RV160およびRV260ルータに接続するためのTheGreenBow IPsec VPN Clientのセットアップと使用

目的

このドキュメントの目的は、TheGreenBow IPsec VPN Clientを設定して使用し、RV160およびRV260ルータに接続することです。

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。企業オフィスでは、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ことが有用で必要であるため、VPN接続を使用することが多くあります。

VPNを使用すると、リモートホストまたはクライアントを、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。RV160ルータは最大10個のVPNトンネルをサポートし、RV260は最大20個のVPNトンネルをサポートします。ルータとエンドポイントの間にVPN接続を設定するには、ルータをインターネット接続に設定します。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。設定が完全に一致している必要があります。一致していないと通信できません。

GreenBow VPN Clientは、ホストデバイスがRV160およびRV260シリーズルータとのクライアント間IPsecトンネル用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。

VPN接続を使用する利点

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、物理的に存在する必要なく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。高度な暗号化アルゴリズムを使用すると、プライベートネットワークを不正アクセスから保護できます。

ユーザの実際の地理的位置は保護され、インターネットなどのパブリックネットワークや共有ネットワークには公開されません。

VPNを使用すると、追加のコンポーネントや複雑な設定を必要とせずに、新しいユーザやユーザグループを追加できます。

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がある可能性があります。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。

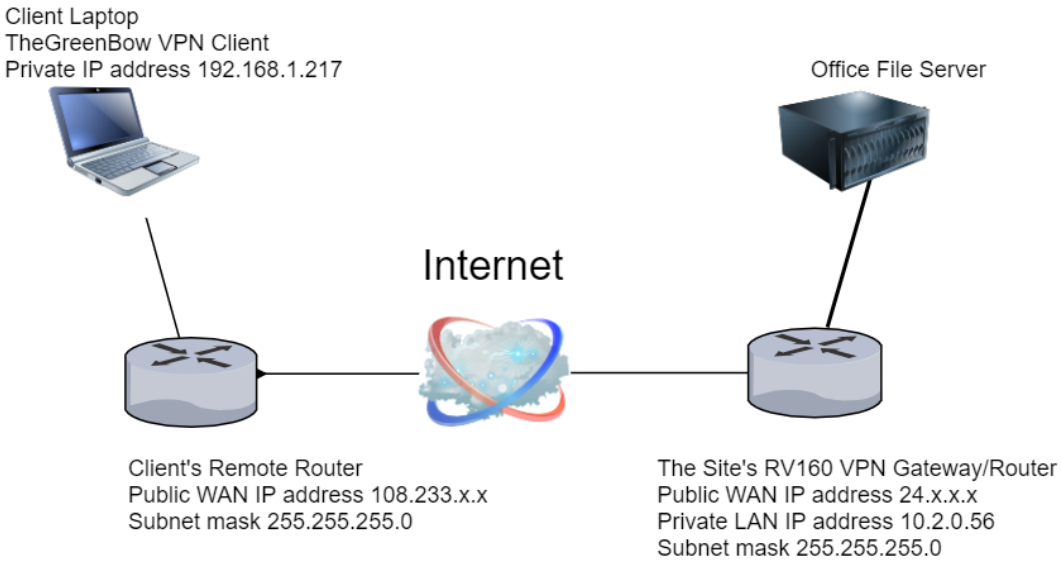
信頼性が低いかもしれません。VPN接続にはインターネット接続が必要であるため、優れたインターネットサービスを提供し、ダウンタイムを最小限に抑えて保証するために、実績とテスト済みのレピュテーションを持つプロバイダーが重要です。

新しいインフラストラクチャまたは新しい構成セットを追加する必要がある状況が発生した場合、特に使用中の製品以外やベンダーが関係する場合は、互換性がないために技術的な問題が発生する可能性があります。

接続速度が遅くなる可能性があります。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。この記事では、この問題を解消する有料のサードパーティを使用します。

クライアントとサイト間ネットワークの基本的なトポロジ

これは、セットアップ用のネットワークの基本的なレイアウトです。パブリックWAN IPアドレスが部分的にぼやけているか、実際の番号の代わりに**xが表示され**、このネットワークを攻撃から保護しています。



この記事では、RV160またはRV260ルータをサイトで設定するために必要な手順について説明します。

- ユーザグループ – **VPNUsers**
- クライアントとしてアクセスを許可されるユーザアカウント（1人以上のユーザ）
- IPsecプロファイル：**TheGreenBow**
- クライアントからサイトへのプロファイル：クライ**アント**
- また、クライアントが接続された後、サイトでVPNステータスを表示する方法も示されます

注：ユーザグループ、IPsecプロファイル、およびクライアントとサイト間プロファイルには、任意の名前を使用できます。リストされている名前は単なる例です。

この記事では、各クライアントがコンピュータでTheGreenBow VPNを設定するために実行する手順についても説明します。

- TheGreenBow VPN Clientソフトウェアのダウンロードとセットアップ
- クライアントのフェーズ1および2の設定の設定
- クライアントとしてのVPN接続の開始と確認

サイト上のルータのすべての設定がクライアントの設定と一致していることが重要です。設定が成功してもVPN接続が確立しない場合は、すべての設定をチェックして一致していることを確認します。この記事に示す例は、接続を設定する方法の1つにすぎません。

目次

該当するデバイス

- RV160
- RV260

[Software Version]

- 1.0.00.15

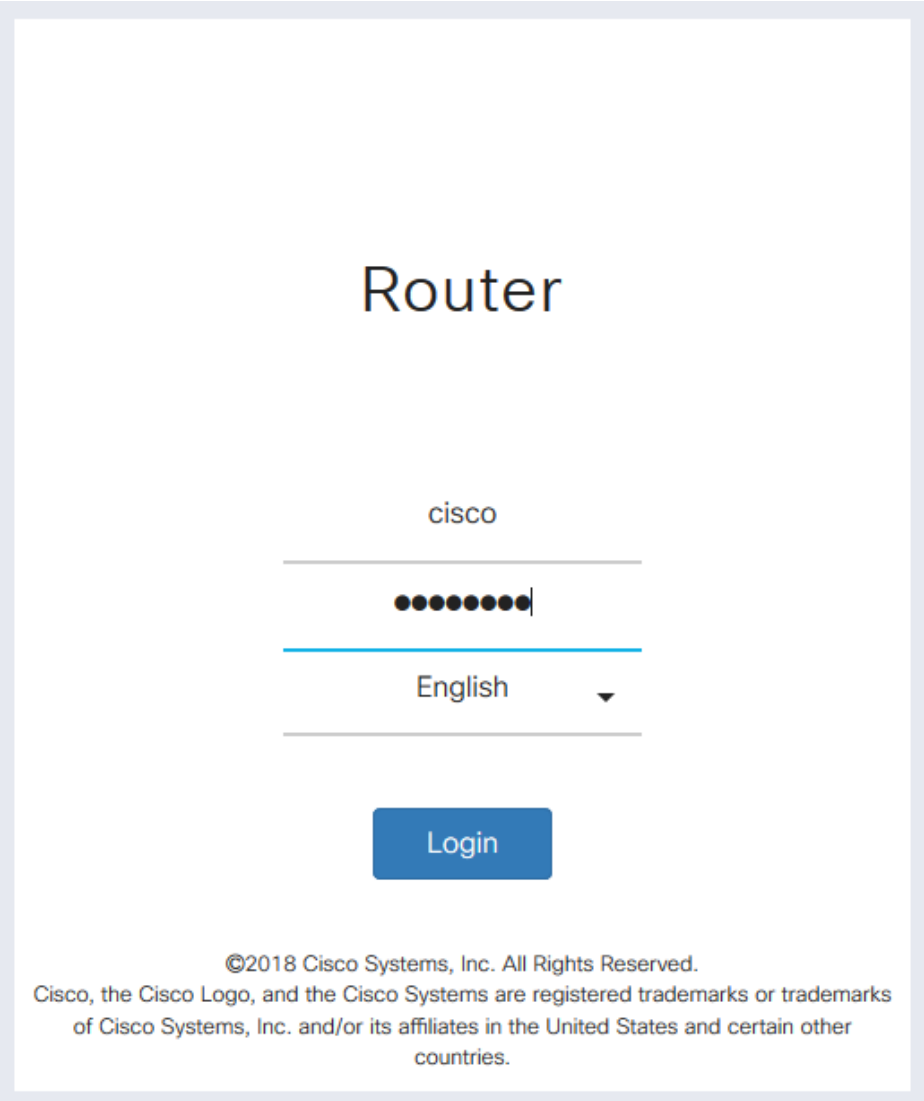
RV160またはRV260ルータのサイトでのVPN Clientの設定

ユーザグループの作成

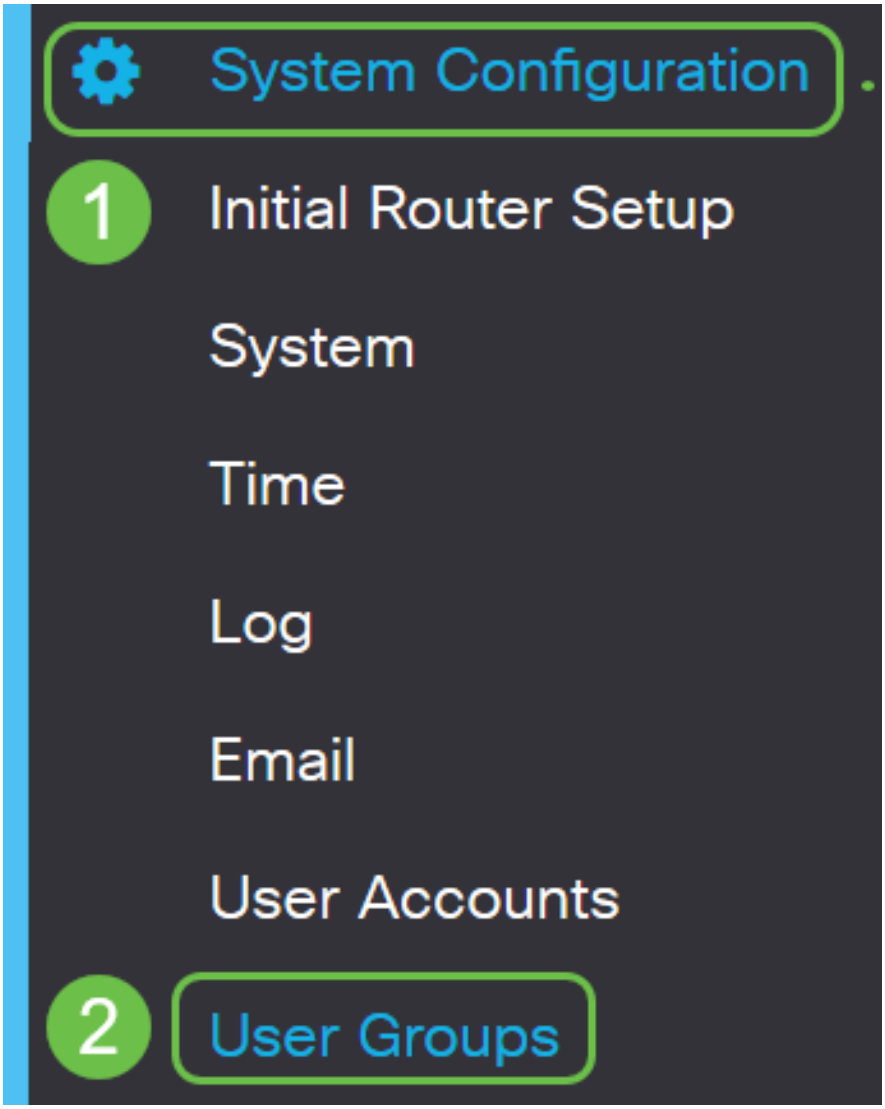
特記事項：管理者グループにデフォルトの管理者アカウントを残し、TheGreenBowの新しいユー

ザアカウントとユーザグループを作成してください。管理者アカウントを別のグループに移動すると、ルータにログインできなくなります。

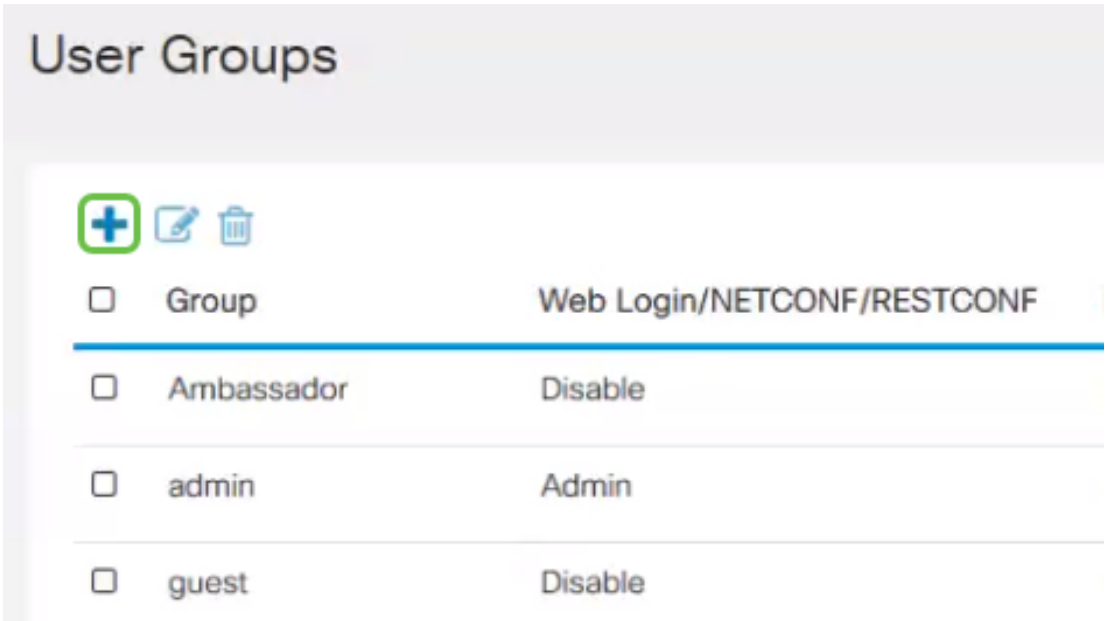
ステップ1：ルータのWebベースユーティリティにログインします。



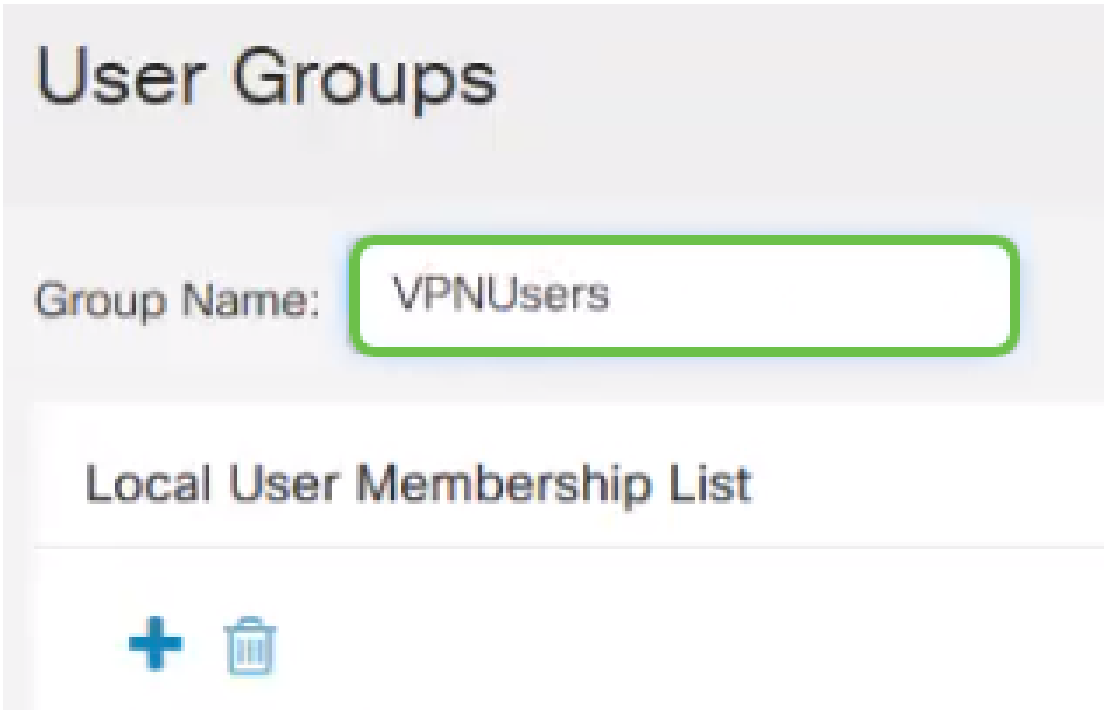
ステップ2:[System Configuration] > [**User Groups**]を選択**します。**



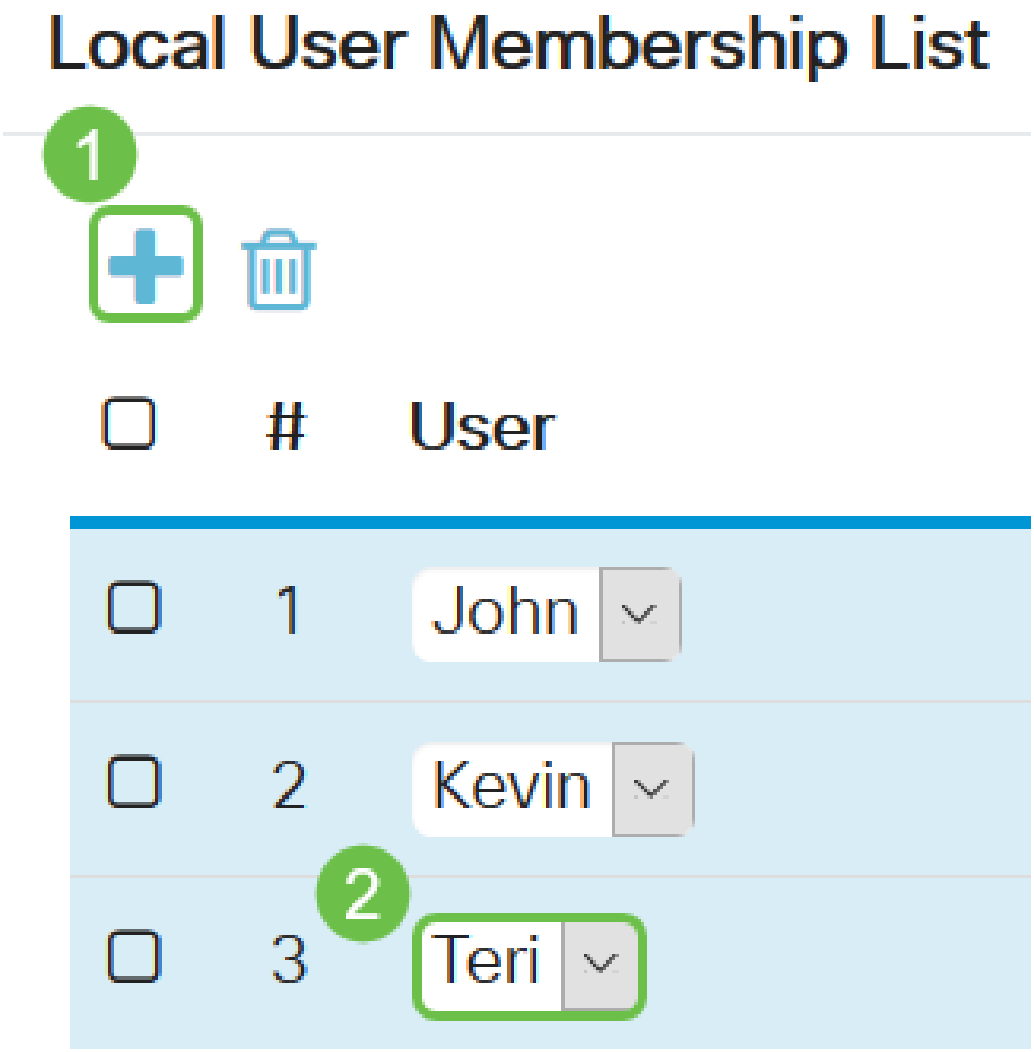
ステップ3:[+]アイコンを**クリック**して、ユーザグループを追加します。



ステップ4:[Overview（概要）]領域の[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。

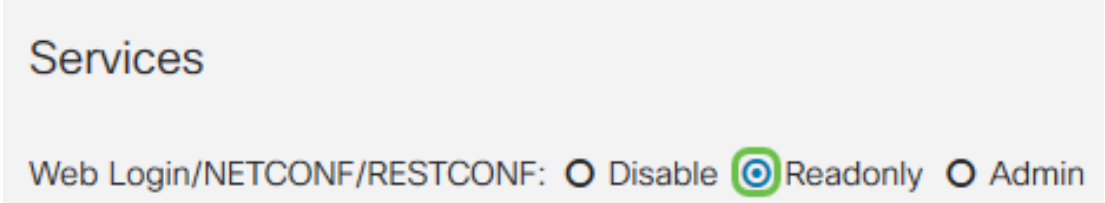


ステップ5:[Local User Membership List]の下のプラス記号アイコンをクリックし、ドロップダウンリストからユーザを選択します。さらに追加する場合は、プラスのアイコンを**もう一度押**し、追加する別のメンバーを選択します。メンバーは1つのグループにのみ属することができます。すべてのユーザーを入力していない場合は、「ユーザーアカウントの作成」セクションで追加できます。

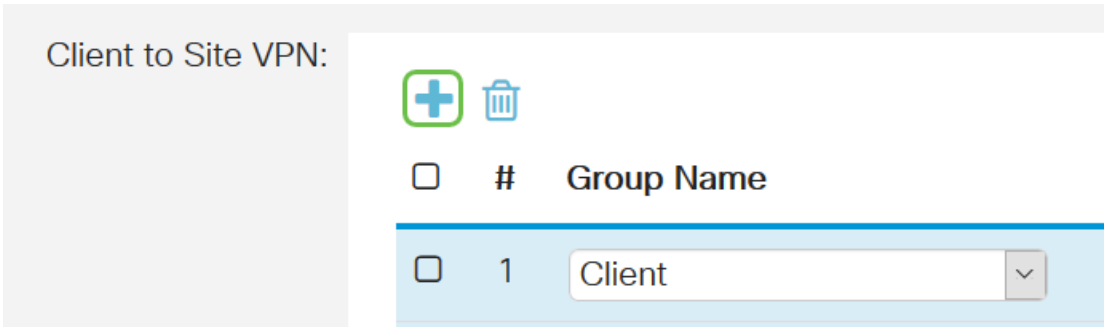


ステップ6:[Services] で、グループ内のユーザに付与する権限を選択します。次のオプションがあります。

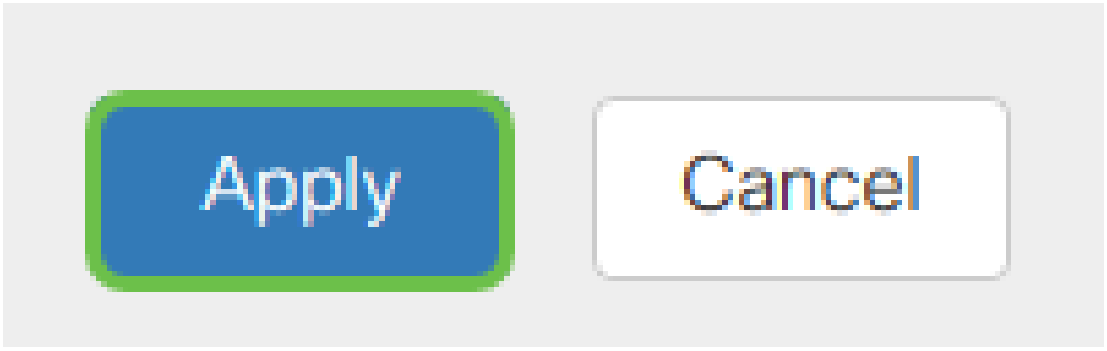
- [無効(Disabled)]：このオプションは、グループのメンバがブラウザを介してWebベースユーティリティにアクセスできないことを意味します。
- Readonly：このオプションは、グループのメンバーがログイン後にシステムのステータスを読み取ることができることを意味します。設定を編集することはできません。
- Admin：このオプションは、グループのメンバーに読み取り/書き込み権限を与え、システムステータスを設定できます。



