CHAPTER 8

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

SSL VPN クライアントをセットアップしたら、リモート ユーザが、接続の確立を試み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。その代わり、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。ユーザの認証に成功し、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、適応型セキュリティ アプライアンスがリモート コンピュータのオペレーティング システムに合ったクライアントを配信します。

（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。接続が終了したら、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していない場合は、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。

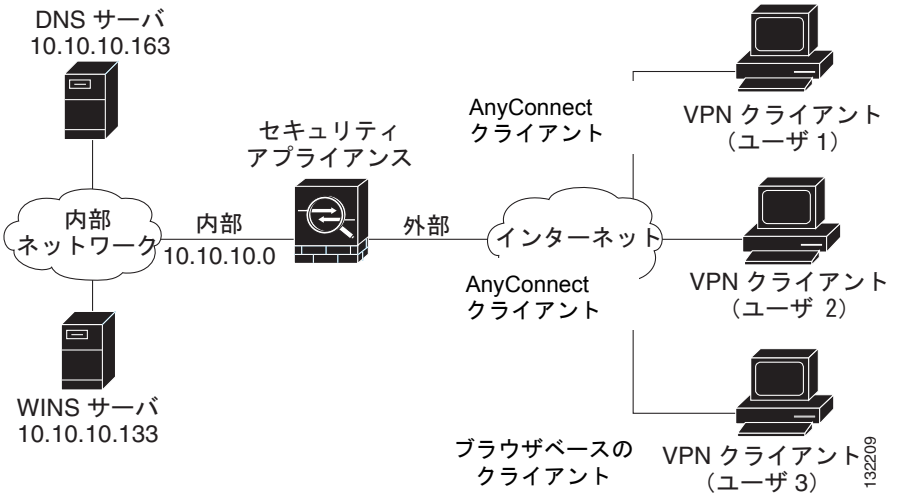
AnyConnect VPN クライアントは、ユーザが適応型セキュリティ アプライアンスからダウンロードするか、システム管理者がリモート PC に手動でインストールすることができます。このクライアント ソフトウェアを手動でインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

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 ソフトウェアを配信します。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配信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を指定するようリモート ユーザに勧めるように設定することができます。後者のケースでは、ユーザが応答しない場合、適応型セキュリティ アプライアンスでは、タイムアウト期間後にクライアントを配信するか、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 8-1 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 8-1　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 8-1 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

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

  ASA 5505 は、デフォルトで自己署名証明書を生成します。しかし、セキュリティを強化するため、システムを本番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）。
- 認証用に 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

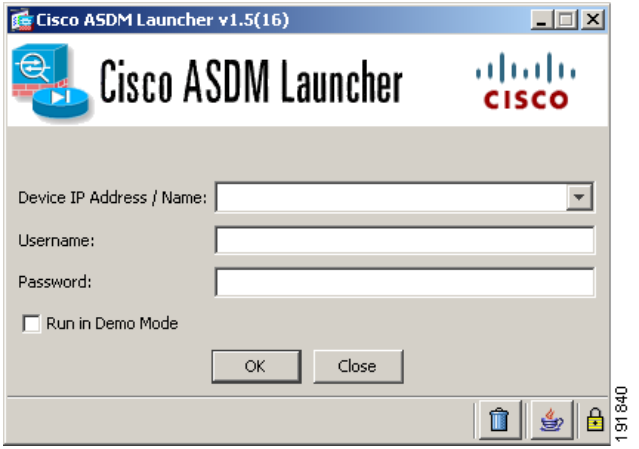
この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアがインストールされていない場合は、P.5-7 の「ASDM Launcher のインストール」を参照してください。

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.5-10 の「Web ブラウザを使用した 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、次の手順に従います。

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 と Password のフィールドは空白のままにしておきます。

