RV34xシリーズルータでのクライアント/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

クライアントからサイトへの仮想プライベートネットワーク(VPN)接続では、インターネットからのクライアントはサーバに接続して、サーバの背後にある企業ネットワークまたはローカルエリアネットワーク(LAN)にアクセスできますが、ネットワークとそのリソースのセキュリティは維持されます。この機能は、新しいVPNトンネルを作成し、VPNクライアントソフトウェアを使用して、プライバシーとセキュリティを犠牲にすることなく、テレワーカーや出張者がネットワークにアクセスできるようにするため、非常に便利です。

このドキュメントの目的は、RV34xシリーズルータでクライアントからサイトへの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

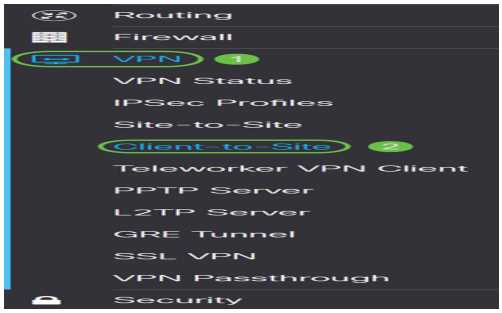
- RV34xシリーズ

[Software Version]

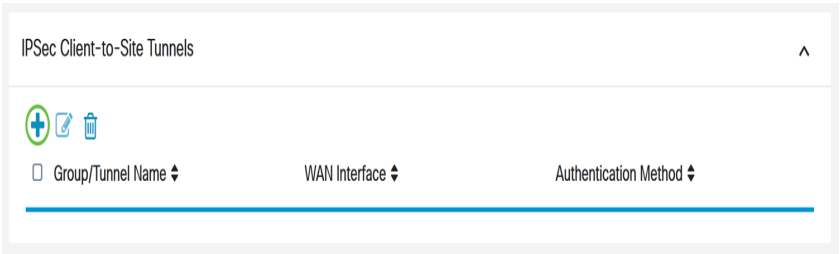
- 1.0.01.16

クライアントからサイトへのVPNの設定

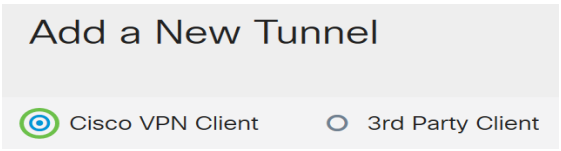
ステップ1：ルータのWebベースユーティリティにログインし、[VPN] > [Client-to-Site]を選択します。



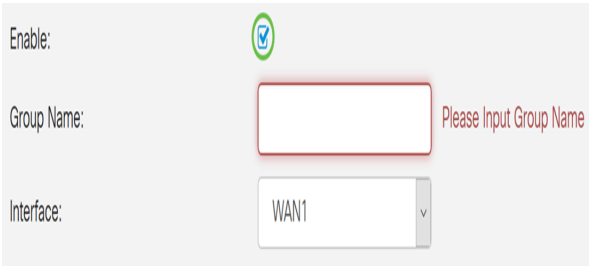
ステップ2:[IPSec Client-to-Site Tunnels]セクションの下の[Add]ボタンをクリックします。



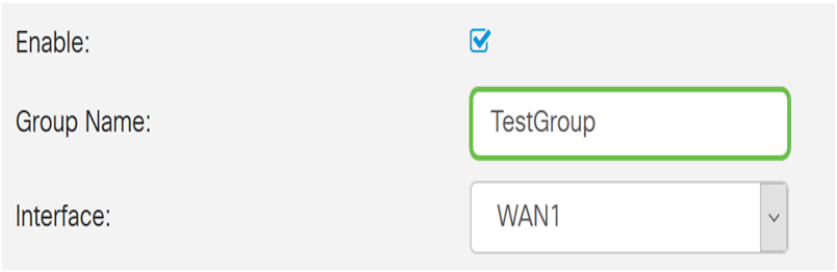
ステップ3:[Add a *New Tunnel*]領域で、[Cisco VPN Client]ラジオボタンをクリックします。



