

在RV130或RV130W路由器上配置高級虛擬專用網路(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。站點到站點(網關到網關)VPN將整個網路相互連線，通過在公共域(也稱為Internet)上建立隧道來維護安全性。每個站點只需要到同一公共網路的本地連線，從而節省了長私人租用線-的費用。

VPN具有高度可擴充性，簡化了網路拓撲，並通過減少遠端使用者的旅行時間和成本提高了工作效率，因此對公司有利。

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。此安全連線稱為安全關聯(SA)。您可以建立IKE策略來定義在此過程中要使用的安全引數，例如對等體的身份驗證、加密演算法等。要使VPN正常工作，兩個端點的IKE策略應相同。

本文旨在展示如何在RV130或RV130W路由器上配置高級VPN設定，其中涵蓋IKE策略設定和VPN策略設定。

適用裝置

- RV130
- RV130W

軟體版本

- 1.0.3.22

配置高級VPN設定

新增/編輯Internet金鑰交換(IKE)策略設定

步驟1.登入到基於Web的實用程式，然後選擇VPN > Site-to-Site IPSec VPN >Advanced VPN Setup。

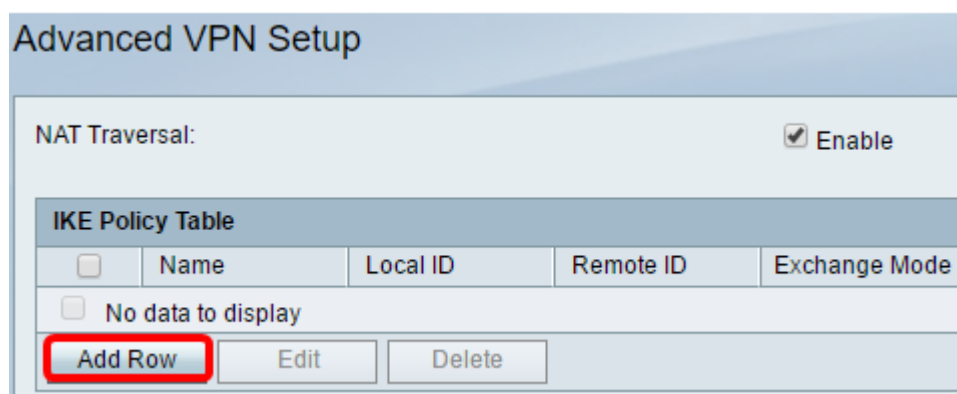


步驟2. (可選) 如果要為VPN連線啟用網路地址轉換(NAT)遍歷，請選中NAT遍歷中的Enable 覈取方塊。NAT遍歷允許在使用NAT的網關之間建立VPN連線。如果VPN連線通過啟用了NAT的網關，請選擇此選項。



步驟3.在IKE策略表中，按一下Add Row以建立新的IKE策略。

附註：如果已配置基本設定，則下表將包含建立的基本VPN設定。可以通過選中策略的覈取方塊並按一下Edit來編輯現有的IKE策略。「高級VPN設定」頁面將更改：



步驟4.在IKE名稱欄位中，輸入IKE策略的唯一名稱。

附註：如果已配置基本設定，則建立的連線名稱將設定為IKE名稱。在本示例中，VPN1是選定的IKE名稱。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

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

Dead Peer Detection: Enable

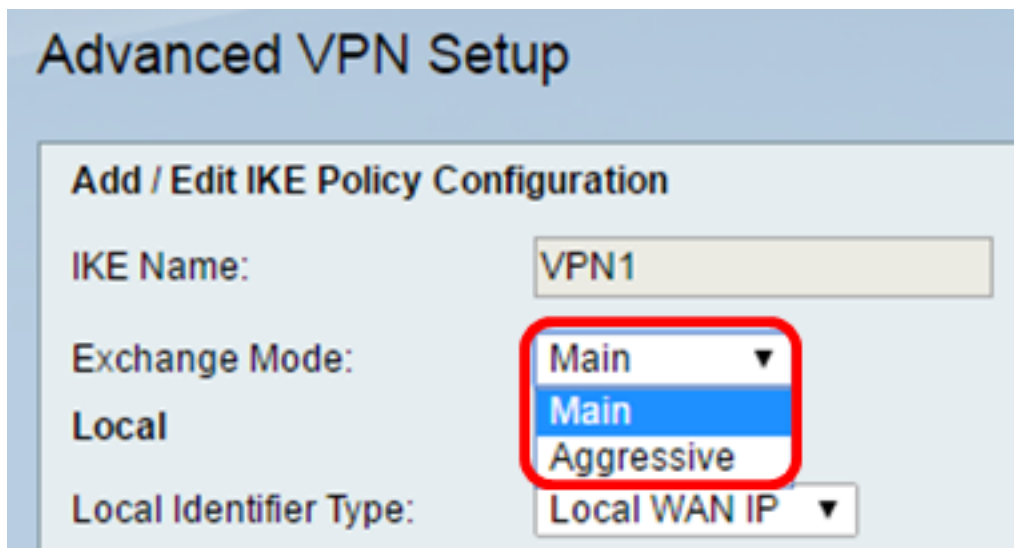
DPD Delay: (Range: 10 - 999, Default: 10)

