CHAPTER 6

シナリオ：SSL VPN クライアントレス接続

この章では、適応型セキュリティ アプライアンスを使用して、ソフトウェア クライアントなしで（クライアントレス）リモート アクセス SSL VPN 接続を受け入れる方法について説明します。クライアントレス SSL VPN では、Web ブラウザを使用して、インターネットを介したセキュアな接続（トンネル）を作成できます。このため、オフサイトのユーザにソフトウェア クライアントまたはハードウェア クライアントを使用せずに、セキュアなアクセスを提供できます。

この章には、次の項があります。

クライアントレス SSL VPN について

クライアントレス SSL VPN 接続を使用すると、インターネット上のほぼすべてのコンピュータから、豊富な Web リソースと Web 対応アプリケーションにセキュアかつ簡単にアクセスできます。アクセスできるものは次のとおりです。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory および FTP ファイル共有
- POP3S、IMAP4S、SMTPS などの電子メール プロキシ
- MS Outlook Web Access
- MAPI
- アプリケーション アクセス（他の TCP ベースのアプリケーションにアクセスするためのポート転送）とスマート トンネル

クライアントレス SSL VPN は、Secure Sockets Layer Protocol（SSL）とその後継プロトコルである Transport Layer Security（TLSI）を使用して、中央サイトで設定するサポート対象の特定内部リソースとリモート ユーザとの間でセキュアな接続を提供します。適応型セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、グループ単位でクライアントレス SSL VPN のユーザにリソースへのアクセス権限を付与します。

クライアントレス SSL VPN 接続のセキュリティに関する検討事項

適応型セキュリティ アプライアンス上のクライアントレス SSL VPN 接続は、特に SSL 対応サーバとの対話方法および証明書の検証に関して、リモート アクセス IPsec 接続とは異なります。

クライアントレス SSL VPN 接続では、適応型セキュリティ アプライアンスがエンドユーザの Web ブラウザとターゲット Web サーバとの間でプロキシとして機能します。ユーザが SSL 対応 Web サーバに接続すると、適応型セキュリティ アプライアンスはセキュアな接続を確立し、サーバの SSL 証明書を検証します。エンドユーザのブラウザは、提示される証明書を受け取ることはありません。したがって、エンドユーザのブラウザでは証明書の検査および検証はできません。

適応型セキュリティ アプライアンス上の現在のクライアントレス SSL VPN の実装では、有効期限が切れた証明書を提示したサイトとの通信は許可されません。また、適応型セキュリティ アプライアンスでは、信頼されている CA 証明書の検証は行われません。そのため、ユーザは、SSL 対応 Web サーバと通信する前に、SSL 対応 Web サーバが提供する証明書を解析することはできません。

SSL 証明書に関するリスクを最小限に抑えるには、次の方法があります。

1. クライアントレス SSL VPN アクセスを必要とするすべてのユーザで構成されるグループ ポリシーを設定し、そのグループ ポリシーに対してのみクライアントレス SSL VPN アクセスをイネーブルにします。
2. クライアントレス SSL VPN ユーザのインターネット アクセスを制限します。たとえば、ユーザがクライアントレス SSL VPN 接続を使用してアクセスできるリソースを制限します。これを実行すると、インターネット上の一般的なコンテンツへのユーザによるアクセスが制限されることがあります。その場合は、クライアントレス SSL VPN ユーザがアクセスできる内部ネットワーク上の特定ターゲットへのリンクを設定できます。
3. ユーザを教育します。SSL 対応サイトがプライベート ネットワーク内部にない場合、ユーザはクライアントレス SSL VPN 接続を介してそのサイトにアクセスすべきではありません。そのようなサイトにアクセスするには、別のブラウザ ウィンドウを開く必要があります。そのブラウザを使用して、提示された証明書を参照します。

