



# シナリオ：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。

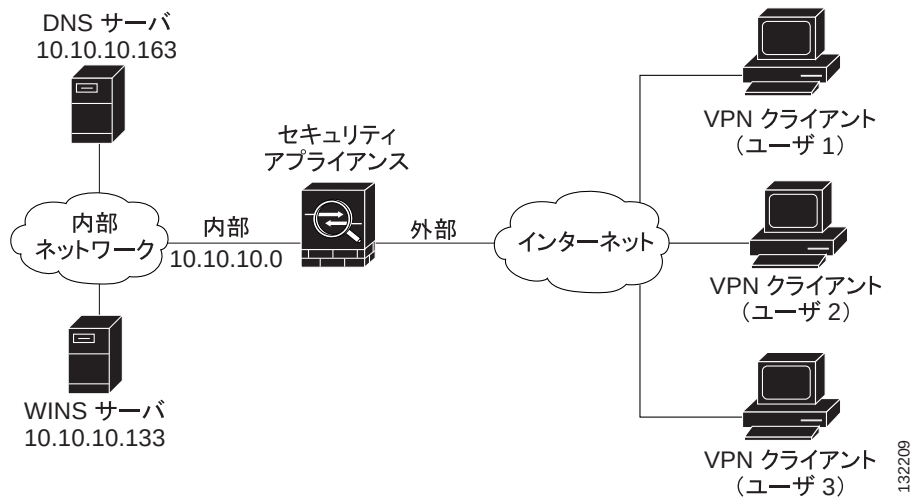
この章は、次の項で構成されています。

- [IPsec リモートアクセス VPN ネットワーク トポロジの例 \(P.7-2\)](#)
- [IPsec リモートアクセス VPN のシナリオの実装 \(P.7-3\)](#)
- [次の手順 \(P.7-22\)](#)

## 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 は、インターネット経由で VPN クライアント（Cisco Easy VPN 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 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



132209

## IPsec リモートアクセス VPN のシナリオの実装

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 7-1](#) 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 \(P.7-4\)](#)
- [ASDM の起動 \(P.7-4\)](#)
- [IPsec リモートアクセス VPN 用の FWSM の設定 \(P.7-6\)](#)
- [VPN クライアント タイプの選択 \(P.7-7\)](#)
- [VPN トンネル グループ名と認証方式の指定 \(P.7-8\)](#)
- [ユーザ認証方式の指定 \(P.7-10\)](#)
- [\(オプション\) ユーザ アカウントの設定 \(P.7-12\)](#)
- [アドレス プールの設定 \(P.7-13\)](#)
- [クライアント アトリビュートの設定 \(P.7-15\)](#)
- [IKE ポリシーの設定 \(P.7-17\)](#)
- [IPsec 暗号化および認証パラメータの設定 \(P.7-18\)](#)
- [アドレス変換の例外とスプリット トンネリングの指定 \(P.7-19\)](#)
- [リモートアクセス VPN の設定の確認 \(P.7-21\)](#)

## 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 プールで使用する 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す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

