RV215W上的高級VPN設定

目標

虛擬專用網路(VPN)是在網路內部或網路之間建立的安全連線。VPN用於將指定主機和網路之間的流量與未經授權的主機和網路的流量隔離。本文說明如何在RV215W上配置高級VPN設定。

適用裝置

·RV215W

軟體版本

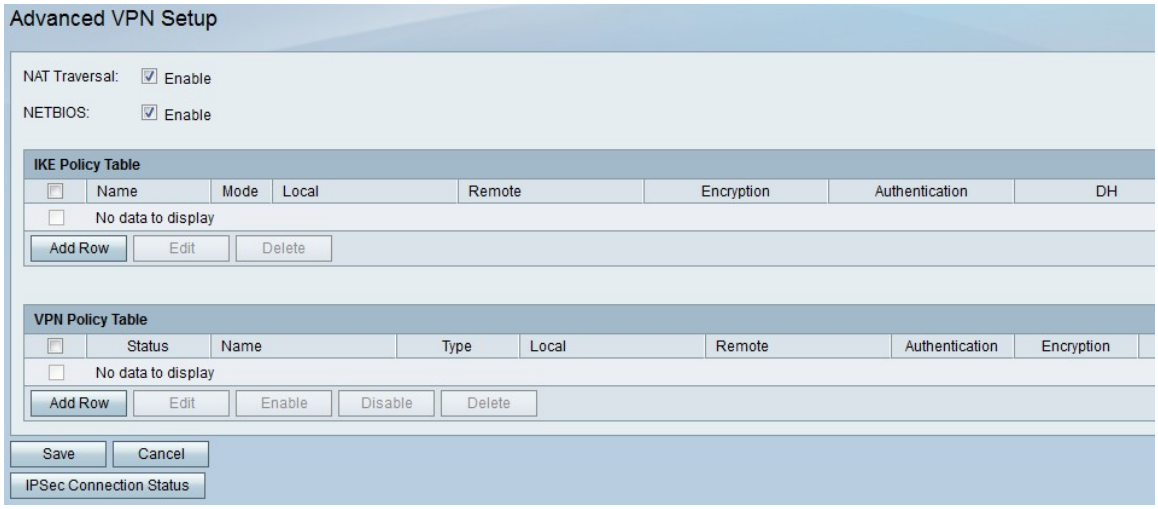
•1.1.0.5

高級VPN設定

初始設定

以下過程介紹了如何配置高級VPN設定的初始設定。

步驟1.登入到Web配置實用程式並選擇**VPN > Advanced VPN Setup**。*Advanced VPN Setup*頁面開啟：



步驟2.（可選）如果要為VPN連線啟用網路地址轉換(NAT)遍歷，請選中NAT遍歷欄位中的**Enable**覈取方塊。NAT遍歷允許在使用NAT的網關之間建立VPN連線。如果VPN連線通過啟用了NAT的網關，請選擇此選項。

