CHAPTER 8

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たサイトツーサイト VPN の作成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 8-1 で、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 の設定シナリオのネットワーク レイアウト

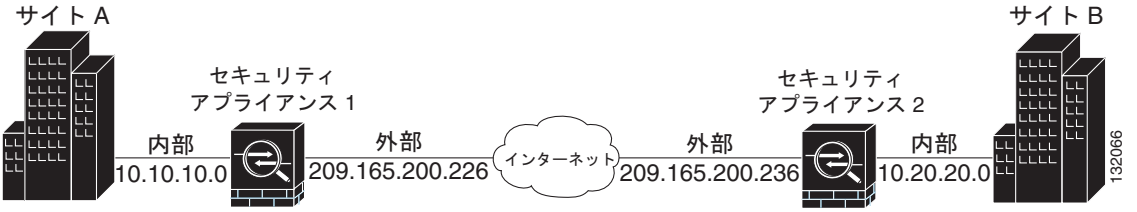


図 8-1 で示すような VPN サイトツーサイト配置の作成では、接続のそれぞれの端で 1 つずつ、合計 2 つの適応型セキュリティ アプライアンスを設定する必要があります。

サイトツーサイトのシナリオの実装

この項では、図 8-1 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を示します。

この項では次のトピックを取り上げます。

必要な情報

設定手順を開始する前に、次の情報を収集します。

- 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。

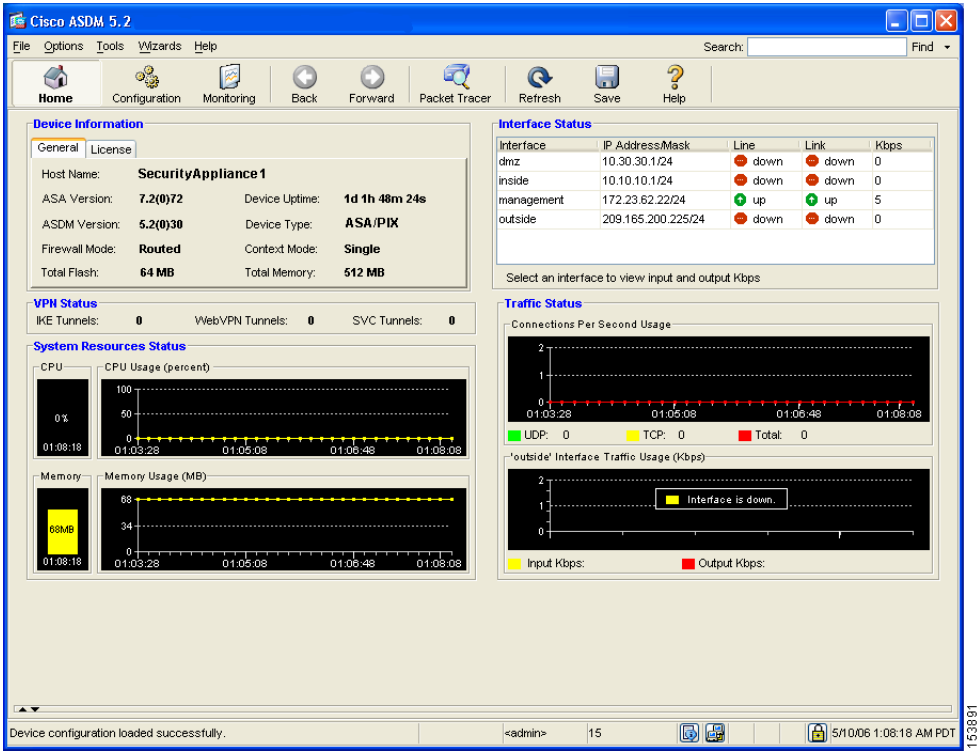
次の項では、各設定手順の実行方法について詳しく説明します。

ASDM の起動

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の 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。



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）　以後、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。

