リモート アクセス VPN の管理の基礎

Cisco Security Manager を使用すると、リモート アクセス IPSec VPN およびリモート アクセス SSL VPN の両方を設定できます。Security Manager では、リモート アクセス VPN を次のように柔軟に設定および管理できます。

既存のライブ デバイス、または設定ファイルから、既存のリモート アクセス VPN 設定ポリシーを検出できる。その後、必要に応じて、新しいポリシーまたは更新されたポリシーを変更および展開できます。

設定ウィザードを使用して、これらの 2 種類のリモート アクセス VPN に基本機能をすばやく簡単に設定できる。

ネットワークに必要な機能を把握している場合は、リモート アクセス VPN を独立して設定できる。ウィザードを使用して基本となるリモート アクセス VPN を作成してから、ウィザードに含まれていない追加機能を別途設定することもできます。

また、Cisco Security Manager に備えられているデバイス ビューまたはポリシー ビューによって、リモート アクセス VPN 設定ポリシーの割り当てを柔軟に行うことができます。

一部のポリシーでは、出荷時のデフォルト ポリシー（プライベート ポリシー）または Security Manager を使用して作成した共有ポリシーのいずれかを割り当てることもできます。

この章は次のトピックで構成されています。

リモート アクセス VPN について

Security Manager では、IPSec と SSL の 2 種類のリモート アクセス VPN をサポートしています。

ここでは、次の内容について説明します。

リモート アクセス IPSec VPN について

リモートアクセス IPSec VPN では、企業のプライベートネットワークとリモートユーザーの間で、暗号化されたセキュアな接続が可能になります。これは、ブロードバンドケーブル接続、DSL 接続、ダイヤルアップ接続などの接続を使用して、インターネットに暗号化された IPSec トンネルを確立して実現されます。

リモート アクセス IPSec VPN は、VPN クライアント、および VPN ヘッドエンド デバイスまたは VPN ゲートウェイで構成されます。VPN クライアントソフトウェアはユーザーのワークステーション上にインストールされ、企業ネットワークへの VPN トンネルアクセスを開始します。VPN トンネルの一方の端が、企業サイトのエッジに位置する VPN ゲートウェイとなります。

VPN クライアントが VPN ゲートウェイ デバイスへの接続を開始すると、Internet Key Exchange（IKE; インターネット キー交換）によるデバイスの認証と、続く IKE Extended Authentication（Xauth; 拡張認証）によるユーザの認証からなるネゴシエーションが行われます。次に、モード設定を使用してグループ プロファイルが VPN クライアントにプッシュされ、IPsec Security Association（SA; セキュリティ アソシエーション）が作成されて VPN 接続が完了します。

ヒント　ASA 8.4(1) 以降のデバイスでホストされるリモートアクセス IPsec VPN には、IKE バージョン 2（IKEv2）を設定するオプションがあります。IKEv2 を使用する場合、通常の IPSec ポリシーに加えて、いくつかの SSL VPN ポリシーを設定する必要があります。また、ユーザは AnyConnect 3.0 以降の VPN クライアントを使用して、IKEv2 接続を確立する必要があります。詳細については、Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （33 ページ）を参照してください。

リモート アクセス IPSec VPN の場合は、AAA（認証、許可、アカウンティング）を使用してセキュアなアクセスを行います。ユーザ認証を行う場合、接続を完了するには有効なユーザ名およびパスワードを入力する必要があります。ユーザ名とパスワードは、VPN デバイス自体に格納することも、他の多数のデータベースに認証を提供できる外部 AAA サーバに格納することもできます。AAA サーバの使用の詳細については、AAA サーバおよびサーバ グループ オブジェクトについてを参照してください。

（注）　サイト間 Easy VPN トポロジでは、リモート アクセス IPsec VPN で使用するものと同じポリシーとポリシー オブジェクトの一部が使用されますが、そのポリシーはリモート アクセス ポリシーとは別に保存されます。Easy VPN でのリモート クライアントは、ルータなどのハードウェア クライアントです。一方、リモート アクセス IPSec VPN でのリモート クライアントは、VPN クライアント ソフトウェアを使用するワークステーションやその他のデバイスです。詳細については、Easy VPN についてを参照してください。

関連項目

- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （33 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス） （48 ページ）
- リモート アクセス VPN ポリシーの概要 （12 ページ）
- リモート アクセス VPN ポリシーの検出 （15 ページ）

リモート アクセス SSL VPN について

SSL VPN を使用すると、ユーザはインターネットが利用できる任意の場所から企業のネットワークにアクセスできます。ユーザーは Secure Socket Layer（SSL）暗号化をネイティブでサポートする Web ブラウザのみを使用して、クライアントレス接続を確立できます。また、フルクライアント（セキュアクライアントなど）やシンクライアントを使用して接続を確立することもできます。

（注） SSL VPN をサポートするのは、ソフトウェア バージョン 8.0 以降が実行され、シングルコンテキスト モードとルータ モードで動作する ASA 5500 デバイス、ソフトウェア バージョン 12.4(6)T 以降が実行されている Cisco 870、880、890、1800、2800、3700、3800、7200、7301 シリーズのルータ、およびソフトウェア バージョン 15.0(1)M 以降が実行されている Cisco 1900、2900、3900 シリーズのルータです。880 シリーズ ルータの場合、ソフトウェアの最小バージョンは 12.4(15)XZ です。これは、Security Manager では 12.4(20)T にマッピングされます。

IOS デバイスでは、SSL 対応の VPN ゲートウェイを介してリモート アクセスが提供されます。リモート ユーザは SSL 対応の Web ブラウザを使用して、SSL VPN ゲートウェイへの接続を確立します。リモート ユーザが Web ブラウザ経由でセキュア ゲートウェイに対して認証されると SSL VPN セッションが確立され、ユーザは企業ネットワーク内部にアクセスできるようになります。ポータルページを使用すると、SSL VPN ネットワークで使用可能なすべてのリソースにアクセスできます。

ASA デバイスでは、リモート ユーザは Web ブラウザを使用して、セキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを確立します。中央サイトで設定した特定のサポート対象内部リソースとリモート ユーザ間のセキュアな接続は、SSL プロトコルによって実現されます。セキュリティ アプライアンスはプロキシ処理が必要な接続を認識し、HTTP ユーザーは認証サブシステムと通信してユーザーを認証します。

ユーザ認証は、ユーザ名とパスワード、証明書、あるいはその両方を使用して行われます。

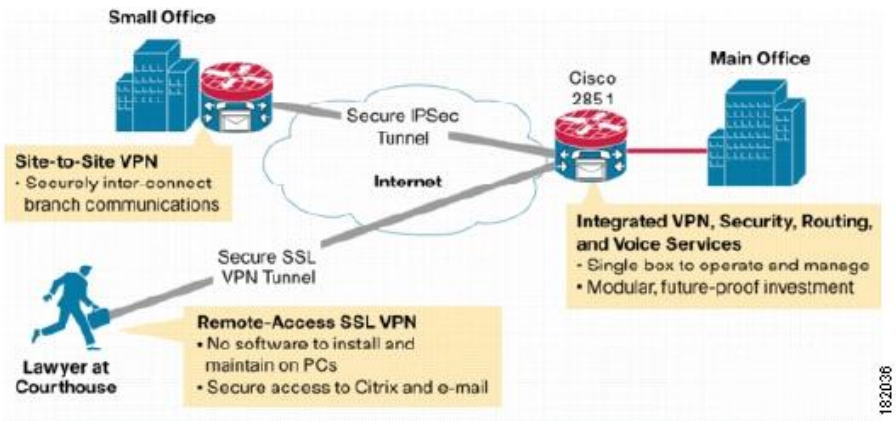
（注） ネットワーク管理者は、SSL VPN リソースへのユーザ アクセスを、個々のユーザ単位ではなくグループ単位で指定します。

ここでは、次の内容について説明します。

リモート アクセス SSL VPN の例

次の図では、モバイル ワーカーが、保護されたリソースにメイン オフィスやブランチ オフィスからアクセスする方法を示します。メイン サイトとリモート サイト間のサイト間 IPSec 接続に変更はありません。モバイル ワーカーが企業ネットワークに安全にアクセスするときに必要なものは、インターネット アクセスとサポートされているソフトウェア（Web ブラウザとオペレーティング システム）だけです。

図 *1*：セキュアな *SSL VPN* アクセスの例



SSL VPN アクセスのモード

SSL VPN には、IOS ルータにリモート アクセスする 3 つのモード（クライアントレス、シンクライアント、およびフル クライアント）が用意されています。ASA デバイスでは、クライアントレス（クライアントレスとシンクライアントポート転送を含む）およびセキュアクライアント（フルクライアント）の 2 つのモードがあります。

クライアントレス アクセス モード

クライアントレス モードでは、リモート ユーザは、クライアント マシンの Web ブラウザを使用して、内部ネットワークまたは企業ネットワークにアクセスします。アプレットのダウンロードは必要ありません。

クライアントレス モードは、インターネット アクセス、データベース、および Web インターフェイスを使用するオンライン ツールなど、想定されるほとんどのコンテンツに Web ブラウザでアクセスする場合に有効です。このモードでは（HTTP および HTTPS による）Web ブラ

ウジング、Common Internet File System（CIFS）によるファイル共有、およびOutlook Web Access（OWA）の電子メールをサポートします。クライアントレスモードが正しく動作するには、リモートユーザーの PC で Windows 2000、Windows XP、または Linux オペレーティングシステムが実行されている必要があります。

Windows オペレーティング システムからブラウザを使用して接続する SSL VPN ユーザは共有ファイル システムを参照でき、フォルダの表示、フォルダとファイルのプロパティの表示、作成、移動、コピー、ローカル ホストからリモート ホストへのコピー、リモート ホストからローカル ホストへのコピー、削除などの操作を実行できます。Web フォルダにアクセスできるようになると、Internet Explorer にそのことが表示されます。このフォルダにアクセスすると、別のウィンドウが開いて共有フォルダが表示されます。フォルダおよびドキュメントのプロパティで許可されている場合、ユーザーはここで Web フォルダの機能を実行できます。

シン クライアント アクセス モード

シン クライアント モードは TCP ポート転送とも呼ばれ、クライアント アプリケーションが TCP を使用して、既知のサーバおよびポートに接続することを前提としています。このモードでは、リモート ユーザはポータル ページに表示されたリンクをクリックして、Java アプレットをダウンロードします。この Java アプレットは、SSL VPN ゲートウェイに設定されているサービスに対する、クライアント マシン上の TCP プロキシとして機能します。Java アプレットは、すべてのクライアント接続に対して新しい SSL 接続を開始します。

Java アプレットは、リモート ユーザ クライアントから SSL VPN ゲートウェイへの HTTP 要求を開始します。HTTP 要求には、内部電子メール サーバの名前およびポート番号が格納されます。SSL VPN ゲートウェイは、その内部電子メール サーバおよびポートに対して TCP 接続を確立します。

シン クライアント モードによって、TCP ベースのアプリケーション（Post Office Protocol Version 3（POP3）、Simple Mail Transfer Protocol（SMTP）、Internet Message Access Protocol（IMAP）、Telnet、Secure Shell（SSH; セキュア シェル）など）へのリモート アクセスがイネーブルになるように Web ブラウザの暗号化機能が拡張されます。

（注） TCP ポート転送プロキシは、Sun の Java ランタイム環境（JRE）バージョン 1.4 以降でのみ動作します。Java アプレットはブラウザを介してロードされ、JRE のバージョンがブラウザで検証されます。互換性のある JRE バージョンが検出されなかった場合、Java アプレットは実行されません。

シン クライアント モードを使用する場合は、次の点に注意する必要があります。

- リモート ユーザが Java アプレットのダウンロードおよびインストールを許可する必要がある。
- TCP ポート転送アプリケーションをシームレスに動作させるには、リモート ユーザの管理権限をイネーブルにする必要がある。
- ポートを動的にネゴシエートする FTP などのアプリケーションには、シン クライアント モードを使用できない。つまり、TCP ポート転送を使用できるのは、スタティックなポートを使用する場合のみです。

