在RV130和RV130W上配置IPSec VPN伺服器

目標

通過IPSec VPN（虛擬專用網路），您可以建立網際網路上的加密隧道，安全地遠端訪問公司資源。

本文檔的目的是向您展示如何在RV130和RV130W上配置IPSec VPN伺服器。

附註：有關如何在RV130和RV130W上使用Shrew Soft VPN Client配置IPSec VPN伺服器的資訊，請參閱*在RV130和RV130W上使用Shrew Soft VPN Client with IPSec VPN Server*。

適用裝置

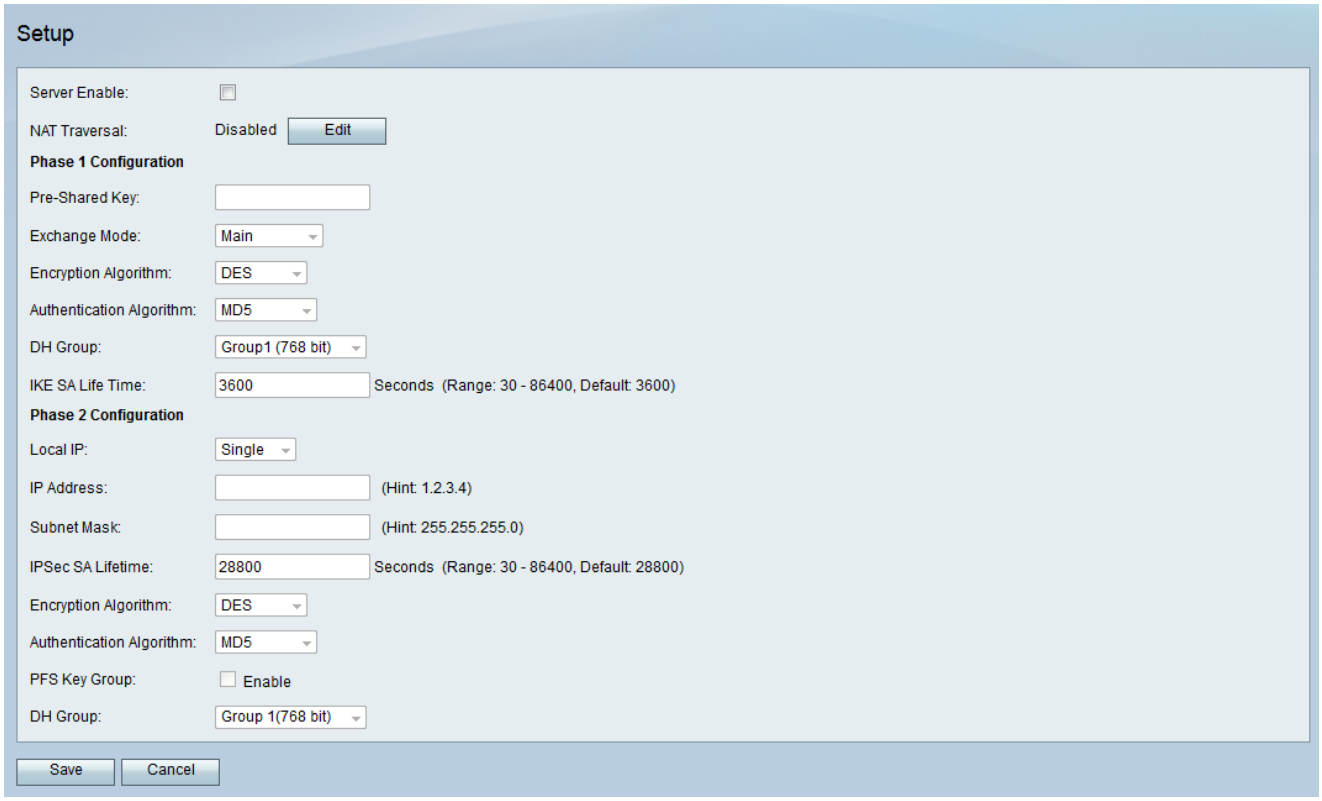
·RV130W無線 — N VPN防火牆
· RV130 VPN防火牆

軟體版本

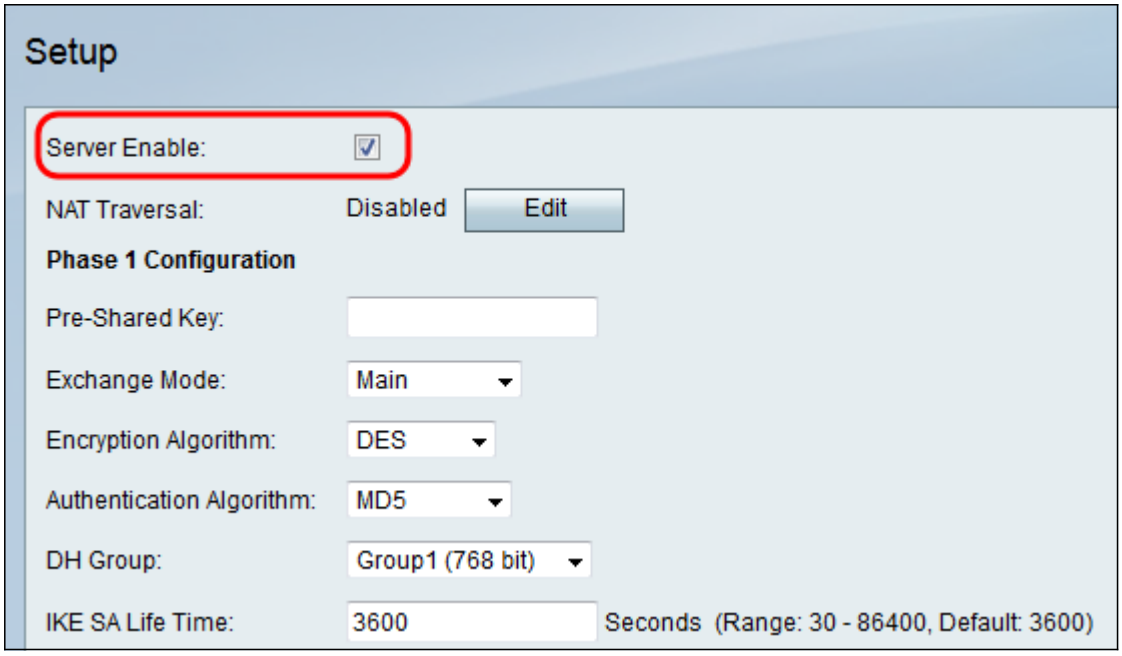
·v1.0.1.3

設定IPSec VPN伺服器

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

