RV016、RV042、RV042G、およびRV082 VPNルータでのゲートウェイ間VPNの設定

目的

仮想プライベートネットワーク(VPN)は、パブリックインターネット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間にセキュアな接続を形成するために使用されます。具体的には、ゲートウェイ間VPN接続では、2台のルータを安全に接続し、一方の端にあるクライアントを、もう一方の端にあるネットワークの一部であるかのように論理的に認識させることができます。これにより、データとリソースをインターネット経由でより簡単かつ安全に共有できます。

ゲートウェイ間VPNを有効にするには、両方のルータで設定を行う必要があります。「ローカルグループの設定」と「リモートグループの設定」のセクションで行った設定は、一方のローカルグループがもう一方のリモートグループになるように、2台のルータ間で逆にする必要があります。

このドキュメントの目的は、RV016、RV042、RV042G、およびRV082 VPNシリーズルータでゲートウェイ間VPNを設定する方法について説明することです。

適用可能なデバイス

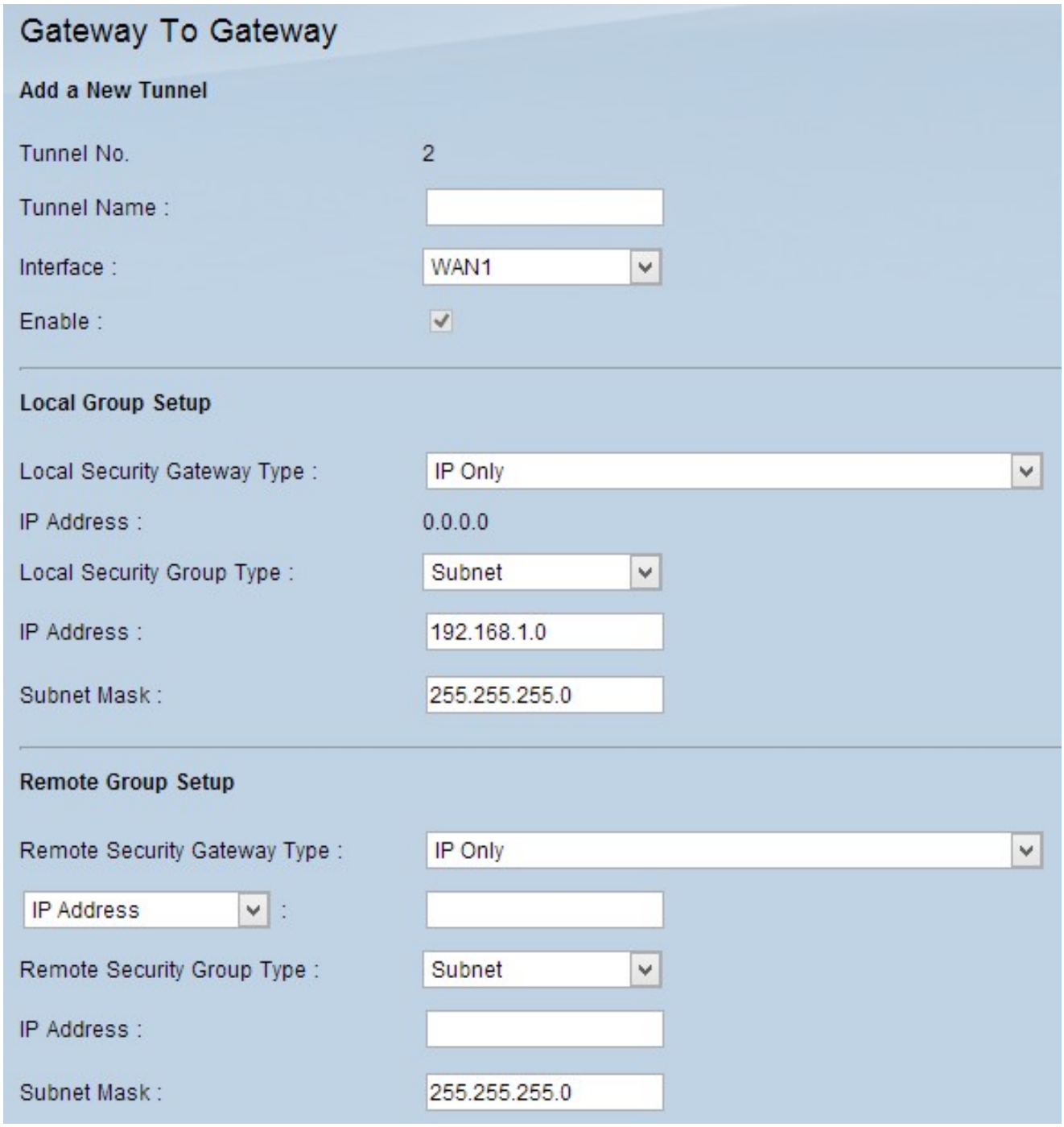
- RV016
- RV042
- RV042G
- RV082

[Software Version]

- v4.2.2.08

ゲートウェイからゲートウェイへのVPNの設定

ステップ 1：Router Configuration Utilityにログインし、VPN > Gateway to Gatewayの順に選択します。「ゲートウェイからゲートウェイへ」ページが開きます。



ゲートウェイからゲートウェイへのVPNを設定するには、次の機能を設定する必要があります。

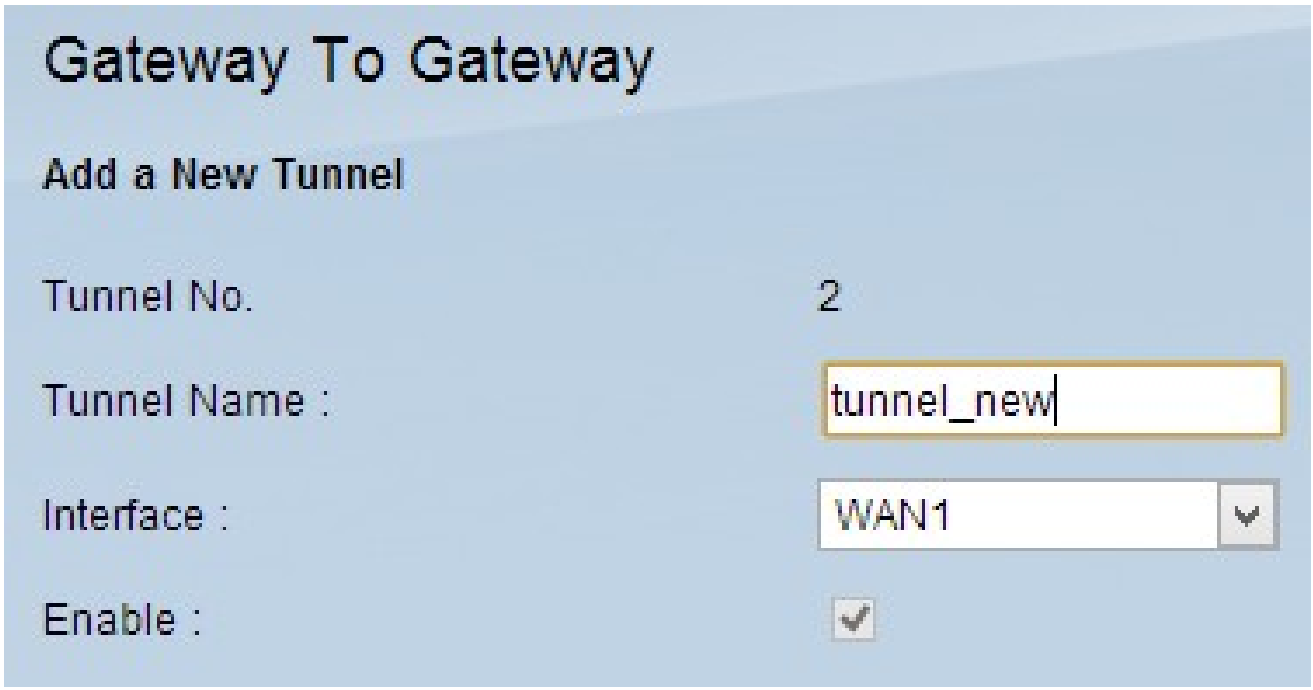
1. 新しいトンネルの追加

2. ローカルグループの設定

3.リモートグループセットアップ

4. IPSecの設定

新しいトンネルの追加



Tunnel No.は、作成される現在のトンネルを表示する読み取り専用フィールドです。

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。トンネルの反対側で使用される名前と一致してい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。

