CHAPTER 7

シナリオ：サイトツーサイト 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サイトツーサイト VPN を作成する方法について説明します。

適応型セキュリティ アプライアンスが提供するサイトツーサイト VPN 機能を使用すると、ネットワーク セキュリティを維持しながら、低コストな公衆インターネット接続で、ビジネス ネットワークを世界中のビジネス パートナーおよびリモート オフィスに拡張できます。VPN 接続を使用すると、あるロケーションから別のロケーションに、セキュアな接続（トンネル）でデータを送信できます。まず、接続の両端が認証され、次に、2 つのサイト間で送信されるすべてのデータが自動的に暗号化されます。

この章には、次の項があります。

サイトツーサイト VPN ネットワーク トポロジの例

図 7-1 に、2 台の適応型セキュリティ アプライアンス間の VPN トンネルの例を示します。

図 7-1　サイトツーサイト VPN の設定シナリオのネットワーク レイアウト

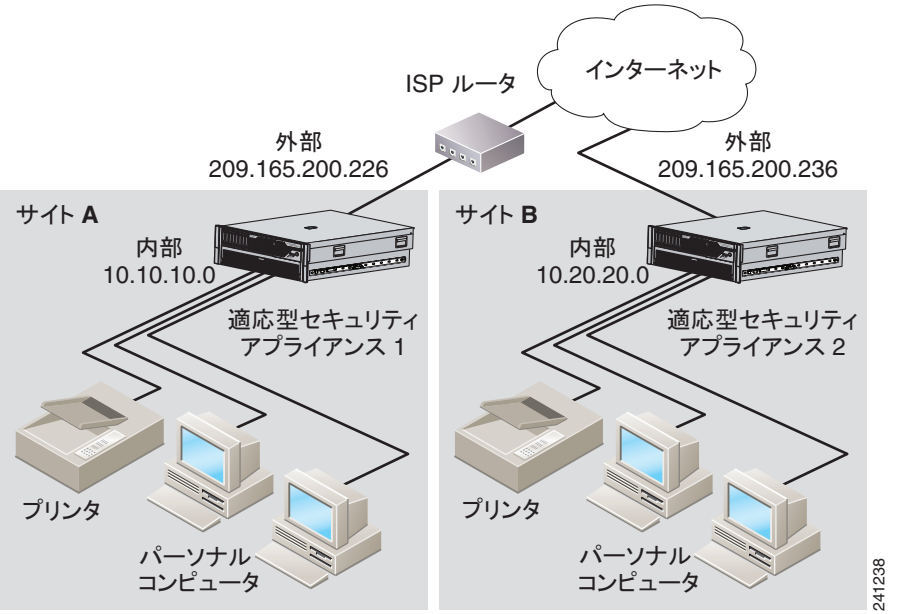


図 7-1 のような VPN サイトツーサイト配置を作成にするには、2 台の適応型セキュリティ アプライアンスを設定する必要があります（接続のそれぞれの側に 1 台ずつ）。

サイトツーサイトのシナリオの実装

この項では、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、サイトツーサイト VPN 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について説明します。

次のトピックについて取り上げます。

必要な情報

設定手順を開始する前に、次の情報を取得します。

- リモート適応型セキュリティ アプライアンス ピアの IP アドレス
- トンネルを使用してリモート サイトのリソースと通信できるローカル ホストおよびネットワークの IP アドレス
- トンネルを使用してローカル リソースと通信できるリモート ホストおよびネットワークの IP アドレス

サイトツーサイト VPN の設定

この項では、ASDM VPN Wizard を使用してサイトツーサイト VPN 用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。

次のトピックについて取り上げます。

次の項では、各設定手順の実行方法について詳しく説明します。

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.4-5 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.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。

