RV130またはRV130Wルータでの Advanced Virtual Private Network(VPN)セットアップの設定

目的

バーチャルプライベートネットワーク(VPN)は、ネットワーク内またはネットワーク間に確立されたセキュアな接続です。VPNは、特定のホストとネットワーク間のトラフィックを、不正なホストとネットワークのトラフィックから分離する役割を果たします。サイト間（ゲートウェイ間）VPNは、ネットワーク全体を相互に接続し、パブリックドメイン（インターネットとも呼ばれる）上にトンネルを作成することによってセキュリティを維持します。各サイトは同じパブリックネットワークへのローカル接続のみを必要とするため、長い専用回線のコストを–減できます。

VPNは、拡張性が高く、ネットワークトポロジを簡素化し、リモートユーザの移動時間とコストを削減して生産性を向上させる点で、企業にとって有益です。

インターネットキー交換(IKE)は、VPN内の通信のためのセキュアな接続を確立するために使用されるプロトコルです。このセキュアな接続は、セキュリティアソシエーション(SA)と呼ばれます。 IKEポリシーを作成して、ピアの認証、暗号化アルゴリズムなど、このプロセスで使用するセキュリティパラメータを定義できます。VPNが正しく機能するためには、両方のエンドポイントのIKEポリシーが同一である必要があります。

この記事では、IKEポリシー設定とVPNポリシー設定をカバーするRV130またはRV130Wルータでの高度なVPNセットアップの設定方法を説明します。

該当するデバイス

- RV130
- RV130W

[Software Version]

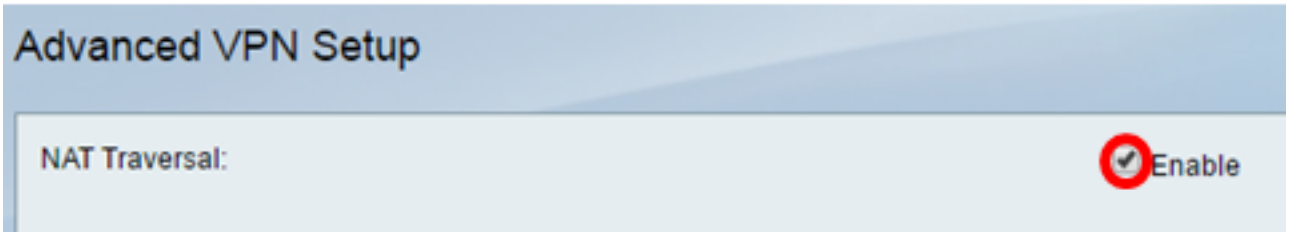
•1.0.3.22

高度なVPNセットアップの設定

インターネットキーエクスチェンジ(IKE)ポリシー設定の追加/編集

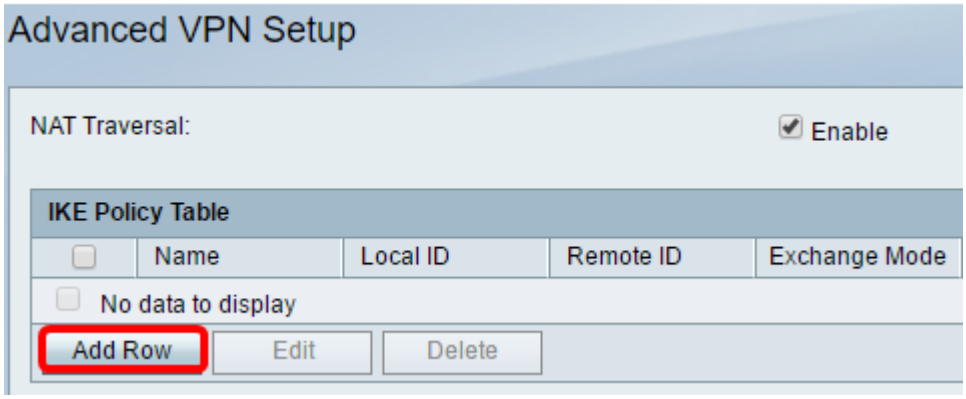
ステップ1:Webベースのユーティリティにログインし、[VPN] > [Site-to-Site IPSec VPN] > [Advanced VPN Setup]を選択します。

ステップ2:（オプション）VPN接続のネットワークアドレス変換(NAT)トラバーサルを有効にする場合は、[NAT Traversal]の[Enable] チェックボックスをオンにします。NATトラバーサルを使用すると、NATを使用するゲートウェイ間でVPN接続を確立できます。VPN接続がNAT対応ゲートウェイを通過する場合は、このオプションを選択します。



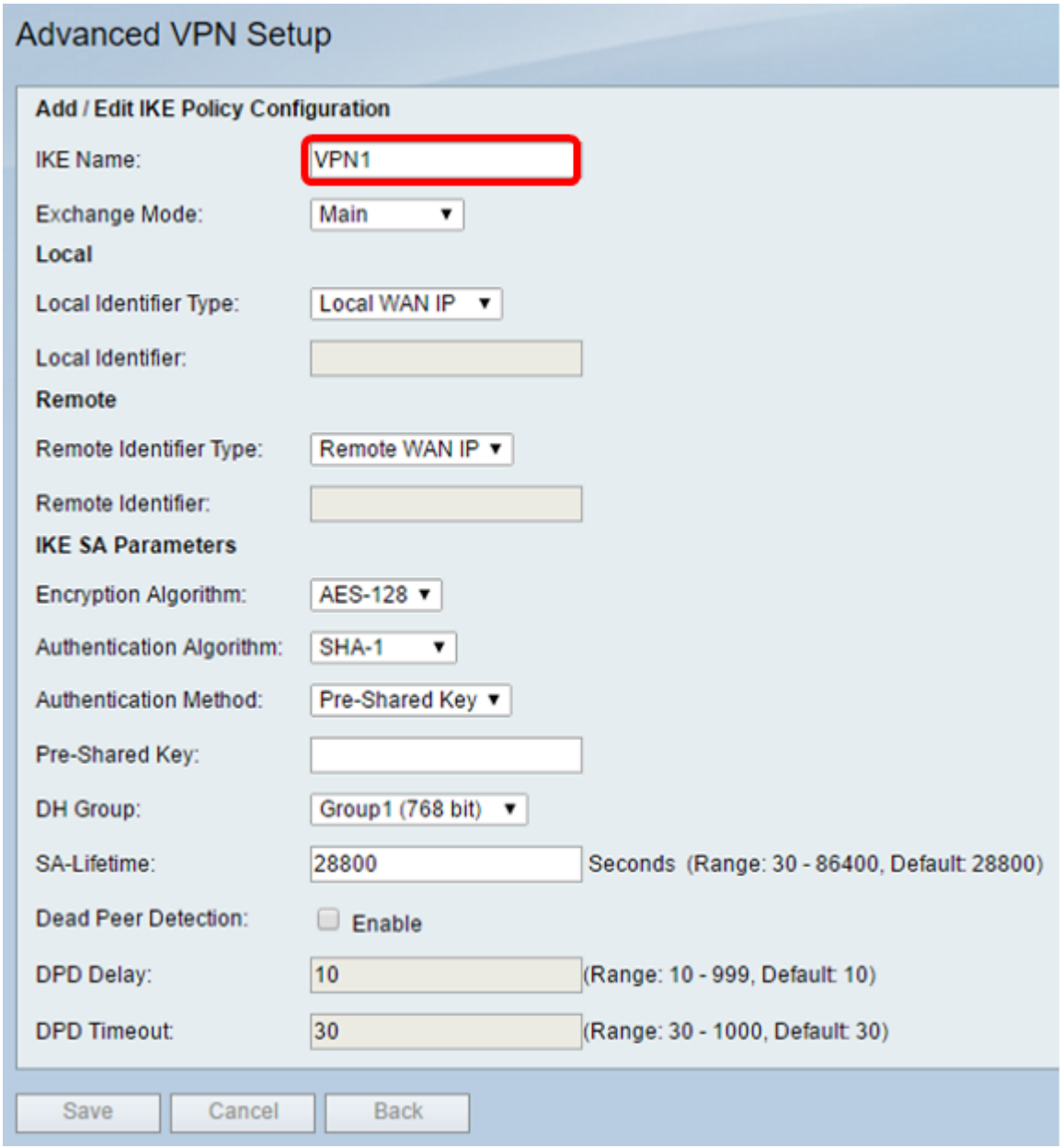
ステップ3:IKEポリシーテーブルで、[Add Row] をクリックして新しいIKEポリシーを作成します。

注：基本設定が設定されている場合、下の表には作成された基本的なVPN設定が含まれます。既存のIKEポリシーを編集するには、ポリシーのチェックボックスをオンにして、[Edit] をクリックします。[Advanced VPN Setup]ページが変更されます。



ステップ4:[IKE Name] フィールドに、IKEポリシーの一意の名前を入力します。

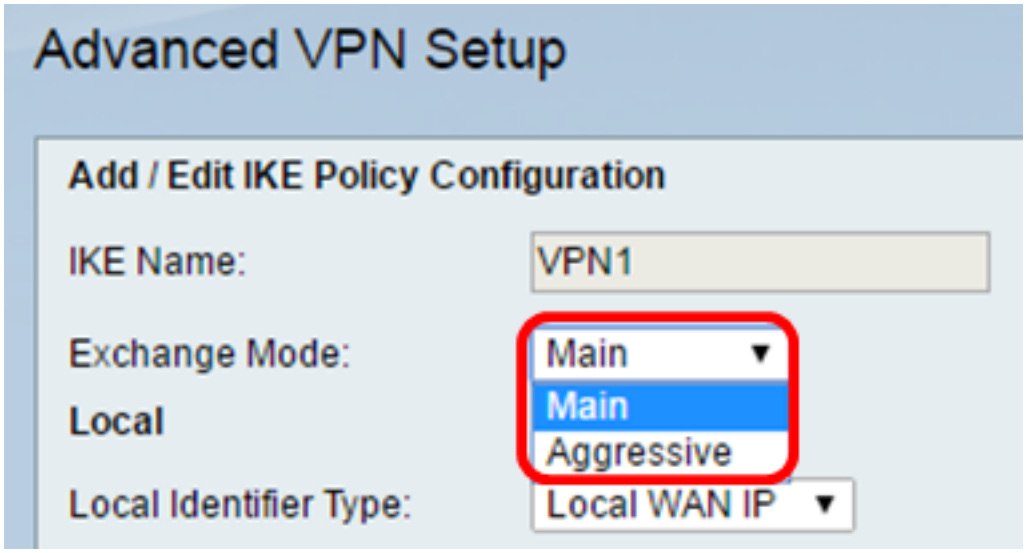
注：基本設定が設定されている場合、作成された接続名はIKE名として設定されます。この例では、VPN1が選択されたIKE名です。



ステップ5:[Exchange Mode]ドロップダウンリストからオプションを選択します。

- Main：このオプションを使用すると、IKEポリシーは、アグレッシブモードよりも高いセキュリティでVPNトンネルをネゴシエートできます。ネゴシエーション速度よりも安全なVPN接続が優先される場合は、このオプションをクリックします。
- [Aggressive]：このオプションを使用すると、IKEポリシーはメインモードよりも高速でセキュアではない接続を確立できます。高速なVPN接続が高いセキュリティよりも優先される場合は、このオプションをクリックします。

