CHAPTER 8

シナリオ：サイトツーサイト 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、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 アプライアンスに備わっているサイトツーサイト VPN 機能を使用すると、企業はネットワーク セキュリティを維持したまま、ネットワークを拡張してビジネス パートナーや世界中のリモート オフィスとの間で低コストのパブリック インターネット接続を実現できます。VPN 接続では、セキュアな接続、つまりトンネル経由で 1 つの場所から別の場所へデータを送信できます。これは、まず接続の両端を認証し、次に 2 つのサイト間で送信されるすべてのデータを自動的に暗号化することによって可能になります。

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 8-1 に、2 つ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 8-1　サイトツーサイト VPN 設定シナリオのネットワーク レイアウト

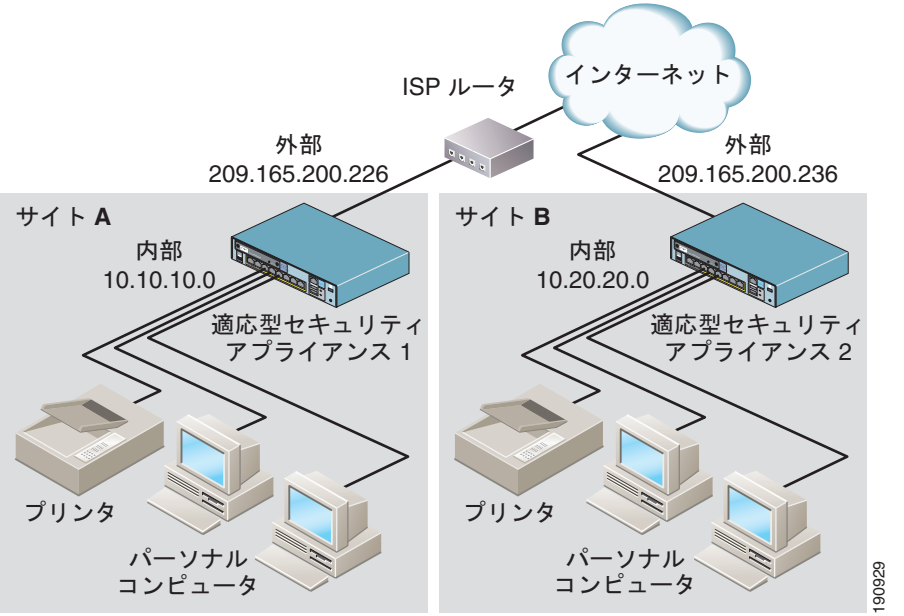


図 8-1 のような VPN サイトツーサイト構成を作成するには、2 台の適応型セキュリティ アプライアンスを設定する必要があります（接続のそれぞれの側に 1 台ずつ）。

サイトツーサイト シナリオの実装

この項では、図 8-1 に表示されているリモートアクセス 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 構成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。

この項は、次の内容で構成されています。

収集する情報

この設定手順を開始する前に、次の情報を取得します。

- リモートの適応型セキュリティ アプライアンス ピアの IP アドレス
- リモート　サイト上のリソースとの通信にトンネルを使用することが許可されたローカル ホストとネットワークの IP アドレス
- ローカル　リソースとの通信にトンネルを使用することが許可されたリモート ホストとネットワークの IP アドレス

