CHAPTER 5

シナリオ：Cisco AnyConnect VPN クライアント用接続の設定

この章では、リモート ユーザが、Cisco AnyConnect VPN クライアントを使用して SSL 接続を確立できるよう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。

この章は、次の項で構成されています。

- 「SSL VPN クライアント接続について」（P.5-1）
- 「Cisco AnyConnect VPN クライアント ソフトウェアの取得」（P.5-2）
- 「AnyConnect SSL VPN クライアントを使用したトポロジの例」（P.5-3）
- 「Cisco SSL VPN シナリオの実装」（P.5-3）
- 「次の作業」（P.5-12）

SSL VPN クライアント接続について

SSL VPN クライアント（AnyConnect）の使用を開始するには、リモート ユーザはブラウザに、適応型セキュリティ アプライアンスの SSL VPN インターフェイスの IP アドレスまたは FQDN を入力します。ブラウザは SSL VPN が有効になっているインターフェイスに接続し、ログイン画面を表示します。

（注） Cisco AnyConnect VPN クライアントを初めてインストールまたはダウンロードする際には、管理者権限が必要となります。

ダウンロードが終わると、クライアントは自動的にインストールおよび設定され、次に、安全な SSL 接続が確立されます。接続が終了すると、クライアント ソフトウェアは、適応型セキュリティ アプライアンスの設定に従って、そのまま残るか自動的にアンインストールされます。

リモート ユーザが過去に SSL VPN 接続を確立したことがあり、クライアント ソフトウェアが自動的にアンインストールされる設定になっていない場合、ユーザ認証時に、適応型セキュリティ アプライアンスによってクライアントのバージョンが確認され、必要に応じてアップグレードされます。

Cisco AnyConnect VPN クライアント ソフトウェアの取得

AnyConnect VPN クライアント ソフトウェアは、適応型セキュリティ アプライアンスによってシスコの Web サイトから取得されます。この章では、設定ウィザードを使用した SSL VPN の設定手順について説明します。Cisco SSL VPN ソフトウェアは、設定プロセス中にダウンロードできます。

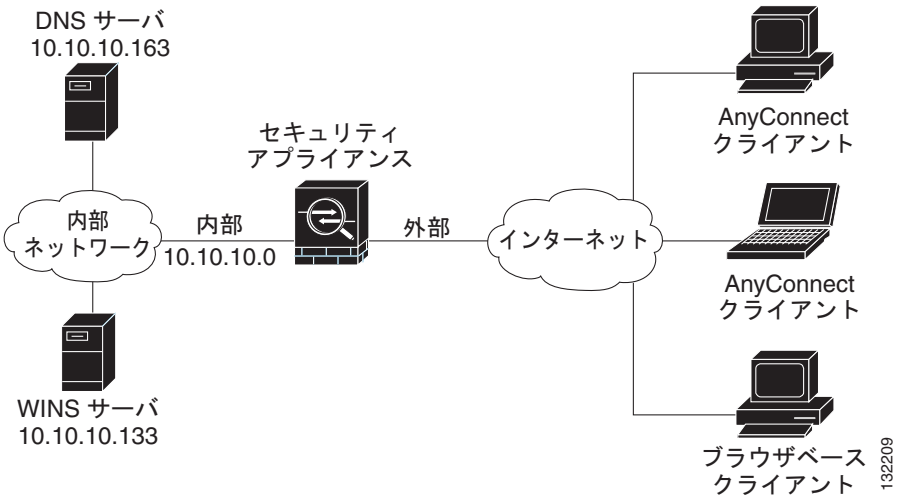
AnyConnect VPN クライアントは、ユーザが適応型セキュリティ アプライアンスからダウンロードするか、システム管理者が手動でリモート PC にインストールできます。手動によるクライアント ソフトウェアのインストールに関する詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

適応型セキュリティ アプライアンスでは、グループ ポリシーまたは接続を確立するユーザのユーザ名アトリビュートに基づいて、クライアント ソフトウェアが適用されます。適応型セキュリティ アプライアンスを、ユーザが接続を確立する度にクライアントが自動的に適用されるように、あるいは、ユーザに対してクライアントをダウンロードするかどうか指定することを求めるように設定できます。後者においては、ユーザが応答しなかった場合に、タイムアウト期間が過ぎた後にクライアントが自動的に適用されるか、あるいは、SSL VPN ログイン画面が表示されるように適応型セキュリティ アプライアンスを設定できます。