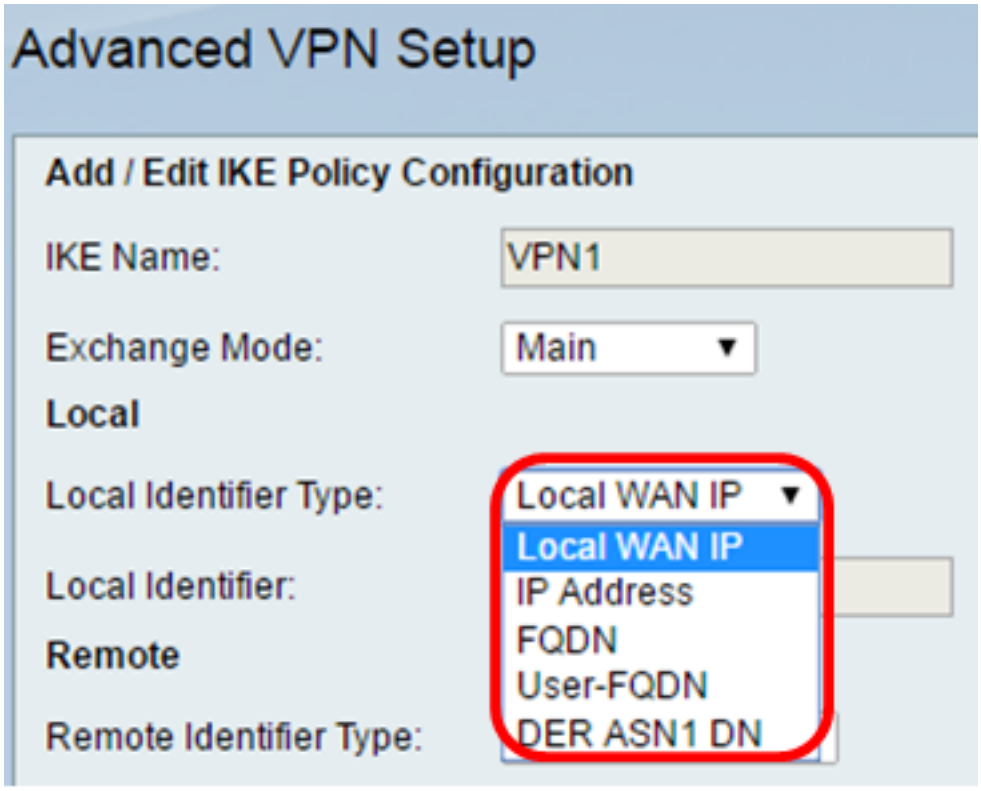
注：この例では、[Main]が選択されています。



ステップ6:[Local Identifier Type]ドロップダウンリストから選択して、ローカルルータのInternet Security Association and Key Management Protocol(ISAKMP)を識別または指定します。次のオプションがあります。

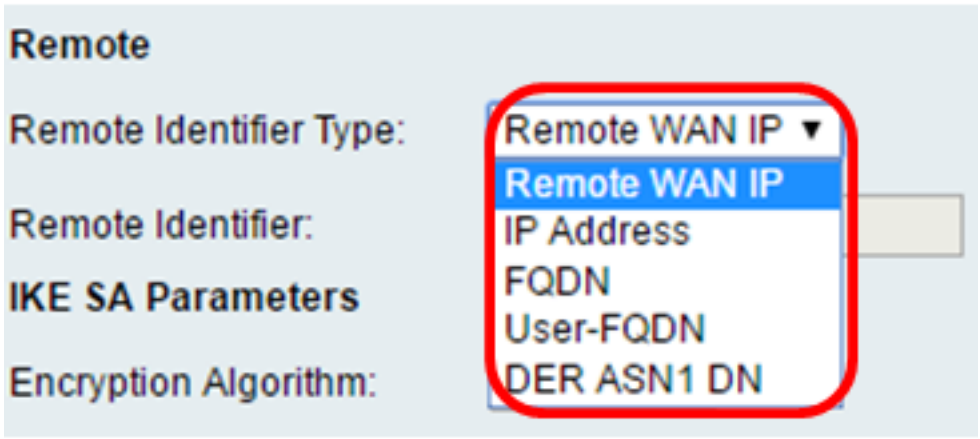
- ローカルWAN IP：ルータはローカルのワイドエリアネットワーク(WAN)IPをメインIDとして使用します。このオプションは、インターネット経由で接続します。このオプションを選択すると、下の[Local *Identifier]フィールドがグレー表示になります。*
- [IP Address]：これをクリックすると、[Local Identifier] フィールドにIPアドレスを入力できます。
- FQDN：完全修飾ドメイン名(FQDN)またはドメイン名(http://www.example.comなど)を使用すると、[Local Identifier] フィールドにドメイン名またはIPアドレスを入力できます。
- User-FQDN：このオプションは、user@email.comなどのユーザ電子メールアドレスです。[Local *Identifier*]フィールドにドメイン名またはIPアドレスを入力します。
- DER ASN1 DN：このオプションは、Distinguished Encoding Rules Abstract Syntax Notation One(DER ASN1)を使用して情報を送信する識別名(DN)のIDタイプです。これは、VPNトンネルがユーザ証明書に関連付けられている場合に発生します。これを選択した場合は、[Local *Identifier*]フィールドにドメイン名またはIPアドレスを入力します。

注：この例では、[Local WAN IP]が選択されています。



ステップ7:[Remote Identifier Type]ドロップダウンリストから選択して、リモートルータのInternet Security Association and Key Management Protocol(ISAKMP)を特定または指定します。オプションは、リモートWAN IP、IPアドレス、FQDN、ユーザFQDN、およびDER ASN1 DNです。

注：この例では、[Remote WAN IP]が選択されています。

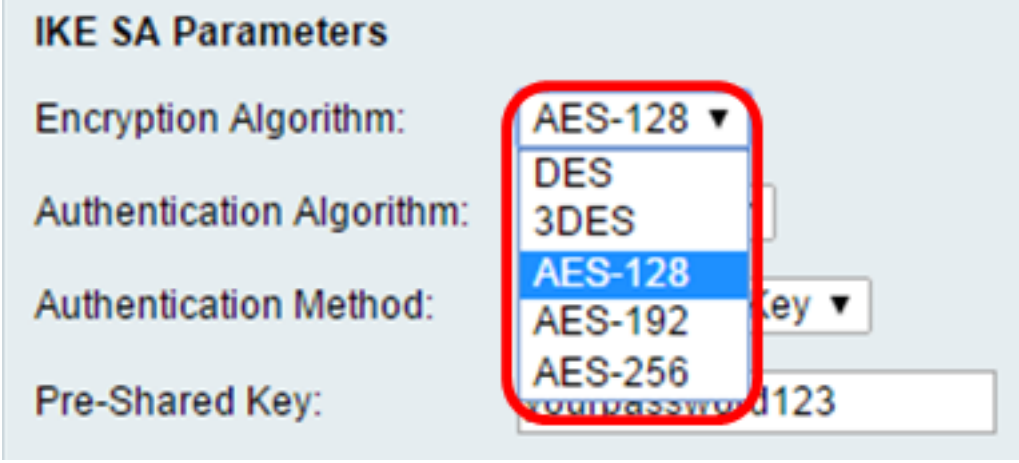


ステップ8:[Encryption Algorithm]ドロップダウンリストからオプションを選択します。

- 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、あまり安全な暗号化方式ではありませんが、下位互換性のために必要になる場合があります。
- 3DES:Triple Data Encryption Standard(3DES)は、データを3回暗号化するため、キーサイズを増やすために使用される168ビットのシンプルな暗号化方式です。これにより、DESよりもセキュリティが高くなりますが、AESよりもセキュリティが低くなります。
- AES-128:Advanced Encryption Standard with 128-bit key(AES-128)は、AES暗号化に128ビットキーを使用します。AESはDESよりも高速で安全です。一般に、AESは3DESよりも高速で安全です。AES-128はデフォルトの暗号化アルゴリズムであり、AES-192およびAES-256よ

りも高速ですが安全性は低くなります。
- AES-192:AES-192はAES暗号化に192ビットキーを使用します。AES-192はAES-128よりも低速ですが高い安全性を備え、AES-256よりも高速ですが低い安全性を備えています。
- AES-256:AES-256はAES暗号化に256ビットキーを使用します。AES-256は低速ですが、AES-128およびAES-192よりも安全です。

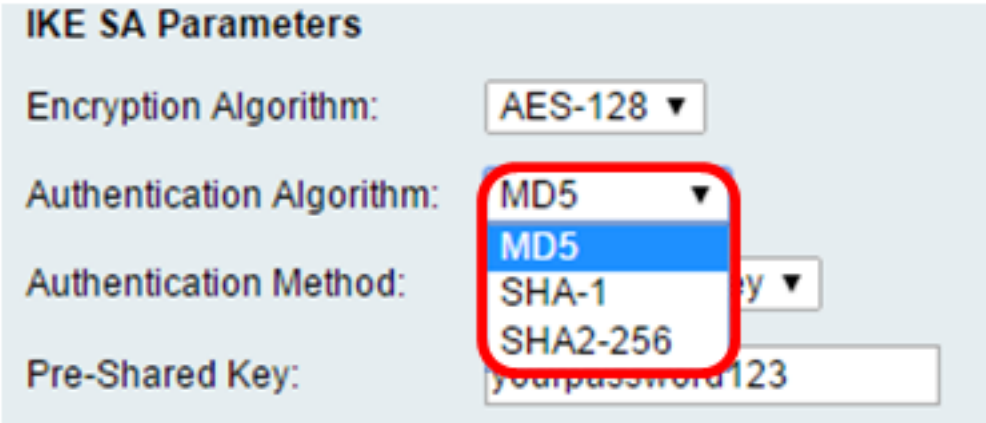
注：この例では、AES-128が選択されています。



ステップ9:[Authentication Algorithm]ドロップダウンリストから、次のオプションを選択します。

- MD5:Message Digest 5(MD5)は、128ビットのハッシュ値を認証に使用する認証アルゴリズムです。MD5はSHA-1およびSHA2-256よりも安全ではありませんが、高速です。
- SHA-1:Secure Hash Function 1(SHA-1)は、認証に160ビットのハッシュ値を使用します。SHA-1はMD5より低速ですが安全です。SHA-1はデフォルトの認証アルゴリズムであり、SHA2-256より高速ですが安全ではありません。
- SHA2-256:256ビットのハッシュ値を持つセキュアハッシュアルゴリズム2(SHA2-256)は、認証に256ビットのハッシュ値を使用します。SHA2-256はMD5およびSHA-1よりも低速ですが、より安全です。

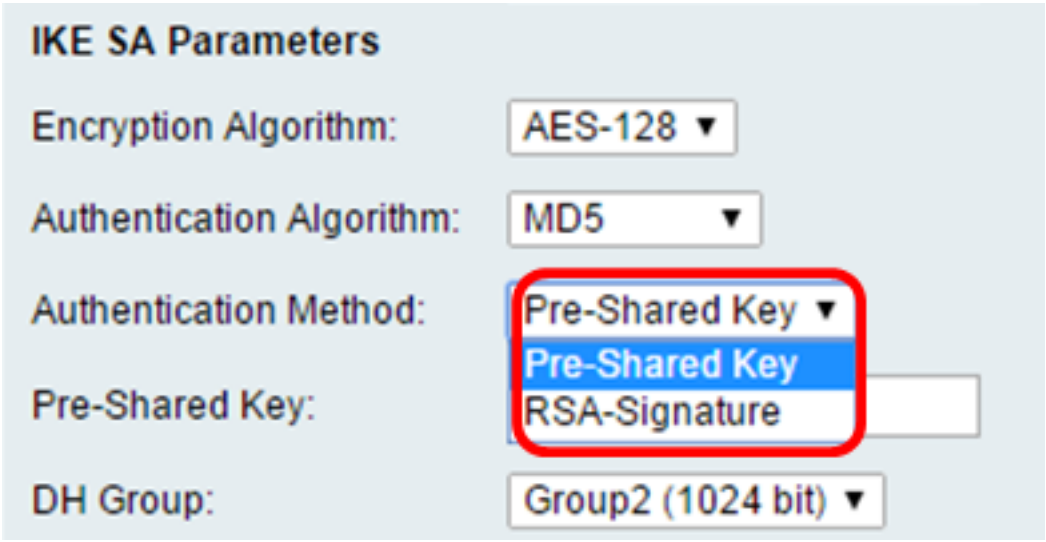
注：この例では、MD5が選択されています。



ステップ10:[Authentication Method]ドロップダウンリストで、次のいずれかのオプションを選択します。

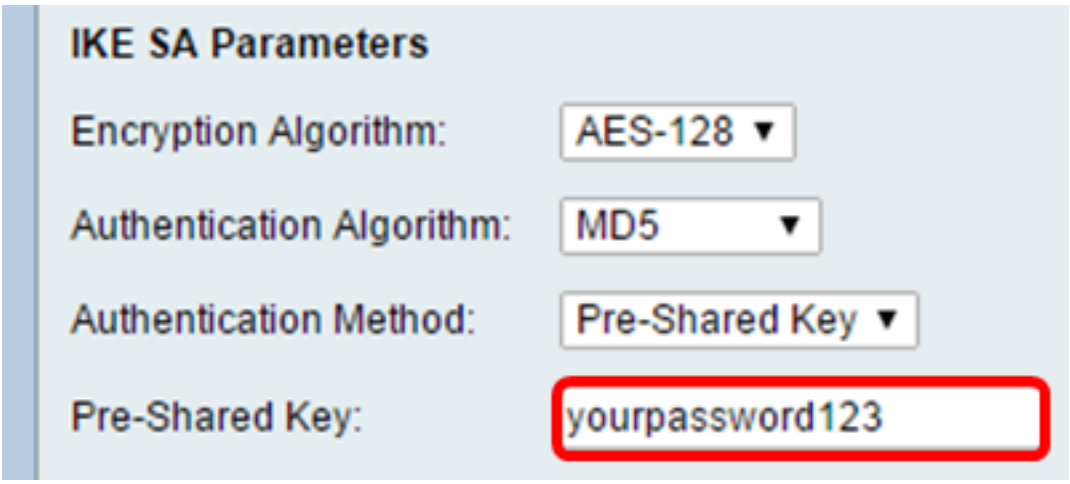
- Pre-Shared Key：このオプションでは、IKEピアと共有されるパスワードが必要です。
- RSA-Signature：このオプションは、証明書を使用して接続を認証します。これを選択すると、[Pre-Shared Key]フィールドは無効になります。ステップ 12 に進みます。

