使用GreenBow VPN客戶端連線RV34x系列路由器

特別宣告:許可結構 — 韌體版本1.0.3.15及更高版本。接下來 ,AnyConnect將只對客戶端許可證收費。

有關RV340系列路由器上的AnyConnect許可的其他資訊,請檢 視<u>RV340系列路由器的AnyConnect許可</u>一文。

簡介

虛擬專用網路(VPN)連線允許使用者通過公共或共用網路(例如Internet)來訪問、傳送和從 專用網路接收資料,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隧道建立私有網路,該私有網路可以使用加密和身份驗證安全地傳送資料。企業辦公室大 多使用VPN連線,因為即使員工不在辦公室,也允許他們訪問其專用網路既有用又必要。

VPN允許遠端主機像位於同一本地網路一樣工作。該路由器最多支援50條隧道。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客戶端完全依賴於 VPN路由器的設定才能建立連線。

GreenBow VPN客戶端是第三方VPN客戶端應用,使主機裝置能夠通過RV34x系列路由器為 站點到站點IPSec隧道配置安全連線。



在圖中,電腦將連線到其網路之外的辦公室的檔案伺服器以訪問其資源。為此,電腦中的 GreenBow VPN客戶端將配置為從RV34x VPN網關提取設定。

使用VPN連線的優點

- 1. 使用VPN連線有助於保護機密的網路資料和資源。
- 2. 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,而無需親 自到場,而且仍然維護專用網路及其資源的安全。
- 9. 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。當今的技術水準已 經使這一點成為可能,從而保護私有網路免受未經授權的訪問。
- 4. 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(如Internet)。
- 5. 由於VPN易於擴展,因此向網路中新增新使用者或使用者組非常容易。無需額外的元件或複雜 的配置即可使網路擴展。

使用VPN連線的風險

- 1. 配置錯誤導致的安全風險。由於VPN的設計和實施可能很複雜,因此必須將配置連線的任務委
 託給知識豐富且經驗豐富的專業人員,以確保專用網路的安全不會受到危害。
- 可靠性。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)。
- 可擴充性。如果需要新增新的基礎架構或新的配置集,則可能會由於不相容性而出現技術問題, 尤其是當涉及的產品或供應商與您正在使用的產品或供應商不同時。
- 流動裝置的安全問題。在流動裝置上啟動VPN連線時,可能會出現安全問題,尤其是當流動裝置無線連線到本地網路時。
- 5. 連線速度慢。如果您使用的是提供免費VPN服務的VPN客戶端,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。

使用GreenBow VPN客戶端的先決條件

以下專案必須首先在VPN路由器上配置,並通過按一下此處<u>建立連線</u>應用於TheGreenBow VPN客戶端。

- 1. 在VPN網關上建立客戶端到站點配置檔案
- 2. <u>在VPN網關上建立使用者組</u>
- 3. 在VPN網關上建立使用者帳戶
- 4. 在VPN網關上建立IPSec配置檔案
- 5. 在VPN網關上配置I階段和II階段設定

適用裝置

• RV34x系列

軟體版本

• 1.0.01.17

使用GreenBow VPN客戶端

<u>在路由器上建立客戶端到站點配置檔案</u>

步驟1.登入到RV34x路由器的基於Web的實用程式,然後選擇VPN > Client-to-Site。



附註:本文中的影象來自RV340路由器。選項可能會有所不同,具體取決於裝置型號。

步驟2.按一下Add。

IPSec Clien	t-to-Site Groups	
Group	_	
Add	Edit	Delete

步驟3.按一下**第三方客戶端**。

附註:AnyConnect是Cisco VPN客戶端的示例,而GreenBow VPN客戶端是第三方VPN客戶 端的示例。



附註:在此示例中,選擇第三方客戶端。

步驟4.在Basic Settings頁籤下,選中Enable覈取方塊以確保VPN配置檔案處於活動狀態。

Basic Settings Ad	vanced Settings	
Enable		
Tunnel Name:		Client
Interface:		WAN1 T

步驟5.在Tunnel Name 欄位中輸入VPN連線的名稱。

Basic Settings	Advanced Settings		
Enable			
Tunnel Name	E.	Client]
Interface:		WAN1 🔻	

附註:在此範例中,輸入Client。

步驟6.從Interface下拉選單中選擇要使用的介面。選項包括WAN1、WAN2、USB1和 USB2,它們將使用路由器上的相應介面進行VPN連線。

Basic Settings	Advanced Settings			
Enable				
Tunnel Name	9:		Client	
Interface:			WAN1 V	1
IKE Authenti	cation Method:		WAN1 WAN2	J
Presha	red Key:		USB1 USB2	
Preshar	ed Key Strength Meter	:		

附註:這些選項取決於您使用的路由器型號。在本示例中,選擇了WAN1。

步驟7.選擇IKE身份驗證方法。選項包括:

- 預共用金鑰(Preshared Key) 此選項允許我們為VPN連線使用共用密碼。
- Certificate 此選項使用的數位證書中包含資訊,例如證書的名稱或IP地址、序列號、到期日 以及證書持有者的公鑰的副本。

IKE Authentication Method:	
Preshared Key:	
Preshared Key Strength Meter:	
Minumum Preshared Key Complexity:	Enable
Show plain text when edit:	Enable
O Certificate:	Default 🔻