AnyConnect SSL VPN クライアントを使用したトポロジの例

図 5-1 に、AnyConnect SSL VPN ソフトウェアが実行されているクライアントの要求を受け付け、そのクライアントからの SSL 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ます。適応型セキュリティ アプライアンスは、AnyConnect VPN ソフトウェアが実行されているクライアントと、ブラウザベースのクライアントの両方に対応できます。

図 5-1　　SSL VPN シナリオのネットワーク レイアウト



Cisco SSL VPN シナリオの実装

この項では、Cisco AnyConnect SSL VPN 接続を受け入れるよう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。設定内容の例で使われる値は、図 5-1 に示す SSL VPN シナリオのものです。

この項は、次の内容で構成されています。

- 「収集する情報」（P.5-4）

- 「Cisco AnyConnect VPN クライアントの適応型セキュリティ アプライアンスの設定」（P.5-5）
- 「SSL VPN インターフェイスの指定」（P.5-6）
- 「ユーザ認証方式の指定」（P.5-7）
- 「グループ ポリシーの指定」（P.5-8）
- 「Cisco AnyConnect VPN クライアントの設定」（P.5-9）
- 「リモートアクセス VPN 設定の確認」（P.5-11）

収集する情報

AnyConnect SSL VPN 接続を受け入れるよう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開始する前に、次の情報を手元に用意してください。

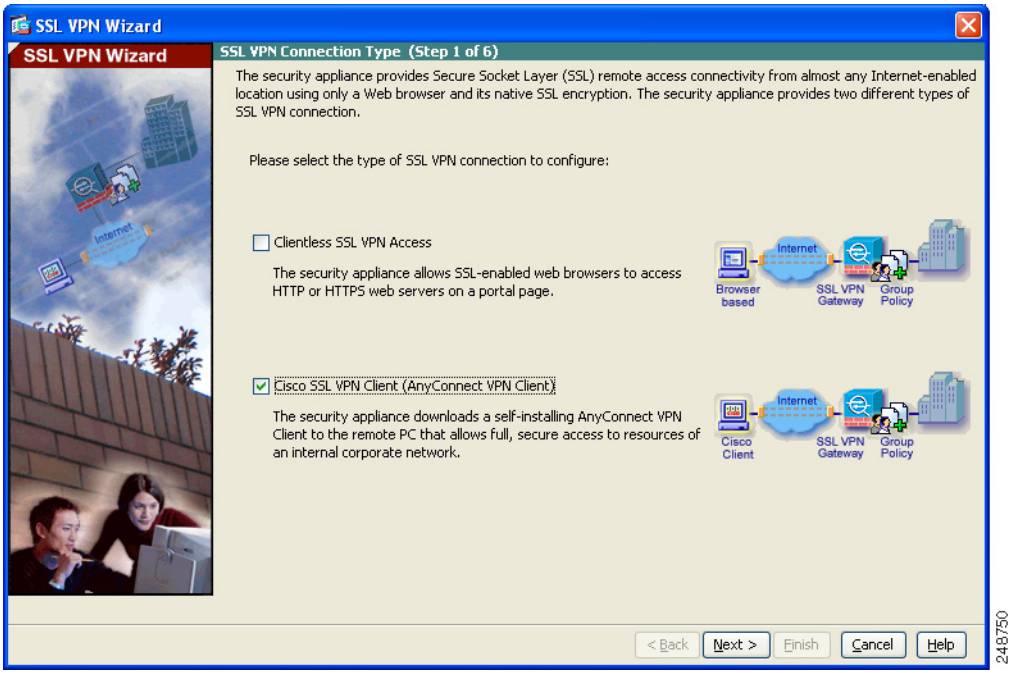
- リモート ユーザが接続する適応型セキュリティ アプライアンスのインターフェイス名。
- デジタル証明書。

