RV016、RV042、RV042G和RV082 VPN路由器上的VPN隧道設定

目標

虛擬專用網路(VPN)是兩個端點之間的安全連線。通過VPN隧道建立可在這兩個位置或網路之間安全地傳送資料的專用網路。VPN隧道連線兩台PC或網路，並允許通過Internet傳輸資料，就像終端在網路中一樣。VPN是員工必須經常出差或離開LAN的公司的理想解決方案。藉助VPN，這些員工可以訪問LAN並使用可用的資源完成工作。此外，VPN可以連線兩個或多個站點，因此具有不同分支機構的公司可以彼此通訊。

注意:RV有線路由器系列提供兩種型別的VPN：網關到網關和客戶端到網關。為了使VPN連線正常工作，連線兩端的IPSec值必須相同。此外，連線的兩端必須屬於不同的LAN。接下來的步驟將介紹如何在RV有線路由器系列上配置VPN。

為了本文的目的，VPN配置將是Gateway to Gateway。

本文說明了如何在RV016 RV042、RV042G和RV082 VPN路由器上設定VPN隧道。

適用裝置

- RV016
- RV042
- RV042G
- RV082

軟體版本

- v4.2.1.02

VPN設定

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

注意：要配置客戶端到網關VPN隧道，請選擇VPN >客戶端到網關。

Gateway To Gateway

Add a New Tunnel

Tunnel No.	1
Tunnel Name :	TestTunnel
Interface :	WAN1
Enable :	☑

Local Group Setup

Local Security Gateway Type :	IP Only
IP Address :	156.26.31.119
Local Security Group Type :	Subnet
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Remote Group Setup

Remote Security Gateway Type :	IP Only
IP Address :	192.0.2.2
Remote Security Group Type :	Subnet
IP Address :	192.168.2.0
Subnet Mask :	255.255.255.0

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

步驟2.在Tunnel Name欄位中，輸入VPN隧道的名稱。

步驟3.在Interface下拉選單中，選擇一個可用的WAN介面。這是將與另一端建立VPN隧道的介面。

步驟4.在Local Group Setup下，在Local Security Gateway Type下拉選單中，選擇列出的選項之一：

·僅IP — 如果您的路由器配置了用於Internet連線的靜態IP地址，請選擇此選項。

· IP +域名(FQDN)身份驗證 — 如果您的路由器配置了靜態IP地址和已註冊域名以進行Internet連線，請選擇此選項。

· IP +電子郵件地址（使用者FQDN）身份驗證 — 如果您的路由器配置為用於Internet連線的靜態IP地址，並且電子郵件地址將用於身份驗證，則選擇此選項。

·動態IP +域名(FQDN)身份驗證 — 如果您的路由器配置了動態IP地址，並且動態域名將用於身份驗證，請選擇此選項。

·動態IP +電子郵件地址（使用者FQDN）身份驗證 — 如果路由器具有用於Internet連線的動態IP地址，但沒有用於身份驗證的動態域名，則選擇此選項，而將使用電子郵件地址進行身份驗證。

步驟5.在Local Group Setup下，在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。您只需要輸入裝置的IP地址。

·子網 — 選擇此選項可允許屬於同一子網的所有裝置使用VPN隧道。您需要輸入網路IP地址及其各自的子網掩碼。

· 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。

步驟6.在Remote Group Setup下的Remote Local Security Gateway Type下拉選單中，選擇以下選項之一：

·僅IP — 如果您的路由器配置了用於Internet連線的靜態IP地址，請選擇此選項。

· IP +域名(FQDN)身份驗證 — 如果您的路由器配置了靜態IP地址和已註冊域名以進行Internet連線，請選擇此選項。

· IP +電子郵件地址（使用者FQDN）身份驗證 — 如果您的路由器配置為用於Internet連線的靜態IP地址，並且電子郵件地址將用於身份驗證，則選擇此選項。

·動態IP +域名(FQDN)身份驗證 — 如果您的路由器配置了動態IP地址，並且動態域名將用於身份驗證，請選擇此選項。

·動態IP +電子郵件地址（使用者FQDN）身份驗證 — 如果路由器具有用於Internet連線的動態IP地址，但沒有用於身份驗證的動態域名，則選擇此選項，而將使用電子郵件地址進行身份驗證。

步驟7.如果選擇IP Only作為遠端本地安全網關型別，請從下面的下拉選單中選擇以下選項之一：

· IP — 選擇此選項可在相鄰欄位中輸入IP地址。

· IP by DNS Resolved — 如果您不知道遠端網關的IP地址，請選擇此選項，然後在相鄰欄位中輸入其他路由器的名稱。

步驟8.在Remote Group Setup下的Remote 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。您只需要輸入裝置的IP地址。

