

# RV34xシリーズルータでのインターネットプロトコルセキュリティ(IPSec)プロファイルの設定

## 目的

Internet Protocol Security(IPSec)は、2台のルータなどの2つのピア間に安全なトンネルを提供します。これらのセキュアなトンネルを介して送信される機密パケットと、これらの機密パケットを保護するために使用するパラメータは、これらのトンネルの特性を指定して定義する必要があります。次に、IPSecピアは、このような機密パケットを検出すると、適切なセキュアトンネルをセットアップし、このトンネルを介してパケットをリモートピアに送信します。

ファイアウォールまたはルータにIPsecを実装すると、境界を通過するすべてのトラフィックに適用できる強力なセキュリティが提供されます。企業またはワークグループ内のトラフィックは、セキュリティ関連の処理のオーバーヘッドを受けません。

このドキュメントの目的は、RV34xシリーズルータでIPSecプロファイルを設定する方法を示すことです。

## 該当するデバイス

- RV34xシリーズ

## [Software Version]

- 1.0.1.16

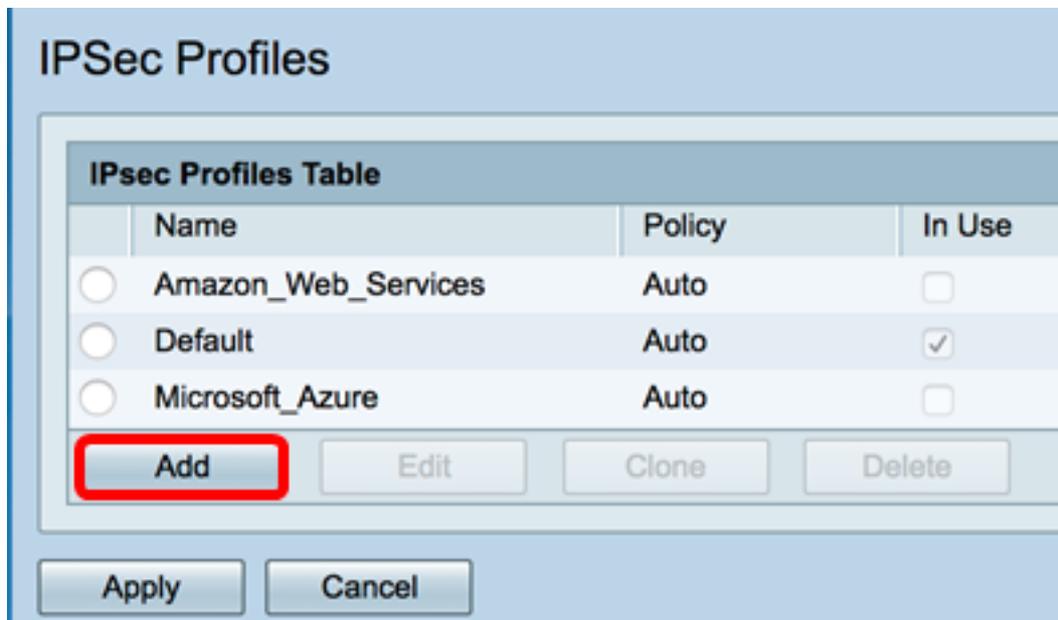
## IPSecプロファイルの設定

### IPSecプロファイルの作成

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、[VPN] > [IPSec Profiles] を選択します。