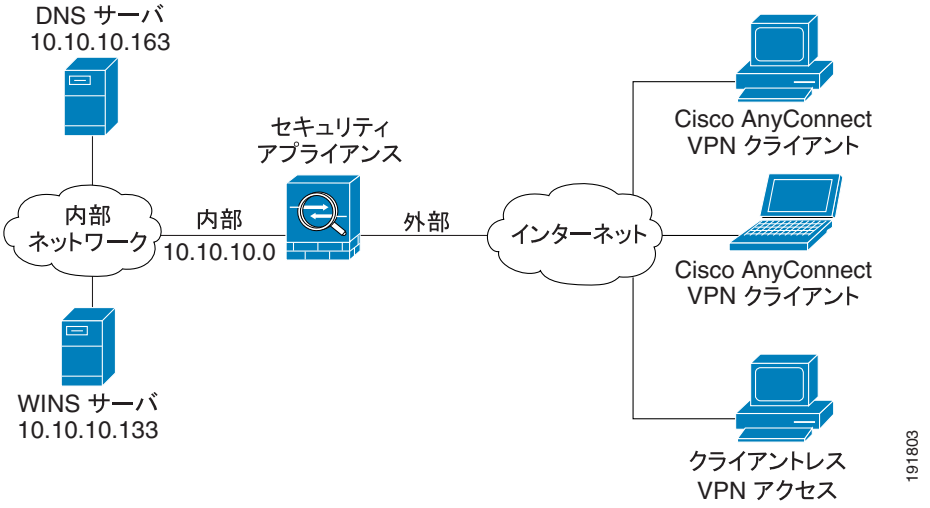
適応型セキュリティ アプライアンスは、クライアントレス SSL VPN 接続に対して、次の機能をサポートしません。

- NAT（グローバルに一意の IP アドレスの必要性を低減する機能）
- PAT（複数のアウトバウンド セッションが単一の IP アドレスから発信されているように見せることを許可する機能）

ブラウザベースの SSL VPN アクセスを使用するネットワークの例

図 6-1 に、Web ブラウザを使用してインターネット経由で SSL VPN 接続要求を受け入れ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。

図 6-1　SSL VPN 接続のネットワーク レイアウト



クライアントレス SSL VPN シナリオの実装

この項では、Web ブラウザからの SSL VPN 要求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 6-1 に示したリモート アクセスの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

リモート アクセス IPsec 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。リモート ユーザがこのインターフェイスに接続すると、SSL VPN ポータル ページが表示されます。
- 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。セキュリティを強化し、かつブラウザの警告メッセージが表示されないようにするために、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。
- 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）。
- AAA サーバ グループ名（認証に AAA サーバを使用している場合）。
- AAA サーバ上のグループ ポリシーに関する次の情報。

  — 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
- リモート ユーザが接続を確立したときに、SSL VPN ポータル ページに表示する内部 Web サイトまたはページのリスト。これは、ユーザが初めて接続を確立したときに表示されるページなので、リモート ユーザが最も頻繁に使用するターゲットを含める必要があります。

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。

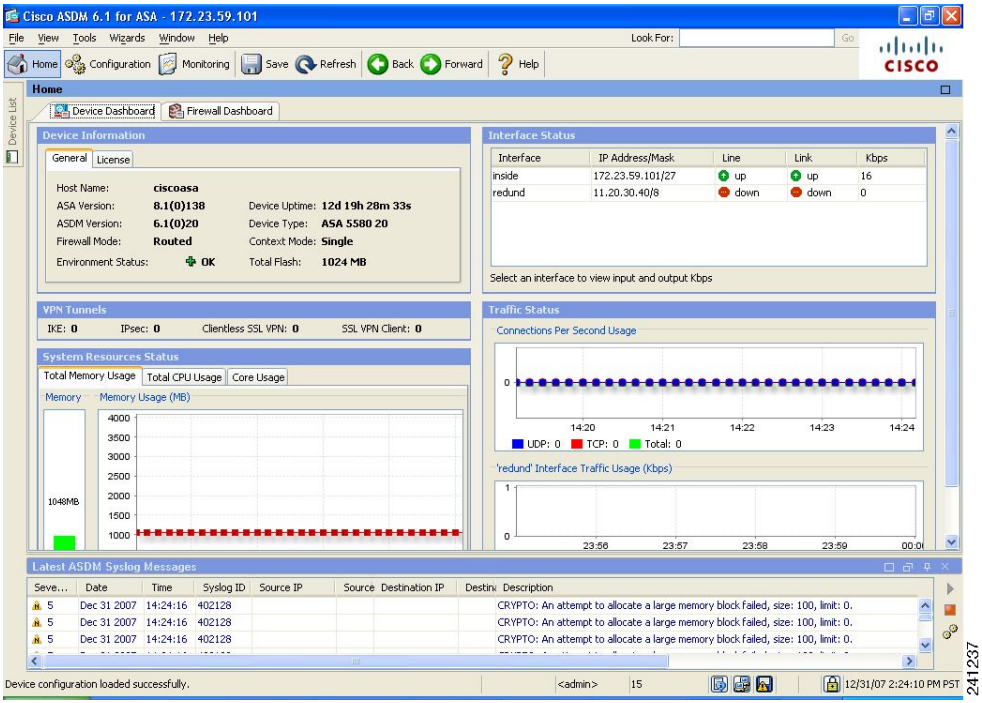
（注）　デフォルトでは、Cisco ASDM Launcher に Username と Password は設定されていません。

