

RV320和RV325 VPN路由器系列上的網關到網關 虛擬專用網路(VPN)配置

目標

VPN用於在公共或共用網際網路上通過兩個端點建立非常安全的連線，通過所謂的VPN隧道。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，並且在一端的客戶端在邏輯上看起來像是另一端的同一遠端網路的一部分。這使資料和資源能夠更輕鬆、更安全地通過Internet共用。必須在連線的兩端完成配置，才能成功建立網關到網關VPN連線。本文旨在指導您在RV32x VPN路由器系列上配置網關到網關VPN連線。

適用裝置

- RV320 Dual WAN VPN路由器
- RV325 Gigabit Dual WAN VPN路由器

軟體版本

·v1.1.0.09

網關到網關

步驟1.登入到Web Configuration Utility，然後選擇VPN > Gateway to Gateway。Gateway to Gateway頁面隨即開啟：

Gateway to Gateway

Add a New Tunnel

Tunnel No. 1

Tunnel Name:

Interface: WAN1 ▼

Keying Mode: IKE with Preshared key ▼

Enable:

Local Group Setup

Local Security Gateway Type: IP Only ▼

IP Address: 0.0.0.0

Local Security Group Type: Subnet ▼

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.128

Remote Group Setup

Remote Security Gateway Type: IP Only ▼

IP Address:

Remote Security Group Type: Subnet ▼

IP Address:

Subnet Mask: 255.255.255.0

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit ▼

Phase 1 Encryption: DES ▼

Phase 1 Authentication: MD5 ▼

Phase 1 SA Lifetime: 28800 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit ▼

Phase 2 Encryption: DES ▼

Phase 2 Authentication: MD5 ▼

Phase 2 SA Lifetime: 3600 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: ■■■■

為了使VPN連線正常工作，連線兩端的網際網路協定安全(IPSec)值必須相同。連線的兩端必須屬於不同的區域網(LAN)，以及至少一台路由器，才能通過靜態IP地址或動態DNS主機名進行識別。

新增新隧道

Add a New Tunnel	
Tunnel No.	1
Tunnel Name:	Example
Interface:	WAN2
Keying Mode:	Manual
Enable:	<input checked="" type="checkbox"/>

·隧道號 — 顯示要建立的當前隧道。路由器支援100個隧道。

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下拉選單中選擇用於通道的廣域網(WAN)埠。

·WAN1 — 路由器的專用WAN埠。

·WAN2 — 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。

·USB1 — 路由器的USB1埠。僅當連線埠上有3G/4G/LTE USB轉換器時才有效。

·USB2 — 路由器的USB2埠。僅當連線埠上有3G/4G/LTE USB轉換器時才有效。

步驟3.從Keying Mode下拉式清單中選擇要使用的通道安全性。

·手動 — 此選項可讓您手動配置金鑰，而不是與VPN連線的另一端協商金鑰。

·使用預共用金鑰的IKE — 選擇此選項可啟用在VPN隧道中設定安全關聯的網際網路金鑰交換協定(IKE)。IKE使用預共用金鑰對遠端對等體進行身份驗證。

·IKE with Certificate — 選擇此選項可啟用帶有證書的Internet金鑰交換(IKE)協定，該協定提供了一種更安全的方式，可自動生成和交換預共用金鑰，為隧道建立更經驗證的安全通訊。

步驟4.選中Enable竅取方塊以啟用VPN隧道。預設情況下，該選項處於啟用狀態。

本地組設定

這些設定應與VPN隧道另一端的路由器的「遠端組設定」設定匹配。

附註：如果從Add a New Tunnel start from Step 1 and skip Steps 2 to 4 (新增新隧道步驟1的步驟3) 的Keying Mode下拉選單中選擇Manual或IKE with Preshared key (使用預共用金鑰的IKE) ，請跳過步驟1。

Local Group Setup	
Local Security Gateway Type:	IP + Email Address(USER FQDN) Authentication
IP Address:	0.0.0.0
Email Address:	example @ router.com
Local Security Group Type:	IP Range
Begin IP:	192.168.1.1
End IP:	192.168.1.254

