CHAPTER 10

シナリオ：Cisco AnyConnect VPN Client 用の接続の設定

この章では、リモート ユーザが Cisco AnyConnect VPN Client 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 Client 接続について

SSL VPN Client をセットアップすると、ユーザは接続の確立を試行する前に、ソフトウェア クライアントをインストールする必要がなくなります。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。ブラウザによってこのインターフェイスに接続され、SSL VPN のログイン画面が表示されます。ユーザの認証が成功し、適応型セキュリティ アプライアンスによってユーザがクライアントを要求していることが確認されると、リモート コンピュータのオペレーティング システムに一致するクライアントがプッシュされます。

（注） 初めて Cisco AnyConnect VPN Client をインストールまたはダウンロードするときに、管理権限が必要です。

ダウンロード後、Cisco AnyConnect VPN Client は自動的にインストールおよび設定が行われ、セキュアな SSL 接続が確立されます。接続が終了すると、適応型セキュリティ アプライアンスの設定に応じて、このクライアント ソフトウェアはそのまま残るか、または自動的に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 ソフトウェアをアンインストールしないよう設定している場合、ユーザ認証のときに、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します。

Cisco AnyConnect VPN Client ソフトウェアの入手

適応型セキュリティ アプライアンスは、Cisco の Web サイトから AnyConnect VPN Client ソフトウェアを入手します。この章では、コンフィギュレーション ウィザードを使用して SSL VPN を設定する手順について説明します。Cisco SSL VPN ソフトウェアは、設定プロセス中に適応型セキュリティ アプライアンスにダウンロードできます。

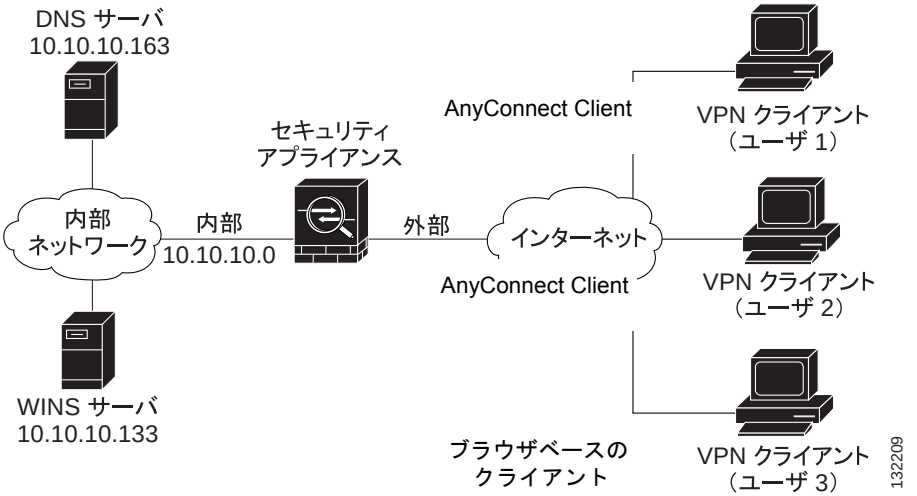
ユーザは、AnyConnect VPN Client を適応型セキュリティ アプライアンスからダウンロードできます。あるいは、システム管理者が手動でリモート PC にインストールできます。このクライアント ソフトウェアのインストールの詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

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。ユーザが接続を確立するたびに自動的にクライアントをプッシュす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か、リモート 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を指定するように求めるよう設定できます。後者の設定では、ユーザが応答しなかった場合に、タイムアウト後にクライアントをプッシュするか、または SSL VPN のログイン画面を表示す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 Client を使用したトポロジの例

図 10-1 は、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要求を受け付け、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ています。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およびブラウザベースのクライアントへの接続をサポートしています。

図 10-1　　SSL VPN シナリオ用のネットワーク レイアウト



Cisco SSL VPN シナリオの実装

この項では、Cisco AnyConnect SSL VPN 接続を受け付け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。設定値の例は、図 10-1 で示す SSL VPN のシナリオから取得されます。

