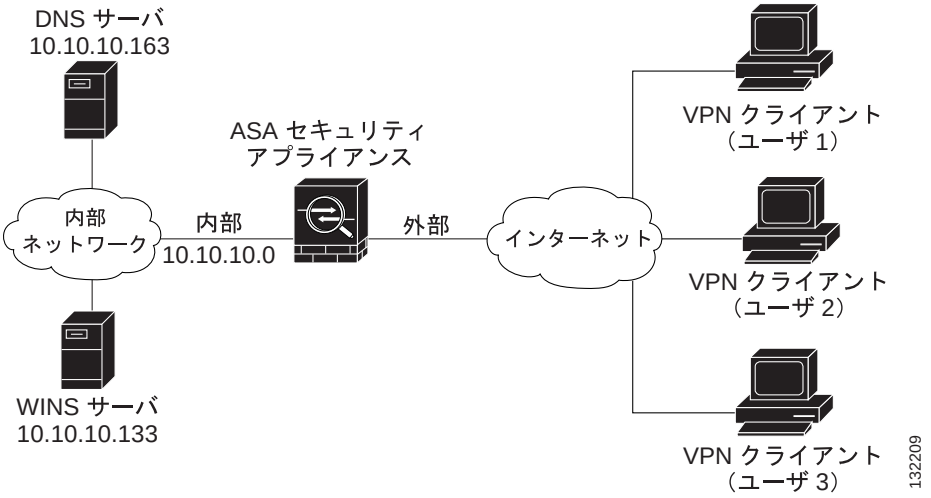
シナリオ：リモートアクセス VPN の設定

リモートアクセス バーチャル プライベート ネットワーク（VPN）によって、オフサイト ユーザにセキュアなアクセスを提供できます。ASDM を使用して、インターネットを経由するセキュアな接続（トンネル）を作成するように、適応型セキュリティ アプライアンスを設定できます。

図 7-1 で、インターネット経由で VPN クライアントからの要求を受け付け、セキュアな接続を確立するように設定された、適応型セキュリティ アプライアンスを示します。

図 7-1　リモート アクセス VPN のシナリオのネットワーク レイアウト



リモートアクセスのシナリオの実装

次の項で、図 7-1 で示したリモートアクセスのシナリオのパラメータ例を使用して、リモートアクセス配置で適応型セキュリティ アプライアンスを設定する方法を示します。

必要な情報

- IP プールに使用する IP アドレスの範囲
- ローカル認証データベースの作成に使用するユーザのリスト（認証に AAA サーバを使用する場合を除く）
- リモート クライアントで使用するネットワーキング情報
  - プライマリおよびセカンダリ DNS サーバの IP アドレス
  - プライマリおよびセカンダリ WINS サーバの IP アドレス
  - デフォルト ドメイン名
  - 認証されたリモート　クライアントにアクセスできるようにするローカル ホスト、グループ、およびネットワークの IP アドレスのリスト

リモートアクセス VPN の設定

ASDM VPN Wizard を使用すると、単純な一連の手順で、適応型セキュリティ アプライアンスをリモートアクセス VPN ヘッドエンド デバイスとして設定できます。

1. リモートアクセス VPN 用の適応型セキュリティ アプライアンスの設定
2. VPN クライアントの選択
3. VPN トンネル グループ名と認証方式の指定
4. ユーザ認証方式の指定
5. ユーザ アカウントの設定（オプション）
6. アドレス プールの設定
7. クライアント アトリビュートの設定
8. IKE ポリシーの設定
9. IPSec 暗号化および認証パラメータの設定

