CHAPTER 9

シナリオ：IPSec リモートアクセス VPN の設定

この章では、適応型セキュリティ アプライアンスを使用して、リモートアクセス IPsec VPN 接続を受け付ける方法について説明します。リモートアクセス VPN を使用すると、インターネットを経由するセキュアな接続（トンネル）を作成できるため、セキュアなアクセスをオフサイト ユーザに提供できます。このタイプの VPN 設定では、リモート ユーザは Cisco VPN クライアントを実行して適応型セキュリティ アプライアンスに接続する必要があります。

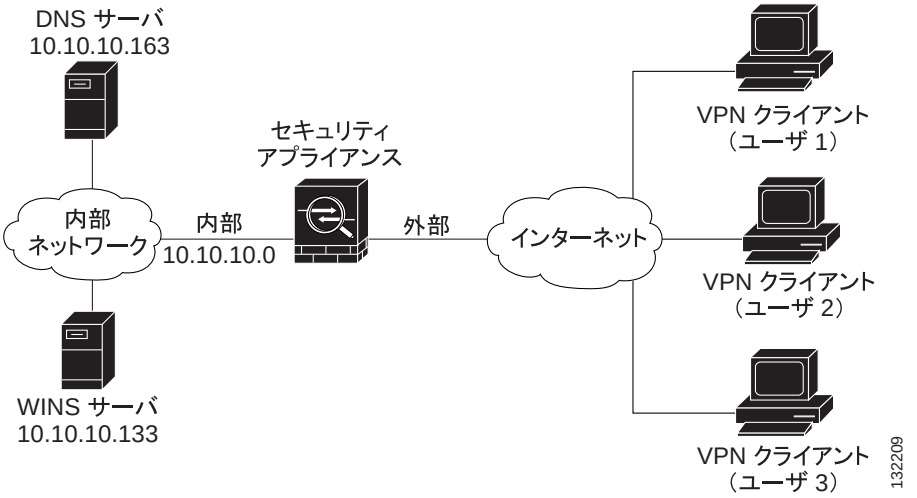
この章では、Easy VPN ソリューションを実装する場合に Easy VPN サーバ（ヘッドエンド デバイスと呼ばれることもあります）を設定する方法について説明します。

この章は、次の項で構成されています。

IPsec リモートアクセス VPN ネットワーク トポロジの例

図 9-1 は、インターネット経由で VPN クライアント（Cisco Easy VPN ソフトウェアまたはハードウェア クライアントなど）からの要求を受け付け、それらのクライアントとの IPsec 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ています。

図 9-1　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



IPsec リモートアクセス VPN シナリオの実装

この章では、適応型セキュリティ アプライアンスを設定して、リモート クライアントおよびリモート デバイスから IPsec VPN 接続を受け付ける方法について説明します。この項では、Easy VPN ソリューションを実装する場合に Easy VPN サーバ（ヘッドエンド デバイスと呼ばれることもあります）を設定する方法について説明します。

設定値の例は、図 9-1 で示すリモートアクセスのシナリオから取得されます。

この項では、次のトピックについて取り上げます。

必要な情報

適応型セキュリティ アプライアンスの設定を開始してリモートアクセス IPsec VPN 接続を受け付けるには、事前に必ず次の情報を準備します。

- IP プールで使用される IP アドレスの範囲。これらのアドレスは、接続が成功するとリモート VPN クライアントに割り当てられます。
- ローカル認証データベースの作成に使用されるユーザのリスト（認証に AAA サーバを使用する場合を除く）。

- VPN への接続時にリモート クライアントで使用されるネットワーキング情報。次の情報が含まれます。
  - 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

ASDM の起動

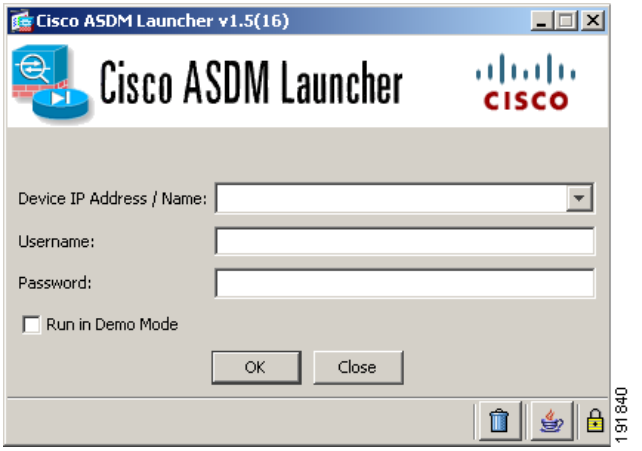
この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 の「Web ブラウザを使用した ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ 1　デスクトップから、Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。



ステップ 2　適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 3　Username および Password フィールドはブランクのままにします。

