SDM を使用したリモート VPN サーバとしての Cisco ルータの設定例

目次

概要

このドキュメントでは、Cisco Security Device Manager（SDM）を使用して Cisco ルータが Easy VPN サーバとして動作するように設定する方法について説明しています。 Cisco SDM では、使いやすい Web ベースの管理インターフェイスを使用して、Cisco VPN Client のための VPN サーバとしてルータを設定できます。 Cisco ルータの設定が完了すると、Cisco VPN Client を使用して検証できます。

前提条件

要件

このドキュメントでは、Cisco ルータが完全に動作しており、Cisco SDM で設定変更できるように設定されていることを想定しています。

注: SDM でルータを設定できるようにするには、『SDM 用の HTTPS アクセスの許可』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS(R) ソフトウェア リリース 12.3(14T) が稼働する Cisco 3640 ルータ
- Security Device Manager バージョン 2.31
- Cisco VPN Client バージョン 4.8

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 こ

のドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

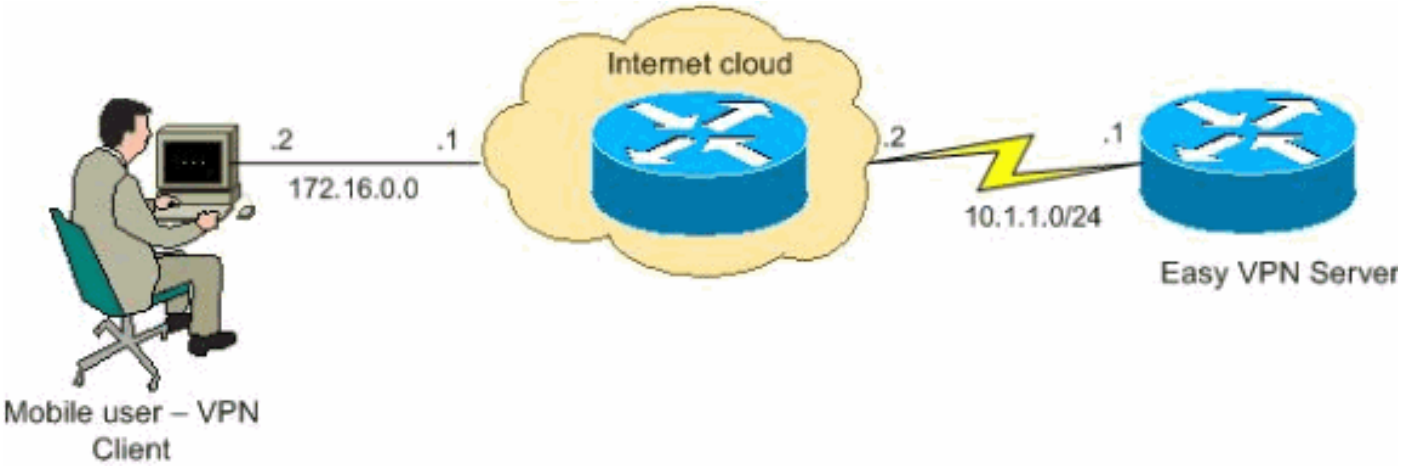
設定

このセクションでは、リモート エンド ユーザが IPSec を使用して任意の Cisco IOS(R) VPN ゲートウェイと通信できるようにする、Easy VPN サーバ機能を設定するための情報を説明しています。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