フル トンネル クライアント アクセス モード

フル トンネル クライアント モードを使用すると、ネットワーク（IP）レイヤでデータを移動するために使用される SSL VPN トンネルを介して、企業ネットワークにフル アクセスできます。このモードは、Microsoft Outlook、Microsoft Exchange、Lotus Notes E-mail、および Telnet など、ほとんどの IP ベース アプリケーションをサポートします。SSL VPN に接続していることは、クライアントで実行されるアプリケーションに対して完全に透過的です。クライアント ホストと SSL VPN ゲートウェイ間のトンネリングを処理するために、Java アプレットがダウンロードされます。ユーザは、クライアント ホストが内部ネットワークに存在するかのように、任意のアプリケーションを使用できます。

トンネル接続は、グループ ポリシー設定によって指定されます。SSL VPN Client（SVC）またはセキュアクライアント がリモートクライアントにダウンロードおよびインストールされ、リモートユーザーが SSL VPN ゲートウェイにログインしたときにトンネル接続が確立されます。デフォルトでは、接続を閉じるとクライアント ソフトウェアはリモート クライアントから削除されますが、必要に応じてクライアント ソフトウェアをインストールしたままにしておくことができます。

（注） フル トンネル SSL VPN アクセスには、リモート クライアントでの管理権限が必要です。

SSL VPN サポート ファイルの概要と管理

SSL VPN では、デバイスのフラッシュストレージにサポートファイルが存在する必要がある場合があります。これは特に、ASA デバイスに設定されている SSL VPN の場合に該当します。サポートファイルには、Cisco Secure Desktop（CSD）パッケージ、セキュアクライアント イメージ、およびプラグインファイルが含まれています。Security Manager には多数のサポートファイルが同梱されているため、ユーザはそれらのファイルを使用できます。ただし、ポータルページに使用するグラフィックファイル、または セキュアクライアント に使用するクライアントプロファイルなどの一部のサポートファイルは、Security Manager では提供されません。

通常は、ファイル オブジェクトを作成してサポート ファイルを指定してから、そのファイル オブジェクトを参照するポリシーを作成するときに、そのファイル オブジェクトを選択する必要があります。必要なファイル オブジェクトは、ポリシーを作成するときに作成することも、ポリシーの定義を開始する前に作成することもできます。詳細については、[Add File Object]/[Edit File Object] ダイアログボックスを参照してください。

デバイスにポリシーを展開すると、ポリシーで参照されるすべてのサポート ファイルがデバイスにコピーされ、フラッシュ メモリの \csm フォルダに配置されます。ほとんどの場合、このための手動による作業は特に必要ありません。次に、手動の作業が必要となり得る状況をいくつか示します。

- 既存の SSL VPN ポリシーを検出または再検出しようとしている場合は、SSL VPN ポリシーからのファイル参照が正しいものである必要があります。ポリシー検出時にサポート ファイルを処理する方法については、リモート アクセス VPN ポリシーの検出 （15 ページ）を参照してください。

- アクティブ/フェールオーバー設定の ASA デバイスの場合は、フェールオーバー デバイスにサポート ファイルを配置する必要があります。サポート ファイルは、フェールオーバー時にフェールオーバー デバイスにコピーされません。フェールオーバー デバイスにファイルを配置するには、次の方法を選択できます。
  - アクティブ装置の \csm フォルダからフェールオーバー装置にファイルを手動でコピーする。
  - アクティブ装置にポリシーを展開した後、フェールオーバーを強制実行して、アクティブになった装置にポリシーを再展開する。
- VPN クラスタを使用してロード バランシングを行っている場合は、クラスタ内のすべてのデバイスに同じサポート ファイルが展開されている必要があります。

Cisco Secure Desktop（CSD）パッケージ

このパッケージは ASA SSL VPN に使用します。Dynamic Access ポリシーでパッケージを選択します。選択するパッケージには、デバイスで実行されている ASA オペレーティング システムのバージョンとの互換性が必要です。ASA デバイスのダイナミック アクセス ポリシーを作成する場合は、そのデバイスのオペレーティングシステムと互換性のあるバージョン番号が [バージョン（Version）] フィールドに表示されます。

CSD パッケージは、Program Files\CSCOpx\files\vms\repository\ にあります。ファイル名の形式は、securedesktop-asa_k9-version.pkg または csd_version.pkg です。ここで、version は CSD バージョン番号（3.5.1077 など）です。

次に、Security Manager に付属する CSD パッケージについて、CSD と ASA バージョンの互換性を示します。

- csd_3_6_181-3.6.181.pkg：ASA 8.4 以降。
- csd_3_5_2008-3.5.2008.pkg：ASA 8.0(4) 以降。
- csd_3_5_2001-3.5.2001.pkg：ASA 8.0(4) 以降。
- csd_3_5_1077-3.5.1077.pkg - ASA 8.0(4) 以降
- csd_3_5_841-3.5.841.pkg - ASA 8.0(4) 以降
- csd_3_4_2048-3.4.2048.pkg - ASA 8.0(4) 以降
- csd_3_4_1108-3.4.1108.pkg - ASA 8.0(4) 以降
- securedesktop_asa_k9-3.3.0.151.pkg - ASA 8.0(3.1) 以降
- securedesktop_asa-k9-3.3.0.118.pkg - ASA 8.0(3.1) 以降
- securedesktop-asa-k9-3.2.1.126.pkg - ASA 8.0(3) 以降
- securedesktop-asa_k9-3.2.0.136.pkg - ASA 8.0(2) 以降

CSD バージョンと ASA バージョンの互換性については、Cisco.com にある CSD リリースノート（ http://www.cisco.com/en/US/products/ps6742/prod_release_notes_list.html）および「Supported VPN Platforms」を参照してください。

ダイナミック アクセス ポリシーを作成して CSD を指定する方法については、ASA デバイスでの Cisco Secure Desktop ポリシーの設定を参照してください。

セキュアクライアント イメージ

これらのイメージは、ASA でホストされるリモート アクセス SSL および IKEv2 IPsec VPN 用です。セキュアクライアント はユーザーの PC にダウンロードされ、クライアントの VPN 接続を管理します。Cisco Security Manager には、いくつかの Secure Client イメージが含まれています。各イメージは Program Files\CSCOpx\files\vms\repository\ に格納されています。パッケージ名には、ワークステーションのオペレーティングシステムと Secure Client のリリース番号が、anyconnect-*client_OS_information* -*anyconnect_release*.pkg という一般的なパターンで示されます。たとえば、anyconnect-win-3.0.0610-k9-3.0.0610.pkg は、Windows ワークステーション用の AnyConnect 3.0(0610) クライアントです。k9 はパッケージに暗号化が含まれることを示します。この例では、Secure Client のリリース番号が繰り返されています。一部のファイル名では、このリリース番号が一度だけ表示される場合もあります。

パッケージは次のワークステーションの Operating System（OS; オペレーティング システム）で使用できます。各クライアントがサポートする OS バージョン固有の情報については、Cisco.com にある セキュアクライアント のマニュアルを参照してください。

- Linux：パッケージは anyconnect-linux で始まります。64 ビットバージョンの場合は anyconnect-linux-64 で始まります。
- Mac OS：i386 ワークステーション上の Mac OS X では、パッケージは anyconnect-macosx で始まります。Power PC ワークステーション上の Mac OS X では、anyconnect-macosx-powerpc で始まります。
- Windows：パッケージは anyconnect-win で始まります。

他の セキュアクライアント パッケージを Cisco Security Manager サーバーまたはローカルの Cisco Security Manager クライアントにダウンロードして、リモートアクセスポリシーで使用することもできます。Security Manager ではこれらのクライアントのより新しいパラメータを設定できない場合があります。ただし、FlexConfigs を使用してより新しいパラメータを設定できる場合もあります。

セキュアクライアント、そのプロファイル、およびデバイスにクライアントをロードするようにポリシーを設定する方法の詳細については、次の項を参照してください。

- SSL VPN セキュアクライアント の設定について
- SSL VPN セキュアクライアント 設定の構成（ASA）
- Cisco Secure Client プロファイルエディタ

プラグイン ファイル

これらのファイルは、ブラウザ プラグインとして使用されます。プラグインファイルは、Program Files\CSCOpx\files\vms\repository\ にあります。使用可能なファイルの詳細については、SSL VPN ブラウザ プラグインの設定（ASA）を参照してください。

SSL VPN を設定するための前提条件

リモート ユーザが SSL VPN ゲートウェイの背後にあるプライベート ネットワークのリソースに安全にアクセスするには、次の前提条件を満たす必要があります。

- ユーザ アカウント（ログイン名およびパスワード）。
- SSL 対応ブラウザ（Internet Explorer、Netscape、Mozilla、または Firefox など）。
- 電子メール クライアント（Eudora、Microsoft Outlook、または Netscape Mail など）。
- 次のいずれかのオペレーティング システム。
  - Microsoft Windows 2000 または Windows XP。Windows 用の JRE バージョン 1.4 以降、または ActiveX コントロールをサポートするブラウザのいずれかを搭載。
  - Linux。Linux 用の JRE バージョン 1.4 以降を搭載。クライアントレス リモート アクセス モードで Linux から Microsoft の共有ファイルにアクセスするには、Samba のインストールも必要です。

関連項目

- SSL VPN アクセスのモード （4 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（18 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（42 ページ）

SSL VPN の制限

Security Manager の SSL VPN 設定には、次の制限があります。

- SSL VPN ライセンス情報を Security Manager にインポートできない。このため、**vpn sessiondb** および **max-webvpn-session-limit** などの特定のコマンドパラメータを検証できません。
- クライアントレス SSL VPN を使用するには、トポロジ内のデバイスごとに DNS を設定する必要がある。DNS の設定がない場合、デバイスは指定された URL を取得できませんが、IP アドレスで指定された URL だけは取得できます。
- 複数の ASA デバイス間で Connection Profiles ポリシーを共有する場合は、すべてのデバイスが同じアドレス プールを共有することに留意する。ただし、デバイス レベルのオブジェクト オーバーライドを使用して、グローバル定義をデバイスごとの一意なアドレス プー

ルに置き換える場合は除きます。NAT を使用していないデバイスでアドレスが重複しないようにするには、一意なアドレス プールが必要です。

- Cisco Security Manager では、CSM_ で始まる名前（Cisco Security Manager で使用される命名ルール）の SSL VPN のアドレスプールがデバイス設定に含まれる場合、そのプール内のアドレスが SSL VPN ポリシーに設定されたプールと重複するかどうかを検出できない（たとえば、異なる Security Manager インストールでユーザーがプールを設定した場合に発生する可能性があります）。この場合は、展開中にエラーが発生する可能性があります。したがって、Security Manager 内のネットワークまたはホスト オブジェクトと同じ IP アドレス プールを設定し、それを SSL VPN ポリシーの一部として定義することを推奨します。このようにすると、検証が正しく行われるようになります。
- 同じ IP アドレスおよびポート番号を、同じ IOS デバイス上の複数の SSL VPN ゲートウェイで共有できない。このため、重複したゲートウェイがデバイス設定に存在しても、Security Manager のインターフェイスを使用して再定義されなかった場合は、展開エラーが発生する可能性があります。このようなエラーが発生した場合は、別の IP アドレスおよびポート番号を選択して再展開する必要があります。
- SSL VPN ポリシーの一部として AAA 認証またはアカウンティングを定義した場合は、AAA サービスをイネーブルにするために **aaa new-model** コマンドが展開される。SSL VPN ポリシーをあとで削除した場合でも、このコマンドは削除されないことに留意してください。これは、デバイス設定の他の部分で、AAA サービスに **aaa new-model** コマンドが必要な場合があるためです。

（注） また、デバイスには、権限レベルを 15 に指定したローカル ユーザを少なくとも 1 人は定義することを推奨します。この定義により、関連する AAA サーバーを指定しないで **aaa new-model** コマンドを設定した場合でも、デバイスからロックアウトされることがなくなります。

関連項目

- SSL VPN アクセスのモード （4 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（18 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（42 ページ）

各リモートアクセスVPNテクノロジーでサポートされるデバイスについて

リモート アクセス VPN には、IKE Version 1（IKEv1; IKE バージョン 1）IPsec、IKE Version 2（IKEv2; IKE バージョン 2）IPsec、SSL の 3 つのタイプがあります。これらのテクノロジーを