ステップ7:[+]アイコンを**クリック**して、既存のクライアントからサイトへのVPNを追加します。この設定を行っていない場合は、この記事の「クライアントとサイト間のプロファイルの作成」の項に記載されています。

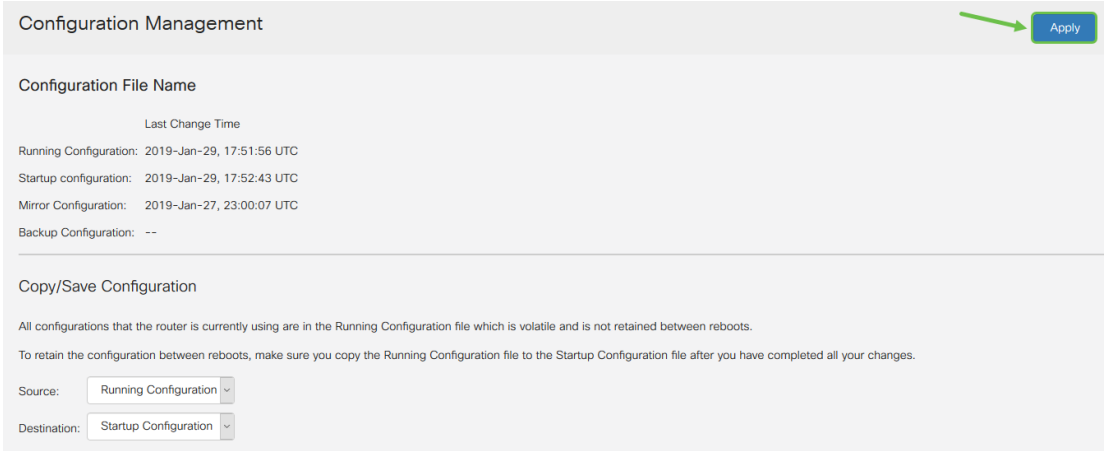


ステップ8:[Apply]をクリックします。



ステップ9:[Save]をクリックします。

ステップ10:[Apply]をもう一度クリックして、実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します。

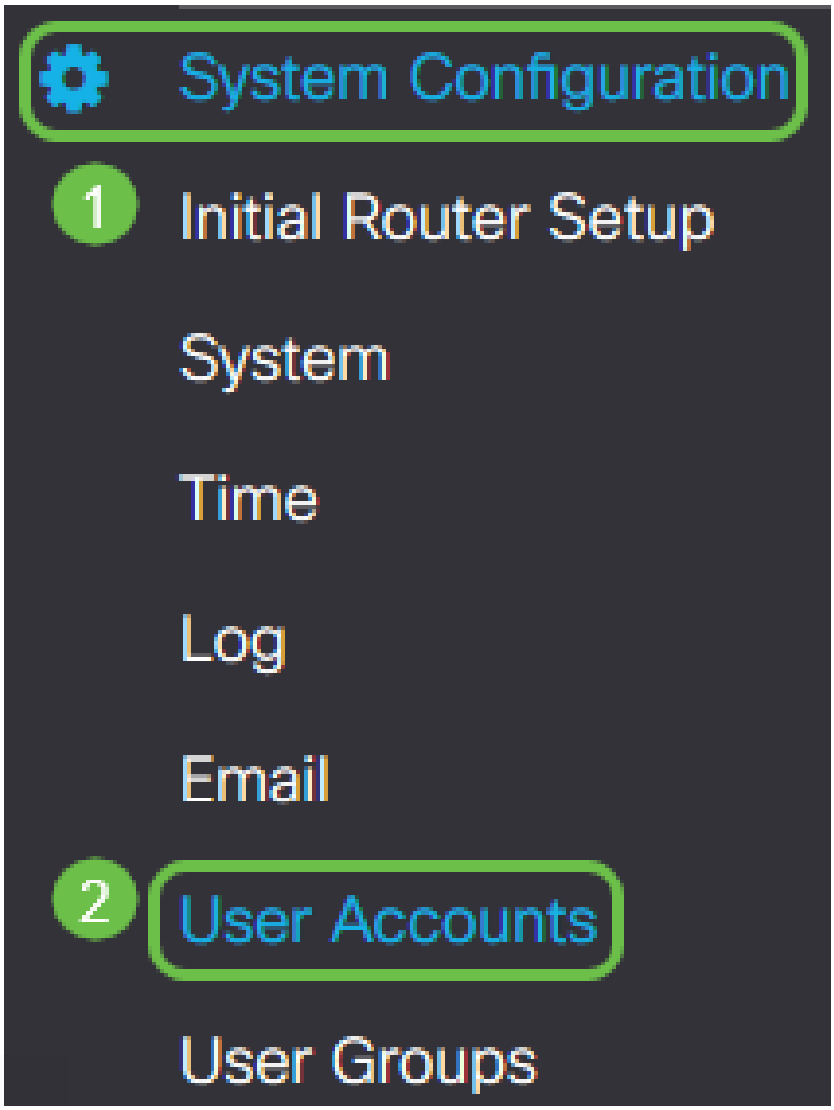


ステップ11：確認メッセージが表示されたら、[OK]をクリックします。

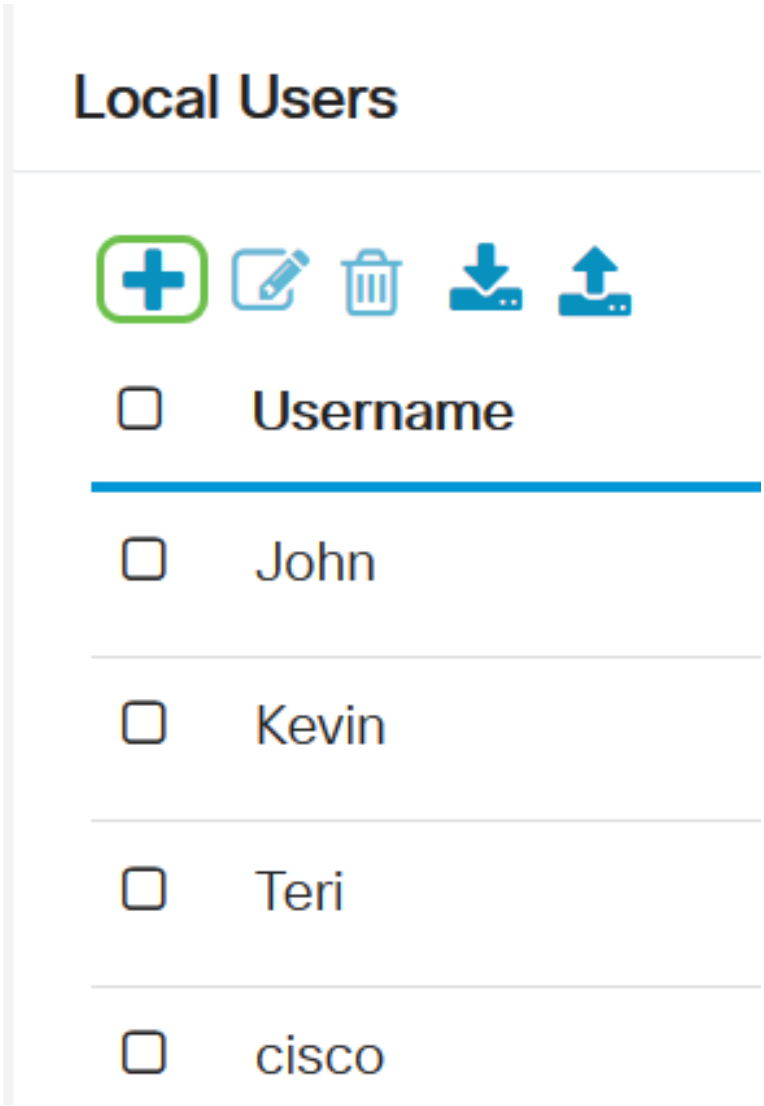
これで、RV160またはRV260シリーズルータにユーザグループが正常に作成されたはずです。

ユーザアカウントの作成

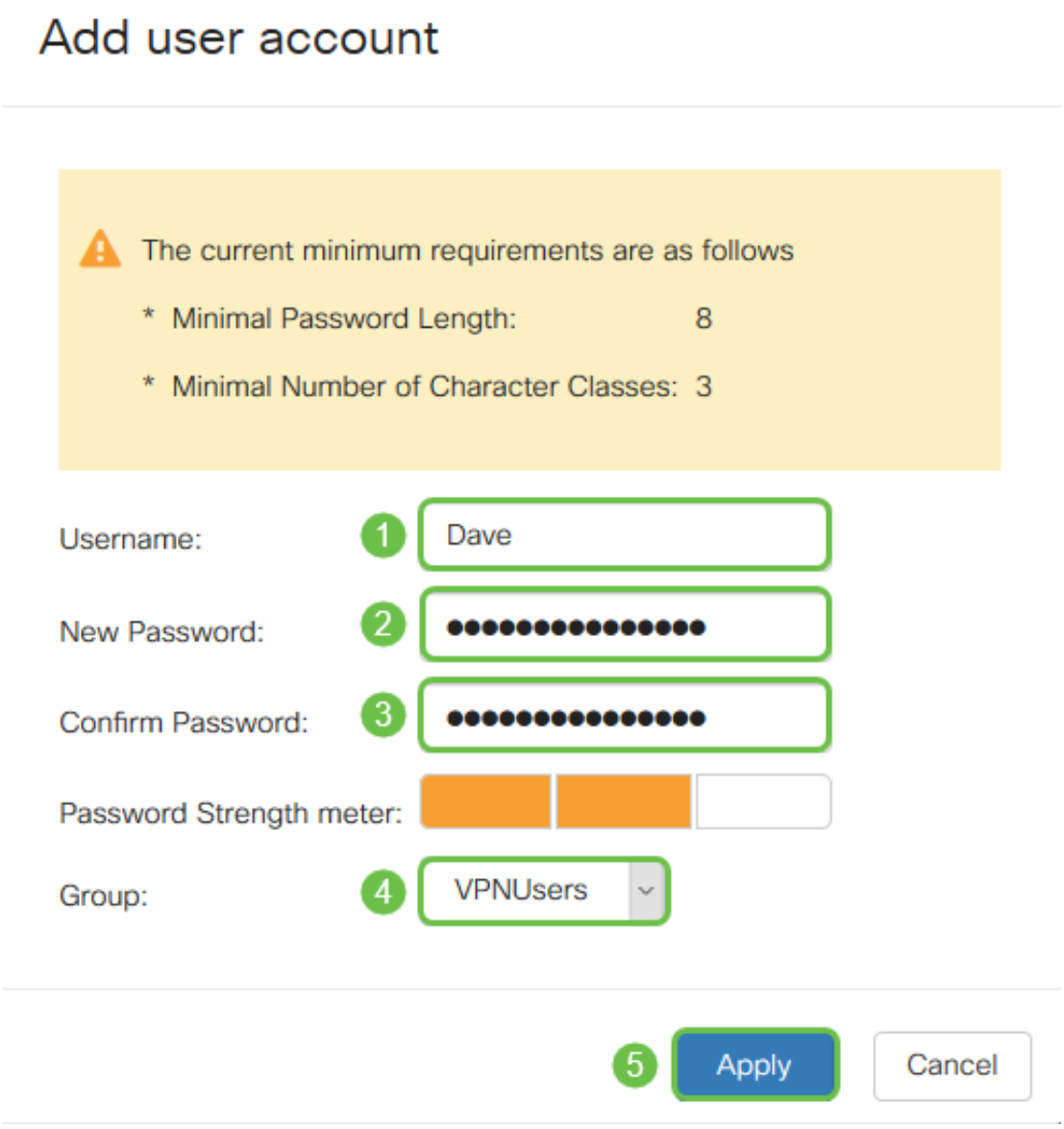
ステップ1：ルータのWebベースのユーティリティにログインし、[**System Configuration**] > [**User Accounts**]を選択します。



ステップ2:[ローカルユーザー*]領域*で、[追加]アイコン**をクリック**します。



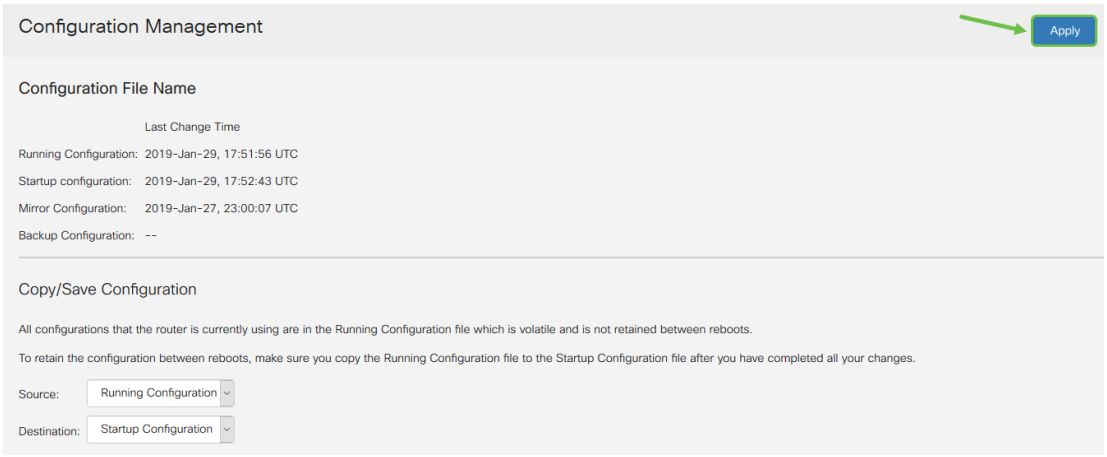
ステップ3:[Username]フィールドにユーザの名前、パスワード、およびドロップダウンメニューからユーザを追加するグループを入力します。[Apply] をクリックします。



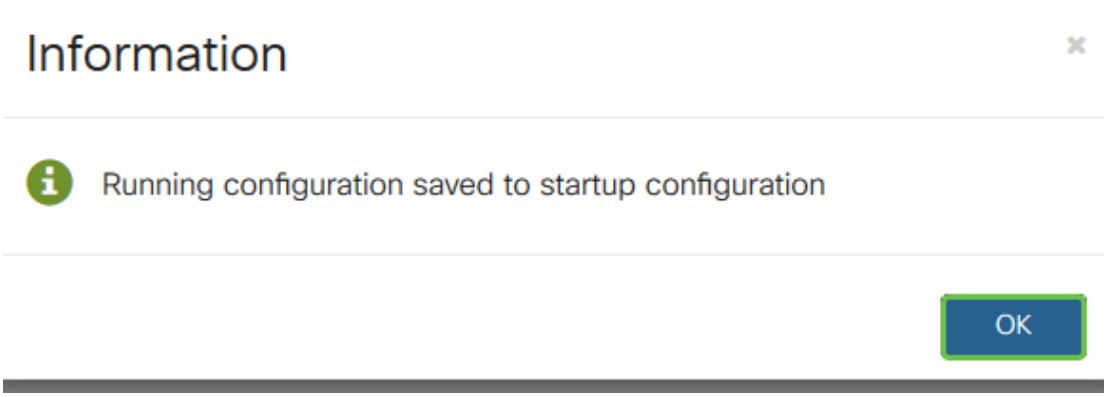
注：クライアントが自分のコンピュータにTheGreenBow Clientをセットアップすると、同じユーザ名とパスワードでログインします。

ステップ4:[Save]をクリックします。

ステップ5:[Apply]をもう一度クリックして、実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します。



ステップ6：確認メッセージが表示されたら、[OK]をクリックします。

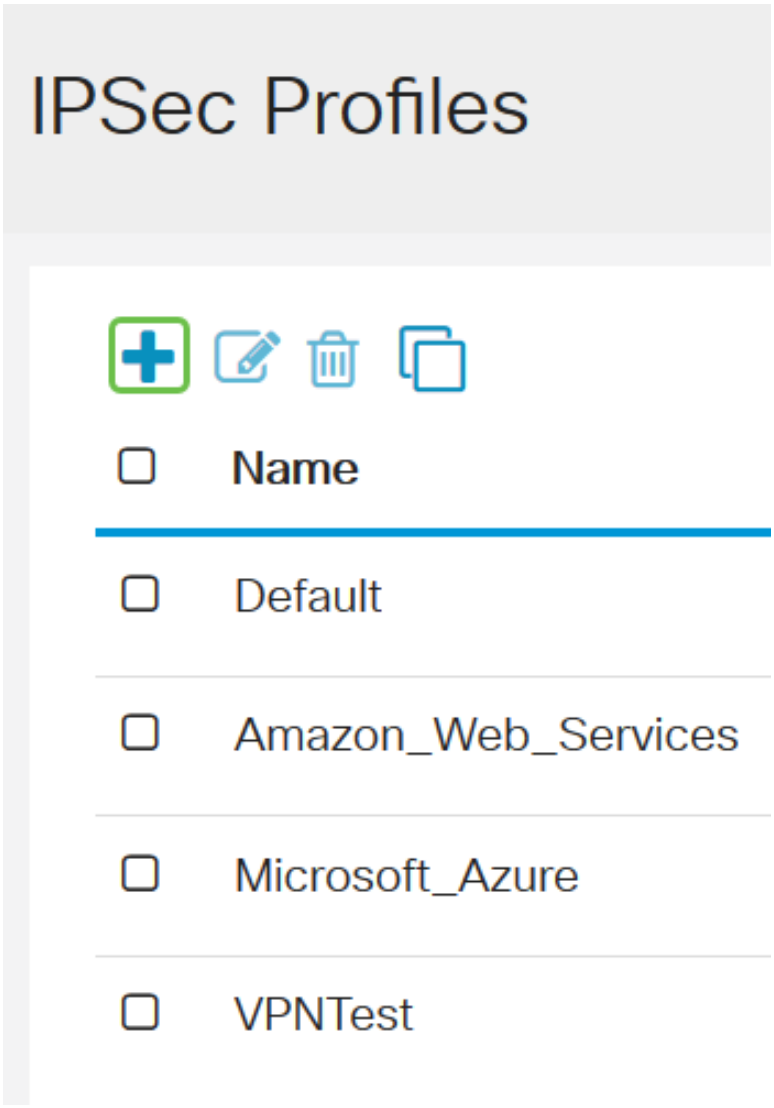


これで、RV160またはRV260ルータにユーザアカウントが作成されたはずです。

IPsecプロファイルの設定

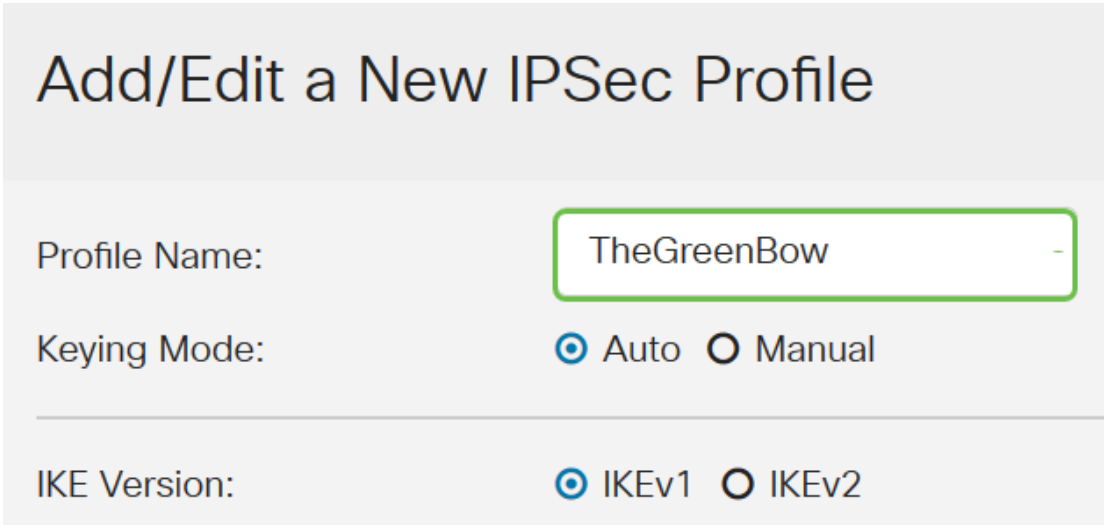
ステップ1:RV160またはRV260ルータのWebベースユーティリティにログインし、[VPN] > [IPSec VPN] > [IPSec Profiles] の順に選択します。

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。プラス(+)アイコンをクリックして、新しい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。

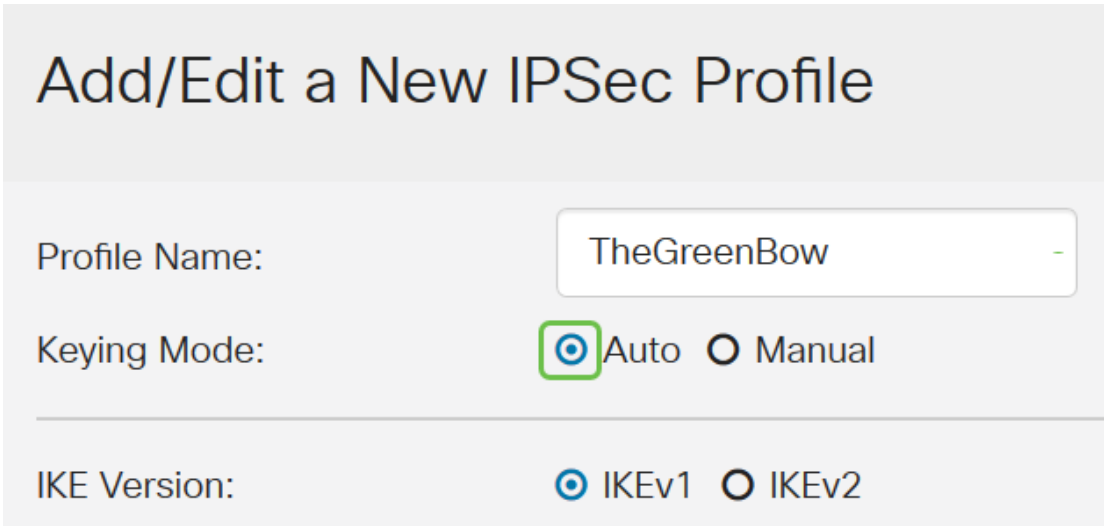
ステップ3:[Profile Name]フィールドにプロファイルの名前を*作成*します。プロファイル名には、英数字と特殊文字のアンダースコア(_)のみを使用してください。