注：この例では、[Pre-Shared key]が選択されています。



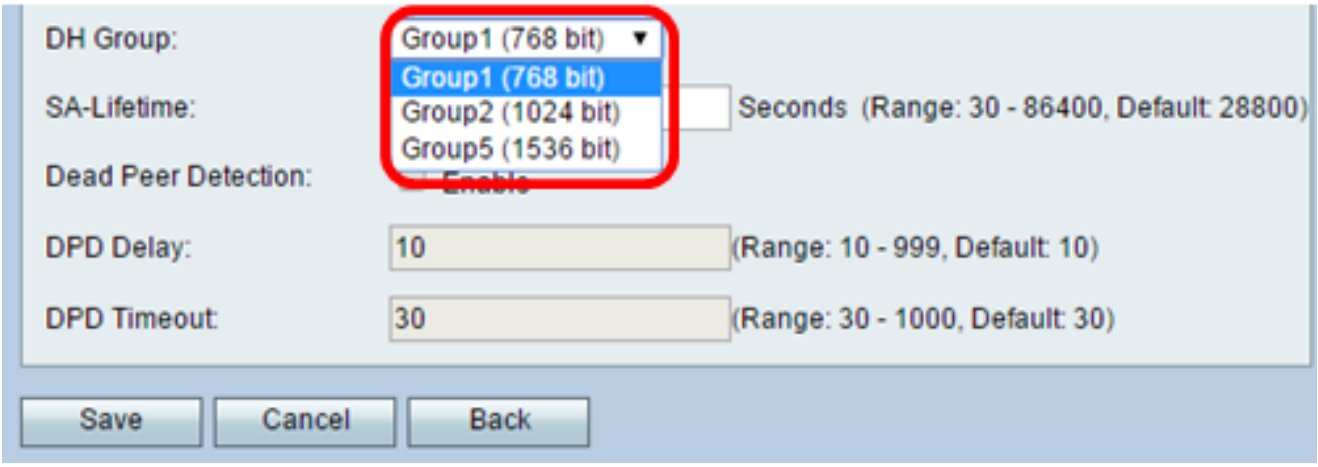
ステップ11:[Pre-Shared Key] フィールドに、8 ～ 49文字の長さのパスワードを入力します。

注：この例では、yourpassword123が使用されています。

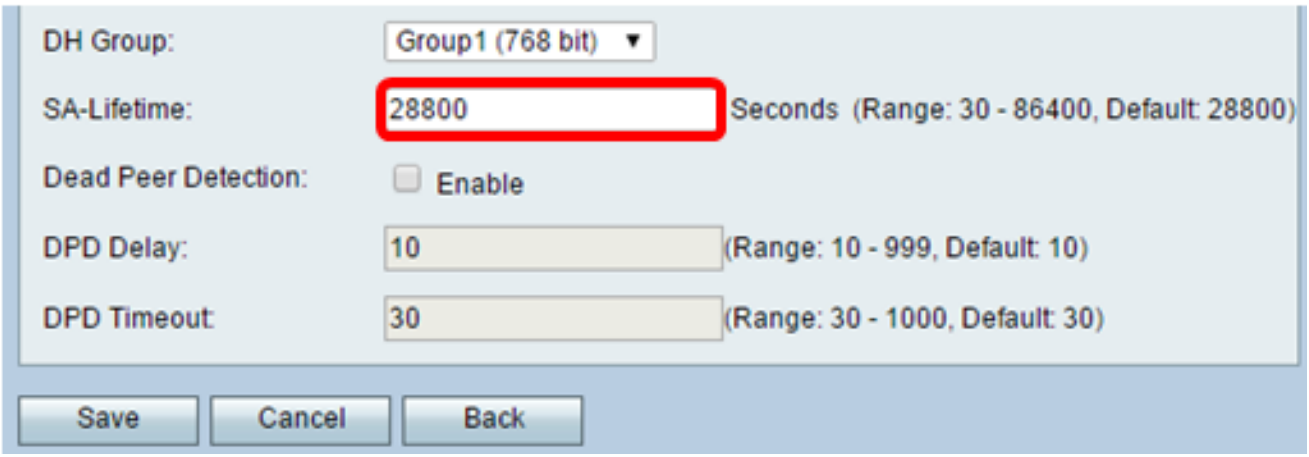


ステップ12:[DH Group]ドロップダウンリストから、IKEが使用するDiffie-Hellman(DH)グループアルゴリズムを選択します。DHグループ内のホストは、互いに認識することなくキーを交換できます。グループビット番号が大きいほど、セキュリティは高くなります。

注：この例では、Group1が選択されています。

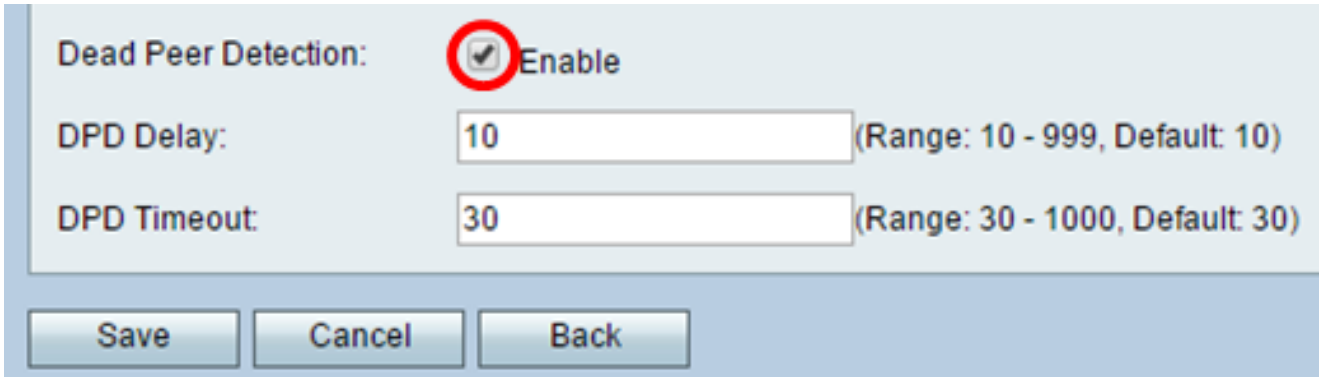


ステップ13:[SA-Lifetime] フィールドに、VPNに対するSAが更新されるまでの時間を秒単位で入力します。範囲は30 ~ 86400秒です。デフォルト値は 28800 です。



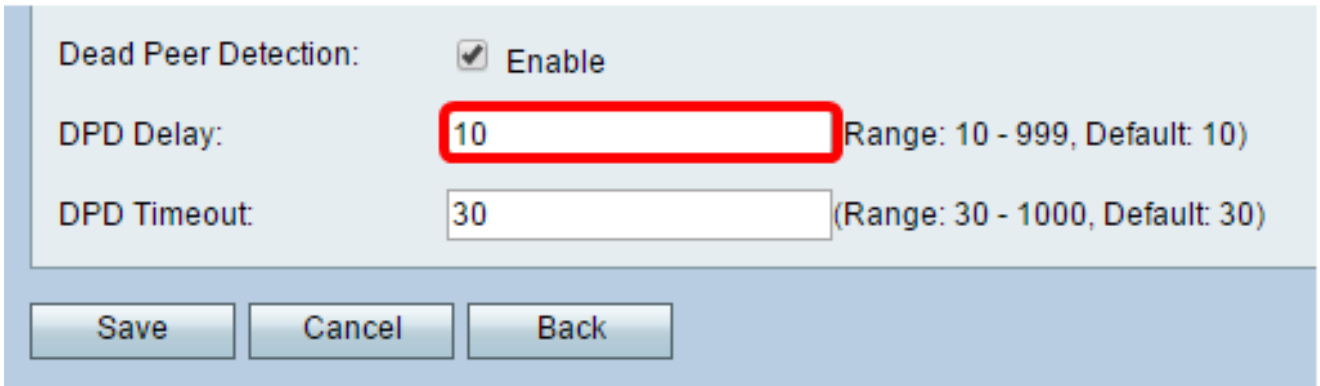
ステップ14(オプション)[Enable Dead Peer Detection] チェックボックスをオンにして、デッドピア検出(DPD)を有効にします。DPDはIKEピアを監視して、ピアが機能しなくなったか、まだ動作しているかどうかを確認します。ピアがデッドとして検出されると、デバイスはIPsecとIKEセキュリティアソシエーション(SA)を削除します。DPDは、非アクティブなピアでのネットワークリソースの浪費を防ぎます。

注：Dead Peer Detectionを有効にしない場合は、ステップ17に進みます。



ステップ15:（オプション）ステップ14でDPDを有効にした場合は、[DPD Delay] フィールドに、ピアのアクティビティを確認する頻度（秒単位）を入力します。

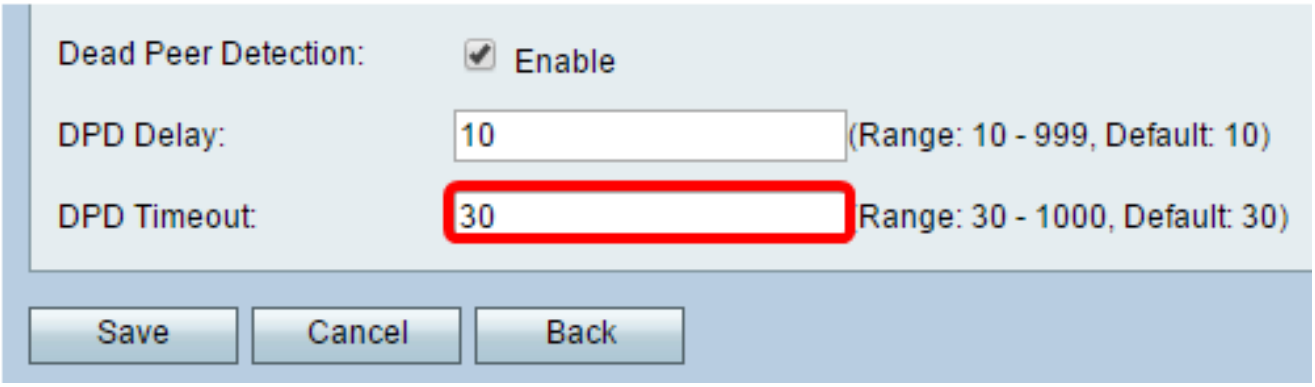
注：DPD Delayは、連続するDPD R-U-THEREメッセージ間の秒数です。DPD R-U-THEREメッセージは、IPsecトラフィックがアイドル状態のときにのみ送信されます。デフォルト値は 10 です。



