シナリオ：サイトツーサイト VPN の設定

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（バーチャル プライベート ネットワーク）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。

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

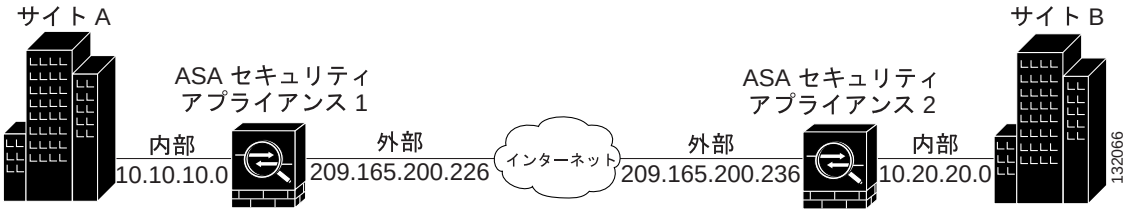


図 8-1 で示すような VPN サイトツーサイト配置の作成では、接続のそれぞれの端で 1 つずつ、合計 2 つの適応型セキュリティ アプライアンスを設定する必要があります。

サイトツーサイトのシナリオの実装

次の項で、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。

必要な情報

- 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

ASDM には、サイトツーサイト VPN の設定プロセスを案内する設定ウィザードがあります。VPN 接続の片側を設定するには、次の手順を実行します。

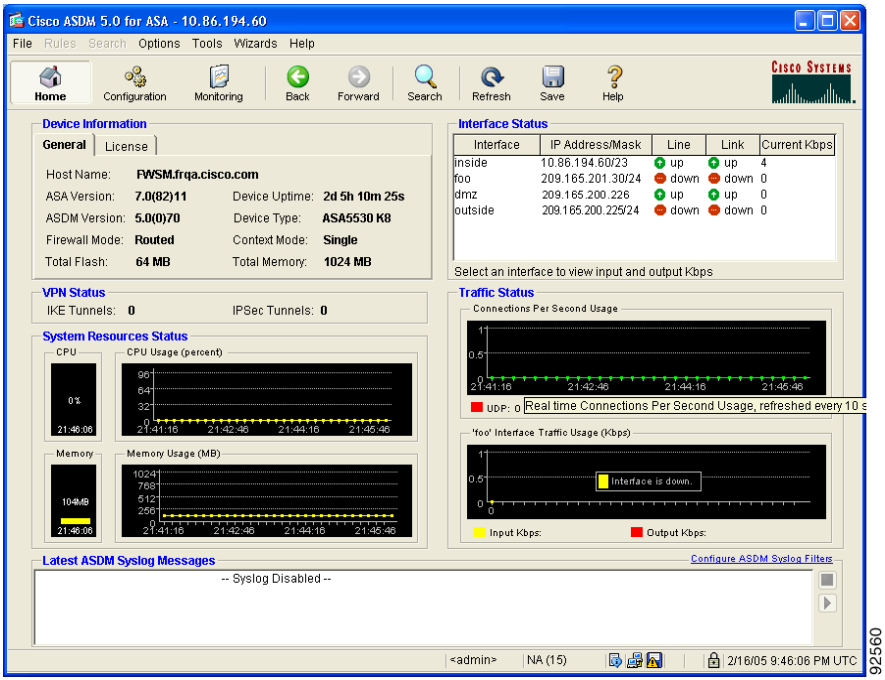
1. ローカル サイトでの適応型セキュリティ アプライアンスの設定
2. VPN ピアに関する情報の入力
3. IKE ポリシーの設定
4. IPSec 暗号化および認証パラメータの設定
5. ローカル ホストおよびネットワークの指定
6. リモート ホストおよびネットワークの指定
7. VPN アトリビュートの確認とウィザードの完了

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

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、ASA 1 と呼びます。

ローカルな適応型セキュリティ アプライアンスを設定するには、次の手順を実行します。

ステップ 1　Web ブラウザのアドレス 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/** を入力して、ASDM を起動します。



