在RV34x系列路由器上配置網際網路協定安全(IPSec)配置檔案

目標

網際網路通訊協定安全(IPSec)在兩個對等體（例如兩個路由器）之間提供安全通道。應通過指定這些隧道的特性來定義視為敏感且應該通過這些安全隧道傳送的資料包，以及應該用於保護這些敏感資料包的引數。然後，當IPsec對等路由器看到此類敏感封包時，它會設定適當的安全通道，並將封包透過此通道傳送到遠端對等路由器。

當在防火牆或路由器中實施IPsec時，它提供了強大的安全性，可以應用於所有通過邊界的流量。公司或工作組內的流量不會產生與安全相關的處理開銷。

本文檔的目的是向您展示如何在RV34x系列路由器上配置IPSec配置檔案。

適用裝置

- RV34x系列

軟體版本

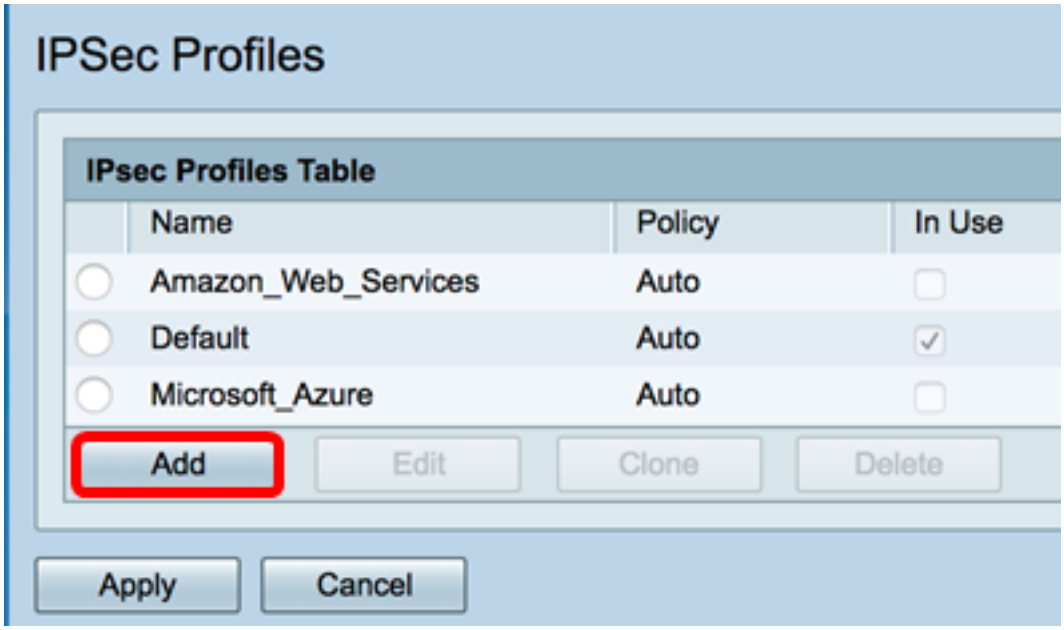
- 1.0.1.16

配置IPSec配置檔案

建立IPSec配置檔案

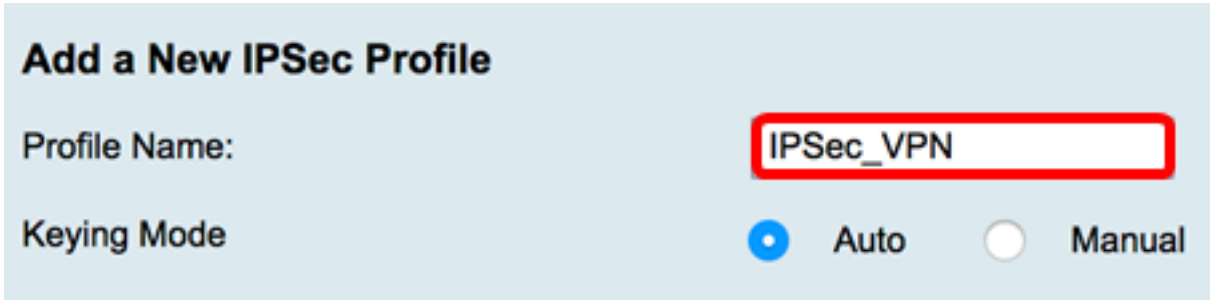
步驟1.登入到路由器的基於Web的實用程式，然後選擇**VPN > IPSec Profiles**。