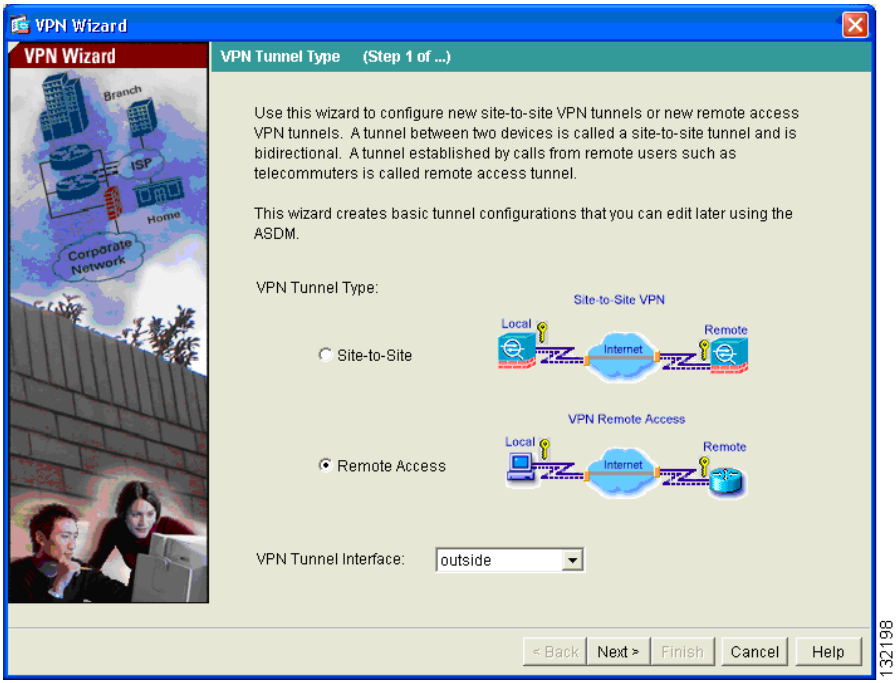
10. アドレス変換の例外とスプリット トンネリングの指定
11. リモートアクセス VPN の設定の確認

リモートアクセス VPN 用の適応型セキュリティ アプライアンスの設定

リモートアクセス VPN の設定プロセスを開始するには、次の手順を実行します。

ステップ 1　Web ブラウザのアドレス フィールドに、工場出荷時のデフォルト IP アドレス **https://192.168.1.1/admin/** を入力して、ASDM を起動します。

ステップ 2　ASDM のメイン ウィンドウの Wizards ドロップダウン リストで、**VPN Wizard** オプションをクリックします。VPN Wizard の Step 1 ウィンドウが表示されます。



ステップ 3　VPN Wizard の Step 1 で、次の手順を実行します。

a. **Remote Access VPN** オプションをクリックします。

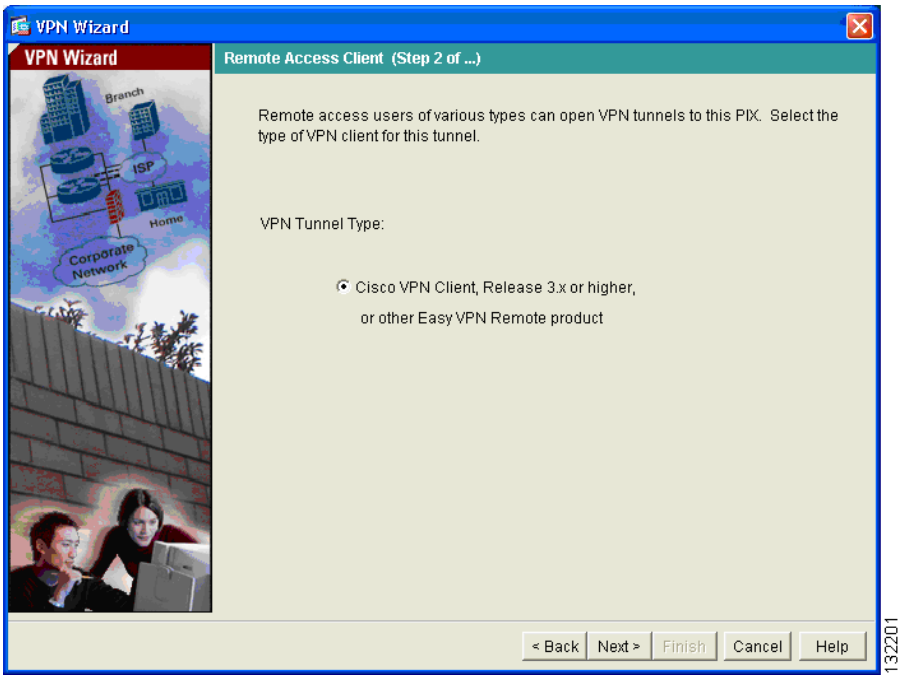
b. ドロップダウン リストで、着信 VPN トンネルに対してイネーブルにするインターフェイスとして **outside** をクリックします。

c. **Next** をクリックして続行します。

VPN クライアントの選択

VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　Cisco VPN クライアント、またはその他の Easy VPN リモート製品を使用して、リモート アクセス ユーザが適応型セキュリティ アプライアンスに接続できるように、オプション ボタンをクリックします。



