RV320およびRV325 VPNルータシリーズでのゲートウェイからゲートウェイへの仮想プライベートネットワーク(VPN)の設定

目的

VPNは、パブリックまたは共有インターネットを介して、いわゆるVPNトンネルを介して、2つのエンドポイントで非常にセキュアな接続を形成するために使用されます。より具体的には、ゲートウェイ間VPN接続では、2台のルータが互いに安全に接続し、一方の端のクライアントが論理的には他方の端の同じリモートネットワークの一部として認識されます。これにより、インターネット経由でデータとリソースをより簡単かつ安全に共有できます。ゲートウェイ間VPN接続を正常に確立するには、接続の両側で設定を行う必要があります。この記事の目的は、RV32x VPNルータシリーズでのゲートウェイ間VPN接続の設定をガイドすることです。

該当するデバイス

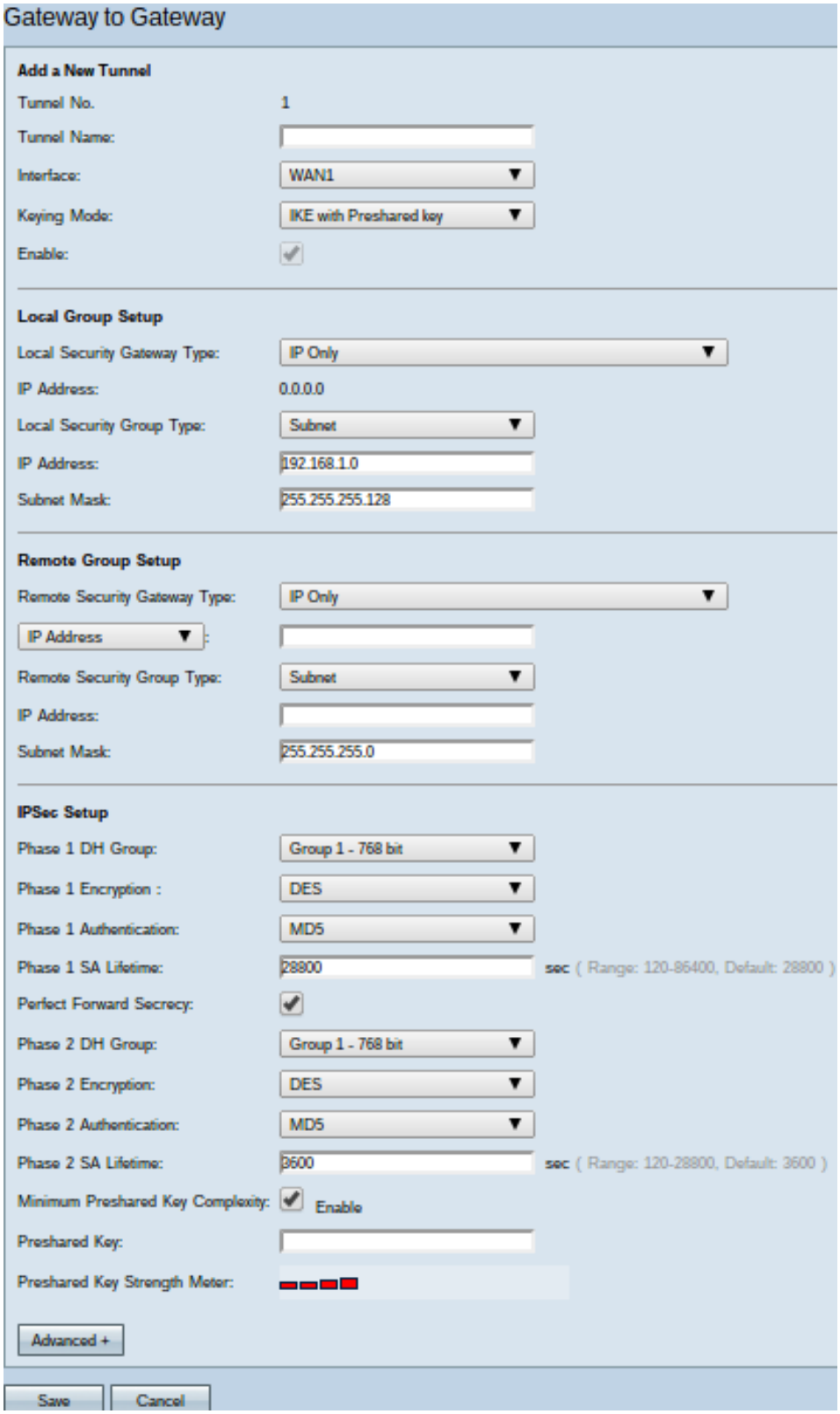
- RV320デュアルWAN VPNルータ
- RV325ギガビットデュアルWAN VPNルータ

[Software Version]

- v1.1.0.09

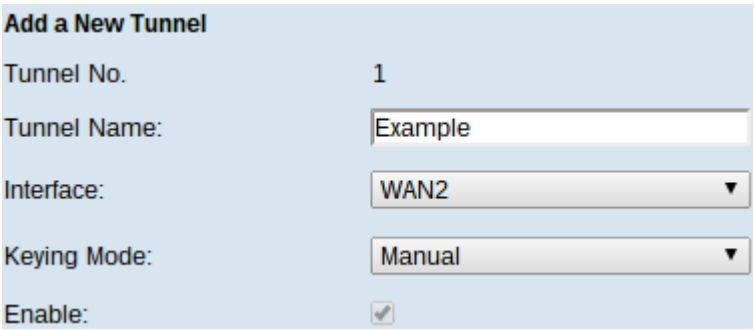
ゲートウェイ間

ステップ1:Webコンフィギュレーションユーティリティにログインし、[VPN] > [Gateway to Gateway]を選択します。「ゲートウェイからゲートウェイ」ページが開きます。



VPN接続が正常に動作するには、接続の両側のInternet Protocol Security(IPSec)値が同じである必要があります。接続の両側が異なるローカルエリアネットワーク(LAN)に属し、少なくとも1つのルータがスタティックIPアドレスまたはダイナミックDNSホスト名で識別できる必要があります。