步驟2. IPsec配置檔案表顯示現有配置檔案。按一下**Add**建立新配置檔案。



步驟3.在「配置檔名稱」欄位中為配*置檔*案建立名稱。配置檔名稱只能包含字母數字字元以及特殊字元的下劃線(_)。

附註：在本示例中，IPSec_VPN用作IPSec配置檔名稱。



步驟4.按一下單選按鈕以確定配置檔案將用於進行身份驗證的金鑰交換方法。選項包括：

- 自動(Auto) — 自動設定策略引數。此選項使用Internet金鑰交換(IKE)策略進行資料完整性和加密金鑰交換。如果選擇此選項，則啟用Auto Policy Parameters區域下的配置設定。按一下here以配置自動設定。
- 手動(Manual) — 此選項可讓您手動配置用於虛擬專用網路(VPN)隧道的資料加密和完整性的金鑰。如果選擇此選項，則啟用Manual Policy Parameters區域下的配置設定。按一下here以配置手動設定。

附註：在本示例中，選擇了Auto。

配置自動設定

步驟1。在Phase 1 Options區域中，從DH Group下拉選單中選擇要與Phase 1中的金鑰一起

使用的適當Diffie-Hellman(DH)組。Diffie-Hellman是一種加密金鑰交換協定，用於交換預共用金鑰集。演算法的強度由位決定。選項包括：

- Group2 - 1024位 — 計算金鑰的速度較慢，但比Group1更安全。
- Group5 - 1536位 — 計算金鑰最慢，但最安全。

附註：在本例中，選擇了Group2-1024位。

步驟2.從Encryption下拉選單中，選擇適當的加密方法來加密和解密封裝安全負載(ESP)和Internet安全關聯和金鑰管理協定(ISAKMP)。 選項包括：

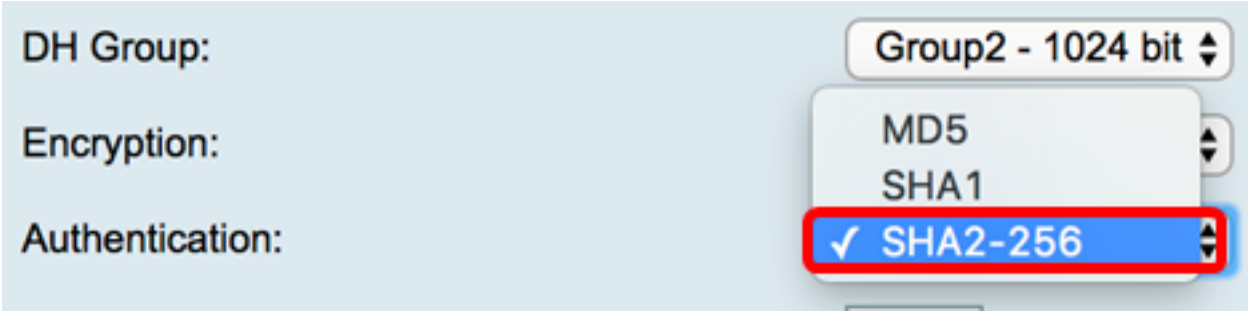
- 3DES — 三重資料加密標準。
- AES-128 — 高級加密標準使用128位金鑰。
- AES-192 — 高級加密標準使用192位金鑰。
- AES-256 — 高級加密標準使用256位金鑰。

