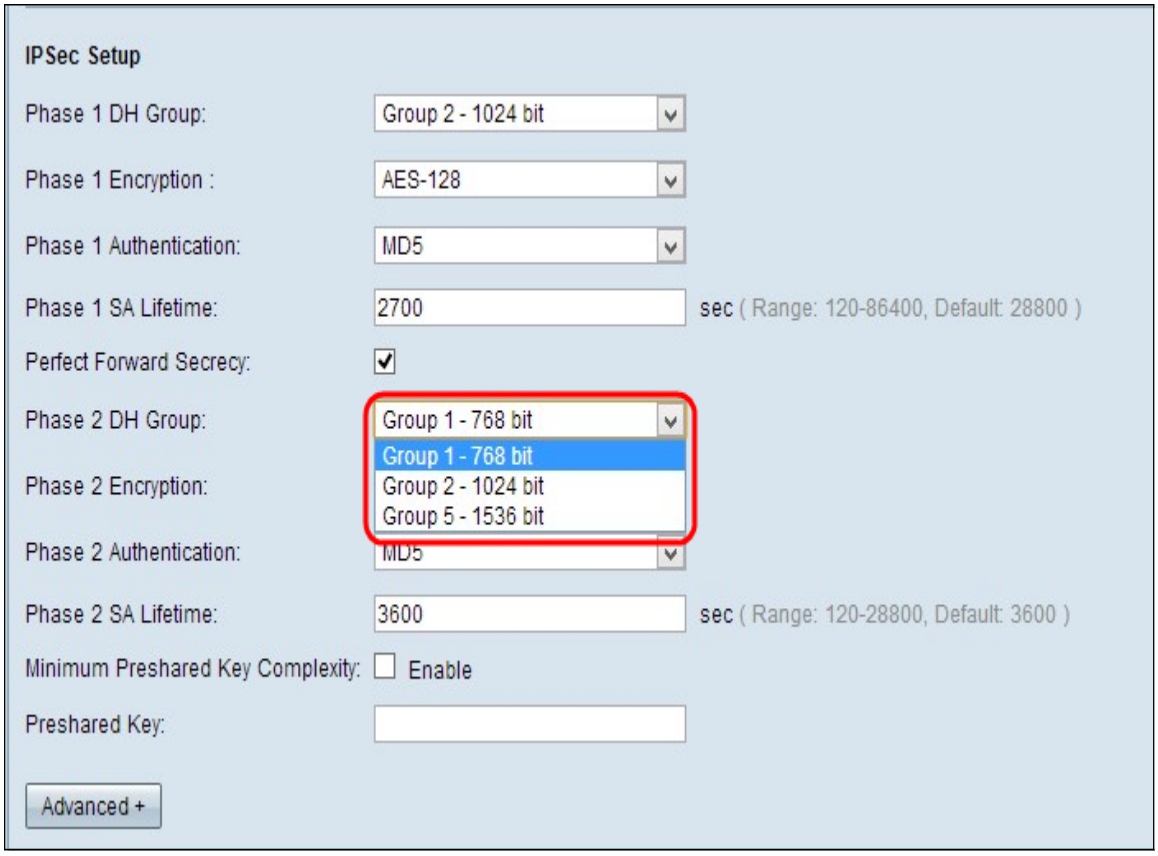
步驟4.在*Phase 1 SA Life Time*欄位中，輸入VPN隧道在第1階段保持活動狀態的時間量（以秒為單位）。預設時間為28,800秒。



步驟5.（可選）要對金鑰提供更多保護，請選中**Perfect Forward Secrecy**覈取方塊。此選項可讓您在任何金鑰受到危害時生成新金鑰。這是推薦的操作，因為它提供了更高的安全性。

