CHAPTER 8

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 接続を受け入れる方法について説明します。リモート アクセス VPN では、インターネットを介したセキュアな接続またはトンネルを作成し、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。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。

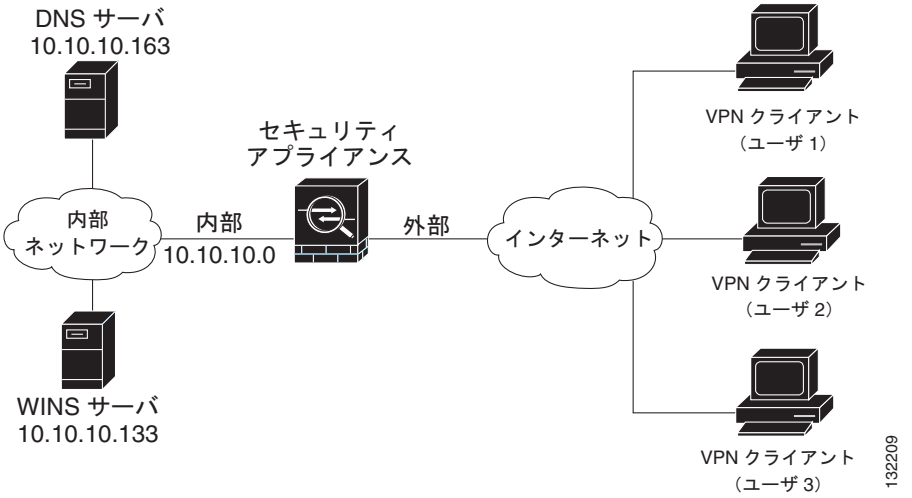
Easy VPN ソリューションを実装している場合は、この章で Easy VPN サーバ（ヘッドエンド デバイスと呼ばれる場合もあります）の設定方法を参照できます。

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 8-1 に、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）からの要求を受け入れ、IPsec 接続を確立するように設定されている適応型セキュリティ アプライアンスを示します。

図 8-1　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 のシナリオの実装

この項では、リモート クライアントおよびデバイスからの IPsec VPN 接続を受け入れるための適応型セキュリティ アプライアンスの設定方法について説明します。Easy VPN ソリューションを実装している場合は、この項で Easy VPN サーバ（ヘッドエンド デバイスと呼ばれる場合もあります）の設定方法を参照できます。

設定内容の値の例は、図 8-1 に示したリモート アクセスのシナリオから使用しています。

次のトピックについて取り上げます。

必要な情報

リモート アクセス IPsec VPN 接続を受け入れるための適応型セキュリティ アプライアンスの設定を開始する前に、次の情報を用意してください。

- IP プールに使用する IP アドレスの範囲。これらのアドレスは、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（認証に AAA サーバを使用している場合を除く）。

- VPN との接続時にリモート クライアントで使用する次の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

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.4-8 の「Web ブラウザでの 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 ASDM に直接アクセスする場合は、P.4-8 の「Web ブラウザでの 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 フィールドと Password フィールドを空のままにします。

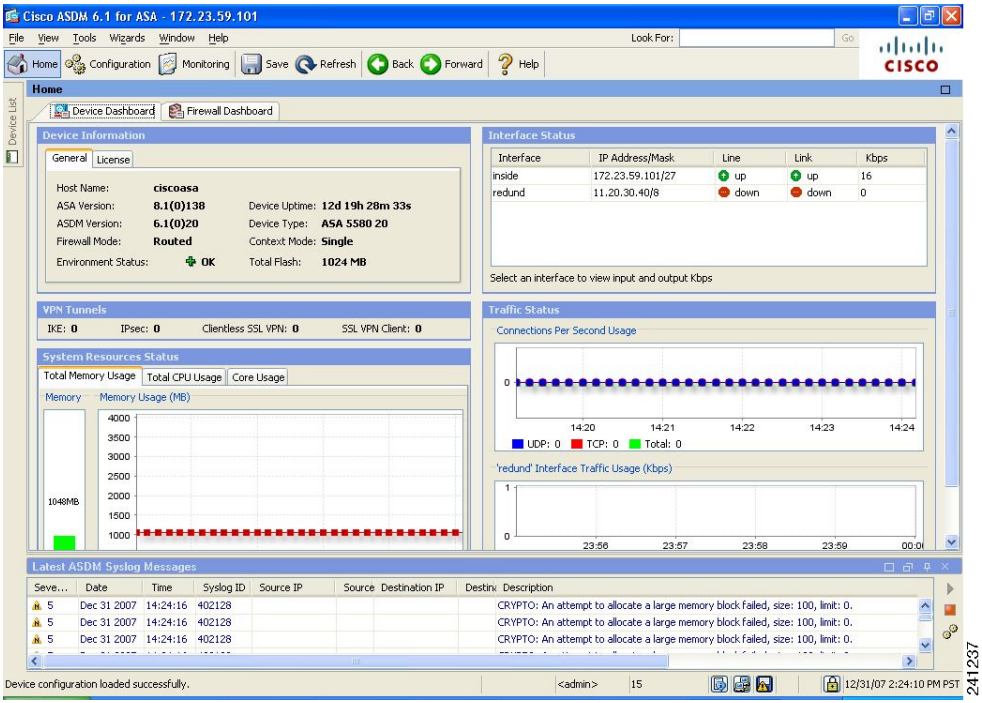
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 4　**OK** をクリックします。