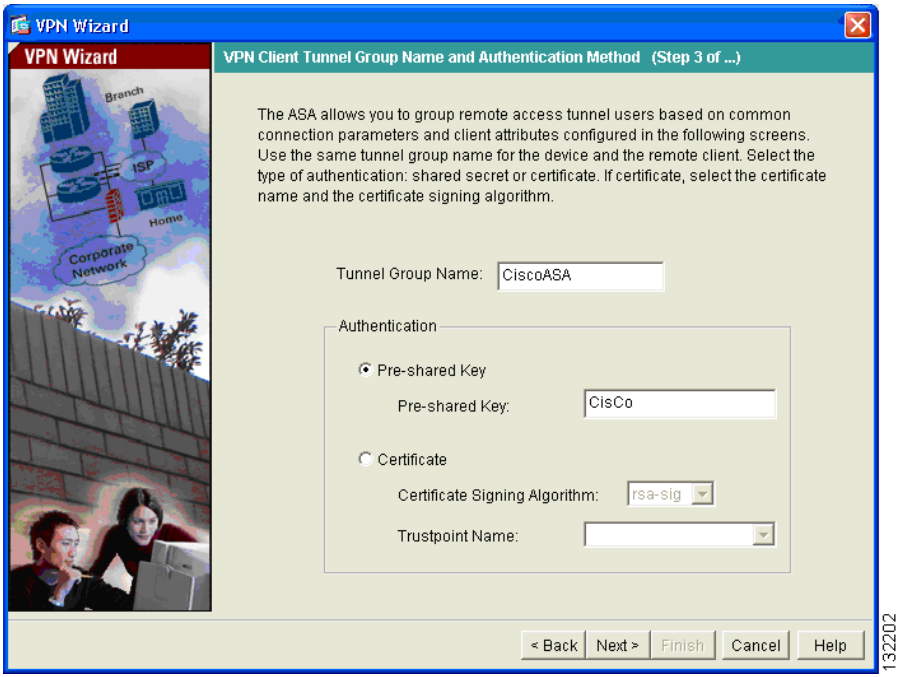
（注）　この画面には現在、選択肢が 1 つだけ表示されていますが、その他のトンネル タイプが使用可能になったときに簡単にイネーブルにできるようにセットアップされています。

ステップ 2　**Next** をクリックして続行します。

VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　共通の接続パラメータとクライアント アトリビュートを使用するユーザのセットに対して、トンネル グループ名（「CiscoASA」など）を入力します。



ステップ 2　次の手順のいずれかを実行して、使用する認証の種類を指定します。

- 認証にスタティックな事前共有キーを使用するには、**Pre-Shared Key** をクリックし、キー（「CisCo」など）を入力します。
- 認証にデジタル証明書を使用するには、**Certificate** をクリックし、Certificate Signing Algorithm ドロップダウン リストで rsa-sig または dsa-sig をクリックし、次のドロップダウン リストで事前設定されたトラストポイント名をクリックします。