（注）　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

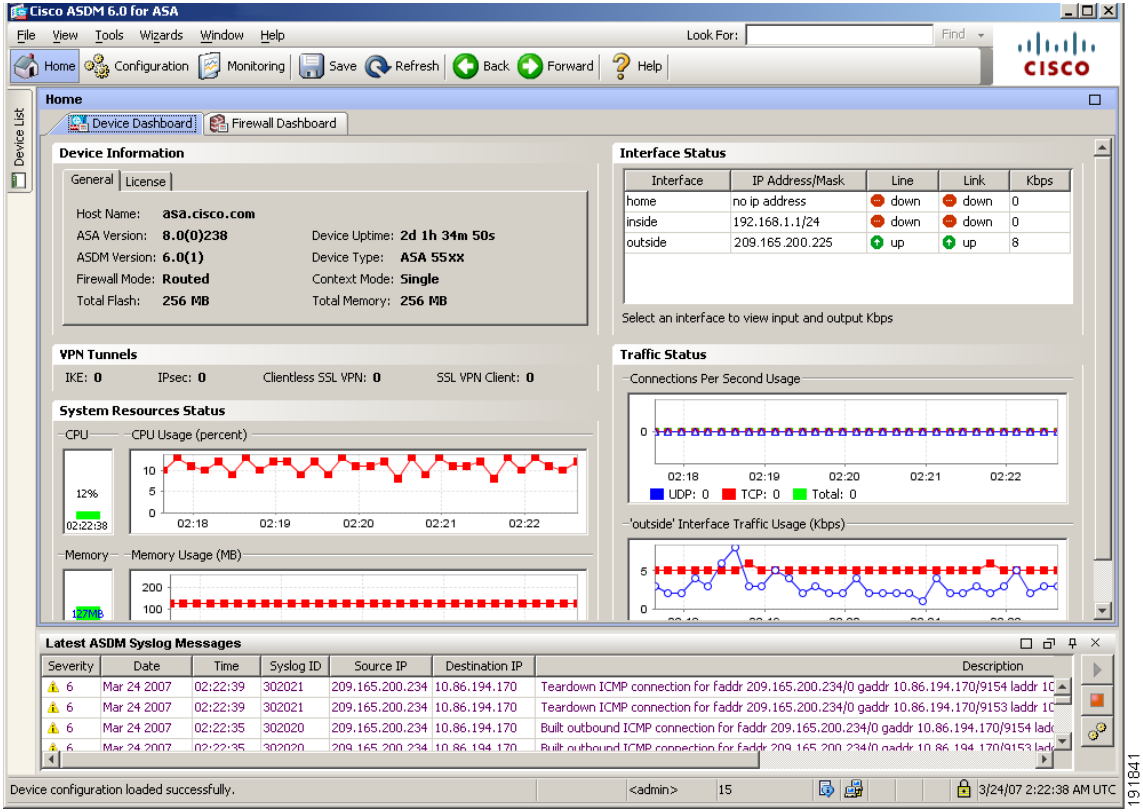
ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes** をクリックします。