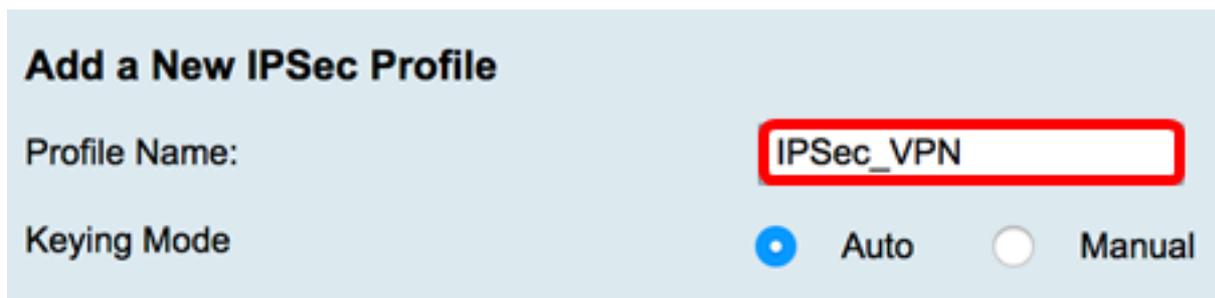


ステップ2: IPsecプロファイルテーブルに既存のプロファイルが表示されます。[Add] をクリックし、新規プロファイルを作成します。



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

注：この例では、IPSec\_VPNがIPSecプロファイル名として使用されます。



ステップ4：オプションボタンをクリックして、プロファイルが認証に使用するキー交換方式を決定します。次のオプションがあります。

- Auto：ポリシーパラメータは自動的に設定されます。このオプションでは、データ整合性と暗号化キー交換にインターネットキー交換(IKE)ポリシーを使用します。これを選択すると、[Auto Policy Parameters]領域の設定が有効になります。ここをクリックして、自動設定を行います。
- [手動(Manual)]：このオプションを使用すると、バーチャルプライベートネットワーク(VPN)トンネルのデータ暗号化と整合性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。ここをクリックして、手動設定を構成します。

注：この例では、[Auto]が選択されています。



## 自動設定の設定

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

- Group2 - 1024 bit : キーの計算は遅くなりますが、Group1よりも安全です。
- Group5 - 1536-bit : 最も遅いキーを計算しますが、最もセキュアです。

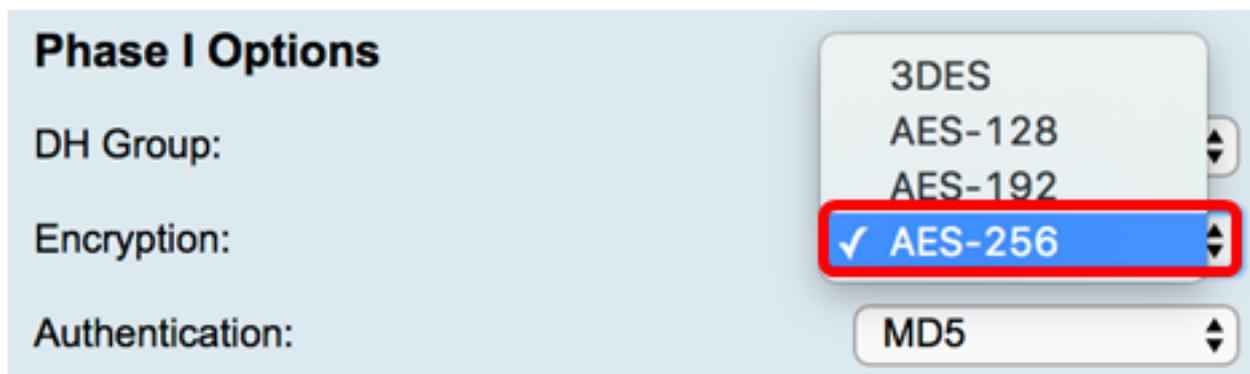
注 : この例では、Group2-1024ビットが選択されています。



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

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

注 : AESはDESと3DESを通じて暗号化を行う標準的な方式で、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、ドロップインパフォーマンスでセキュリティが向上します。この例では、AES-256が選択されています。



ステップ3:[Authentication]ドロップダウンメニューから、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128ビットのハッシュ値があります。
- SHA-1:Secure Hash Algorithm ( SHA-1 ; セキュアハッシュアルゴリズム ) に160ビットのハッシュ値があります。

- SHA2-256:256ビットのハッシュ値を使用したセキュアハッシュアルゴリズム。

注：MD5とSHAは、どちらも暗号化ハッシュ関数です。データの一部を取り込み、圧縮し、通常は再生可能ではない一意の16進数出力を作成します。この例では、SHA2-256が選択されています。

The screenshot shows three configuration fields: 'DH Group' set to 'Group2 - 1024 bit', 'Encryption' with a dropdown menu showing 'MD5', 'SHA1', and 'SHA2-256' (the latter is highlighted with a red box and a checkmark), and 'Authentication'.