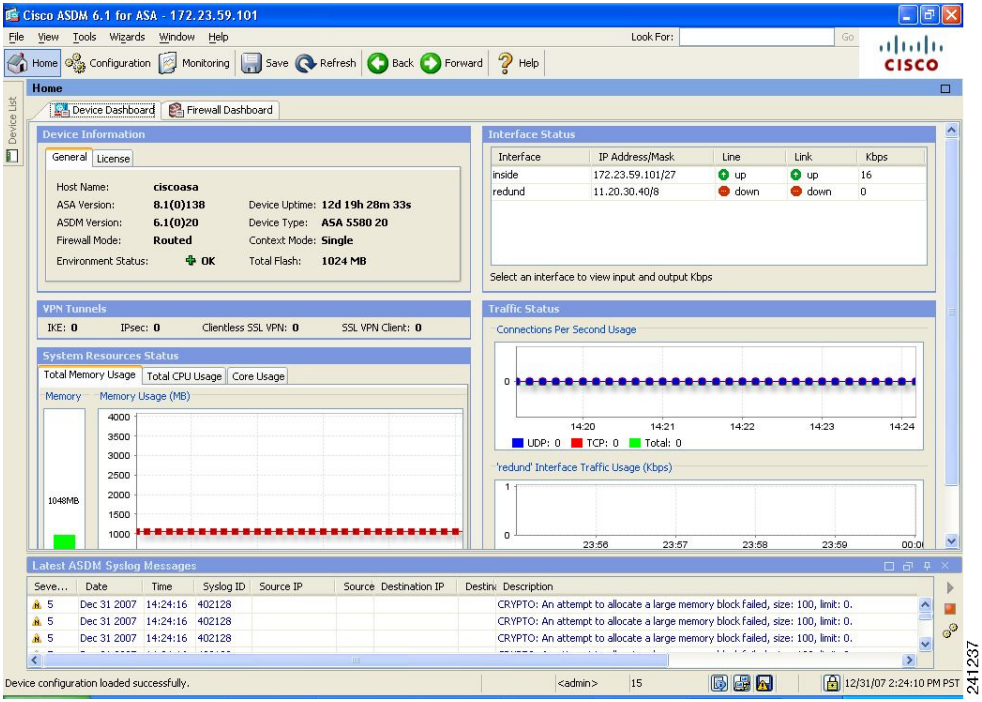
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

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。

ASA 5580 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。



ローカル サイトでの適応型セキュリティ アプライアンスの設定

（注）　このシナリオでは、最初のサイトの適応型セキュリティ アプライアンスをセキュリティ アプライアンス 1 と呼びます。

セキュリティ アプライアンス 1 を設定するには、次の手順を実行します。

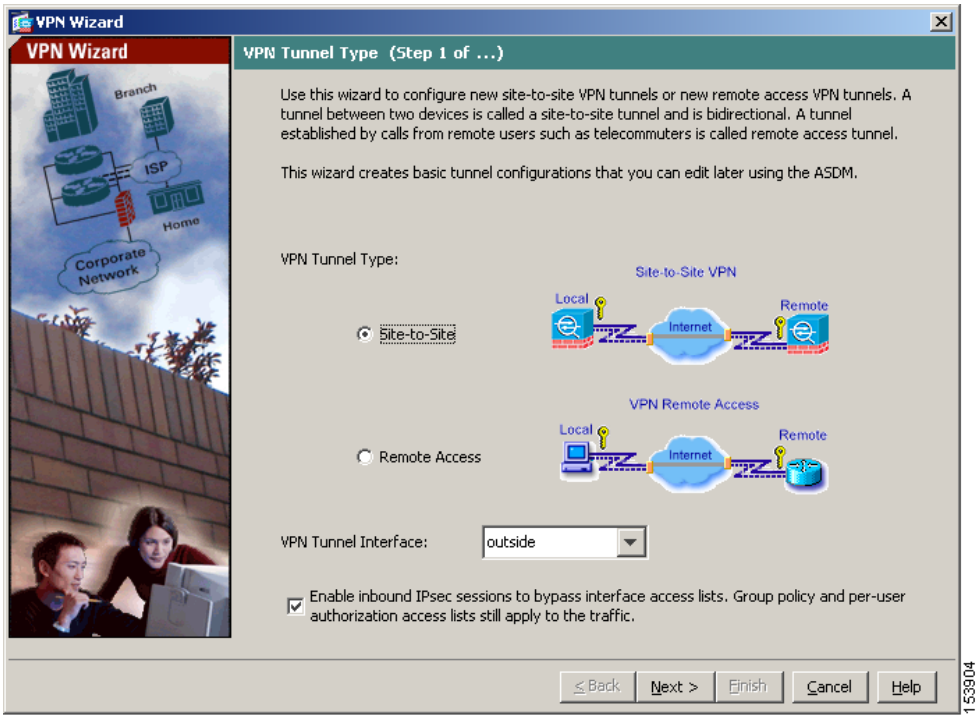
ステップ 1　ASDM のメイン ウィンドウで、Wizards ドロップダウン リストから **IPsec VPN Wizard** オプションを選択します。最初の VPN Wizard 画面が表示されます。