この項では、次のトピックについて取り上げます。

必要な情報

適応型セキュリティ アプライアンスの設定を開始して AnyConnect SSL VPN 接続を受け付けるには、事前に必ず次の情報を準備します。

- リモート ユーザの接続先である、適応型セキュリティ アプライアンス上のインターフェイスの名前。
- デジタル証明書。

  適応型セキュリティ アプライアンスは、デフォルトで自己署名証明書を生成します。ただし、より高度なセキュリティのためには、システムを実稼働環境に配置する前に、公式に信頼できる SSL VPN 証明書を購入する必要があります。
- IP プールで使用される IP アドレスの範囲。これらのアドレスは、接続が成功すると 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の作成に使用されるユーザのリスト（認証に AAA サーバを使用する場合を除く）。
- 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 サーバでの認証を行うための秘密鍵

ASDM の起動

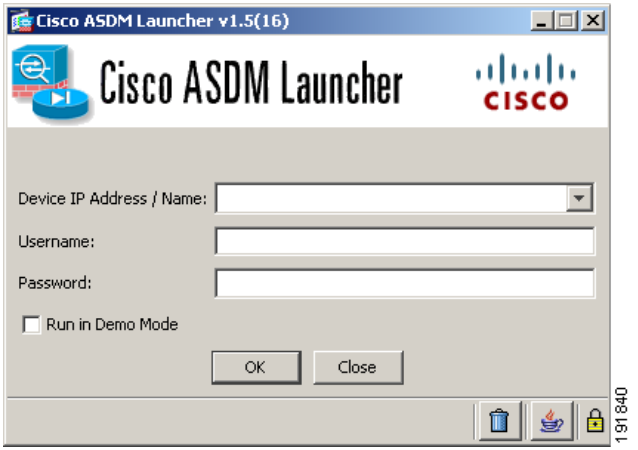
この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法について説明します。ASDM Launcher ソフトウェアをまだインストールしていない場合は、P.7-7 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して直接 ASDM にアクセスする場合は、P.7-10 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 および Password フィールドはブランクのままにします。

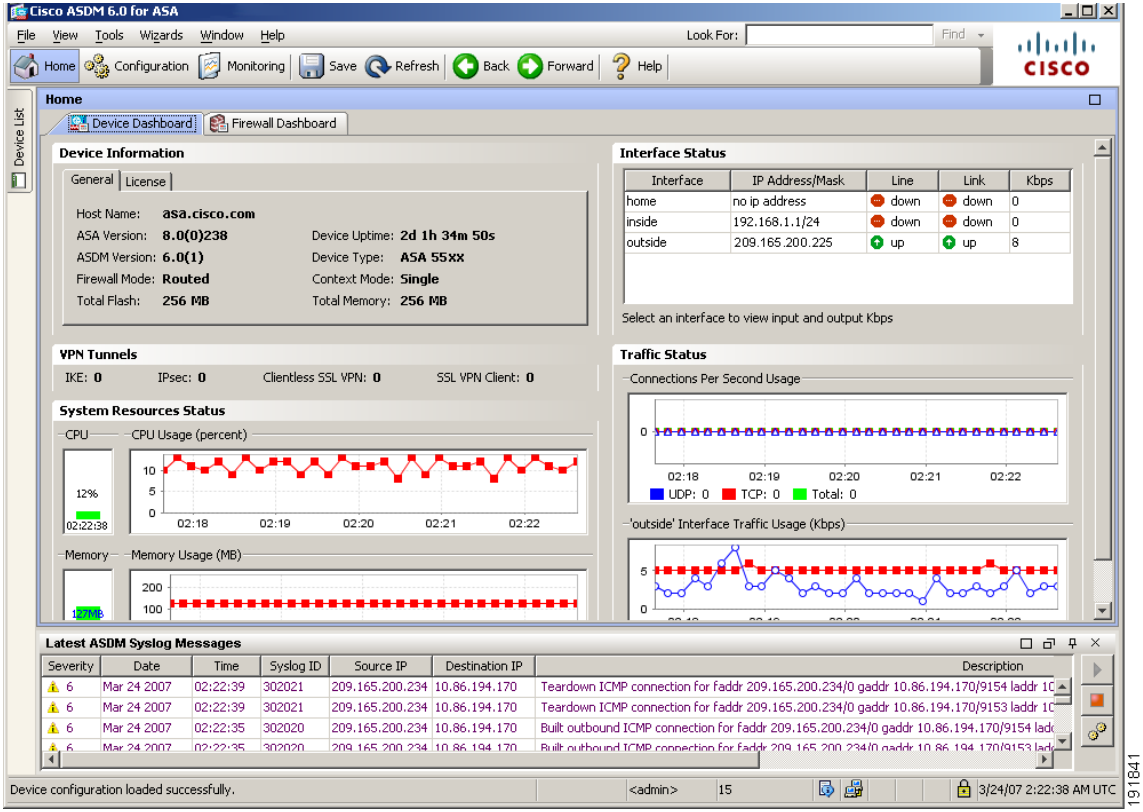
（注）　デフォルトで、Cisco ASDM Launcher には Username および Password は設定されていません。