ステップ 3　**Next** をクリックして続行します。

ユーザ認証方式の指定

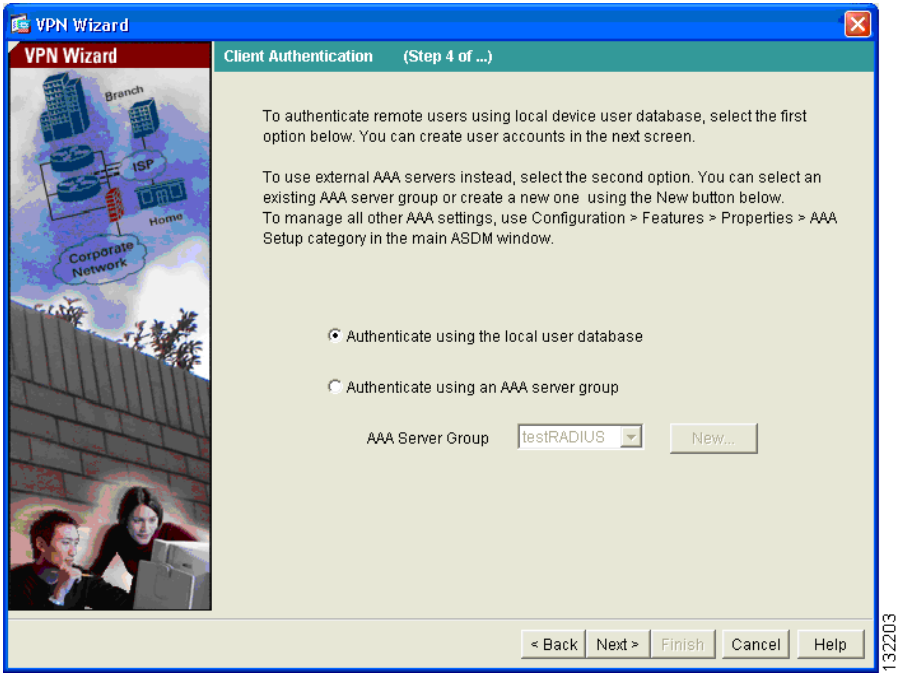
ユーザは、ローカル認証データベース、または外部認証、認可、アカウンティング（AAA）サーバ（RADIUS、TACACS+、SDI、NT、および Crabbers）で認証できます。

VPN Wizard の Step 4 で、次の手順を実行します。

ステップ 1　適切なオプション ボタンをクリックして、使用するユーザ認証の種類を指定します。

- ローカル認証データベース
- 外部 AAA サーバ グループ

ステップ 2　ドロップダウン リストで、事前設定済みのサーバ グループをクリックします。または、**New** をクリックして、新しいサーバ グループを追加します。

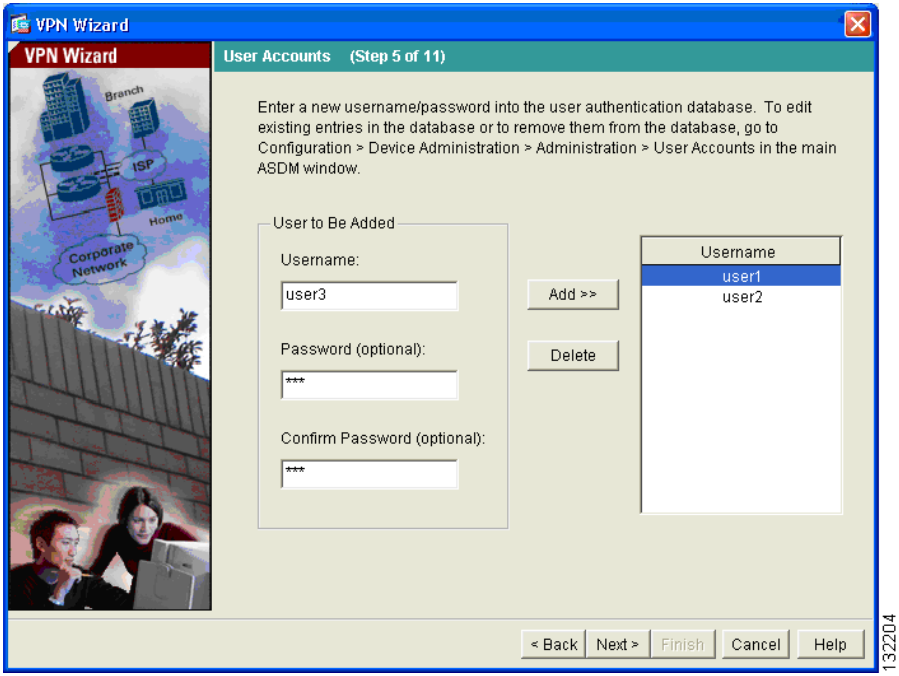


ステップ 3　**Next** をクリックして続行します。

ユーザ アカウントの設定（オプション）

ローカル ユーザ データベースでユーザを認証する場合は、新しいユーザ アカウントを作成します。VPN Wizard の Step 5 で、次の手順を実行します。

ステップ 1　新しいユーザを追加するには、ユーザ名とパスワードを入力し、**Add** をクリックします。



ステップ 2　新しいユーザの追加が終了したら、**Next** をクリックして続行します。

アドレス プールの設定

リモート クライアントがネットワークにアクセスできるようにするには、正常に接続したときにリモート VPN クライアントに割り当てることができる IP アドレスのプールを設定する必要があります。このシナリオでは、IP アドレス 209.165.201.1 ～ 209.166.201.20 を使用するようにプールを設定します。

