GreenBow VPN Clientを使用したRV34xシリー ズルータへの接続

特記事項:ライセンス構造:ファームウェアバージョン 1.0.3.15以降。今後、AnyConnectはクライアントライセンスに 対してのみ課金されます。

RV340シリーズルータのAnyConnectライセンスの詳細につい ては、「<u>AnyConnect Licensing for the RV340 Series</u> <u>Routers」を参照してください</u>。

概要

バーチャルプライベートネットワーク(VPN)接続を使用すると、インターネットなどのパブ リックネットワークまたは共有ネットワークを介してプライベートネットワークとの間でデ ータのアクセス、送受信が可能になりますが、基盤となるネットワークインフラストラクチ ャへの安全な接続を確保してプライベートネットワークとそのリソースを保護します。

VPNトンネルは、暗号化と認証を使用してデータを安全に送信できるプライベートネットワ ークを確立します。企業オフィスはVPN接続を主に使用します。これは、従業員がオフィス の外からでもプライベートネットワークにアクセスできるようにするために便利で必要な機 能です。

VPNを使用すると、リモートホストを同じローカルネットワーク上に配置されているかのように動作させることができます。ルータは最大50のトンネルをサポートします。ルータが インターネット接続用に設定された後、ルータとエンドポイントの間にVPN接続を設定でき ます。VPNクライアントは、接続を確立できるVPNルータの設定に完全に依存しています 。

GreenBow VPN Clientは、ホストデバイスがRV34xシリーズルータとのサイト間IPSecトン ネルのセキュアな接続を設定できるようにするサードパーティ製VPNクライアントアプリケ ーションです。



この図では、コンピュータはネットワークの外部にあるオフィスのファイルサーバに接続し 、リソースにアクセスします。そのためには、コンピュータのTheGreenBow VPN Clientを

、RV34x VPNゲートウェイから設定を引き出すように設定します。

VPN接続を使用する利点

- 1. VPN接続を使用すると、機密のネットワークデータとリソースを保護できます。
- リモートワーカーや企業の従業員は、物理的に存在しなくても簡単に本社にアクセスでき、 プライベートネットワークとそのリソースのセキュリティを維持できるため、利便性とアク セシビリティが向上します。
- VPN接続を使用した通信は、他のリモート通信方式よりも高いレベルのセキュリティを提供します。現在の高度なテクノロジーは、これを可能にし、プライベートネットワークを不正アクセスから保護します。
- 4. ユーザの実際の地理的位置は保護され、インターネットのようなパブリックまたは共有ネットワークには公開されません。
- 5. VPNは簡単に拡張できるため、新しいユーザやユーザグループをネットワークに追加することは簡単です。追加のコンポーネントや複雑な設定を必要とせずに、ネットワークを拡張できます。

VPN接続を使用するリスク

- 設定ミスによるセキュリティリスクVPNの設計と実装は複雑になる可能性があるため、プラ イベートネットワークのセキュリティが損なわれないように、接続を設定する作業を高度な 知識と経験を持つプロフェッショナルに委ねる必要があります。
- 信頼性.VPN接続にはインターネット接続が必要であるため、優れたインターネットサービスを提供し、ダウンタイムを最小限に抑えて保証するために、実績とテスト済みのレピュテーションを持つプロバイダーが重要です。
- 拡張性.新しいインフラストラクチャや新しい構成セットを追加する必要がある状況では、 特に使用中の製品以外の異なる製品やベンダーが関係する場合に、互換性がないことが原因 で技術的な問題が発生する可能性があります。
- 4. モバイルデバイスのセキュリティの問題。モバイルデバイスでVPN接続を開始すると、特に

モバイルデバイスがローカルネットワークにワイヤレスで接続されている場合に、セキュリ ティの問題が発生する可能性があります。

5. 接続速度が遅い。無料のVPNサービスを提供するVPNクライアントを使用している場合、こ れらのプロバイダーは接続速度を優先しないため、接続が遅くなる可能性があります。

GreenBow VPN Clientの使用の前提条件

次の項目は、まずVPNルータで設定する必要があり、ここをクリックして接続を確立することにより、TheGreenBow VPN Clientに適用さ<u>れま</u>す。

- 1. <u>VPNゲートウェイでのクライアントとサイト間のプロファイルの作成</u>
- 2. VPNゲートウェイでのユーザグループの作成
- 3. <u>VPNゲートウェイでのユーザアカウントの作成</u>
- 4. VPNゲートウェイでのIPSecプロファイルの作成
- 5. VPNゲートウェイでのフェーズIおよびフェーズIIの設定

該当するデバイス

• RV34xシリーズ

[Software Version]

• 1.0.01.17

GreenBow VPN Clientの使用

<u>ルータでのクライアントとサイト間プロファイルの作成</u>

ステップ1:RV34xルータのWebベースのユーティリティにログインし、[**VPN] > [Client-to-Site]を選択します**。



注:この記事の画像は、RV340ルータのものです。オプションは、デバイスのモデルによって異なります。

ステップ2:[Add]をクリ**ックします**。

IPSec Client-to	-Site Groups	
Group		
Add	Edit	Delete

ステップ3:[Rd Party Client]をクリックします。

注: AnyConnectはCisco VPN Clientの例であり、GreenBow VPN Clientはサードパーティ製 VPN Clientの例です。



注:この例では、サードパーティクライアントが選択されています。

ステップ4:[Basic Settings]タブで、[Enable] チェックボックスをオンにして、VPNプロファ

イルがアクティブであることを確認します。

Basic Settings	Advanced Settings	
Enable		
Tunnel Name	e:	Client
Interface:		WAN1 🔻