新しいトンネルの追加



・トンネル番号 – 作成される現在のトンネルを表示します。ルータは100のトンネルをサポートします。

ステップ1:[Tunnel Name]フィールドにVPNトンネルの名前を入力します。トンネルのもう一方の端で使用される名前と一致する必要はありません。

ステップ2:[Interface]ドロップダウンリストから、トンネルに使用するワイドエリアネットワーク(WAN)ポートを選択します。

・ WAN1：ルータの専用WANポート。

・ WAN2：ルータのWAN2/DMZポート。WANとして設定されており、非武装地帯(DMZ)ポートではない場合にのみ、ドロップダウンメニューに表示されます。

・ USB1 – ルータのUSB1ポート。ポートに3G/4G/LTE USBドングルが接続されている場合にのみ動作します。

・ USB2 – ルータのUSB2ポート。ポートに3G/4G/LTE USBドングルが接続されている場合にのみ動作します。

ステップ3:[Keying Mode]ドロップダウンリストから、使用するトンネルセキュリティを選択します。

・ Manual：このオプションを使用すると、キーをVPN接続の反対側とネゴシエートする代わりに、キーを手動で設定できます。

・ IKE with Preshared key:VPNトンネルでセキュリティアソシエーションを設定するInternet Key Exchange Protocol(IKE)を有効にするには、このオプションを選択します。IKEは事前共有キーを使用してリモートピアを認証します。

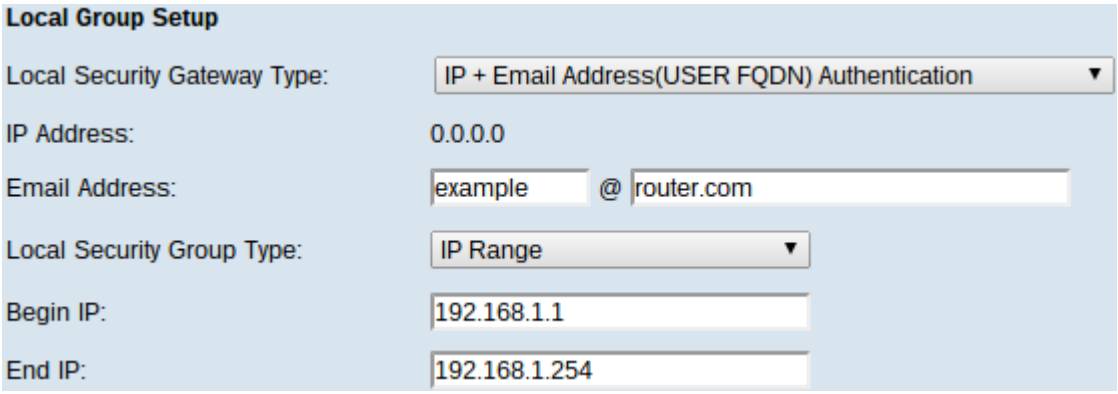
・ IKE with Certificate：事前共有キーを自動的に生成して交換し、より安全な方法でトンネルの認証済みの安全な通信を確立する、証明書を使用したインターネットキー交換(IKE)プロトコルを有効にするには、このオプションを選択します。

ステップ4:[Enable]チェックボックスをオンにして、VPNトンネルを有効にします。デフォルトでは有効になっています。

ローカルグループの設定

これらの設定は、VPNトンネルの反対側にあるルータの「Remote Group Setup」設定と一致している必要があります。

注：「ステップ1から開始する新しいトンネルの追加」のステップ3のKeying Modeドロップダウンリストから**Manual**または**IKE with Preshared key**が選択されている場合は、ステップ2 ~ 4をスキップします。



ステップ1:[Local Security Gateway Type]ドロップダウンリストから、VPNトンネルを確立するルータを識別する方法を選択します。

・ IP Only：トンネルへのアクセスは、スタティックWAN IPからのみ可能です。このオプションは、ルータだけにスタティックWAN IPがある場合に選択できます。スタティックWAN IPアドレスは、自動生成されたフィールドです。

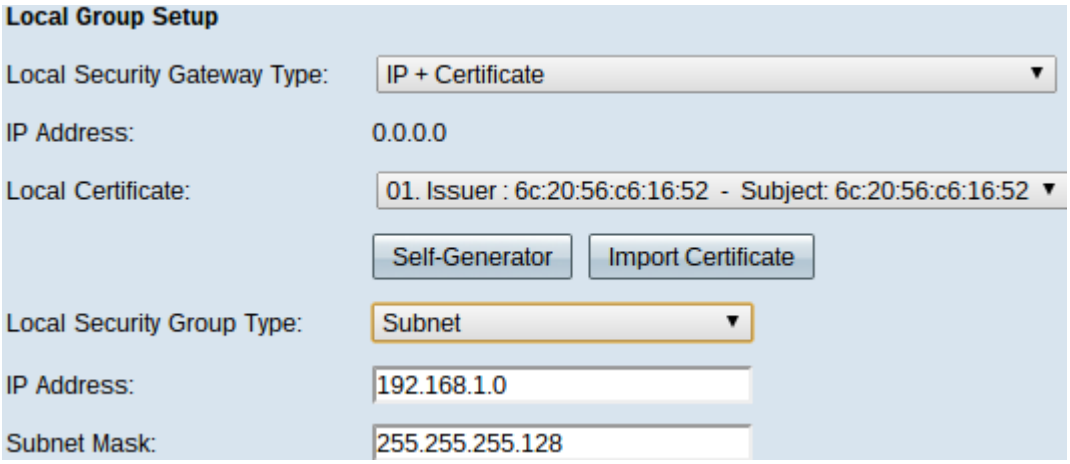
・ IP +ドメイン名(FQDN)認証：トンネルへのアクセスは、スタティックIPアドレスと登録済みドメインを使用して可能です。このオプションを選択した場合は、[Domain Name]フィールドに登録済みドメインの名前を入力します。スタティックWAN IPアドレスは、自動生成されたフィールドです。

・ IP + E-mail Addr(USER FQDN)認証：静的IPアドレスと電子メールアドレスを使用してトンネルにアクセスできます。このオプションを選択した場合は、[Email Address]フィールドに電子メールアドレスを入力します。スタティックWAN IPアドレスは、自動生成されたフィールドです。

・ダイナミックIP +ドメイン名(FQDN)認証：トンネルへのアクセスは、ダイナミックIPアドレスと登録済みドメインを通じて可能です。このオプションを選択した場合は、[Domain Name]フィールドに登録済みドメインの名前を入力します。

・ Dynamic IP + Email Addr(USER FQDN)認証：トンネルへのアクセスは、ダイナミックIPアドレスと電子メールアドレスを使用して可能です。このオプションを選択した場合は、[Email Address]フィールドに電子メールアドレスを入力します。

注：証明書を使用したIKEを使用する場合、[Local Group Setup]領域で次の変更が行われます。



[ローカルセキュリティゲートウェイタイプ(Local Security Gateway Type)]ドロップダウンリストが編集できなくなり、[IP + Certificate]が表示されます。これは、トンネルを使用できるLANリソースです。

[IP Address]フィールドには、デバイスのWAN IPアドレスが表示されます。ユーザは編集できません。

ステップ2:[Local Certificate]ドロップダウンリストから証明書を選択します。証明書は、VPN接続の認証セキュリティを強化します。

ステップ3:（オプション）[Self-**Generator]ボタンをクリック**し、[Certificate Generator]ウィンドウを表示して証明書を構成および生成します。

