Cisco RV路由器VPN概述和最佳實踐

目標

本文檔旨在向任何新接觸思科RV系列路由器的使用者概述虛擬專用網路(VPN)最佳實踐。

目錄

簡介

似乎在很久以前，你唯一可以工作的地方就是辦公室。你可能還記得，回到過去，週末必須去辦公室解決一件工作上的事情。沒有其他方法可以從公司資源獲取資料，除非您親自到辦公室。那樣的日子已經結束了。在當今時代，您可以隨時隨地辦公；在家、其他辦公室、咖啡店甚至其他國家/地區開展業務。缺點是駭客總是想竊取你的敏感資料。僅僅使用公共網際網路是不安全的。您能做些什麼來獲得靈活性和安全性？設定VPN!

VPN連線允許使用者通過公共或共用網路（例如Internet）來訪問、傳送和接收來自專用網路的資料，但仍確保與底層網路基礎設施的安全連線，以保護專用網路及其資源。

VPN隧道建立專用網路，該專用網路可以使用加密來編碼資料，並使用身份驗證來確保客戶端的身份，從而安全地傳送資料。企業辦公室經常使用VPN連線，因為即使員工不在辦公室，允許他們訪問其專用網路也是非常有用和必要的。

通常，站點到站點VPN會將整個網路相互連線。它們擴展了網路，並允許來自一個位置的電腦資源在其它位置可用。通過使用支援VPN的路由器，公司可以通過公共網路（例如Internet）連線多個固

定站點。

VPN的客戶端到站點設定允許遠端主機或客戶端像位於同一本地網路一樣工作。在路由器配置用於Internet連線後，可以在路由器和終端之間建立VPN連線。VPN客戶端除了需要匹配的設定外，還依賴於VPN路由器的設定來建立連線。此外，某些VPN客戶端應用程式是特定於平台的，它們也依賴於作業系統(OS)版本。設定必須完全相同，否則它們無法通訊。

VPN可以使用以下任何一項進行設定：

- 安全通訊端層 (SSL)
- 網際網路通訊協定安全(IPSec)
- 點對點通道通訊協定(PPTP) — 不如SSL或IPSec安全
- 通用路由封裝(GRE)
- 第2層通道通訊協定(L2TP)

如果您以前從未設定過VPN，則將在本文中收到許多新資訊。本指南不是分步指南，而是供參考的更多概述。因此，在繼續操作並嘗試在網路中設定VPN之前，最好完整閱讀本文。具體步驟的連結貫穿本文始終。

思科不支援第三方非思科產品，包括TheGreenBow、OpenVPN、Shrew Soft和EZ VPN。它們嚴格出於指導目的被包括在內。如果您在文章之外需要這些方面的支援，應與第三方聯絡以獲得支援。

使用VPN連線的優點

- 使用VPN連線有助於保護機密的網路資料和資源。
- 它為遠端工作人員或公司員工提供了便利和可訪問性，因為他們可以輕鬆訪問總部資源，而不必親自到場，同時還可以維護專用網路及其資源的安全。
- 與其他遠端通訊方法相比，使用VPN連線的通訊可提供更高級別的安全性。高級加密演算法使這一點成為可能，從而保護私有網路免受未經授權的訪問。
- 使用者的實際地理位置受到保護，不會暴露於公共網路或共用網路（例如Internet）。
- VPN允許新增新使用者或使用者組，而無需新增其他元件或進行複雜的配置。

使用VPN連線的風險

- 由於配置錯誤，可能會存在安全風險。由於VPN的設計和實施可能很複雜，因此有必要將配置連線的任務委託給知識豐富且經驗豐富的專業人士，以確保專用網路的安全不會受到危害。
- 它可能就不那麼可靠了。由於VPN連線需要網際網路連線，因此必須有一個經過驗證和測試的信譽的提供商，以提供卓越的網際網路服務，並保證最短（甚至無停機時間）。
- 如果出現需要新增新基礎架構或新配置的情況，技術問題可能因不相容而產生，尤其是當所使用產品或供應商不是涉及到其他產品或供應商時。
- 可能會出現連線速度慢的情況。如果您使用的是提供免費VPN服務的ISP連線，則連線速度可