ステップ5:[Tunnel Name]フィールドにVPN接続の名前を入力します。

Basic Settings Adv	anced Settings	
Enable		
Tunnel Name:		Client
Interface:		WAN1 V

注:この例では、[Client] と入力しています。

ステップ6:[Interface]ドロップダウンリストから、使用するインターフェイスを選択します 。オプションは、WAN1、WAN2、USB1、およびUSB2で、VPN接続にルータ上の対応する インターフェイスを使用します。

Basic Settings	Advanced Settings			
Enable				
Tunnel Name	e:		Client	
Interface:			WAN1 🔻	1
IKE Authentio	cation Method:		WAN1 WAN2	
Presha	red Key:		USB1 USB2	
Preshare	ed Key Strength Meter:	:		

注:オプションは、使用しているルータのモデルによって異なります。この例では、 WAN1が選択されています。

ステップ7:IKE認証方式を選択します。次のオプションがあります。

•事前共有キー:このオプションでは、VPN接続に共有パスワードを使用できます。

• [証明書(Certificate)]: このオプションは、名前、IPアドレス、シリアル番号、証明書の有効期 限、証明書のベアラの公開キーのコピーなどの情報を含むデジタル証明書を使用します。

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

注:この例では、[Preshared Key]が選択されています。

ステップ8:[Preshared Key]フィールドに接続パスワードを入力します。

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

ステップ9:(オプション)[Minimum Preshared Key Complexity **Enable]チェックボ**ックスを オフにして、シンプルパスワードを使用できるようにします。

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

注:この例では、[Minimum Preshared Key Complexity]は有効のままにしておきます。

ステップ10:(オプション)パスワードをプレーンテキストで表示するには、[編集時にプレ ーンテキストを表**示する**]チェックボックスをオンにします。

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

注:この例では、[編集を無効のままにした場合にプレーンテキストを表示する]を選択しま す。 ステップ11:[Local Identifier]ドロップダウンリストからローカルIDを選択します。次のオプ ションがあります。

- ローカルWAN IP:このオプションでは、VPNゲートウェイのワイドエリアネットワーク (WAN)インターフェイスのIPアドレスを使用します。
- [IP Address]:このオプションを使用すると、VPN接続のIPアドレスを手動で入力できます。
- FQDN:このオプションは、完全修飾ドメイン名(FQDN)とも呼ばれます。 インターネット上の特定のコンピュータに完全なドメイン名を使用できます。
- [ユーザFQDN(User FQDN)]: このオプションを使用すると、インターネット上の特定のユー ザに完全なドメイン名を使用できます。

Local Identifier:	Local WAN IP 🔻	124.6.115.177.
	Local WAN IP	
Remote Identifier:	IP Address	124.6.177.118
	FQDN	
	User FQDN	9

注:この例では、[Local WAN IP]が選択されています。このオプションを使用すると、ローカルWAN IPが自動的に検出されます。

ステップ12:(オプション)リモートホストの識別子を選択します。次のオプションがあり ます。

- [IP Address]: このオプションでは、VPNクライアントのWAN IPアドレスを使用します。
- FQDN:このオプションを使用すると、インターネット上の特定のコンピュータに完全なドメイン名を使用できます。
- [ユーザFQDN(User FQDN)]: このオプションを使用すると、インターネット上の特定のユー ザに完全なドメイン名を使用できます。

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

注:この例では、[IP Address]が選択されています。

ステップ13:[Remote Identifier]フィールドにリモートIDを入力します。

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

注:この例では、124.6.115.177と入力します。

ステップ14:(オプション)[拡張認証(**Extended Authentication)]チェックボ**ックスをオンに して、機能をアクティブにします。アクティブ化すると、リモートユーザがVPNへのアクセ スを許可される前にクレデンシャルを入力するように要求する、追加レベルの認証が提供さ れます。

	Group Name
Extended Authentication:	
~	Add Delete

注:この例では、[Extended Authentication]はオフのままにします。

ステップ15:[Group Name]で、[**Add**]をクリ**ックします**。

Extended Authentication:	Group Nan	ne
	Add	Delete

ステップ16:[Group Name]ドロップダウンリストから、拡張認証を使用するグループを選択 します。

Group Name	
admin 🔻	
admin	
guest	
 IPSecVPN	
VPN	

注:この例では、VPNが選択されています。

ステップ17:[Pool Range for Client LAN]で、VPNクライアントに割り当てることができる最初のIPアドレスを[*Start IP*]フィールドに*入力*します。

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

注:この例では、10.10.100.100と入力します。

ステップ18:[End IP]フィールドに、VPNクライアントに割り当てることができる最後のIPア ドレスを入力します。

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

注:この例では、10.10.100.245と入力します。

ステップ19:[Apply]をクリ**ックします**。

Pool Range for Client LAN:	
Start IP:	10.10.100
End IP:	10.100.245
Apply Cancel	

ステップ20:[Save]をクリックします。



これで、TheGreenBow VPN Client用にルータのクライアントとサイト間プロファイルを設 定できました。

<u>ユーザグループの作成</u>

ステップ1:ルータのWebベースのユーティリティにログインし、[**System Configuration**] > [User Groups]を選択します。

注:この記事の画像は、RV340ルータのものです。オプションは、デバイスのモデルによって異なります。

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

ステップ2:[**Add**]をクリックし**て**、ユーザグループを追加します。

User	User Groups		
Us	er Groups Table		
	Group	Web Login	S2S-VPN
	admin	Admin	Disabled
	guest	Disabled Disabled	
	Add Edit Delete		
	Apply Cancel		