設定できるデバイスは異なります。一般的に、IOS/PIX 6.3 デバイスと比較して、ASA/PIX 7.0 以降では各 VPN タイプの設定は異なります。

次の表に、基本的なデバイスのサポートについて示します。デバイスを選択すると、デバイス タイプによって表示または設定可能なリモート アクセス ポリシーが決まります。

ヒント　デバイスモデルによっては、VPN設定をサポートしていないNO-VPNバージョンがあります。したがって、あるタイプの VPN で 3845 モデルがサポートされていても、3845 NOVPN モデルはサポートされません。さらに、Cisco Catalyst 6500 シリーズ ASA サービスモジュール（ソフトウェアリリース 8.5(x) を実行）は、どのタイプの VPN もサポートしていません。

表 *1*:各リモート アクセス テクノロジーでサポートされているデバイス

テクノロジー	サポートされるプラットフォーム
IKE バージョン 1 IPsec	• ASA/PIX 7.0 以降：シングルコンテキスト モードおよびルータ モードで実行している ASA 5500 シリーズおよび PIX 515、515E、525、535（PIX ソフトウェア 7.0 以降（8.0 以降を含む）を搭載）。 • IOS/PIX 6.3：PIX ソフトウェア 6.3 のみを実行している Cisco IOS セキュリティ ルータ（Aggregation Services Router（ASR; アグリゲーション サービス ルータ）を含む）、Catalyst 6500/7600、および PIX ファイアウォール。
IKE バージョン 2 IPsec	ASA ソフトウェア 8.4(x) のみを実行している ASA 5500 シリーズのみ。
SSL	• ASA：ソフトウェアバージョン 8.0 以降を実行し、シングルコンテキストモードおよびルータモードで実行中の ASA 5500 シリーズ デバイス。 • IOS：ソフトウェア バージョン 12.4(6)T 以降を実行している Cisco 870、880、890、1800、2800、3700、3800、7200、7301 シリーズ ルータ、およびソフトウェア バージョン 15.0(1)M 以降を実行している Cisco 1900、2900、3900 シリーズ ルータ。880 シリーズ ルータの場合、ソフトウェアの最小バージョンは 12.4(15)XZ です。これは、Security Manager では 12.4(20)T にマッピングされます。 ヒント　SSL VPN 設定をサポートしている PIX のバージョンはありません。

関連項目

- リモート アクセス IPSec VPN について　（2 ページ）
- リモート アクセス SSL VPN について　（3 ページ）

• Remote Access VPN Configuration ウィザードの使用 （17 ページ）
• ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要
• IOS および PIX 6.3 デバイスのリモート アクセス VPN ポリシーの概要

リモート アクセス VPN ポリシーの概要

次のリストでは、VPN で使用されているテクノロジーに基づいて、リモート アクセス VPN 設定で使用されているさまざまなポリシーの概要を説明します。可能なリモート アクセス VPN タイプは、IKE Version 1（IKEv1; IKE バージョン 1）IPsec、IKE Version 2（IKEv2; IKE バージョン 2）IPsec および SSL です。これらのポリシーの多くは、特定のデバイス タイプにのみ適用されます。その場合は、そのデバイス タイプが示されます。デバイス タイプごとにまとめられたこのリストについては、次の項を参照してください。

• ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要
• IOS および PIX 6.3 デバイスのリモート アクセス VPN ポリシーの概要

（注） PIX デバイスでは SSL VPN を設定できません。PIX デバイスでは、リモート アクセス IKEv1 IPsec VPN だけをサポートしています。

（注） ダイナミック アクセス ポリシーなどの特定のリモートアクセス VPN ポリシーで、統合 ACL オブジェクト即座にを作成できます。ただし、即座に統合 ACL オブジェクトを作成すると、Cisco Security Manager にエラーメッセージが表示されます。この問題を解決するには、作成した ACL をセレクタウィンドウで選択し、ポリシーを保存する必要があります。

- **リモート アクセス IKEv1 と IKEv2 IPsec および SSL VPN で使用されているポリシー**：
  - **ASA グループロードバランシング**（ASA/PIX 7.0 以降）：リモート クライアント コンフィギュレーションで、複数のデバイスを同じネットワークに接続してリモート セッションを処理している場合、それらのデバイスでセッション負荷を分担するように設定できます。この機能は、ロード バランシングと呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッショントラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロード バランシングは、ASA デバイスで開始されたリモートセッションの場合にだけ有効です。詳細については、グループのロードバランシングについて（ASA）を参照してください。
  - **接続プロファイル**（ASA/PIX 7.0 以降）：接続プロファイルは、トンネル自体の作成に関連する属性を含む、VPN トンネルの接続ポリシーが格納されたレコードのセットです。接続プロファイルでは、ユーザ指向の属性が含まれる特定の接続のグループ ポリシーを識別します。詳細については、接続プロファイルの設定（ASA、PIX 7.0+）を参照してください。

- **ダイナミックアクセス**（ASA 8.0 以降）：個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザが持つさまざまなロール、および設定とセキュリティレベルが異なるリモートアクセスサイトからのログインなど、複数の変数が影響する可能性があります。Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）により、これらの多くの変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。詳細については、リモートアクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス）を参照してください。

- **グローバル設定**：リモートアクセス VPN のすべてのデバイスに適用されるグローバル設定を定義できます。グローバル設定には、Internet Key Exchange（IKE; インターネット キー交換）、IKEv2、IPsec、NAT、フラグメンテーションの定義などがあります。グローバル設定には、通常、ほとんどの状況に適用できるデフォルトが設定されています。そのため、ほとんどの場合、グローバル設定ポリシーの設定はオプションです。デフォルト以外の動作が必要な場合、または IKEv2 ネゴシエーションをサポートする場合だけ設定してください。詳細については、VPN グローバル設定を参照してください。

- **グループポリシー**（ASA/PIX 7.0 以降）：リモートアクセス VPN 接続プロファイルに定義されているユーザグループポリシーを表示できます。このページから、新しい ASA ユーザ グループを指定したり、既存の ASA ユーザ グループを編集したりできます。接続プロファイルを作成するときに、デバイスで使用されていないグループ ポリシーを指定した場合、このグループ ポリシーは自動的に [Group Policies] ページに追加されます。接続プロファイルを作成する前に、このポリシーに追加する必要はありません。詳細については、リモート アクセス VPN のグループ ポリシーの設定を参照してください。

- **Public Key Infrastructure**：Public Key Infrastructure（PKI）ポリシーを作成して、CA 証明書および RSA キーの登録要求を生成し、キーや証明書を管理できます。Certification Authority（CA; 認証局）サーバは、これらの証明書要求を管理し、IPsec または SSL リモート アクセス VPN に接続するユーザに対して証明書を発行するために使用されます。詳細については、Public Key Infrastructure ポリシーについておよびリモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定を参照してください。

- **リモート アクセス IPsec VPN だけで使用されるポリシー**：

  - **証明書から接続プロファイルへのマップ、ポリシーとルール**（IKEv1 IPSec のみ、ASA/PIX 7.0 以降のみ）：証明書から接続プロファイルへのマップポリシーを使用すると、指定したフィールドに基づいて、ユーザの証明書を権限グループと照合するルールを定義できます。認証を確立するため、証明書の任意のフィールドを使用することも、またはすべての証明書ユーザが権限グループを共有することもできます。グループは、DN ルール、[Organization Unit (OU)] フィールド、IKE ID、またはピア IP アドレスから照合できます。これらの方式のいずれかまたはすべてを使用できます。詳細については、Certificate to Connection Profile Map ポリシーの設定（ASA）を参照してください。

- **IKE プロポーザル**：インターネットキーエクスチェンジ（IKE）は、ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーションプロトコルです。IKE は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動確立に使用されます。IKE プロポーザル ポリシーは、IKE ネゴシエーションのフェーズ 1 の要件を定義するときに使用します。詳細については、IKE プロポーザルの設定を参照してください。

- **IPsec プロポーザル（ASA/PIX 7.x）**：IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。このポリシーは、IKE フェーズ 2 ネゴシエーションに使用されます。詳細については、リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）を参照してください。

- **IPsec プロポーザル（IOS/PIX 6.x）**：IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。このポリシーは、IKE フェーズ 2 ネゴシエーションに使用されます。詳細については、リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）を参照してください。

- **ハイアベイラビリティ**（IOS/PIX 6.3）：ハイアベイラビリティ（HA）グループを作成すると HA がサポートされます。HA グループは、Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを実現する、複数のハブデバイスで構成されます。詳細については、リモートアクセス VPN での高可用性の設定（IOS）を参照してください。

- **ユーザーグループ（IOS/PIX 6.x）**：ユーザーグループポリシーには、VPN へのユーザーアクセスおよびVPNの使用を決定する属性を指定します。詳細については、ユーザ グループ ポリシーの設定を参照してください。

- **リモート アクセス IKEv2 IPSec および SSL VPN だけで使用されるポリシー**：

  - **アクセス**（ASA のみ）：アクセスポリシーには、リモートアクセス SSL または IKEv2 IPsec VPN 接続プロファイルをイネーブルにできるセキュリティアプライアンスのインターフェイス、接続プロファイルで使用するポート、Datagram Transport Layer Security（DTLS）設定、SSL VPN セッションタイムアウト、および最大セッション数を指定します。AnyConnect VPN クライアントまたは Secure Client Essentials を使用するかどうかも指定できます。詳細については、SSL VPN アクセスポリシーについて（ASA）を参照してください。

  - **その他の設定**（ASA のみ）：SSL VPN のその他の設定ポリシーでは、キャッシング、コンテンツの書き換え、文字エンコード、プロキシとプロキシバイパス定義、ブラウ

ザプラグイン、Secure Client イメージ と Secure Client プロファイル、Kerberos の制約付き委任、およびその他の詳細設定を定義します。詳細については、他の SSL VPN 設定の定義（ASA）を参照してください。

- **共有ライセンス**（ASA のみ）：[SSL VPN共有ライセンス（SSL VPN Shared License）] ページを使用して、SSL VPN 共有ライセンスを設定します。詳細については、SSL VPN 共有ライセンスの設定（ASA 8.2+）を参照してください。
- **SSL VPN**（IOS デバイスのみ）：SSL VPN ポリシーテーブルには、SSL VPN の仮想設定を定義するすべてのコンテキストが一覧表示されます。各コンテキストには、ゲートウェイ、ドメインまたは仮想ホスト名、およびユーザ グループ ポリシーが含まれます。詳細については、SSL VPN ポリシーの設定（IOS）を参照してください。

リモート アクセス VPN ポリシーの検出

Security Manager を使用すると、ポリシー検出中にリモート アクセス IPSec VPN のポリシー設定をインポートできます。また、ASA デバイス上の SSL VPN ポリシーを検出できます。ただし、IOS デバイス上のポリシーは検出できません。リモートアクセス VPN ポリシーを検出するには、デバイスをインベントリに追加するときや、すでにインベントリにあるデバイス上のポリシーを検出するときに、[デバイスの検出（Discover Device）] 設定で [RA VPNポリシー（RA VPN Policies）] オプションを選択します。デバイスの追加やポリシーの検出の詳細については、次の項を参照してください。

- デバイス インベントリへのデバイスの追加
- Security Manager にすでに存在するデバイス上のポリシーの検出

リモート アクセス VPN ネットワークに配置済みのデバイスの設定を検出して、Security Manager でその設定を管理できます。これらの設定は、リモートアクセス VPN ポリシーとして Security Manager にインポートされます。リモート アクセス VPN ポリシーの検出は、ライブ デバイスの設定をインポートするか、または設定ファイルをインポートして実行されます。ただし、設定ファイルからは、フラッシュ ストレージ内のファイルを参照する SSL VPN ポリシーを検出できません。したがって、設定ファイルからは SSL VPN を検出しないことを推奨します。

リモート アクセス VPN 内のデバイスのポリシー検出を開始すると、デバイスの設定が分析され、この設定が Security Manager ポリシーに変換されてデバイスを管理できるようになります。インポートした設定によって一部のポリシーだけが定義される場合、警告が表示されます。追加の設定が必要な場合は、Security Manager インターフェイスの関連するページに移動して、ポリシー定義を完了する必要があります。すでに Security Manager で管理しているデバイスの設定を再検出することもできます。