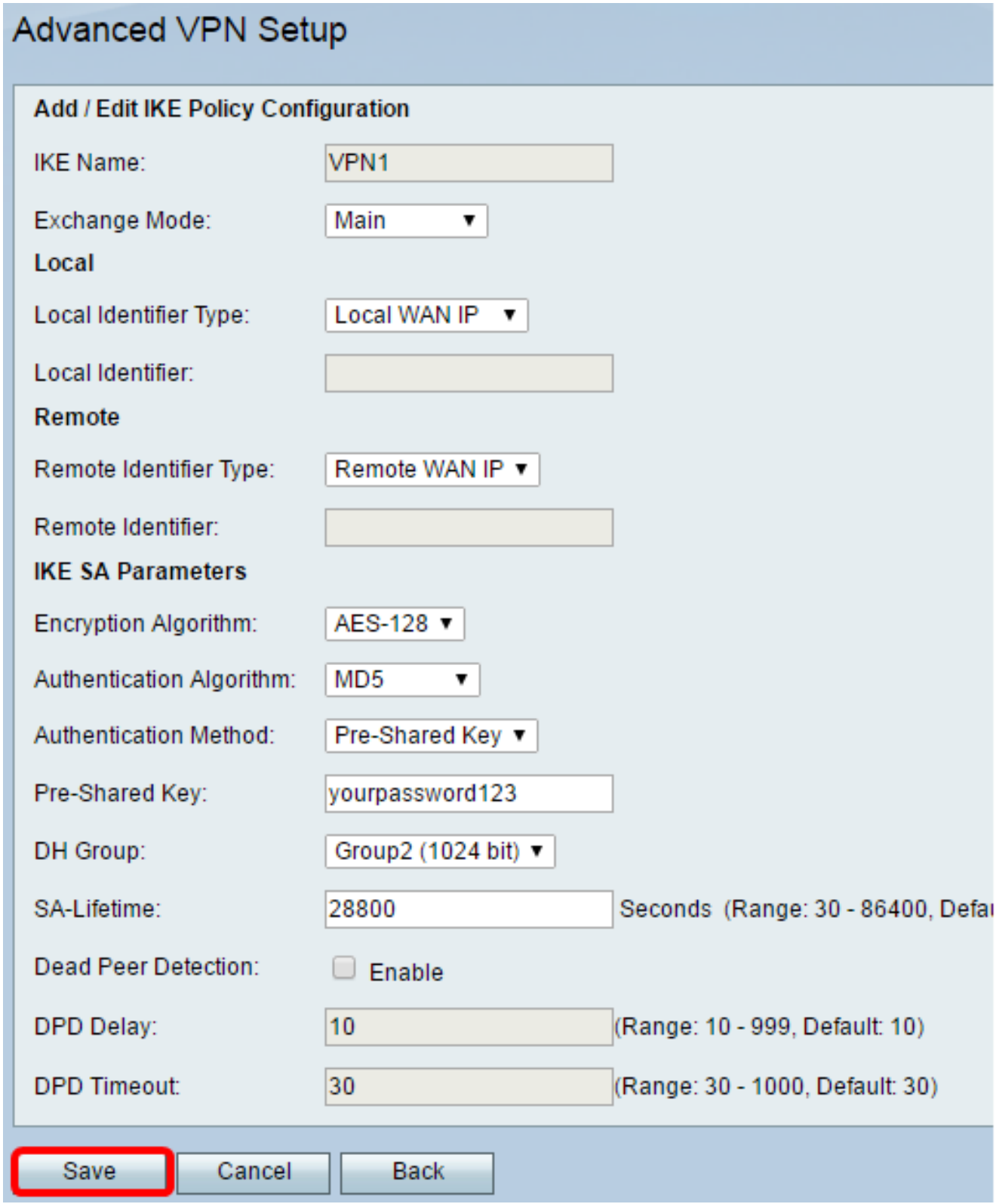
ステップ16:（オプション）ステップ14でDPDを有効にした場合は、非アクティブピアがド

ロップされるまでの秒数を*DPD Timeout*フィールドに入力します。

注：これは、ピアがダウンしていると見なす前に、デバイスがDPDメッセージへの応答を受信するのを待つ必要がある最大時間です。デフォルト値は 30 です。



ステップ17:[Save]をクリックします。



注：メインの[Advanced VPN Setup]ページが再表示されます。

これで、ルータのIKEポリシー設定が正常に設定されました。

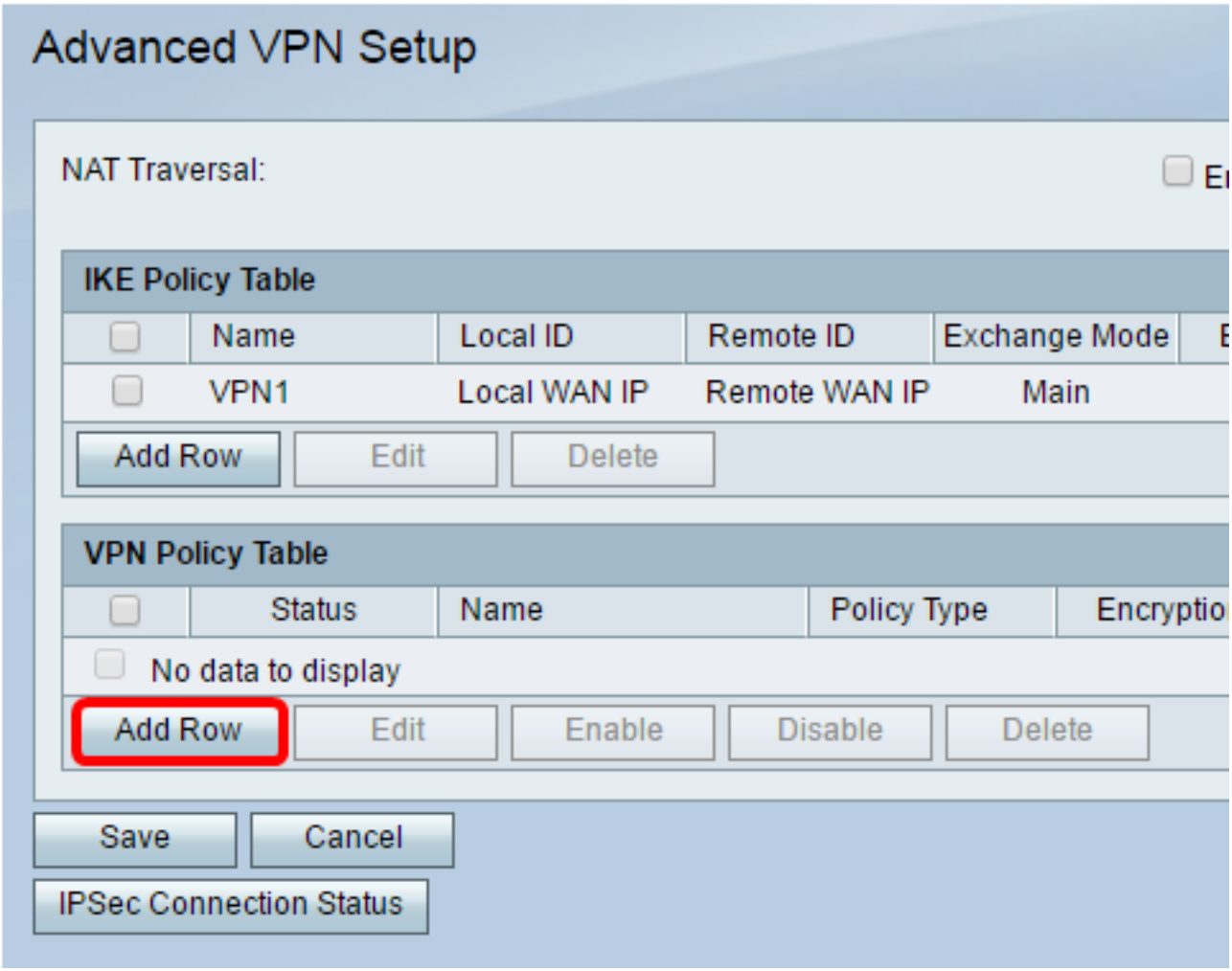
VPNポリシーの設定

注:VPNが正しく機能するためには、両方のエンドポイントのVPNポリシーが同じである必要があります。

ステップ1:VPNポリシーテーブルで、[Add Row] をクリックして新しいVPNポリシーを作成

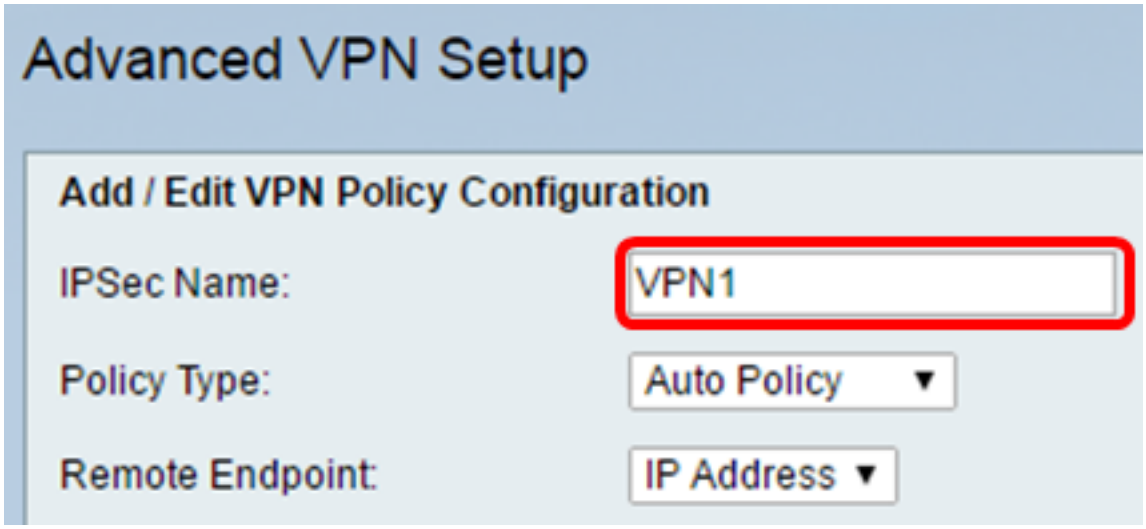
します。

注：ポリシーのチェックボックスをオンにして[Edit] をクリックすることで、VPNポリシーを編集することもできます。[Advanced VPN Setup]ページが表示されます。



ステップ2:[Add/Edit VPN Configuration]領域の[IPSec *Name]フィールドに、VPNポリシーの名前を入力します。*

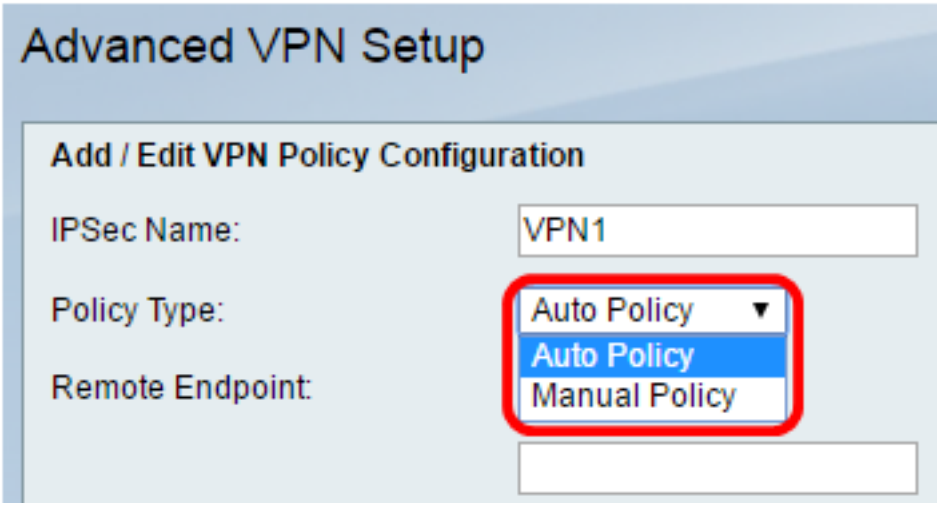
注：この例では、VPN1が使用されています。



ステップ3:[Policy Type]ドロップダウンリストから、オプションを選択します。

- [Manual Policy]：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]領域の構成設定が有効になります。[Remote Traffic Selection]まで手順を続行します。ここをクリックして手順を確認してください。
- [Auto Policy]：ポリシーパラメータが自動的に設定されます。このオプションは、データ整合性と暗号化キーの交換に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。ここをクリックして手順を確認してください。IKEプロトコルが2つのVPNエンドポイント間で自動的にネゴシエートされることを確認します。