ステップ4:[Enable] チェックボックスをオンにして、設定を有効にします。



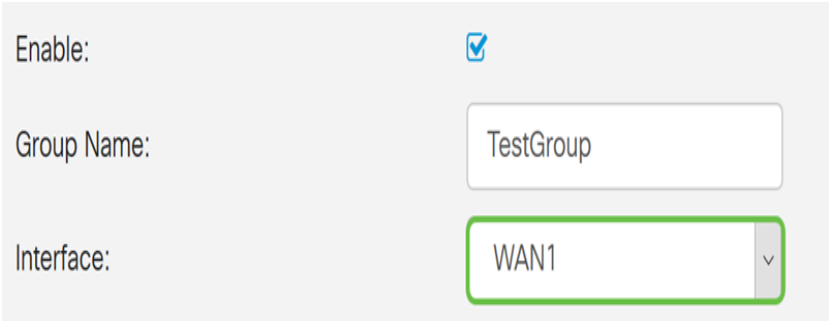
ステップ5：表示されたフィールドにグループ名を入力します。これは、インターネットキー交換(IKE)ネゴシエーション中に、このグループのすべてのメンバーの識別子として機能します。



注：A ～ Zまたは0 ～ 9の間の文字を入力してください。グループ名にはスペースと特殊文字は使用できません。この例では、TestGroupが使用されています。

ステップ6：ドロップダウンリストをクリックして、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



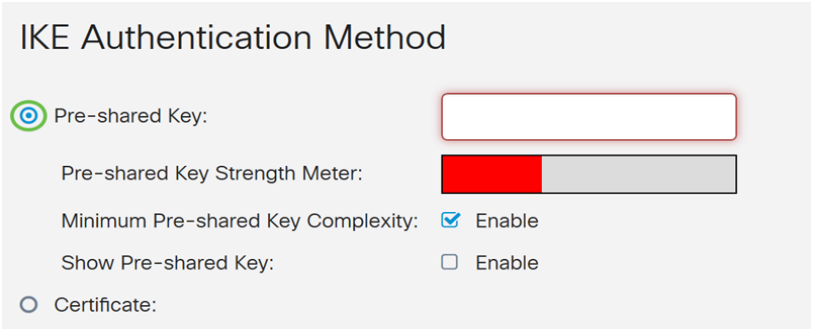
注：この例では、WAN1が選択されています。これがデフォルト設定です。

ステップ7:[IKE Authentication Method]領域で、IKEベースのトンネルのIKEネゴシエーションで使用する認証方法を選択します。次のオプションがあります。

- 事前共有キー：IKEピアは、事前共有キーを含むデータのキー付きハッシュを計算して送信することで、相互に認証します。受信側ピアが事前共有キーを使用して別々に同じ

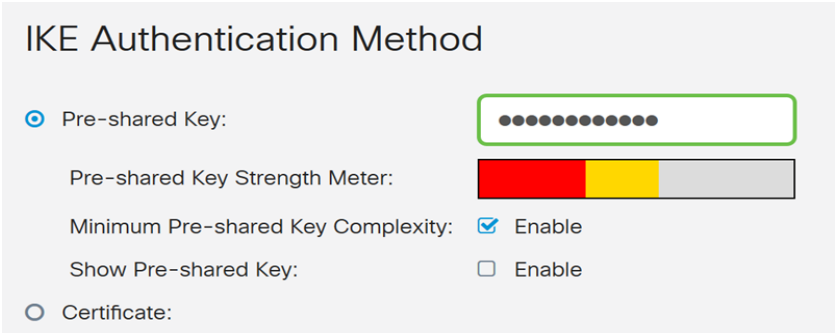
ハッシュを作成できる場合、両方のピアが同じシークレットを共有する必要があることを認識しているため、他方のピアが認証されます。各IPSecピアは、セッションを確立する他のすべてのピアの事前共有キーを使用して設定する必要があるため、事前共有キーは適切に拡張されません。