步驟1.從Local Security Gateway Type下拉選單中，選擇識別路由器以建立VPN隧道的方法。

·僅IP — 只能通過靜態WAN IP訪問隧道。如果只有路由器具有任何靜態WAN IP，則可以選擇此選項。靜態WAN IP地址是自動生成的欄位。

·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地址是自動生成的欄位。

·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地址是自動生成的欄位。

·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 — 可以通過動態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。

附註：使用IKE with Certificate時，「本地組設定」區域上的以下更改會更改。

Local Group Setup

Local Security Gateway Type: IP + Certificate

IP Address: 0.0.0.0

Local Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject 6c:20:56:c6:16:52

Self-Generator Import Certificate

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.128

Local Security Gateway Type下拉選單不可編輯，並顯示IP + Certificate。這是可以使用通道的LAN資源。

IP地址欄位顯示裝置的WAN IP地址。使用者不可編輯。

步驟2.從Local Certificate下拉選單中選擇一個證書。證書在VPN連線上提供更強的身份驗證安全性。

步驟3. (可選) 按一下**Self-Generator**按鈕以顯示*Certificate Generator*視窗以設定和產生憑證。

步驟4. (可選) 按一下**Import Certificate**按鈕以顯示*My Certificate*視窗來檢視和設定憑證。

步驟5.從Local Security Group Type下拉選單中選擇以下選項之一：

·IP地址 — 此選項可讓您指定一個可使用此VPN隧道的裝置。您只需在IP地址欄位中輸入裝置的IP地址。

·子網 — 選擇此選項以允許屬於同一子網的所有裝置使用VPN隧道。您需要在IP Address欄位中輸入網路IP地址，並在Subnet Mask欄位中輸入其各自的子網掩碼。

·IP範圍 — 選擇此選項可指定可以使用VPN隧道的裝置範圍。您需要在Begin IP (開始IP) 欄位和End IP (結束IP) 欄位中輸入裝置範圍的第一個IP地址和最後一個IP地址。

遠端組設定

這些設定應與VPN隧道另一端的路由器的「本地組設定」設定匹配。

附註：如果從Add a New Tunnel start from Step 1 and skip Step 2 to 5(從步驟1開始新增新隧道的步驟3的Keying Mode下拉選單中選擇Manual或IKE with Preshared key，請跳過步驟2。如果選擇IKE with Certificate，請跳過步驟1。

Remote Group Setup

Remote Security Gateway Type: IP Only

IP by DNS Resolved : example.com

Remote Security Group Type: IP

IP Address: 192.0.2.4

步驟1.從Remote Security Gateway Type下拉選單中，選擇用於標識其它路由器以建立VPN隧道的方法。

·僅IP — 只能通過靜態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，並在IP by DNS Resolved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，並在IP by DNS Resolved欄位中輸入路由器的域名。如果選擇此選項，請在「域名」欄位中輸入已註冊域的名稱。

·IP +郵件地址（使用者FQDN）身份驗證 — 通過靜態IP地址和電子郵件地址可以訪問隧道。如果您知道遠端路由器的IP地址，請選擇「遠端安全網關型別」欄位正下方下拉選單中的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，並在IP by DNS Resolved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 — 可以通過動態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。

附註：如果兩台路由器都有動態IP地址，請不要為兩台網關選擇Dynamic IP + Email Address。

附註：使用IKE使用證書時，「遠端組設定」區域上的以下更改會更改。

Remote Group Setup

Remote Security Gateway Type: IP + Certificate

IP by DNS Resolved : example.com

Remote Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Import Remote Certificate Authorize CSR

Remote Security Group Type: IP

IP Address: 192.0.2.4

Remote Security Gateway Type (遠端安全網關型別) 下拉選單不可編輯，並顯示IP +證書。這是可以使用通道的LAN資源。

步驟2.如果您知道遠端路由器的IP地址，請選擇Remote Security Gateway Type欄位正下方下拉選單中的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 (IP by DNS已解析)，並在IP by DNS Resolved (IP by DNS已解析) 欄位中輸入遠端路由器的域名