適応型セキュリティ アプライアンスは更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

ASDM のメイン ウィンドウが表示されます。

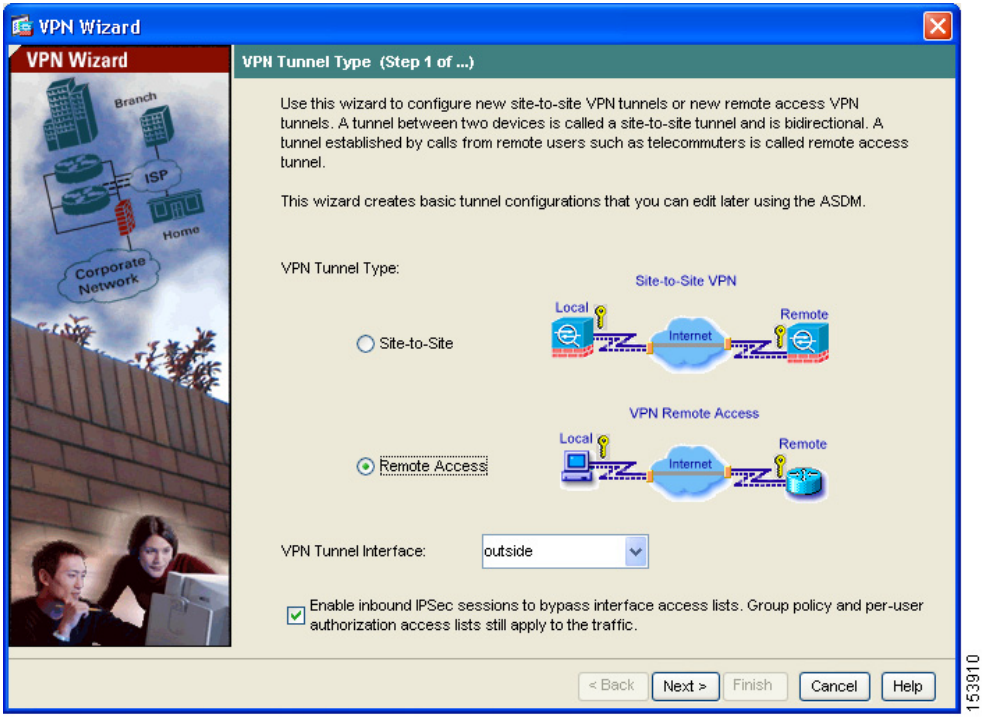
IPsec リモートアクセス VPN シナリオの実装



IPsec リモートアクセス VPN の設定

リモートアクセス VPN を設定するには、次の手順を実行します。

ステップ 1　ASDM のメイン ウィンドウの Wizards ドロップダウン メニューで、**Ipsec VPN Wizard** を選択します。VPN Wizard の Step 1 画面が表示されます。



ステップ 2　VPN Wizard の Step 1 で、次の手順を実行します。

a. **Remote Access** オプション ボタ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** を選択します。

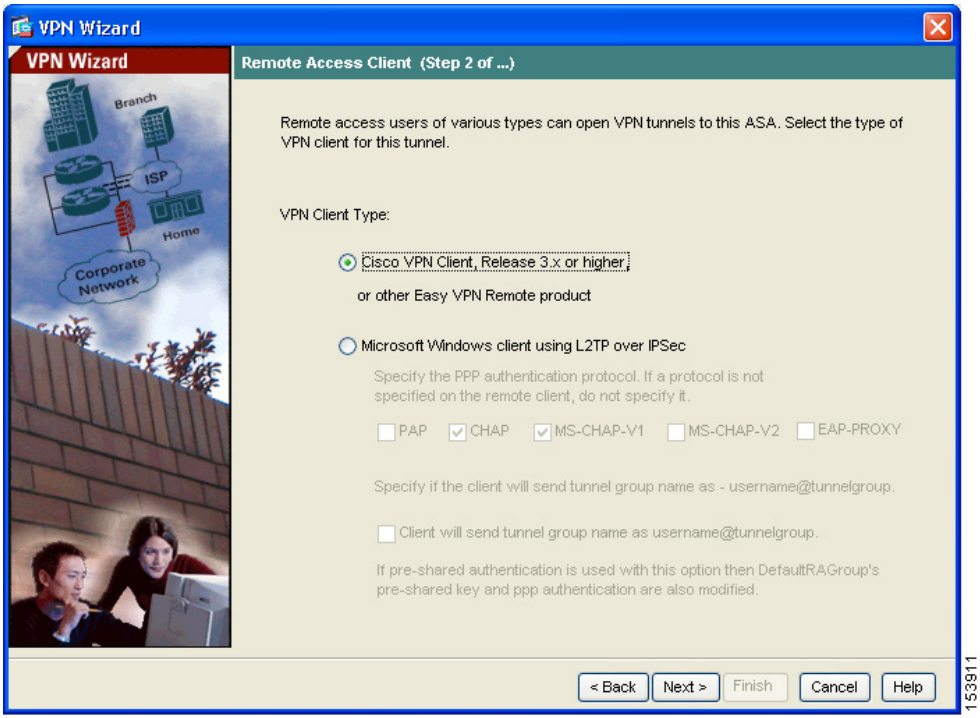
c. **Next** をクリックして続行します。

VPN クライアント タイプの選択

VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　この適応型セキュリティ アプライアンスにリモート ユーザが接続できる VPN クライアントのタイプを指定します。このシナリオでは、**Cisco VPN Client** オプション ボタンをクリックします。

その他の Cisco Easy VPN リモート製品もすべて使用することができます。



ステップ 2　**Next** をクリックして続行します。

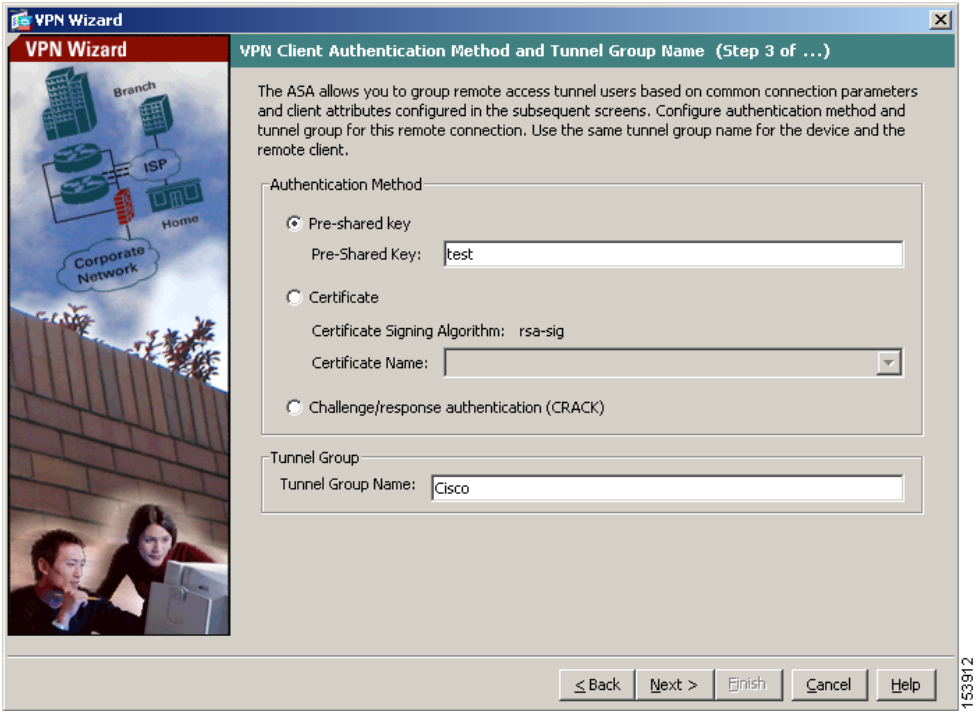
VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　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** オプション ボタンをクリックし、事前共有キー（「Cisco」など）を入力します。このキーは、IPsec ネゴシエーションに使用します。
- 認証にデジタル証明書を使用するには、**Certificate** オプション ボタンをクリックし、ドロップダウン リストで Certificate Signing Algorithm を選択し、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選択します。