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。

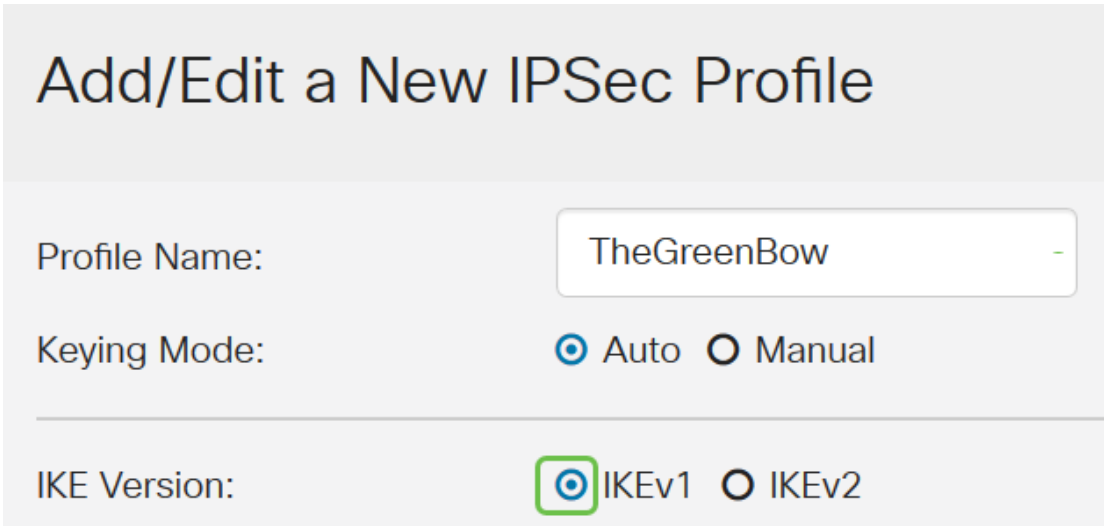
- Auto：ポリシーパラメータは自動的に設定されます。このオプションでは、データ整合性と暗号化キー交換にインターネットキー交換(IKE)ポリシーを使用します。これを選択すると、[Auto Policy Parameters]領域の設定が有効になります。

- [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。これは広く使われていない。



注：この例では、[Auto]が選択されています。

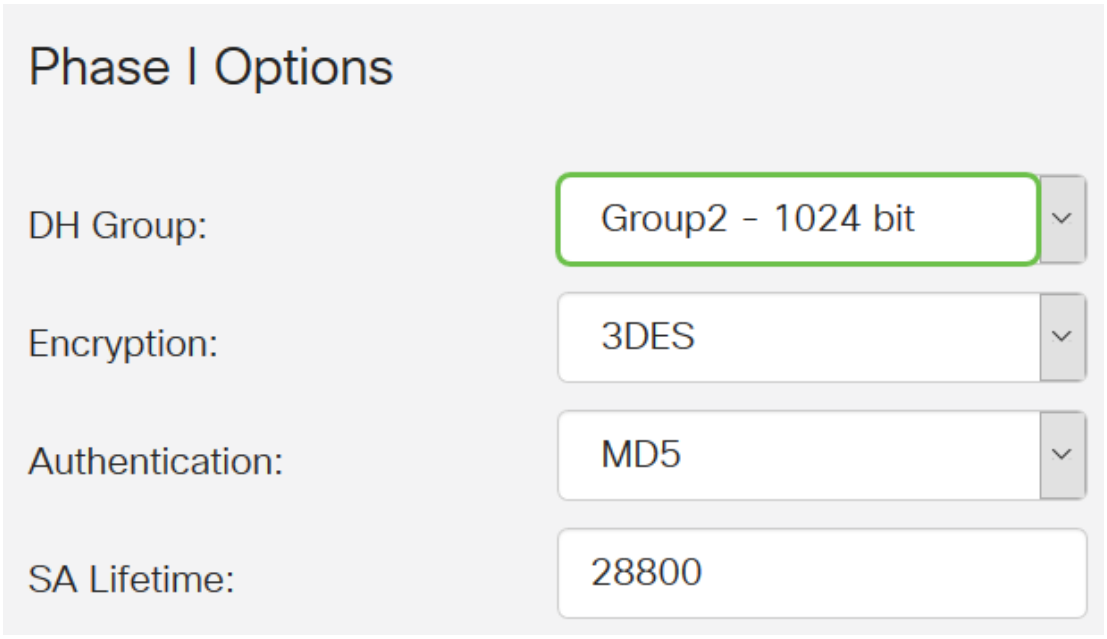
ステップ5:IKEバージョンを選択します。クライアント側でTheGreenBowを設定するときは、同じバージョンが選択されていることを確認してください。



フェーズ1および2の設定

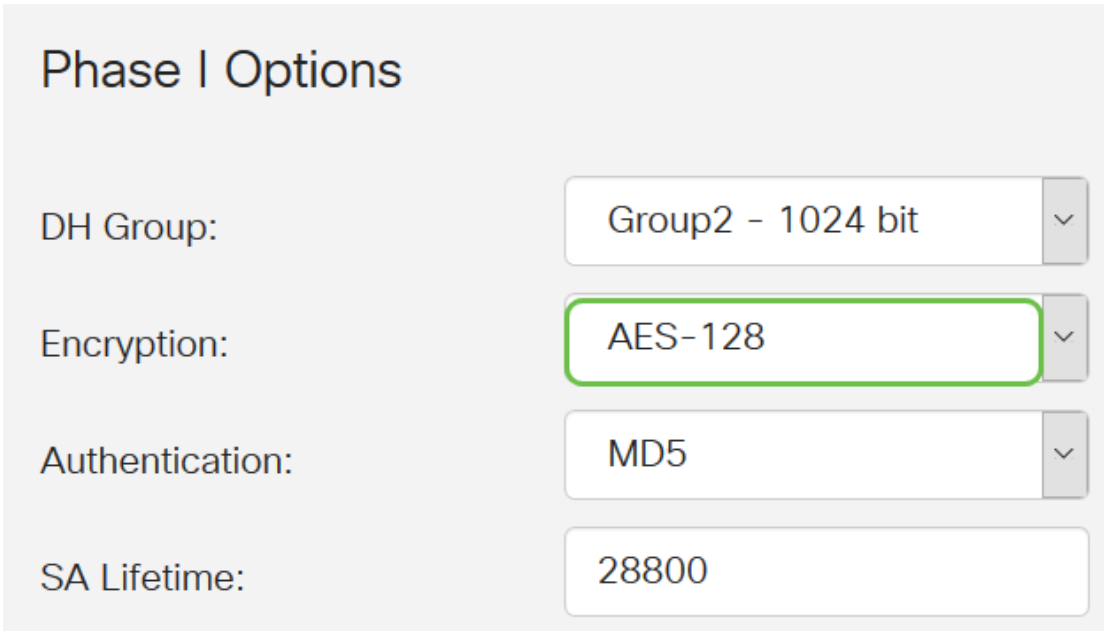
ステップ1:[Phase 1 Options]領域で、[DH Group]ドロップダウンリストから、フェーズ1のキーで使用する適切なDiffie-Hellman (DH)グループを選択します。Diffie-Hellmanは、事前共有キーセットを交換するための接続で使用される暗号キー交換プロトコルです。アルゴリズムの強度はビットによって決まります。次のオプションがあります。

- 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。



ステップ2:[Encryption] ドロップダウンリストから、暗号化および復号化のための暗号化方式を選択し、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）。推奨されない。一部の「ブロックコリジョン」攻撃に対して脆弱であるため、後方互換性のために必要な場合にのみ使用してください。
- AES-128:Advanced Encryption Standard(AES-128)は128ビットキーを使用します。Advanced Encryption Standard（AES；高度暗号化規格）は、DESよりも安全に設計された暗号化アルゴリズムです。AESでは、より大きなキーサイズを使用します。これにより、メッセージを復号化する唯一の既知のアプローチは、侵入者が可能なすべてのキーを試すことになります。
- 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。これは最も安全な暗号化オプションです。



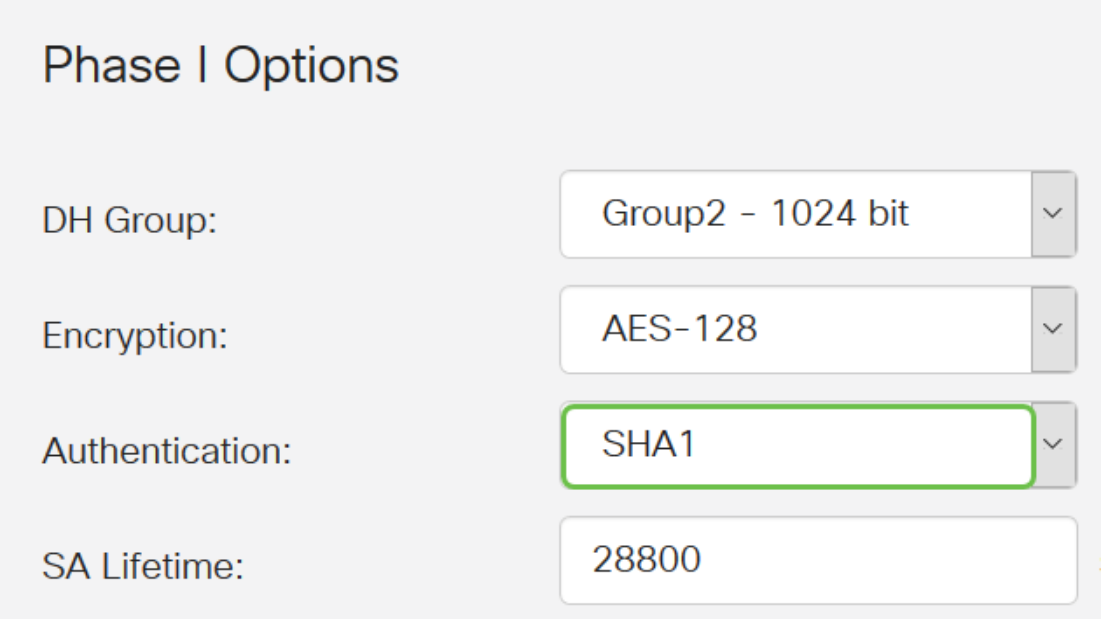
注：AESは、DESおよび3DESを介した暗号化の標準的な方式であり、パフォーマンスとセキュリティを向上させます。AESキーを長くすると、パフォーマンスが低下し、セキュリティが向上

します。

ステップ3:[Authentication] ドロップダウンリストから、ESPおよびISAKMPの認証方法を決定する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。これは、最も安全で推奨されるアルゴリズムです。

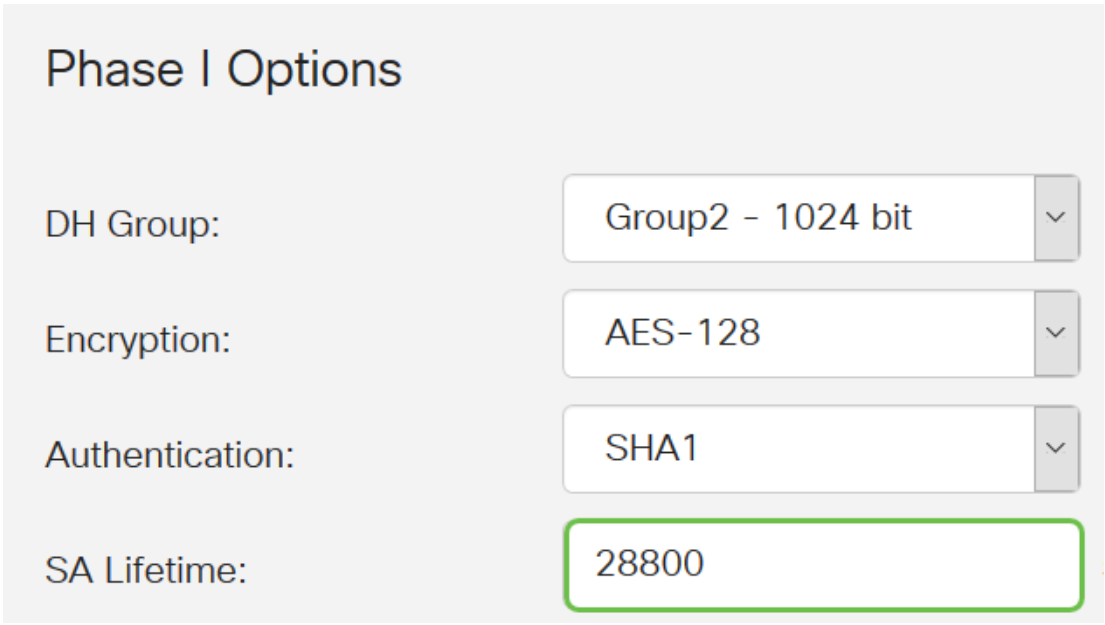
注：VPNトンネルの両端で同じ認証方式が使用されていることを確認します。



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。

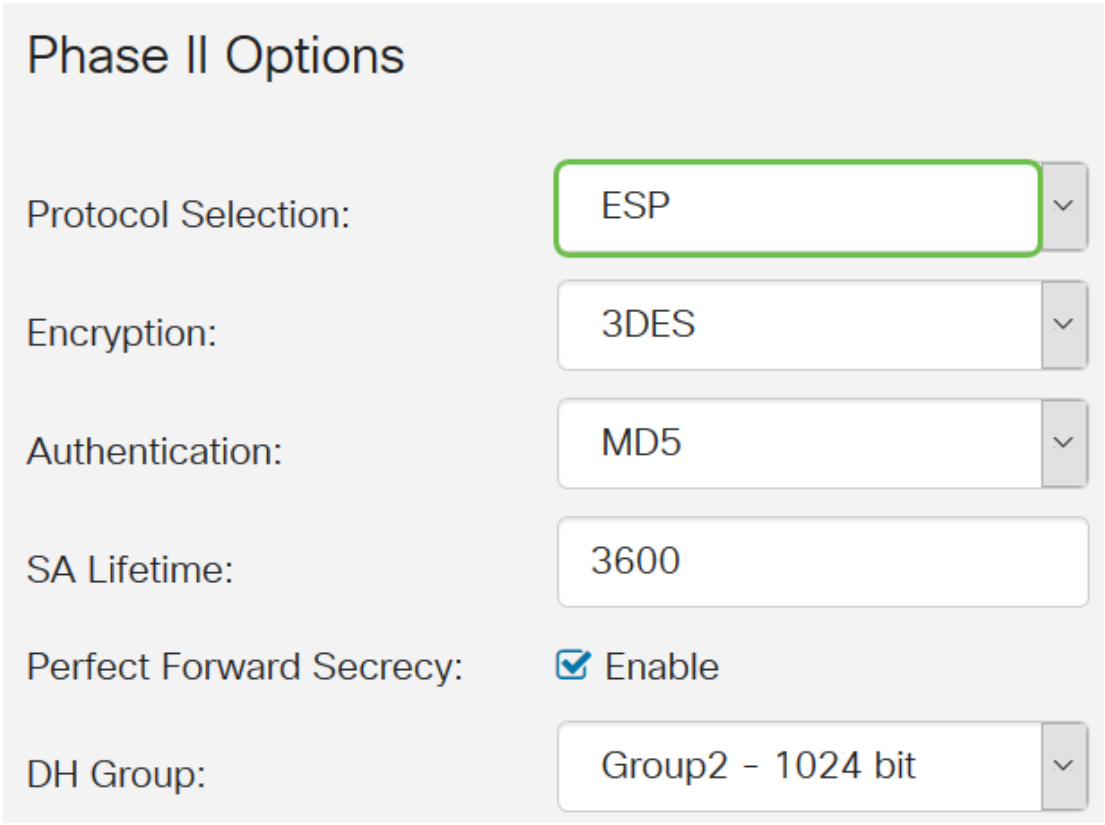
ステップ4:[SA Lifetime] フィールドに、120 ~ 86400の値を入力します。デフォルト値は28800です。*SA Lifetime (Sec)は、このフェーズでIKE SAがアクティブになっている時間を秒で示します*。新しいセキュリティアソシエーション(SA)は、ライフタイムが期限切れになる前にネゴシエートされ、古いセキュリティアソシエーション(SA)の有効期限が切れたときに新しいSAを使用する準備が整っていることを確認します。デフォルトは28800で、範囲は120 ~ 86400です。フェーズ1のSAライフタイムとして28800秒を使用します。

注：フェーズIのSAライフタイムは、フェーズIIのSAライフタイムよりも長くすることをお勧めします。フェーズIをフェーズIIよりも短くする場合、データトンネルとは対照的に、頻繁にトンネルの前後を再ネゴシエートする必要があります。データトンネルはより多くのセキュリティを必要とするため、フェーズIIのライフタイムをフェーズIよりも短くすることをお勧めします。



ステップ5:[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。

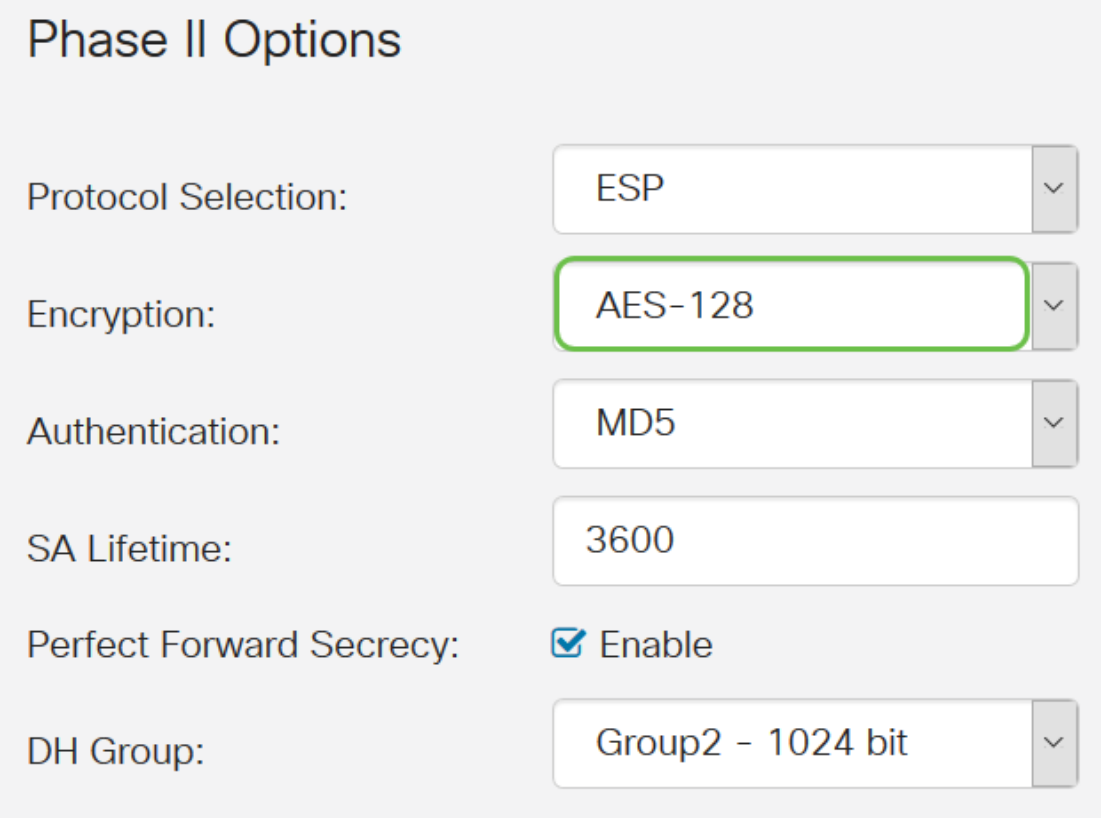
- ESP：このオプションは、Encapsulating Security Payloadとも呼ばれます。このオプションは、保護するデータをカプセル化します。このオプションを選択した場合は、ステップ6に進み、暗号化方式を選択します。
- AH：このオプションは、認証ヘッダー(AH)とも呼ばれます。 データ認証とオプションのアンチリプレイサービスを提供するセキュリティプロトコルです。AHは、保護されるIPデータグラムに埋め込まれています。このオプションを選択した場合は、ステップ7に進みます。



ステップ6：ステップ6でESPを選択した場合は、暗号化を選択します。次のオプションがあります。

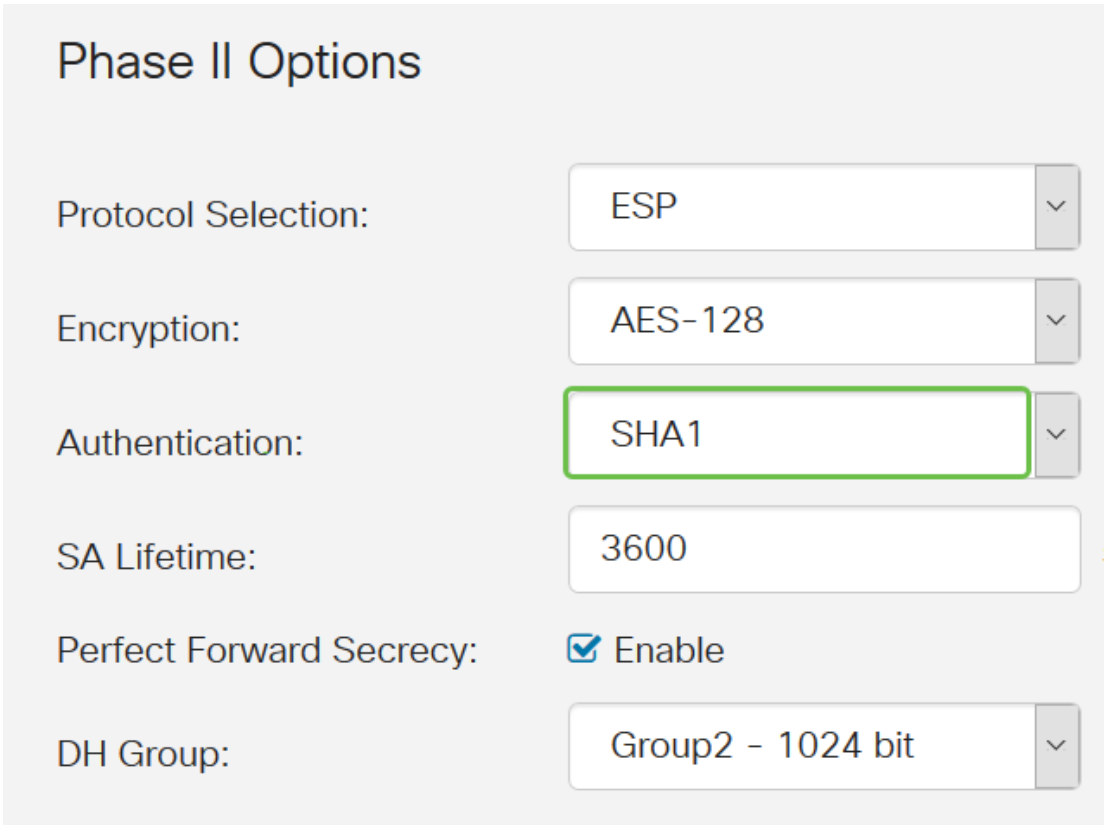
- 3DES:Triple Data Encryption Standard（トリプルデータ暗号化規格）