ステップ 4　OK をクリックします。

ステップ 5　証明書を受け入れるよう要求するセキュリティ警告が表示されたら、**Yes**　をクリックします。

ASA は更新するソフトウェアがあるかどうかを確認し、ある場合は自動的にダウンロードします。

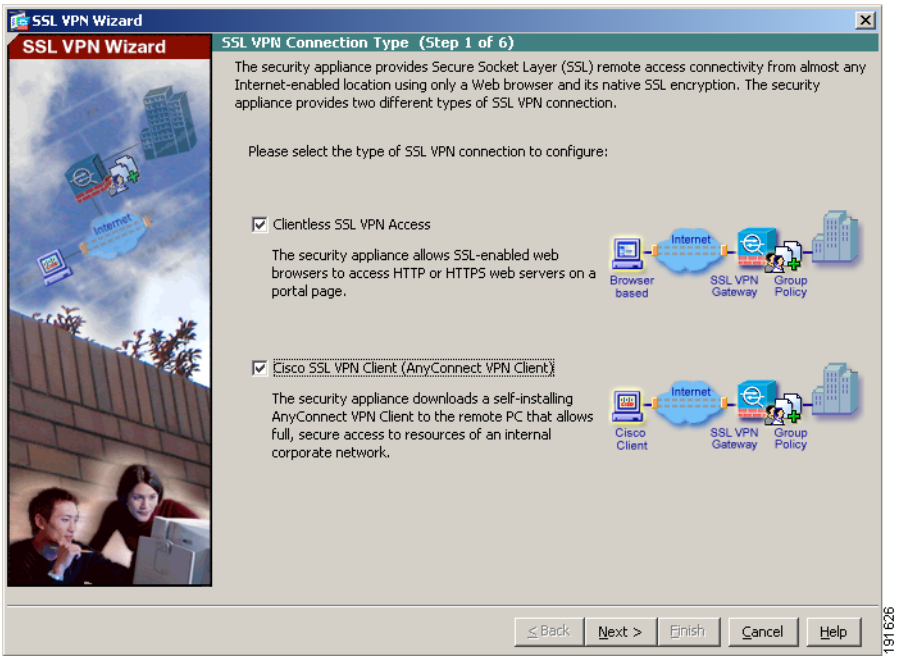
ASDM のメイン ウィンドウが表示されます。


Cisco 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
System Resources Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
'outside' Interface Traffic Usage (Kbps)
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 Client のため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 ウィンドウの Wizards ドロップダウン メニューで、**SSL VPN Wizard** を選択します。SSL VPN Wizard の 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

