



CHAPTER 11

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 クライアントを使用しない (クライアントレス) でリモート 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 を使用すると、Web ブラウザを使用する、インターネットを介したセキュアな接続、つまりトンネルを作成できます。これにより、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していないオフサイトのユーザにセキュアなアクセスを提供できます。

この章は、次の項で構成されています。

- 「クライアントレス SSL VPN について」 (P.11-2)
- 「ブラウザベースの SSL VPN アクセスを使用したネットワークの例」 (P.11-4)
- 「クライアント SSL VPN シナリオの実装」 (P.11-4)
- 「次の作業」 (P.11-15)

クライアントレス SSL VPN について

クライアントレス SSL VPN 接続によって、インターネット上のほぼすべてのコンピュータから、さまざまな Web リソースおよび Web 対応アプリケーションに対する、セキュアで簡単なアクセスが可能になります。アクセスできるものには次のものがあります。

- 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、および SMTPS などの E 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 フォワーディング）およびスマート トンネル

クライアントレス SSL VPN では、Secure Sockets Layer (SSL) プロトコルとその後継プロトコルである Transport Layer Security (TLS) を使用することで、リモート ユーザと、中央サイトで設定した特定のサポート対象のリソース間のセキュアな接続を実現しています。適応型セキュリティ アプライアンスが、プロキシする必要がある接続を認識し、HTTP サーバが認証サブシステムと情報をやりとり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 接続に関するセキュリティ上の考慮事項

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 対応サーバと情報をやりとりする方法と、証明書の確認に関して、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 サーバ間のプロキシとなります。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 アプライアンスによってセキュアな接続が確立され、サーバの SSL 証明書が確認されま

す。エンド ユーザのブラウザが提示された証明書を受け取ることはありません。そのため、エンド ユーザのブラウザによってその証明書を検証および確認はできません。

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 の現在の実装では、有効期限が切れた証明書を提示する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 アプライアンスによって、信頼されている CA 証明書が確認されることもありません。そのためユーザは、SSL 対応 Web サーバと通信する前に同サーバが提示する証明書を分析できません。

SSL 証明書に関するリスクを最小限に抑えるには、次を実行します。

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 ポリシーに関してだけ、そのアクセスをイネーブルにする。
2. 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するなどして、クライアントレス SSL VPN ユーザのインターネット アクセスに制限を加える。そのために、ユーザのインターネット上の一般的なコンテンツへのアクセスを制限することも可能です。その場合、クライアントレス SSL VPN のユーザにアクセスを許可したい内部ネットワーク上の特定のターゲットへのリンクをすることも可能です。
3. ユーザを教育する。SSL 対応サイトがプライベート ネットワーク内でない場合、ユーザがクライアントレス SSL VPN 接続を介してそのサイトにアクセスすることを禁止する必要があります。ユーザは、別のブラウザ ウィンドウを開いてこのサイトにアクセスし、そのブラウザを使用して提示された証明書を表示する必要があります。

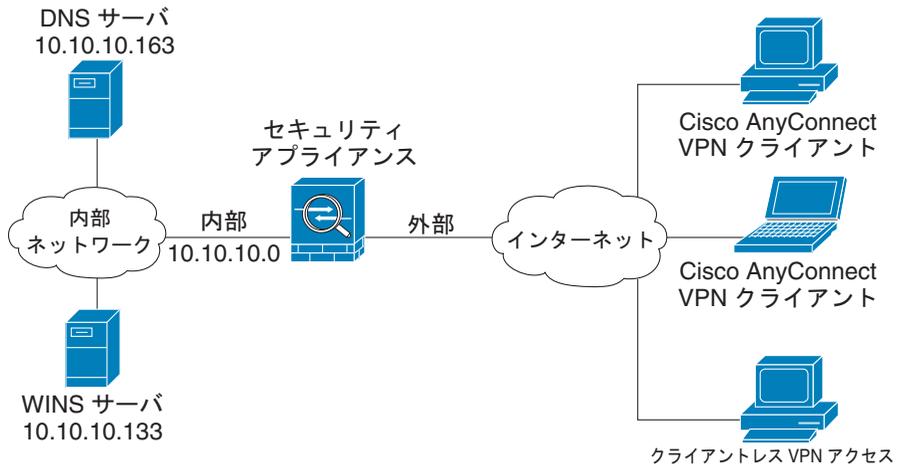
適応型セキュリティ アプライアンスは、クライアントレス SSL VPN 接続の次の機能についてはサポートしていません。

