

RV130和RV130W VPN路由器上的網際網路金鑰交換(IKE)策略設定

目標

網際網路金鑰交換(IKE)是建立兩個網路之間安全通訊的通訊協定。使用IKE時，封包會被加密和鎖定，並使用雙方使用的金鑰解除鎖定。

在配置VPN策略之前，需要建立Internet金鑰交換策略。有關詳細資訊，請參閱[RV130和RV130W上的VPN策略配置](#)。

本文檔的目的是向您展示如何向RV130和RV130W VPN路由器新增IKE配置檔案。

適用裝置

- RV130
- RV130W

程式步驟

步驟1.使用路由器配置實用程式從左側選單中選擇VPN > 站點到站點IPSec VPN > Advanced VPN Setup。出現Advanced VPN Setup頁面：

Advanced VPN Setup

NAT Traversal: Enable

IKE Policy Table

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

Add Row Edit Delete

VPN Policy Table

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

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

步驟2.在IKE策略表下，按一下Add Row。此時會出現一個新視窗：

IKE Policy Table

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

Add Row Edit Delete

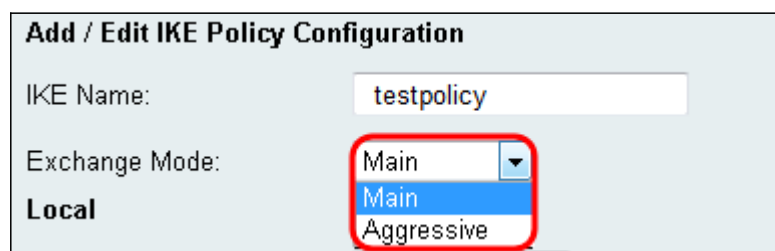
步驟3.在IKE Name (IKE名稱) 欄位中輸入IKE策略的名稱。

Add / Edit IKE Policy Configuration

IKE Name: testpolicy

Exchange Mode: Main

步驟4.從Exchange Mode下拉選單中，選擇使用金鑰交換建立安全通訊的模式。



Add / Edit IKE Policy Configuration

IKE Name: testpolicy

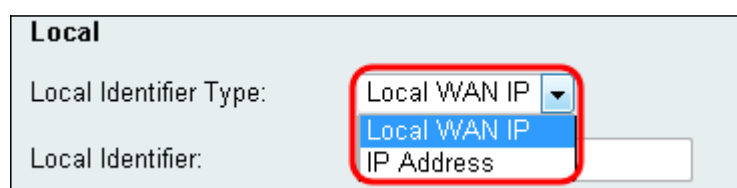
Exchange Mode: Main

Local

可用選項定義如下：

- Main — 保護對等體的身份以提高安全性。
- 積極 — 不保護對等體身份，但提供更快的連線。

步驟5.從Local Identifier Type下拉選單中選擇配置檔案具有的身份型別。



Local

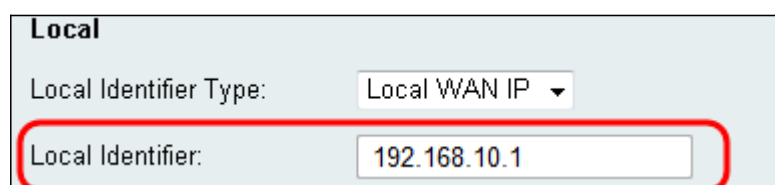
Local Identifier Type: Local WAN IP

Local Identifier:

可用選項定義如下：

- 本地WAN(Internet)IP — 通過Internet連線。
- IP地址 — 由句點分隔的唯一數字字串，用於標識使用Internet協定通過網路進行通訊的每台電腦。

步驟6. (可選) 如果從步驟5中的下拉選單中選擇IP Address，請在Local Identifier欄位中輸入本地IP地址。

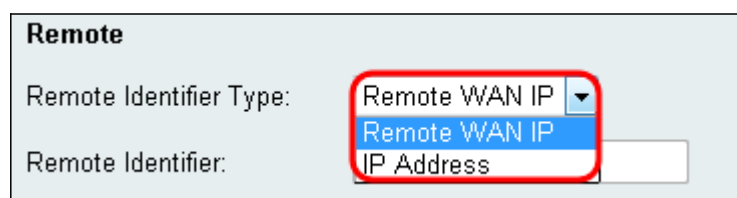


Local

Local Identifier Type: Local WAN IP

Local Identifier: 192.168.10.1

步驟7.從Remote Identifier Type下拉選單中選擇配置檔案具有的身份型別。



Remote

Remote Identifier Type: Remote WAN IP

Remote Identifier:

可用選項定義如下：

- 本地WAN(Internet)IP — 通過Internet連線。
- IP地址 — 由句點分隔的唯一數字字串，用於標識使用Internet協定通過網路進行通訊的每台電腦。

步驟8. (可選) 如果從步驟7中的下拉選單中選擇IP Address，請在Remote Identifier欄位中輸入遠端IP地址。

Remote

Remote Identifier Type: Remote WAN IP ▾

Remote Identifier: 192.168.2.100

步驟9.從*Encryption Algorithm*下拉菜單中選擇一個演算法來加密您的通訊。**AES-128**被選為預設值。

IKE SA Parameters

Encryption Algorithm: DES
DES
3DES
AES-128
AES-192
AES-256 ▾

Authentication Algorithm:

Pre-Shared Key:

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)

可用選項從最低到最高安全性如下列出：

- DES — 資料加密標準。
- 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：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金鑰將增加安全性，但效能會下降。建議使用AES-128，因為它在速度和安全性之間提供了最佳折衷。

步驟10.從*Authentication Algorithm*下拉選單中，選擇一種演算法以對您的通訊進行身份驗證。預設選擇為SHA-1。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

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

Pre-Shared Key:

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)

可用選項定義如下：

- 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：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。MD5基本上不提供雜湊衝突的安全保護，並且只能在不需防衝突的小型企業環境中使用。與MD5相比，SHA1是一個更好的選擇，因為它在極慢的速度下提供了更好的安全性。為了獲得最佳效果，SHA2-256沒有已知的實際相關攻擊，並將提供最佳安全性。如前所述，更高的安全性意味著更低的速度。

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

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

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)

步驟12.從*DH Group*下拉選單中選擇DH組。位數表示安全級別。連線的兩端必須位於同一個組中。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: **Group1 (768 bit) ▾**

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13.在SA-Lifetime欄位中，輸入安全關聯的有效時間（以秒為單位）。預設值為28800秒。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 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14.（可選）如果要停用與非活動對等點的連線，請選中Dead Peer Detection欄位中的Enable覆取方塊。如果未啟用Dead peer Detection，請跳到步驟17。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

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15.（可選）如果您已啟用Dead Peer Detection，請在DPD Delay欄位中輸入值。此值將指定路由器等待檢查客戶端連線的時間。

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

步驟16。(可選)如果您已啟用Dead Peer Detection，請在*DPD Timeout*欄位中輸入值。該值將指定客戶端在超時之前保持連線的時間。

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

步驟17.按一下**Save**以儲存變更。

IKE SA Parameters	
Encryption Algorithm:	<input type="text" value="AES-128"/> ▼
Authentication Algorithm:	<input type="text" value="SHA-1"/> ▼
Pre-Shared Key:	<input type="text"/>
DH Group:	<input type="text" value="Group1 (768 bit)"/> ▼
SA-Lifetime:	<input type="text" value="28800"/> Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>	

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）。