SSL VPN ポリシーを検出すると、SSL VPN ポリシーで参照される、フラッシュ ストレージに保存されているファイルが Security Manager サーバにコピーされ、Security Manager からポリシーが展開されると、ターゲットデバイスの /csm ディレクトリに格納されます。使用するファイルがフラッシュ ストレージに格納されていても、そのファイルが SSL VPN ポリシーから参照されていない場合は、ファイルを参照するコマンドを設定するか、または Security Manager

サーバにファイルを手動でコピーします。デバイスの SSL VPN ポリシーが、フラッシュから削除されたファイルを参照している場合、ポリシーの検出は失敗します。失敗した場合、デバイス検出の前に設定を直接修正するか、またはデバイスを追加するときに [RA VPNポリシー（RA VPN Policies）] オプションの選択を解除して、Cisco Security Manager で適切な SSL VPN 設定を作成します。

ヒント

- デバイスでポリシーを検出したら、ポリシーを変更する前またはデバイスからポリシーの割り当てを解除する前に、ただちに展開を実行する必要があります。すぐに展開を実行しないと、Security Manager で設定した変更が、デバイスに展開されない場合があります。
- ASA および PIX 7.0 以降のデバイスでは、デフォルトの接続プロファイルとグループ ポリシーが検出され、[Connection Profiles] と [Group Policies] ポリシーに追加されます。これらのデフォルト プロファイルとグループは変更できますが、削除はできません。
  - DefaultRAGroup：リモート アクセス IPsec VPN のデフォルトの接続プロファイル。
  - DefaultWEBVPNGroup：SSL VPN のデフォルトの接続プロファイル。この接続プロファイルは、ASA 8.0+ デバイスだけで検出されます。
  - DfltGrpPolicy：デフォルトのグループ ポリシーです。デフォルトの接続プロファイルで使用されます。検出されると、Cisco Security Manager では <device_display_name> DfltGrpPolicy という名前が使用されます。ただし、設定を展開すると、デバイスの表示名は削除され、DfltGrpPolicy が使用されます。

グループ ポリシーは共有ポリシー オブジェクトとしてモデル化され、デフォルトグループ ポリシーをデバイス上で変更している可能性があるため、この命名ルールは必要です。ただし、この命名ルールにより、デフォルトのグループ ポリシーが組み込まれている共有ポリシーが使用できなくなることはありません。デバイス表示名は、割り当てられているデバイスにかかわらず、オブジェクト名から削除されます。たとえば、デバイス 10.200.11.1 でオブジェクト 10.100.10.1DfltGrpPolicy を使用する場合、Cisco Security Manager は設定内で引き続き「DfltGrpPolicy」を使用します。

重要 共有ポリシーを接続プロファイルやグループポリシーに割り当てる場合は、デフォルトのグループポリシーに複数エントリが存在しないように、最初に接続プロファイルに割り当て、次にグループポリシーに割り当てます。

（注） これらのデフォルト接続プロファイルでは、SSL VPN ポータル カスタマイゼーションに DfltCustomization オブジェクトを使用しますが、Security Manager では検出されません。DfltCustomization を変更するには、デバイス上で直接変更する必要があります。ただし、単にカスタマイゼーション オブジェクトを作成して、そのオブジェクトをデフォルト接続プロファイルに指定し、デフォルト以外の設定を使用できます。

関連項目

- ポリシーの検出
- サイト間 VPN ディスカバリ
- VPN ディスカバリ ルール

Remote Access VPN Configuration ウィザードの使用

Remote Access VPN Configuration ウィザードを使用して、基本的な IPsec または SSL VPN の設定に必要なポリシーを作成できます。このウィザードで示される簡単なオプションを使用して、基本の項目を設定できます。したがって、ウィザードを使用したあとに、個別のリモートアクセス VPN ポリシーで、追加の設定を行う必要が生じることがあります。

ヒント このウィザードでは有効な IKEv2 IPSec VPN は作成されません。IKEv2 設定を完了するには、常に追加のポリシーを設定する必要があります。

（注） リモートアクセス VPN マルチコンテキストモードの場合、ソフトウェアバージョン 9.5(2) 以降を実行している ASA デバイスでは、リモートアクセス SSL VPN のみがサポートされます。

このウィザードには、デバイス タイプおよび VPN タイプ（IPSec または SSL）に応じて、基本的なリモート アクセス VPN を設定する手順が示されます。

Remote Access Configuration ウィザードにアクセスするには、次の手順を実行します。

1. デバイス ビューで、リモート アクセス サーバとして設定するデバイスをデバイス セレクタから選択します。
2. ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [構成ウィザード（Configuration Wizard）] を選択します。
3. 作成するリモートアクセス VPN のタイプに対応するオプションボタン（[リモートアクセスSSL VPN（Remote Access SSL VPN）] または [リモートアクセスIPSec VPN（Remote Access IPSec VPN）]）を選択します。
4. [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックして、適切なウィザードを開きます。

ウィザードの各バージョンの使用方法については、次の項を参照してください。

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（18 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）（33 ページ）

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（42 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス）　（48 ページ）

Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）

ここでは、Remote Access SSL VPN Configuration ウィザードを使用して、ASA デバイスで SSL VPN を作成または編集する方法について説明します。

関連項目

- リモート アクセス SSL VPN について　（3 ページ）
- 各リモートアクセスVPNテクノロジーでサポートされるデバイスについて　（10ページ）

ステップ 1　デバイス ビューで、目的の ASA デバイスを選択します。

ステップ 2　ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）]>[構成ウィザード（Configuration Wizard）] を選択します。

ステップ 3　[リモートアクセスSSL VPN（Remote Access SSL VPN）] オプションボタンを選択します。

ステップ 4　[リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックします。[Access] ページが開きます。このページの要素の詳細については、 SSL VPN Configuration ウィザード：[Access] ページ（ASA）　（20 ページ）を参照してください。

ステップ 5　SSL VPN 接続をイネーブルにするインターフェイスを指定します。[選択（Select）] をクリックして、インターフェイス、またはインターフェイスを識別するインターフェイス ロール オブジェクトを選択します。

ステップ 6　SSL VPN セッションに使用するポート番号を指定します。ポート番号を入力するか、番号を定義するポートリストオブジェクトの名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。

HTTPS トラフィックの場合、デフォルト ポートは 443 です。ポート番号は 443 にすることも、1024 ～ 65535 の範囲で指定することもできます。ポート番号を変更すると、現在の SSL VPN 接続がすべて終了するため、現在のユーザは再接続が必要になります。

（注）　HTTP ポート リダイレクションがイネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。

ステップ 7　ログイン時に、ユーザーがデバイスに設定されたトンネルグループ接続プロファイルのリストからトンネルグループを選択できるようにするには、[ユーザーにポータルページでの接続プロファイルの選択を許可する（Allow Users to Select Connection Profile in Portal Page)] オプションを選択します。

ステップ 8　ユーザーが AnyConnect VPN クライアントを使用して SSL VPN に接続できるようにするには、[Secure Clientアクセスの有効化（Enable Secure Client Access）] チェックボックスをオンにします。

ステップ 9 [次へ（Next）] をクリックします。[Connection Profile] ページが開きます。このページの要素の詳細については、SSL VPN Configuration ウィザード：[Connection Profile] ページ（ASA） （21 ページ）を参照してください。

ステップ 10 [接続プロファイル名（Connection Profile Name）] で、接続プロファイルの名前を入力します。これはトンネル グループの名前であり、[Remote Access VPN] > [Connection Profiles] ポリシーに表示されます。Connection Profile ポリシーの詳細については、接続プロファイルの設定（ASA、PIX 7.0+）を参照してください。

ステップ 11 [Connection Profile] ページで、あとで接続プロファイルの [General] タブに表示されるこれらのオプションを設定します（[General] タブ（[Connection Profiles]）を参照）。

- [グループポリシー（Group Policy）]：接続プロファイルのデフォルトグループになる [ASAグループポリシー（ASA Group Policy）] ポリシーオブジェクトの名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択します。必要なオブジェクトがまだ存在しない場合、[選択（Select）] をクリックしてから、[ASAユーザーグループセレクタ（ASA User Groups Selector）] ダイアログボックスで [作成（Create）]（+）ボタンをクリックすると、作成プロセスを実行できるウィザードが開きます（ Create Group Policy ウィザードによるユーザ グループの作成 （25 ページ）の説明を参照）。

ASA グループ ポリシー オブジェクトの詳細については、[ASA Group Policies] ダイアログボックスを参照してください。

- [グループポリシー（Group Policies）]：このテーブルには、SSL または IPsec VPN に関係なく、現在デバイスで使用されているすべてのグループポリシーが一覧表示されます。[編集（Edit）] をクリックすると、他のグループポリシーを追加できます。

- [グローバルIPアドレスプール（Global IP Address Pool）]：IP アドレスが割り当てられるアドレスプールを入力します。サーバはこれらのアドレス プールをリスト内の順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。

アドレスの範囲またはアドレスの範囲が含まれるネットワークまたはホストオブジェクトとして、Start_Address-End_Address の形式でプールを指定します（例：10.100.10.2-10.100.10.254）。[選択（Select）] をクリックして、ネットワークまたはホストオブジェクトを選択するか、または新しいオブジェクトを作成します。

ステップ 12 [Connection Profile] ページで、あとで接続プロファイルの [SSL VPN] タブに表示されるこれらのオプションを設定します（[SSL] タブ（[Connection Profiles]）を参照）。

- [ポータルページカスタマイゼーション（Portal Page Customization）]：VPN のデフォルトのポータルページを定義する SSL VPN カスタマイゼーション ポリシー オブジェクトの名前。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。

（注） カスタマイゼーション プロファイルとトンネル グループの組み合わせを使用することで、個々のグループにそれぞれ異なるログイン ウィンドウを設定できます。たとえば、salesgui という名前のカスタマイゼーション プロファイルを作成済みである場合、そのカスタマイゼーション プロファイルを使用する sales という名前の SSL VPN トンネル グループを作成できます。

- [接続URL（Connection URL）]：接続プロファイルの URL。ユーザは、この URL を使用して、カスタマイズ済みのポータル ページにダイレクト アクセスできます。リストからプロトコル（[http] または [https]）を選択し、表示されたフィールドで、接続プロファイルの名前が含まれている URL を指定します。

URL は、ASA デバイスのホスト名または IP アドレス、ポート番号、および SSL VPN 接続プロファイルを識別するためのエイリアスで構成されています。

（注） URL を指定しない場合は、ポータル ページの URL を入力し、デバイスに設定されている設定済みの接続プロファイルエイリアス リストから接続プロファイルエイリアスを選択することによって、ポータル ページにアクセスできます。 SSL VPN Configuration ウィザード：[Access] ページ（ASA） （20 ページ）を参照してください。

ステップ 13 [Connection Profile] ページで、認証、許可、アカウンティングおよびセカンダリ認証の AAA オプションを設定します。このオプションはあとで接続プロファイルの [AAA] タブおよび [Secondary AAA] タブに表示されます（[AAA] タブ（[Connection Profiles]）および[Secondary AAA] タブ（[Connection Profiles]）を参照）。

ステップ 14 [終了（Finish）] をクリックして変更を保存します。

SSL VPN Configuration ウィザード：[Access] ページ（ASA）

SSL VPN Configuration ウィザードの [Access] ページを使用して、SSL VPN セッションのセキュリティ アプライアンス インターフェイスを設定します。ウィザードを完了したら、後で SSL VPN アクセスポリシーで設定を編集できます。[SSL VPN Access Policy] ページを参照してください。

ナビゲーション パス

（デバイス ビュー）ASA デバイスでリモート アクセス SSL VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（ Remote Access VPN Configuration ウィザードの使用 （17 ページ）を参照）。最初に表示されるページは [Access] ページです。

関連項目

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（18 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 *2 : SSL VPN* ウィザード：*[Access]* ページ（*ASA*）