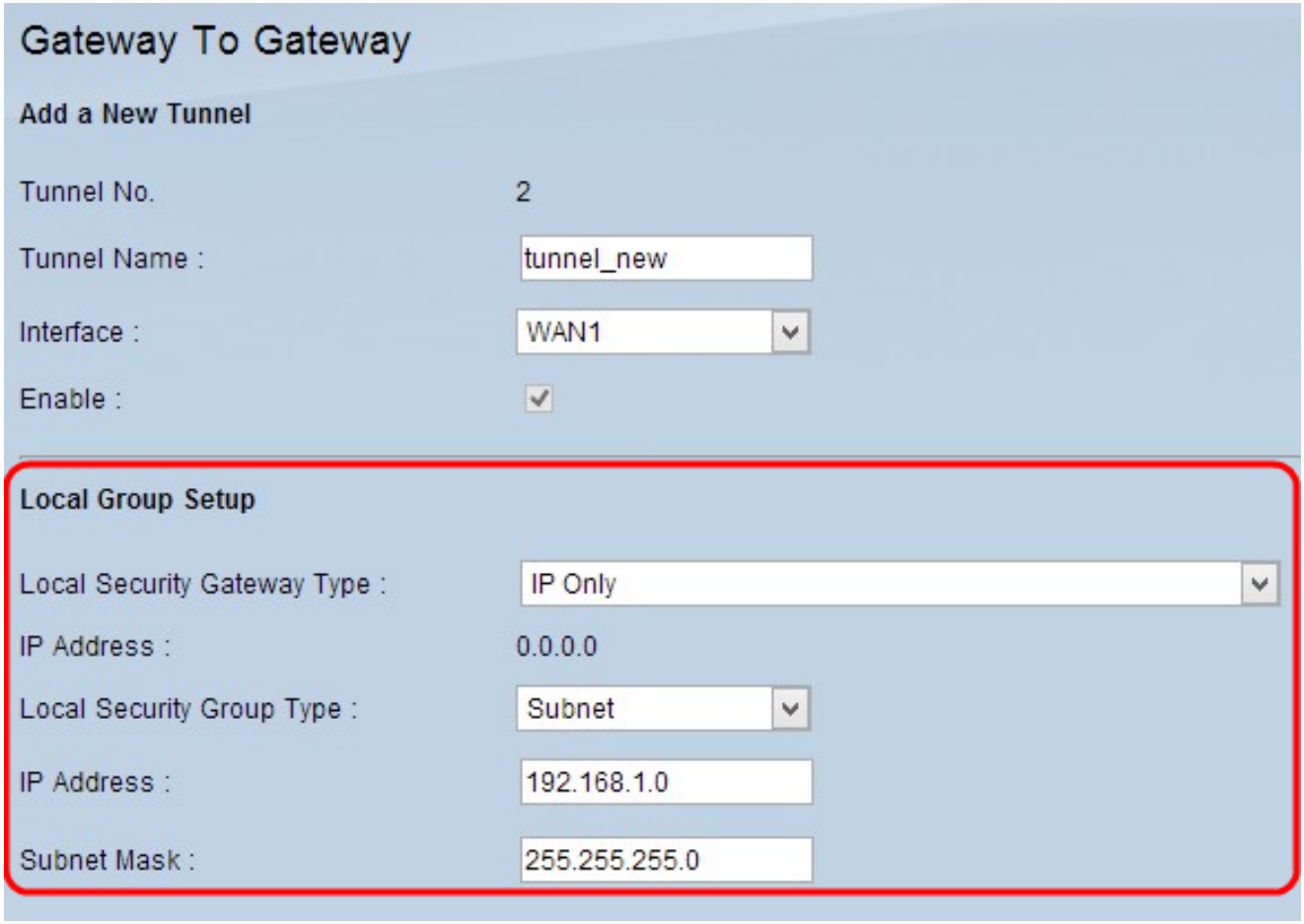
- WAN1:RV0XXシリーズVPNルータの専用WANポート。

- WAN2:RV0XXシリーズVPNルータのWAN2/DMZポート。WANとして設定され、非武装地帯(DMZ)ポートとして設定されていない場合にのみ、ドロップダウンメニューに表示されます。

ステップ3: (オプション) VPNを有効にするには、Enableフィールドのチェックボックスをオンにします。VPNはデフォルトで有効になっています。

ローカルグループの設定

注：一方のルータのローカルグループセットアップの設定は、もう一方のルータのリモートグループセットアップの設定と同じである必要があります。



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ための適切なルータ識別方法を選択します。

・ IPのみ：ローカルルータ（このルータ）はスタティックIPアドレスによって認識されます。このオプションは、ルータにスタティックWAN IPがある場合にのみ選択できます。スタティックWAN IPアドレスがIP Addressフィールドに自動的に表示されます。

・ IP +ドメイン名(FQDN)認証：静的IPアドレスと登録済みドメイン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、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アドレスがIP Addressフィールドに自動的に表示されます。

・ 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、[電子メールアドレス]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アドレスがIP Addressフィールドに自動的に表示されます。

・ダイナミックIP +ドメイン名(FQDN)認証：ダイナミックIPアドレスと登録済みドメインを介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、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。

・ダイナミックIP + Email Addr(USER FQDN)認証：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、[電子メールアドレス]フィールドに電子メールアドレスを入力します。

ステップ 2：Local Security Groupドロップダウンリストから、VPNトンネルにアクセスできる適切なローカルLANユーザまたはユーザグループを選択します。デフォルトはSubnetです。

・ IP:1つのLANデバイスのみがVPN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、IP AddressフィールドにLANデバイスのIPアドレスを入力します。

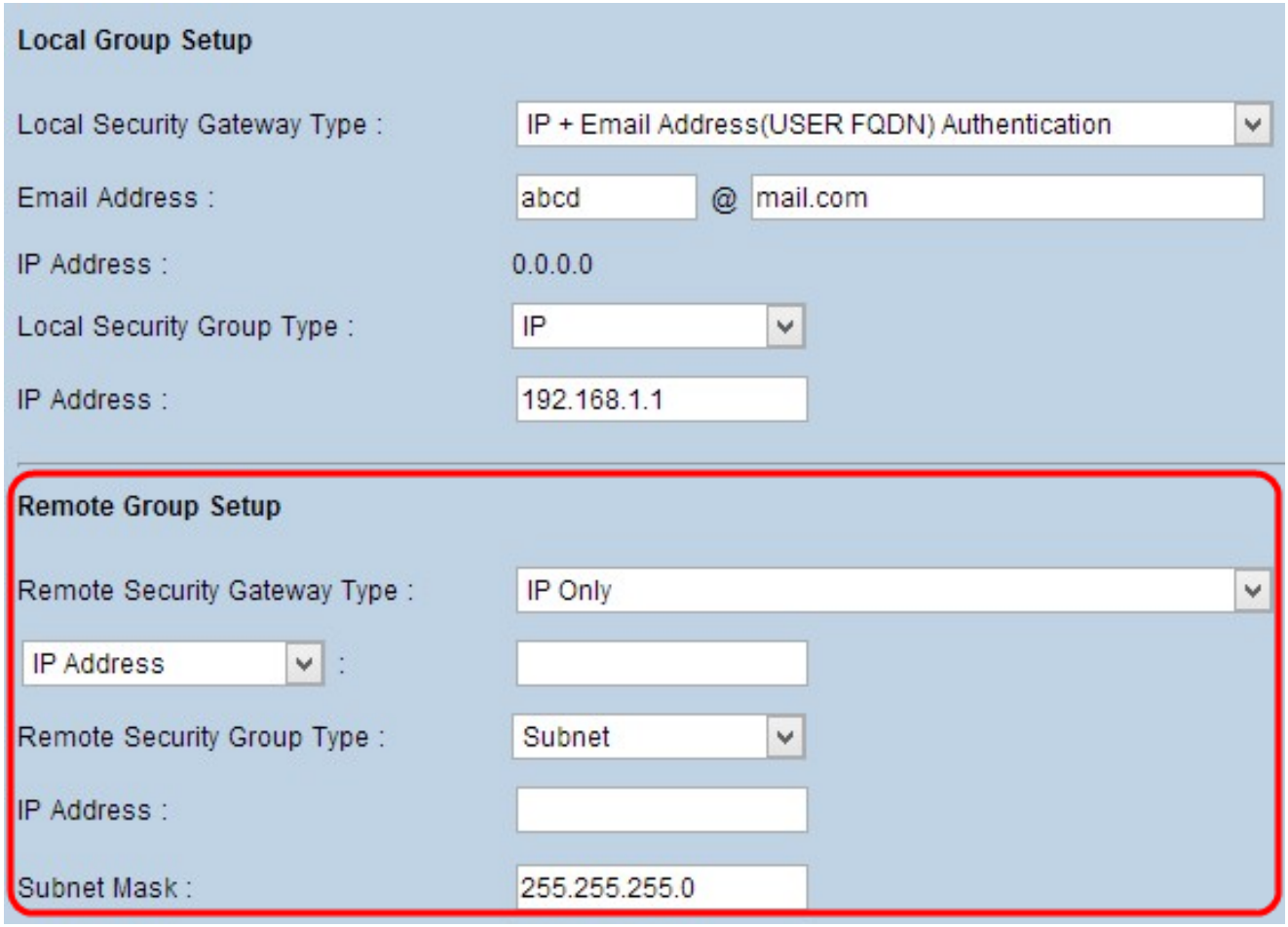
・サブネット：特定のサブネット上のすべてのLANデバイスがトンネルにアクセスできます。このオプションを選択した場合は、LANデバイスのサブネットワークIPアドレスとサブネットマスクをそれぞれIPアドレスフィールドとサブネットマスクフィールドに入力します。デフォルトマスクは255.255.255.0です。

・ IP範囲：一定範囲のLANデバイスが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、Begin IPフィールドに開始IPアドレスを、End IPフィールドに終了IPアドレスを、それぞれ入力します。

ステップ 3：[Save] をクリックして、設定を保存します。

リモートグループ設定

注：一方のルータのリモートグループセットアップの設定は、もう一方のルータのローカルグループセットアップの設定と同じである必要があります。



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リモートルータを識別する方法を選択します。

・ IPのみ：スタティックWAN IPを介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にあるドロップダウンリストからIPアドレスを選択し、IPアドレスを入力します。IPアドレスはわからないがドメイン名はわかっている場合は、IP by DNS Resolvedを選択し、IP by DNS Resolvedフィールドにルータのドメイン名を入力します。

・ IP +ドメイン名(FQDN)認証：ルータの静的IPアドレスと登録済みドメインを使用して、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にある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アドレスはわからないがドメイン名はわかっている場合は、IP by DNS Resolvedを選択し、IP by DNS Resolvedフィールドにルータのドメイン名を入力します。Domain Nameフィールドに、ルータのドメイン名を入力します。この際、ルータの識別方法に関係なく、この名前を使用します。

・ 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にある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アドレスはわからないがドメイン名はわかって

いる場合は、IP by DNS Resolvedを選択し、IP by DNS Resolvedフィールドにルータのドメイン名を入力します。Email Addressフィールドに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：ダイナミックIPアドレスと登録済みドメインを介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、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。

・ダイナミックIP + Email Addr(USER FQDN)認証：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 Email Addressを入力します。

ステップ 2：Remote Security Group Typeドロップダウンリストから、VPNトンネルにアクセスできる適切なリモートLANユーザまたはユーザグループを選択します。

・ IP：特定の1つのLANデバイスだけが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、IP AddressフィールドにLANデバイスのIPアドレスを入力します。