  デフォルトでは、ASA 5580 によって自己署名証明書が生成されます。しかし、セキュリティを強化するために、公的に信頼された SSL VPN 証明書を購入してからシステムを実稼動環境に移行することもできます。
- 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、正常に接続されると、SSL AnyConnect 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を作成するときに使用するユーザのリスト（認証用に AAA サーバを使用している場合を除く）。
- 認証に AAA サーバを使用する場合は、次の情報を手元に用意してください。
  - AAA サーバのグループ名
  - 使用する認証プロトコル（TACACS、SDI、NT、Kerberos、LDAP）
  - AAA サーバの IP アドレス
  - 認証に使用する適応型セキュリティ アプライアンスのインターフェイス
  - AAA サーバで認証を行うための秘密キー

Cisco AnyConnect VPN クライアントの適応型セキュリティ アプライアンスの設定

設定プロセスを始めるには、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 [SSL VPN Wizard] を選択します。SSL VPN Wizard の Step 1 の画面が表示されます。



ステップ 2　SSL VPN Wizard の Step 1 で、次の手順に従います。

a.　[Cisco SSL VPN Client] チェックボックスをオンにします。

b.　[Next] をクリックして続行します。

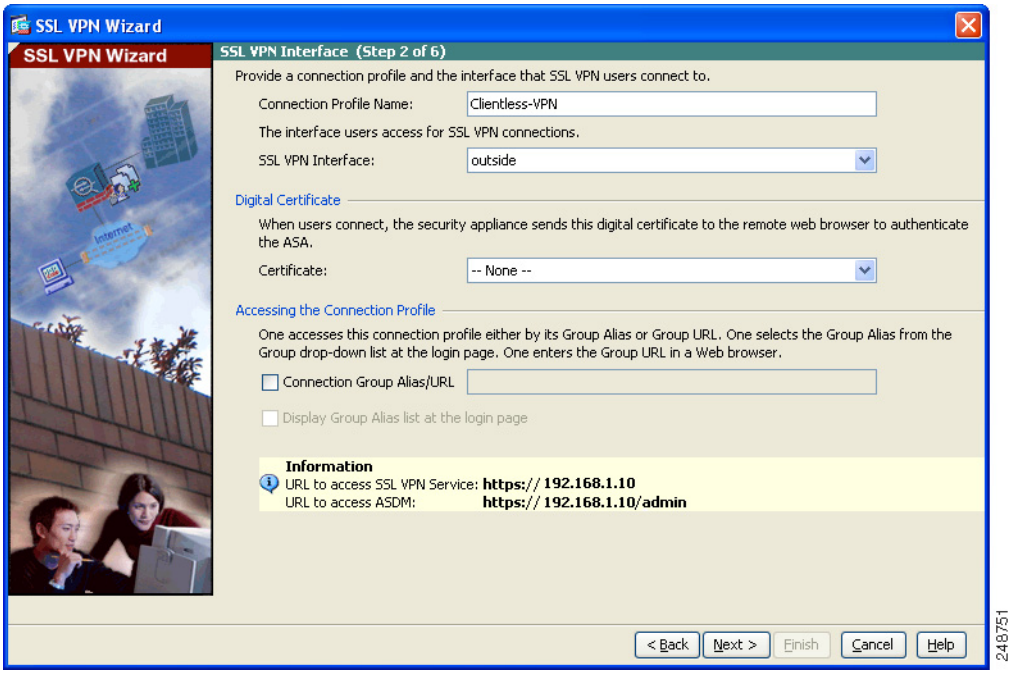
SSL VPN インターフェイスの指定

SSL VPN Wizard の Step 2 で、次の手順に従います。

ステップ 1　リモート ユーザが接続する接続名を指定します。

ステップ 2　[SSL VPN Interface] ドロップダウン リストから、リモート ユーザが接続するインターフェイスを選択します。ユーザがこのインターフェイスへの接続を確立すると、SSL VPN のポータル ページが表示されます。

ステップ 3　[Certificate] ドロップダウン リストから、適応型セキュリティ アプライアンスを認証するために適応型セキュリティ アプライアンスによってリモート ユーザに送信される証明書を選択します。