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

步驟5.從Exchange Mode下拉選單中，選擇一個選項。

- Main — 此選項允許IKE策略以比主動模式更高的安全性協商VPN隧道。如果更安全的VPN連線優先於協商速度，請按一下此選項。
- 主動 — 此選項允許IKE策略建立比主模式更快但安全性更低的連線。如果更快的VPN連線優先於高安全性，請按一下此選項。

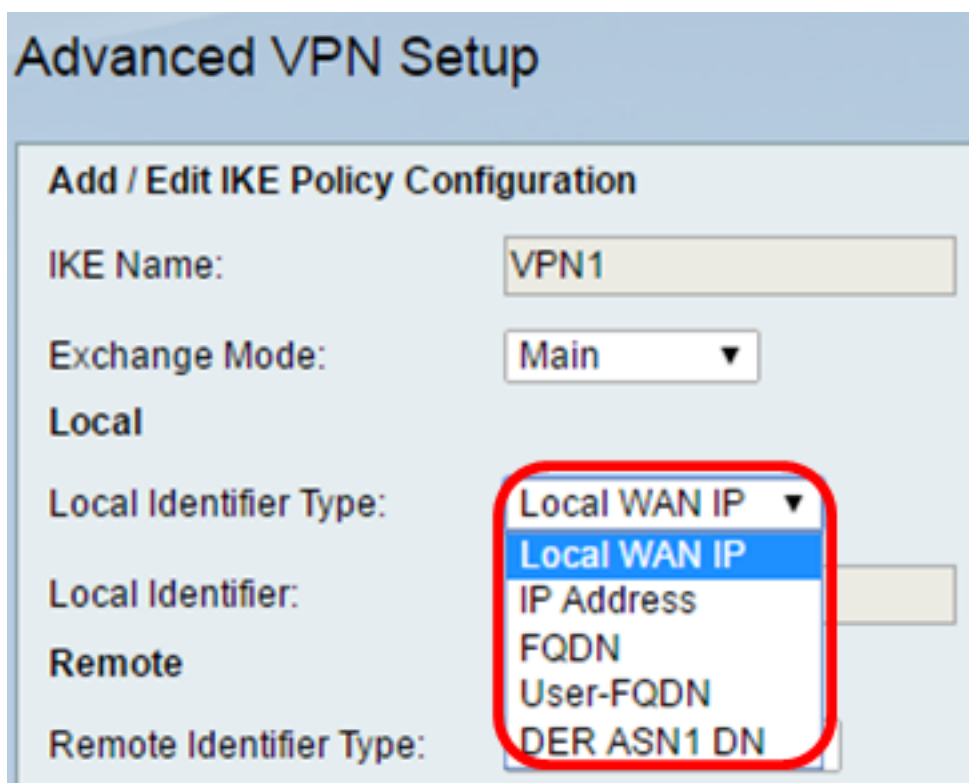
附註：在此示例中，選擇Main。



步驟6.從Local Identifier Types下拉選單中選擇，以標識或指定本地路由器的Internet安全關聯和金鑰管理協定(ISAKMP)。選項包括：

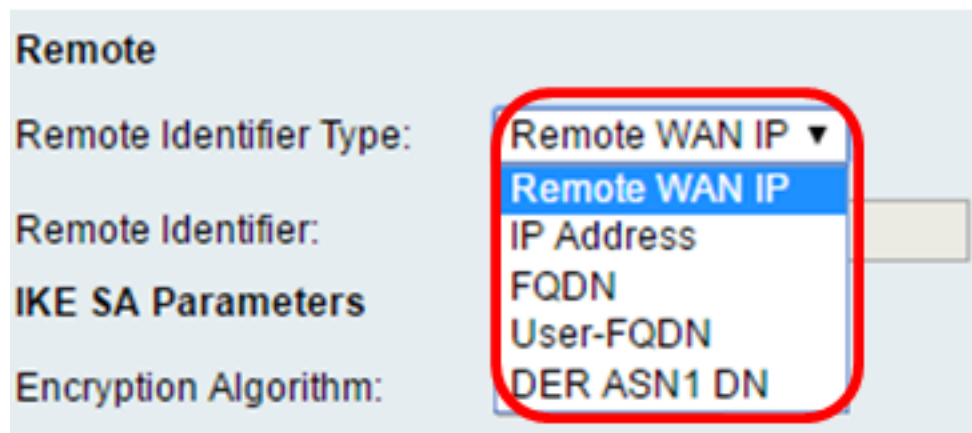
- 本地WAN IP — 路由器使用本地廣域網(WAN)IP作為主要識別符號。此選項通過Internet連線。選擇此選項會使下面的Local Identifier欄位變灰。
- IP地址 — 按一下此選項可以在Local Identifier欄位中輸入IP地址。
- FQDN — 完全限定域名(FQDN)或域名(如<http://www.example.com>)允許您在「本地識別符號」(Local Identifier)欄位中輸入域名或IP地址。