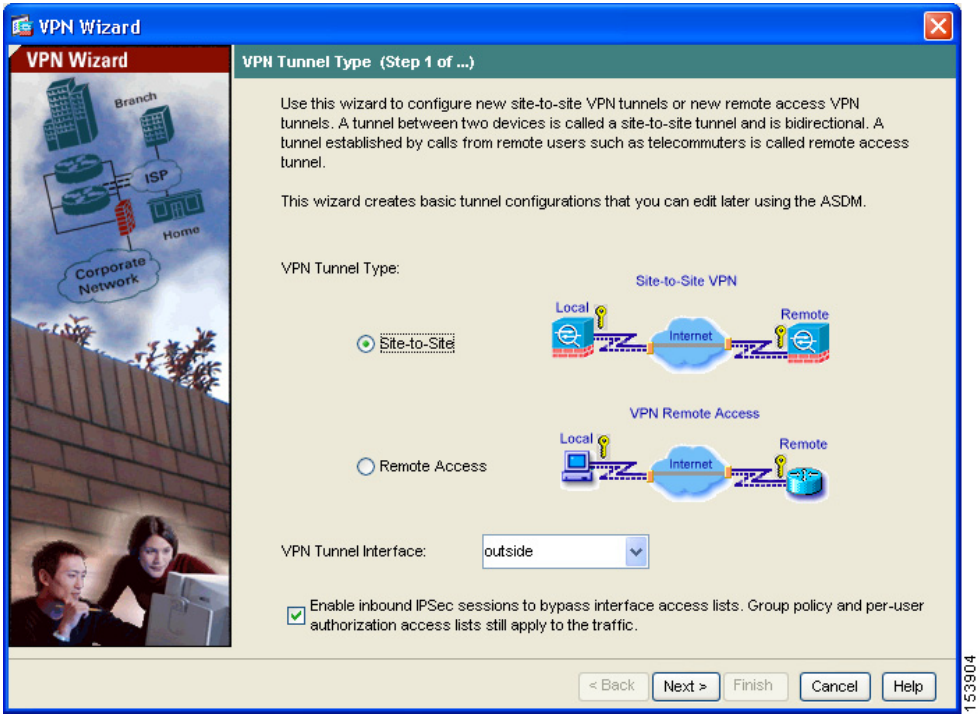
ステップ 1　ASDM のメイン ウィンドウの Wizards ドロップダウン リストで、VPN Wizard オプションを選択します。最初の VPN Wizard 画面が表示されます。

VPN Wizard の Step 1 で、次の手順を実行します。

a. **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. ドロップダウン リストで、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、以後、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。