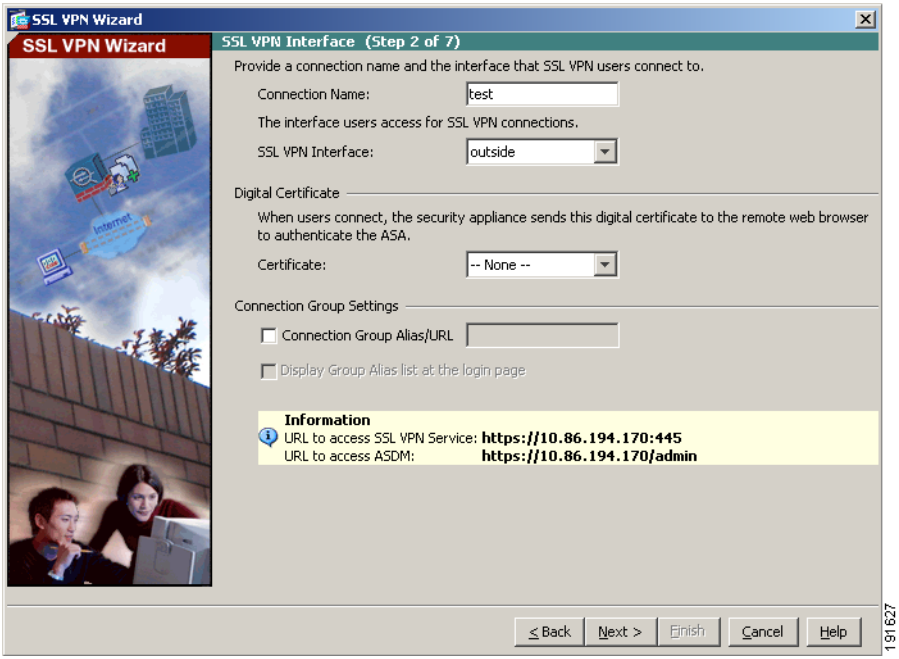
SSL VPN Wizard の Step 2 で、次の手順を実行します。

ステップ 1　リモート ユーザの接続先の接続名を指定します。

ステップ 2　SSL VPN Interface ドロップダウン リストで、リモート ユーザの接続先の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 リストで、ASA が認証のためにリモート ユーザに送信する証明書を選択します。

（注）　適応型セキュリティ アプライアンスは、デフォルトで自己署名証明書を生成します。ただし、より高度なセキュリティのためには、システムを実稼働環境に配置する前に、公式に信頼できる SSL VPN 証明書を購入する必要があります。



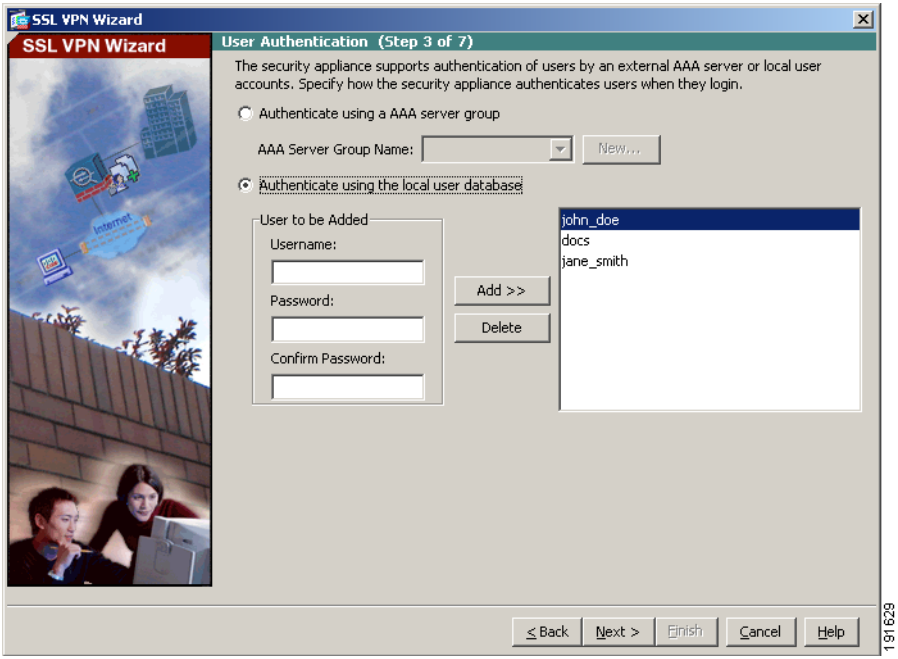
ステップ 4　**Next** をクリックして続行します。

ユーザ認証方式の指定

SSL VPN Wizard の Step 3 で、次の手順を実行します。

ステップ 1　認証に AAA サーバまたはサーバ グループを使用している場合は、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. 既存の AAA サーバ グループ名をドロップダウン リストから選択するか、または **New** をクリックして、新しいサーバ グループを作成します。