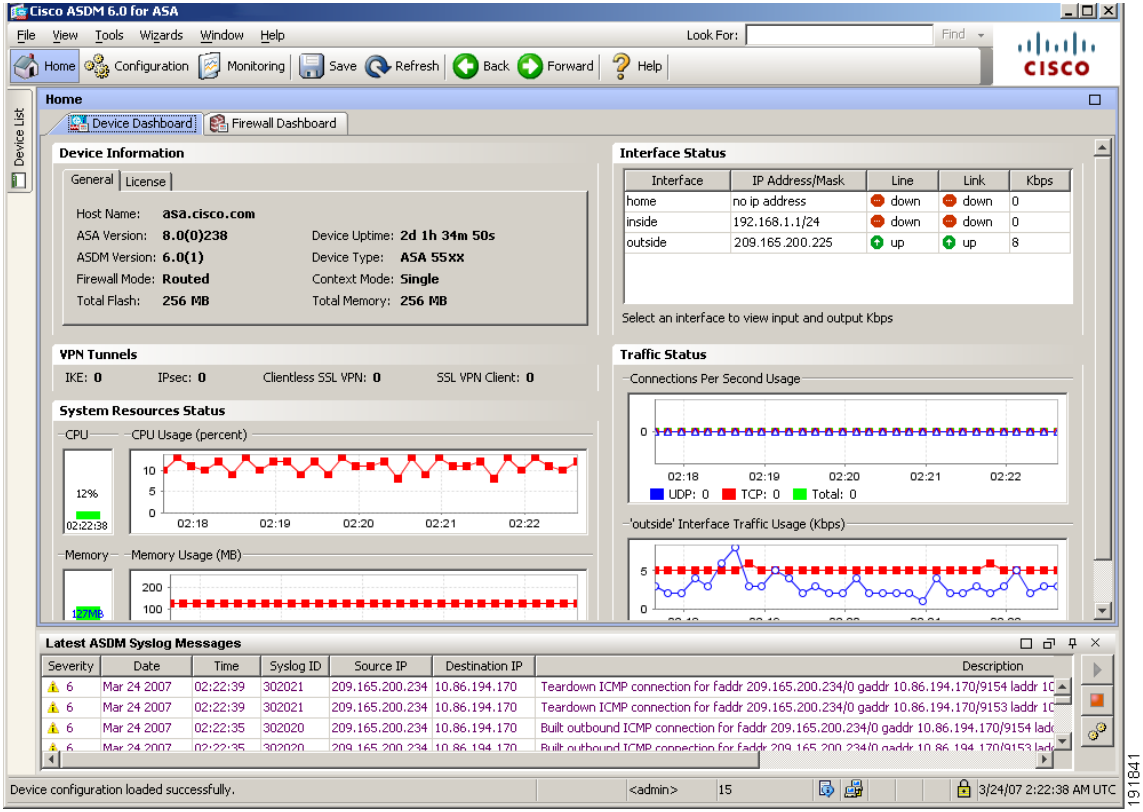
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書の受け入れ要求を含む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 が、アップデートされたソフトウェアがあるかどうか確認し、ある場合は自動的にダウンロードします。