- 証明書：デジタル証明書は、ベアラの証明書IDなどの情報を含むパッケージです。名前またはIPアドレス、証明書のシリアル番号の有効期限、証明書ベアラの公開キーのコピー。標準のデジタル証明書形式は、X.509仕様で定義されています。X.509 version 3は、証明書のデータ構造を定義します。



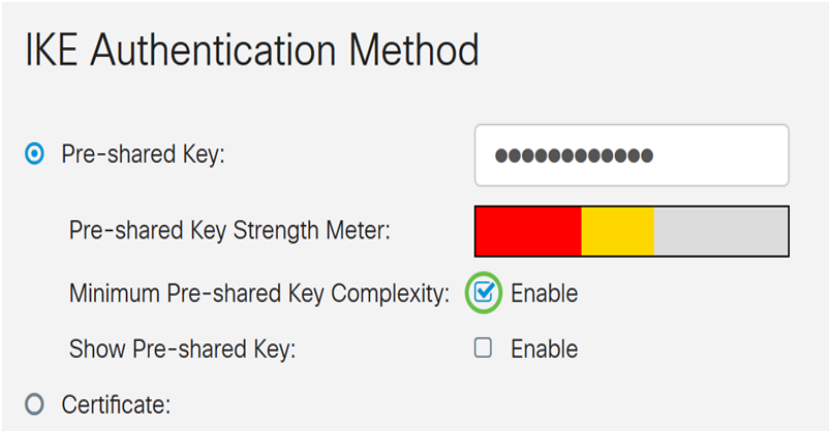
注：この例では、[Pre-shared Key]が選択されています。これがデフォルト設定です。

ステップ8：表示されたフィールドに事前共有キーを入力します。これは、IKEピアのグループ間の認証キーになります。

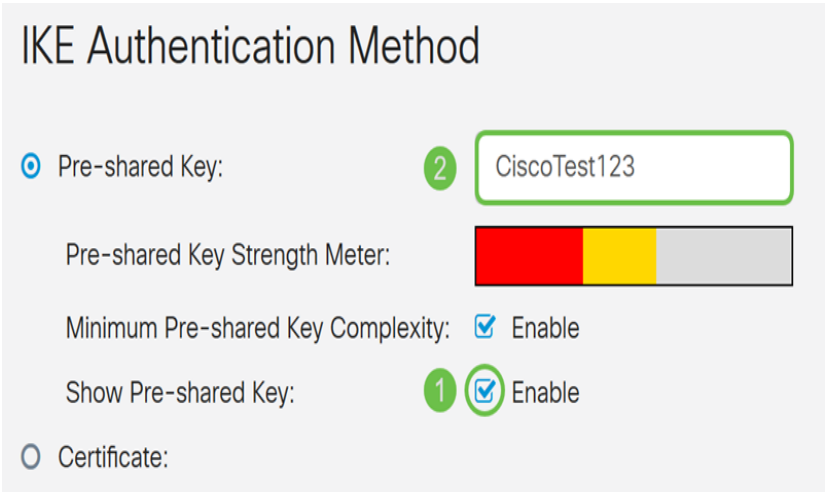


ステップ9:（オプション）事前共有キーの最小複雑度の**Enable**チェックボックスをオンにして、事前共有キーの強度メーターを表示し、キーの強度を決定します。キーの強度は次のように定義されます。

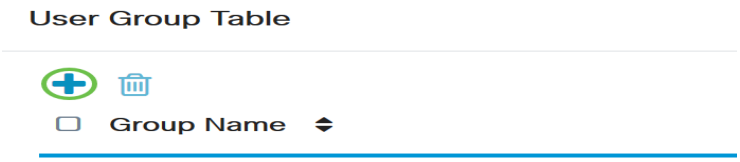
- 赤色：パスワードが脆弱です。
- オレンジ：パスワードがかなり強い。
- 緑：パスワードが強力です。



