

RV340またはRV345ルータでのサイト間仮想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)は、インターネットを介したローカルネットワークとリモートホスト間の接続です。ローカルホストとリモートホストは、コンピュータ、または設定が同期されて通信が可能になっている別のネットワークである可能性があります。これは、すべてのタイプのVPNに当てはまります。通常は、両方のネットワークが接続の両側のリソースにアクセスできるようにします。VPN接続は通常、2番目のオフィスを本社に接続する場合や、リモートワーカーがネットワークインフラストラクチャに物理的に接続していなくても、リモートワーカーがオフィスのコンピュータネットワークに接続できるようにする場合に使用されます。リモートワーカーは通常、AnyConnect、Shrew Soft、GreenBowなどのVPNソフトウェアクライアント経由で接続します。

この記事では、RV340とRV345ルータ間のサイト間VPN接続を設定する方法について説明します。プライマリルータをローカルルータと呼び、セカンダリルータをリモートルータと呼びます。セカンダリルータへのリモートアクセスまたは物理アクセスが可能であることを確認します。

LANネットワークは、異なるサブネット (192.168.1.xと192.168.2.xなど) 上にあるか、完全に異なるネットワーク (192.168.1.xと10.10.1.xなど) 上にある必要があります。両方のネットワークが同じサブネット上にある場合、ルータはVPN経由でパケットを送信しようとしません。

適用可能なデバイス

- RV340
- RV340W
- RV345
- RV345P

[Software Version]

- 1.0.03.15

特記事項：ライセンス構造 – ファームウェアバージョン1.0.3.15以降。
AnyConnectでは、クライアントライセンスだけが課金されます。

CDW などのパートナーまたは貴社のデバイス調達部門を通じてクライアントライセンスを購入する必要があります。1 ユーザー用ライセンス (L-AC-PLS-3Y-S5) または 1 年間/25 ユーザー用ライセンスパッケージ (AC-PLS-P-25-S) を選択できます。その他のライセンスオプション (永久ライセンスなど) も用意されています。ライセンスの詳細については、下記の「ライセンス情報」セクションにあるリンクを確認してください。

RV340シリーズルータでのAnyConnectライセンスの詳細については、『[RV340シリーズルータ用AnyConnectライセンス](#)』の記事を参照してください。

VPN接続の設定

ローカルルータ

ステップ 1 : ローカルルータのWebベースユーティリティにログインし、VPN > Site-to-Siteの順に選択します。

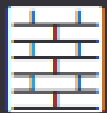
注 : この例では、RV340が使用されています。



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

Site-to-Site

2

Client-to-Site

Teleworker VPN Client

PPTP Server

ステップ 2 : プラスアイコンをクリックします。

Site to Site Table



□ Connection Name ⇅ Remote Endpoint ⇅ Interface ⇅ IPsec Profile ⇅ Local Traffic Selection ⇅ Remote Traffic Selection ⇅ Sta

ステップ 3 : Enableチェックボックスにチェックマークが付いていることを確認します。デフォルトではオンになっています。

Basic Settings Advanced Settings Failover

Enable:

Connection Name: Please Input Connection Name

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

ステップ 4 : Connection Nameフィールドに接続名を入力します。

注 : この例では、名前はTestVPN1です。

Basic Settings Advanced Settings Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

ステップ 5 : IPsec Profile ドロップダウンリストから、接続のセキュリティ設定を選択します。オプションは、作成された IPsec プロファイルによって異なります。IPsec プロファイルの作成方法については、[ここ](#)をクリックしてください。

注 : この例では、CiscoTestVPN が選択されています。

Basic Settings Advanced Settings Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

手順 6 : ローカルルータが使用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 : このオプションは、VPN 接続にローカルルータのワイドエリアネットワーク 1(WAN1) インターフェイスの IP アドレスを使用します。

- WAN2：このオプションは、VPN接続にローカルルータのWAN2インターフェイスのIPアドレスを使用します。WAN2はシングルWANルータでは使用できません。
- USB1：ローカルルータのUniversal Serial Bus 1(USB1)インターフェイスのIPアドレスをVPN接続に使用します。
- USB2:VPN接続にローカルルータのUSB2インターフェイスのIPアドレスを使用します。USB2はシングルUSBルータでは使用できません。

注：この例では、WAN1が選択されています。

The screenshot shows a configuration interface with three tabs: 'Basic Settings' (active), 'Advanced Settings', and 'Failover'. Under 'Basic Settings', there are several fields:

- Enable:** A checkbox that is checked.
- Connection Name:** A text input field containing 'TestVPN1'.
- IPsec Profile:** A dropdown menu showing 'CiscoTestVPN'. To its right, the text 'Auto (IKEv1) Profile is Chosen.' is displayed.
- Interface:** A dropdown menu showing 'WAN1', which is highlighted with a green border.
- Remote Endpoint:** A dropdown menu showing 'Static IP'.
- Below the 'Remote Endpoint' dropdown, there is an empty text input field with a red border.