VPN Wizard の Step 1 で、次の手順を実行します。

a. VPN Tunnel Type 領域で、**Site-to-Site** オプション ボタンをクリックします。

（注）　Site-to-Site VPN オプションは、2 つの IPsec セキュリティ ゲートウェイを接続します。これには、適応型セキュリティ アプライアンス、VPN コンセントレータ、またはサイトツーサイト IPsec 接続をサポートするその他のデバイスが含まれます。

b. VPN Tunnel Interface ドロップダウン リストから、現在の 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。

リモート VPN ピアに関する情報の入力

VPN ピアは、設定している接続の反対側にあるシステムで、通常、リモート サイトにあります。

（注） このシナリオでは、リモート VPN ピアをセキュリティ アプライアンス 2 と呼びます。

VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　Peer IP Address（セキュリティ アプライアンス 2 の IP アドレス。このシナリオでは 209.165.200.236）と、Tunnel Group Name（「Cisco」など）を入力します。

ステップ 2　次のいずれかの手順を選択して、使用する認証の種類を指定します。

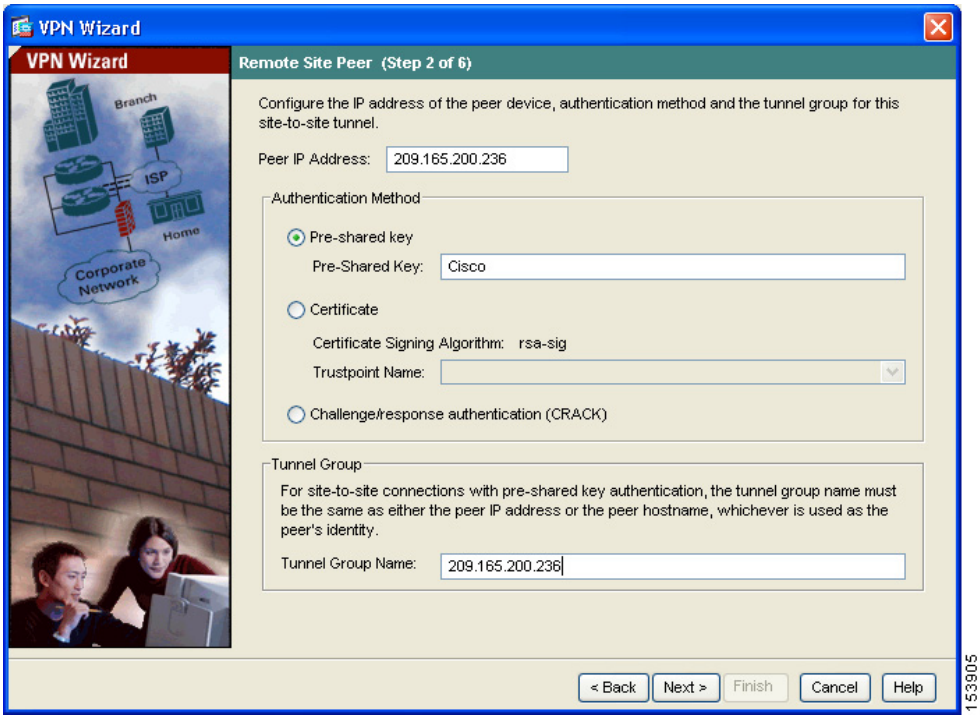
- 認証にスタティックな事前共有キーを使用するには、**Pre-Shared Key** オプション ボタンをクリックし、事前共有キー（「Cisco」など）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPsec ネゴシエーションに使用されます。

  （注）　事前共有キーの認証を使用する場合、トンネル グループ名はピアの IP アドレスにする必要があります。

- 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、Certificate Signing Algorithm 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 Trustpoint Name 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 画面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。