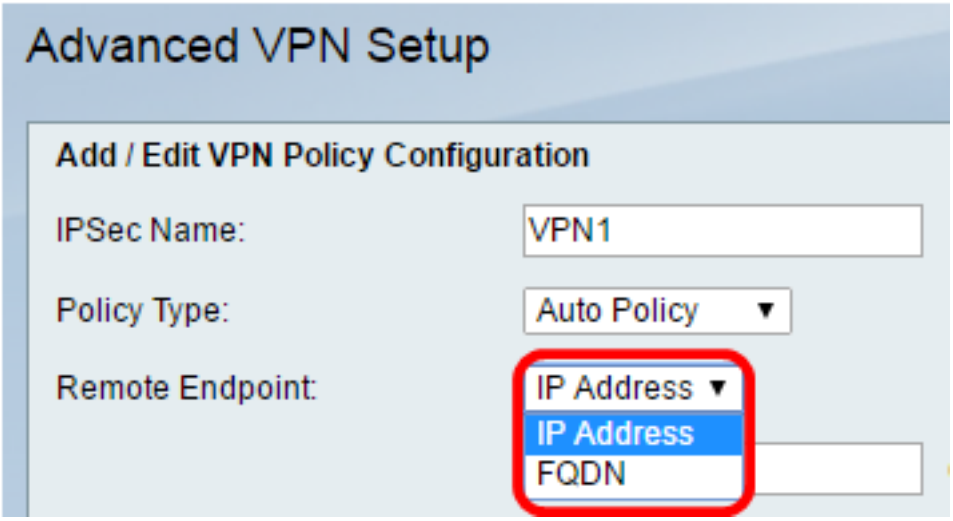
  注：この例では、[Auto Policy]が選択されています。



ステップ4:[Remote Endpoint]ドロップダウンリストから、オプションを選択します。

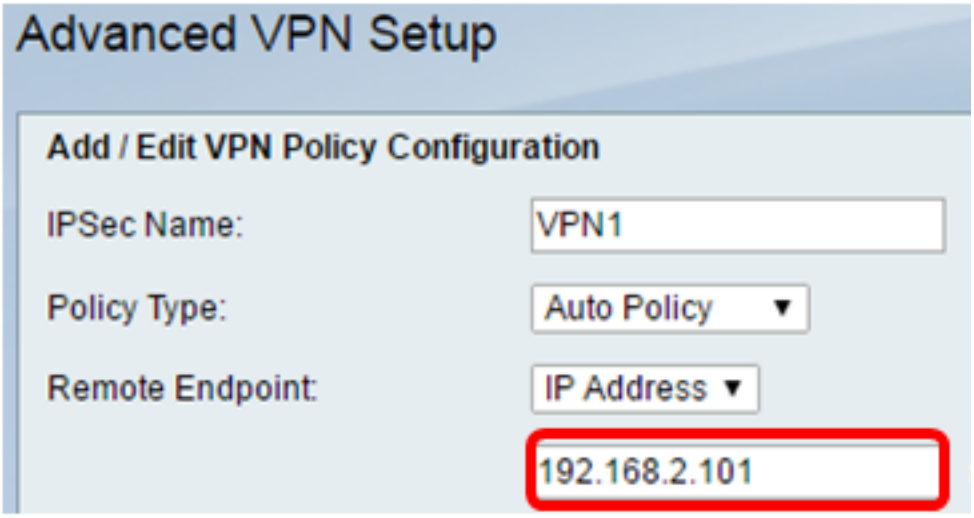
- [IP Address]：このオプションは、リモートネットワークをパブリックIPアドレスで識別します。
- FQDN：特定のコンピュータ、ホスト、またはインターネットの完全なドメイン名。FQDNは次の2つの部分で構成されます。ホスト名とドメイン名。このオプションは、ステップ3で**自動ポリシー**が選択されている場合にのみ有効にできます。

  注：この例では、[IP Address]が選択されています。



ステップ5:[Remote Endpoint] フィールドに、リモートアドレスのパブリックIPアドレスまたはドメイン名を入力します。

注：この例では、192.168.2.101が使用されています。

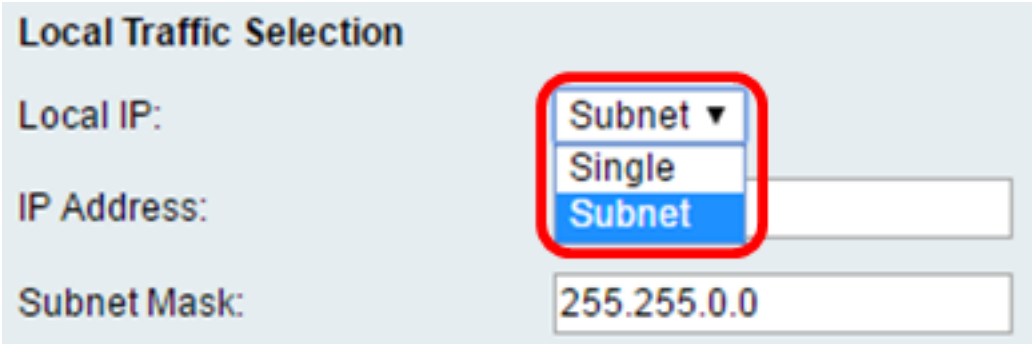


ステップ6: (オプション) Network Basic Input/Output System(NetBIOS)ブロードキャストをVPN接続を介して送信できるようにするには、[NetBios Enabled] チェックボックスをオンにします。NetBIOSを使用すると、ホストはローカルエリアネットワーク(LAN)内で相互に通信できます。

ステップ7:[Local Traffic Selection]領域の[Local IP]ドロップダウンリストから、オプションを選択します。

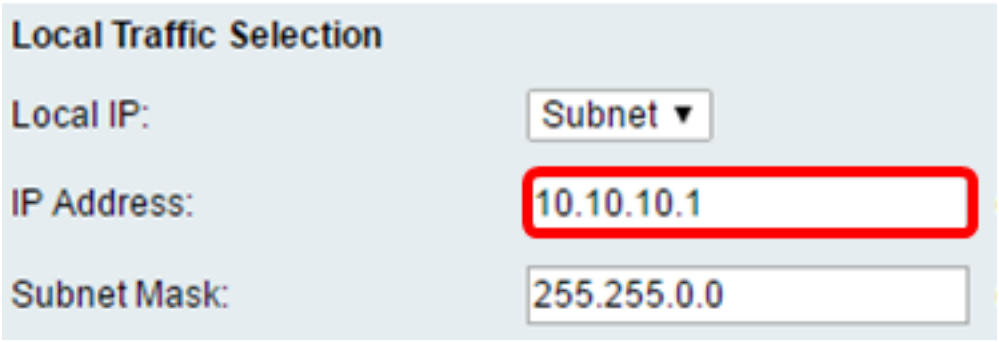
- Single：ポリシーを1つのホストに制限します。
- サブネット：IPアドレス範囲内のホストがVPNに接続できるようにします。

注：この例では、[Subnet]が選択されています。



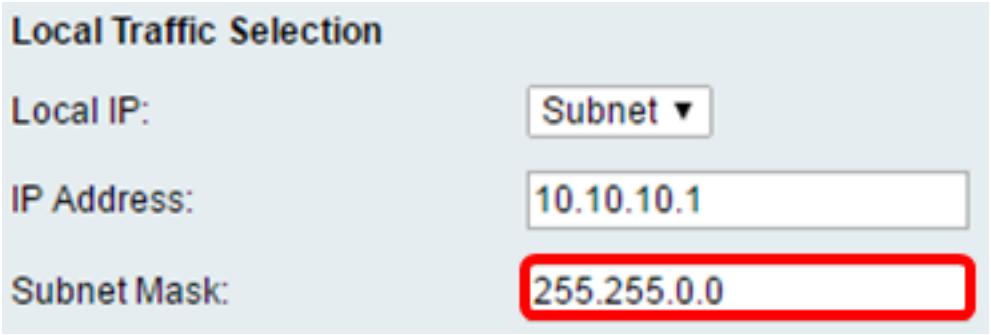
ステップ8:[IP Address]フィールドに、ローカルサブネットまたはホストのホストまたはサブネットのIPアドレスを入力します。

注：この例では、ローカルサブネットのIPアドレス10.10.10.1が使用されます。



ステップ9:（オプション）ステップ7で[Subnet]を選択した場合は、クライアントのサブネットマスクを[Subnet Mask] フィールドに入力します。手順1で[Single]を選択すると、[Subnet Mask]フィールドは無効になります。

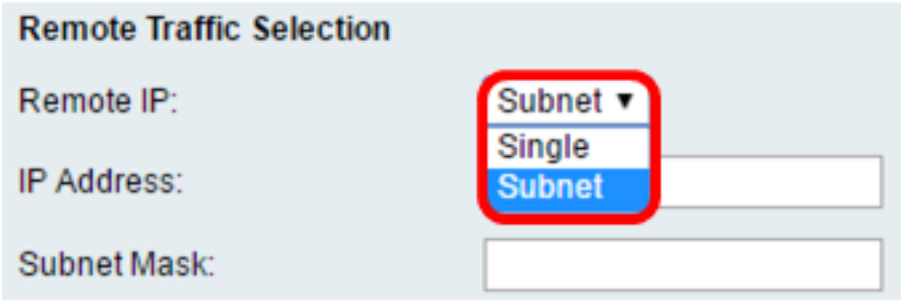
注：この例では、サブネットマスク255.255.0.0が使用されます。



ステップ10:[Remote Traffic Selection]領域の[Remote IP]ドロップダウンリストから、オプションを選択します。

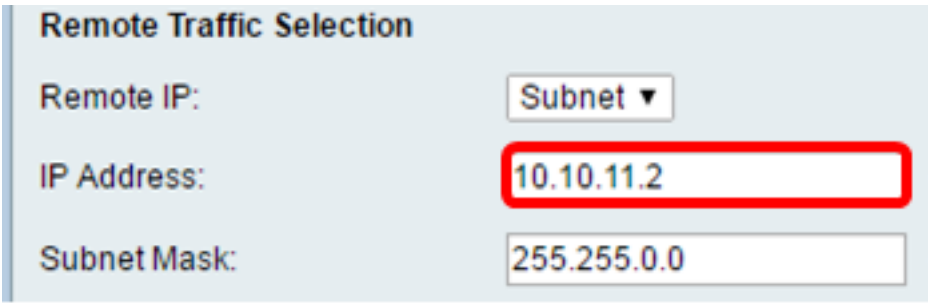
- Single：ポリシーを1つのホストに制限します。
- サブネット：IPアドレス範囲内のホストがVPNに接続できるようにします。

注： この例では、[Subnet]が選択されています。



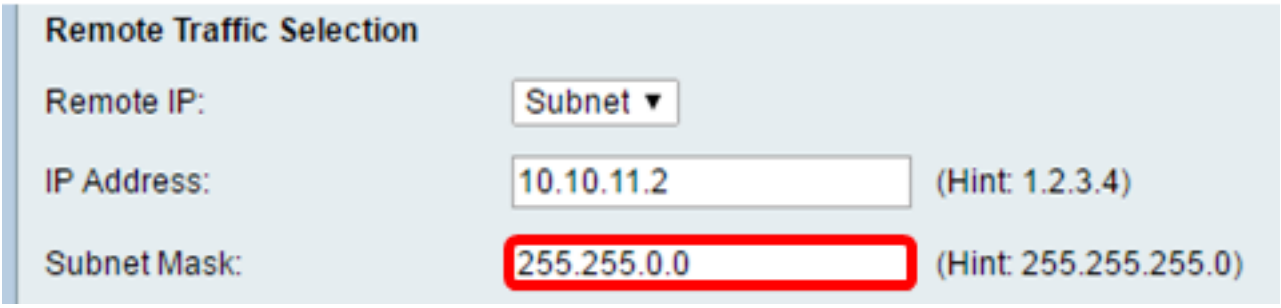
ステップ11:VPNの一部となるホストのIPアドレスの範囲を[IP Address] フィールドに入力します。ステップ10で[Single] を選択した場合は、IPアドレスを入力します。

注：次の例では、10.10.11.2が使用されています。



ステップ12: (オプション) ステップ10で[Subnet] を選択した場合は、[Subnet Mask] フィールドにサブネットIPアドレスのサブネットマスクを入力します。

注：次の例では、255.255.0.0が使用されています。

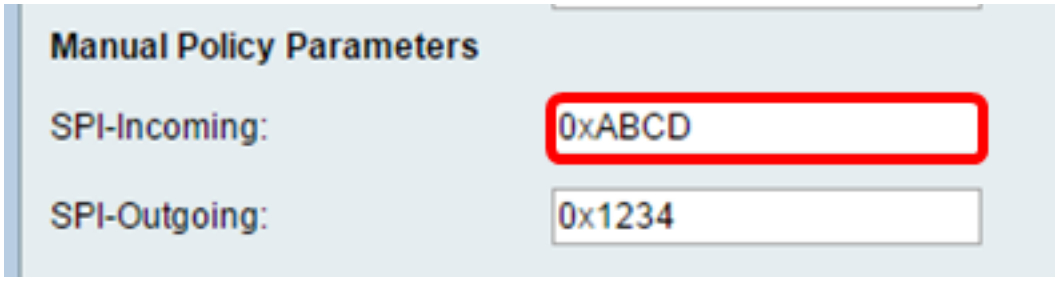


手動ポリシー パラメータ

注：これらのフィールドは、[手動ポリシー(Manual Policy)] が選択されている場合にのみ編集できます。

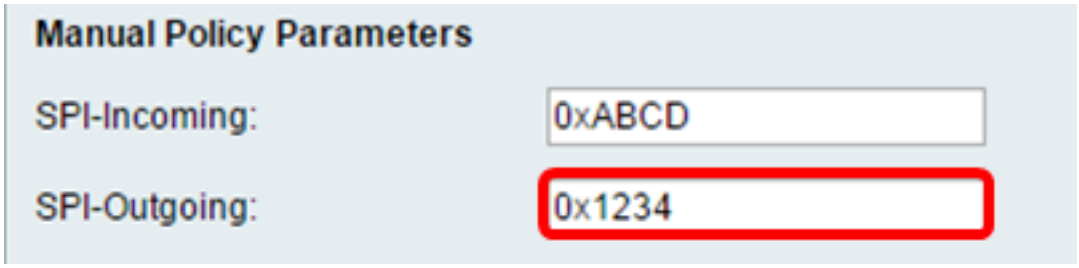
ステップ1:[SPI-Incoming] フィールドに、VPN接続の着信トラフィックのセキュリティパラメータインデックス(SPI)タグとして3 ~ 8個の16進文字を入力します。SPIタグは、あるセッションのトラフィックを他のセッションのトラフィックと区別するために使用されます。