手順 7：リモートルータのWANインターフェイスのIDを選択します。次のオプションがあります。

- スタティックIP：このオプションを使用すると、VPN接続を確立するときに、ローカルルータはリモートルータのスタティックIPアドレスを使用できます。ローカルルータでこのオプションを選択した場合は、リモートルータも同じオプションで設定する必要があります。
- FQDN：このオプションは、VPN接続を確立するときに、リモートルータの完全修飾ドメイン名(FQDN)を使用します。
- ダイナミックIP：このオプションは、VPN接続を確立するときに、リモートルータのダイナミックIPアドレスを使用します。

注：リモートルータのインターフェイスIDは、ローカルルータのインターフェイスIDと同じにする必要があります。この例では、スタティックIPが選択されています。

Basic Settings

Advanced Settings

Failover

Enable:

Connection Name: TestVPN1

IPsec Profile: CiscoTestVPN Auto (IKEv1) Profile is Chosen.

Interface: WAN1

Remote Endpoint: Static IP
Static IP
FQDN
Dynamic IP

ステップ 8 : リモートルーターのWANインターフェイスのIPアドレスを入力します。

注 : この例では、124.123.122.123が使用されています。

Enable:

Connection Name: TestVPN

IPsec Profile: CiscoTestVPN Auto (IKEv1) Profile is Chosen.

Interface: WAN1

Remote Endpoint: Static IP

124.123.122.123

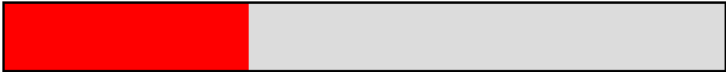
ステップ 9 : 必要なInternet Key Exchange (IKE) Authentication Methodのオプションボタンをクリックします。次のオプションがあります。

- Preshared Key : このオプションは、接続が接続を完了するためにパスワードが必要であることを意味します。事前共有キーは、VPN接続の両端で同じである必要があります。
- Certificate : このオプションは、認証方法が接続時にパスワードではなくルータによって生成された証明書を使用していることを意味します。

注 : この例では、Preshared Keyが選択されています。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

ステップ 10 : Preshared KeyフィールドにVPN接続の事前共有キーを入力します。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

ステップ11: (オプション) VPN接続に単純なパスワードを使用する場合は、Minimum Preshared Key Complexity Enableチェックボックスのチェックマークを外します。このチェックボックスは、デフォルトではオンになっています。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:



Minimum Pre-shared Key Complexity:

Enable

Show Pre-shared Key:

Enable

Certificate:

ステップ12: (オプション) 事前共有キーをプレーンテキストで表示するには、Show plain text when edit Enableチェックボックスにチェックマークを付けます。デフォルトではオフになっています。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:



Minimum Pre-shared Key Complexity:

Enable

Show Pre-shared Key:

Enable

Certificate:

ステップ 13Local Identifier Typeドロップダウンリストから、ローカルネットワークのIDタイプを選択します。次のオプションがあります。

- Local WAN IP : このオプションは、インターフェイスのWAN IPを介してローカルネットワークを識別します。
- IPアドレス : このオプションは、ローカルIPアドレスを使用してローカルネットワークを識別します。
- Local FQDN : このオプションを選択すると、ローカルネットワークがFQDNを使用して識別されます (存在する場合) 。
- Local User FQDN : このオプションは、ユーザのEメールアドレスであるユーザのFQDNを

使用してローカルネットワークを識別します。

注：この例では、IPアドレスが選択されています。

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="Local WAN IP"/> <input type="text" value="IP Address"/> <input type="text" value="Local FQDN"/> <input type="text" value="Local User FQDN"/>
Local IP Type:	
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

ステップ 14 : Local IdentifierフィールドにローカルネットワークのIDを入力します。

注：この例では、124.123.122.121と入力します。

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

ステップ 15 : Local IP Typeドロップダウンリストから、VPN ClientがアクセスできるIPアドレスタイプを選択します。次のオプションがあります。