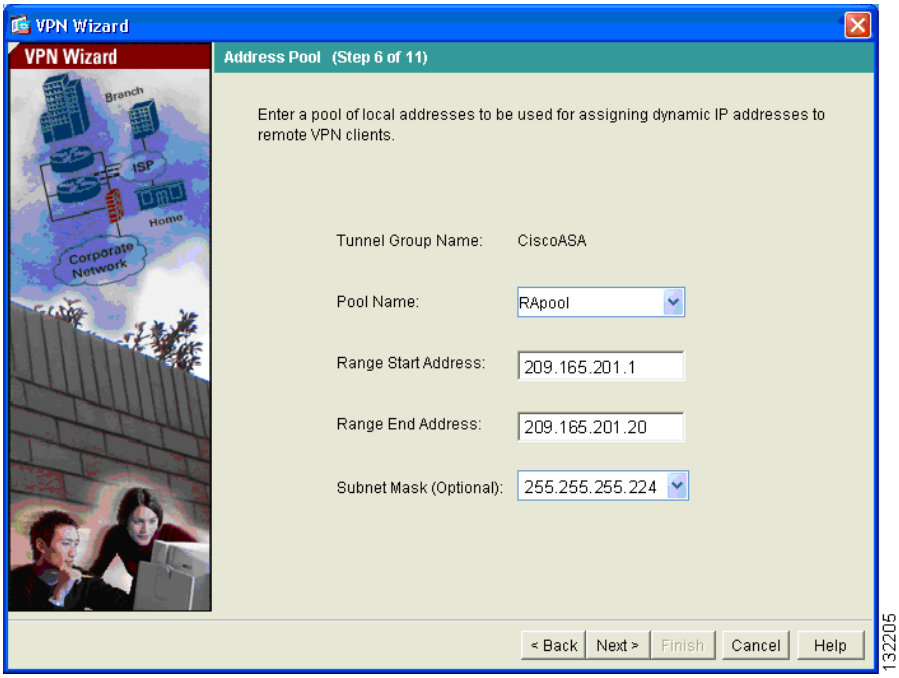
VPN Wizard の Step 6 で、次の手順を実行します。

ステップ 1　ドロップダウン リストで、プール名を入力するか、事前設定済みのプールをクリックします。

ステップ 2　プールで使用する IP アドレスの範囲の開始値を入力します。

ステップ 3　プールで使用する IP アドレスの範囲の終了値を入力します。

ステップ 4　ドロップダウン リストで、サブネット マスクを入力するか、事前設定済みの値をクリックします。



ステップ 5　**Next** をクリックして続行します。

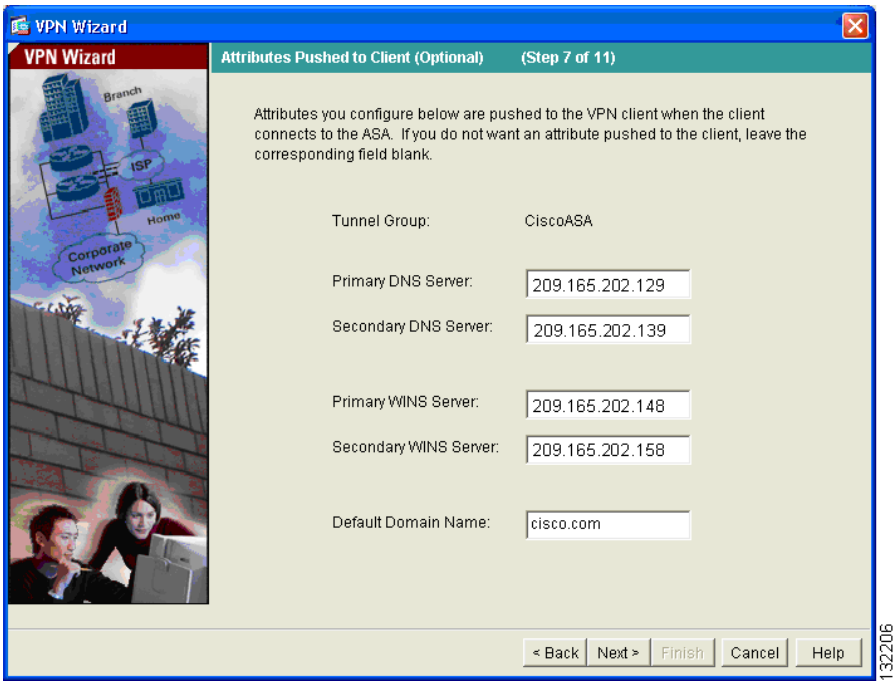
クライアント アトリビュートの設定

ネットワークにアクセスするには、各リモート アクセス クライアントに基本ネットワーク設定情報（使用する DNS サーバおよび WINS サーバ、デフォルト ドメイン名など）が必要です。各リモート クライアントを個別に設定する代わりに、ASDM にクライアント情報を入力できます。適応型セキュリティ アプライアンスは、接続が確立されたときに、この情報をリモート クライアントにプッシュします。