ステップ3:[Overview(概要)]領域で、[Group Name(グループ名)]フィールドにグループ の*名前を入力*します。

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

注:この例では、VPNが使用されています。

ステップ4:[Local Membership List(ローカルメンバーシップリスト)]で、同じグループに 属する必要があるユーザ名のチェックボックスをオンにします。

User Groups				
Overview				
Group N	lame: VP	N		
Local	User Men	ibership List		
#	Join	User Name		Joined Groups *
1		CiscoTest		VPN
2		cisco		admin
3		guest		guest
4		vpnuser		VPN
* Should	d have at le	east one account in the "a	admin" group	

注:この例では、CiscoTestとvpnuserが選択されています。

ステップ5:[Services(サービス)]で、グループ内のユーザに付与する権限を選択します。 次のオプションがあります。

- [無効(Disabled)]: このオプションは、グループのメンバがブラウザを介してWebベースユー ティリティにアクセスできないことを意味します。
- [読み取り専用(Read Only)]:このオプションは、グループのメンバーがログイン後にシステムのステータスを読み取ることができることを意味します。設定を編集することはできません。
- Administrator:このオプションは、グループのメンバーに読み取り/書き込み権限を与え、シ ステムステータスを設定できます。

Services			
Web Login	Disabled	Read Only 🔘	Administrator

注:この例では、[Read Only]が選択されています。

ステップ6:[EzVPN/3rd Party Profile Member In-use]テーブルで、[Add]をクリックします。

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

ステップ7:[Select a Profile]ドロップダウンリストからプロファイルを選択します。オプションは、VPNゲートウェイに設定されているプロファイルによって異なります。

Add Feature List

Select a Profile:	Clients Clients	
Add	Cancel	

注:この例では、[Clients]が選択されています。

ステップ8:[Add]をクリ**ックします**。

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

ステップ9:[Apply]をクリ**ックします**。

SSL VPN	Select a Profile 🔻
PPTP VPN	Permit
L2TP	Permit
802.1x	Permit
Apply	Cancel

ステップ10:[Save]をクリ**ックします**。



これで、RV34xシリーズルータにユーザグループが正常に作成されたはずです。

<u>ユーザアカウントの作成</u>

ステップ1:ルータのWebベースのユーティリティにログインし、[**System Configuration**] > [User Accounts]を選択します。

注:この記事の画像は、RV340ルータのものです。オプションは、デバイスのモデルによって異なります。



ステップ2:[Local User Membership List]領域で、[Add]をクリックします。

ι	User Accounts				
	Local Users Password Complexity Password Complexity Settings: Enable Local Users				
	Lo	cal User I	Membership List		
		#	User Name	Group *	
		1	guest	VPN	
		2	cisco	admin	
		Add	Edit Delete	Import	
	* Sho	ould have	at least one account in the "admin" gr	oup	

ステップ3:[User Name]フィールドにユーザの名前を入力します。

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

注:この例では、CiscoTestが入力されています。

ステップ4:[New Password]フィールドにユーザパスワード*を入力*します。

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

ステップ5:[New Password Confirm]ボックスでパスワ*ードを確認*します。

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

ステップ6:[Group]ドロップダウンリストからグループを選択します。これは、ユーザが関 連付けられるグループです。

Group		VP	NV
		VP	N
		aur	mn
		gue	est
Apply	Cance	I	

- 注:この例では、VPNが選択されています。
- ステップ7:[Apply]をクリ**ックします**。

	User Accounts	
	Add User Account	
	User Name	CiscoTest
	New Password	•••••
	New Password Confirm	•••••
	Group	VPN T
(Apply Cance	

ステップ8:[**Save**]をクリ**ックします**。



これで、RV34xシリーズルータにユーザアカウントが作成されました。

<u>IPSecプロファイルの設定</u>

ステップ1:RV34xルータのWebベースのユーティリティにログインし、[**VPN**] > [**IPSec Profiles]を選択します**。

	Getting Started
►	Status and Statistics
•	Administration
•	System Configuration
•	WAN
•	QoS
•	LAN
•	Routing
►	Firewall
	VPN
_	
	VPN Setup Wizard IPSec Profiles Site-to-Site Client-to-Site Teleworker VPN Client PPTP Server L2TP Server SSL VPN VPN Passthrough

注:この記事の画像は、RV340ルータのものです。オプションは、デバイスのモデルによって異なります。

ステップ2:IPSecプロファイルテーブルに既存のプロファイルが表示されます。[Add] をク リックし、新規プロファイルを作成します。

PSe	ec Profiles	
IPs	sec Profiles Table	
	Name	Policy
\bigcirc	Amazon_Web_Services	Auto
\bigcirc	Default	Auto
\bigcirc	Microsoft_Azure	Auto
	Add Edit Clon	Delete
A	pply Cancel	

注: Amazon_Web_Services、Default、およびMicrosoft_Azureはデフォルトプロファイルです。

ステップ3:[Profile Name]フィールドにプロファイルの名前*を作成*します。プロファイル名 には、英数字と特殊文字のアンダースコア(_)のみを使用してください。

IPSec Profiles				
Add a New IPSec Profile				
Profile Name:	Cli	ent		
Keying Mode	۲	Auto	0	Manual

