

RV130およびRV130WでのIPSec VPNサーバの設定

目的

IPSec VPN (バーチャルプライベートネットワーク) を使用すると、インターネット上に暗号化されたトンネルを確立することによって、企業リソースへのリモートアクセスを安全に取得できます。

このドキュメントの目的は、RV130およびRV130WでIPSec VPNサーバを設定する方法を説明することです。

注 : RV130およびRV130W上でShrew Soft VPN Clientを使用してIPSec VPNサーバを設定する方法については、『[RV130およびRV130W上でIPSec VPNサーバを使用するShrew Soft VPN Client](#)』を参照してください。

該当するデバイス

- ・ RV130W Wireless-N VPNファイアウォール
- ・ RV130 VPNファイアウォール

[Software Version]

- ・ v1.0.1.3

IPSec VPNサーバのセットアップ

ステップ1:Web設定ユーティリティにログインし、[VPN] > [IPSec VPN Server] > [Setup] を選択します。[Setup]ページが開きます。

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP: Single

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES

Authentication Algorithm: MD5

PFS Key Group: Enable

DH Group: Group 1(768 bit)

ステップ2:[Server Enable] チェックボックスをオンにして、証明書を有効にします。

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

ステップ3: (オプション) VPNルータまたはVPN ClientがNATゲートウェイの背後にある場合は、[Edit] をクリックしてNATトラバーサルを設定します。そうでない場合は、NATトラバーサルを無効のままにします。

注 : NATトラバーサル設定の設定方法についての詳細は、『[RV130およびRV130W VPNルータでのインターネットキー交換\(IKE\)ポリシー設定](#)』を参照してください。

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

ステップ4:[Pre-Shared Key] フィールドに、デバイスとリモートエンドポイント間で交換されるキーを8 ~ 49文字の範囲で入力します。

Phase 1 Configuration

Pre-Shared Key: Testkey

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

ステップ5:[Exchange Mode]ドロップダウンリストから、IPSec VPN接続のモードを選択します。Mainはデフォルトモードです。ただし、ネットワーク速度が低い場合は、アグレッシブモードを選択します。

Server Enable:

Phase 1 Configuration

Pre-Shared Key: Testkey

Exchange Mode: Main
Main
Aggressive

Encryption Algorithm: DES

Authentication Algorithm: MD5

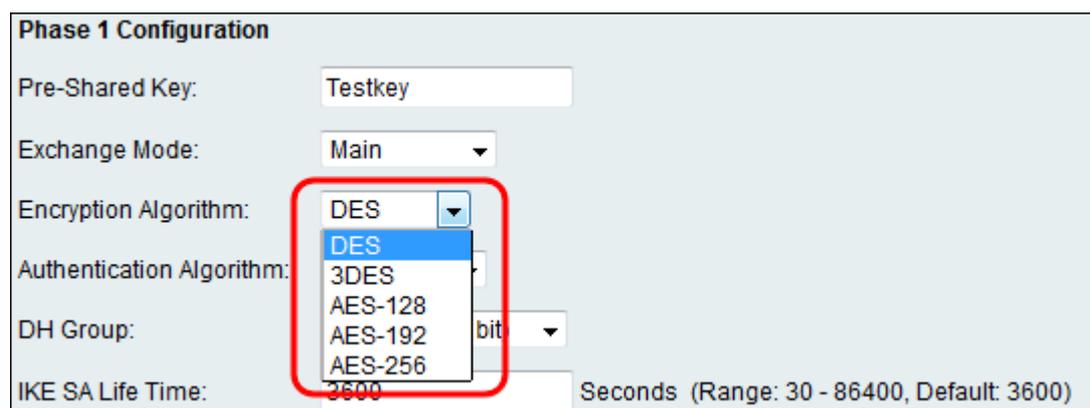
DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

注：アグレッシブモードでは、接続中にトンネルのエンドポイントのIDがクリアテキストで交換されます。交換に必要な時間は短くなりますが、安全性は低下します。

ステップ6:[Encryption Algorithm] ドロップダウンリストから、フェーズ1の事前共有キーを

暗号化するための適切な暗号化方式を選択します。AES-128は、高いセキュリティと高速なパフォーマンスを実現するために推奨されます。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。

