

# 在RV110W防火牆上配置高級虛擬專用網路 (VPN)設定

## 目標

虛擬專用網路(VPN)使用公共網路或Internet建立專用網路以進行安全通訊。Internet金鑰交換(IKE)是在兩個網路之間建立安全通訊的協定。它用於在流量流之前交換金鑰，確保VPN隧道兩端的真實性。

VPN的兩端應遵循相同的VPN策略以成功相互通訊。

本文檔的目的是解釋如何在RV110W無線路由器上新增IKE配置檔案和配置VPN策略。

## 適用裝置

·RV110W

## 軟體版本

·1.2.0.9

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

IKE Policy Table							
<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
Add Row							
Edit							
Delete							

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
Add Row							
Edit							
Enable							
Disable							
Delete							

Save Cancel

IPSec Connection Status

Advanced VPN Setup

IKE Policy Table				
<input type="checkbox"/>	Name	Mode	Local	Remote
No data to display				
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

VPN Policy Table				
<input type="checkbox"/>	Status	Name	Type	Local
No data to display				
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>				

步驟2. 按一下Add Row建立新的IKE策略。Advanced VPN Setup頁面開啟：

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:  ▼

**IKE SA Parameters**

Encryption Algorithm:  ▼

Authentication Algorithm:  ▼

Pre-Shared Key:

Diffie-Hellman (DH) Group:  ▼

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

步驟3. 在Policy Name欄位中，輸入IKE策略的名稱，以便輕鬆識別。

### Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode: Main  
Main  
Aggressive

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

步驟4.從Exchange Mode下拉式清單中選擇一個選項：

·主要 — 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 — 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。

。

**Advanced VPN Setup**

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:  (Dropdown menu showing: AES-128, DES, 3DES, AES-128, AES-192, AES-256)

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

步驟5.從*Encryption Algorithm*下拉式清單中選擇一個演演算法：

·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)執行DES三次，但金鑰大小從168位變為112位，從112位變為56位，具體取決於所執行的DES循環。3DES比DES和AES更安全。

·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比3DES更快，但安全性較低，但某些型別的硬體使3DES更快。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，而AES-192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。

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

步驟6.從*Authentication Algorithm* 下拉式清單中選擇所需的驗證：

- 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。

**Advanced VPN Setup**

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

**Pre-Shared Key:**

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

步驟7.在Pre-Shared Key欄位中，輸入IKE策略使用的預共用金鑰。

**Advanced VPN Setup**

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

步驟8.從Diffie-Hellman(DH)Group下拉清單中，選擇IKE使用的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。

·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金鑰所需的時間更短。如果網路速度低，則首選此選項。

·組2 - 1024位 — 強度更高的金鑰和更安全的身份驗證組。但需要一些時間來計算IKE金鑰。

·組5 - 1536位 — 表示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。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

步驟9.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10。（可選）選中Dead Peer Detection欄位中的Enable覈取方塊以啟用Dead Peer Detection。Dead Peer Detection監控IKE對等體以檢視對等體是否停止工作。失效對等體檢測可防止非活動對等體上浪費網路資源。

步驟11。（可選）如果在步驟9中啟用了「契據對等體檢測」，請在「契據對等體延遲」欄位中輸入檢查對等體活動的頻率(以秒為單位)。

步驟12。（可選）如果您已在步驟9中啟用Dead Peer Detection，請在「Dead Peer Detection Timeout」欄位中輸入在刪除非活動對等體之前等待的秒數。

步驟13.按一下Save以套用所有設定。

## VPN策略配置

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

**Advanced VPN Setup**

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						

Add Row Edit Delete


<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

**Advanced VPN Setup**

 Configuration settings have been saved successfully

<input type="checkbox"/>	Name	Mode	Local	Remote
<input type="checkbox"/>	policy1	Aggressive		

Add Row Edit Delete

<input type="checkbox"/>	Status	Name	Type	Local
<input type="checkbox"/>	No data to display			

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

步驟2.按一下VPN Policy Table中的Add Row。出現Advanced VPN Policy Setup視窗：

**Advanced VPN Setup**

**Add / Edit VPN Policy Configuration**

Policy Name:

Policy Type:  ▼

Remote Endpoint:  ▼

(Hint: 1.2.3.4 or abc.com)

**Local Traffic Selection**

Local IP:  ▼

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

**Remote Traffic Selection**

Remote IP:  ▼

IP Address:  (Hint: 1.2.3.4)



## 新增/編輯VPN策略配置

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

步驟1.在 *Policy Name* 欄位中輸入策略的唯一名稱以輕鬆識別。

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

步驟2.從 *Policy Type* 下拉選單中選擇適當的策略型別。

- 自動策略 — 可以自動設定引數。在這種情況下，除了策略之外，還要求IKE ( Internet金鑰交換 ) 協定在兩個VPN端點之間進行協商。
- 手動策略 — 在這種情況下，包括用於VPN隧道的金鑰設定的所有設定都會為每個端點手動輸入。

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

步驟3.從 *Remote Endpoint* 下拉選單中選擇用於標識遠端端點處的網關的IP識別符號型別。

- IP地址 — 遠端終端上網關的IP地址。如果選擇此選項，請在欄位中輸入IP地址。
- FQDN ( 完全限定域名 ) — 輸入遠端終結點上網關的完全限定域名。如果選擇此選項，請在提供的欄位中輸入完全限定域名。

## 本地流量選擇

**Local Traffic Selection**

Local IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

步驟1.從Local IP (本地IP) 下拉選單中選擇要為終端提供的標識符型別。

**Local Traffic Selection**

Local IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

·Single — 這將策略限制為一個主機。如果選擇此選項，請在IP地址欄位中輸入IP地址。

**Local Traffic Selection**

Local IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

·子網 — 這是定義IP邊界的掩碼。這僅允許來自指定子網的主機連線到VPN。要連線到VPN，電腦由邏輯AND操作選擇。如果IP處於所需的相同範圍，則選擇電腦。如果選擇此選項，請在IP地址和子網欄位中輸入IP地址和子網。

## Remote Traffic選擇

**Remote Traffic Selection**

Remote IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

步驟1.從本地IP下拉選單中選擇要為端點提供的識別符號型別：

**Remote Traffic Selection**

Remote IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

·Single — 這將策略限制為一個主機。如果選擇此選項，請在IP地址欄位中輸入IP地址。

Remote Traffic Selection		
Remote IP:	Subnet ▼	
IP Address:	192.168.1.5	(Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)

子網 — 這是定義IP邊界的掩碼。這僅允許來自指定子網的主機連線到VPN。要連線到VPN，電腦由邏輯AND操作選擇。如果IP處於所需的相同範圍，則選擇電腦。如果選擇此選項，請在IP地址和子網欄位中輸入IP地址和子網。

## 手動策略引數

要配置Manual Policy Parameters，請從Add/Edit VPN Policy Configuration部分的Policy Type下拉選單中選擇Manual Policy。

Manual Policy Parameters	
SPI-Incoming:	014C
SPI-Outgoing:	014C
Encryption Algorithm:	AES-128 ▼
Key-In:	
Key-Out:	
Integrity Algorithm:	SHA-1 ▼
Key-In:	
Key-Out:	

步驟1。在SPI-Incoming欄位中輸入一個介於3和8之間的十六進位制值。狀態包檢測(SPI)是一種稱為深度包檢測的技術。SPI實施了多種安全功能，有助於確保電腦網路的安全。SPI-Incoming值對應於上一裝置的SPI-Outgoing。如果遠端VPN終端在其SPI-Outgoing欄位中具有相同的值，則任何值都是可接受的。

步驟2。在SPI-Outgoing欄位中輸入一個介於3和8之間的十六進位制值。

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm: 


- 3DES
- DES
- AES-128
- AES-192
- AES-256

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

步驟3.從Encryption Algorithm下拉選單中選擇適當的加密演算法。

·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)執行3次DES，但根據執行的DES循環將金鑰大小從168位變為112位，從112位變為56位。3DES比DES和AES更安全。

·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比3DES更快，但安全性較低，但某些型別的硬體使3DES更快。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，而AES-192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。

