

RV320およびRV325 VPNルータシリーズでの Easy Client to Gateway Virtual Private Network(VPN)の設定

目的

バーチャルプライベートネットワーク(VPN)は、パブリックネットワークまたは信頼できないネットワークからインターネットに接続するリモートユーザにセキュリティを提供します。VPNのタイプの1つは、クライアントからゲートウェイへのVPNです。クライアントとゲートウェイを使用すると、地理的に異なるエリアにある会社の異なるブランチをリモートで接続して、エリア間のデータをより安全に送受信できます。Easy VPNは、Cisco VPN Client Utilityを使用してVPNのセットアップと設定を迅速に行います。

このドキュメントの目的は、RV32x VPNルータシリーズでEasy Client to Gateway VPNを設定する方法を示すことです。

該当するデバイス | ファームウェアのバージョン

- RV320デュアルWAN VPNルータ | 1.1.0.09 (最新の[ダウンロード](#))
- RV325ギガビットデュアルWAN VPNルータ | 1.1.0.09 (最新の[ダウンロード](#))

Easy ClientからゲートウェイへのVPNの設定

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

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No. 1
Tunnel Name:
Interface: WAN1
Keying Mode: IKE with Preshared key
Enable:

Local Group Setup

Local Security Gateway Type: IP Only
IP Address: 0.0.0.0
Local Security Group Type: Subnet
IP Address: 192.168.1.0
Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Security Gateway Type: IP Only
IP Address :

ステップ2:[Easy VPN]ラジオボタンをクリックします。

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

注：グループ番号は、グループの番号を表します。自動生成フィールドです。

ステップ3:[Name]フィールドに、トンネルの名前を入力します。

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

ステップ4: (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、[パスワードの最小複雑度(Minimum Password Complexity)]チェックボックスをオンにします。

ステップ5:[パスワード]フィールドに、パスワードを入力します。

- Password Strength Meter – 色付きのバーを使用してパスワードの強度を表示します。赤は弱い強さを示し、黄色は許容される強さを示し、緑は強い強さを示します。ステップ4で[Minimum Password Complexity]チェックボックスにチェックマークを付けていない場合は、[Password Strength Meter]が表示されません。

ステップ6:[Interface]ドロップダウンリストから、クライアントがゲートウェイへのEasy VPNを確立するために使用する適切なインターフェイスを選択します。

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface: ▼
WAN1
WAN2
USB1
USB2

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

ステップ7:[Enable] チェックボックスをオンにして、クライアントからゲートウェイへのVPNを有効にします。デフォルトでは有効になっています。

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

ステップ8:[Tunnel Mode]ドロップダウンリストから適切なトンネリングモードを選択します。

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

使用可能なオプションは次のように定義されます。

- 完全トンネル：トラフィックに対するセキュリティを強化するために、VPNトンネル経由ですべてのトラフィックを送信します。このオプションを選択した場合は、ステップ[11に進みます](#)。
- スプリットトンネル：VPNクライアントがパブリックインターネットとVPNリソースに同時にアクセスできるようにし、帯域幅を節約します。

ステップ9:[IP Address]フィールドに、Easy VPNのインターフェイスに割り当てるIPアドレスを入力します。

The screenshot shows the 'Client to Gateway' configuration window. Under the 'Add a New Easy VPN' section, the 'Easy VPN' radio button is selected. The 'Group No.' is set to 1, and the 'Name' is 'group_1'. The 'Minimum Password Complexity' is checked and set to 'Enable', with a password of 'password_1' entered. The 'Interface' is set to 'WAN2', and the 'Tunnel Mode' is 'Split Tunnel'. The 'IP Address' field is highlighted with a red box and contains '192.168.2.0', and the 'Subnet Mask' field contains '255.255.255.0'. The 'Extended Authentication' is set to 'Default - Local Database'. There are 'Save', 'Cancel', and 'Add/Edit' buttons at the bottom.

ステップ10:[Subnet Mask] フィールドに、Easy VPNインターフェイスに割り当てられたIPアドレスのサブネットマスクを入力します。

ステップ11:[*Extended Authentication*]ドロップダウンリストからVPNクライアントに適切な認証を選択し、IPSecホストのユーザ名とパスワードを使用してVPNクライアントを認証するか、またはユーザ管理にあるデータベースを使用します。両方のデバイスでこの機能を有効にする必要があります。

Client to Gateway

Add a New Easy VPN

Tunnel Group VPN Easy VPN

Group No. 1

Name: group_1

Minimum Password Complexity: Enable

Password: password_1

Password Strength Meter:

Interface: WAN2

Enable:

Tunnel Mode: Split Tunnel

IP Address: 192.168.2.0

Subnet Mask: 255.255.255.0

Extended Authentication: **1 - Active Directory** Add/Edit

 Default - Local Database

 1 - Active Directory

Save Cancel

使用可能なオプションは次のように定義されます。

- 1 - Active Directory – 認証はActive Directoryを介して拡張されます。 Active Directoryは、Windowsドメインネットワークのネットワークセキュリティを提供するサービスです。新しいディレクトリを追加するか、既存のディレクトリを編集する場合は、[追加/編集]をクリックします。
- デフォルト：ローカルデータベース：認証はルータによって実行されます。データベースを追加または編集する場合は、[追加/編集]をクリックします。

注：Active Directoryまたはローカルデータベースの追加または編集方法の詳細については、『[User and Domain Management Configuration on RV320 and RV325 VPN Router Series](#)』というタイトルのドキュメントを参照してください。

ステップ12:[Save]をクリックして、設定を保存します。