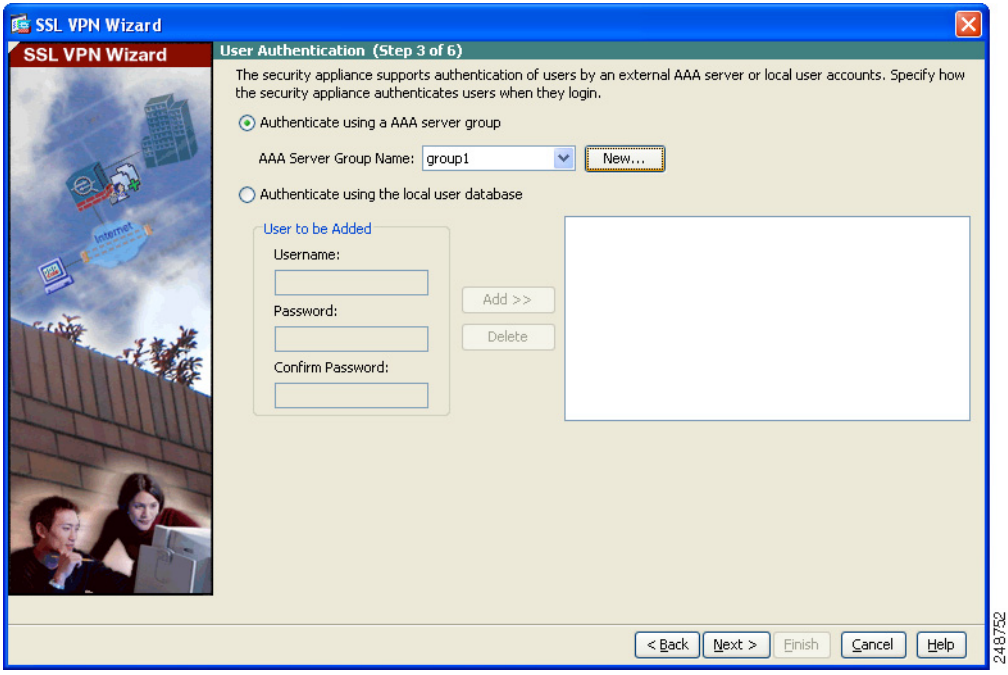
ステップ 4　[Next] をクリックして続行します。

ユーザ認証方式の指定

SSL VPN Wizard の Step 3 で、次の手順に従います。

ステップ 1　認証に AAA サーバまたはサーバ グループを使用する場合、次の手順に従います。

a. [Authenticate using a AAA server group] オプション ボタンをクリックします。



b. AAA サーバ グループ名を指定します。

c. ドロップダウン リストから、既存の AAA サーバ グループ名を選択するか、[New] をクリックして新しいサーバ グループを作成できます。

新しい AAA サーバ グループを作成するには、[New] をクリックします。[New Authentication Server Group] ダイアログボックスが表示されます。

このダイアログボックスで、次の項目を指定します。

- サーバ グループ名

- 使用する認証プロトコル（RADIUS、TACACS、SDI、NT、Kerberos、LDAP）
- AAA サーバの IP アドレス
- 適応型セキュリティ アプライアンスのインターフェイス
- AAA サーバとの通信時に使用する秘密キー

d. [OK] をクリックします。

ステップ 2　ローカル ユーザ データベースを使用してユーザを認証する場合、次の手順で新しいユーザ 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。

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 3　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。