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、次のものを指定します。

- 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。

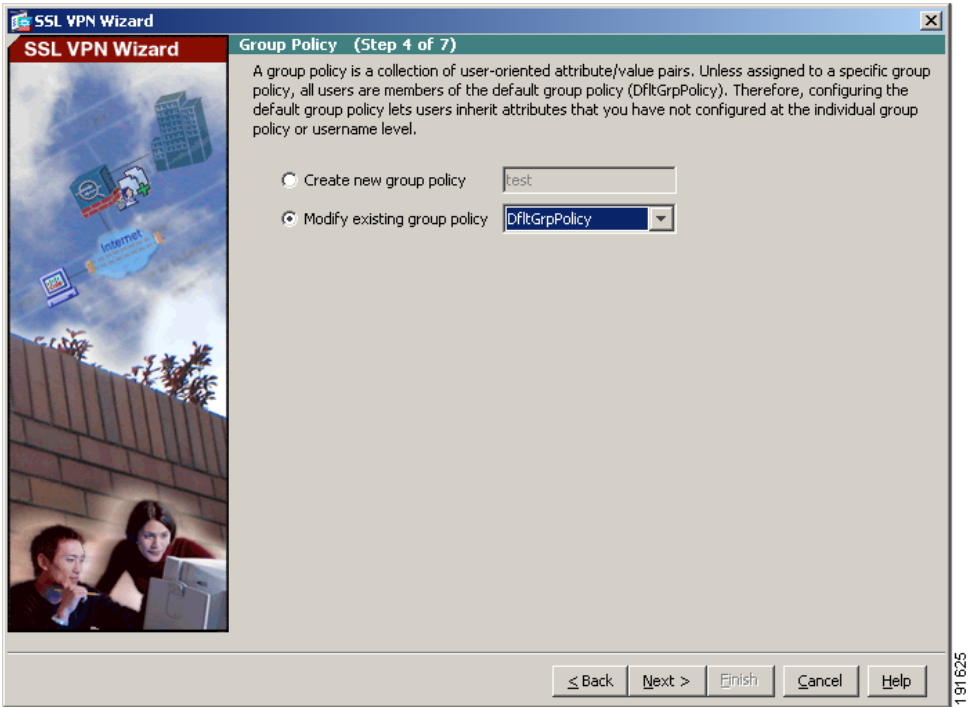
グループ ポリシーの指定

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て、グループ名を指定します。

あるいは、

Modify 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 2　**Next** をクリックします。

ステップ 3　SSL VPN Wizard の Step 5 が表示されます。このステップは AnyConnect VPN Client 接続には適用されないため、もう一度 **Next** をクリックします。