注:この例では、Clientと入力します。

ステップ4:オプションボタンをクリックして、プロファイルが認証に使用するキー交換方 式を決定します。次のオプションがあります。

- Auto:ポリシーパラメータは自動的に設定されます。このオプションでは、データ整合性と 暗号化キー交換にインターネットキー交換(IKE)ポリシーを使用します。これを選択すると、 [Auto Policy Parameters]領域の設定が有効になります。このオプションを選択した場合は、 「自動設定の構成」に進みます。
- [Manual]:このオプションを使用すると、VPNトンネルのデータ暗号化と整合性のためのキ ーを手動で設定できます。これを選択すると、[Manual Policy Parameters]領域の設定が有効 になります。このオプションを選択した場合は、「手動設定の構成」に進みます。

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

注:この例では、[Auto]が選択されています。

<u>フェーズIおよびフェーズIIの設定</u>

0

ステップ1:[Phase 1 Options(フェーズ1オプション)]領域で、[DH Group(DHグループ)]ドロップダウンリストから、フェーズ1のキーで使用する適切なDiffie-Hellman(DH)グル ープを選択します。Diffie-Hellmanは、事前共有キーセットを交換するための接続で使用さ れる暗号キー交換プロトコルです。アルゴリズムの強度はビットによって決まります。次の オプションがあります。

- Group2-1024 bit : このオプションでは、キーの計算は遅くなりますが、グループ1よりも安 全です。
- Group5-1536ビット:このオプションは、最も遅いキーを計算しますが、最もセキュアです

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

注:この例では、Group5-1536ビットが選択されています。

ステップ2:[Encryption]ドロップダウンリストから、Encapsulating Security Payload(ESP)およびInternet Security Association and Key Management Protocol(ISAKMP)を暗号化および 復号化する暗号化方式を選択します。 次のオプションがあります。

- 3DES:Triple Data Encryption Standard (トリプルデータ暗号規格)。
- AES-128:Advanced Encryption Standard(AES-128)は128ビットキーを使用します。
- AES-192:Advanced Encryption Standard(AES-192;高度暗号化規格)は192ビットキーを 使用します。
- AES-256:Advanced Encryption Standard(AES-256)は256ビットキーを使用します。

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

注:AESは、DESおよび3DESを介した暗号化の標準的な方式であり、パフォーマンスとセキュリティを向上させます。AESキーを長くすると、パフォーマンスが低下し、セキュリティが向上します。この例では、AES-128が選択されています。

ステップ3:[Authentication]ドロップダウンリストから、ESPおよびISAKMPの認証方法を選択します。次のオプションがあります。

- MD5:Message-Digest Algorithm (MD5;メッセージダイジェストアルゴリズム)には、 128ビットのハッシュ値があります。
- SHA-1:Secure Hash Algorithm (SHA-1;セキュアハッシュアルゴリズム)に160ビットのハ ッシュ値があります。
- SHA2-256:256ビットのハッシュ値を使用したセキュアハッシュアルゴリズム。

Phase I Options	
DH Group:	Group5 - 1536 bit 🔻
Encryption:	AES-128 V
Authentication:	SHA1 V
	MD5
SA Lifetime:	SHA1
Perfect Forward Secrecy:	SHA2-200 Enable

注:MD5とSHAは両方とも暗号化ハッシュ関数です。データの一部を取り、圧縮し、通常 は再生できない一意の16進数出力を作成します。この例では、SHA1が選択されています。

ステップ4:[*SA Lifetime]フィールド*に、120 ~ 86400の範囲の値を入力します。これは、 Internet Key Exchange(IKE)セキュリティアソシエーション(SA)がフェーズでアクティブな ままである時間の長さです。デフォルト値は 28800 です。

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

注:この例では、86400と入力します。

ステップ5:(オプション)[Enable Perfect Forward Secrecy]チェックボックスをオンにして、IPSecトラフィックの暗号化と認証のための新しいキーを生成します。

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

注:この例では、Perfect Forward Secrecy (PFS;完全転送秘密)が有効になっています。

ステップ6:[Phase II Options]領域の[Protocol Selection]ドロップダウンリストから、ネゴシ エーションの2番目のフェーズに適用するプロトコルタイプを選択します。次のオプション があります。

- ESP:このオプションは、保護するデータをカプセル化します。このオプションを選択した 場合は、ステップ7<u>に進んで</u>暗号化方式を選択します。
- AH:このオプションは、認証ヘッダー(AH)とも呼ばれます。データ認証とオプションのアンチリプレイサービスを提供するセキュリティプロトコルです。AHは、保護されるIPデータグラムに埋め込まれています。このオプションを選択した場合は、ステップ8に<u>進みます</u>。

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

注:この例では、ESPが選択されています。

ス<u>テップ7</u>:ステップ6でESPを選択した場合は、ESPとISAKMPの認証方法を決定する認証 方式を選択します。次のオプションがあります。

- 3DES:Triple Data Encryption Standard (トリプルデータ暗号化規格)
- AES-128:Advanced Encryption Standard(AES-128)は128ビットキーを使用します。
- AES-192:Advanced Encryption Standard (AES-192;高度暗号化規格)は192ビットキーを 使用します。
- AES-256:Advanced Encryption Standard(AES-256)は256ビットキーを使用します。

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

注:この例では、AES-128が選択されています。

<u>ステップ8</u>:[Authentication]ドロップダウンリストから、ESPおよびISAKMPの認証方法を選 択します。次のオプションがあります。

- MD5:Message-Digest Algorithm (MD5;メッセージダイジェストアルゴリズム)には、 128ビットのハッシュ値があります。
- SHA-1:Secure Hash Algorithm(SHA-1;セキュアハッシュアルゴリズム)に160ビットのハ ッシュ値があります。
- SHA2-256:256ビットのハッシュ値を使用したセキュアハッシュアルゴリズム。

