

在RV016、RV042、RV042G和RV082 VPN路由器上配置網關VPN

目標

虛擬專用網路(VPN)用於通過公共或共用Internet通過所謂的VPN隧道在兩個端點之間建立安全連線。更具體地說，網關到網關VPN連線允許兩個路由器安全地彼此連線，並且一端上的客戶端在邏輯上顯示為像是另一端網路的一部分。這使資料和資源能夠更輕鬆、更安全地通過Internet共用。

必須在兩台路由器上完成配置，才能啟用網關到網關VPN。在兩台路由器之間應顛倒在Local Group Setup和Remote Group Setup部分中完成的配置，以便其中一個的本地組成為另一個的遠端組。

本文檔的目的是解釋如何在RV016、RV042、RV042G和RV082 VPN系列路由器上配置網關到網關VPN。

適用裝置

- RV016
- RV042
- RV042G
- RV082

軟體版本

- v4.2.2.08

配置網關到網關VPN

步驟 1. 登入路由器配置實用程式並選擇VPN > Gateway to Gateway。Gateway to Gateway頁面隨即開啟：

Gateway To Gateway

Add a New Tunnel

Tunnel No.	2
Tunnel Name :	<input type="text"/>
Interface :	WAN1 <input type="button" value="v"/>
Enable :	<input checked="" type="checkbox"/>

Local Group Setup

Local Security Gateway Type :	IP Only <input type="button" value="v"/>
IP Address :	0.0.0.0
Local Security Group Type :	Subnet <input type="button" value="v"/>
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

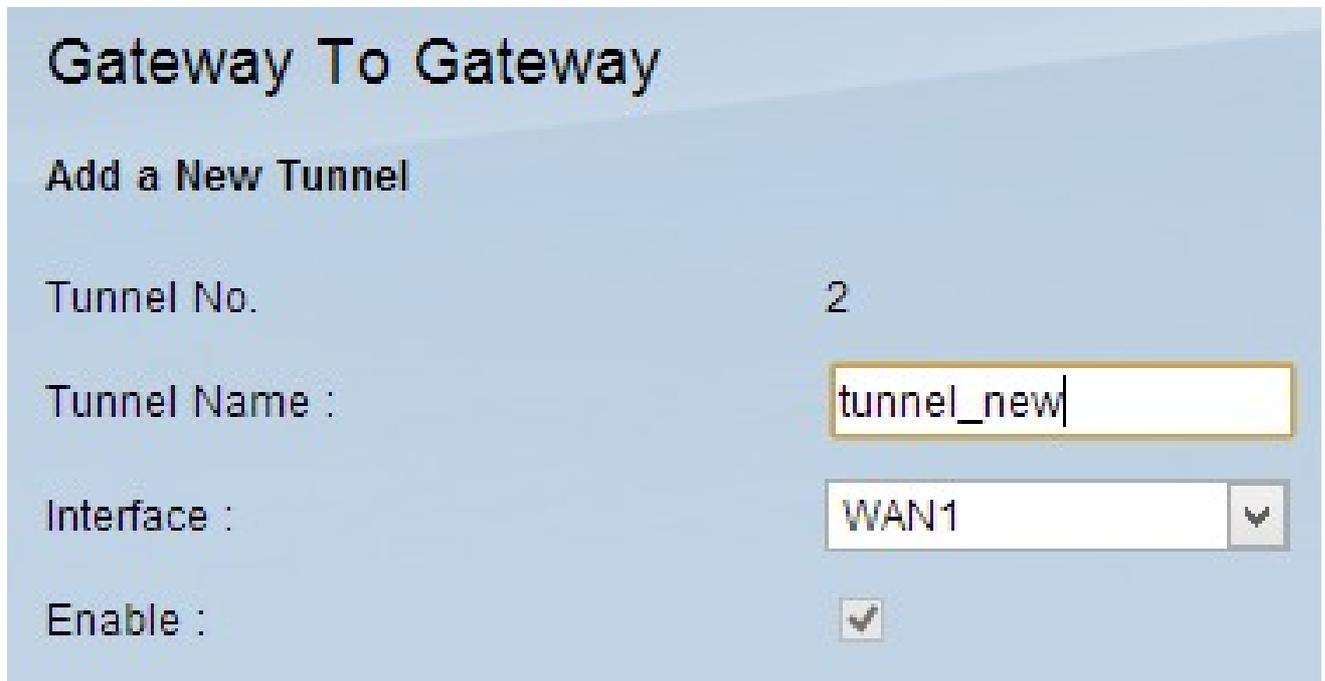
Remote Group Setup

Remote Security Gateway Type :	IP Only <input type="button" value="v"/>
<input type="button" value="v"/> IP Address :	<input type="text"/>
Remote Security Group Type :	Subnet <input type="button" value="v"/>
IP Address :	<input type="text"/>
Subnet Mask :	255.255.255.0