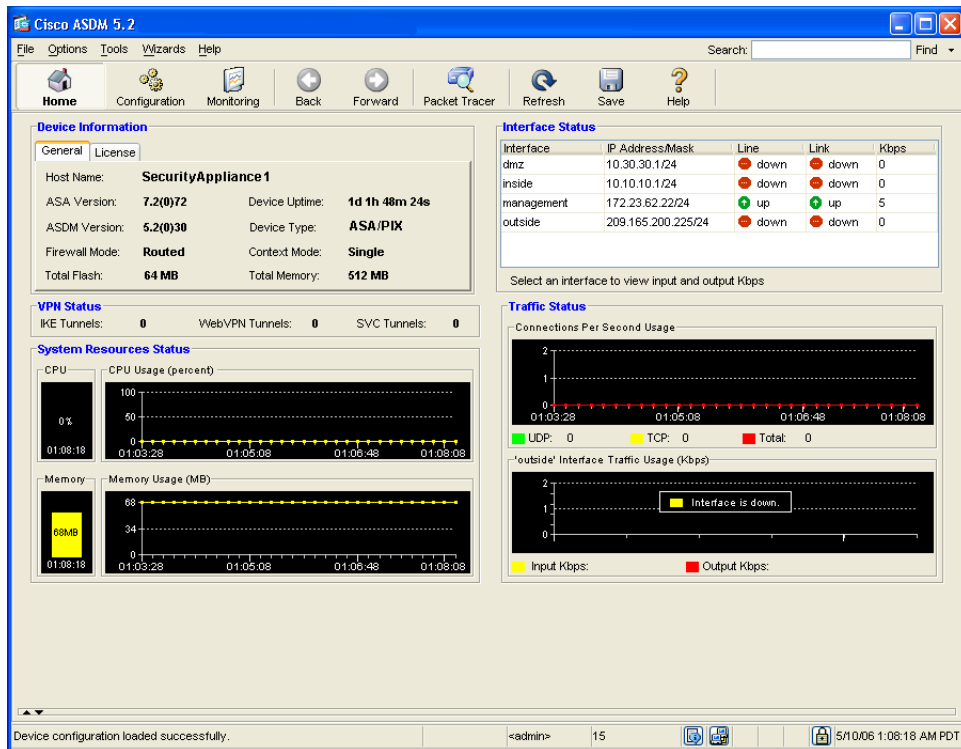
## ASDM の起動

ASDM を Web ブラウザで実行するには、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/** を入力します。



**(注)** 「s」を追加して「https」にすることに注意してください。追加しないと、接続が失敗します。HTTPS（HTTP over SSL）は、ブラウザと適応型セキュリティ アプライアンスとの間でセキュアな接続を提供します。

ASDM のメイン ウィンドウが表示されます。



153891

## IPsec リモートアクセス VPN 用の FWSM 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** ASDM のメイン ウィンドウの Wizards ドロップダウン メニューで、**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。

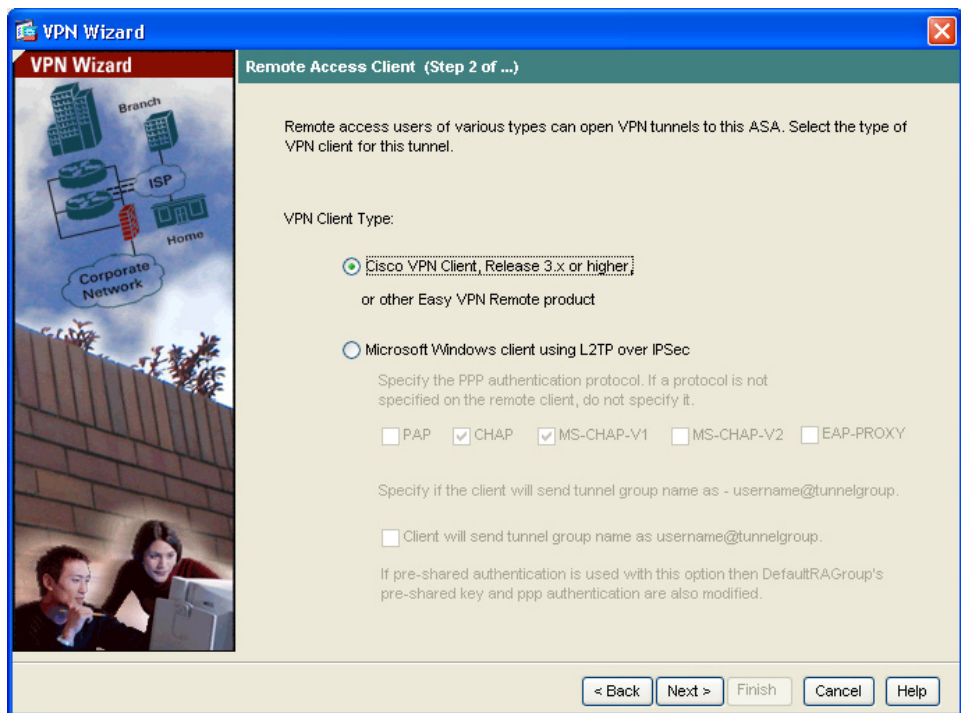
- a. **Remote Access VPN** オプション ボタンをクリックします。
- b. ドロップダウン リストで、着信 VPN トンネルに対してイネーブルにするインターフェイスとして **Outside** を選択します。
- c. **Next** をクリックして続行します。