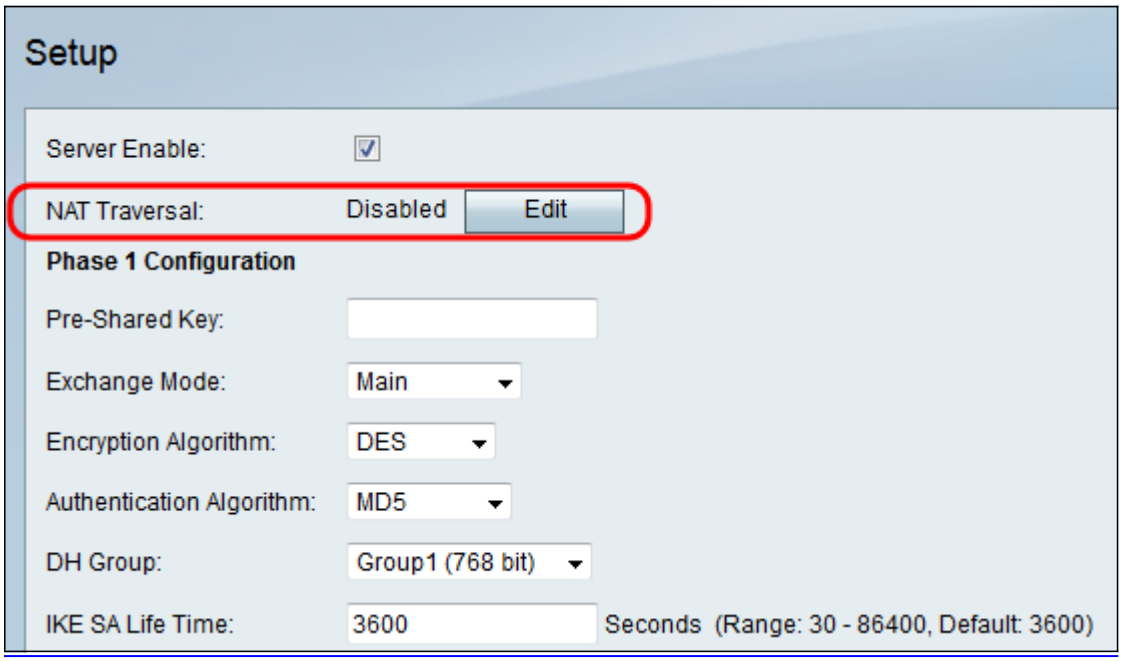


步驟2.勾選**Server Enable**覈取方塊以啟用證書。

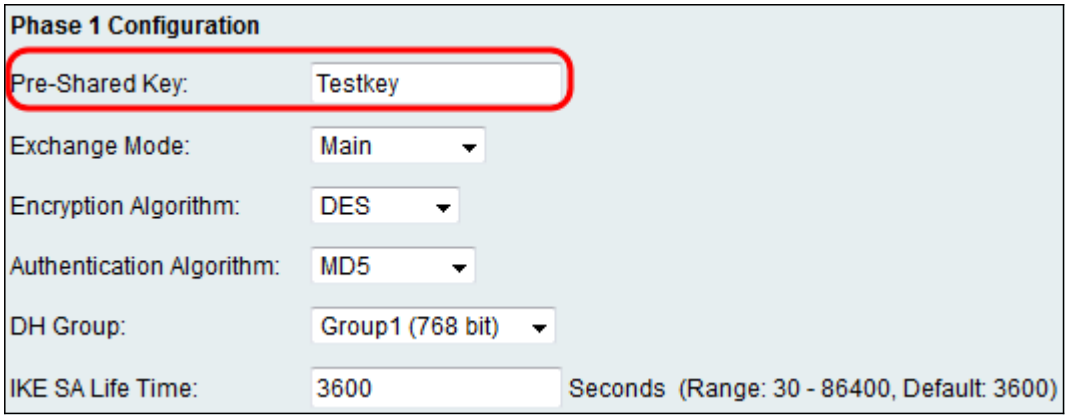


步驟3.（可選）如果您的VPN路由器或VPN客戶端位於NAT網關後面，請按一下**Edit**配置NAT穿越。否則，請禁用NAT穿越。

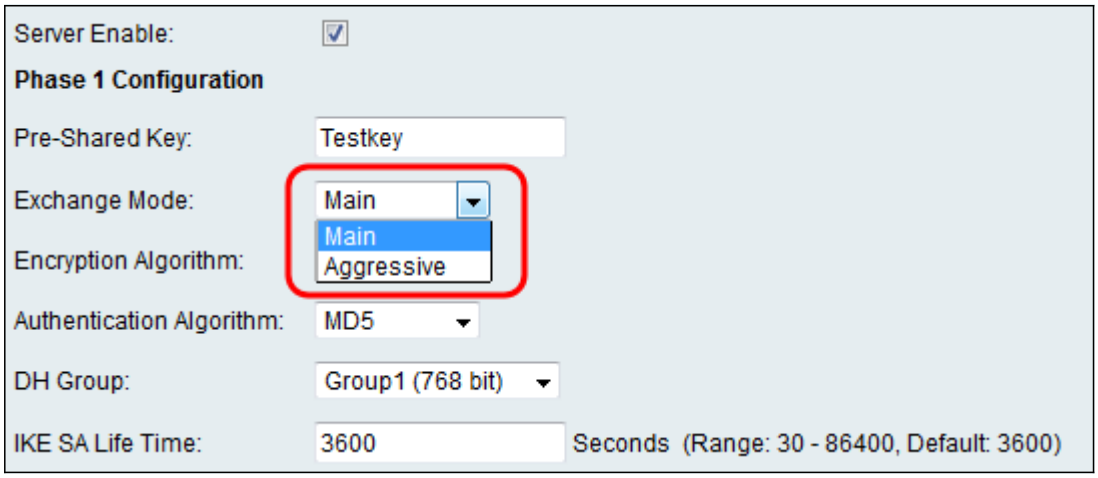
附註：有關如何配置NAT遍歷設定的詳細資訊，請參閱*RV130和RV130W VPN路由器上的網際網路金鑰交換(IKE)策略設定*。



步驟4.在*Pre-Shared Key*欄位中，輸入要在您的裝置和遠端終端之間交換的長度為8到49個字元的金鑰。

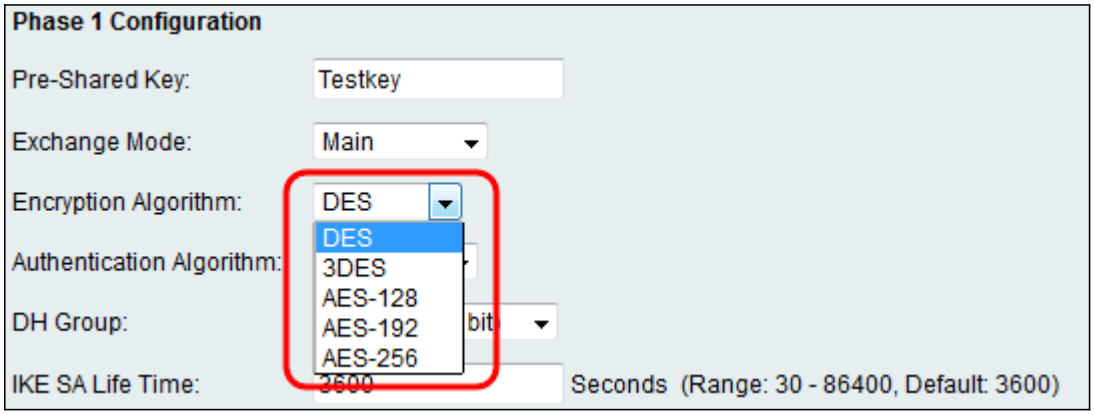