サイトツーサイト VPN の設定

ここでは、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。

この項は、次の内容で構成されています。

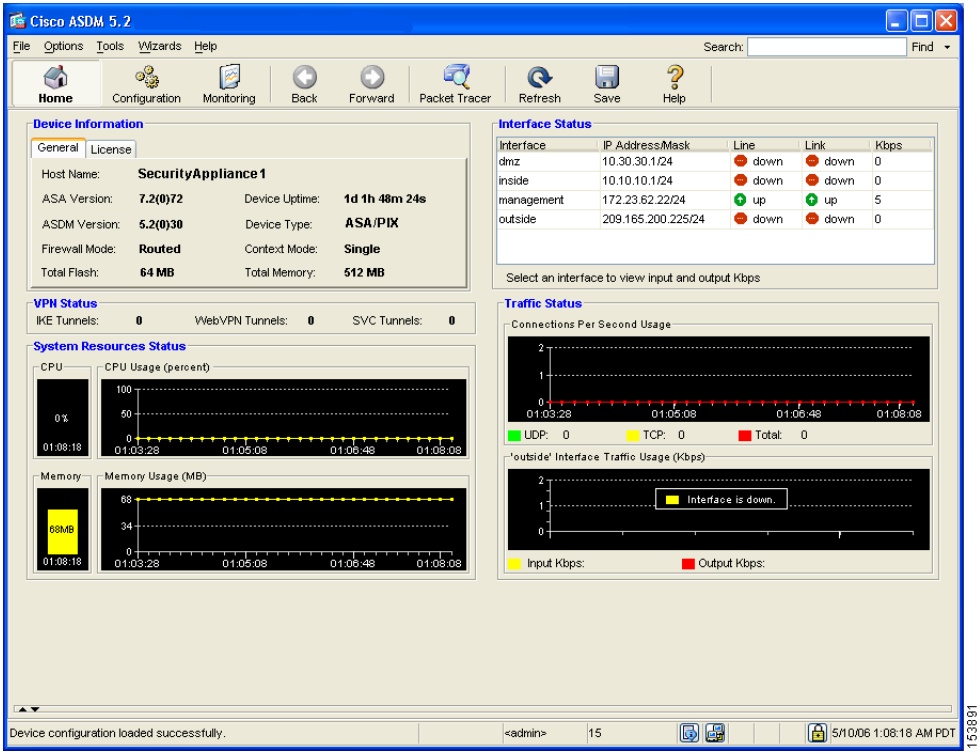
次の項では、各設定手順を実行する方法を詳細に説明します。

ASDM の起動

Web ブラウザで ASDM を実行するには、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） 「**https**」の「**s**」を付け忘れると、接続は失敗します。HTTP over SSL（HTTPS）を使用すると、ブラウザと適応型セキュリティ アプライアンスとの間の安全な接続が可能になります。

ASDM メイン ウィンドウが表示されます。



ローカル サイトでのセキュリティ 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 Security Appliance 1 と呼びます。

Security Appliance 1 を設定するには、次の手順に従います。

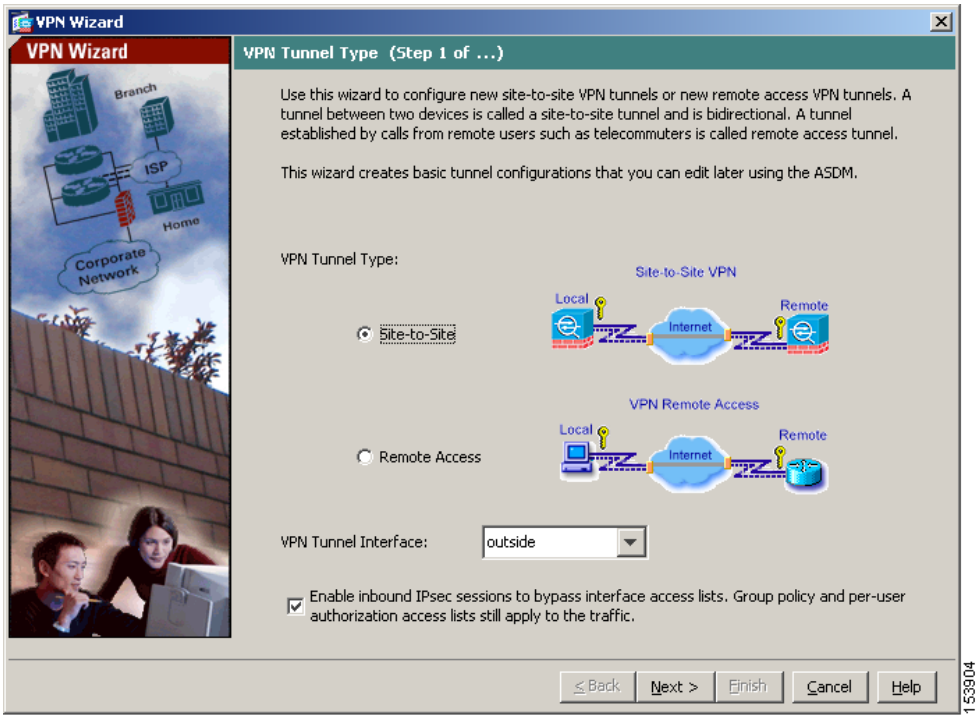
ステップ 1　ASDM メイン ウィンドウで、Wizards ドロップダウン メニューから VPN Wizard オプションを選択します。ASDM で、最初の VPN Wizard 画面が開きます。