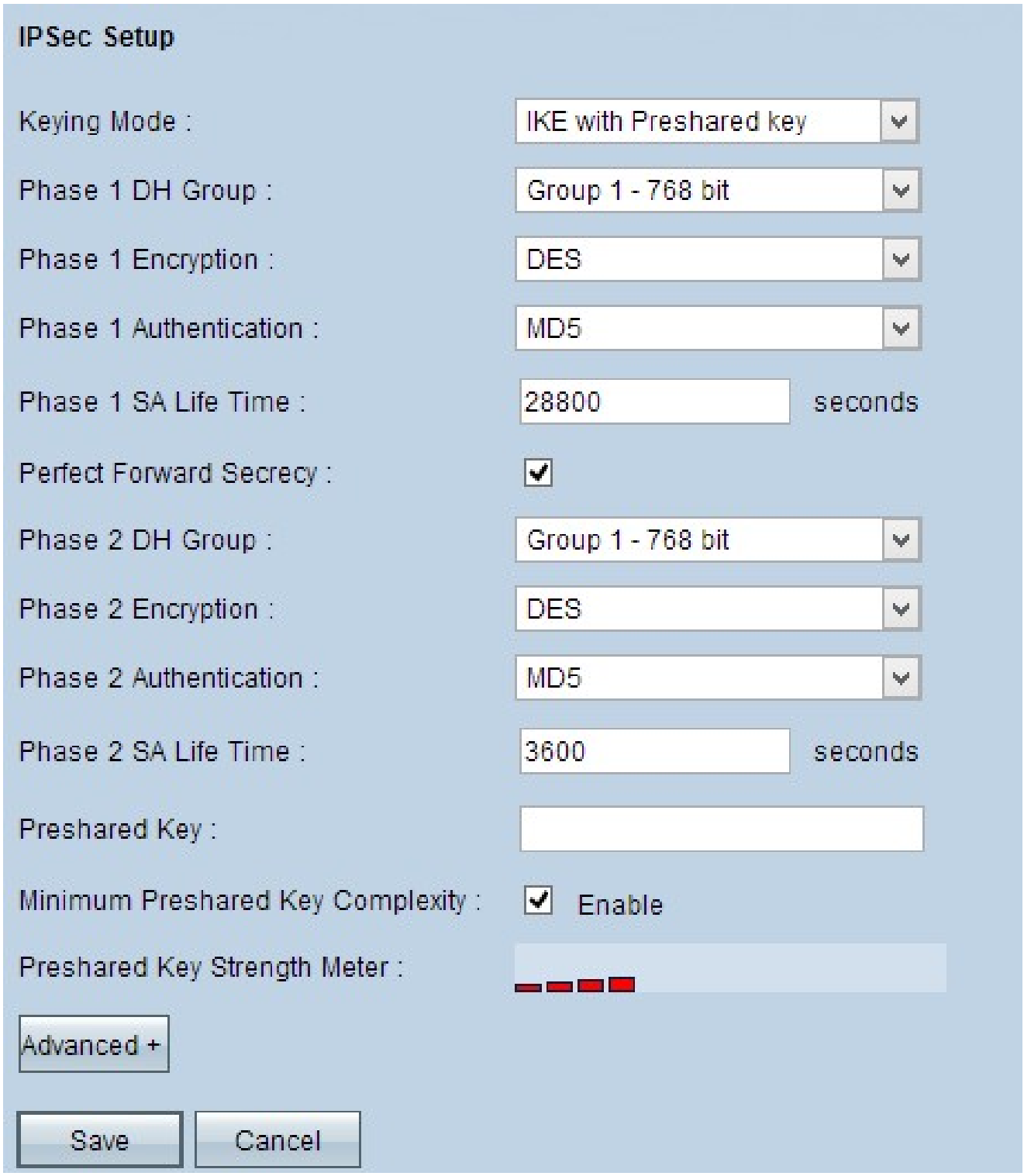
・サブネット：特定のサブネット上のすべてのLANデバイスがトンネルにアクセスできます。このオプションを選択した場合は、LANデバイスのサブネットワークIPアドレスとサブネットマスクをそれぞれIPアドレスフィールドとサブネットマスクフィールドに入力します。

・ IP範囲：一定範囲のLANデバイスが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、Begin IPフィールドに開始IPアドレスを、End IPフィールドに終了IPアドレスを、それぞれ入力します。

注：トンネルの終端にある2台のルータを同じサブネット上に配置することはできません。

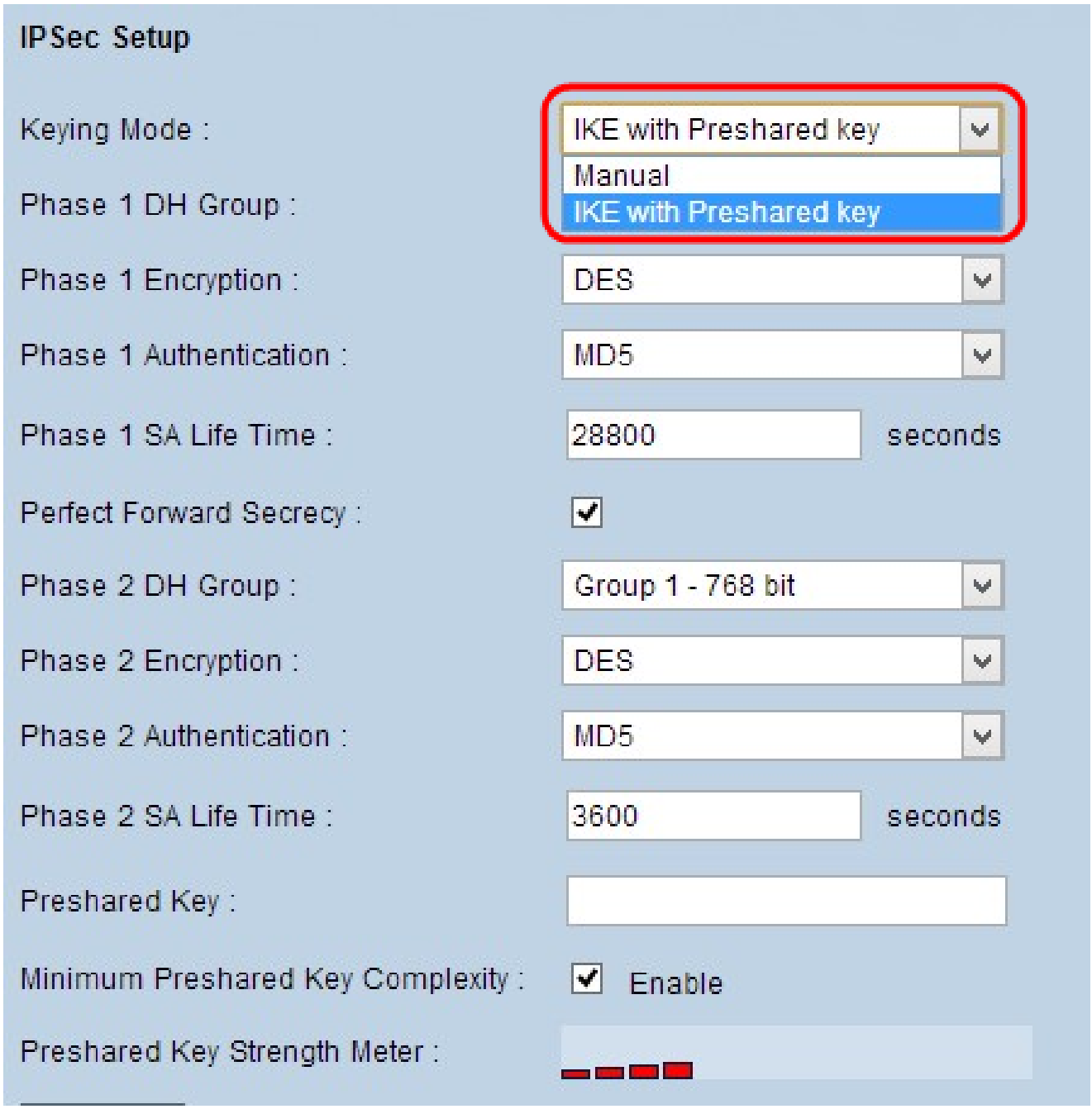
ステップ 3：[Save] をクリックして、設定を保存します。

IPSecの設定



Internet Protocol Security(IPSec)は、通信セッション中に認証と暗号化を通じてエンドツーエンドのセキュリティを提供するインターネット層のセキュリティプロトコルです。