步驟5.從*Exchange Mode*下拉選單中，選擇IPSec VPN連線的模式。**Main**是預設模式。但是如果您的網路速度低，請選擇**Aggressive**模式。



附註：主動模式在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6.從**Encryption Algorithm**下拉選單中，選擇適當的加密方法以加密階段1中的預共用金鑰。建議使用AES-128來實現它的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，它不是很安全，但為了向後相容，可能需要這種加密方法。

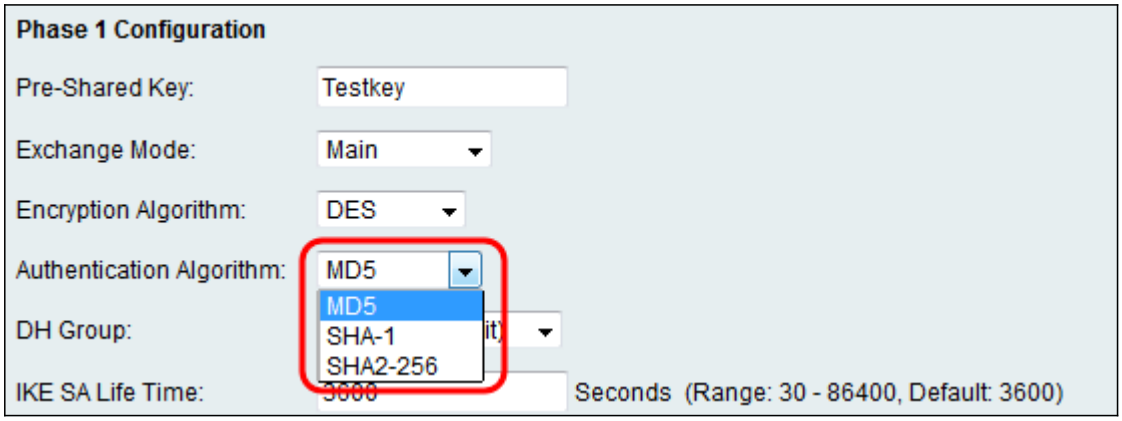
·3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法，用於增加金鑰大小，因為它將資料加密三次。這比DES提供了更高的安全性，但比AES提供的安全性更低。