## 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。

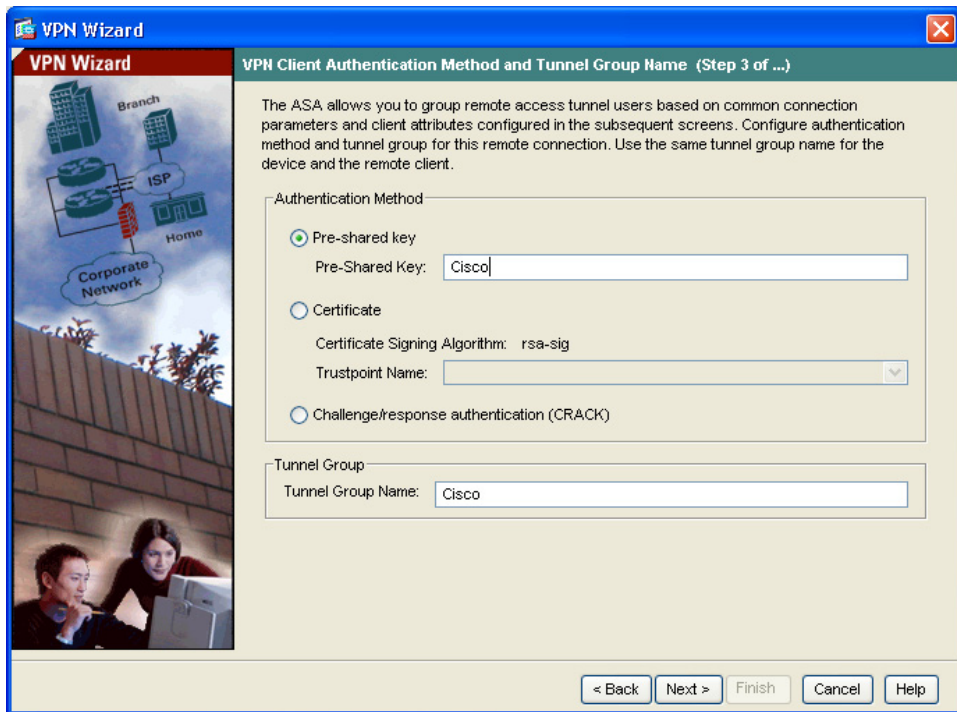
## VPN トンネル グループ名と認証方式の指定

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、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 画面を使用して、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、アカウントイング（AAA）サーバ（RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP）で認証できます。