- 使用者FQDN — 此選項是使用者電子郵件地址，例如user@email.com。在Local Identifier欄位中輸入域名或IP地址。
- DER ASN1 DN — 此選項是標識名(DN)的識別符號型別，它使用標識編碼規則抽象語法標籤法1(DER ASN1)來傳輸資訊。當VPN隧道與使用者證書關聯時會發生這種情況。如果選擇此選項，請在本地識別符號欄位中輸入域名或IP地址。

附註：在本示例中，選擇本地WAN IP。



步驟7.從Remote Identifier Type下拉選單中選擇，以標識或指定遠端路由器的Internet安全關聯和金鑰管理協定(ISAKMP)。選項包括遠端WAN IP、IP地址、FQDN、使用者FQDN和DER ASN1 DN。

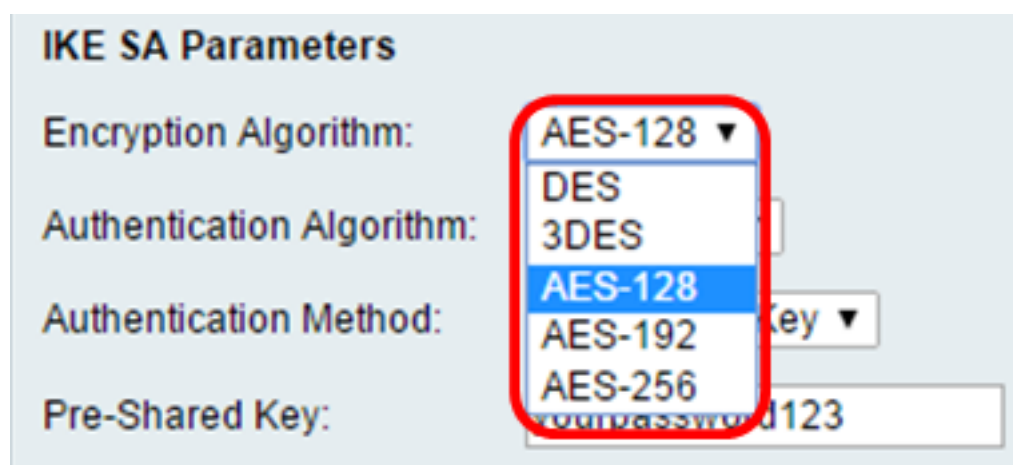
附註：在本示例中，選擇遠端WAN IP。



步驟8.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是預設加密演演算法，比AES-192和AES-256快但安全性低。
- 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。