ステップ 5　証明書の受け入れを求める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。

適応型セキュリティ アプライアンスは最新ソフトウェアが存在するかどうかを調べ、存在する場合は自動的にダウンロードします。

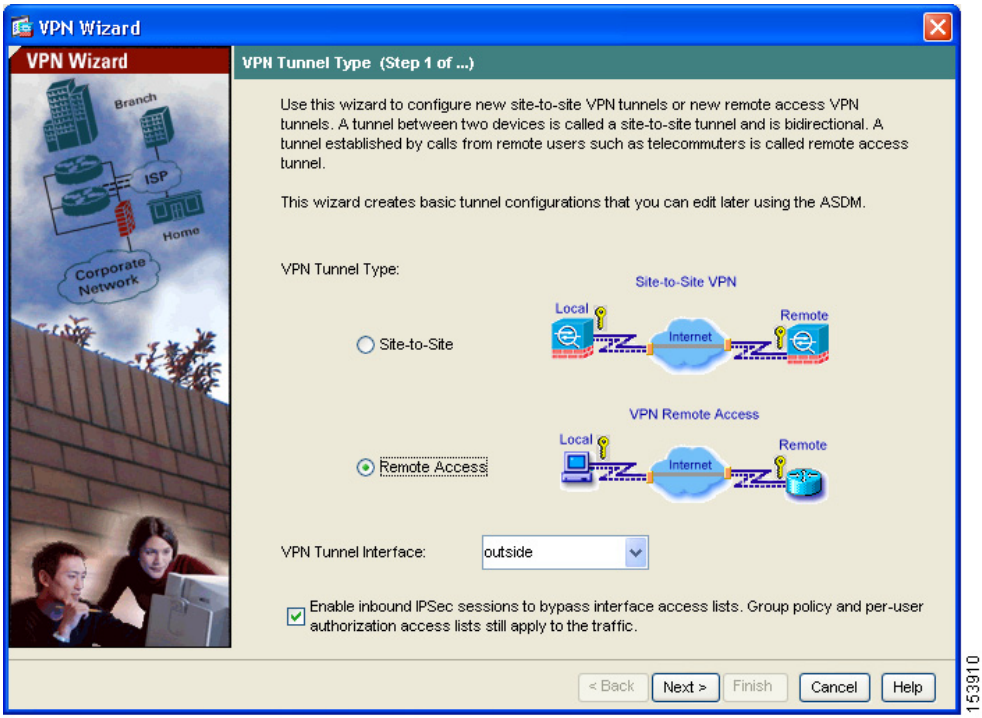
ASDM のメイン ウィンドウが表示されます。



IPSec リモート アクセス VPN 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 リストから、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。