ステップ4:（オプション）[証明書のインポー**ト]ボタンをクリ**ックし、[証明書のマイズ]ウィンドウを表示して証明書を表示します。

ステップ5:[Local Security Group Type]ドロップダウンリストから、次のいずれかを選択します。

- IP Address：このオプションでは、このVPNトンネルを使用できるデバイスを1つ指定できます。デバイスのIPアドレスを[IP address]フィールドに入力するだけで済みます。

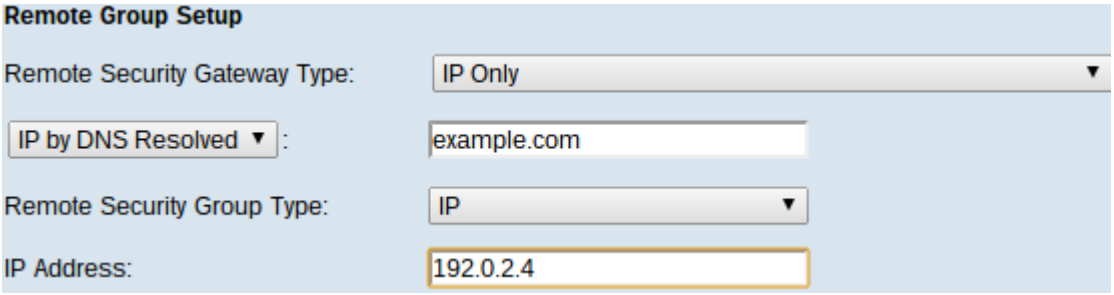
- サブネット：同じサブネットに属するすべてのデバイスがVPNトンネルを使用できるようにするには、このオプションを選択します。[IP Address]フィールドにネットワークIPアドレスを、[Subnet Mask]フィールドにそれぞれのサブネットマスクを入力する必要があります。

- IP Range:VPNトンネルを使用できるデバイスの範囲を指定するには、このオプションを選択します。[Begin IP]フィールドと[End IP]フィールドに、デバイス範囲の最初のIPアドレスと最後のIPアドレスを入力する必要があります。

リモートグループの設定

これらの設定は、VPNトンネルの反対側にあるルータの[Local Group Setup]設定と一致している必要があります。

注：「新しいトンネルの追加」のステップ3のKeying Modeドロップダウンリストから ManualまたはIKE with Preshared keyを選択した場合は、ステップ1から開始し、ステップ2から5をスキップします。または、証明書を指定したIKEを選択した場合は、ステップ1をスキップします。



ステップ1:[Remote Security Gateway Type]ドロップダウンリストから、VPNトンネルを確立する他のルータを識別する方法を選択します。

- IP Only：トンネルへのアクセスは、スタティックWAN IPからのみ可能です。リモートルータのIPアドレスがわかっている場合は、[Remote Security Gateway Type]フィールドのすぐ下のドロップダウンリストで[IP address]を選択し、アドレスを入力します。IPアドレスがわからないがドメイン名がわかっている場合は[IP by DNS Resolved]を選択し、ルータのドメイン名を[IP by DNS Resolved]フィールドに入力します。

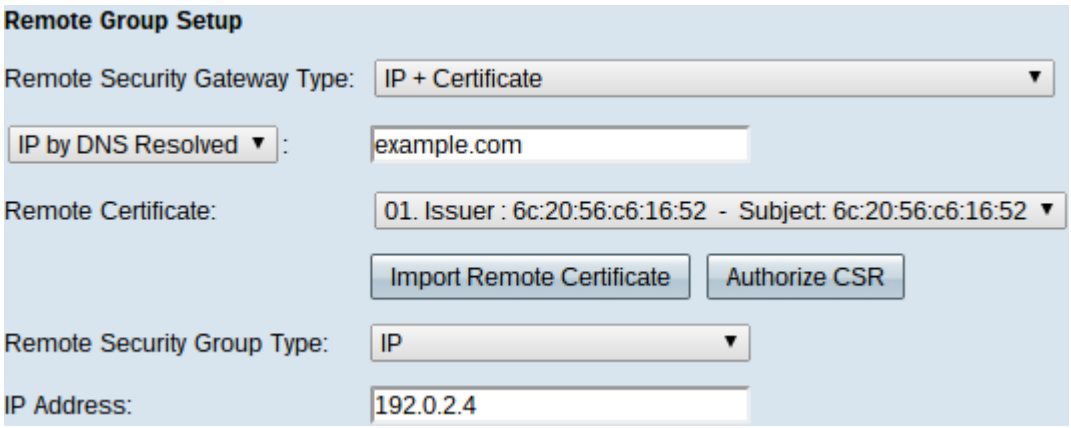
・ IP +ドメイン名(FQDN)認証：トンネルへのアクセスは、スタティックIPアドレスとルータの登録済みドメインを使用して可能です。リモートルータのIPアドレスがわかっている場合は、[Remote Security Gateway Type]フィールドのすぐ下のドロップダウンリストで[IP address]を選択し、アドレスを入力します。IPアドレスがわからないがドメイン名がわかっている場合は[IP by DNS Resolved]を選択し、ルータのドメイン名を[IP by DNS Resolved]フィールドに入力します。このオプションを選択した場合は、[Domain Name]フィールドに登録済みドメインの名前を入力します。

・ IP + Email Addr(USER FQDN)認証：静的IPアドレスと電子メールアドレスを使用してトンネルにアクセスできます。リモートルータのIPアドレスがわかっている場合は、Remote Security Gateway Typeフィールドのすぐ下のドロップダウンリストでIPアドレスを選択し、アドレスを入力します。IPアドレスがわからないがドメイン名がわかっている場合は[IP by DNS Resolved]を選択し、ルータのドメイン名を[IP by DNS Resolved]フィールドに入力します。[Email Address]フィールドに電子メールアドレスを入力します。

・ダイナミックIP +ドメイン名(FQDN)認証：トンネルへのアクセスは、ダイナミックIPアドレスと登録済みドメインを通じて可能です。このオプションを選択した場合は、[Domain Name]フィールドに登録済みドメインの名前を入力します。

・ Dynamic IP + Email Addr(USER FQDN)認証：トンネルへのアクセスは、ダイナミックIPアドレスと電子メールアドレスを使用して可能です。このオプションを選択した場合は、[Email Address]フィールドに電子メールアドレスを入力します。
注：両方のルータにダイナミックIPアドレスがある場合は、両方のゲートウェイに[ダイナミックIP + Eメールアドレス(Dynamic IP + E-Mail Address)]を選択しないでください。