注：VPNの両端が正しく動作するには、暗号化、復号化、および認証の方式が同じである必要があります。両方のルータで同じIPSecセットアップ設定を入力します。

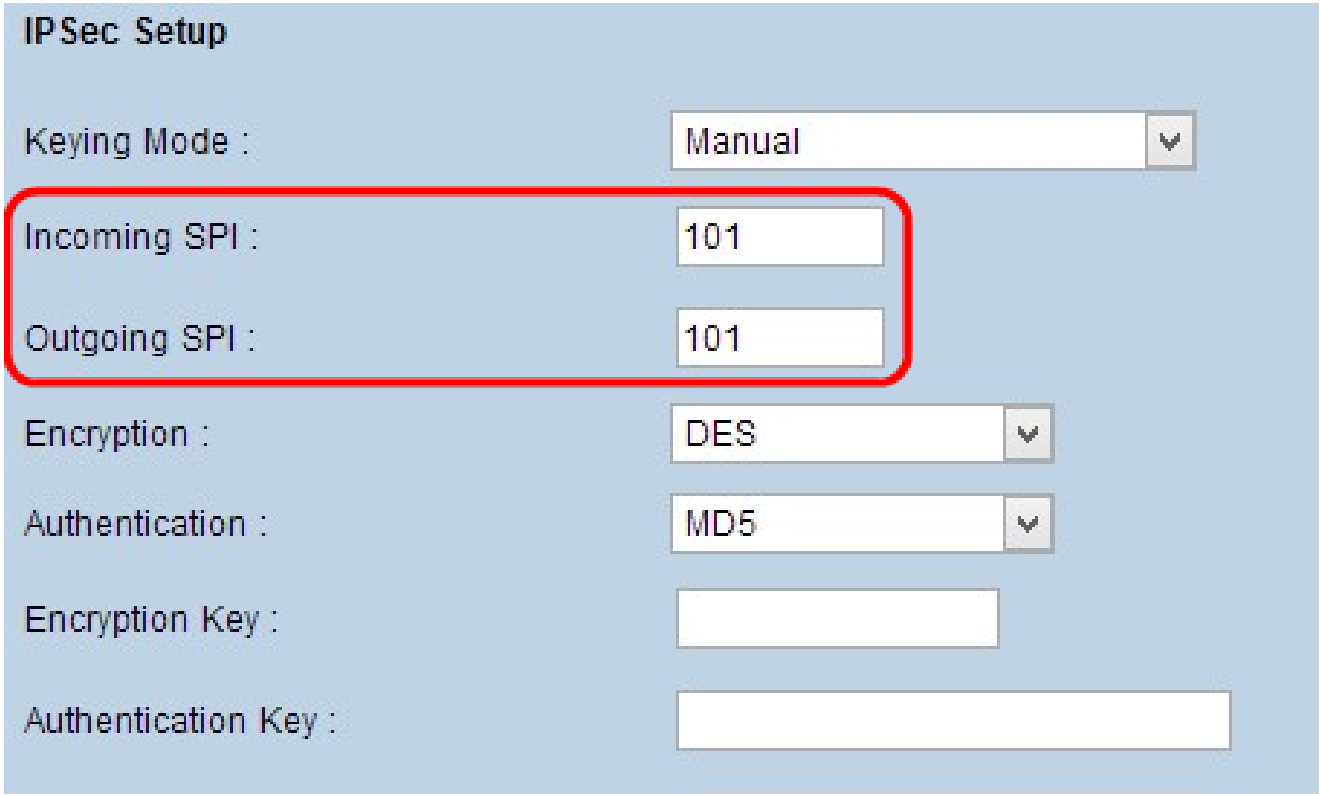


ステップ 1：Keying Modeドロップダウンリストから、セキュリティを確保するための適切なキー管理モードを選択します。デフォルトのモードは、事前共有キーを使用したIKEです。

・ Manual：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。これは、トラブルシューティング時や小規模な静的な環境で使用するのが最適です。

・ 事前共有キーを使用したIKE:Internet Key Exchange（IKE；インターネットキーエクスチェンジ）プロトコルは、事前共有キーを自動的に生成して交換し、トンネルの認証通信を確立するために使用されます。

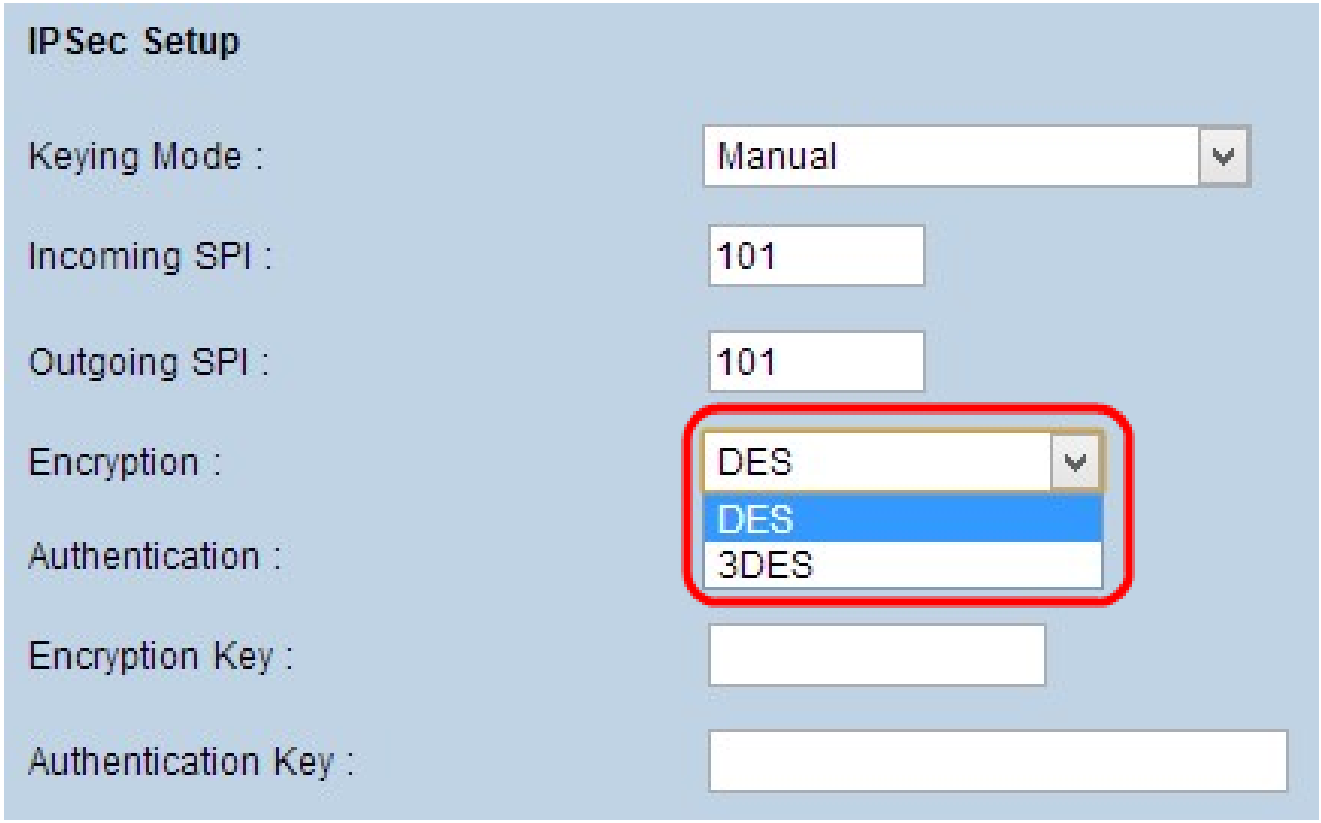
手動キーイングモードのIPSec設定



ステップ 1：着信SPIフィールドに、着信SPIの一意の16進数値を入力します。SPIはEncapsulating Security Payload Protocol(ESP)ヘッダーで伝送され、着信パケットの保護を決定します。100 ~ ffffffffの値を入力できます。ローカルルータの着信SPIは、リモートルータの発信SPIと一致する必要があります。

ステップ 2：発信SPIフィールドに、発信SPIの一意の16進数値を入力します。 100 ~ ffffffffの値を入力できます。リモートルータの発信SPIは、ローカルルータの着信SPIと一致する必要があります。

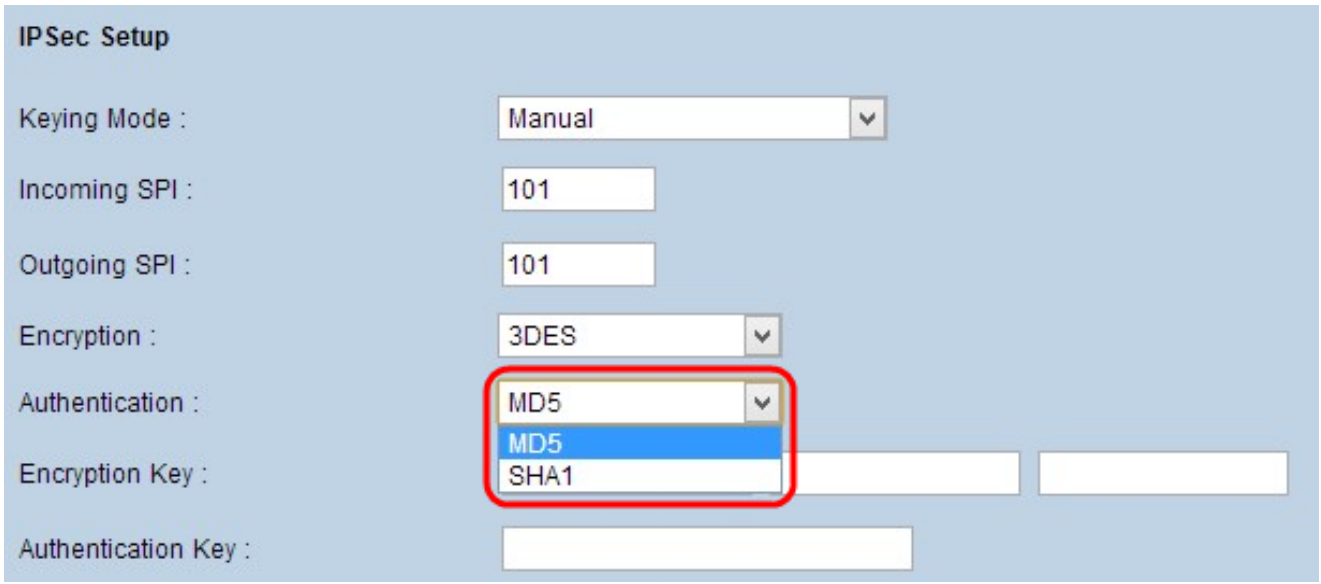
注：2つのトンネルに同じSPIを設定することはできません。



ステップ 3：Encryptionドロップダウンリストから、データに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トンネルでは、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）では、データ暗号化に56ビットのキーサイズが使用されます。DESは旧式であり、1つのエンドポイントがDESのみをサポートする場合にのみ使用する必要があります。

