



CHAPTER 5

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

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。

この章には、次の項があります。

- [SSL VPN クライアント接続について \(P.5-2\)](#)
- [Cisco AnyConnect VPN クライアント ソフトウェアの取得 \(P.5-3\)](#)
- [AnyConnect SSL VPN クライアントを使用したトポロジの例 \(P.5-4\)](#)
- [Cisco SSL VPN シナリオの実装 \(P.5-5\)](#)
- [次の手順 \(P.5-17\)](#)

SSL VPN クライアント接続について

SSL VPN クライアントがセットアップされている場合、リモート ユーザは、接続を確立する前にソフトウェア クライアントをインストールする必要はありません。代わりに、リモート ユーザは Cisco SSL VPN インターフェイスの IP アドレスまたは DNS 名をブラウザに入力します。ブラウザは、そのインターフェイスに接続し、SSL VPN ログイン画面を表示します。ユーザが正常に認証された後、適応型セキュリティ アプライアンスは、そのユーザがクライアントを必要としていると認識すると、リモート コンピュータのオペレーティング システムに適合するクライアントをプッシュします。



(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場合は、管理者権限が必要です。

ダウンロード後、クライアント自身がインストールと設定を行ってから、セキュアな SSL 接続を確立します。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方法に応じてそのまま残るか、アンインストールされます。

リモート ユーザが以前に SSL VPN 接続を確立したことがあり、クライアント ソフトウェア自身がアンインストールするよう指示されていない場合は、ユーザ認証時に適応型セキュリティ アプライアンスがクライアントのバージョンを調べ、必要に応じてアップグレードを行います。

Cisco AnyConnect VPN クライアント ソフトウェアの取得

適応型セキュリティ アプライアンスは、シスコの Web サイトから AnyConnect VPN クライアント ソフトウェアを取得します。この章では、設定ウィザードを使用して SSL VPN を設定する方法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。

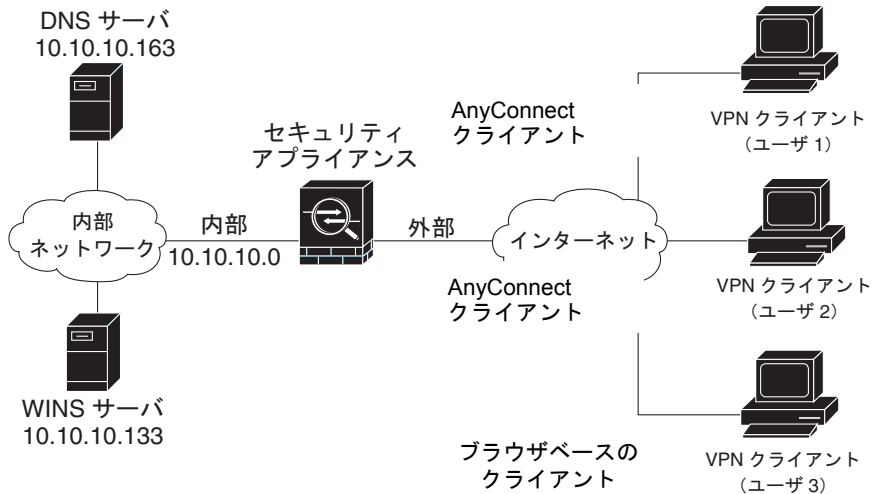
AnyConnect VPN クライアントは、ユーザが適応型セキュリティ アプライアンスからダウンロードするか、システム管理者がリモート PC に手動でインストールすることができます。このクライアント ソフトウェアを手動でインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

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 ソフトウェアをプッシュします。適応型セキュリティ アプライアンスでは、ユーザが接続を確立するたびにクライアントを自動的にプッシュするように設定するか、クライアントをダウンロードするかどうかの確認をリモート ユーザに求めるように設定することができます。後者の場合、ユーザからの応答がないときに、適応型セキュリティ アプライアンスでは、タイムアウト時間の経過後にクライアントをプッシュするように設定するか、SSL VPN ログイン画面を表示するように設定することができます。

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 ソフトウェアを実行しているクライアントからの SSL 接続要求を受け入れ、SSL 接続を確立するように設定されている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 ソフトウェアを実行し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への接続をサポートすることができます。