要配置網關到網關VPN，需要配置以下功能：

1. [新增通道](#)
2. [本地組設定](#)
3. [遠程組設定](#)
4. [IPSec設定](#)

新增新隧道



Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name : tunnel_new

Interface : WAN1

Enable :

隧道號是一個只讀欄位，顯示要建立的當前隧道。

步驟 1. 在 Tunnel Name 欄位中輸入 VPN 隧道的名稱。它不必與通道另一端使用的名稱相匹配。

步驟 2. 從 Interface 下拉選單中，選擇要用於隧道的廣域網(WAN)埠。

- WAN1 - RV0XX 系列 VPN 路由器的專用 WAN 埠。
- WAN2 - RV0XX 系列 VPN 路由器的 WAN2/DMZ 埠。僅當將其配置為 WAN 而不是非軍事區 (DMZ) 埠時，才會顯示在下拉選單中。

步驟 3. (可選) 要啟用 VPN，請選中 Enable 欄位中的覈取方塊。預設情況下，VPN 處於啟用狀態。

本地組設定

注意：一台路由器上本地組設定的配置應與另一台路由器上遠端組設定的配置相同。

Gateway To Gateway

Add a New Tunnel

Tunnel No.	2
Tunnel Name :	<input type="text" value="tunnel_new"/>
Interface :	<input type="text" value="WAN1"/> ▼
Enable :	<input checked="" type="checkbox"/>

Local Group Setup

Local Security Gateway Type :	<input type="text" value="IP Only"/> ▼
IP Address :	0.0.0.0
Local Security Group Type :	<input type="text" value="Subnet"/> ▼
IP Address :	<input type="text" value="192.168.1.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>

步驟 1. 從Local Security Gateway Type下拉選單中選擇相應的路由器標識方法以建立VPN隧道。

· 僅IP — 本地路由器 (此路由器) 由靜態IP地址識別。僅當路由器具有靜態WAN IP時才能選擇此選項。靜態WAN IP地址會自動顯示在IP地址欄位中。

· 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地址會自動顯示在IP地址欄位中。

· 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「電子郵件地址」欄位中輸入電子郵件地址。靜態WAN IP地址會自動顯示在IP地址欄位中。

· 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 + 郵件地址 (使用者FQDN) 身份驗證 — 通過動態IP地址和電子郵件地址可以訪問隧道。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. 從Local Security Group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LAN裝置可以訪問VPN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。
- 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裝置的子網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，請在開始IP和結束IP欄位中分別輸入開始和結束IP地址。

步驟 3.按一下「Save」以儲存設定。

遠端組設定

注意：一台路由器上遠端組設定的配置應與另一台路由器上本地組設定的配置相同。

The screenshot shows a configuration interface with two sections: 'Local Group Setup' and 'Remote Group Setup'. The 'Remote Group Setup' section is enclosed in a red border.

Local Group Setup	
Local Security Gateway Type :	IP + Email Address(USER FQDN) Authentication
Email Address :	abcd @ mail.com
IP Address :	0.0.0.0
Local Security Group Type :	IP
IP Address :	192.168.1.1

Remote Group Setup	
Remote Security Gateway Type :	IP Only
IP Address :	
Remote Security Group Type :	Subnet
IP Address :	
Subnet Mask :	255.255.255.0

步驟 1.從Remote Security Gateway Type下拉選單中，選擇用於識別遠端路由器以建立

VPN隧道的方法。

- 僅IP — 可通過靜態WAN IP訪問隧道。如果您知道遠端路由器的IP地址，請從Remote Security Gateway Type欄位正下方的下拉選單中選擇IP地址並輸入IP地址。如果您不知道IP地址，但知道域名，請選擇IP by DNS Resolved (按DNS解析IP)，並在IP by DNS Resolved (按DNS解析IP) 欄位中輸入路由器的域名。

- IP +域名(FQDN)身份驗證 — 可以通過路由器的靜態IP地址和註冊域訪問隧道。如果您知道遠端路由器的IP地址，請在Remote Security Gateway Type欄位正下方下拉選單中選擇IP地址並輸入地址。如果您不知道IP地址，但知道域名，請選擇IP by DNS Resolved (按DNS解析IP)，並在IP by DNS Resolved (按DNS解析IP) 欄位中輸入路由器的域名。在Domain Name欄位中輸入路由器的域名，而不管您選擇用哪種方法標識路由器。