附註:在此示例中,選擇預共用金鑰。

步驟8.在預共用金鑰欄位中輸入連線密碼。

IKE Authentication Method:	
Preshared Key:	
Preshared Key Strength Meter:	
Minumum Preshared Key Complexity:	Enable
Show plain text when edit:	Enable

步驟9.(可選)取消選中Minimum Preshared Key Complexity **Enable**覈取方塊以可以使用簡 單密碼。

IKE Authentication Method:	
Preshared Key:	
Preshared Key Strength Meter:	
Minumum Preshared Key Complexity:	Enable
Show plain text when edit:	Enable

附註:在此示例中,保留啟用最小預共用金鑰複雜性。

步驟10。(可選) 選中Show plain text when edit Enable 覈取方塊以純文字檔案顯示密碼。

IKE Authentication Method:	
Preshared Key:	•••••
Preshared Key Strength Meter:	
Minumum Preshared Key Complexity:	Enable
Show plain text when edit:	Enable

附註:在此示例中,禁用編輯時顯示純文字檔案。

步驟11.從Local Identifier下拉選單中選擇本地識別符號。選項包括:

- •本地WAN IP 此選項使用VPN網關的廣域網(WAN)介面的IP地址。
- IP地址 此選項允許您手動輸入VPN連線的IP地址。
- FQDN 此選項也稱為完全限定域名(FQDN)。 它允許您對Internet上的特定電腦使用完整的域 名。
- 使用者FQDN 此選項允許您對Internet上的特定使用者使用完整的域名。

AN IP 🔻 124.6.115.177.
AN IP
ess 124.6.177.118
2DN ₿

附註:在本示例中,選擇本地WAN IP。使用此選項,將自動檢測本地WAN IP。

步驟12。(可選)選擇遠端主機的識別符號。選項包括:

- IP地址 此選項使用VPN客戶端的WAN IP地址。
- FQDN 此選項允許您對Internet上的特定電腦使用完整的域名。
- 使用者FQDN 此選項允許您對Internet上的特定使用者使用完整的域名。

Local Identifier:	Local WAN IP V 124.6.115.177.
Remote Identifier:	IP Address T 124.6.177.118 IP Address
Extended Authentication:	User FQDN

附註:在本例中,選擇了IP地址。

步驟13.在這端識別符號欄位中輸入遠端識別符號。

Local Identifier:	Local WAN IP	124.6.115.177.
Remote Identifier:	IP Address 🔻	124.6.177.118

附註:在本示例中,輸入了124.6.115.177。

步驟14。(可選)勾選**Extended Authentication**覈取方塊以啟用該功能。啟用後,這將提供額 外的身份驗證級別,要求遠端使用者在獲得對VPN的訪問許可權之前輸入其憑據。

	Group Name
Extended Authentication:	
~	Add Delete

附註:在本示例中,擴展身份驗證未選中。

步驟15.在「組名」下,按一下Add。

	Group Na	me
Extended Authentication:		
	Add	Delete

步驟16.從Group Name下拉選單中選擇將使用擴展身份驗證的組。

Group Name	
admin 🔹	
admin guest	
IPSecVPN	
VPN	

附註:在此示例中,選擇VPN。

步驟17.在Pool Range for Client LAN下,在*Start IP*欄位中輸入可分配給VPN客戶端的第一個 IP地址。

Pool Range for Client LAN:	
Start IP:	10.10.100.100
End IP:	10.10.100.245

附註:在此示例中,輸入了10.10.100.100。

步驟18.在End IP欄位中輸入可分配給VPN客戶端的最後一個IP地址。

Pool Range for Client LAN:	
Start IP:	10.10.100.100
End IP:	10.10.100.245

附註:在此示例中,輸入了10.10.100.245。

步驟19.按一下Apply。

8 Save

	Pool Range for Client LAN:	
	Start IP:	10.10.100.100
	End IP:	10.10.100.245
	Apply Cancel	
ł	步驟20.按一下 「Save 」。	

cisco (admin) Log Out About

Help

現在,您應該在路由器上為TheGreenBow VPN客戶端配置客戶端到站點配置檔案。

<u>建立使用者組</u>

步驟1.登入到路由器的基於Web的實用程式,然後選擇**System Configuration > User Groups**。

附註:本文中的影象來自RV340路由器。選項可能會因裝置型號而異。

Getting Started
 Status and Statistics
 Administration
 System Configuration
Initial Setup Wizard
System
Time
Log
Email
User Accounts
User Groups
IP Address Group
SNMP
Discovery-Bonjour
LLDP
Automatic Updates
Service Management
Schedule

步驟2.按一下Add以新增使用者群組。

U	ser	Groups	3			
	Us	er Groups ⁻	Table			
		Group		Web Login	I	S2S-VPN
		admin		Admin		Disabled
		guest		Disabled		Disabled
		Add	Ed	lit	Delete	
		Apply	Cance	el		

步驟3.在「概覽」區域的「組名稱」欄位中輸入組名稱。

User Groups					
Overview Group Name VPN					
Local	User Men	nbership List			
#	Join	User Name	Joined Groups *		
1	I	CiscoTest	VPN		
2		cisco	admin		
3		guest	guest		
4 🕑 vpnuser VPN					
* Should have at least one account in the "admin" group					