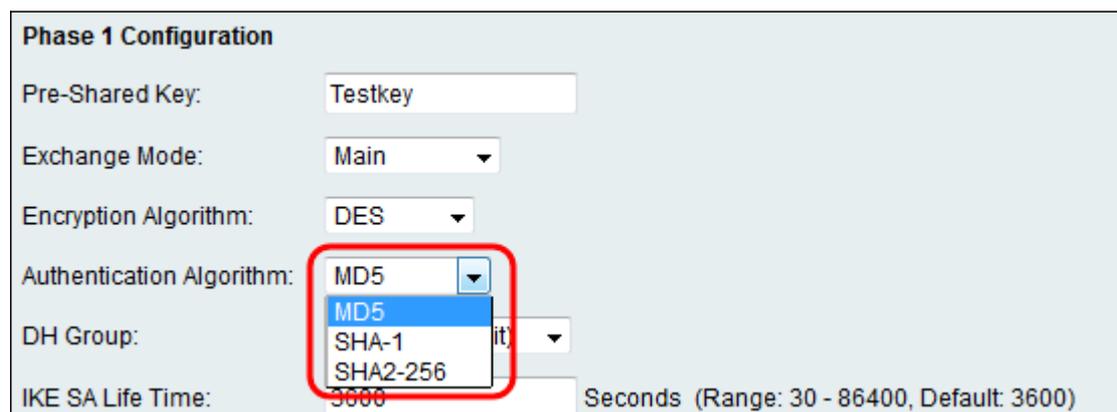


The screenshot shows the 'Phase 1 Configuration' dialog box. The 'Pre-Shared Key' is 'Testkey', 'Exchange Mode' is 'Main', and 'IKE SA Life Time' is '3600' seconds. The 'Encryption Algorithm' dropdown menu is open, showing options: DES, 3DES, AES-128, AES-192, and AES-256. The 'Authentication Algorithm' dropdown menu is also open, showing options: MD5, SHA-1, and SHA2-256. A red box highlights the 'Encryption Algorithm' dropdown menu.

使用可能なオプションは次のように定義されています。

- ・ DES:Data Encryption Standard(DES)は56ビットの古い暗号化方式で、安全性はそれほど高くありませんが、下位互換性のために必要な場合があります。
- ・ 3DES:Triple Data Encryption Standard(3DES)は、データを3回暗号化するため、鍵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)では、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、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-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セキュリティを備え、AES-256よりも高速ですが低いセキュリティを備えています。
- ・ 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。

ステップ7:[Authentication Algorithm] ドロップダウンリストから、フェーズ1でカプセル化セキュリティペイロード(ESP)プロトコルヘッダーパケットがどのように検証されるかを決定する適切な認証方式を選択します。VPNトンネルでは、接続の両端で同じ認証方式を使用する必要があります。



The screenshot shows the 'Phase 1 Configuration' dialog box. The 'Pre-Shared Key' is 'Testkey', 'Exchange Mode' is 'Main', and 'IKE SA Life Time' is '3600' seconds. The 'Encryption Algorithm' is set to 'DES'. The 'Authentication Algorithm' dropdown menu is open, showing options: MD5, SHA-1, and SHA2-256. A red box highlights the 'Authentication Algorithm' dropdown menu.

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:MD5は、128ビットのダイジェストを生成する一方方向ハッシュアルゴリズムです。MD5はSHA-1より高速で計算されますが、SHA-1より安全性が低くなります。MD5は推奨されません。
- ・ SHA-1:SHA-1は、160ビットのダイジェストを生成する一方方向ハッシュアルゴリズムです。SHA-1はMD5よりも低速で計算しますが、MD5よりも安全です。
- ・ SHA2-256:256ビットのダイジェストを使用してセキュアハッシュアルゴリズムSHA2を指定します。

ステップ8:[DH Group] 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。

Phase 1 Configuration	
Pre-Shared Key:	<input type="text" value="Testkey"/>
Exchange Mode:	<input type="text" value="Main"/>
Encryption Algorithm:	<input type="text" value="DES"/>
Authentication Algorithm:	<input type="text" value="MD5"/>
DH Group:	<input type="text" value="Group1 (768 bit)"/> <ul style="list-style-type: none"> <input checked="" type="text" value="Group1 (768 bit)"/> <input type="text" value="Group2 (1024 bit)"/> <input type="text" value="Group5 (1536 bit)"/>
IKE SA Life Time:	Seconds (Range: 30 - 86400, Default: 3600)
Phase 2 Configuration	