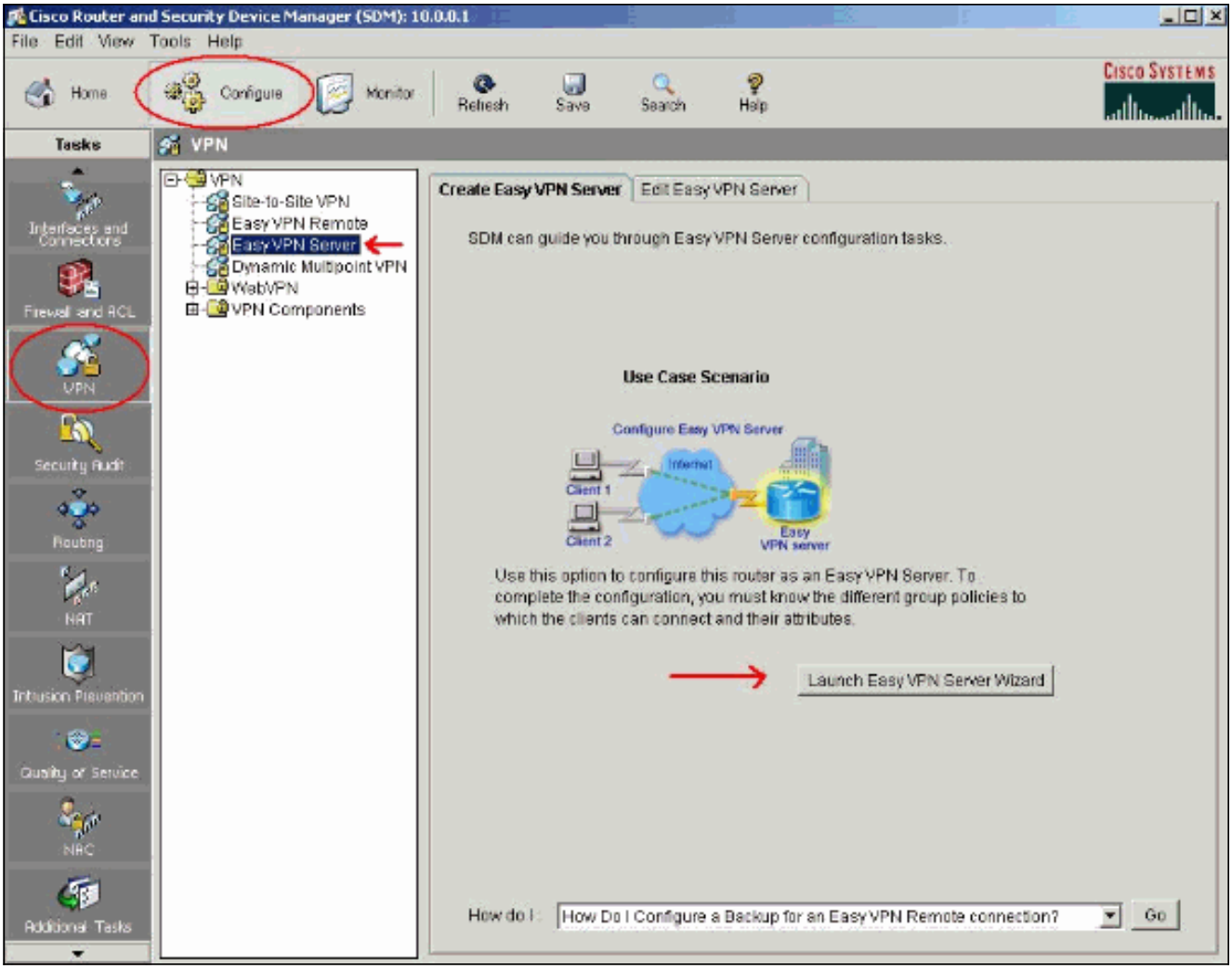
このドキュメントでは、次のネットワーク構成を使用しています。



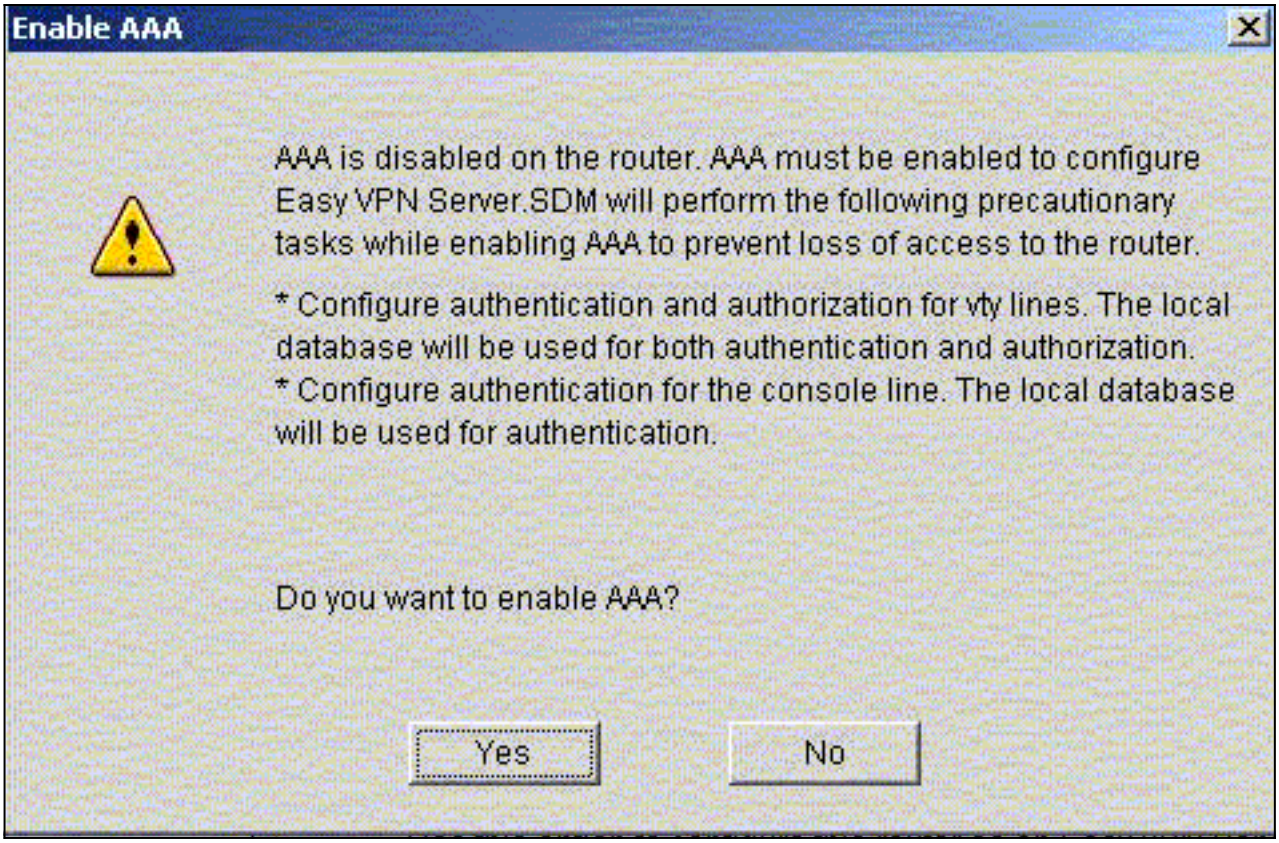
設定手順

SDM を使用して Cisco ルータをリモート VPN サーバとして設定するには、次の手順を実行します。

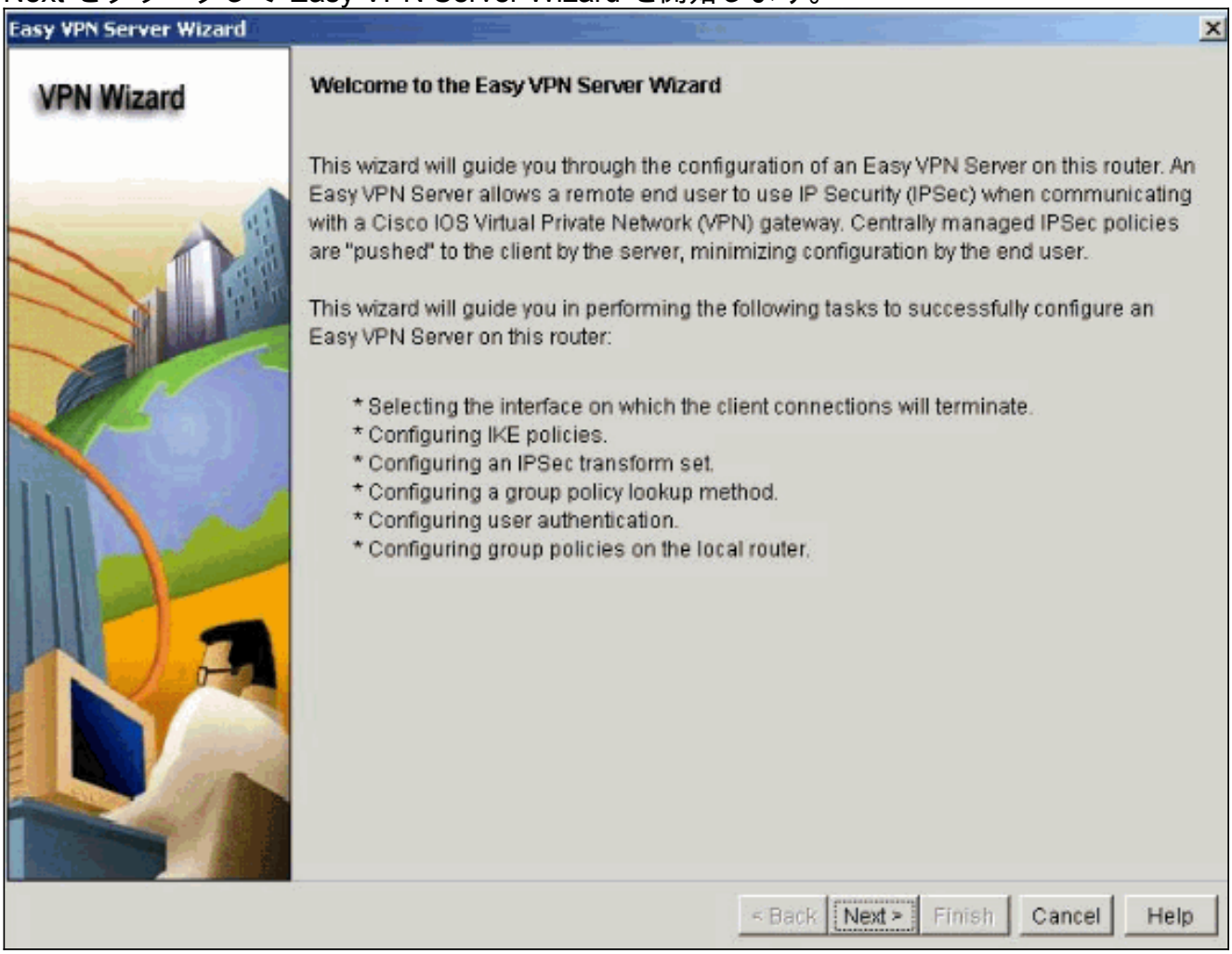
1. Home ウィンドウから Configure > VPN > Easy VPN Server の順に選択 し、『Launch Easy VPN Server Wizard』 をクリック して下さい。



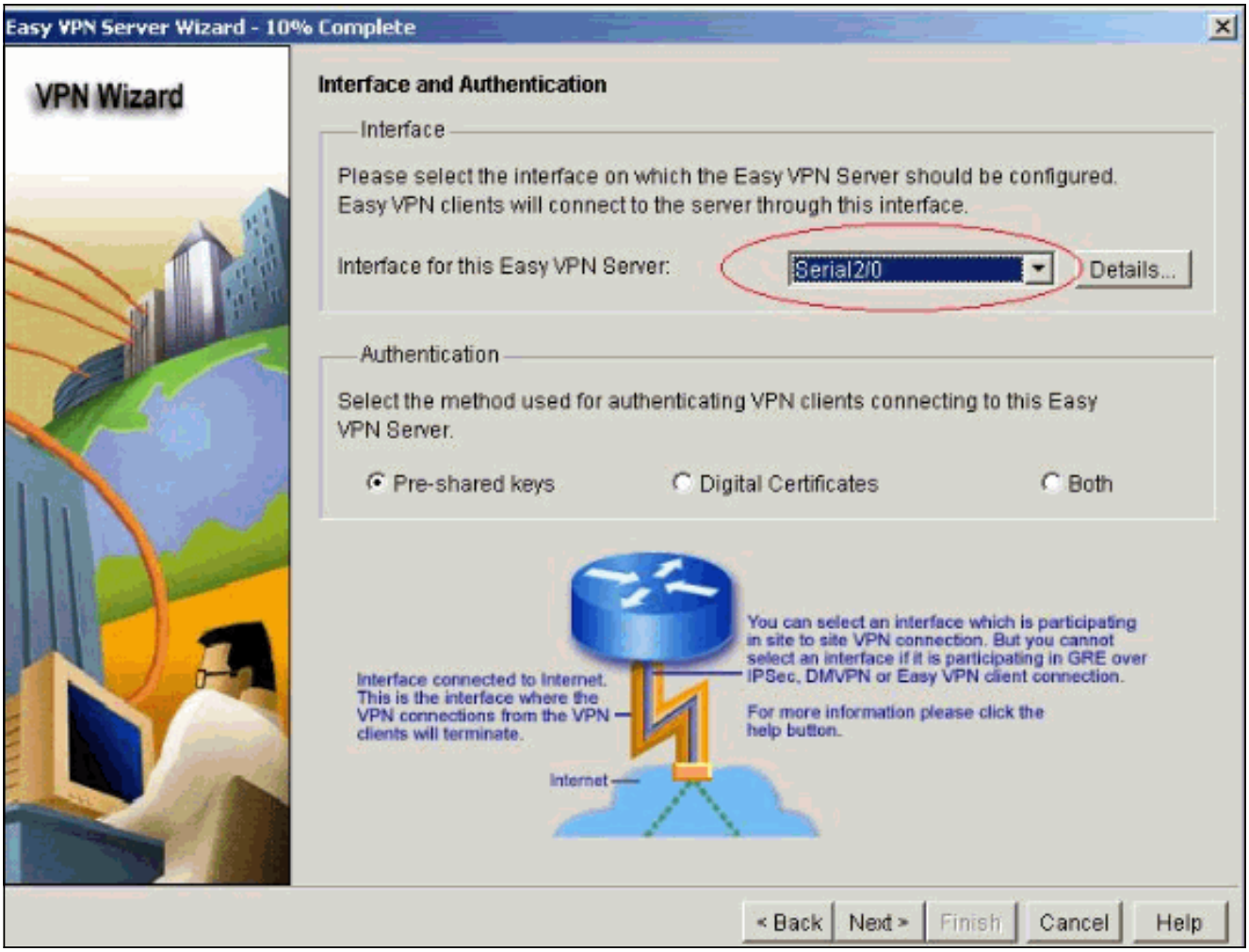
2. Easy VPN サーバの設定を始めるには、ルータ上で AAA が有効になっている必要があります。 Yes をクリックして設定を継続します。ウィンドウに「AAA has been successfully enabled on the router」というメッセージが表示されます。 OK をクリックして Easy VPN サーバの設定を開始します。