步驟3.從Remote Certificate下拉選單中選擇一個證書。證書在VPN連線上提供更強的身份驗證安全性。

步驟4。(可選)按一下**Import Remote Certificate**按鈕以匯入新證書。

步驟5。(可選)按一下**Authorize CSR**按鈕，以使用數位簽署要求識別憑證。

步驟6.從Local Security Group Type下拉選單中選擇以下選項之一：

- IP地址 — 此選項可讓您指定一個可使用此VPN隧道的裝置。您只需在IP地址欄位中輸入裝置的IP地址。
- 子網 — 選擇此選項以允許屬於同一子網的所有裝置使用VPN隧道。您需要在IP Address欄位中輸入網路IP地址，並在Subnet Mask欄位中輸入其各自的子網掩碼。
- IP範圍 — 選擇此選項可指定可以使用VPN隧道的裝置範圍。您需要輸入裝置範圍的第一個IP地址和最後一個IP地址。在Begin IP欄位和End IP欄位中。

IPSec設定

要正確設定VPN隧道兩端之間的加密，它們必須具有完全相同的設定。在這種情況下，IPSec會在兩台裝置之間建立安全身份驗證。分兩個階段進行。

手動鍵控模式的IPSec設定

僅當從Add a New Tunnel的步驟3的Keying Mode下拉選單中選擇Manual時才可用。這是一種自定義安全模式，可自行生成新的安全金鑰，且不與金鑰協商。這是進行故障排除和小型靜態環境時的最佳選擇。

IPSec Setup		
Incoming SPI:	<input type="text" value="100A"/>	(Range: 100-FFFFFFF, Default: 100)
Outgoing SPI:	<input type="text" value="1BCD"/>	(Range: 100-FFFFFFF, Default: 100)
Encryption:	<input type="text" value="DES"/>	
Authentication:	<input type="text" value="SHA1"/>	
Encryption Key:	<input type="text" value="ABC12675BC0ACD"/>	(HEX Number, DES: 16bits, 3DES: 48bits)
Authentication Key:	<input type="text" value="AC67BCD00A12876CB"/>	(HEX Number, MD5: 32bits, SHA1: 40bits)

步驟1.在「傳入SPI」欄位中輸入傳入的安全引數索引(SPI)的唯一十六進位制值。SPI在封裝安全負載(ESP)協定報頭中傳輸，共同確定對傳入資料包的保護。可以輸入100到FFFFFFF。

步驟2.在Outgoing SPI欄位中輸入唯一的SPI十六進位制值。ESP報頭中攜帶SPI，ESP報頭共同確定對傳出資料包的保護。可以輸入100到FFFFFFF。

附註：傳入和傳出SPI應在兩端相互匹配以建立通道。

步驟3.從Encryption下拉選單中選擇適當的加密方法。推薦的加密是3DES。VPN通道的兩端需要使用相同的加密方法。

- DES — DES (資料加密標準) 是一種56位舊的、向後相容的加密方法，它不是那麼安全，容易破解。

- 3DES — 3DES (三重資料加密標準) 是一種168位、簡單的加密方法，通過對資料進行三次加密來增加金鑰大小，這比DES提供了更高的安全性。

步驟4.從Authentication下拉選單中選擇相應的身份驗證方法。推薦的身份驗證是SHA1。VPN隧道的兩端需要使用相同的身份驗證方法。

- MD5 - MD5 (消息摘要演算法-5) 代表32位十六進位制雜湊函式，通過校驗和計算為資料提供保護，使其免受惡意攻擊。

- SHA1 — SHA1 (安全雜湊演算法版本1) 是一個160位雜湊函式，比MD5更安全。

步驟5.在Encryption Key欄位中輸入要加密和解密資料的金鑰。如果在步驟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。如果您在步驟4中選擇MD5作為身份驗證方法，請輸入一個32位的十六進位制值。如果您在步驟4中選擇SHA作為驗證方法，請輸入一個40位的十六進位制值。VPN隧道的兩端需要使用相同的預共用金鑰。