·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7.從*Authentication Algorithm*下拉選單中，選擇適當的身份驗證方法以確定如何在第1階段驗證封裝安全負載(ESP)協定報頭資料包。VPN隧道需要為連線的兩端使用相同的身份驗證方法。



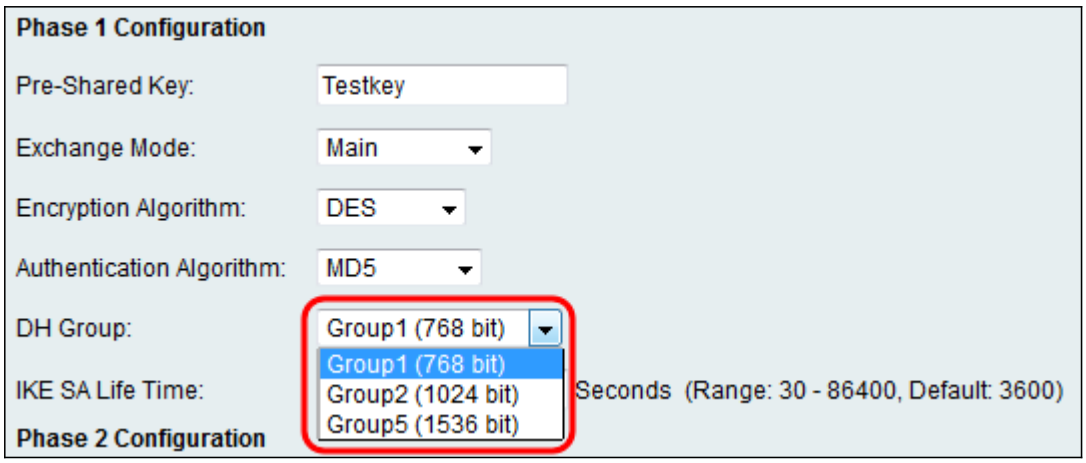
可用選項定義如下：

·MD5 — MD5是產生128位摘要的單向雜湊演算法。MD5的計算速度比SHA-1快，但比SHA-1更不安全。不建議使用MD5。

·SHA-1 — SHA-1是產生160位摘要的單向雜湊演算法。SHA-1的計算速度比MD5慢，但比MD5更安全。

·SHA2-256 — 指定具有256位摘要的安全雜湊演算法SHA2。

步驟8.從*DH Group*下拉選單中，選擇要與階段1中的金鑰一起使用的相應Diffie-Hellman(DH)組。Diffie-Hellman是一種用於交換預共用金鑰集的連線的金鑰交換協定。演算法的強度由位決定。