附註:本示例使用VPN。

步驟4.在Local Membership List下,選中需要位於同一組中的使用者名稱的覈取方塊。

User Groups				
Overview Group Name: VPN				
Local	User Mem	ibership List		
#	Join	User Name	Joined Groups *	
1		CiscoTest	VPN	
2		cisco	admin	
3		guest	guest	
4		vpnuser	VPN	
* Should have at least one account in the "admin" group				

附註:在本例中,選擇了CiscoTest和vpnuser。

步驟5.在「服務」下,選擇要授予組中的使用者的許可權。選項包括:

- •已禁用 此選項表示不允許組成員通過瀏覽器訪問基於Web的實用程式。
- 只讀 此選項表示組的成員只有在登入後才能讀取系統的狀態。它們無法編輯任何設定。
- 管理員 此選項為組的成員提供讀寫許可權,並能夠配置系統狀態。

Services					
Web Login	\bigcirc	Disabled 🔘	Read Only	\bigcirc	Administrator

附註:在此範例中,選擇了「唯讀」。

步驟6.在EzVPN/第三方配置檔案成員使用表中,按一下Add。

EzVPN/3rd Party	EzVPN/3rd Party Profile Member In-use Table		
		#	Group Name
		Add	Delete

步驟7.從「選擇配置檔案」下拉選單中選擇配置檔案。選項可能會有所不同,具體取決於 VPN網關上配置的配置檔案。

Add Feature List			
Select a Profile	Clients T		
Add	Cancel		

- 附註:在本例中,選擇了Clients。
- 步驟8.按一下Add。

Add Feature List		
Select a Profile	e: Clients ▼ Clients	
Add	Cancel	

步驟9.按一下Apply。



步驟10.按一下「Save」。



現在,您應該已經在RV34x系列路由器上成功建立了使用者組。

建立使用者帳戶

步驟1.登入到路由器的基於Web的實用程式,然後選擇**System Configuration > User Accounts**。

附註:本文中的影象來自RV340路由器。選項可能會因裝置型號而異。



步驟2.在Local User Membership List區域中,按一下Add。

User Accounts			
Local Users Password Complexity Password Complexity Settings: Description Enable Local Users			
Local User Mem	bership List		
📄 # Us	er Name		Group *
🗌 1 gu	est		VPN
2 cis	со		admin
Add	Edit	Delete	Import

步驟3.在User Name欄位中輸入使用者的名稱。

User Accounts		
Add User Account		
User Name	CiscoTest	
New Password	•••••	
New Password Confirm	••••••	
Group	VPN V	
Apply Cance	2	

附註:在此範例中,輸入CiscoTest。

步驟4.在New Password欄位中輸入使用者密碼。

User Accounts		
Add User Account		
User Name	CiscoTest	
New Password	•••••	
New Password Confirm		
Group	VPN V	
Group	VPN T	

步驟5.在New Password Confirm框中確認密碼。

User Accounts		
Add User Account		
User Name	CiscoTest	
New Password	•••••	
New Password Confirm		
Group		
Oroup	VPN V	
	VPN V	

步驟6.從「組」下拉選單中選擇一個組。這是將與使用者關聯的組。

Group		VP	NV
		VP	N
		aur	mn
		gue	est
Apply	Cance		

附註:在此示例中,選擇VPN。

步驟7.按一下Apply。

User Accounts		
Add User Accou	Int	
User Name	CiscoTest	
New Password	•••••	
New Password Cont	firm •••••	
Group	VPN V	
Apply C	ancel	

步驟8.按一下「Save」。



您現在應該已經在RV34x系列路由器上建立使用者帳戶。

配置IPSec配置檔案

步驟1.登入到RV34x路由器的基於Web的實用程式,然後選擇**VPN > IPSec Profiles**。



附註:本文中的影象來自RV340路由器。選項可能會因裝置型號而異。

步驟2. IPSec簡檔表顯示現有簡檔。按一下Add建立新配置檔案。

PSe	c Profiles	
IPs	ec Profiles Table	
	Name	Policy
\odot	Amazon_Web_Services	Auto
\odot	Default	Auto
\bigcirc	Microsoft_Azure	Auto
	Add Edit Clone Delet	e
Ap	Cancel	

附註:Amazon_Web_Services、Default和Microsoft_Azure是預設配置檔案。

步驟3.在Profile Name 欄位中建立檔案的名稱。配置檔名稱只能包含字母數字字元以及特殊字 元的下劃線(_)。

IPSec Profiles					
	Add a New IPSec Profile				
	Profile Name:	Clie	ent		
	Keying Mode	۲	Auto	\bigcirc	Manual

附註:在本示例中,輸入客戶端。

步驟4.按一下單選按鈕以確定配置檔案將用於進行身份驗證的金鑰交換方法。選項包括:

- 自動(Auto) 自動設定策略引數。此選項使用Internet金鑰交換(IKE)策略進行資料完整性和加密金鑰交換。如果選擇此選項,則啟用Auto Policy Parameters區域下的配置設定。如果選擇此選項,請跳至配置自動設定。
- 手動(Manual) 此選項允許您手動配置VPN隧道的資料加密和完整性的金鑰。如果選擇此選項 ,則啟用Manual Policy Parameters區域下的配置設定。如果選擇此選項,請跳至<u>配置手動設定</u>

