CHAPTER 7

シナリオ：IPsec リモートアクセス VPN 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 接続を受け入れ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、インターネットを越えてセキュアな接続（トンネル）を作成でき、オフサイトのユーザにセキュアなアクセスを提供できます。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。

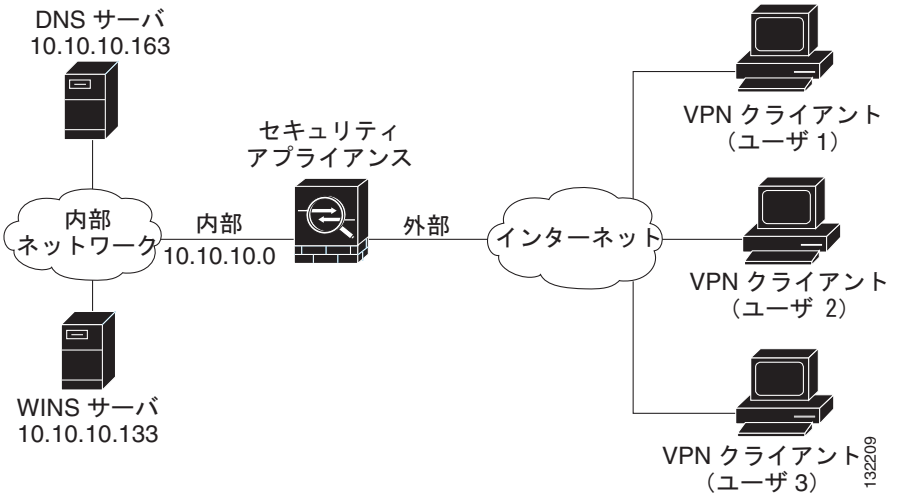
Easy VPN ソリューションを実装する場合、この章では、Easy VPN サーバ（別名、ヘッドエンド デバイス）を設定する方法について説明します。

この章には、次の項があります。

IPsec リモートアクセス VPN ネットワーク トポロジの例

図 7-1 に、インターネットを越えて Cisco Easy VPN ソフトウェア クライアントまたはハードウェア クライアントなどの VPN クライアントからの要求を受け入れ、VPN 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ます。

図 7-1　　リモート アクセス VPN 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

ここでは、リモート クライアントおよびデバイスから IPsec VPN 接続を受け入れるように適応型セキュリティ アプライアンスを設定する方法について説明します。Easy VPN ソリューションを実装する場合、この項では、Easy VPN サーバ（別名、ヘッドエンド デバイス）を設定する方法について説明します。

設定内容の例で使われる値は、図 7-1 に示すリモートアクセス シナリオのものです。

この項は、次の内容で構成されています。

収集する情報

リモート アクセス IPsec VPN 接続を受け入れるよう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開始する前に、次の情報を手元に用意してください。

- IP プールで使用する IP アドレスの範囲。これらのアドレスは、正常に接続されると、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を作成するときに使用するユーザのリスト（認証用に AAA サーバを使用している場合を除く）。

- VPN に接続する場合に、リモート クライアントが使用するネットワーキング情報。内容は次のとおりです。
  - プライマリおよびセカンダリの DNS サーバの IP アドレス
  - プライマリおよびセカンダリの WINS サーバの IP アドレス
  - デフォルトのドメイン名
  - 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

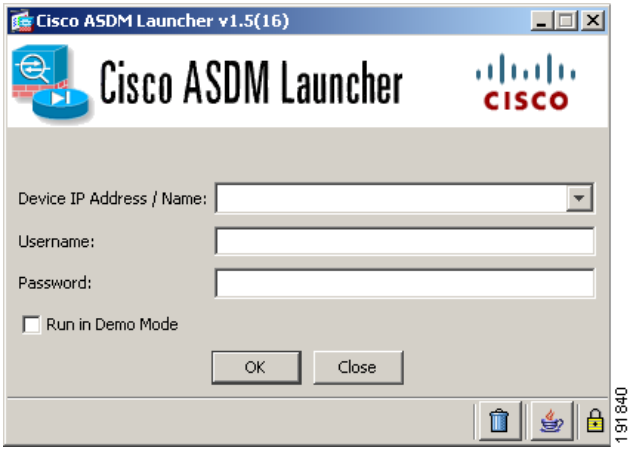
この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアがインストールされていない場合は、P.5-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して ASDM に直接アクセスする場合は、P.5-10 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、次の手順に従います。

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 と Password のフィールドは空白のままにしておきます。

