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、「AnyConnect Licensing for the RV340 Series Routers」を参照してください。

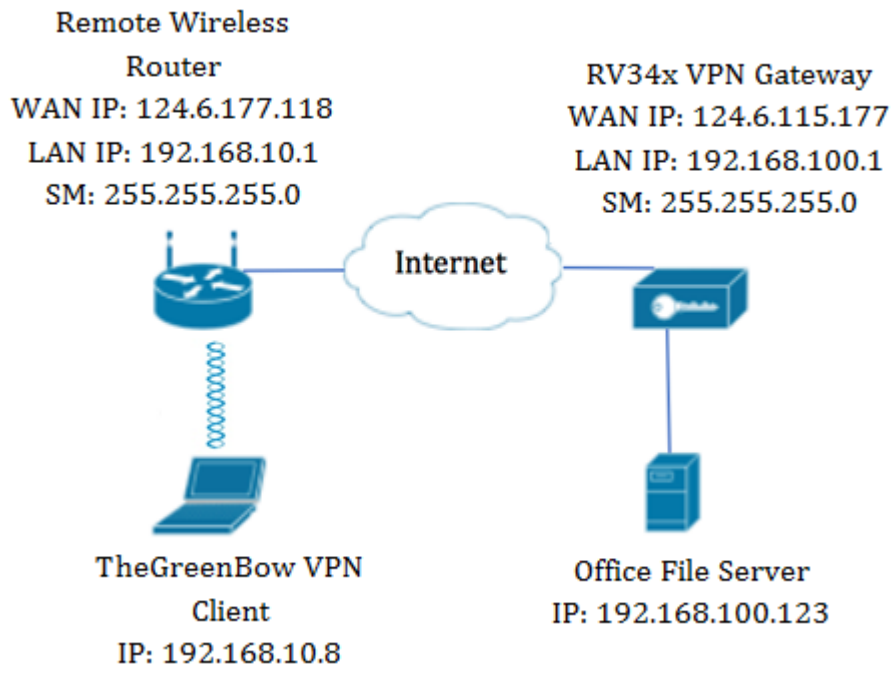
概要

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。
2. 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。
3. 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

1. 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。
2. 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。
3. 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に適用されます。

1. 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
2. VPNゲートウェイでのユーザグループの作成
3. VPNゲートウェイでのユーザアカウントの作成
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

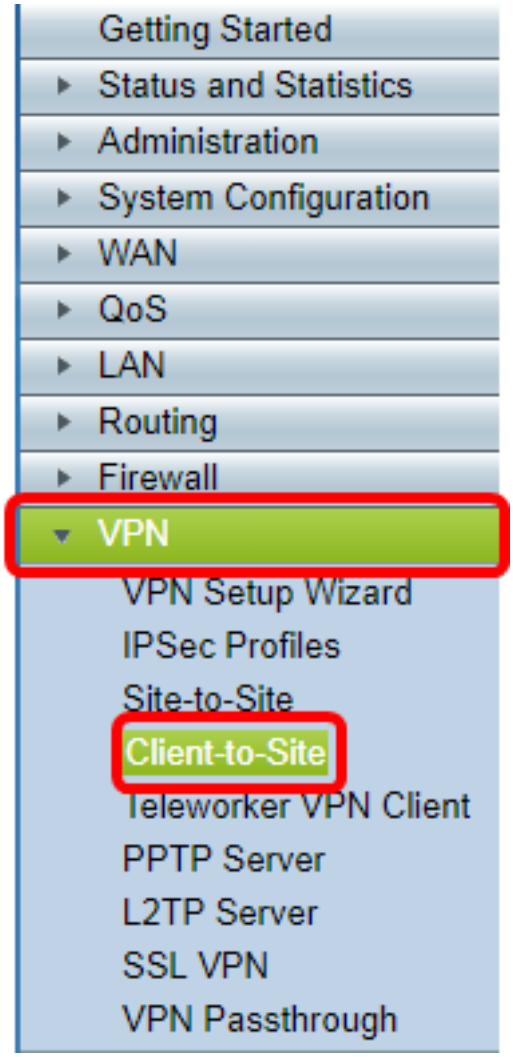
[Software Version]

- 1.0.01.17

GreenBow VPN Clientの使用

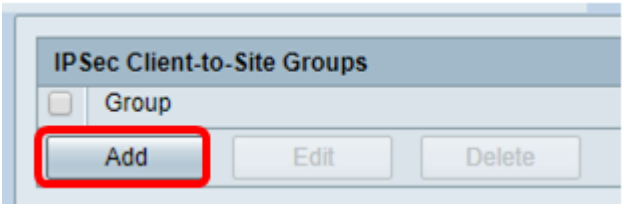
ルータでのクライアントとサイト間プロファイルの作成

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。**



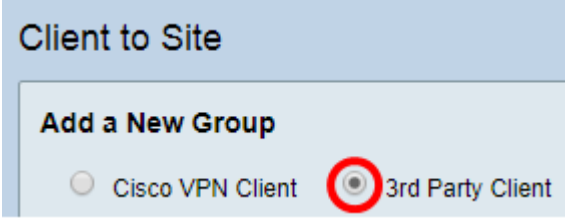
注：この記事の画像は、RV340ルータのものです。オプションは、デバイスのモデルによって異なります。

ステップ2:[Add]をクリックします。



ステップ3:[Rd Party Client]をクリックします。

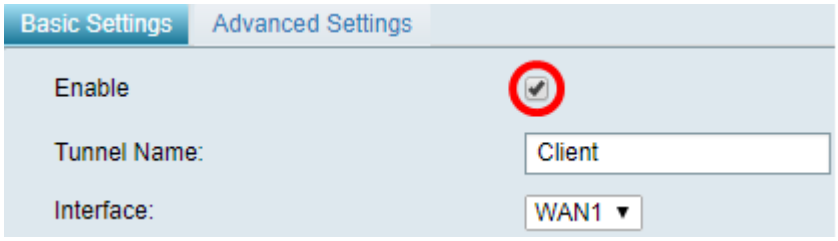
注：AnyConnectはCisco VPN Clientの例であり、GreenBow VPN Clientはサードパーティ製VPN Clientの例です。



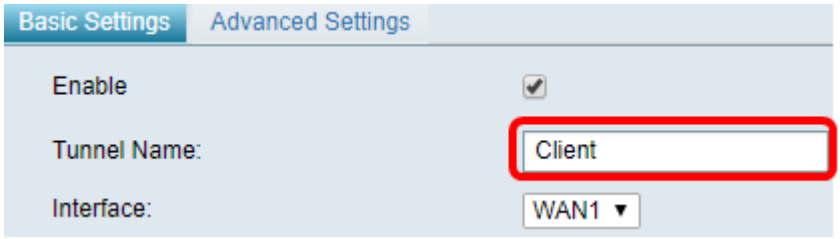
注：この例では、サードパーティクライアントが選択されています。

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。

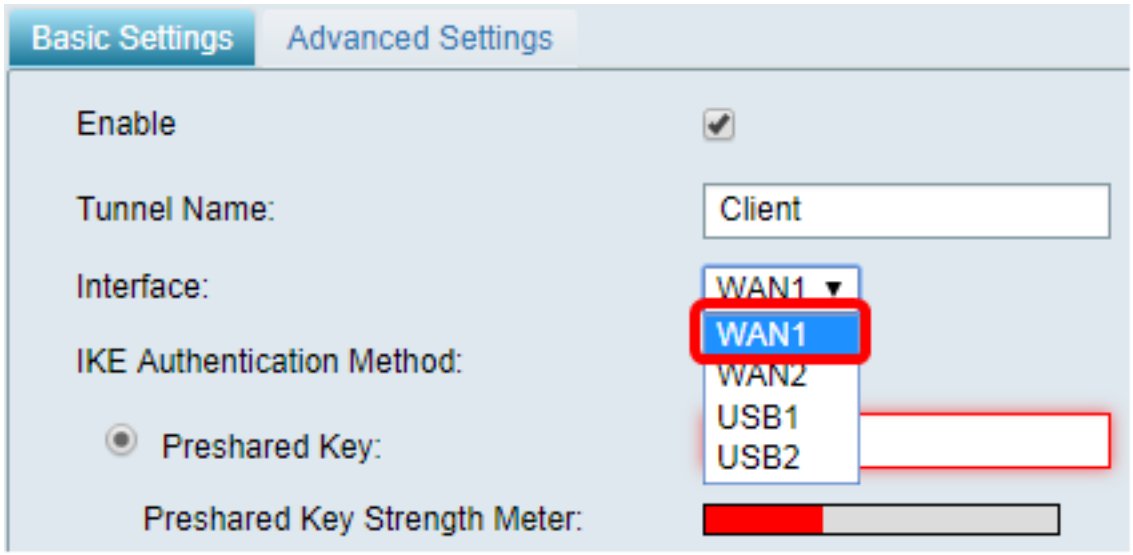


ステップ5:[Tunnel Name]フィールドにVPN接続の名前を入力します。



注：この例では、[Client] と入力しています。

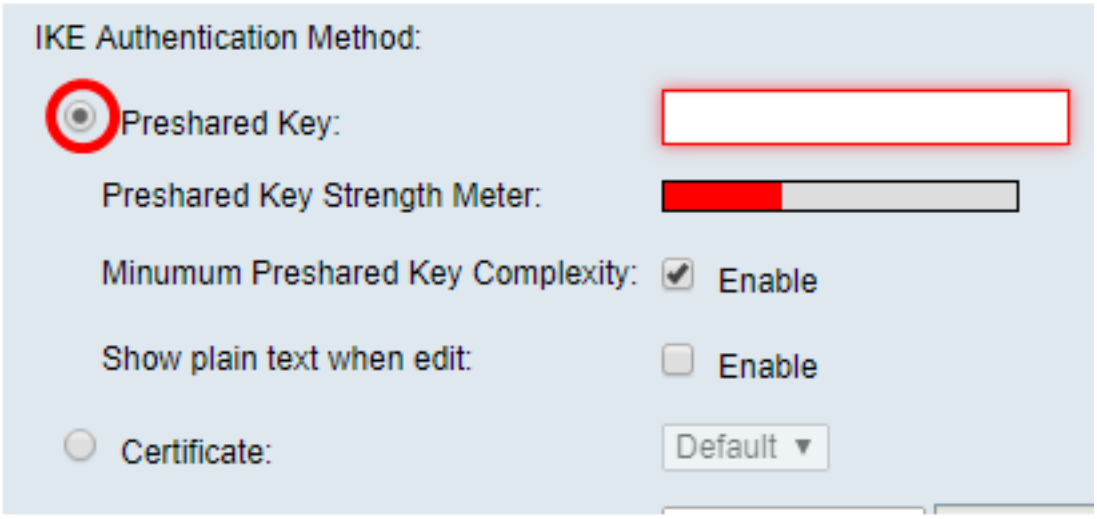
ステップ6:[Interface]ドロップダウンリストから、使用するインターフェイスを選択します。オプションは、WAN1、WAN2、USB1、およびUSB2で、VPN接続にルータ上の対応するインターフェイスを使用します。



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。

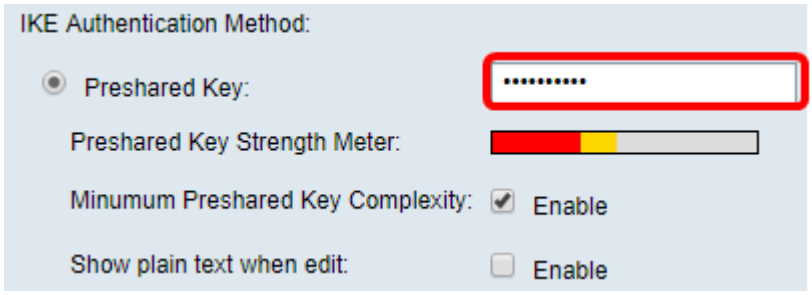
ステップ7:IKE認証方式を選択します。次のオプションがあります。

- 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。

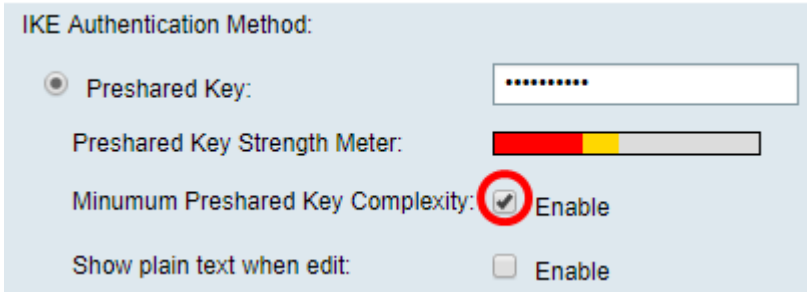


注：この例では、[Preshared Key]が選択されています。

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。

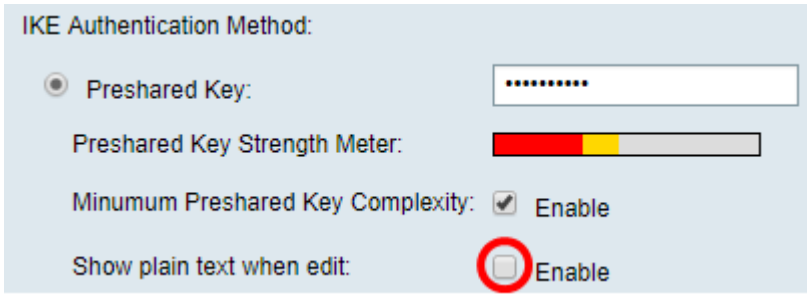


ステップ9:（オプション）[Minimum Preshared Key Complexity **Enable]チェックボ**ックスをオフにして、シンプルパスワードを使用できるようにします。



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

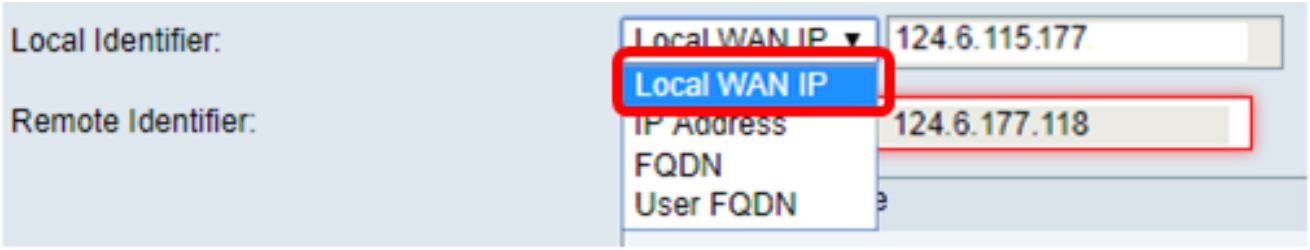
ステップ10:（オプション）パスワードをプレーンテキストで表示するには、[編集時にプレーンテキストを表**示する**]チェックボックスをオンにします。



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。

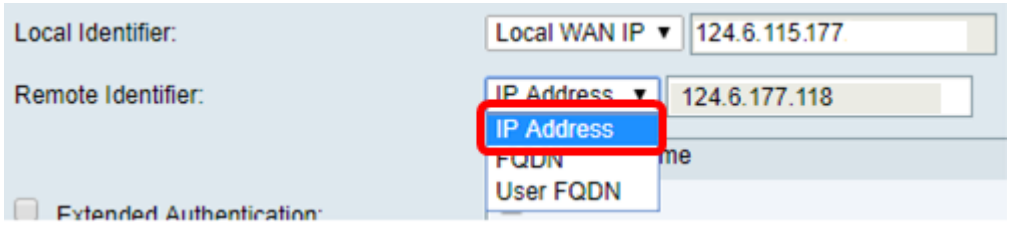
- ローカルWAN IP：このオプションでは、VPNゲートウェイのワイドエリアネットワーク(WAN)インターフェイスのIPアドレスを使用します。
- [IP Address]：このオプションを使用すると、VPN接続のIPアドレスを手動で入力できます。
- FQDN：このオプションは、完全修飾ドメイン名(FQDN)とも呼ばれます。 インターネット上の特定のコンピュータに完全なドメイン名を使用できます。
- [ユーザFQDN(User FQDN)]：このオプションを使用すると、インターネット上の特定のユーザに完全なドメイン名を使用できます。



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。

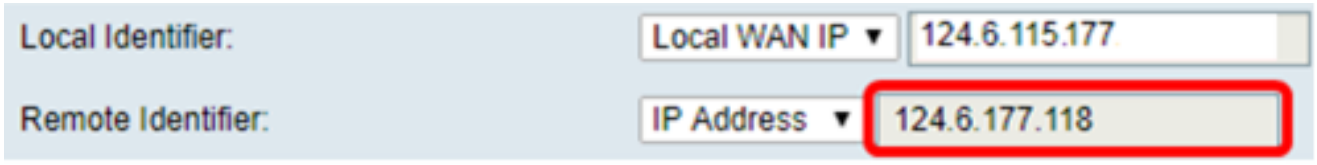
ステップ12:（オプション）リモートホストの識別子を選択します。次のオプションがあります。

- [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。



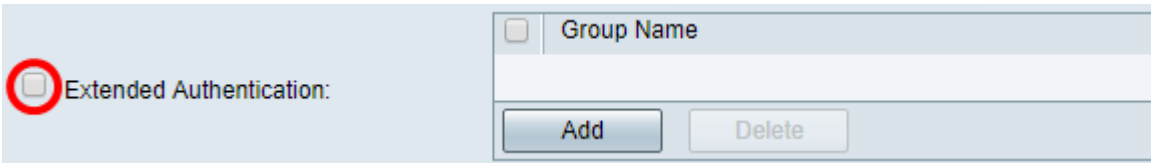
注：この例では、[IP Address]が選択されています。

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



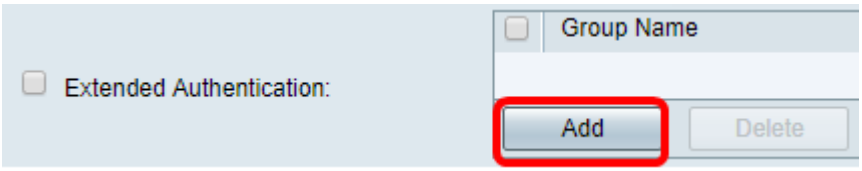
注：この例では、124.6.115.177と入力します。

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。

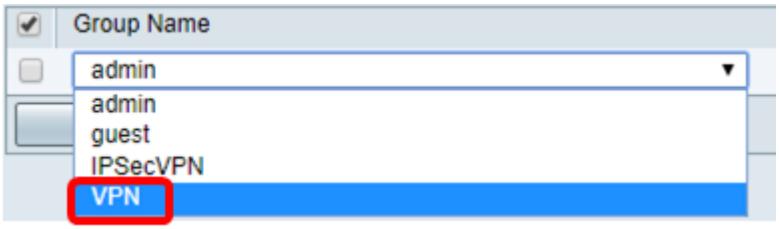


注：この例では、[Extended Authentication]はオフのままにします。

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



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。



注：この例では、VPNが選択されています。

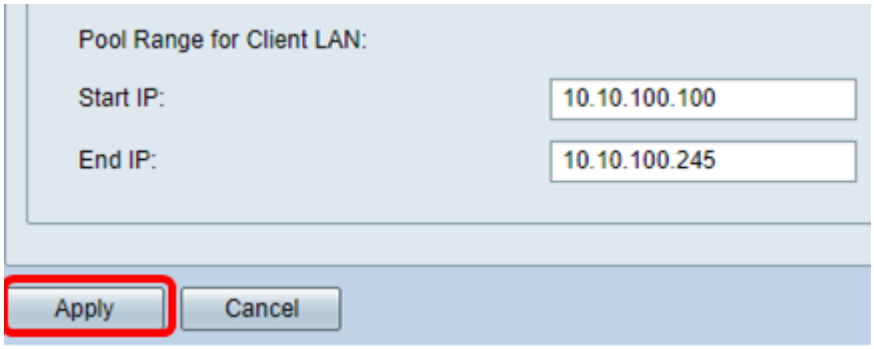
ステップ17:[Pool Range for Client LAN]で、VPNクライアントに割り当てることができる最初のIPアドレスを[*Start IP*]フィールドに入力します。

注：この例では、10.10.100.100と入力します。

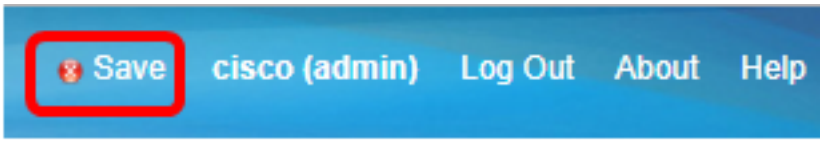
ステップ18:[End IP]フィールドに、VPNクライアントに割り当てることができる最後のIPアドレスを入力します。