能也會很慢，因為這些提供商不優先選擇連線速度。必須注意的是，VPN吞吐量取決於路由器的硬體功能。

有關VPN工作方式的更多資訊，請按一下此處。

配置VPN時使用的提示

1. 配置不同站點之間的VPN時，請在兩端使用不同的LAN IP子網。例如，如果您連線的站點使用192.168.x.x編址方案，則您需要使用10.x.x.x或172.16.x.x - 172.31.x.x子網。另一種方法是使用不同的子網掩碼。當您更改路由器IP地址時，動態主機配置協定(DHCP)上的裝置將自動獲取該子網中的IP地址。
2. 使用路由器WAN介面上的靜態公共IP實現穩定的VPN連線。
3. 確保所選的加密和身份驗證級別與要為VPN建立VPN隧道的路由器相同。
4. 確保輸入的PSK和金鑰生存期與遠端路由器相同。PSK可以是任何您想要的，只要在站點上與客戶端匹配，當他們在其電腦上設定為客戶端時，PSK必須與客戶端匹配。根據裝置的不同，可能存在禁止使用的符號。Key Lifetime是系統更改金鑰的頻率。憑證是優先使用，因為它被認為更安全。
5. 對於大多數VPN，客戶端使用VPN不需要證書，它只是通過路由器進行驗證。例如，OpenVPN需要客戶端和站點證書。
6. 在第I階段設定您的SA生存時間比在第II階段設定SA生存時間長。如果您使第I階段比第II階段短，那麼您將不得不頻繁地來回重新協商隧道，而不是資料隧道。資料隧道需要更高的安全性，因此最好在II階段具有比I階段更短的生存期。
7. 將所有密碼更改為更複雜的密碼。

VPN的型別

安全套接字層(SSL)

Cisco RV34x系列路由器使用AnyConnect支援SSL VPN。RV160和RV260可以選擇使用OpenVPN，這是另一個SSL VPN。SSL VPN伺服器允許遠端使用者使用Web瀏覽器建立安全VPN隧道。此功能可透過SSL超文字傳輸通訊協定安全(HTTPS)瀏覽器支援，使用原生超文字傳輸通訊協定(HTTP)，輕鬆存取各種Web資源和啟用Web的應用程式。

SSL VPN允許使用者通過加密網路流量來使用安全且經過身份驗證的路徑遠端訪問受限網路。

有兩個選項可在SSL中設定訪問：

1. 自簽名證書：由自己的建立者簽名的證書。不建議這樣做，因此只能在測試環境中使用。
2. CA簽名證書：此證書更安全，強烈建議使用。第三方會付費驗證網路是否合法，並建立一個CA證書，然後將其附加到站點。有關CA證書的詳細資訊，請參閱本文的證書部分。

本檔案內提供指向AnyConnect上文章的連結。有關AnyConnect的概述，請按一下此處。

IPsec設定檔

Easy VPN(EZVPN)、TheGreenBow和Shrew Soft是網際網路協定安全(IPSec)VPN。IPSec VPN在

兩個對等體之間或從客戶端到站點提供安全隧道。視為敏感的資料包應該通過這些安全隧道傳送。要保護這些敏感資料包，必須使用雜湊演算法、加密演算法、金鑰生存期和模式等引數，應通過指定這些隧道的特徵來定義這些引數。然後，當IPsec對等路由器看到此類敏感封包時，它會設定適當的安全通道，並將封包透過此通道傳送到遠端對等路由器。

當在防火牆或路由器中實施IPsec時，它提供了強大的安全性，可以應用於所有通過邊界的流量。公司或工作組內的流量不會產生與安全相關的處理開銷。

為了成功加密和建立VPN隧道的兩端，雙方需要就加密、解密和身份驗證的方法達成一致。IPsec設定檔是IPsec中的中央組態，定義加密、驗證和Diffie-hellman(DH)群組等演演算法，用於自動模式以及手動鍵控模式下的第I階段和II階段交涉。

IPsec的重要元件包括網際網路金鑰交換(IKE)第1階段和第2階段。

IKE第一階段的基本用途是驗證IPSec對等體並在對等體之間建立安全通道以啟用IKE交換。IKE第一階段執行以下功能：

- 驗證和保護IPSec對等體的身份
- 在對等體之間協商匹配的IKE安全關聯(SA)策略以保護IKE交換
- 使用具有匹配共用金鑰的最終結果執行經過身份驗證的Diffie-Hellman交換
- 設定安全隧道以協商IKE第二階段引數
- 在主模式和主動模式中發生