VPN Wizard の Step 1 で、次の手順に従います。

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

（注）　Site-to-Site VPN オプションを選択すると、2 つの IPSec セキュリティ ゲートウェイが接続されますが、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る可能性があります。

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。

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もう一方の端にあるシステムで、通常はリモート 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 Security Appliance 2 と呼びます。

VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　リモートのピアの IP アドレス（209.165.200.236）およびトンネル グループ名（たとえば、「Cisco」）を入力します。

ステップ 2　次のいずれかの認証方式を選択して、使用する認証のタイプを指定します。

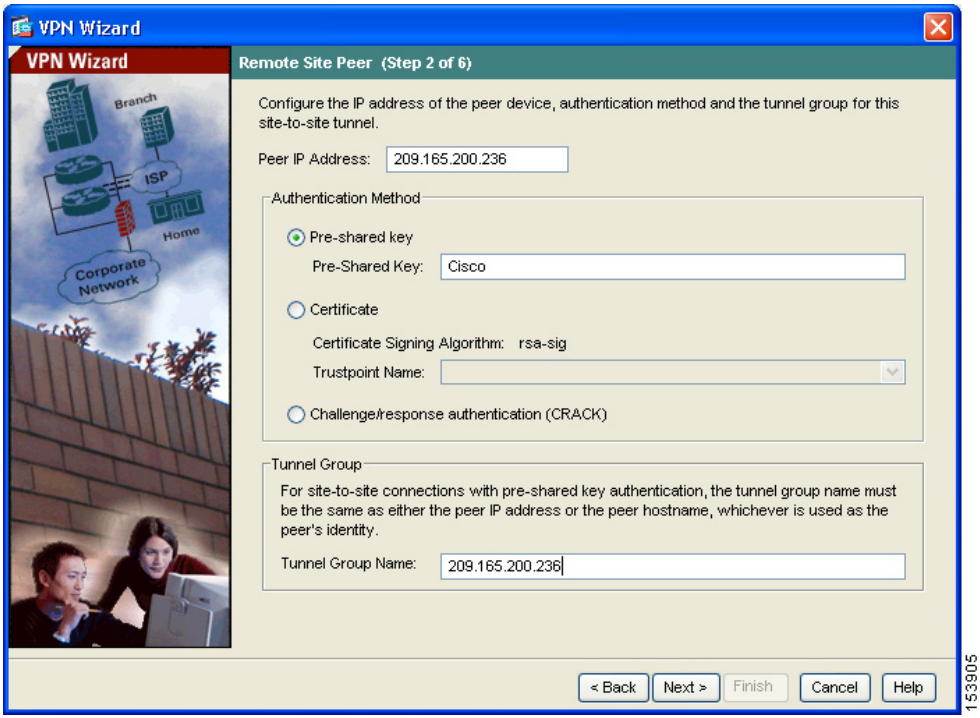
- 認証にスタティック事前共有キーを使用するには、**Pre-Shared Key** オプション ボタンをクリックし、事前共有キー（たとえば、「Cisco」）を入力します。このキーは、適応型セキュリティ アプライアンス間の IPSec ネゴシエーションで使用されます。

  （注） このシナリオのように、事前共有キー認証を使用したサイトツーサイト接続を行う場合、トンネル グループ名は、ピアの IP アドレスとピアのホスト名のうち、ピアの ID として使用されているものと同一である必要があります。

- 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、事前設定されているトラストポイント名を Trustpoint Name 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、同じ ASDM 画面を使用して後で修正できます。