要素	説明
Interfaces to Enable SSL VPN Service	SSL VPN 接続をイネーブルにするインターフェイス、またはインターフェイスを識別するインターフェイス ロール。[選択（Select）] をクリックして、インターフェイスまたはインターフェイスロールを選択するか、または新しいインターフェイスロールを作成します。
ポート番号（Port Number）	SSL VPN セッションに使用するポート番号。ポート番号またはポートリストオブジェクト名を入力します。または、[選択（Select）] をクリックしてポート定義するオブジェクトを選択するか、または新しいオブジェクトを作成します。 HTTPS トラフィックの場合、デフォルト ポートは 443 です。ポート番号は 443 にすることも、1024 ～ 65535 の範囲で指定することもできます。ポート番号を変更すると、現在の SSL VPN 接続がすべて終了するため、現在のユーザは再接続が必要になります。 （注） HTTP ポート リダイレクションがイネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。
Portal Page URLs	VPN に接続するためにユーザが使用する URL。インターフェイスとポート番号を指定すると、URL が表示されます。
Allow Users to Select Connection Profile in Portal Page	ログイン時（たとえば、SSL VPN ポータル ページ）にユーザが適切なプロファイルを選択するときに使用できる設定済み接続プロファイル（トンネル グループ）のリストを提供するかどうかを指定します。このオプションを選択しない場合、ユーザはプロファイルを選択できず、接続にはデフォルト プロファイルを使用する必要があります。
[Secure Clientアクセスの有効化（Enable Secure Client Access）]	ユーザが AnyConnect VPN クライアントを使用して SSL または IKEv2 IPSec VPN 接続を確立できるようにするかどうかを指定します。このオプションは、デフォルトでオンになっています。AnyConnect VPN クライアントの詳細については、SSL VPN セキュア クライアントの設定についてを参照してください。 （注） Secure Client Essentials をイネーブルにするには、[リモート アクセス VPN（Remote Access VPN）] > [SSL VPN（SSL VPN）] >[アクセス（Access）] に移動します。詳細については、Access ポリシーの設定 を参照してください。

SSL VPN Configuration ウィザード：[Connection Profile] ページ（ASA）

SSL VPN Configuration ウィザードの [Connection Profile] ページを使用して、セキュリティ アプライアンスでトンネル グループ ポリシーを設定します。追加するトンネル接続プロファイル

ポリシーの名前を指定し、ユーザ グループ ポリシーを選択できます。また、このポリシーのアドレス プールを指定し、認証サーバ グループ設定を指定できます。

ナビゲーション パス

（デバイスビュー）ASA デバイスでリモートアクセス SSL VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用（17 ページ）を参照）。次に、このページが表示されるまで [次へ（Next）] をクリックします。

関連項目

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（18 ページ）
- [ASA Group Policies] ダイアログボックス
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定
- ネットワーク/ホストオブジェクトについて
- AAA サーバおよびサーバ グループ オブジェクトについて

フィールド リファレンス

表 *3 : SSL VPN Configuration* ウィザード、*[Connection Profile]* ページ（*ASA*）

要素	説明
Connection Profile Name	接続プロファイルの名前（トンネル グループ）。
[グループ ポリシー（Group Policy）]	デバイスに関連付けられているデフォルトの ASA ユーザ グループ。ASA ユーザーグループポリシーを入力します。または、[選択（Select）] をクリックしてリストからポリシーを選択するか、新しいポリシーを作成します。 必要な場合、接続プロファイルに関連付けられているデフォルトユーザ グループを定義する ASA グループ ポリシー オブジェクトの名前。グループ ポリシーはユーザ指向の属性と値のペアの集合であり、デバイスで内部的に、または RADIUS/LDAP サーバで外部的に格納されます。 [選択（Select）]をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。グループポリシーの選択ダイアログボックスで [作成（Create）]（+）ボタンをクリックすると、Create Group Policy ウィザードによるユーザ グループの作成 （25 ページ）に説明されているように、ウィザードを使用してグループ作成手順を実行できます。

要素	説明
Full Tunnel	[Group Policy] フィールドで選択されているオブジェクトにフル トンネル アクセス モードが設定されているかどうかを示す読み取り専用フィールド。
グループ ポリシー	デバイスに設定されているすべての ASA ユーザ グループ ポリシーの名前（IPSec VPN 接続にのみ設定されているポリシーも含む）。このテーブルの内容は、[Remote Access VPN] > [Group Policies] ポリシーの内容と同じです。テーブルには、グループ ポリシーごとにフル トンネル アクセス モードがイネーブルかディセーブルかが示されます。 [編集（Edit）] をクリックして、リストを変更できます。[Edit] をクリックすると、ダイアログボックスが開きます。このダイアログボックスでは、追加のグループポリシーを選択したり、現在選択されているポリシーの選択を解除したりできます（他の接続プロファイルで使用されているポリシーの選択は解除しないでください）。また、新しいグループポリシーを作成したり（使用可能なグループポリシーリストの下にある [作成（Create）]（+）ボタンをクリック）、グループ ポリシー オブジェクトを選択してから、いずれかのリストの下にある [編集（Edit）]（鉛筆）ボタンをクリックして、グループポリシーを編集したりできます。 新しいグループ ポリシーを作成する場合、[Create Group Policy] ウィザードを使用して手順を実行できます。Create Group Policy ウィザードによるユーザ グループの作成 （25 ページ）を参照してください。
Portal Page Customization	VPN のデフォルト ポータル ページを定義する [SSL VPN Customization] ポリシー オブジェクトの名前。このプロファイルでは、リモート ユーザが SSL VPN 上で使用可能なすべてのリソースにアクセスできるようにするためのポータル ページの外観を定義します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。
Connection URL	接続プロファイルの URL。ユーザは、この URL を使用して、カスタマイズ済みのポータル ページにダイレクト アクセスできます。 リストからプロトコル（[http] または [https]）を選択し、URL を指定します。URL には、ASA デバイスのホスト名または IP アドレス、ポート番号、および SSL VPN 接続プロファイルの識別に使用するエイリアスを含めます。 （注） URL を指定しない場合は、ポータル ページの URL を入力し、デバイスに設定されている設定済みの接続プロファイル エイリアス リストから接続プロファイル エイリアスを選択することによって、ポータル ページにアクセスできます。SSL VPN Configuration ウィザード：[Access] ページ（ASA） （20 ページ）を参照してください。

要素	説明
[グローバル IPv4 アドレスプール（Global IPv4 Address Pool）]	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IPv4 アドレスをクライアントに割り当てるために使用されるアドレスプール。アドレス プールは、アドレスの範囲として入力します（10.100.12.2-10.100.12.254 など）。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。 アドレス プール範囲を入力するか、これらのプールを定義するネットワークまたはホスト オブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
[グローバル IPv6 アドレスプール（Global IPv6 Address Pool）]	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IPv6 アドレスをクライアントに割り当てるために使用されるアドレスプール。アドレスプールは、アドレスの範囲として入力します（2001:db8::1-2001:db8::2:1 など）。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。。 アドレス プール範囲を入力するか、これらのプールを定義するネットワークまたはホスト オブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
Authentication Server Group	認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合はLOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Authorization Server Group	認可サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合はLOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Accounting Server Group	アカウンティング サーバ グループの名前。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。

要素	説明
Secondary Authentication	リモートアクセスVPN接続を完了する前に、ユーザに2つのクレデンシャルセット（ユーザ名とパスワード）を要求する二重認証をイネーブルにするかどうか。 • [セカンダリ認証を有効化（Enable Secondary Authentication）]：二重認証を要求するには、このオプションを選択します。 • [認証サーバーグループ（Authentication Server Group）]：2 番めのクレデンシャルセットで使用する認証サーバーグループの名前（トンネルグループがローカルデバイスに設定されている場合はLOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 • [サーバーグループに障害が発生した場合はローカルを使用（UseLOCAL if Server Group Fails）]：選択した認証サーバーグループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。

Create Group Policy ウィザードによるユーザ グループの作成

Remote Access SSL VPN Configuration ウィザードを使用して、ASA または IOS デバイス上で SSL VPN を作成する場合、ウィザードを使用して、新しい ASA グループ ポリシーまたは IOS ユーザ グループ オブジェクトを作成できます。このウィザードを使用すると、グループの選択要素を設定できるため、オブジェクトを作成したあとに、そのオブジェクトを編集して追加の設定を行う必要が生じる場合があります。

Create Group Policy ウィザードは、Remote Access SSL VPN Configuration ウィザードからのみ使用できます。このウィザードの起動および使用方法については、次の項を参照してください。

次の手順では、次の項の説明に従って、すでに Remote Access SSL VPN Configuration ウィザードを実行していることを前提とします。

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（18 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（42 ページ）

関連項目

- SSL VPN アクセスのモード （4 ページ）

ステップ 1 SSL VPN に Remote Access VPN Configuration ウィザードを使用する場合、グループ ポリシーを選択するページに進みます。このページでは、次のようにしてユーザ グループの選択ページを開くことができます。

- ASA デバイス：ウィザードの [接続プロファイル（Connection Profile）] ページで、[グループポリシー（Group Policy）] フィールドの隣にある [選択（Select）] をクリックします。または、[グループポリシー（Group Policies）] テーブルの隣にある [編集（Edit）] をクリックします。
- IOS デバイス：ウィザードの [ゲートウェイとコンテキスト（Gateway and Context）] ページで、[グループポリシー（Group Policies）] テーブルの隣にある [編集（Edit）] をクリックします。

ステップ 2 [グループポリシーセレクタ（Group Policy Selector）] ダイアログボックスで、使用可能なグループポリシーのリストの下にある [作成（Create）]（+）ボタンをクリックして、Create Group Policy ウィザードを起動します。このウィザードは、[Group Policy] ページから始まります。

グループ ポリシー セレクタでは、次の項目も実行できます。

- 既存のグループを選択して [>>] をクリックし、グループを SSL VPN で使用する。ASA のデフォルト グループ用にグループを選択する場合は（[Group Policy] フィールド）、単にそのオブジェクトをリストからクリックします。
- 既存のグループを選択して [編集（Edit）]（鉛筆）をクリックし、既存のグループのプロパティを変更する。

ステップ 3 [Group Policy] ページで、次のオプションを設定します。

- [名前（Name）]：ユーザーグループの名前。最大 128 文字を入力します。大文字、小文字、およびほとんどの英数字または記号を使用できます。
- [アクセス方式（Access Method）]：目的のリモートアクセス方式オプションを、次から選択します。
  - [フルトンネル（Full Tunnel）]：SSL VPN トンネルを介して企業ネットワークにフルアクセスします。これは推奨オプションです。
  - [クライアントレス（Clientless）]：クライアントマシンで Web ブラウザを使用して内部ネットワーク、または企業ネットワークにアクセスします。
  - [シンクライアント（Thin Client）]：クライアントマシンで TCP プロキシとして機能する Java アプレットをダウンロードします。

ステップ 4 [次へ（Next）] をクリックします。次に開くページは、選択したアクセス方式によって異なります。この手順では、すべての方式を選択したと想定します。この場合は、[Full Client] ページが開きます。

ステップ 5 [Full Client] ページで、フル トンネルのみにアクセスを制限するか、またはフル クライアントのダウンロードに失敗した場合、他のアクセス方式を許可するかどうかを選択します。また、DNS および WINS サーバ情報を指定し、スプリット トンネリングを許可する場合は設定します。オプションの説明については、Create Group Policy ウィザード：[Full Tunnel] ページ （27 ページ）を参照してください。

ステップ 6 [次へ（Next）] をクリックします。[Clientless and Thin Client] ページが開きます。

ステップ 7 [Clientless and Thin Client] ページで、これらのアクセス モードを設定します。オプションの説明については、Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ （31 ページ）を参照してください。

ステップ 8 [終了（Finish）] をクリックして、グループ ポリシー オブジェクトを作成します。

ステップ 9 ウィザードを完了すると、使用可能なグループ リストにグループ ポリシーが追加されますが、（設定してるグループが ASA のデフォルト グループではない限り）そのグループは選択されていません。グループを選択するには、使用可能なグループリストで強調表示して、[>>] をクリックし、そのグループを選択したグループリストに移動します。

（注） ユーザーグループをデフォルトユーザーグループとして指定するには、ユーザーグループを選択し、[デフォルトとして設定（Set As Default）] をクリックします。このオプションは、IOS ルータの場合にのみ使用可能です。

ステップ 10 [グループポリシーセレクタ（Group Policy Selector）]ページで [OK] をクリックして変更を保存し、Remote Access SSL VPN Configuration ウィザードに戻ります。

Create Group Policy ウィザード：[Full Tunnel] ページ

（注） このページは、Create Group Policy ウィザードの [グループポリシー（Group Policy）] で [フルクライアント（Full Client）] オプションを選択した場合にのみ使用可能です。