IKE第二階段的目的是協商IPSec SA以設定IPSec隧道。IKE第二階段執行以下功能：

- 協商受現有IKE SA保護的IPSec SA引數
- 建立IPSec安全關聯
- 定期重新協商IPSec SA以確保安全性
- （可選）執行額外的Diffie-Hellman交換
- 僅使用一種模式，快速模式

如果在IPSec策略中指定了完全向前保密(PFS)，則在每個快速模式中執行新的DH交換，提供具有更大的熵（金鑰材料壽命）的金鑰材料，從而對加密攻擊具有更大的抵抗力。每個DH交換需要較大的指數值，從而增加CPU使用並消耗效能成本。

- 在RV34x系列路由器上配置網際網路協定安全(IPSec)配置檔案
- 在RV160和RV260上配置IPSec配置檔案（自動金鑰模式）
- 在RV160和RV260路由器上配置IPsec配置檔案手動金鑰模式

點對點通道通訊協定(PPTP)

PPTP是用於建立公共網路之間的VPN隧道的網路協定。PPTP伺服器也稱為虛擬專用撥接網路(VPDN)伺服器。 PPTP有時會用於其他協定，因為它速度更快，並且能夠在流動裝置上工作。但是，必須注意的是，它不如其他型別的VPN安全。有多種方法可連線PPTP型別帳戶。點選連結瞭解更多資訊：

- 在Rv34x系列路由器上配置點對點隧道協定(PPTP)伺服器
- 在Windows的RV320和RV325 VPN路由器系列上配置點對點隧道協定(PPTP)伺服器

通用路由封裝

通用路由封裝(GRE)是一種通道通訊協定，提供了一種簡單的通用方法，透過封裝方式透過另一個通訊協定傳輸其中一個通訊協定的封包。

GRE將有效負載（即需要傳送到外部IP資料包中的目的網路的內部資料包）封裝在一起。GRE通道的工作方式與虛擬點對點連結相同，該虛擬點對點連結具有兩個透過通道來源和通道目的地位址識別的端點。

通道端點會透過介入IP網路路由封裝封包，透過GRE通道傳送負載。沿途的其他IP路由器不會分析負載（內部資料包）；它們只分析外部IP資料包，並將其轉發到GRE隧道端點。到達通道端點時，會移除GRE封裝，並將負載轉送到封包的最終目的地。

網路中資料包的封裝出於多種原因，例如源伺服器想要影響資料包到達目的主機所採用的路由。源伺服器也稱為封裝伺服器。

IP內IP封裝涉及在現有IP報頭上插入外部IP報頭。外部IP標頭中的來源和目的地位址指向IP內IP通道的端點。IP報頭堆疊用於將資料包通過預定路徑轉發到目的地，前提是網路管理員知道傳輸資料包的路由器的環回地址。

此隧道機制可用於確定大多數網路架構的可用性和延遲。應該注意的是，從來源到目的地的整個路徑不必包括在標頭中，但是可以選擇網段來定向資料包。

第2層通道通訊協定

L2TP不為其通道流量的加密機制。相反，它依靠其他安全協定（如IPSec）來加密資料。

在L2TP訪問集中器(LAC)和L2TP網路伺服器(LNS)之間建立L2TP隧道。在這些裝置之間還建立了IPSec隧道，並且所有L2TP隧道流量都使用IPSec進行加密。

L2TP的一些關鍵術語：

- CHAP — 質詢握手身份驗證協定。點對點驗證通訊協定(PPP)。
- L2TP存取集中器(LAC)- LAC可以是連線到公共交換電話網路(PSTN)的Cisco網路存取伺服器。LAC僅需要實現用於通過L2TP操作的介質。LAC可以使用區域網或廣域網（如公共或專用幀中繼）連線到LNS。LAC是傳入呼叫的發起者和傳出呼叫的接收者。
- L2TP網路伺服器(LNS) — 幾乎所有連線到區域網或廣域網（如公共或專用幀中繼）的Cisco路由器都可以充當LNS。它是L2TP協定的伺服器端，必須在任何終止PPP會話的平台上運行。LNS是傳出呼叫的發起者和傳入呼叫的接收者。圖1描述了LAC和LNS之間的呼叫常式。
- 虛擬私人撥號網路(VPDN) — 使用PPP交付服務的存取VPN型別。