·子網 — 選擇此選項可允許屬於同一子網的所有裝置使用VPN隧道。您需要輸入網路IP地址及其各自的子網掩碼。

· 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。

步驟9.在IPSec Setup下，在Keying Mode下拉選單中，選擇以下選項之一：

·手動 — 此選項可讓您手動配置金鑰，而不是與VPN連線中的其他路由器協商金鑰。

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

步驟10 。DH(Diffie - Hellman)是允許VPN隧道兩端共用加密金鑰的金鑰交換協定。 在Phase 1 DH Group和Phase 2 DH Group下拉選單中，選擇以下選項之一：

·組1 - 768位 — 提供更快的交換速度，但安全性較低。如果您需要VPN會話快速且安全性不是問題，則選擇此選項。

·組2 - 1024位 — 提供比組1更高的安全性，但它的處理時間更長。就安全性和速度而言，這是一個更為平衡的選擇。

·第3組 — 1536位 — 速度較慢，但安全性較高。如果您需要VPN會話是安全的，並且速度不是問題，則選擇此選項。

步驟11.在Phase 1 Encryption和Phase 2 Encryption下拉選單中，為金鑰的加密和解密選擇以下選項之一：

· DES — 資料加密標準，這是用於加密在56位資料包中加密金鑰的資料的基本演算法。

· 3DES — 三重資料加密標準，此演算法將金鑰加密在三個64位資料包中。它比DES更安全。

· AES-128 — 高級加密標準，此演算法使用相同的金鑰進行加密和解密。它比DES提供更高的安全性。其金鑰大小為128位

· AES-192 — 與AES-128類似，但其金鑰大小為192位。

· AES-256 — 與AES-128類似，但其金鑰大小為256位。這是可用的最安全的加密演算法。

步驟12.在Phase 1 Authentication和Phase 2 Authentication下拉選單中，選擇以下選項之一：

· SHA1 — 此演算法產生160位元的雜湊值。使用該值，演算法將檢查所交換的資料的完整性，並確保資料未發生更改。

· MD5 — 這是用於身份驗證的演算法設計。此演算法檢查VPN隧道兩端之間共用資訊的完整性。它產生一個雜湊值，通過共用該雜湊值來驗證VPN隧道兩端的金鑰。

步驟13.在Phase 1 SA Lifetime和Phase 2 SA Lifetime欄位中，輸入VPN隧道在某個階段處於活動狀態的時間（以秒為單位）。階段1的預設值為28800秒。階段2的預設值為3600秒。

注意：兩台路由器上的階段1和階段2配置必須相同。

步驟14。（可選）選中Perfect Forward Secrecy覈取方塊以啟用完全向前保密(PFS)。使用PFS，IKE第2階段協商將生成用於加密和身份驗證的新資料，從而增強安全性。

步驟15.在預共用金鑰中，輸入兩台路由器將共用用於身份驗證的金鑰。

步驟16.（可選）選中Minimum Preshared Key Complexity覈取方塊以啟用Preshared Key Strength Meter，該指示器將告訴您建立的金鑰的強度。