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。



ステップ20:[Save]をクリックします。

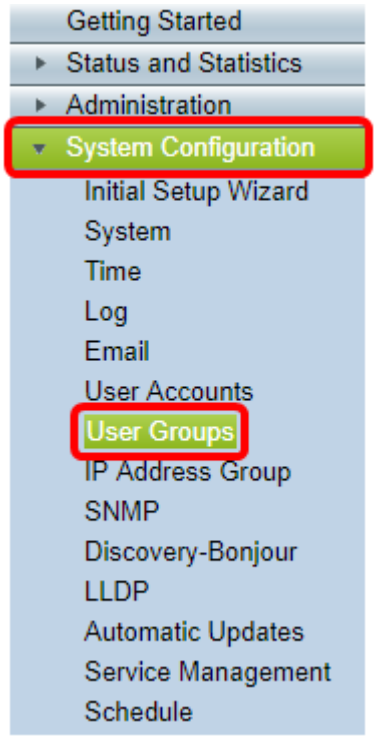


これで、TheGreenBow VPN Client用にルータのクライアントとサイト間プロファイルを設定できました。

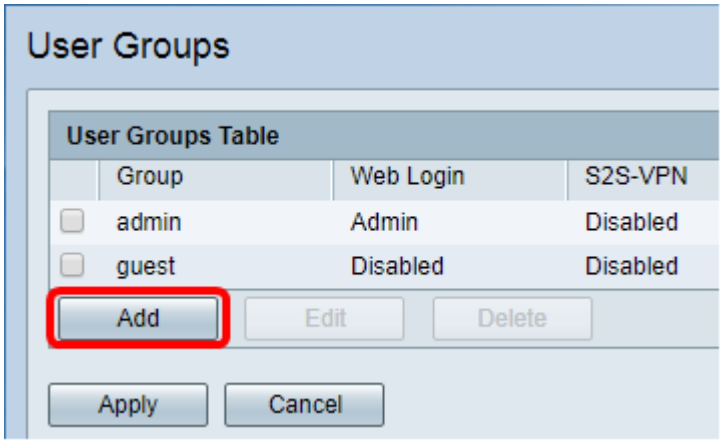
ユーザグループの作成

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。

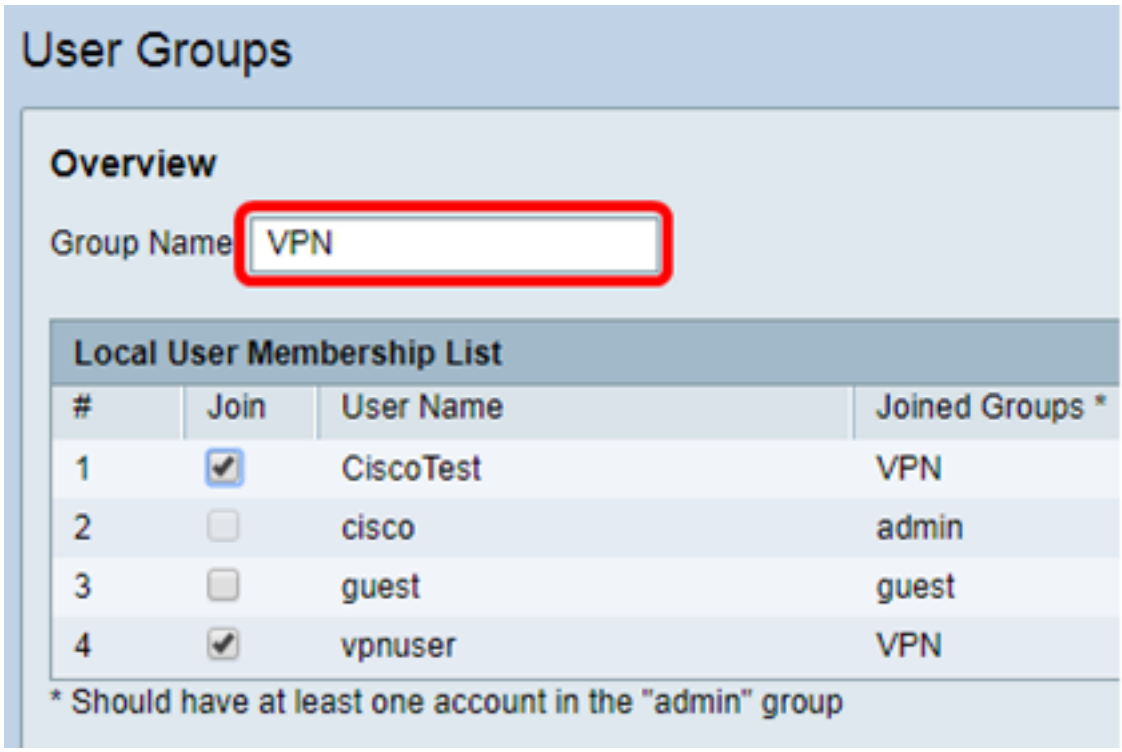
注：この記事の画像は、RV340ルータのものです。オプションは、デバイスのモデルによって異なります。



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。

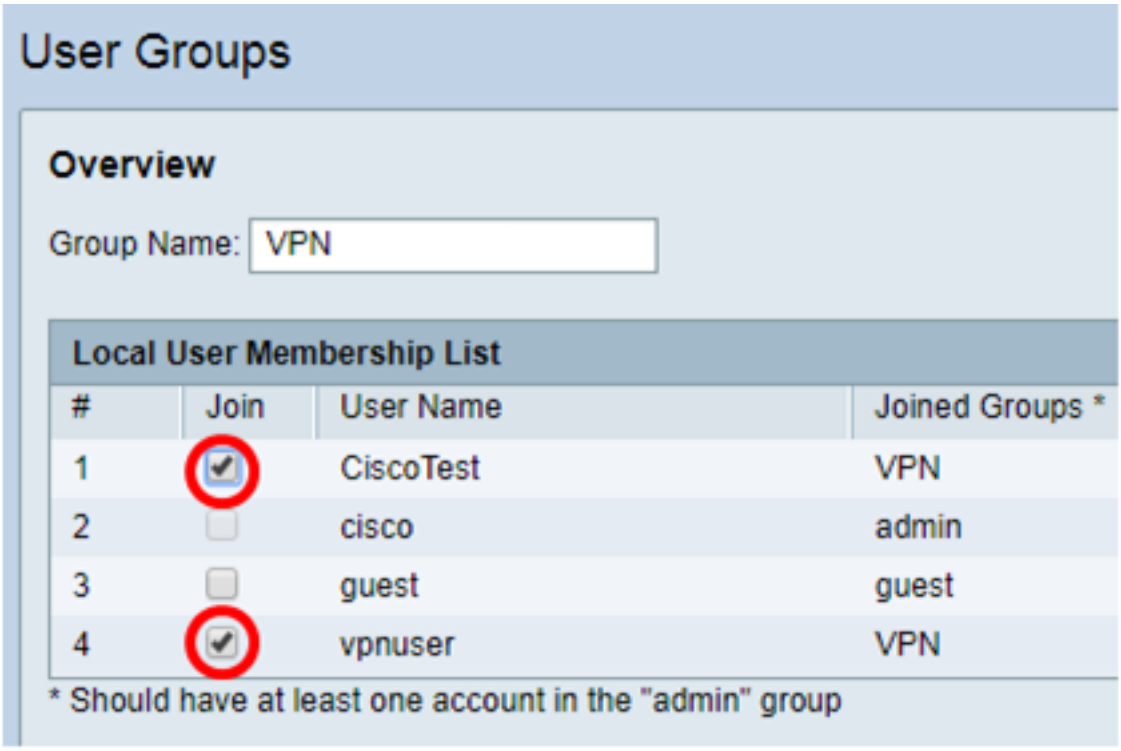


ステップ3:[Overview（概要）]領域で、[Group Name（グループ名）]フィールドにグループの*名前を入力*します。



注：この例では、VPNが使用されています。

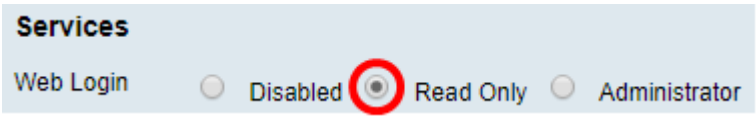
ステップ4:[Local Membership List（ローカルメンバーシップリスト）]で、同じグループに属する必要があるユーザ名のチェックボックスをオンにします。



注：この例では、CiscoTestとvpnuserが選択されています。

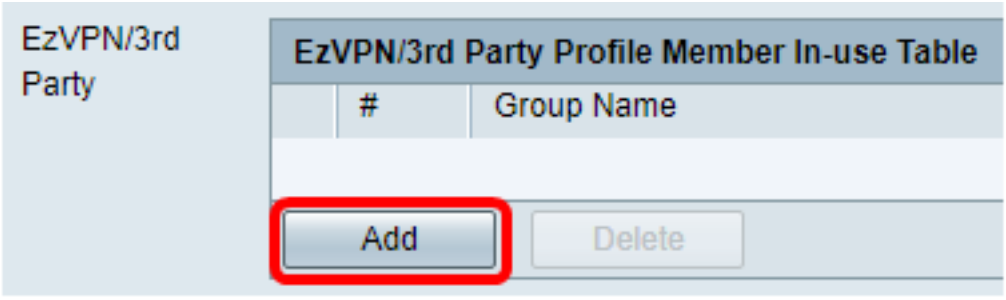
ステップ5:[Services（サービス）]で、グループ内のユーザに付与する権限を選択します。次のオプションがあります。

- [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。

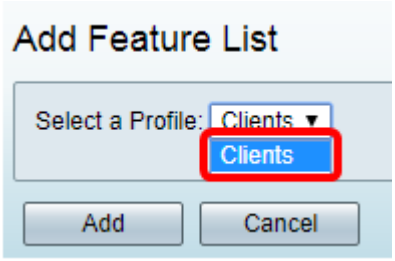


注：この例では、[Read Only]が選択されています。

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。

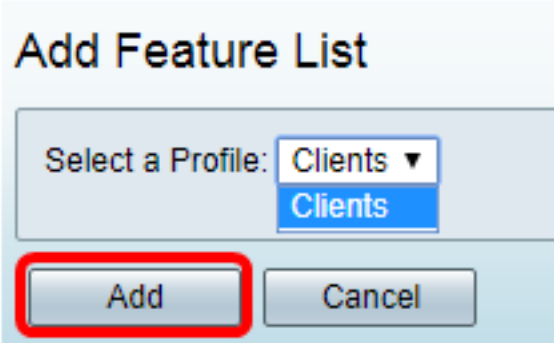


ステップ7:[Select a Profile]ドロップダウンリストからプロファイルを選択します。オプションは、VPNゲートウェイに設定されているプロファイルによって異なります。

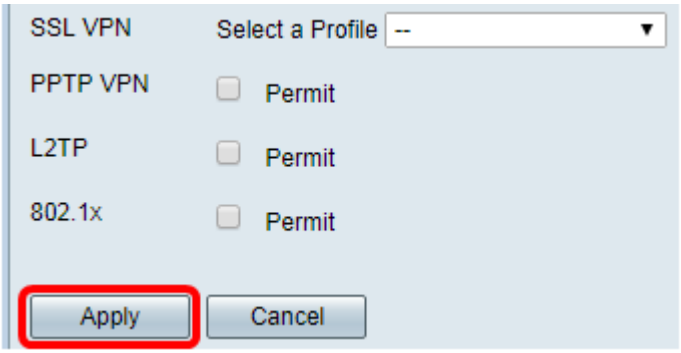


注：この例では、[Clients]が選択されています。

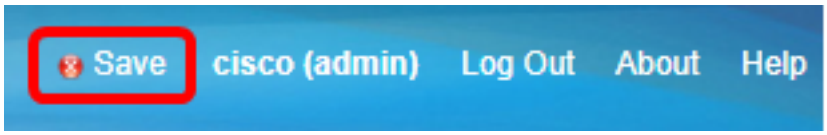
ステップ8:[Add]をクリックします。



ステップ9:[Apply]をクリックします。



ステップ10:[Save]をクリックします。

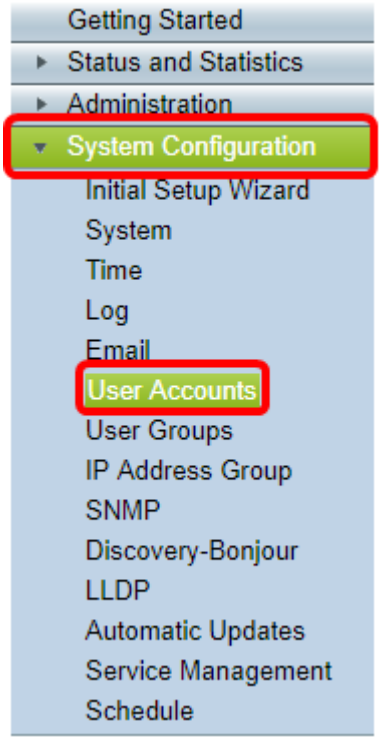


これで、RV34xシリーズルータにユーザグループが正常に作成されたはずです。

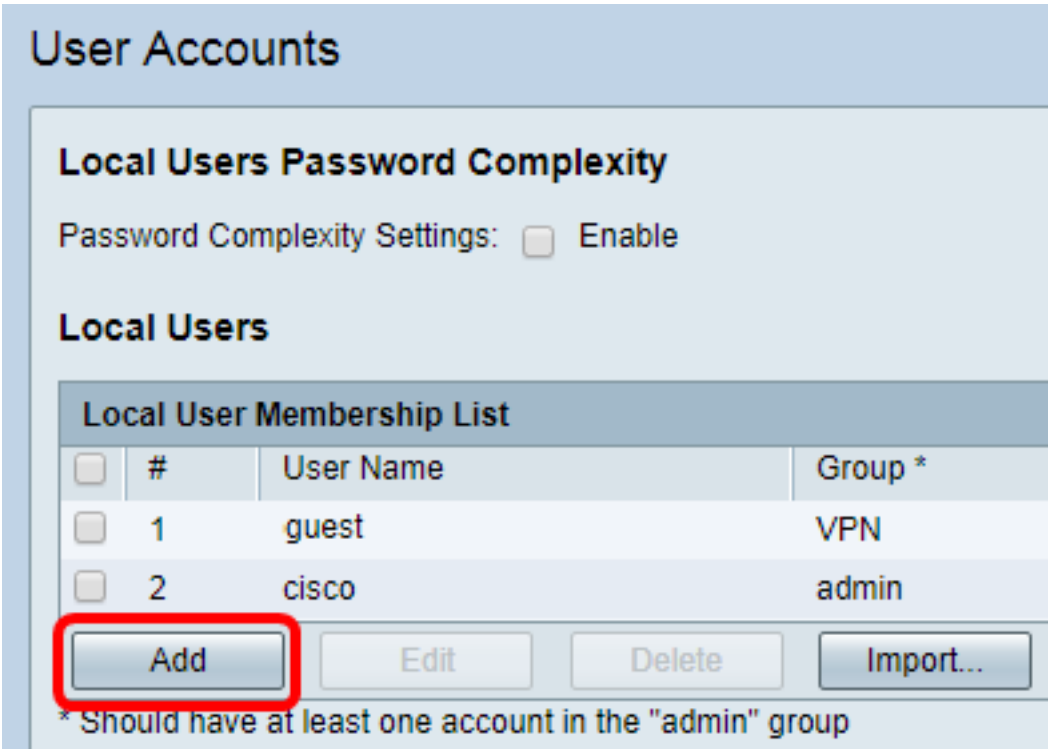
ユーザアカウントの作成

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。

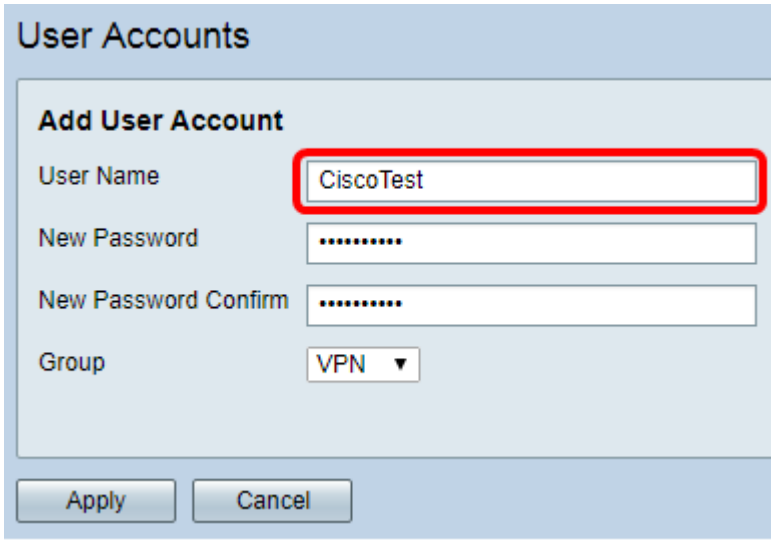
注：この記事の画像は、RV340ルータのものです。オプションは、デバイスのモデルによって異なります。



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

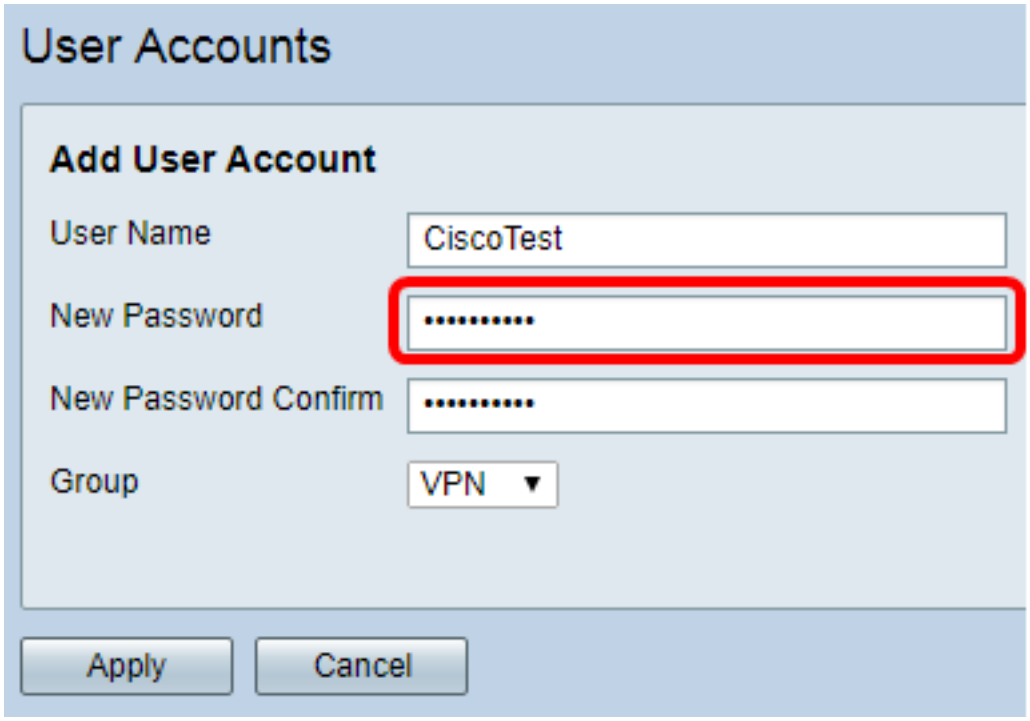


ステップ3:[User Name]フィールドにユーザの名前を入力します。

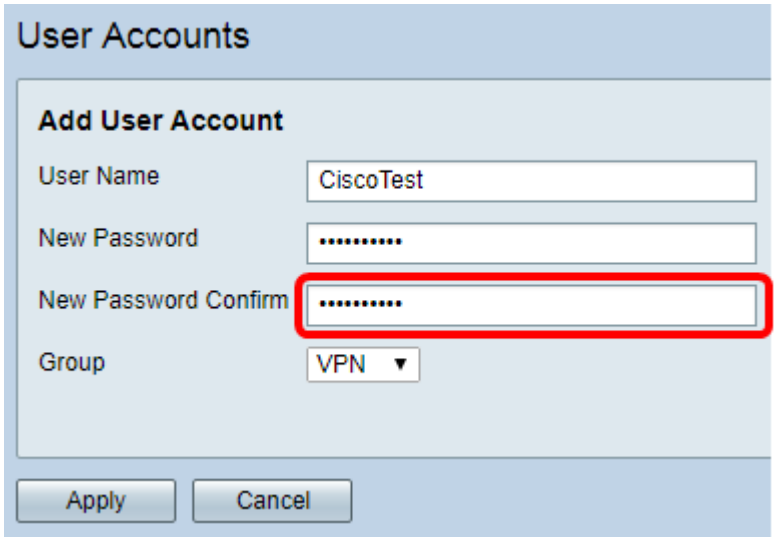


注：この例では、CiscoTestが入力されています。

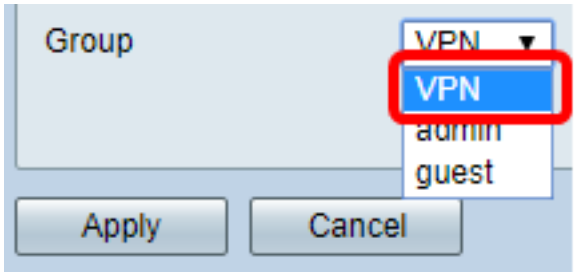
ステップ4:[New Password]フィールドにユーザパスワードを入力します。