- 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。

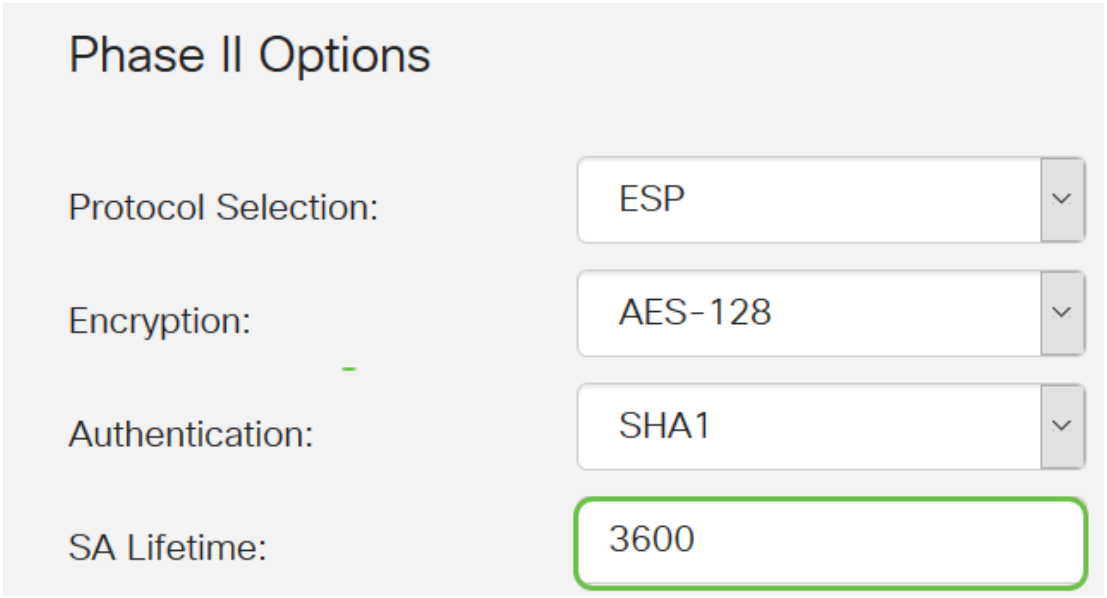


ステップ7:[Authentication] ドロップダウンリストから、ESPおよびISAKMPの認証方法を選択します。次のオプションがあります。

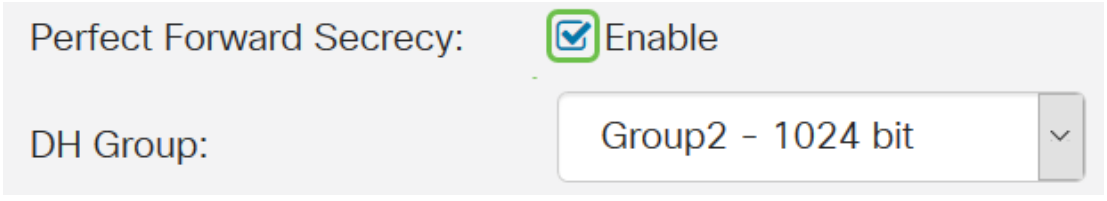
- MD5:Message-Digest Algorithm（MD5；メッセージダイジェストアルゴリズム）には、128ビットのハッシュ値があります。
- SHA-1:Secure Hash Algorithm（SHA-1；セキュアハッシュアルゴリズム）に160ビットのハッシュ値があります。
- SHA2-256:256ビットのハッシュ値を使用したセキュアハッシュアルゴリズム。



ステップ8:[*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。

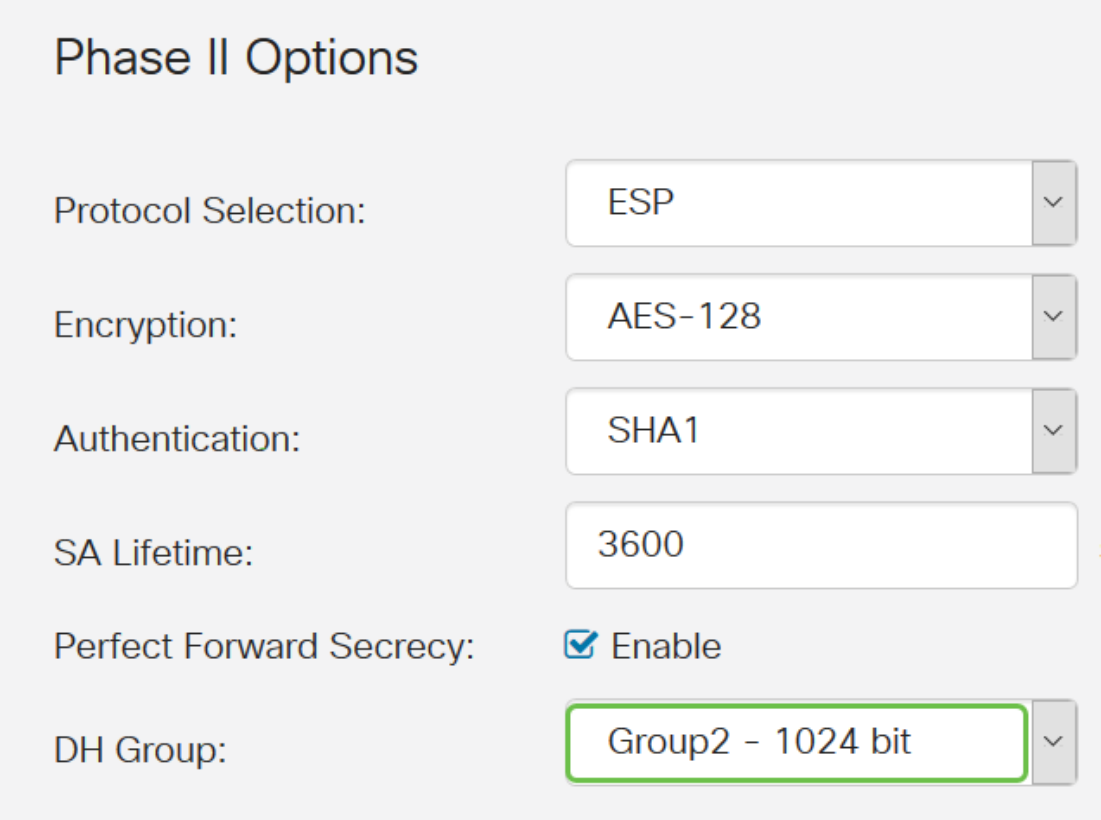


ステップ9:（オプション）[Enable Perfect Forward Secrecy]チェックボックスをオンにして、IPSecトラフィックの暗号化と認証のための新しいキーを生成します。Perfect Forward Secrecy（PFS；完全転送秘密）は、公開キー暗号化を使用してインターネット経由で送信される通信のセキュリティを向上するために使用されます。この機能を有効にするには、このチェックボックスをオンにします。無効にするには、このチェックボックスをオフにします。この機能が推奨されます。

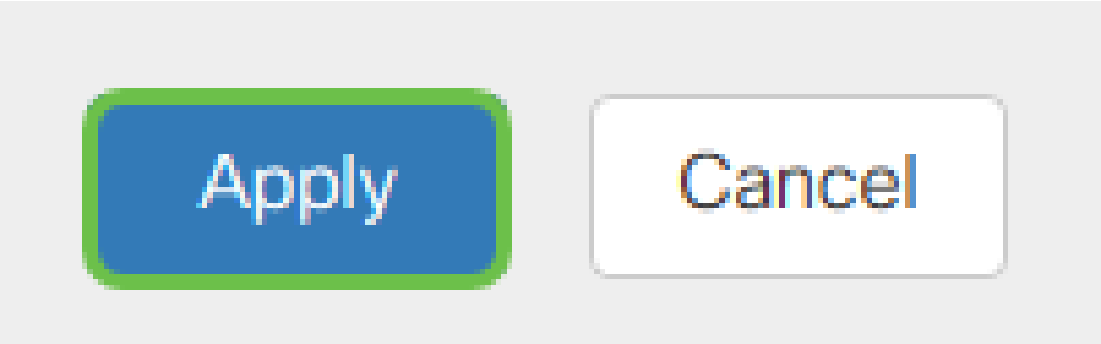


ステップ10:[*DHグループ*]ドロップダウンリストから、フェーズ2のキーで使用するDHグループを選択します。オプションは次のとおりです。

- Group2-1024ビット：このオプションは、キーをより高速に計算しますが、安全性は低くなります。
- 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。

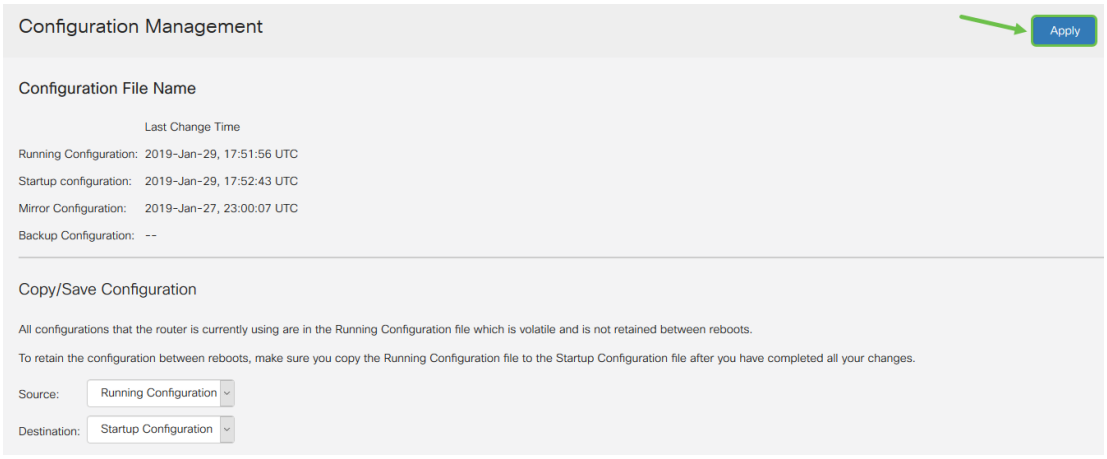


ステップ11:[Apply]をクリックします。

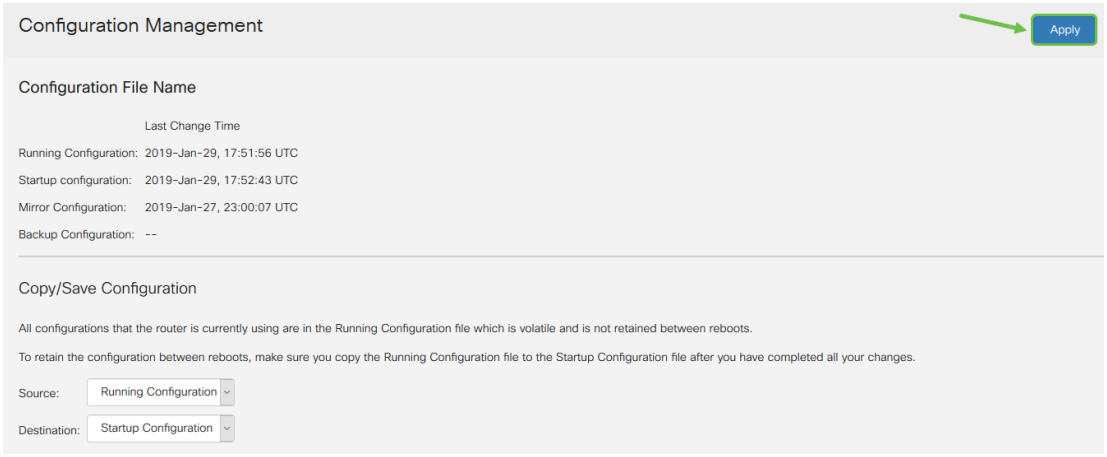


ステップ12:[Save]をクリックし、設定を永続的に保存します。

ステップ13:[Apply]をもう一度クリックして、実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します。



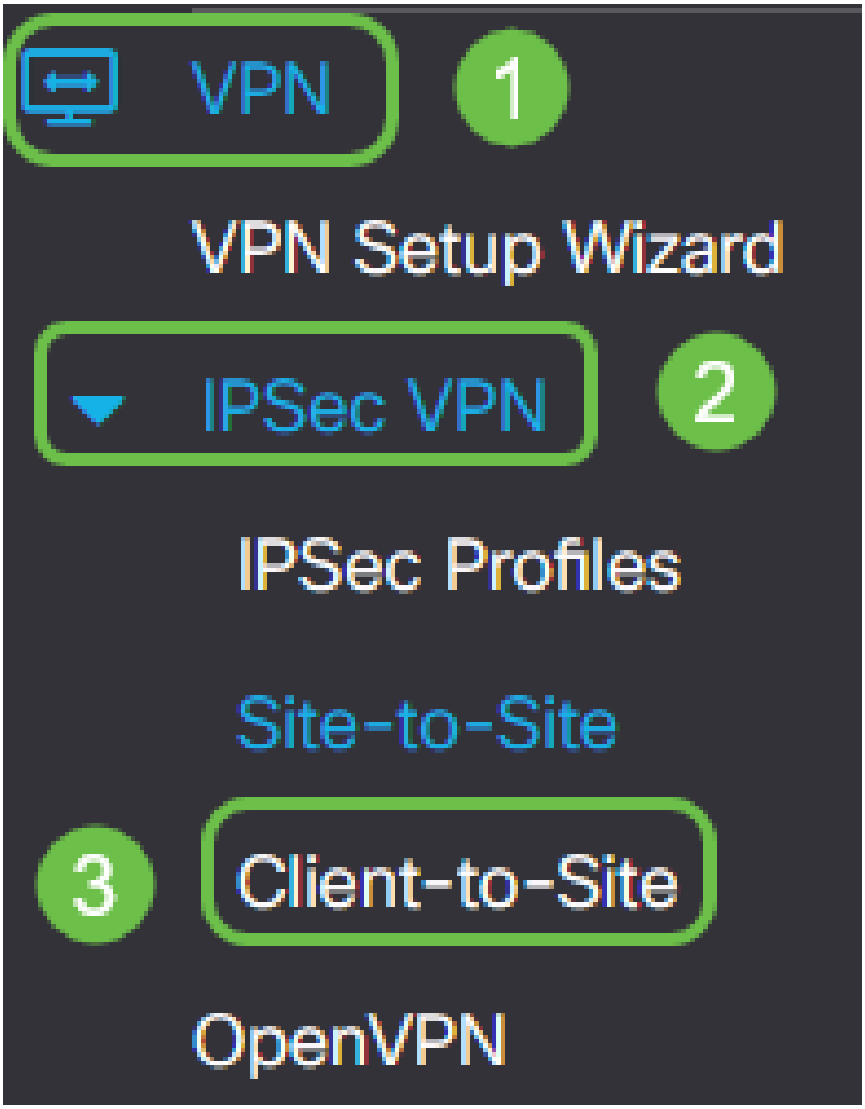
ステップ14：確認メッセージが表示されたら、[OK]をクリックします。



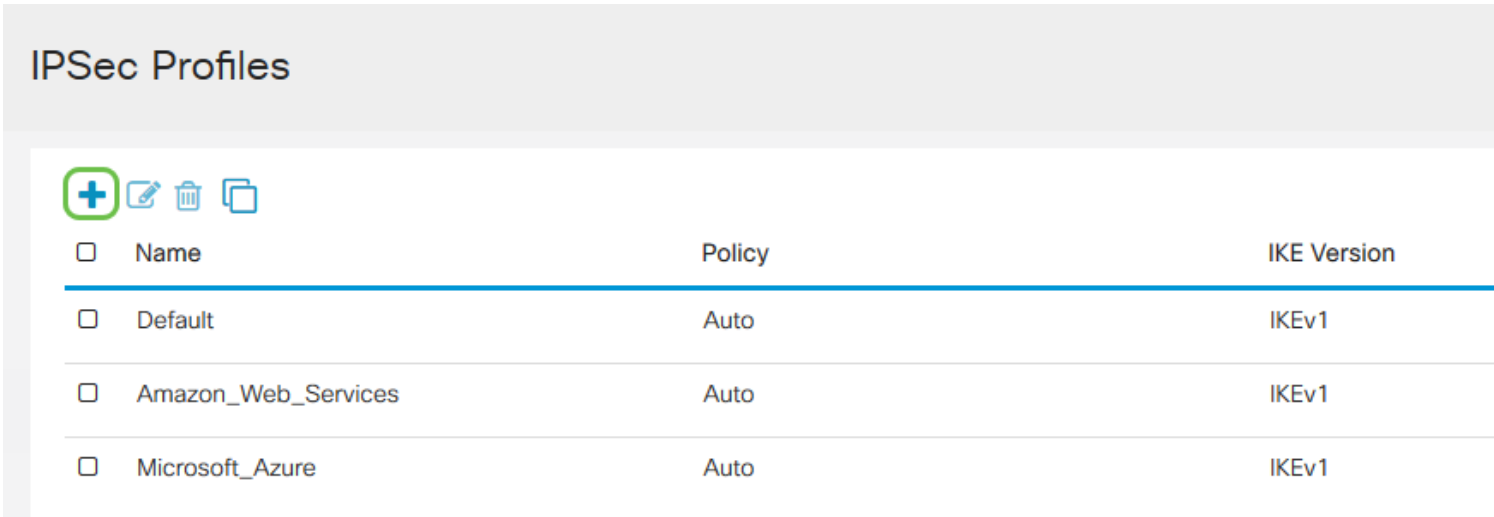
これで、RV160またはRV260ルータでIPsecプロファイルが正しく設定されたはずです。

クライアントからサイトへのプロファイルの作成

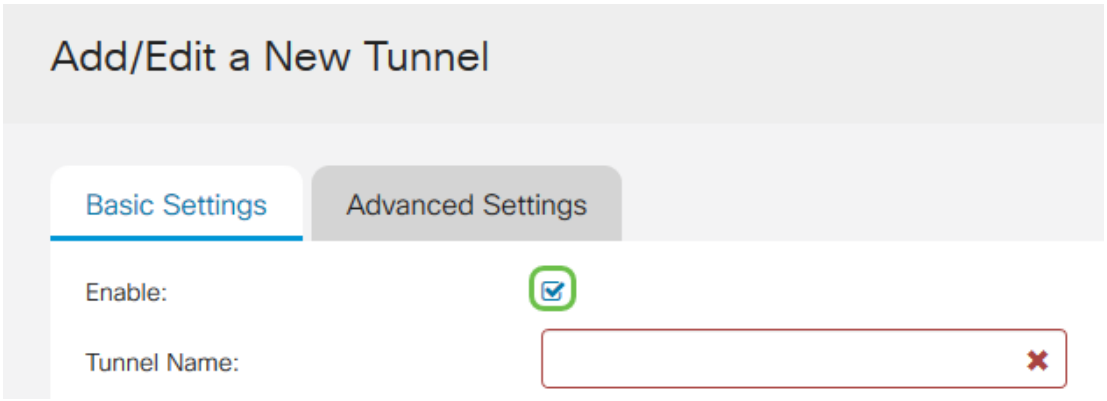
ステップ1:[VPN] > [IPSec VPN] > [Client-to-Site] の順に選択します。



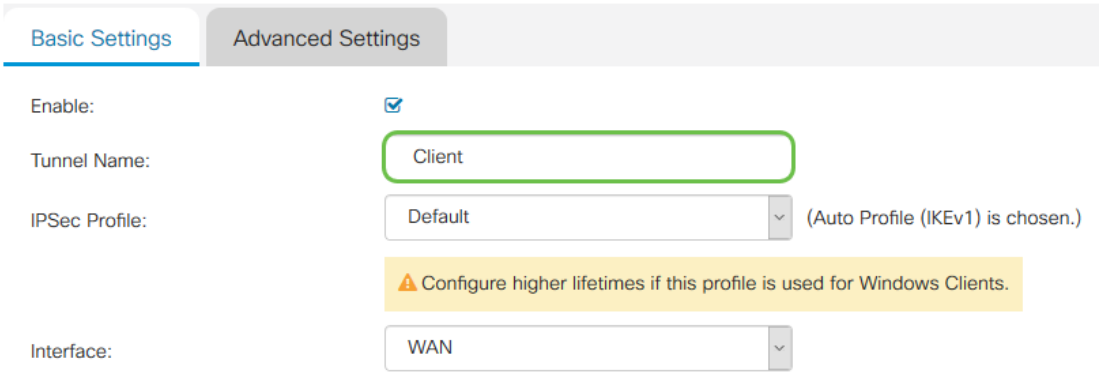
ステップ2:[+]アイコンを**クリック**します。



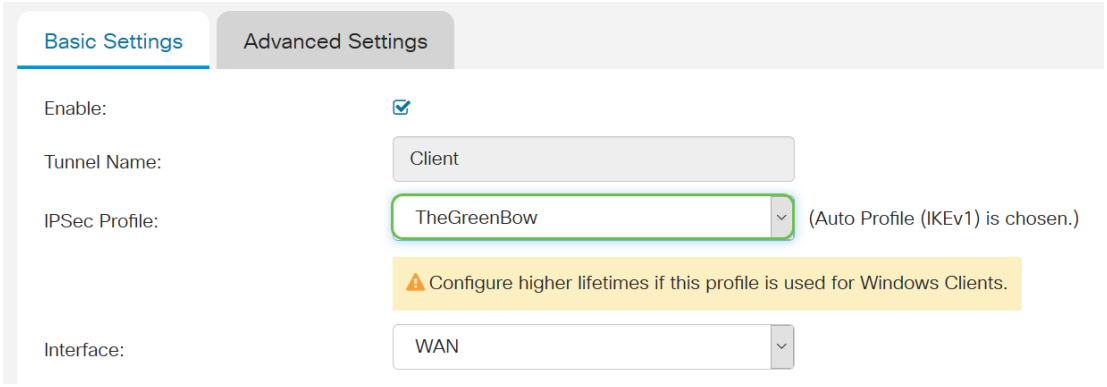
ステップ3:[Basic Settings]タブで、[Enable] チェックボックスをオンにして、VPNプロファイルがアクティブであることを確認します。



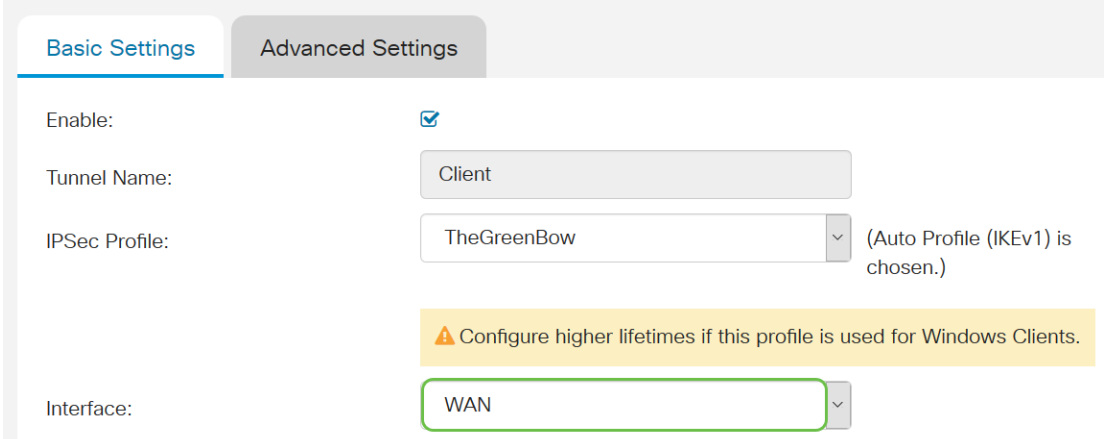
ステップ4:[Tunnel Name]フィールドにVPN接続の名前を入力します。