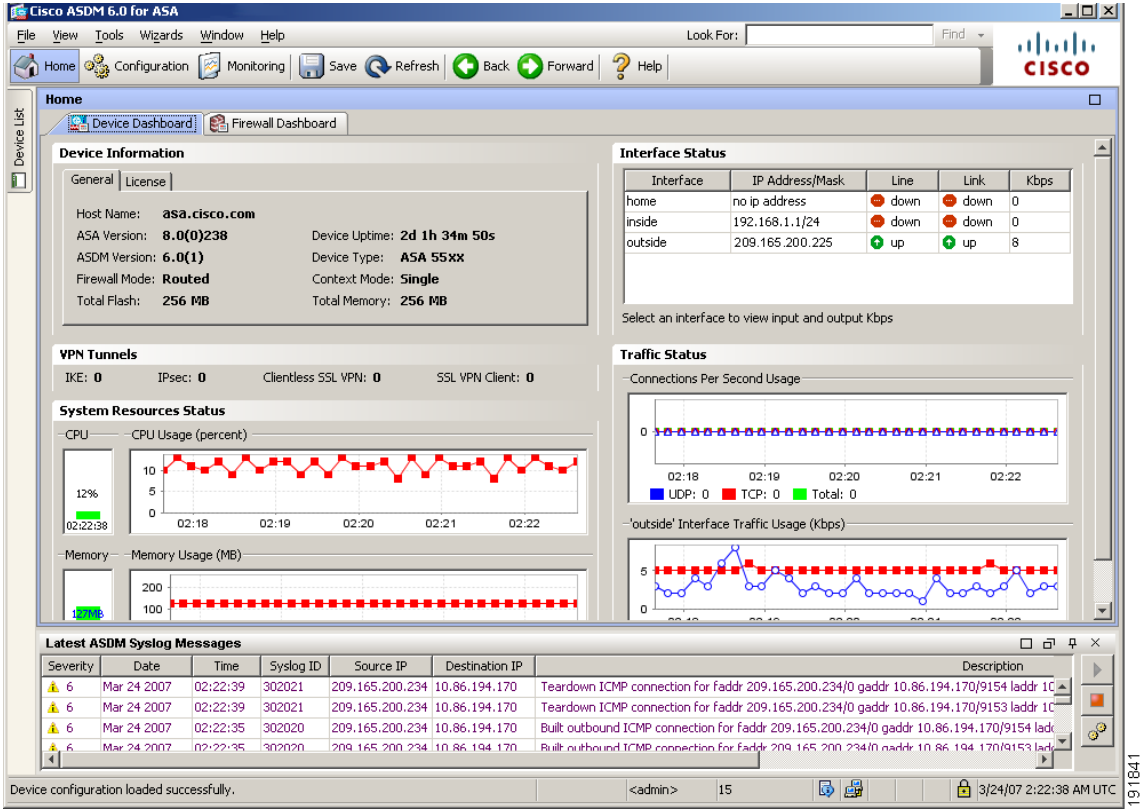
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書の受け入れ要求を含むセキュリティ警告が表示された場合は、**Yes** をクリックします。

ASA が、アップデートされたソフトウェアがあるかどうか確認し、ある場合は自動的にダウンロードします。

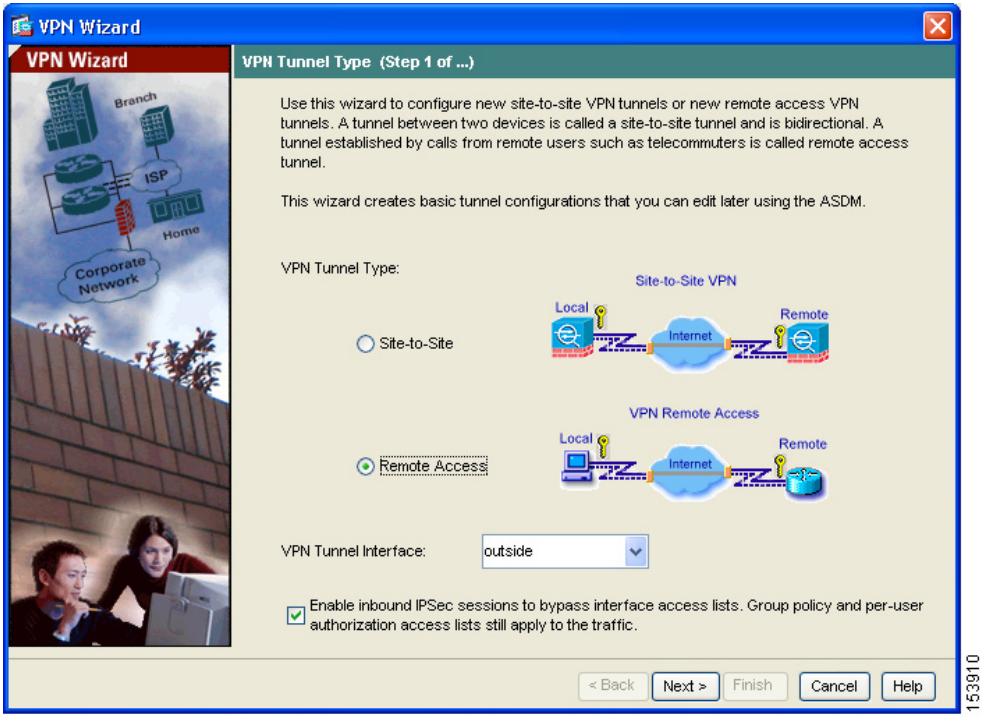
メイン ASDM ウィンドウが表示されます。



IPsec リモートアクセス VPN 用の ASA 5505 の設定

リモートアクセス VPN の設定用のプロセスを開始するには、次の手順に従います。

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



ステップ 2　VPN Wizard の Step 1 で、次の手順に従います。

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 リストから、着信 VPN トンネルで有効なインターフェイスとして **Outside** を選択します。