注：証明書を使用してIKEを操作する場合、[Remote Group Setup]領域の[Following changes]が変更されます。



[リモートセキュリティゲートウェイタイプ(Remote Security Gateway Type)]ドロップダウンリストが編集できなくなり、[IP + Certificate]が表示されます。これは、トンネルを使用できるLANリソースです。

ステップ2：リモートルータのIPアドレスがわかっている場合は、[Remote Security Gateway Type]フィールドのすぐ下のドロップダウンリストで[IP address]を選択し、アドレスを入力します。IPアドレスが不明で、ドメイン名が不明な場合は[IP by DNS Resolved]を選択し、リモートルータのドメイン名を[IP by DNS Resolved]フィールドに入力します

ステップ3:[Remote Certificate]ドロップダウンリストから証明書を選択します。証明書は、VPN接続の認証セキュリティを強化します。

ステップ4:（オプション）新しい証明書をインポートするには、**[Import Remote Certificate]ボタン**をクリックします。

ステップ5:（オプション）[Authorize CSR]ボタンをクリックして、デジタル署名要求のある証明書を識別します。

ステップ6:[Local Security Group Type]ドロップダウンリストから、次のいずれかを選択します。

・ IP Address：このオプションでは、このVPNトンネルを使用できるデバイスを1つ指定できます。デバイスのIPアドレスを[IP address]フィールドに入力するだけで済みます。

・サブネット：同じサブネットに属するすべてのデバイスがVPNトンネルを使用できるようにするには、このオプションを選択します。[IP Address]フィールドにネットワークIPアドレスを、[Subnet Mask]フィールドにそれぞれのサブネットマスクを入力する必要があります。

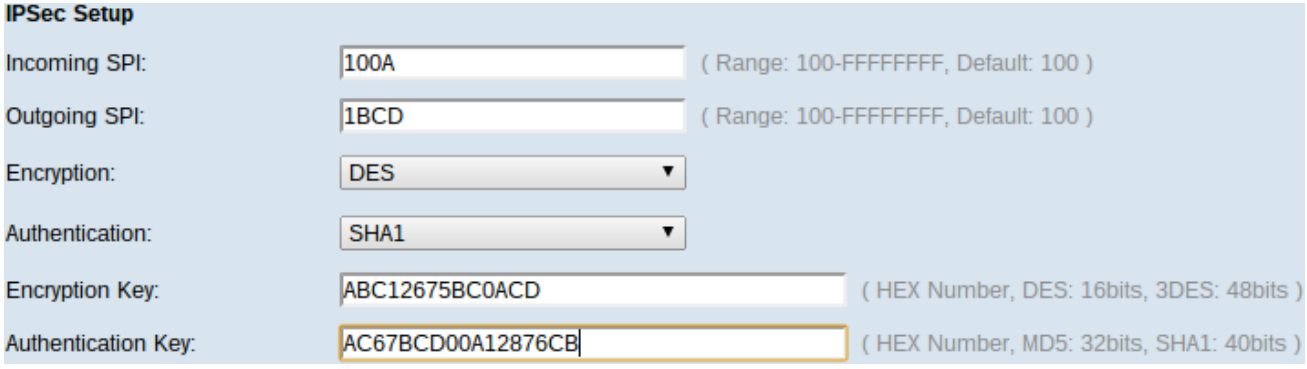
・ IP Range:VPNトンネルを使用できるデバイスの範囲を指定するには、このオプションを選択します。デバイスの範囲の最初のIPアドレスと最後のIPアドレスを入力する必要があります。[Begin IP]フィールドと[End IP]フィールド

IPSecの設定

VPNトンネルの両端の間で暗号化を正しく設定するには、両方の設定が完全に同じである必要があります。この場合、IPSecは2つのデバイス間にセキュアな認証を作成します。これは2つのフェーズで行われます。

手動キーイングモードのためのIPSecセットアップ

[Add a New Tunnel]のステップ3の[Keying Mode]ドロップダウンリストから[Manual]が選択されている場合にのみ使用できます。これは、新しいセキュリティキーを自分で生成し、キーとのネゴシエーションを行わないカスタムセキュリティモードです。トラブルシューティングや小規模なスタティック環境で使用するのが最適です。



ステップ1:[Incoming SPI]フィールドに、着信セキュリティパラメータインデックス(SPI)の一意の16進値を入力します。SPIはEncapsulating Security Payload(ESP)Protocol(ESP)ヘッダー内で伝送され、ともに着信パケットの保護を決定します。100 ~ FFFFFFFFの範囲で入力できます。

ステップ2:[発信SPI(Outgoing SPI)]フィールドにSPIの一意の16進数値を入力します。SPIは、発信パケットの保護を決定するESPヘッダーで一緒に伝送されます。100 ~ FFFFFFFFの範囲で入力できます。

注：トンネルを確立するには、着信SPIと発信SPIが両端で一致している必要があります。

ステップ3:[Encryption]ドロップダウンリストから適切な暗号化方式を選択します。推奨される暗号化は3DESです。VPNトンネルは、両端で同じ暗号化方式を使用する必要がありま

す。

・ DES — DES(Data Encryption Standard)は、56ビットの古い、より下位互換性があり、暗号化の方式であり、セキュリティが低く、破りやすい方式です。

・ 3DES — 3DES(Triple Data Encryption Standard)は168ビットの簡単な暗号化方式で、DESよりもセキュリティが高いデータを3回暗号化することで、キーサイズを大きくします。

ステップ4:[Authentication]ドロップダウンリストから適切な認証方式を選択します。推奨される認証はSHA1です。VPNトンネルは、両端で同じ認証方式を使用する必要があります。

・ MD5 — MD5 (Message Digest Algorithm-5)は、チェックサム計算による悪意のある攻撃からデータを保護する32桁の16進数ハッシュ関数を表します。