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

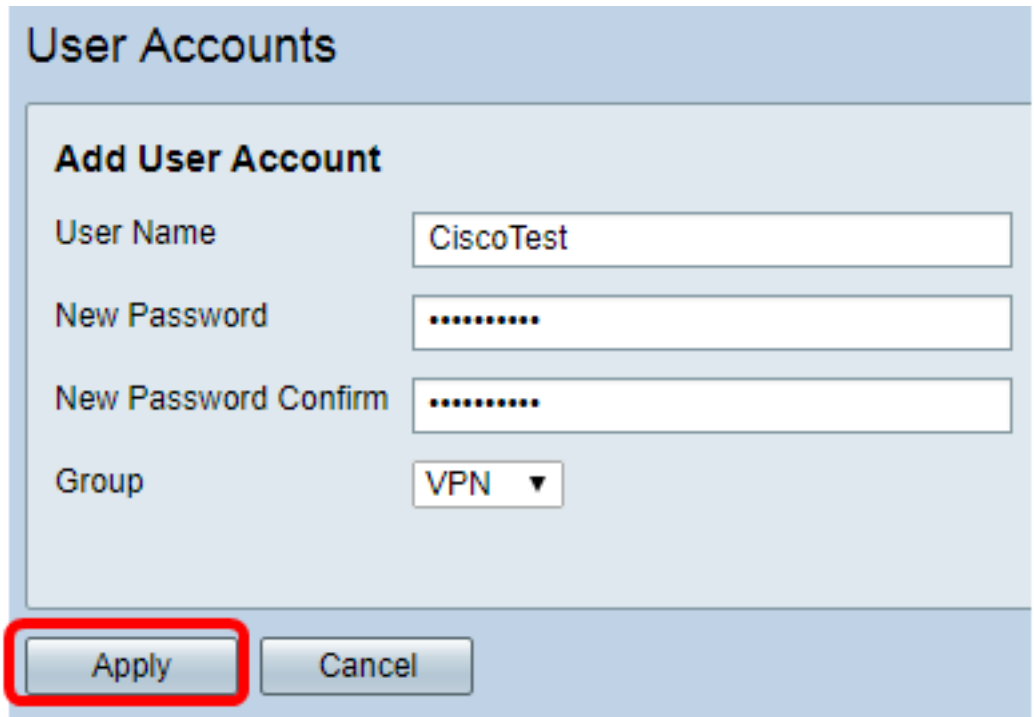


ステップ6:[Group]ドロップダウンリストからグループを選択します。これは、ユーザが関連付けられるグループです。

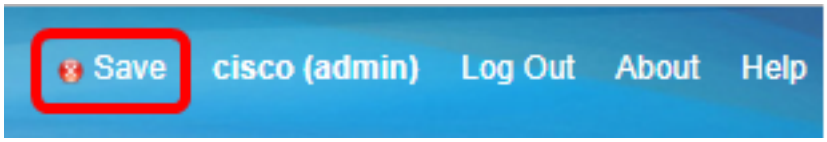


注：この例では、VPNが選択されています。

ステップ7:[Apply]をクリックします。



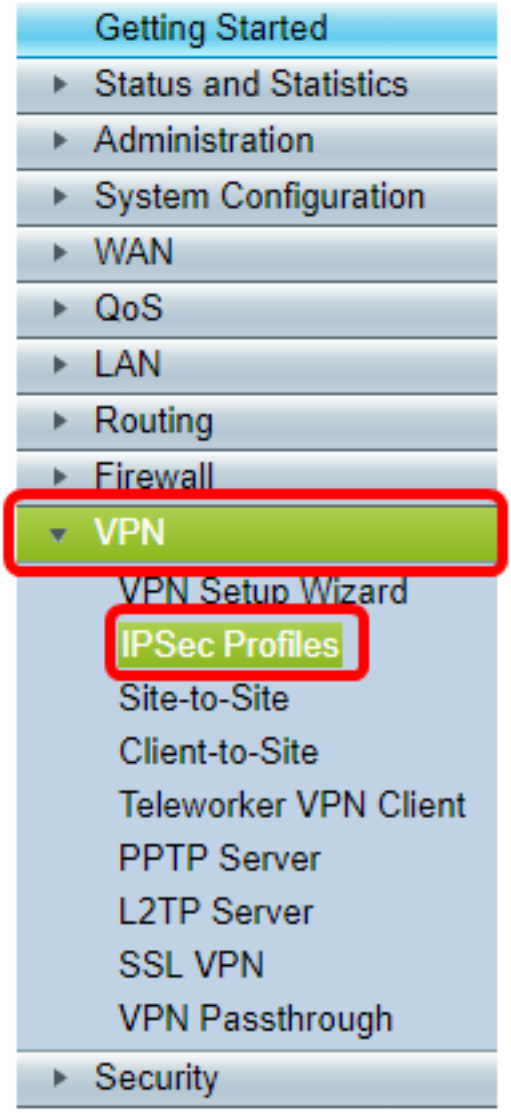
ステップ8:[Save]をクリックします。



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。

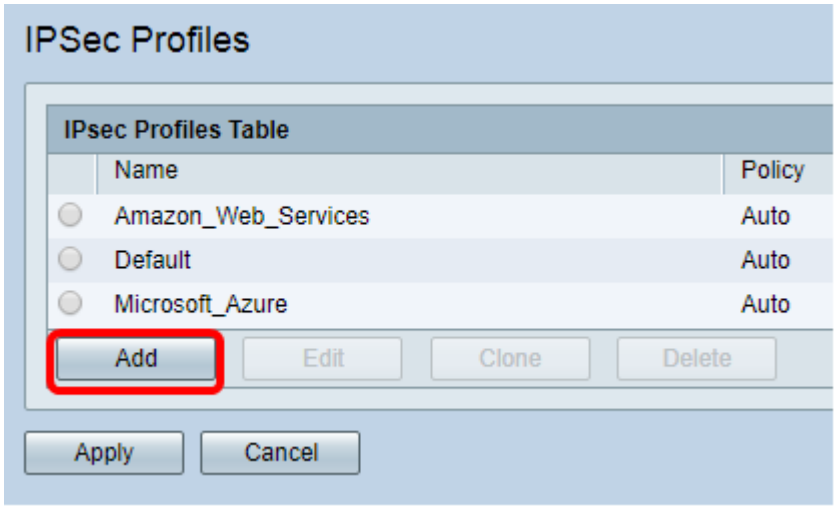
IPSecプロファイルの設定

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。**



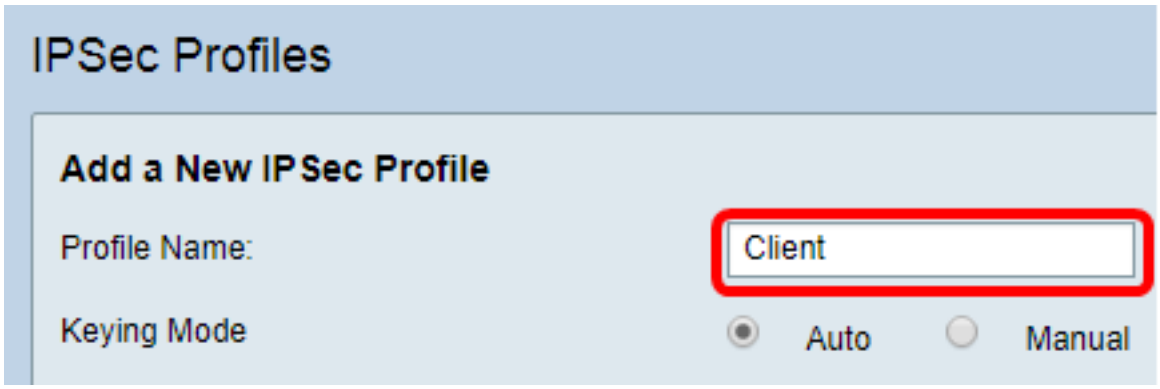
注：この記事の画像は、RV340ルータのものです。オプションは、デバイスのモデルによって異なります。

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。



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

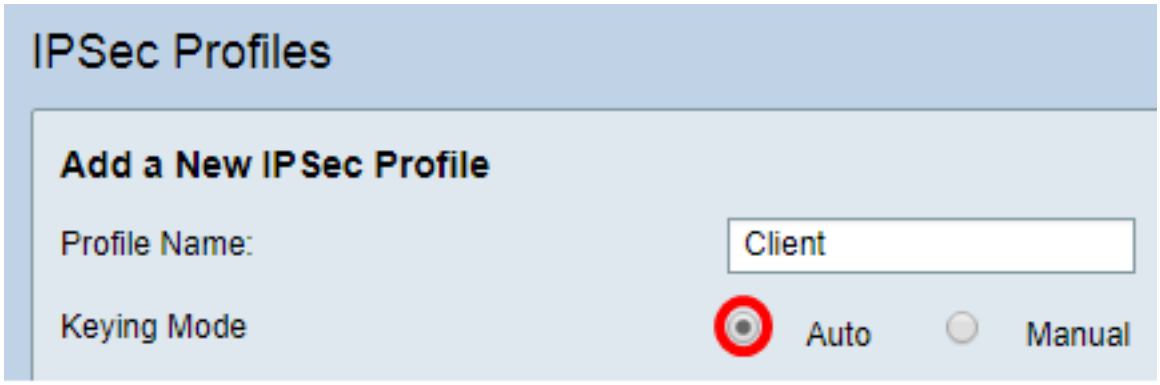
ステップ3:[Profile Name]フィールドにプロファイルの名前を*作成*します。プロファイル名には、英数字と特殊文字のアンダースコア(_)のみを使用してください。



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。



注：この例では、[Auto]が選択されています。

フェーズIおよびフェーズIIの設定

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。

注：この例では、Group5-1536ビットが選択されています。

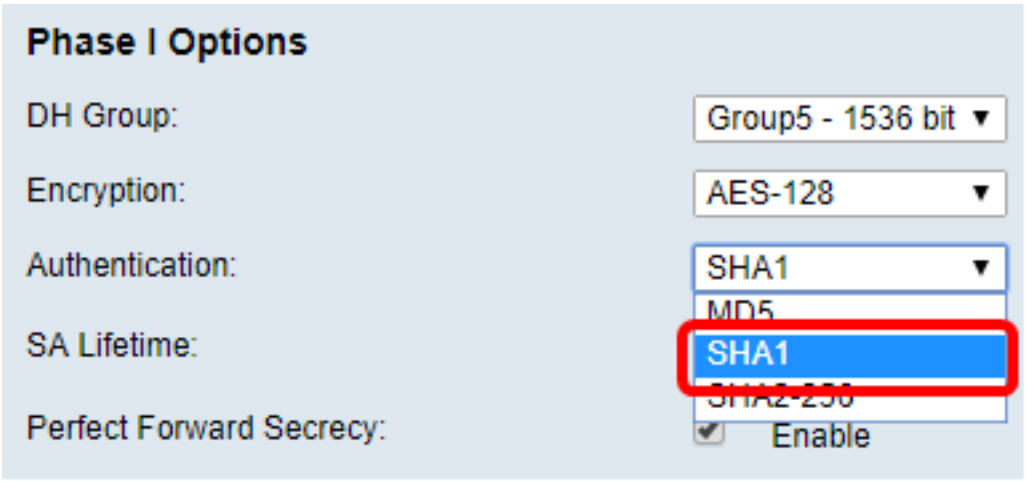
ステップ2:[Encryption]ドロップダウンリストから、Encapsulating Security Payload(ESP)およびInternet Security Association and Key Management Protocol(ISAKMP)を暗号化および復号化する暗号化方式を選択します。 次のオプションがあります。

- 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。

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。

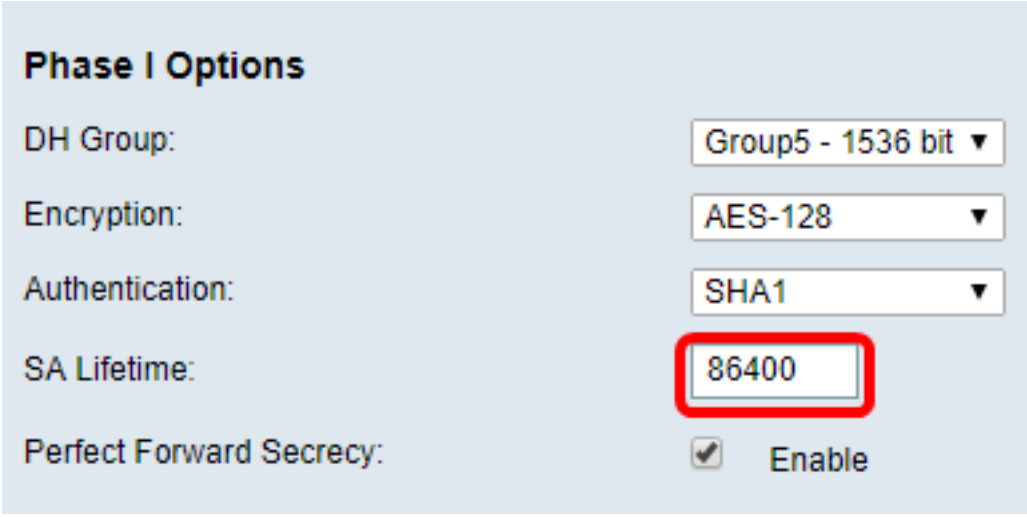
ステップ3:[Authentication]ドロップダウンリストから、ESPおよびISAKMPの認証方法を選択します。次のオプションがあります。

- 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。



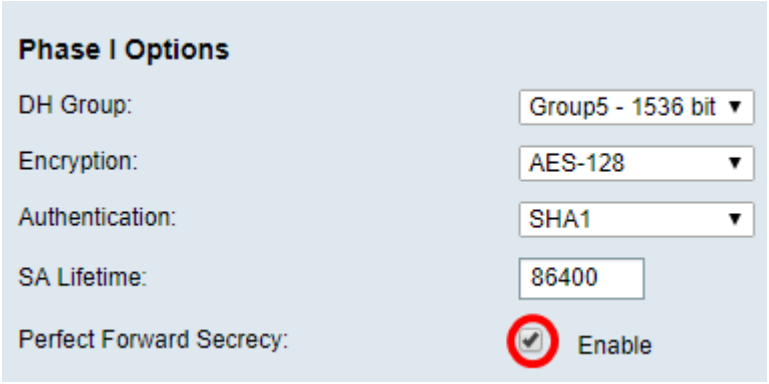
注：MD5とSHAは両方とも暗号化ハッシュ関数です。データの一部を取り、圧縮し、通常は再生できない一意の16進数出力を作成します。この例では、SHA1が選択されています。

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。



注：この例では、86400と入力します。

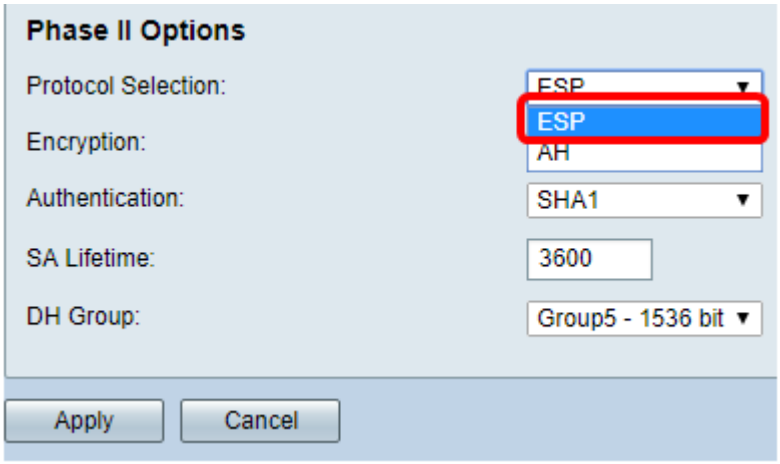
ステップ5:（オプション）[Enable Perfect Forward Secrecy]チェックボックスをオンにして、IPSecトラフィックの暗号化と認証のための新しいキーを生成します。



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。

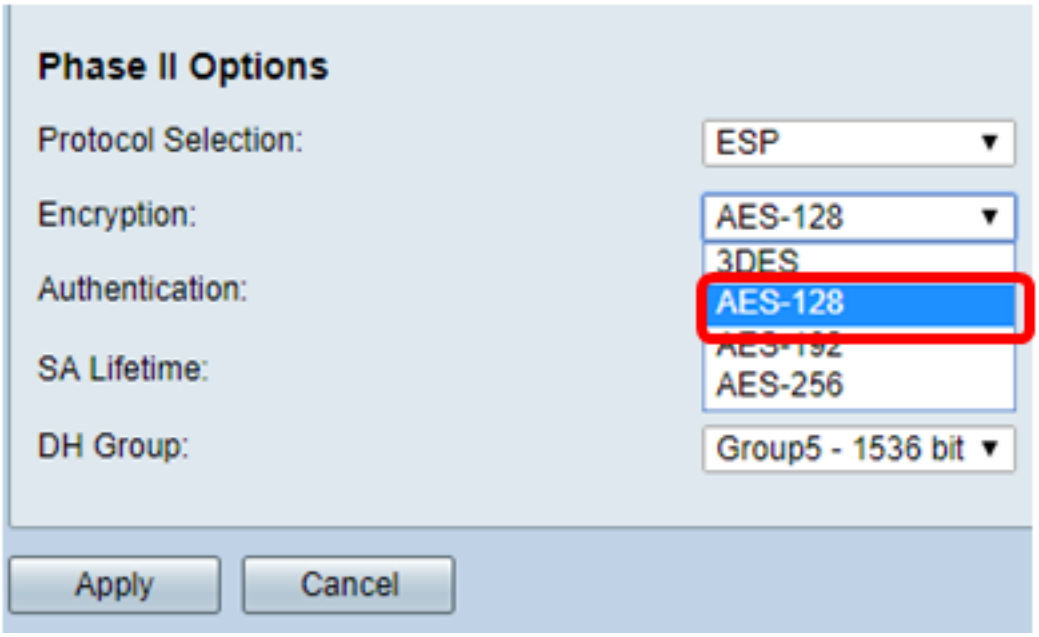
- ESP：このオプションは、保護するデータをカプセル化します。このオプションを選択した場合は、ステップ7に進んで暗号化方式を選択します。
- AH：このオプションは、認証ヘッダー(AH)とも呼ばれます。 データ認証とオプションのアンチリプレイサービスを提供するセキュリティプロトコルです。AHは、保護されるIPデータグラムに埋め込まれています。このオプションを選択した場合は、ステップ8に進みます。



注：この例では、ESPが選択されています。

ステップ7：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。

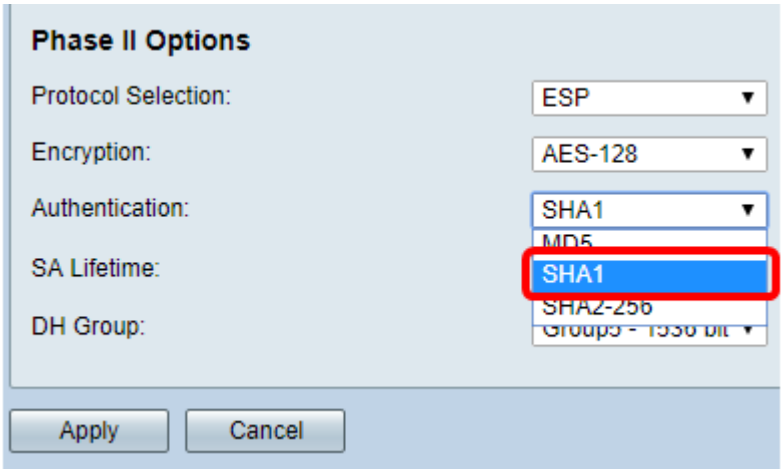
- 3DES:Triple Data Encryption Standard（トリプルデータ暗号化規格）
- AES-128:Advanced Encryption Standard(AES-128)は128ビットキーを使用します。
- AES-192:Advanced Encryption Standard（AES-192；高度暗号化規格）は192ビットキーを使用します。
- AES-256:Advanced Encryption Standard(AES-256)は256ビットキーを使用します。



