

RV130およびRV130W VPNルータのインターネットキーエクスチェンジ(IKE)ポリシー設定

目的

インターネットキー交換(IKE)は、2つのネットワーク間でセキュアな通信を確立するプロトコルです。IKEを使用すると、パケットは暗号化およびロックされ、2つのパーティが使用するキーでロック解除されます。

VPNポリシーを設定する前に、インターネットキーエクスチェンジ(IKE)ポリシーを作成する必要があります。詳細については、『[RV130およびRV130WでのVPNポリシーの設定](#)』を参照してください。

このドキュメントの目的は、RV130およびRV130W VPNルータにIKEプロファイルを追加する方法を示すことです。

該当するデバイス

- ・ RV130
- ・ RV130W

手順

ステップ1:Router Configuration Utilityを使用して、左側のメニューから[VPN] > [Site-to-Site IPSec VPN] > [Advanced VPN Setup] を選択します。[Advanced VPN Setup] ページが表示されます。

Advanced VPN Setup

NAT Traversal: Enable

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group	
<input type="checkbox"/>	No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>								

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Algorithm	Local	Remote	
<input type="checkbox"/>	No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>								

ステップ2:[IKE Policy Table]で[Add Row] をクリックします。新しいウィンドウが表示されます。

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group	
<input type="checkbox"/>	No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>								

ステップ3:[IKE Name] フィールドにIKEポリシーの名前を入力します。

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

ステップ4:[Exchange Mode] ドロップダウンメニューから、キー交換を使用してセキュアな通信を確立するモードを選択します。

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

- Main
- Aggressive

使用可能なオプションは次のように定義されています。

- ・ Main : ピアのIDを保護してセキュリティを強化します。
- ・ アグレッシブ : ピアIDは保護されませんが、接続は迅速になります。

ステップ5:[Local Identifier Type] ドロップダウンメニューから、プロファイルのIDのタイプを選択します。

Local

Local Identifier Type:

Local Identifier:

使用可能なオプションは次のように定義されています。

- ・ ローカルWAN (インターネット) IP : インターネット経由で接続します。
- ・ IPアドレス : ネットワーク上で通信するためにインターネットプロトコルを使用している各マシンを識別する、ピリオドで区切られた一意の数字ストリング。

ステップ6: (オプション) ステップ5でドロップダウンリストから[IP Address] を選択した場合は、[Local Identifier] フィールドにローカルIPアドレスを入力します。

Local

Local Identifier Type:

Local Identifier:

ステップ7:[Remote Identifier Type] ドロップダウンメニューから、プロファイルのIDのタイプを選択します。

Remote

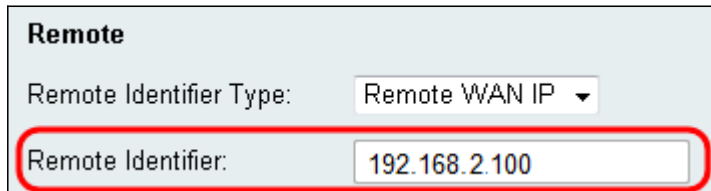
Remote Identifier Type:

Remote Identifier:

使用可能なオプションは次のように定義されています。

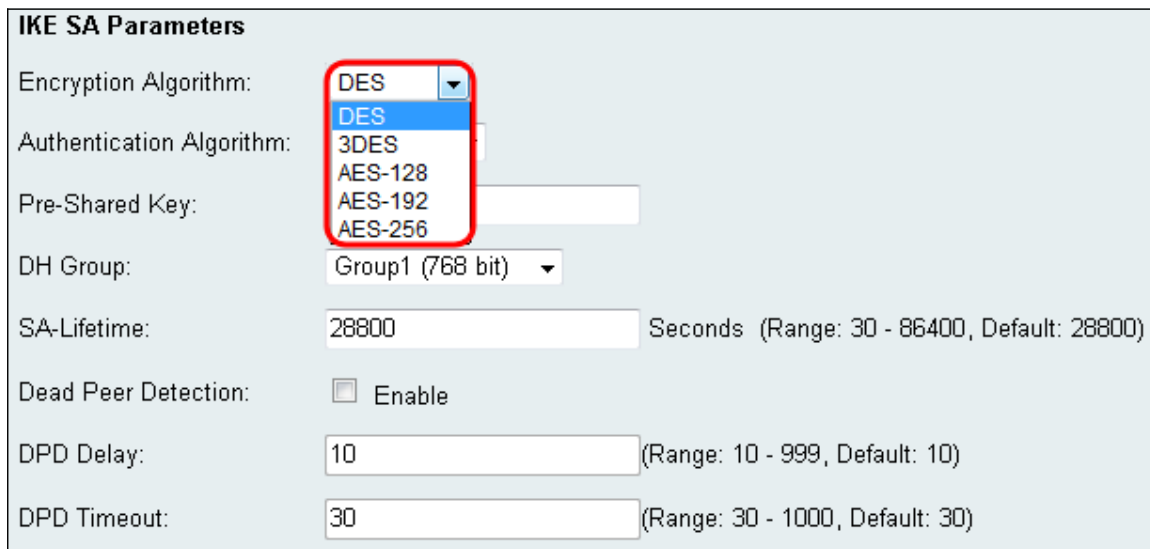
- ・ ローカルWAN (インターネット) IP : インターネット経由で接続します。
- ・ IPアドレス : ネットワーク上で通信するためにインターネットプロトコルを使用している各マシンを識別する、ピリオドで区切られた一意の数字ストリング。