図 5-1 SSL VPN シナリオのネットワーク レイアウト



132209

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。設定内容の値の例は、[図 5-1](#) に示した SSL VPN シナリオから使用しています。

次のトピックについて取り上げます。

- [必要な情報 \(P.5-5\)](#)
- [ASDM の起動 \(P.5-6\)](#)
- [Cisco AnyConnect VPN クライアント用の ASA 5580 の設定 \(P.5-9\)](#)
- [SSL VPN インターフェイスの指定 \(P.5-10\)](#)
- [ユーザ認証方式の指定 \(P.5-11\)](#)
- [グループ ポリシーの指定 \(P.5-12\)](#)
- [Cisco AnyConnect VPN クライアントの設定 \(P.5-14\)](#)
- [リモート アクセス VPN の設定の確認 \(P.5-15\)](#)

必要な情報

AnyConnect SSL VPN 接続を受け入れるための適応型セキュリティ アプライアンスの設定を開始する前に、次の情報を用意してください。

- 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の名前。
- デジタル証明書。

ASA 5580 は、デフォルトで自己署名証明書を生成します。ただし、セキュリティを強化するために、システムを実稼働環境に設置する前に、公的に信頼されている SSL VPN 証明書を購入することもできます。

- IP プールに使用する 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 サーバを使用している場合：
 - AAA サーバ 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鍵

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。

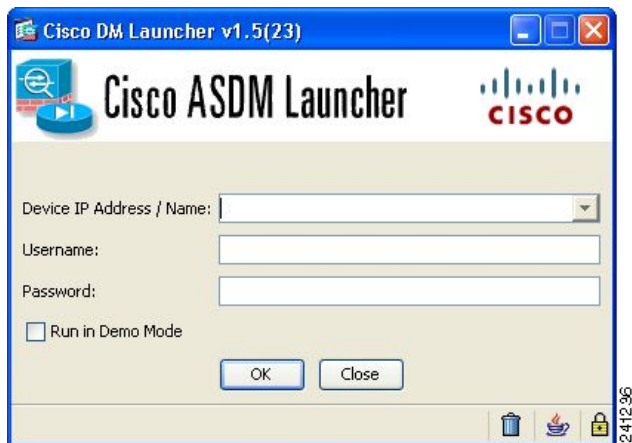
Web ブラウザまたは Java を使用して ASDM に直接アクセスする場合は、[P.4-8 の「Web ブラウザでの ASDM の起動」](#)を参照してください。