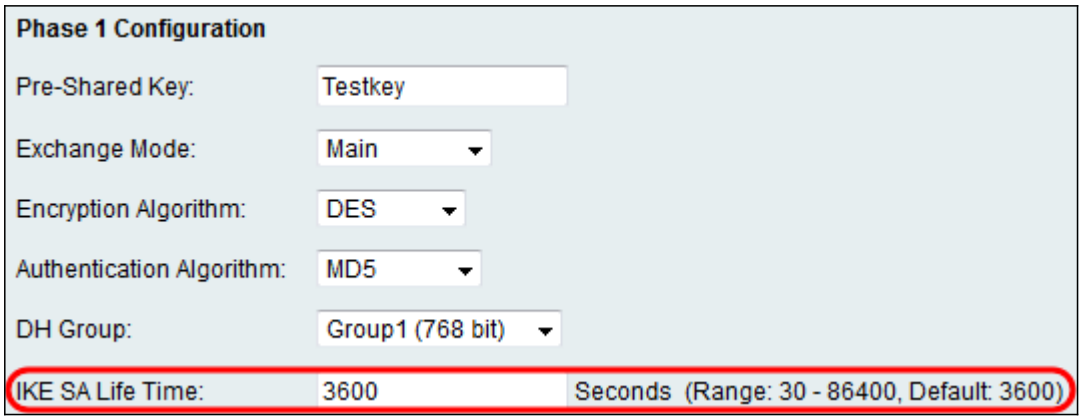
可用選項定義如下：

·組1（768位） — 以最快的速度計算金鑰，但最不安全。

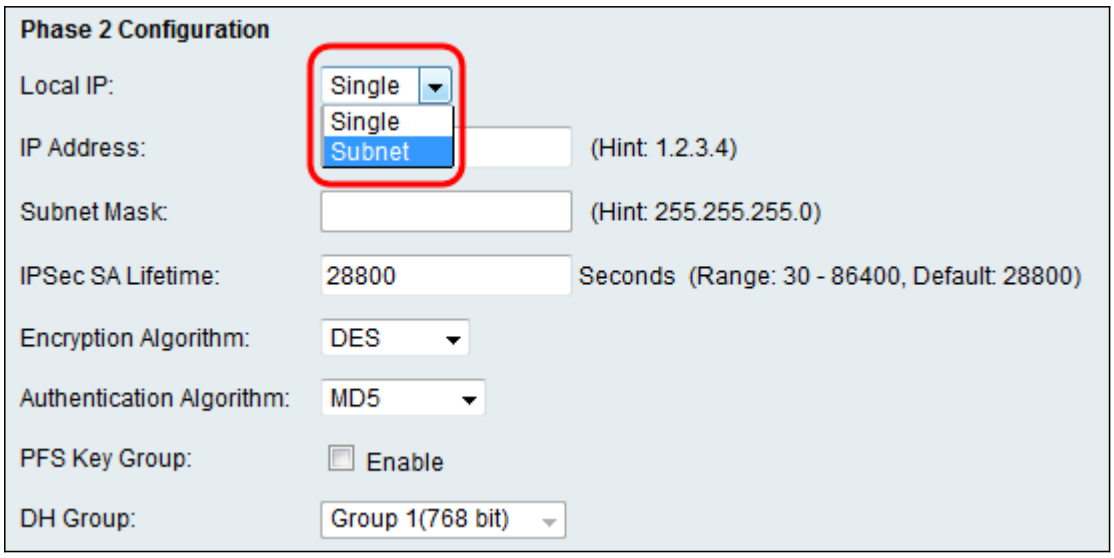
·Group2（1024位） — 計算金鑰的速度較慢，但比Group1更安全。

·組5（1536位） — 計算金鑰最慢，但最安全。

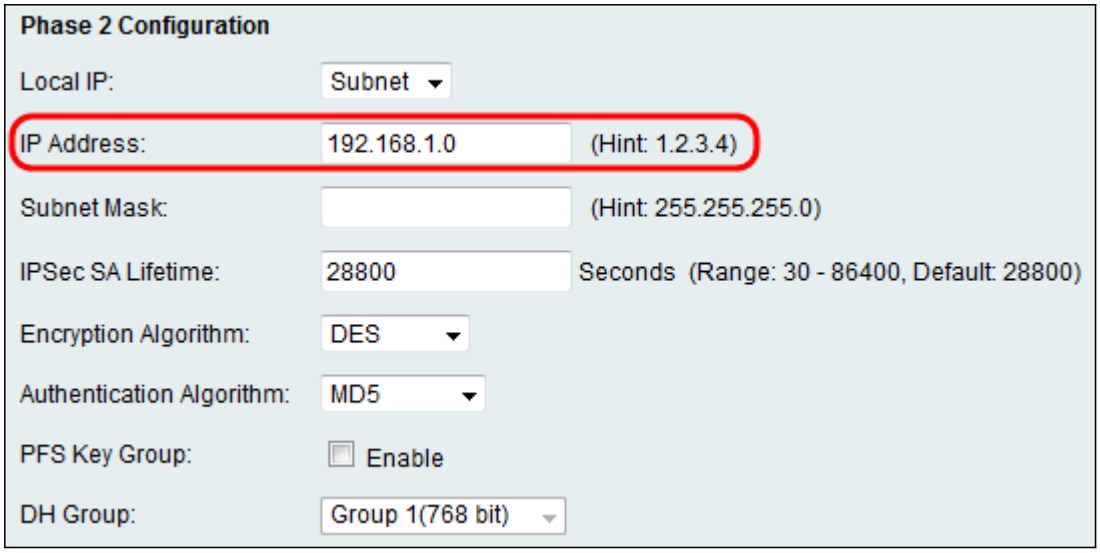
步驟9.在*IKE SA Life Time*欄位中，輸入自動IKE金鑰的有效時間（以秒為單位）。此時間到期後，將自動協商新金鑰。



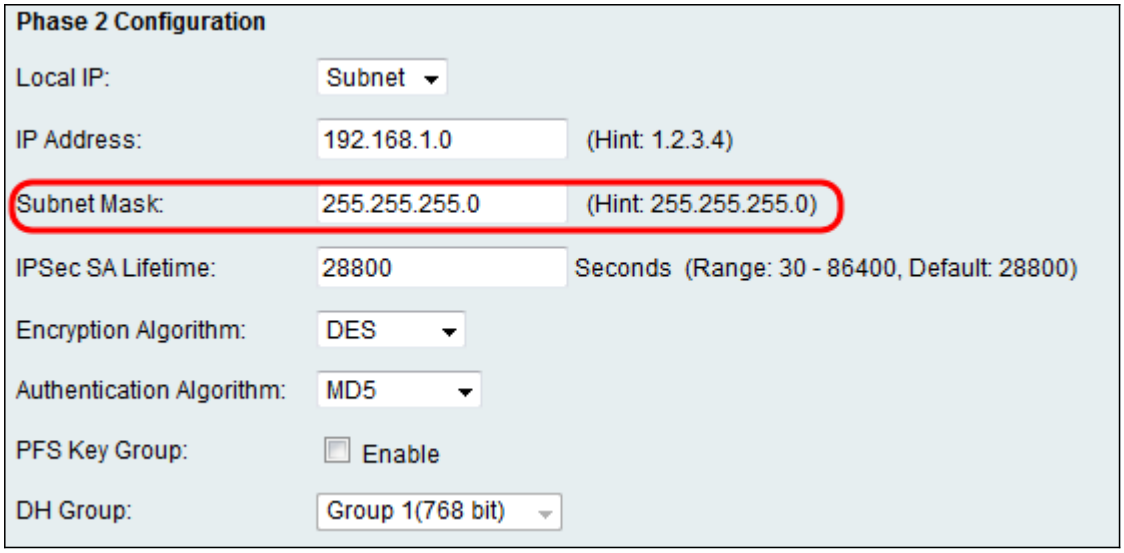
步驟10.從*本地IP*下拉選單中，如果要讓一個本地LAN使用者訪問VPN隧道，請選擇**Single**；如果要讓多個使用者能夠訪問VPN隧道，請選擇**Subnet**。