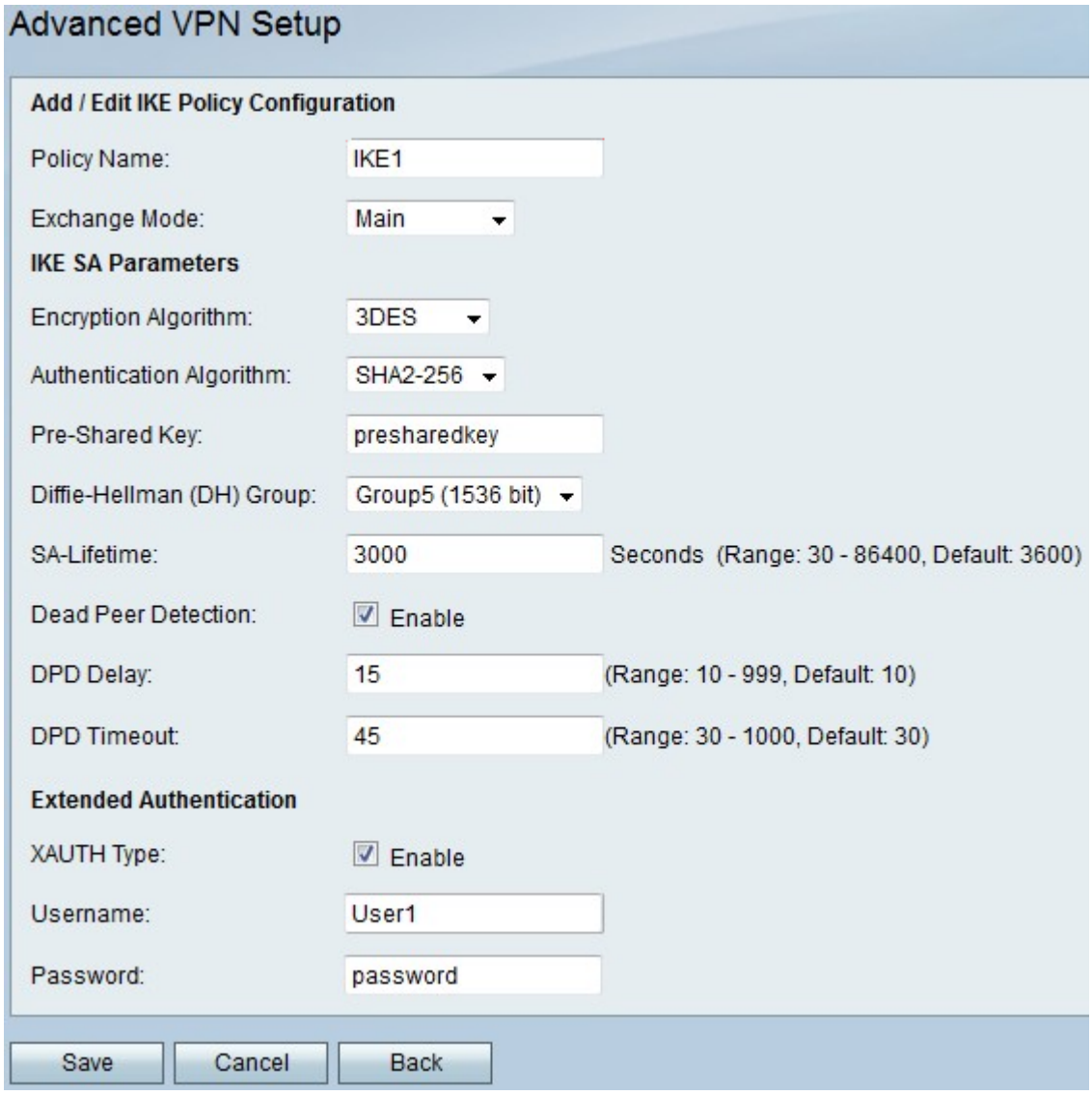
步驟3.（可選）如果要啟用要通過VPN連線傳送的網路基本輸入/輸出系統(NetBIOS)廣播，請選中NETBIOS欄位中的**Enable**覈取方塊。NetBIOS允許主機在LAN中彼此通訊。

IKE策略設定

Internet金鑰交換(IKE)是一種協定，用於為VPN中的通訊建立安全連線。這種已建立的安全連線稱為安全關聯(SA)。 以下過程介紹了如何為VPN連線配置IKE策略以用於安全性。要使

VPN正常工作，兩個端點的IKE策略應相同。

步驟1.在IKE策略表中，按一下**Add Row**以建立新的IKE策略。要編輯IKE策略，請選中該策略的覈取方塊，然後按一下**Edit**。*Advanced VPN Setup*頁面將更改：