  認証にデジタル署名を使用する場合でも、トラストポイント名をまだ設定していないときは、他の 2 つのオプションのいずれかを使用して Wizard を続行できます。標準の ASDM ウィンドウを使用して、後で認証設定を変更できます。
- **Challenge/response authentication (CRACK)** オプション ボタンをクリックして、その認証方式を使用します。



ステップ 2　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（「Cisco」など）を入力して、この適応型セキュリティ アプライアンスに接続します。

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、Kerberos、および LDAP）で認証できます。

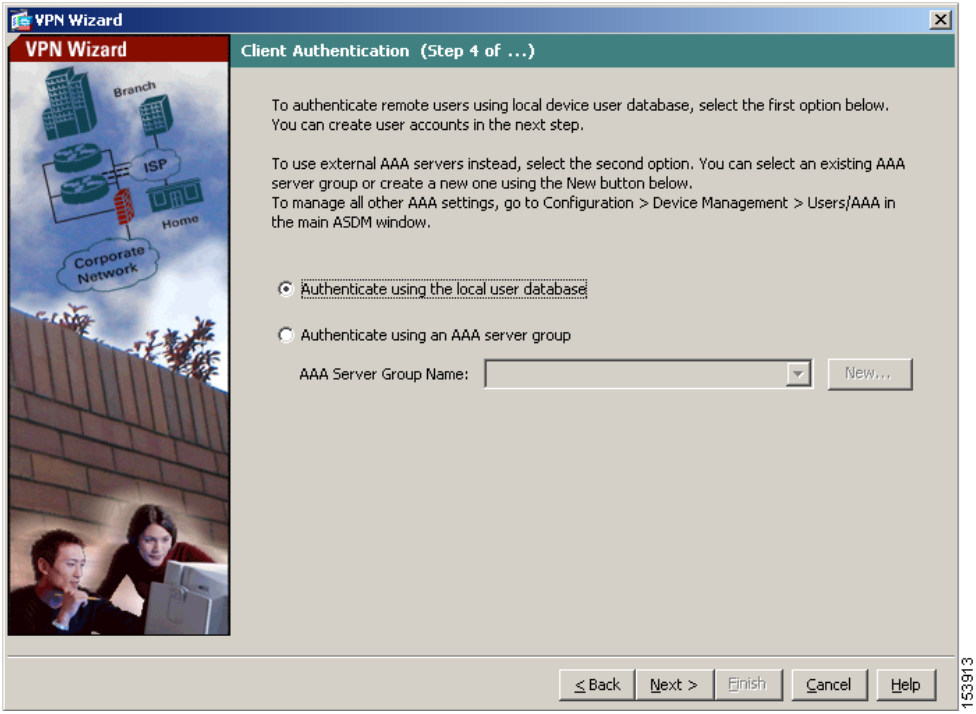
VPN Wizard の Step 4 で、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにユーザ データベースを作成してユーザを認証する場合は、**Authenticate using the local user database** オプション ボタンをクリックします。

ステップ 2　外部 AAA サーバ グループでユーザを認証する場合は、次の手順を実行します。

a. **Authenticate using an AAA server group** オプション ボタンをクリックします。

b. Authenticate using an AAA server group ドロップダウン リストから事前設定済みのサーバ グループを選択するか、または **New** をクリックして、新しい AAA サーバ グループを追加します。