・ SHA1 — SHA1（セキュアハッシュアルゴリズムバージョン1）は、MD5よりも安全な160ビットのハッシュ関数です。

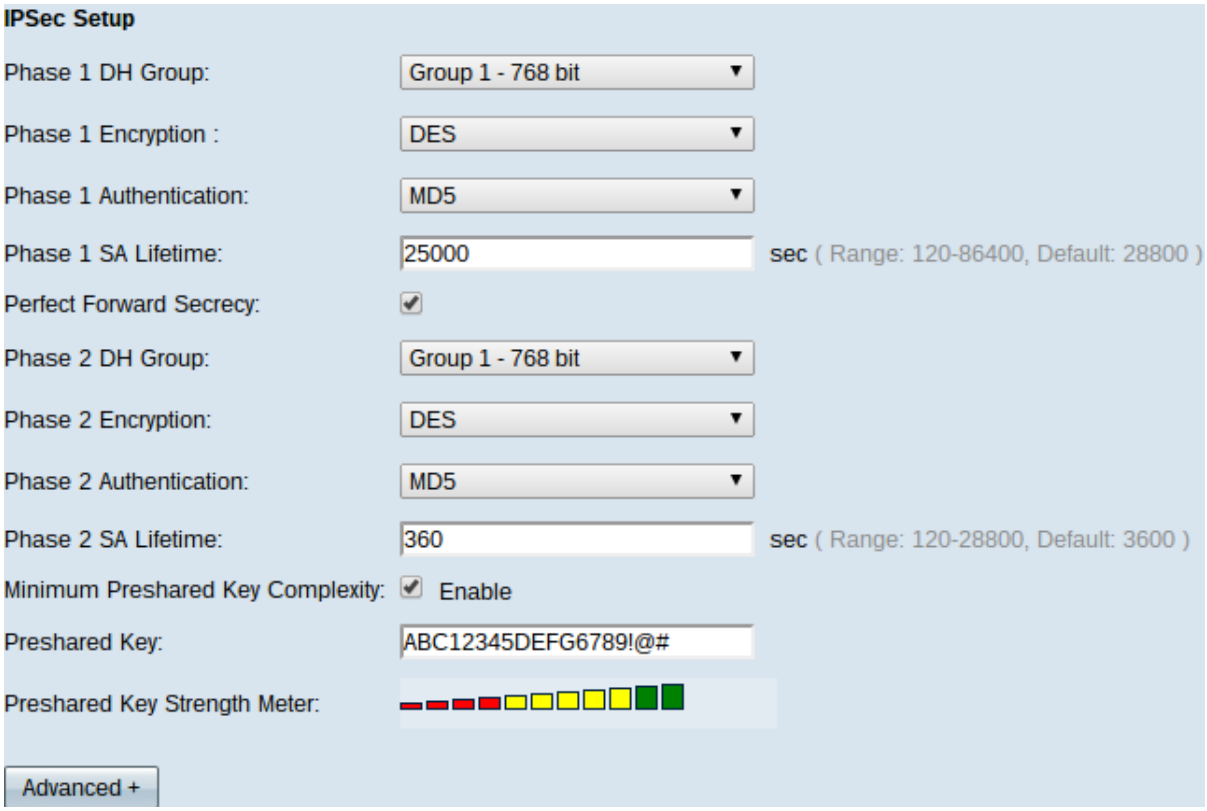
ステップ5:[Encryption Key]フィールドに、データを暗号化および復号化するキーを入力します。ステップ3で暗号化方式としてDESを選択した場合は、16桁の16進数値を入力します。ステップ3で暗号化方式として3DESを選択した場合は、40桁の16進数値を入力します。

ステップ6:[Authentication Key]フィールドに、トラフィックを認証するための事前共有キーを入力します。ステップ4で認証方式として[MD5]を選択した場合は、32桁の16進数値を入力します。ステップ4で認証方式として[SHA]を選択した場合は、40桁の16進数値を入力します。VPNトンネルは、両端で同じ事前共有キーを使用する必要があります。

ステップ7:[Save]をクリックして設定を保存します。

事前共有キーを使用したIKEのIPSecセットアップ

事前共有キーを持つIKEが、『新しいトンネルの追加』のステップ3の[キーイングモード(Keying Mode)]ドロップダウンリストから選択されている場合にのみ使用できます。



ステップ1:[Phase 1 DH Group]ドロップダウンリストから適切なフェーズ1 DHグループを選択します。フェーズ1は、セキュアな認証通信をサポートするために、トンネルの両端の間にシンプレックス論理セキュリティアソシエーション(SA)を確立するために使用されます。Diffie-Hellman(DH)は、フェーズ1の接続中に通信を認証するために秘密キーを共有するために使用される暗号鍵交換プロトコルです。

・グループ1 - 768ビット：最高強度キーと最もセキュアな認証グループを表します。IKEキーを計算する時間が長くなる。ネットワークの速度が高い場合に推奨されます。

・グループ2 - 1024ビット：強度の高いキーとよりセキュアな認証グループを表します。IKEキーの計算には時間が必要です。

・グループ5 - 1536ビット：最小強度キーと最も安全でない認証グループを表します。IKEキーを計算する時間が短縮されます。ネットワークの速度が低い場合に推奨されます。

ステップ2:[Phase 1 Encryption]ドロップダウンリストから、適切なフェーズ1暗号化を選択してキーを暗号化します。AES-128、AES-192、またはAES-256が推奨されます。VPNトンネルは、両端で同じ暗号化方式を使用する必要があります。

・ DES:Data Encryption Standard（DES；データ暗号規格）は、56ビットの古い暗号化方式であり、現在の世界ではあまり安全な暗号化方式ではありません。

・ 3DES — Triple Data Encryption Standard(3DES)は168ビットの簡単な暗号化方式で、DESよりもセキュリティが高いデータを3回暗号化することでキーサイズを大きくします。

・ AES-128：高度暗号化規格(AES)は、プレーンテキストを10サイクルの繰り返しで暗号テキストに変換する128ビットの暗号化方式です。

・ AES-192：プレーンテキストを12サイクルの繰り返しで暗号テキストに変換する192ビットの暗号化方式。

・ AES-256：プレーンテキストを14サイクルの繰り返しで暗号テキストに変換する256ビットの暗号化方式。

ステップ3:[Phase 1 Authentication]ドロップダウンリストから適切な認証方式を選択します。VPNトンネルは、両端で同じ認証方式を使用する必要があります。SHA1が推奨されます。

・ MD5:Message Digest Algorithm-5(MD5)は、チェックサム計算による悪意のある攻撃からデータを保護する32桁の16進数ハッシュ関数を表します。

・ SHA1:MD5よりも安全な160ビットのハッシュ関数。

ステップ4:[Phase 1 SA Life Time]フィールドに、VPNトンネルがアクティブなままである時間（秒）を入力します。

ステップ5:[Perfect Forward Secrecy]チェックボックスをオンにして、キーに対する保護を強化します。このオプションを使用すると、キーが侵害された場合に新しいキーを生成できます。暗号化されたデータは、侵害されたキーによってのみ侵害されます。そのため、キーが侵害されても他のキーを保護するため、より安全で認証された通信を提供します。これは、セキュリティを強化するために推奨されるアクションです。

ステップ6:[Phase 2 DH Group]ドロップダウンリストから適切なフェーズ2 DHグループを選択します。フェーズ1は、セキュアな認証通信をサポートするために、トンネルの両端の間にシンプレックス論理セキュリティアソシエーション(SA)を確立するために使用されます。DHは、フェーズ1接続時に通信を認証するために秘密キーを共有するために使用される暗号キー交換プロトコルです。