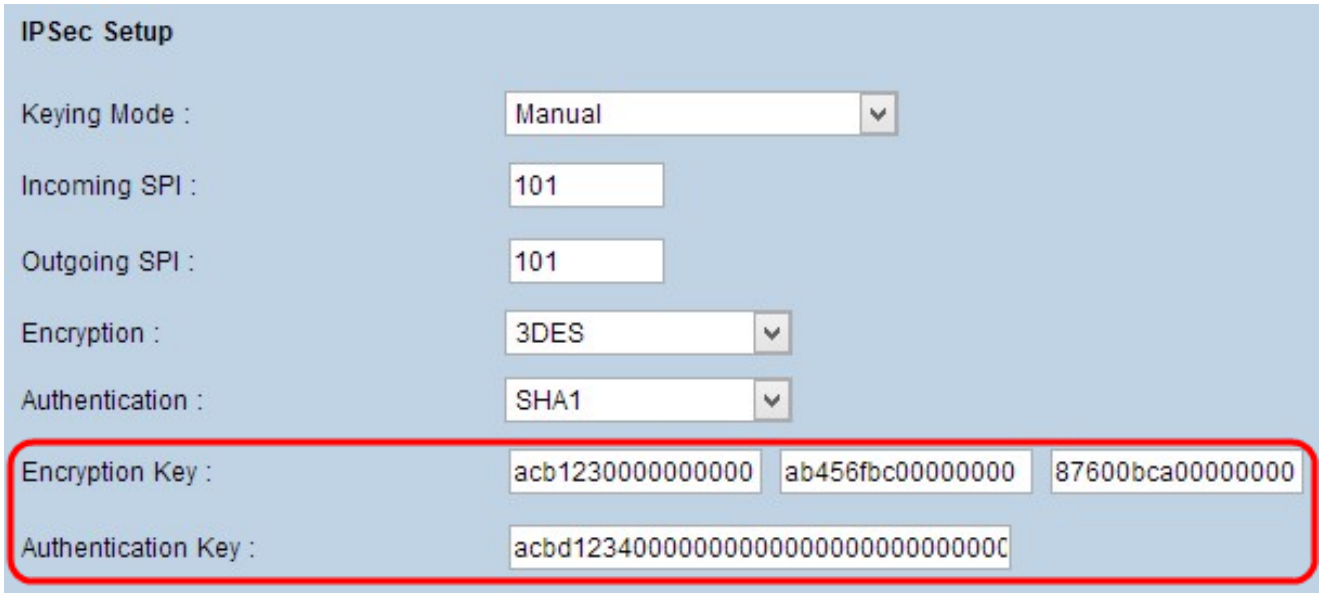
・ 3DES:Triple Data Encryption Standard(3DES)は168ビットのシンプルな暗号化方式です。3DESはデータを3回暗号化するため、DESよりもセキュリティが強化されます。



ステップ 4： Authenticationドロップダウンリストから、データに適切な認証方式を選択します。MD5よりも安全であるため、推奨される認証はSHA1です。 VPNトンネルでは、両端で同じ認証方式を使用する必要があります。

・ MD5:Message Digest Algorithm-5(MD5)は、チェックサム計算によって悪意のある攻撃からデータを保護する128ビットハッシュ関数です。

・ SHA1:Secure Hash Algorithm(SHA)バージョン1(SHA1)は160ビットのハッシュ関数で、MD5よりも安全ですが、計算に時間がかかります。

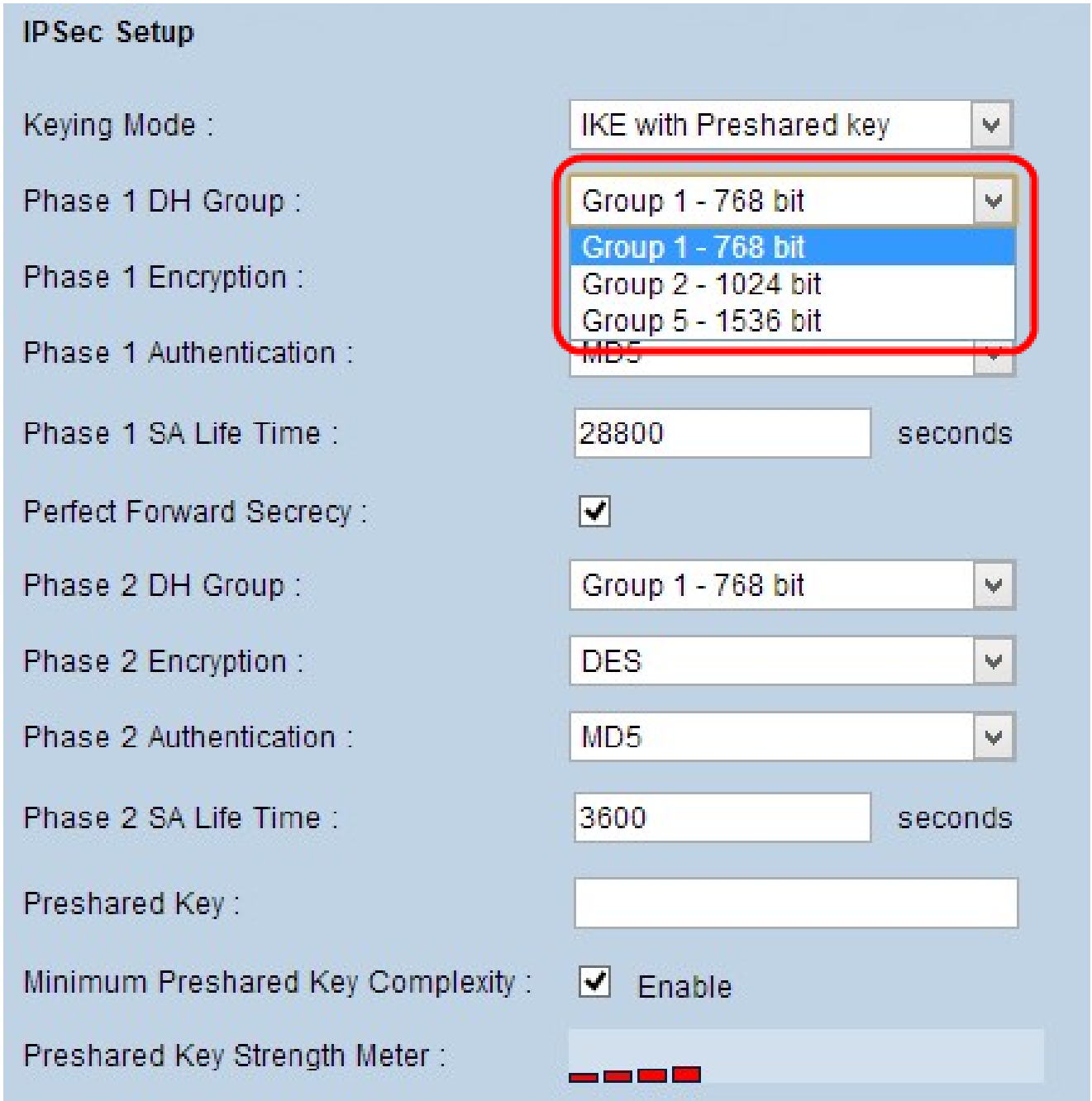


ステップ 5：Encryption Keyフィールドに、データを暗号化および復号化するためのキーを入力します。ステップ3で暗号化方式としてDESを選択した場合は、16桁の16進数値を入力します。手順3で暗号化方式として3DESを選択した場合は、40桁の16進数値を入力します。

手順 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。 手順4で認証方式としてMD5を選択する場合は、32桁の16進数値を入力します。手順4で認証方式としてSHA1を選択した場合は、40桁の16進数値を入力します。十分な桁数を追加しないと、十分な桁数になるまで末尾にゼロが追加されます。VPNトンネルでは、両端で同じ事前共有キーを使用する必要があります。

手順 7：[Save] をクリックして、設定を保存します。

事前共有キーモードを使用したIKEの設定

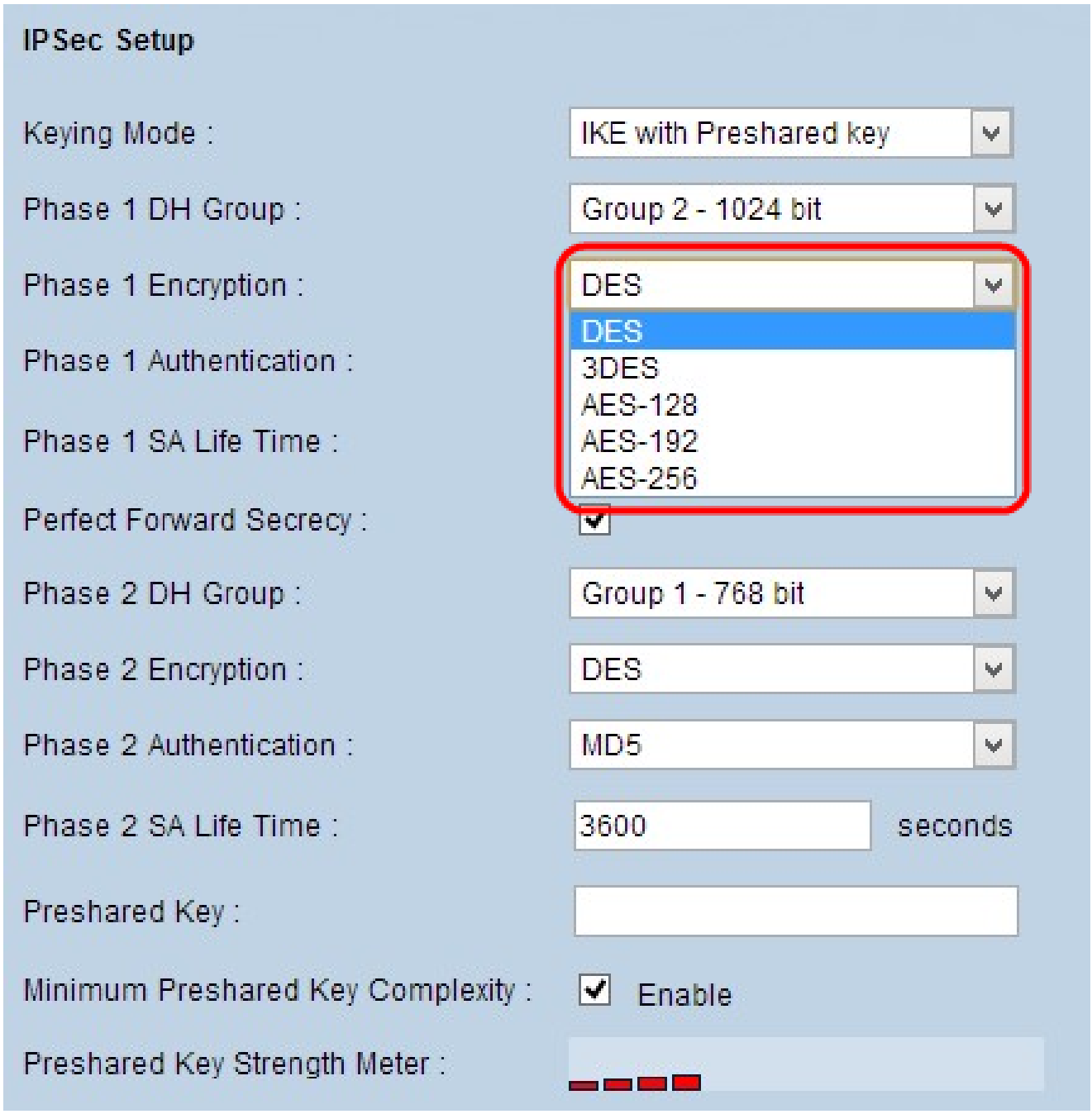


ステップ 1：Phase 1 DH Groupドロップダウンリストから、適切なPhase 1 DH Groupを選択します。フェーズ1は、トンネルの両端の間にシンプレックスの論理セキュリティアソシエーション(SA)を確立して、セキュアな認証通信をサポートするために使用されます。Diffie-Hellman(DH)は、フェーズ1の間にキーの強度を決定するために使用される暗号鍵交換プロトコルであり、通信を認証するために秘密鍵も共有します。