注：この例では、AES-128が選択されています。

ステップ8:[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。

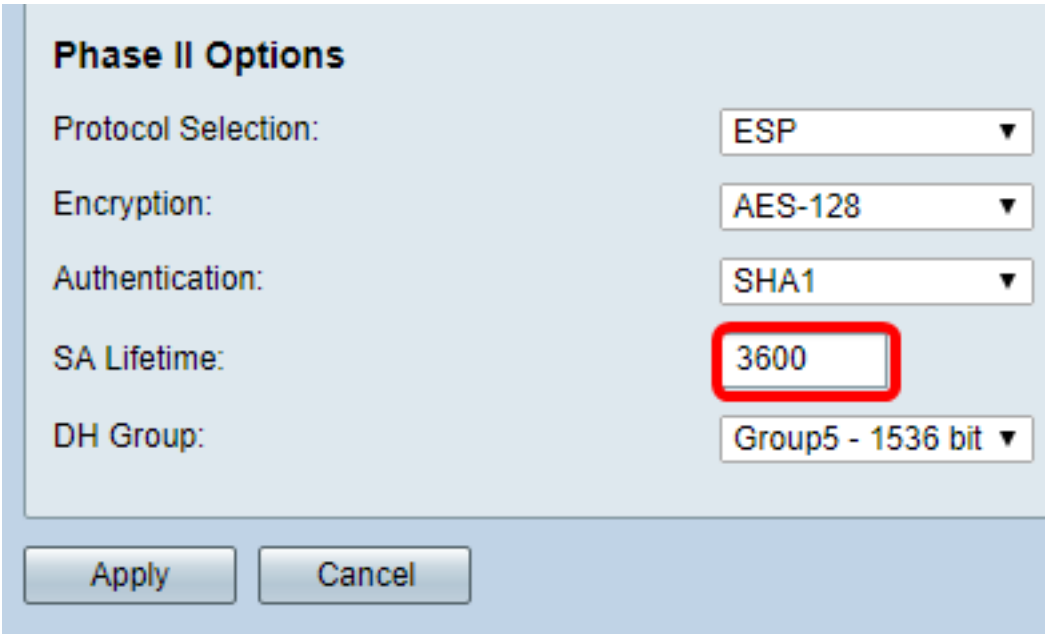


注：この例では、SHA1が選択されています。

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。

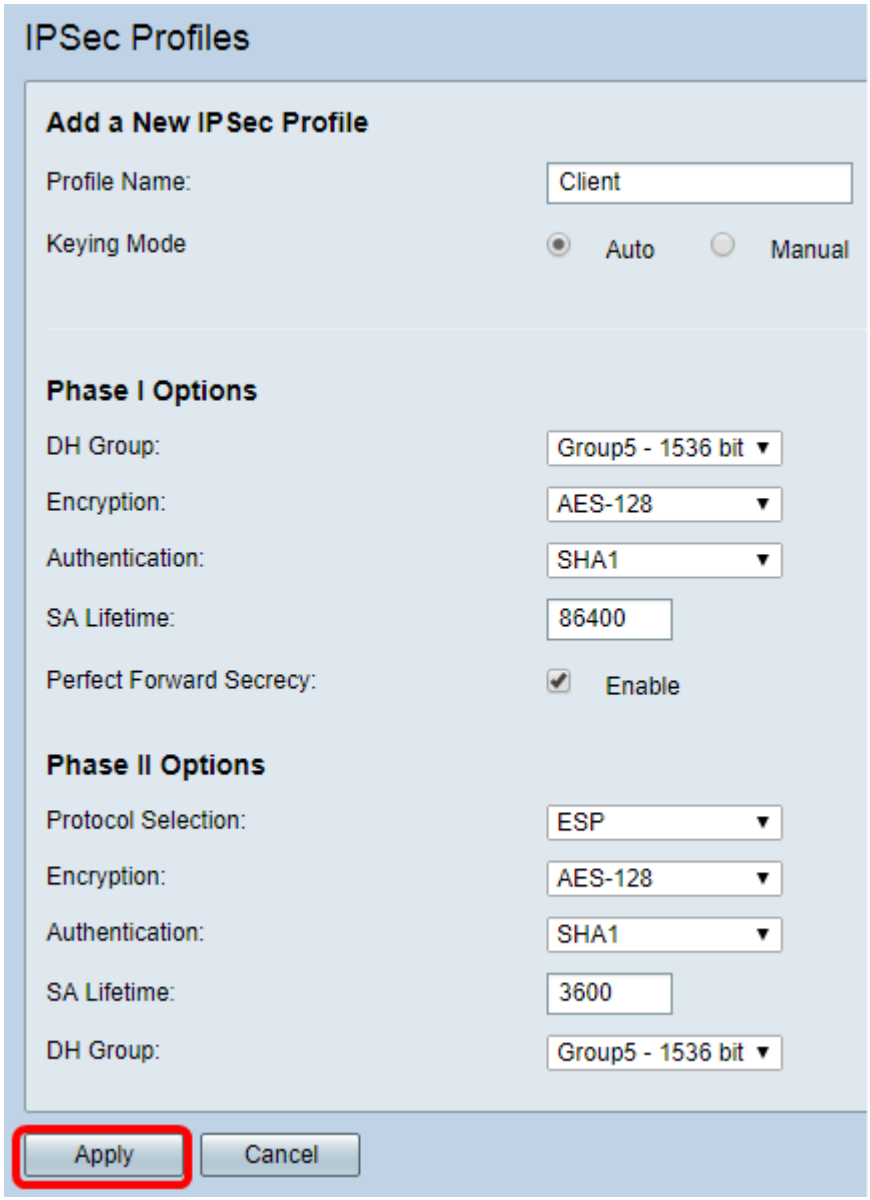
ステップ10:[DHグループ(DH Group)]ドロップダウンリストから、フェーズ2のキーで使用するDHグループを選択します。オプションは次のとおりです。

- 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。

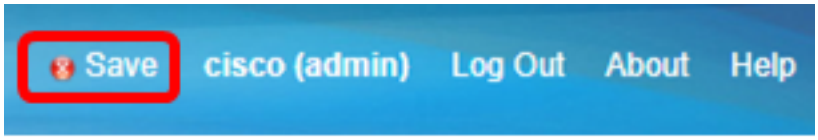


注：この例では、3600と入力します。

ステップ11:[Apply]をクリックします。



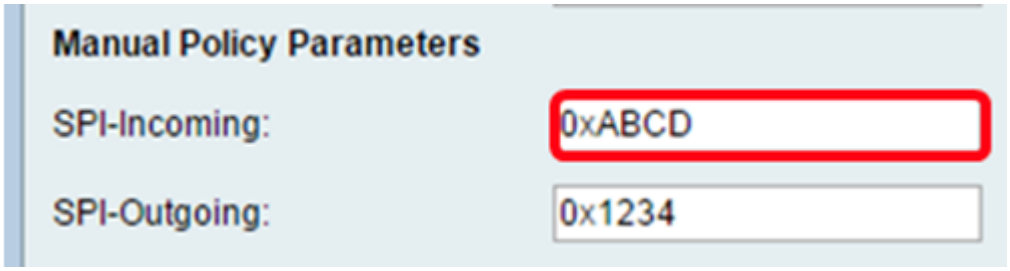
ステップ12:[Save]をクリックし、設定を永続的に保存します。



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。

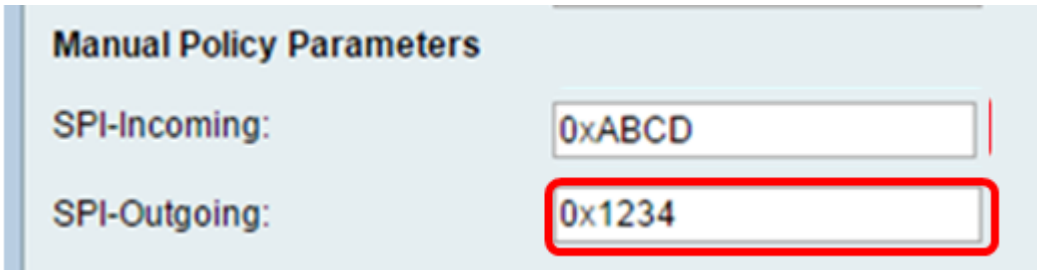
手動設定の設定

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 ~ FFFFFFF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。



注：この例では、0xABCDと入力します。

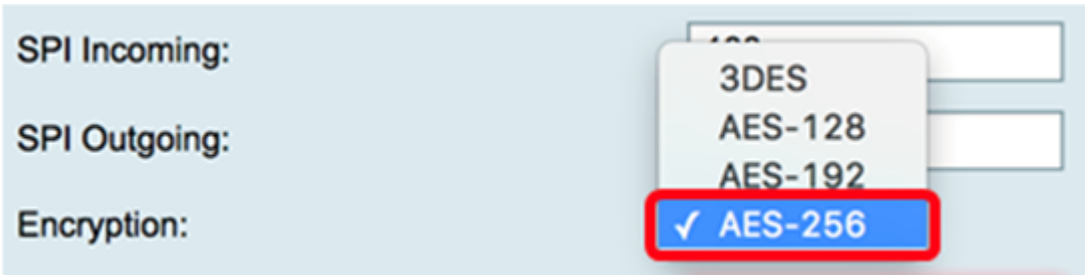
ステップ2:[*SPI-Outgoing*]フィールドに、VPN接続の発信トラフィックのSPIタグとして、100 ~ FFFFFFFの16進数値を入力します。



注：この例では、0x1234と入力します。

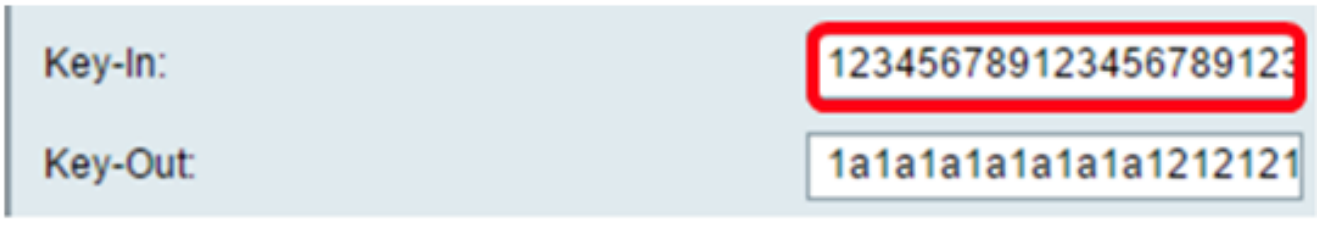
ステップ3：ドロップダウンリストから暗号化値を選択します。次のオプションがあります。

- 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。



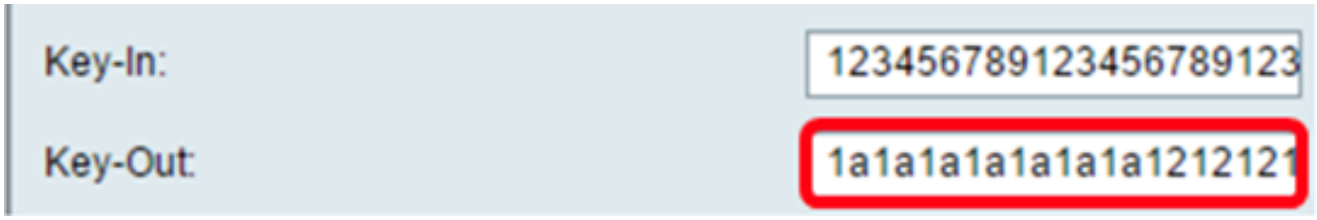
注：この例では、AES-256が選択されています。

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。



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

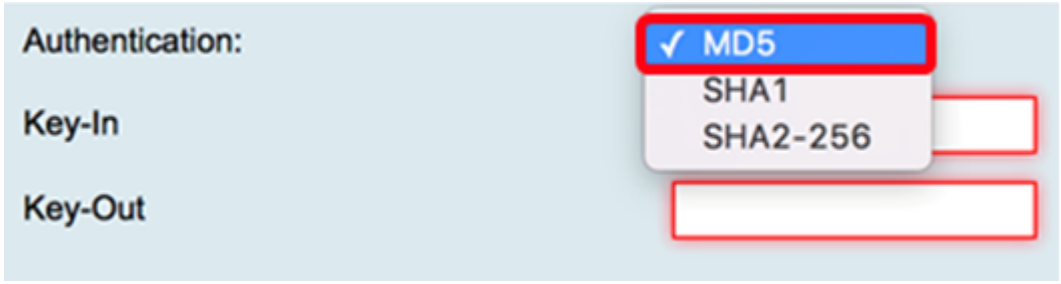
ステップ5:[*Key-Out*]フィールドに、発信ポリシーのキーを入力します。キーの長さは、ステップ3で選択したアルゴリズムによって異なります。



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

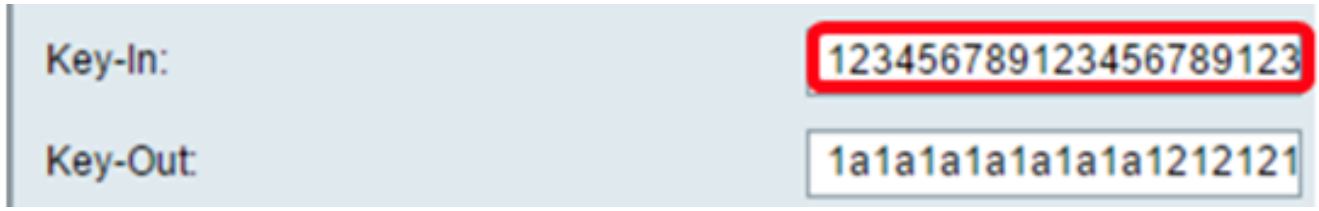
ステップ6:[Authentication]ドロップダウンリストから認証方法を選択します。次のオプションがあります。