注意：AES是使用DES和3DES進行加密的標準方法，因為它具有更高的效能和安全性。延長AES金鑰將提高安全性，降低效能。在本範例中，選擇AES-256。

步驟3.從Authentication下拉選單中，選擇確定ESP和ISAKMP身份驗證方式的身份驗證方法。選項包括：

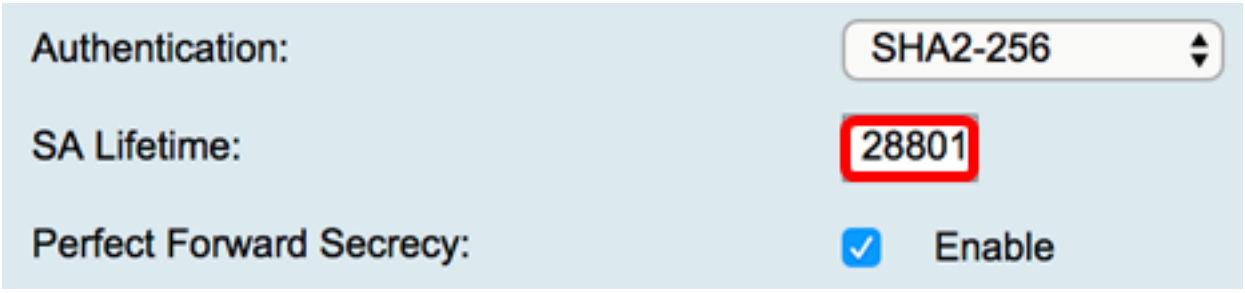
- MD5 — 消息摘要演算法具有128位雜湊值。
- SHA-1 — 安全雜湊演算法具有160位雜湊值。
- SHA2-256 — 具有256位雜湊值的安全雜湊演算法。

注意：MD5和SHA都是加密雜湊函式。他們獲取一段資料，將其壓縮，然後建立通常不可再現的唯一的十六進位制輸出。在此範例中，選擇SHA2-256。

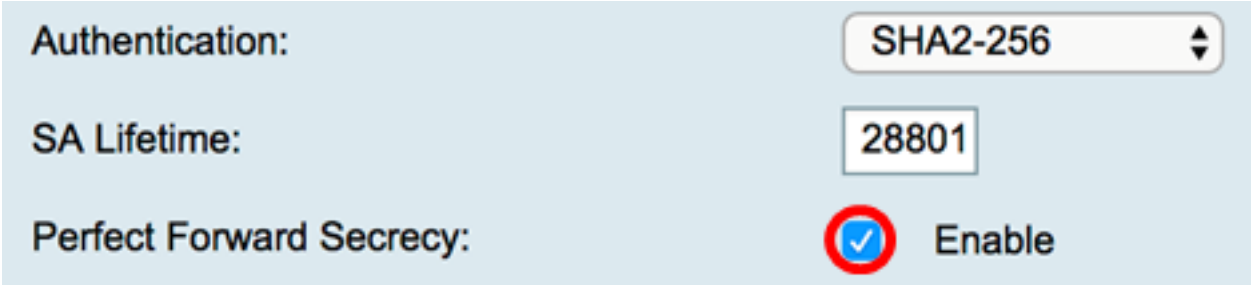


步驟4.在*SA Lifetime*欄位中，輸入範圍在120到86400之間的值。這是Internet金鑰交換(IKE)安全關聯(SA)在此階段保持活動狀態的時間長度。預設值為 28800。