注：この例では、0xABCDが使用されます。



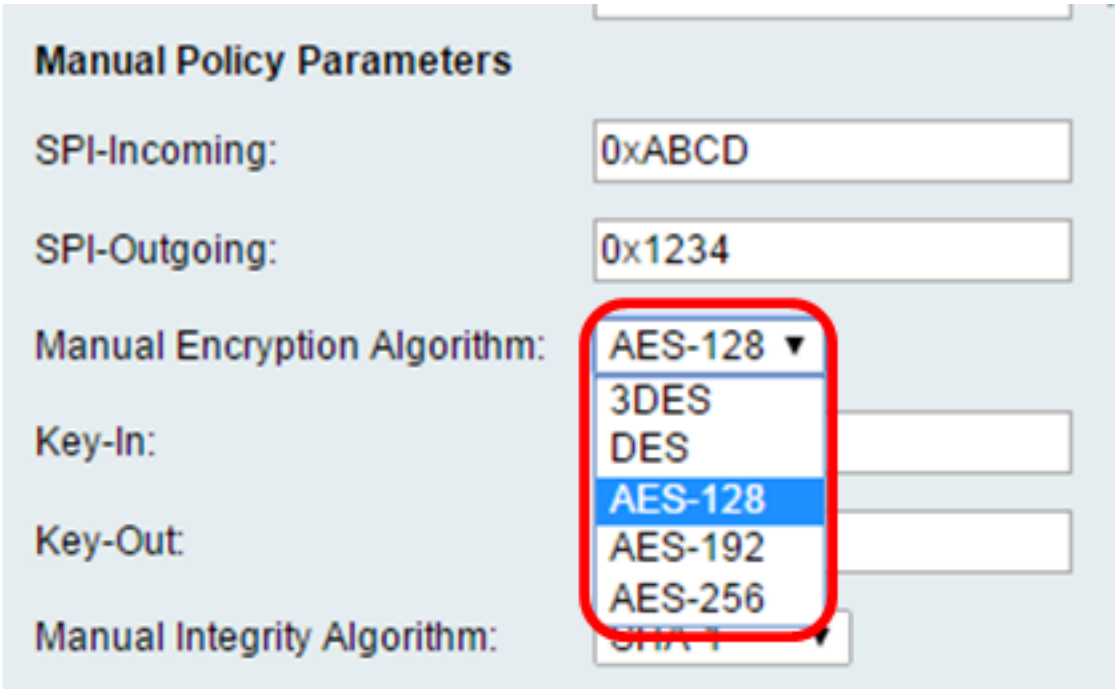
ステップ2:[SPI-Outgoing] フィールドに、VPN接続の発信トラフィックのSPIタグとして3 ~ 8個の16進文字を入力します。

注：この例では、0x1234が使用されます。



ステップ3:[Manual Encryption Algorithm]ドロップダウンリストから、オプションを選択します。選択肢は、DES、3DES、AES-128、AES-192、およびAES-256です。

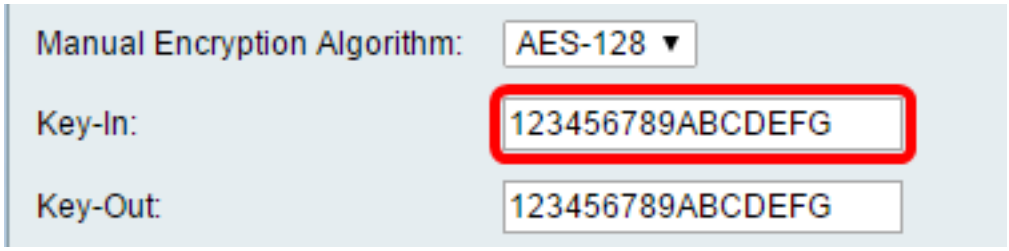
注：この例では、AES-128が選択されています。



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。

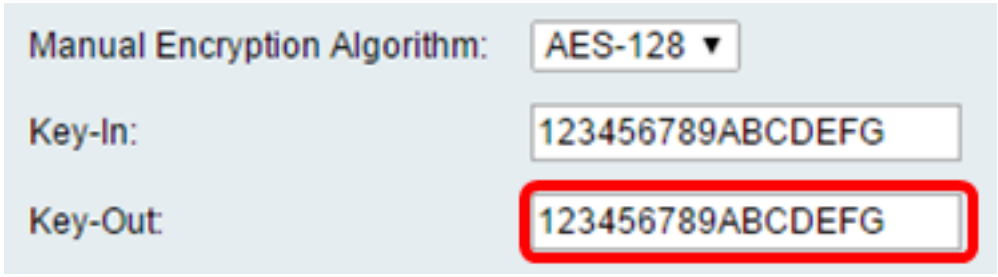
- DESは8文字のキーを使用します。
- 3DESは24文字のキーを使用します。
- AES-128は16文字のキーを使用します。
- AES-192は24文字のキーを使用します。
- AES-256は32文字のキーを使用します。

注：この例では、123456789ABCDEFGを使用します。



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。

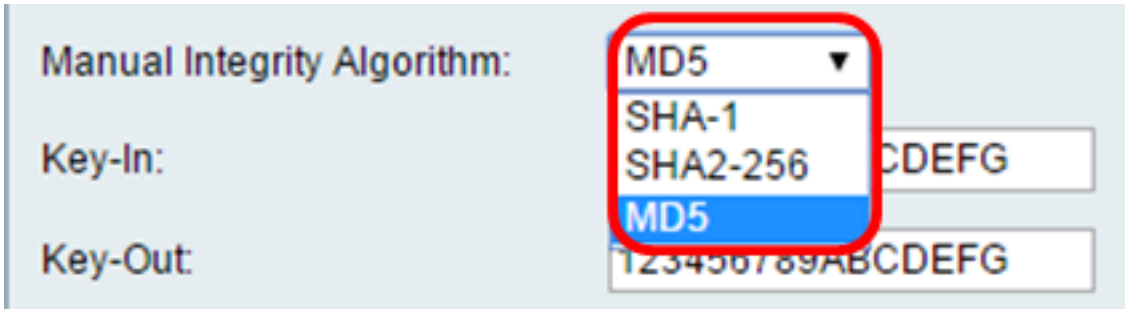
注：この例では、123456789ABCDEFGを使用します。



ステップ6:[Manual Integrity Algorithm]ドロップダウンリストからオプションを選択します。

- MD5：データ整合性のために128ビットのハッシュ値を使用します。MD5はSHA-1およびSHA2-256よりも安全ではありませんが、高速です。
- SHA-1：データ整合性のために160ビットのハッシュ値を使用します。SHA-1はMD5より低速ですが安全です。SHA-1はSHA2-256より高速ですが安全ではありません。
- SHA2-256：データ整合性のために256ビットのハッシュ値を使用します。SHA2-256はMD5およびSHA-1よりも低速ですが安全です。

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。

- MD5は16文字のキーを使用します。
- SHA-1は20文字のキーを使用します。
- SHA2-256は32文字のキーを使用します。

注：この例では、123456789ABCDEFGを使用します。

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、123456789ABCDEFGを使用します。

オートoポリシーパラメータ

注：自動VPNポリシーを作成する前に、自動VPNポリシーを作成するIKEポリシーに基づいてIKEポリシーを作成してください。これらのフィールドは、ステップ3で**自動ポリシー**が選択されている場合にのみ編集できます。

ステップ1:[IPSec *SA-Lifetime]* フィールドに、更新までのSAの存続時間を秒単位で入力します。範囲は30 ~ 86400です。デフォルトは3600です。

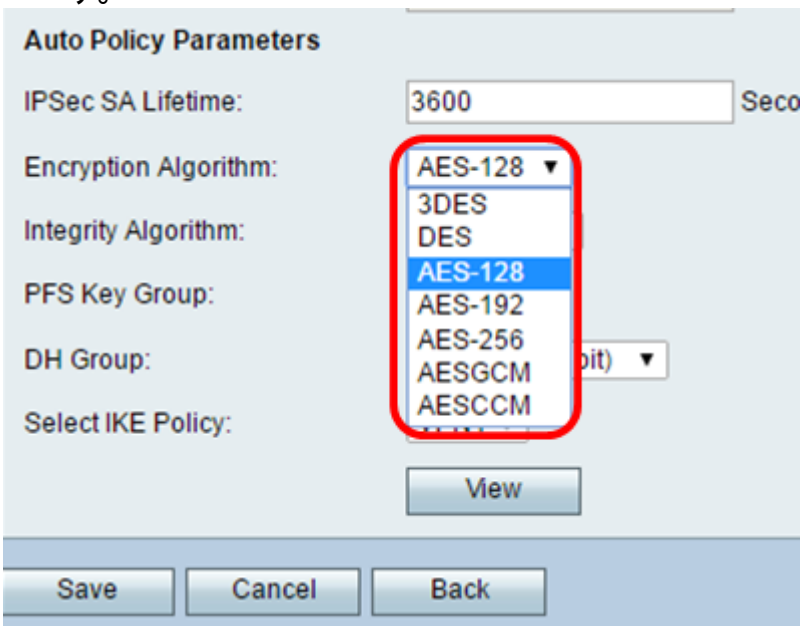
ステップ2:[Encryption Algorithm]ドロップダウンリストから、オプションを選択します。次のオプションがあります。

注：この例では、AES-128が選択されています。

- DES:56ビットの古い暗号化方式で、あまり安全な暗号化方式ではありませんが、下位互換性のために必要になる場合があります。
- 3DES：データを3回暗号化するため、キーサイズを増やすために使用される168ビットの単純な暗号化方式。これにより、DESよりもセキュリティが高くなりますが、AESよりもセキュリティが低くなります。
- AES-128:AES暗号化に128ビットキーを使用します。AESはDESよりも高速で安全です。ー

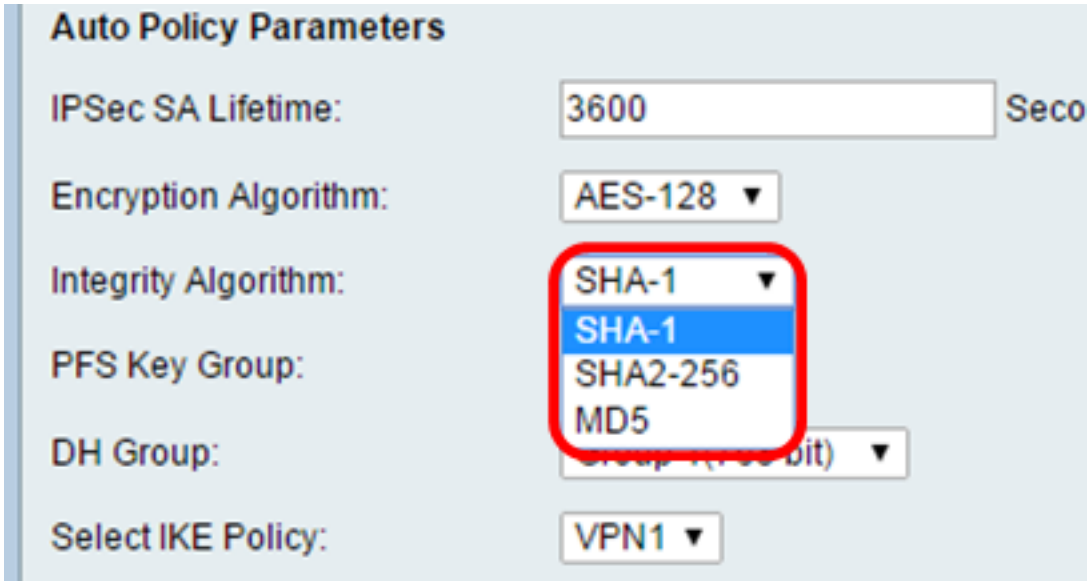
般に、AESは3DESよりも高速で安全です。AES-128は、AES-192およびAES-256よりも高速ですが安全性が低くなります。