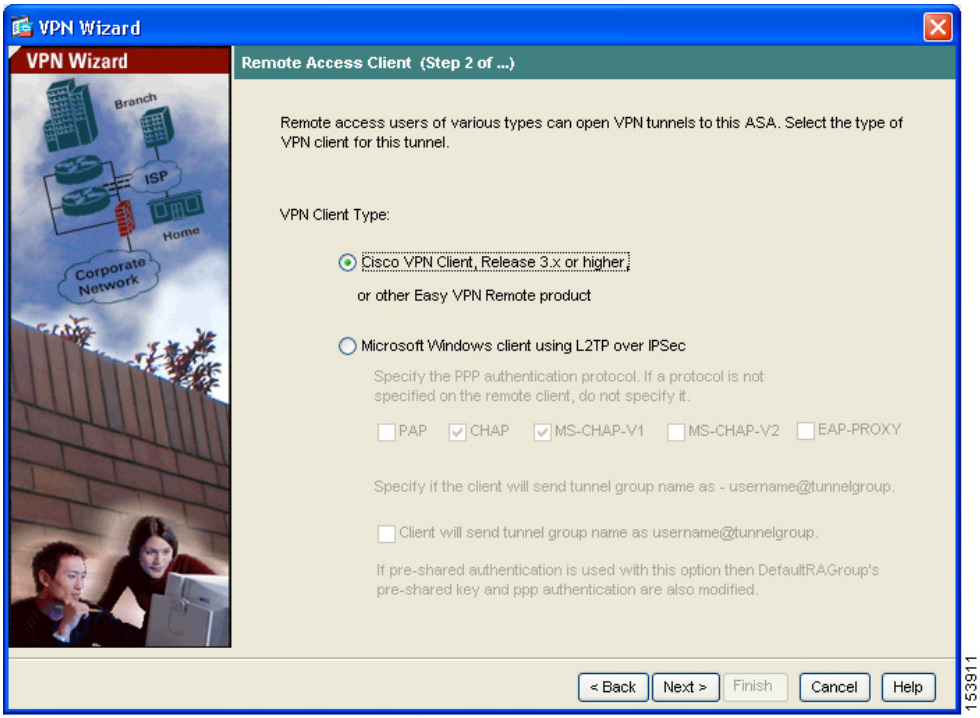
c. **Next** をクリックして続行します。

VPN クライアントの種類の選択

VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　リモート ユーザをこの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する VPN クライアントの種類を指定します。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。

他の任意の Cisco Easy VPN Remote 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。

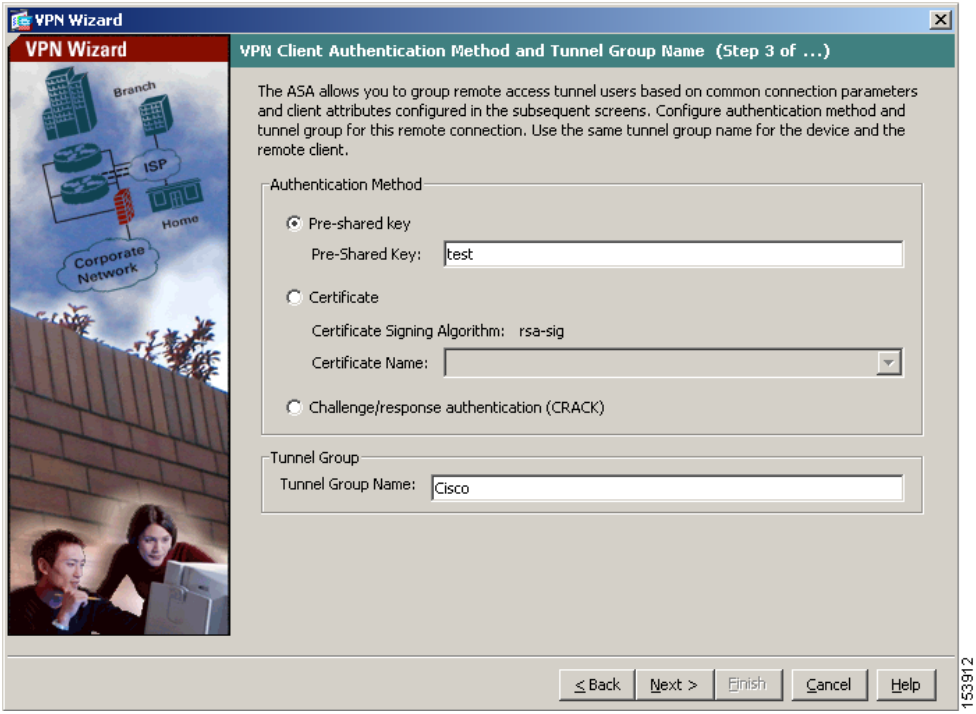
VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　次のいずれかの手順を実行して、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 Certificate Signing Algorithm を選択し、次のドロップダウン リストから事前設定済みのトラスト ポイント名を選択します。

  デジタル証明書を認証に使用するがトラストポイント名をまだ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 Wizard を続行できます。認証方式の設定は、標準の ASDM ウィンドウを使用して後で変更できます。
- **Challenge/response authentication (CRACK)** オプション ボタンをクリックすると、この方法で認証されます。