正しい値を指定したことを確認してください。値が正しくない場合、リモート クライアントは、DNS 名を使用した解決や Windows ネットワーキングの使用ができなくなります。

VPN Wizard の Step 7 で、次の手順を実行します。

ステップ 1　リモート クライアントで使用するネットワーク設定情報を入力します。



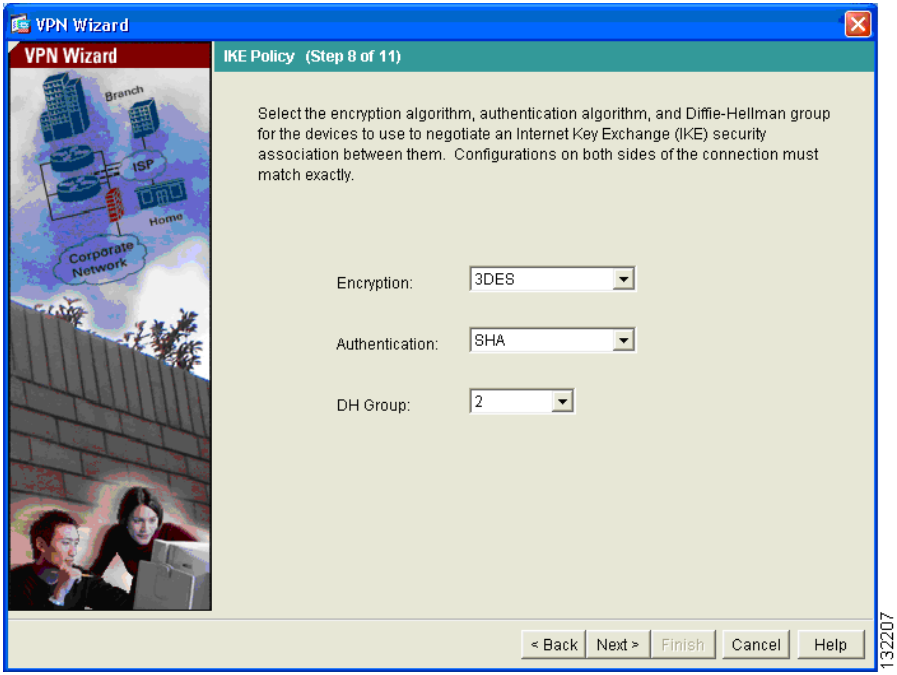
ステップ 2　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、暗号化方式を含むネゴシエーション プロトコルで、データを保護し、機密性を保証します。また、ピアのアイデンティティも保証する認証方式でもあります。ほとんどの場合、ASDM のデフォルト値で、セキュアな VPN トンネルを確立できます。

IKE ポリシーを指定するには、次の手順を実行します。

ステップ 1　IKE セキュリティ アソシエーションで、適応型セキュリティ アプライアンスが使用する暗号化アルゴリズム（DES、3DES、または AES）、認証アルゴリズム（MD5 または SHA）、および Diffie-Helman グループ（1、2、5、または 7）をクリックします。