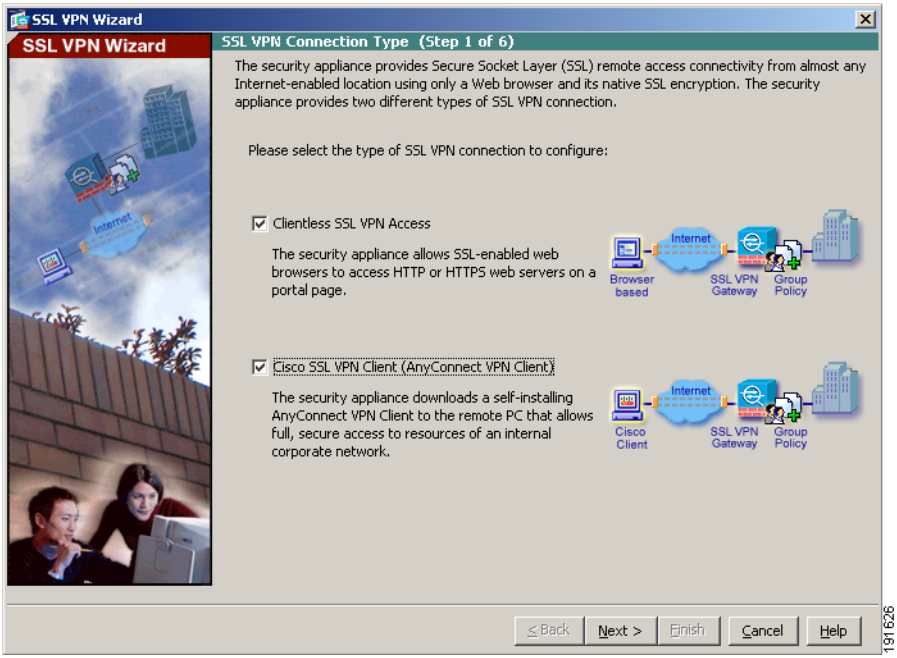
メイン ASDM ウィンドウが表示されます。


Cisco ASDM 6.0 for ASA
File View Tools Wizards Window Help
Look For:
Find
Home Configuration Monitoring Save Refresh Back Forward Help
cisco
Device List
Home
Device Dashboard
Firewall Dashboard
Device Information
General License
Host Name: asa.cisco.com
ASA Version: 8.0(0)238
Device Uptime: 2d 1h 34m 50s
ASDM Version: 6.0(1)
Device Type: ASA 55xx
Firewall Mode: Routed
Context Mode: Single
Total Flash: 256 MB
Total Memory: 256 MB
Interface Status
Interface IP Address/Mask Line Link Kbps
home no ip address down down 0
inside 192.168.1.1/24 down down 0
outside 209.165.200.225 up up 8
Select an interface to view input and output Kbps
VPN Tunnels
IKE: 0 IPsec: 0 Clientless SSL VPN: 0 SSL VPN Client: 0
Traffic Status
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
System Resources Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
Latest ASDM Syslog Messages
Severity Date Time Syslog ID Source IP Destination IP Description
6 Mar 24 2007 02:22:39 302021 209.165.200.234 10.86.194.170 Teardown ICMP connection for faddr 209.165.200.234/0 gaddr 10.86.194.170/9154 laddr
6 Mar 24 2007 02:22:39 302021 209.165.200.234 10.86.194.170 Teardown ICMP connection for faddr 209.165.200.234/0 gaddr 10.86.194.170/9153 laddr
6 Mar 24 2007 02:22:35 302020 209.165.200.234 10.86.194.170 Built outbound ICMP connection for faddr 209.165.200.234/0 gaddr 10.86.194.170/9154
Device configuration loaded successfully.
<admin> 15
3/24/07 2:22:38 AM UTC
191841

Cisco AnyConnect VPN クライアント用の ASA 5505 の設定

設定プロセスを開始するには、次の手順に従います。

ステップ 1　メイン ASDM 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

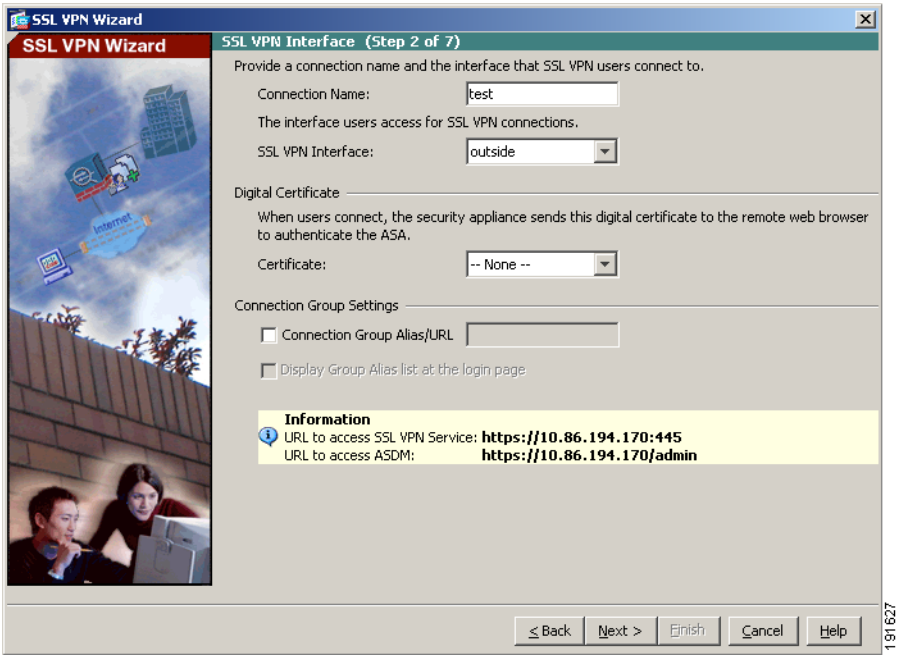
SSL VPN Wizard の Step 2 で、次の手順に従います。

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

（注）　ASA 5505 は、デフォルトで自己署名証明書を生成します。しかし、セキュリティを強化するため、システムを本番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。