使用可能なオプションは次のように定義されています。

- ・ Group1 (768ビット) : キーを最も高速で計算しますが、最もセキュアではありません。
- ・ Group2 (1024ビット) : キーの計算は低速ですが、Group1よりも安全です。
- ・ Group5 (1536ビット) : 最も遅いキーを計算しますが、最も安全です。

ステップ9:[IKE SA Life Time] フィールドに、自動IKEキーが有効である時間を秒単位で入力します。この時間が経過すると、新しいキーが自動的にネゴシエートされます。

Phase 1 Configuration	
Pre-Shared Key:	<input type="text" value="Testkey"/>
Exchange Mode:	<input type="text" value="Main"/>
Encryption Algorithm:	<input type="text" value="DES"/>
Authentication Algorithm:	<input type="text" value="MD5"/>
DH Group:	<input type="text" value="Group1 (768 bit)"/>
IKE SA Life Time:	<input type="text" value="3600"/> Seconds (Range: 30 - 86400, Default: 3600)

ステップ10:[Local IP]ドロップダウンリストから、1人のローカルLANユーザがVPNトンネルにアクセスできるようにする場合は[Single] を選択し、複数のユーザがアクセスできるようにする場合は[Subnet] を選択します。

Phase 2 Configuration

Local IP: Single ▼
Single
Subnet

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

ステップ11：ステップ10で[Subnet] を選択した場合は、[IP Address]フィールドにサブネットワークのネットワークIPアドレスを入力します。ステップ10で[Single] を選択した場合は、シングルユーザのIPアドレスを入力してステップ13に進みます。

Phase 2 Configuration

Local IP: Subnet ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

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] フィールドにローカルネットワークのサブネットマスクを入力します。

Phase 2 Configuration

Local IP: Subnet ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

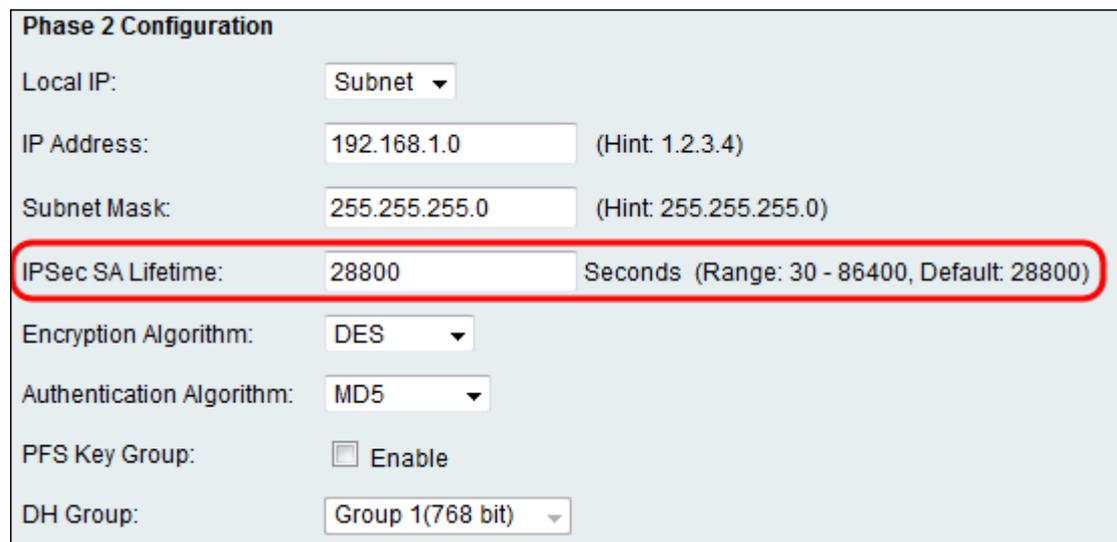
Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