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。

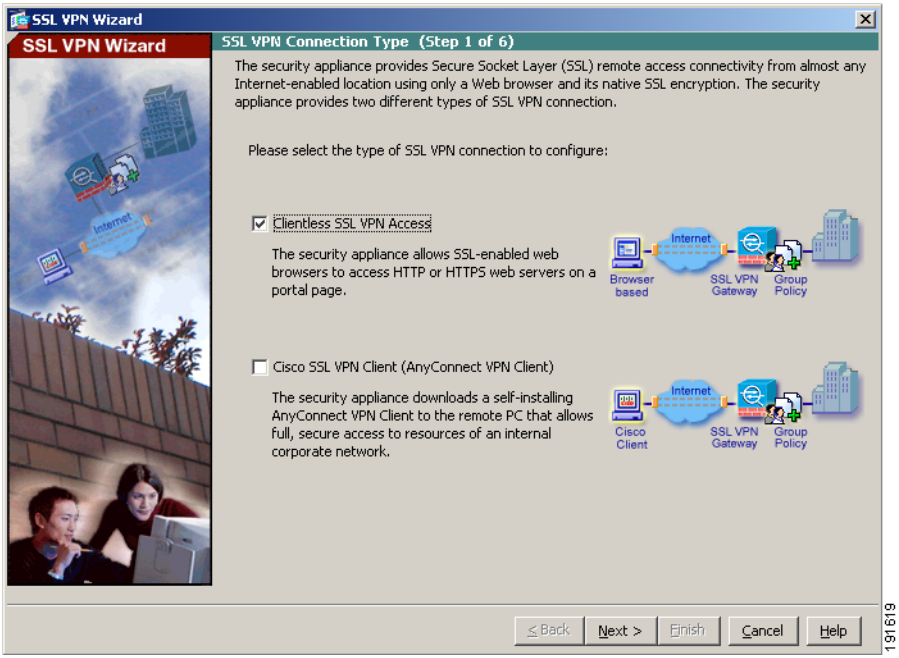
ASDM のメイン ウィンドウが表示されます。


Cisco ASDM 6.1 for ASA - 172.23.59.101
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Home
Device Dashboard Firewall Dashboard
Device Information
General License
Host Name: ciscoasa
ASA Version: 8.1(0)138
ASDM Version: 6.1(0)20
Firewall Mode: Routed
Environment Status: OK
Device Uptime: 12d 19h 28m 33s
Device Type: ASA 5580 20
Context Mode: Single
Total Flash: 1024 MB
Interface Status
Interface IP Address/Mask Line Link Kbps
inside 172.23.59.101/27 up up 16
redund 11.20.30.40/8 down down 0
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
'redund' Interface Traffic Usage (Kbps)
System Resources Status
Total Memory Usage Total CPU Usage Core Usage
Memory Usage (MB)
1048MB
Latest ASDM Syslog Messages
Seve... Date Time Syslog ID Source IP Source Destination IP Destin Description
5 Dec 31 2007 14:24:16 402128 CRYPTO: An attempt to allocate a large memory block failed, size: 100, limit: 0.
5 Dec 31 2007 14:24:16 402128 CRYPTO: An attempt to allocate a large memory block failed, size: 100, limit: 0.
5 Dec 31 2007 14:24:16 402128 CRYPTO: An attempt to allocate a large memory block failed, size: 100, limit: 0.
Device configuration loaded successfully.
<admin> 15
12/31/07 2:24:10 PM PST
241237