步驟17。（可選）若要配置更多高級加密選項，請按一下Advanced+。

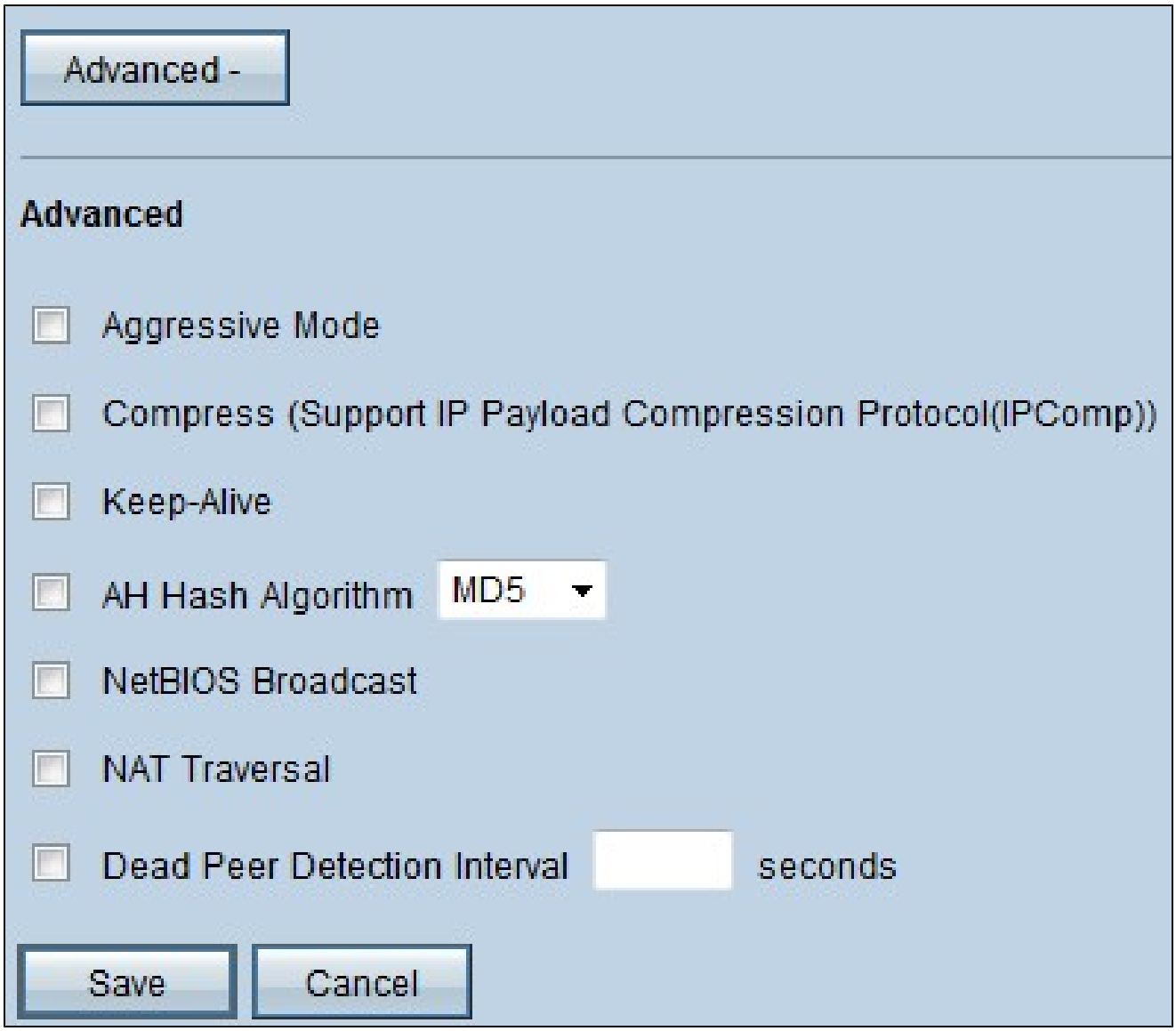
步驟18.按一下Save儲存您的配置。

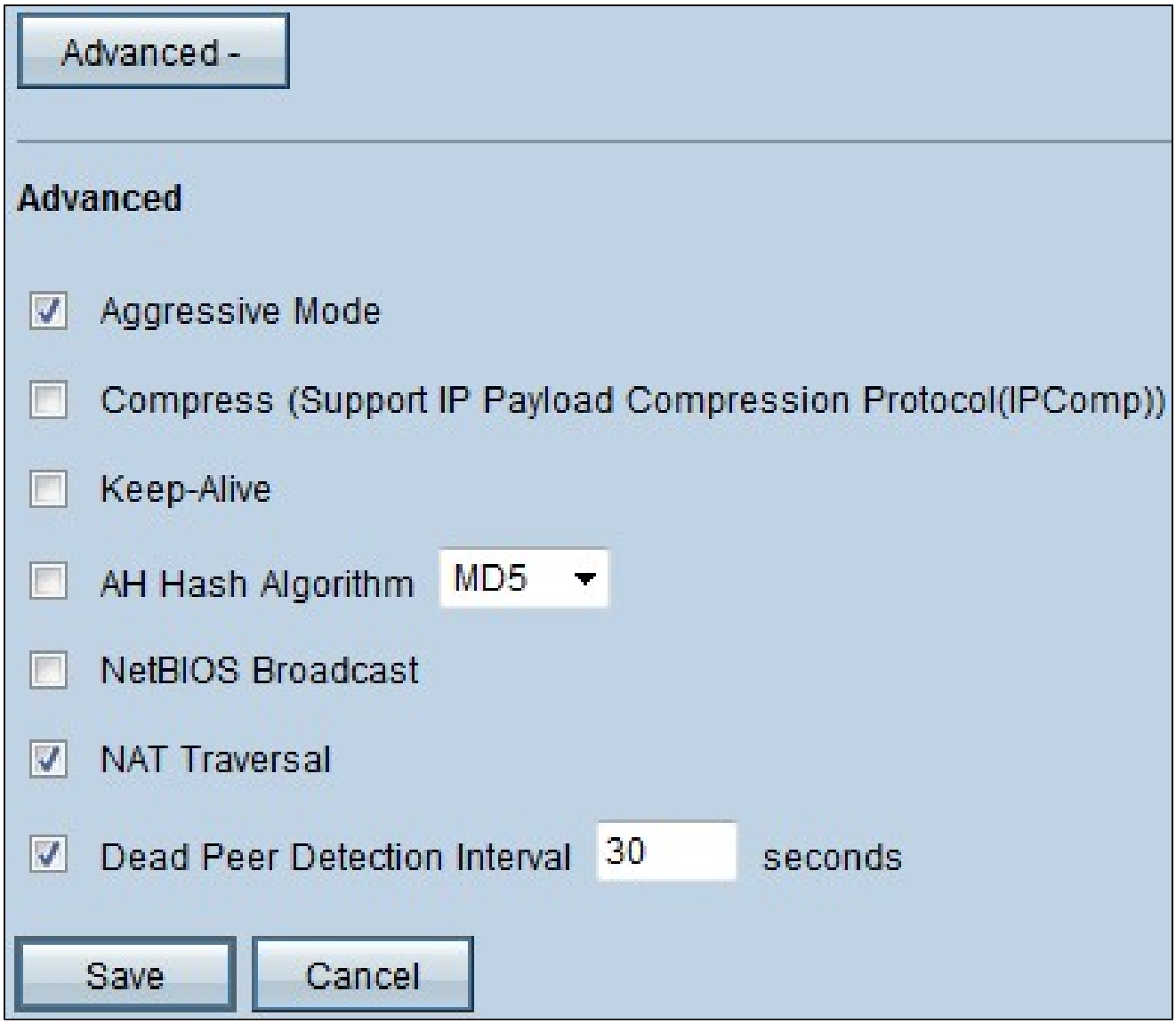
高級VPN選項

如果您想在VPN設定中新增更多功能，RV有線路由器系列可提供高級選項。這些選項增強了VPN隧道的安全功能。這些選項是可選的，但如果您在一個路由器上設定高級選項，請確保在另一個路由器上設定相同的選項。下一節將介紹這些選項。

步驟1.在IPSec欄位中，按一下Advanced+按鈕。Advanced頁面隨即開啟：

注意：要配置客戶端到網關VPN隧道的高級選項，請選擇VPN >客戶端到網關。然後按一下Advanced+。


Advanced -
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
Save
Cancel



上圖顯示了高級選項的配置示例。

步驟2.在Advanced下，選中要新增到VPN設定中的選項：

·主動模式 — 使用此選項時，金鑰協商速度更快，從而降低安全性。如果要提高VPN隧道的速度，請選中Aggressive Mode覈取方塊。