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

注:この例では、SHA1が選択されています。

ステップ9:[*SA Lifetime]フィールド*に、120 ~ 28800の範囲の値を入力します。これは、 IKE SAがこのフェーズでアクティブなままである時間の長さです。デフォルト値は 3600 で す。

ステップ10:[DHグループ(DH Group)]ドロップダウンリストから、フェーズ2のキーで使用 するDHグループを選択します。オプションは次のとおりです。

- Group2-1024ビット:このオプションは、キーの計算は遅くなりますが、Group1よりも安全です。
- Group5-1536ビット:このオプションは、最も遅いキーを計算しますが、最もセキュアです

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

注:この例では、3600と入力します。

0

ステップ11:[Apply]をクリ**ックします**。

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 🔻
Encryption:	AES-128 V
Authentication:	SHA1 T
SA Lifetime:	3600
DH Group:	Group5 - 1536 bit 🔻
Apply Cancel	

ステップ12:[Save]をクリックし、設定を永続的に保存します。



これで、RV34xシリーズルータの自動IPSecプロファイルが正常に設定されました。

<u>手動設定の設定</u>

ステップ1:[*SPI-Incoming]フィールド*に、VPN接続の着信トラフィックのセキュリティパラ メータインデックス(SPI)タグの100 ~ FFFFFFの16進数値を入力します。SPIタグは、あ るセッションのトラフィックを他のセッションのトラフィックと区別するために使用されま す。

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

注:この例では、0xABCDと入力します。

ステップ2:[*SPI-Outgoing]フィールド*に、VPN接続の発信トラフィックのSPIタグとして、 100 ~ FFFFFFの16進数値を入力します。

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

注:この例では、0x1234と入力します。

ステップ3:ドロップダウンリストから暗号化値を選択します。次のオプションがあります。

- 3DES:Triple Data Encryption Standard (トリプルデータ暗号化規格)
- AES-128:Advanced Encryption Standard(AES-128)は128ビットキーを使用します。
- AES-192:Advanced Encryption Standard (AES-192;高度暗号化規格)は192ビットキーを 使用します。

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

注:この例では、AES-256が選択されています。

ステップ4:[*Key-In*]フィールドに、インバウンドポリシーのキーを入力します。キーの長さは、ステップ3で選択したアルゴリズムによって異なります。

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1212121

注:この例では、123456789123456789123...と入力します。

ステップ5:[*Key-Out*]フィールドに、発信ポリシーのキーを入力します。キーの長さは、ステップ3で選択したアルゴリズムによって異なります。



注:この例では、1a1a1a1a1a1a1a12121212...と入力します。

ステップ6:[Authentication]ドロップダウンリストから認証方法を選択します。次のオプションがあります。

- MD5:Message-Digest Algorithm (MD5;メッセージダイジェストアルゴリズム)には、 128ビットのハッシュ値があります。
- SHA-1:Secure Hash Algorithm(SHA-1;セキュアハッシュアルゴリズム)に160ビットのハ ッシュ値があります。
- SHA2-256:256ビットのハッシュ値を使用したセキュアハッシュアルゴリズム。

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

注:この例では、MD5が選択されています。

ステップ7:[*Key-In*]フィールドに、インバウンドポリシーのキーを入力します。キーの長さ は、ステップ6で選択したアルゴリズムによって異なります。

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1212121

注:この例では、123456789123456789123...と入力します。

ステップ8:[*Key-Out*]フィールドに、発信ポリシーのキーを入力します。キーの長さは、ステップ6で選択したアルゴリズムによって異なります。

Key-In:	123456789123456789123
Key-Out	1a1a1a1a1a1a1a121212 ⁺

Apply

注:この例では、1a1a1a1a1a1a1a12121212...と入力します。

ステップ9:をクリックします

ステップ10:[Save]をクリックし、設定を永続的に保存します。



これで、RV34xシリーズルータで手動IPSecプロファイルが正しく設定されました。

GreenBow VPNクライアントソフトウェアの設定

フェーズ1の設定

ステップ1:[TheGreenBow VPN Client]アイコンを右クリックし、[**Run as administrator]を選 択します**。

	5.)	
		Open
w VPN		Troubleshoot compatibility
		Open file location
	0	Run as administrator
		Pin to Taskbar
		Pin to Start Menu
		Restore previous versions
		Send to 🕨
//;		Cut
		Сору
		Create shortcut
		Delete
		Rename
		Properties

ステップ2:左側のペインの[VPN configuration]で、[**IKE V1**]を右クリックして、[**New Phase 1]を選択します**。

😔 TheGreenBo	w VPN Client		_ _ ×
Configuration	Tools ?		
THEGF	REENBOL	J	
			VPN Client
		IKE V1	
VPN Configu	ration	IKE V1	
o 🗁 🚾 🚥	Emert		
	Export	F V1 Configuration	
	Save	Ctrl+S	
i i	New Phase 1	Ctrl+N his folder enables the creation of IKE V1 tunnels. It is possi	ble to
THE V2		Create as many phases 1 and phases 2 as required. The con menu (right dick on IKE V1) enables to create, copy or paste	Phases 1
		and Phases 2.	
		IKE V1 IPsec tunnel creation wizard	
		Export all IKE V1 tunnels	
VPN Client	ready		

ステップ3:[Authentication]タブの[Addresses]で、[Interface]エリアのIPアドレスが、 TheGreenBow VPN ClientがインストールされているコンピュータのWAN IPアドレスと同 じであることを確認します。