ステップ5:[IPsec]ドロップダウンリストから、使用するIPsecプロファイルを選択します。



ステップ6:[Interface]ドロップダウンリストから[*Interface*]を選択します。

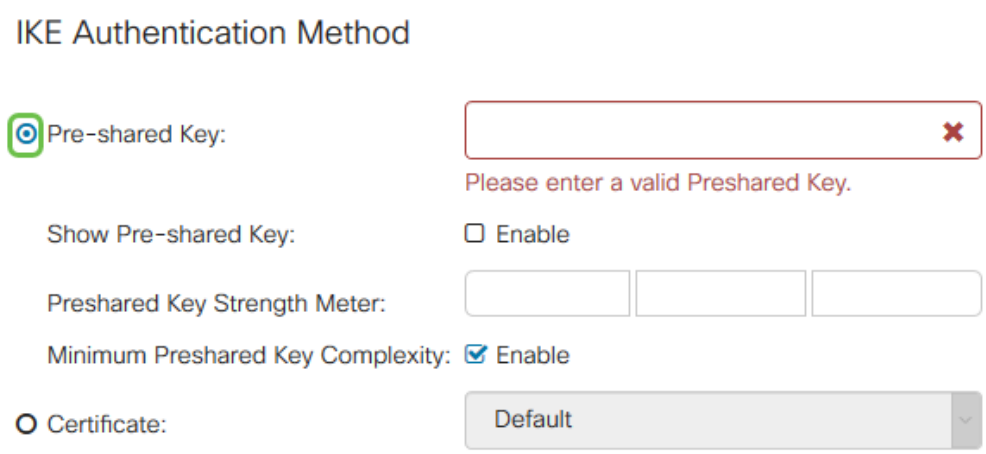


注：オプションは、使用しているルータのモデルによって異なります。この例では、WANが選択されています。

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。

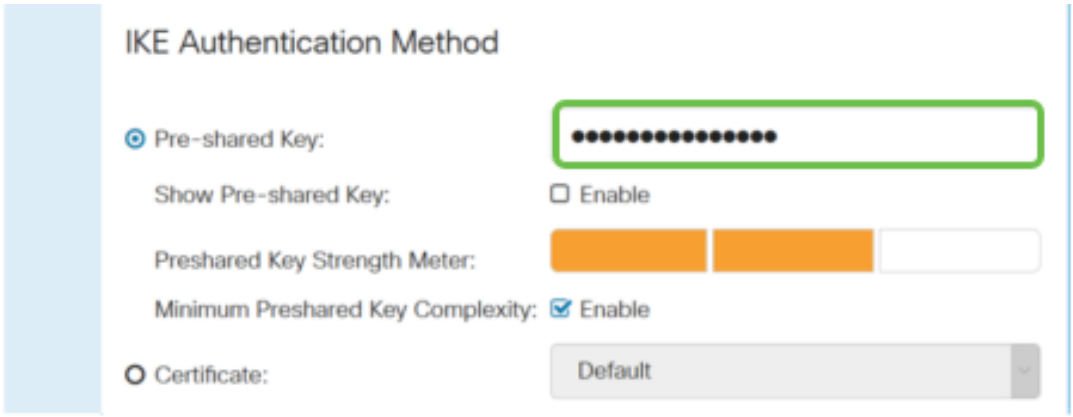
- 事前共有キー：このオプションでは、VPN接続に共有パスワードを使用できます。

- [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。

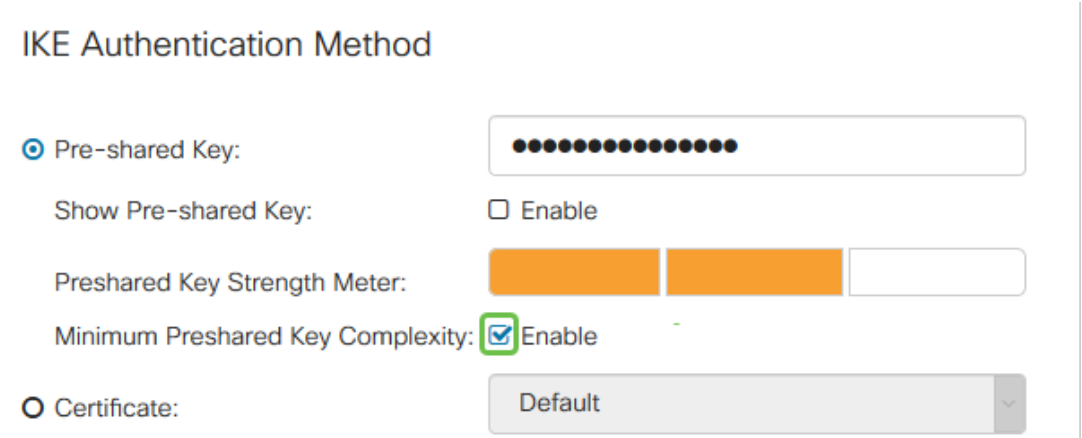


注：事前共有キーは何でも構いません。サイトとクライアントがコンピュータにTheGreenBow Clientをセットアップするときに、クライアントと一致する必要があります。

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

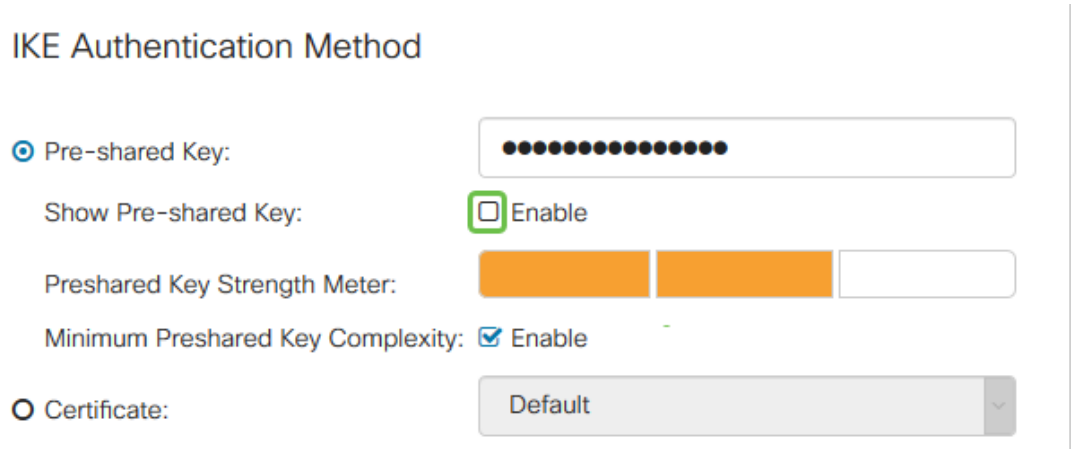


ステップ9:（オプション）[*Minimum Pre-shared Key Complexity* **Enable**]チェックボックスをオフにして、シンプルパスワードを使用できるようにします。



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

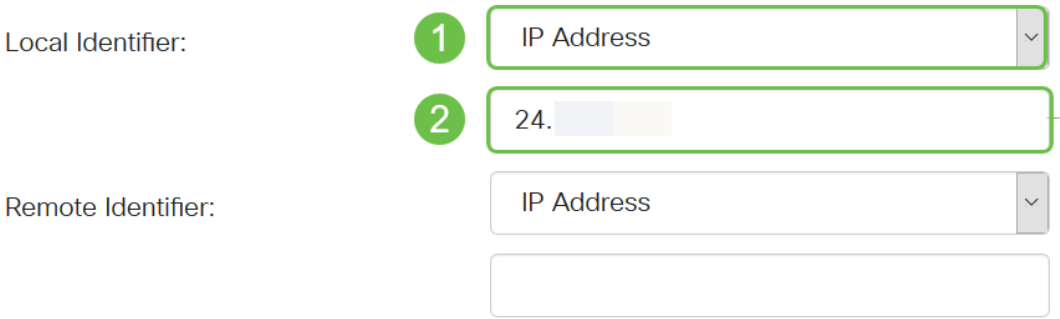
ステップ10:（オプション）パスワードをプレーンテキストで表示するには、*[Show Pre-shared Key* **Enable]**チェックボックスをオンにします。



注：この例では、[Show Pre-shared key]は無効のままにしておきます。

ステップ11:[Local Identifier]ドロップダウンリストから*ローカル*識別子を選択します。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。これは、サイト（オフィス）のルータのWAN IPアドレスです。
- 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。

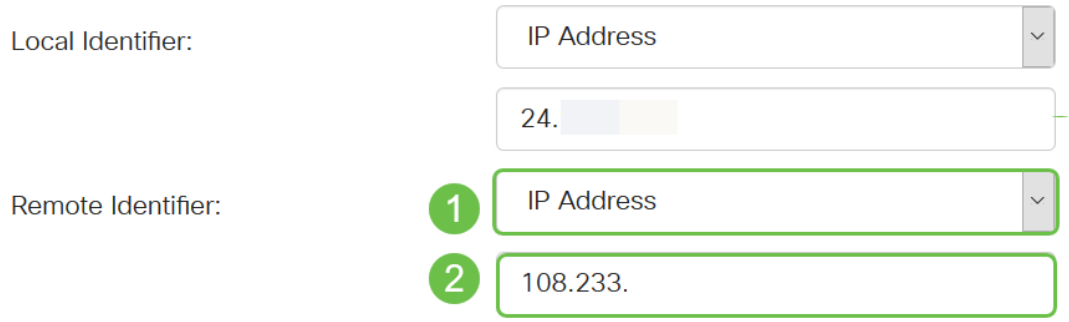


注：この例では、IPアドレスを選択し、サイトのルータのWAN IPアドレスを入力します。この例では、24.x.x.xが入力されています。完全なアドレスは、プライバシーのために不明確になっています。

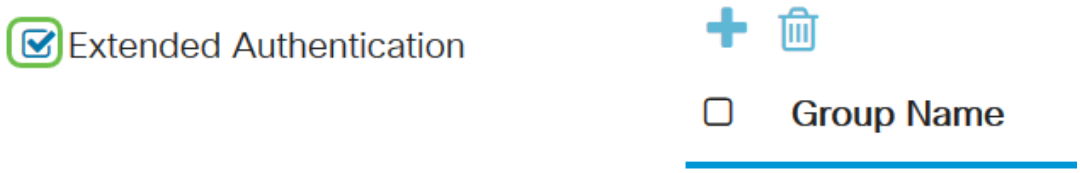
ステップ12：リモートホストのIDを選択します。次のオプションがあります。

- [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。WAN IPアドレスを確認するには、Webブラウザに「What is my IP」と入力します。これはクライアントのIPアドレスです。
- FQDN：完全修飾ドメイン名。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。

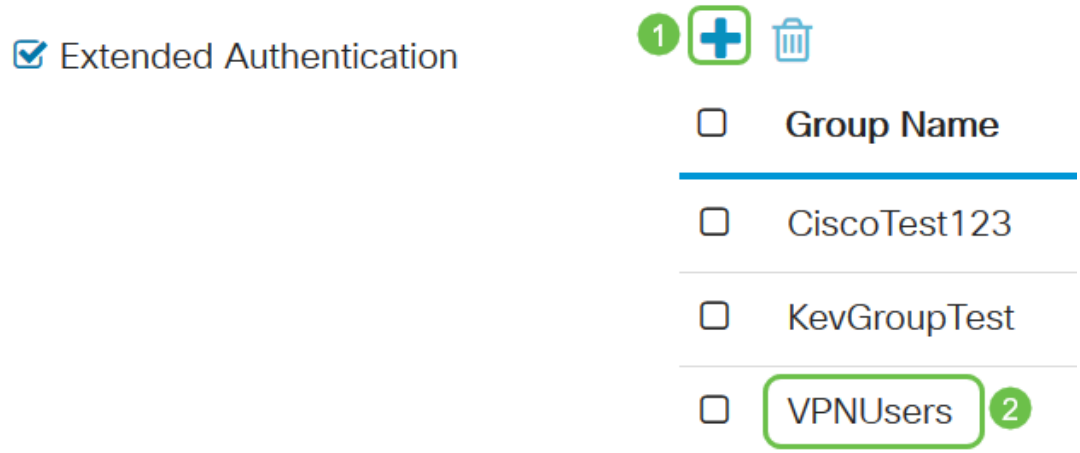
注：この例では、IPアドレスを選択し、クライアントの場所にあるルータの現在のIPv4アドレスを入力します。これは、Webブラウザで「What's my IP address」を検索することで確認できます。このアドレスは変更されるため、設定が正常に完了した後に接続で問題が発生した場合は、クライアントとサイトの両方で確認と変更を行うためのエリアになります。



ステップ13:（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。



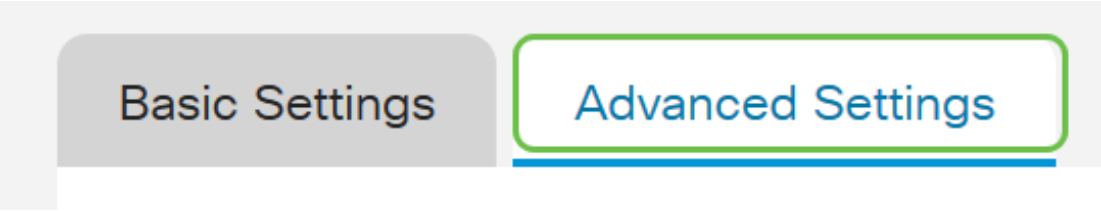
ステップ14:（オプション）拡張認証を使用するグループを選択するには、プラス**アイコンをクリックし**、ドロップダウンリストからユーザを選択します。



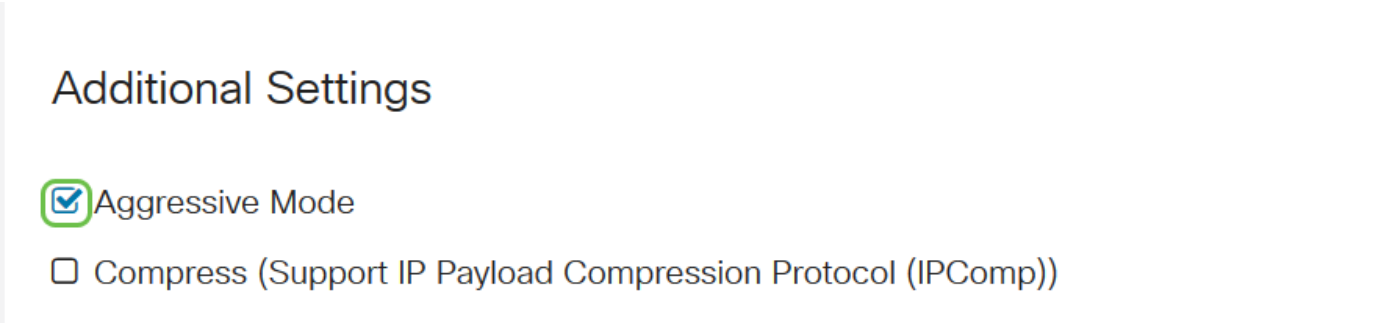
注：この例では、**VPNUsers**が選択されています。

ステップ15:[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アドレスと最後のIPアドレスを入力します。これは、サイトアドレスと重複しないアドレスプールである必要があります。これらは仮想インターフェイスと呼ばれることがあります。仮想インターフェイスを変更する必要があるというメッセージが表示された場合は、ここで修正します。

ステップ16:[詳細設定]**タブを選択**します。

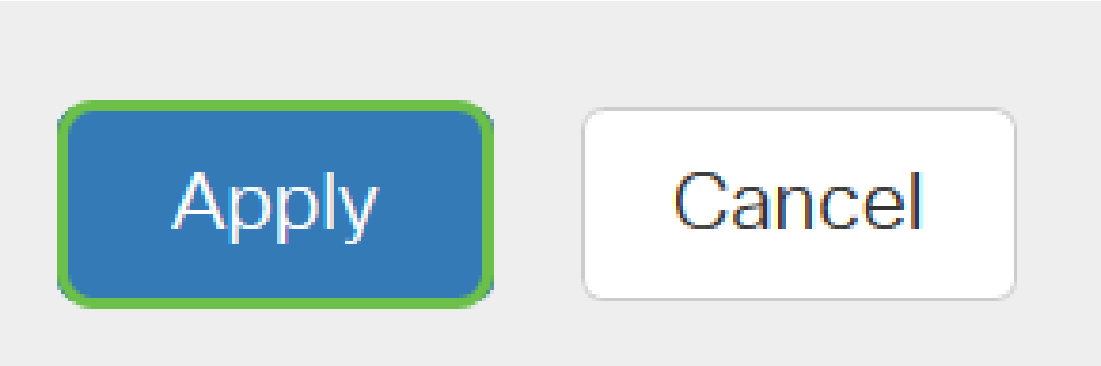


ステップ17:（オプション）ページの下部までスクロールし、[アグレッシブモード]を**選択します**。アグレッシブモード機能を使用すると、IPセキュリティ(IPsec)ピアのRADIUSトンネル属性を指定し、トンネルとのInternet Key Exchange(IKE)アグレッシブモードネゴシエーションを開始できます。アグレッシブモードとメインモードの詳細については、ここをクリックし[てください](#)。



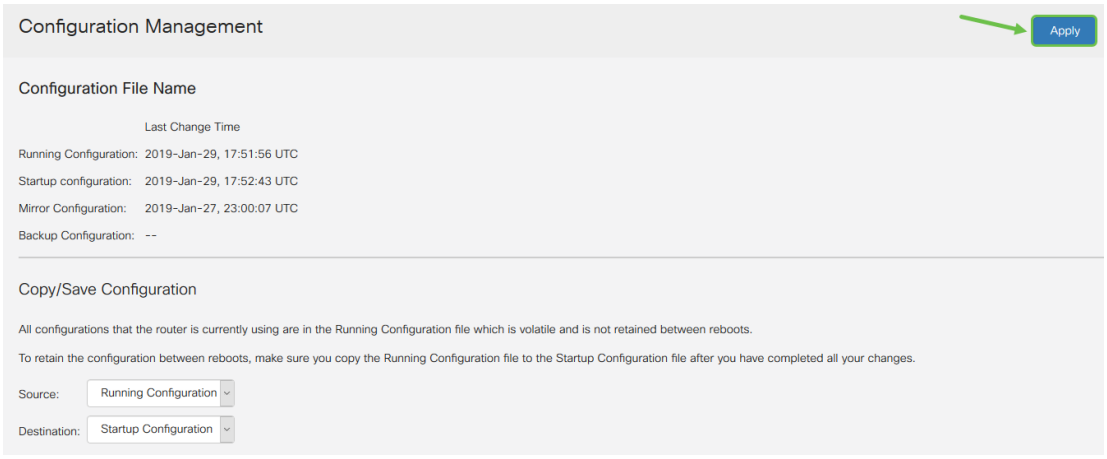
注：[圧縮]チェックボックスをオンにすると、ルータは接続を開始するときに圧縮を提案できます。このプロトコルは、IPデータグラムのサイズを縮小します。応答側がこの提案を拒否した場合、ルータは圧縮を実装しません。ルータが応答側の場合、圧縮が有効になっていなくても、圧縮を受け入れます。このルータでこの機能を有効にする場合は、リモートルータ（トンネルのもう一方の端）で有効にする必要があります。 この例では、[Compress]はオフのままになっています。

ステップ18:[Apply]をクリ**ックします**。

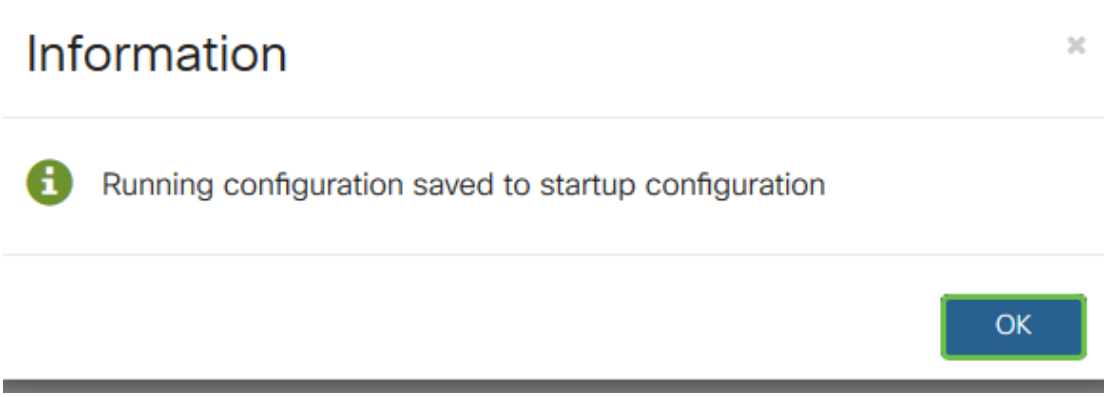


ステップ19:[**Save**]をクリ**ックします**。

ステップ20:[**Apply**]をもう一度クリックして、実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します。