・ Group 1 - 768ビット：最も強度の低いキーで、最も安全性の低い認証グループですが、IKEキーの計算に必要な時間は最も短くなります。このオプションは、ネットワークの速度が遅い場合に推奨されます。

・ グループ2 - 1024ビット：グループ1よりも強度が高くセキュアな認証グループですが、IKEキーの計算に時間がかかります。

・ グループ5 - 1536ビット：最も強度の高いキーで、最も安全な認証グループ。IKEキーを計算するには、さらに時間が必要です。ネットワークの速度が速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、キーを暗号化するための適切なPhase 1 Encryptionを選択します。AES-128、AES-192、またはAES-256が推奨されます。 VPNトンネルでは、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）では、データ暗号化に56ビットのキーサイズが使用されます。DESは旧式であり、1つのエンドポイントがDESのみをサポートする場合にのみ使用する必要があります。

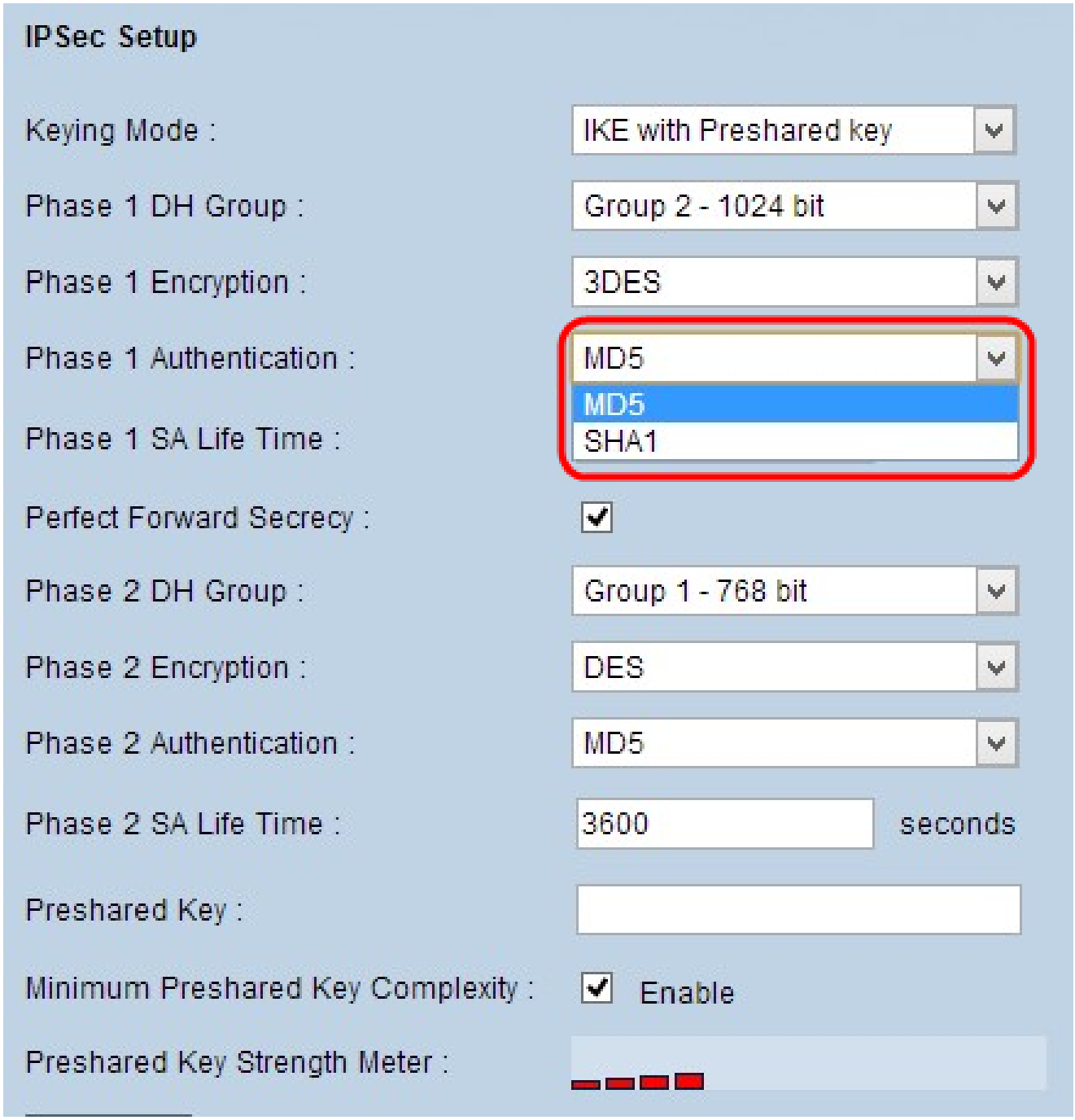
・ 3DES:Triple Data Encryption Standard(3DES)は168ビットのシンプルな暗号化方式です。3DESはデータを3回暗号化するため、DESよりもセキュリティが強化されます。

・ AES-128:Advanced Encryption Standard(AES)は、10サイクルの繰り返しによってプレ

ーンテキストを暗号化テキストに変換する128ビットの暗号化方式です。

・ AES-192:Advanced Encryption Standard(AES)は、12サイクルの繰り返しによってプレーンテキストを暗号化テキストに変換する192ビットの暗号化方式です。AES-128よりもAES-192の方が安全です。

・ AES-256:Advanced Encryption Standard(AES)は、14サイクルの繰り返しによってプレーンテキストを暗号テキストに変換する256ビットの暗号化方式です。AES-256は、最も安全な暗号化方式です。