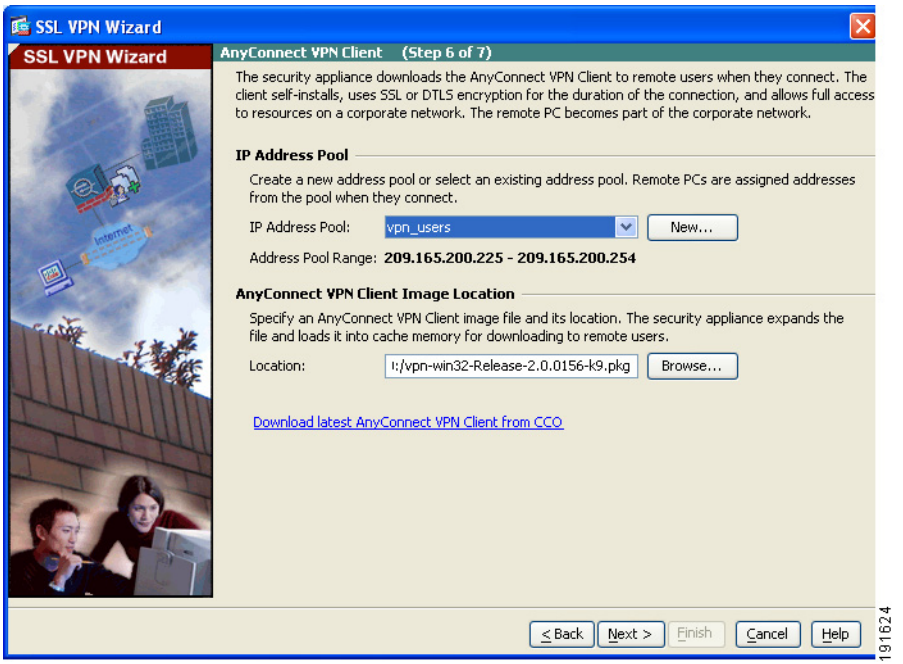
Cisco AnyConnect VPN Client の設定

リモート クライアントが Cisco VPN Client 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。

また、適応型セキュリティ アプライアンスがユーザにプッシュできるようにするため、AnyConnect ソフトウェアのロケーション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 リストからアドレス プールの名前を選択します。



ステップ 2　あるいは、**New** をクリックして、新しいアドレス プールを作成します。

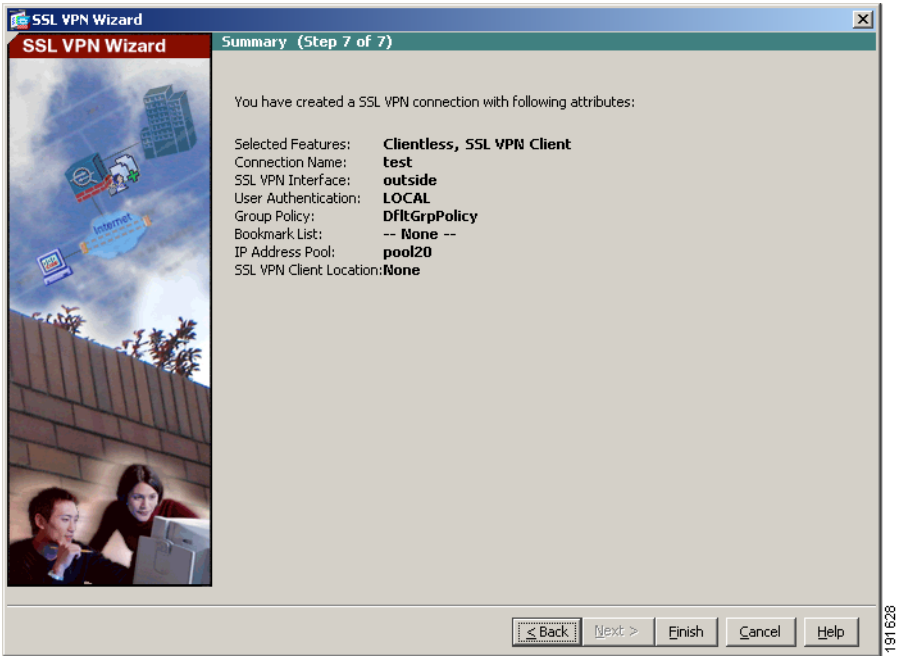
ステップ 3　AnyConnect VPN Client ソフトウェア イメージのロケーションを指定します。

最新バージョンのソフトウェアを入手するには、cisco.com で Download Latest AnyConnect VPN Client をクリックします。この操作により、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、設定を見直して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。

次回のデバイス起動時に変更が適用されるように、設定変更をスタートアップ設定に保存する場合は、File メニューで **Save** をクリックします。あるいは、ASDM の終了時に設定変更の保存を要求するプロンプトが表示されます。

設定変更を保存しない場合は、次回のデバイス起動時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 8 章「シナリオ：DMZ の設定」
サイトツーサイト VPN の設定	第 12 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 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
クライアントレス（ブラウザベース）SSL VPN の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」