ステップ 2　このセキュリティ アプライアンスとの接続で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。

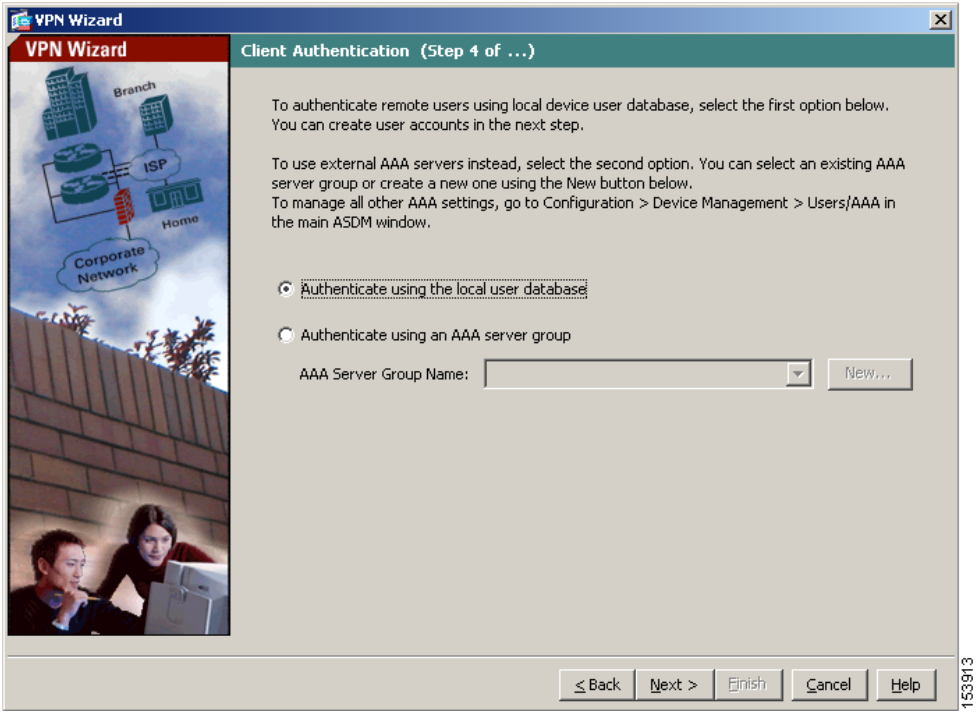
VPN Wizard の Step 4 で、次の手順を実行します。

ステップ 1　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. AAA Server Group Name 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、**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。



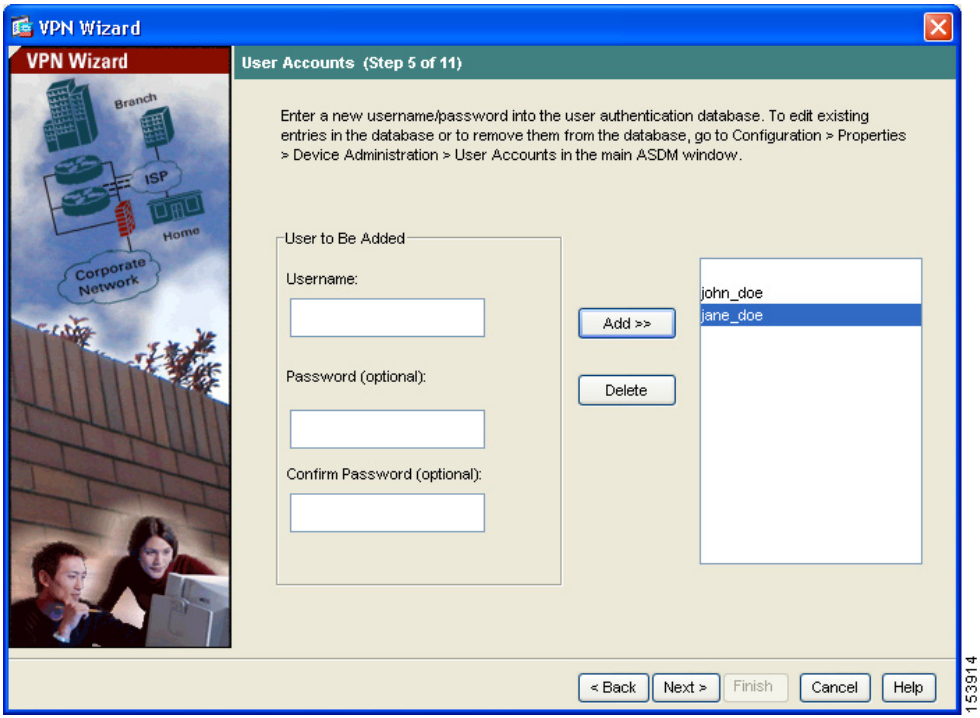
ステップ 3　**Next** をクリックして続行します。

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、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。