如果您想瞭解有關L2TP的詳細資訊，請按一下以下連結：

- 在RV34x路由器上配置L2TP WAN設定
- 廣域網配置指南：第2層服務，Cisco IOS XE版本3S

與Cisco RV系列VPN路由器相容的VPN

	RV34X	RV32X	RV160X/RV260X
IPSec(IKEv1)			
ShrewSoft	是	是	是
格林博	是	是	是
Mac內建客戶端	是	是	否
iPhone/iPad	是	是	否
Android	是	是	是
L2TP/IPSec	是(PAP)	否	否
PPTP	是(PAP)	是*	是(PAP)
其他			
AnyConnect	是	否	否
Openvpn	否	是	是
IKEv2			
Windows	是*	否	是*
Mac	是	否	是
iPhone	是	否	是
Android	是	否	是

VPN技術	支援的裝置	支援的客戶端*	詳細資訊和警告
IPSec(IKEv1)	RV34X、RV32X、RV160X/RV260X	原生：Mac、iPhone、iPad、Android 其他：EasyVPN（Cisco VPN客戶端）、ShrewSoft、Greenbow	最易於設定、故障排除和支援。它可在所有路由器上使用，設定簡單（大多數情況下），具有最佳的日誌記錄進行故障排除。包括大多數裝置。這就是為什麼我們通常推薦ShrewSoft（免費而且有效）和Greenbow（不免費，但是有效）。 對於Windows，我們選擇ShrewSoft和Greenbow客戶端，因為Windows沒有純IPSec本地VPN客戶端。對瑞威軟和綠寶來說，它參與度更高一些，但並不難做到。在首次設定後，可以匯出客戶端配置檔案，然後在其他客戶端匯入。 對於RV160X/RV260X路由器，因為我們沒有Easy VPN選項，因此必須使用第三方客戶端選項，該選項不能用於Mac、iPhone或iPad。不過，我們可以設定ShrewSoft、Greenbow和Android客戶端進

			行連線。對於Mac、iPhone和iPad客戶端，我推薦使用IKEv2（請參閱下文）。
AnyConnect	RV34X	Windows、Mac、iPhone、iPad、Android	某些客戶要求完整的思科解決方案，僅此而已。其設定簡單、具有日誌記錄，但難以理解日誌。需要客戶端許可要求，產生成本。它是一個完整的思科解決方案並且已更新。故障排除並不像IPSec那麼簡單，但比其他VPN選項更好。
L2TP/IPSec	RV34X	原生：Windows	對於需要在Windows中使用內建VPN客戶端的客戶，我將會建議這樣做。以下是兩個警告： 1.我們僅在使用本地身份驗證時支援PAP身份驗證。我們必須進入每個客戶端，選擇可選或不加密，禁用MS-CHAP選項並啟用PAP。這表示使用者名稱/密碼以明文方式傳送。這並不是一筆很大的交易，因為所有內容都使用IPSec加密，並且必須在每個客戶端上進行設定。在Windows上，這是可配置的，但在Mac、iPhone、iPad或Android裝置上不可配置，因此實際上只能由Windows客戶端使用，除非它們具有外部身份驗證伺服器（如Radius或LDAP）。 2.如果路由器位於NAT裝置之後，則在Windows電腦上連線將失敗。因應措施是在每個客戶端上建立登錄檔項，以允許客戶端和路由器上都進行NAT。
IPSec(IKEv2)	RV34X、RV160X/RV260X	原生：Windows、Mac、iPhone、iPad、Android	用於IKEv2的Windows本機客戶端需要證書身份驗證，這需要PKI基礎架構，因為路由器和所有客戶端都需要具有來自同一CA（或其他受信任的CA）的證書。 對於想要使用IKEv2的客戶，我們會為其Mac、iPhone、iPad和Android裝置設定該設定，並且我們通常為其Windows電腦（ShrewSoft、Greenbow或L2TP/IPSec）設定IKEv1。
開放式VPN	RV32X、	Open VPN是客戶端	設定較難，故障排除和支援較難。受

RV160X/RV260X	RV160X/RV260X和RV320支援。設定比IPSec或AnyConnect更複雜，尤其是當它們使用證書時（大多數情況下使用證書）。由於路由器上沒有任何有用的日誌，並且依賴於客戶端日誌，因此故障排除更加困難。此外，OpenVPN客戶端版本更新已無警告地更改了他們接受的證書。此外，我們發現此解決方案在Chromebooks上不起作用，因此必須使用IPSec解決方案。