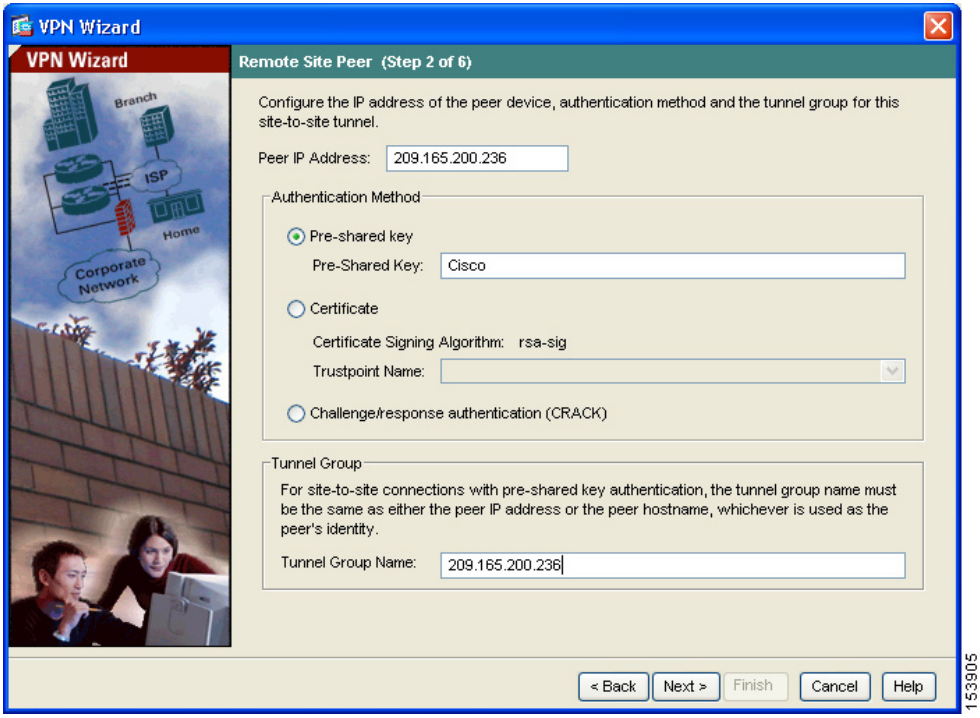
ステップ 2　次の手順のいずれかを実行して、使用する認証の種類を指定します。

- 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 ネゴシエーションで使用されます。

  （注） リモート サイトでセキュリティ アプライアンス 2 を設定するとき、VPN ピアはセキュリティ アプライアンス 1 になります。ここで使用するものと同じ事前共有キー（Cisco）を入力してください。

- **Challenge/Response Authentication** 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。
- 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。

  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。



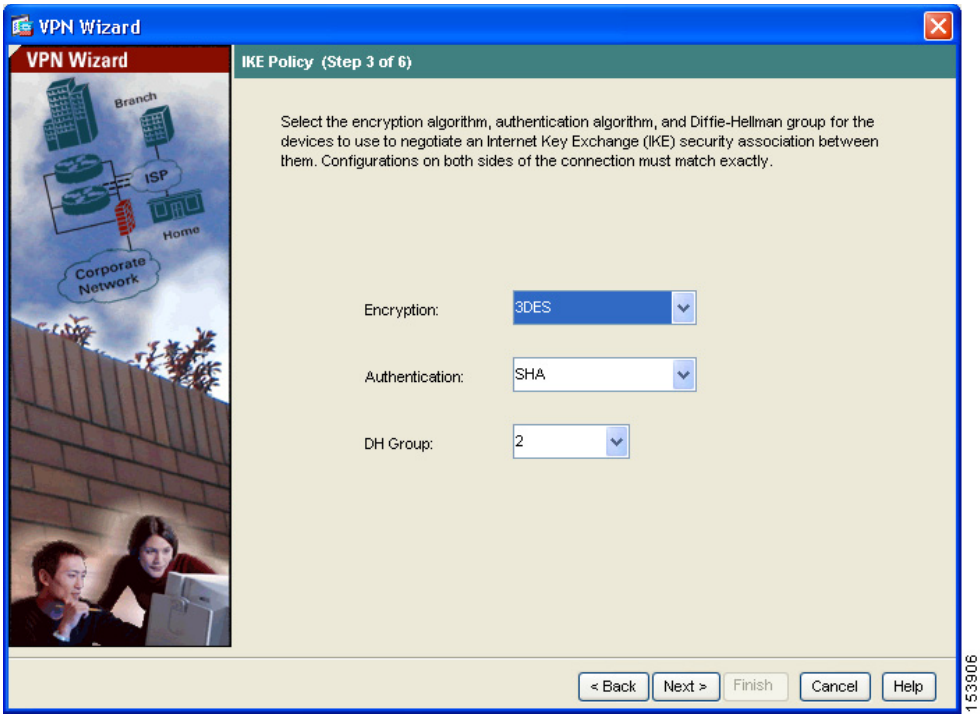
ステップ 3　**Next** をクリックして続行します。

IKE ポリシーの設定

IKE は、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、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。