ステップ21：確認メッセージが表示されたら、[OK]をクリックします。



これで、TheGreenBow VPN Client用にルータでクライアントからサイトへのトンネルを設定できました。

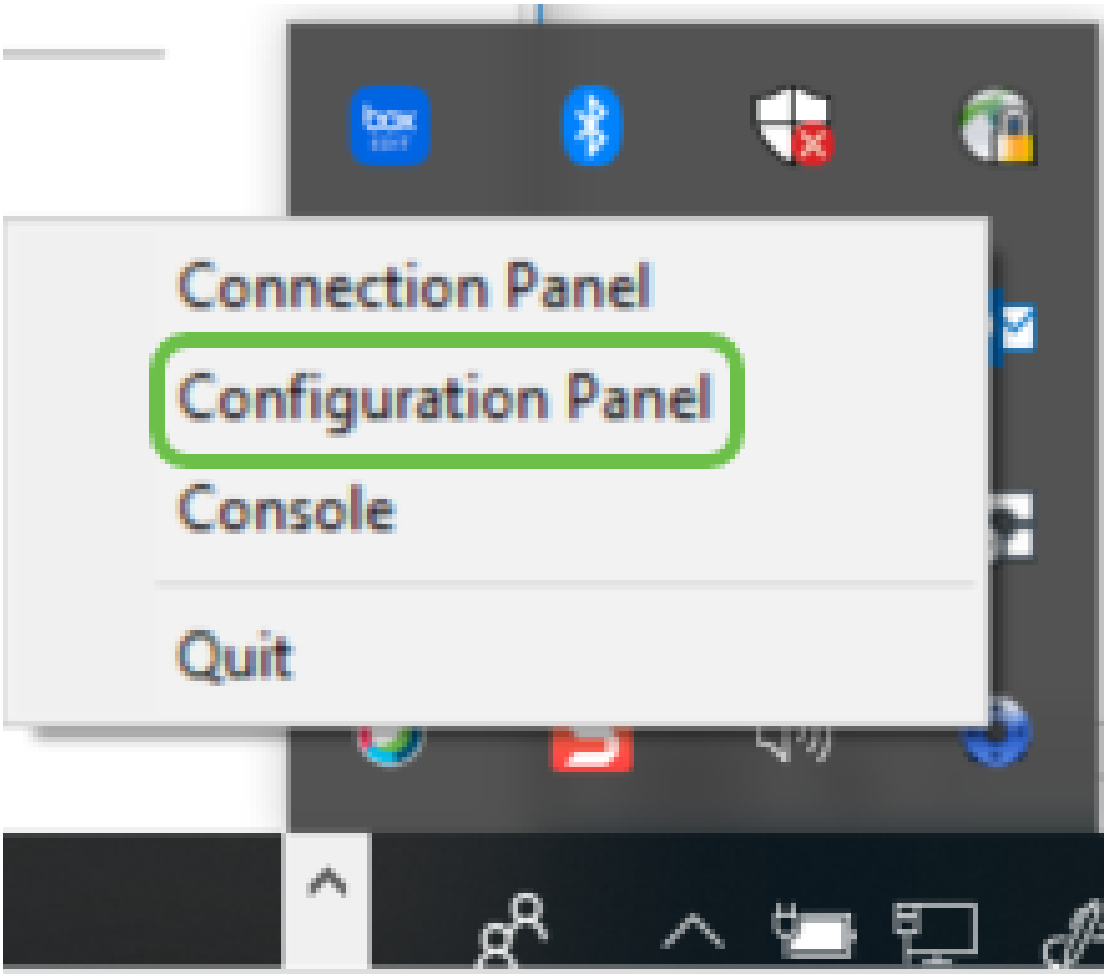
リモートワーカーのコンピュータでのGreenBow VPNクライアントの設定

フェーズ1の設定

TheGreenBow IPsec VPN Clientソフトウェアの最新リリースをダウンロードするには、ここをクリックしてください。

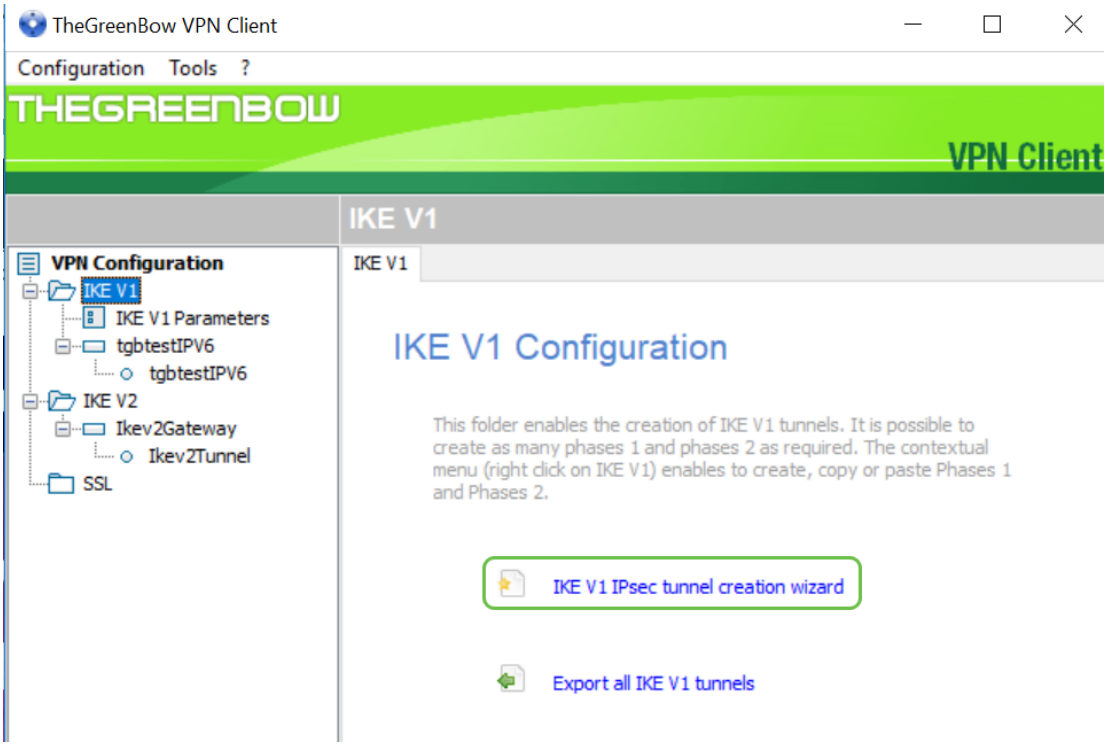
ステップ1:[GreenBow VPN Client]アイコンを右クリックします。これは、タスクバーの右下隅にあります。

ステップ2:[Configuration Panel]を選択します。



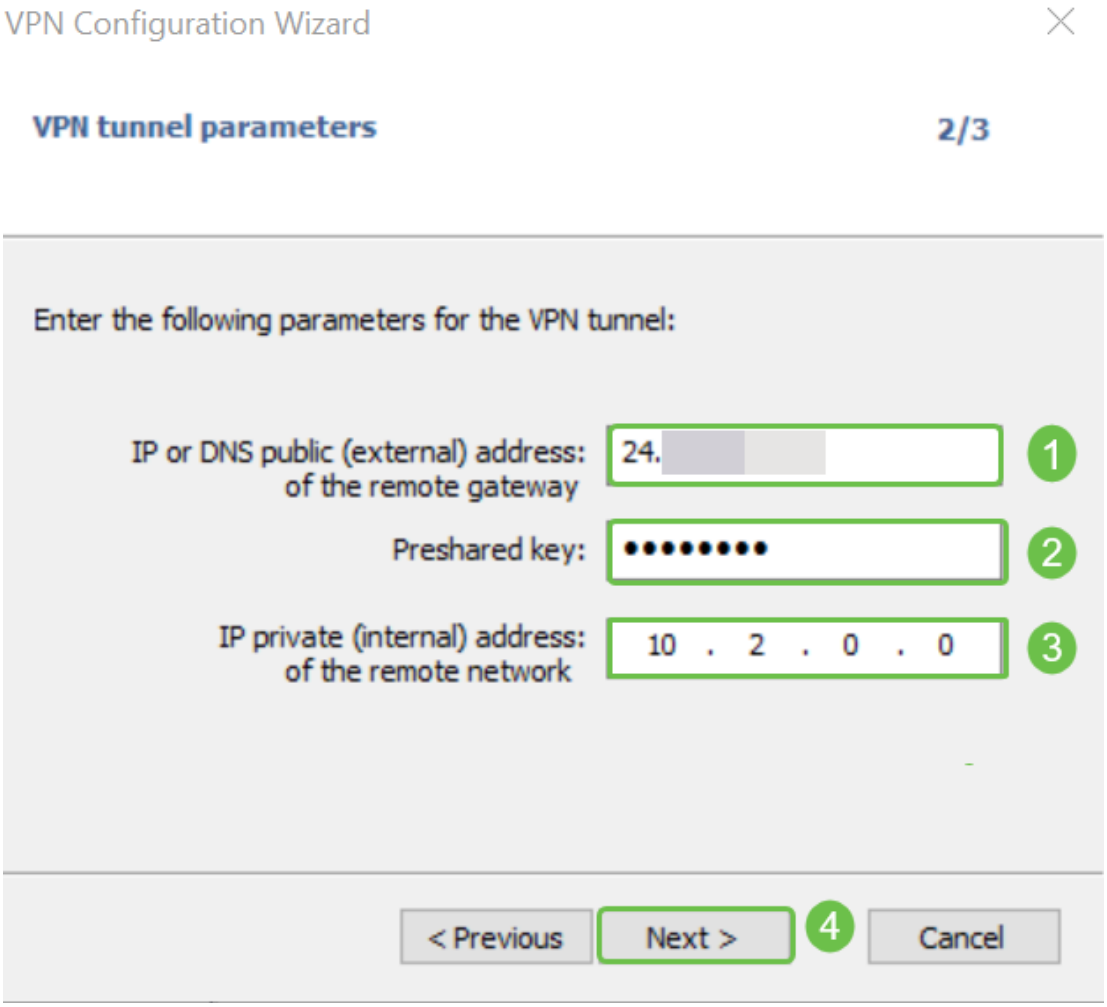
注：これは、Windowsコンピュータの例です。これは、使用するソフトウェアによって異なります。

ステップ3:**[IKE V1 IPsec tunnel creation wizard]を選択します。**

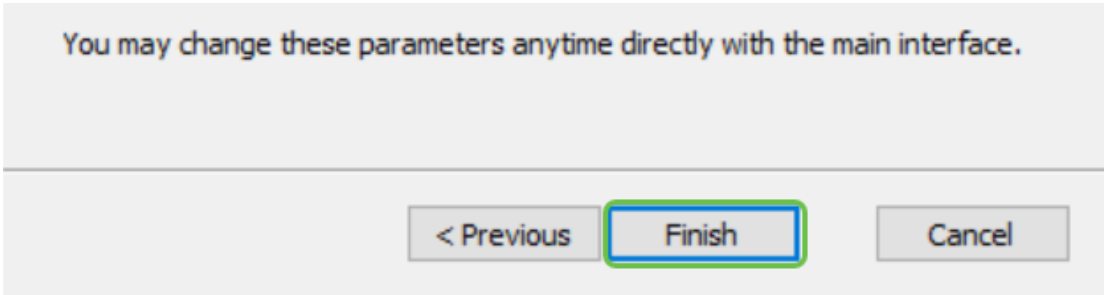


注：この例では、IKEバージョン1が設定されています。IKEバージョン2を設定する場合は、同じ手順に従いますが、IKE V2フォルダを右クリックします。また、サイトのルータのIPsecプロファイルにIKEv2を選択する必要もあります。

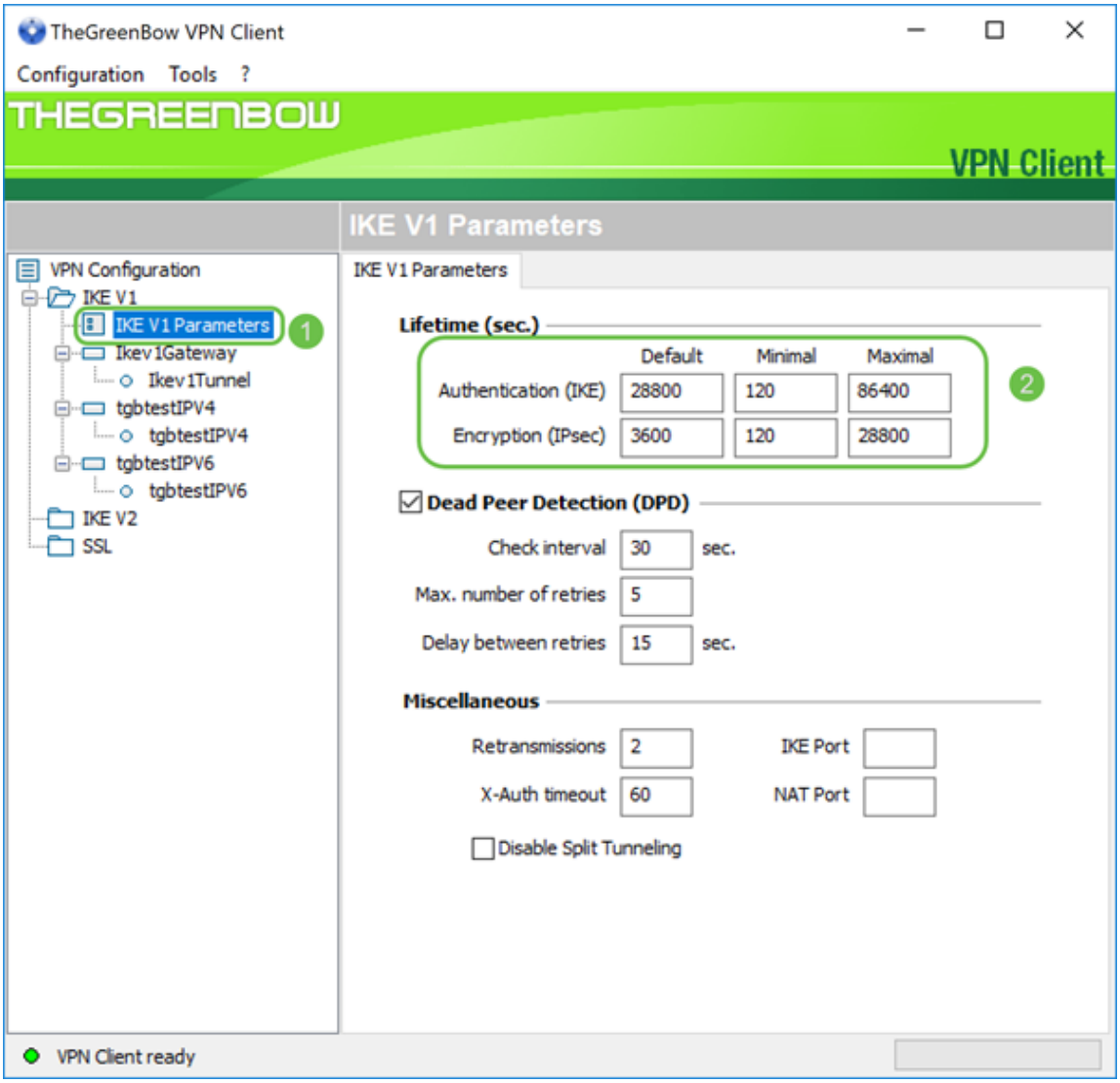
ステップ4：ファイルサーバがあるサイト（オフィス）のルータのパブリックWAN IPアドレス、事前共有キー、およびサイトのリモートネットワークのプライベート内部アドレスを入力します。[next] をクリックします。この例では、サイトは24.x.x.xです。このネットワークを保護するために、最後の3つのオクテット（このIPアドレス内の番号のセット）がxに置き換えられました。完全なIPアドレスを入力します。



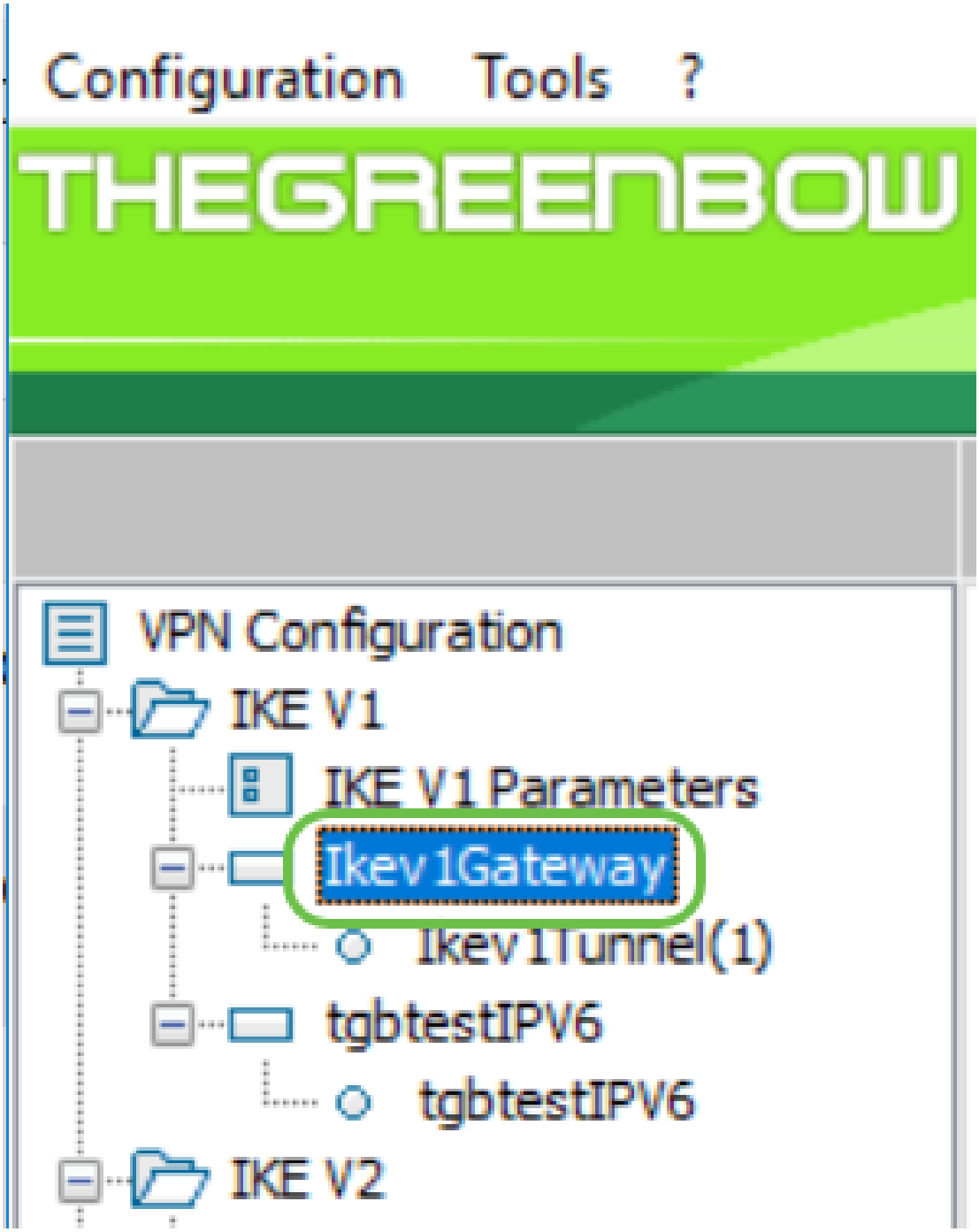
ステップ5:[Finish]をクリックします。



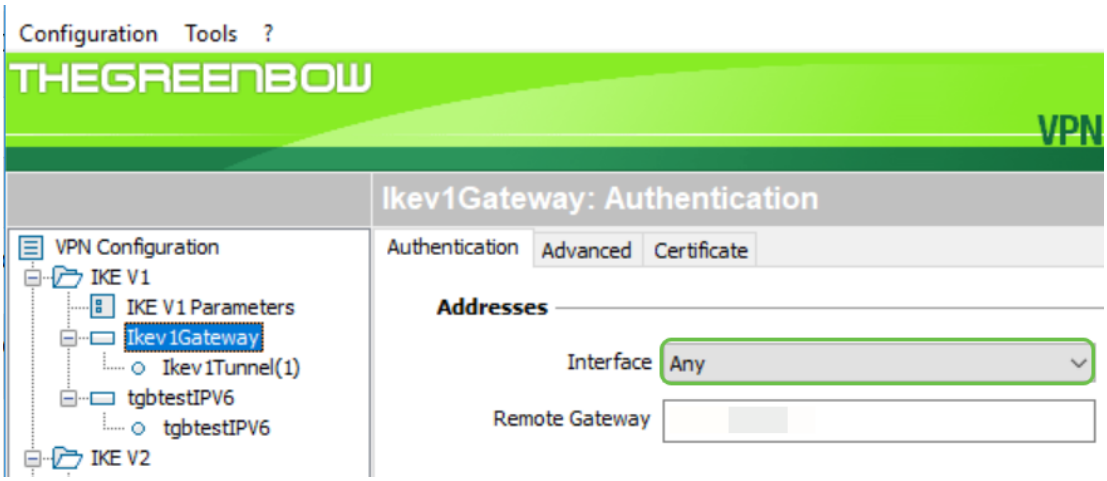
ステップ6（オプション）IKE V1パラメータを変更できます。GreenBow Default、Minimal、Maximalライフタイムを調整できます。この場所では、ルータが受け入れるライフタイムの範囲を入力できます。



ステップ7：作成したゲートウェイをクリックします。

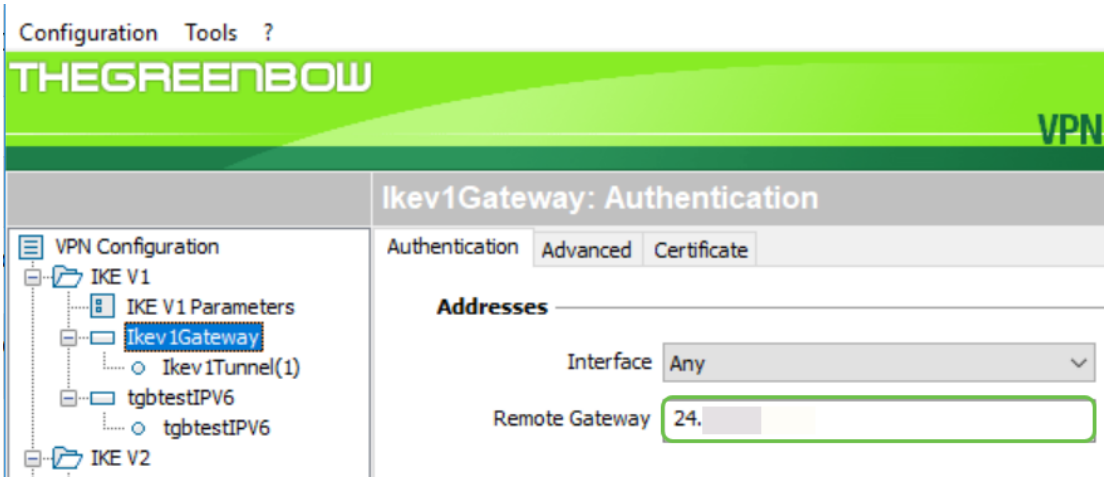


ステップ8:[*Authentication*]タブの[*Addresses*]に、ローカルアドレスのドロップダウンリストが表示されます。次に示すように、1つ選択するか**[Any]**を選択できます。



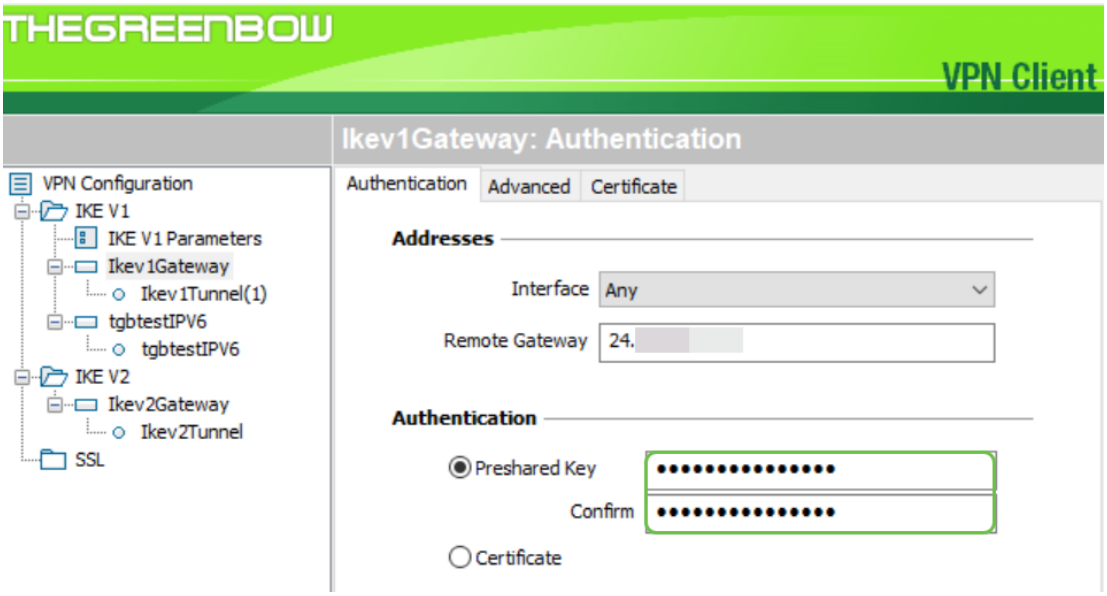
ステップ9:[Remote Gateway]フィールドにリモートゲートウェイのアドレスを入力します。IPアドレスまたはDNS名を指定できます。これは、サイト（オフィス）のルータのパブリックIPアド