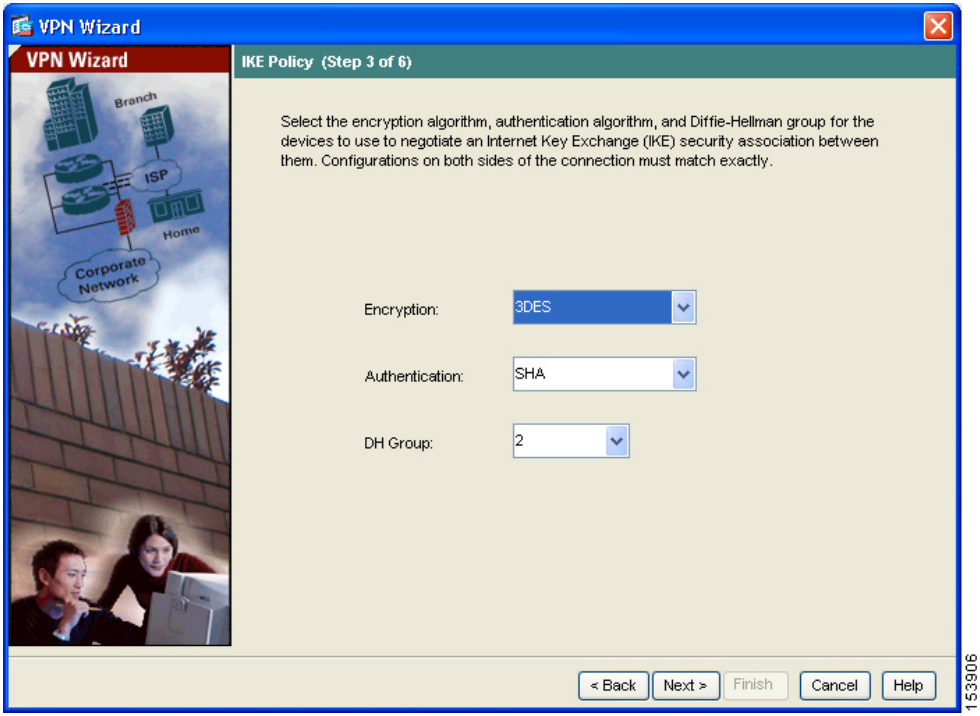
ステップ 3　**Next** をクリックして続行します。

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、2 つのピア間でセキュアな VPN トンネルを確立できます。

VPN Wizard の Step 3 で、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）をクリックします。



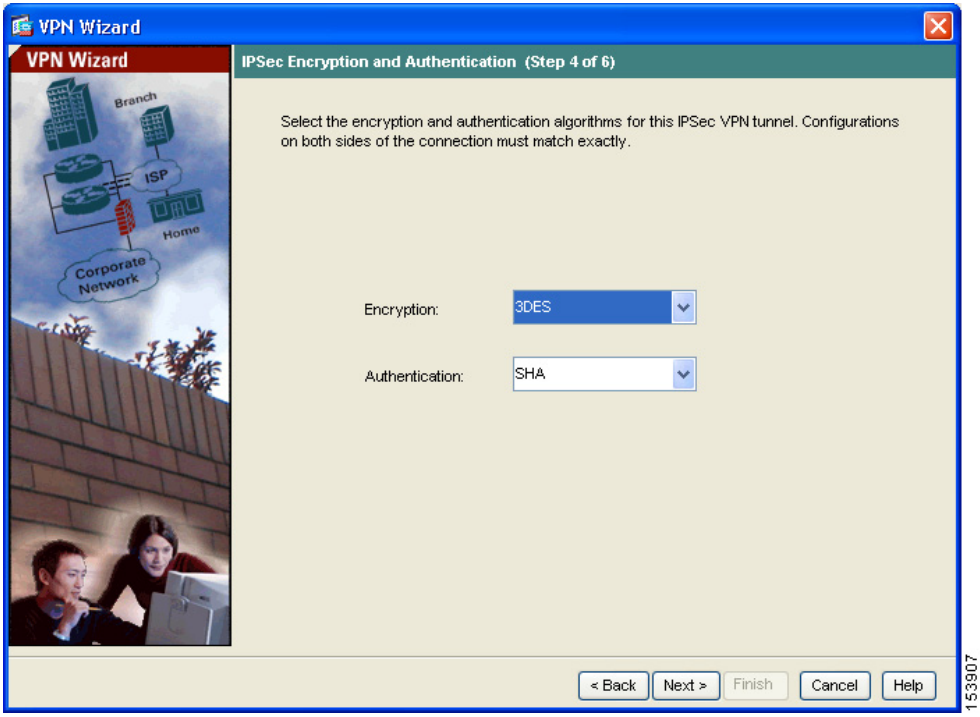
（注）　セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1 で選択した各オプションの値を正確に入力する必要があります。暗号化の不一致は、VPN トンネル障害の一般的な原因であり、設定プロセスの遅れにつながります。