- Subnet : このオプションを使用すると、VPNのリモート側から、指定されたサブネット内のローカルホストにアクセスできます。
- IP Address : このオプションを使用すると、VPNのリモート側が、指定されたIPアドレスを

持つローカルホストにアクセスできます。

- Any : このオプションを使用すると、VPNのリモート側から任意のローカルホストにアクセスできます。

注 : この例では、Subnetが選択されています。

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<div style="border: 1px solid #0070C0; padding: 2px;">Subnet</div> <ul style="list-style-type: none">IP AddressIP GroupGRE InterfaceAny
Subnet Mask:	<input type="text"/>

ステップ 16 : IP Addressフィールドに、VPNクライアントがアクセスするネットワークまたはホストのIPアドレスを入力します。

注 : この例では、IPアドレスは10.10.10.1です。

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input style="border: 2px solid #008000;" type="text" value="10.10.10.1"/>
Subnet Mask:	<input style="border: 2px solid #C00000;" type="text"/>

ステップ 17 : Subnet MaskフィールドにIPアドレスのサブネットマスクを入力します。

注 : この例では、サブネットマスクは255.255.255.0です。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.121

Local IP Type:

Subnet

IP Address:

10.10.10.1

Subnet Mask:

255.255.255.0

ステップ 18 : ドロップダウンリストからリモートIDタイプを選択します。次のオプションがあります。

- リモートWAN IP : このオプションは、インターフェイスのWAN IPを介してリモートネットワークを識別します。
- リモートFQDN : このオプションは、FQDNを使用してリモートネットワークを識別します (存在する場合)。
- Remote User FQDN : このオプションは、ユーザのFQDN (電子メールアドレスなど) によってリモートネットワークを識別します。

注 : この例では、リモートWAN IPが選択されています。

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

Remote WAN IP

Remote FQDN

Remote User FQDN

Remote IP Type:

Subnet

IP Address:

Subnet Mask:

ステップ 19 : Remote IdentifierフィールドにリモートルータのWAN IPアドレスを入力します。

注 : この例では、リモートIDは124.123.122.123です。

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="124.123.122.123"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

ステップ 20 : Remote IP Typeドロップダウンリストから、ローカルネットワークがアクセスする必要があるネットワークタイプを選択します。次のオプションがあります。

- IP Address : このオプションを使用すると、ローカルホストは指定されたIPアドレスを持つリモートホストにアクセスできます。
- Subnet : このオプションを使用すると、ローカルホストは指定されたサブネットのリモートホスト上のリソースにアクセスできます。
- Any : このオプションを使用すると、ローカルホストは任意のIPアドレスを使用してリモートホスト上のリソースにアクセスできます。

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 124.123.122.123

Remote IP Type: Subnet

IP Address:

Subnet Mask:

- Subnet
- IP Address
- IP Group
- Any

ステップ 21 : IP AddressフィールドにリモートネットワークのLAN IPアドレスを入力します。

注 : この例では、IPアドレスは192.168.2.1です。

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 124.123.122.123

Remote IP Type: Subnet

IP Address: 192.168.2.1

Subnet Mask:

ステップ 22 : Subnet Maskフィールドにリモートネットワークのサブネットマスクを入力します。

注 : この例では、サブネットマスクは255.255.255.0です。

Remote Group Setup

Remote Identifier Type:	Remote WAN IP
Remote Identifier:	124.123.122.123
Remote IP Type:	Subnet
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0

ステップ 23 : [APPLY] をクリックします。

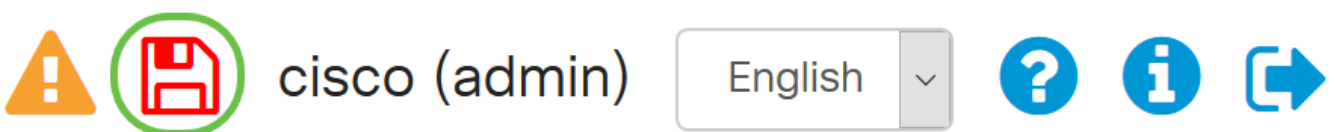
Add/Edit a New Connection Apply Cancel

Local IP Type:	Subnet
IP Address:	10.10.10.1
Subnet Mask:	255.255.255.0

Remote Group Setup

Remote Identifier Type:	Remote WAN IP
Remote Identifier:	124.123.122.123
Remote IP Type:	Subnet
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0