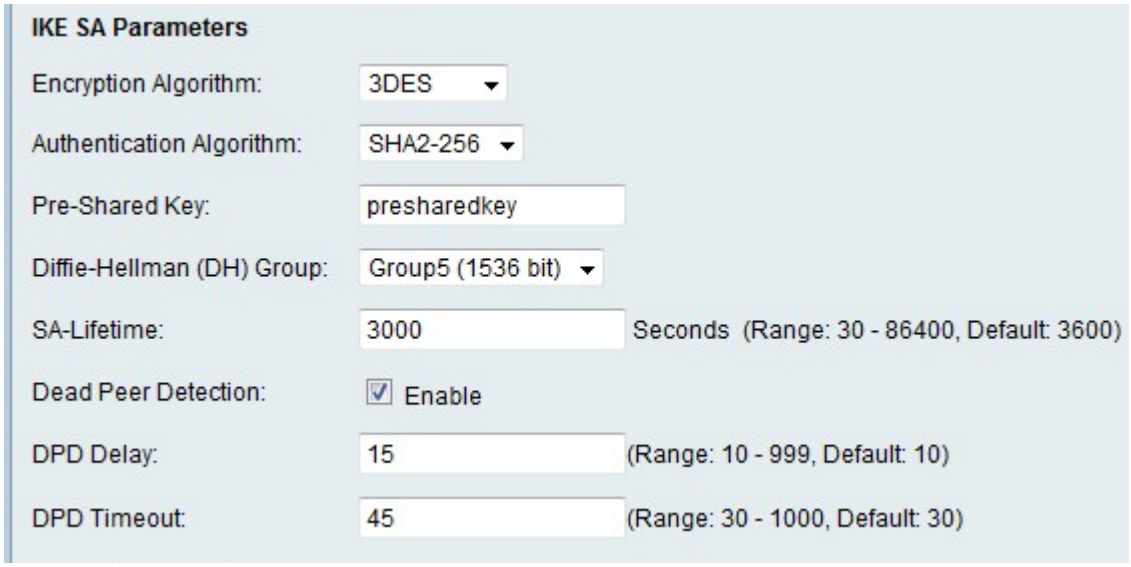


步驟2.在Policy Name欄位中，輸入IKE策略的名稱。

步驟3.從Exchange Mode下拉選單中，選擇一個選項。

·主要 — 此選項允許IKE策略比主動模式更安全地運行，但速度更慢。如果需要更安全的VPN連線，請選擇此選項。

·積極 — 此選項允許IKE策略比主模式運行更快，但安全性較低。如果需要更快的VPN連線，請選擇此選項。



步驟4.從Encryption Algorithm下拉式清單中選擇一個選項。

·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5.從Authentication Algorithm下拉選單中，選擇一個選項。

·MD5 — 消息摘要演算法5(MD5)使用128位雜湊值進行身份驗證。MD5的安全性較低，但比SHA-1和SHA2-256更快。

·SHA-1 — 安全雜湊函式1(SHA-1)使用160位雜湊值進行身份驗證。SHA-1比MD5更慢但更安全，而SHA-1比SHA2-256更快但更安全。

·SHA2-256 — 具有256位雜湊值(SHA2-256)的安全雜湊演算法2使用256位雜湊值進行身份驗證。SHA2-256比MD5和SHA-1速度慢但安全。

步驟6.在Pre-Shared Key欄位中，輸入IKE策略使用的預共用金鑰。

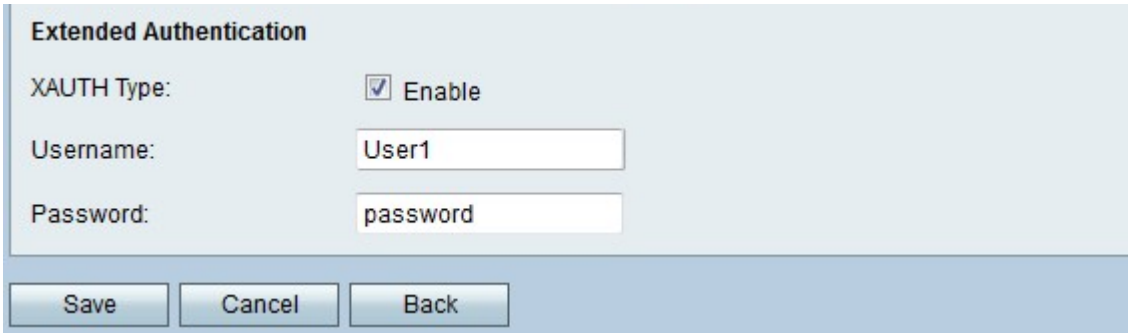
步驟7.從Diffie-hellman(DH)組下拉選單中，選擇IKE使用哪個DH組。DH組中的主機可以在彼此不知情的情況下交換金鑰。組位號越高，組越安全。