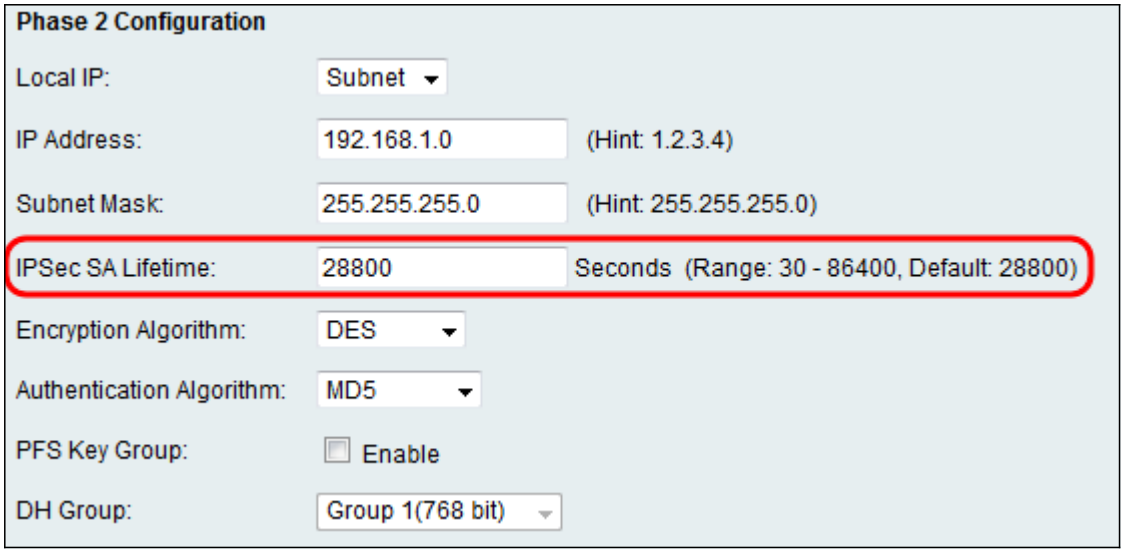
步驟11.如果在步驟10中選擇了**子網**，請在「IP地址」欄位中輸入子網路的網路IP地址。如果在步驟10中選擇了**Single**，請輸入單個使用者的IP地址並跳至步驟13。



步驟12。（可選）如果在步驟10中選擇了**子網**，請在*子網掩碼*欄位中輸入本地網路的子網掩碼。

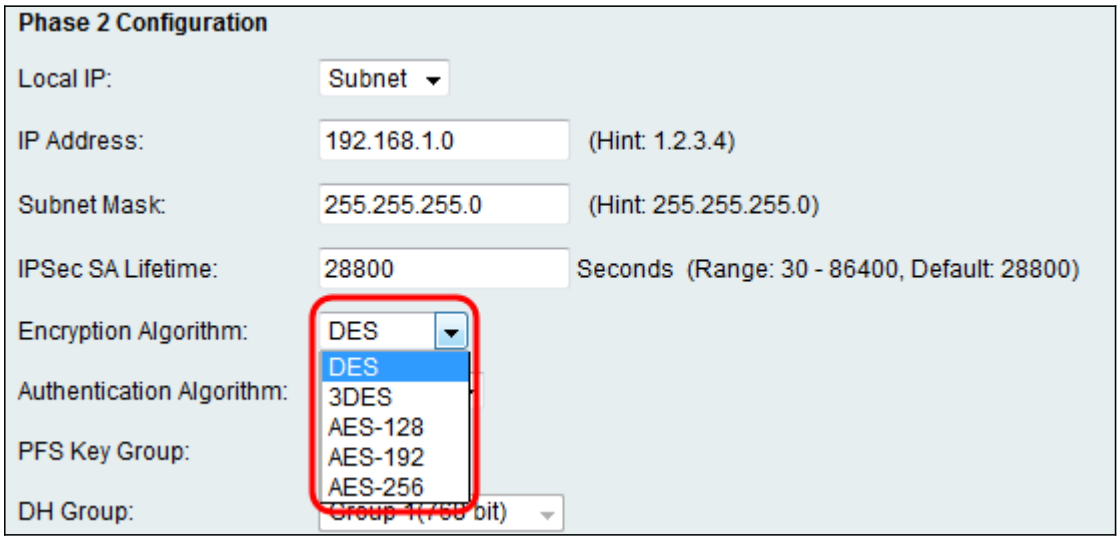


步驟13.在*IPSec SA Lifetime*欄位中，輸入VPN連線在第2階段保持活動狀態的時間（以秒為單位）。此時間到期後，將重新協商VPN連線的IPSec安全關聯。