- **Challenge/Response Authentication** オプション ボタンをクリックして、この認証方式を使用できます。



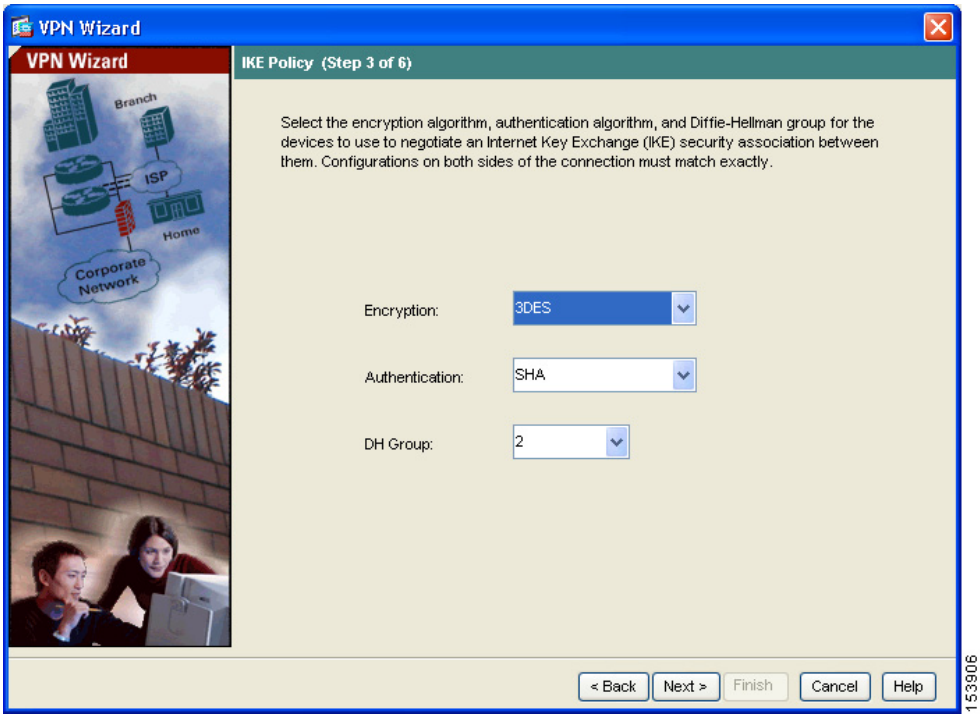
ステップ 3　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、セキュアな VPN トンネルを通じてデータの完全性を保護し、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 のデフォルト値を使用すれば、十分にセキュアな VPN トンネルを 2 つのピア間に確立できます。

VPN Wizard の Step 3 で、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、または 5）をクリックします。



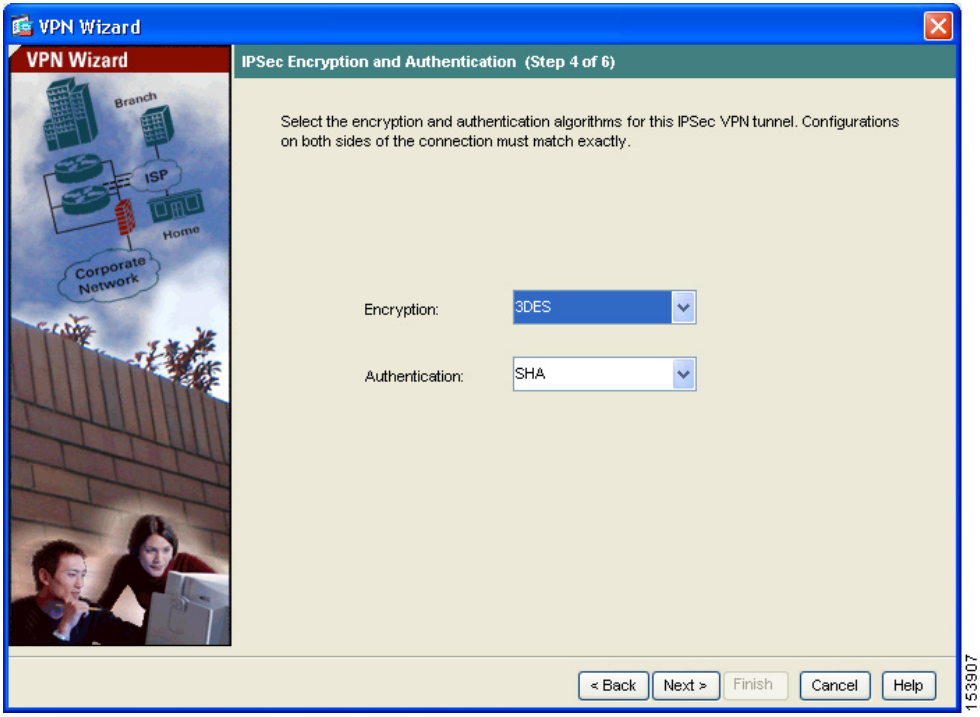
（注）　Security Appliance 2 を設定する場合は、Security Appliance 1 で選択した各オプションと同じ値を入力します。VPN トンネルが失敗し、処理速度を低下させる一般的な原因は、暗号化の不整合です。