附註：在本例中，使28801了ACL。

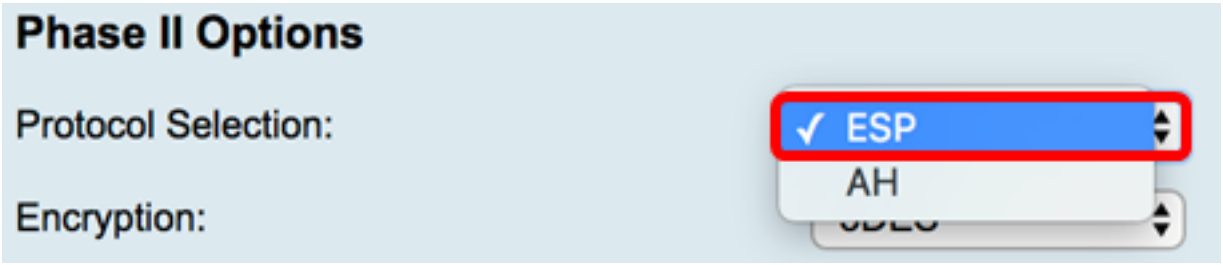


步驟5.（可選）選中**Enable Perfect Forward Secrecy**覈取方塊以生成IPSec流量加密和身份驗證的新金鑰。



步驟6.從Phase II Options區域的Protocol Selection下拉選單中，選擇應用於協商第二階段的一種協定型別。選項包括：

- ESP — 如果選擇此選項，請跳至步驟7，選擇有關如何加密和解密ESP資料包的加密方法。一種安全協定，提供資料隱私服務、可選資料身份驗證和反重播服務。ESP封裝要保護的資料。
- AH — 身份驗證報頭(AH)是一種安全協定，它提供資料身份驗證和可選的反重播服務。AH嵌入要保護的資料（完整的IP資料包）。 如果選擇此選項，請跳至步驟8。

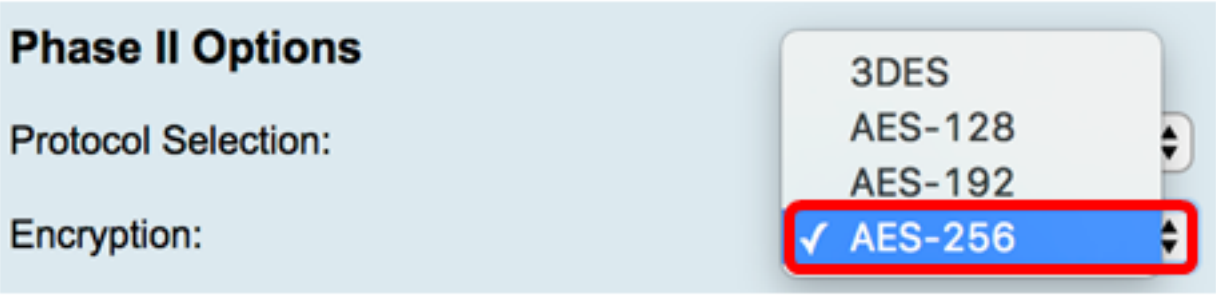


步驟7.如果在步驟6中選擇了ESP，請從Encryption下拉選單中選擇相應的加密方法來加密和解密ESP和ISAKMP。選項包括：

- 3DES — 三重資料加密標準。
- AES-128 — 高級加密標準使用128位金鑰。

- AES-192 — 高級加密標準使用192位金鑰。
- AES-256 — 高級加密標準使用256位金鑰。

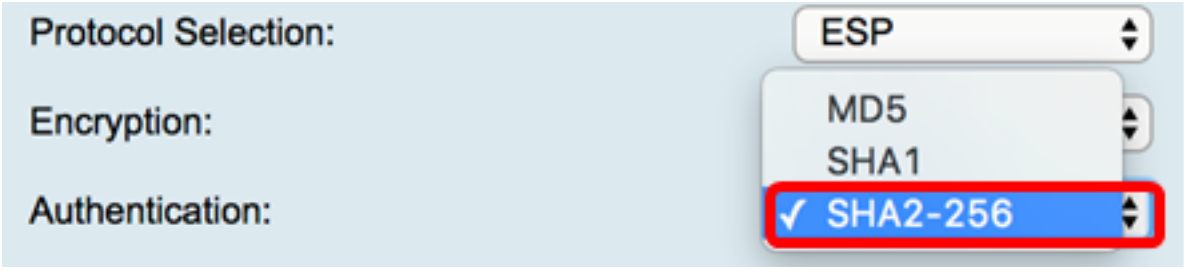
附註：在此範例中，選擇AES-256。



步驟8.從Authentication下拉選單中，選擇確定ESP和ISAKMP身份驗證方式的身份驗證方法。選項包括：

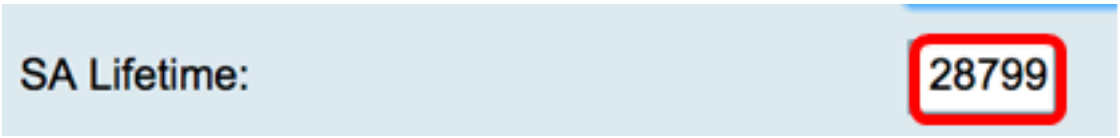
- MD5 — 消息摘要演算法具有128位雜湊值。
- SHA-1 — 安全雜湊演算法具有160位雜湊值。
- SHA2-256 — 具有256位雜湊值的安全雜湊演算法。