附註：在此示例中，選擇了AES-128。

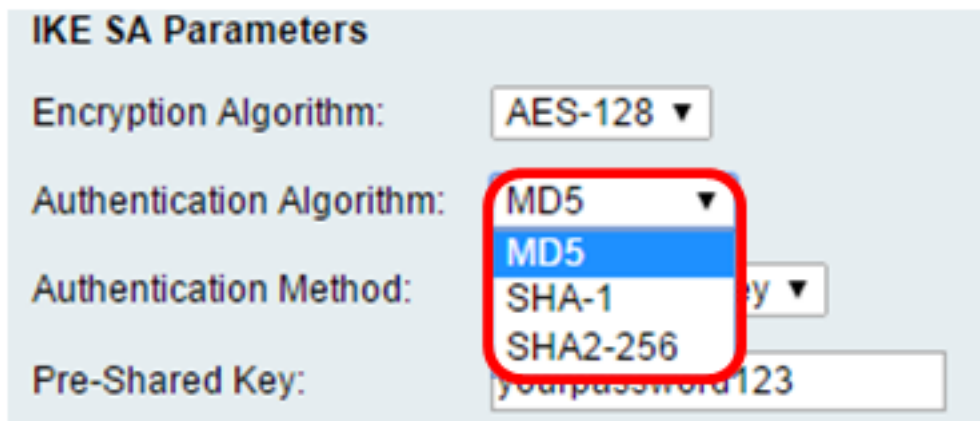


步驟9.從Authentication Algorithm下拉選單中，選擇以下選項：

- MD5 — 消息摘要5(MD5)是一種使用128位雜湊值進行身份驗證的身份驗證演算法。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慢，但更安全

- 。SHA-1是預設身份驗證演算法，比SHA2-256更快，但安全性更低。
- 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速度更慢，但更安全。

附註：在本例中，選擇了MD5。

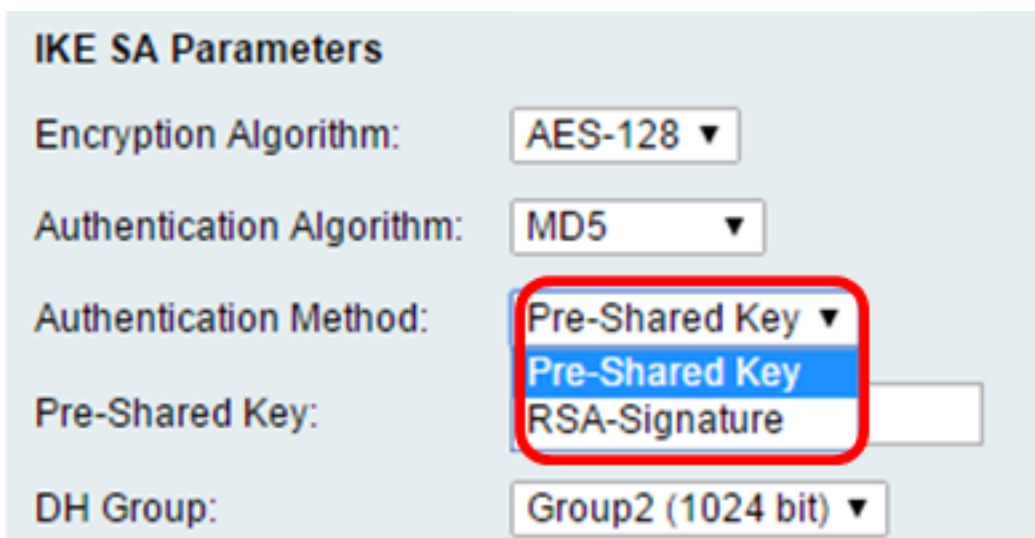


The screenshot shows the 'IKE SA Parameters' configuration interface. The 'Authentication Method' dropdown menu is open, displaying three options: 'MD5', 'SHA-1', and 'SHA2-256'. The 'MD5' option is highlighted in blue. A red rectangular box is drawn around the dropdown menu to draw attention to the selection process.

步驟10.在Authentication Method下拉選單中，選擇以下選項：

- 預共用金鑰 — 此選項需要與IKE對等體共用的密碼。
- RSA簽名 — 此選項使用證書對連線進行身份驗證。如果選擇此項，則預共用金鑰欄位將被禁用。
 - 。跳至[步驟12](#)。

附註：在此範例中選擇預共用金鑰。



The screenshot shows the 'IKE SA Parameters' configuration interface. The 'Authentication Method' dropdown menu is open, displaying three options: 'Pre-Shared Key', 'Pre-Shared Key', and 'RSA-Signature'. The first 'Pre-Shared Key' option is highlighted in blue. A red rectangular box is drawn around the dropdown menu to draw attention to the selection process.