*我們測試儘可能多的組合，如果有具體的硬體/軟體組合，請訪問此處。否則，請參見相關的配置指南（按裝置），瞭解最新測試版本。

憑證

您曾經訪問過一個網站並收到過它不安全的警告嗎？它不會讓您相信您的私人資訊是安全的，而且它不是安全的！如果站點是安全的，您將在站點名稱前看到一個已關閉的鎖定圖示。這是一個表明該站點已驗證安全的符號。您需確保看到該鎖定圖示已關閉。您的VPN也是如此。

設定VPN時，您應該從憑證授權單位(CA)取得憑證。從第三方站點購買證書並用於身份驗證。這是證明您的站點安全的官方方式。實質上，CA是受信任的來源，用於驗證您的企業是否合法以及是否值得信任。對於VPN，您只需要最低成本的較低級證書。您會由CA簽出，並且他們驗證您的資訊後，會向您頒發證書。此證書可作為檔案下載到您的電腦上。然後，您可以進入您的路由器（或VPN伺服器）並上傳到那裡。

CA在頒發數位證書時使用公鑰基礎架構(PKI)，它使用公鑰或私鑰加密來確保安全。CA負責管理證書請求和頒發數位證書。一些第三方CA包括IdenTrust、Comodo、GoDaddy、GlobalSign、GeoTrust和Verisign。

VPN中的所有網關都必須使用相同的演算法，否則它們將無法通訊。為簡單起見，建議從同一受信任的第三方購買所有證書。這使多個證書更易於管理，因為它們必須手動續訂。

註：客戶端通常不需要證書即可使用VPN；它只是通過路由器進行驗證。OpenVPN是一個例外，它需要客戶端證書。

為簡單起見，有些小型企業會選擇使用密碼或預共用金鑰來代替證書。這種設定安全性較低，但可以免費設定。

有關證書的詳細資訊，請參閱以下連結：

- RV160和RV260系列路由器上的證書（匯入/匯出/生成CSR）
- 在RV34x系列路由器上使用第三方SSL證書替換預設自簽名證書

路由器上的站點到站點VPN

對於本地和遠端路由器，必須確保用於VPN連線的預共用金鑰(PSK)/密碼/證書和安全設定都匹配。如果一個或多個路由器使用大多數Cisco RV系列路由器使用的網路地址轉換(NAT)，則需要為本地和遠端路由器上的VPN連線執行防火牆例外。

如需詳細資訊，請參閱以下站點到站點文章：

- 在RV34x上配置站點到站點VPN
- 在RV340或RV345路由器上配置站點到站點VPN
- Cisco Tech Talk：在RV340系列路由器上配置站點到站點VPN（影片）
- 在RV160和RV260路由器上配置站點到站點VPN（基本設定）
- RV160和RV260路由器上的站點到站點VPN（高級設定和故障轉移）

路由器上的客戶端到站點VPN

在客戶端上設定VPN之前，管理員需要在路由器上對其進行配置。

按一下檢視以下路由器配置文章：

- 在RV160和RV260路由器上配置VPN設定嚮導
- 使用RV160和RV260配置Shrew Soft VPN客戶端
- 思科技術講座：在RV160和RV260上配置軟體VPN（影片）
- 設定並使用GreenBow IPsec VPN客戶端與RV160和RV260路由器連線

建立客戶端到站點配置檔案

在客戶端到站點VPN連線中，來自Internet的客戶端可以連線到伺服器，以訪問伺服器後面的企業網路或LAN，但仍然維護網路及其資源的安全。此功能非常有用，因為它建立了一個新的VPN隧道，允許遠端工作人員和商務旅行者使用VPN客戶端軟體訪問您的網路，而不會損害隱私和安全性。以下文章專用於RV34x系列路由器：

- 在RV34x系列路由器上配置客戶端到站點的虛擬專用網路(VPN)連線
- 在 RV34x 系列路由器上設定 AnyConnect Virtual Private Network (VPN) 連線

如果為源 All Traffic（所有流量）和目標 All Traffic（所有流量）設定了Port Forwarding（埠轉發），則客戶端到站點VPN 將無法工作。

使用者組

在路由器上為共用同一組服務的使用者集合建立使用者組。這些使用者組包括組的選項，如關於如何訪問VPN的許可權清單。根據裝置的不同，可以允許PPTP、站點到站點IPSec VPN和客戶端到站點IPSec VPN。例如，RV260的選項包括OpenVPN，但不支援L2TP。RV340系列配備了用於SSL VPN的AnyConnect，以及強制網路門戶或EZ VPN。