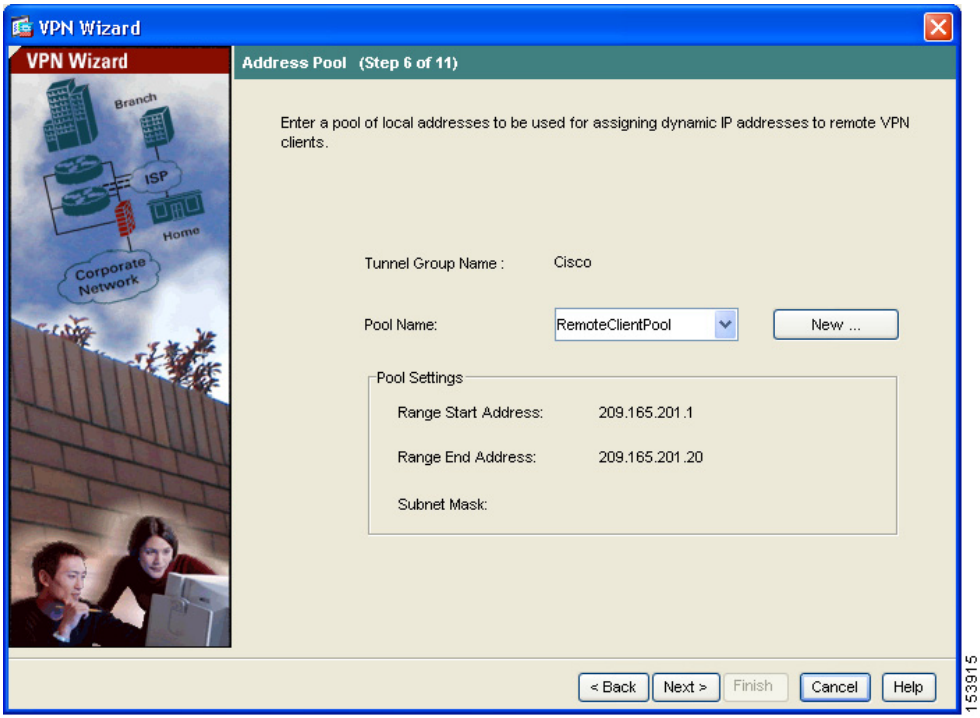
ステップ 2　新しいユーザの追加が終了したら、**Next** をクリックして続行します。

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。

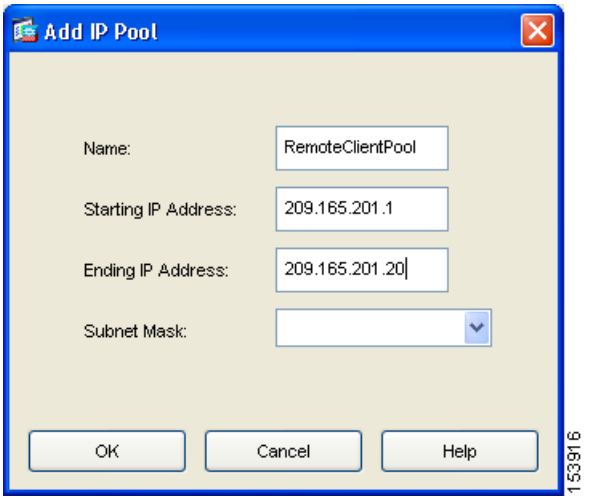
VPN Wizard の Step 6 で、次の手順を実行します。

ステップ 1　プール名を入力するか、ドロップダウン リストから事前設定済みのプールを選択します。



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、次の手順を実行します。

a. アドレスの範囲を指定する Starting IP Address と Ending IP Address 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。