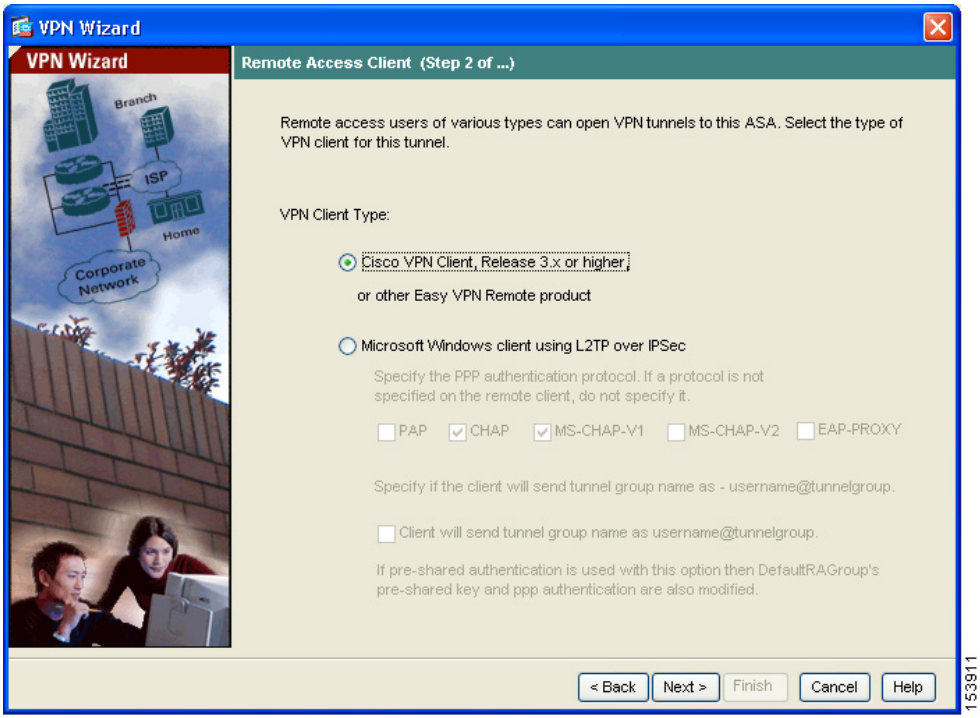
c. **Next** をクリックして続行します。

VPN クライアント タイプの選択

VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　この適応型セキュリティ アプライアンスに接続するリモート ユーザを有効にする 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 リモート製品も使用できます。



ステップ 2　**Next** をクリックして続行します。

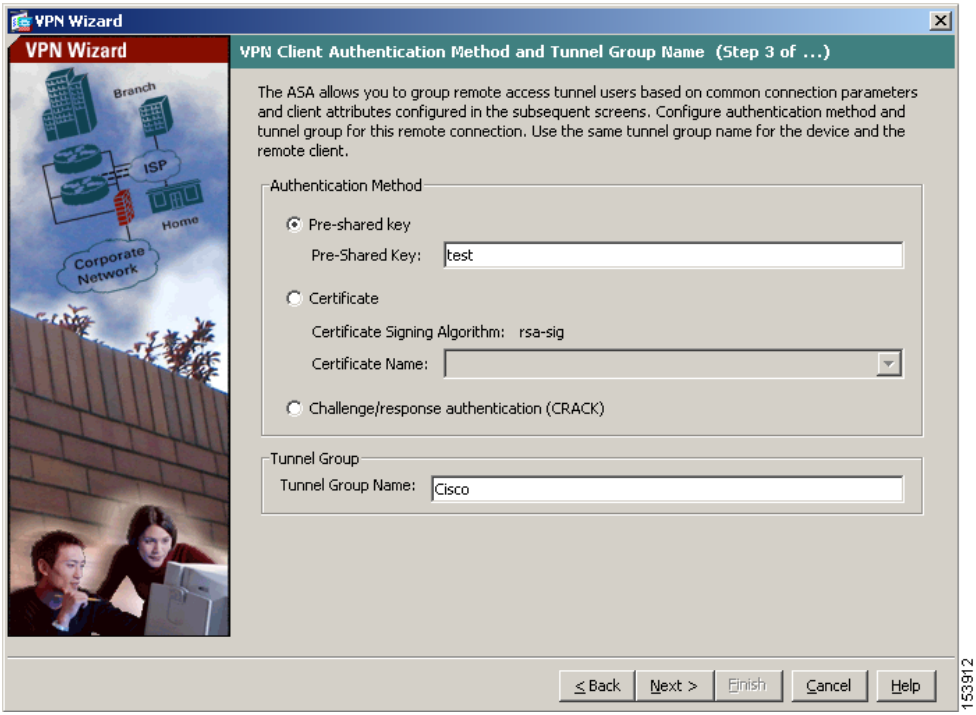
VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順に従います。