ブラウザベースの SSL VPN 接続用の ASA 5580 の設定

ブラウザベースの SSL VPN の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。

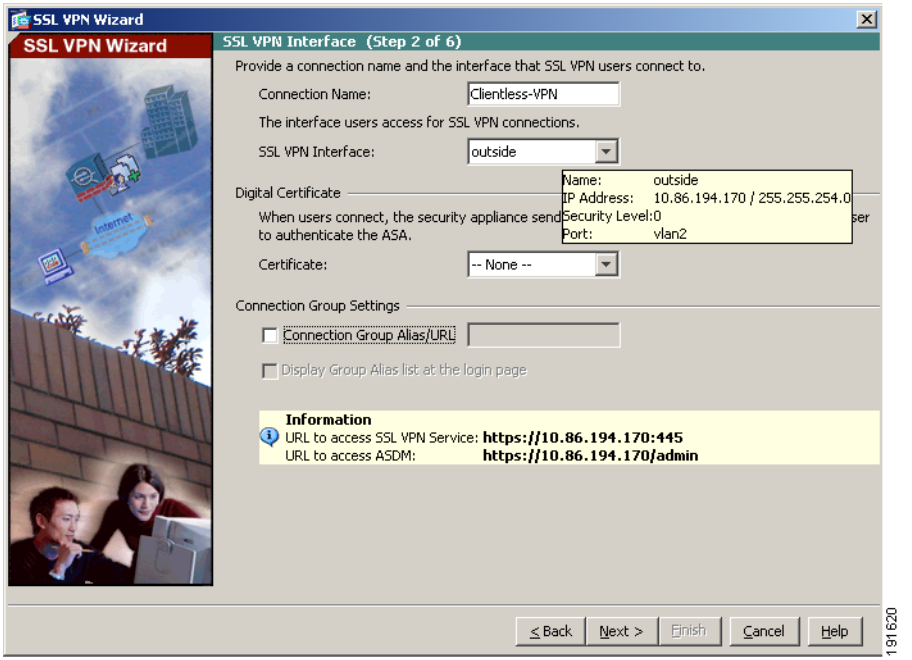
a. **Clientless SSL VPN Access** チェックボックスをオンにします。

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。

（注）　ASA 5580 は、デフォルトで自己署名証明書を生成します。セキュリティを強化し、かつブラウザの警告メッセージが表示されないようにするために、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。

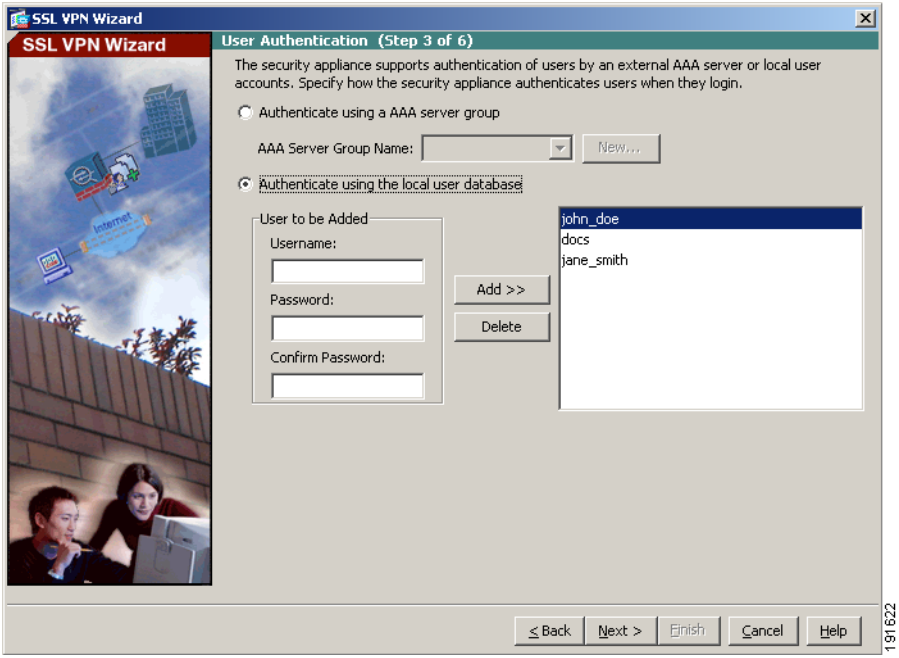
ユーザ認証方式の指定

ユーザは、ローカル認証データベース、または外部認証、認可、アカウンティング（AAA）サーバ（RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP）で認証できます。