ステップ 24 : [Save] をクリックします。



これで、ローカルルータのVPN設定が完了しました。

リモート ルータ

ステップ 1：次のようなローカルルータのVPN設定を決定します。

- VPN接続に使用されるローカルルータとリモートルータのインターフェイス。
- ローカルルータとリモートルータのワイドエリアネットワーク(WAN)インターネットプロトコル(IP)アドレス。
- ローカルエリアネットワーク(LAN)アドレス、およびローカルネットワークとリモートネットワークのサブネットマスク。
- VPN接続用の事前共有キー、パスワード、または証明書。
- ローカルルータのセキュリティ設定。
- VPN接続のファイアウォール除外。

ステップ 2：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の順に選択します。



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

2

Site-to-Site

Client-to-Site

Teleworker VPN Client

PPTP Server

ステップ 3 : ローカルルータのVPNセキュリティ設定と一致するように、リモートルータのVPNセキュリティ設定を設定します。手順については[ここ](#)をクリックしてください。

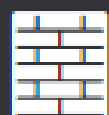
ステップ 4 : ローカルルータのWebベースのユーティリティで、VPN > Site-to-Siteの順に選択します。



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

Site-to-Site

2

Client-to-Site

Teleworker VPN Client

PPTP Server

ステップ 5 : プラスアイコンをクリックします。

Site to Site Table

^



□ Connection Name ◆ Remote Endpoint ◆ Interface ◆ IPsec Profile ◆ Local Traffic Selection ◆ Remote Traffic Selection ◆ Sta

手順 6 : Enableチェックボックスにチェックマークが付いていることを確認します。デフォルトではオンになっています。

Enable:



Connection Name:

Please Input Connection Name

IPsec Profile:

Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

手順 7 : Connection NameフィールドにVPN接続の名前を入力します。リモートルータの接続名は、ローカルルータで指定されている接続名と異なる場合があります。

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

注：この例では、接続名はTestVPNです。

ステップ 8：ドロップダウンリストからIPSecプロファイルを選択します。オプションは、作成されたIPSecプロファイルによって異なります。IPSecプロファイルの作成手順については、[ここ](#)をクリックしてください。

注：この例では、CiscoTestVPNが選択されています。

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

ステップ 9 : ドロップダウンリストから、リモートルータがVPN接続に使用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 : このオプションは、VPN接続にリモートルータのワイドエリアネットワーク 1(WAN1)インターフェイスのIPアドレスを使用します。
- WAN2 : このオプションは、VPN接続にリモートルータのWAN2インターフェイスのIPアドレスを使用します。WAN2はシングルWANルータでは使用できません。
- USB1 : このオプションは、VPN接続にリモートルータのUniversal Serial Bus 1(USB1)インターフェイスのIPアドレスを使用します。
- USB2 : このオプションは、VPN接続にリモートルータのUSB2インターフェイスのIPアドレスを使用します。USB2はシングルUSBルータでは使用できません。

注 : この例では、WAN1が選択されています。

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

ステップ 10 : Remote Endpointドロップダウンリストから、ローカルルータのWANインターフェイスのIDを選択します。次のオプションがあります。

- スタティックIP : このオプションを使用すると、リモートルータはVPN接続を確立するときに、ローカルルータのスタティックIPアドレスを使用します。ローカルルータでこのオプションを選択した場合は、リモートルータも同じオプションで設定する必要があります。
- FQDN : このオプションは、VPN接続を確立するときにローカルルータの完全修飾ドメイン名(FQDN)を使用します。
- ダイナミックIP : このオプションは、VPN接続を確立するときに、ローカルルータのダイナミックIPアドレスを使用します。

注：リモートルータのインターフェイスIDは、ローカルルータのインターフェイスIDと同じにする必要があります。この例では、スタティックIPが選択されています。

Enable:

Connection Name:

IPsec Profile:

Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

ステップ 11ローカルルータのWAN IPアドレスを入力します。

注：この例では、IPアドレスは124.123.122.121です。

Enable:

Connection Name:

IPsec Profile:

Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

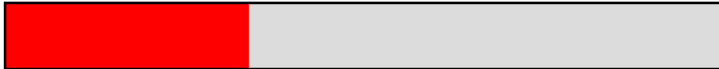
ステップ 12 必要な Internet Key Exchange (IKE) Authentication Method のオプションボタンをクリックします。次のオプションがあります。

- Preshared Key : このオプションは、接続が接続を完了するためにパスワードが必要であることを意味します。事前共有キーは、VPN 接続の両端で同じである必要があります。
- Certificate : このオプションは、認証方法が接続時にパスワードではなくルータによって生成された証明書を使用していることを意味します。

注 : この例では、Preshared Key が選択されています。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