步驟11.在Pre-Shared Key欄位中，輸入長度為8到49個字元的密碼。

附註：本例中使用的是password123。

IKE SA Parameters

Encryption Algorithm: AES-128 ▼

Authentication Algorithm: MD5 ▼

Authentication Method: Pre-Shared Key ▼

Pre-Shared Key: yourpassword123

步驟12. 從DH Group下拉選單中，選擇IKE使用哪個Diffie-Hellman(DH)組演算法。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，安全性越好。

附註： 在本例中，選擇了Group1。

DH Group: Group1 (768 bit) ▼

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

Dead Peer Detection: Enable

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

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

Save Cancel Back

步驟13. 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）。範圍是從30到86400秒。預設值為28800。

DH Group: Group1 (768 bit) ▼

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

Dead Peer Detection: Enable

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

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

Save Cancel Back

步驟14. (可選) 勾選**Enable** Dead Peer Detection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運行或仍然處於活動狀態。如果檢測到對等體已死，裝置將刪除IPsec和IKE安全關聯。DPD可防止非活動對等體上的網路資源浪費。

附註： 如果您不希望啟用Dead Peer Detection，請跳至**步驟17**。

Dead Peer Detection: Enable

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

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

Save Cancel Back

步驟15。(可選)如果在[步驟14](#)中啟用了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）。

附註：DPD延遲是連續DPD R-U-THERE消息之間的時間間隔（以秒為單位）。DPD R-U-THERE消息僅在IPsec流量空閒時傳送。預設值為 10。

Dead Peer Detection: Enable

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

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

Save Cancel Back

步驟16。(可選)如果在[步驟14](#)中啟用了DPD，請在DPD超時欄位中輸入在刪除非活動對等體之前等待的秒數。

附註：這是裝置在認為對等體失效之前應等待接收對DPD消息的響應的最長時間。預設值為 30。

Dead Peer Detection: Enable

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

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

Save Cancel Back

[步驟17](#).按一下「Save」。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Local Identifier Type:

Local Identifier:

Remote

Remote Identifier Type:

Remote Identifier:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:

Pre-Shared Key:

DH Group:

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

Dead Peer Detection: Enable

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

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

附註：系統將重新顯示Advanced VPN Setup首頁面。

現在，您應該在路由器上成功配置IKE策略設定。

配置VPN策略設定

注意：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。

附註：您也可以通過選中策略的覈取方塊並按一下**Edit**來編輯VPN策略。系統將顯示 Advanced VPN Setup頁面：

The screenshot shows the 'Advanced VPN Setup' interface. At the top, there is a 'NAT Traversal' section with an unchecked checkbox. Below it is the 'IKE Policy Table' with columns for Name, Local ID, Remote ID, and Exchange Mode. A row is visible with 'VPN1' in the Name column, 'Local WAN IP' in the Local ID column, 'Remote WAN IP' in the Remote ID column, and 'Main' in the Exchange Mode column. Below the table are 'Add Row', 'Edit', and 'Delete' buttons. The 'VPN Policy Table' section below it has columns for Status, Name, Policy Type, and Encryption. It shows 'No data to display' and has 'Add Row', 'Edit', 'Enable', 'Disable', and 'Delete' buttons. At the bottom, there are 'Save', 'Cancel', and 'IPSec Connection Status' buttons. The 'Add Row' button in the VPN Policy Table is highlighted with a red box.

步驟2.在Add/Edit VPN Configuration區域下的IPSec Name欄位中，輸入VPN策略的名稱。

附註：本示例使用VPN1。

The screenshot shows the 'Add / Edit VPN Policy Configuration' section. It has three fields: 'IPSec Name' with the value 'VPN1', 'Policy Type' with a dropdown menu set to 'Auto Policy', and 'Remote Endpoint' with a dropdown menu set to 'IP Address'. The 'IPSec Name' field is highlighted with a red box.

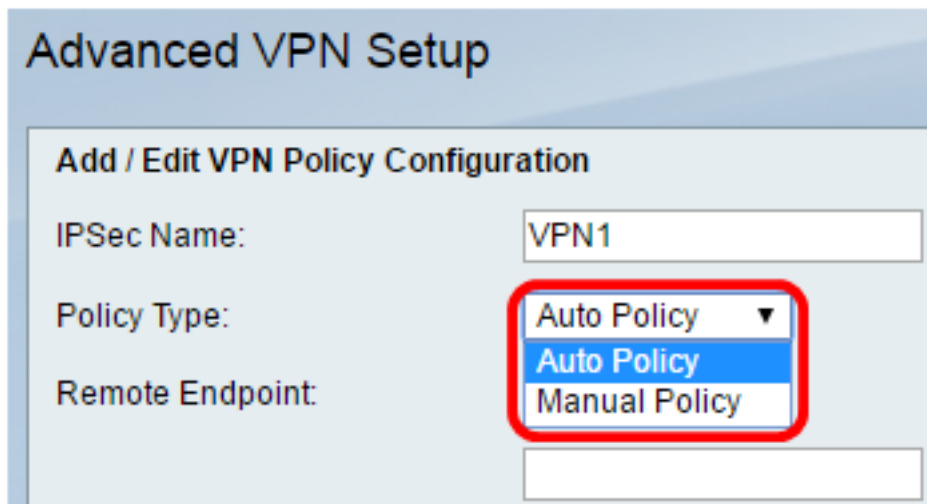
步驟3.從Policy Type下拉選單中選擇一個選項。

- 手動策略(Manual Policy) — 此選項允許您手動配置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。繼續這些步驟，直到選擇「