ステップ8: (オプション) ステップ7のドロップダウンリストから[IP Address] を選択した場合は、[Remote Identifier] フィールドにリモートIPアドレスを入力します。



The screenshot shows a configuration window titled "Remote". It contains two fields: "Remote Identifier Type:" with a dropdown menu set to "Remote WAN IP", and "Remote Identifier:" with a text input field containing "192.168.2.100". A red rectangular box highlights the "Remote Identifier:" field and its content.

ステップ9:[Encryption Algorithm] ドロップダウンメニューから、通信を暗号化するアルゴリズムを選択します。AES-128がデフォルトとして選択されています。



The screenshot shows the "IKE SA Parameters" configuration window. The "Encryption Algorithm:" dropdown menu is open, showing a list of options: DES, 3DES, AES-128, AES-192, and AES-256. The "DES" option is highlighted in blue. A red rectangular box highlights the dropdown menu and its list of options. Other fields include "Authentication Algorithm:", "Pre-Shared Key:", "DH Group:" (set to "Group1 (768 bit)"), "SA-Lifetime:" (28800), "Dead Peer Detection:" (checkbox unchecked), "DPD Delay:" (10), and "DPD Timeout:" (30).

使用可能なオプションは、セキュリティのレベルが最も高いものから最も高いものまで、次のとおりです。

- ・ DES:Data Encryption Standard (データ暗号規格) 。
- ・ 3DES:Triple Data Encryption Standard。
- ・ AES-128:Advanced Encryption Standard(AES)では128ビットキーを使用します。
- ・ AES-192:Advanced Encryption Standard (AES ; 高度暗号化規格) では192ビットキーが使用されます。
- ・ AES-256:Advanced Encryption Standard(AES)では256ビットキーを使用します。

注 : AESは、より優れたパフォーマンスとセキュリティを実現する、DESおよび3DESを介した標準的な暗号化方式です。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。AES-128は、速度とセキュリティの間で最適な妥協点を提供するため、推奨されます。

ステップ10:[Authentication Algorithm] ドロップダウンメニューから、通信を認証するアルゴリズムを選択します。SHA-1がデフォルトとして選択されます。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: MD5 ▾
 MD5
 SHA-1
 SHA2-256

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

使用可能なオプションは次のように定義されています。

- ・ MD5:Message Digest Algorithm(MD5)には128ビットのハッシュ値があります。
- ・ SHA-1:Secure Hash Algorithmのハッシュ値は160ビットです。
- ・ SHA2-256:256ビットのハッシュ値を使用するセキュア・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、通常は再現性のない一意の16進数出力を作成します。MD5は基本的にハッシュ衝突に対するセキュリティを提供しないため、衝突耐性が不要なスモールビジネス環境でのみ使用してください。SHA1はMD5よりも優れた選択肢です。SHA1は非常に遅い速度で優れたセキュリティを提供するからです。最良の結果を得るために、SHA2-256には実用的な攻撃がなく、最高のセキュリティを提供します。すでに説明したように、セキュリティが高いほど速度が遅くなります。

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。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

ステップ12:[DH Group] ドロップダウンメニューから、DHグループを選択します。ビット数は、セキュリティのレベルを示します。接続の両端は同じグループ内にある必要があります。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: **Group1 (768 bit) ▾**

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ13:[SA-Lifetime] フィールドに、セキュリティアソシエーションが有効になる時間を秒単位で入力します。デフォルト値は 28800 秒です。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ14: (オプション) 非アクティブピアとの接続を無効にする場合は、[Dead Peer Detection] フィールドの[Enable] チェックボックスをオンにします。Dead peer Detectionをイネーブルにしていない場合は、ステップ17に進みます。

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ15: (オプション) Dead Peer Detectionを有効にした場合は、[DPD Delay] フィー

ルドに値を入力します。この値は、ルータがクライアント接続の確認を待機する時間を指定します。

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

ステップ16: (オプション) Dead Peer Detectionを有効にした場合は、[DPD Timeout] フィールドに値を入力します。この値は、クライアントがタイムアウトになるまで接続を維持する時間を指定します。

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)

ステップ17:[Save] をクリックして変更を保存します。

IKE SA Parameters	
Encryption Algorithm:	<input type="text" value="AES-128"/>
Authentication Algorithm:	<input type="text" value="SHA-1"/>
Pre-Shared Key:	<input type="text"/>
DH Group:	<input type="text" value="Group1 (768 bit)"/>
SA-Lifetime:	<input type="text" value="28800"/> Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	<input type="text" value="10"/> (Range: 10 - 999, Default: 10)
DPD Timeout:	<input type="text" value="30"/> (Range: 30 - 1000, Default: 30)
<input type="button" value="Save"/>	<input type="button" value="Cancel"/> <input type="button" value="Back"/>

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。