

# 在RV016、RV042、RV042G和RV082 VPN路由器上配置網關到網關VPN的高級設定

## 目標

虛擬專用網路(VPN)是一種專用網路，用於通過公共網路虛擬連線遠端使用者的裝置以提供安全性。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。必須在連線的兩端執行相同的配置，才能成功建立網關到網關VPN連線。

通過高級網關到網關VPN配置，可以靈活地配置VPN隧道的可選配置，從而使VPN使用者更易於使用。「高級」選項僅適用於具有預共用金鑰模式的IKE。VPN連線兩端的高級設定應該相同。

本文檔的目的是向您展示如何在RV016、RV042、RV042G和RV082 VPN路由器上配置網關到網關VPN隧道的高級設定。

注意：如果您想瞭解有關如何配置網關到網關VPN的更多資訊，請參閱[在RV016、RV042、RV042G和RV082 VPN路由器上配置網關到網關VPN的文章](#)。

## 適用裝置

- RV016
- RV042
- RV042G
- RV082

## 軟體版本

- v4.2.2.08

## 網關到網關VPN的高級設定的配置

步驟 1. 登入到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 :

Interface :  ▼

Enable :

---

### Local Group Setup

Local Security Gateway Type :  ▼

IP Address : 0.0.0.0

Local Security Group Type :  ▼

IP Address :

Subnet Mask :

---

### Remote Group Setup

Remote Security Gateway Type :  ▼

▼ :

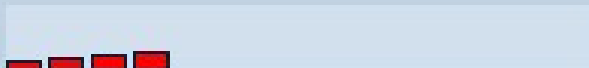
Remote Security Group Type :  ▼

IP Address :

Subnet Mask :

步驟 2. 向下滾動到IPSec Setup部分，然後按一下Advanced +。系統將顯示Advanced區域：

### 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 :	abcd1234	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/>	Enable
Preshared Key Strength Meter :		
<b>Advanced +</b>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

步驟 3. 如果您的網路速度低，請勾選Aggressive Mode覈取方塊。這會在SA連線（第1階段）期間以明文交換隧道端點的ID，這要求交換的時間較短，但安全性較低。

步驟 4. 如果要壓縮IP資料包的大小，請選中Compress(Support IP Payload Compression Protocol(IPComp))覈取方塊。IPComp是一種用於壓縮IP資料包大小的IP壓縮協定。IP壓縮在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時非常有用，但它不提供任何安全性

步驟 5.如果您始終希望VPN隧道的連線保持活動狀態，請選中Keep-Alive覈取方塊。Keep-Alive有助於在任何連線變為非活動狀態時立即重新建立連線。

**Advanced**

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5 ▼
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval  seconds
- Tunnel Backup :  
Remote Backup IP Address :   
Local Interface : WAN1 ▼  
VPN Tunnel Backup Idle Time :  seconds (Range:30~999 sec)
- Split DNS :  
DNS1 :   
DNS2 :   
Domain Name 1 :   
Domain Name 2 :   
Domain Name 3 :   
Domain Name 4 :

步驟 6. 如果要啟用Authenticate Header(AH)，請選中AH Hash Algorithm覈取方塊。AH通過校驗和為IP報頭提供源資料身份驗證、資料完整性保護。通道的兩端應具有相同的演算法。

- MD5 — 消息摘要演算法5(MD5)是一個128位的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。

## Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm MD5 ▼  
MD5  
SHA1

NetBIOS Broadcast

NAT Traversal

Dead Peer Detection Interval  seconds

Tunnel Backup :

Remote Backup IP Address :

Local Interface :  ▼

VPN Tunnel Backup Idle Time :  seconds (Range:30~999 sec)

Split DNS :

DNS1 :

DNS2 :

Domain Name 1 :

Domain Name 2 :

Domain Name 3 :

Domain Name 4 :

步驟 7. 如果要允許不可路由的流量通過VPN隧道，請選中NetBIOS Broadcast覆取方塊。預設設定為未選中。NetBIOS用於通過某些軟體應用程式和Windows功能（如Network Neighborhood）檢測網路資源（如網路中的印表機和電腦）。

步驟 8. 如果要通過公共IP地址從專用LAN訪問Internet，請選中NAT穿越覆取方塊。如果您的

VPN路由器位於NAT網關之後，請選中此覈取方塊以啟用NAT穿越。通道的兩端必須具有相同的設定。

步驟 9.檢查失效對等體檢測間隔，以定期方式通過hello或ACK檢查VPN隧道的生命力。如果選中此覈取方塊，請輸入問候消息之間的時間間隔（以秒為單位）。

注意：如果未選中Dead Peer Detection Interval，請跳至步驟11。

## Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm

NetBIOS Broadcast

NAT Traversal

Dead Peer Detection Interval  seconds

Tunnel Backup :

Remote Backup IP Address :

Local Interface :

VPN Tunnel Backup Idle Time :  seconds (Range:30~999 sec)

Split DNS :

DNS1 :

DNS2 :

Domain Name 1 :

Domain Name 2 :

Domain Name 3 :

Domain Name 4 :

步驟 10.選中Tunnel Backup覈取方塊以啟用隧道備份。只有在選中Dead Peer Detection Interval後，此功能才可用。此功能使裝置能夠通過備用本地WAN介面或遠端IP地址重新建立VPN隧道。

·遠端備份IP地址 — 輸入遠端網關的備用IP地址，或在此欄位中輸入已為遠端網關設定的



WAN IP地址。

·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 — 輸入主通道在使用備份通道之前必須連線的時間（秒）。

**Advanced**

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval  seconds
- Tunnel Backup :
  - Remote Backup IP Address :
  - Local Interface :
  - VPN Tunnel Backup Idle Time :  seconds (Range:30~999 sec)
- Split DNS :
  - DNS1 :
  - DNS2 :
  - Domain Name 1 :
  - Domain Name 2 :
  - Domain Name 3 :
  - Domain Name 4 :

步驟 11.選中Split DNS覈取方塊以啟用拆分DNS。拆分DNS允許指定域名的請求由不同於通常使用的DNS伺服器處理。當路由器收到來自客戶端的任何DNS請求時，它會檢查DNS請求並與域名匹配，然後將請求傳送到該特定的DNS伺服器。

**Advanced**

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval  seconds
- Tunnel Backup :  
Remote Backup IP Address :   
Local Interface :   
VPN Tunnel Backup Idle Time :  seconds (Range:30~999 sec)
- Split DNS :  
DNS1 :   
DNS2 :   
Domain Name 1 :   
Domain Name 2 :   
Domain Name 3 :   
Domain Name 4 :

步驟 12.在DNS1欄位中輸入DNS服務器IP地址。如果有另一個DNS伺服器，請在DNS2欄位中輸入DNS伺服器IP地址。

步驟 13. 在Domain Name 1至Domain Name 4欄位中輸入域名。對這些域名的請求將由步驟 12中指定的DNS伺服器處理。

步驟 14. 按一下Save儲存更改。

## 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）。