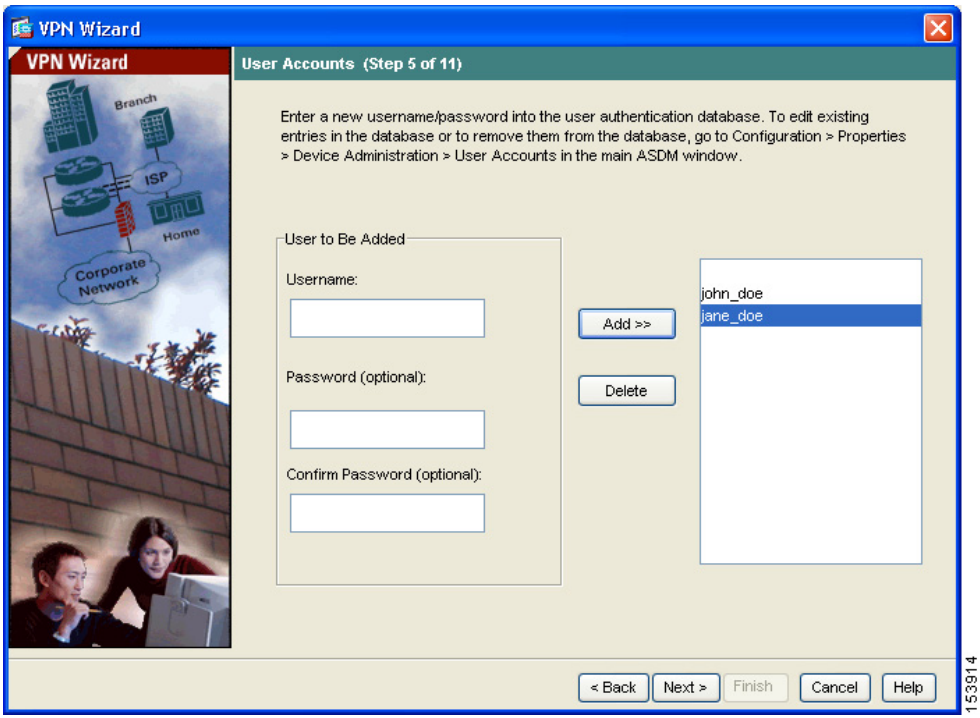
ステップ 3　**Next** をクリックして続行します。

（オプション）ユーザ アカウントの設定

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、ここで新しいユーザ アカウントを作成できます。ASDM 設定インターフェイスを使用して、後でユーザを追加することもできます。

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。



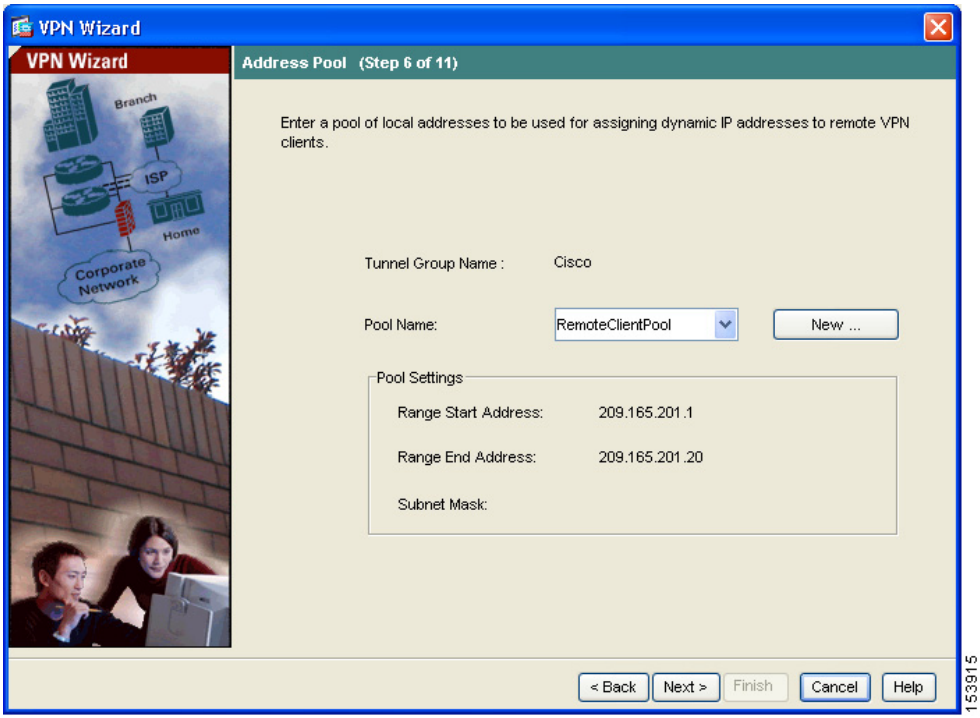
ステップ 2　新しいユーザの追加が終了したら、**Next** をクリックして続行します。