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 4 で、次の手順に従います。

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、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

トンネルの反対側のホストおよびネットワークとの通信にこの IPSec トンネルを使用することが許可されたローカル 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、トンネルへのアクセスが許可された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、ネットワーク A（10.10.10.0）からのトラフィックは Security Appliance 1 によって暗号化され、VPN トンネル経由で送信されます。

さらに、ローカル ホストおよびネットワークへのアクセスにこの IPSec トンネルを使用することを許可するリモート 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するには **Add**、削除するには **Delete** をクリックします。このシナリオにおいて、Security Appliance 1 では、リモート ネットワークはネットワーク B（10.20.20.0）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経由で許可されます。

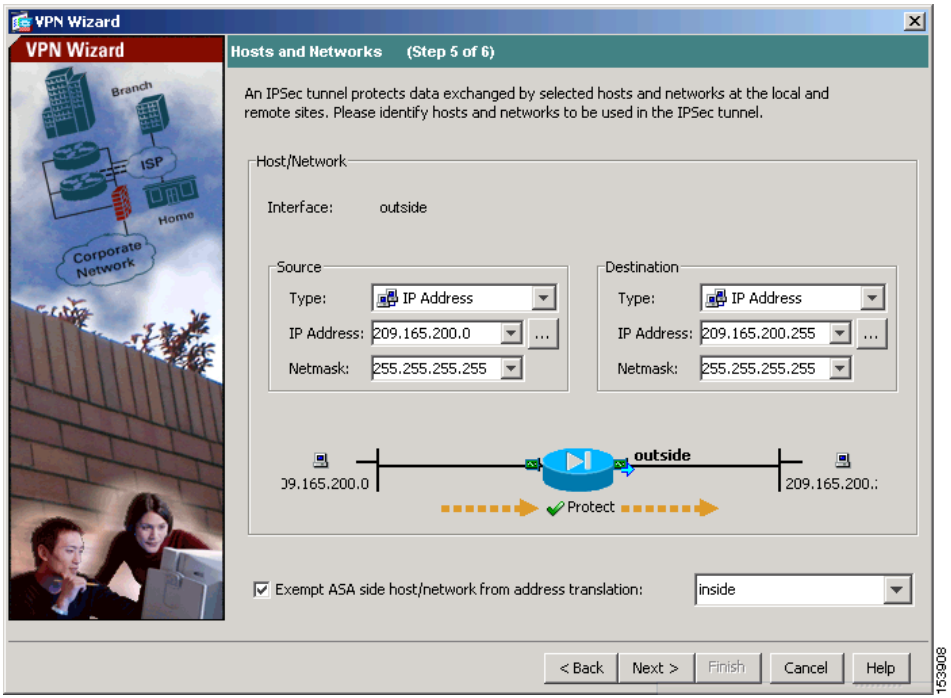
VPN Wizard の Step 5 で、次の手順に従います。

（注） ここでは、暗号化による保護により、セキュアな VPN トンネルを通じて 2 つのホスト間のデータ完全性が保たれます。あるホストから別のホストに、セキュアでない接続で暗号化されずに送信される平文の情報は、保護されていないデータと考えられます。保護されていないデータをセキュアでない接続で送信すると、データが改ざんされる可能性があります。