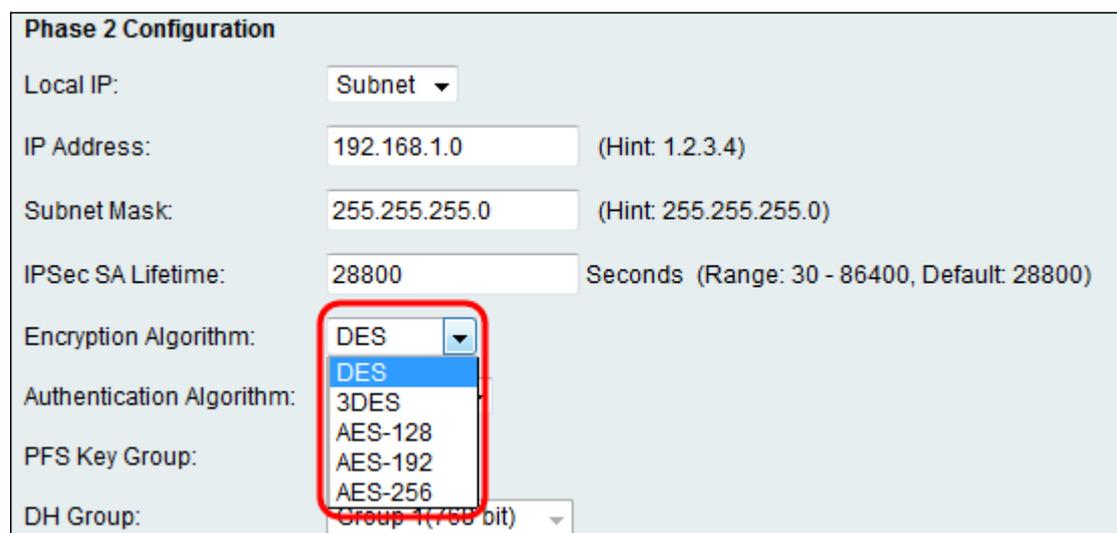
ステップ13:[IPSec SA Lifetime] フィールドに、フェーズ2でVPN接続がアクティブなままに

なる時間 (秒) を入力します。この時間が経過すると、VPN接続のIPSecセキュリティアソシエーション(SA)が再ネゴシエートされます。



The screenshot shows the 'Phase 2 Configuration' form. The 'IPsec SA Lifetime' field is highlighted with a red rectangle. The value is '28800' and the unit is 'Seconds (Range: 30 - 86400, Default: 28800)'. Other fields include 'Local IP' (Subnet), 'IP Address' (192.168.1.0), 'Subnet Mask' (255.255.255.0), 'Encryption Algorithm' (DES), 'Authentication Algorithm' (MD5), 'PFS Key Group' (unchecked), and 'DH Group' (Group 1(768 bit)).

ステップ14:[Encryption Algorithm] ドロップダウンリストから、フェーズ2の事前共有キーを暗号化するための適切な暗号化方式を選択します。AES-128は、高いセキュリティと高速なパフォーマンスを実現するために推奨されます。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。



The screenshot shows the 'Phase 2 Configuration' form with the 'Encryption Algorithm' dropdown menu open. The menu options are: DES, 3DES, AES-128, AES-192, and AES-256. The 'IPsec SA Lifetime' field is still set to 28800. Other fields are the same as in the previous screenshot.