ステップ4:[SA Lifetime]フィールドに、120 ~ 86400の範囲の値を入力します。これは、インターネットキー交換(IKE)セキュリティアソシエーション(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 28800 です。

注：この例では、28801 が使用されます。

The screenshot shows three configuration fields: 'Authentication' set to 'SHA2-256', 'SA Lifetime' set to '28801' (highlighted with a red box), and 'Perfect Forward Security' checked and labeled 'Enable'.

ステップ5: ( オプション ) IPSecトラフィックの暗号化と認証に新しいキーを生成するには、[Enable Perfect Forward Security]チェックボックスをオンにします。

The screenshot shows three configuration fields: 'Authentication' set to 'SHA2-256', 'SA Lifetime' set to '28801', and 'Perfect Forward Security' checked and labeled 'Enable'.

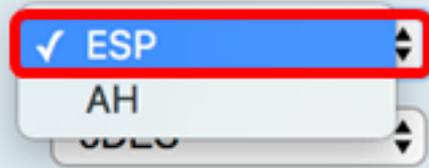
ステップ6:[Phase II Options]領域の[Protocol Selection]ドロップダウンメニューから、ネゴシエーションの2番目のフェーズに適用するプロトコルタイプを選択します。次のオプションがあります。

- ESP：これが選択されている場合は、[ステップ7に進み](#)、ESPパケットの暗号化と復号化の方法を選択します。データプライバシーサービス、オプションのデータ認証、および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。ESPは保護するデータをカプセル化します。
- AH：認証ヘッダー(AH)は、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、保護されるデータ(完全なIPデータグラム)に埋め込まれます。これを[選択した場合](#)は、ステップ8に進みます。

## Phase II Options

Protocol Selection:

Encryption:



**ステップ7** : ステップ6でESPを選択した場合は、[Encryption]ドロップダウンリストから、ESPおよびISAKMPを暗号化および復号化するための適切な暗号化方式を選択します。次のオプションがあります。

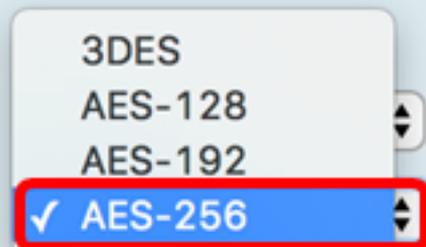
- 3DES:Triple Data Encryption Standard ( トリプルデータ暗号規格 )。
- AES-128:Advanced Encryption Standard(AES-128)は128ビットキーを使用します。
- AES-192:Advanced Encryption Standard ( AES-192 ; 高度暗号化規格 ) は192ビットキーを使用します。
- AES-256:Advanced Encryption Standard(AES-256)は256ビットキーを使用します。

注 : この例では、AES-256が選択されています。

## Phase II Options

Protocol Selection:

Encryption:



**ステップ8**:[Authentication]ドロップダウンメニューから、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。

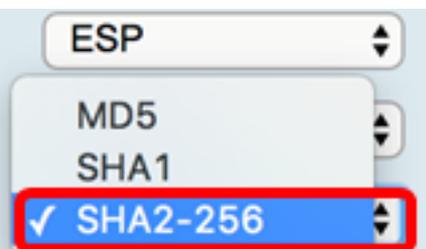
- MD5:Message Digest Algorithm ( MD5 ; メッセージダイジェストアルゴリズム ) に128ビットのハッシュ値があります。
- SHA-1:Secure Hash Algorithm ( SHA-1 ; セキュアハッシュアルゴリズム ) に160ビットのハッシュ値があります。
- SHA2-256:256ビットのハッシュ値を使用したセキュアハッシュアルゴリズム。

注 : この例では、SHA2-256が使用されています。

Protocol Selection:

Encryption:

Authentication:



**ステップ9**:[SA Lifetime]フィールドに、120 ~ 28800の範囲の値を入力します。これは、IKE SAがこのフェーズでアクティブなままである時間の長さです。デフォルト値は3600です。

注 : この例では、28799 が使用されます。

SA Lifetime:

28799

ステップ10:[DHグループ(DH Group)]ドロップダウンリストから、フェーズ2のキーで使用する適切なDiffie-Hellman(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 bit : キーの計算は遅くなりますが、Group1よりも安全です。
- Group5 - 1536 bit : 最も遅いキーを計算しますが、最もセキュアです。

注 : この例では、Group5 - 1536ビットが選択されています。

SA Lifetime:

28799

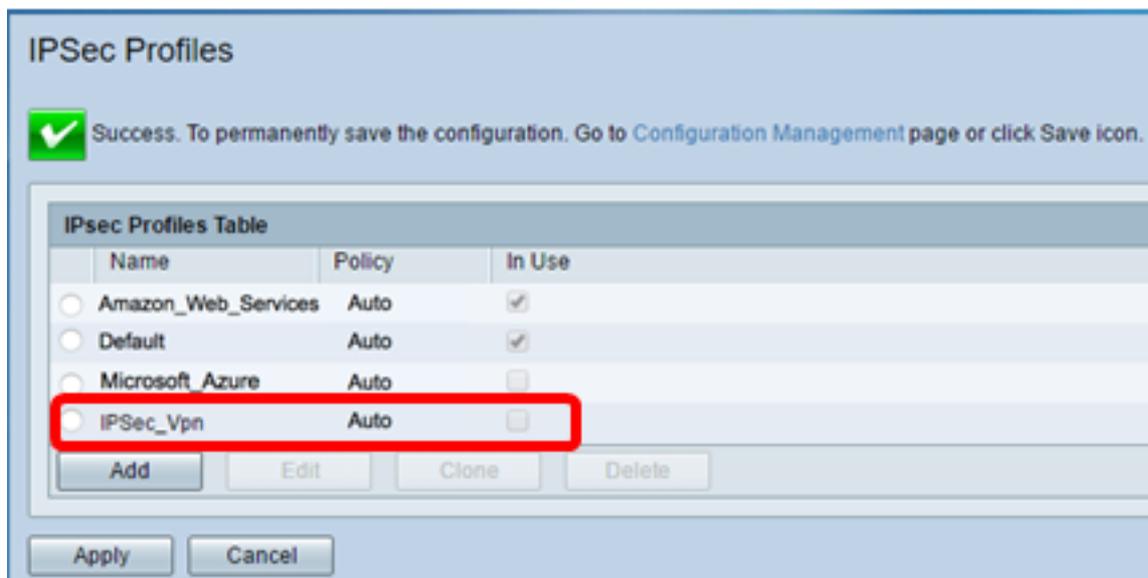
DH Group:

Group2 - 1024 bit

✓ Group5 - 1536 bit

ステップ11 : をクリックします 。

注 : IPSecプロファイルテーブルに戻り、新しく作成されたIPSecプロファイルが表示されます。



IPSec Profiles

Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

IPsec Profiles Table			
Name	Policy	In Use	
<input type="radio"/> Amazon_Web_Services	Auto	<input checked="" type="checkbox"/>	
<input type="radio"/> Default	Auto	<input checked="" type="checkbox"/>	
<input type="radio"/> Microsoft_Azure	Auto	<input type="checkbox"/>	
<input type="radio"/> IPSec_Vpn	Auto	<input type="checkbox"/>	

ステップ12: ( オプション ) 構成を永続的に保存するには、[構成のコピー/保存(Copy/Save Configuration)]ページに移動するか、ページの上にあるアイコンをクリックします。



これで、RV34xシリーズルータでAuto IPSecプロファイルが正常に設定されました。

## 手動設定の設定

ステップ1:[SPI-Incoming]フィールドに、VPN接続の着信トラフィックのセキュリティパラメータインデックス(SPI)タグの100 ~ FFFFFFFFの16進数を入力します。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。

**Manual Policy Parameters**

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

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

注：この例では、0x1234が使用されています。

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

ステップ3:[Encryption]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3DES、AES-128、AES-192、およびAES-256です。

注：この例では、AES-256が選択されています。

SPI Incoming:

SPI Outgoing:

Encryption:  AES-256

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。

- 3DESは48文字のキーを使用します。
- AES-128は32文字キーを使用します。
- AES-192は48文字キーを使用します。
- AES-256は64文字キーを使用します。