注意：如果您在步驟5中取消選中**Perfect Forward Secrecy**，則無需配置階段2 DH組。

步驟6.從*Phase 2 DH Group*下拉選單中*選擇適當的DH組。*



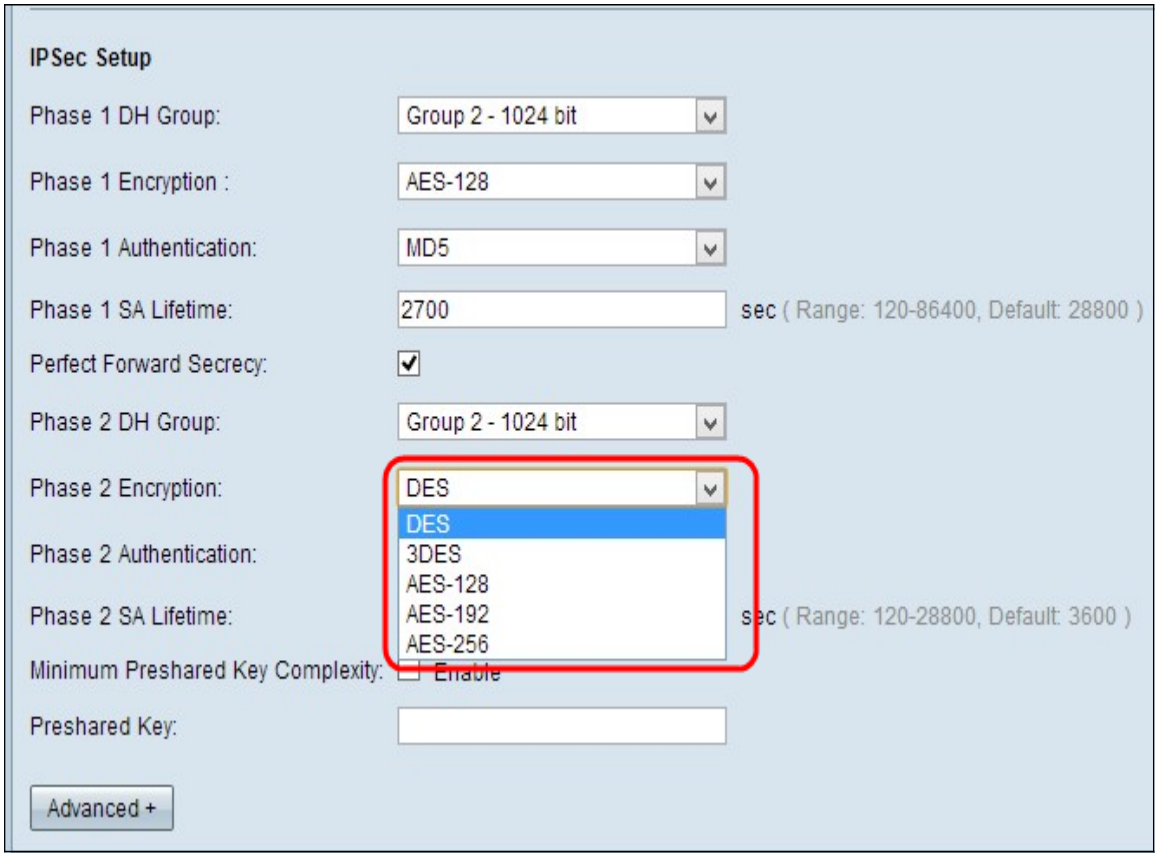
可用選項定義如下：

·組1（768位）— 以最快的速度計算金鑰，但最不安全。

·Group2（1024位）— 計算金鑰的速度較慢，但比Group1更安全。

·組5（1536位）— 計算金鑰最慢，但最安全。

步驟2.從*Phase 1 Encryption* 下拉式清單中選擇適當的加密方法來加密金鑰。建議使用AES-128來實現其高安全性和快速效能。VPN隧道的兩端需要使用相同的加密方法。