ステップ 1　次のいずれかの操作を実行して、使用する認証のタイプを指定します。

- 認証にスタティック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（たとえば、「Cisco」）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPsec ネゴシエーションで使用されます。
- 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 リストから証明書署名アルゴリズムを選択し、次に、事前設定されているトラストポイント名をドロップダウン リストから選択します。

  認証にデジタル証明書を使用する予定で、まだトラストポイント名を設定していない場合は、他の 2 つのオプションのいずれかを使用してウィザードを続行できます。認証設定は、標準 ASDM ウィンドウを使用して後で修正できます。
- **Challenge/Response Authentication (CRACK)** オプション ボタンをクリックすると、この認証方式を使用できます。



ステップ 2　共通の接続パラメータおよびクライアント アトリビュートを使用して、この適応型セキュリティ アプライアンスに接続する複数ユーザのセットのトンネル グループ名（たとえば、「Cisco」）を入力します。

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

ユーザの認証は、ローカル認証データベース、または外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバを使用して実行できます（AAA サーバには RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP があります）。

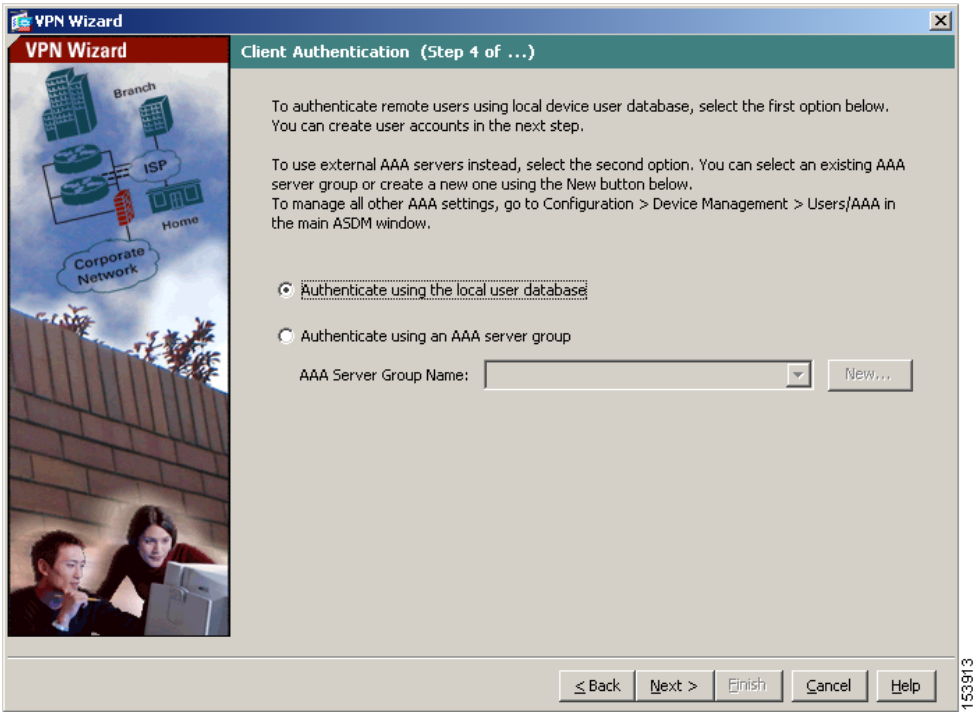
VPN Wizard の Step 4 で、次の手順に従います。

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には、**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 グループを使用してユーザを認証する場合は、次の手順に従います。

a. **Authenticate Using an AAA Server Group** オプション ボタンをクリックします。

b. 事前設定されているサーバ グループを Authenticate using an AAA Server Group ドロップダウン リストから選択するか、**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。