注：[Show Pre-shared Key]フィールドの[**Enable**]チェックボックスをオンにして、パスワードを平文で確認できます。

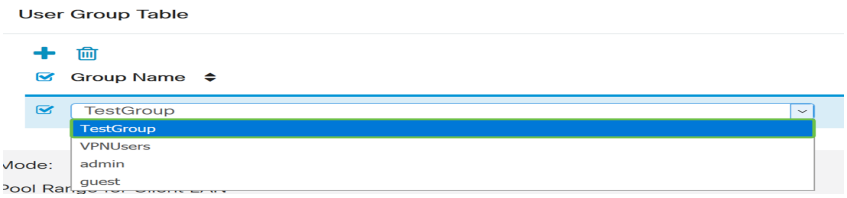


ステップ10: (オプション) グループを追加するには、「ユーザグループ」(User Group)テーブルのプラス(+)アイコンをクリックします。



ステップ11: (オプション) ドロップダウンリストから、ユーザグループがadmin用かguests用かを選択します。ユーザアカウントを使用して独自のユーザグループを作成した場合は、そのユーザグループを選択できます。この例では、[TestGroup]を選択します。

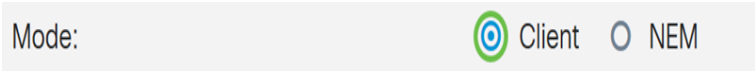
注：TestGroupは、[システムの設定(System Configuration)] > [ユーザグループ(User Groups)]で**作成したユーザグループです**。



注：この例では、TestGroupが選択されています。ユーザグループを削除する場合は、ユーザグループの横にあるチェックボックスをオンにし、[**Delete**]ボタンをクリックすることもできます。

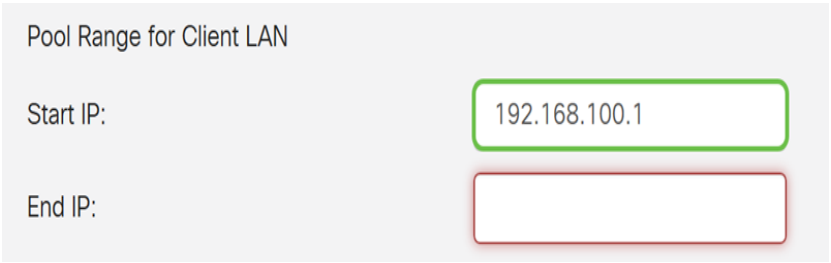
ステップ12：オプションボタンをクリックして、モードを選択します。次のオプションがあります。

- Client：このオプションを使用すると、クライアントはIPアドレスを要求でき、サーバは設定されたアドレス範囲からIPアドレスを提供します。
- Network Extension Mode(NEM)：このオプションを使用すると、クライアントは、サーバの背後にあるLANとクライアントによって提案されたサブネット間のトラフィックにVPNサービスを適用する必要があるサブネットを提案できます。