可用選項定義如下：

·DES — 資料加密標準(DES)是一種56位舊加密方法，它不是非常安全的加密方法，但為了向後相容，可能需要這種加密方法。

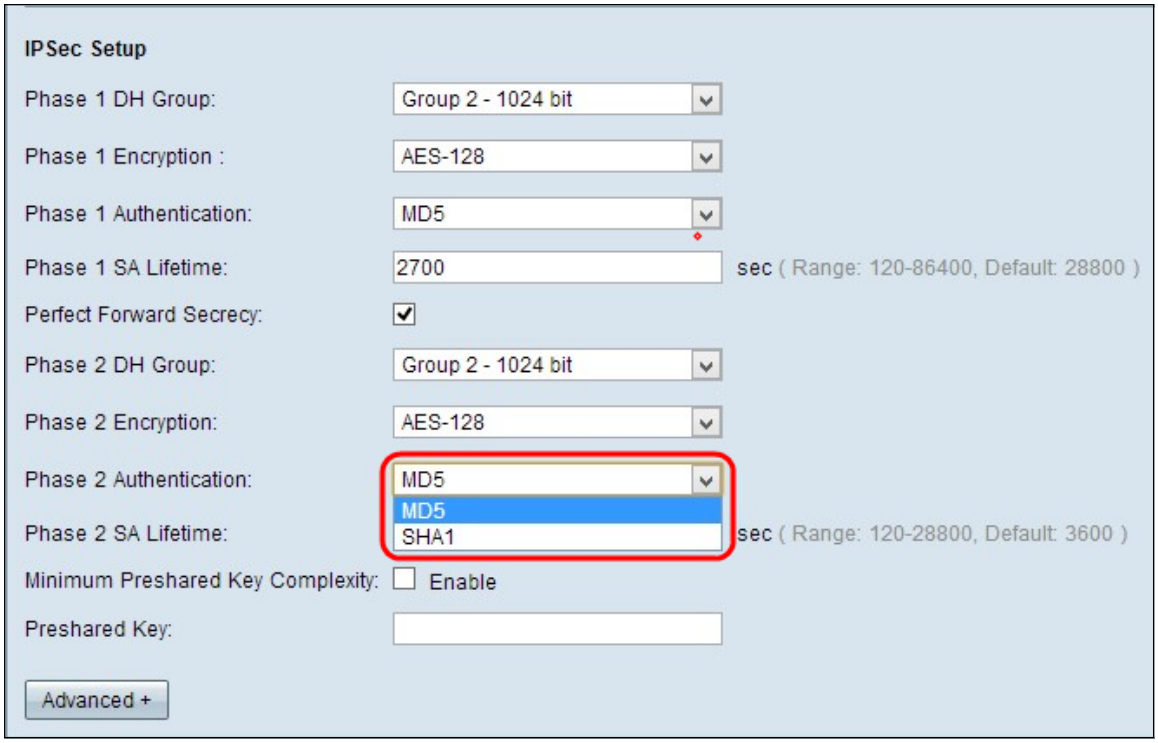
·3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法，用於增加金鑰大小，因為它將資料加密三次。這比DES提供了更高的安全性，但比AES提供的安全性更低。

·AES-128 — 具有128位金鑰的高級加密標準(AES-128)使用128位金鑰進行AES加密。AES比DES更快、更安全。一般來說，AES也比3DES更快和更安全。AES-128比AES-192和AES-256更快，但安全性較低。