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 Server Group Name ドロップダウン リストから事前設定済みのサーバ グループを選択するか、**New** をクリックして新しい AAA サーバ グループを追加します。

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（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。

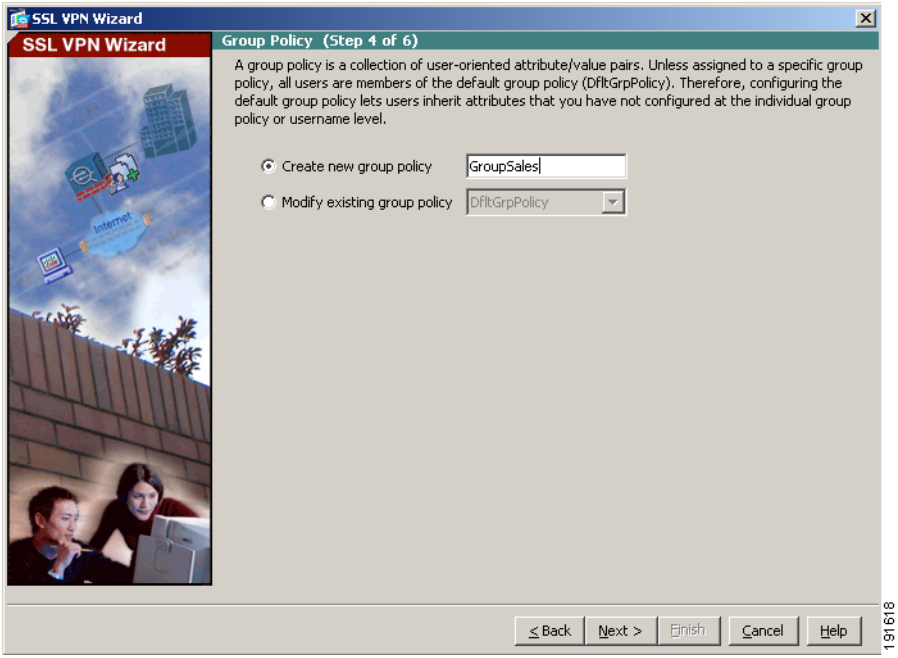
グループ ポリシーの指定

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

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。



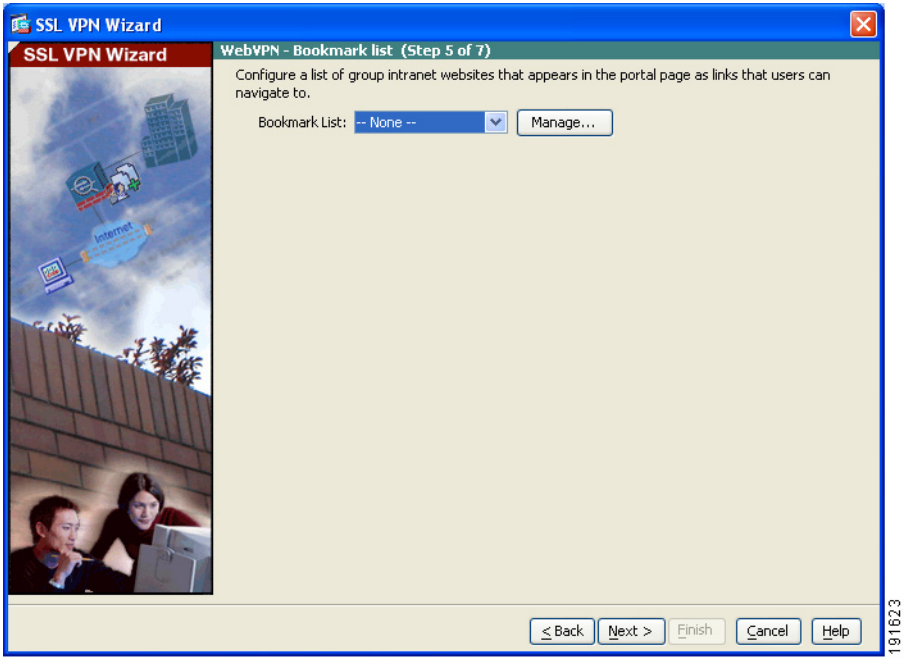
ステップ 2　**Next** をクリックします。

リモート ユーザ用のブックマーク リストの作成

ユーザが簡単にアクセスできるように URL のリストを指定して、ポータル ページ（ブラウザベースのクライアントが適応型セキュリティ アプライアンスへの VPN 接続を確立したときに表示される特別な Web ページ）を作成できます。