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。

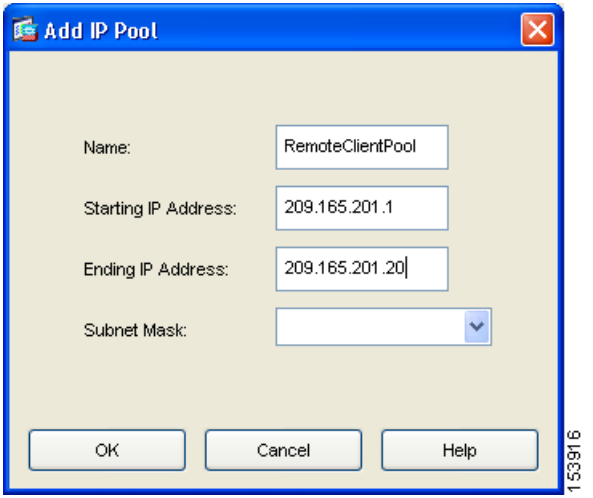
VPN Wizard の Step 6 で、次の手順を実行します。

ステップ 1　Pool Name 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選択します。



あるいは、**New** をクリックして、新しいアドレス プールを作成します。

Add IP Pool ダイアログボックスが表示されます。



ステップ 2　Add IP Pool ダイアログボックスで、次の手順を実行します。

a. IP アドレスの範囲の開始値と終了値を入力します。

b. （オプション）サブネット マスクを入力するか、または Subnet Mask ドロップダウン リストから、IP アドレスの範囲のサブネット マスクを選択します。

c. **OK** をクリックして、VPN Wizard の Step 6 に戻ります。

ステップ 3　**Next** をクリックして続行します。

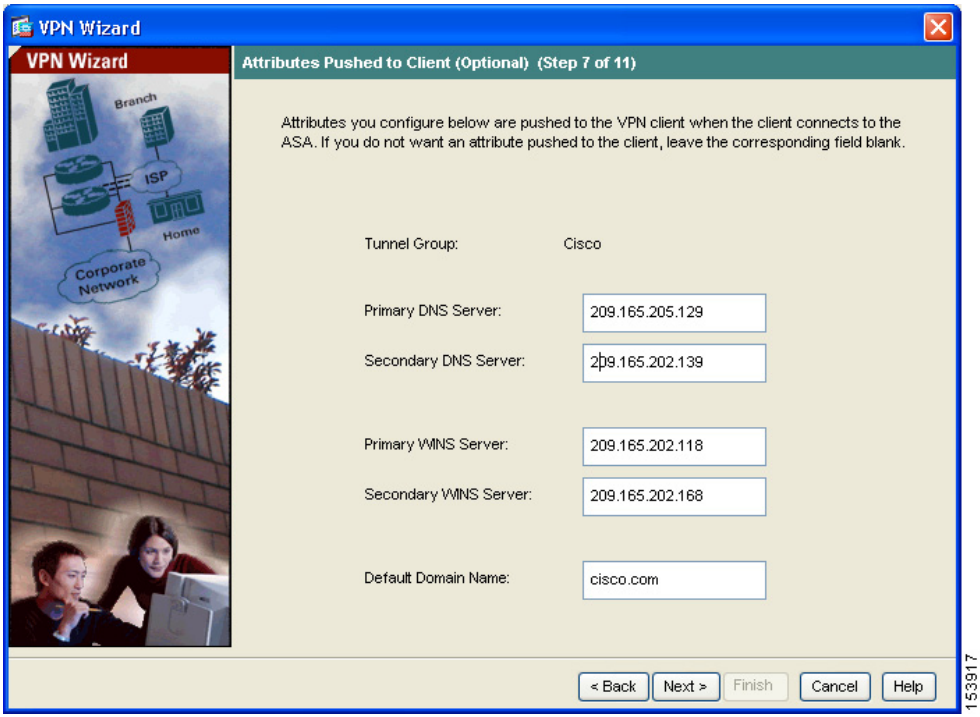
クライアント アトリビュートの設定

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 クライアントまたは Easy VPN ハードウェア 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 クライアントにプッシュするネットワーク設定情報を入力します。