·AES-192 — AES-192使用192位金鑰進行AES加密。AES-192比AES-128速度較慢但更安全，比AES-256速度更快但安全性較低。

·AES-256 — AES-256使用256位金鑰進行AES加密。AES-256比AES-128和AES-192慢，但更安全。

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。

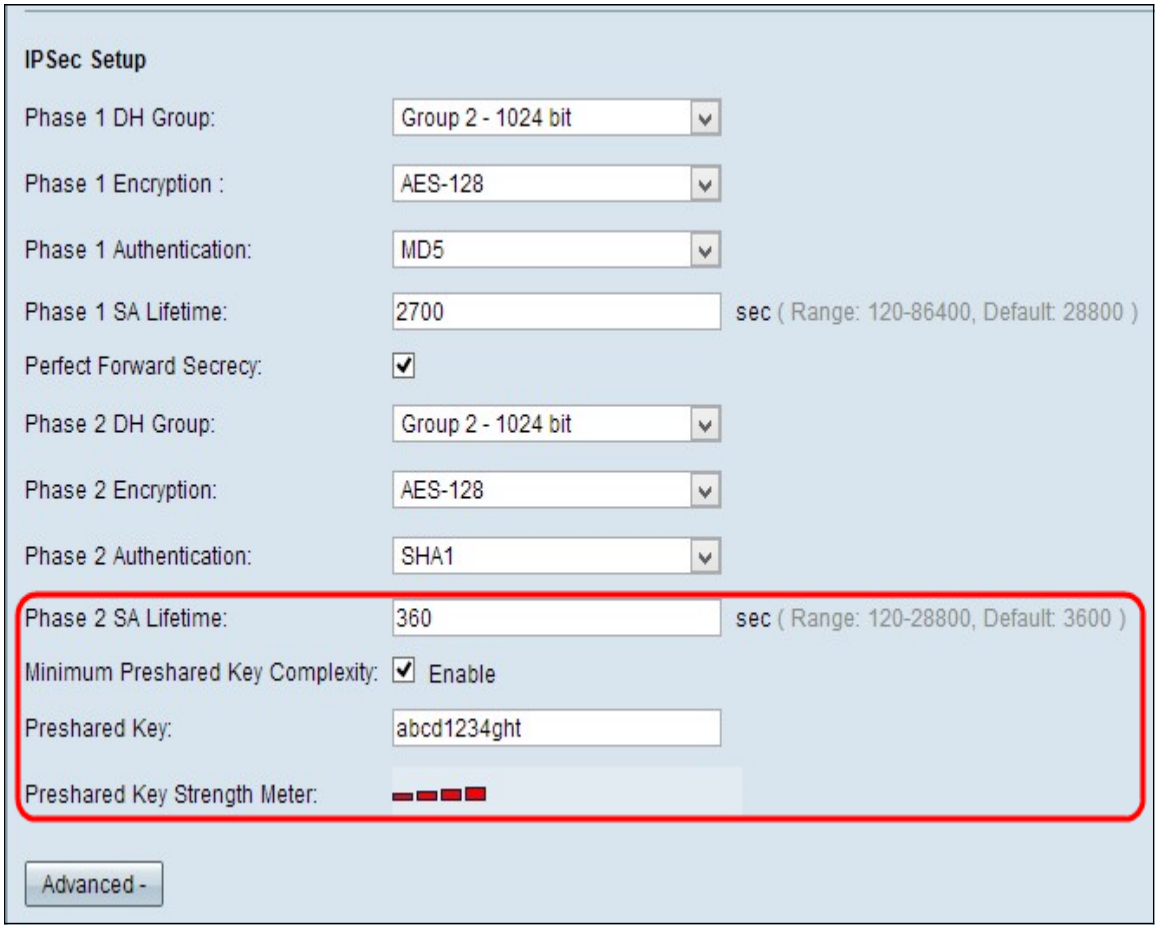


可用選項定義如下：

·MD5 — 消息摘要演算法5(MD5)代表128位雜湊函式，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)是一個160位雜湊函式，比MD5更安全。

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



步驟10。（可選）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。

附註：如果選中**最小預共用金鑰複雜性**覈取方塊，*預共用金鑰強度表*將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。