レスのアドレスです。



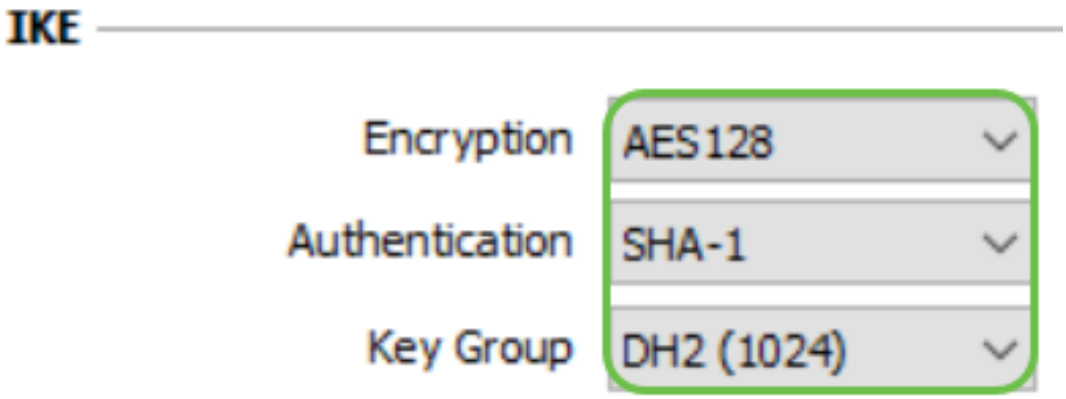
ステップ10:[Authentication] で、認証タイプを選択します。次のオプションがあります。

- 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。

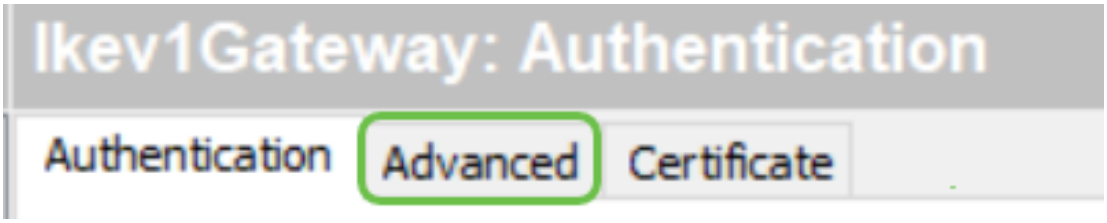


注：この例では、ルータに設定された事前共有キー(PSK)が入力され、確認されています。

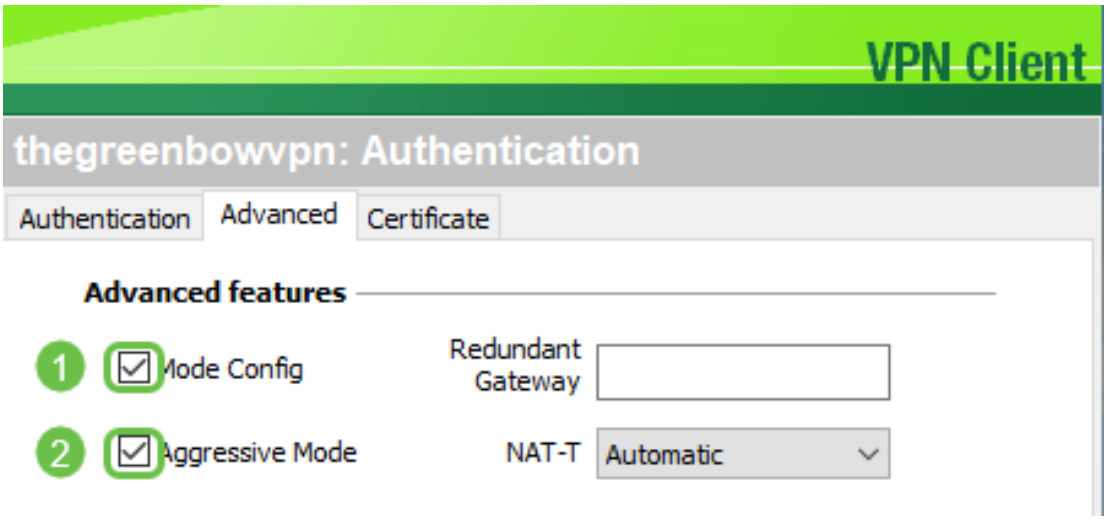
ステップ11:[IKE] で、[Encryption]、[Authentication]、および[Key Group]の設定をルータの設定と一致するように設定します。



ステップ12:[Advanced]タブをクリックします。

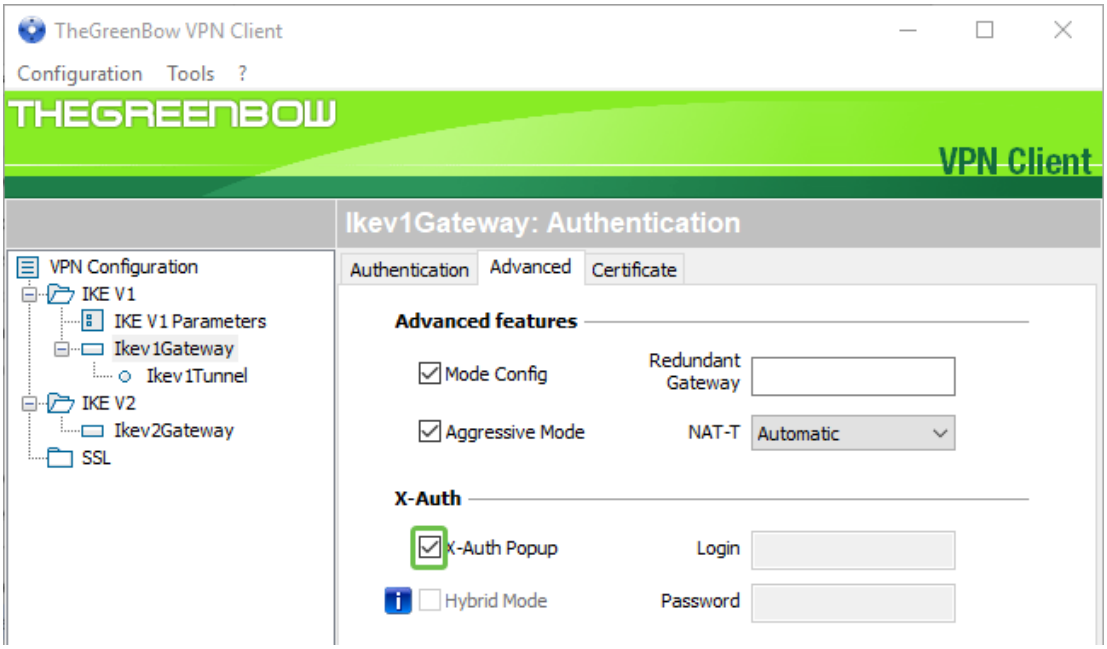


ステップ13:[Advanced features]で、[Mode Config]および[**Aggressive Mode**]チェックボックスをオンにします。この例のClient-to-Siteプロファイルでは、RV160で[Aggressive Mode]が選択されています。[NAT-T]設定は[Automatic]のままにします。

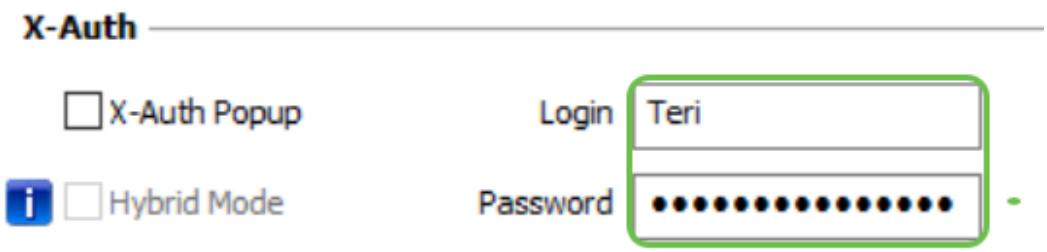


注：Mode Configを有効にすると、GreenBow VPN ClientはVPNゲートウェイから設定を取得し、トンネルの確立を試みます。NAT-Tにより、接続の確立が高速になります。

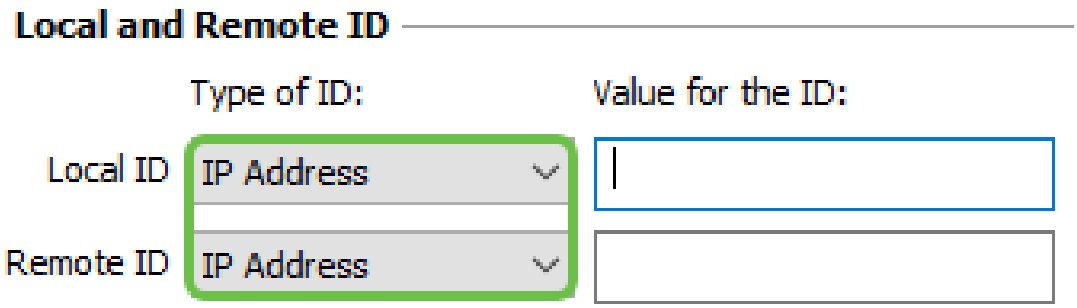
ステップ14:（オプション）[*X-Auth*]の[**X-Auth Popup**]チェックボックスをオンにすると、接続を開始するときに自動的にログインウィンドウが表示されます。ログインウィンドウでは、ユーザがクレデンシャルを入力して、トンネルを完了できます。



ステップ15:（オプション）[*X-Auth Popup*]を選択しない場合は、*[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アカウントを作成し、サイトのパスワードを入力したときに入力されたユーザ名です。

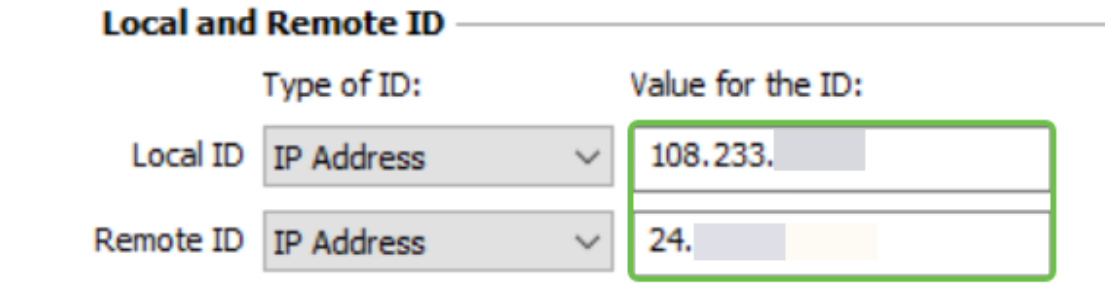


ステップ16:[Local and Remote ID] で、[Local ID]と[Remote ID]をVPNゲートウェイの設定と一致するように設定します。

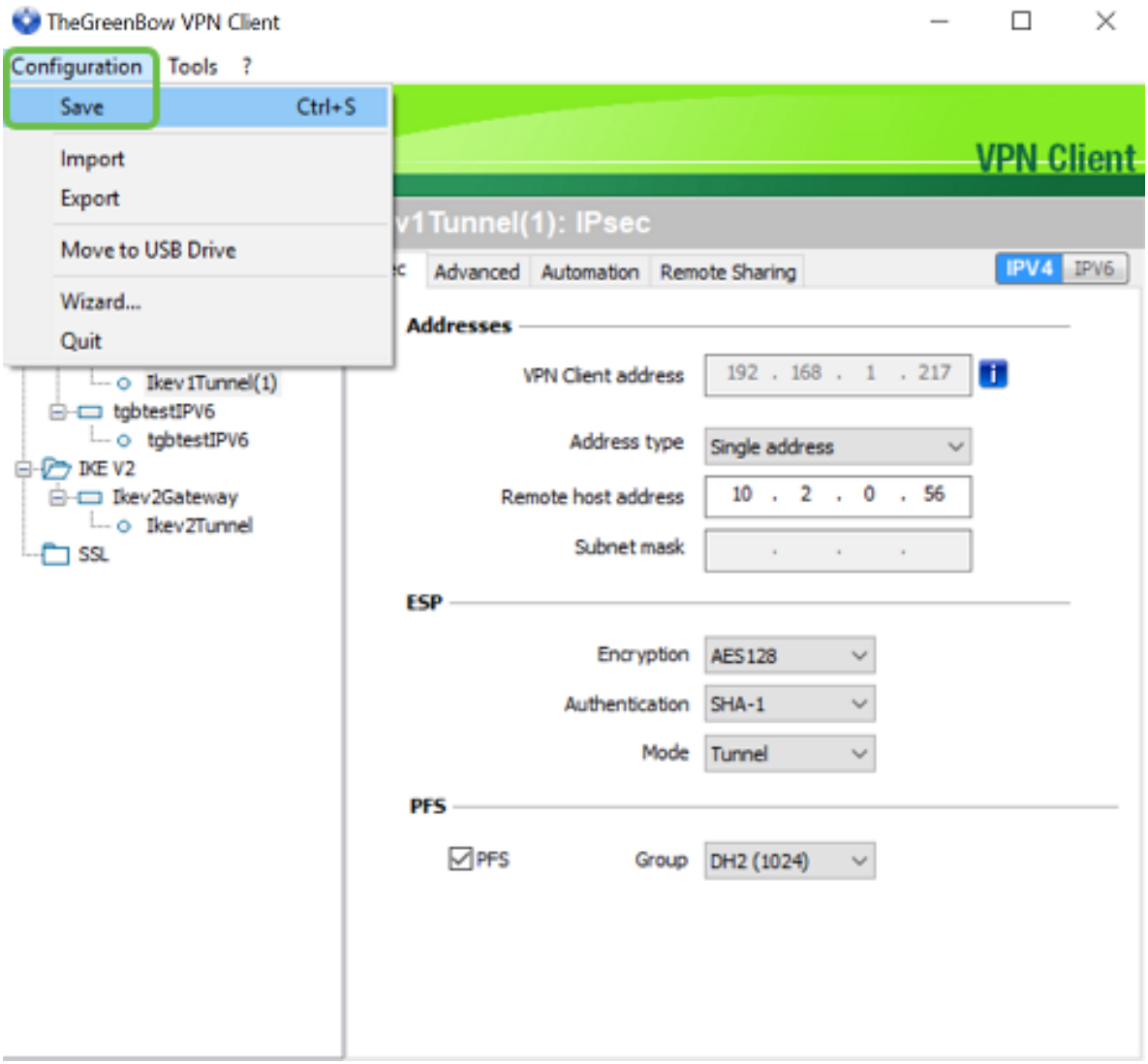


注：この例では、RV160またはRV260 VPNゲートウェイの設定に一致するように、ローカルIDとリモートIDの両方がIPアドレスに設定されています。

ステップ17:[IDの*値(Value for the ID)]の下*で、それぞれのフィールドにローカルIDとリモートIDを入力します。ローカルIDは、クライアントのWAN IPアドレスです。これは、「What's my IP」のWeb検索を実行することで確認できます。リモートIDは、サイトのルータのWAN IPアドレスです。

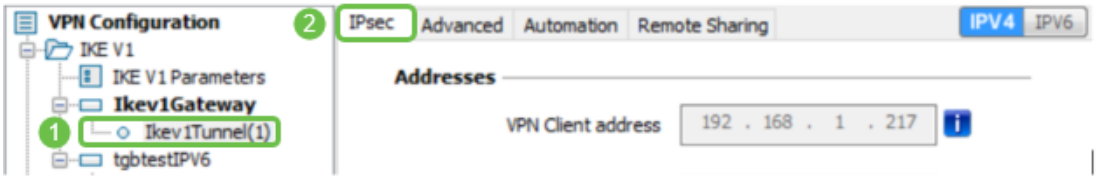


ステップ18:[Configuration]をクリックし、[Save]を選択します。



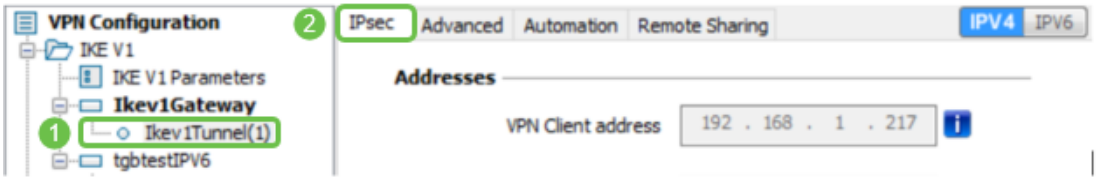
トンネル設定の設定

ステップ1:[IKev1Tunnel(1)](自分の名前が異なる場合があります)と[IPsec]タブをクリックします。Ikev1Gatewayの詳細設定で[Mode Config]を選択すると、VPN Clientアドレスが自動的に入力されます。これにより、リモートの場所にあるコンピュータ/ラップトップのローカルIPアドレスが表示されます。



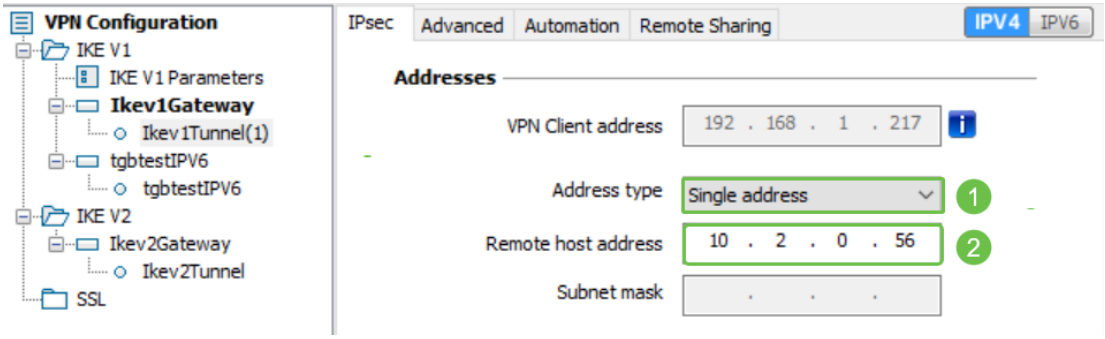
ステップ2:[Address type]ドロップダウンリストから、VPN Clientがアクセスできるアドレスの種

*類*を選択します。これは、単一のアドレス、アドレスの範囲、またはサブネットアドレスです。デフォルトのサブネットアドレスには、VPN Clientアドレス（コンピュータのローカルIPアドレス）、リモートLANアドレス、サブネットマスクが自動的に含まれます。[Single address]または[Range of addresses]を選択した場合、これらのフィールドには手動で入力する必要があります。VPNトンネルからアクセスするネットワークアドレスを*Remote LAN address*フィールドに入力し、リモートネットワークのサブネットマスクをSubnet maskフィールドに入力します。

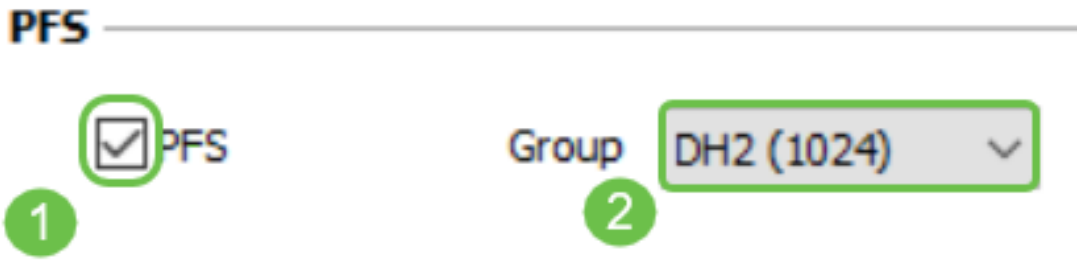


注：この例では、[Single address]が選択され、サイトのルータのローカルIPアドレスが入力されています。

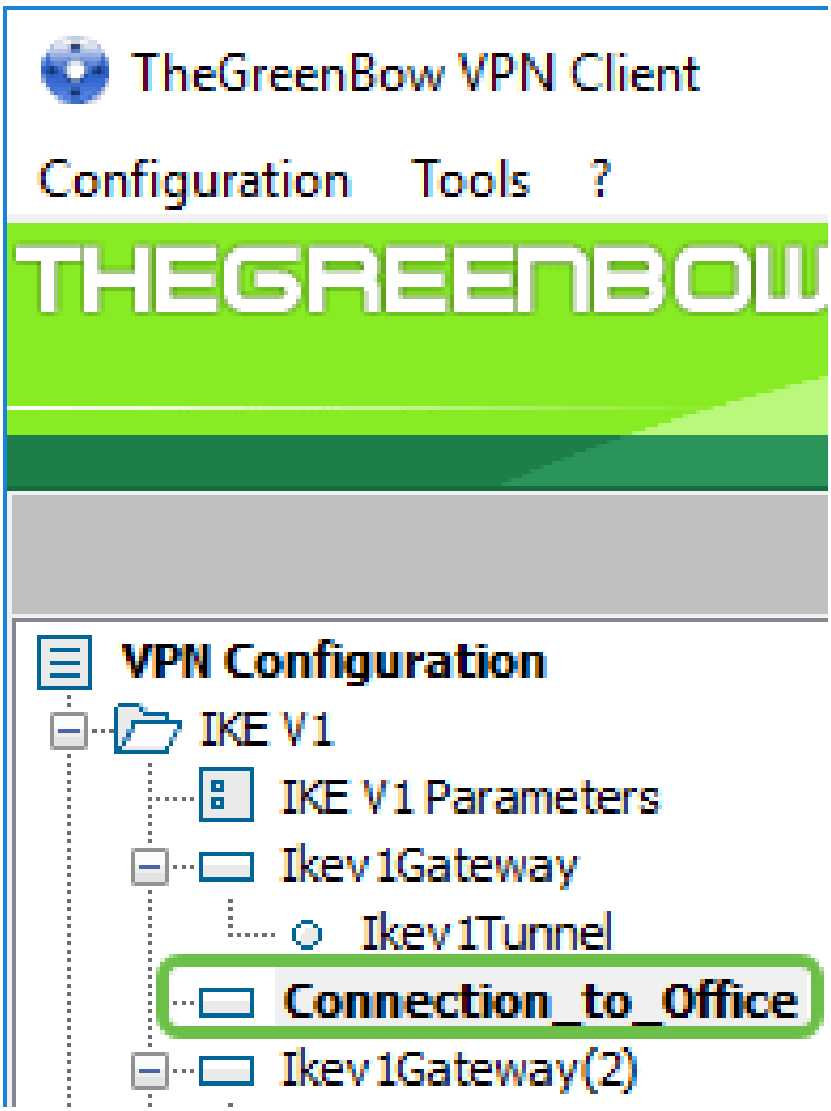
ステップ3:[ESP] で、サイト（オフィス）のVPNゲートウェイの設定と一致するように[Encryption]、[Authentication]、および[Mode]を設定します。