附註：本例中使用的是SHA2-256。



步驟9.在*SA Lifetime*欄位中，輸入範圍在120到28800之間的值。這是IKE SA在此階段保持活動狀態的時間長度。預設值為 3600。

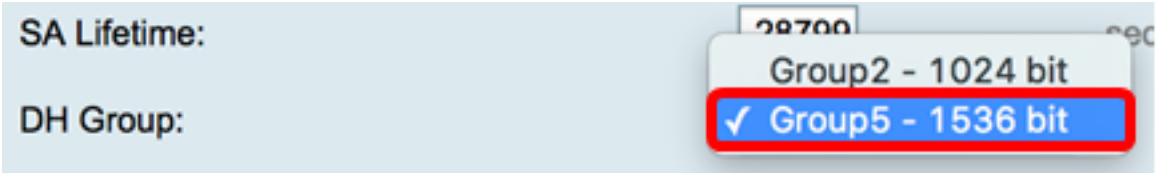
附註：在本例中，使28799了ACL。

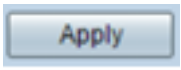


步驟10.從DH組下拉選單中，選擇要與階段2中的金鑰一起使用的相應Diffie-Hellman(DH)組。選項包括：

- Group2 - 1024位 — 計算金鑰的速度較慢，但比Group1更安全。
- Group5 - 1536位 — 計算金鑰最慢，但最安全。

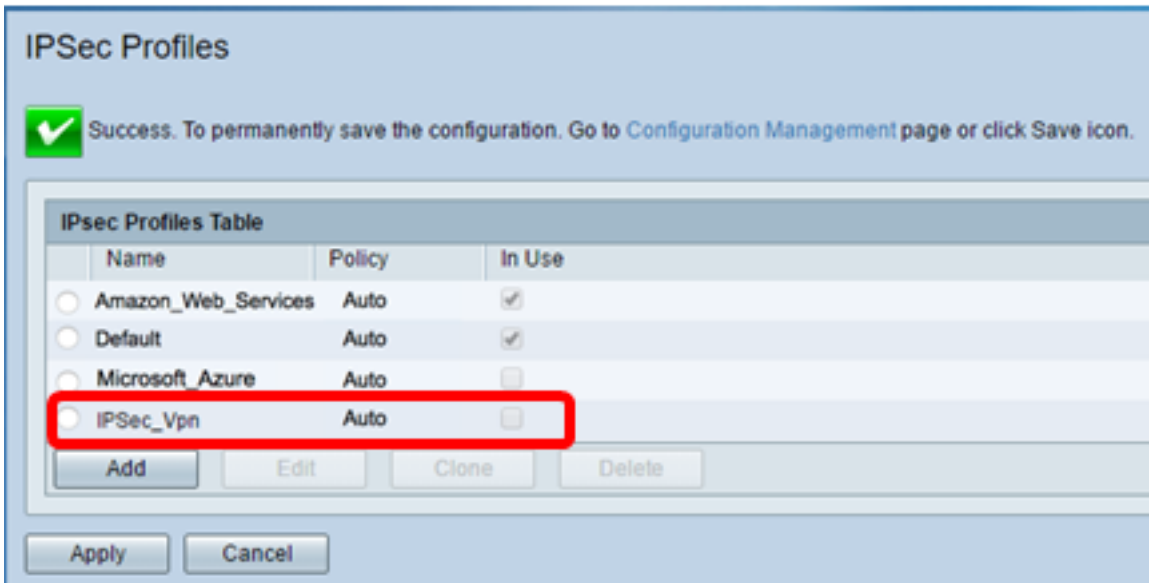
附註：在本例中，選擇了Group5 - 1536位。



步驟11.單 

擊。