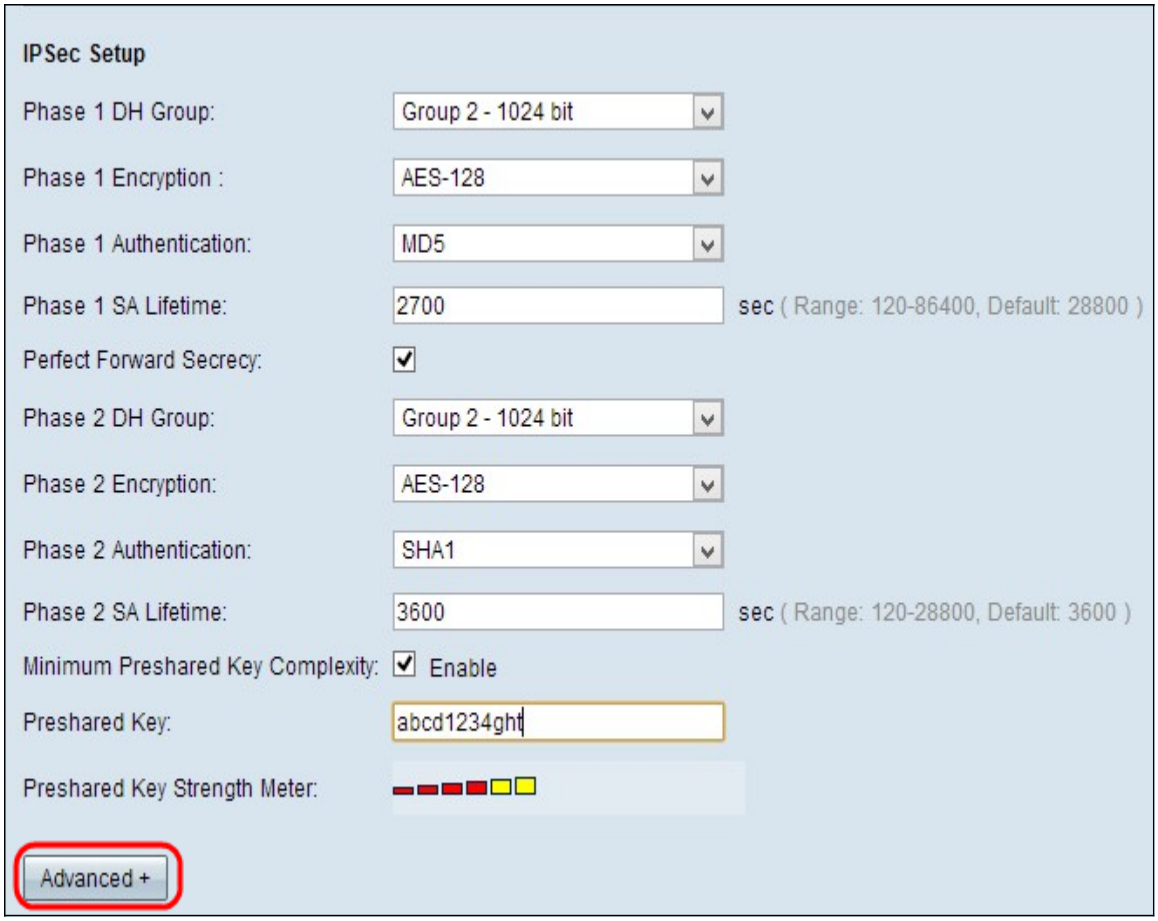
步驟11.在*Preshared Key*欄位中輸入所需的金鑰。最多可將30個十六進位制數用作預共用金鑰。VPN隧道的兩端需要使用相同的預共用金鑰。