步驟8.在SA-Lifetime欄位中，輸入VPN的SA在續訂SA之前持續的時間（以秒為單位）。

步驟9.（可選）選中Dead Peer Detection欄位中的**Enable**覈取方塊以啟用Dead Peer Detection(DPD)。DPD監控IKE對等體以檢視對等體是否停止工作。DPD可防止非活動對等體上的網路資源浪費。

步驟10。（可選）如果在步驟9中啟用DPD，請在「DPD延遲」欄位中輸入檢查對等體活動的頻率（以秒為單位）。

步驟11。（可選）如果在步驟9中啟用DPD，請在DPD Timeout欄位中輸入在刪除非活動對等體之前等待的秒數。



步驟12。（可選）勾選XAUTH Type欄位中的**Enable**覈取方塊以啟用擴充驗證(XAUTH)。XAUTH允許多個使用者使用單個VPN策略，而不是為每個使用者使用一個VPN策略。

步驟13。（可選）如果在步驟12中啟用了XAUTH，請在「使用者名稱」欄位中輸入用於策略的使用者名稱。

步驟14。（可選）如果在步驟12中啟用了XAUTH，請在「密碼」欄位中輸入要用於策略的密碼。

步驟15.按一下「**Save**」。*系統將重新顯示原始Advanced VPN Setup*頁面。

VPN策略設定

以下過程說明如何配置VPN策略以供VPN連線使用。要使VPN正常工作，兩個端點的VPN策略應該相同。

步驟1.在VPN策略表中，按一下**Add Row**以建立新的VPN策略。要編輯VPN策略，請選中該策略的覈取方塊，然後按一下**Edit**。*Advanced VPN Setup*頁面將更改：

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name: VPN1

Policy Type: Manual Policy

Remote Endpoint: IP Address

209.165.201.1 (Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP: Subnet

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: Subnet

IP Address: 192.168.2.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Encryption Algorithm: AES-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Integrity Algorithm: SHA2-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Auto Policy Parameters