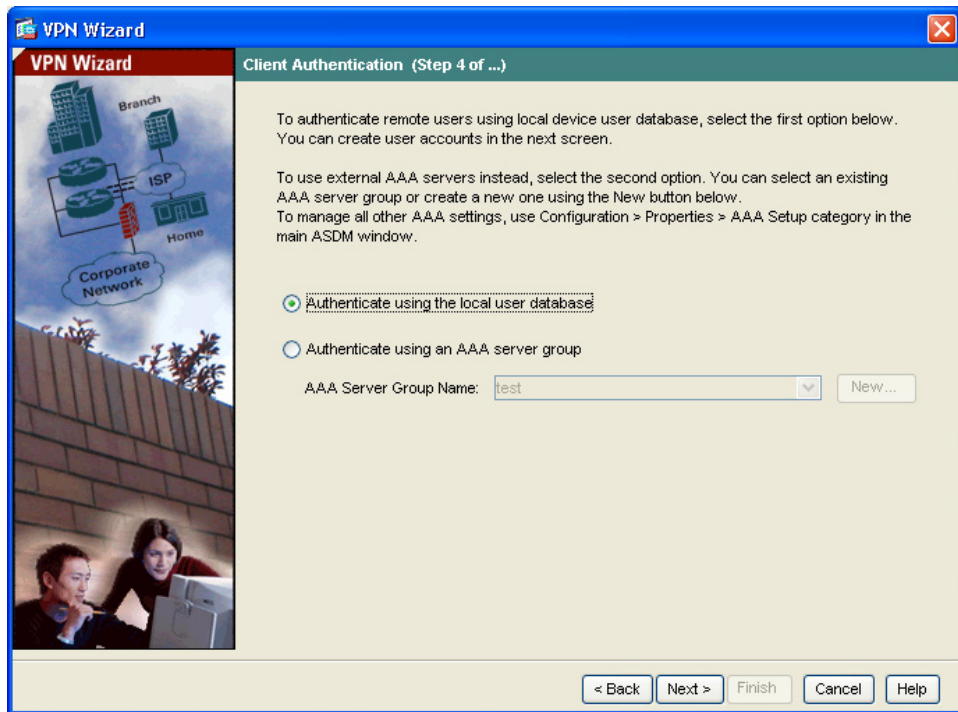
VPN Wizard の Step 4 で、次の手順を実行します。

---

**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. ドロップダウン リストで、事前設定済みのサーバ グループを選択します。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。