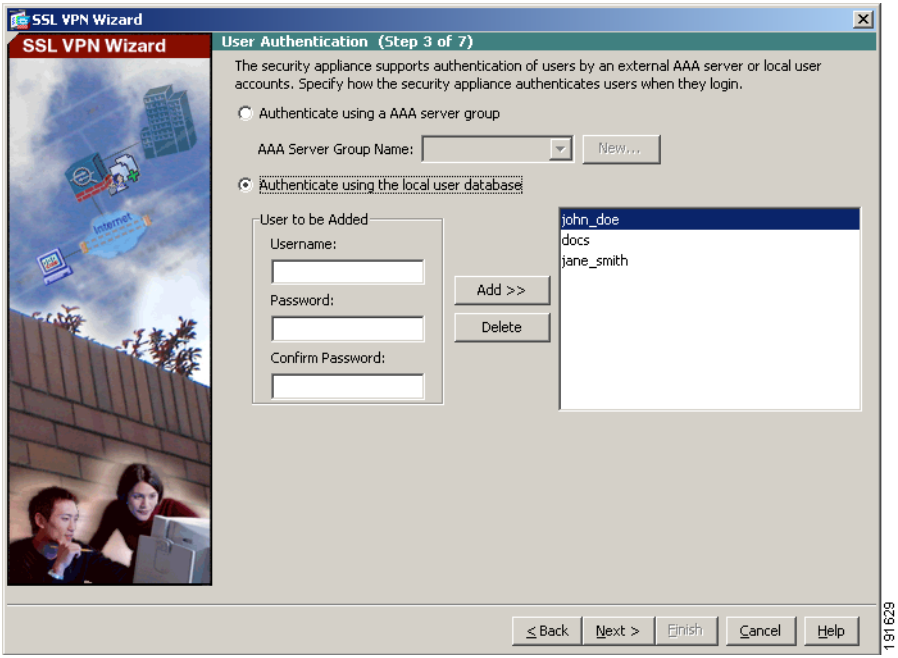
ステップ 4　**Next** をクリックして続行します。

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　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、次の手順に従います。

a. **Authenticate Using an 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。

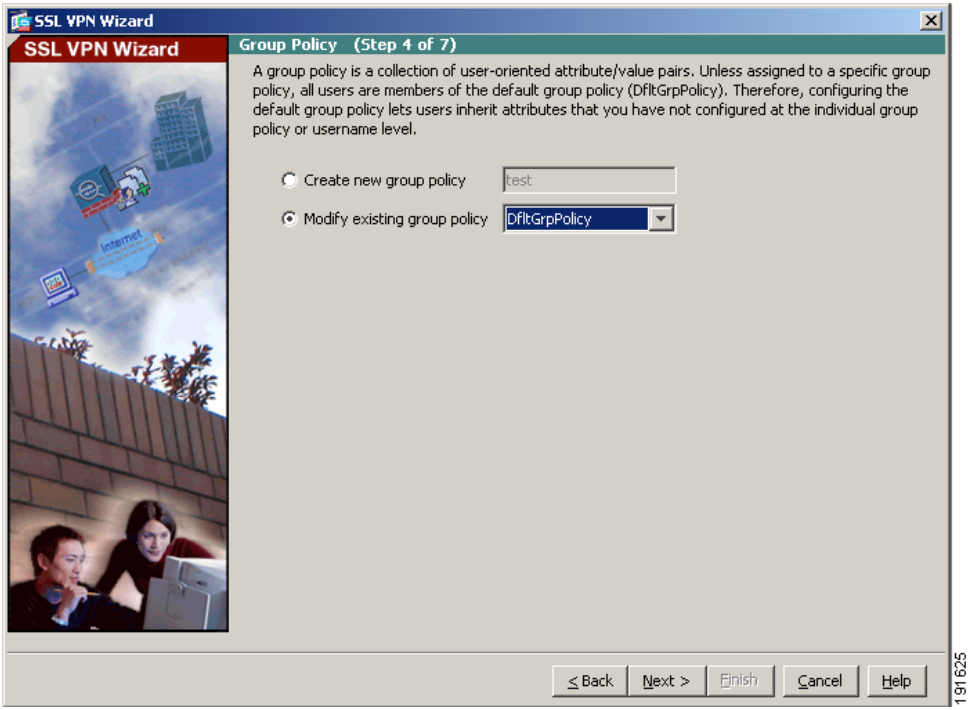
グループ ポリシーの指定

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。この手順は AnyConnect VPN クライアント接続には適用されないので、**Next** を再度クリックします。