步驟7.按一下**Save**以儲存設定。

使用預共用金鑰的IKE的IPSec設定

僅當從Add a New Tunnel的第3步的Keying Mode下拉選單中選擇IKE with Preshared key時才可用。

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

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，在第1階段連線期間用於共用金鑰以驗證通訊。

- 組1 - 768位 — 代表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。
- 組2 - 1024位 — 代表強度更高的金鑰和更安全的身份驗證組。它需要一些時間來計算IKE金鑰。
- 組5 - 1536位 — 表示強度最低的金鑰和最不安全的身份驗證組。計算IKE金鑰所需的時間更短。如果網路速度低，則優先使用。

步驟2.從Phase 1 Encryption下拉選單中選擇適當的階段1加密來加密金鑰。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)是56位舊加密方法，在當今的世界中並不是非常安全的加密方法。
- 3DES — 三重資料加密標準(3DES)是一種168位、簡單的加密方法，通過對資料加密三次，來增加金鑰大小，從而提供比DES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 — 是192位加密方法，通過12個循環重複將純文字檔案轉換為加密文本。
- AES-256 — 一種256位加密方法，通過14個循環重複將純文字檔案轉換為加密文本。

步驟3.從Phase 1 Authentication下拉選單中選擇相應的身份驗證方法。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)代表32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 — 比MD5更安全的160位雜湊函式。

步驟4.在Phase 1 SA Life Time欄位中輸入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。此選項允許在任何金鑰受到危害時生成新金鑰。加密資料僅通過被洩露的金鑰被洩露。因此，當通過金鑰洩露保護其他金鑰時，它可提供更安全的身份驗證通訊。這是推薦的操作，因為它提供了更高的安全性。

步驟6.從Phase 2 DH Group下拉選單中選擇適當的階段2 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。DH是在階段1連線期間使用的金鑰交換協定，用於共用金鑰以驗證通訊。

·組1 - 768位 — 代表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。

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

·組5 - 1536位 — 表示強度最低的金鑰和最不安全的身份驗證組。計算IKE金鑰所需的時間更短。如果網路速度低，則優先使用。

附註：由於未生成任何新金鑰，如果您在步驟5中取消選中Perfect Forward Secrecy，則無需配置階段2 DH組。

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。

·DES — DES是56位舊加密方法，在當今的世界中並不是非常安全的加密方法。

·3DES — 3DES是168位、簡單的加密方法，通過對資料進行三次加密來增加金鑰大小，從而提供比DES更高的安全性。

·AES-128 — 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 — 是192位加密方法，通過12個循環重複將純文字檔案轉換為加密文本。

·AES-256 — 一種256位加密方法，通過14個循環重複將純文字檔案轉換為加密文本。

步驟8.從Phase 2 Authentication下拉選單中選擇相應的身份驗證方法。VPN隧道的兩端需要使用相同的身份驗證方法。

·MD5 - MD5代表32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位雜湊函式，比MD5更安全。

·空 — 不使用身份驗證方法。

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

步驟10.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。

步驟11.在Preshared Key欄位中輸入之前在IKE對等體之間共用的金鑰。最多30個十六進位制和字元可用作預共用金鑰。VPN隧道的兩端需要使用相同的預共用金鑰。

附註：強烈建議頻繁更改IKE對等體之間的預共用金鑰，以使VPN保持安全。

預共用金鑰強度表通過顏色條顯示預共用金鑰的強度。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。

IKE的IPSec設定與證書

僅當從Add a New Tunnel的步驟3的Keying Mode下拉選單中選擇IKE with Certificate時才可用。

IPsec Setup

Phase 1 DH Group: Group 2 - 1024 bit

Phase 1 Encryption: DES

Phase 1 Authentication: MD5

Phase 1 SA Lifetime: 88029 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: DES