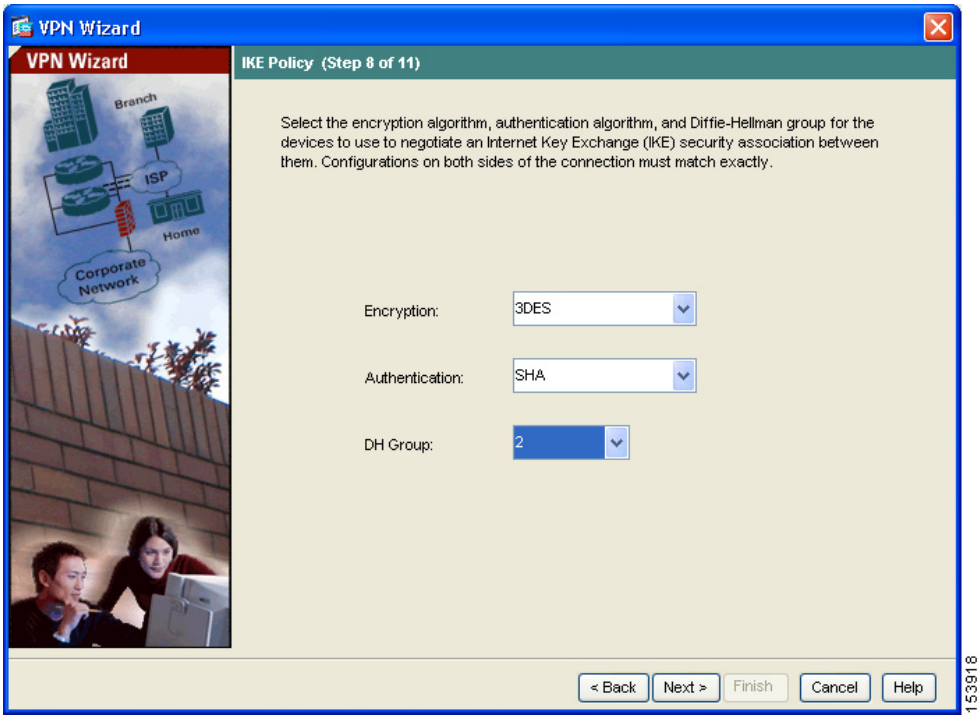
ステップ 2　**Next** をクリックして続行します。

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。

VPN Wizard の Step 8 で 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-Hellman グループ（1、2、または 5）を選択します。

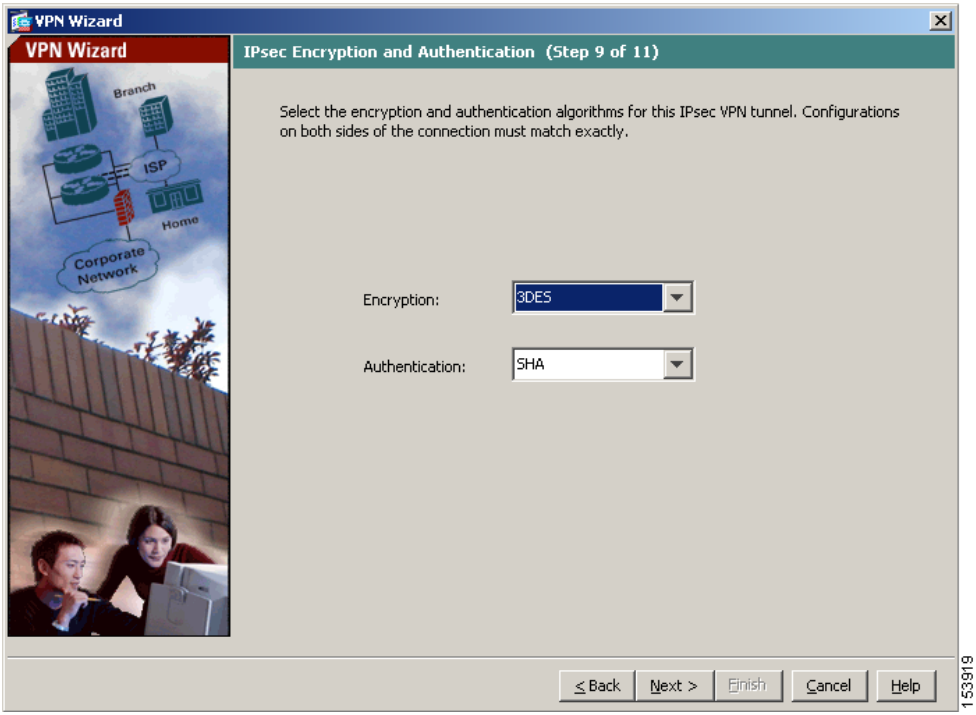


ステップ 2　**Next** をクリックして続行します。

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

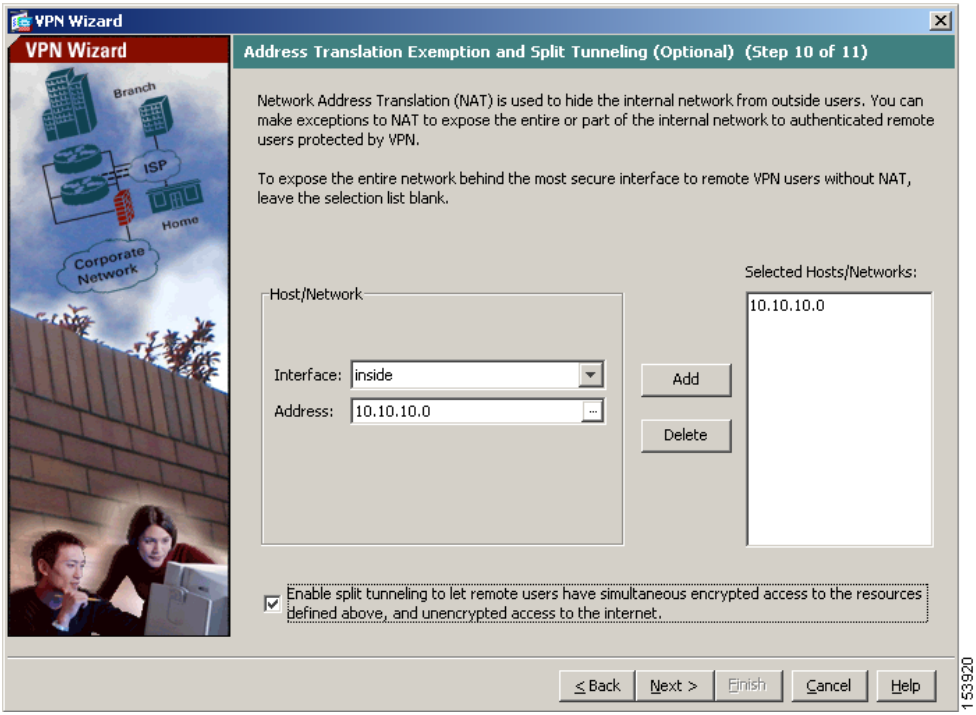
スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントは一定の条件に従い、パケットを暗号化形式で IPsec トンネルに送信したり、テキスト形式でネットワーク インターフェイスに送信したりすることができます。