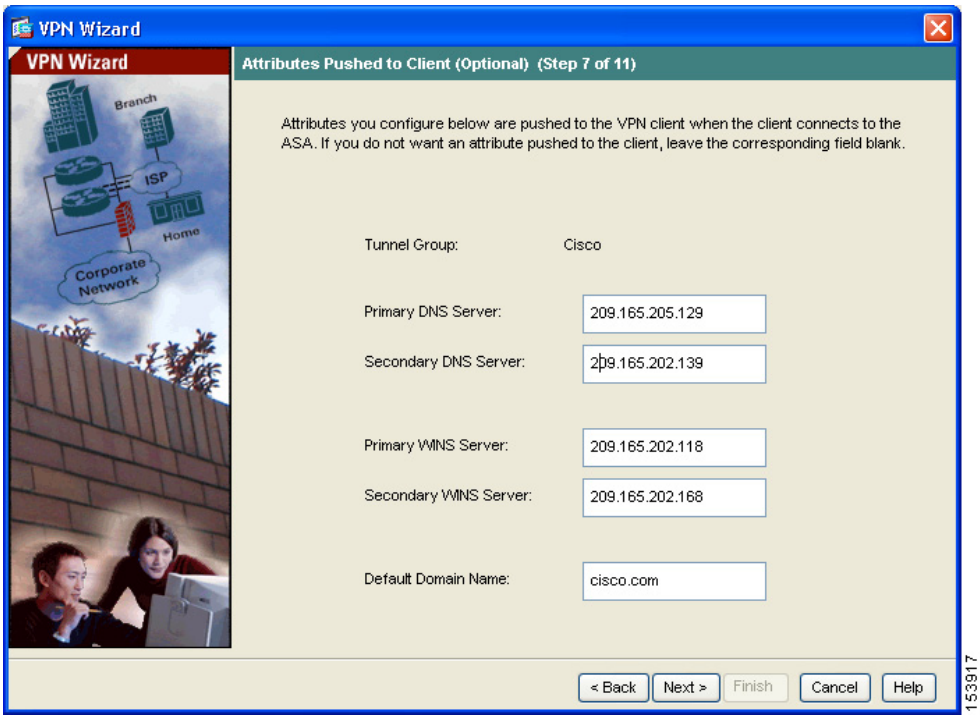
クライアント アトリビュートの設定

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。



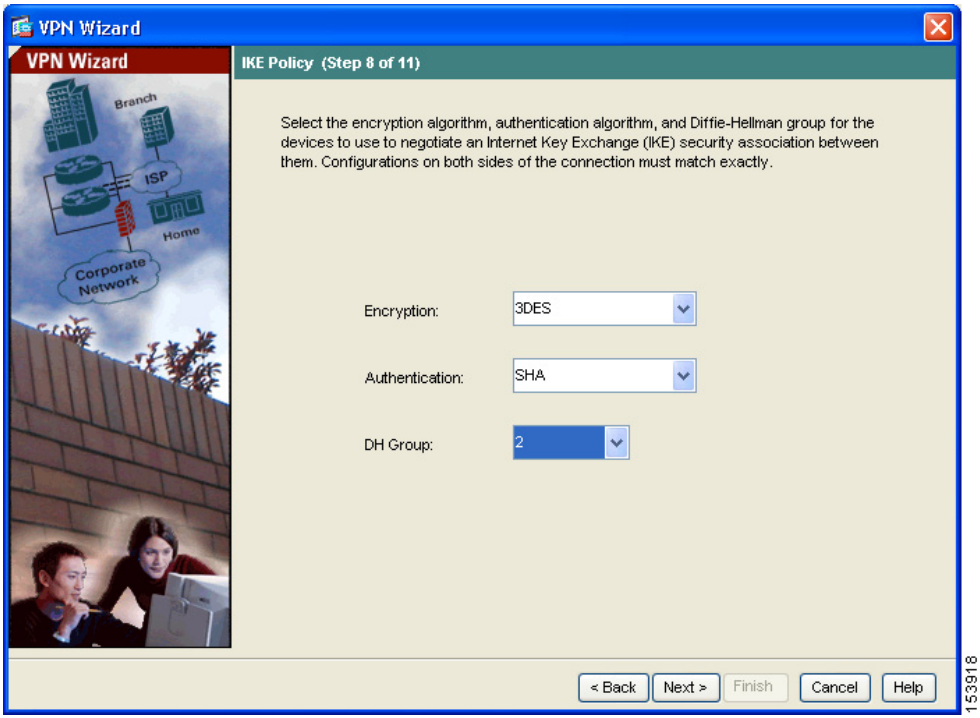
ステップ 2　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、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 を確認する認証も提供します。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、5、または 7）をクリックします。