・グループ1 - 768ビット：最高強度キーと最もセキュアな認証グループを表します。IKEキーを計算する時間が長くなる。ネットワークの速度が高い場合に推奨されます。

・グループ2 - 1024ビット：強度の高いキーとよりセキュアな認証グループを表します。IKEキーの計算には時間が必要です。

・グループ5 - 1536ビット：最小強度キーと最も安全でない認証グループを表します。IKEキーを計算する時間が短縮されます。ネットワークの速度が低い場合に推奨されます。

注：新しいキーは生成されないため、ステップ5で[Perfect Forward Secrecy]のチェックを外した場合は、フェーズ2 DHグループを設定する必要はありません。

ステップ7:[Phase 2 Encryption]ドロップダウンリストから、適切なフェーズ2暗号化を選択してキーを暗号化します。AES-128、AES-192、またはAES-256が推奨されます。VPNトンネルは、両端で同じ暗号化方式を使用する必要があります。

・ DES:DESは56ビットの古い暗号化方式で、現在の世界ではあまり安全な暗号化方式ではありません。

・ 3DES:3DESは168ビットの簡単な暗号化方式で、DESよりもセキュリティが高いデータを3回暗号化することでキーサイズを大きくします。

・ AES-128:AESは、プレーンテキストを10サイクルの繰り返しで暗号テキストに変換する128ビット暗号化方式です。

・ AES-192：プレーンテキストを12サイクルの繰り返しで暗号テキストに変換する192ビットの暗号化方式。

・ AES-256：プレーンテキストを14サイクルの繰り返しで暗号テキストに変換する256ビットの暗号化方式。

ステップ8:[Phase 2 Authentication]ドロップダウンリストから適切な認証方式を選択します。VPNトンネルは、両端で同じ認証方式を使用する必要があります。

・ MD5 — MD5は32桁の16進数ハッシュ関数を表し、チェックサム計算による悪意のある攻撃からデータを保護します。

・ SHA1 — Secure Hash Algorithm version 1(SHA1)は、MD5よりも安全な160ビットのハッシュ関数です。

・ Null：認証方式は使用されません。

ステップ9:[Phase 2 SA Life Time]フィールドに、VPNトンネルがアクティブなままである時間（秒）を入力します。

ステップ10：事前共有キーの強度計を有効にするには、[最小事前共有キーの複雑度(Minimum Preshared Key Complexity)]チェックボックスをオンにします。

ステップ11:[Preshared Key]フィールドに、IKEピア間で以前共有されていたキーを入力します。事前共有キーとして最大30の16進数と文字を使用できます。VPNトンネルは、両端で同じ事前共有キーを使用する必要があります。

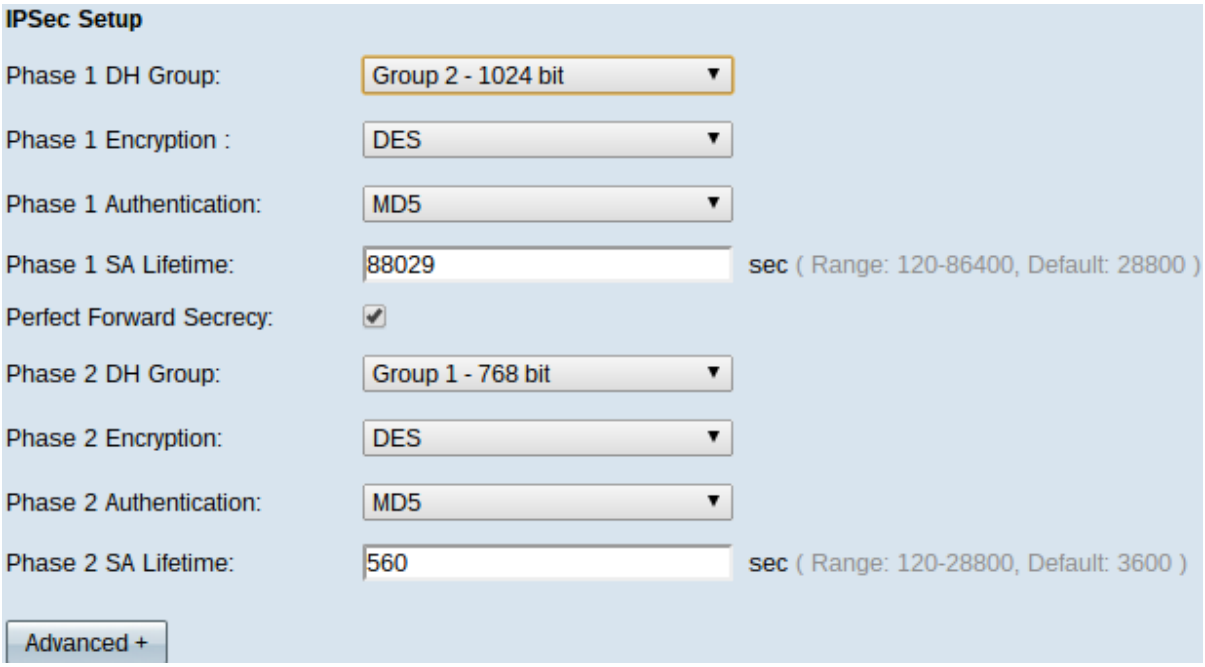
注：VPNが安全な状態を維持するために、IKEピア間で事前共有キーを頻繁に変更することを強く推奨します。

事前共有キーの強度メーターは、カラーバーを介した事前共有キーの強度を示します。赤は弱い強さを示し、黄色は許容される強さを示し、緑は強い強さを示します。

ステップ12:[**Save**]をクリックして、設定を保存します。

証明書を使用したIKEのIPSecセットアップ

[Add a New Tunnel]のステップ3で[Keying Mode]ドロップダウンリストから[IKE with Certificate]が選択されている場合にのみ使用できます。



ステップ1:[Phase 1 DH Group]ドロップダウンリストから適切なフェーズ1 DHグループを選択します。フェーズ1は、セキュアな認証通信をサポートするために、トンネルの両端の間にシンプレックス論理SA（セキュリティアソシエーション）を確立するために使用されます。DHは、フェーズ1接続時に通信を認証するために秘密キーを共有するために使用される暗号キー交換プロトコルです。

・グループ1 - 768ビット：最高強度キーと最もセキュアな認証グループを表します。しかし、IKEキーの計算にはより多くの時間が必要です。ネットワークの速度が高い場合に推奨されます。

・グループ2 - 1024ビット：強度の高いキーとよりセキュアな認証グループを表します。しかし、IKEキーを計算するには時間が必要です。

・グループ5 - 1536ビット：最小強度キーと最も安全でない認証グループを表します。IKEキーを計算する時間が短縮されます。ネットワークの速度が低い場合に推奨されます。