IPSec Profiles			
	Add a New IPSec Profile		
	Profile Name:	Client	
	Keying Mode	🗿 Auto 🔍 Manual	

附註:在本示例中,選擇了Auto。

<u>配置|階段和||階段設定</u>

0

步驟1。在Phase 1 Options區域中,從DH Group下拉選單中選擇要與Phase 1中的金鑰一起 使用的適當Diffie-Hellman(DH)組。Diffie-Hellman是一種加密金鑰交換協定,用於交換預共用 金鑰集。演算法的強度由位決定。選項包括:

• Group2-1024位 — 此選項計算金鑰的速度較慢,但比組1更安全。

• Group5-1536位 — 此選項計算金鑰最慢,但最安全。

Phase I Options	
DH Group:	Group5 - 1536 bit 💌
Encryption:	Group2 - 1024 bit
Encryption.	Groupo - 1536 bit
Authentication:	SHA1 V
SA Lifetime:	86400
Perfect Forward Secrecy:	Enable

附註:在本例中,選擇了Group5-1536位。

步驟2.從Encryption下拉選單中,選擇一種加密方法以加密和解密封裝安全負載(ESP)和網際 網路安全關聯和金鑰管理協定(ISAKMP)。 選項包括:

- 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。

Phase I Options	
DH Group:	Group5 - 1536 bit 🔻
Encryption:	AES-128 V
Authentication:	AES-128
SA Lifetime:	AES-192 AES-256
Perfect Forward Secrecy:	Enable

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。在此範例中,選擇AES-128。

步驟3.從Authentication下拉選單中,選擇確定ESP和ISAKMP身份驗證方式的身份驗證方法。 選項包括:

- 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。

Phase I Options	
DH Group:	Group5 - 1536 bit 🔻
Encryption:	AES-128 •
Authentication:	SHA1 V
SA Lifetime:	MD5 SHA1
Perfect Forward Secrecy:	SHA2-230 Senable

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,然後建立通常無法再 現的唯一的十六進位制輸出。在此範例中,選擇SHA1。

步驟4.在*SA Lifetime*欄位中,輸入介於120和86400之間的值。這是Internet金鑰交換(IKE)安全 關聯(SA)在該階段保持活動狀態的時間長度。預設值為 28800。

Phase I Options	
DH Group:	Group5 - 1536 bit 🔻
Encryption:	AES-128 V
Authentication:	SHA1 T
SA Lifetime:	86400
Perfect Forward Secrecy:	Enable

附註:在此範例中,86400入錯誤。

步驟5.(可選)選中**Enable** Perfect Forward Secrecy覈取方塊以生成IPSec流量加密和身份驗 證的新金鑰。

Phase I Options	
DH Group:	Group5 - 1536 bit 🔻
Encryption:	AES-128 •
Authentication:	SHA1 T
SA Lifetime:	86400
Perfect Forward Secrecy:	Enable

附註:在此範例中,已啟用「完全向前保密」。

步驟6.從Phase II Options區域的Protocol Selection下拉選單中,選擇要應用於協商第二階段 的協定型別。選項包括:

- ESP 此選項封裝要保護的資料。如果選擇此選項,請繼續步驟7以選擇加密方法。
- AH 此選項也稱為身份驗證報頭(AH)。 它是一種安全協定,提供資料身份驗證和可選的反重 播服務。AH嵌入到要保護的IP資料包中。如果選擇此選項,請跳至步驟8。

Phase II Options	
Protocol Selection:	ESP V
Encryption:	ESP AH
Authentication:	SHA1 V
SA Lifetime:	3600
DH Group:	Group5 - 1536 bit 🔻
Apply Cancel	

附註:在本示例中,選擇了ESP。

<u>步驟7</u>.如果在步驟6中選擇了ESP,請選擇確定ESP和ISAKMP身份驗證方式的身份驗證方法 。選項包括:

- 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。

Phase II Options	
Protocol Selection:	ESP •
Encryption:	AES-128 T
Authentication:	AES-128
SA Lifetime:	AES-192 AES-256
DH Group:	Group5 - 1536 bit 🔻
Apply Cancel	

附註:在此範例中,選擇AES-128。

<u>步驟8</u>.從Authentication下拉選單中,選擇一種將確定ESP和ISAKMP身份驗證方式的身份驗證 方法。選項包括:

- 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。

Phase II Options	
Protocol Selection:	ESP v
Encryption:	AES-128 •
Authentication:	SHA1 V
SA Lifetime:	MD5 SHA1
DH Group:	SHA2-256 Groups - 1550 Dit +
Apply Cancel	

附註:在此範例中,選擇SHA1。

步驟9.在*SA Lifetime*欄位中,輸入介於120和28800之間的值。這是IKE SA在此階段保持活動 狀態的時間長度。預設值為 3600。

步驟10.從DH組下拉選單中,選擇要與階段2中的金鑰一起使用的DH組。選項包括:

• Group2-1024位 — 此選項計算金鑰的速度較慢,但比Group1更安全。

• Group5-1536位 — 此選項計算金鑰最慢,但最安全。

Phase II Options	
Protocol Selection:	ESP 🔻
Encryption:	AES-128 •
Authentication:	SHA1 T
SA Lifetime:	3600
DH Group:	Group5 - 1536 bit 🔻
Apply Cancel	