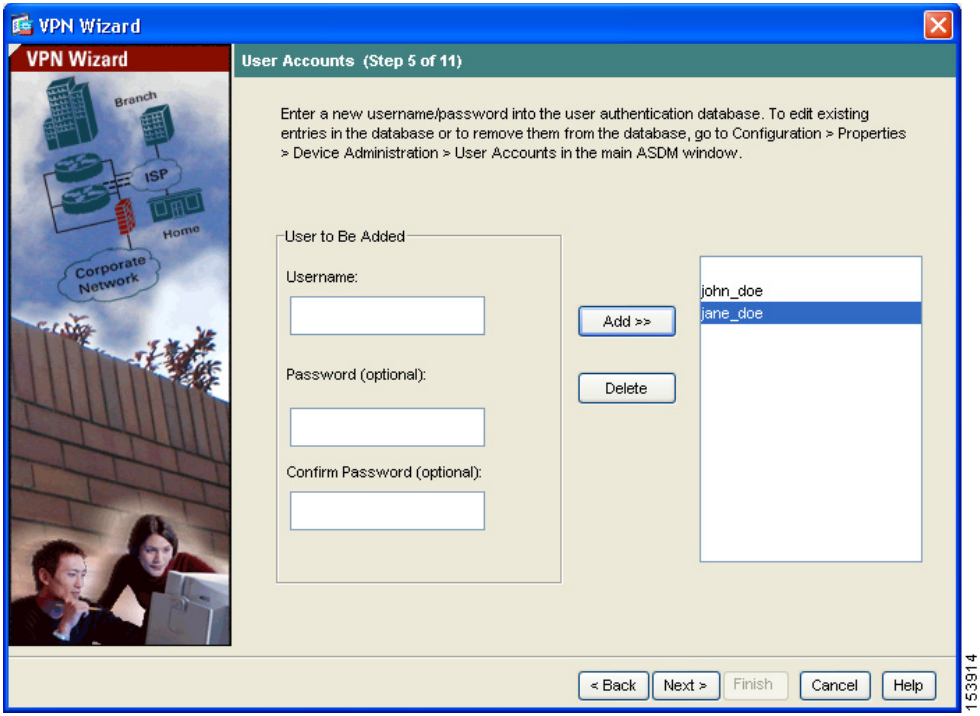
ステップ 3　**Next** をクリックして続行します。

（オプション）ユーザ アカウントの設定

ローカル ユーザ データベースを使用してユーザを認証する場合、次の手順で新しいユーザ 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、次の手順に従います。

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。



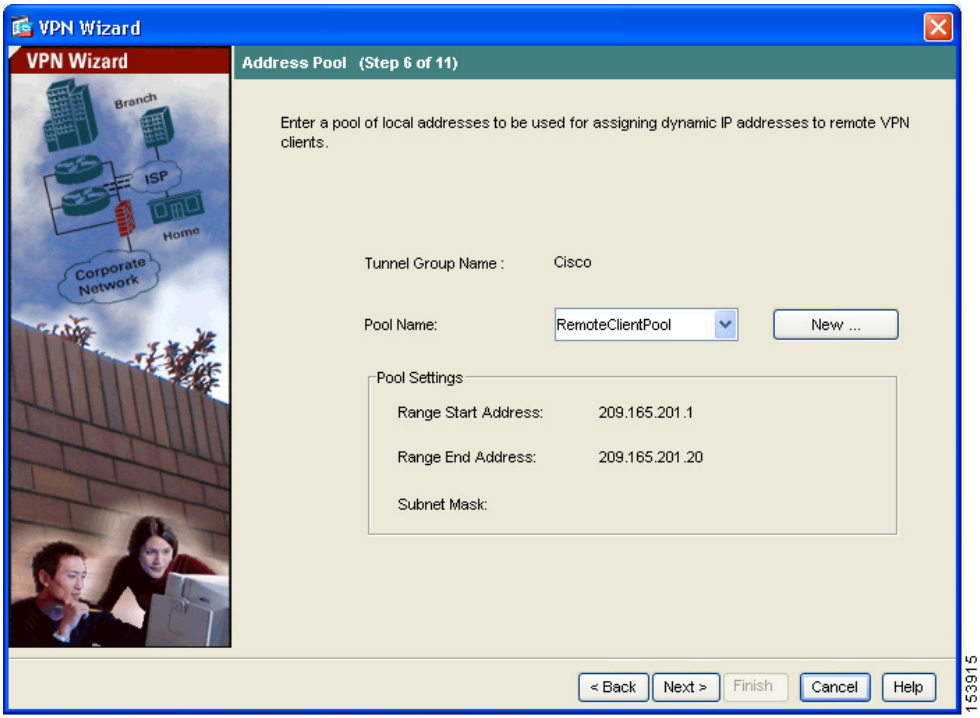
ステップ 2　新しいユーザの追加が終了したら、**Next** をクリックして続行します。

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するには、接続に成功したときにリモート VPN クライアントに割り当てられる可能性のある 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、プールは 209.165.201.1 ～ 209.166.201.20 の範囲の IP アドレスを使用するように設定します。