このページでは、企業ネットワークへのアクセスに使用するモードを設定できます。

ナビゲーション パス

Create Group Policy ウィザードの開始については、Create Group Policy ウィザードによるユーザグループの作成 （25 ページ）を参照してください。

フィールド リファレンス

表 *4 : Create User Group* ウィザード：*[Full Tunnel]* ページ

要素	説明
[モード（Mode）]	SSL VPN で許可するアクセス モード。次のいずれかを選択します。 • [SSL VPN クライアントのダウンロードに失敗した場合に他のアクセスモードを使用する（Use Other Access Modes if SSL VPN Client Download Fails）]：VPN クライアントのダウンロードに失敗した場合に、リモートクライアントでクライアントレス アクセス モードまたはシン クライアント アクセス モードの使用を許可します。 • [フルトンネルのみ（Full Tunnel Only）]：クライアントレスまたはシンクライアントアクセスを禁止します。ユーザは、フル クライアントをインストールし、VPN への接続に使用できるようにしておく必要があります。 デバイス上でフル クライアント イメージを必ず設定してください。ASA デバイスでは、SSL VPN の [Client Settings] タブ > [Other Settings] ポリシーを使用します。SSL VPN セキュアクライアント 設定の構成（ASA）を参照してください。IOS デバイスでは、クライアントは [FlexConfig] ポリシーを使用して管理されます。定義済みの FlexConfig ポリシー オブジェクトを参照してください。
Client IP Address Pools （IOS デバイスのみ）	フル トンネル クライアントがログインしたときに取得するアドレス プールの IP アドレス範囲。このアドレスプールは、デバイスのインターフェイス IP アドレスのいずれかと同じサブネットに存在する必要があります。 アドレス範囲を指定する場合は、最初と最後の IP アドレスをハイフンで区切って入力します。たとえば、10.100.10.2-10.100.10.255 です。1 つのアドレスを入力した場合、プールには 1 つのアドレスだけが含まれます。サブネット指定は入力しないでください。 範囲を定義するネットワーク/ホストポリシーオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成することもできます。複数の範囲を指定する場合は、カンマで区切ります。
プライマリ IPv4 DNS サーバー	グループのプライマリ DNS サーバーの IPv4 アドレス。ネットワーク/ホストオブジェクトの IPv4 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
セカンダリ IPv4 DNS サーバー	グループのセカンダリ DNS サーバーの IPv4 アドレス。ネットワーク/ホストオブジェクトの IPv4 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
プライマリ IPv6 DNS サーバー	グループのプライマリ DNS サーバーの IPv6 アドレス。ネットワーク/ホストオブジェクトの IPv6 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
セカンダリ IPv6 DNS サーバー	グループのセカンダリ DNS サーバーの IPv6 アドレス。ネットワーク/ホストオブジェクトの IPv6 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
デフォルト DNS ドメイン	フルクライアント SSL VPN 接続に使用される DNS サーバのドメイン名。
プライマリ WINS サーバ（Primary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。
セカンダリ WINS サーバ（Secondary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。
Split Tunnel Option	IPv4 トラフィックのスプリットトンネリングを許可するかどうかを指定し、許可する場合は、保護するトラフィック、または暗号化されずにパブリックネットワークを介して送信するトラフィックを指定します。 • [無効（Disabled）]（デフォルト）：IPv4 トラフィックは、暗号化されずに送信されることがないか、またはゲートウェイ以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカル ネットワークにはアクセスできません。 • [指定されたトラフィックをトンネル化（Tunnel Specified Traffic）]：[ネットワーク（Networks）] または [宛先（Destinations）] フィールドに一覧表示されているアドレスを通過するすべての IPv4 トラフィックをトンネル化します。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザーのインターネット サービス プロバイダーによってルーティングされます。 • [指定されたトラフィックを除外（Exclude Specified Traffic）]：[ネットワーク（Networks）] または [宛先（Destinations）] フィールドに一覧表示されているアドレスを通過する IPv4 トラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。

要素	説明
[IPv6 スプリットトンネル オプション（IPv6 Split Tunnel Option）]	IPv6 トラフィックのスプリットトンネリングを許可するかどうかを指定し、許可する場合は、保護するトラフィック、または暗号化されずにパブリックネットワークを介して送信するトラフィックを指定します。 • [無効（Disabled）]（デフォルト）：IPv6 トラフィックは、暗号化されずに送信されることがないか、またはゲートウェイ以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカル ネットワークにはアクセスできません。 • [指定されたトラフィックをトンネル化（Tunnel Specified Traffic）]：[ネットワーク（Networks）] または [宛先（Destinations）] フィールドに一覧表示されているアドレスを通過するすべてのトラフィックをトンネル化します。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザーのインターネット サービス プロバイダーによってルーティングされます。 • [指定されたトラフィックを除外（Exclude Specified Traffic）]：[ネットワーク（Networks）] または [宛先（Destinations）] フィールドに一覧表示されているアドレスを通過するトラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。
ネットワーク （ASA デバイスのみ）	[Split Tunnel Option] で [Tunnel Specified Traffic] または [Exclude Specified] トラフィックを選択する場合、トンネルを通過するトラフィックまたは除外されるトラフィックを定義する ACL オブジェクトの名前を入力します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。
宛先 （IOS デバイスのみ）	[Split Tunnel Option] で [Tunnel Specified Traffic] または [Exclude Specified] トラフィックを選択する場合、トンネルを通過するトラフィックまたは除外されるトラフィックを定義する IP アドレスを指定します。 10.100.10.0/24 などのネットワーク アドレスまたは 10.100.10.12 などのホスト アドレスを入力します。ネットワーク/ホストポリシーオブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成することもできます。カンマで複数のアドレスを区切ります。

要素	説明
Exclude Local LANs （IOS デバイスのみ）	ローカル LAN を暗号化されたトンネルから除外するかどうかを指定します。このオプションは、[指定されたトラフィックを除外（Exclude Specified Traffic）] スプリット トンネル オプションを選択している場合にのみ選択できます。このオプションを選択すると、LAN に接続しているシステム（プリンタなど）との通信をユーザに許可するために、ローカル LAN アドレスを宛先フィールドに入力する必要がなくなります。 選択した場合、この属性によって、クライアントと同時にローカル サブネットワークにアクセスする非スプリット トンネリング接続が許可されなくなります。
Split DNS Names	スプリット トンネルを介してプライベート ネットワークに解決されるドメイン名のリスト。他のすべての名前は、パブリック DNS サーバを使用して解決されます。 ドメインのリストに最大 10 のエントリをカンマで区切って入力します。文字列全体は、255 文字以下である必要があります。

Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ

Create Group Policy ウィザードの [Clientless and Thin Client] ページで、SSL VPN で企業ネットワークにアクセスするために使用する [Clientless] モードおよび [Thin Client] クライアント モードを設定できます。

（注） このページは、Create Group Policy ウィザードの手順 1 で [クライアントレス（Clientless）] オプションまたは [シンクライアント（Thin Client）] オプションを選択した場合にのみ表示されます。

ナビゲーション パス

Create Group Policy ウィザードの開始については、Create Group Policy ウィザードによるユーザ グループの作成 （25 ページ）を参照してください。

関連項目

- SSL VPN アクセスのモード （4 ページ）
- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定
- [Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス

フィールド リファレンス

表 *5 : Create User Group* ウィザード：*[Clientless and Thin Client]* ページ

要素	説明
[クライアントレス（Clientless）]：ウィザードの手順 1 で [クライアントレス（Clientless）] を選択した場合にのみ表示されます。	
Portal Page Websites	ポータル ページ上に表示する Web サイト URL が含まれる SSL VPN ブックマーク ポリシー オブジェクトの名前。これらの Web サイトを使用すると、ユーザは目的のリソースにアクセスできます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Allow Users to Enter Websites	ブラウザへの Web サイト URL の直接入力をリモート ユーザに許可するかどうかを指定します。このオプションを選択しない場合、ユーザはポータルに表示されている URL だけにアクセスできます。
[シンクライアント（Thin Client）]：ウィザードの手順 1 で [シンクライアント（Thin Client）] を選択した場合にのみ表示されます。	
Port Forwarding List	このグループに割り当てるポート転送リスト ポリシー オブジェクトの名前。ポート転送リストには、クライアントレス SSL VPN セッションのユーザが転送先 TCP ポートを介してアクセスできるアプリケーションのセットが含まれます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Port Forwarding Applet Name（ASA デバイスのみ）	ポータル上の [Port Forwarding Java] アプレット画面に表示されるアプリケーション名または短い説明。最大 64 文字です。これは、ユーザがダウンロードするアプレットの名前です。このアプレットは、SSL VPN ゲートウェイで設定したサービス用の TCP プロキシとしてクライアント マシン上で動作します。
Download Port Forwarding Applet on Client Login	ユーザが SSL VPN にログインしたときに、ポート転送 Java アプレットがクライアントに自動的にダウンロードされるかどうかを指定します。アプレットを自動的にダウンロードしない場合、ユーザがログイン後に手動でダウンロードする必要があります。

Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

ここでは、Remote Access VPN Configuration ウィザードを使用して、ASA または PIX 7.0 以降のデバイスで IPSec VPN を作成する方法について説明します。

ヒント このウィザードの [Defaults] ページ（ウィザードの最後のステップ）では、VPN で使用する共有ポリシーを選択できます。この機能を使用する場合、必要なすべての共有ポリシーがデータベースに設定および送信されていることを最初に確認する必要があります。共有ポリシーと VPN ポリシーのデフォルトの設定については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定を参照してください。

関連項目

- リモート アクセス IPSec VPN について （2 ページ）
- 各リモートアクセス VPN テクノロジーでサポートされるデバイスについて （10 ページ）

ステップ 1 [Device] ビューで、目的の ASA または PIX 7.0 以降のデバイスを選択します。

ステップ 2 ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）]>[構成ウィザード（Configuration Wizard）] を選択します。

ステップ 3 [リモートアクセスIPSec VPN（Remote Access IPSec VPN）] オプションボタンを選択します。

ステップ 4 [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックします。[Connection Profile] ページが開きます。このページに表示されるオプションの説明については、 Remote Access VPN Configuration ウィザード：[IPSec VPN Connection Profile] ページ（ASA） （37 ページ）を参照してください。

ステップ 5 [Connection Profile] ページで、これらの基本オプションを設定します。

- [接続プロファイル名（Connection Profile Name）]：接続プロファイルの名前を入力します。これはトンネル グループの名前であり、[Remote Access VPN] > [Connection Profiles] ポリシーに表示されます。Connection Profile ポリシーの詳細については、接続プロファイルの設定（ASA、PIX 7.0+）を参照してください。
- [IKEバージョン（IKE Versions）]：IKE ネゴシエーション中に VPN サーバーとリモートユーザー間で使用する IKE バージョン（バージョン 1、2 または両方）を選択します。IKEv2 は、ASA ソフトウェア リリース 8.4(1)+ だけでサポートされます。

ステップ 6 [Connection Profile] ページで、あとで接続プロファイルの [General] タブに表示されるこれらのオプションを設定します（[General] タブ（[Connection Profiles]）を参照）。

- [グループポリシー（Group Policy）]：接続プロファイルのデフォルトグループになる [ASAグループポリシー（ASA Group Policy）] ポリシーオブジェクトの名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択します。必要なオブジェクトがまだ存在しない場合、[選択（Select）] をクリックしてから、[ASAユーザーグループセレクタ（ASA User Groups Selector）] ダイアログボックスで [作成（Create）]（+）ボタンをクリックすると、これらのオブジェクトを作成するために使用するダイアログボックスが開きます。

新しいグループ ポリシー オブジェクトを作成する場合、ウィザードの [Connection Profile] ページで選択する IKE バージョンと同じバージョンを選択する必要があります。これらのオプションは [Add ASA Group Policies] ダイアログボックスの [Technology] ページにあります。オプションは、[Easy VPN]、[IPSec IKEv1] および [Easy VPN/IPSec IKEv2] です。

ASA グループ ポリシー オブジェクトの詳細については、[ASA Group Policies] ダイアログボックスを参照してください。

- [グローバルIPアドレスプール（Global IP Address Pool）]：IP アドレスが割り当てられるアドレスプールを入力します。サーバはこれらのアドレス プールをリスト内の順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。