注:この例では、IP アドレスは 124.6.177.118 です。

😧 TheGreenBow VPN Client			
Configuration Tools ?			
THEGREENBOW			
			VPN Client
	Ikev1Gateway: Authen	tication	
VPN Configuration KE V1 IKE V1 Parameters UKE V1 Parameters UKE V1 Parameters UKE V1 Parameters UKE V1 Parameters UKE V1 UKE V1 Parameters UKE V1 UKE V1 UKE V1 Parameters UKE V1 UKE V2 UKE V2 UKE V2 UKE V2 UKE V2 UKE V2	Authentication Advanced Certific Addresses Interface 124. Remote Gateway 124 Authentication © Preshared Key Confirm © Certificate	cate 6.177.118 .6.115.177	

ステップ4:[Remote Gateway]フィールドにリモートゲートウェイのアドレスを入力します

注:この例では、リモートRV34xルータのIPアドレスは124.6.115.177です。

o

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOL		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration VPN Configuration KE V1 KE V1 KE V1 Parameters Control tgbtestIPV4 Control tgbtestIPV4 Control tgbtestIPV6 Co	Authentication Advanced Certificate Addresses Interface 124.6.177.118 Remote Gateway 124.6.115.177 Authentication © Preshared Key Confirm © Certificate	

ステップ5:[Authentication]で、認証タイプを選択します。次のオプションがあります。

- •事前共有キー:このオプションを使用すると、ユーザはVPNゲートウェイで設定されたパス ワードを使用できます。VPNトンネルを確立するには、ユーザがパスワードを照合する必要 があります。
- [Certificate] : このオプションは、証明書を使用して、VPNクライアントとVPNゲートウェイ 間のハンドシェイクを完了します。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOL		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration VE V1 KE V1 VI Parameters UE V1 Parameters vgbtestIPV4 vgbtestIPV4 vgbtestIPV6 VgbtestIPV6 VgbtestIPV6 VgbtestIPV6 VgbtestIPV6 SSL	Authentication Advanced Certificate Addresses Interface 124.6.177.118 Remote Gateway 124.6.115.177 Authentication Confirm Confirm Confirm Certificate	· · · · · · · · · · · · · · · · · · ·

注:この例では、RV34x VPNゲートウェイの設定と一致するように[Preshared Key]が選択 されています。

ステップ6:ルータで設定されている事前共有キーを入力します。

TheGreenBow VPN Client	
Configuration Tools ?	
THEGREENBOW	
	VPN Client
	Ikev1Gateway: Authentication
VPN Configuration IKE V1 IKE V1 Parameters UgbtestIPV4 UgbtestIPV6 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

ステップ7:[Confirm]フィールドに同じ事前共有キーを*入力*します。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOL		
		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration KE V1 IKE V1 V1 Parameters UptestIPV4 UptestIPV6 UptestIPV6 Ikev1Gateway KE V2 SSL	Authentication Advanced Certificate Addresses Interface 124.6.177.118 Remote Gateway 124.6.115.177 Authentication © Preshared Key Confirm Confirm Confirm	

ステップ8:IKEの下で、ルータの設定と一致するように[Encryption]、[Authentication]、および[Key Group]の設定を設定します。

- • · ×

Configuration Tools ?

TheGreenBow VPN Client

VP	N Client
Ikev1Tunnel: IPsec	
Image: WPN Configuration Image: WE V1 Image: WE V1 Image: WE V2 Image: WE V1 Image: WE V2 Image: WE V2 State Image: WE V2 State	
VPN Client ready	

ステップ9:[Advanced]タブをク**リック**します。

	VPN Client
	IT IT OFFICIT
Authentication	
Audientication Revences Cerdicate	

ステップ10:(オプション)[拡張機能(Advanced features)]で、[モードの設定(**Mode Config)]チェックボックス**と[アグレッシブモード(Aggressive Mode)]チェックボックスをオ ンにし、NAT-Tの設定を[自動(Automatic)]に設定します。

	×

TheGreenBow VPN Client Configuration Tools ?

THEGREENBOW

				VPN Client
	Ikev1Gateway: Auth	entication		
VPN Configuration IKE V1 IKE V1 Parameters Ikev1Gateway UptestIPV4 UptestIPV6 UptestIPV6 IKE V2 SSL	Authentication Advanced C Advanced features Mode Config Aggressive Mode X-Auth X-Auth Popup Hybrid Mode Local and Remote ID Type of ID: Local ID IP Address Remote ID IP Address	Redundant Gateway NAT-T Login Password Value • 124	Automatic vpnuser 1 •••••••• e for the ID: 4.6.177.115	
 VPN Client ready 				

注:Mode Configを有効にすると、GreenBow VPN ClientはVPNゲートウェイから設定を引き出してトンネルの確立を試みると同時に、アグレッシブモードとNAT-Tを有効にすると接続の確立が高速になります。

ステップ11:(オプション)[X-Auth]で、[**X-Auth Popup**]チェックボックスをオンにして、接 続を開始するときに自動的にログインウィンドウを表示します。ログインウィンドウでは、 ユーザがクレデンシャルを入力して、トンネルを完了できます。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate	
IKE V1	Advanced features	
- Ikev1Gateway	Redundant	
tobtestIPV4	Mode Config Gateway	
e-□ tgbtestIPV6	☑ Aggressive Mode NAT-T Aut	omatic 👻
- o tgbtestIPV6		
SSL	X-Auth	
	Auth Popup Login vpm	user
	Hybrid Mode Password •••	•••••
	Local and Remote ID	
	Type of ID: Value for t	he ID:
	Local ID IP Address I24.6.11	5.177
	Remote ID IP Address 124.6.17	7.118
 VPN Client ready 		