步驟14.從*Encryption Algorithm*下拉選單中，選擇適當的加密方法以加密階段2中的預共用金鑰。建議使用AES-128來實現它的高安全性和快速效能。VPN隧道的兩端都需要使用相同的加

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，雖然安全性最低，但為了向後相容，可能需要這種加密方法。

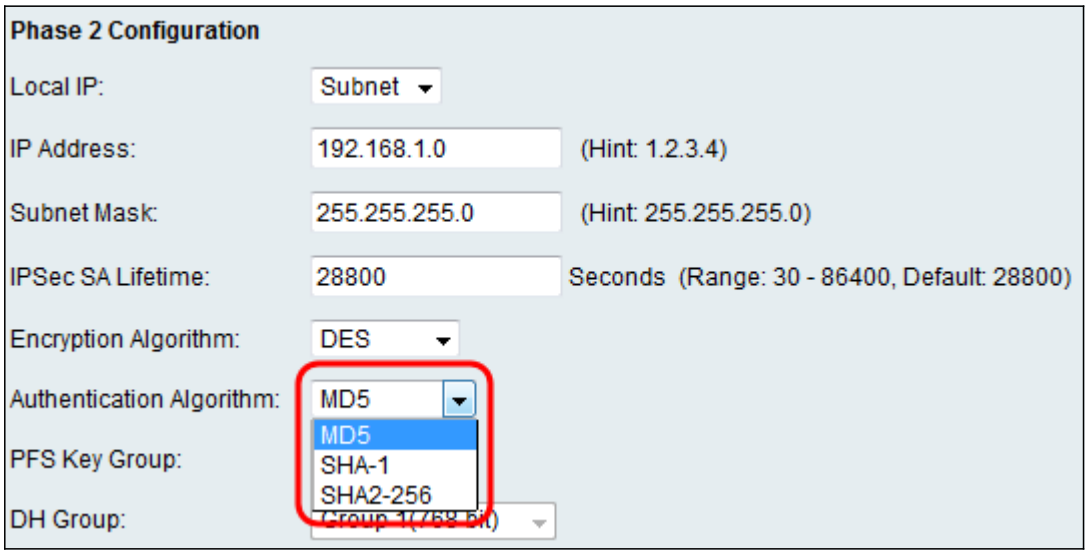
·3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法，用於增加金鑰大小，因為它將資料加密三次。這比DES提供了更高的安全性，但比AES提供的安全性更低。

·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15.從*Authentication Algorithm*下拉選單中，選擇適當的身份驗證方法以確定如何在第2階段驗證封裝安全負載(ESP)協定報頭資料包。VPN隧道的兩端需要使用相同的身份驗證方法。



