

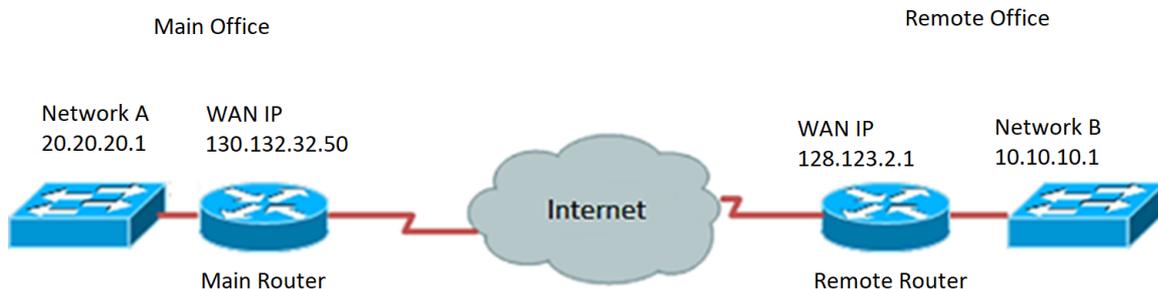
# RV34xシリーズルータのセットアップウィザードを使用したバーチャルプライベートネットワーク(VPN)接続の設定

## 目的

バーチャルプライベートネットワーク(VPN)接続を使用すると、インターネットなどのパブリックネットワークまたは共有ネットワークを介してプライベートネットワークとの間でデータのアクセス、送受信が可能になりますが、基盤となるネットワークインフラストラクチャへのセキュアな接続を確保してプライベートネットワークとそのリソースを保護します。

VPNトンネルは、暗号化と認証を使用してデータを安全に送信できるプライベートネットワークを確立します。企業オフィスはVPN接続を主に使用します。これは、従業員がオフィスの外からでもプライベートネットワークにアクセスできるようにするために便利で必要な機能です。

VPNを使用すると、リモートホストを同じローカルネットワーク上に配置されているかのように動作させることができます。ルータは50のトンネルをサポートします。VPNセットアップウィザードを使用すると、サイト間IPSecトンネルのセキュアな接続を設定できます。この機能により、設定がシンプルになり、複雑な設定やオプションのパラメータが防止されます。これにより、誰でも高速で効率的な方法でIPSecトンネルを設定できます。



## VPN接続を使用する利点：

1. VPN接続を使用すると、機密のネットワークデータとリソースを保護できます。
2. リモートワーカーや企業の従業員は、物理的に存在しなくても本社に簡単にアクセスでき、プライベートネットワークとそのリソースのセキュリティを維持できるため、利便性とアクセシビリティを提供します。
3. VPN接続を使用した通信は、他のリモート通信方式よりも高いレベルのセキュリティを提供します。現在の高度なテクノロジーは、これを可能にし、プライベートネットワークを不正アクセスから保護します。
4. ユーザの実際の地理的位置は保護され、インターネットのようなパブリックまたは共有ネットワークには公開されません。
5. VPNは非常に調整可能であるため、新しいユーザまたはユーザグループをネットワークに追加することは簡単です。追加の新しいコンポーネントや複雑な設定を必要とせず、ネットワークを拡張できます。