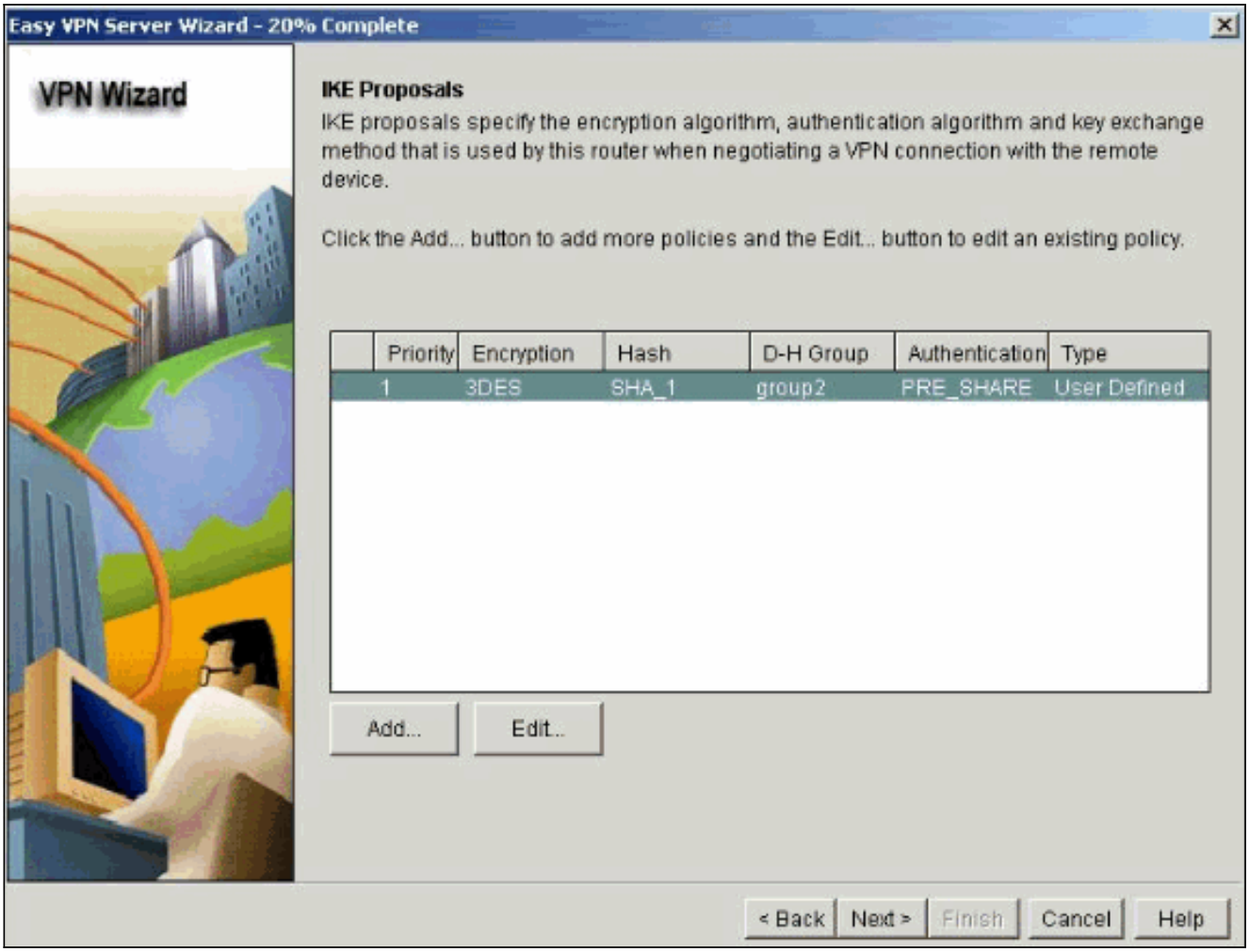
3. Next をクリックして Easy VPN Server Wizard を開始します。



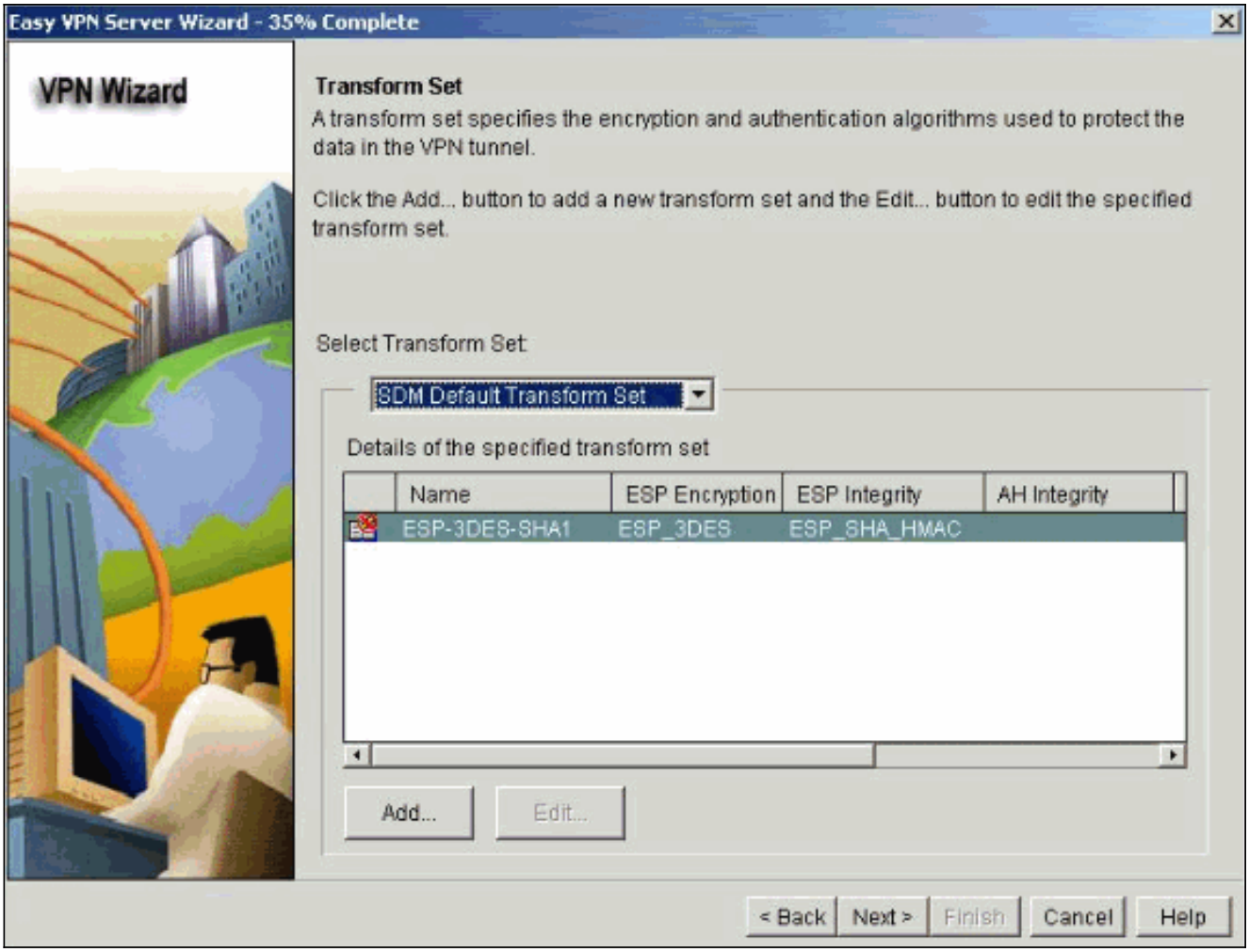
4. クライアント接続の終端となるインターフェイスと、認証タイプを選択します。



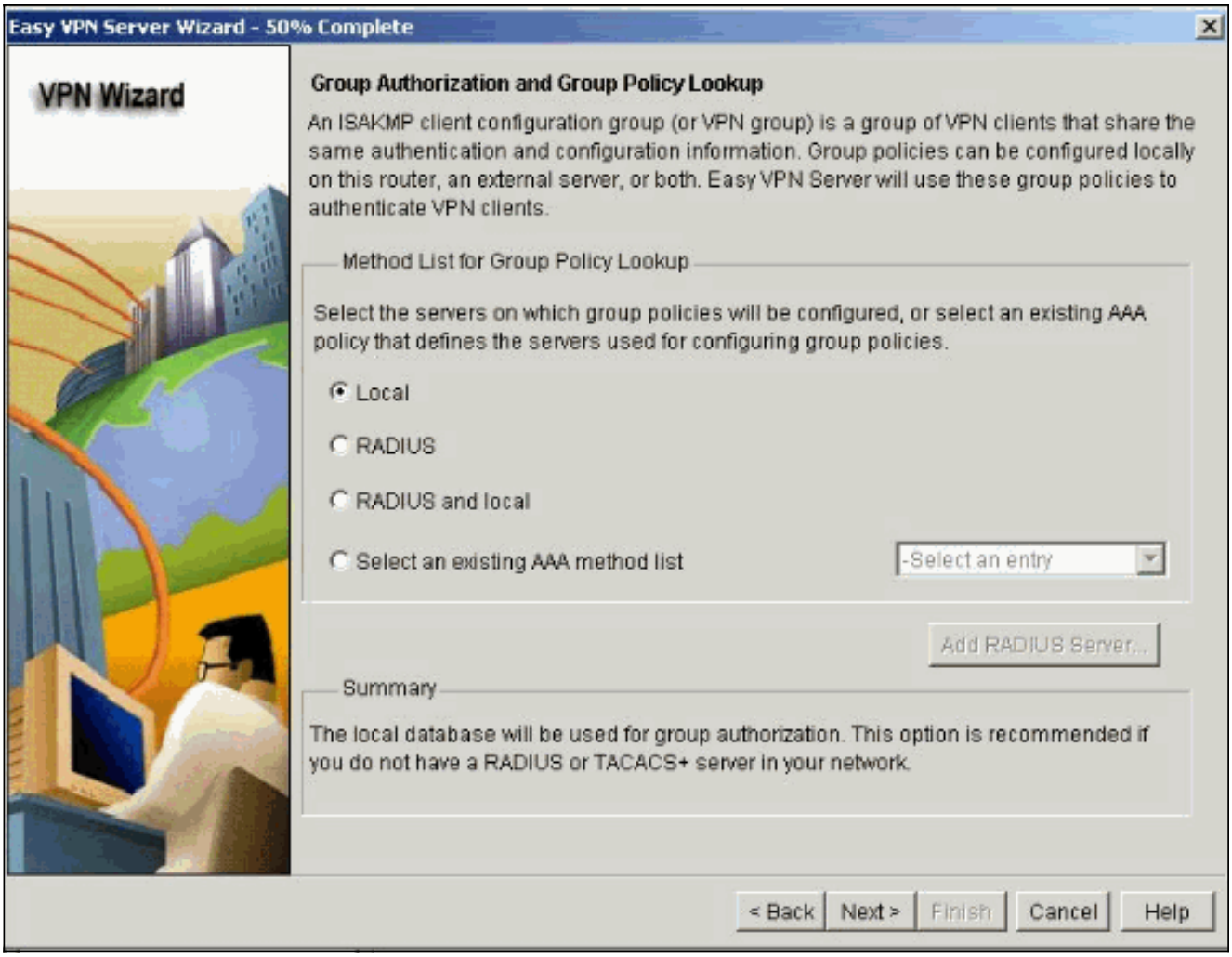
5. Next をクリックして Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ポリシーを設定し、Add ボタンを使用して新しいポリシーを作成します。トンネルの両側の設定は完全に一致している必要があります。 ただし、Cisco VPN Client では適切な設定が自動的に選択されます。 そのため、クライアント PC で IKE を設定する必要はありません。