SA-Lifetime: 20000 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-256

Integrity Algorithm: SHA2-256

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: IKE1

步驟2.在Policy Name欄位中，輸入VPN策略的名稱。

步驟3.從Policy Type下拉選單中選擇一個選項。

·手動策略 — 此選項可讓您配置用於資料加密和完整性的金鑰。

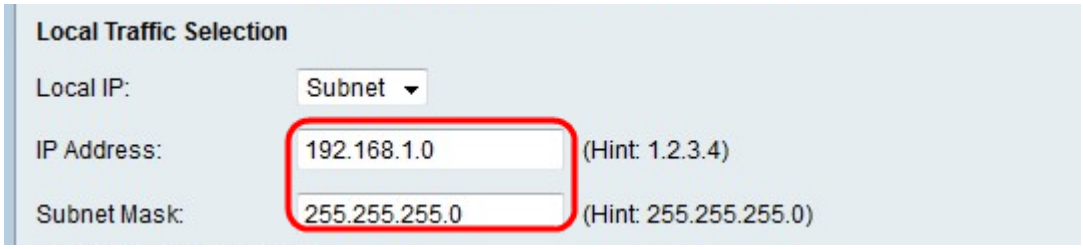
·自動策略 — 此選項使用IKE策略進行資料完整性和加密金鑰交換。

步驟4.從Remote Endpoint下拉選單中選擇一個選項。

·IP地址 — 此選項通過公共IP地址標識遠端網路。

·FQDN — 此選項使用完全限定域名(FQDN)來標識遠端網路。

步驟5.在「遠端終端」下拉選單下方的文本輸入欄位中，輸入遠端地址的公共IP地址或域名。



步驟6.從Local IP下拉選單中選擇一個選項。

·單一 — 此選項使用單個主機作為本地VPN連線點。

·子網 — 此選項使用本地網路的子網作為本地VPN連線點。

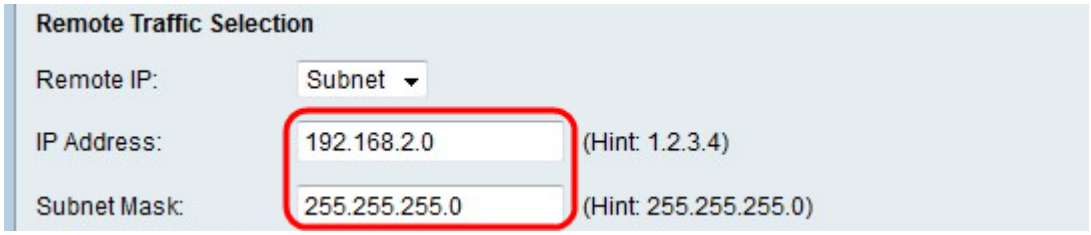
步驟7.在IP地址欄位中，輸入本地子網或主機的主機或子網IP地址。

步驟8.（可選）如果在步驟6中選擇子網，請在「子網掩碼」欄位中輸入本地子網的子網掩碼。

步驟9.從Remote IP下拉選單中選擇一個選項。

·單一 — 此選項使用單個主機作為遠端VPN連線點。

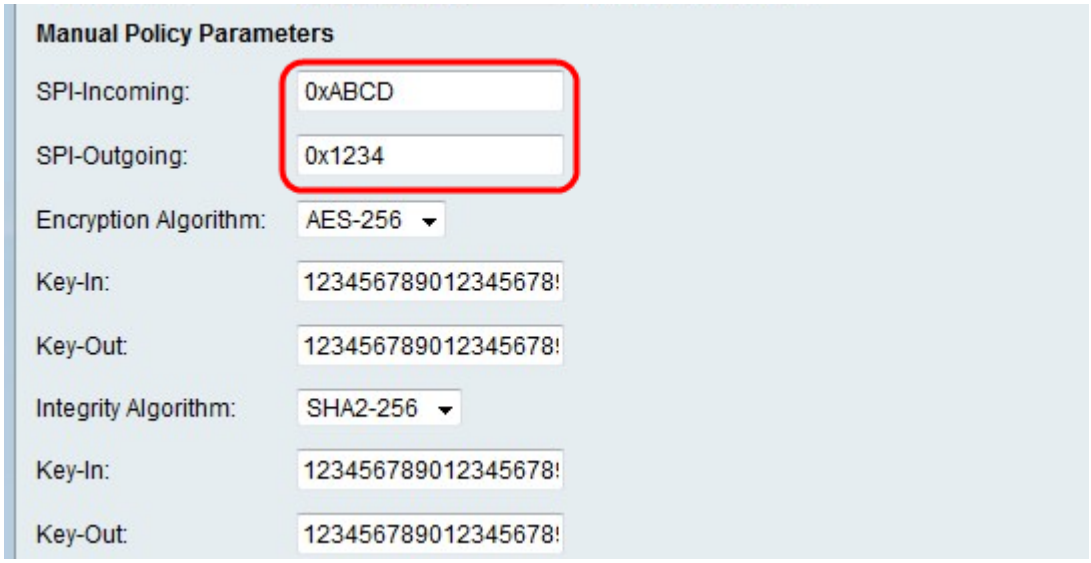
·子網 — 此選項使用遠端網路的子網作為遠端VPN連線點。



步驟10.在IP地址欄位中，輸入遠端子網或主機的主機或子網IP地址。

步驟11。（可選）如果在步驟9中選擇子網，請在「子網掩碼」欄位中輸入遠端子網的子網掩碼。

附註：如果您在步驟3中選擇了手動策略，請執行步驟12到步驟19;否則，請跳過步驟20。



步驟12.在SPI-Incoming欄位中，為VPN連線上的傳入流量的安全引數索引(SPI)標籤輸入三到八個十六進位制字元。SPI標籤用於區分一個會話的流量和其他會話的流量。