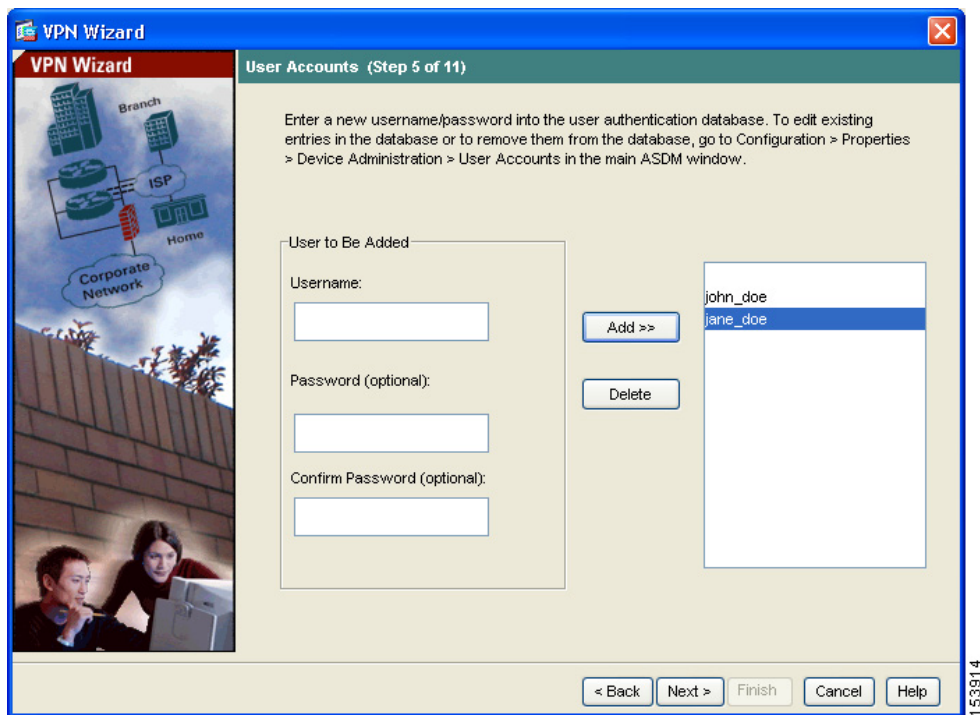
**ステップ 3**   **Next** をクリックして続行します。

## (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

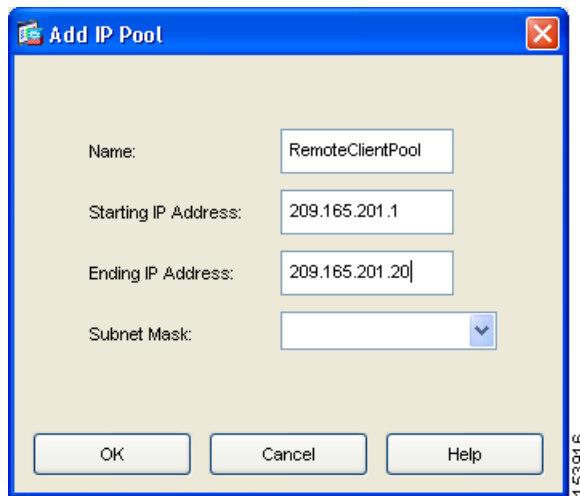
リモート クライアントがネットワークにアクセスできるようにするには、正常に接続したときにリモート VPN クライアントに割り当てることができる IP アドレスのプールを設定する必要があります。このシナリオでは、IP アドレス 209.165.201.1 ～ 209.166.201.20 を使用するようにプールを設定します。

VPN Wizard の Step 6 で、次の手順を実行します。

**ステップ 1** 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。

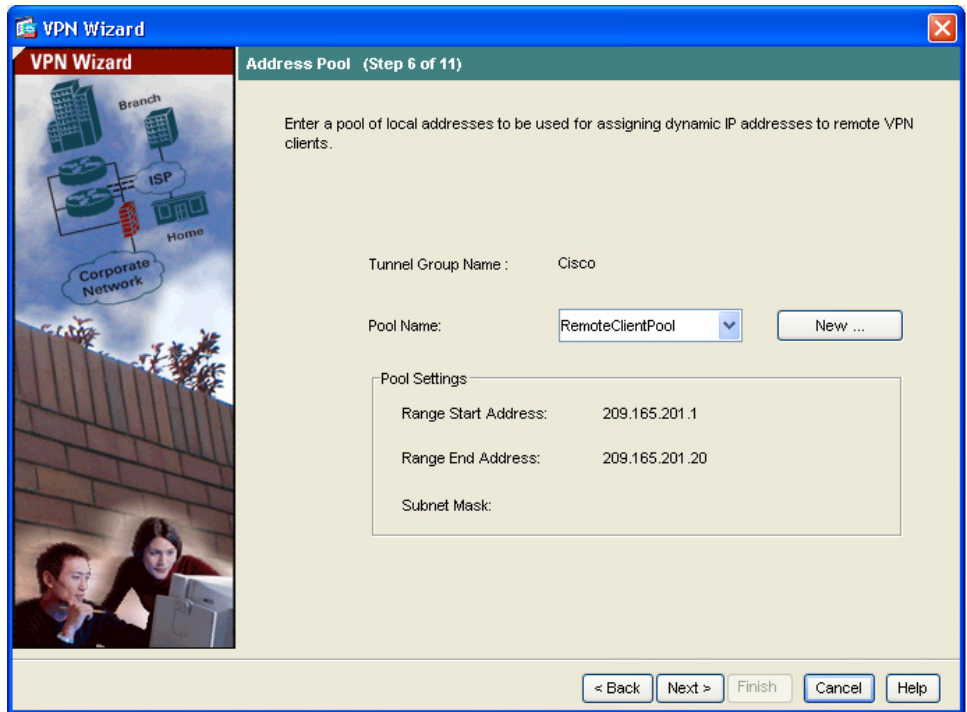
Add IP Pool ダイアログボックスが表示されます。



**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) IP アドレスの範囲のネットマスクを入力します。
- c. **OK** をクリックして、VPN Wizard の Step 6 に戻ります。