ステップ2:[Phase 1 Encryption]ドロップダウンリストから、適切なフェーズ1暗号化を選択してキーを暗号化します。AES-128、AES-192、またはAES-256が推奨されます。VPNトンネルは、両端で同じ暗号化方式を使用する必要があります。

・ DES:DESは56ビットの古い暗号化方式で、現在の世界ではあまり安全な暗号化方式ではありません。

・ 3DES:3DESは168ビットの簡単な暗号化方式で、DESよりもセキュリティが高いデータを3回暗号化することでキーサイズを大きくします。

・ AES-128:AESは、プレーンテキストを10サイクルの繰り返しで暗号テキストに変換する128ビット暗号化方式です。

・ AES-192：プレーンテキストを12サイクルの繰り返しで暗号テキストに変換する192ビットの暗号化方式。

・ AES-256：プレーンテキストを14サイクルの繰り返しで暗号テキストに変換する256ビットの暗号化方式。

ステップ3:[Phase 1 Authentication]ドロップダウンリストから適切な認証方式を選択します。VPNトンネルは、両端で同じ認証方式を使用する必要があります。SHA1が推奨されます。

・ MD5 — MD5は32桁の16進数ハッシュ関数を表し、チェックサム計算による悪意のある攻撃からデータを保護します。

・ SHA1:MD5よりも安全な160ビットのハッシュ関数。

ステップ4:[Phase 1 SA Life Time]フィールドに、VPNトンネルがアクティブなままである時間（秒）を入力します。

ステップ5:[Perfect Forward Secrecy]チェックボックスをオンにして、キーに対する保護を強化します。このオプションを使用すると、キーが侵害された場合に新しいキーを生成できます。暗号化されたデータは、侵害されたキーによってのみ侵害されます。したがって、別のキーが侵害されたときに他のキーを保護するため、より安全で認証された通信が提供されます。これは、セキュリティを強化するために推奨されるアクションです。

ステップ6:[Phase 2 DH Group]ドロップダウンリストから適切なフェーズ2 DHグループを

選択します。フェーズ1は、セキュアな認証通信をサポートするために、トンネルの両端の間にシンプレックス論理SAを確立するために使用されます。DHは、フェーズ1接続時に通信を認証するために秘密キーを共有するために使用される暗号キー交換プロトコルです。

・ グループ1 - 768ビット：最高強度キーと最もセキュアな認証グループを表します。しかし、IKEキーの計算にはより多くの時間が必要です。ネットワークの速度が高い場合に推奨されます。

・ グループ2 - 1024ビット：強度の高いキーとよりセキュアな認証グループを表します。しかし、IKEキーを計算するには時間が必要です。

・ グループ5 - 1536ビット：最小強度キーと最も安全でない認証グループを表します。IKEキーを計算する時間が短縮されます。ネットワークの速度が低い場合に推奨されます。

注：新しいキーは生成されないため、ステップ5で[Perfect Forward Secrecy]をオフにした場合は、フェーズ2 DHグループを設定する必要はありません。

ステップ7:[Phase 2 Encryption]ドロップダウンリストから、適切なフェーズ2暗号化を選択してキーを暗号化します。AES-128、AES-192、またはAES-256が推奨されます。VPNトンネルは、両端で同じ暗号化方式を使用する必要があります。

・ DES:DESは56ビットの古い暗号化方式で、現在の世界ではあまり安全な暗号化方式ではありません。

・ 3DES:3DESは168ビットの簡単な暗号化方式で、DESよりもセキュリティが高いデータを3回暗号化することでキーサイズを大きくします。

・ AES-128:AESは、プレーンテキストを10サイクルの繰り返しで暗号テキストに変換する128ビット暗号化方式です。

・ AES-192：プレーンテキストを12サイクルの繰り返しで暗号テキストに変換する192ビットの暗号化方式。

・ AES-256：プレーンテキストを14サイクルの繰り返しで暗号テキストに変換する256ビットの暗号化方式。

ステップ8:[Phase 2 Authentication]ドロップダウンリストから適切な認証方式を選択します。VPNトンネルは、両端で同じ認証方式を使用する必要があります。

・ MD5 — MD5は32桁の16進数ハッシュ関数を表し、チェックサム計算による悪意のある攻撃からデータを保護します。

・ SHA1 — SHA1はMD5よりも安全な160ビットハッシュ関数です。

・ Null：認証方式は使用されません。

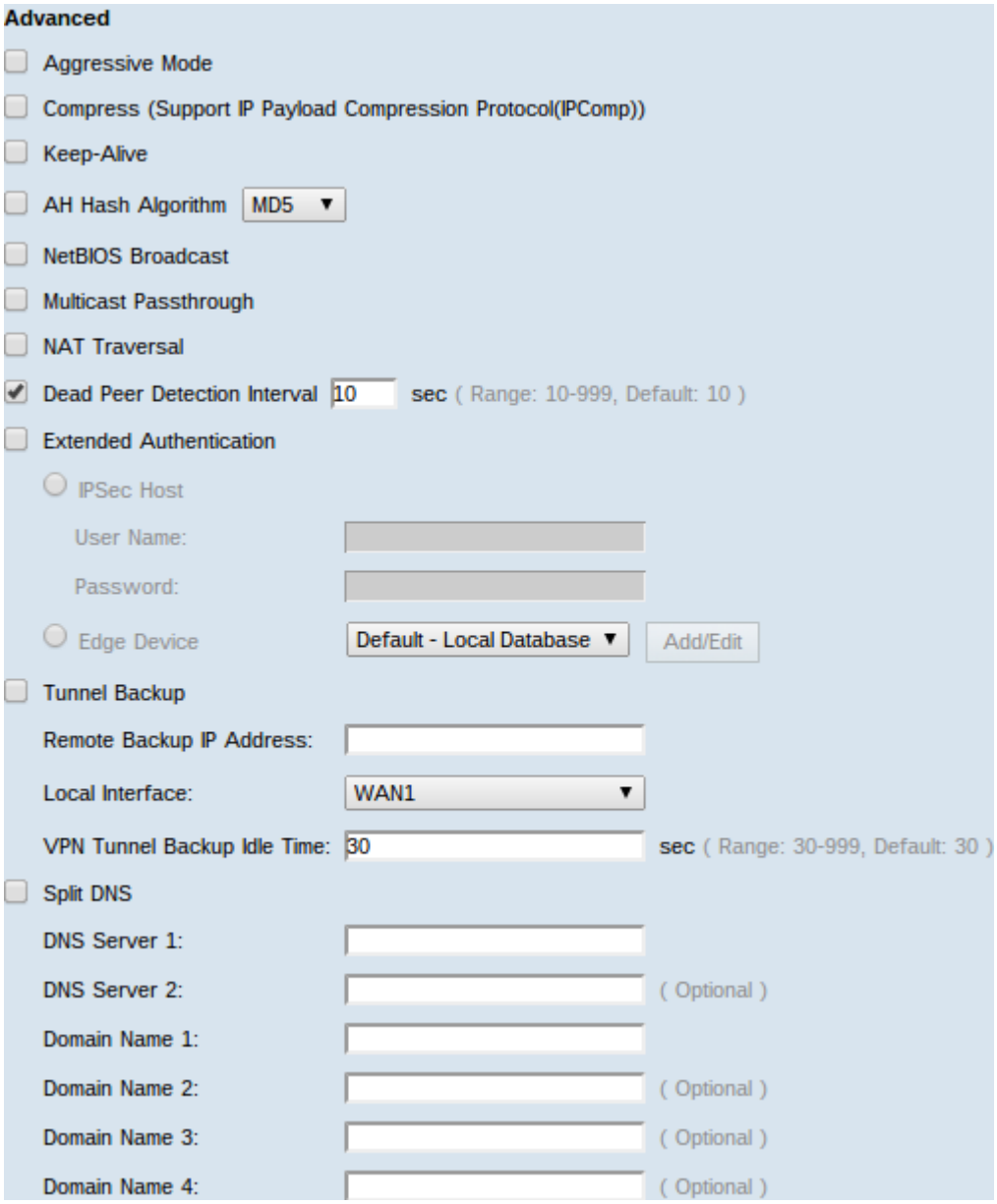
ステップ9:[Phase 2 SA Life Time]フィールドに、VPNトンネルがアクティブなままである時間（秒）を入力します。