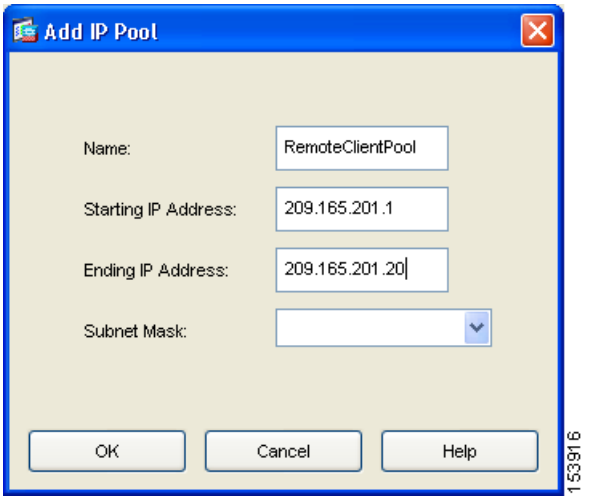
VPN Wizard の Step 6 で、次の手順に従います。

ステップ 1　プール名を入力するか、事前設定されているプールを Pool Name ドロップダウンリストから選択します。



または、**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、次の内容を実行します。

a. 範囲の開始 IP アドレスと終了 IP アドレスを入力します。

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

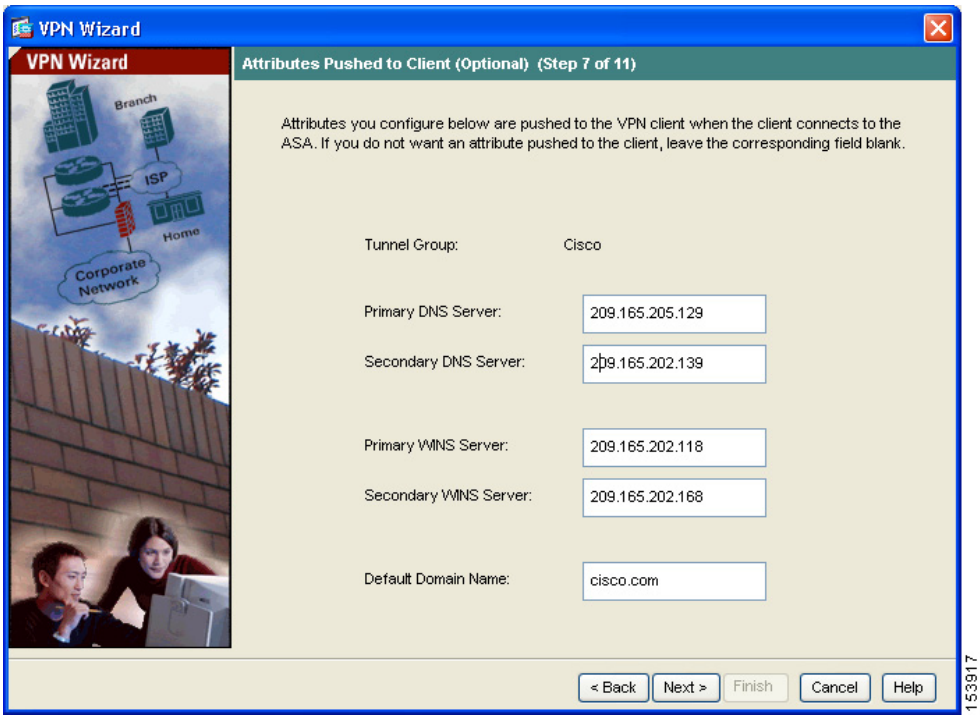
クライアント アトリビュートの設定

各リモート アクセス クライアントがネットワークにアクセスするには、使用する DNS サーバと WINS サーバ、デフォルトのドメイン名などの基本的なネットワーク設定情報が必要です。各リモート クライアントを個々に設定するのではなく、ASDM にクライアント情報を設定できます。接続が確立されると、適応型セキュリティ アプライアンスは、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 クライアントに適用します。

必ず正しい値を指定してください。値が正しくない場合、リモート クライアントが解決に DNS 名を使用できない、または Windows ネットワーキングを使用できないという問題が発生します。

VPN Wizard の Step 7 で、次の手順に従います。

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



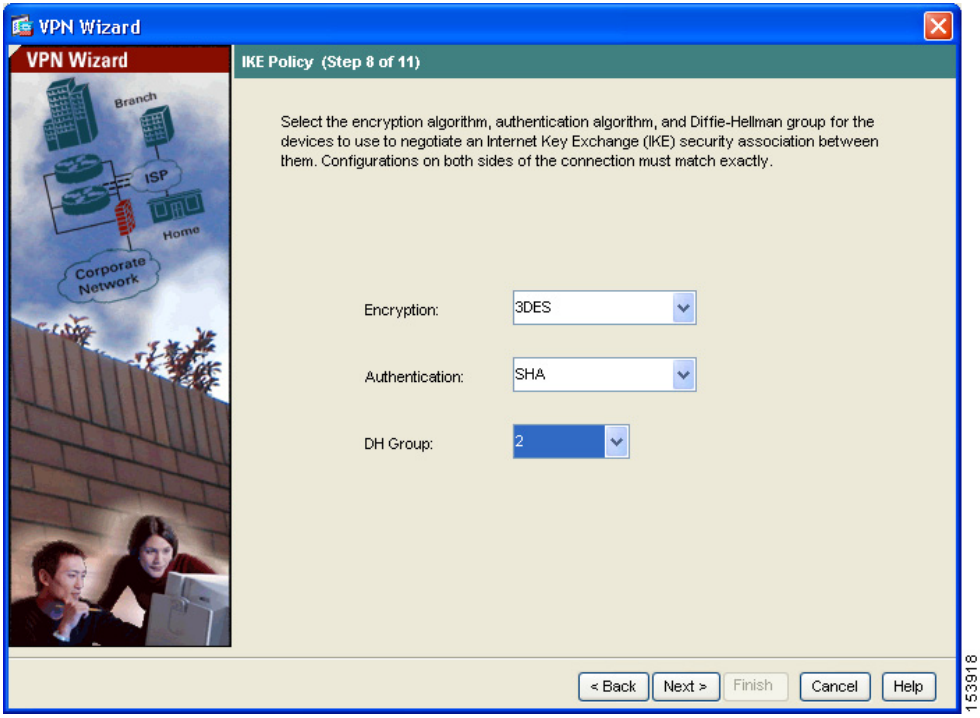
ステップ 2　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、データを保護しプライバシーを保証する暗号化方式を含むネゴシエーション プロトコルで、ピアの ID を確認する認証方式でもあります。ほとんどの場合、ASDM のデフォルト値を使用すれば、十分にセキュアな 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、次の手順に従います。