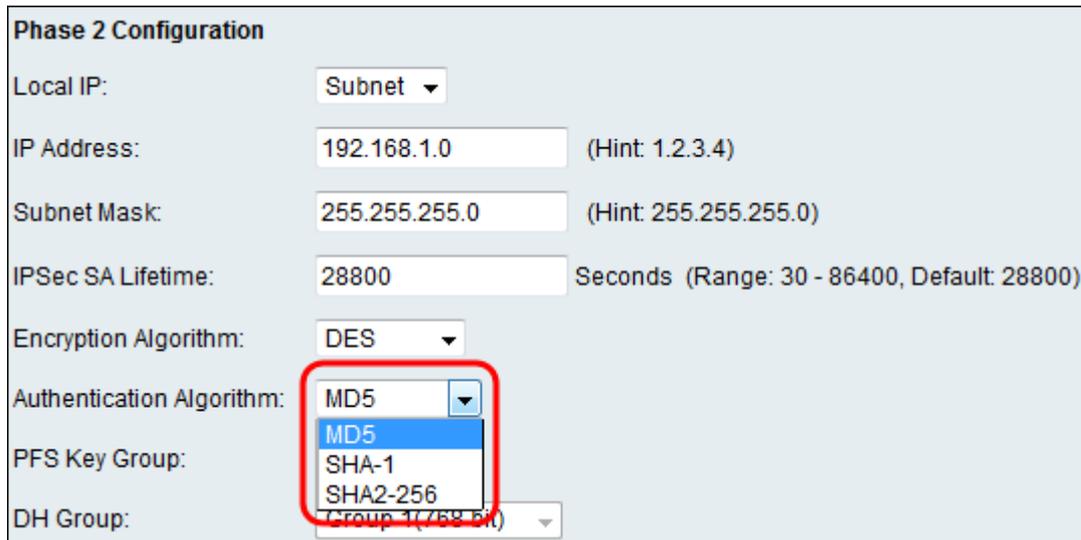
使用可能なオプションは次のように定義されています。

- ・ DES:Data Encryption Standard(DES)は、56ビットの古い暗号化方式で、最も安全性が低いですが、下位互換性のために必要な場合があります。
- ・ 3DES:Triple Data Encryption Standard(3DES)は、データを3回暗号化するため、鍵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)では、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、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-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。

ステップ15:[Authentication Algorithm] ドロップダウンリストから、フェーズ2でカプセル化セキュリティペイロード(ESP)プロトコルヘッダーパケットがどのように検証されるかを決定するための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。



The screenshot shows the 'Phase 2 Configuration' window. The 'Authentication Algorithm' dropdown menu is open, showing three options: MD5, SHA-1, and SHA2-256. The MD5 option is currently selected and highlighted in blue. A red rectangle is drawn around the dropdown menu to highlight the available options.

Local IP:	Subnet
IP Address:	192.168.1.0 (Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0 (Hint: 255.255.255.0)
IPSec SA Lifetime:	28800 Seconds (Range: 30 - 86400, Default: 28800)
Encryption Algorithm:	DES
Authentication Algorithm:	MD5 (selected), MD5, SHA-1, SHA2-256
PFS Key Group:	
DH Group:	Group 1 (768 bit)

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: MD5は、128ビットのダイジェストを生成する一方方向ハッシュアルゴリズムです。MD5はSHA-1より高速で計算されますが、SHA-1より安全性が低くなります。MD5は推奨されません。
- ・ SHA-1: SHA-1は、160ビットのダイジェストを生成する一方方向ハッシュアルゴリズムです。SHA-1はMD5よりも低速で計算しますが、MD5よりも安全です。
- ・ SHA2-256: 256ビットのダイジェストを使用してセキュアハッシュアルゴリズムSHA2を指定します。

ステップ16: (オプション) [PFS Key Group] フィールドで、[Enable] チェックボックスをオンにします。Perfect Forward Secrecy(PFS)は、フェーズ2で新しいDHキーを確保することで、データ保護のセキュリティをさらに強化します。このプロセスは、フェーズ1で生成されたDHキーが送信中に危険にさらされた場合に実行されます。

Phase 2 Configuration

Local IP: Subnet ▾

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▾

Authentication Algorithm: MD5 ▾

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▾

ステップ17:[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。

Phase 2 Configuration

Local IP: Subnet ▾

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▾

Authentication Algorithm: MD5 ▾

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▾

Group 1(768 bit)
Group 2(1024 bit)
Group 5(1536 bit)

Save Cancel

使用可能なオプションは次のように定義されています。

- ・ Group1 (768ビット) : キーを最も高速で計算しますが、最もセキュアではありません。
- ・ Group2 (1024ビット) : キーの計算は低速ですが、Group1よりも安全です。
- ・ Group5 (1536ビット) : 最も遅いキーを計算しますが、最も安全です。

ステップ18:[Save] をクリックして設定を保存します。

Phase 2 Configuration

Local IP: Subnet ▾

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▾

Authentication Algorithm: MD5 ▾

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▾

Save **Cancel**

詳細については、次のドキュメントを参照してください。

- [RV130データシート](#):RV130シリーズルータのVPN機能について説明します。
- [RV130製品ページ](#) : シスコからのRV130に関するすべての記事へのリンクが含まれています
-

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。