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 4 で、次の手順を実行します。

ステップ 1　Encryption ドロップダウン リストから暗号化アルゴリズム（DES、3DES、または AES）を選択し、Authentication ドロップダウン リストから認証アルゴリズム（MD5 または SHA）を選択します。



ステップ 2　**Next** をクリックして続行します。

ホストおよびネットワークの指定

この IPsec トンネルを使用してトンネルの反対側のホストおよびネットワークと通信できるローカル サイトのホストおよびネットワークを指定します。**Add** または **Delete** をクリックして、トンネルにアクセスできるホストおよびネットワークを指定します。現在のシナリオでは、Network A（10.10.10.0）からのトラフィックはセキュリティ アプライアンス 1 で暗号化され、VPN トンネルを使用して送信されます。

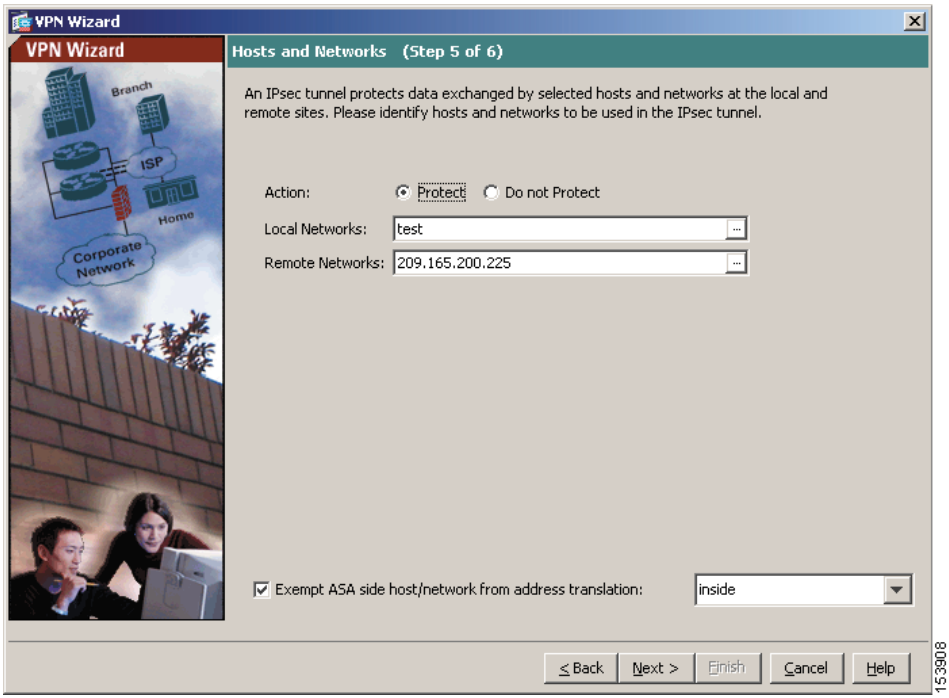
さらに、この IPsec トンネルを使用してローカル ホストおよびネットワークにアクセスできるリモート サイトのホストおよびネットワークを指定します。ホストおよびネットワークを動的に追加または削除するには、それぞれ、**Add** または **Delete** をクリックします。このシナリオでは、セキュリティ アプライアンス 1 のリモート ネットワークは Network B（10.20.20.0）なので、このネットワークからの暗号化されたトラフィックは、トンネルを使用できます。