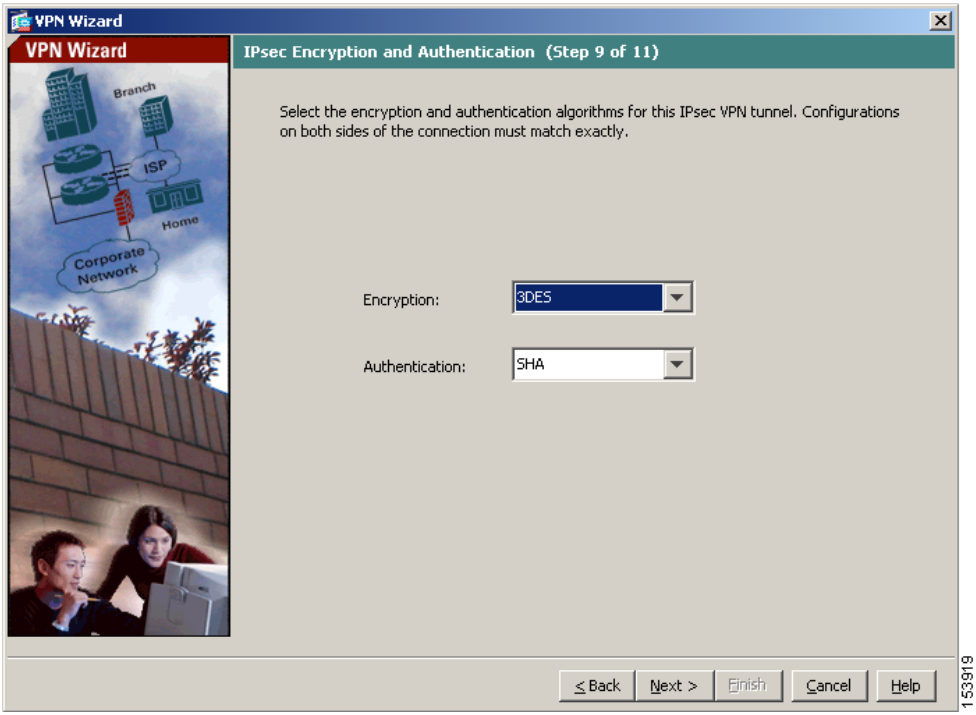


ステップ 2　**Next** をクリックして続行します。

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

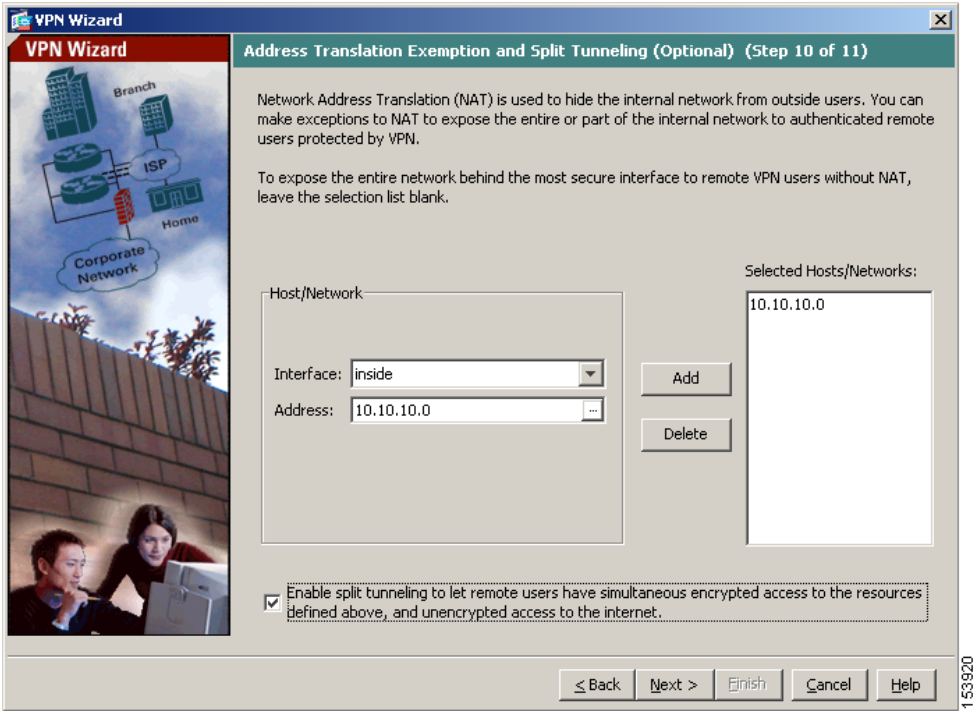
スプリット トンネリングを使用すると、リモート アクセス IPsec クライアントは、IPsec トンネル経由での暗号化形式のパケット、またはネットワーク インターフェイスへのテキスト形式のパケットを、条件付きで送信できます。