- 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。



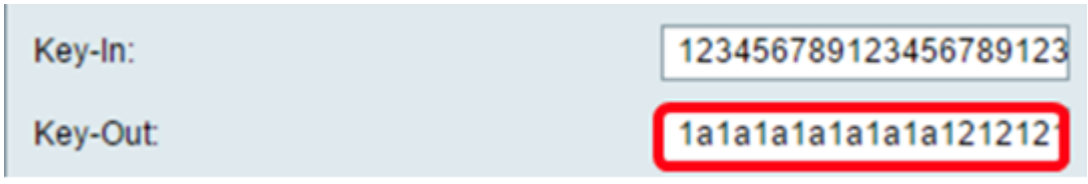
注：この例では、MD5が選択されています。

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。

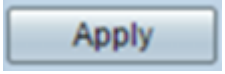


注：この例では、123456789123456789123...と入力します。

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。

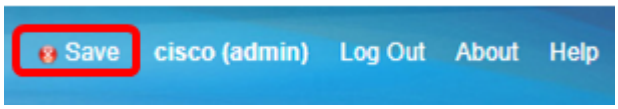


注：この例では、1a1a1a1a1a1a1a12121212...と入力します。

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。

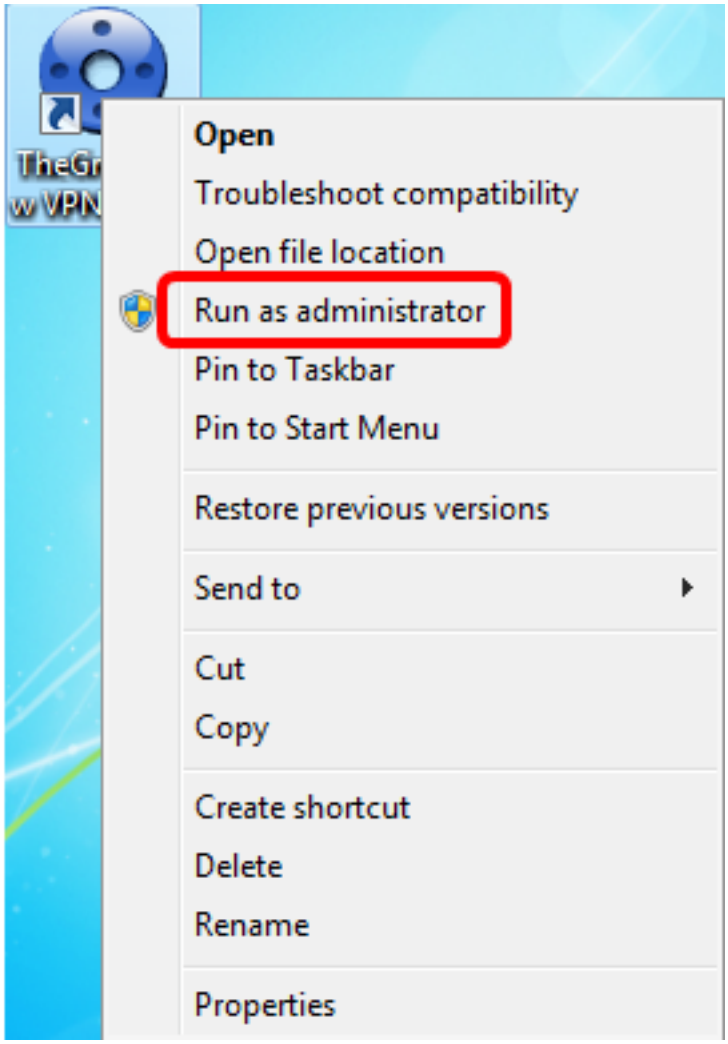


これで、RV34xシリーズルータで手動IPSecプロファイルが正しく設定されました。

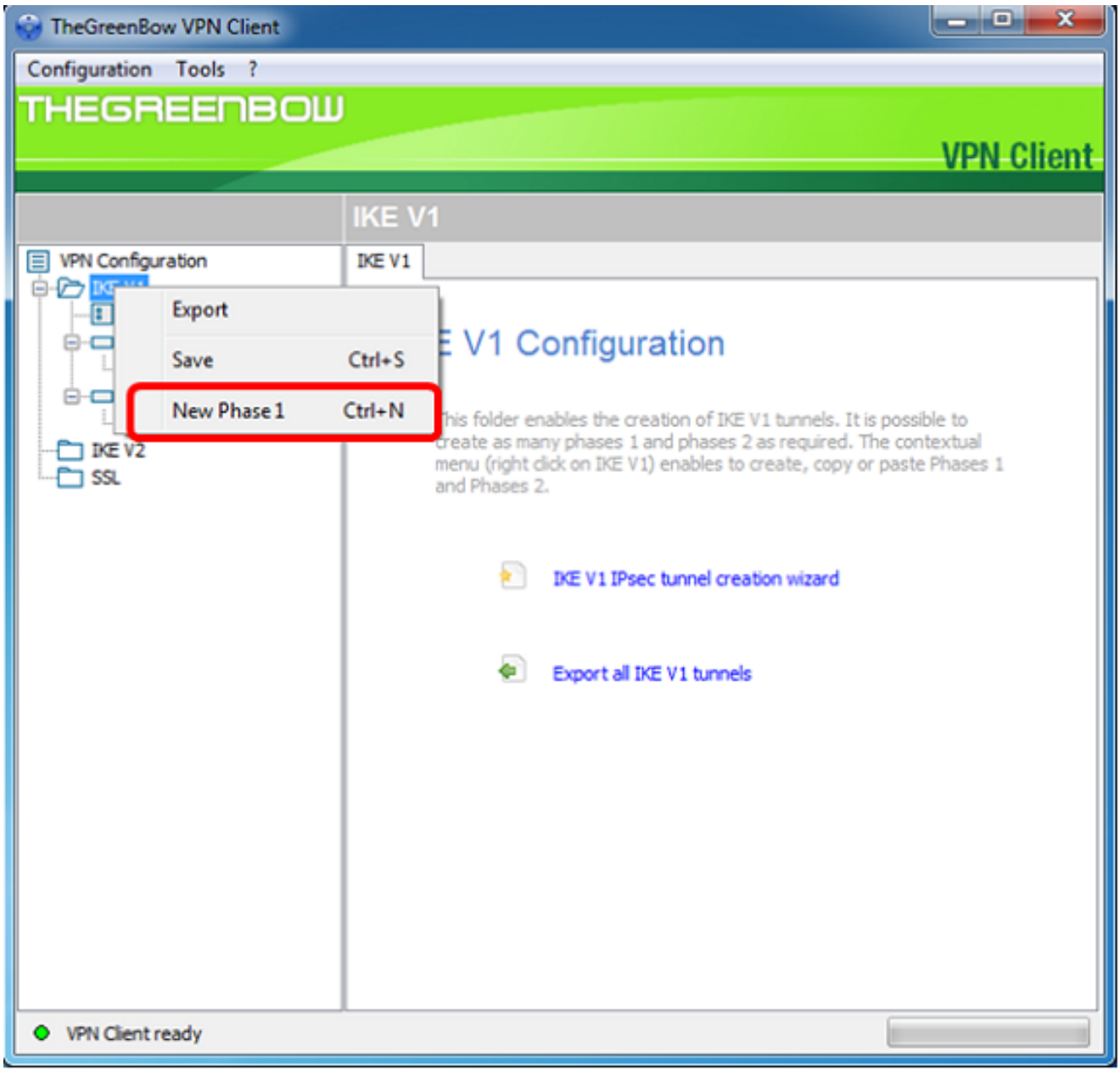
GreenBow VPNクライアントソフトウェアの設定

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。**

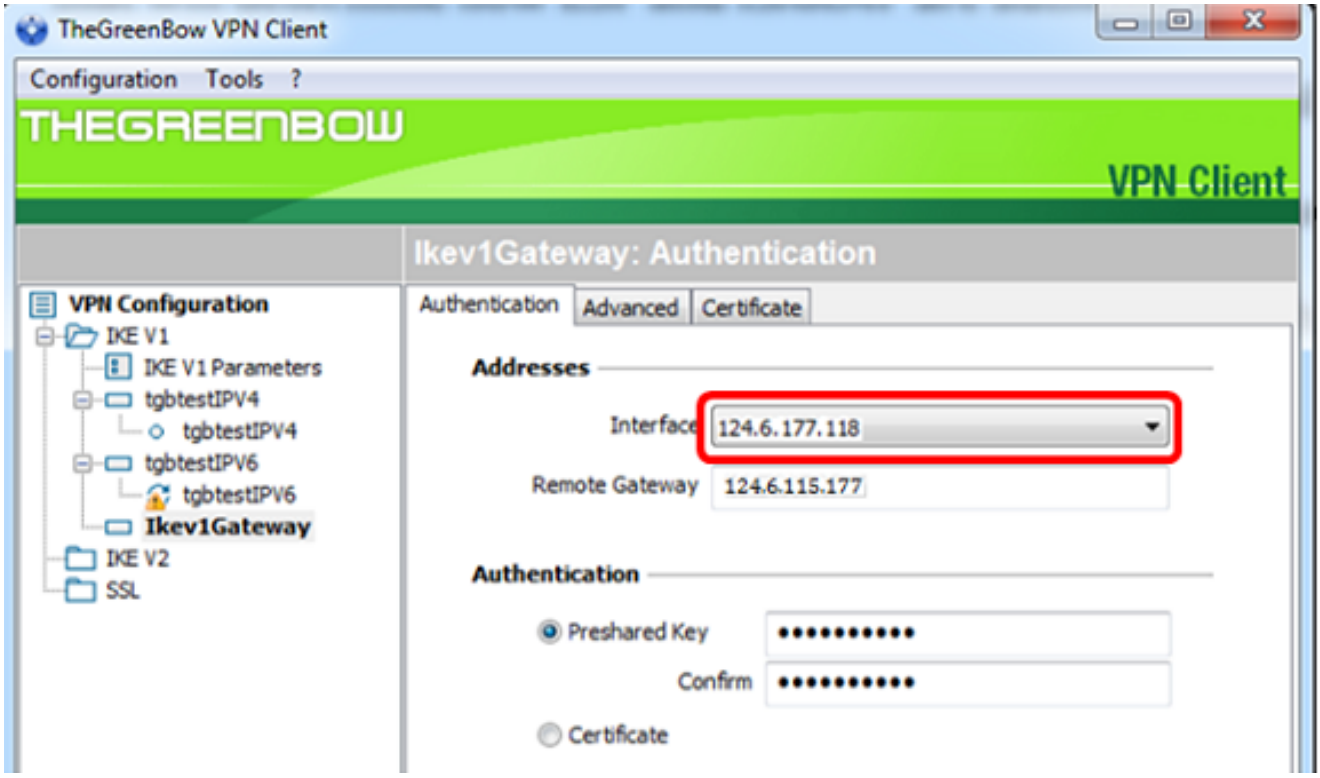


ステップ2：左側のペインの[VPN configuration]で、**[IKE V1]**を右クリックして、**[New Phase 1]を選択します。**



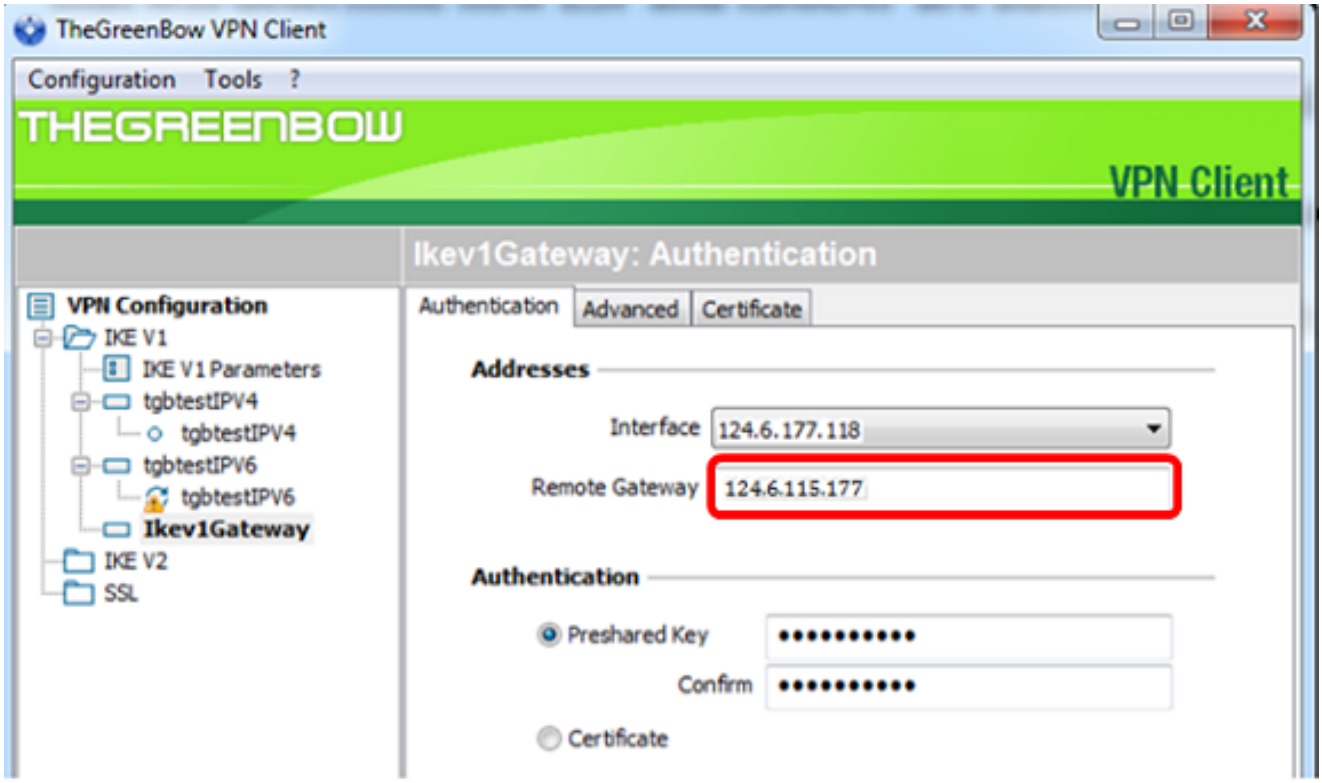
ステップ3:[Authentication]タブの[Addresses]で、[Interface]エリアのIPアドレスが、TheGreenBow VPN Clientがインストールされているコンピュータのwan IPアドレスと同じであることを確認します。

注：この例では、IP アドレスは 124.6.177.118 です。



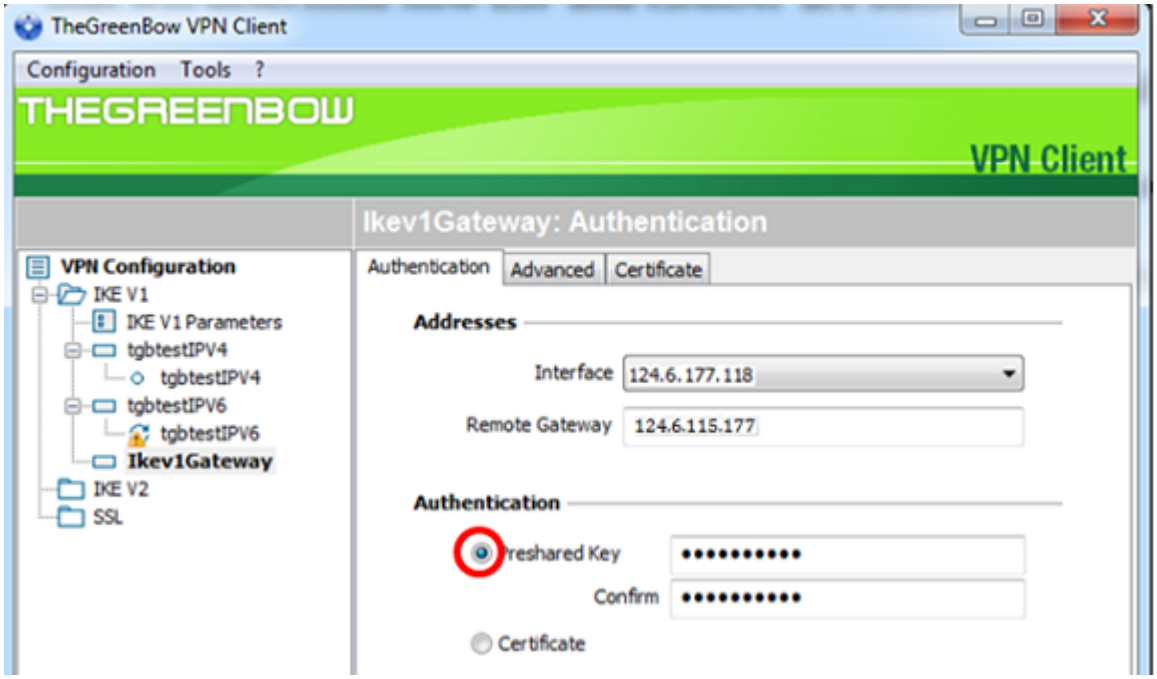
ステップ4:[Remote Gateway]フィールドにリモートゲートウェイのアドレスを入力します。

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。



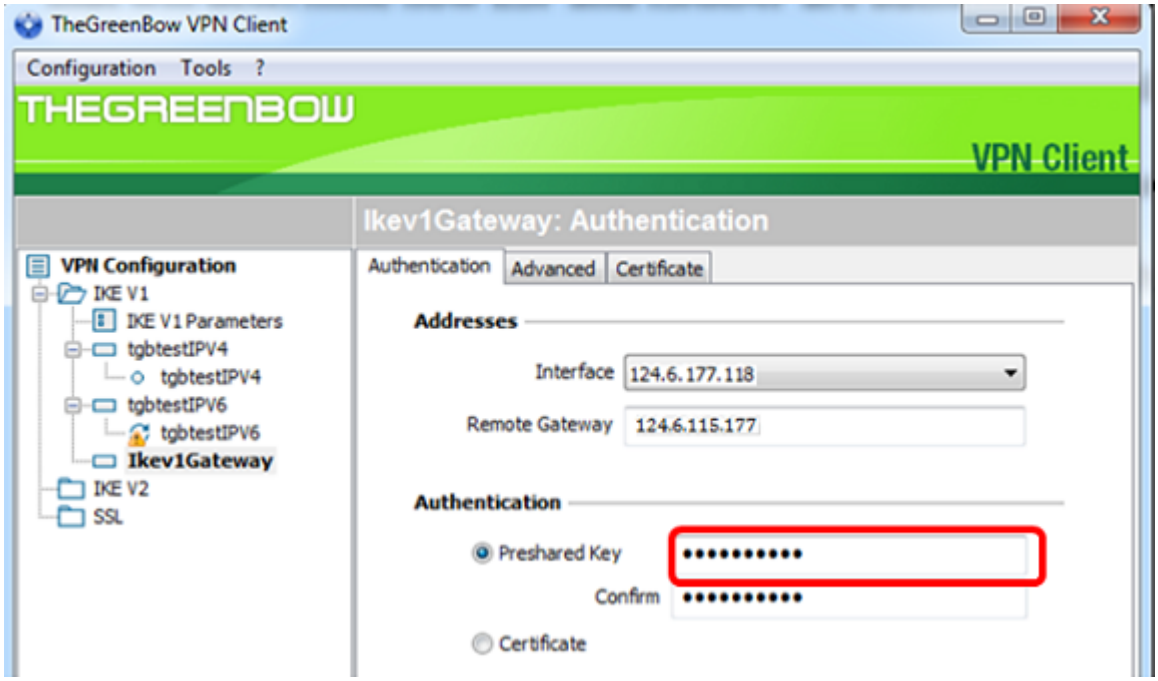
ステップ5:[Authentication]で、認証タイプを選択します。次のオプションがあります。

- 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。

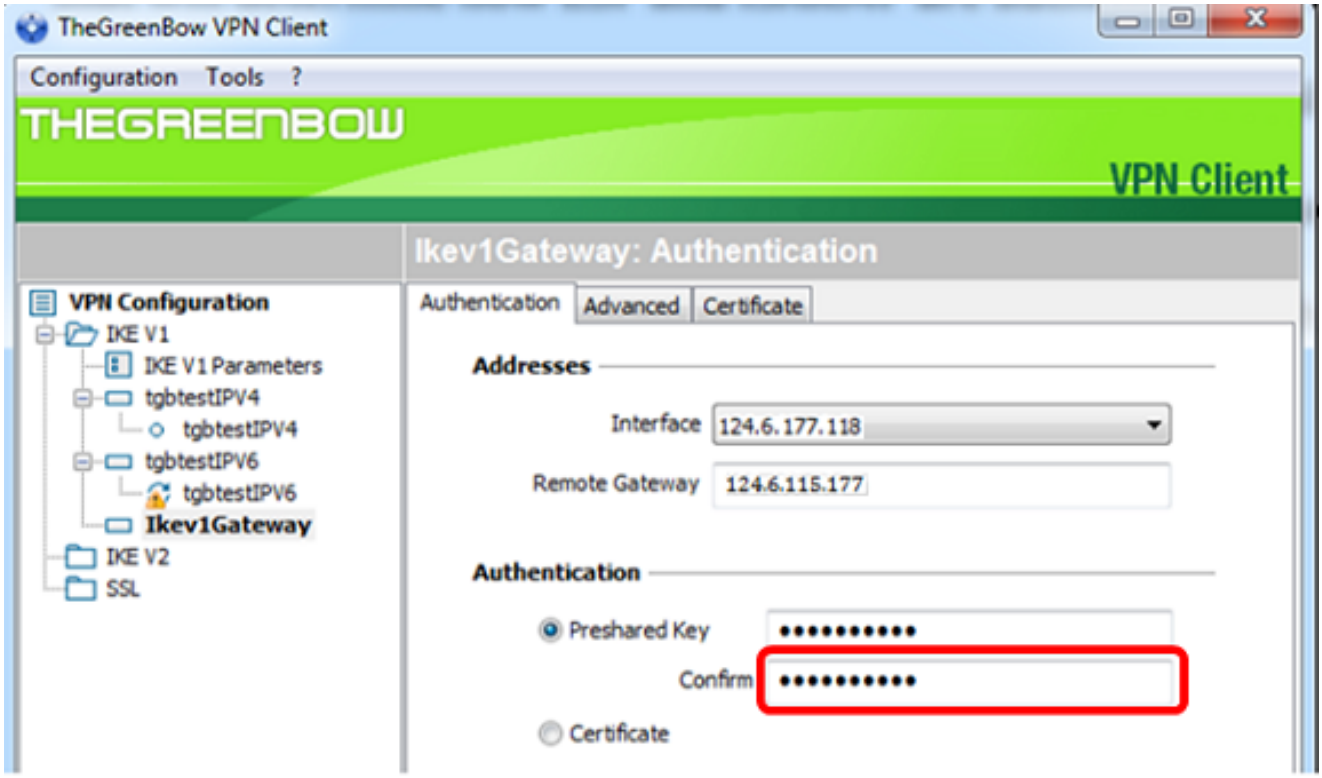


注：この例では、RV34x VPNゲートウェイの設定と一致するように[Preshared Key]が選択されています。

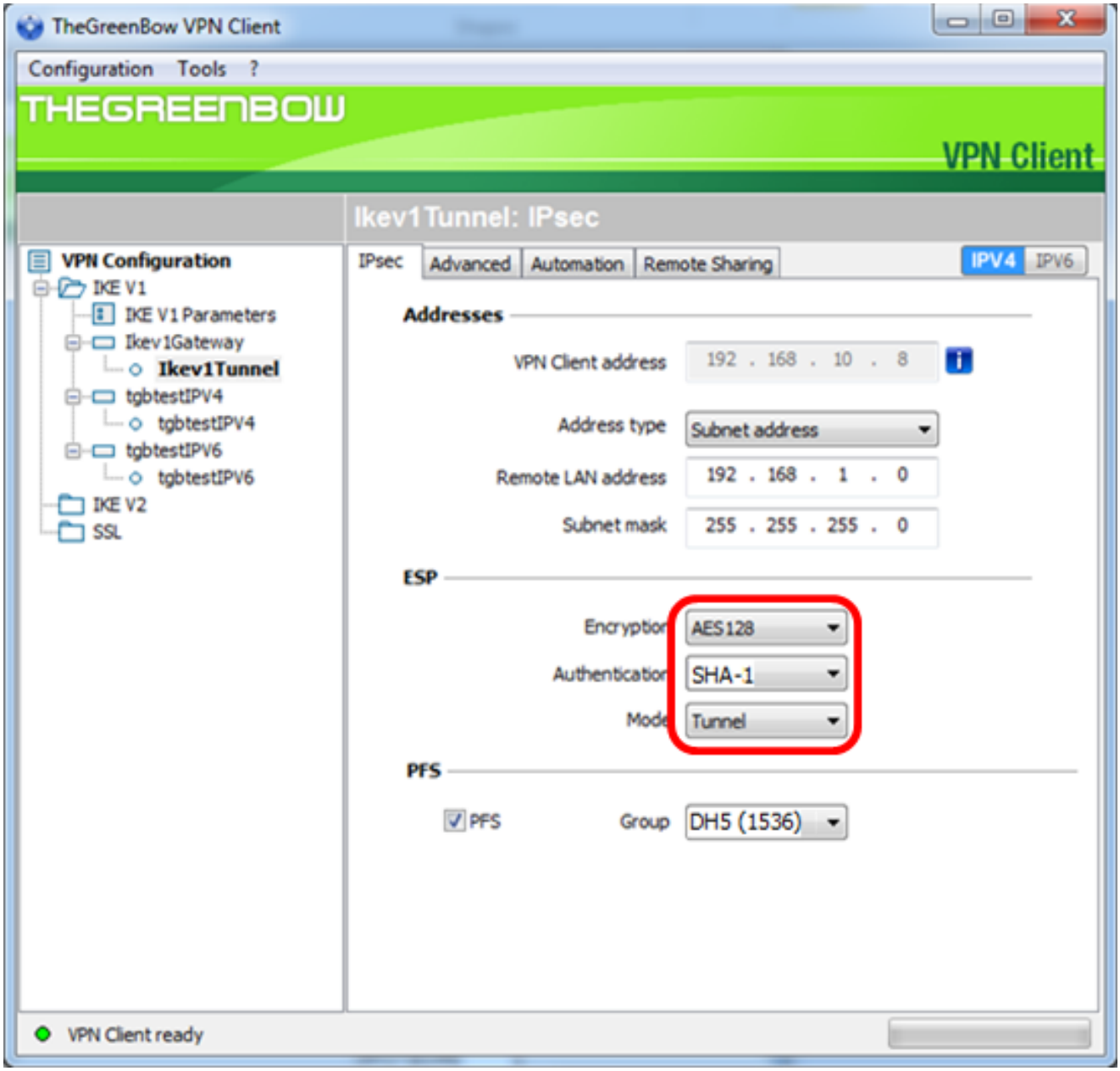
ステップ6：ルータで設定されている事前共有キーを入力します。



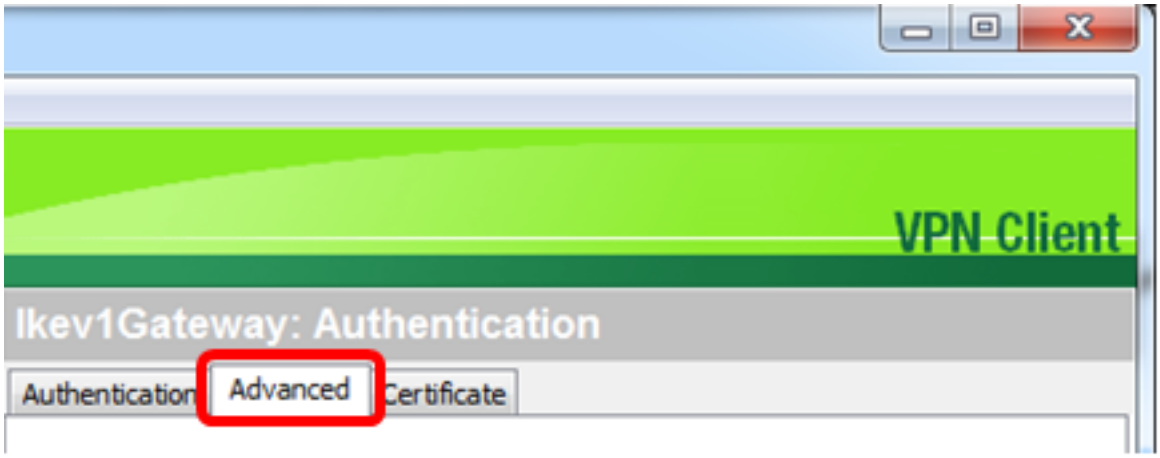
ステップ7:[Confirm]フィールドに同じ事前共有キーを入力します。



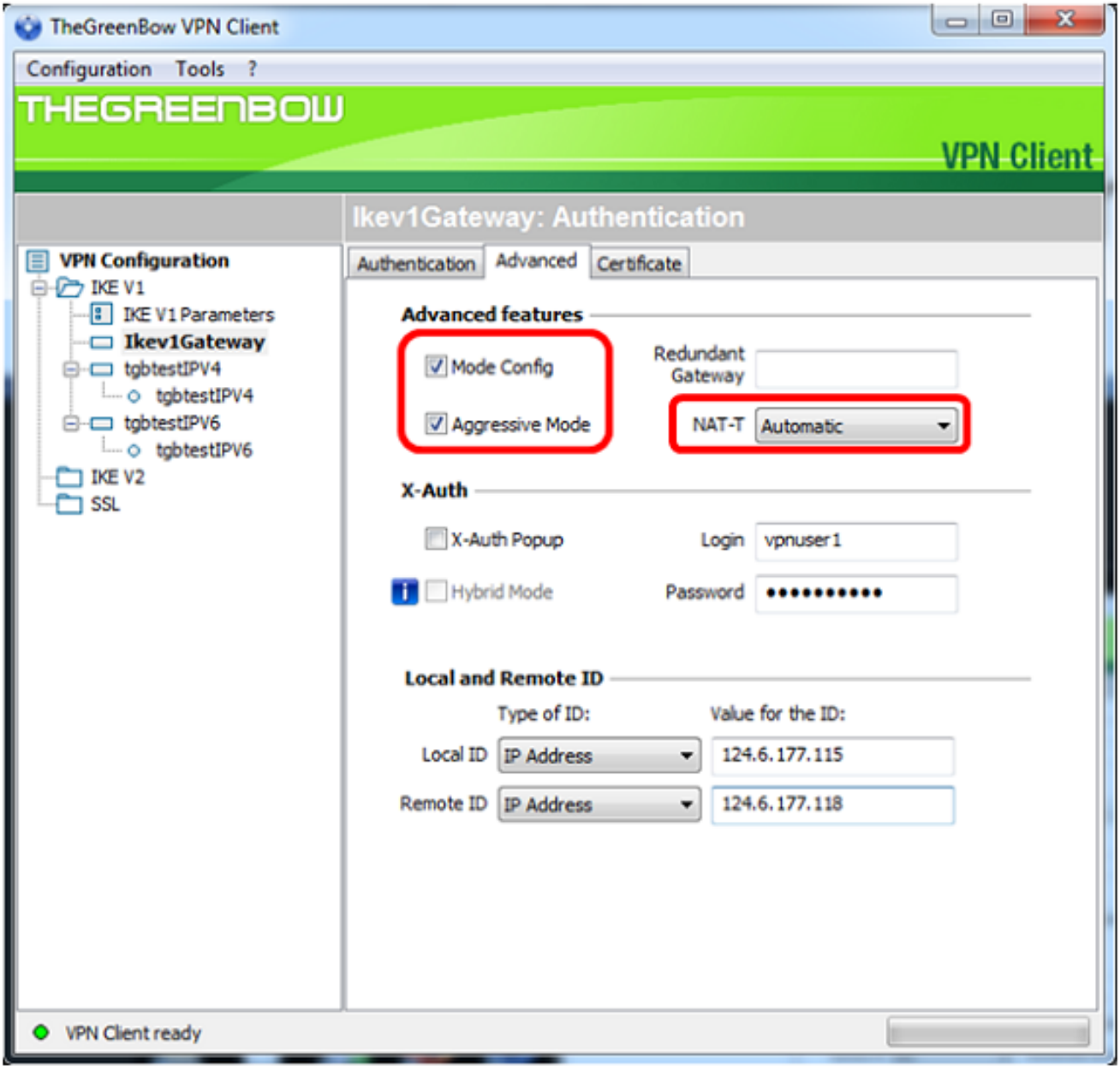
ステップ8:IKEの下で、ルータの設定と一致するように[Encryption]、[Authentication]、および[Key Group]の設定を設定します。