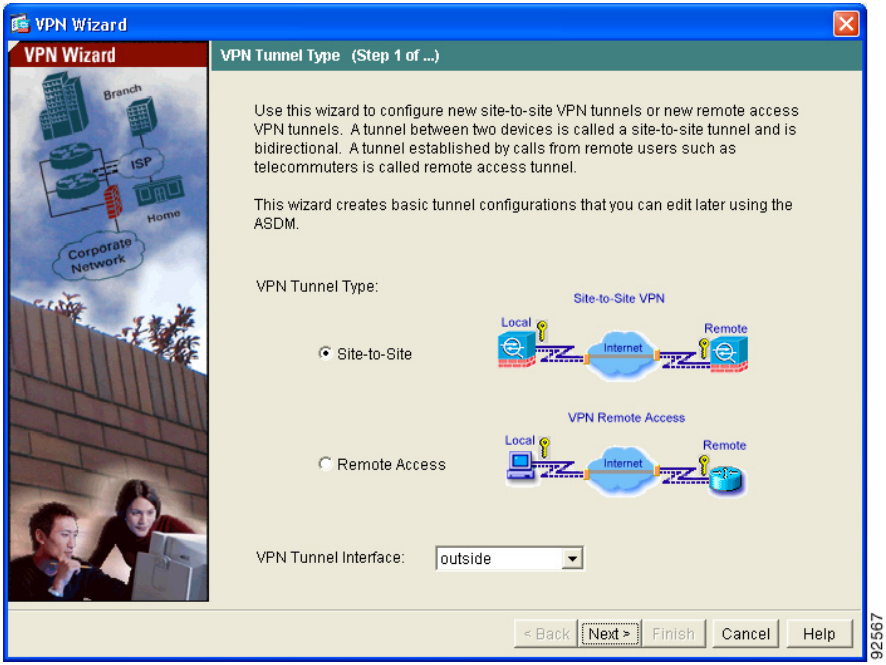
ステップ 2　ASDM のメイン ウィンドウの Wizards ドロップダウン リストで、**VPN Wizard** オプションをクリックします。最初の VPN Wizard 画面が表示されます。

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** をクリックします。



c. **Next** をクリックして続行します。

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。このシナリオでは、リモート VPN ピアは ASA セキュリティ アプライアンス 2 です。以後、ASA 2 と呼びます。

VPN Wizard の Step 2 で、次の手順を実行します。

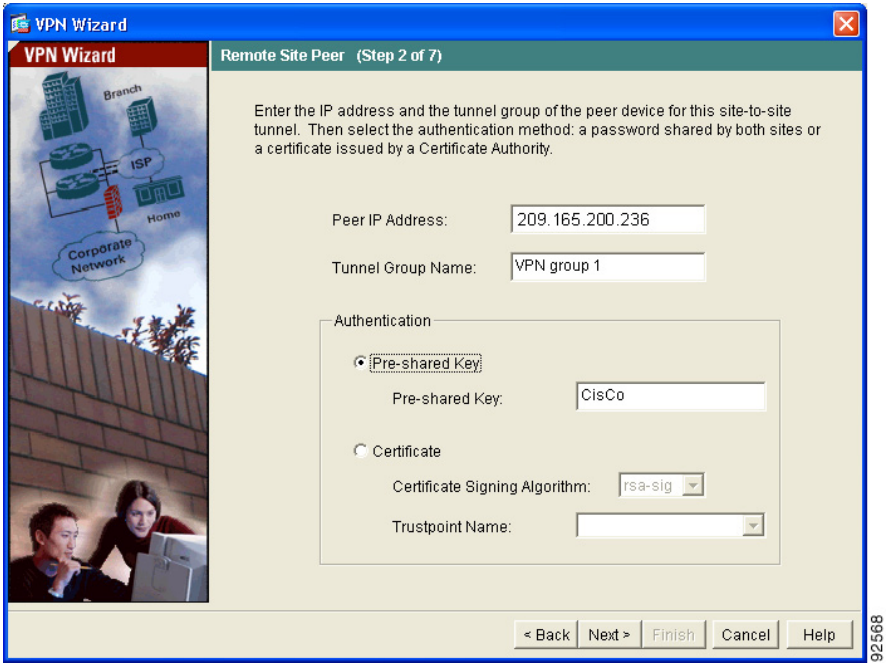
ステップ 1　**Peer IP Address**（ASA 2）と **Tunnel Group Name** を入力します。