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 ユーザにアクセスできるように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

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 Hosts/Networks 領域のホスト、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。

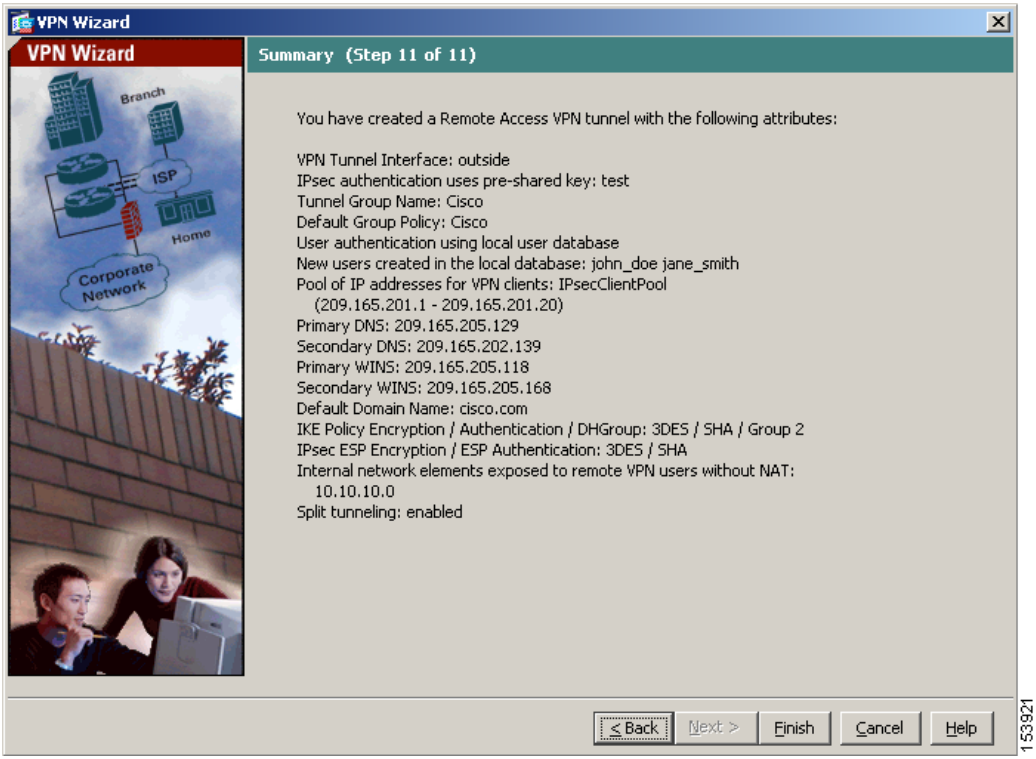


（注）　画面の下部にある **Enable split tunneling...** チェックボックスをオンにして、スプリット トンネリングをイネーブルにします。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックを、暗号化された VPN トンネルを使用せずに直接インターネットに送出できるようになります。

ステップ 2　**Next** をクリックして続行します。

リモートアクセス VPN 設定の確認

VPN Wizard の Step 11 で、新しい 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、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。

次回のデバイス起動時に変更が適用されるように、設定変更をスタートアップ設定に保存する場合は、File メニューで **Save** をクリックします。あるいは、ASDM の終了時に設定変更の保存を要求するプロンプトが表示されます。

設定変更を保存しない場合は、次回のデバイス起動時に以前の設定が有効になります。

次の手順

モバイル ユーザやテレワーカのためのセキュアな接続用のエンドツーエンドの暗号化 VPN トンネルを確立するには、Cisco VPN クライアント ソフトウェアを入手してください。

Cisco Systems VPN クライアントの詳細については、次の URL を参照してください。http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html

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*

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 8 章「シナリオ：DMZ の設定」
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」

次の手順