- NAT (IP アドレスがグローバルに一意である必要性を減少させる)
- 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が可能)

ブラウザベースの SSL VPN アクセスを使用したネットワークの例

図 11-1 に、Web ブラウザを使用してインターネットを介した SSL VPN 接続を受け入れ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。

図 11-1 SSL VPN 接続のネットワーク レイアウト



191803

クライアント 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。設定内容の例で使われる値は、図 11-1 に示すリモートアクセス シナリオのものであります。

この項は、次の内容で構成されています。

- 「収集する情報」 (P.11-5)
- 「ブラウザベースの SSL VPN 接続のための適応型セキュリティ アプライアンスの設定」 (P.11-6)
- 「SSL VPN インターフェイスの指定」 (P.11-7)

- 「ユーザ認証方式の指定」 (P.11-8)
- 「グループ ポリシーの指定」 (P.11-10)
- 「リモート ユーザのブックマーク リストの作成」 (P.11-11)
- 「設定内容の確認」 (P.11-14)

収集する情報

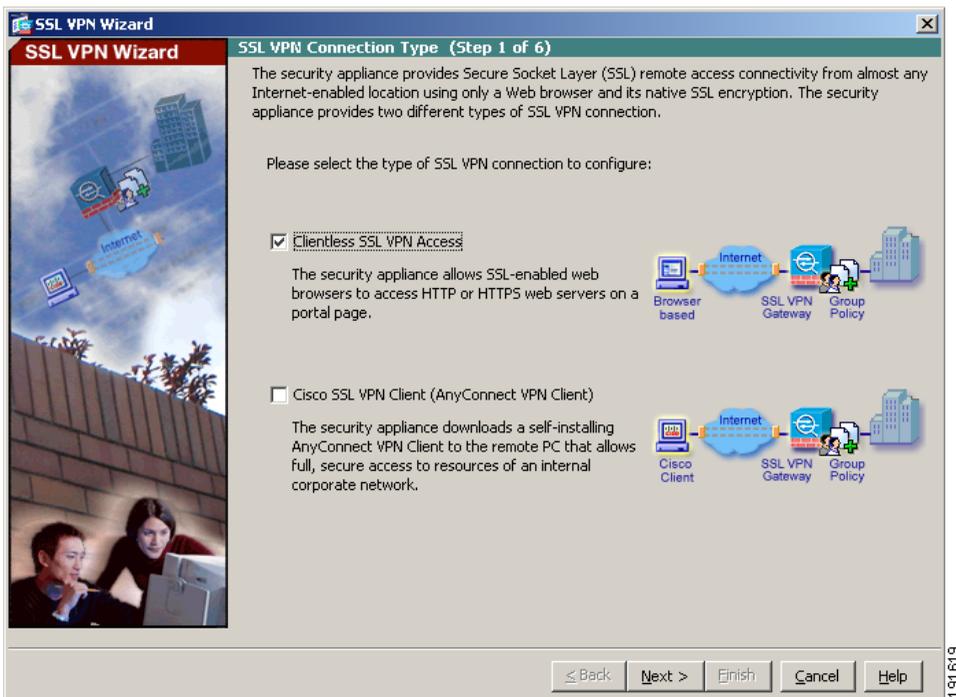
リモート アクセス IPsec VPN 接続を受け入れるように適応型セキュリティ アプライアンスを設定する手順を開始する前に、次の情報を手元に用意してください。

- 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。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。
デフォルトでは、ASA 5500 シリーズによって自己署名証明書が生成されます。セキュリティを強化し、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、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。
- ローカル認証データベースを作成するとき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）。
- AAA サーバ グループ名（認証に AAA サーバを使用する場合）。
- 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キー
- リモート ユーザが接続を確立した時に SSL VPN ポータル ページに表示させる内部 Web サイトまたはページのリスト。これは、ユーザが最初に接続を確立した時に目にするページなので、リモート ユーザにとって最も頻繁に使用するターゲットが表示されている必要があります。