附註：您將回到IPSec簡檔表，現在應會顯示新建立的IPSec簡檔。



步驟12.（可選）若要永久儲存組態，請前往「複製/儲存組態」頁面，或按一下頁面上部的圖 

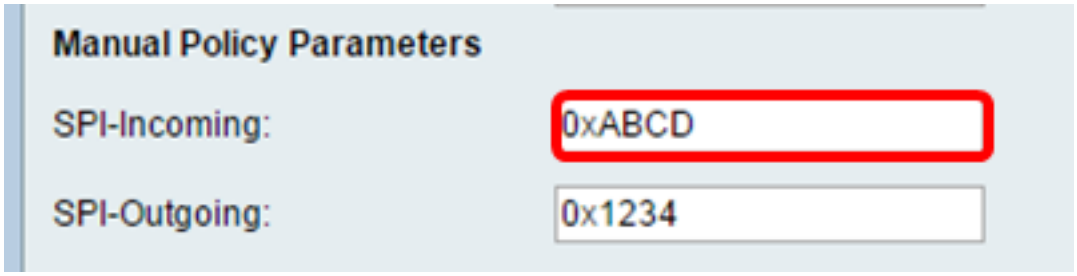
標。

現在，您應該已經在RV34x系列路由器上成功配置了Auto IPSec配置檔案。

配置手動設定

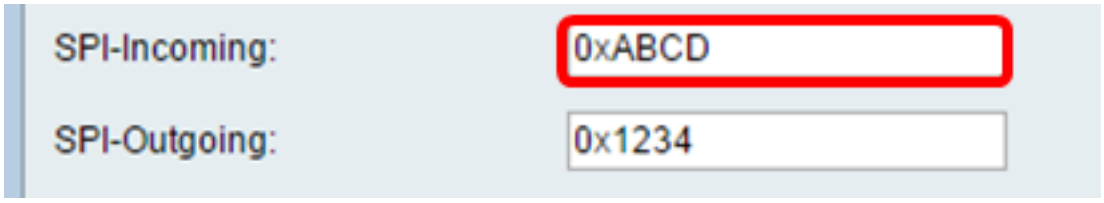
步驟1.在*SPI-Incoming*欄位中，為VPN連線上的傳入流量的安全引數索引(SPI)標籤輸入從100到FFFFFFF的十六進位制數。SPI標籤用於區分一個會話的流量和其他會話的流量。

附註：在本示例中，使用了0xABCD。



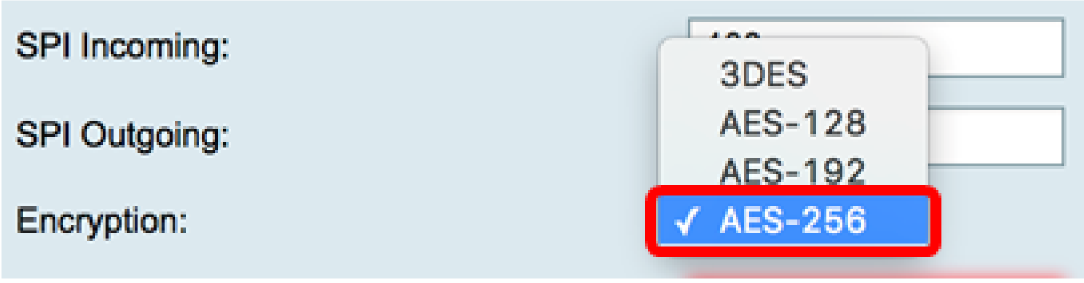
步驟2.在*SPI-Outgoing*欄位中，為VPN連線上的傳出流量的SPI標籤輸入從100到FFFFFFF的十六進位制數。