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。

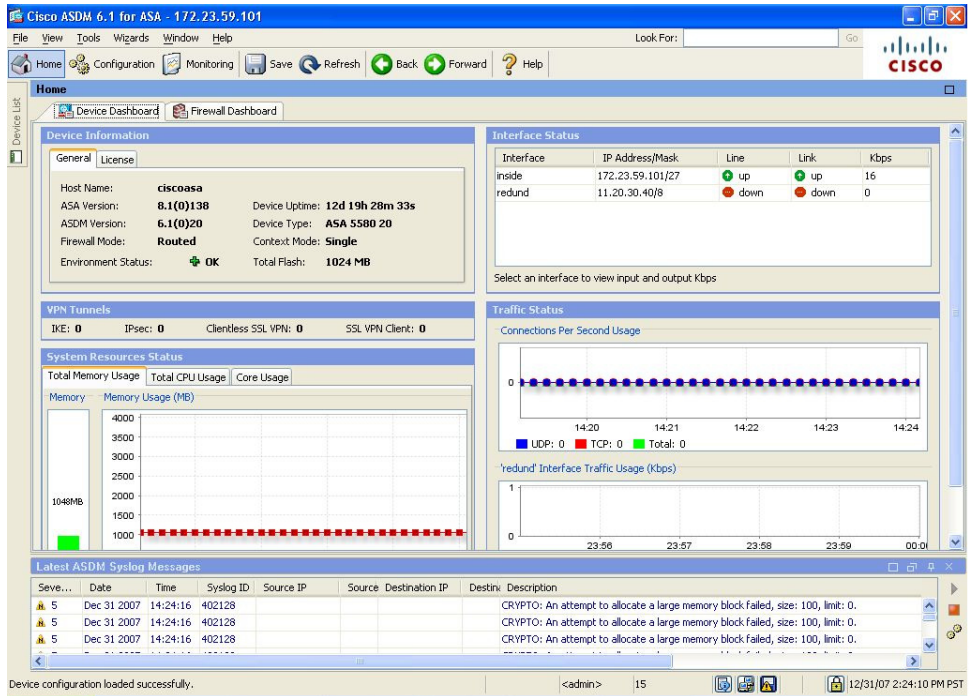
ステップ 4 OK をクリックします。

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。

Cisco SSL VPN シナリオの実装

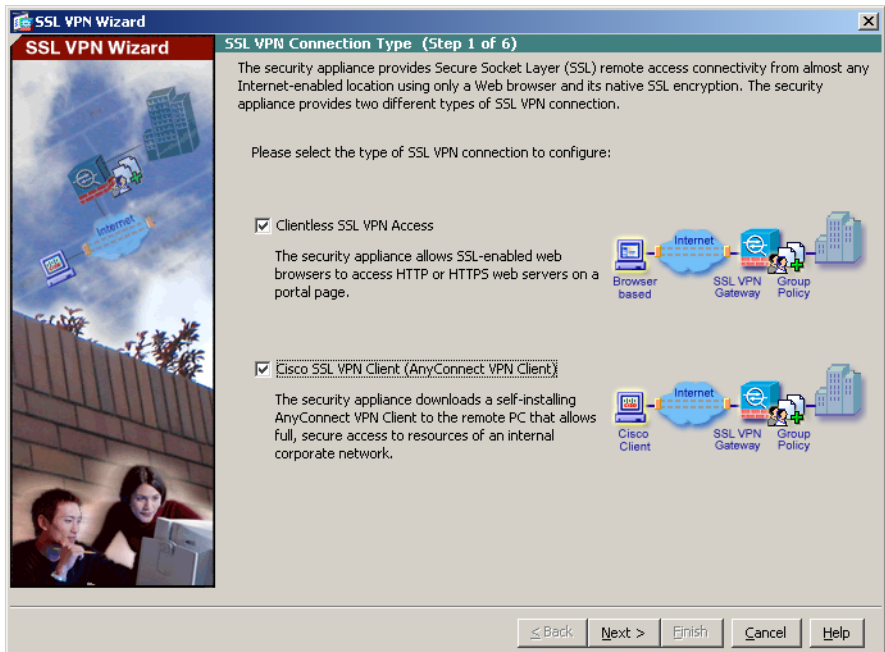


241237

Cisco AnyConnect VPN クライアント用の ASA 5580 の設定

設定プロセスを開始するには、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 メニューから **SSL VPN Wizard** を選択します。SSL VPN Wizard Step 1 画面が表示されます。



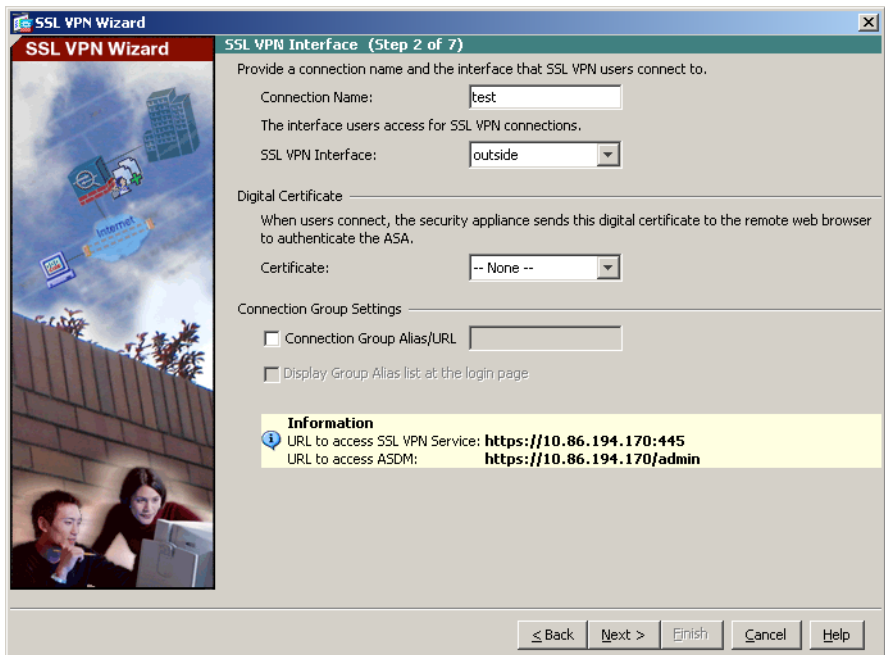
- ステップ 2** SSL VPN Wizard の Step 1 で、次の手順を実行します。

- 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、次の手順を実行します。

- 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 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、ASA 5580 を認証するために ASA 5580 がリモート ユーザに送信する証明書を選択します。



SSL VPN Wizard

SSL VPN Interface (Step 2 of 7)

Provide a connection name and the interface that SSL VPN users connect to.