注：この例では、123456789123456789123...が使用されています。

Key-In: 123456789123456789123

Key-Out: 1a1a1a1a1a1a1a1a1212121

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、手順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、1a1a1a1a1a1a1a1a121212...を使用します。

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

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よりもセキュアではありませんが、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よりも低速ですが安全性が高く、SHA-1はSHA2-256よりも高速ですが安全性が低くなります。
- SHA2-256：データ整合性に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、セキュアです。

注：この例では、MD5が選択されています。

Authentication:	<input checked="" type="checkbox"/> MD5
	<input type="checkbox"/> SHA1
	<input type="checkbox"/> SHA2-256
Key-In	
Key-Out	

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32文字キーを使用します。
- SHA-1は40文字のキーを使用します。
- SHA2-256は64文字キーを使用します。

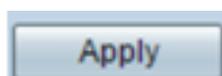
注：この例では、123456789123456789123...が使用されています。

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

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、1a1a1a1a1a1a1a1a121212...を使用します。

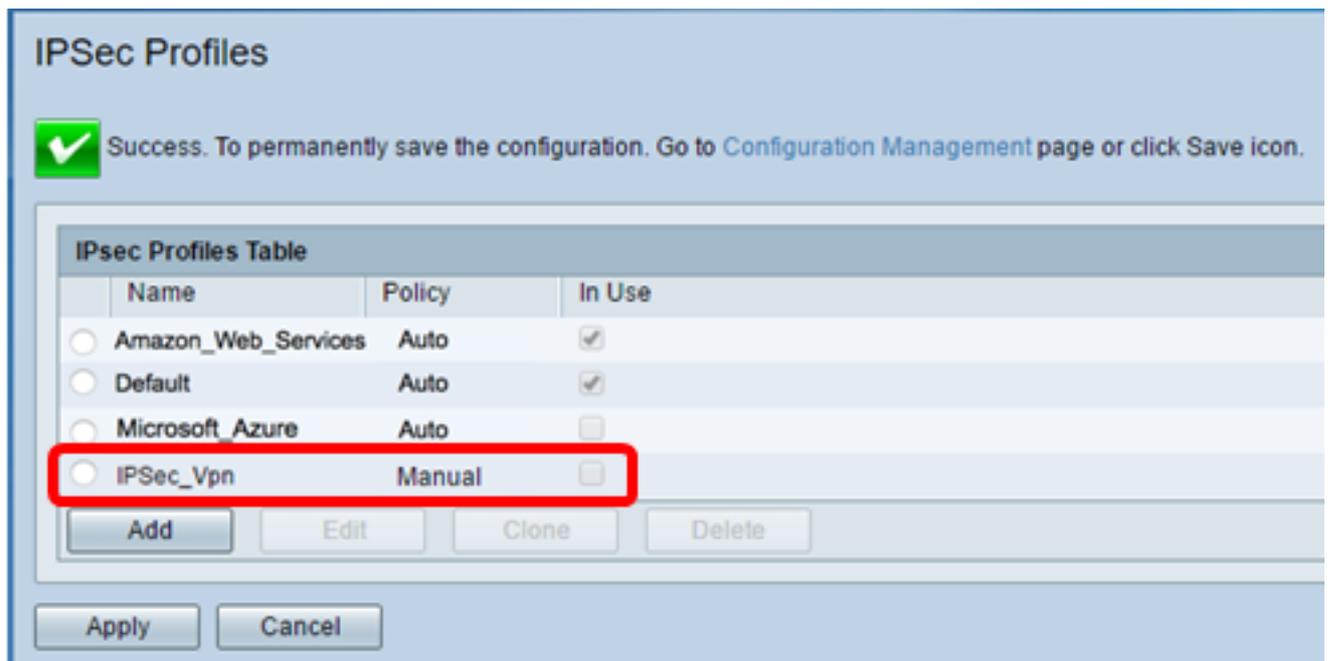
Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121



ステップ9：をクリックします。

注：IPSecプロファイルテーブルに戻り、新しく作成されたIPSecプロファイルが表示され

ます。



ステップ10: ( オプション ) 構成を永続的に保存するには、[構成のコピー/保存(Copy/Save Configuration)]ページに移動するか、ページの上にあるアイコンをクリックします。



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