附註：在本示例中，使用0x1234。



步驟3.從「加密」下拉選單中選擇一個選項。選項包括3DES、AES-128、AES-192和AES-256。

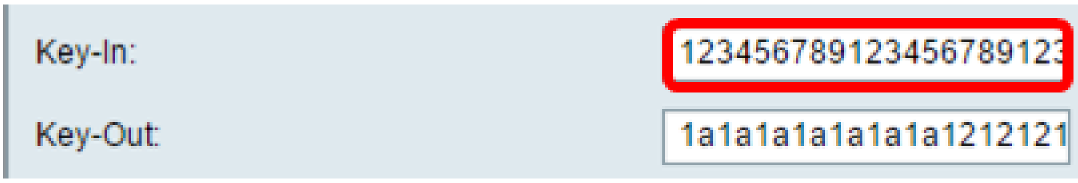
附註：在此範例中，選擇AES-256。



步驟4.在*Key-In*欄位中輸入入站策略的金鑰。金鑰長度取決於步驟3中選擇的演算法。

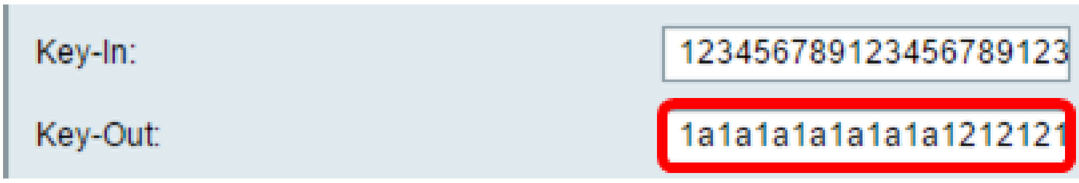
- 3DES使用48個字元的金鑰。
- AES-128使用32個字元的金鑰。
- AES-192使用48個字元的金鑰。
- AES-256使用64個字元的金鑰。

附註：在本示例中123456789123456789123使用......。



步驟5.在*Key-Out*欄位中輸入傳出策略的金鑰。金鑰長度取決於步驟3中選擇的演算法。

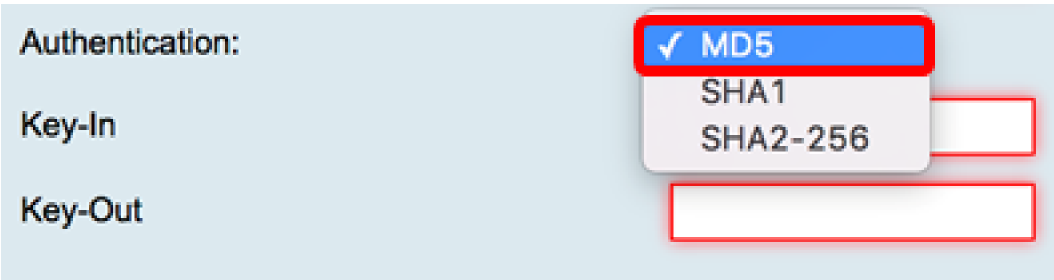
附註：在此示例中，使用1a1a1a1a1a121212...。



步驟6.從Manual Integrity Algorithm下拉選單中選擇一個選項。

- MD5 — 使用128位雜湊值實現資料完整性。MD5的安全性較低，但比SHA-1和SHA2-256更快。
- SHA-1 — 使用160位雜湊值實現資料完整性。SHA-1比MD5更慢但更安全，而SHA-1比SHA2-256更快但更安全。
- SHA2-256 — 使用256位雜湊值實現資料完整性。SHA2-256比MD5和SHA-1速度慢但安全。