附註:在此範例中輸入3600。

步驟11.按一下Apply。

IPSec Profiles	
Add a New IPSec Profile	
Profile Name:	Client
Keying Mode	🖲 Auto 💛 Manual
Phase I Options	
DH Group:	Group5 - 1536 bit 🔻
Encryption:	AES-128 V
Authentication:	SHA1 V
SA Lifetime:	86400
Perfect Forward Secrecy:	Enable
Phase II Options	
Protocol Selection:	ESP V
Encryption:	AES-128 V
Authentication:	SHA1 T
SA Lifetime:	3600
DH Group:	Group5 - 1536 bit 🔻
Apply Cancel	

步驟12.按一下Save以永久儲存組態。



現在,您應該已經在RV34x系列路由器上成功配置了Automatic IPSec Profile。

配置手動設定

步驟1.在*SPI-Incoming*欄位中,為VPN連線上的傳入流量的安全引數索引(SPI)標籤輸入從 100到FFFFFF的十六進位制值。SPI標籤用於區分一個會話的流量和其他會話的流量。

Manual Policy Parameters	
SPI-Incoming:	0xABCD
SPI-Outgoing:	0×1234

步驟2.在*SPI-Outgoing*欄位中,為VPN連線上的傳出流量的SPI標籤輸入從100到FFFFFF的 十六進位制值。

Manual Policy Parameters	
SPI-Incoming:	0xABCD
SPI-Outgoing:	0x1234

附註:在此示例中,輸入0x1234。

步驟3.從下拉選單中選擇加密值。選項包括:

- 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。

SPI Incoming:	3DES
SPI Outgoing:	AES-128 AES-192
Encryption:	✓ AES-256

附註:在此範例中,選擇AES-256。

步驟4.在Key-In欄位中輸入入站策略的金鑰。金鑰的長度取決於步驟3中選擇的演算法。

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1212121

附註:在此示例中123456789123456789123輸入.....。

步驟5.在Key-Out欄位中輸入傳出策略的金鑰。金鑰的長度取決於步驟3中選擇的演算法。

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1212121

附註:在此範例中,輸入1a1a1a1a1a12121212...。

步驟6.從Authentication下拉選單中選擇身份驗證方法。選項包括:

• 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。

Authentication:	✓ MD5	
Key-In	SHA1 SHA2-256	
Key-Out		

附註:在本例中,選擇了MD5。

步驟7.在Key-In欄位中輸入入站策略的金鑰。金鑰的長度取決於步驟6中選擇的演算法。

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1212121

附註:在此示例中123456789123456789123輸入.....。

步驟8.在Key-Out欄位中輸入傳出策略的金鑰。金鑰的長度取決於步驟6中選擇的演算法。

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a121212 ⁻

附註:在此範例中,輸入1a1a1a1a1a12121212...。

步驟9.單 Apply 擊。

步驟10.按一下Save以永久儲存組態。



現在,您應該已經在RV34x系列路由器上成功配置手動IPSec配置檔案。

配置GreenBow VPN客戶端軟體

配置階段1設定

步驟1.按一下右鍵GreenBow VPN Client圖示並選擇Run as administrator。



步驟2.在VPN配置下的左窗格中,按一下右鍵IKE V1,然後選擇New Phase 1。

😔 TheGreenBo	ow VPN Client		- • • ×
Configuration	Tools ?		
THEGF	REENBOU		
			VPN Client
		IKE V1	
VPN Configu	ration	IKE V1	
	Export		
8-0	Cours	E V1 Configuration	
	Save	Ctri+S	
	New Phase 1	Ctrl+N his folder enables the creation of IKE V1 tunnels. It is pose	sible to
SSL		menu (right dick on IKE V1) enables to create, copy or past and Phases 2.	e Phases 1
		IKE V1 IPsec tunnel creation wizard	
		Export all IKE V1 tunnels	
VPN Client	ready		

步驟3.在Addresses下的Authentication頁籤中,驗證Interface區域中的IP地址與安裝了 GreenBow VPN客戶端的電腦的WAN IP地址相同。

附註:在本例中,IP地址為124.6.177.118。

ItheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOU		VDN Client
		VPN Glient
	Ikev1Gateway: Authen	ntication
VPN Configuration KE V1 KE V1 KE V1 Parameters Control typestIPV4 Control typestIPV4 Control typestIPV6 Control typestI	Authentication Advanced Certific Addresses Interface 124. Remote Gateway 124 Authentication © Preshared Key Confirm © Certificate	ficate .6.177.118 4.6.115.177

步驟4.在Remote Gateway欄位中輸入遠端網關的地址。

附註:在本示例中,遠端RV34x路由器的IP地址為124.6.115.177。

Interview Client			
Configuration Tools ?			
THEGREENBOU	J		
			VPN Client
	Ikev1Gateway: Authen	tication	
VPN Configuration	Authentication Advanced Certifi	cate	
	Addresses Interface 124. Remote Gateway 124 Authentication	6.177.118 .6.115.177	
	Preshared Key	•••••	
	Confirm	•••••	
	Certificate		

步驟5.在Authentication下,選擇身份驗證型別。選項包括:

- 預共用金鑰(Preshared Key) 此選項允許使用者使用已在VPN網關上配置的密碼。使用者必 須匹配密碼才能建立VPN隧道。
- 證書(Certificate) 此選項將使用證書來完成VPN客戶端和VPN網關之間的握手。

Cient Client		
Configuration Tools ?		
THEGREENBOW		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate Addresses Interface 124.6.177.118 Remote Gateway 124.6.115.177 Authentication Oreshared Key Confirm Ocertificate	

附註:在本示例中,選擇預共用金鑰以匹配RV34x VPN網關的配置。

步驟6.輸入在路由器中配置的預共用金鑰。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOU		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration VPN Configuration VE V1 IKE V1 Parameters o tgbtestIPV4 tgbtestIPV6 Ikev1Gateway IKE V2 SSL	Authentication Advanced Certificate Addresses Interface 124.6.177.118 Remote Gateway 124.6.115.177 Authentication Preshared Key Confirm Confirm Confirm	

步驟7.在Confirm欄位中輸入相同的預共用金鑰。

TheGreenBow VPN Client	
Configuration Tools ?	
THEGREENBOI	
	VPN Client
	Ikev1Gateway: Authentication
VPN Configuration	Authentication Advanced Certificate
IKE V1 Parameters UptestIPV4	Addresses
└─ o tgbtestIPV4 □── tgbtestIPV6	Interface 124.6.177.118
↓ gbtestIPV6	Remote Gateway 124.6.115.177
IKE V2	Authentication
	Preshared Key
	Confirm •••••
	Certificate

步驟8.在IKE下,設定加密、身份驗證和金鑰組設定以匹配路由器的配置。

- O -X

Configuration Tools ?

TheGreenBow VPN Client

VPN C	
	lient
Ikev1Tunnel: IPsec	
VPN Configuration IPsec Advanced Automation Remote Sharing IPv4 Iter V1 Iter V1 Parameters Addresses VPN Client address 192.168.10.8 I tpbtestIPV4 tpbtestIPV6 tpbtestIPv6 Subnet address VPN Client address 192.168.10.8 I DKE V2 SSL SSL Subnet mask 255.255.255.0 I ESP Encryptor AES128 Authentication SHA-1 Mode PFS Group DH5 (1536) I I I	
VPN Client ready	

步驟9.按一下Advanced索引標籤。

	VPN Client
Ikev1Gateway: Authen	tication
Authentication Advanced Certific	cate
Authentication Advanced Certific	cate

步驟10。(可選)在Advanced features下,選中**Mode Config**和**Aggressive Mode**覈取方塊 ,並將NAT-T設定設定為Automatic。

	×

TheGreenBow VPN Client Configuration Tools ?

THEGREENBOW

				VPN Client
VPN Configuration KE V1 KE V1 KE V1 Parameters Kev1Gateway Guidential to btestIPV4	Ikev1Gateway: Aut Authentication Advanced Advanced features	certificate Redund Gate	on lant way	
G-C tgbtestIPV6 L⊙ tgbtestIPV6 L⊙ tgbtestIPV6 IKE V2 SSL	Aggressive Mode X-Auth X-Auth Popup Hybrid Mode	Lo Passw	AT-T Automatic	
	Local and Remote II	.		
	Type of ID:	Ň	/alue for the ID:	
	Local ID IP Address	-	124.6.177.115	
	Remote ID IP Address	•	124.6.177.118	
VPN Client ready				

附註:啟用模式配置後,GreenBow VPN客戶端將從VPN網關提取設定以嘗試建立隧道,同時啟用主動模式和NAT-T使建立連線更快。

步驟11。(可選)在X-Auth下,勾選X-Auth Popup覈取方塊以在啟動連線時自動拉出登入視 窗。使用者可在登入視窗輸入其憑證以完成隧道。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate	
IKE V1	Advanced features	
- Ikev1Gateway	Redundant	
tgbtestIPV4	Mode Config Gateway	
□-□ tgbtestIPV6	✓ Appressive Mode NAT-T	Automatic
- o tgbtestIPV6		
IKE V2	X-Auth	
	Auth Popup Login	vpnuser
	Hybrid Mode Password	•••••
	Local and Remote ID	
	Type of ID: Valu	e for the ID:
	Local ID IP Address 💌 12	4.6.115.177
	Remote ID IP Address	4.6.177.118
VPN Client ready		

附註:在本示例中,未選中X-Auth Popup。

步驟12.在Login欄位中輸入您的使用者名稱。這是為在VPN網關中建立使用者組而配置的使用者名稱。



步驟13.在Password欄位中輸入密碼。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate	
IKE V1 IKE V1 Parameters	Advanced features	
- Ikev1Gateway	Redundant	
o tgbtestIPV4	Gateway	
tgbtestIPV6 tobtestIPV6	Aggressive Mode NAT-T Automatic	•
IKE V2	X-Auth	
55L	X-Auth Popup Login vpnuser	
	Browned Anda	-
	nyunu Hobe Password	
	Local and Remote ID	
	Type of ID: Value for the ID:	
	Local ID IP Address	
	Remote ID IP Address	
VPN Client ready		