## VPN接続を使用するリスク：

1. 設定ミスによるセキュリティリスクVPNの設計と実装は複雑になる可能性があるため、プライベートネットワークのセキュリティが損なわれないように、接続を設定する作業を高度な知識と経験を持つプロフェッショナルに委ねる必要があります。
2. 信頼性.VPN接続にはインターネット接続が必要なので、優れたインターネットサービスを提供し、ダウンタイムを最小限に抑えて保証することが実証され、テストされているプロバイダーを選択することが重要です。
3. 拡張性.新しいインフラストラクチャを追加したり、新しい構成を設定したりする必要がある状況では、使用中の製品以外の異なる製品やベンダーが関係している場合に特に非互換性が原因で技術的な問題が発生する可能性があります。
4. モバイルデバイスのセキュリティの問題。VPN接続を開始するときにモバイルデバイスを使用すると、特にワイヤレス接続を使用するときにセキュリティの問題が発生する場合があります。未検証のプロバイダーの中には、「無料のVPNプロバイダー」と見なされ、コンピュータにマルウェアをインストールすることもできます。そのため、モバイルデバイス使用時にセキュリティ対策を追加して、このような問題を防止することが可能です。
5. 接続速度が遅い。無料のVPNサービスを提供するVPNクライアントを使用している場合、これらのプロバイダーは接続速度に優先順位を付けないため、接続速度が遅くなる可能性があります。

このドキュメントの目的は、セットアップウィザードを使用してRV34xシリーズルータでVPN接続を設定する方法を示すことです。

## 該当するデバイス

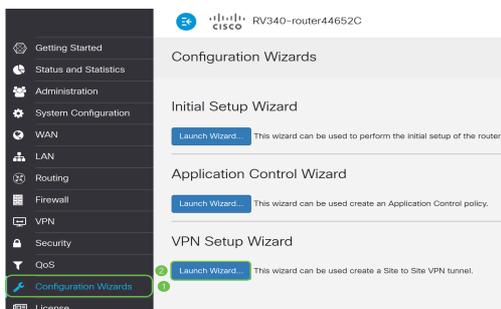
- RV34xシリーズ

## [Software Version]

- 1.0.01.16

## セットアップウィザードを使用したVPN接続の設定

ステップ1：ルータのWebベースユーティリティにログインし、[Configuration Wizard]を選択します。次に、[VPN Setup Wizard]セクションの下の[Launch Wizard]をクリックしてください。



ステップ2：表示されたフィールドに、この接続を識別する名前を入力します。

This Setup Wizard helps you to configure a secure connection between two routers that physically separated over the IPsec VPN tunnel. Before you begin, you need to know the subnet addresses of your local and remote networks, and import the digital certificates for authentication between two peers if needed.

Give this connection a name:  E.g Homeoffice

注：この例では、TestVPNが使用されています。

ステップ3:[Interface ( インターフェイス ) ]領域で、ドロップダウンメニューをクリックし、この接続を有効にするインターフェイスを選択します。次のオプションがあります。

- WAN1
- WAN2
- USB1
- USB2



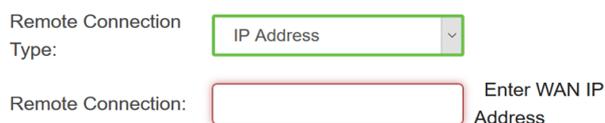
注：この例では、WAN1が使用されています。

ステップ 4 : [Next] をクリックします。

A screenshot of a VPN configuration form. The 'Give this connection a name:' field contains 'TestVPN' and 'E.g Homeoffice'. The 'Interface:' dropdown menu is set to 'WAN1'. At the bottom, there are 'Next' and 'Cancel' buttons.

ステップ5：ドロップダウン矢印をクリックして、[Remote Connection Type]を選択します。次のオプションがあります。

- [IP Address]:VPNトンネルの反対側のリモートルータのIPアドレスを使用する場合は、このオプションを選択します。
- [FQDN]: ( 完全修飾ドメイン名 ) :VPNトンネルの反対側のリモートルータのドメイン名を使用する場合は、このオプションを選択します。

A screenshot of the 'Remote Connection Type:' dropdown menu. The menu is open, and 'IP Address' is selected and highlighted. Below the dropdown, there is a text input field with a red border and the label 'Enter WAN IP Address'.