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 560 sec (Range: 120-28800, Default: 3600)

Advanced +

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SA (安全關聯)，以支援安全身份驗證通訊。DH是在階段1連線期間使用的金鑰交換協定，用於共用金鑰以驗證通訊。

- 組1 - 768位 — 代表強度最高的金鑰和最安全的身份驗證組。但需要更多時間計算IKE金鑰。如果網路速度高，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 — 表示強度最低的金鑰和最不安全的身份驗證組。計算IKE金鑰所需的時間更短。如果網路速度低，則優先使用。

步驟2.從Phase 1 Encryption下拉選單中選擇適當的階段1加密來加密金鑰。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 — DES是56位舊加密方法，在當今的世界中並不是非常安全的加密方法。
- 3DES — 3DES是168位、簡單的加密方法，通過對資料進行三次加密來增加金鑰大小，從而提供比DES更高的安全性。
- AES-128 — 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 — 是192位加密方法，通過12個循環重複將純文字檔案轉換為加密文本。

- AES-256 — 一種256位加密方法，通過14個循環重複將純文字檔案轉換為加密文本。

步驟3.從Phase 1 Authentication下拉選單中選擇相應的身份驗證方法。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 - MD5代表32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 — 比MD5更安全的160位雜湊函式。

步驟4.在Phase 1 SA Life Time欄位中輸入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。此選項允許在任何金鑰受到危害時生成新金鑰。加密資料僅通過被洩露的金鑰被洩露。因此，當另一個金鑰受損時，它保護其他金鑰的安全性時，可提供更安全且經過驗證的通訊。這是推薦的操作，因為它提供了更高的安全性。

步驟6.從Phase 2 DH Group下拉選單中選擇適當的階段2 DH組。階段1用於在隧道兩端之間建立單純的邏輯SA，以支援安全身份驗證通訊。DH是在階段1連線期間使用的金鑰交換協定，用於共用金鑰以驗證通訊。

- 組1 - 768位 — 代表強度最高的金鑰和最安全的身份驗證組。但需要更多時間計算IKE金鑰。如果網路速度高，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 — 表示強度最低的金鑰和最不安全的身份驗證組。計算IKE金鑰所需的時間更短。如果網路速度低，則優先使用。

附註：由於未生成任何新金鑰，如果您在步驟5中取消選中Perfect Forward Secrecy，則無需配置第2階段DH組。

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。

- DES — DES是56位舊加密方法，在當今的世界中並不是非常安全的加密方法。

- 3DES — 3DES是168位、簡單的加密方法，通過對資料進行三次加密來增加金鑰大小，從而提供比DES更高的安全性。

- AES-128 — 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 — 是192位加密方法，通過12個循環重複將純文字檔案轉換為加密文本。

- AES-256 — 一種256位加密方法，通過14個循環重複將純文字檔案轉換為加密文本。

步驟8.從Phase 2 Authentication下拉選單中選擇相應的身份驗證方法。VPN隧道的兩端需要使用相同的身份驗證方法。

- MD5 - MD5代表32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 — SHA1是160位雜湊函式，比MD5更安全。

- 空 — 不使用身份驗證方法。

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

步驟10.按一下**Save**以儲存設定。

(可選) IPSec Advance Setup for IKE with Certificate和IKE with Preshared key

如果從Add a New Tunnel的步驟3的Keying Mode下拉選單中選擇IKE with Certificate或IKE with Preshared key，則高級選項可用。這兩種金鑰模式可使用相同的設定。