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 ユーザのアクセスを可能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特定して、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。

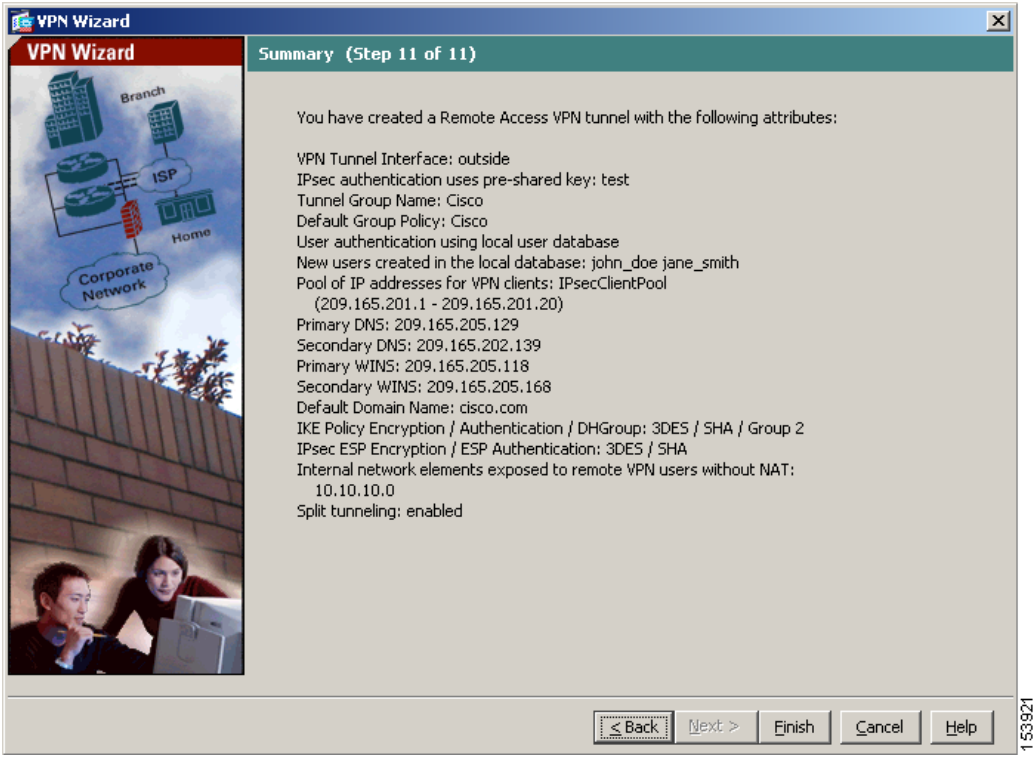


（注）　画面の下部にある **Enable split tunneling** チェックボックスをオンにして、スプリット トンネリングをイネーブルにします。スプリット トンネリングを使用すると、設定したネットワークの外部のトラフィックを、暗号化された VPN トンネルを使用せずに直接インターネットに送出できるようになります。

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 の設定の確認

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。

設定の変更をスタートアップ設定に保存して、デバイスを次回に起動したときにこの変更が適用されるようにする場合は、File メニューの **Save** をクリックします。あるいは、ASDM の終了時に、設定の変更を保存するかどうかの確認を求めるメッセージが表示されます。

設定の変更を保存しないと、次回にデバイスを起動したときに、以前の設定が有効になります。

次の手順

エンドツーエンドの暗号化された VPN トンネル（外勤社員や在宅勤務者向けにセキュアな接続を提供）を確立するには、Cisco VPN クライアント ソフトウェアを取得します。

シスコシステムズの 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了です。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
Cisco AnyConnect ソフトウェア クライアント用の SSL VPN の設定	第 5 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 5 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
サイトツーサイト VPN の設定	第 7 章「シナリオ：サイトツーサイト VPN の設定」