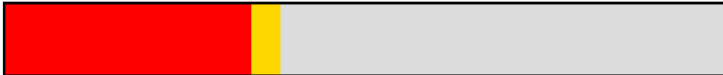
Certificate:

ステップ 13 Preshared Key フィールドに VPN 接続の事前共有キーを入力します。

IKE Authentication Method

Pre-shared Key:

●●●●●●●●

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

ステップ 14: (オプション) VPN 接続に簡単なパスワードを使用する場合は、Minimum Preshared Key Complexity チェックボックス Enable ボックスのチェックマークを外します。このチェックボ

ックスは、デフォルトではオンになっています。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:



Minimum Pre-shared Key
Complexity:

Enable

Show Pre-shared Key:

Enable

Certificate:

ステップ15: (オプション) Show plain text when edit Enableチェックボックスにチェックマークを入れて、事前共有キーをプレーンテキストで表示します。デフォルトではオフになっています。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:



Minimum Pre-shared Key
Complexity:

Enable

Show Pre-shared Key:

Enable

Certificate:

ステップ 16 : リモートルータのLocal Identifier Typeドロップダウンリストから、リモートネットワークのIDタイプを選択します。次のオプションがあります。

- ローカルWAN IP : このオプションは、インターフェイスのWAN IPを介してリモートネットワークを識別します。
- IPアドレス : このオプションは、ローカルIPアドレスを使用してリモートネットワークを識別します。
- ローカルFQDN : このオプションは、FQDNを使用してリモートネットワークを識別します

(存在する場合)。

- Local User FQDN : このオプションは、ユーザのFQDN (電子メールアドレスなど) によってリモートネットワークを識別します。

注 : この例では、IPアドレスが選択されています。

Local Group Setup

Local Identifier Type:	IP Address
Local Identifier:	Local WAN IP IP Address Local FQDN Local User FQDN
Local IP Type:	
IP Address:	
Subnet Mask:	

ステップ 17 : リモートルータのLocal IdentifierフィールドにリモートネットワークのIDを入力します。

注 : この例では、124.123.122.123と入力します。

Local Group Setup

Local Identifier Type:	IP Address
Local Identifier:	124.123.122.123
Local IP Type:	Subnet
IP Address:	
Subnet Mask:	

ステップ 18 : Local IP Typeドロップダウンリストから、VPN ClientがアクセスできるIPアドレスタイプを選択します。次のオプションがあります。

- Subnet : このオプションを使用すると、VPNのローカル側が指定されたサブネットのリモ

ートホストにアクセスできます。

- IP Address : このオプションを使用すると、VPNのローカル側が、指定されたIPアドレスを持つリモートホストにアクセスできます。
- Any : このオプションを使用すると、VPNのローカル側が任意のリモートホストにアクセスできます。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.123

Local IP Type:

Subnet

IP Address:

Subnet

IP Address

IP Group

GRE Interface

Any

Subnet Mask:

注 : この例では、Subnetが選択されています。

ステップ 19 : IP Addressフィールドに、VPNクライアントがアクセスするネットワークまたはホストのIPアドレスを入力します。

注 : この例では、IPアドレスは192.168.2.1です。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.123

Local IP Type:

Subnet

IP Address:

192.168.2.1

Subnet Mask:

ステップ 20 : Subnet MaskフィールドにIPアドレスのサブネットマスクを入力します。

注：この例では、サブネットマスクは255.255.255.0です。

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.123"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

ステップ 21：ドロップダウンリストからLocal Identifier Typeを選択します。次のオプションがあります。

- リモートWAN IP：このオプションは、インターフェイスのWAN IPを介してローカルネットワークを識別します。
- リモートFQDN：このオプションは、ローカルネットワークにFQDNが設定されている場合に、そのFQDNを使用してローカルネットワークを識別します。
- リモートユーザFQDN：このオプションは、ユーザのEメールアドレスであるユーザのFQDNを使用してローカルネットワークを識別します。

注：この例では、リモートWAN IPが選択されています。

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="124.123.122.121"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="10.10.10.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

ステップ 22 : [APPLY] をクリックします。

Add/Edit a New Connection

Apply Cancel

Local IP Type:

IP Address:

Subnet Mask:

Remote Group Setup

Remote Identifier Type:

Remote Identifier:

Remote IP Type:

IP Address:

Subnet Mask:

ステップ 23 : [Save] をクリックします。



これで、リモートルータのVPN設定が完了しました。

この記事の関連ビデオを見る...

[シスコの他のテクニカルトークを表示するには、こちらをクリックしてください](#)

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。