アドレスの範囲またはアドレスの範囲が含まれるネットワークまたはホストオブジェクトとして、Start_Address -End_Address の形式でプールを指定します（例：10.100.10.2-10.100.10.254）。[選択（Select）] をクリックして、ネットワークまたはホストオブジェクトを選択するか、または新しいオブジェクトを作成します。

ステップ 7 [Connection Profile] ページで、認証、許可、アカウンティングの AAA オプションを設定します。このオプションはあとで接続プロファイルの [AAA] タブに表示されます（[AAA] タブ（[Connection Profiles]）を参照）。

ステップ 8 [次へ（Next）] をクリックして、[IPsec設定（IPsec Settings）] ページに移動します。

ステップ 9 [IPSec Settings] ページで、IPSec のオプションを設定します。このオプションはあとで接続プロファイルの [IPSec] タブに表示されます（[IPSec] タブ（[Connection Profiles]）を参照）。これらの設定の一部は IKEv1 にのみ適用されます。

- [事前共有キー（Preshared Key）]、[確認（Confirm）]：各フィールドに、トンネルグループの IKEv1 事前共有キーを入力します。事前共有キーの最大長は 127 文字です。

リモート アクセス IKEv2 IPsec VPN に事前共有キーは設定できません。

- [トラストポイント名（Trustpoint Name）]：トラストポイントが設定されている場合、IKEv1 接続用のトラストポイント名を定義する PKI 登録ポリシーオブジェクトの名前を入力します。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

IKEv2 の場合、トラストポイント名はここではなく、[Global Settings] ポリシーの [IKEv2 Settings] タブで設定します。設定は、この手順の後半で説明されています。

- 他のオプション（クライアント テーブル以外）は IKEv1 と IKEv2 の両方に適用されます。デフォルト以外の動作が必要な場合は、設定を変更します。クライアント ソフトウェアの更新テーブルなどのオプションの説明については、Remote Access VPN Configuration ウィザード：[IPSec Settings] ページ（ASA） （39 ページ）を参照してください。

ステップ 10 [次へ（Next）] をクリックして、[VPNデフォルト（VPN Defaults）] ページに移動します。

ステップ 11 [Defaults] ページで、VPN に割り当てる追加の共有ポリシーを選択します。最初から一覧表示されているポリシーは、[Security Manager Administration] の [VPN Defaults] ページで選択されているポリシーです。

これらのポリシーの選択については、Remote Access VPN Configuration ウィザード：[Defaults] ページ（40 ページ）を参照してください。

ステップ 12 [終了（Finish）] をクリックして変更を保存します。

ウィザードでは、設定可能なすべてのオプションを設定するわけではないため、作成したポリシーを調べて、実装するオプションを追加で設定します。

サポート対象 IKE バージョンとして IKE バージョン 2 を選択した場合や IPsec トラストポイントを指定した場合、これ以降の手順は必須です。

ステップ 13 （IKEv2 で任意）必要に応じて、グループエイリアスと二重認証を設定します。

a) [Connection Profiles] ポリシーを選択します。

b) ウィザードで設定した接続プロファイルを選択して、[行の編集（Edit Row）]（鉛筆）ボタンをクリックし、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。

- 二重認証を設定する場合は、[Secondary AAA] タブを選択して、必要な値を設定します。詳細については、[Secondary AAA] タブ（[Connection Profiles]）を参照してください。
- ログイン中にユーザが正しいプロファイルを選択できるようにするため、プロファイルにエイリアスを設定する場合、[SSL] タブを選択して、エイリアステーブルを設定します。詳細については、[SSL] タブ（[Connection Profiles]）を参照してください。
- ウィザードでは設定されない追加の接続プロファイル設定がいくつかあります。[Connection Profile] ダイアログボックスのタブを調べて、追加の変更が必要かどうかを決定します。

c) [接続プロファイル（Connection Profiles）] ダイアログボックスで [OK] をクリックして、変更を保存します。

ステップ 14 （IKEv2 で必須）[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [アクセス（Access）] ポリシーを選択して、少なくとも次の項目を設定します。[Access] ポリシーの設定については、SSL VPN セキュアクライアント 設定の構成（ASA）を参照してください。

- リモート アクセス VPN インターフェイスをアクセス インターフェイス テーブルに追加します。
- [ユーザーにポータルページでの接続プロファイルの選択を許可する（Allow Users to Select Connection Profile in Portal Page）] を選択します。
- [Secure Clientアクセスの有効化（Enable Secure Client Access）] を選択します。

ステップ 15 （IKEv2 で必須）[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] ポリシーを選択して、[クライアント設定（Client Settings）] タブをクリックします。

Secure Client イメージテーブルで、IKEv2 ネゴシエーションをサポートしている AnyConnect 3.0 以降のクライアントイメージを追加します。

クライアントイメージの設定については、VPN グローバル IKEv2 設定を参照してください。

ステップ 16 （IKEv2 で必須）[リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）] ポリシーを選択して、[IKEv2設定（IKEv2 Settings）] タブをクリックします。

少なくとも、リモートアクセス IKEv2 認証用に [RAトラストポイント（RA Trustpoint）] を設定します。認証局（CA）サーバーを識別する PKI 登録オブジェクトの名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。

IKEv2 グローバル設定については、[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス）を参照してください。

ステップ 17 （IKEv1、IKEv2 で必須）[リモートアクセスVPN（Remote Access VPN）] > [公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーを選択して、次の PKI 登録オブジェクトが選択されていることを確認します。

- （IKEv1）トラストポイントが設定されている場合、接続プロファイルの [IPSec] タブで指定したオブジェクト。
- （IKEv2）[Global Settings] ポリシーの [IKEv2 Settings] タブで指定したオブジェクト。

（注） これらのオブジェクトをすでに指定している共有の [Public Key Infrastructure] ポリシーは、ウィザードによって適用されている場合もあります。

ステップ 18 （IKEv2 で任意）IKEv2 接続には、AnyConnect 3.0 以降のクライアントを使用する必要があります。セキュアクライアントでは、場合によっては、ソフトウェアアップグレード、プロファイル、ローカリゼーションファイルおよびカスタマイゼーション ファイル、CSD、SCEP などのファイルをダウンロードする必要があります。ウィザードでは、これらのタイプのダウンロードがイネーブルにされません。

Secure Client ファイルのダウンロードをイネーブルにする手順は次のとおりです。

a) [リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPSecプロポーザル（IPSec Proposal）] を選択します。
b) ウィザードで作成された IPSec プロポーザルを選択して、[行の編集（Edit Row）]（鉛筆）をクリックして IPSec Proposal Editor を開きます。さまざまなオプションの詳細については、[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス）を参照してください。
c) デフォルトのポート 443 を使用しない場合は、[クライアントサービスの有効化（Enable Client Services）] オプションを選択して、ポート番号を入力します。（SSL VPN や他の SSL が使用するポート番号と同じ番号を使用できます）。
d) [OK] をクリックして変更を保存します。

Remote Access VPN Configuration ウィザード：[IPSec VPN Connection Profile] ページ（ASA）

Remote Access VPN Configuration ウィザードの [Connection Profile] ページを使用して、リモート アクセス IPSec VPN 用の Connection Profile ポリシーをセキュリティ アプライアンスで設定します。追加する Connection Profile ポリシーの名前を指定し、IKE ネゴシエーション中に許可する IKE バージョンを選択し、ユーザ グループ ポリシーを選択できます。また、このポリシーのアドレス プールを指定し、認証、許可、アカウンティングのサーバ グループ設定を指定できます。

このウィザードを使用した ASA でのリモート アクセス IPsec VPN の設定については、Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）　（33 ページ）を参照してください。

ナビゲーション パス

（デバイス ビュー）ASA または PIX 7.0 以降のデバイスでリモート アクセス IPsec VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用　（17 ページ）を参照）。最初に表示されるページは [IPSec Connection Profile] ページです。

フィールド リファレンス

表 *6 : Remote Access VPN Configuration* ウィザード、*[IPSec VPN Connection Profile]* ページ（*ASA*）

要素	説明
Connection Profile Name	接続プロファイルの名前（トンネル グループ）。
IKE Versions	IKE ネゴシエーション中に VPN サーバとリモート ユーザ間で使用する IKE バージョン。IKEv2 は、ASA ソフトウェア リリース 8.4(1)+ だけでサポートされます。他のタイプのデバイスでは、オプションの選択を変更できません。 [IKEバージョン1（IKE Version 1）]、[IKEバージョン2（IKE Version 2）]、または [両方（Both）]（どちらのバージョンも許可する場合）を選択します。IKEv2 接続は セキュアクライアント を使用した場合にのみ許可されます。

要素	説明
[グループ ポリシー（Group Policy）]	必要な場合、接続プロファイルに関連付けられているデフォルト ユーザ グループを定義する ASA グループ ポリシー オブジェクトの名前。グループ ポリシーはユーザ指向の属性と値のペアの集合であり、デバイスで内部的に、または RADIUS/LDAP サーバで外部的に格納されます。 [選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** この VPN で IKEv2 をイネーブルにする場合、選択するグループ ポリシーには特別の考慮事項が必要です。詳細については、Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）（33 ページ）を参照してください。
Global IP Address Pool	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IP アドレスをクライアントに割り当てるために使用されるアドレス プール。アドレス プールは、アドレスの範囲として入力します（10.100.12.2-10.100.12.254 など）。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。 アドレス プール範囲を入力するか、これらのプールを定義するネットワークまたはホスト オブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホスト オブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
Authentication Server Group	認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Authorization Server Group	認可サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Accounting Server Group	アカウンティング サーバ グループの名前。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。

Remote Access VPN Configuration ウィザード：[IPSec Settings] ページ（ASA）

Remote Access VPN Configuration ウィザードの [IPSec Settings] ページを使用して、リモート アクセス IPSec VPN 用の IPSec をセキュリティ アプライアンスで設定します。これらの設定の一部は IKE Version 1（IKEv1; IKE バージョン 1）にのみ適用されます。IKEv2 のみの VPN を設定している場合、これらのフィールドはグレー表示され、設定できません。

このウィザードを使用した ASA でのリモート アクセス IPsec VPN の設定については、Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）　（33 ページ）を参照してください。

ナビゲーション パス

（デバイスビュー）ASA または PIX 7.0 以降のデバイスでリモートアクセス IPsec VPN を設定するための Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用　（17 ページ）を参照）。その後、このページが表示されるまで [次へ（Next）] をクリックします。

フィールド リファレンス

表 *7 : Remote Access VPN Configuration* ウィザード、*IPSec VPN* ウィザード：*IPSec Settings*（*ASA*）

要素	説明
事前共有キー（Preshared Key） （IKEv1 のみ）	接続プロファイルの事前共有キー。事前共有キーの最大長は 127 文字です。確認フィールドでもう一度キーを入力します。 **ヒント**　IKEv2 リモート アクセス VPN に事前共有キーを設定できません。
Trustpoint Name （IKEv1 のみ）	トラストポイント名を定義する PKI 登録ポリシー オブジェクトの名前（トラストポイントが IKEv1 接続で設定されている場合）。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。 [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント**　このトラストポイントは IKEv1 ネゴシエーションにのみ使用されます。IKEv2 ネゴシエーションにグローバル トラストポイントを設定するには、[Global Settings] ポリシーの [IKEv2 Settings] タブを使用します。VPN グローバル IKEv2 設定を参照してください。