注:この例では、[X-Auth Popup]はオンになっていません。

ステップ12:[ログイン]フィールドにユーザ名*を入力*します。これは、VPNゲートウェイでユ ーザグループを作成するために設定されたユーザ名です。



ステップ13:[Password]フィールドにパスワードを入力します。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate	
IKE V1 IKE V1 Parameters	Advanced features	
- Ikev1Gateway	Mode Config Redundant	
tgbtestIPV4	Gateway	
□-□ tgbtestIPV6 □ ○ tgbtestIPV6	Aggressive Mode NAT-T Automatic	•
IKE V2	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 I24.6.177.118	
VPN Client ready		

ステップ14:[Local and Remote ID]で、ローカルIDとリモートIDをVPNゲートウェイの設定 と一致するように設定します。

TheGreenBow VPN Client				
Configuration Tools ?				
THEGREENBOW				
				VPN Client
	Ikev1Gateway: Aut	inentication		
VPN Configuration	Authentication Advanced	Certificate		
IKE V1 Parameters	Advanced features			
- Ikev1Gateway	Made Coofa	Redundant		_
o tgbtestIPV4		Gateway		
de tabtestIPV6 de tabtestIPV6	Aggressive Mode	NAT-T	Automatic	•
- IKE V2	Y-Auth			
	A-A001			
	X-Auth Popup	Login	vpnuser	
	🚺 🗌 Hybrid Mode	Password	•••••	
	Local and Remote II	0		
	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				

注:この例では、ローカルIDとリモートIDの両方がIPアドレスに設定され、RV34x VPNゲ ートウェイの設定と一致します。

ステップ15:[IDの値(Value for the ID)]の各フィールドにローカルIDとリモートIDを入力しま す。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOU		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate	
IXE V1 IXE V1 Parameters	Advanced features	
e-c tgbtestIPV4	Mode Config Redundant Gateway	
e-c tgbtestIPV6	Aggressive Mode NAT-T Automatic	-
	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		

ステップ16:[**Configuration] > [Save]をクリック**して、設定を保存します。

Check Content	The second se	
Configuration Tools ?		
Save	Ctrl+S	
Import		VPN Client
Export	v1Gateway: Authentication	
Move to USB Drive	nentication Advanced Certificate	
Wizard	Advanced features	
Quit	Mode Config Gateway	
e-c tgbtestIPV4	Aggressive Mode NAT-T Automatic	•
IKE V2	V Ath	

フェーズ2の設定

ステップ1:[**Ikev**1 Gateway]を右クリ**ックします**。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
	Ikev1Gateway: Authentication	
VPN Configuration	Authentication Advanced Certificate	
IKE V1	Advanced features	
Ikev1Gateway	Mode Config Redundant Gateway	
⊡-⊡ tgbtestIPV6	Aggressive Mode NAT-T Automatic	-
IKE V2	X-Auth	

ステップ2:[**New Phase 2**]を選択します。

😧 TheGreenBow VPN Clie	ent		100				
Configuration Tools ?							
THEGREENE	зош						
							VPN Client
		lkev	1Gatew	vay: Au	thentication		
VPN Configuration		Auther	ntication	Advanced	Certificate		
IKE V1	rs	,	Advanced	features			
	Сору		Ctrl+	C	Redundant Gateway		
e-□ tgbtestIPV6	Delete	e	D	el Mode	NAT-T	Automatic	•
SSL	New Pl	hase 2	Ctrl+	N			
						-	

ステップ3:[IPsec]タブを**クリック**します。

TheGreenBow VPN Client			
Configuration Tools ?			
THEGREENBOW			
			VPN Client
	Ikev1Tunnel: IPsec		
VPN Configuration	IPsec Advanced Automation Remo	te Sharing	IPV4 IPV6
IKE V1	Addresses		
Ikev1Gateway Ikev1Tunnel tobtestIPV4	VPN Client address	192 . 168 . 10 . 8	•
- o tgbtestIPV4	Address type	Subnet address	-
tgbtestIPV6	Remote LAN address	192 . 168 . 1 . 0	- I
IKE V2	Submat mark	255 255 255 0	- 1
SSL	Sourcemask	233 . 233 . 233 . 0	
	ESP		
	Encryption	Auto 👻	
	Authentication	Auto 👻	
	Mode	Tunnel 💌	
	DEC		
	Prs		
	PFS Group	Ŧ	
VPN Client ready			

ステップ4:[Address type]ドロップダウンリストから、VPN Clientがアクセスできるアドレ スタイプを選択します。

Interview WPN Client	Trans.	
Configuration Tools ?		
THEGREENBOW		
		VPN Client
	Ikev1Tunnel: IPsec	
VPN Configuration	IPsec Advanced Automation Remote Sharing	IPV4 IPV6
IKE V1	Addresses	
- Ikev1Gateway	192 158 10 8	
tobtestIPV4	VPN Client address	
- o tgbtestIPV4	Address type Subnet address	-
tgbtestIPV6 tobtestIPV6	Remote LAN address	n
- TKE V2	Subnet address	-
L-C SSL	Subnet mask 255 . 255 . 255 . 0	
	ESP	
	Encryption Auto	
	Authentication Auto	
	Made Transl	
	Mode Tunnel V	
	PFS	
	PFS Group -	
UDN Cleant ready		
 WHY Client ready 		