- AES-192:AES暗号化に192ビットキーを使用します。AES-192はAES-128よりも低速ですが高い安全性を備え、AES-256よりも高速ですが低い安全性を備えています。
- AES-256:AES暗号化に256ビットキーを使用します。AES-256は低速ですが、AES-128およびAES-192よりも安全です。
- AESGCM:Advanced Encryption Standard(AES)Galois Counter Modeは、汎用認証暗号化ブロック暗号モードです。GCM認証は、ハードウェアへの効率的な実装に特に適した操作を使用するため、高速な実装や効率的でコンパクトな回路への実装に特に適しています。
- AESCCM:CBC-MACモードのAdvanced Encryption Standard(AES)カウンタは、汎用認証暗号化ブロック暗号モードです。CCMは、コンパクトなソフトウェア実装での使用に適しています。

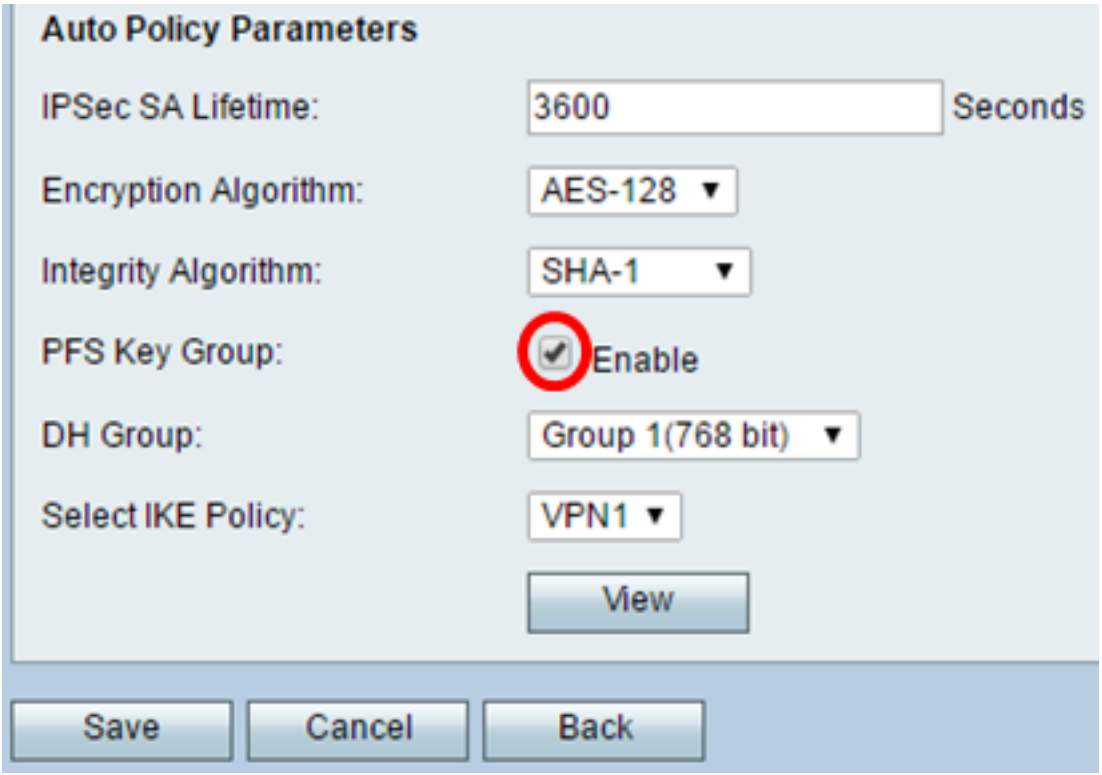


ステップ3:[Integrity Algorithm]ドロップダウンリストから、オプションを選択します。オプションは、MD5、SHA-1、およびSHA2-256です。

注：この例では、SHA-1が選択されています。

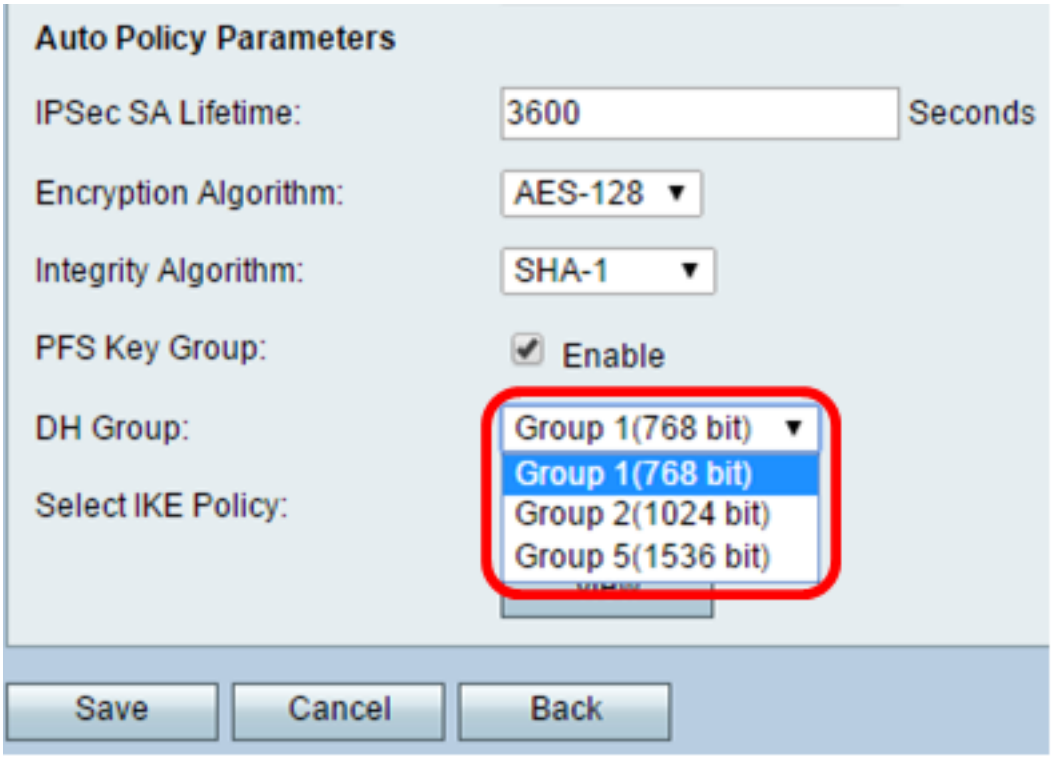


ステップ4:Perfect Forward Secrecy(PFS)を有効にするには、PFSキーグループの[Enable]チェックボックスをオンにします。PFSはVPNセキュリティを強化しますが、接続速度を遅くします。



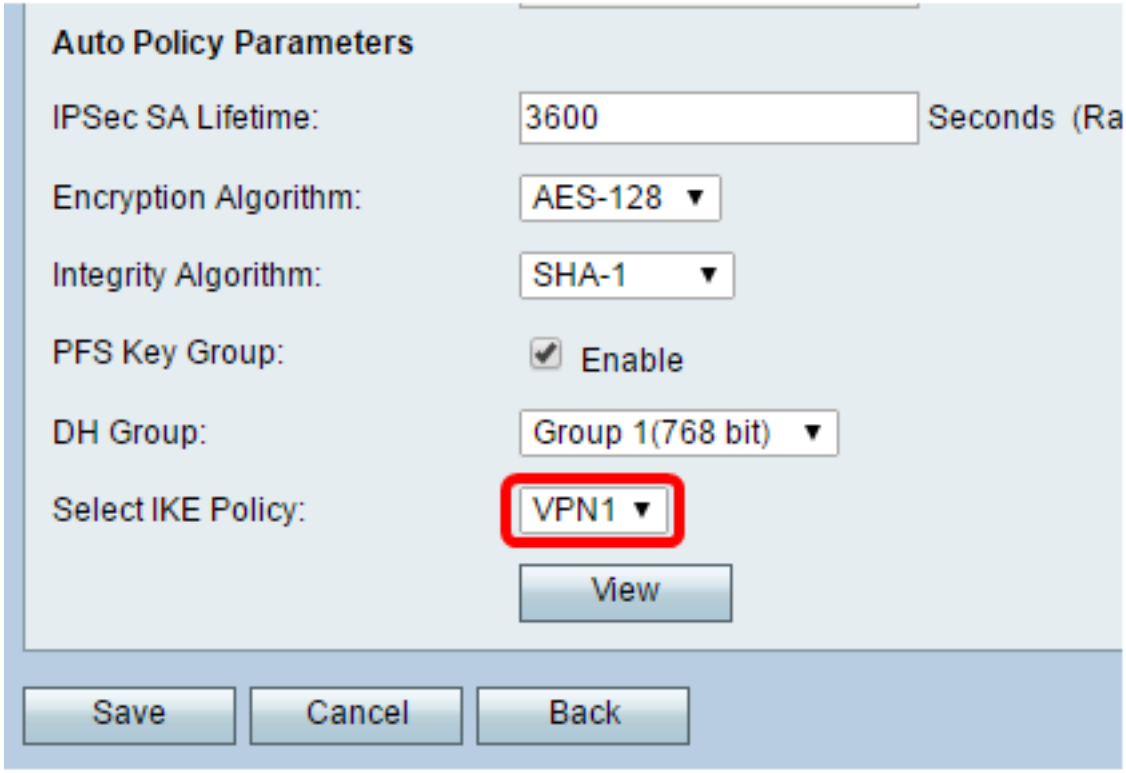
ステップ5:（オプション）ステップ4でPFSを有効にすることを選択した場合は、DHグループのドロップダウンリストから参加するDHグループを選択します。グループ番号が大きいほど、セキュリティは高くなります。