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。

- 認証に事前共有キー（「CisCo」など）を使用するには、**Pre-Shared Key** オプション ボタンをクリックし、両方の適応型セキュリティ アプライアンスの間の IPSec ネゴシエーションで共有される、事前共有キーを入力します。

  （注）　リモート サイトで ASA 2 を設定するとき、VPN ピアは ASA 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。

- 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、**Trustpoint Name** ドロップダウン リストで、トラストポイント名を選択します。



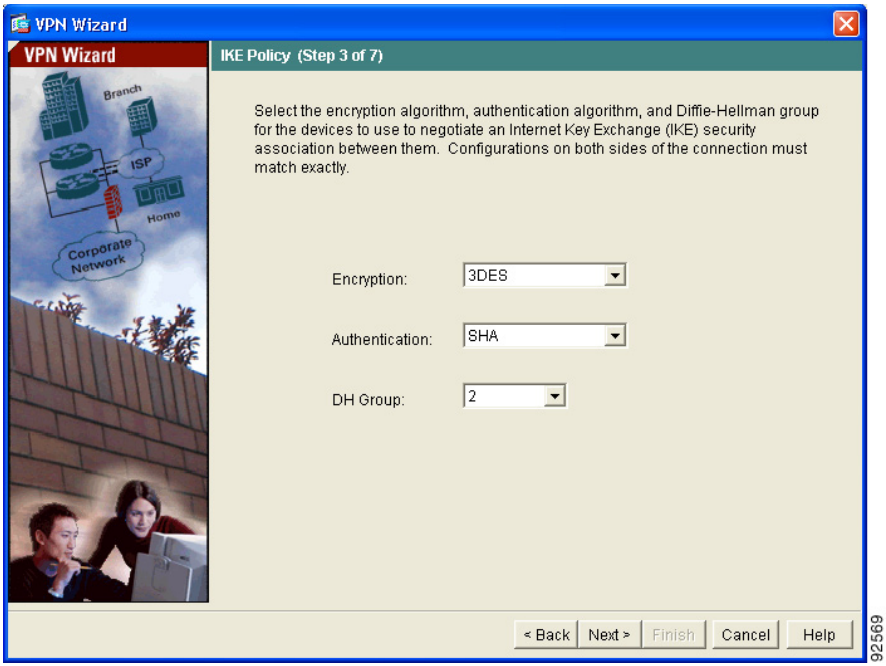
ステップ 3　**Next** をクリックして続行します。

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。



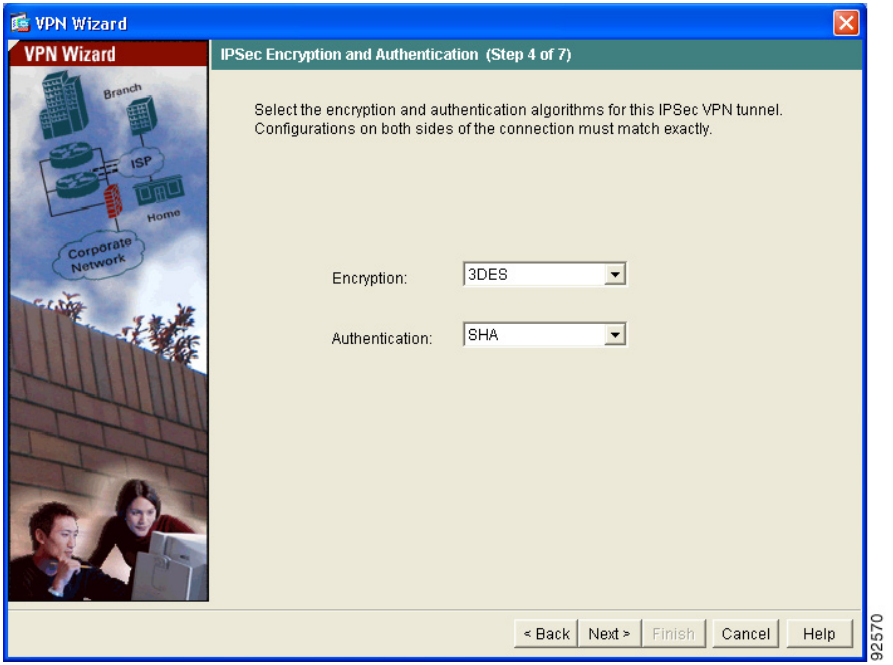
（注）　ASA 2 を設定するときは、ASA 1 で選択した各オプションの値を正確に入力する必要があります。暗号化の不一致は、VPN トンネル障害のよくある原因で、設定プロセスを遅らせる原因になります。