## ■ IPsec リモートアクセス VPN のシナリオの実装



**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

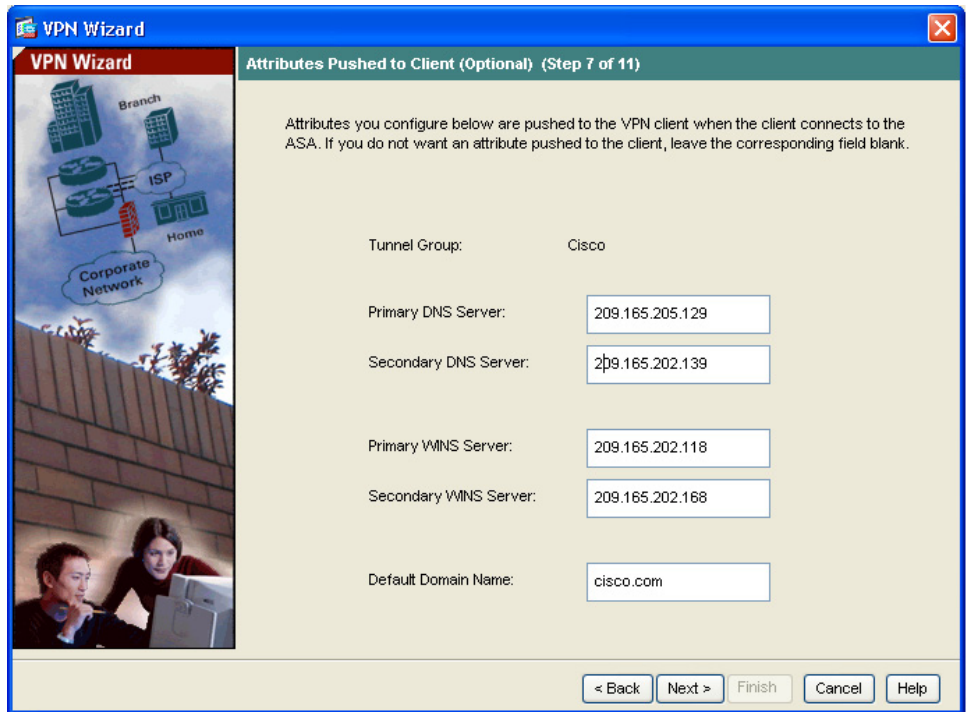
ネットワークにアクセスするには、各リモート アクセス クライアントに基本ネットワーク設定情報（使用する DNS サーバおよび WINS サーバ、デフォルトドメイン名など）が必要です。各リモート クライアントを個別に設定する代わりに、ASDM にクライアント情報を入力できます。適応型セキュリティ アプライアンスは、接続が確立されたときに、この情報をリモート クライアントまたは Easy VPN ハードウェア クライアントにプッシュします。