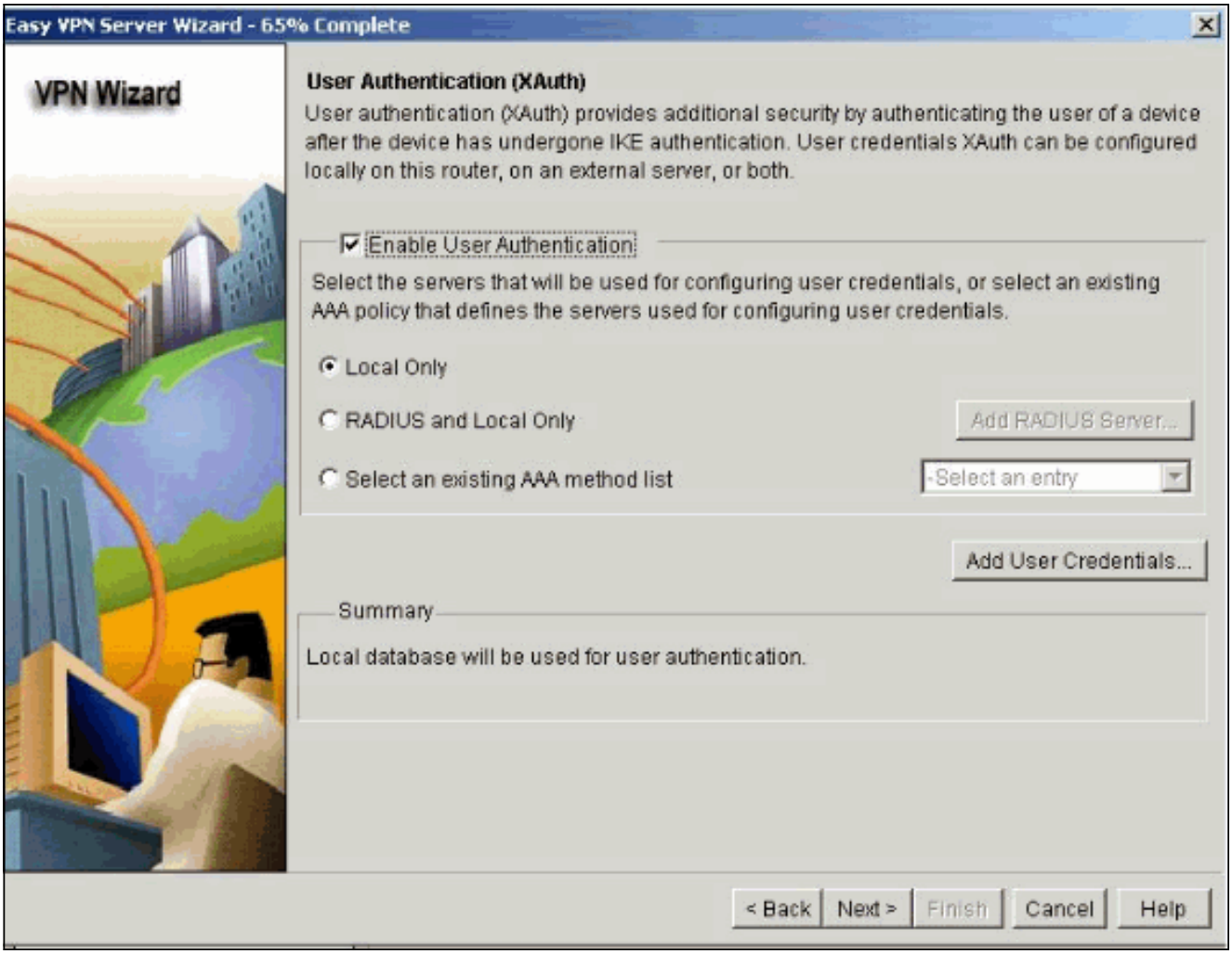
6. Next をクリックして、デフォルトのトランスフォーム セットを選択するか、新しいトランスフォーム セットを追加して暗号化と認証のアルゴリズムを指定します。 このケースでは、デフォルトのトランスフォーム セットを使用しています。



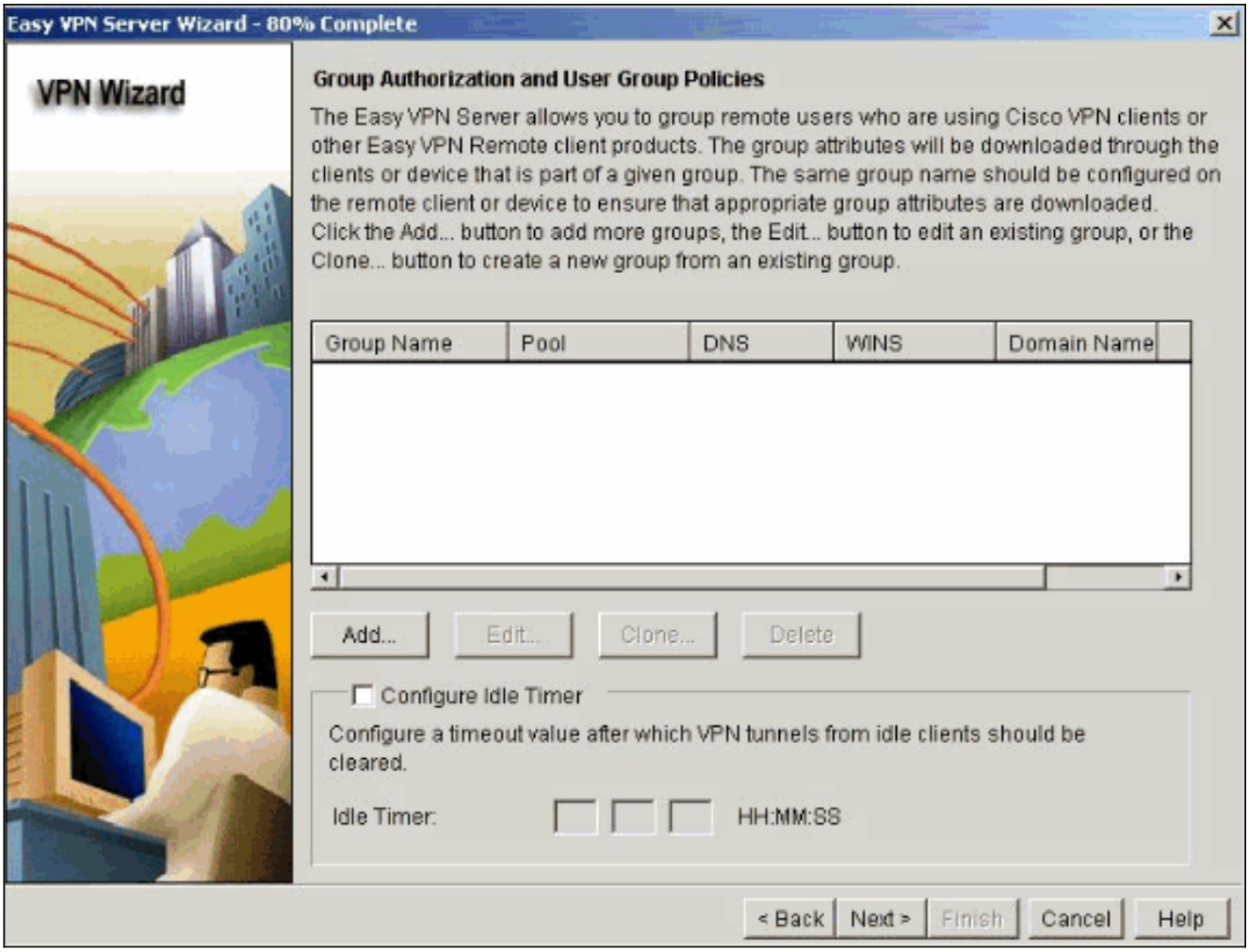
7. Next をクリックして、グループ ポリシー検索用の新しい Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）認可ネットワーク方式リストを作成するか、グループ認可に使用する既存のネットワーク方式リストを選択します。