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。

ローカル 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（リモートサイト ピアは、後で指定します）。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 ASA 1 で暗号化され、VPN トンネルを使用して送信されます。

VPN Wizard の Step 5 で、次の手順を実行します。

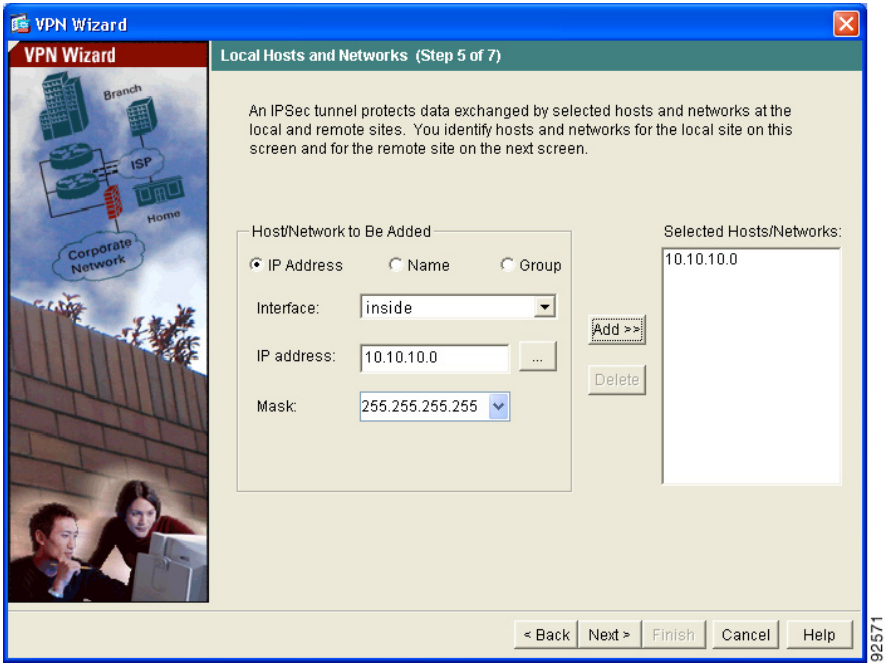
ステップ 1　**IP Address** をクリックします。

ステップ 2　ドロップダウン リストで、インターフェイスが **inside** か **outside** かを指定するために、インターフェイスをクリックします。

ステップ 3　**IP アドレス**とマスクを入力します。

ステップ 4　**Add** をクリックします。

ステップ 5　トンネルにアクセスできるホストまたはネットワークごとに、ステップ 1 からステップ 4 を繰り返します。



ステップ 6　**Next** をクリックして続行します。

リモート 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、ステップ 5 で指定したローカル ホストおよびネットワークと通信できる、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。現在のシナリオでは、ASA 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 6 で、次の手順を実行します。