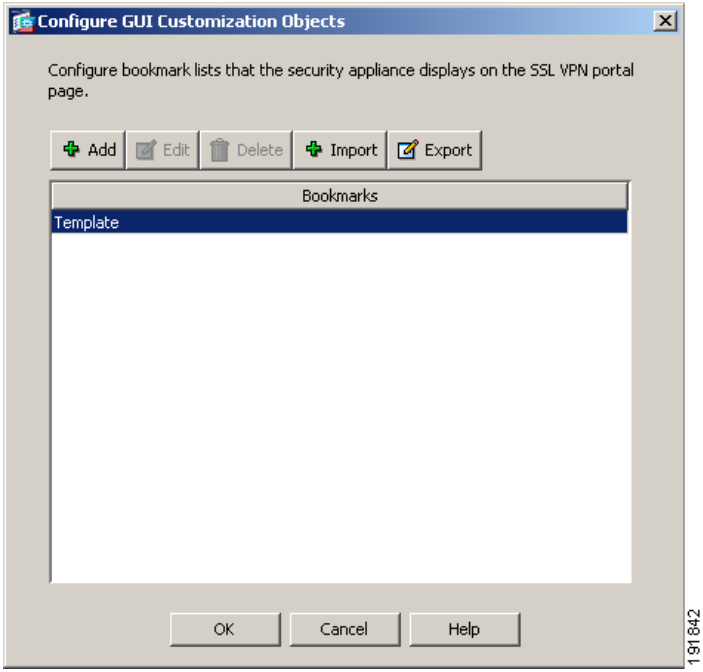
SSL VPN Wizard の Step 5 で、次の手順を実行して、VPN ポータル ページに表示する URL を指定します。

ステップ 1　既存のブックマーク リストを指定するには、ドロップダウン リストからブックマーク リスト名を選択します。



新しいリストを追加するか、既存のリストを編集するには、**Manage** をクリックします。

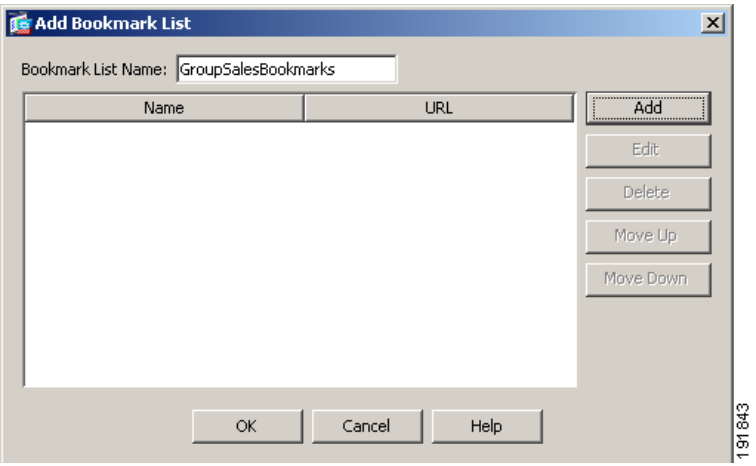
Configure GUI Customization Objects ダイアログボックスが表示されます。



ステップ 2　新しいブックマーク リストを作成するには、**Add** をクリックします。

既存のブックマーク リストを編集するには、リストを選択し、**Edit** をクリックします。

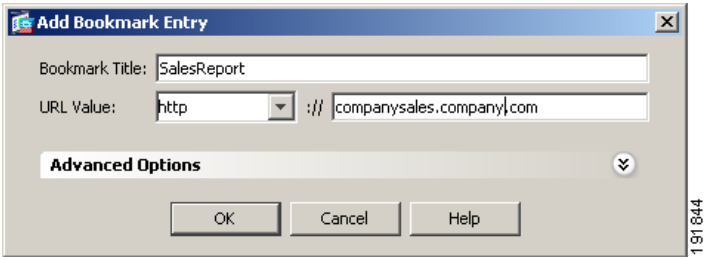
Add Bookmark List ダイアログボックスが表示されます。



ステップ 3　Bookmark List Name フィールドで、作成するブックマーク リストの名前を指定します。この名前は、VPN ポータル ページのタイトルとして使用されます。