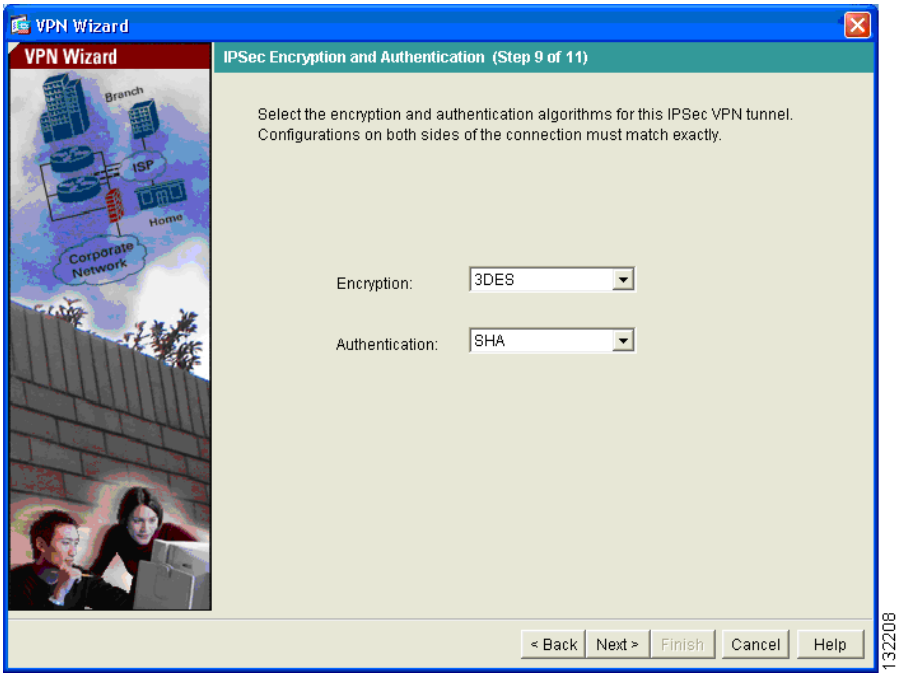


ステップ 2　**Next** をクリックして続行します。

IPSec 暗号化および認証パラメータの設定

VPN Wizard の Step 9 で、次の手順を実行します。

ステップ 1　暗号化アルゴリズム（DES、3DES、または AES）および認証アルゴリズム（MD5 または SHA）をクリックします。



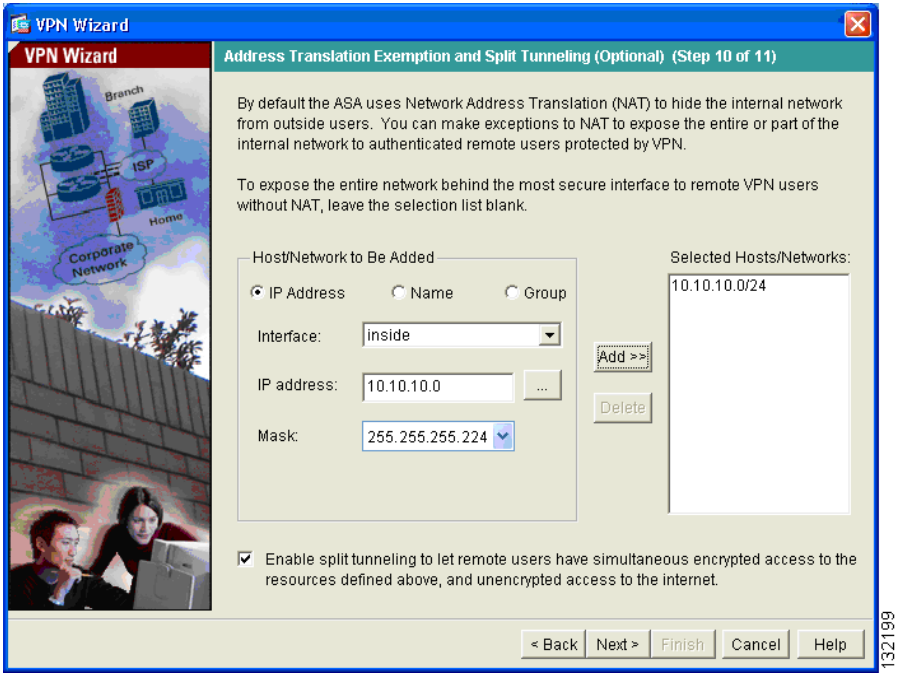
ステップ 2　**Next** をクリックして続行します。

アドレス変換の例外とスプリット トンネリングの指定

適応型セキュリティ アプライアンスは、ネットワーク アドレス変換（NAT）を使用して、内部 IP アドレスが外部に公開されることを防いでいます。認証されたリモート ユーザに公開する必要があるローカル ホストおよびネットワークを指定して、このネットワーク保護の例外を作成できます。公開するリソースは、ホストまたはネットワークの IP アドレス、名前、またはグループで指定します（このシナリオでは、内部ネットワーク 10.10.10.0 全体をすべてのリモート クライアントに公開します）。

VPN Wizard の Step 10 で、次の手順を実行します。

ステップ 1　認証されたリモート ユーザがアクセスできるようにする内部リソースのリストに含めるホスト、グループ、およびネットワークを指定します。Selected パネルのホスト、グループ、およびネットワークを動的に追加または削除するには、それぞれ、**Add** または **Delete** をクリックします。