步驟13.在SPI-Outgoing欄位中，為VPN連線上的傳出流量的SPI標籤輸入三到八個十六進位制字元。

步驟14.從Encryption Algorithm下拉選單中，選擇一個選項。

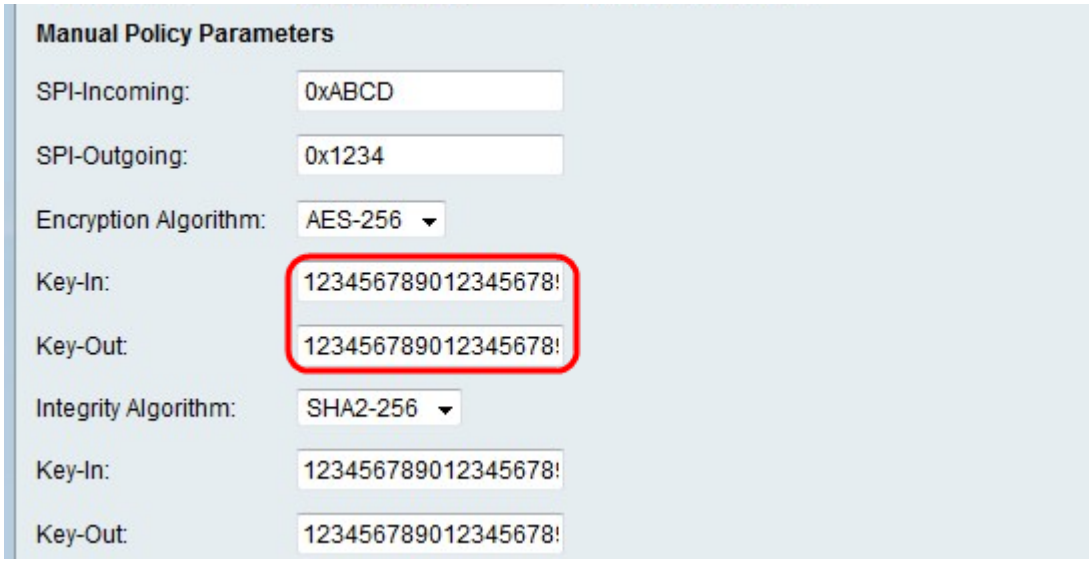
·DES — 資料加密標準(DES)是一種56位舊加密方法，它不是非常安全的加密方法，但為了向後相容，可能需要這種加密方法。

·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15.在Key-In欄位中，輸入入站策略的金鑰。金鑰長度取決於步驟14中選擇的演算法。

·DES使用8個字元的金鑰。

·3DES使用24個字元的金鑰。

·AES-128使用12個字元的金鑰。

·AES-192使用24個字元的金鑰。

·AES-256使用32個字元的金鑰。

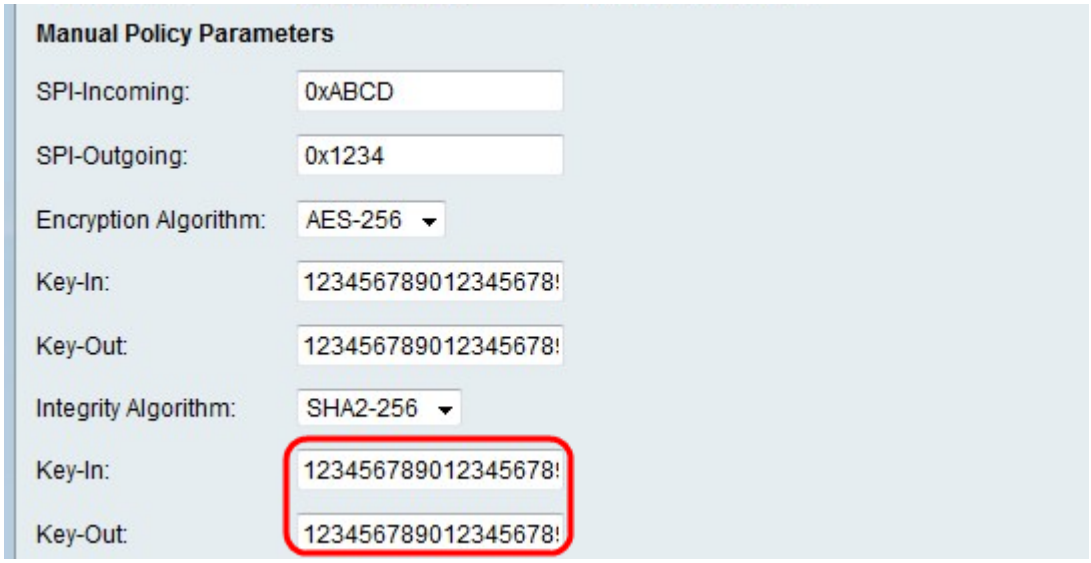
步驟16.在Key-Out欄位中，輸入傳出策略的金鑰。金鑰長度取決於步驟14中選擇的演算法。金鑰長度與步驟15相同。