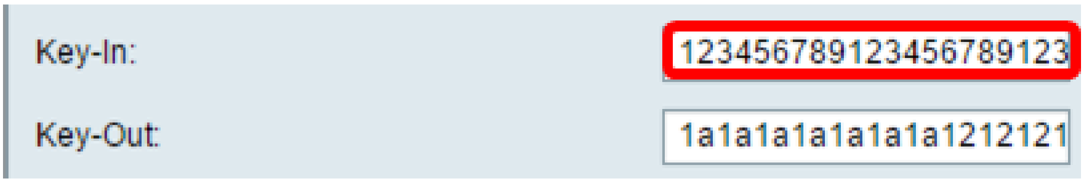
附註：在本例中，選擇了MD5。



步驟7.在*Key-In*欄位中輸入入站策略的金鑰。金鑰長度取決於步驟6中選擇的演算法。

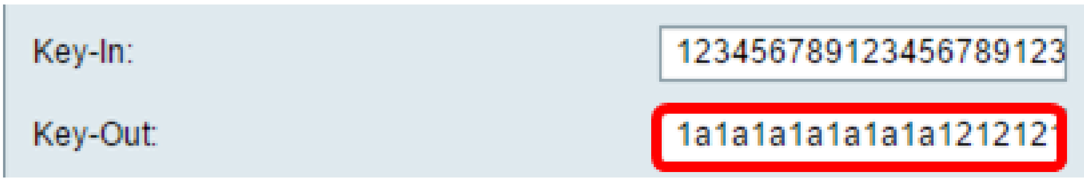
- MD5使用32個字元的金鑰。
- SHA-1使用40個字元的金鑰。
- SHA2-256使用64個字元的金鑰。

附註：在本示例中123456789123456789123使用......。



步驟8.在*Key-Out*欄位中輸入傳出策略的金鑰。金鑰長度取決於步驟6中選擇的演算法。

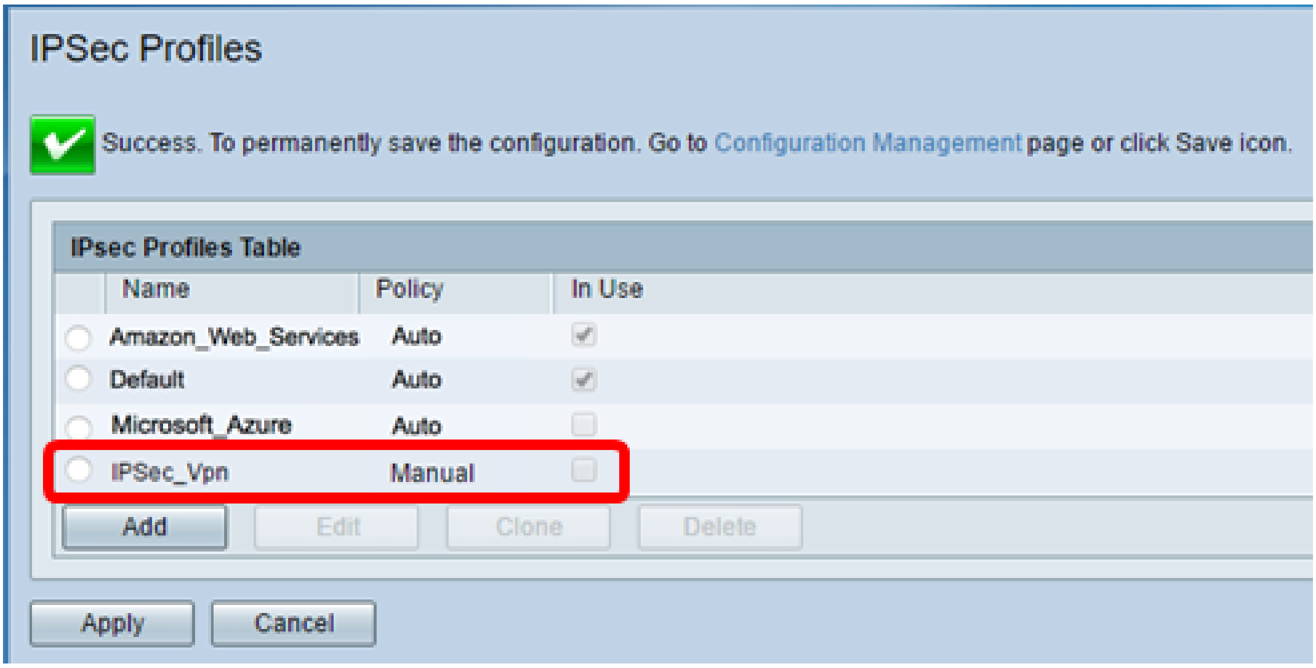
附註：在此示例中，使用1a1a1a1a1a121212...。



步驟9.單 

擊。

附註：您將回到IPSec簡檔表，現在應會顯示新建立的IPSec簡檔。



步驟10。（可選）若要永久儲存配置，請轉到「複製/儲存配置」頁面，或按一下該頁面上部的圖 

標。

現在，您應該已經在RV34x系列路由器上成功配置手動IPSec配置檔案。