附註：強烈建議頻繁更改IKE對等體之間的預共用金鑰，以確保VPN安全。

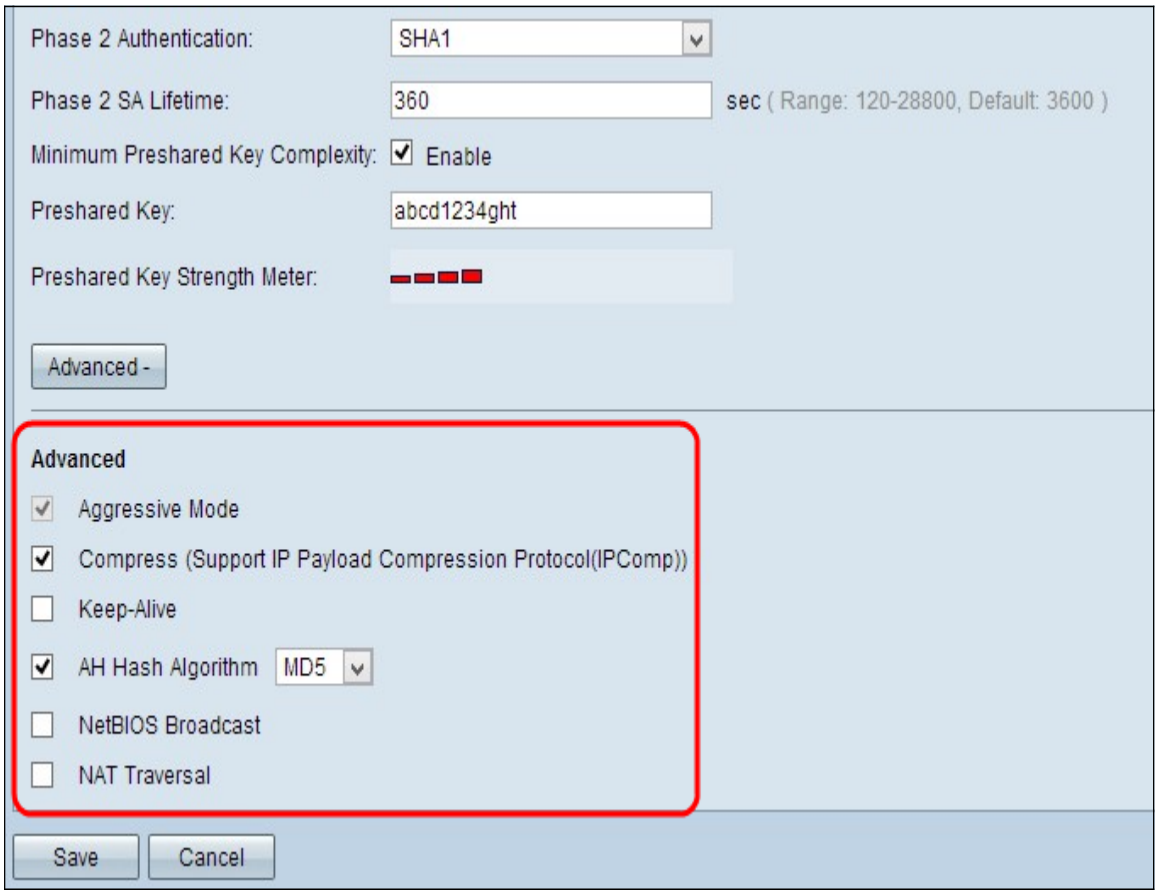
步驟12.要儲存您到目前為止的設定並將其餘設定保留為預設值，請向下滾動並按一下**Save**儲存設定。

高級設定

步驟1。按一下**Advanced** 以設定進階設定。



此時將顯示*Advanced*區域，其中顯示有可用的新欄位。



步驟2.（可選）如果您的網路速度較低，請勾選**Aggressive Mode**覈取方塊。主動模式在SA連線期間以明文形式交換隧道端點的ID，這要求交換的時間較短，但安全性較低。

步驟3.（可選）如果要壓縮IP資料包的大小，請選中**Compress(Support IP Payload Compression Protocol(IPComp))**覈取方塊。IPComp是一種IP壓縮協定，用於在網路速度較低且使用者希望快速傳輸資料而不丟失的情況下壓縮IP資料包的大小。

步驟4.（可選）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。Keep-Alive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.（可選）如果要對資料來源進行身份驗證、通過校驗和確保資料完整性，以及保護擴展到IP報頭，請選中AH雜湊演算法覈取方塊。然後從下拉選單中選擇相應的身份驗證方法。通道的兩端應使用相同的演算法。

可用選項定義如下：

·MD5 — 消息摘要演算法5(MD5)代表128位雜湊函式，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)是一個160位雜湊函式，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，請選中**NetBIOS Broadcast**覈取方塊。預設設定為未選中。NetBIOS用於通過軟體應用程式和Windows功能（如網路鄰居）檢測網路中的網路資源（如印表機、電腦等）。

步驟7.（可選）如果要通過公共IP地址從專用LAN訪問Internet，請選中**NAT Traversal**覈取方塊。NAT遍歷用於使內部系統的私有IP地址顯示為公共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.按一下**Save**以儲存設定。