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。

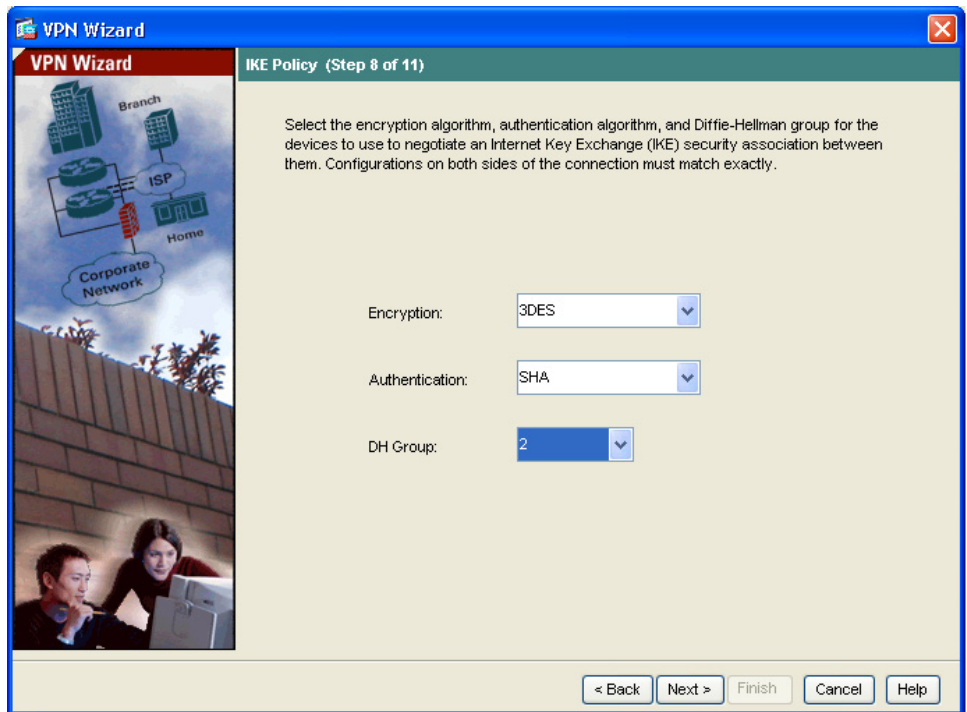


## IKE ポリシーの設定

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、5、または 7）をクリックします。



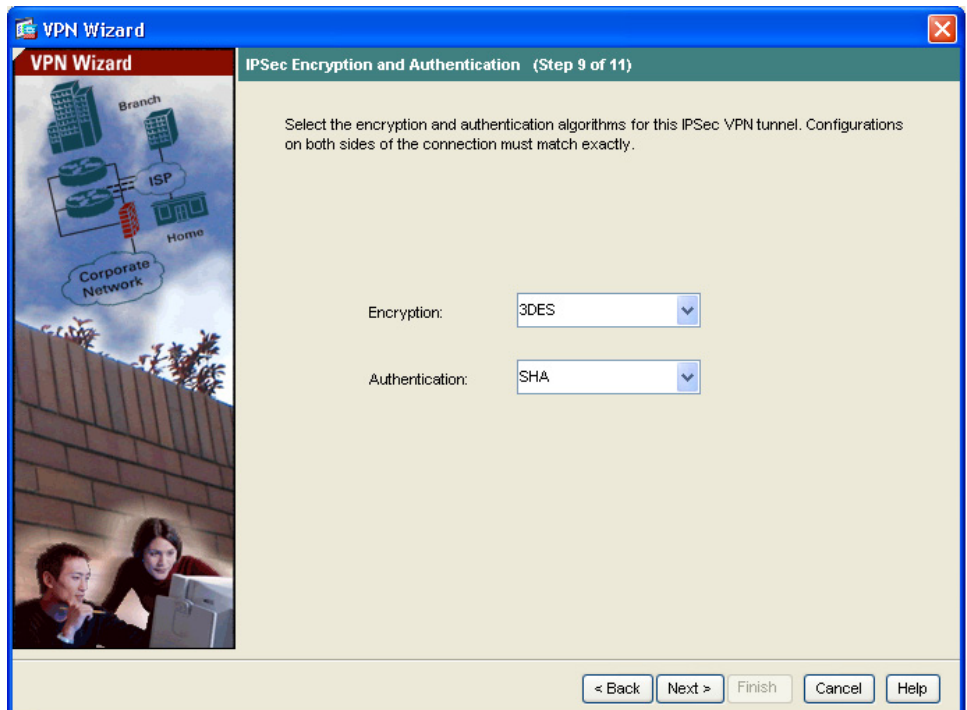
153918

**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 トンネルに誘導したり、クリア テキスト形式でネットワーク インターフェイスに誘導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（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）。