注：この例では、[IP Address]が選択されています。

ステップ6：表示されたフィールドにリモート接続のWAN IPアドレスを入力し、[Next]をクリックします。

Remote Connection Type: IP Address

Remote Connection: 128.123.2.1 Enter WAN IP Address

Back Next Cancel

注：この例では、128.123.2.1が使用されています。

ステップ7:[Local Traffic Selection]領域で、ドロップダウンをクリックして[Local IP]を選択します。次のオプションがあります。

- [サブネット(Subnet)]：ローカルネットワークのIPアドレスとサブネットマスクの両方を入力する場合に、これを選択します。
- [IP Address]：ローカルネットワークのIPアドレスだけを入力する場合に選択します。
- Any：この2つのオプションのいずれかを使用する場合は、このオプションを選択します。

Local Traffic Selection

Local IP: Subnet

IP Address: Subnet  
IP Address

Subnet Mask: Any

Remote Traffic Selection:

Remote IP: Subnet

IP Address:

Subnet Mask:

注：この例では、[Any]が選択されています。

ステップ8:[Remote Traffic Selection]領域で、ドロップダウン矢印をクリックして[Remote IP]を選択します。表示されたフィールドにリモートIPアドレスとサブネットマスクを入力し、[次へ]をクリックします。次のオプションがあります。

- [サブネット(Subnet)]：リモートネットワークのIPアドレスとサブネットマスクの両方を入力する場合に、これを選択します。
- [IP Address]：リモートネットワークのIPアドレスだけを入力する場合に、このオプションを選択します。

Local Traffic Selection

Local IP: Any

Remote Traffic Selection:

Remote IP: Subnet

IP Address: 10.10.10.0

Subnet Mask: 255.255.255.0

Back Next Cancel

注：この例では、[Subnet]が選択されています。10.10.10.0がIPアドレスとして入力され、255.255.255.0がサブネットマスクとして入力されました。

ステップ9:[IPSec Profile]領域のドロップダウン矢印をクリックして、使用するプロファイルを選択します。

IPSec Profile:

IKE Version:  IKEv1  IKEv2

注：この例では、[Default]が選択されています。

ステップ10:[Phase 1 Options ( フェーズ1オプション )]領域で、この接続の事前共有キーをフィールドに入力します。これは、リモートインターネットキー交換(IKE)ピアの認証に使用される事前共有キーです。VPNトンネルの両端で、同じ事前共有キーを使用する必要があります。このキーには、最大30文字または16進数値を使用できます。

注：VPN接続のセキュリティを維持するために、事前共有キーを定期的に変更することを強く推奨します。

Pre-Shared Key:

Pre-shared Key Strength Meter: 

Show Pre-shared Key:  Enable

注：事前共有キー強度メーターは、次の条件に基づいて入力したキーの強度を示します。

- 赤色：パスワードが脆弱です。
- オレンジ：パスワードがかなり強い。
- 緑：パスワードが強力です。

ステップ11:( オプション ) 編集の際にプレーンテキストを表示するチェックボックスの有効化をオンにして、パスワードをプレーンテキストで表示することもできます。

Pre-Shared Key:

Pre-shared Key Strength Meter: 

Show Pre-shared Key:  Enable

ステップ12:[Next]をクリック.

ステップ13：ページに、VPN接続のすべての設定の詳細が表示されます。[Submit] をクリックします。

## VPN Setup Wizard



Getting Started

Remote Router Settings

Local and Remote Networks

Profile

Summary

Connection Name: TestVPN

Local Interface: WAN1

IPSec Profile: Default

### Phase I Options

DH Group: Group5 - 1536 bit

Encryption: AES 128

Authentication: SHA1

Lifetime(sec) 28800

Pre-Shared Key: CiscoTest123!

Perfect Forward Secrecy: Enable

### Phase II Options:

DH Group: Group5 - 1536 bit

Protocol Selection: ESP

Back

Submit

Cancel

これで、セットアップウィザードを使用して、RV34xシリーズルータでVPN接続が正常に設定されました。サイト間VPNを正常に接続するには、リモートルータでセットアップウィザードを設定する必要があります。