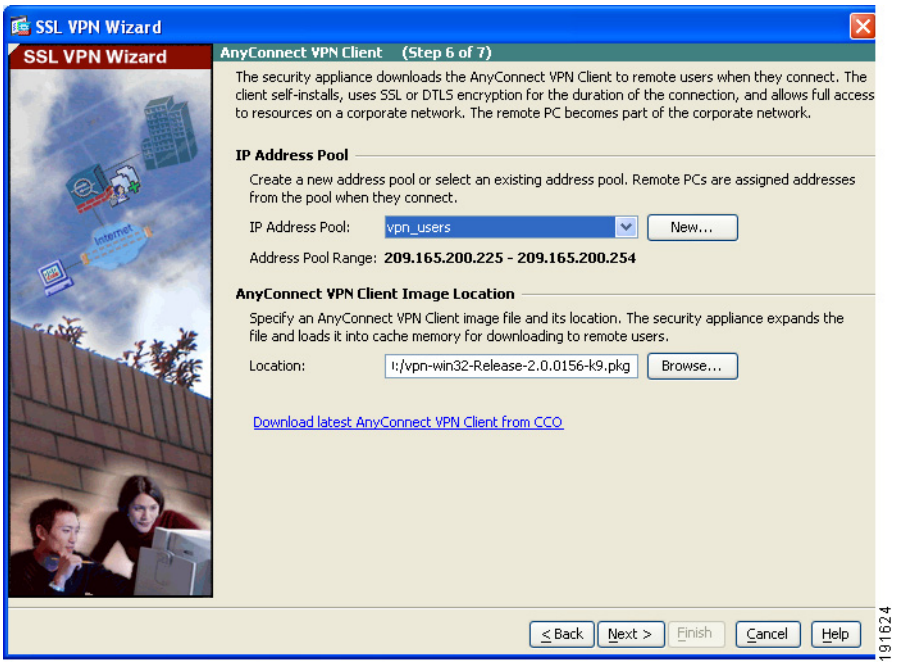
Cisco AnyConnect VPN クライアントの設定

リモート クライアントが Cisco VPN クライアントを使用してネットワークにアクセスするには、接続に成功したときにリモート VPN クライアントに割り当てられる可能性のある 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、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 アプライアンスが AnyConnect ソフトウェアをユーザに配信できるよう、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　事前設定されているアドレス 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。

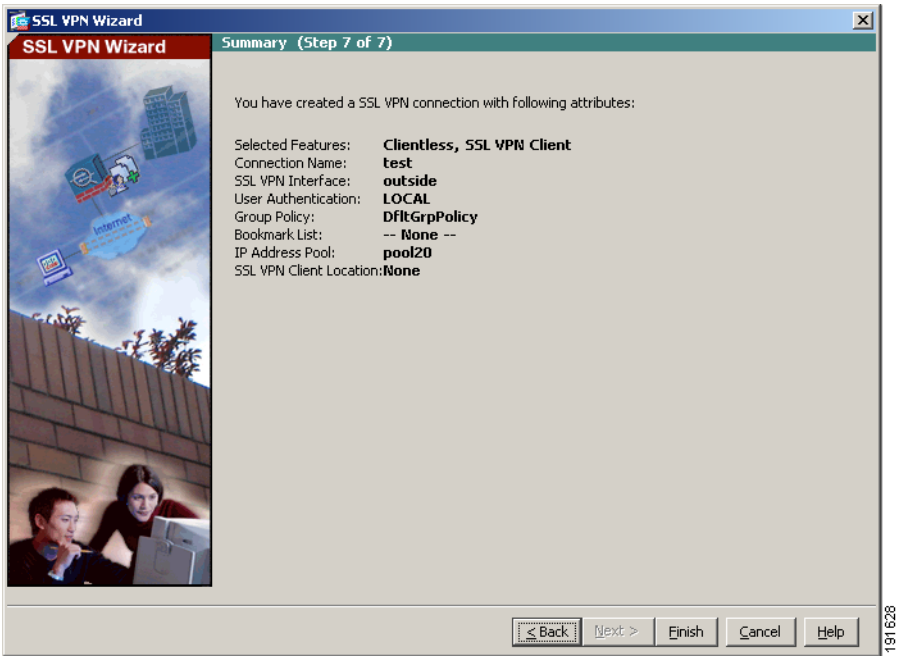
ステップ 3　AnyConnect VPN クライアント ソフトウェア イメージの場所を指定します。

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 cisco.com 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 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 接続のサポートのみを目的として適応型セキュリティ アプライアンスを配置する場合は、これで初期設定が終了しました。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」
サイトツーサイト VPN の設定	第 10 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：Cisco AnyConnect VPN クライアント用の接続の設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 9 章「シナリオ：SSL VPN クライアントレス接続」

次の作業