- IP +郵件地址 (使用者FQDN) 身份驗證 — 可通過靜態IP地址和電子郵件地址訪問隧道。如果您知道遠端路由器的IP地址，請在Remote Security Gateway Type欄位正下方下拉選單中選擇IP地址並輸入地址。如果您不知道IP地址，但知道域名，請選擇IP by DNS Resolved (按DNS解析IP)，並在IP by DNS Resolved (按DNS解析IP) 欄位中輸入路由器的域名。在「電子郵件地址」欄位中輸入電子郵件地址。

- 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 +郵件地址 (使用者FQDN) 身份驗證 — 通過動態IP地址和電子郵件地址可以訪問隧道。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. 從Remote Security Group Type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。

- 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。

- 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，請在IP地址和子網掩碼欄位中分別輸入LAN裝置的子網IP地址和子網掩碼。

- IP範圍 — 一系列LAN裝置可以訪問隧道。如果選擇此選項，請在開始IP和結束IP欄位中分別輸入開始和結束IP地址。

注意：通道兩端的路由器不能位於同一個子網中。

步驟 3. 按一下「Save」以儲存設定。

IPSec設定

IPSec Setup

Keying Mode :	IKE with Preshared key	▼
Phase 1 DH Group :	Group 1 - 768 bit	▼
Phase 1 Encryption :	DES	▼
Phase 1 Authentication :	MD5	▼
Phase 1 SA Life Time :	28800	seconds
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>	
Phase 2 DH Group :	Group 1 - 768 bit	▼
Phase 2 Encryption :	DES	▼
Phase 2 Authentication :	MD5	▼
Phase 2 SA Life Time :	3600	seconds
Preshared Key :	<input type="text"/>	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/>	Enable
Preshared Key Strength Meter :		
<input type="button" value="Advanced +"/>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

網際網路通訊協定安全(IPSec)是一種網際網路層安全通訊協定，可在任何通訊作業階段期間透過驗證和加密提供端對端安全。

注意：VPN的兩端都需要使用相同的加密、解密和身份驗證方法才能正常工作。為兩台路由器輸入相同的IPSec設定設定。

IPSec Setup

Keying Mode :	<div style="border: 2px solid red; padding: 2px;"><div style="border: 1px solid gray; padding: 2px;">IKE with Preshared key ▼</div><div style="border: 1px solid gray; padding: 2px;">Manual</div><div style="border: 1px solid gray; padding: 2px; background-color: #0070C0; color: white;">IKE with Preshared key</div></div>
Phase 1 DH Group :	
Phase 1 Encryption :	DES ▼
Phase 1 Authentication :	MD5 ▼
Phase 1 SA Life Time :	<input type="text" value="28800"/> seconds
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>
Phase 2 DH Group :	Group 1 - 768 bit ▼
Phase 2 Encryption :	DES ▼
Phase 2 Authentication :	MD5 ▼
Phase 2 SA Life Time :	<input type="text" value="3600"/> seconds
Preshared Key :	<input type="text"/>
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/> Enable
Preshared Key Strength Meter :	<div style="border: 1px solid gray; width: 100%; height: 15px; background-color: #D3D3D3;"><div style="width: 20%; height: 100%; background-color: red;"></div></div>

步驟 1.從Keying Mode下拉選單中選擇相應的金鑰管理模式以確保安全性。預設模式為IKE，使用預共用金鑰。

- [手動](#) — 一種自定義安全模式，用於由您自己生成新的安全金鑰，並且不與金鑰協商。在排除故障和小型靜態環境中使用它最好。
- [使用預共用金鑰的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身份驗證通訊。

手動鍵控模式的IPSec設定

IPSec Setup

Keying Mode :	Manual
Incoming SPI :	101
Outgoing SPI :	101
Encryption :	DES
Authentication :	MD5
Encryption Key :	
Authentication Key :	

步驟 1. 在Incoming SPI欄位中輸入傳入安全引數索引(SPI)的唯一十六進位制值。SPI在封裝安全負載協定(ESP)報頭中傳輸，並確定對傳入資料包的保護。您可以輸入一個介於100到ffffff之間的值。本地路由器的傳入SPI必須與遠端路由器的傳出SPI匹配。

步驟 2. 在Outgoing SPI欄位中輸入傳出安全引數索引(SPI)的唯一十六進位制值。您可以輸入一個介於100到ffffff之間的值。遠端路由器的傳出SPI需要與本地路由器的傳入SPI匹配。

注意：兩個隧道不能具有相同的SPI。

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :
DES
3DES

Authentication :

Encryption Key :

Authentication Key :