ブラウザベースの SSL VPN 接続のための適応型セキュリティ アプライアンスの設定

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 機能の Step 1 の画面が表示されます。

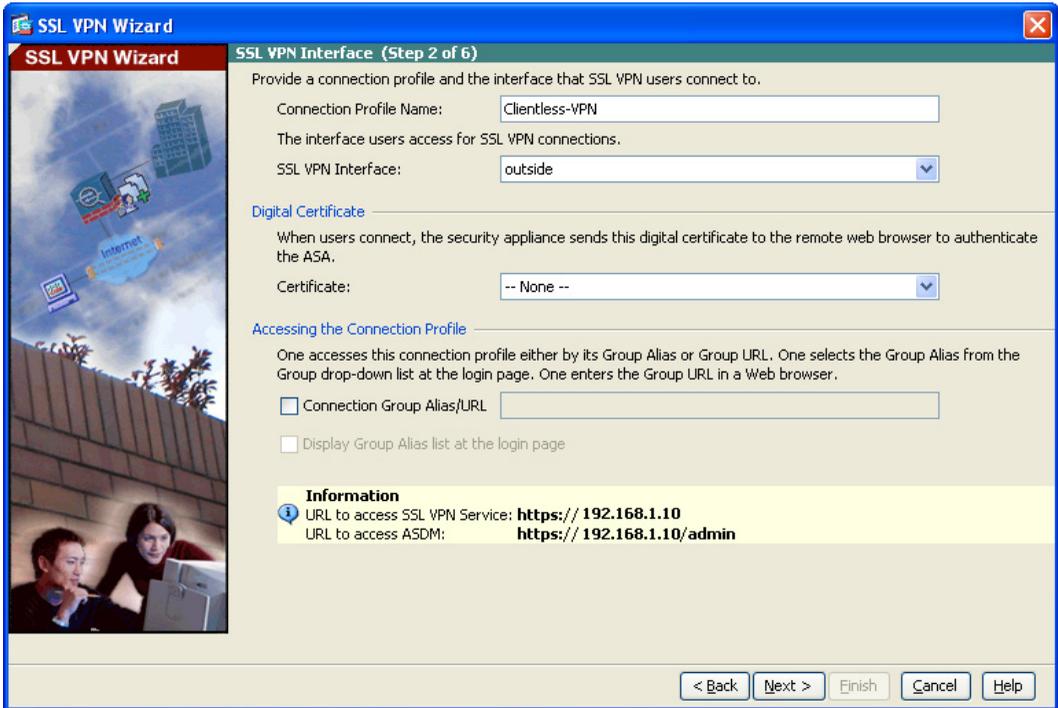


- ステップ 2** SSL VPN Wizard の Step 1 で、次の手順に従います。
- [Browser-based SSL VPN (Web VPN)] チェックボックスをオンにします。
 - [Next] をクリックして続行します。

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。



The screenshot shows the 'SSL VPN Wizard' window at Step 2 of 6, titled 'SSL VPN Interface'. The window has a blue title bar and a red 'X' close button. The main content area is divided into sections:

- SSL VPN Wizard** (left sidebar): A vertical panel with a background image of a person at a computer and various icons (Internet, VPN, etc.).
- SSL VPN Interface (Step 2 of 6)** (main area):
 - Text: 'Provide a connection profile and the interface that SSL VPN users connect to.'
 - Field: 'Connection Profile Name:' with a text box containing 'Clientless-VPN'.
 - Text: 'The interface users access for SSL VPN connections.'
 - Field: 'SSL VPN Interface:' with a dropdown menu showing 'outside'.
 - Digital Certificate** section:
 - Text: 'When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.'
 - Field: 'Certificate:' with a dropdown menu showing '-- None --'.
 - Accessing the Connection Profile** section:
 - Text: 'One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group URL in a Web browser.'
 - Field: 'Connection Group Alias/URL' with a text box.
 - Checkbox: 'Display Group Alias list at the login page' (unchecked).
 - Information** section (yellow background):
 - Text: 'URL to access SSL VPN Service: [https:// 192.168.1.10](https://192.168.1.10)
 - Text: 'URL to access ASDM: [https:// 192.168.1.10/admin](https://192.168.1.10/admin)
- Buttons** (bottom right): '< Back', 'Next >', 'Finish', 'Cancel', 'Help'.