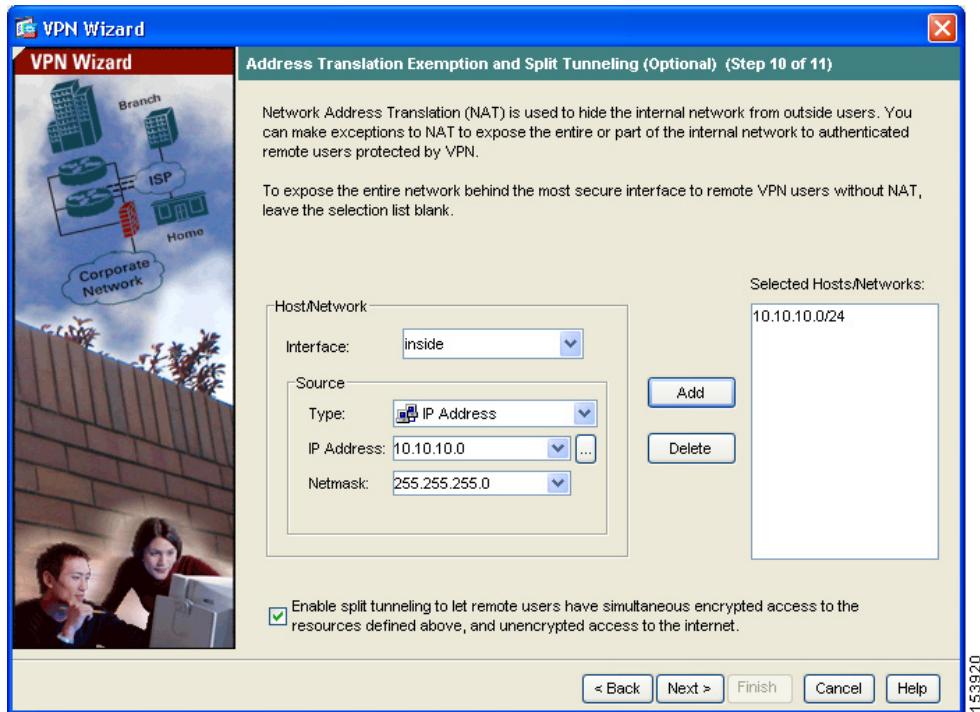
VPN Wizard の Step 10 で、次の手順を実行します。

---

**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 Hosts/Networks ペインのホスト、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。

## ■ IPsec リモートアクセス VPN のシナリオの実装



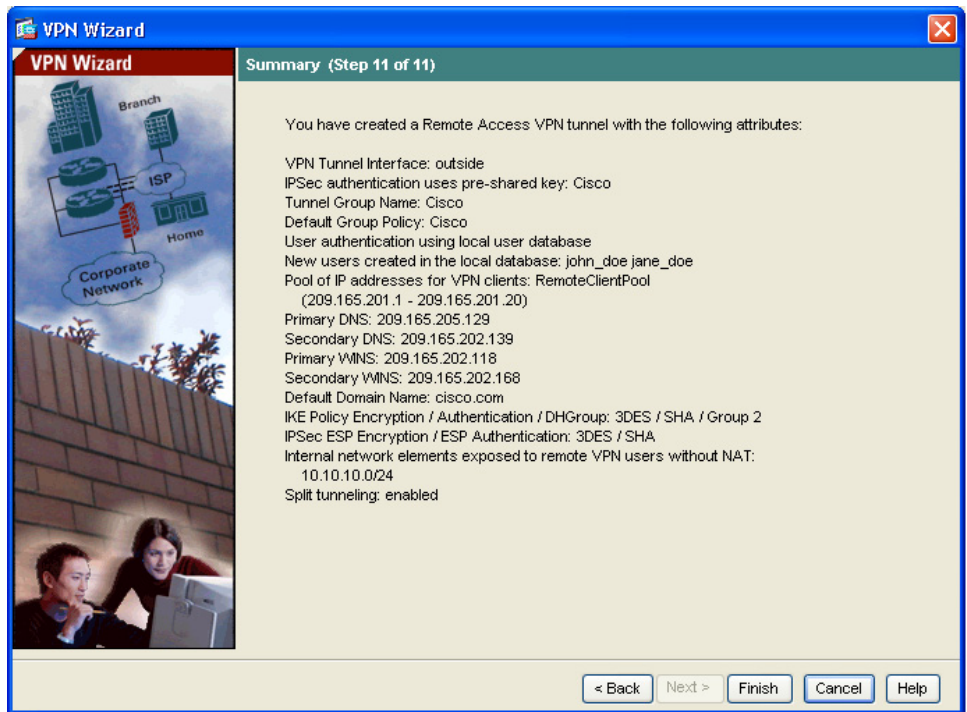
(注)

画面の下部にある **Enable split tunneling** チェックボックスをオンして、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、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、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

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         | <i>Cisco Security Appliance Command Line Configuration Guide</i>                                                                       |
| 日常のオペレーションの学習                    | <i>Cisco Security Appliance Command Reference</i><br><br><i>Cisco Security Appliance Logging Configuration and System Log Messages</i> |
| 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 | <i>Cisco ASA 5500 Series Hardware Installation Guide</i>                                                                               |

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」 |