ステップ 4　**Add** をクリックして新しい URL をブックマーク リストに追加します。

Add Bookmark Entry ダイアログボックスが表示されます。



ステップ 5　Bookmark Title フィールドで、リストのタイトルを指定します。

ステップ 6　URL Value ドロップダウン リストから、指定する URL のタイプを選択します。たとえば、http、https、ftp などを選択します。

次に、ページの完全な URL を指定します。

ステップ 7　**OK** をクリックして Add Bookmark List ダイアログボックスに戻ります。

ステップ 8　ブックマーク リストの追加が終了したら、**OK** をクリックして Configure GUI Customization Objects ダイアログボックスに戻ります。

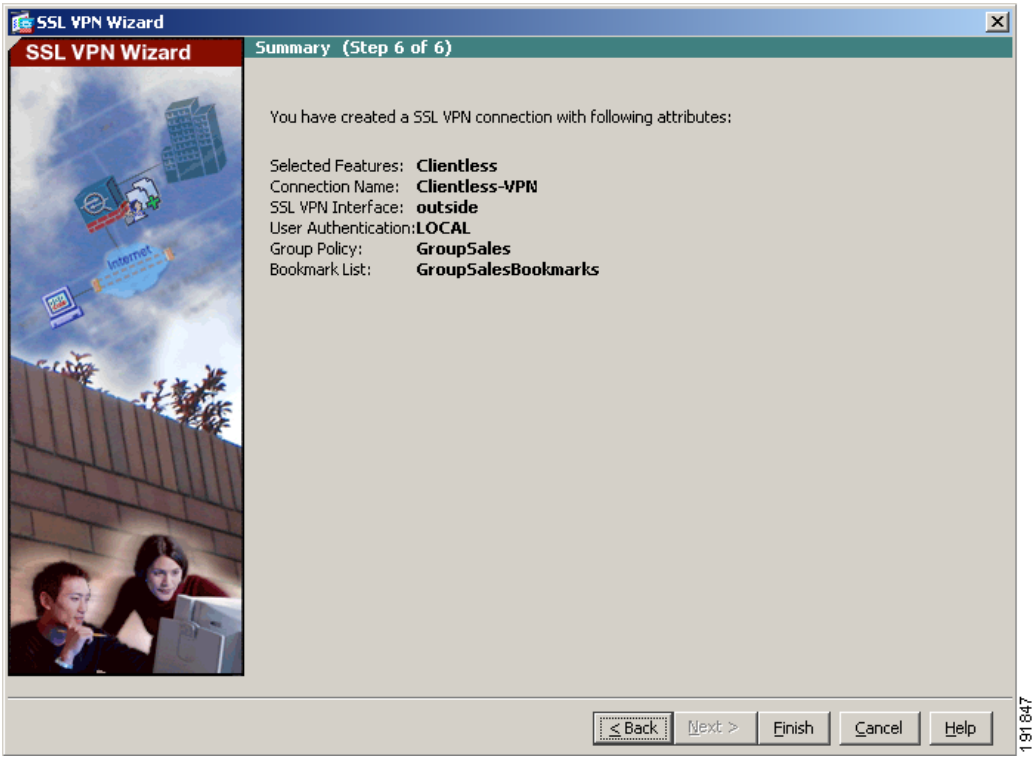
ステップ 9　ブックマーク リストの追加および編集が終了したら、**OK** をクリックして SSL VPN Wizard の Step 5 に戻ります。

ステップ 10　Bookmark List ドロップダウン リストから、この VPN グループのブックマーク リストの名前を選択します。

ステップ 11　**Next** をクリックして続行します。

設定の確認

SSL VPN Wizard の Step 6 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

クライアントレス SSL 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	*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
AnyConnect VPN の設定	第 5 章「シナリオ：Cisco AnyConnect VPN クライアント用の接続の設定」
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 VPN の設定	第 8 章「シナリオ：IPsec リモート アクセス VPN の設定」