Connection Name:

The interface users access for SSL VPN connections.

SSL VPN Interface:

Digital Certificate

When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.

Certificate:

Connection Group Settings

☐ Connection Group Alias/URL

☐ Display Group Alias list at the login page

Information

URL to access SSL VPN Service: <https://10.86.194.170:445>

URL to access ASDM: <https://10.86.194.170/admin>

≤ Back Next > Finish Cancel Help

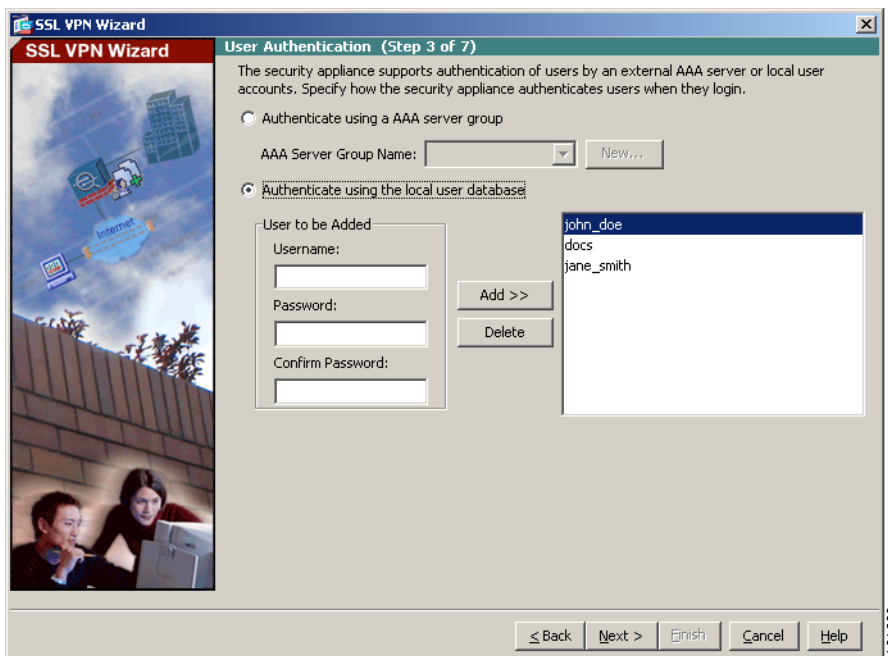
- ステップ 4** Next をクリックして続行します。

ユーザ認証方式の指定

SSL VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1 AAA サーバまたはサーバ グループを認証に使用している場合、次の手順を実行します。

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 グループを作成することができます。

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、次の内容を指定します。

- 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 サーバと通信するときに使用する秘密鍵
- OK をクリックします。

ステップ 2 ローカル ユーザ データベースでユーザを認証する場合は、ここで新しいユーザ 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、次の手順を実行してグループ 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、グループ名を指定します。

または

ステップ 2 **Modify existing group policy** オプション ボタンをクリックし、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 4 SSL VPN Wizard の Step 5 が表示されます。この手順は AnyConnect VPN クライアント接続には適用されないの、もう一度 **Next** をクリックします。