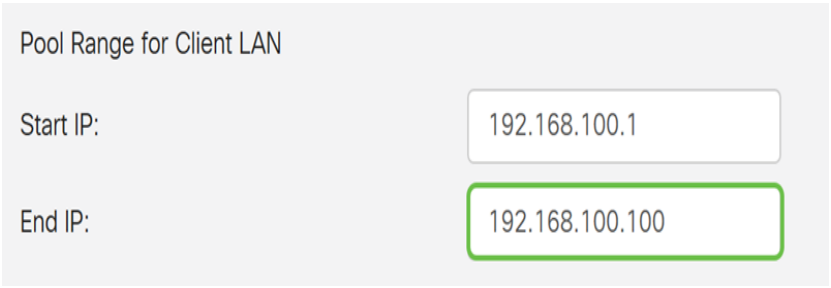
注：この例では、[Client]が選択されています。

ステップ13:[Start IP]フィールドに開始IPアドレスを入力します。これは、クライアントに割り当てることができるプール内の最初のIPアドレスです。



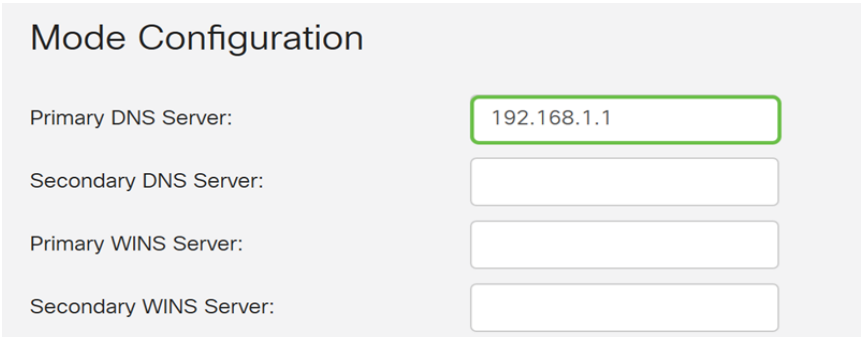
注：この例では、192.168.100.1が使用されています。

ステップ14:[End IP]フィールドに終了IPアドレスを入力します。これは、クライアントに割り当てることができるプール内の最後のIPアドレスです。



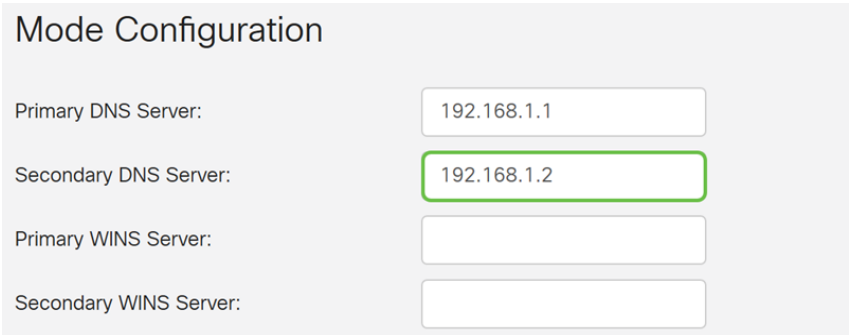
注：この例では、192.168.100.100 が使用されます。

ステップ15:（オプション）[*Mode Configuration*]領域で、表示されたフィールドにプライマリDNSサーバのIPアドレスを入力します。



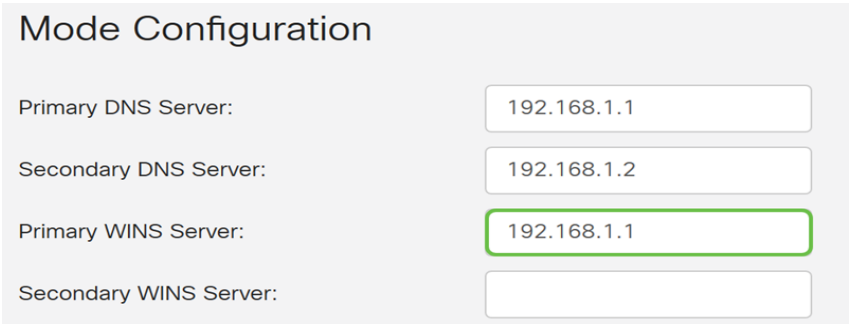
注：この例では、192.168.1.1が使用されています。

ステップ16:（オプション）表示されたフィールドにセカンダリDNSサーバのIPアドレスを入力します。



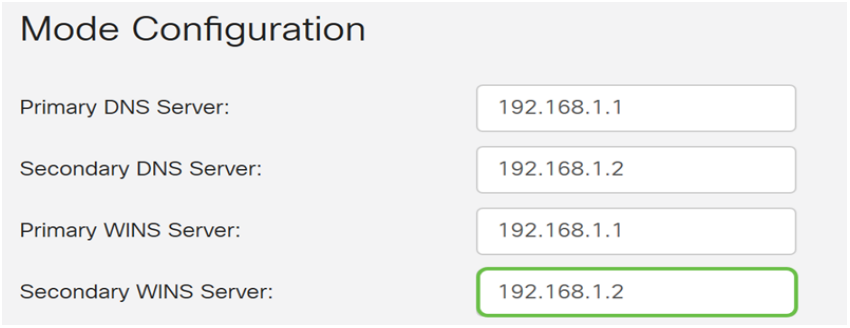
注：この例では、192.168.1.2が使用されています。

ステップ17: (オプション) フィールドにプライマリWINSサーバのIPアドレスを入力します。



注：この例では、192.168.1.1が使用されています。