步驟14.在Local和Remote ID下,設定Local ID和Remote ID以匹配VPN網關的設定。

IntegreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate	
IKE V1 Parameters	Advanced features	
- Ikev1Gateway	Redundant	
e-c tgbtestIPV4	Mode Config Gateway	
E- tgbtestIPV6	☑ Aggressive Mode NAT-T	Automatic 👻
- o tgbtestIPV6		
SSL	X-Auth	
	X-Auth Popup Login	vpnuser
	Hybrid Mode Password	•••••
	Local and Remote ID	
	Type of ID: Value	e for the ID:
	Local ID IP Address • 124	.6.115.177
	Remote ID IP Address • 124	.6.177.118
 VPN Client ready 		

附註:在本示例中,本地ID和遠端ID都設定為IP地址以匹配RV34x VPN網關的設定。

步驟15.在ID的值下,在各自的欄位中輸入本地ID和遠端ID。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOL		VPN-Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate	
IKE V1 Parameters	Advanced features	
	Mode Config Redundant Gateway	
□-□ tgbtestIPV6 □ ○ tgbtestIPV6	Aggressive Mode NAT-T Automatic	•
SSL	X-Auth	
	X-Auth Popup Login vpnuser	
	Hybrid Mode Password	•
	Local and Remote ID	
	Type of ID: Value for the ID:	_
	Local ID IP Address • 124.6.115.177	
	Remote ID IP Address • 124.6.177.118	
VPN Client ready	^	

步驟16.按一下Configuration > Save以儲存設定。

Check Content	Transa Contra Co	
Configuration Tools ?		
Save	Ctrl+S	
Import		VPN Client
Export	v1Gateway: Authentication	
Move to USB Drive	nentication Advanced Certificate	
Wizard	Advanced features	
Quit	Mode Config Redundant Gateway	
E-C tgbtestIPV6	Aggressive Mode NAT-T Automatic	•
IKE V2	V A.M	

配置階段2設定

步驟1.按一下右鍵Ikev1Gateway。

TheGreenBow VPN Client			l	
Configuration Tools ?				
THEGREENBOW				
				VPN Client
	Ikev1Gateway: Authen	tication		
VPN Configuration	Authentication Advanced Certifi	icate		
IKE V1	Advanced features			
Ikev1Gateway	V Mode Config	Redundant Gateway		
E-□ tgbtestIPV6	Aggressive Mode	NAT-T	Automatic	-
IKE V2	X-Auth			

步驟2.選擇**新階段2**。

TheGreenBow VPN Clien	t					
Configuration Tools ?						
THEGREENB	ОШ					
						VPN Client
	lke	v1Gatew	ay: Au	thentication		
VPN Configuration	Auti	hentication A	dvanced	Certificate		
IKE V1		Advanced f	eatures			
	Сору	Ctrl+0		Redundant		
- o tgbtestI	Rename	E2	2	Gateway		
□-□ tgbtestIPV6 □-□ tgbtestI	Delete	De	I Mode	NAT-T	Automatic	•
	New Phase 2	2 Ctrl+N	-			
			-		-	

步驟3.按一下IPsec選項卡。

TheGreenBow VPN Client			
Configuration Tools ?			
THEGREENBOW			
			VPN Client
			the officient
	Ikev1Tunnel: IPsec		
VPN Configuration	IPsec Advanced Automation Remo	ote Sharing	IPV4 IPV6
IKE V1 IKE V1 Parameters	Addresses		
	VPN Client address	192 . 168 . 10 . 8	•
- o tgbtestIPV4	Address type	Subnet address	-
tgbtestIPV6 tgbtestIPV6	Remote LAN address	192 . 168 . 1 . 0	- I
IKE V2	C hoat mark	255 255 255 0	- 1
SSL	Sourcemask	255 . 255 . 255 . 0	
	ESP		
	Encryption	Auto 💌	
	Authentication	Auto 👻	
	Mode	Tunnel	
	PES		
	PFS Group	Ŧ	
VPN Client ready			

步驟4.從Address type下拉選單中選擇VPN客戶端可以訪問的地址型別。

😳 TheGreenBow VPN Client	Trans.	- • ×
Configuration Tools ?		
THEGREENBOW		
		VPN Client
		IT IT CHOIL
	Ikev1Tunnel: IPsec	
VPN Configuration	IPsec Advanced Automation Remote Sharing	IPV4 IPV6
IKE V1	Addresses	
- Ikev1Gateway	102 100 10 0	
☐ ○ Ikev1Tunnel	VPN Client address 192 . 108 . 10 . 8	•
i o tgbtestIPV4	Address type Subnet address	-
- tgbtestIPV6	Citagle address	
tgbtestIPV6	Remote LAN address Subnet address	
SSL	Subnet mask 255 . 255 . 255 . 0	_
	ESP	
	Farmalian Auto	
	Encryption Auto +	
	Authentication Auto 💌	
	Mode Tunnel 💌	
	PFS	
	PFS Group v	
VPN Client ready		

附註:在本例中,選擇了子網地址。

步驟5.在Remote LAN address欄位中輸入應由VPN隧道訪問的網路地址。



附註:在本示例中,輸入了192.168.100.1。

步驟6.在Subnet mask欄位中輸入遠端網路的子網掩碼。

附註:在本例中,輸入了255.255.255.0。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
		TH OHEIR
	Ikev1Tunnel: IPsec	
VPN Configuration	IPsec Advanced Automation Repote Sharing	IPV4 IPV6
IKE V1	Addresses	
⊟-⊡ Ikev1Gateway	VPN Client address 192 . 168 . 10 . 8	
tgbtestIPV4 o tgbtestIPV4	Address type Subnet address	
i⊡⊡ tgbtestIPV6	Remote LAN address 192 . 168 . 1 . 0	
TKE V2	Subnet mask 255 . 255 . 255 . 0	