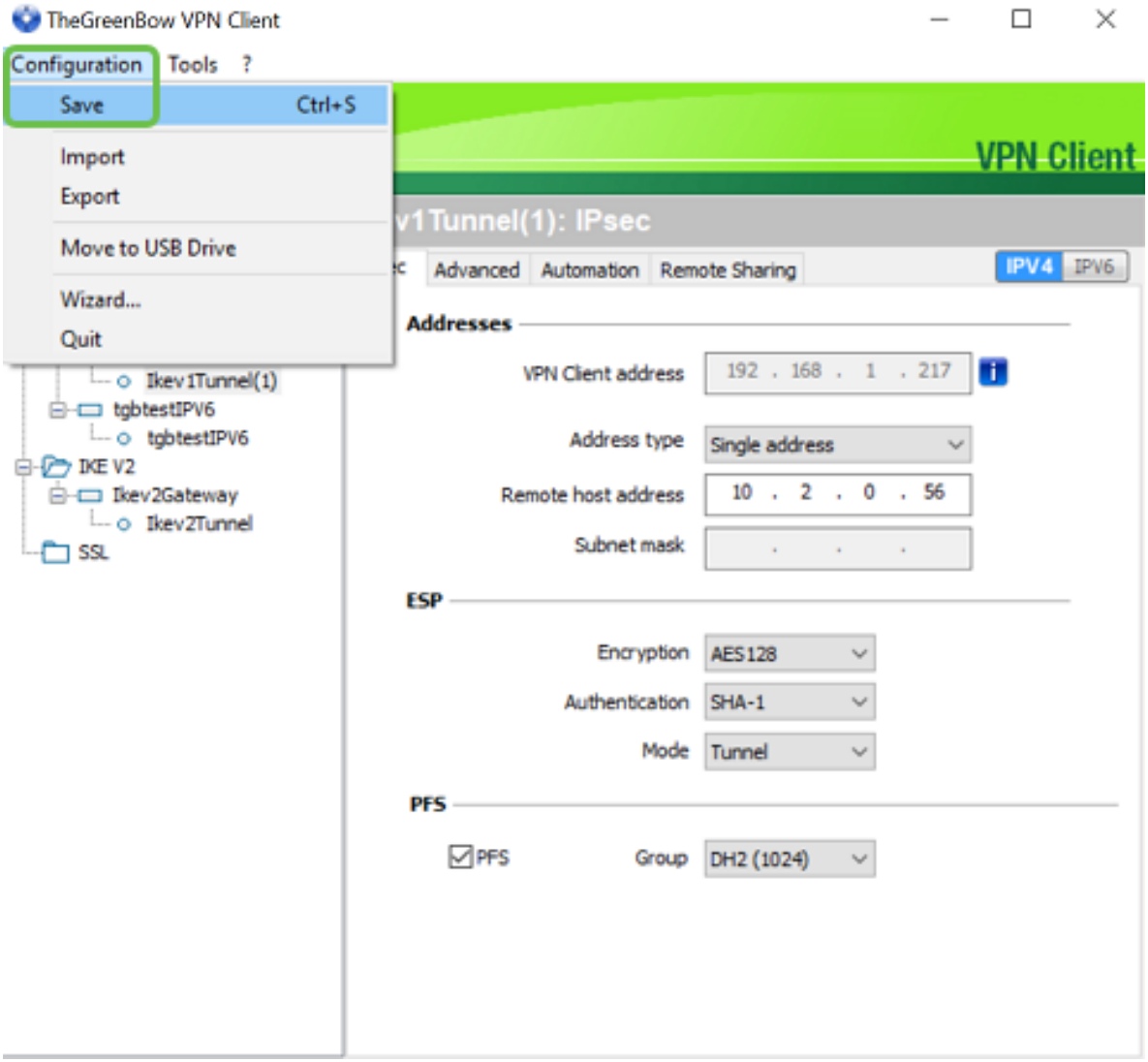
ステップ4:（オプション）PFSの下で*PFS*チェックボ**ックスをオン**にして、Perfect Forward Secrecy(PFS)を有効にします。PFSは、セッションを暗号化するためのランダム・キーを生成します。[グループ]ドロップダウンリストからPFSグループ設定を選択します。ルータで有効になっている場合は、ここでも有効にする必要があります。



ステップ5:（オプション）Ikev1Gatewayの名前を右クリックし、名前を変更する場合は名前の変更セクションをクリックします。



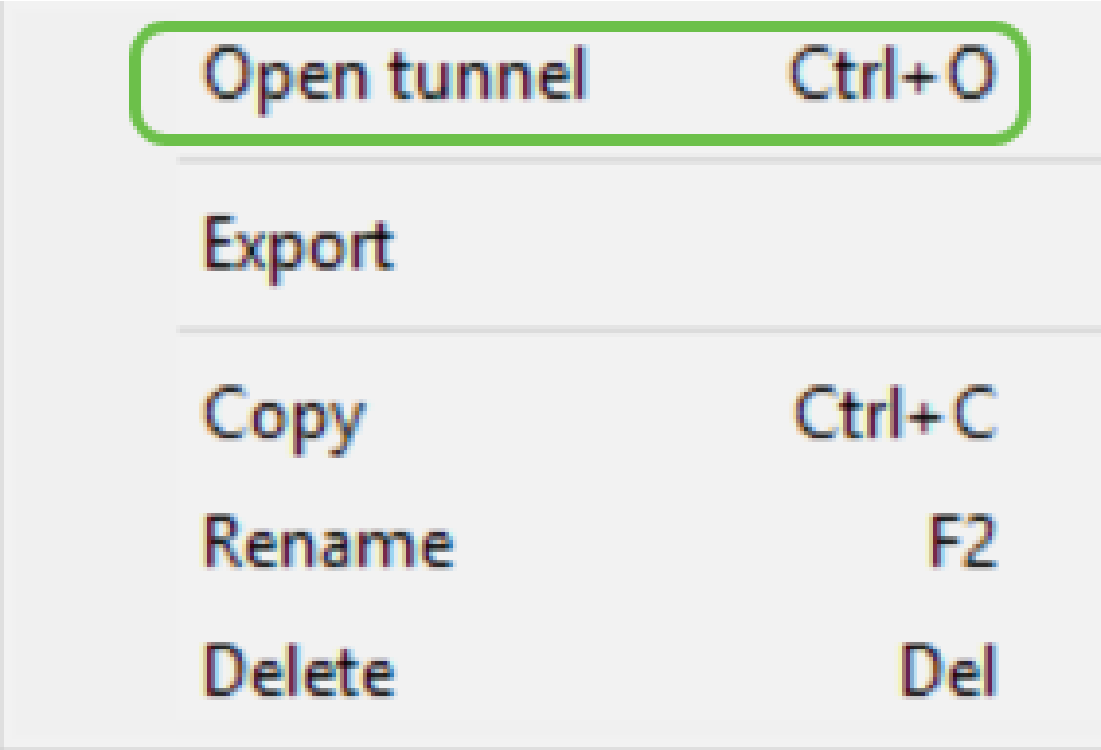
ステップ6:[Configuration]をクリックし、[Save]を選択します。



これで、VPN経由でRV160またはRV260ルータに接続するようにTheGreenBow VPN Clientが正しく設定されたはずです。

クライアントとしてのVPN接続の開始

ステップ1:TheGreenBowが開いているため、トンネルを右クリックして[Open Tunnel]を選択して、**接続を開始できます**。

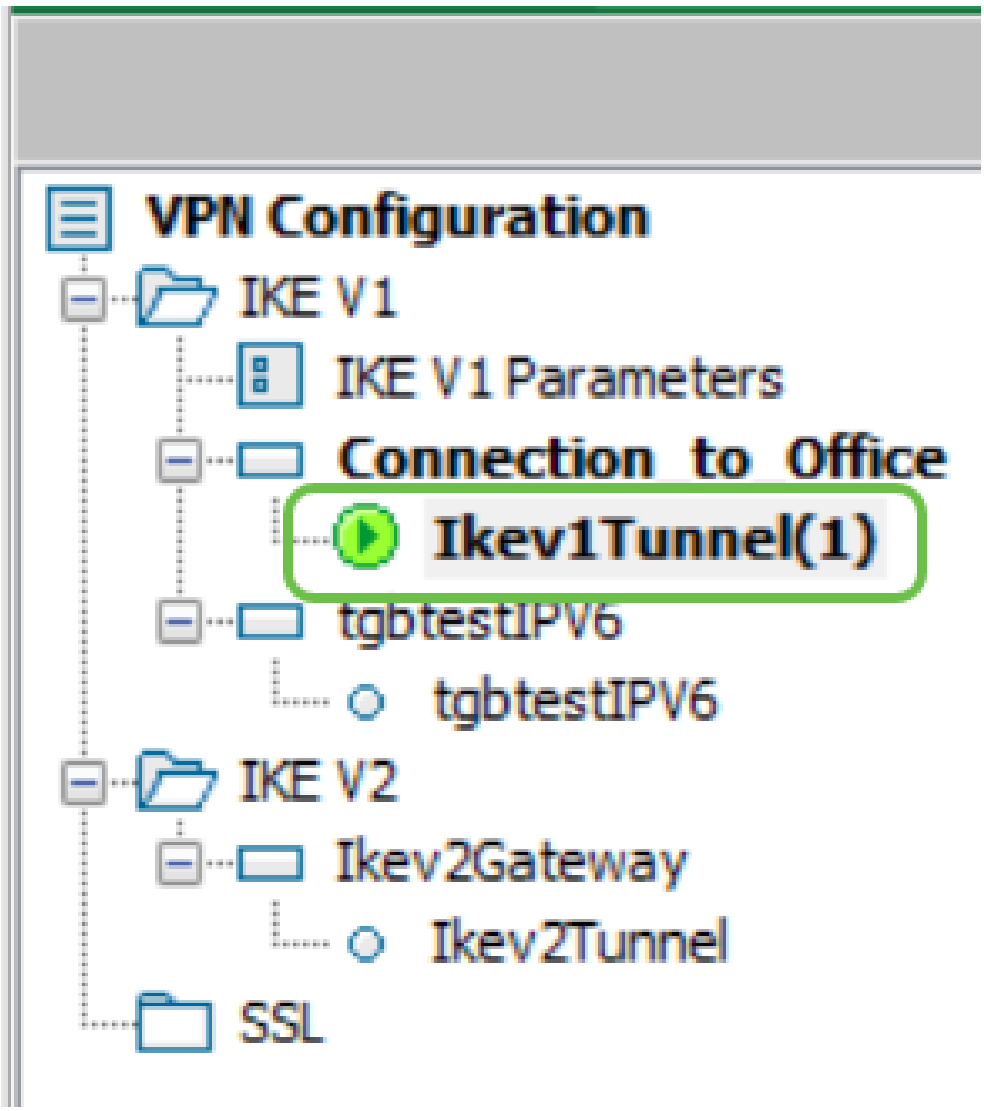


注：トンネルをダブルクリックしてトンネルを開くこともできます。

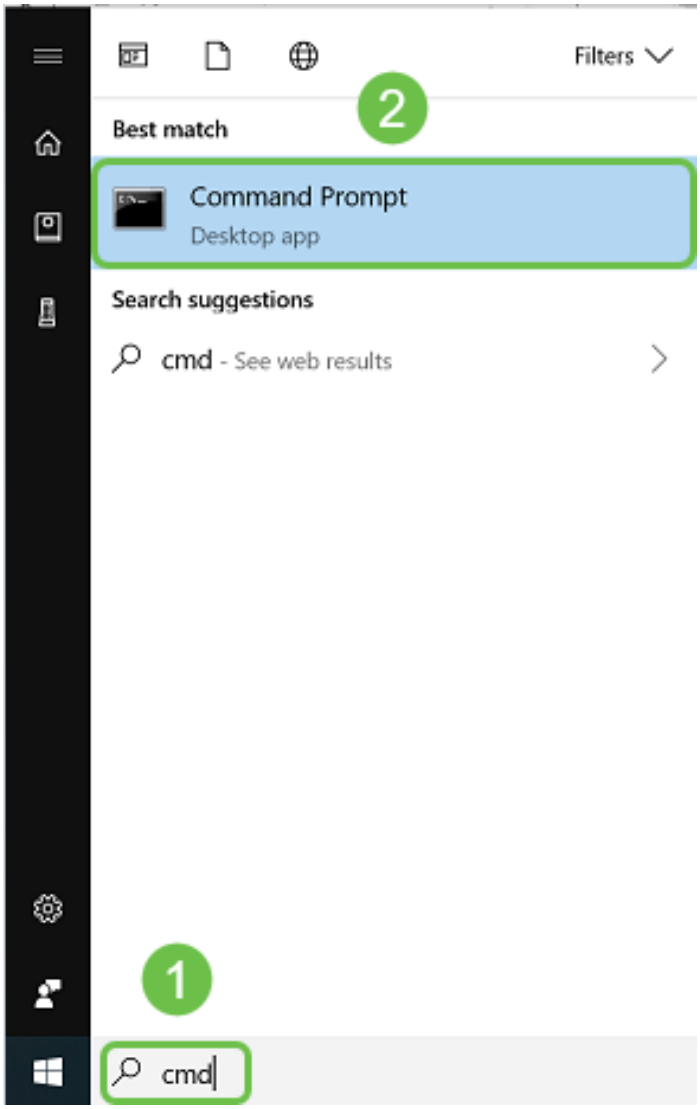
ステップ2: (オプション) 新しいセッションを開始し、TheGreenBowを閉じた場合は、画面の右側にある**GreenBow VPN Clientアイコンをクリックします**。

ステップ3:（オプション）このステップは、新しいセッションを設定し、ステップ2に従う場合にのみ必要です。使用する必要がある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。

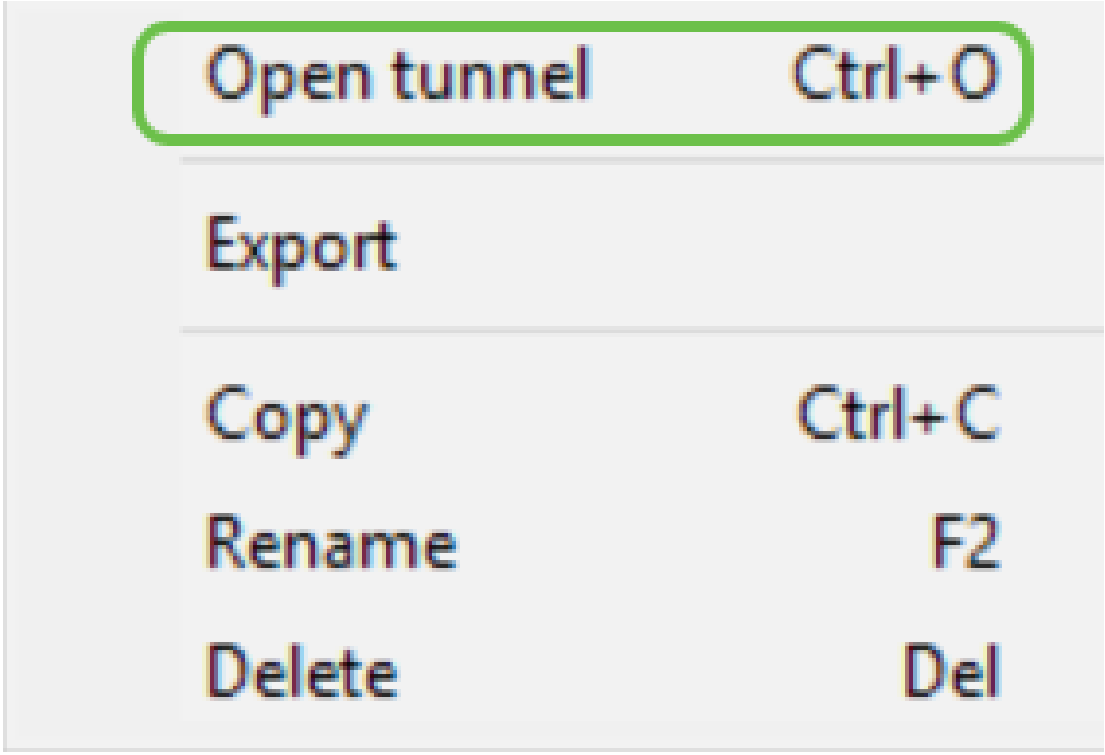
ステップ4：トンネルが接続されると、トンネルの横に緑色の円が表示されます。感嘆符(!)が表示された場合は、それをクリックしてエラーを検索できます。



ステップ5: (オプション) 接続されていることを確認するには、クライアントコンピュータからコマンドプロンプトにアクセスします。



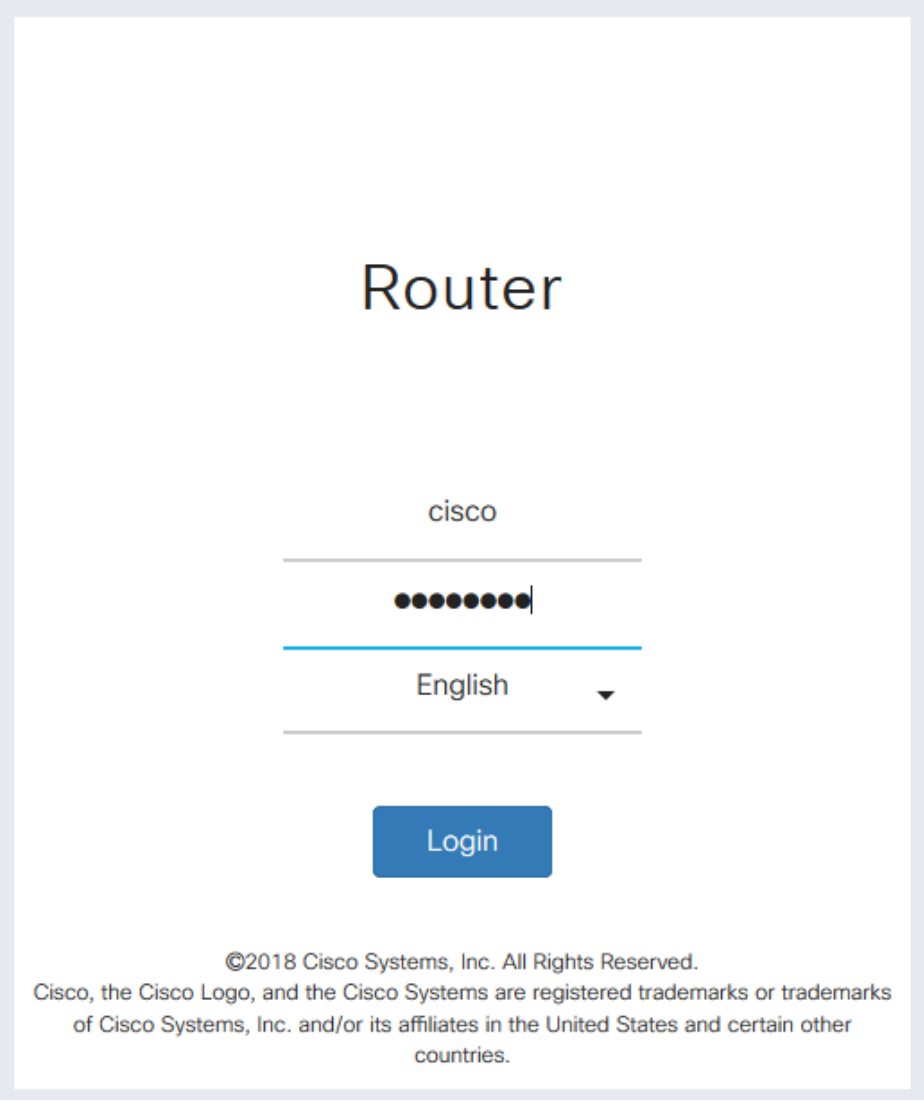
ステップ6: (オプション) サイトでpingを入力し、ルータのプライベートLAN IPアドレスを入力します。返信を受信した場合は、接続しています。



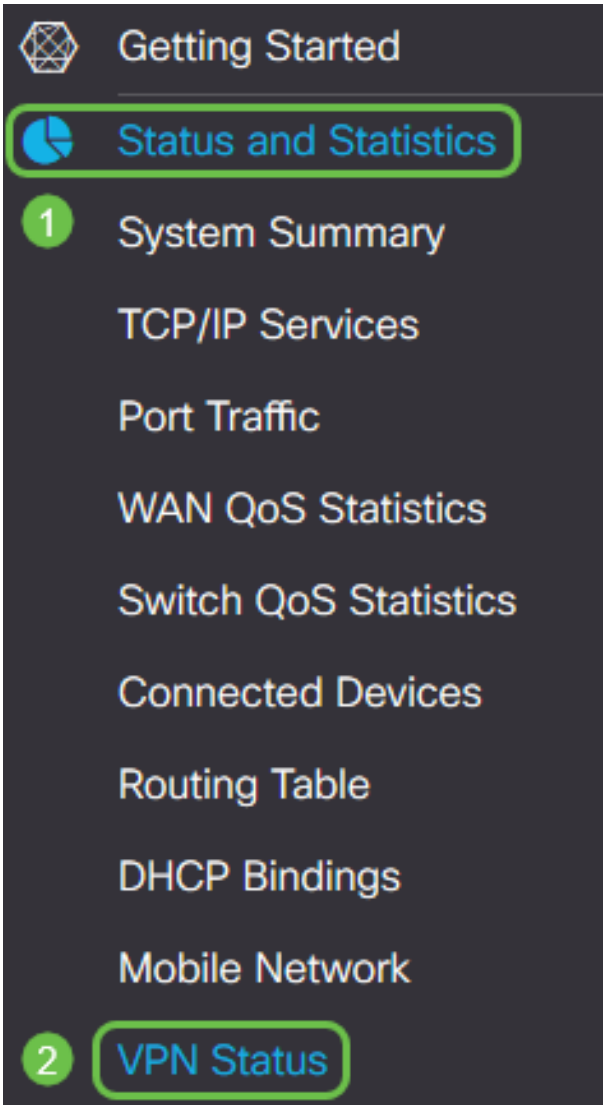
VPNステータスの確認

サイトでのVPNステータスの確認

ステップ1:RV160またはRV260の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]の順に選択します。

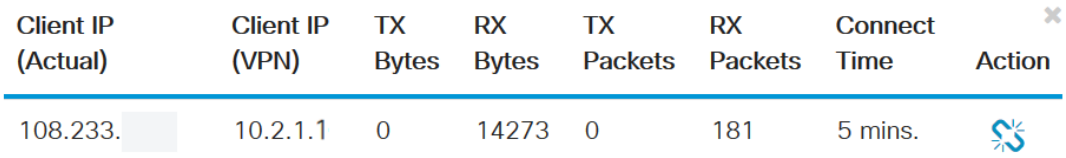


ステップ3:[Client-to-*Site Tunnel Status*]で、*接続*テーブルの[*Connections*]列を確認します。確認されたVPN接続が表示されます。

ステップ4：目のアイコンをクリックして、詳細を確認します。

ステップ5：クライアントとサイト間のVPNステータスの詳細を次に示します。クライアントのWAN IPアドレス、セットアップ時に設定されたアドレスプールから割り当てられたローカルIPアドレスが表示されます。また、送受信されたバイトとパケット、および接続時間も表示されます

。クライアントを切断する場合は、[Action]の下の青い壊れたチェーン**アイコン**をクリックします。検査後に閉**じるには**、右上隅のxをクリックします。



Client IP (Actual)	Client IP (VPN)	TX Bytes	RX Bytes	TX Packets	RX Packets	Connect Time	Action
108.233.	10.2.1.1	0	14273	0	181	5 mins.	

結論

これで、RV160またはRV260ルータのVPN接続が正常にセットアップおよび確認され、VPN経由でルータに接続するようにTheGreenBow VPN Clientが設定されているはずです。