ステップ18: (オプション) 表示されたフィールドにセカンダリWINSサーバのIPアドレスを入力します。



注：この例では、192.168.1.2が使用されています。

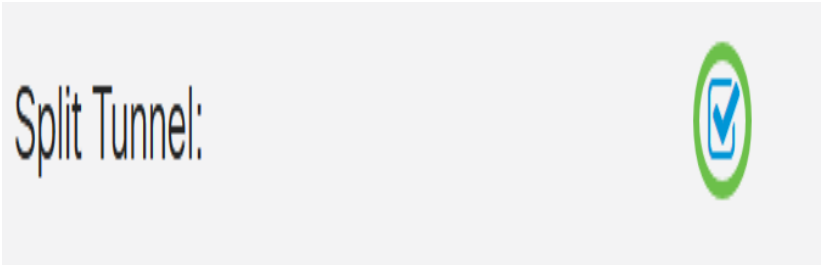
ステップ19: (オプション) 表示されたフィールドに、リモートネットワークで使用するデフォルトドメインを入力します。

注：この例では、sample.comが使用されています。

ステップ20: (オプション) [*バックアップサーバ1]フィールド*に、バックアップサーバのIPアドレスまたはドメイン名を入力します。これは、プライマリIPSec VPNサーバに障害が発生した場合に、デバイスがVPN接続を開始できる場所です。表示されるフィールドには、最大3つのバックアップサーバを入力できます。バックアップサーバ1は3つのサーバの中で最も優先度が高く、バックアップサーバ3は最も優先度が低い。

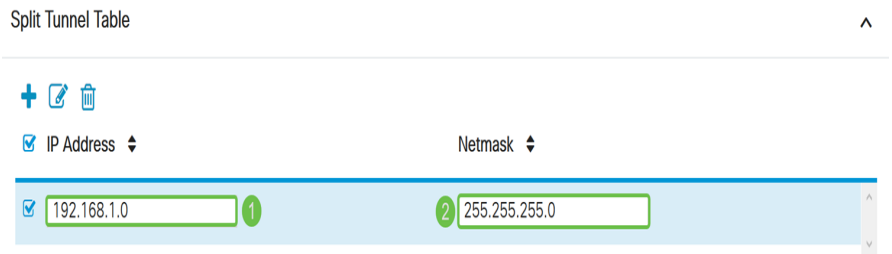
注：この例では、バックアップサーバ1にExample.comが使用されます。

ステップ21: (オプション) スプリットトンネルを有効にするには、**[スプリットトンネル]**チェックボックスをオンにします。スプリットトンネリングでは、プライベートネットワークとインターネットのリソースに同時にアクセスできます。



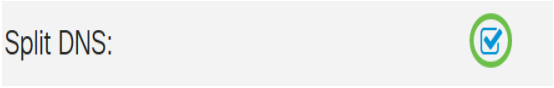
ステップ22: (オプション) スプリットトンネルテーブルの下で、プラス**アイコン**をクリックして、スプリットトンネルのIPアドレスを追加します。