注:この例では、[Subnet address]が選択されています。

ステップ5:[Remote LAN address]フィールドに、VPNトンネルからアクセスする必要がある ネットワーク*アドレスを入力*します。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
		of the officiat
	Ikev1Tunnel: IPsec	
VPN Configuration	IPsec Advanced Automation Remote Sharing	IPV4 IPV6
E-C IKE V1 IKE V1 Parameters E-C Ikev1Gateway Kev1Tunnel	Addresses VPN Client address 192 . 168 . 10 . 8	
tgbtestIPV4 tgbtestIPV4 tgbtestIPV4 tgbtestIPV6	Address type Subnet address -	
tgbtestIPV6	Remote LAN address 192 . 168 . 100 . 1	
	Subnet mask 255 . 255 . 255 . 0]

注:この例では、192.168.100.1と入力します。

ステップ6:[Subnet mask]フィールドにリモートネットワークのサブネットマス*クを入力*します。

注:この例では、255.255.255.0と入力します。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		
		VPN Client
		TH OHEIR
	lkev1Tunnel: IPsec	
VPN Configuration	IPsec Advanced Automation Repote Sharing	IPV4 IPV6
E-C IKE V1 IKE V1 Parameters IKE V1 Parameters	Addresses	
IkevIGateway O IkevITunnel tobtestIPV4	VPN Client address 192 . 168 . 10 . 8	•
o tgbtestIPV4 dotestIPV6	Address type Subnet address •	
 tgbtestIPV6 	Remote LAN address 192 . 168 . 1 . 0	
SSL	Subnet mask 255 . 255 . 255 . 0	

ステップ7:ESPで、VPNゲートウェイの設定に一致するようにEncryption、Authentication、 およびModeを設定します。

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

ステップ8:(オプション)PFSの下で、PFSチェック**ボックス**をオンにして、Perfect Forward Secrecy(PFS)を有効にします。PFSは、セッションを暗号化するためのランダム ・キーを生成します。

TheGreenBow VPN Client	in the second		
Configuration Tools ?			
THEGREENBOW			
		VPN Client	
		TH OICH	
	Ikev1Tunnel: IPsec		
VPN Configuration	IPsec Advanced Automation Rem	ote Sharing IPV4 IPV6	
IKE V1	Addresses		
- Ikev1Gateway	VPN Charles delana	102 169 10 9	
- O Ikev1Tunnel	VPN Client address	152 . 100 . 10 . 0	
└─○ tgbtestIPV4	Address type	Subnet address	
	Demote I AN address	192 . 168 . 1 . 0	
IKE V2	Relifice LAN dual ess		
🛅 SSL	Subnet mask	255 . 255 . 255 . 0	
	ESP		
	Encryption	AES128	
	Authentisation		
	Autientication	SHA-1	
	Mode	Tunnel	
	PFS		
	Group	DH5 (1536)	
 VPN Client ready 			

ステップ9:[Group]ドロップダウンリストからPFSグループ設定を選択します。

注:この例では、ルータのDHグループ設定と一致するようにDH5(1536)が選択されていま す。

TheGreenBow VPN Client		
Configuration Tools ?		
THEGREENBOW		VPN Client
	Ikev1Tunnel: IPsec	
VPN Configuration	IPsec Advanced Automation Remote Sharing	IPV4 IPV6
IKE V1 Parameters	Addresses	
Ikev1Gateway Ikev1Tunnel tobtestIPV4	VPN Client address 192 . 168 . 10 . 8	
o tgbtestIPV4	Address type Subnet address	•
gbtestIPV6 u o tgbtestIPV6	Remote LAN address 192 . 168 . 1 . 0	
	Subnet mask 255 . 255 . 255 . 0	
	ESP	
	Encryption AES128	
	Authentication SHA-1 -	
	Mode Tunnel 💌	
	PFS	
	PFS Group	
	DH1 (768)	
	DH5 (1536)	
	DH14 (2048) DH15 (3072)	
	DH 16 (4096) DH 17 (6144)	
 VPN Client ready 	DH 18 (8192)	

ステップ10:[Configuration]を右クリックし、[Save]を選択します。

TheGreenBow VPN Client		
Configuration Tools ?		
Save Ctrl+S		
Import Export Move to USB Drive Wizard Quit Unit Wizard Quit Unit Unit Unit Unit Unit Unit Unit Un	v1Tunnel: IPsec C Advanced Automation Remo Addresses VPN Client address Address type	VPN-Client te Sharing IPV4 IPV6 192 . 168 . 10 . 8
L O tgbtestIPV6	Remote LAN address Subnet mask ESP Encryption Authentication Mode PFS IV PFS Group	192 . 168 . 1 . 0 255 . 255 . 255 . 0 AES 128 • Auto • Tunnel •
 VPN Client ready 		

これで、VPNを介してRV34xシリーズルータに接続するようにTheGreenBow VPN Clientを 正しく設定できました。

VPN接続の開始

ステップ1:[TheGreenBow VPN Client]を右クリックし、[**Run as administrator]を選択します**。



ステップ2:使用するVPN接続を選択し、[OPEN]をクリッ**クします**。VPN接続が自動的に開 始されます。



注:この例では、設定されたlkev1ゲートウェイが選択されています。

VPNステータスの確認

ステップ1:VPNゲートウェイのWebベースのユーティリティにログインします。

ステップ2:[Status and **Statistics] > [VPN Status]を選択します**。



ステップ3:[Client-to-Site Tunnel Status]で、[Connection Table]の[Connections]列を確認します。

注:この例では、1つのVPN接続が確立されています。



これで、RV34xシリーズルータのVPN接続ステータスを正常に確認できました。これで、 GreenBow VPN ClientがVPN経由でルータに接続するように設定されました。