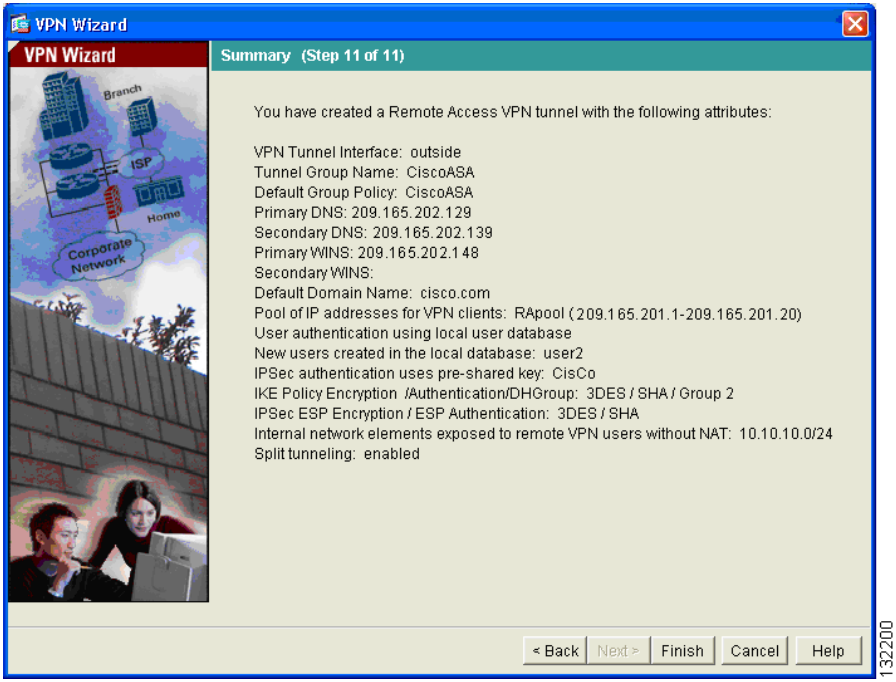


（注） 画面の下部のオプション ボタンをクリックして、スプリット トンネリングをイネーブルにします。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックを、暗号化された VPN トンネルを使用せずに直接インターネットに送出できるようになります。

ステップ 2　リモート クライアントに公開するリソースの指定が終了したら、**Next** をクリックして続行します。

リモートアクセス VPN の設定の確認

ここで作成した VPN トンネルの設定アトリビュートを確認します。表示される設定は、次のようになります。



設定が正しいことを確認したら、**Finish** をクリックしてウィザードを完了し、設定の変更を適応型セキュリティ アプライアンスに適用します。

次の手順

リモートアクセス VPN 環境に適応型セキュリティ アプライアンスを配置するだけの場合は、これで初期設定は終わりです。このほかに、次の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に、適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
DMZ 内の Web サーバを保護する適応型セキュリティ アプライアンスの設定	第 6 章「シナリオ：DMZ の設定」
サイトツーサイト VPN の設定	第 8 章「シナリオ：サイトツーサイト VPN の設定」