步驟 3. 從Encryption下拉選單中選擇資料的適當加密方法。推薦的加密是3DES。VPN隧道需要在兩端使用相同的加密方法。

- DES — 資料加密標準(DES)使用56位金鑰大小進行資料加密。DES已過時，應僅在一個終端僅支援DES的情況下使用。
- 3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法。3DES對資料進行三次加密，比DES具有更高的安全性。

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :
MD5
SHA1

Encryption Key :

Authentication Key :

步驟 4. 從Authentication下拉選單中選擇資料的相應身份驗證方法。推薦的身份驗證是SHA1，因為它比MD5更安全。VPN隧道需要為兩端使用相同的身份驗證方法。

- MD5 — 消息摘要演算法5(MD5)是一個128位雜湊函式，通過計算校驗和來保護資料免受惡意攻擊。
- SHA1 — 安全雜湊演算法版本1(SHA1)是一個160位元的雜湊函式，比MD5更安全，但計算時間更長。

IPSec Setup

Keying Mode : Manual

Incoming SPI : 101

Outgoing SPI : 101

Encryption : 3DES

Authentication : SHA1

Encryption Key : acb1230000000000 ab456fbc00000000 87600bca00000000

Authentication Key : acbd123400000000000000000000000000000000

步驟 5. 在Encryption Key欄位中輸入要加密和解密資料的金鑰。如果您在步驟3中選擇DES作為加密方法，請輸入一個16位的十六進位制值。如果您在步驟3中選擇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SHA1作為身份驗證方法，請輸入40位十六進位制值。如果沒有新增足夠的數字，則在數字足夠之前會附加零。VPN隧道需要為兩端使用相同的預共用金鑰。

步驟 7. 按一下「Save」以儲存設定。

使用預共用金鑰模式配置的IKE

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 1 - 768 bit
Phase 1 Encryption :	Group 1 - 768 bit
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>
Phase 2 DH Group :	Group 1 - 768 bit
Phase 2 Encryption :	DES
Phase 2 Authentication :	MD5
Phase 2 SA Life Time :	3600 seconds
Preshared Key :	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/> Enable
Preshared Key Strength Meter :	

步驟 1.從Phase 1 DH Group下拉選單中選擇適當的階段1 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)是一種加密金鑰交換協定，用於在第1階段確定金鑰的強度，並且它還共用金鑰以驗證通訊。

·組1 - 768位 — 強度最低的金鑰和最不安全的身份驗證組，但計算IKE金鑰所需的時間最少。如果網路速度低，則首選此選項。

·組2 - 1024位 — 比組1的強度更高、身份驗證組更安全，但計算IKE金鑰需要更多時間。

·組5 - 1536位 — 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。

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : **DES**

Phase 1 Authentication :

Phase 1 SA Life Time :

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

步驟 2. 從Phase 1 Encryption下拉選單中選擇適當的Phase 1 Encryption以加密金鑰。建議使用AES-128、AES-192或AES-256。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)使用56位金鑰大小進行資料加密。DES已過時，應僅在一個終端僅支援DES的情況下使用。
- 3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法。3DES對資料進行三次加密，比DES具有更高的安全性。
- AES-128 — 高級加密標準(AES)是128位加密方法，它通過10個循環重複將純文字檔案轉換為加密文本。

· AES-192 — 高級加密標準(AES)是192位加密方法，它通過12個循環重複將純文字檔案轉換為加密文本。AES-192比AES-128更安全。

· AES-256 — 高級加密標準(AES)是256位加密方法，它通過14個循環重複將純文字檔案轉換為加密文本。AES-256是最安全的加密方法。

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 2 - 1024 bit
Phase 1 Encryption :	3DES
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>
Phase 2 DH Group :	Group 1 - 768 bit
Phase 2 Encryption :	DES
Phase 2 Authentication :	MD5
Phase 2 SA Life Time :	3600 seconds
Preshared Key :	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/> Enable
Preshared Key Strength Meter :	

步驟 3.從Phase 1 Authentication下拉選單中選擇相應的階段1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。建議使用SHA1。

· MD5 — 消息摘要演算法-5(MD5)是一個128位的雜湊函式，通過計算校驗和來保護資料免受惡意攻擊。

· SHA1 — 安全雜湊演算法版本1(SHA1)是一個160位元的雜湊函式，比MD5更安全，但計算時間更長。

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

步驟 4.在Phase 1 SA Life Time欄位中輸入階段1金鑰有效和VPN隧道保持活動狀態的時間量 (以秒為單位)。

步驟 5.選中Perfect Forward Secrecy覈取方塊以對金鑰提供更多保護。此選項允許路由器在任一金鑰受損時生成新金鑰。加密資料僅通過被洩露的金鑰被洩露。這是推薦的操作，因為它提供了更高的安全性。