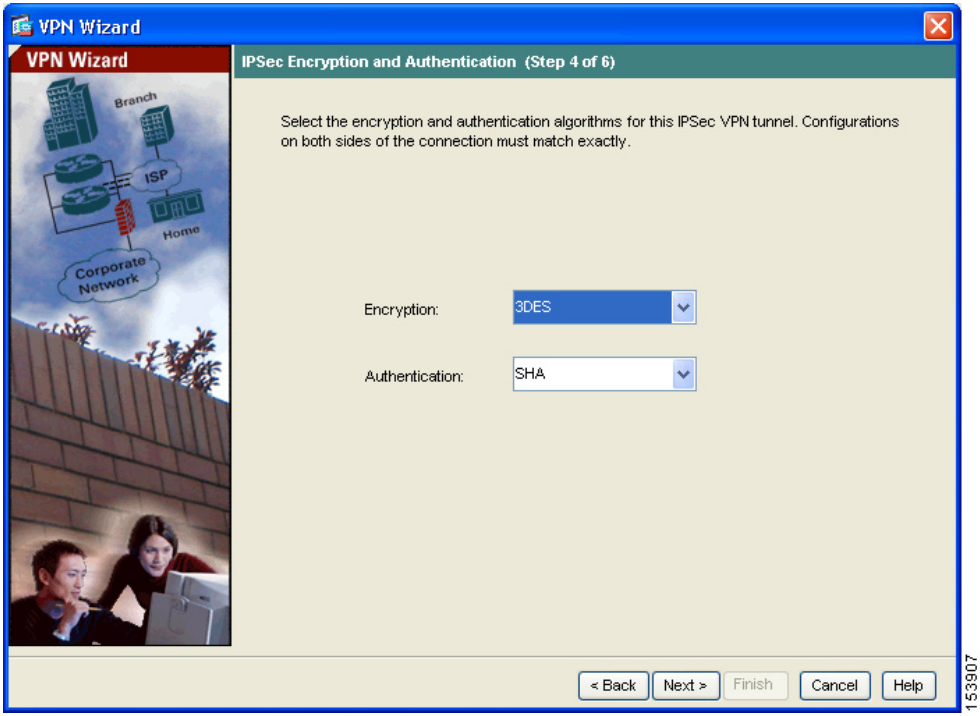
（注）　セキュリティ アプライアンス 2 を設定するときは、セキュリティ アプライアンス 1 で選択した各オプションの値を正確に入力する必要があります。暗号化の不一致は、VPN トンネル障害のよくある原因で、設定プロセスを遅らせる原因になります。

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　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）をそれぞれのドロップダウン リストから選択します。



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リモートサイト ピア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。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。