248/751

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。



(注)

デフォルトでは、ASA 5500 シリーズによって自己署名証明書が生成されます。セキュリティを強化し、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、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。

ユーザ認証方式の指定

ユーザの認証は、ローカル認証データベース、または外部の Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントティング) サーバを使用して実行できます (AAA サーバには RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP があります)。

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. 事前設定されているサーバグループを [Authenticate using an AAA Server Group] ドロップダウン リストから選択するか、[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 (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

[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。
-

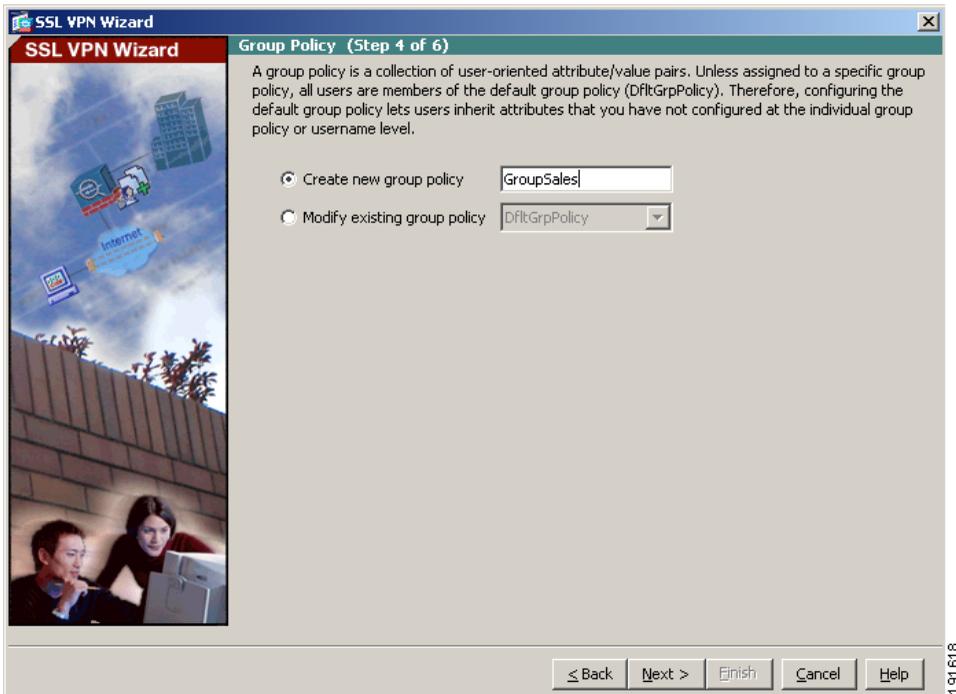
グループ ポリシーの指定

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、

[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。



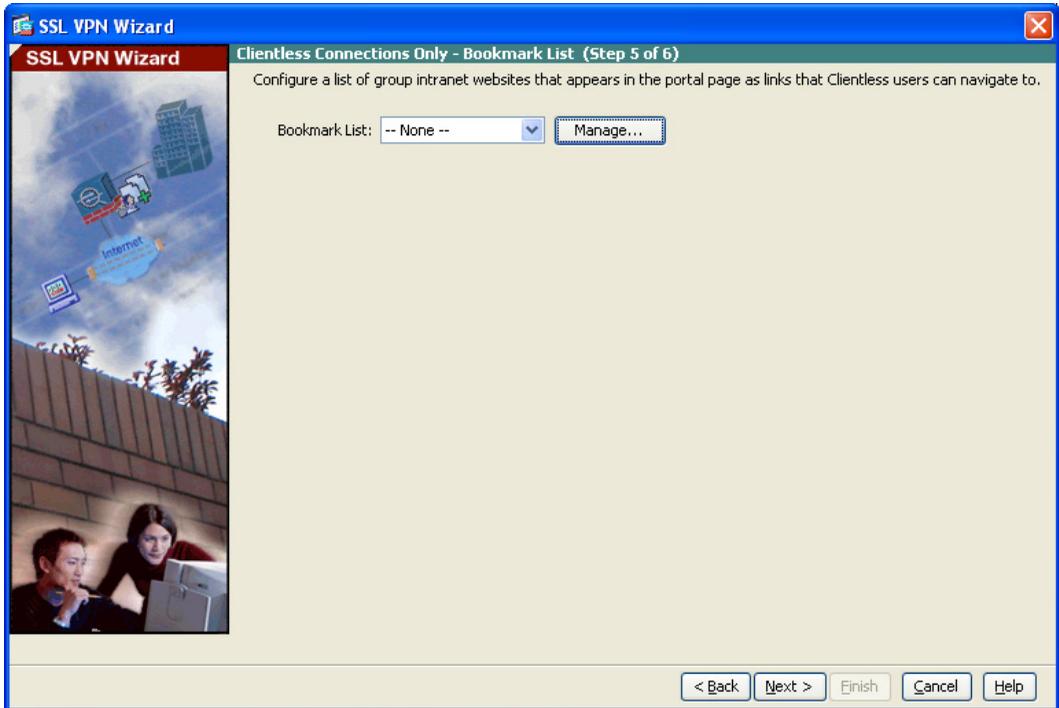
ステップ 2 [Next] をクリックします。

リモート ユーザのブックマーク リストの作成

ユーザが簡単にアクセスできる URL のリストを指定することによって、ポータル ページ、つまり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 接続を確立した時に表示される特別な Web ページを作成できます。

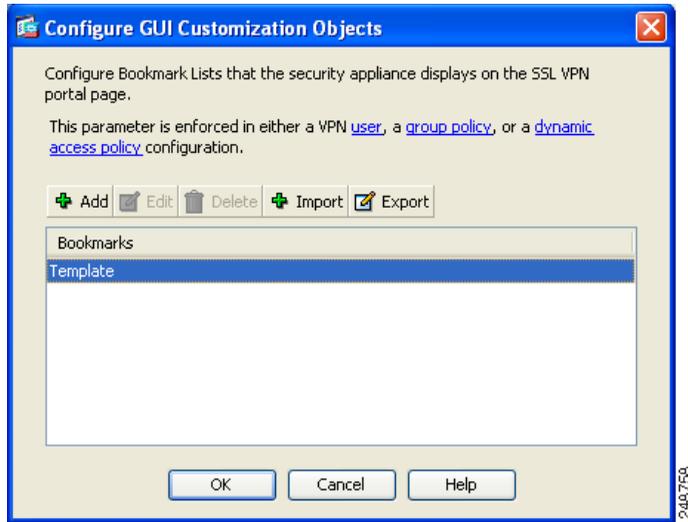
SSL VPN Wizard の Step 5 で、次の手順に従って VPN ポータル ページに表示する URL を指定します。

- 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 リストの名前を選択します。



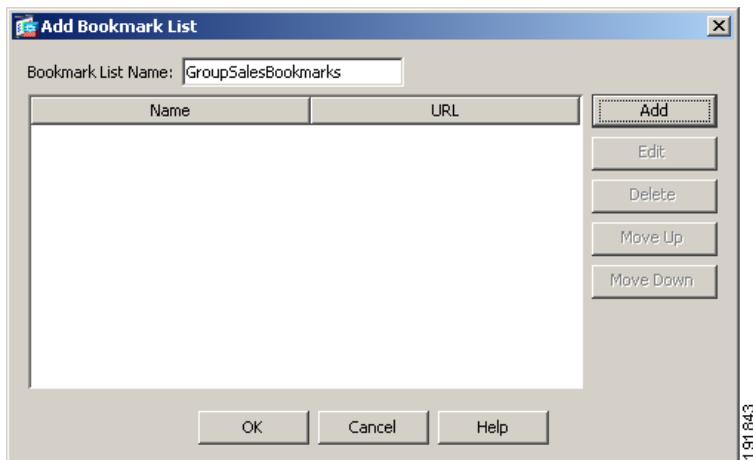
新しいリストを追加したり、既存のリストを編集したりするには、[Manage] をクリックします。