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

步驟4.在Key-In欄位中輸入入站策略的加密金鑰。金鑰的長度取決於步驟3中選擇的演算法。

步驟5.在Key-Out欄位中輸入出站策略的加密金鑰。

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm: 

- AES-128
- 3DES
- DES
- AES-128
- AES-192
- AES-256

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

步驟6.從 *Integrity Algorithm* 下拉選單中選擇相應的完整性演算法。此演算法將驗證資料的完整性：

·MD5 — 此演算法將金鑰長度指定為16個字元。Message-Digest Algorithm 5(MD5)不防衝突，適用於依賴此屬性的SSL憑證或數位簽章等應用程式。MD5將任何位元組流壓縮為128位值，但SHA將其壓縮為160位值。MD5的計算成本略低，但是MD5是雜湊演算法的較舊版本，易受衝突攻擊。

·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。

·SHA2-256 — 此演算法將金鑰長度指定為32個字元。

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

步驟7.為入站策略輸入完整性金鑰（對於具有完整性模式的ESP）。金鑰的長度取決於步驟6中選擇的演算法。

步驟8.在Key-Out欄位中輸入出站策略的完整性金鑰。VPN連線設定為出站到入站，因此一端的出站金鑰需要與另一端的入站金鑰匹配。

**附註：**SPI傳入和傳出、加密演算法、完整性演算法和金鑰在VPN隧道的另一端需要相同，才能成功連線。

## 自動策略引數

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group:  Enable  
DH-Group 1(768 bit)

Select IKE Policy: policy1

View

步驟1.在SA Lifetime欄位中輸入安全關聯(SA)的持續時間 (以秒為單位)。SA生存期是當任何金鑰達到其生存期時，任何關聯的SA都會自動重新協商。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group:  Enable  
DH-Group 1(768 bit)

Select IKE Policy: policy1

View

步驟2.從Encryption Algorithm下拉選單中選擇適當的加密演算法：

- 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)執行3次DES，但根據執行的DES循環將金鑰大小從168位變為112位，從112位變為56位。3DES比DES和AES更安全。
- 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比3DES更快，但安全性較低，但某些型別的硬體使3DES更快。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，而AES-192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。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group: SHA2-256, MD5

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

步驟3.從「完整性演算法」下拉選單中選擇相應的完整性演算法。該演算法驗證資料的完整性。

·MD5 — 此演算法將金鑰長度指定為16個字元。Message-Digest Algorithm 5(MD5)不防衝突，適用於依賴此屬性的SSL憑證或數位簽章等應用程式。MD5將任何位元組流壓縮為128位值，但SHA將其壓縮為160位值。MD5的計算成本略低，但是MD5是雜湊演算法的較舊版本，易受衝突攻擊。

·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。

·SHA2-256 — 此演算法將金鑰長度指定為32個字元。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

步驟4. (可選) 選中 *PFS Key Group* 欄位中的 **Enable** 覆取方塊以啟用 Perfect Forward Secrecy，這樣可以提高安全性。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

Select IKE Policy: **DH-Group 1(768 bit)**  
DH-Group 2(1024 bit)  
DH-Group 5(1536 bit)

View

步驟5.如果您在步驟4中選中了**Enable**，請從**PFS Key Group**欄位下拉式清單中選擇適當的Diffie-Hellman金鑰交換。

·組1 - 768位 — 表示強度最低的金鑰和最不安全的身份驗證組。但計算IKE金鑰所需的時間更少。如果網路速度低，則優先使用。

·組2 - 1024位 — 代表強度更高的金鑰和更安全的身份驗證組。但需要一些時間來計算IKE金鑰。

·組5 - 1536位 — 表示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。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: **policy1**  
policy1

view

步驟6.從選擇**IKE策略**下拉選單中選擇適當的IKE策略。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)。要使VPN正常工作，兩個端點的IKE策略應相同。

步驟7.按一下**Save**以套用所有設定。

**附註：**SA -Lifetime、加密演算法、完整性演算法、PFS金鑰組和IKE策略在VPN隧道的另一端需要相同才能成功連線。

如果您想檢視RV110W上的更多文章，請按一下[此處](#)。