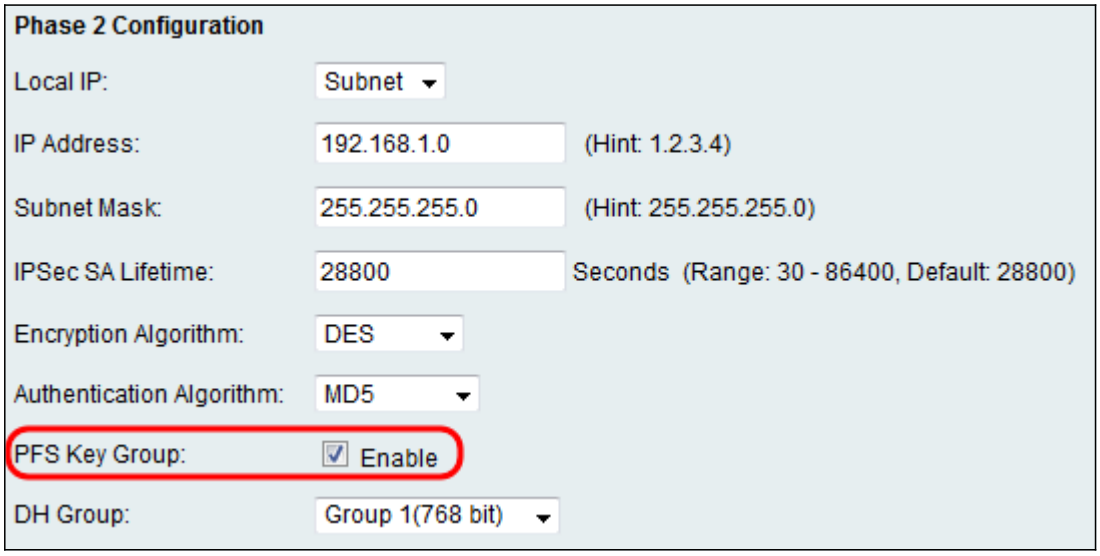
可用選項定義如下：

·MD5 — MD5是產生128位摘要的單向雜湊演算法。MD5的計算速度比SHA-1快，但比SHA-1更不安全。不建議使用MD5。

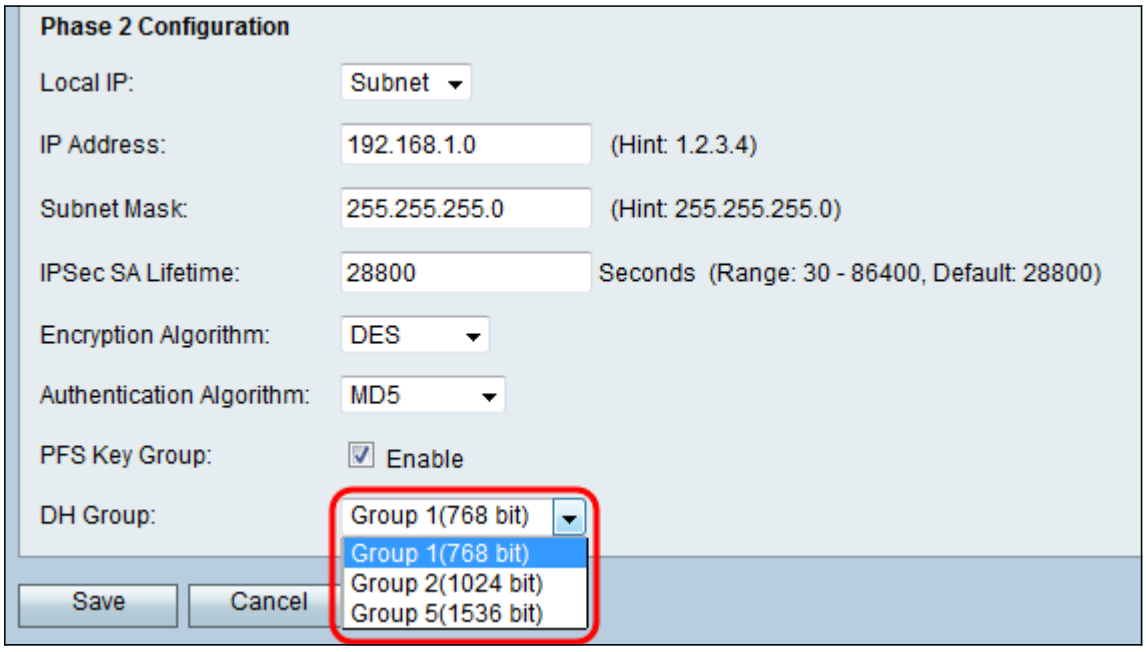
·SHA-1 — SHA-1是產生160位摘要的單向雜湊演算法。SHA-1的計算速度比MD5慢，但比MD5更安全。

·SHA2-256 — 指定具有256位摘要的安全雜湊演算法SHA2。

步驟16。（可選）在*PFS Key Group欄位*中，選中**Enable**復選框。完全轉發保密(PFS)通過確保在第2階段使用新的DH金鑰來保護資料，建立額外的安全層。該過程將在第1階段生成的DH金鑰在傳輸過程中遭到破壞的情況下完成。



步驟17.從*DH Group*下拉選單中，選擇適當的要在階段2中與金鑰一起使用的Diffie-Hellman(DH)組。



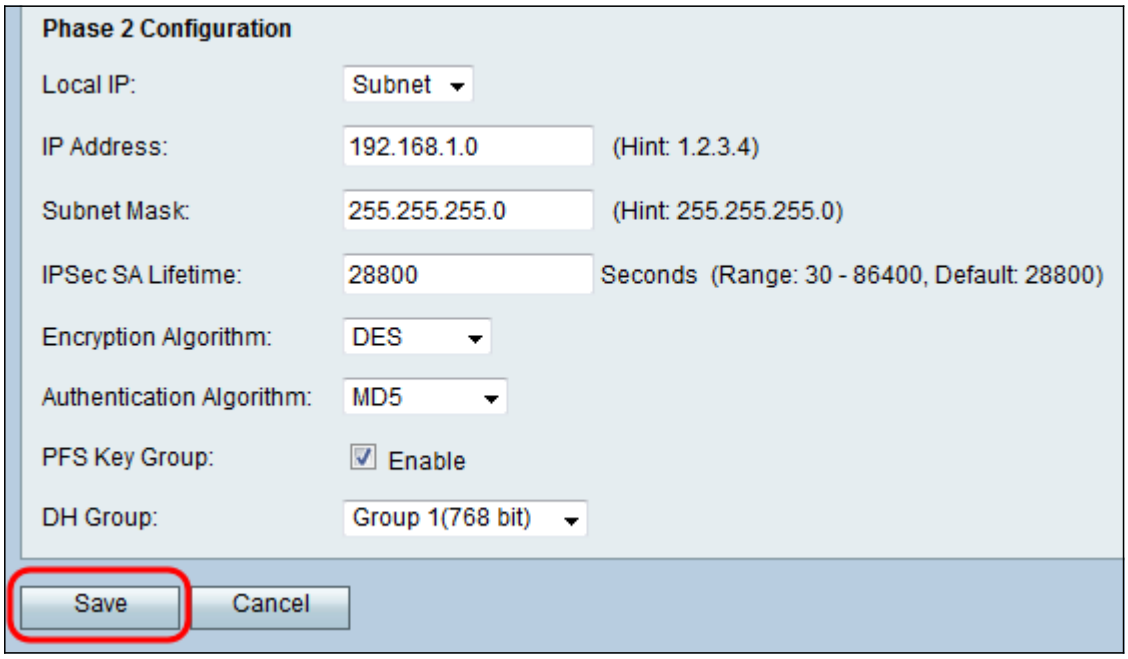
可用選項定義如下：

·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18.按一下**Save**以儲存設定。



有關詳細資訊，請參閱以下文檔：

- RV130產品手冊 — 介紹RV130系列路由器的VPN功能
- RV130產品頁面 — 包含思科所有RV130文章的連結

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）。