注：この例では、グループ1が選択されています。

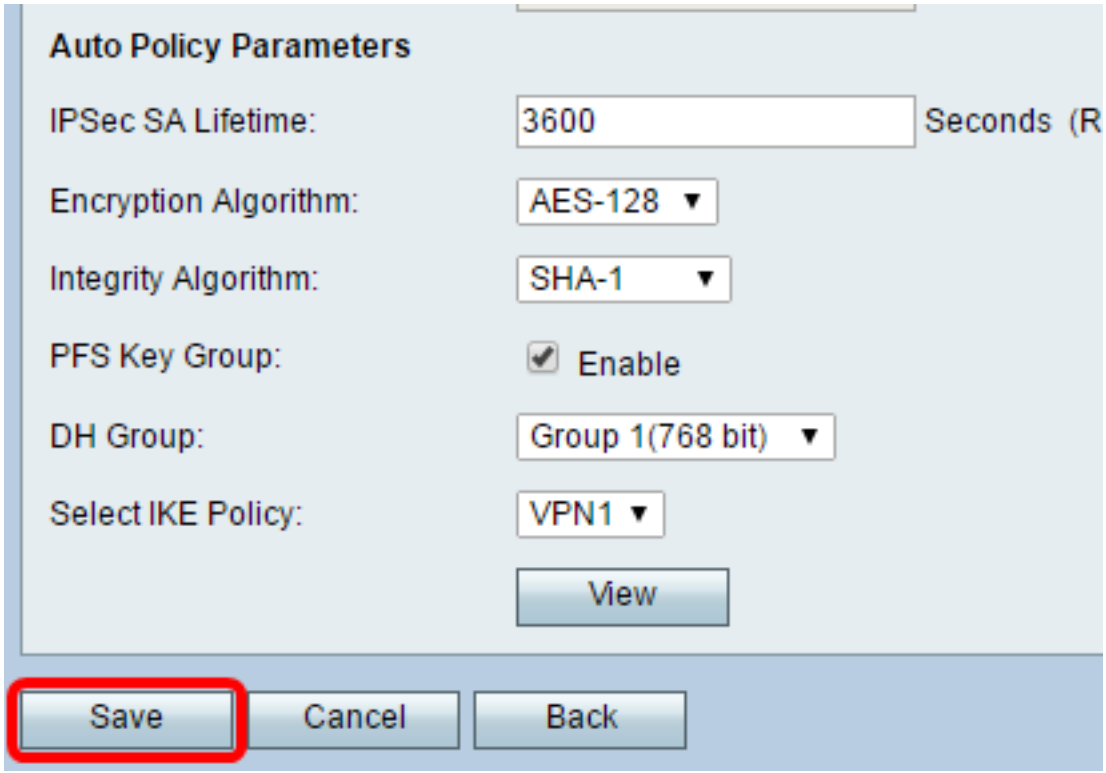


ステップ6:[Select IKE Policy]ドロップダウンリストから、VPNポリシーに使用するIKEポリシーを選択します。

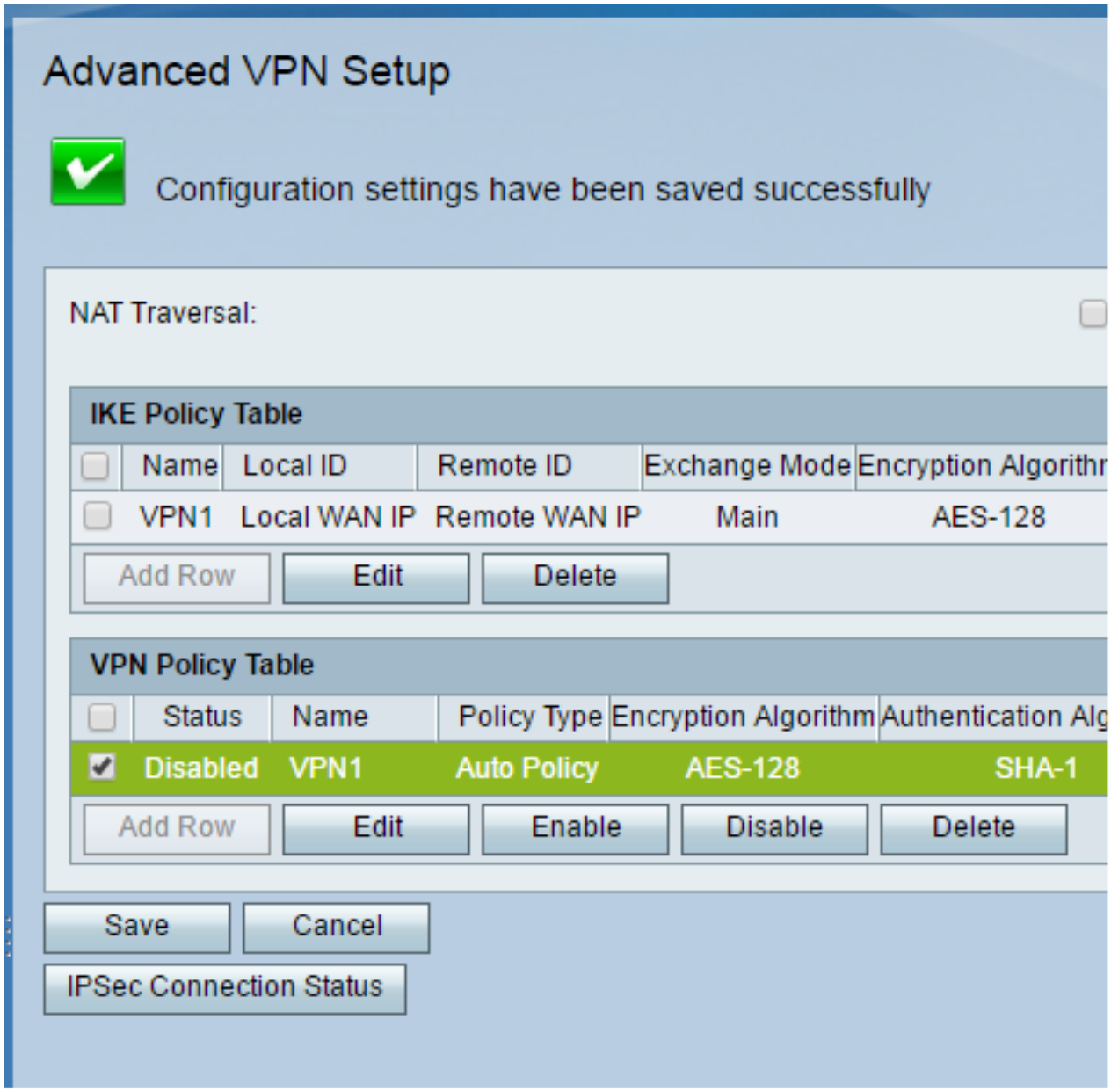
注：この例では、1つのIKEポリシーだけが設定されているため、1つのポリシーだけが表示されます。



ステップ7:[Save] をクリックします。

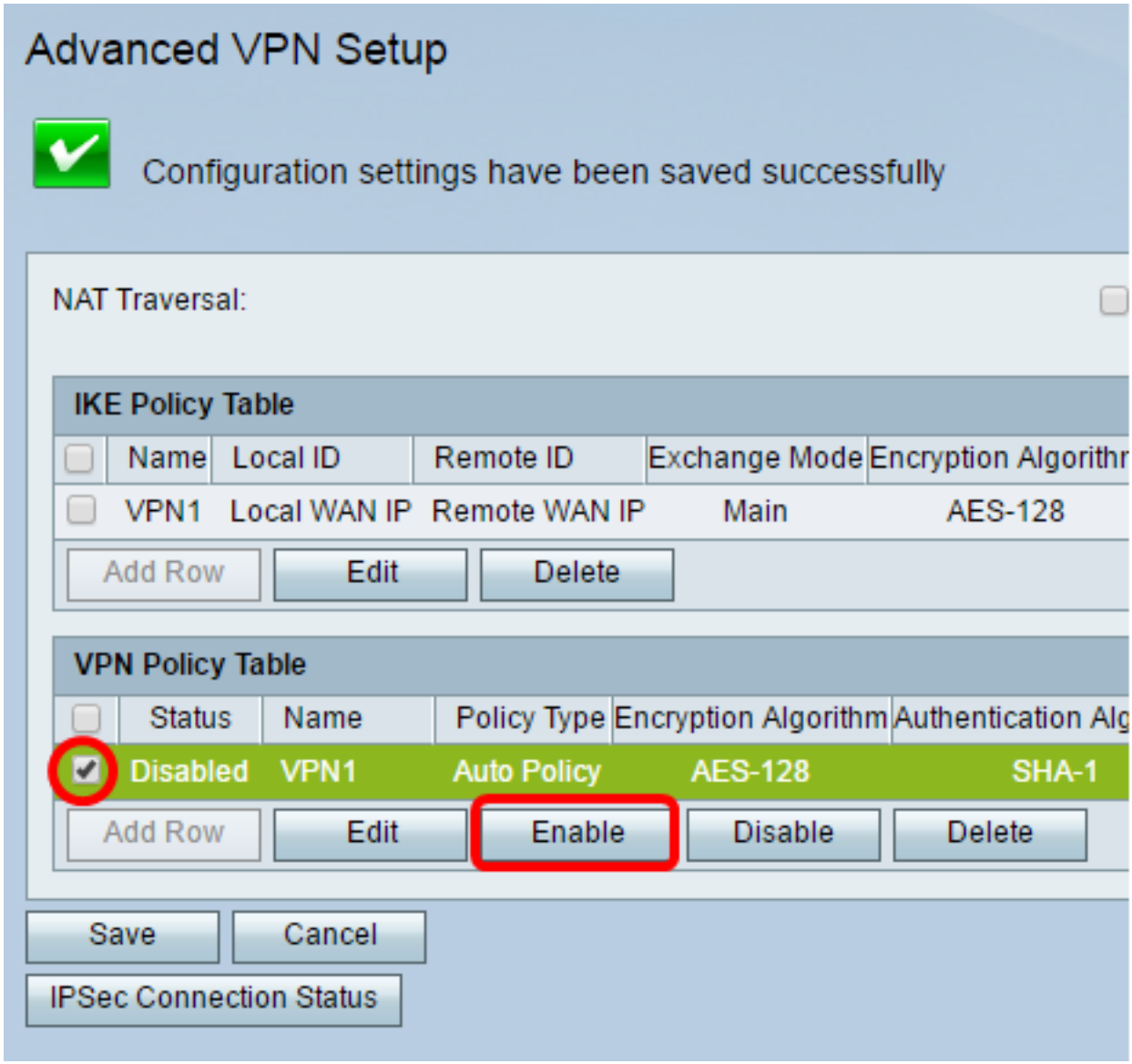


注：メインの[Advanced VPN Setup]ページが再表示されます。構成設定が正常に保存されたことを示す確認メッセージが表示されます。

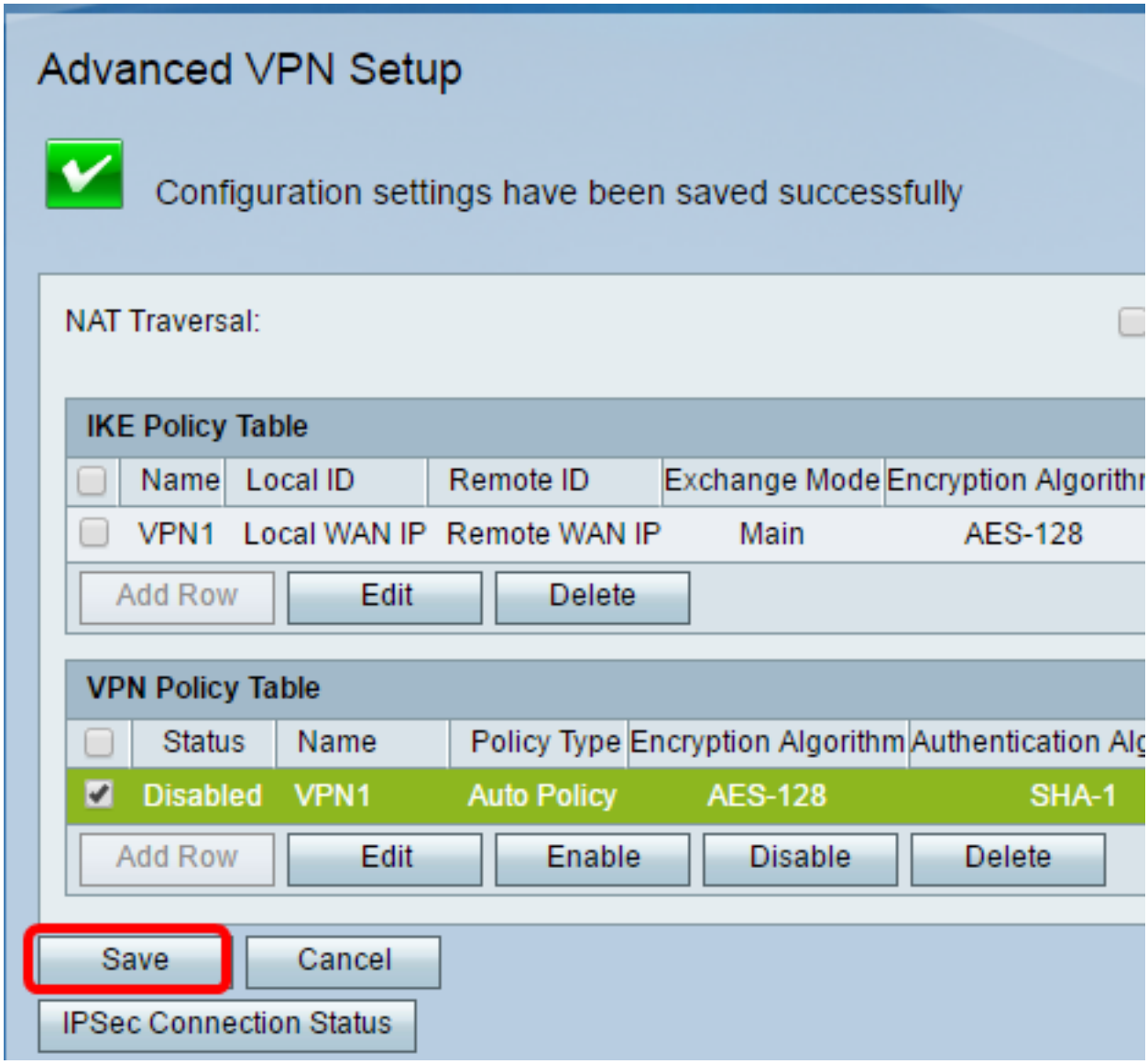


ステップ8:[VPN Policy]テーブルで、VPNを選択するチェックボックスをオンにして、[Enable] をクリックします。

注：設定されたVPNポリシーはデフォルトで無効になっています。



ステップ9:[Save] をクリックします。



これで、RV130またはRV130Wルータに VPNポリシーが正常に設定されました。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。