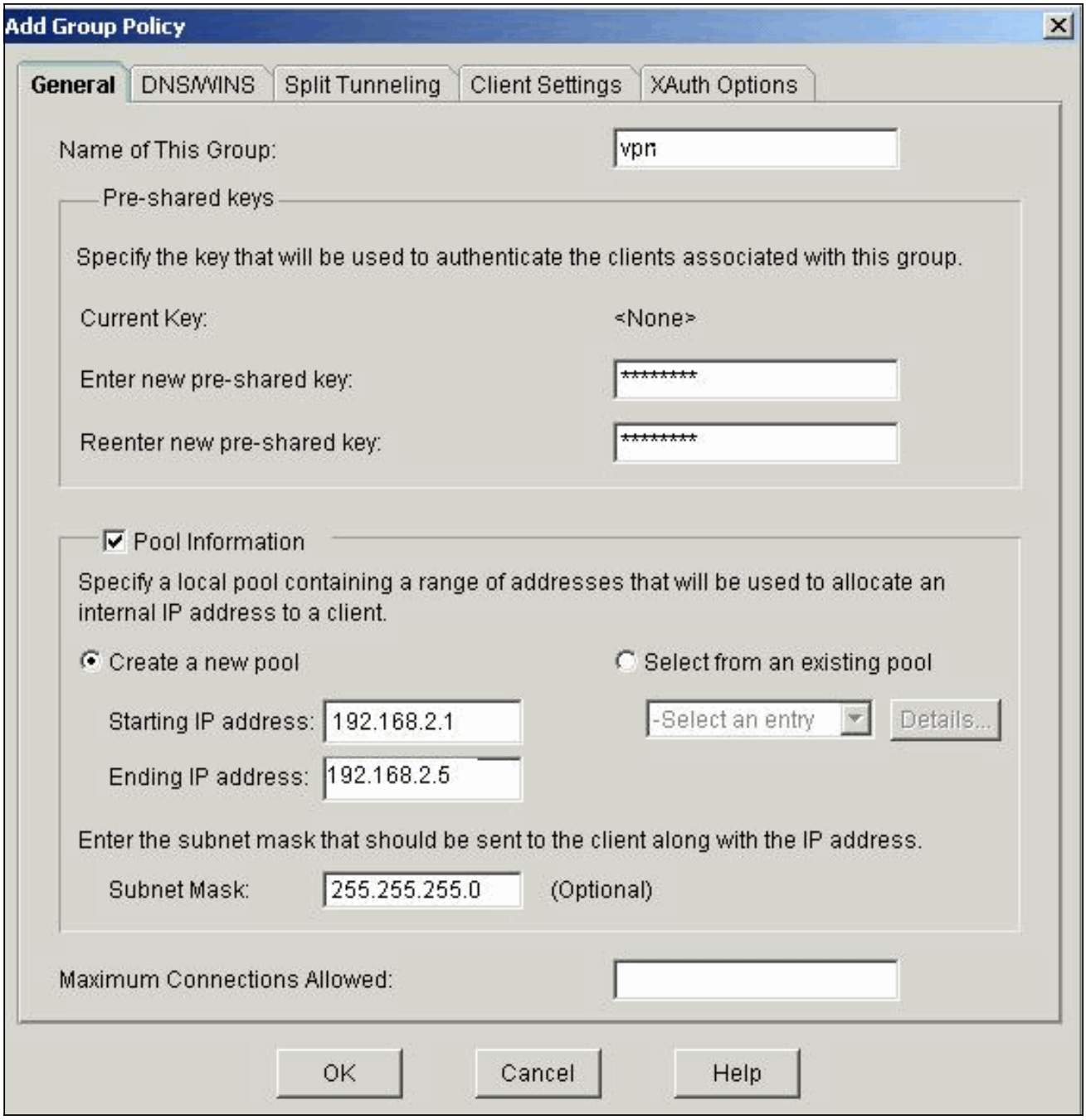
8. Easy VPN サーバでユーザ認証を設定します。ユーザ認証の詳細情報は、RADIUS サーバなどの外部サーバかローカル データベース、またはその両方に格納できます。 AAA ログイン認証方式リストは、ユーザ認証の詳細情報を検索する順序を決定するために使用されます。



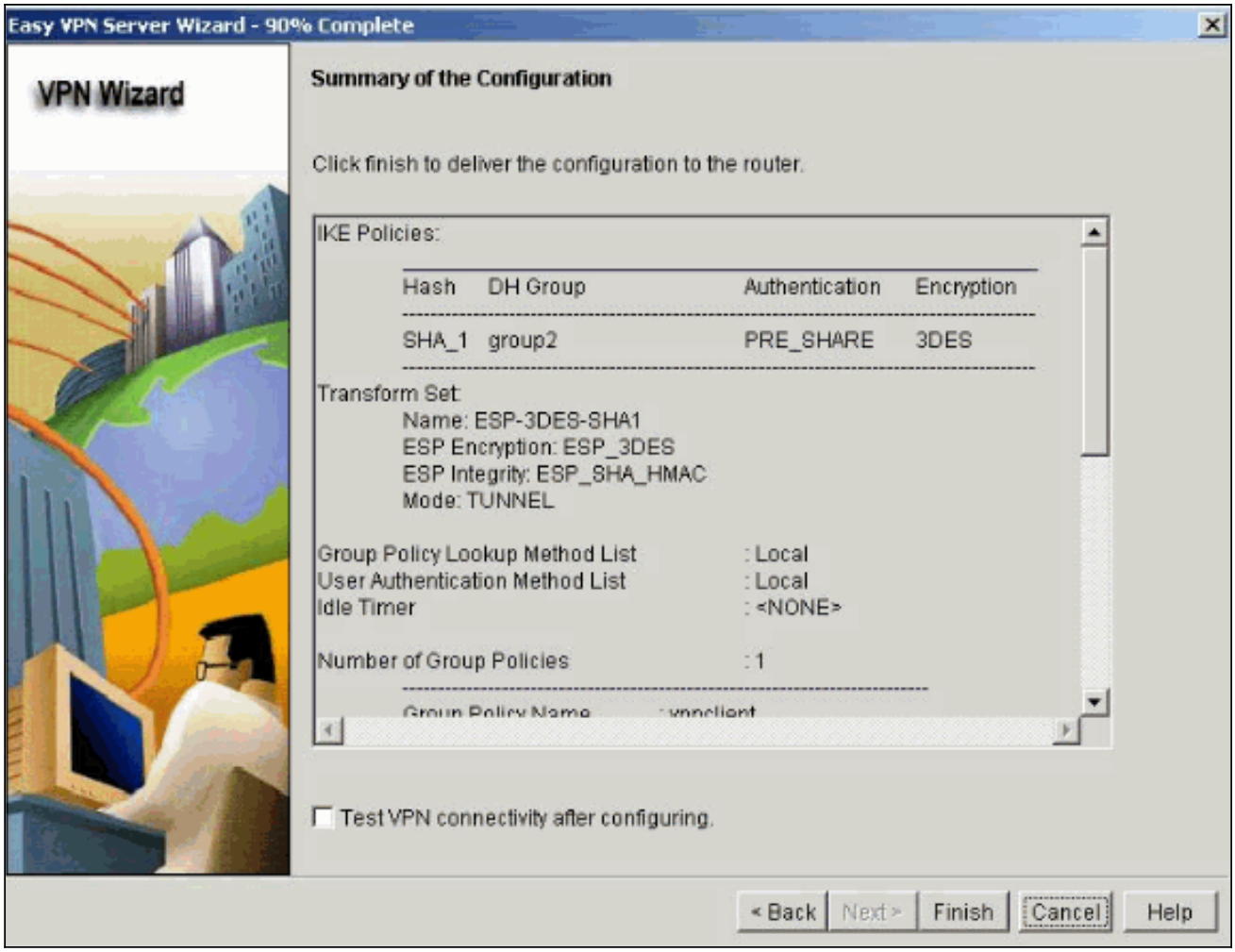
9. このウィンドウを使用すると、ローカル データベース上でユーザ グループ ポリシーを追加、編集、複製、または削除できます。