VPN Wizard の Step 5 で、次の手順を実行します。

ステップ 1　Action 領域で、**Protect** オプション ボタンまたは **Do not Protect** オプション ボタンをクリックします。

ステップ 2　保護する、または保護を解除するローカル ネットワークの IP アドレスを入力するか、省略（**...**）ボタンをクリックしてホストとネットワークのリストから選択します。

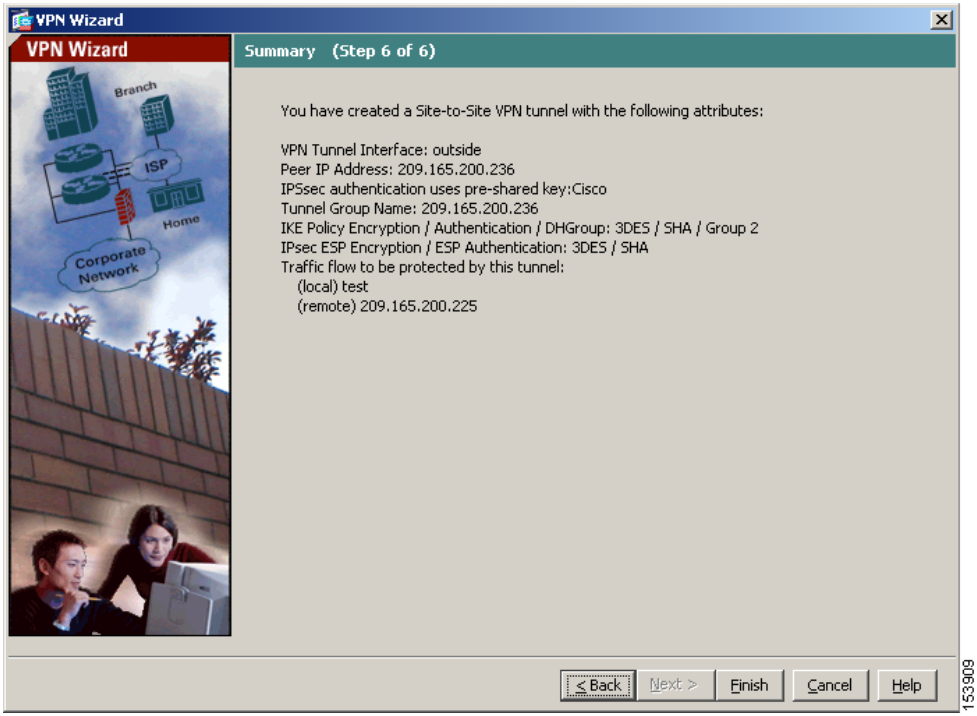
ステップ 3　保護する、または保護を解除するリモート ネットワークの IP アドレスを入力するか、省略（**...**）ボタンをクリックしてホストとネットワークのリストから選択します。



ステップ 4　**Next** をクリックして続行します。

VPN アトリビュートの確認とウィザードの完了

VPN Wizard の Step 6 で、ここで作成した VPN トンネルの設定リストを確認します。



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。

これで、セキュリティ アプライアンス 1 の設定プロセスは終了です。

VPN 接続の反対側の設定

これで、ローカルな適応型セキュリティ アプライアンスが設定されました。次に、リモート サイトの適応型セキュリティ アプライアンスを設定する必要があります。

リモート サイトでは、VPN ピアとして機能するように、2 番目の適応型セキュリティ アプライアンスを設定します。ローカルな適応型セキュリティ アプライアンスの設定手順のうち、P.7-6 の「ローカル サイトでの適応型セキュリティ アプライアンスの設定」から P.7-14 の「VPN アトリビュートの確認とウィザードの完了」までを使用します。

（注） セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1 で選択した各オプション（ローカル ホストおよびネットワークは除く）と同じ値を使用する必要があります。VPN の設定が失敗する一般的な原因は、不整合です。

次の手順

サイトツーサイト 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 6 章「シナリオ：SSL VPN クライアントレス接続」
リモート アクセス VPN の設定	第 8 章「シナリオ：IPsec リモート アクセス VPN の設定」