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 2 - 1024 bit
Phase 1 Encryption :	3DES
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	27800 seconds
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>
Phase 2 DH Group :	Group 1 - 768 bit
Phase 2 Encryption :	Group 1 - 768 bit
Phase 2 Authentication :	MD5
Phase 2 SA Life Time :	3600 seconds
Preshared Key :	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/> Enable
Preshared Key Strength Meter :	

步驟 6. 從Phase 2 DH Group下拉選單中選擇適當的第2階段DH組。階段2使用安全關聯，用於確定資料包經過兩個端點時的安全性。

·組1 - 768位 — 強度最低的金鑰和最不安全的身份驗證組，但計算IKE金鑰所需的時間最少。如果網路速度低，則首選此選項。

·組2 - 1024位 — 比組1的強度更高、身份驗證組更安全，但計算IKE金鑰需要更多時間。

·組5 - 1536位 — 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。

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 2 - 1024 bit
Phase 1 Encryption :	3DES
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	27800 seconds
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>
Phase 2 DH Group :	Group 2 - 1024 bit
Phase 2 Encryption :	DES
Phase 2 Authentication :	
Phase 2 SA Life Time :	
Preshared Key :	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/> Enable
Preshared Key Strength Meter :	

步驟 7. 從Phase 2 Encryption下拉選單中選擇適當的Phase 2 Encryption以加密金鑰。建議使用AES-128、AES-192或AES-256。VPN通道的兩端需要使用相同的加密方法。

- NULL — 未使用加密。
- DES — 資料加密標準(DES)使用56位金鑰大小進行資料加密。DES已過時，應僅在一個終端僅支援DES的情況下使用。
- 3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法。3DES對資料進行三次加密，比DES具有更高的安全性。

· AES-128 — 高級加密標準(AES)是128位加密方法，它通過10個循環重複將純文字檔案轉換為加密文本。

· AES-192 — 高級加密標準(AES)是192位加密方法，它通過12個循環重複將純文字檔案轉換為加密文本。AES-192比AES-128更安全。

· AES-256 — 高級加密標準(AES)是256位加密方法，它通過14個循環重複將純文字檔案轉換為加密文本。AES-256是最安全的加密方法。

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 2 - 1024 bit
Phase 1 Encryption :	3DES
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	27800 seconds
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>
Phase 2 DH Group :	Group 2 - 1024 bit
Phase 2 Encryption :	DES
Phase 2 Authentication :	MD5
Phase 2 SA Life Time :	
Preshared Key :	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/> Enable
Preshared Key Strength Meter :	

步驟 8.從Phase 2 Authentication下拉選單中選擇相應的身份驗證方法。VPN隧道需要為兩端使用相同的身份驗證方法。建議使用SHA1。

- MD5 — 消息摘要演算法5(MD5)是一個128位十六進位制雜湊函式，通過計算校驗和來保護資料免受惡意攻擊。
- SHA1 — 安全雜湊演算法版本1(SHA1)是一個160位元的雜湊函式，比MD5更安全，但計算時間更長。
- Null — 不使用身份驗證方法。

IPSec Setup

Keying Mode :	IKE with Preshared key	▼
Phase 1 DH Group :	Group 2 - 1024 bit	▼
Phase 1 Encryption :	3DES	▼
Phase 1 Authentication :	MD5	▼
Phase 1 SA Life Time :	27800	seconds
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>	
Phase 2 DH Group :	Group 2 - 1024 bit	▼
Phase 2 Encryption :	DES	▼
Phase 2 Authentication :	SHA1	▼
Phase 2 SA Life Time :	3700	seconds
Preshared Key :	abcd1234	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/> Enable	
Preshared Key Strength Meter :		

步驟 9. 在Phase 2 SA Life Time欄位中輸入階段2金鑰有效和VPN隧道保持活動狀態的時間量 (以秒為單位)。

步驟 10. 在Preshared Key欄位中輸入之前在IKE對等體之間共用的金鑰，以對對等體進行身份驗證。最多可使用30個十六進位制和字元作為預共用金鑰。VPN隧道的兩端需要使用相同的預共用金鑰。

注意：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11。（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。它用於通過色條確定預共用金鑰的強度。

·預共用金鑰強度計 — 這顯示通過彩色條形的預共用金鑰的強度。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 12. 按一下「Save」以儲存設定。

注意：如果要配置Advanced部分中可用的網關到網關VPN的選項，請參閱[在RV016、RV042、RV042G和RV082 VPN路由器上配置網關到網關VPN的高級設定](#)。

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）。