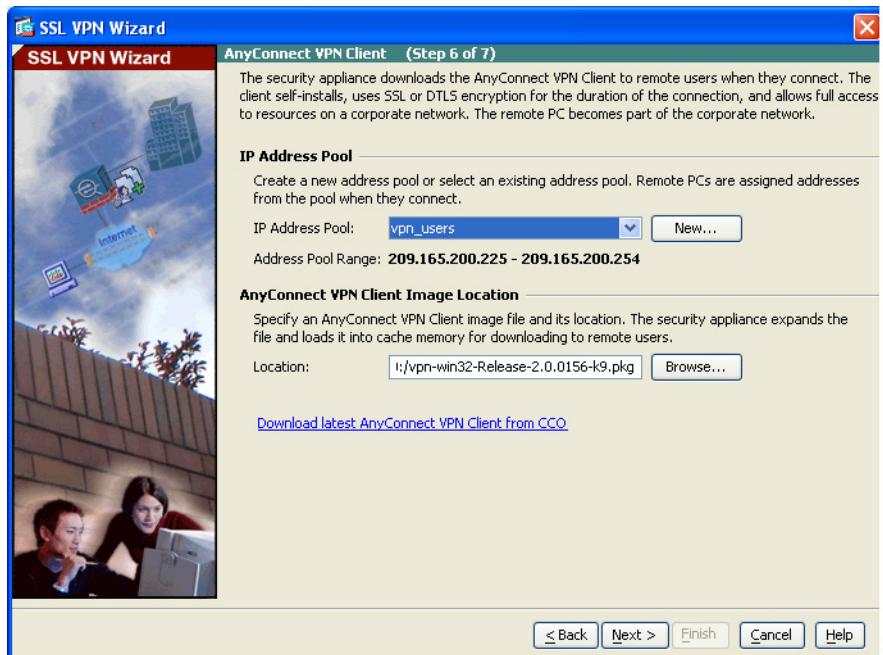
Cisco AnyConnect VPN クライアントの設定

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、正常に接続したときにリモート VPN クライアントに割り当てることができる 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、IP アドレス 209.165.201.1 ~ 209.166.201.20 を使用するようにプールを設定します。

適応型セキュリティ アプライアンスが AnyConnect ソフトウェアをユーザにプッシュできるように、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、次の手順を実行します。

- ステップ 1** 事前設定済みのアドレス プールを使用するには、IP Address Pool ドロップダウンリストからプールの名前を選択します。



191624

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。

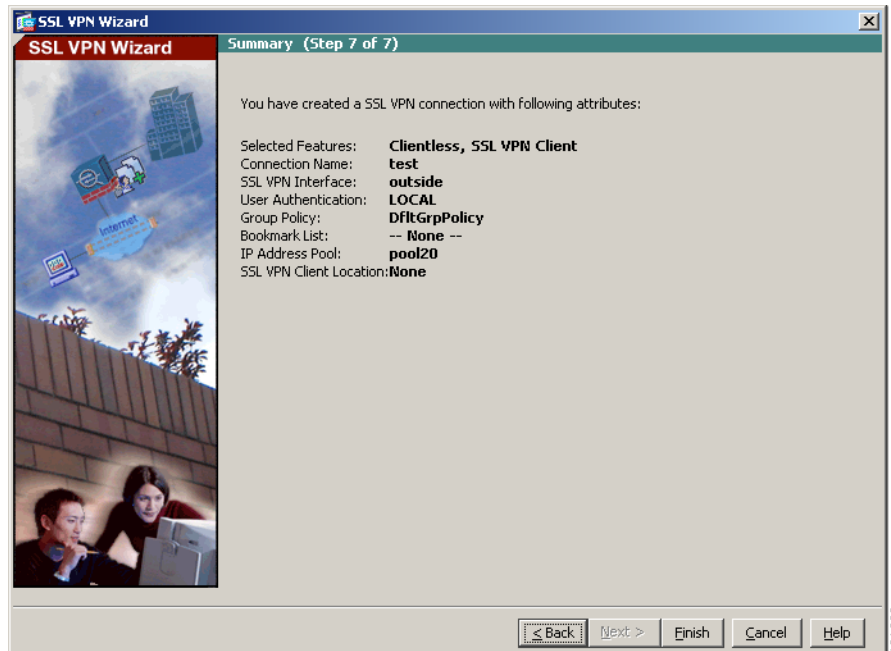
ステップ 3 AnyConnect VPN クライアント ソフトウェア イメージの場所を指定します。

このソフトウェアの最新バージョンを取得するには、**Download latest AnyConnect VPN Client from CCO** をクリックします。この操作を行うと、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 の設定の確認

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。



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。

次の手順

AnyConnect VPN 接続をサポートするため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	<i>Cisco Security Appliance Command Line Configuration Guide</i>
日常のオペレーションの学習	<i>Cisco Security Appliance Command Reference</i> <i>Cisco Security Appliance Logging Configuration and System Log Messages</i>

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
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 の設定」
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 の設定」

■ 次の手順