10. Tunnel Group Name の名前を入力します。 認証情報に使用される事前共有キーを入力します。VPN Client への IP アドレスの割り当てに使用される、新しいプールを作成するか、既存のプールを選択します。

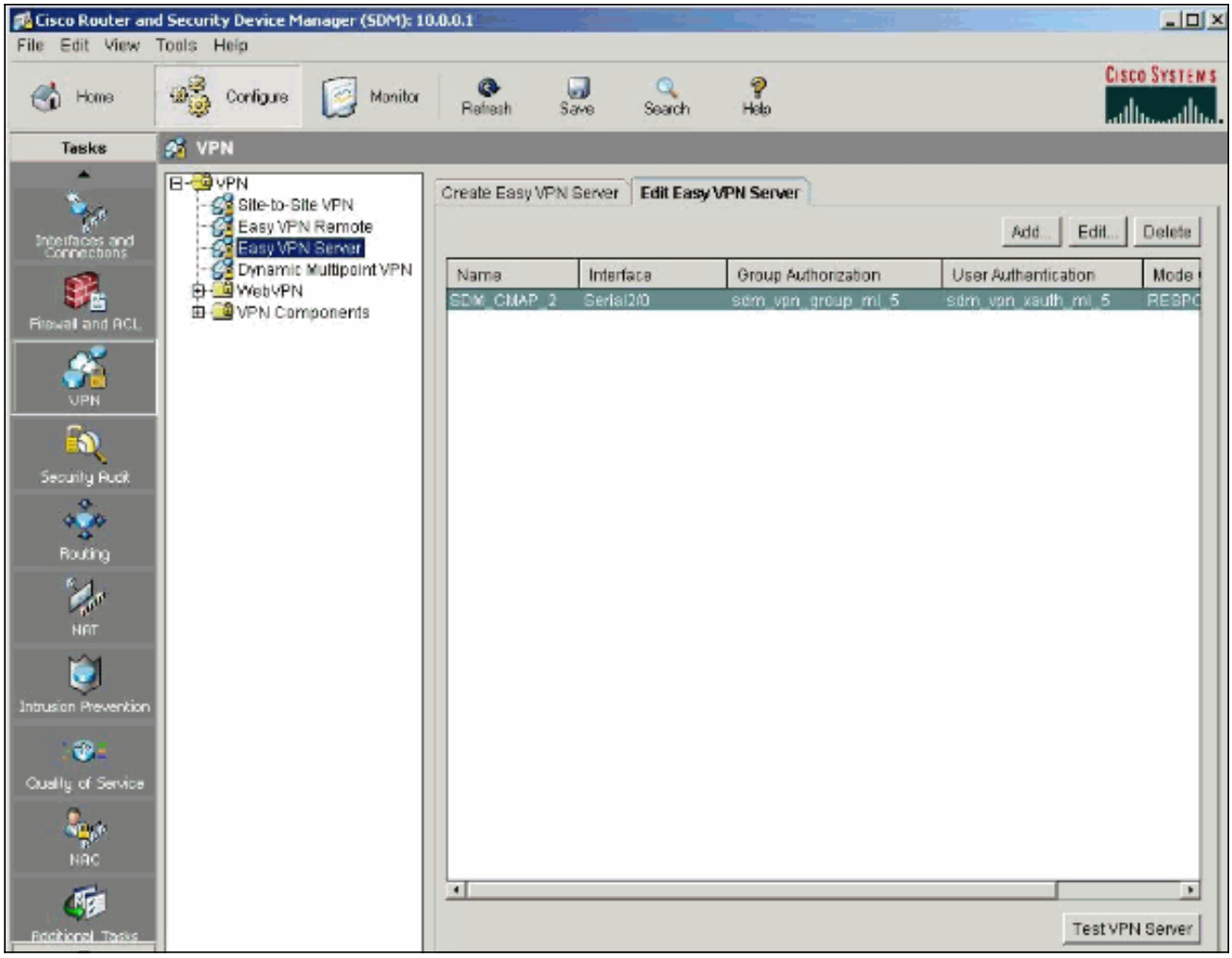


11. このウィンドウにはユーザが行った操作の概要が表示されます。 設定に問題がなければ、[Finish] をクリックします。



12. SDM は設定をルータに送信し、Running Configuration が更新されます。 [OK] をクリックして完了します。

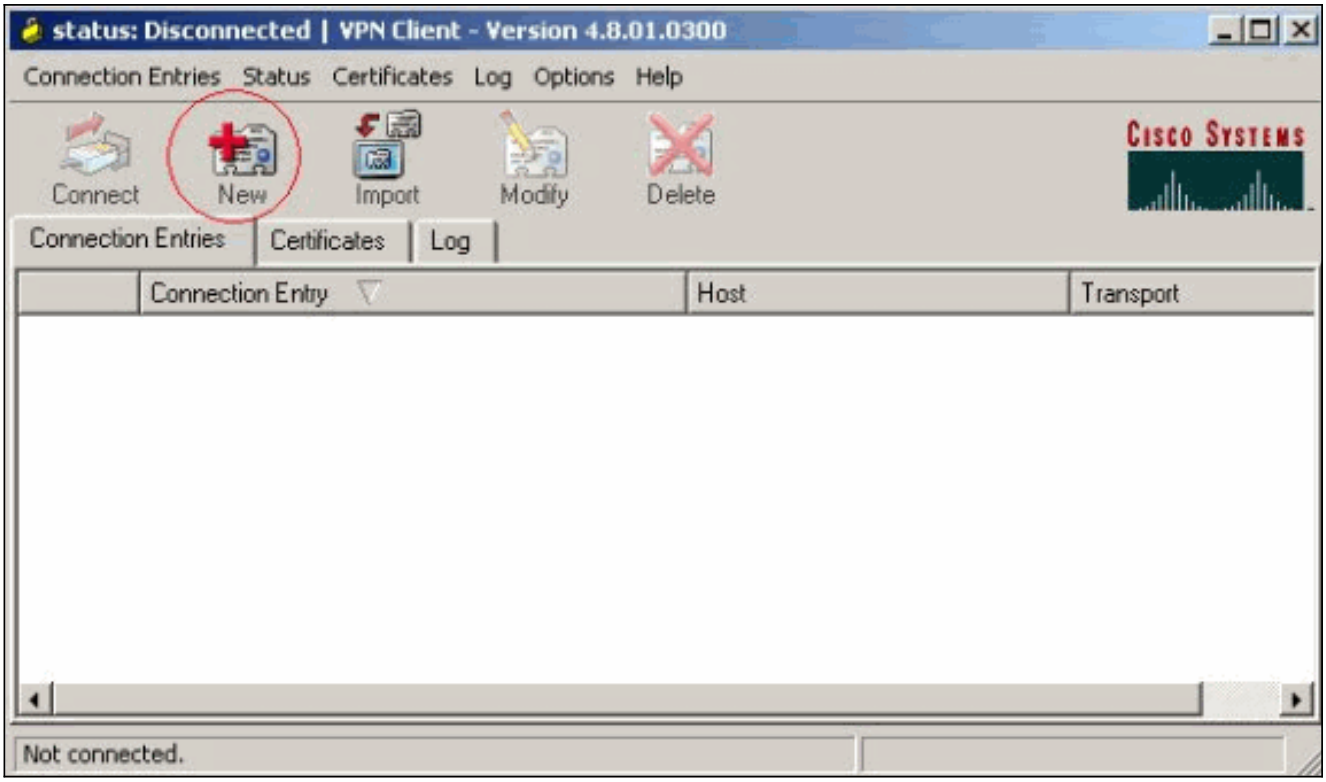
13. 完了後、必要に応じて設定内の変更を編集および修正できます。



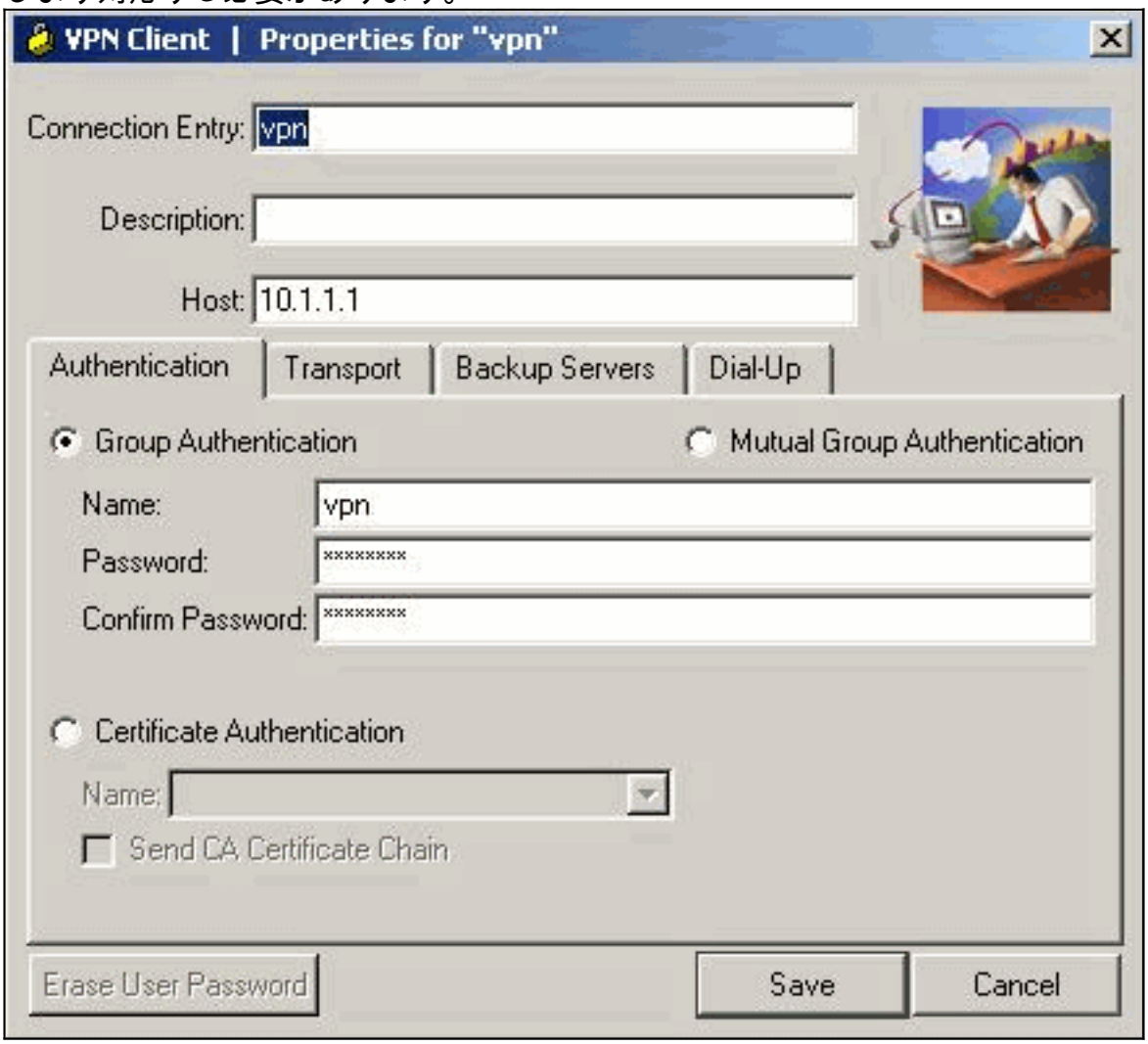
確認

Cisco ルータの設定に成功したことを確認するには、Cisco VPN Client を使用して Cisco ルータに接続してみます。

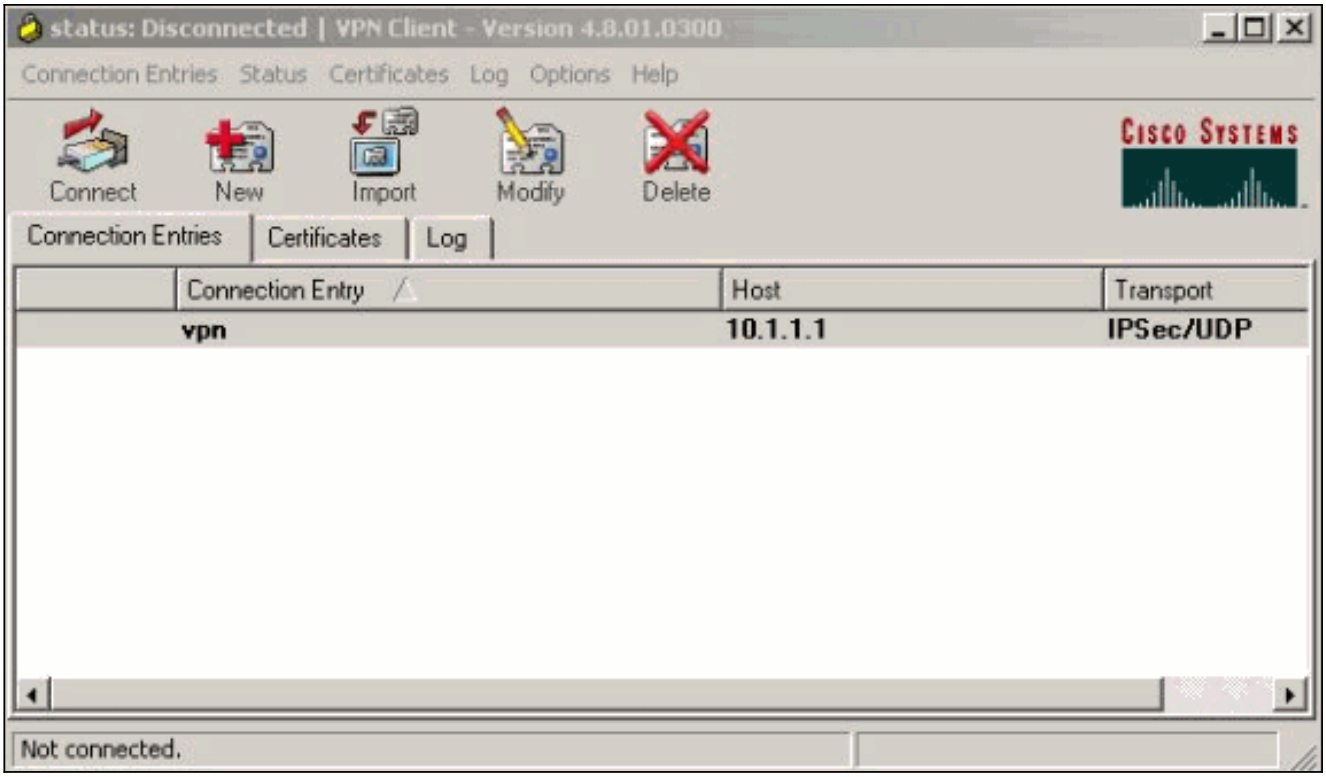
1. **Connection Entries > New** の順に選択します。