ステップ9:[Advanced]タブをクリックします。

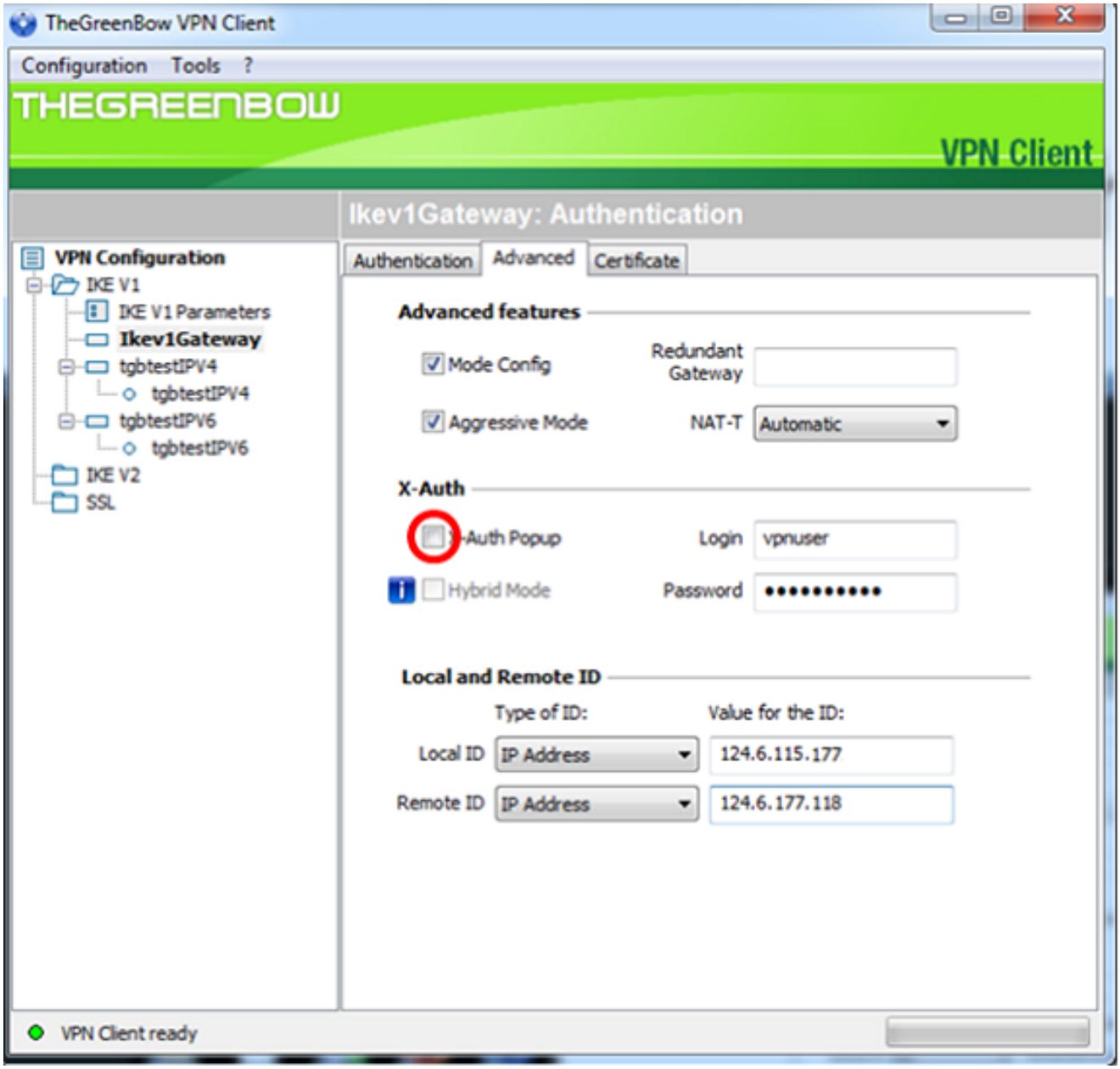


ステップ10:（オプション）[拡張機能(Advanced features)]で、[モードの設定(Mode Config)]チェックボックスと[アグレッシブモード(Aggressive Mode)]チェックボックスをオンにし、NAT-Tの設定を[自動(Automatic)]に設定します。



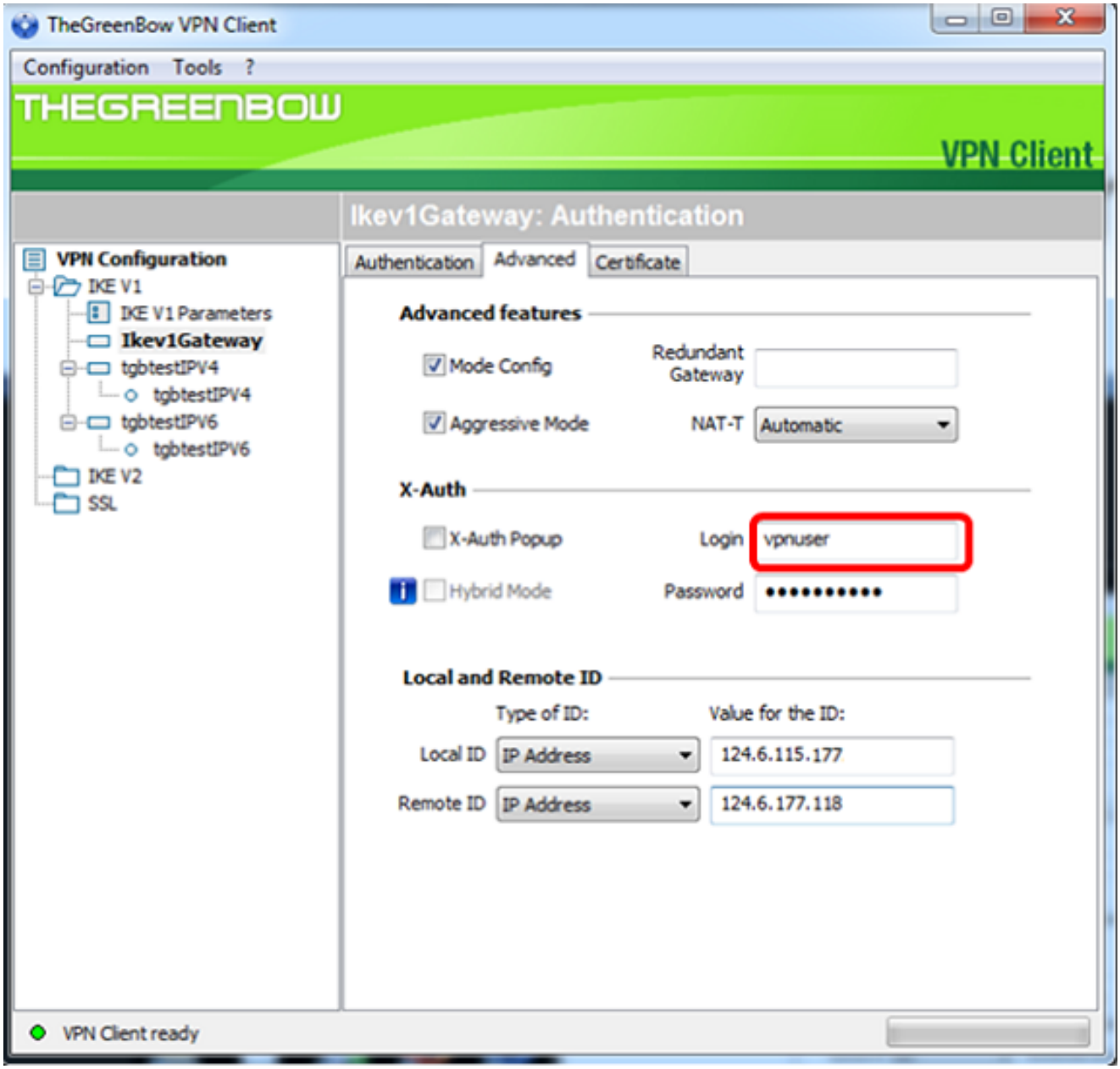
注：Mode Configを有効にすると、GreenBow VPN ClientはVPNゲートウェイから設定を引き出してトンネルの確立を試みると同時に、アグレッシブモードとNAT-Tを有効にすると接続の確立が高速になります。

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。

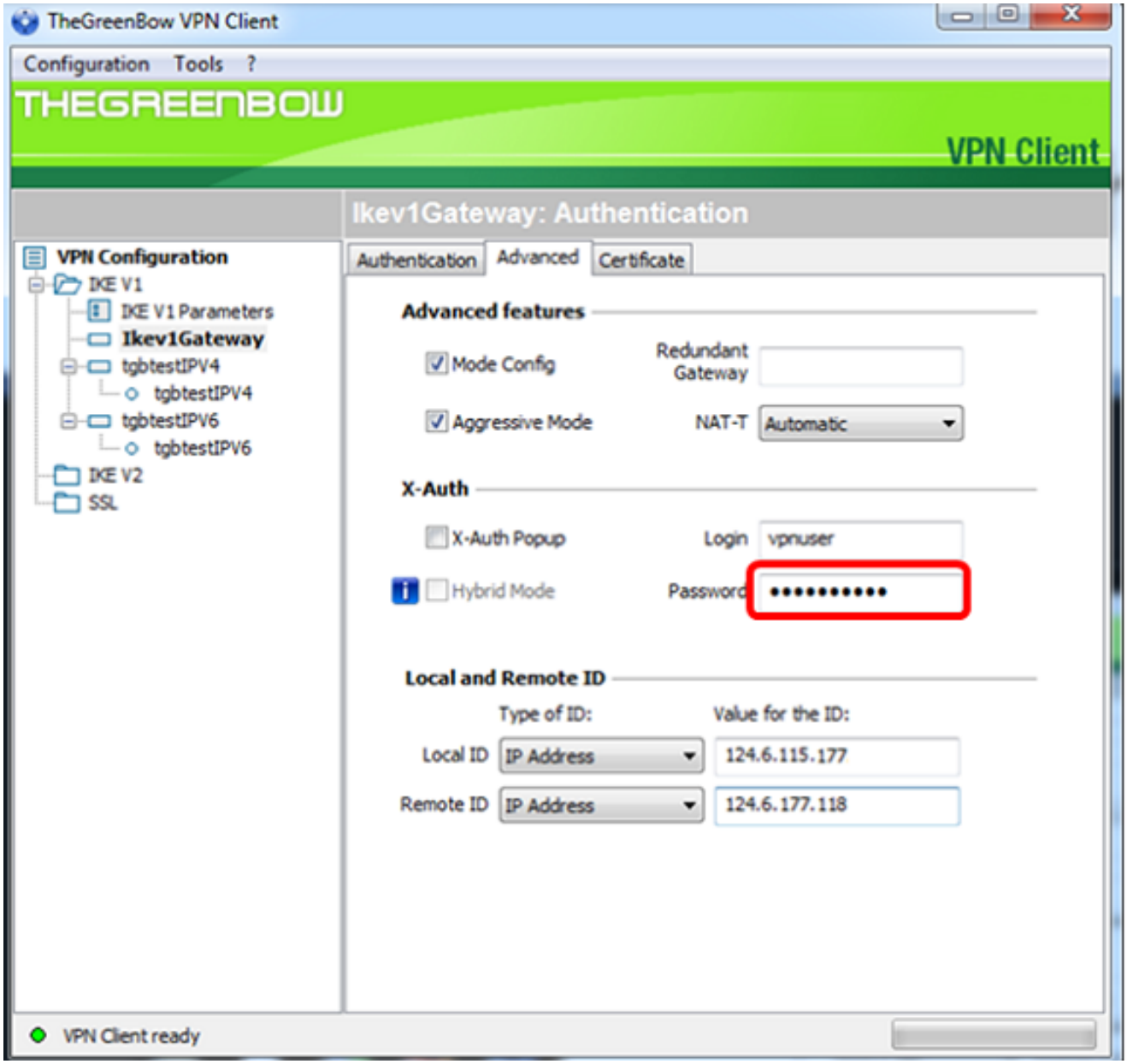


注：この例では、[X-Auth Popup]はオンになっていません。

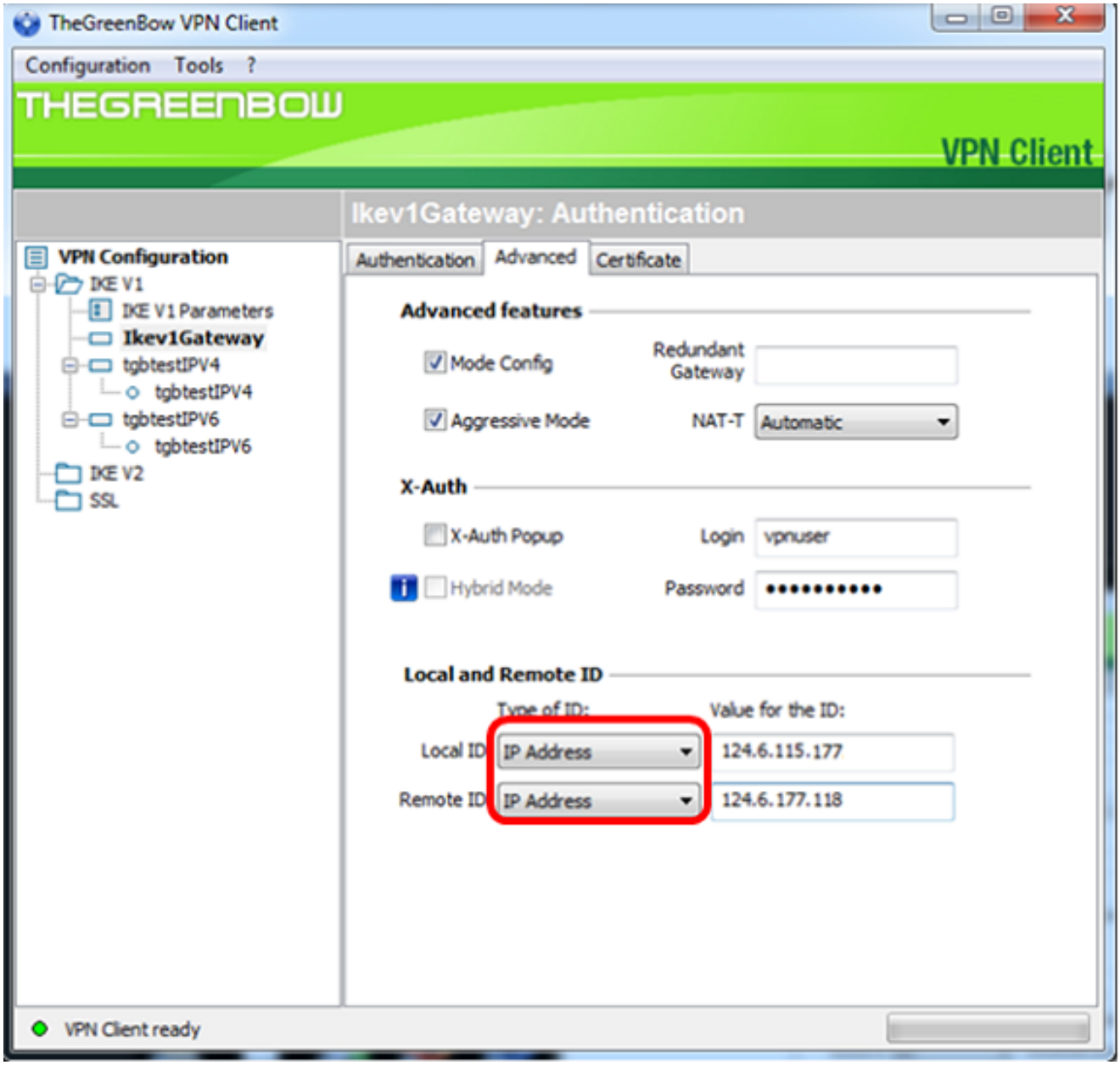
ステップ12:[ログイン]フィールドにユーザ名を入力します。これは、VPNゲートウェイでユーザグループを作成するために設定されたユーザ名です。