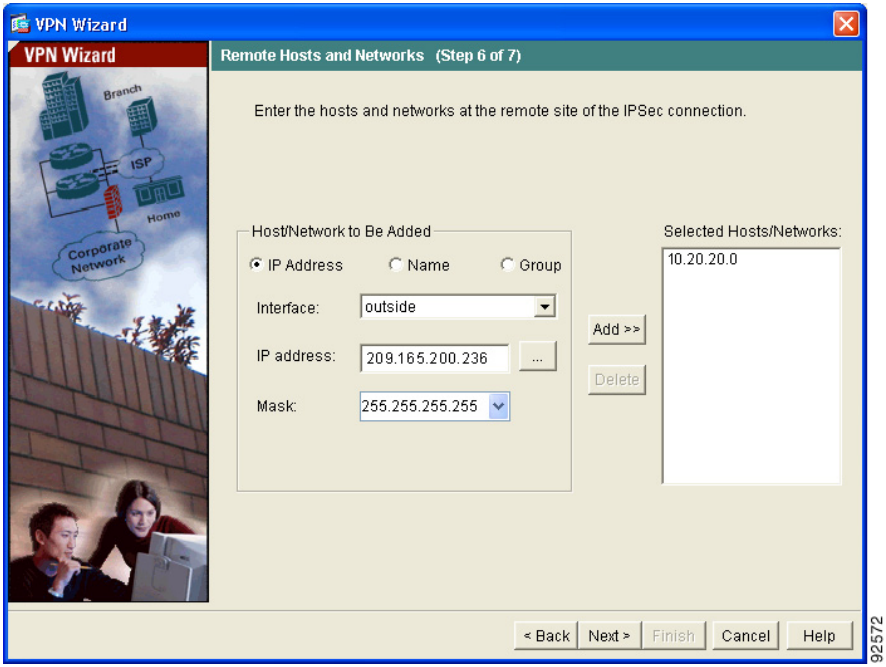
ステップ 1　**IP Address** をクリックします。

ステップ 2　Interface ドロップダウン リストで、インターフェイスが **inside** か **outside** かを指定するために、インターフェイスをクリックします。

ステップ 3　IP アドレスとマスクを入力します。

ステップ 4　**Add** をクリックします。

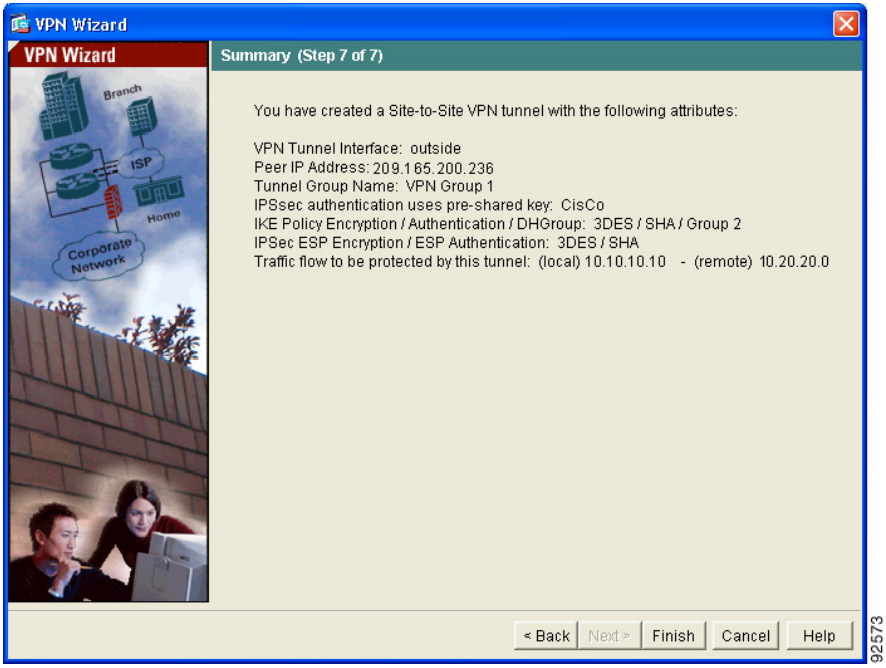
ステップ 5　トンネルにアクセスできるホストまたはネットワークごとに、ステップ 1 からステップ 4 を繰り返します。



ステップ 6　**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 7 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。



これで、ASA 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.8-3 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.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） ASA 2 を設定するときは、ASA 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*
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	*Cisco ASA 5500 Series Hardware Installation Guide*

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」