遠端流量」。按一下[此處](#)瞭解步驟。

- 自動策略 — 自動設定策略引數。此選項使用IKE策略進行資料完整性和加密金鑰交換。如果選擇此選項，則會啟用「自動策略引數」區域下的配置設定。按一下[此處](#)瞭解步驟。確保IKE協定在兩個VPN端點之間自動協商。

附註：在本示例中，選擇了Auto Policy。



Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name: VPN1

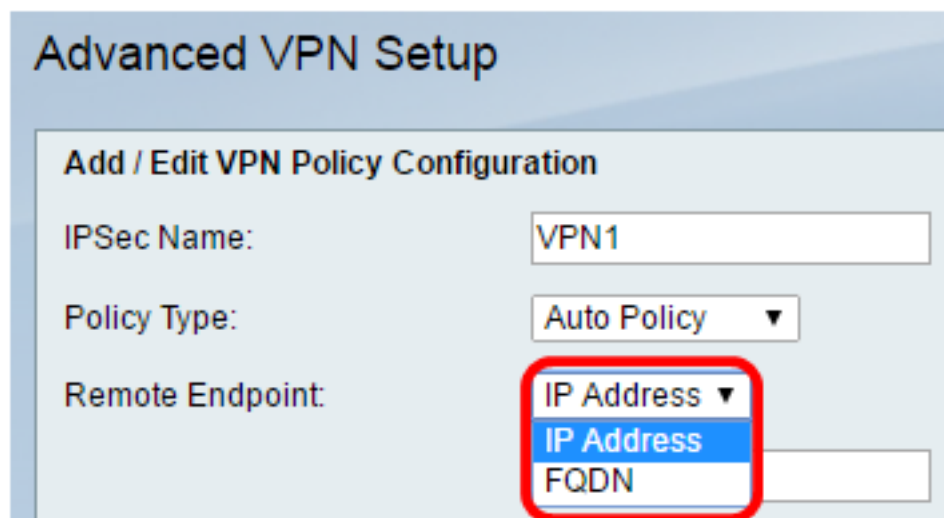
Policy Type: Auto Policy

Remote Endpoint:

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 — 特定電腦、主機或Internet的完整域名。FQDN由兩部分組成：主機名和域名。只有在[步驟3](#)中選擇了自動策略時，才能啟用此選項。

附註：在本例中，選擇了IP地址。



Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name: VPN1

Policy Type: Auto Policy

Remote Endpoint: IP Address

步驟5.在Remote Endpoint欄位中，輸入遠端地址的公共IP地址或域名。

附註：本示例使用192.168.2.101。

Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

步驟6. (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 Enabled**覈取方塊。NetBIOS允許主機在區域網(LAN)中彼此通訊。

Advanced VPN Setup

Add / Edit VPN Policy Configuration

IPSec Name:

Policy Type:

Remote Endpoint:

(Hi

NetBios Enabled:

[步驟7.](#)從Local Traffic Selection區域下的Local IP下拉選單中，選擇一個選項。

- Single — 將策略限制為一個主機。
- 子網 — 允許IP地址範圍內的主機連線到VPN。

附註：在本示例中，選擇了Subnet。

Local Traffic Selection

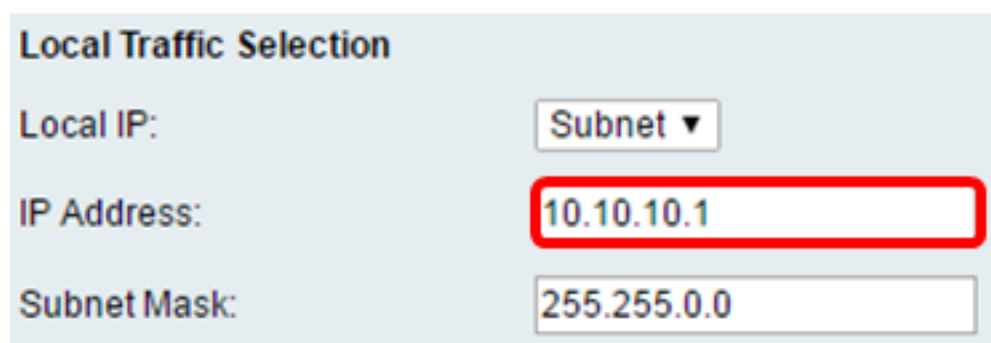
Local IP:

IP Address:

Subnet Mask:

步驟8.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。

附註：在本示例中，使用本地子網IP地址10.10.10.1。



The screenshot shows the 'Local Traffic Selection' configuration panel. It contains three input fields: 'Local IP:' with a dropdown menu set to 'Subnet', 'IP Address:' with the value '10.10.10.1' (highlighted with a red box), and 'Subnet Mask:' with the value '255.255.0.0'.

步驟9。（可選）如果在[步驟7](#)中選擇了子網，請在子網掩碼欄位中輸入客戶端的子網掩碼。如果在步驟1中選擇了Single，則禁用Subnet Mask欄位。

附註：本例中使用的是子網掩碼255.255.0.0。

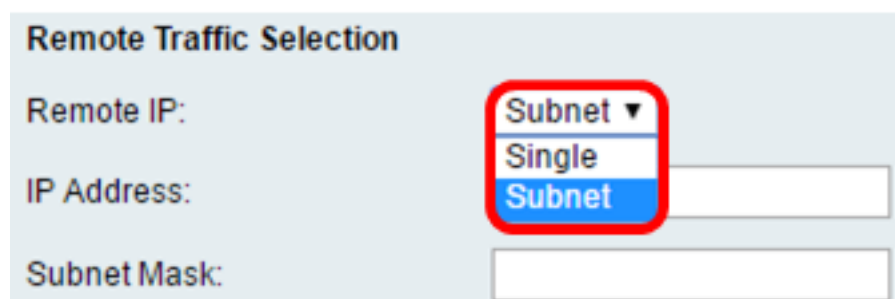


This screenshot is identical to the previous one, showing the 'Local Traffic Selection' configuration. The 'Subnet Mask:' field with the value '255.255.0.0' is highlighted with a red box.

[步驟10](#).從Remote Traffic Selection區域下的Remote IP下拉選單中，選擇一個選項。

- Single — 將策略限制為一個主機。
- 子網 — 允許IP地址範圍內的主機連線到VPN。

附註：在本示例中，選擇了Subnet。



The screenshot shows the 'Remote Traffic Selection' configuration panel. The 'Remote IP:' dropdown menu is open, showing three options: 'Subnet' (selected and highlighted with a blue bar), 'Single', and 'Subnet'. The dropdown menu is highlighted with a red box. Below it are empty input fields for 'IP Address:' and 'Subnet Mask:'.

步驟11.在IP Address欄位中輸入將成為VPN一部分的主機的IP地址範圍。如果在[步驟10](#)中選擇了Single，請輸入IP地址。

附註：在下面的示例中，使用了10.10.11.2。

Remote Traffic Selection

Remote IP: Subnet ▼

IP Address: 10.10.11.2

Subnet Mask: 255.255.0.0

步驟12。(可選)如果在[步驟10](#)中選擇了子網，請在[子網掩碼](#)欄位中輸入子網IP地址的子網掩碼。

附註：在以下示例中，使用了255.255.0.0。

Remote Traffic Selection

Remote IP: Subnet ▼

IP Address: 10.10.11.2 (Hint: 1.2.3.4)

Subnet Mask: 255.255.0.0 (Hint: 255.255.255.0)

[手動策略 引數](#)

注意：只有選擇「手動策略」，才能編輯這些欄位。

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。

附註：在本示例中，使用了0xABCD。

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

步驟2.在*SPI-Outgoing*欄位中，為VPN連線上的傳出流量的SPI標籤輸入三到八個十六進位制字元。

附註：在本示例中，使用0x1234。

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

[步驟3](#).從Manual Encryption Algorithm下拉式清單中選擇一個選項。選項包括DES、3DES、

AES-128、AES-192和AES-256。

附註：在此範例中，選擇AES-128。

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Manual Encryption Algorithm: AES-128 ▼

Key-In: []

Key-Out: []

Manual Integrity Algorithm: []

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](#)。

- DES使用8個字元的金鑰。
- 3DES使用24個字元的金鑰。
- AES-128使用16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。