步驟17.從Integrity Algorithm下拉選單中，選擇一個選項。

·MD5 — 消息摘要演算法5(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 — 安全雜湊函式1(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 — 具有256位雜湊值(SHA2-256)的安全雜湊演算法2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。



步驟18.在Key-In欄位中，輸入入站策略的金鑰。金鑰長度取決於步驟17中選擇的演算法。

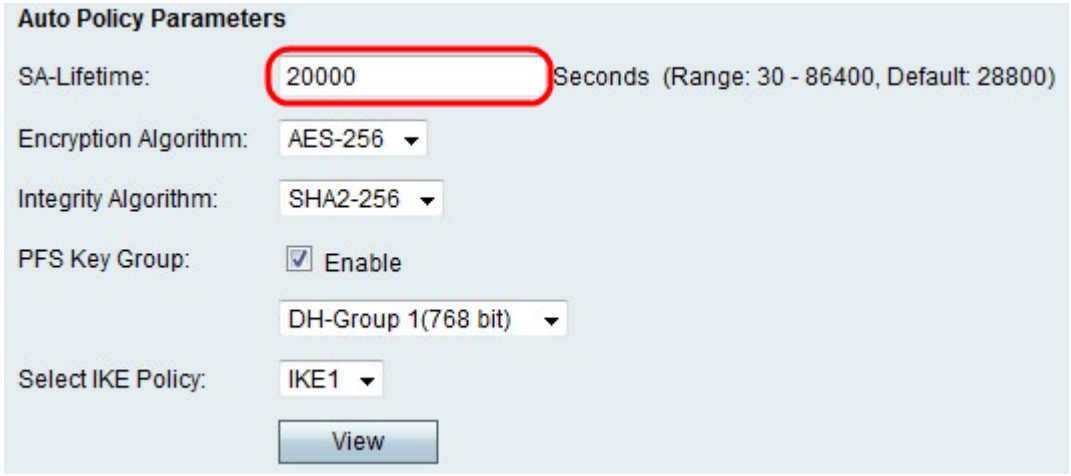
·MD5使用16個字元的金鑰。

·SHA-1使用20個字元的金鑰。

·SHA2-256使用32個字元的金鑰。

步驟19.在Key-Out欄位中，輸入傳出策略的金鑰。金鑰長度取決於步驟17中選擇的演算法。金鑰長度與步驟18相同。

附註：如果您在步驟3中選擇了Auto Policy，請執行步驟20到步驟25;否則，請跳至步驟26。



步驟20.在SA-Lifetime欄位中，輸入SA在續訂之前的持續時間（以秒為單位）。

步驟21.從Encryption Algorithm下拉選單中，選擇一個選項。

·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22.從Integrity Algorithm下拉選單中，選擇一個選項。

·MD5 — 消息摘要演算法5(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 — 安全雜湊函式1(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 — 具有256位雜湊值(SHA2-256)的安全雜湊演算法2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。

步驟23.選中PFS金鑰組中的**Enable**覈取方塊以啟用完全向前保密(PFS)。PFS提高了VPN安全性，但降低了連線速度。

步驟24。（可選）如果您選擇在步驟23中啟用PFS，請為以下下拉選單選擇要加入的Diffie-Hellman(DH)組。組編號越高，組越安全。

步驟25.從Select IKE Policy下拉選單中，選擇要用於VPN策略的IKE策略。

附註：如果按一下**檢視**，則會將您引導到*Advanced VPN Setup*頁面的IKE配置部分。

步驟26.按一下**「Save」**。*系統將重新顯示原始Advanced VPN Setup*頁面。

步驟27.按一下**「Save」**。