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

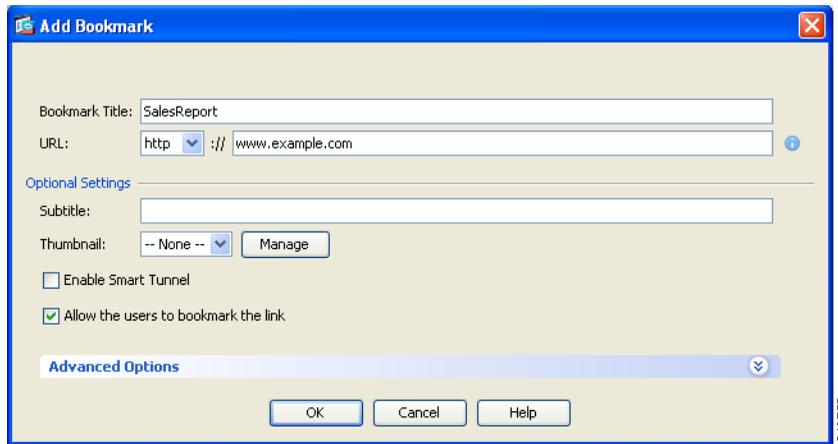


- ステップ 2** 新しいブックマーク リストを作成するには、[Add] をクリックします。
- 既存のブックマーク リストを編集するには、編集するリストを選択して、[Edit] をクリックします。

[Add Bookmark List] ダイアログボックスが表示されます。



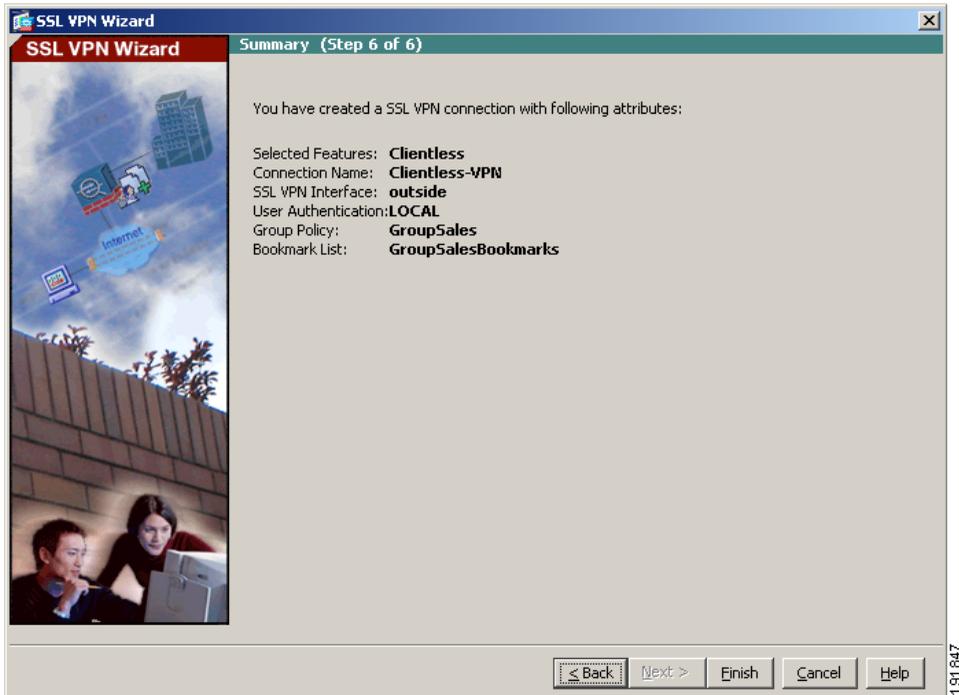
- ステップ 3** [URL List Name] フィールドで、作成するブックマークのリスト名を指定します。このリスト名が VPN ポータル ページのタイトルになります。
- ステップ 4** [Add] をクリックして、ブックマーク リストに新しい URL を追加します。
[Add Bookmark Entry] ダイアログボックスが表示されます。



- 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 の種類を指定します。たとえば、http、https、ftp などを選択します。
次に、ページの完全 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場合、[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。

設定内容の確認

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

クライアントレス SSL VPN 環境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 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
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 8 章「シナリオ : DMZ 設定」
リモートアクセス VPN の設定	第 9 章「シナリオ : IPsec リモートアクセス VPN 設定」
AnyConnect VPN の設定	第 10 章「シナリオ : Cisco AnyConnect VPN クライアント用接続の設定」
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 設定」

■ 次の作業