附註：在此示例中，使用123456789ABCDEFGG。

Manual Encryption Algorithm: AES-128 ▼

Key-In: 123456789ABCDEFGG

Key-Out: 123456789ABCDEFGG

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123456789ABCDEFGG。

Manual Encryption Algorithm: AES-128 ▼

Key-In: 123456789ABCDEFGG

Key-Out: 123456789ABCDEFGG

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。

附註：在此示例中，使用123456789ABCDEFG。

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123456789ABCDEFG。

[Auto策略引數](#)

注意：建立自動VPN策略之前，請確保建立要基於其建立自動VPN策略的IKE策略。只有在步驟3中選擇了Auto Policy時，才能編輯這些欄位。

步驟1。在IPSec SA-Lifetime欄位中，輸入SA在續訂前持續的時間（以秒為單位）。範圍為30-86400。預設值為3600。

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

步驟2.從Encryption Algorithm下拉式清單中選擇一個選項。選項包括：

附註：在此範例中，選擇AES-128。

- DES — 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，可能需要它。
- 3DES — 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 — 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 — 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 — 使用256位金鑰進行AES加密。AES-256比AES-128和AES-192慢，但更安全。
- AESGCM — 高級加密標準伽羅瓦計數器模式是通用身份驗證加密塊密碼模式。GCM身份驗證使用特別適合於在硬體中高效實施的操作，使其特別適用於高速實施或在高效緊湊電路中的實施。
- AESCCM — 採用CBC-MAC模式的高級加密標準計數器是經過身份驗證的通用加密塊密碼模式。CCM非常適合用於緊湊的軟體實施。

Auto Policy Parameters

IPSec SA Lifetime: Seco

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group:

DH Group:

Select IKE Policy:

步驟3.從Integrity Algorithm下拉選單中，選擇一個選項。選項包括MD5、SHA-1和SHA2-256。

附註：在此範例中，選擇SHA-1。

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seco

Encryption Algorithm: AES-128 ▾

Integrity Algorithm: SHA-1 ▾
SHA-1
SHA2-256
MD5

PFS Key Group:

DH Group: Group 1(768 bit) ▾

Select IKE Policy: VPN1 ▾

[步驟4](#). 勾選PFS金鑰組中的**Enable**核取方塊，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。

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seconds

Encryption Algorithm: AES-128 ▾

Integrity Algorithm: SHA-1 ▾

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▾

Select IKE Policy: VPN1 ▾

View

Save Cancel Back

步驟5. (可選) 如果您選擇在[步驟4](#)中啟用PFS，請從DH組下拉選單中選擇要加入的DH組。組數越高，安全性越好。

附註：在本例中，選擇了組1。

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seconds

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group: Enable

DH Group: Group 1(768 bit)

Select IKE Policy: Group 1(768 bit)

Group 1(768 bit)

Group 2(1024 bit)

Group 5(1536 bit)

Save Cancel Back

步驟6.從Select IKE Policy下拉選單中，選擇要用於VPN策略的IKE策略。

附註：在本示例中，只配置了一個IKE策略，因此只顯示一個策略。

Auto Policy Parameters

IPSec SA Lifetime: 3600 Seconds (Ra

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group: Enable

DH Group: Group 1(768 bit)

Select IKE Policy: VPN1

View

Save Cancel Back

步驟7.按一下「Save」。

Auto Policy Parameters

IPSec SA Lifetime: Seconds (R)

Encryption Algorithm: ▼

Integrity Algorithm: ▼

PFS Key Group: Enable

DH Group: ▼

Select IKE Policy: ▼

附註：系統將重新顯示Advanced VPN Setup首頁面。此時將顯示確認消息，確認配置設定已成功儲存。

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

步驟8.在VPN策略表下，選中一個竅取方塊以選擇VPN，然後按一下**Enable**。

附註：預設情況下禁用配置的VPN策略。

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

Add Row

Edit

Delete

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

Add Row

Edit

Enable

Disable

Delete

Save

Cancel

IPSec Connection Status

步驟9.按一下「Save」。

Advanced VPN Setup



Configuration settings have been saved successfully

NAT Traversal:

IKE Policy Table

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm
<input type="checkbox"/>	VPN1	Local WAN IP	Remote WAN IP	Main	AES-128

VPN Policy Table

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Alg
<input checked="" type="checkbox"/>	Disabled	VPN1	Auto Policy	AES-128	SHA-1

您現在應該已經在RV130或RV130W路由器上成功配置了VPN策略。

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）。