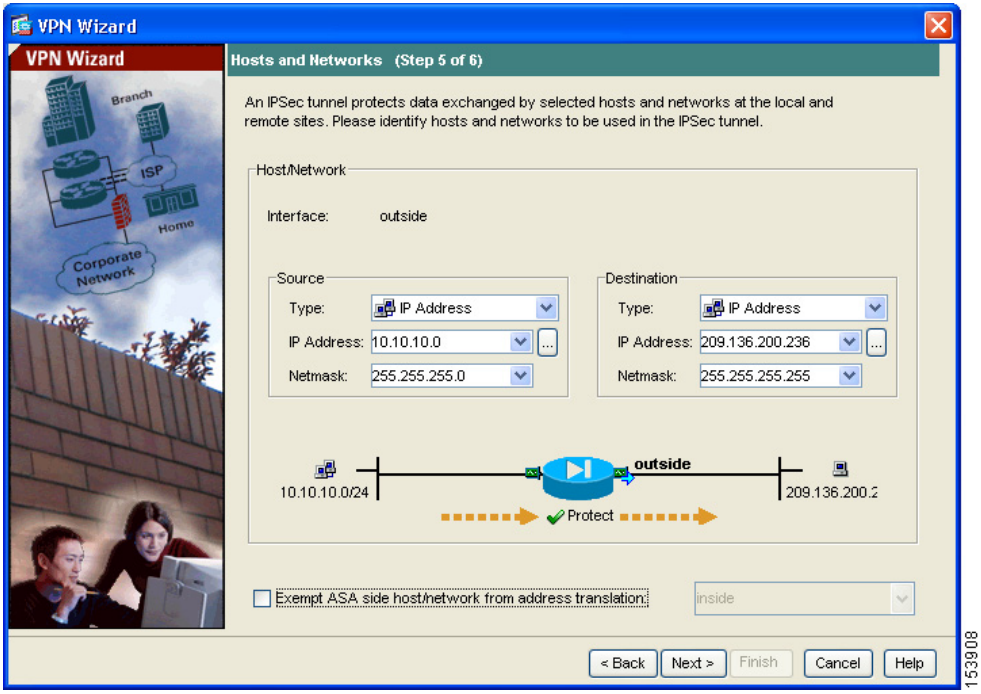
VPN Wizard の Step 5 で、次の手順を実行します。

ステップ 1　Source 領域の Type ドロップダウン リストで、IP Address を選択します。

ステップ 2　ローカル IP アドレスとネットマスクを IP Address と Netmask の各フィールドに入力します。

ステップ 3　Destination 領域の Type ドロップダウン リストで、IP Address を選択します。

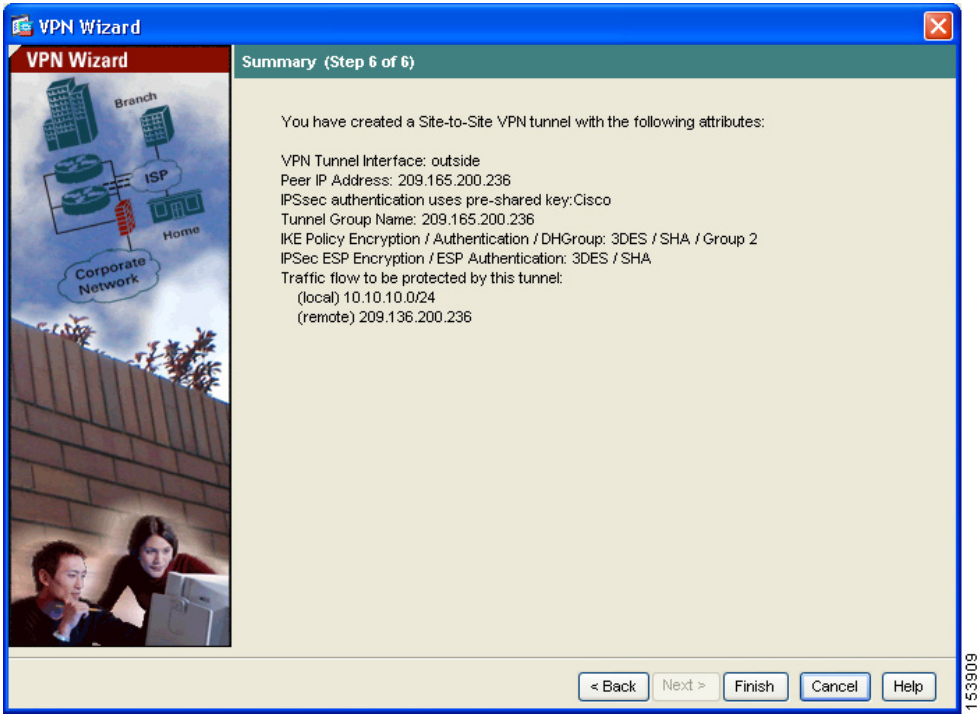
ステップ 4　リモート ホストまたはネットワークの IP アドレスおよびネットマスクを入力します。



ステップ 5　**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、設定の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わりです。

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.8-5 の「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」から P.8-12 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と同じ値を、正確に入力する必要があります。不一致は、VPN トンネル設定エラーのよくある原因です。

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	*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
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」
リモートアクセス VPN の設定	第 7 章「シナリオ：リモートアクセス VPN の設定」

次の手順