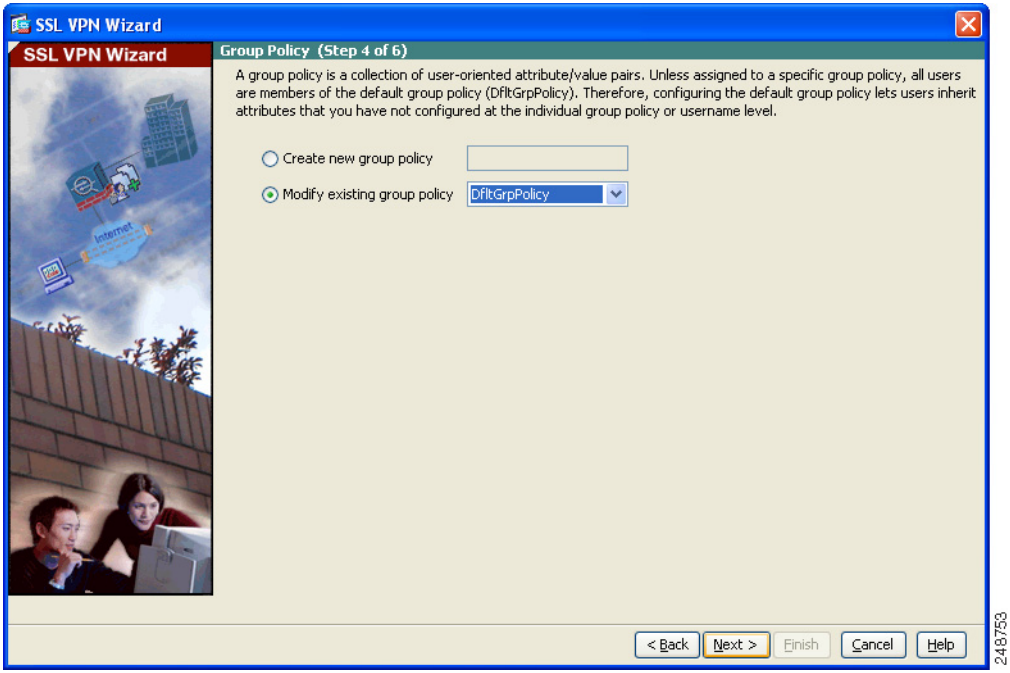
グループ ポリシーの指定

SSL VPN Wizard の Step 4 で、次の手順に従ってグループ ポリシーを指定します。

ステップ 1　[Create new group policy] オプション ボタンをクリックして、グループ名を指定します。

または、

ステップ 2　[Modify an existing group policy] オプション ボタンをクリックして、ドロップダウン リストからグループを選択します。



ステップ 3　[Next] をクリックします。

ステップ 4　SSL VPN Wizard の Step 5 が表示されます。このステップは AnyConnect VPN クライアント接続には関係ないので、再度 [Next] をクリックします。

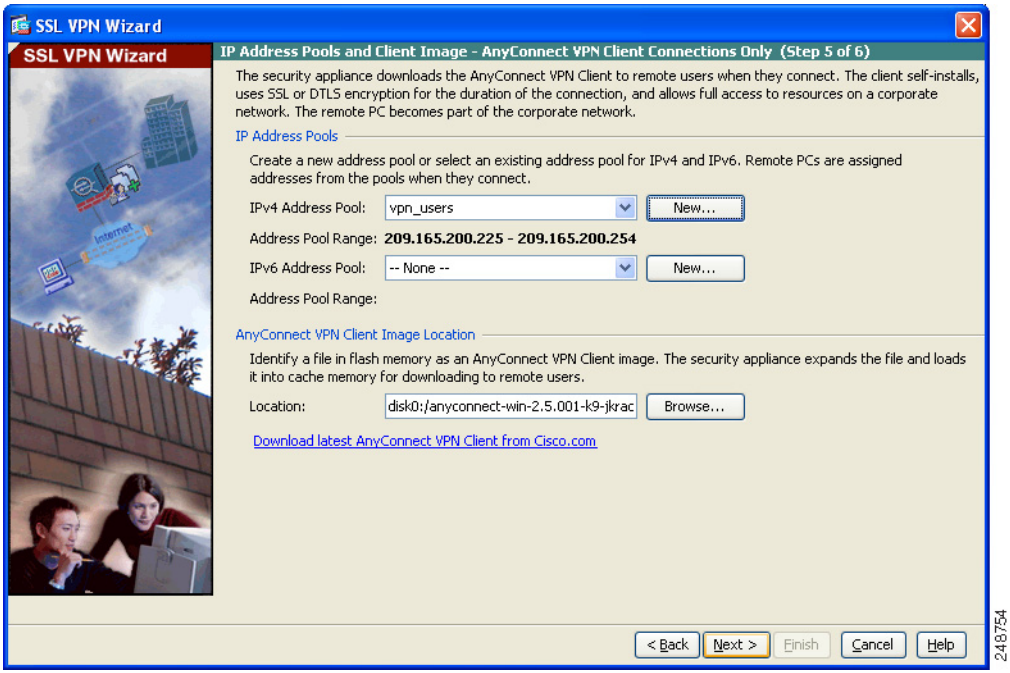
Cisco AnyConnect VPN クライアントの設定

リモート クライアントが Cisco AnyConnect VPN クライアントを使用してネットワークにアクセスできるようにするには、接続に成功した時にリモート VPN クライアントに割り当て可能な 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、プールは 209.165.201.1 ～ 209.166.201.20 の範囲の IP アドレスを使用するように設定します。