ステップ23: (オプション) 表示されたフィールドに、スプリットトンネルのIPアドレスとネットマスクを入力します。

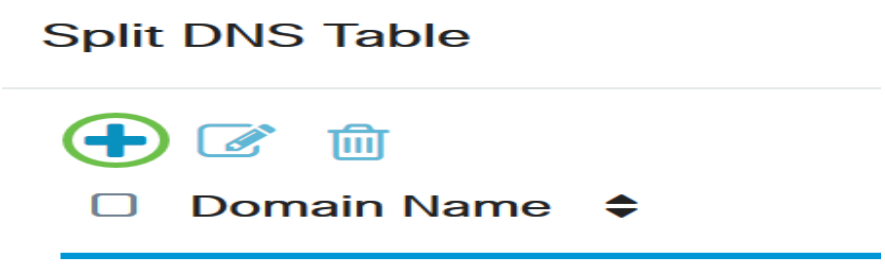


注：この例では、192.168.1.0と255.255.255.0が使用されています。このボックスをオンにし、**[Add]**、**[Edit]**、および**[Delete]**ボタンをそれぞれクリックして、スプリットトンネルを追加、編集、または削除することもできます。

ステップ24: (オプション) [スプリットDNS]チェックボックスを**オン**にして、スプリットDNSを有効にします。スプリットDNSを使用すると、ネットワークリソースのセキュリティとプライバシーを維持するために、内部および外部ネットワーク用に個別のDNSサーバを作成できます。



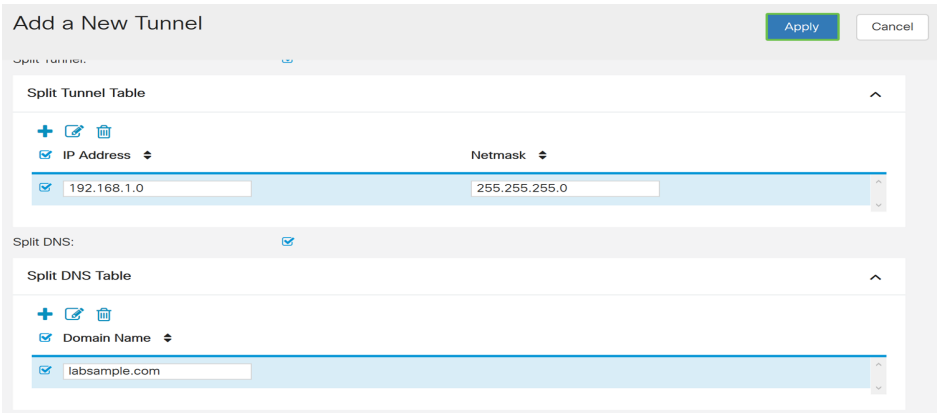
ステップ25:（オプション）スプリットDNSテーブルの下のプラス記号アイコンをクリックし、スプリットDNSのドメイン名を追加します。



ステップ26:（オプション）フィールドにスプリットDNSのドメイン名を入力します。

注：この例では、labsample.comが使用されています。このボックスをオンにし、[Add]、[Edit]、および[Delete]ボタンをクリックして、スプリットDNSをそれぞれ追加、編集、または削除することもできます。

ステップ27:[Apply]をクリックします。



結論

これで、RV34xシリーズルータでクライアントとサイト間の接続が正常に設定されました。

次のトピックの詳細については、次の記事をクリックしてください。

- RV34xシリーズルータでのテレワーカーVPNクライアントの設定
- GreenBow VPN Clientを使用したRV34xシリーズルータへの接続
- RV34xルータでのVPN Clientセットアップ用ユーザアカウントの作成
- RV34xルータでのVPN設定用のユーザグループの作成

この記事に関連するビデオを表示...

シスコのその他のテクニカルトークを表示するには、ここをクリックしてください