ステップ13:[Password]フィールドにパスワードを入力します。

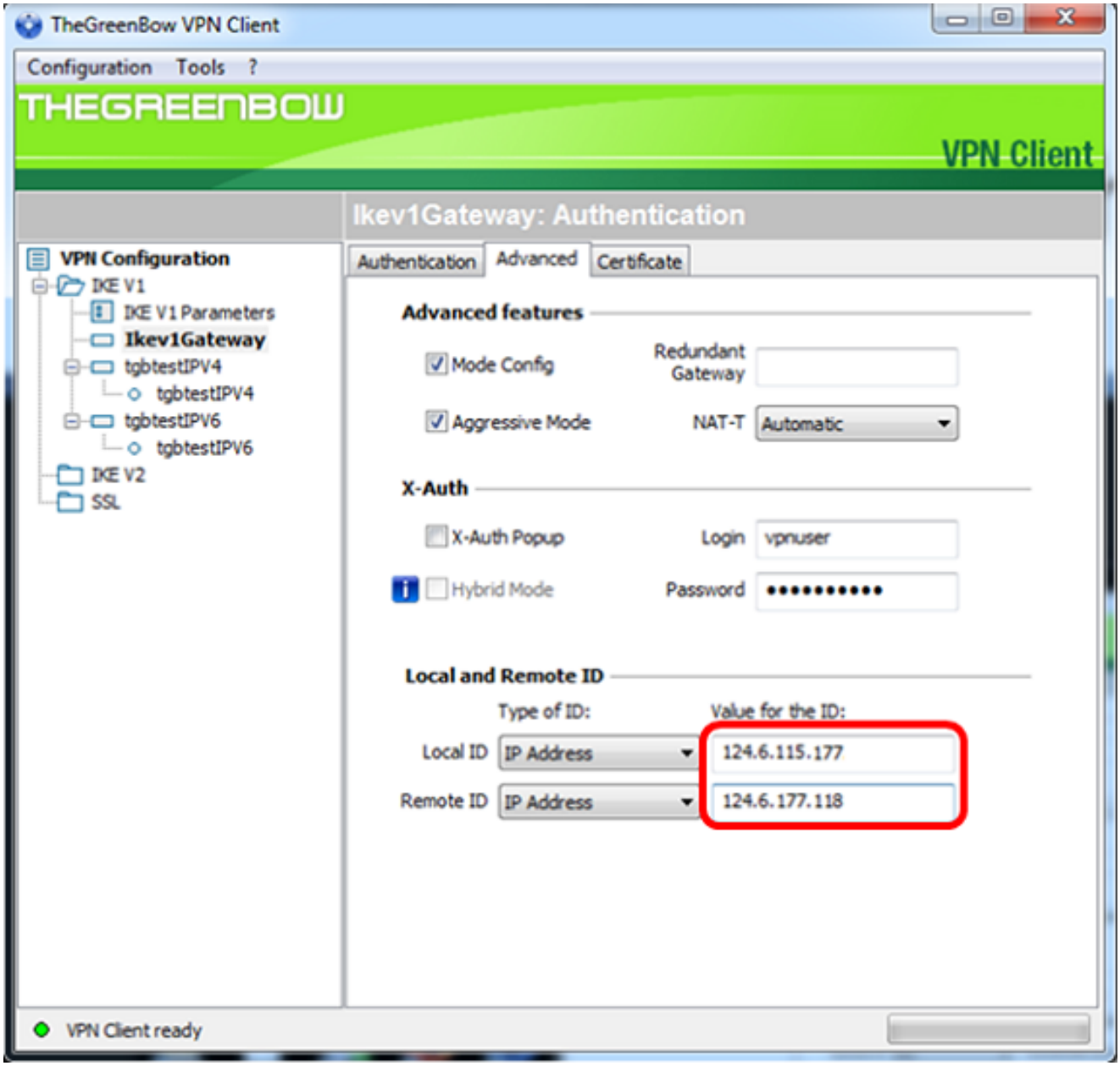


ステップ14:[Local and Remote ID]で、ローカルIDとリモートIDをVPNゲートウェイの設定と一致するように設定します。

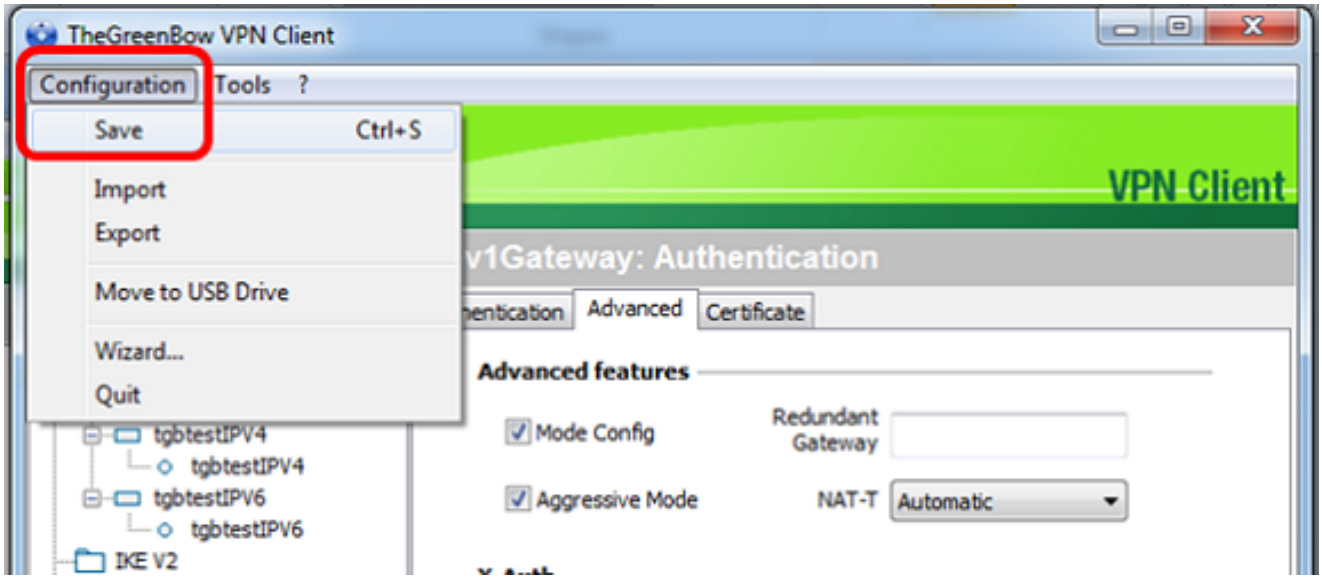


注：この例では、ローカルIDとリモートIDの両方がIPアドレスに設定され、RV34x VPNゲートウェイの設定と一致します。

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。

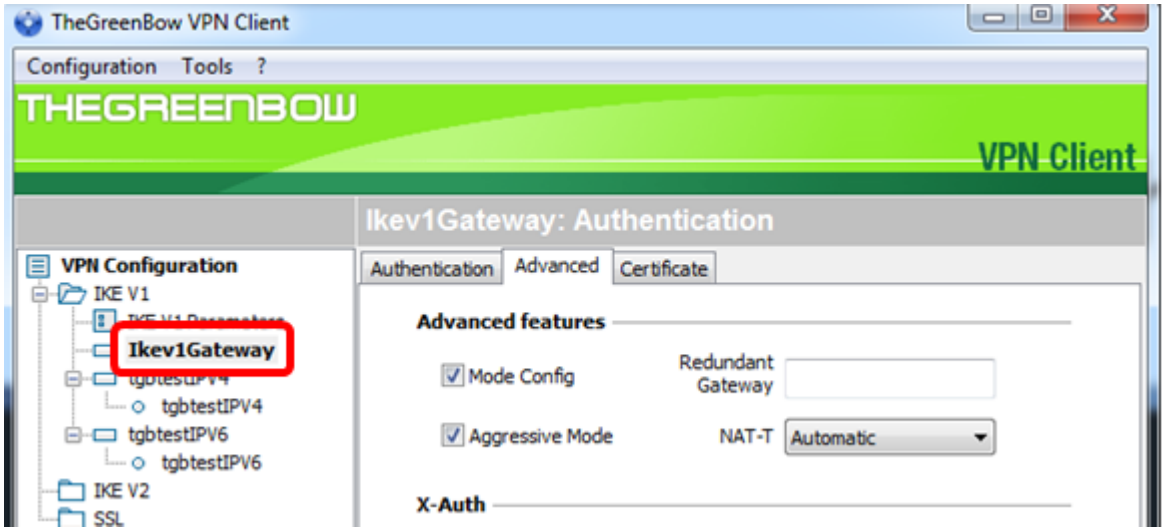


ステップ16:[Configuration] > [Save]をクリックして、設定を保存します。

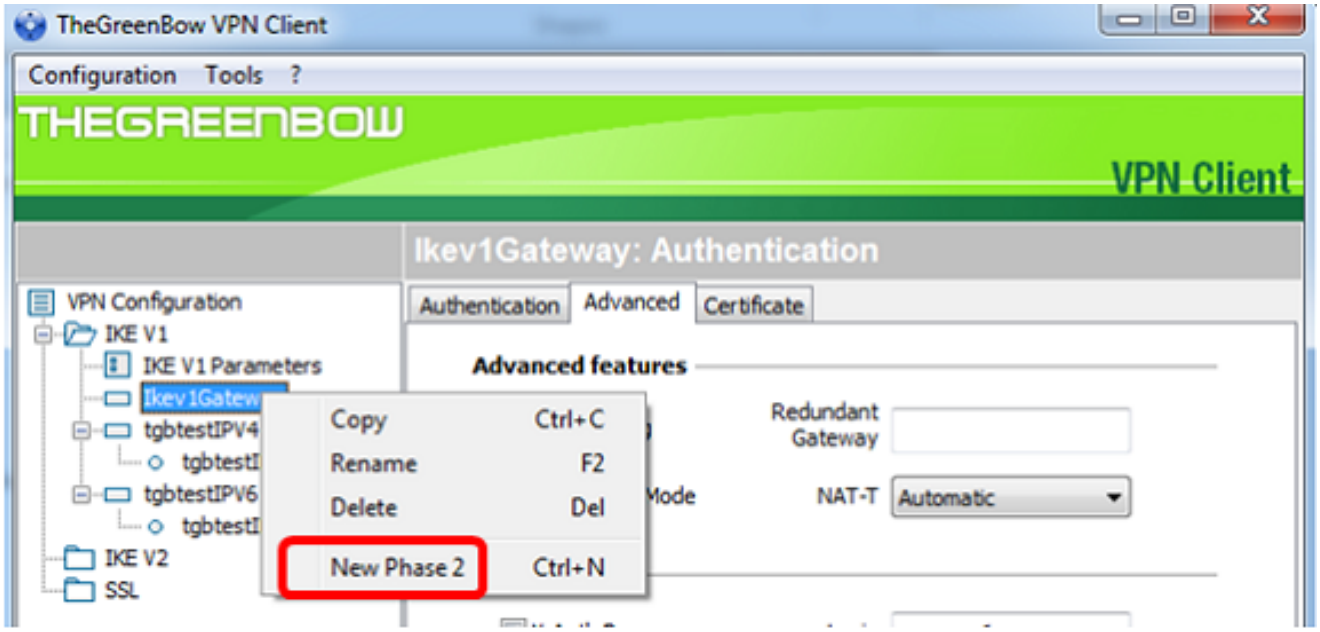


フェーズ2の設定

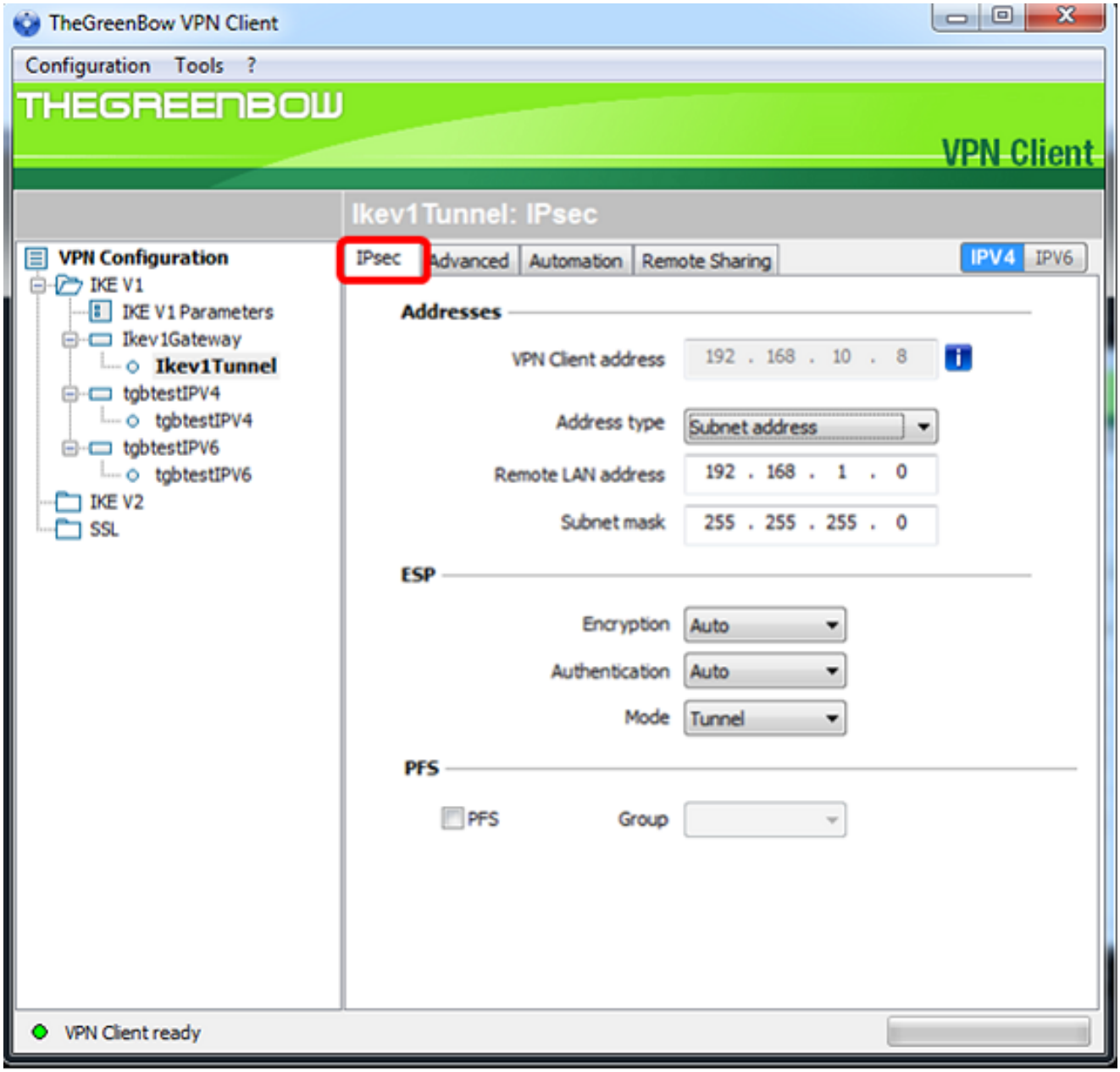
ステップ1:[Ikev1 Gateway]を右クリックします。



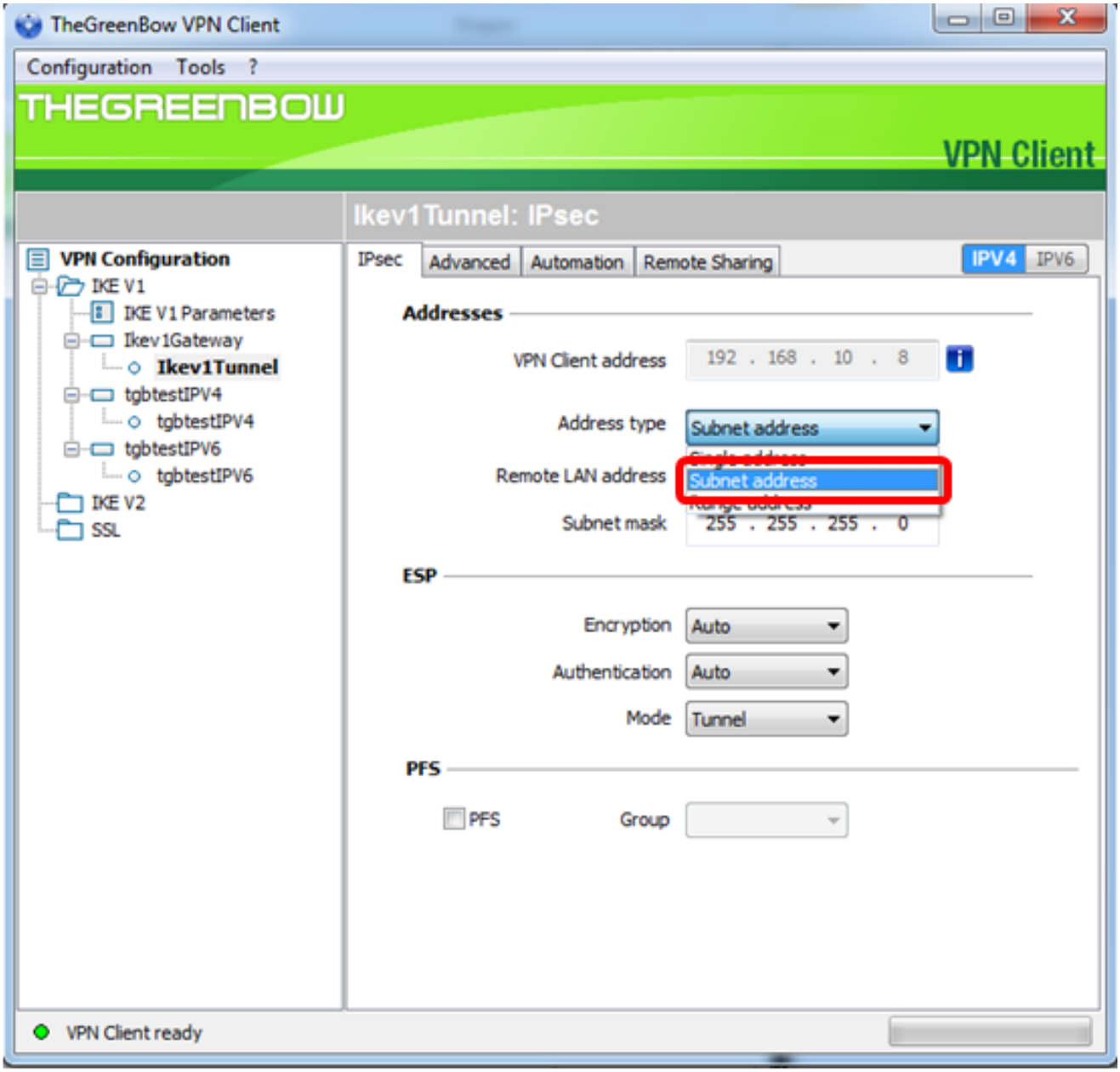
ステップ2:[New Phase 2]を選択します。



ステップ3:[IPsec]タブをクリックします。

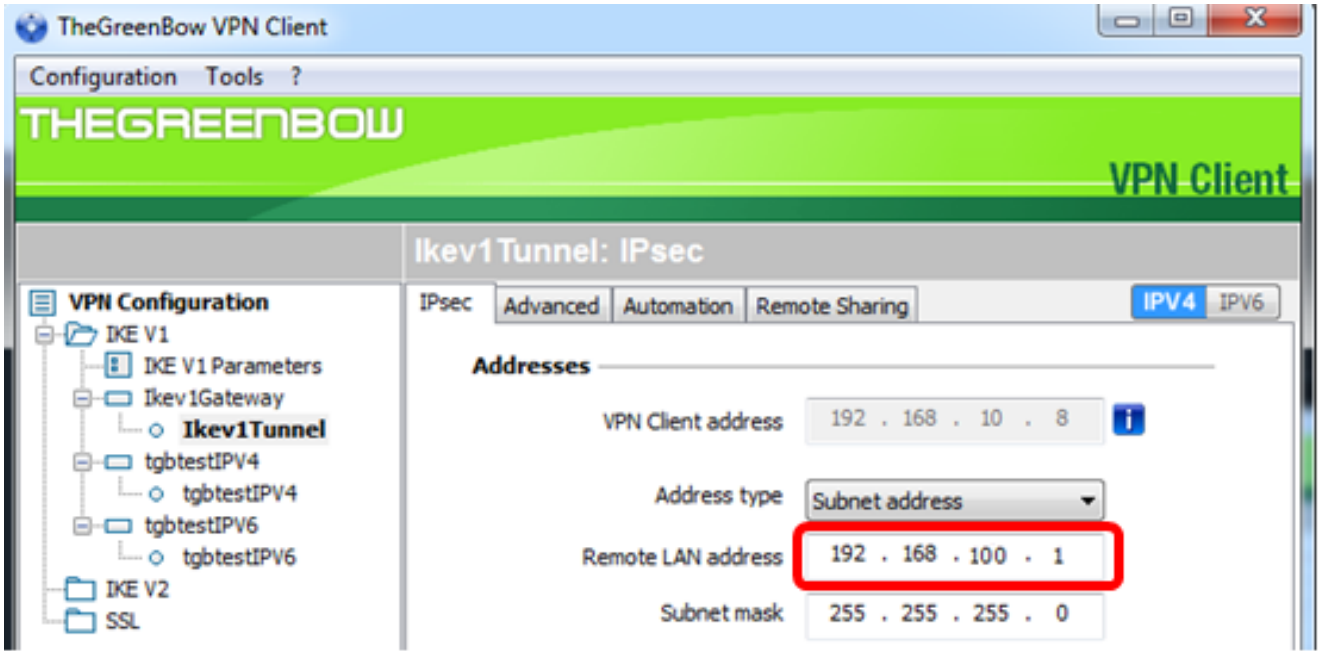


ステップ4:[Address type]ドロップダウンリストから、VPN Clientがアクセスできるアドレスタイプを選択します。



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。

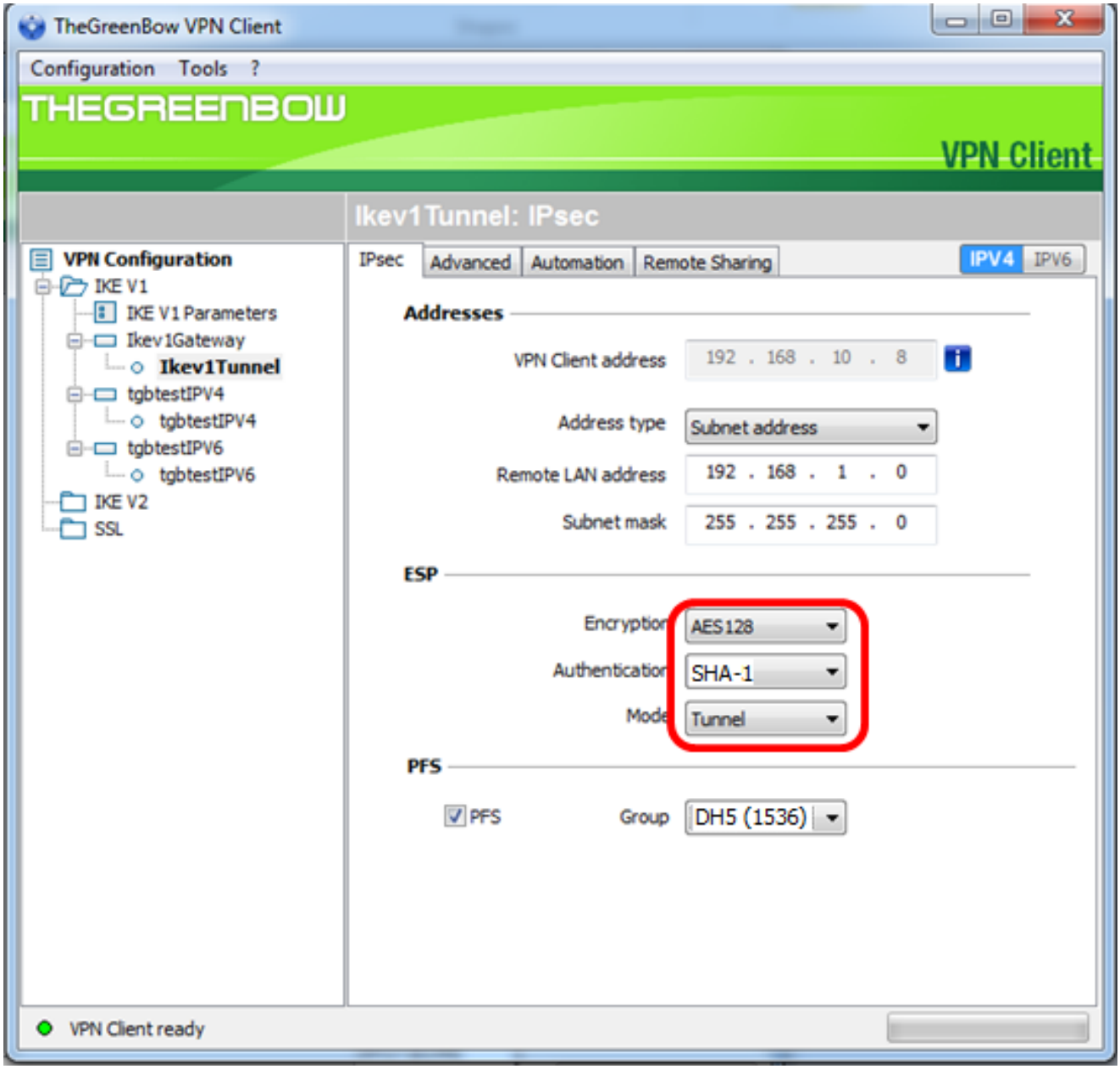


注：この例では、192.168.100.1と入力します。