ステップ 1　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 2　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。

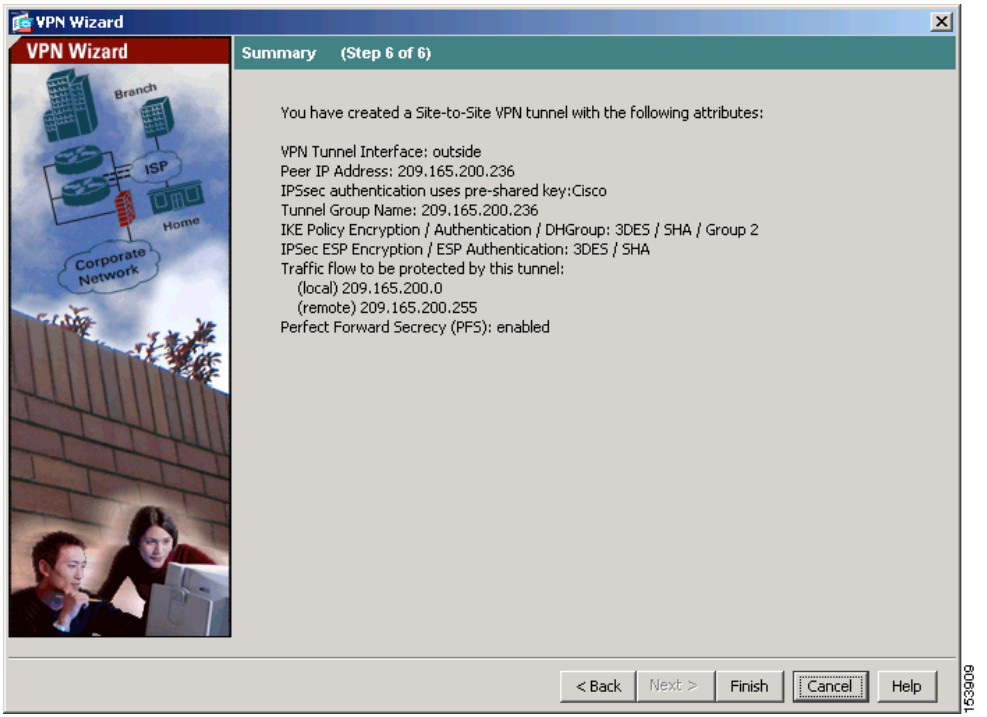
（注） リモートのピアが動的 IP アドレスを持っている場合は、ピアの IP アドレスとしてホスト名を使用できます。



ステップ 3　**Next** をクリックして続行します。

VPN アトリビュートの表示とウィザードの終了

VPN Wizard の手順 6 では、作成した VPN トンネルの設定を確認します。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。



ステップ 4　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。

この操作により、Security Appliance 1 の設定プロセスが終了します。

VPN 接続の反対側の設定

これで、ローカルの適応型セキュリティ アプライアンスの設定は完了しました。次は、リモート サイトで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 ピアとしての役割を果たす 2 つ目の適応型セキュリティ アプライアンスを設定します。ローカルの適応型セキュリティ アプライアンスを設定したときと同じ手順を使用します。「ローカル サイトでのセキュリティ アプライアンスの設定」（8-5 ページ）から開始し、「VPN アトリビュートの表示とウィザードの終了」（8-14 ページ）で終了します。

（注） Security Appliance 2 を設定する場合、ローカル ホストおよびネットワークを除いて、Security Appliance 1 で選択した各オプションと同じ値を使用します。VPN 構成が失敗する一般的な原因は、不整合です。

次の作業

サイトツーサイト 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、これで初期設定が完了しました。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」
リモートアクセス VPN の設定	第 7 章「シナリオ：IPSec リモートアクセス VPN 設定」