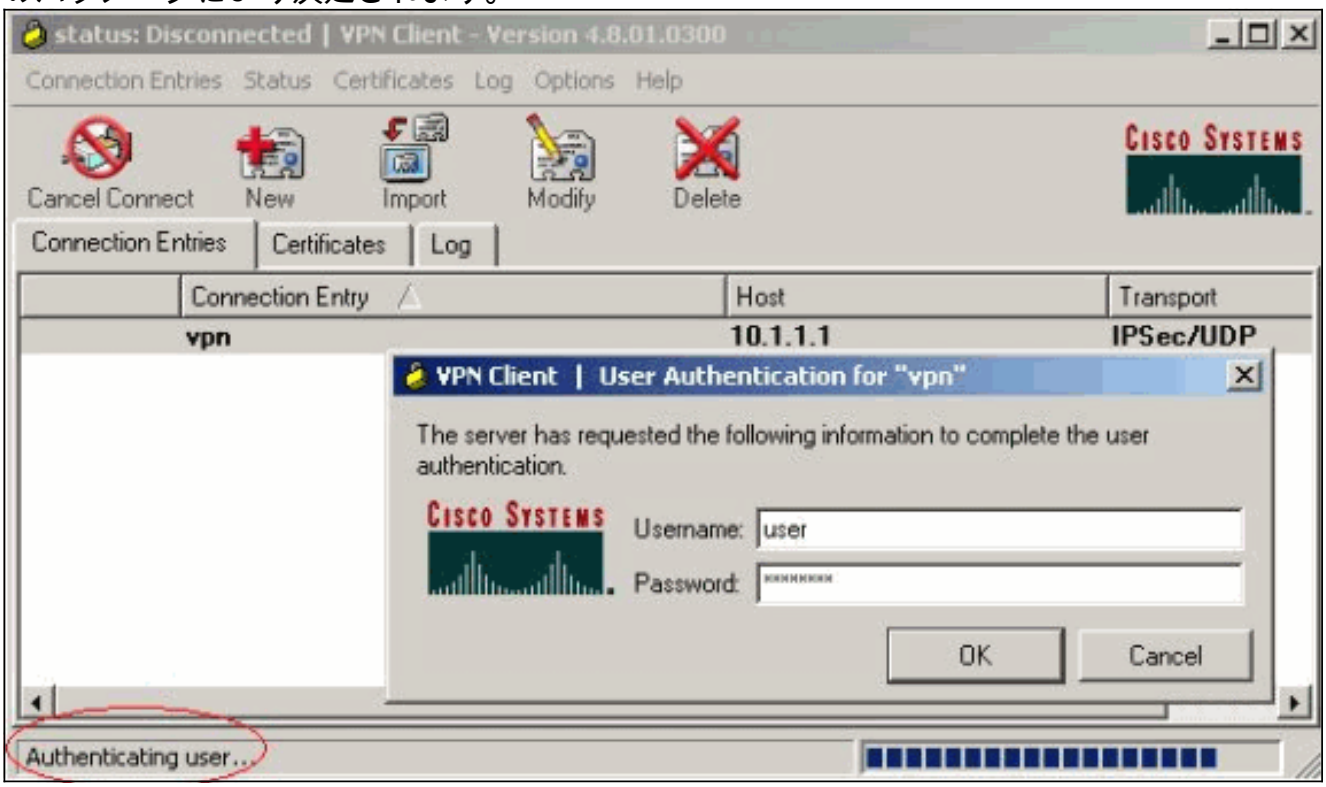
2. 新しい接続の詳細情報を入力します。Host フィールドには、Easy VPN サーバ（Cisco ルータ）のトンネル エンド ポイントの IP アドレスまたはホスト名が含まれている必要があります。 グループ 認証情報はステップ 9.で使用されるそれに終了したら『SAVE』 をクリックします対応する必要があります。