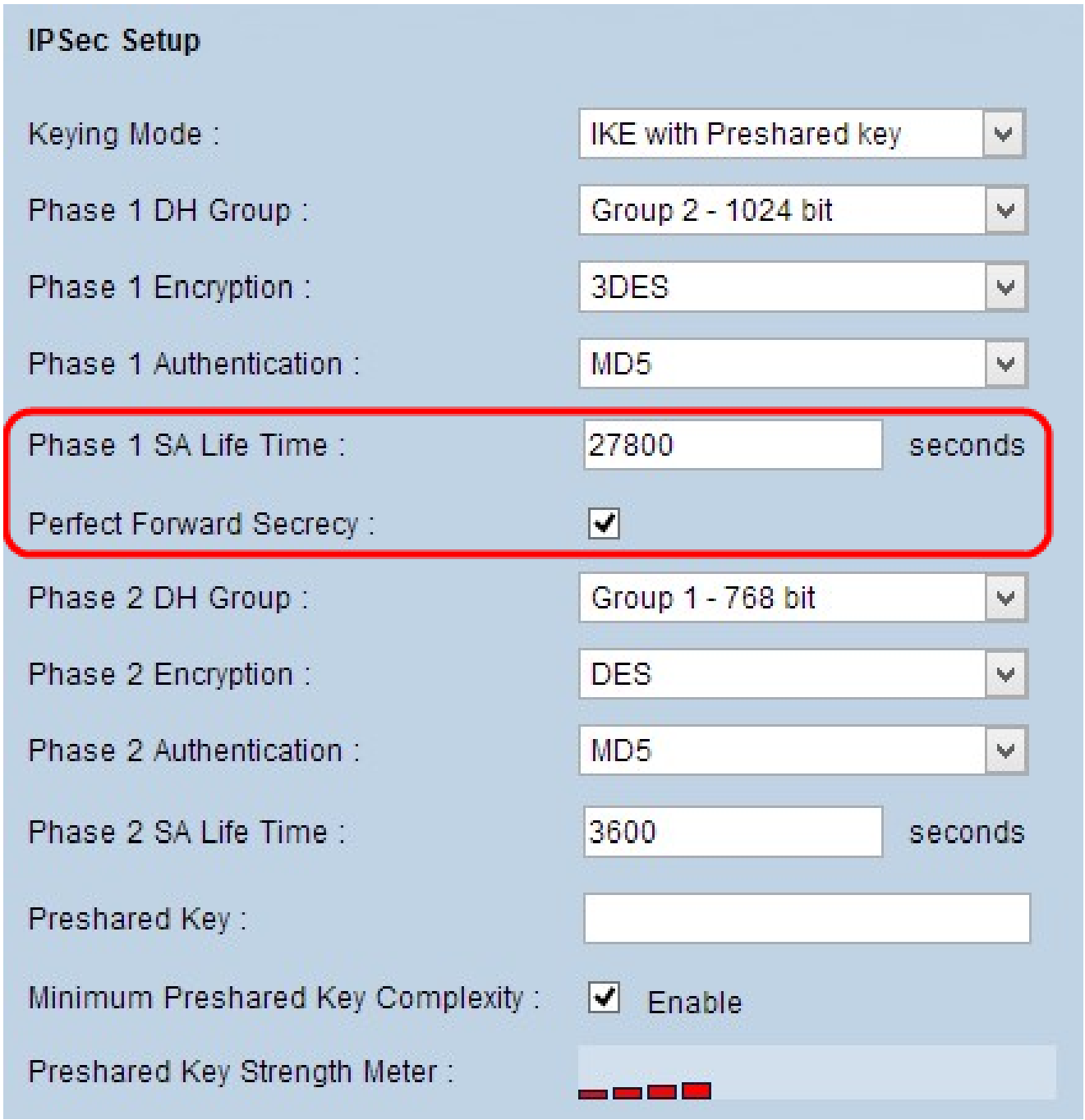


ステップ 3：Phase 1 Authenticationドロップダウンリストから、適切なPhase 1認証方式を

選択します。 VPNトンネルでは、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。

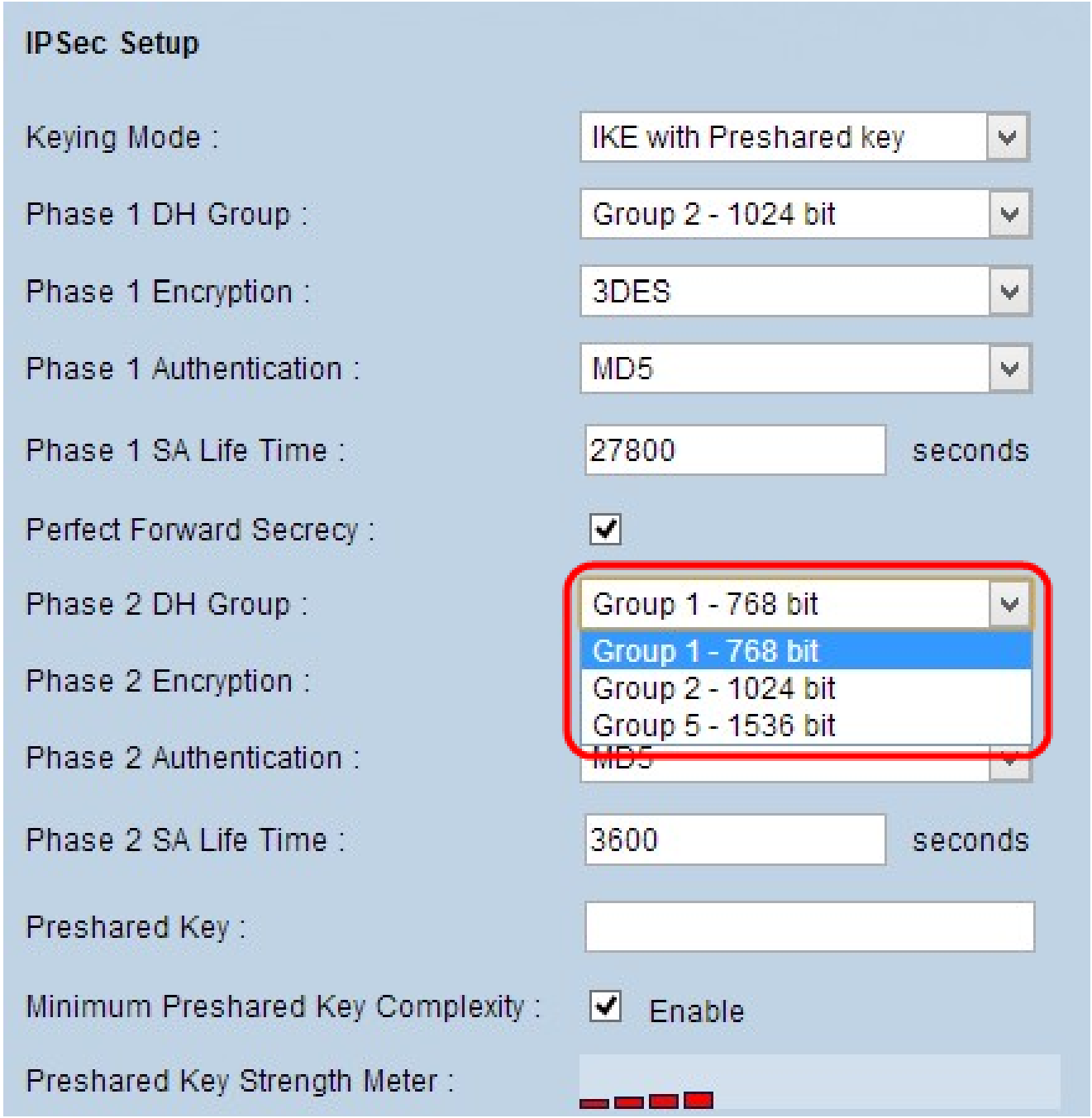
・ MD5:Message Digest Algorithm-5(MD5)は、チェックサム計算によって悪意のある攻撃からデータを保護する128ビットハッシュ関数です。

・ SHA1:Secure Hash Algorithm(SHA)バージョン1(SHA1)は160ビットのハッシュ関数で、MD5よりも安全ですが、計算に時間がかかります。



ステップ 4：Phase 1 SA Life Timeフィールドに、フェーズ1キーが有効でVPNトンネルがアクティブなままの時間を秒単位で入力します。

ステップ 5：キーの保護を強化するには、Perfect Forward Secrecyチェックボックスにチェックマークを付けます。このオプションを使用すると、キーが侵害された場合にルータが新しいキーを生成できます。暗号化されたデータは、侵害されたキーを介してのみ侵害されます。セキュリティが強化されるため、これは推奨されるアクションです。

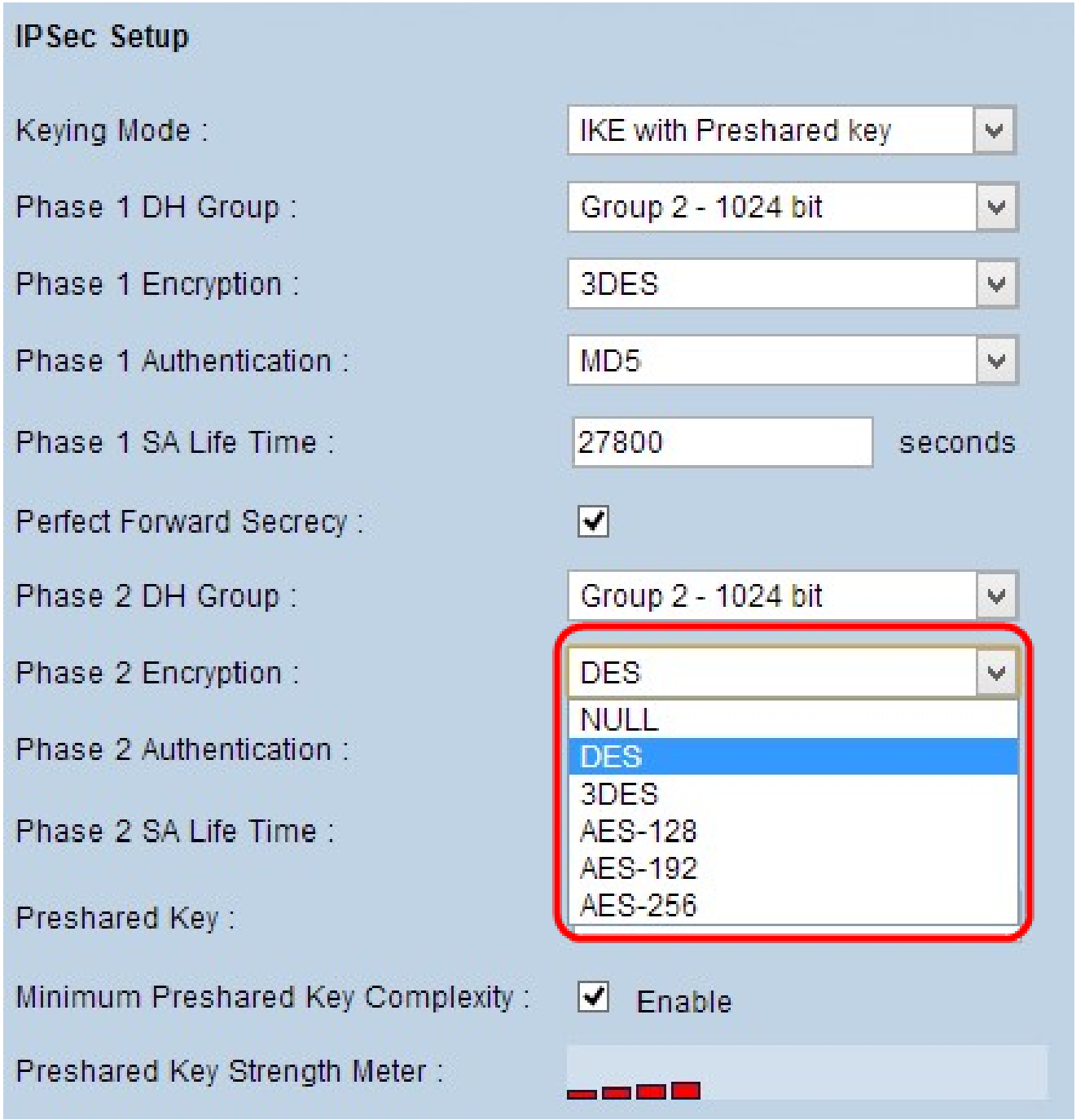


手順 6： Phase 2 DH Groupドロップダウンリストから、適切なPhase 2 DH Groupを選択します。フェーズ2はセキュリティアソシエーションを使用し、データパケットが2つのエンドポイントを通過する際のセキュリティを決定するために使用されます。

・ Group 1 - 768ビット：最も強度の低いキーで最も安全性の低い認証グループですが、IKEキーの計算に必要な時間は最も短くなります。このオプションは、ネットワークの速度が遅い場合に推奨されます。

・ グループ2 - 1024ビット：グループ1よりも強度が高く安全な認証グループですが、IKEキーの計算に時間がかかります。

・ グループ5 - 1536ビット：最も強度の高いキーで、最も安全な認証グループ。IKEキーを計算するには、さらに時間が必要です。ネットワークの速度が速い場合に推奨されます。



手順 7： Phase 2 Encryptionドロップダウンリストから、キーを暗号化するための適切なPhase 2 Encryptionを選択します。AES-128、AES-192、またはAES-256が推奨されます。VPNトンネルでは、両端で同じ暗号化方式を使用する必要があります。