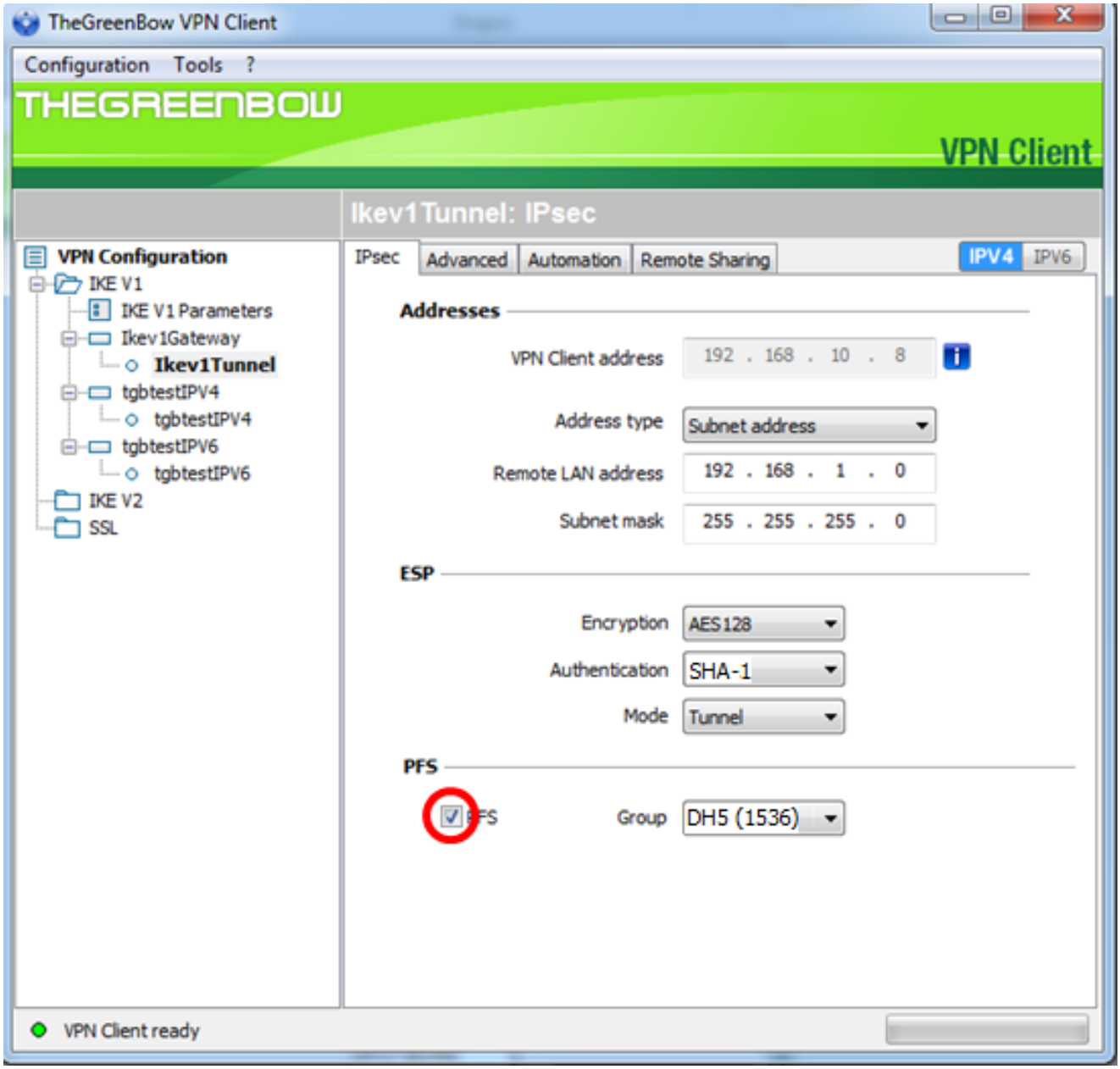
ステップ6:[Subnet mask]フィールドにリモートネットワークのサブネットマスクを入力します。

注：この例では、255.255.255.0と入力します。

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。

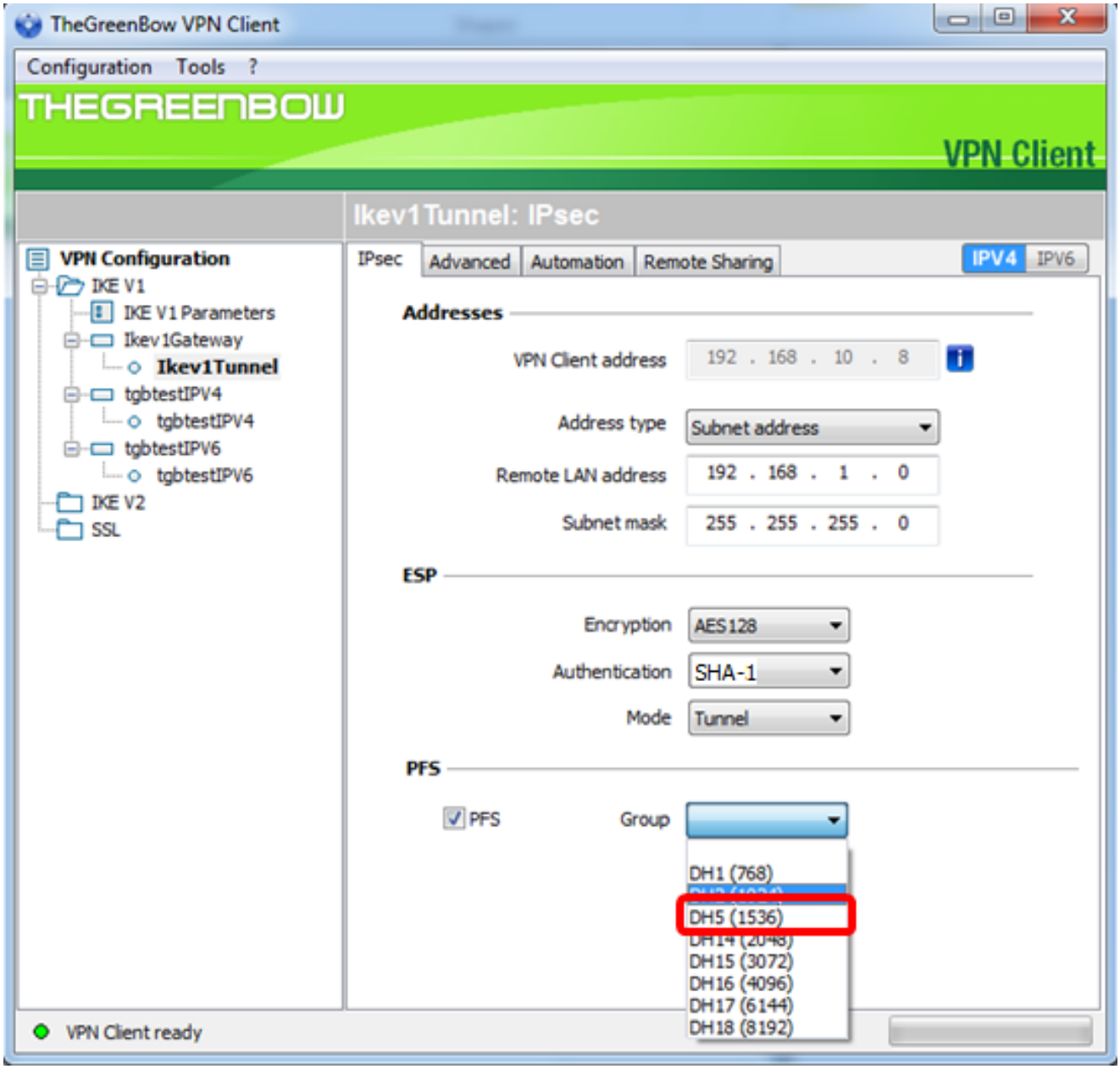


ステップ8: (オプション) PFSの下で、PFSチェックボックスをオンにして、Perfect Forward Secrecy(PFS)を有効にします。PFSは、セッションを暗号化するためのランダム・キーを生成します。

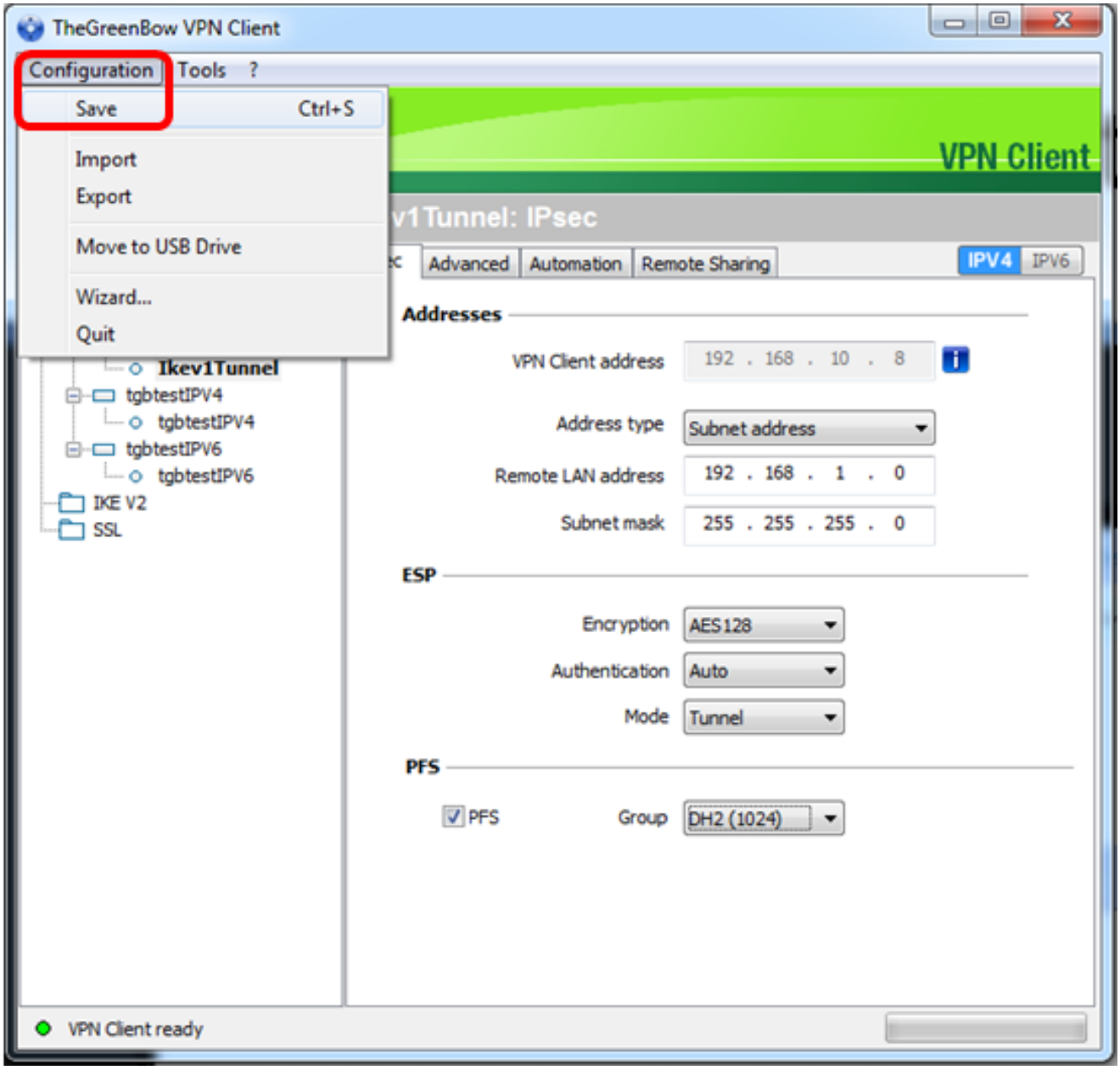


ステップ9:[Group]ドロップダウンリストからPFSグループ設定を選択します。

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。



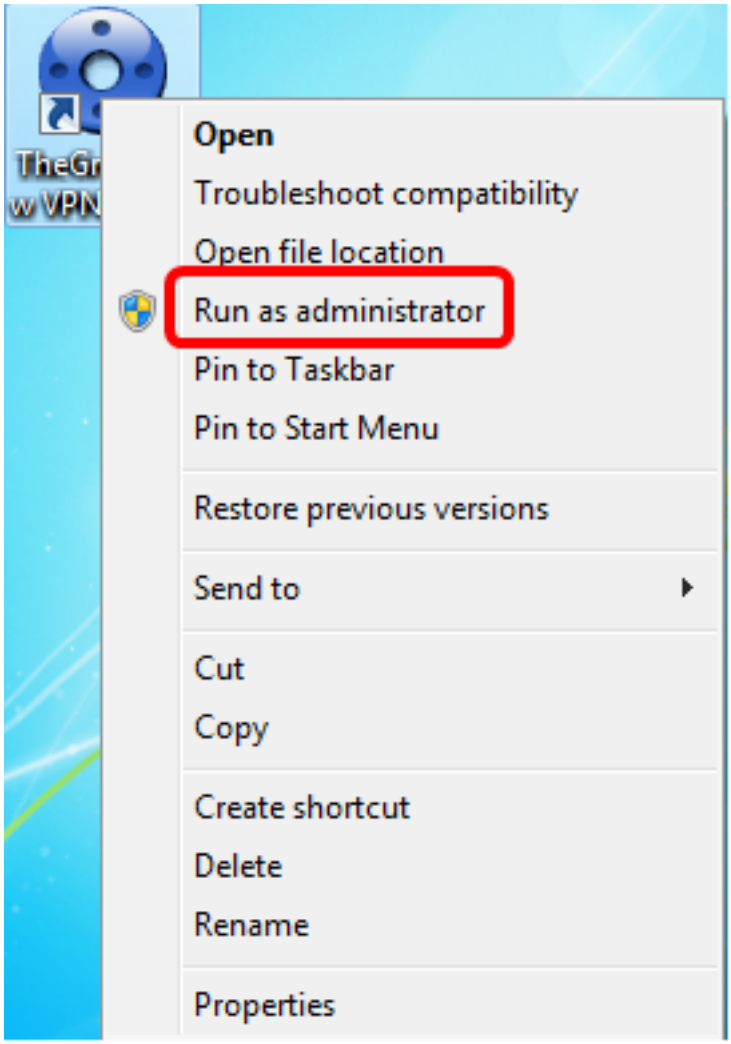
ステップ10:[Configuration]を右クリックし、[Save]を選択します。



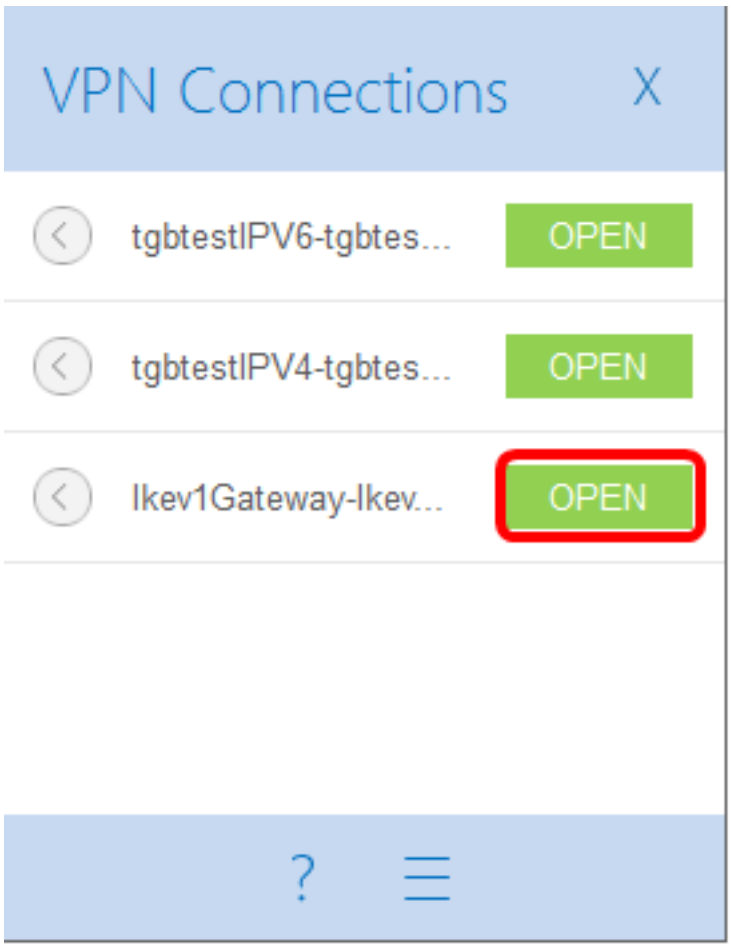
これで、VPNを介してRV34xシリーズルータに接続するようにTheGreenBow VPN Clientを正しく設定できました。

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。

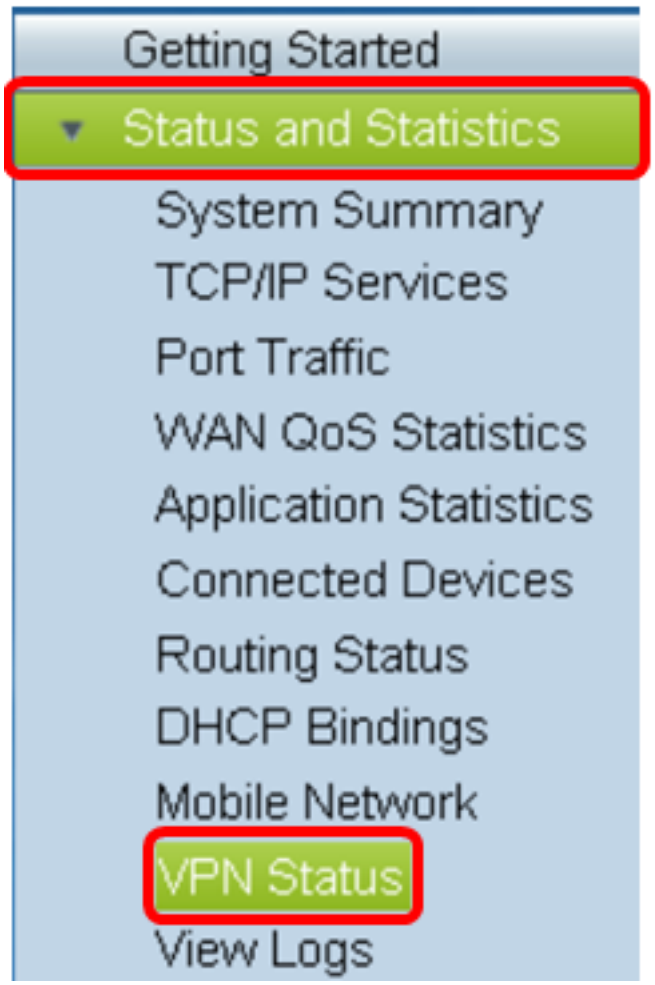


注：この例では、設定されたIkev1ゲートウェイが選択されています。

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。