這些設定使管理員能夠進行控制和過濾，以便只有授權使用者才能訪問網路。Shrew Soft和TheGreenBow是兩個最常見的可下載VPN客戶端。它們需要根據路由器的VPN設定進行配置，才能成功建立VPN隧道。以下文章專門介紹了使用者組的建立過程：

- 在RV34x路由器上為VPN設定建立使用者組

為VPN設定使用者組時，請確保將預設管理員帳戶保留在管理組中，並為VPN建立新的使用者帳戶和使用者組。如果將管理員帳戶移動到不同的組，您將阻止自己登入路由器。因此，您必須對該路由器再次執行出廠重置和配置，並單獨保留管理組中的預設管理帳戶。

使用者帳戶

在路由器上建立使用者帳戶是為了允許使用本地資料庫對本地使用者進行身份驗證，用於各種服務，如PPTP、VPN客戶端、Web圖形使用者介面(GUI)登入和安全套接字層虛擬專用網路(SSLVPN)。這樣，管理員就可以控制和過濾僅訪問網路的授權使用者。以下文章專門討論了建立使用者帳戶的問題：

- 為RV34x路由器上的VPN客戶端設定建立使用者帳戶

客戶端位置上的客戶端到站點

在客戶端到站點VPN連線中，來自Internet的客戶端可以連線到伺服器，以訪問伺服器後面的公司網路或LAN，但仍然維護網路及其資源的安全。此功能非常有用，因為它建立了一個新的VPN隧道，允許遠端工作人員和商務旅行者使用VPN客戶端軟體訪問您的網路，而不會影響隱私和安全性。VPN設定為在傳送和接收資料時對資料進行加密和解密。

AnyConnect應用可與SSL VPN配合使用，並且專門用於RV34x路由器。其他RV系列路由器不提供此功能。從版本1.0.3.15開始，不再需要路由器許可證，但需要為VPN的客戶端購買許可證。有關Cisco AnyConnect安全移動客戶端的詳細資訊，請按一下此處。有關安裝說明，請從以下文章中進行選擇：

- 在 Mac 電腦上安裝 Cisco AnyConnect 安全行動用戶端
- 在Windows電腦上安裝Cisco AnyConnect安全移動客戶端

對於所有RV系列路由器的客戶端到站點VPN，可以使用某些第三方應用程式。如前所述，思科不支援這些應用；提供此資訊只是為了提供指導。

GreenBow VPN客戶端是第三方VPN客戶端應用，使主機裝置能夠為客戶端到站點IPsec隧道或SSL配置安全連線。這是一個包含支援的付費應用程式。

- 設定並使用GreenBow IPsec VPN客戶端與RV160和RV260路由器連線

OpenVPN是一個免費的開源應用程式，它可以設定並用於SSL VPN。它使用客戶端 — 伺服器連線，通過Internet在伺服器和遠端客戶端位置之間提供安全通訊。

- RV160和RV260路由器上的OpenVPN

Shrew Soft是一個免費的開源應用程式，可以設定並用於IPsec VPN。它使用客戶端 — 伺服器連線

，通過Internet在伺服器和遠端客戶端位置之間提供安全通訊。

- 使用RV160和RV260配置Shrew Soft VPN客戶端

Easy VPN通常用於RV32x路由器。以下是一些供參考的資訊：

- 在RV320和RV325 VPN路由器系列上配置Easy Client to Gateway虛擬專用網路(VPN)
- Cisco Easy VPN問答
- 基於Cisco IOS軟體的路由器上的Easy VPN

安裝嚮導

最新的Cisco RV系列路由器附帶一個VPN設定嚮導，該嚮導將引導您完成設定步驟。通過VPN設定嚮導，可以配置基本LAN到LAN和遠端訪問VPN連線，並分配預共用金鑰或數位證書進行身份驗證。如需詳細資訊，請參閱以下文章：

- 在RV160和RV260上配置VPN設定嚮導
- 使用RV34x系列路由器上的設定嚮導配置虛擬專用網路(VPN)連線

結論

這篇文章引導您更好地瞭解VPN，並提供了幫助您順利前進的技巧。現在，您應準備好配置自己的配置！花一些時間檢視連結，並確定在Cisco RV系列路由器上設定VPN的最佳方法。

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）。