ステップ10:[**Save**]をクリックして、設定を保存します。

（オプション）証明書を使用するIKEのIPSecアドバンスセットアップと事前共有キーを使用するIKE

高度なオプションは、[Add a New Tunnel]のステップ3で[Keying Mode]ドロップダウンリストから[Certificate]を含むIKEまたは[Preshared key]を含むIKEを選択した場合に使用できます。両方のキーイングモードで同じ設定を使用できます。

ステップ1:**[Advanced +]ボタンをクリック**して、詳細IPSecオプションを表示します。



ステップ2：ネットワーク速度が低い場合は、[Aggressive Mode]チェックボックスをオンにします。SA接続時にトンネルのエンドポイントのIDをクリアテキストで交換するため、交換に必要な時間は短いが、セキュリティは低くなります。

ステップ3:IPデータグラムのサイズを圧縮する場合は、[Compress (Support IP Payload Compression Protocol (IPComp))]チェックボックスをオンにします。IPCompはIPデータグラムのサイズを圧縮するために使用されるIP圧縮プロトコルです。ネットワーク速度が低く、ユーザが低速ネットワークを介して損失なく迅速にデータを送信したい場合に使用します。

ステップ4:VPNトンネルの接続を常にアクティブのままにする場合は、[Keep-Alive]チェックボックスをオンにします。接続が非アクティブになった場合は、すぐに接続を再確立できます。

ステップ5：認証ヘッダー(AH)を認証する場合は、[AH Hash Algorithm]チェックボックスを

オンにします。AHはデータの送信元に認証を提供し、チェックサムを通じてデータの整合性を確保し、IPヘッダーに保護を拡張します。トンネルの両側で同じアルゴリズムが必要です。

・ MD5 — MD5は128桁の16進数ハッシュ関数を表し、チェックサム計算による悪意のある攻撃からデータを保護します。

・ SHA1 — SHA1はMD5よりも安全な160ビットハッシュ関数です。

ステップ6：ルーティング不能トラフィックをVPNトンネル経由で許可する場合は、[NetBIOS Broadcast]をオンにします。デフォルトはオフです。NetBIOSは、ネットワーク内のプリンタやコンピュータなどのネットワークリソースを、一部のソフトウェアアプリケーションやネットワークネイバーフッドなどのWindows機能を介して検出するために使用されます。

ステップ7:VPNルータがNATゲートウェイの背後にある場合は、NATトラバーサルを有効にするチェックボックスをオンにします。ネットワークアドレス変換(NAT)を使用すると、プライベートLANアドレスを持つユーザは、公的にルーティング可能なIPアドレスを送信元アドレスとして使用してインターネットリソースにアクセスできます。ただし、着信トラフィックの場合、NATゲートウェイには、パブリックIPアドレスをプライベートLAN上の特定の宛先に自動変換する方法はありません。この問題により、IPSec交換が正常に行われなくなります。NATトラバーサルは、このインバウンド変換を設定します。トンネルの両端で同じ設定を使用する必要があります。

ステップ8:[Dead Peer Detection Interval]をチェックして、HelloまたはACKを定期的に通過するVPNトンネルの状態をチェックします。このチェックボックスをオンにした場合、必要なhelloメッセージの継続時間または間隔（秒）を入力します。

ステップ9:[Extended Authentication]をオンにして、IPSecホストのユーザ名とパスワードを使用してVPNクライアントを認証するか、[User Management]にあるデータベースを使用します。両方のデバイスでこの機能を有効にする必要があります。IPSecホストとユーザ名を使用するには、[IPSecホスト(IPSec Host)]オプションボタンをクリックし、[ユーザ名(User Name)]フィールドと[パスワード(Password)]フィールドにユーザ名とパスワードを入力します。または、[エッジデバイス]ラジオボタンをクリックしてデータベースを使用します。[エッジデバイス(Edge Device)]ドロップダウンリストから目的のデータベースを選択します。

ステップ10:[Tunnel Backup]チェックボックスをオンにして、トンネルバックアップを有効にします。この機能は、[Dead Peer Detection Interval]がチェックされている場合に使用できます。この機能により、デバイスは代替WANインターフェイスまたはIPアドレスを介してVPNトンネルを再確立できます。

・リモートバックアップIPアドレス：リモートピアの代替IP。このフィールドに、リモートゲートウェイ用にすでに設定されているWAN IPを入力します。

・ローカルインターフェイス：接続の再確立に使用されるWANインターフェイス。ドロップダウンリストから目的のインターフェイスを選択します。

・ VPN Tunnel Backup Idle Time：プライマリトンネルが接続されていない場合にバックアップトンネルを使用するタイミングとして選択した時間。秒単位で入力します。

ステップ11：スプリットDNSを有効にするには、[スプリットDNS(Split DNS)]チェックボックスをオンにします。この機能を使用すると、指定されたドメイン名に基づいて、定義されたDNSサーバにDNS要求を送信できます。[DNS Server 1]および[DNS Server 2]フィールドにDNSサーバ名を入力し、[Domain Name #]フィールドにドメイン名を入力します。

ステップ12:[Save]をクリックし、デバイスの設定を終了します。