ステップ 1　IKE セキュリティ アソシエーションにおいて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、5、または 7）を選択します。

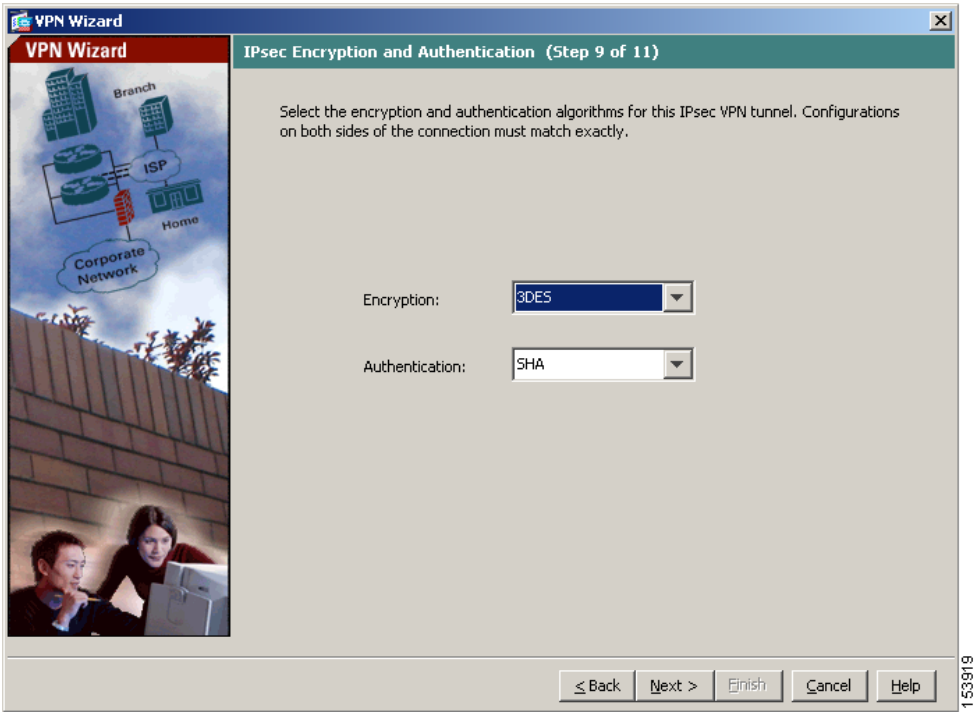


ステップ 2　**Next** をクリックして続行します。

IPsec Encryption パラメータ および Authentication パラメータの設定

VPN Wizard の Step 9 で、次の手順に従います。

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およびスプリット トンネリングの指定

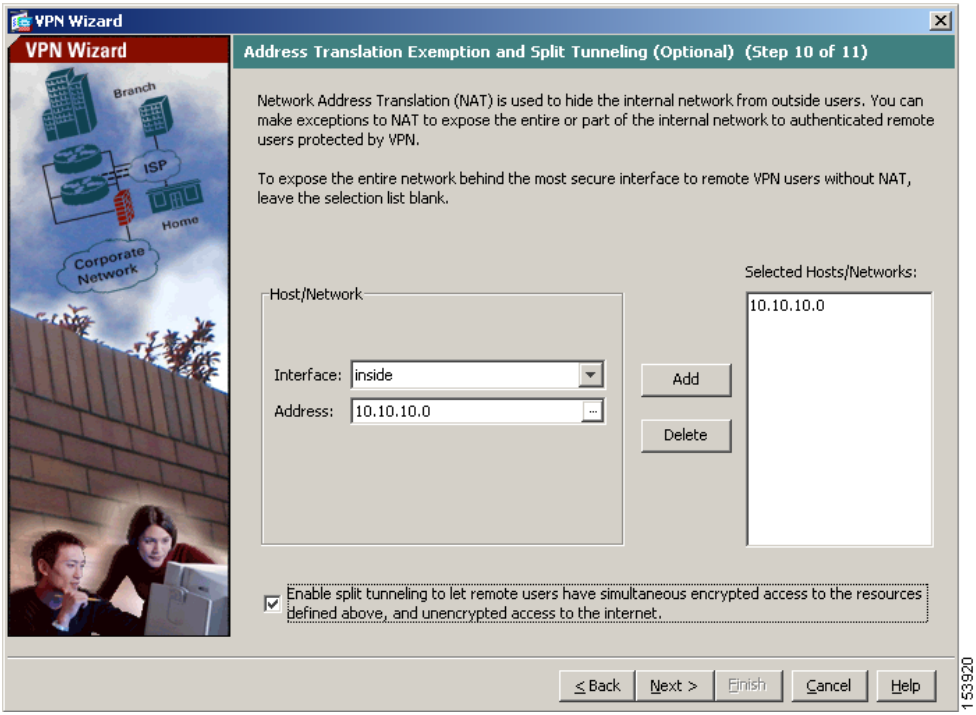
スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントは、パケットを条件によって、IPsec トンネル経由で送信することや（暗号化形式）、ネットワーク インターフェイスに送信することが（テキスト形式）できます。

適応型セキュリティ アプライアンスは、Network Address Translation（NAT; ネットワーク アドレス変換）を使用して、内部 IP アドレスが外部に公開されないようにしています。認証されたリモート ユーザにアクセスを許可するローカル ホストおよびネットワークを特定することで、このネットワーク保護に例外を設定できます。

VPN Wizard の Step 10 で、次の手順に従います。

ステップ 1　認証されたリモート ユーザにアクセスを許可する内部リソースのリストに入れるホスト、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するには **Add**、動的に削除するには **Delete** をクリックします。

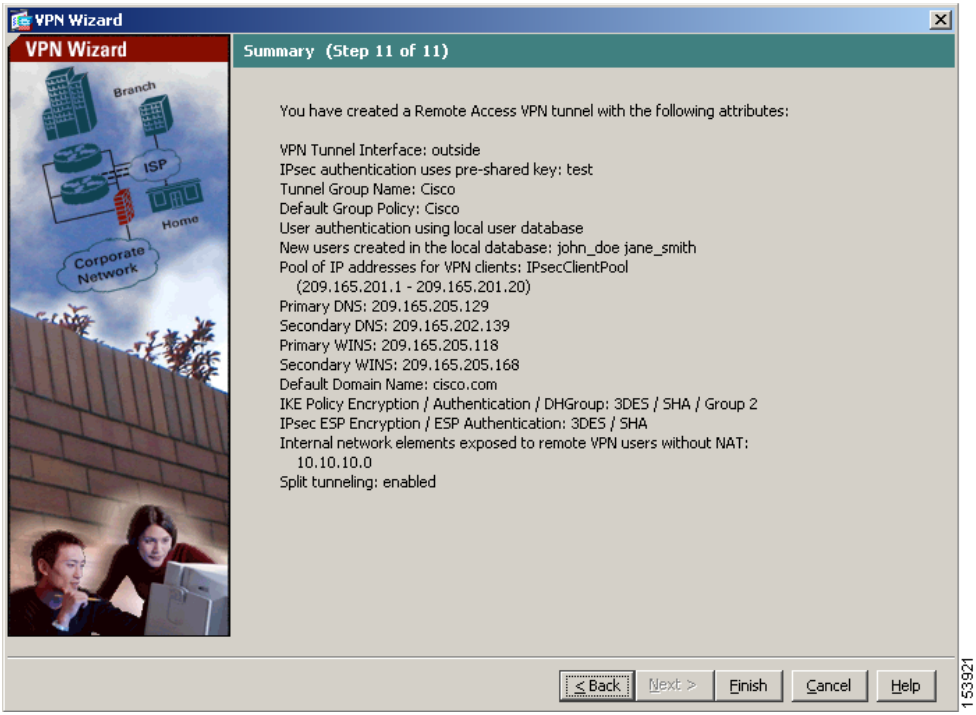


（注）　画面下部の **Enable Split Tunneling ...** チェックボックスをオンにすると、スプリット トンネリングがイネーブルになります。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックは、暗号化された VPN トンネルを経由せずにインターネットに直接送信されます。

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。



適切に設定されている場合は **Finish** をクリックして、適応型セキュリティ アプライアンスに変更内容を適用します。

次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、File メニューから **Save** をクリックします。または、ASDM を終了するときに設定変更を半永久的に保存するように求められます。

設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそのまま適用されます。

次の作業

モバイル従業員またはテレワーカー向けの安全な接続用に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ます。

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

リモートアクセス VPN 環境だけに適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が終了しました。さらに、次の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常的な運用について	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
DMZ 内の Web サーバを保護するための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 設定」
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 8 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 9 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 10 章「シナリオ:サイトツーサイト VPN 設定」

次の作業