步驟1.按一下**Advanced+**按鈕以顯示高級IPSec選項。

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm **MD5** ▼
- NetBIOS Broadcast
- Multicast Passthrough
- NAT Traversal
- Dead Peer Detection Interval **10** sec (Range: 10-999, Default: 10)
- Extended Authentication
 - IPsec Host
 - User Name:
 - Password:
 - Edge Device **Default - Local Database** ▼ **Add/Edit**
- Tunnel Backup
 - Remote Backup IP Address:
 - Local Interface: **WAN1** ▼
 - VPN Tunnel Backup Idle Time: **30** sec (Range: 30-999, Default: 30)
- Split DNS
 - DNS Server 1:
 - DNS Server 2: (Optional)
 - Domain Name 1:
 - Domain Name 2: (Optional)
 - Domain Name 3: (Optional)
 - Domain Name 4: (Optional)

步驟2.如果網路速度低，請選中Aggressive Mode覈取方塊。在SA連線期間，它以明文形式交換隧道端點的ID，這要求交換時間較短，但安全性較低。

步驟3.如果要壓縮IP資料包的大小，請選中Compress(支援IP負載壓縮協定(IPComp))覈取方塊。IPComp是一種IP壓縮協定，用於壓縮IP資料包的大小，如果網路速度低且使用者希望快速傳輸資料而不丟失慢速網路。

步驟4.如果始終希望VPN隧道的連線保持活動狀態，請選中Keep-Alive覈取方塊。它有助於在任何連線變為非活動狀態時立即重新建立連線。

步驟5.如果要驗證驗證標頭(AH)，請選中AH Hash Algorithm覈取方塊。AH為資料來源提供身份驗證，通過校驗和資料完整性檢查，並將保護擴展到IP報頭。通道的兩端應使用相同的演算

法。

- MD5 — MD5代表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 — SHA1是160位雜湊函式，比MD5更安全。

步驟6.如果要允許不可路由的流量通過VPN隧道，請檢查NetBIOS廣播。預設設定為未選中。NetBIOS用於通過一些軟體應用程式和Windows功能（如Network Neighborhood）檢測網路中的網路資源（如印表機、電腦等）。

步驟7.如果您的VPN路由器位於NAT網關之後，請選中該框以啟用NAT穿越。網路位址轉譯(NAT)允許具有私人LAN位址的使用者使用可公開路由的IP位址作為來源位址來存取網際網路資源。但是，對於入站流量，NAT網關沒有將公有IP地址轉換為專用LAN上特定目的地的自動方法。此問題會阻止成功的IPSec交換。NAT遍歷設定此入站轉換。隧道兩端必須使用相同的設定。

步驟8.檢查Dead Peer Detection Interval（失效對等體檢測間隔），以定期通過hello或ACK檢查VPN隧道的活躍性。如果選中此覈取方塊，請輸入所需的hello消息的持續時間或時間間隔（以秒為單位）。

步驟9.選中Extended Authentication以使用IPSec主機使用者名稱和密碼來驗證VPN客戶端或使用使用者管理中找到資料庫。必須在兩台裝置中啟用此功能，才能使其正常工作。按一下**IPSec Host**單選按鈕以使用IPSec主機和使用者名稱，並在User Name欄位和Password欄位中輸入使用者名稱和密碼。或按一下**Edge Device**單選按鈕使用資料庫。從Edge Device下拉選單中選擇所需資料庫。

步驟10.選中Tunnel Backup覈取方塊以啟用隧道備份。選中失效對等體檢測間隔後，此功能可用。此功能使裝置能夠通過備用WAN介面或IP地址重新建立VPN隧道。

- 遠端備份IP地址 — 遠端對等體的備用IP。在此欄位中輸入已為遠端網關設定的WAN IP。
- 本地介面 — 用於重建連線的WAN介面。從下拉選單中選擇所需的介面。
- VPN通道備份空閒時間 — 選擇時間，用於當主通道未連線時使用備份通道。以秒為單位輸入。

步驟11.選中Split DNS覈取方塊以啟用分割DNS。此功能允許根據指定的域名向定義的DNS伺服器傳送DNS請求。在DNS Server 1和DNS Server 2欄位中輸入DNS伺服器名稱，並在Domain Name #欄位中輸入域名。

步驟12.按一下**Save**完成裝置的配置。