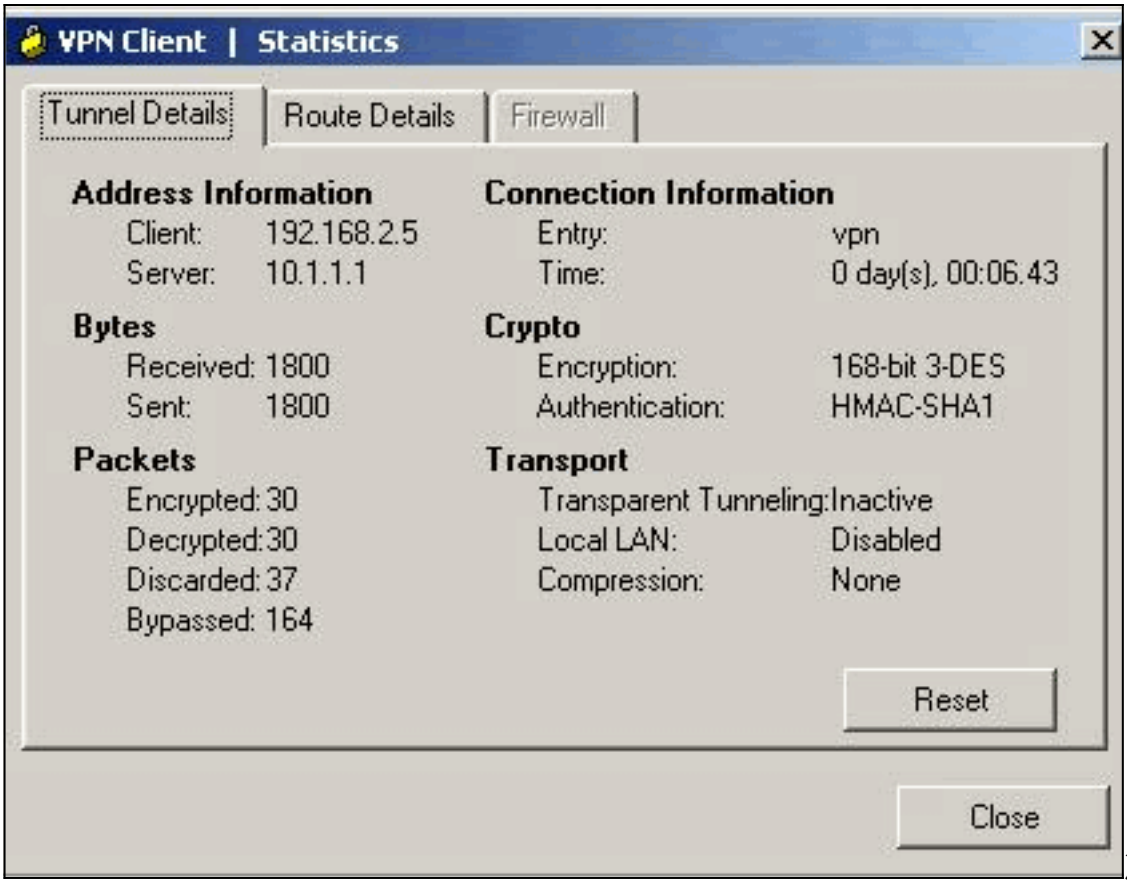
3. 新しく作成した接続を選択し、Connect をクリックします。



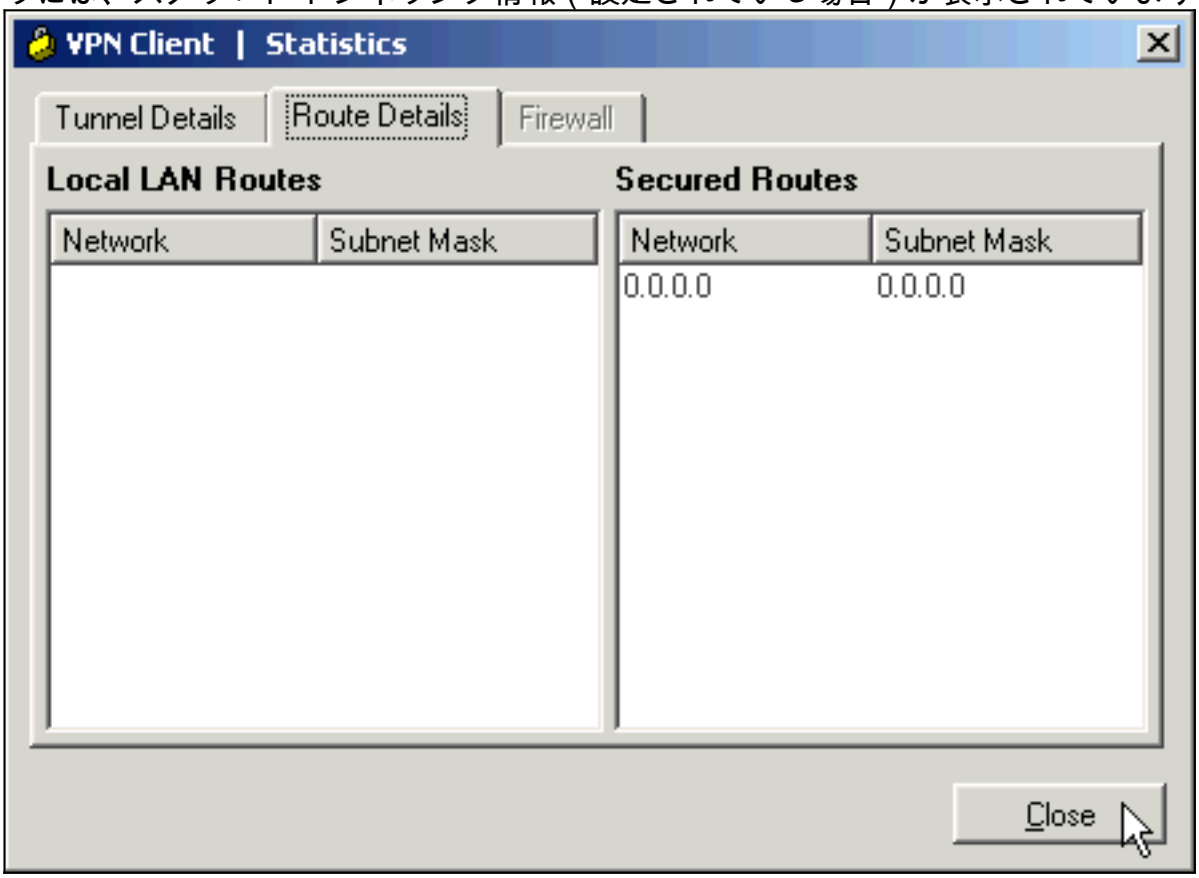
4. 拡張認証（Xauth）用のユーザ名とパスワードを入力します。 この情報は、手順 7 の Xauth のパラメータにより決定されます。



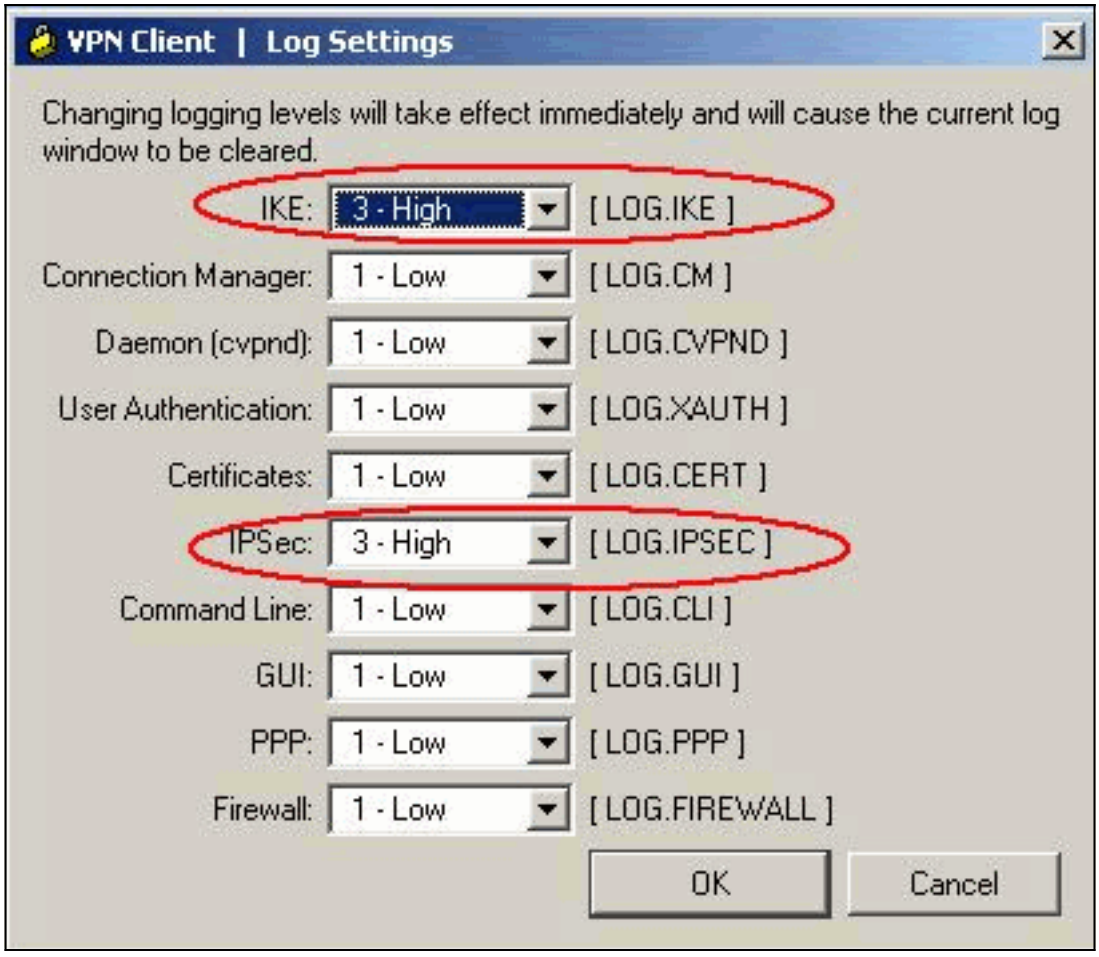
5. 接続が正常に確立されたら、Status メニューから **Statistics** を選択し、トンネルの詳細情報を確認します。次のウィンドウには、トラフィックと暗号の情報が表示されています。



次のウィンドウには、スプリット トンネリング情報 (設定されている場合) が表示されています。

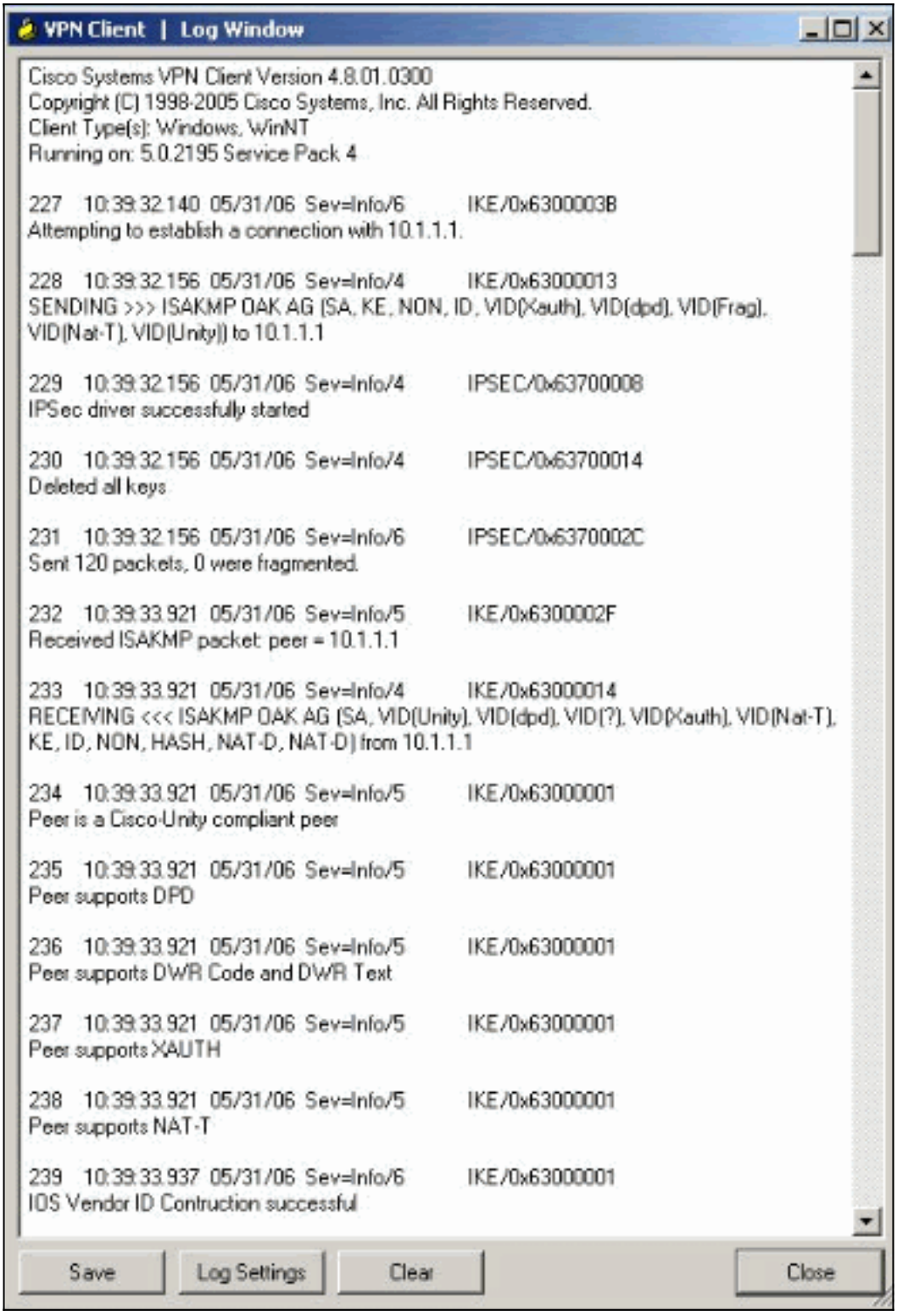


6. Cisco VPN Client のログ レベルを有効にするために Log > Log Settings の順に選択 して下



さい。

7. Cisco VPN Client の Log エントリを表示するために Log > Log Windows の順に選択 して下



さい。

関連情報

- Cisco ルータと Security Device Manager のダウンロードとインストール
- Cisco VPN Client に関するサポート ページ
- IPSec ネゴシエーション/IKE プロトコル
- テクニカルサポートとドキュメント - Cisco Systems