・ NULL – 暗号化は使用されません。

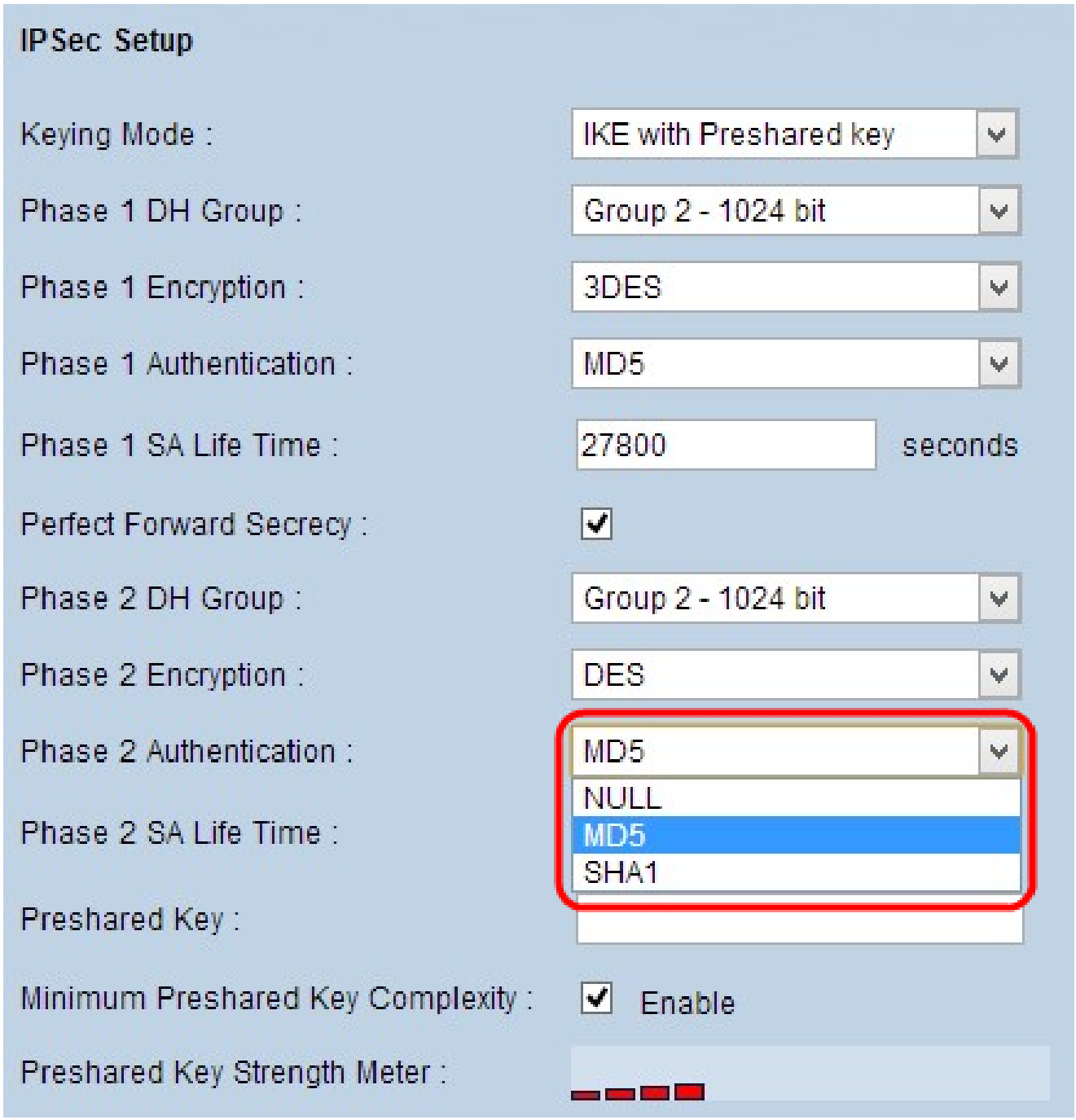
・ DES:Data Encryption Standard（DES；データ暗号規格）では、データ暗号化に56ビットのキーサイズが使用されます。DESは旧式であり、1つのエンドポイントがDESのみをサポートする場合にのみ使用する必要があります。

・ 3DES:Triple Data Encryption Standard(3DES)は168ビットのシンプルな暗号化方式です。3DESはデータを3回暗号化するため、DESよりもセキュリティが強化されます。

・ AES-128:Advanced Encryption Standard(AES)は、10回の繰り返しでプレーンテキストを暗号化テキストに変換する128ビットの暗号化方式です。

・ AES-192:Advanced Encryption Standard(AES)は、12サイクルの繰り返しによってプレーンテキストを暗号化テキストに変換する192ビットの暗号化方式です。AES-128よりもAES-192の方が安全性が高い。

・ AES-256:Advanced Encryption Standard(AES)は、14サイクルの繰り返しによってプレーンテキストを暗号テキストに変換する256ビットの暗号化方式です。AES-256は、最も安全な暗号化方式です。

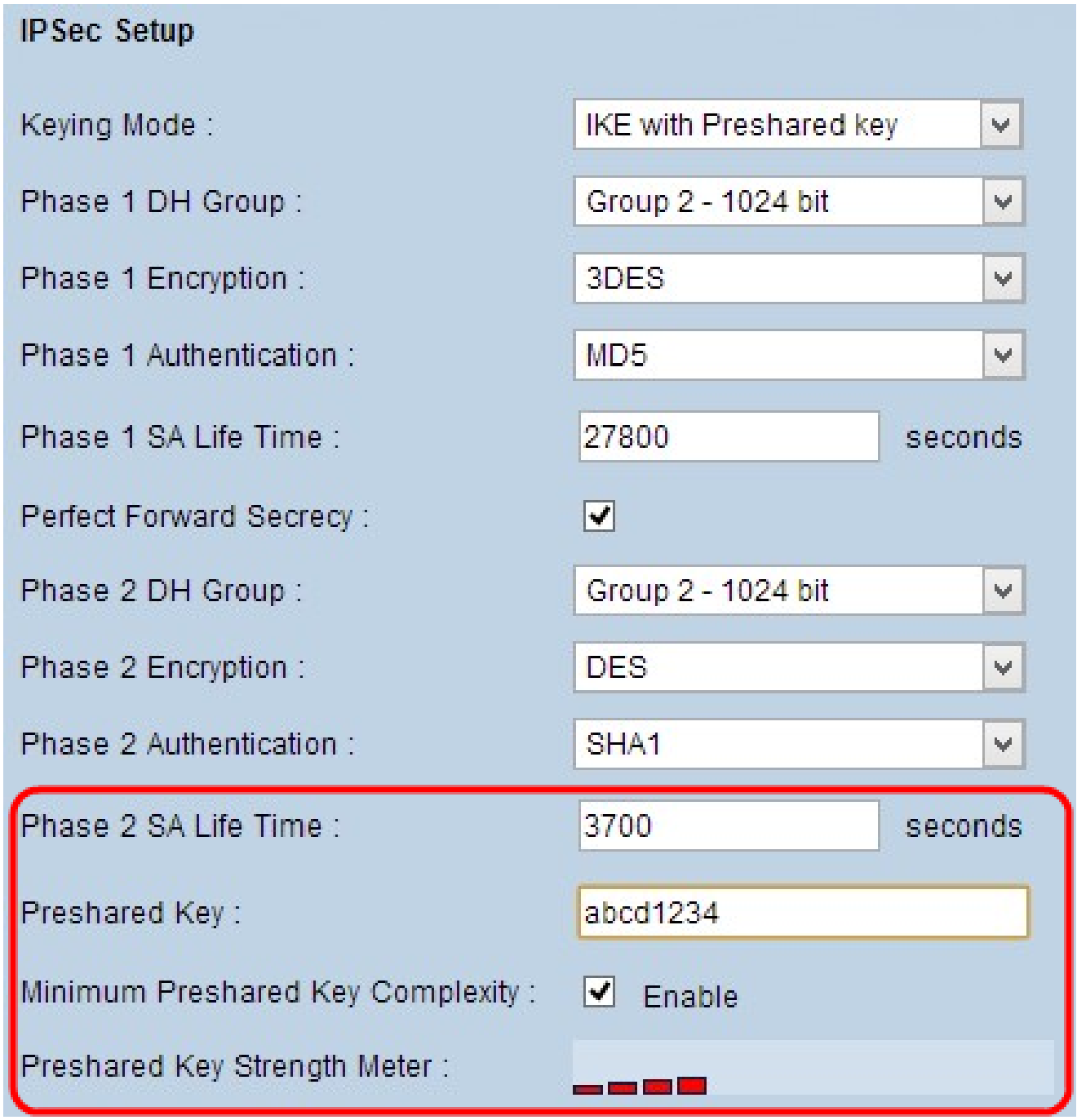


ステップ 8：Phase 2 Authenticationドロップダウンリストから、適切な認証方式を選択します。 VPNトンネルでは、両端で同じ認証方式を使用する必要があります。SHA1が推奨されます。

・ MD5:Message Digest Algorithm-5(MD5)は、チェックサム計算によって悪意のある攻撃からデータを保護する、128ビットの16進数ハッシュ関数です。

・ SHA1:Secure Hash Algorithm(SHA)バージョン1(SHA1)は160ビットのハッシュ関数で、MD5よりも安全ですが、計算に時間がかかります。

・ 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、フェーズ2キーが有効でVPNトンネルがアクティブなままの時間を秒単位で入力します。

ステップ 10：Preshared Keyフィールドに、ピアを認証するためにIKEピア間で事前に共有されているキーを入力します。事前共有キーとして、最大30個の16進数と文字を使用できます。VPNトンネルでは、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がセキュリティで保護されるように、IKEピア間で事前共有キーを頻繁に変更することを強くお勧めします。

ステップ11: (オプション) 事前共有キーの強度メーターを有効にする場合は、Minimum

Preshared Key Complexityチェックボックスにチェックマークを付けます。これは、カラーバーを通して事前共有キーの強度を決定するために使用されます。

・事前共有キーの強度メーター：これは、色付きのバーを通して事前共有キーの強度を示します。赤は弱い強度、黄色は許容可能な強度、緑は強い強度を示します。

ステップ 12[Save] をクリックして、設定を保存します。

注：ゲートウェイ間VPNのAdvancedセクションで使用可能なオプションを設定する場合は、『RV016、RV042、RV042G、およびRV082 VPNルータでのゲートウェイ間VPNの詳細設定の設定』を参照してください。

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。