·壓縮(支援IP負載壓縮協定(IP Comp)) — 使用此選項，IP Comp協定將減小IP資料包的大小。 選中Compress(Support IP Payload Compression Protocol(IP Comp))覈取方塊以啟用此選項

·保持活動狀態 — 如果被丟棄，此選項將嘗試重新建立VPN會話。選中Keep Alive覈取方塊以啟用此選項。

· AH雜湊演算法 — 此選項將保護擴展到IP報頭，以驗證整個資料包的完整性。MD5或

SHA1均可用於此目的。選中AH Hash Algorithm覈取方塊，然後從下拉選單中選擇MD5或SHA1以啟用整個資料包的身份驗證。

· NetBIOS廣播 — 這是一種Windows協定，提供有關插入LAN中的不同裝置（如印表機、電腦和檔案伺服器）的資訊。通常，VPN不會傳輸此資訊。選中NetBIOS Broadcast覈取方塊以通過VPN隧道傳送這些資訊。

· NAT穿越 — 網路地址轉換使專用LAN中的使用者能夠使用公有IP地址作為源地址訪問Internet資源。如果您的路由器位於NAT網關之後，請選中NAT Traversal覈取方塊。

· Dead Peer Detection Interval — 選中Dead Peer Detection Interval覈取方塊，並輸入路由器傳送另一個資料包以檢查VPN隧道連線之前的時間間隔（以秒為單位）。

步驟3.按一下Save儲存配置。

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）。