適応型セキュリティ アプライアンスによってユーザに割り当てられるように、AnyConnect ソフトウェアの場所も指定する必要があります。

SSL VPN Wizard の Step 6 で、次の手順に従います。

ステップ 1　事前に設定されたアドレス プールを使用するには、[IPv4 Address Pool] ドロップダウン リストまたは [IPv6 Address Pool] ドロップダウン リストからプール名を選択します。



ステップ 2　または、[New] をクリックして、新しいアドレス プールを作成します。

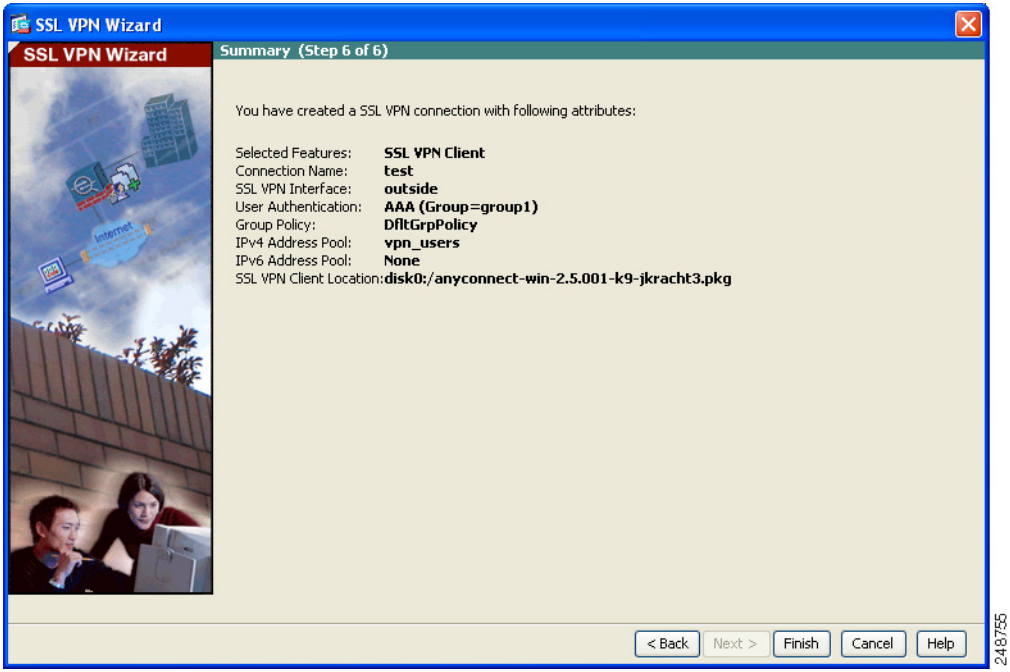
ステップ 3　AnyConnect VPN クライアント ソフトウェア イメージの場所を指定します。

最新バージョンのソフトウェアを取得するには、[Download Latest AnyConnect VPN Client from cisco.com] をクリックします。これにより、クライアント ソフトウェアが PC にダウンロードされます。

ステップ 4　[Next] をクリックして続行します。

リモートアクセス VPN 設定の確認

SSL VPN Wizard の Step 7 で、設定内容が正しいことを確認します。表示される設定は次のようになります。



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。

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。

次の作業

AnyConnect VPN 接続をサポートするため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 ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series 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
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」
サイトツーサイト VPN の設定	第 7 章「シナリオ：サイトツーサイト VPN 設定」
リモートアクセス IPSec VPN の設定	第 8 章「シナリオ：IPsec リモートアクセス VPN 設定」