步驟7.在ESP下,設定加密、身份驗證和模式以匹配VPN網關的設定。

- O X TheGreenBow VPN Client Configuration Tools ? THEGREENBOW **VPN** Client Ikev1Tunnel: IPsec IPV4 IPV6 IPsec Advanced Automation Remote Sharing VPN Configuration 🖻 - 🗁 IKE V1 IKE V1 Parameters Addresses - Ikev1Gateway 192 . 168 . 10 . 8 T VPN Client address Ikev1Tunnel ⊡−□ tgbtestIPV4 tgbtestIPV4 Address type Subnet address -⊡ tgbtestIPV6 192 . 168 . 1 . 0 d tgbtestIPV6 Remote LAN address - 🛅 IKE V2 Subnet mask 255 . 255 . 255 . 0 - CI SSL ESP -Encryption AES128 ٠ Authentication SHA-1 • Mode Tunnel Ŧ PFS -V PFS Group DH5 (1536) -VPN Client ready

步驟8.(可選)在PFS下,勾選**PFS**覈取方塊以啟用完全向前保密(PFS)。PFS生成用於加密 會話的隨機金鑰。

TheGreenBow VPN Client				
Configuration Tools ?				
THEGREENBOW				
		VPN Client		
		TH OICHT		
	Ikev1Tunnel: IPsec			
VPN Configuration	IPsec Advanced Automation Rem	tote Sharing		
IKE V1	IKE V1 Addresses Addresses			
- Ikev1Gateway	VDN Classt address	192 . 168 . 10 . 8		
tabtestIPV4	VEN CICIL DOULESS			
- o tgbtestIPV4	Address type	Subnet address 🔹		
□ tgbtestIPV6	Remote LAN address	192 . 168 . 1 . 0		
	Si boat mark	255 255 255 0		
SSL	Juditechidak	233 . 233 . 233 . 0		
	ESP			
	Encryption	AES128 -		
	Authentication	SHA-1 -		
	Mode	Tunnel		
	PFS			
	Group	DH5 (1536) 🔻		
 VPN Client ready 				

步驟9.從Group下拉選單中選擇PFS組設定。

附註:在本例中,選擇DH5(1536)以匹配路由器的DH組設定。

TheGreenBow VPN Client Configuration Tools ? THEGREENBOW **VPN** Client Ikev1Tunnel: IPsec VPN Configuration IPV4 IPV6 IPsec Advanced Automation Remote Sharing 😑 🥟 IKE V1 IKE V1 Parameters Addresses - Ikev1Gateway 192 . 168 . 10 . 8 VPN Client address i i Ikev1Tunnel igbtestIPV4 tgbtestIPV4 Address type Subnet address • ⊨ gbtestIPV6 192 . 168 . 1 . 0 tgbtestIPV6 Remote LAN address IKE V2 Subnet mask 255 . 255 . 255 . 0 -🛅 SSL ESP -Encryption AES128 ٠ Authentication SHA-1 • Mode Tunnel ٠ PFS PFS Group ÷ DH1 (768) DH5 (1536) DH14 (2048) DH15 (3072) DH16 (4096) DH17 (6144) DH18 (8192) VPN Client ready

步驟10.按一下右鍵Configuration並選擇「儲存」。

TheGreenBow VPN Client		
Configuration Tools ?		
Save Ctrl+S	s	
Import		VPN Client
Export		
Move to USB Drive	v1Tunnel: IPsec	
MOVE TO USD Drive	C Advanced Automation Remote Sharing	IPV4 IPV6
Wizard	Addresses	
Quit	VPN Client address 192 . 168 . 10	. 8 📑
e-c tgbtestIPV4		
	Address type Subnet address	•
- o tgbtestIPV6	Remote LAN address 192 . 168 . 1	. 0
IKE V2	Subnet mask 255 . 255 . 255	. 0
	rcn	
	CSP	
	Encryption AES128	
	Authentication Auto 💌	
	Mode Tunnel 💌	
	PFS	
	Group DH2 (1024)	
 VPN Client ready 		

您現在應該已經成功配置TheGreenBow VPN客戶端,通過VPN連線到RV34x系列路由器。

啟動VPN連線

步驟1.按一下右鍵TheGreenBow VPN Client並選擇Run as administrator。



步驟2.選擇您需要使用的VPN連線,然後按一下**OPEN**。VPN連線應自動啟動。



附註:在本示例中,選擇了配置的Ikev1Gateway。

驗證VPN狀態

步驟1.登入到VPN網關的基於Web的實用程式。

步驟2.選擇Status and Statistics > VPN Status。



步驟3.在Client-to-Site Tunnel Status下,檢查Connection表的Connections列。

附註:在本示例中,已建立了一個VPN連線。



現在,您應該已經成功驗證了RV34x系列路由器上的VPN連線狀態。GreenBow VPN客戶端 現在配置為通過VPN連線到路由器。