要素	説明
IKE Peer ID Validation	IKE ピア ID 検証を無視する（確認しない）か、必須とするか、または証明書によってサポートされている場合にかぎり確認するかを選択します。IKE ネゴシエーション中、ピアは互いに自身を識別する必要があります。
Enable Sending Certificate Chain	認可の証明書チェーンの送信をイネーブルにするかどうか。証明書チェーンには、ルート CA 証明書、ID 証明書、およびキー ペアが含まれます。
Enable Password Update with RADIUS Authentication	選択すると、RADIUS 認証プロトコルを使用してパスワードを更新できます。 RADIUS認証プロトコルを使用してパスワードを更新できるかどうか。詳細については、サポートされる AAA サーバ タイプを参照してください。
ISAKMP Keepalive	ISAKMP キープアライブをモニタするかどうか。[キープアライブのモニター（Monitor Keepalive）] オプションを選択した場合、デフォルトのフェールオーバーおよびルーティングのメカニズムとして IKE キープアライブを設定できます。次のパラメータを入力します。 • [信頼間隔（Confidence Interval）]：IKE キープアライブパケット送信から次の送信までのデバイスの待機時間（秒単位）。 • [再試行間隔（Retry Interval）]：デバイスがリモートピアとの IKE 接続の確立を試行する間隔（秒単位）。デフォルト値は2秒です。 詳細については、VPN グローバル ISAKMP/IPsec 設定を参照してください。
[Client Software Update] テーブル （IKEv1 のみ）	クライアント プラットフォームの VPN クライアントのリビジョン レベルおよび URL。すべての [All Windows Platforms]、[Windows 95/98/ME]、[Windows NT4.0/2000/XP]、または [VPN3002 Hardware Client] に対して別々のリビジョン レベルを設定できます。 プラットフォームにクライアントを設定するには、クライアントを選択して [行の編集（Edit Row）] ボタンをクリックし、[IPSec Client Software Update] ダイアログボックスに入力します。

Remote Access VPN Configuration ウィザード：[Defaults] ページ

Remote Access VPN Configuration ウィザードの [Defaults] ページを使用して、リモート アクセス IPSec VPN に割り当てる共有ポリシーを選択します。最初から選択されているポリシーは、リモート アクセス VPN 用に [Security Manager Administration] の [VPN Defaults] で設定されているポリシーです。これらのデフォルトを設定する方法については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定を参照してください。

必須のポリシーでは、常にポリシーが 1 つ選択されている必要があります。「Factory Default」が表示されている場合、適用されているポリシーは共有ポリシーではなく、Security Manager で指定されるデフォルトポリシー設定です。空のオプションを選択できる場合、ポリシーはオプションであり、関連機能が必要な場合にのみオプションを設定する必要があります。

ポリシーを割り当てる場合、割り当てるポリシーを検討するときには、次の点を考慮してください。

- 各ポリシー タイプのドロップダウン リストには、選択可能な既存の共有ポリシーが一覧表示されます。選択できる共有ポリシーは、Security Manager データベースにコミットされている（また、Workflow モードでアプルーバを使用している場合は承認されている）ポリシーだけです。共有ポリシーを作成して、送信前に使用することはできません。
- ポリシーの内容を表示するには、ポリシーを選択して [View Content（コンテンツの表示）] ボタンをクリックします。ポリシーが読み取り専用で表示されます。この表示を使用して、目的のポリシーを選択していることを確認します。

（注） 別のユーザによって現在ロックされているデフォルトポリシーを選択しようとすると、ロックの問題を警告するメッセージが表示されます。ロックを回避するには、別のポリシーを選択するか、またはロックが解除されるまで VPN の作成をキャンセルします。詳細については、ポリシーのロックについてを参照してください。

ナビゲーション パス

（デバイスビュー）リモートアクセス IPsec VPN を設定するための Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用 （17 ページ）を参照）。その後、このページが表示されるまで [次へ（Next）] をクリックします。

関連項目

- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （33 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス） （48 ページ）
- リモート アクセス VPN ポリシーの概要 （12 ページ）

フィールド リファレンス

表 *8 : Remote Access VPN Configuration* ウィザード、*[Defaults]* ページ

要素	説明
ASA グループの負荷分散	リモート アクセス VPN にある ASA デバイスのロード バランシングを定義します。

要素	説明
ハイ アベイラビリティ	リモート アクセス VPN の Cisco IOS ルータのハイ アベイラビリティ（HA）ポリシーを定義します。
Certificate to Connection Profile Map Policy	（IKEv1 のみ）リモートアクセス VPN にある ASA デバイスの証明書/接続プロファイル マップ オプションを定義します。
IKE Proposal	2 つのピアの間の IKE ネゴシエーションを保護するために使用するアルゴリズム セットを定義します。
IPSec Proposal	IPsec Security Associations（SA; セキュリティ アソシエーション）の設定に必要なクリプト マップを定義します。この定義内容には、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要なその他のパラメータが含まれます。
公開キーインフラストラクチャ	Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）証明書および RSA キーに対する PKI 登録要求の生成に使用する PKI ポリシーを定義します。
VPN Global Settings	リモートアクセス VPN にあるデバイスに適用される IKE、IPsec、IKEv2、NAT、およびフラグメンテーションのグローバル設定を定義します。

Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）

ここでは、Remote Access SSL VPN Configuration ウィザードを使用して、IOS デバイスで SSL VPN を作成または編集する方法について説明します。

関連項目

- リモート アクセス SSL VPN について （3 ページ）
- 各リモートアクセス VPN テクノロジーでサポートされるデバイスについて （10 ページ）

ステップ 1 デバイス ビューで、目的の IOS デバイスを選択します。

ステップ 2 ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）]>[構成ウィザード（Configuration Wizard）] を選択します。

ステップ 3 [リモートアクセスSSL VPN（Remote Access SSL VPN）] オプションボタンを選択します。

ステップ 4 [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックします。[Gateway and Context] ページが開きます。このページの要素の詳細については、SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS） （44 ページ）を参照してください。

ステップ 5 SSL VPN 内の保護されたリソースに接続する場合のプロキシとして使用するゲートウェイを選択します。次のオプションがあります。

- [既存のゲートウェイを使用（Use Existing Gateway）]：既存のゲートウェイオブジェクトを使用できます。このオプションを選択する場合、ゲートウェイを定義する [SSL VPN Gateway] ポリシー オブジェクトの名前を指定します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。
- [IP アドレスを使用して作成（Create Using IP Address）]：ルータ上の到達可能な（パブリックスタティック）IP アドレスを使用して、新しいゲートウェイオブジェクトを設定できます。IP アドレスを入力します。
- [インターフェイスを使用して作成（Create Using Interface）]：ルータインターフェイスのパブリックスタティック IP アドレスを使用して、新しいゲートウェイを設定できます。インターフェイスまたはインターフェイス ロール オブジェクトを選択します。

IP アドレスやインターフェイスを使用して新しいゲートウェイを作成することを選択した場合は、次の手順を実行します。

- ゲートウェイ名を指定します。
- HTTPS トラフィックを伝送するポート番号を指定します。HTTP ポート リダイレクトがイネーブルになっていない限り、デフォルトは 443 です。イネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。別のポートを使用する場合、1024 ～ 65535 の間で指定する必要があります。

ステップ 6 SSL VPN の仮想設定を定義するコンテキストの名前を入力します。

ステップ 7 SSL VPN ポリシー内で使用されるユーザ グループを選択します。ユーザ グループでは、SSL VPN ゲートウェイへの接続時にユーザが使用できるリソースを定義します。テーブルには、そのグループでフルクライアント アクセスがイネーブルであるかどうかが示されます。[編集（Edit）] をクリックして、目的のグループを選択するか、新しいグループを作成します。

ステップ 8 認証、認証ドメイン、およびアカウンティング用の AAA オプションを設定します。詳細については、SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS） （44 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックします。[Portal Page Customization] ページが開きます。このページの要素の詳細については、SSL VPN Configuration ウィザード：[Portal Page Customization] ページ（IOS） （47 ページ）を参照してください。

ステップ 10 [Portal Customization] ページで、次のオプションを設定します。ページの下部には、ポータル ページの外観のプレビューが、選択内容に応じて表示されます。このプレビューを使用して選択内容を調整します。

- [タイトル（Title）]：ページの上部に表示されるポータルページの名前。
- [ロゴ（Logo）]：ページのタイトル領域に表示されるグラフィック。[なし（None）]、[デフォルト（Default）]（Cisco のロゴグラフィック）、[カスタム（Custom）] から選択できます。[カスタム（Custom）] を選択する場合、[選択（Select）] をクリックして、Security Manager サーバー上にあるグラフィックを選択します。ポータル カスタマイゼーションでカスタム グラフィックを使用する前に、そのグラフィックをサーバにコピーする必要があります。

ロゴのソース イメージ ファイルに指定できるのは、GIF ファイル、JPG ファイル、または PNG ファイルです。ファイル名は最大 255 文字、サイズは最大 100 KB です。

- [ログインメッセージ（Login Message）]：ログインプロンプトの上に表示されるテキスト。

- [タイトルとテキストの色（Title and Text Colors）]：タイトルとログイン領域に使用する色とフォント。

ステップ 11 [終了（Finish）] をクリックして変更を保存します。

SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

リモート ユーザが SSL VPN の背後にあるプライベート ネットワーク上のリソースにアクセスできるように、デバイスでゲートウェイおよびコンテキストをあらかじめ設定しておく必要があります。SSL VPN Configuration ウィザードのこの手順を使用して、ユーザにポータル ページへのアクセスを許可する情報を含むゲートウェイおよびコンテキスト設定を指定します。

ナビゲーション パス

（デバイス ビュー）IOS デバイスでリモート アクセス SSL VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用 （17 ページ）を参照）。最初に表示されるページは [Gateway and Context] ページです。

関連項目

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（42 ページ）
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス
- AAA サーバおよびサーバ グループ オブジェクトについて

フィールド リファレンス

表 *9 : SSL VPN Configuration* ウィザード、*[Gateway and Context]* ページ

要素	説明
ゲートウェイ	SSL VPN 内の保護されたリソースに接続する場合のプロキシとして使用するゲートウェイ。次のオプションがあります。 • [既存のゲートウェイを使用（Use Existing Gateway）]：選択すると、SSL VPN に既存のゲートウェイを使用できます。 • [IPアドレスを使用して作成（Create Using IP Address）]：選択すると、ルータ上の到達可能な（パブリックスタティック）IP アドレスを使用して、新しいゲートウェイを設定できます。 • [インターフェイスを使用して作成（Create Using Interface）]：選択すると、ルータインターフェイスのパブリックスタティック IP アドレスを使用して、新しいゲートウェイを設定できます。
ゲートウェイ名	ゲートウェイを定義する [SSL VPN Gateway] ポリシー オブジェクトの名前。 • [既存のゲートウェイを使用（Use Existing Gateway）] を選択した場合、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） ゲートウェイを選択すると、セキュアな接続の確立に必要なポート番号とデジタル証明書が、関連するフィールドに表示されます。 • [Create Using IP Address] または [Interface] を選択した場合は、作成するオブジェクトの名前を入力します（最大 128 文字）。
IPアドレス	IP アドレスを使用してゲートウェイを作成するように選択した場合にのみ使用できます。 ゲートウェイ アドレスとして使用されるルータの IP アドレスです。
インターフェイス	インターフェイスを使用してゲートウェイを作成するように選択した場合にのみ使用できます。 SSL VPN ゲートウェイとして使用されるインターフェイスの名前、またはインターフェイスを定義するインターフェイス ロール オブジェクト。[選択（Select）] をクリックして、インターフェイスまたはインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。

要素	説明
[ポート（Port）]	SSL VPN 接続に使用するポート番号。HTTP ポート リダイレクトがイネーブルになっていない限り、デフォルトは 443 です。イネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。別の番号を入力する場合、1024 ～ 65535 の間で指定する必要があります。 • [Use Existing Gateway] を選択した場合、このフィールドは読み取り専用になり、選択したオブジェクトに設定されているポート番号が示されます。 • [IPアドレスを使用して作成（Create Using IP Address）] または [インターフェイス（Interface）] を選択した場合、ポート番号、または番号を指定するポートリストオブジェクトの名前を入力するか、[選択（Select）] をクリックしてポートリストオブジェクトを選択します。
Trustpoint	セキュアな接続を確立するために必要なデジタル証明書。SSL VPN ゲートウェイがアクティブな場合は、自己署名証明書が生成されます。
Context Name	SSL VPN の仮想設定を定義するコンテキストの名前。 （注） 多数のコンテキスト設定の管理を簡素化するには、コンテキスト名をドメインまたは仮想ホスト名と同じ名前にします。
Portal Page URL	SSL VPN の URL。ゲートウェイ オブジェクトを選択（または定義）すると入力されます。ユーザは、この URL に接続して VPN に入ります。
グループ ポリシー	SSL VPN ポリシー内で使用されるユーザ グループ。ユーザ グループでは、SSL VPN ゲートウェイへの接続時にユーザが使用できるリソースを定義します。テーブルには、そのグループでフル クライアント アクセスがイネーブルであるかどうかが示されます。[編集（Edit）] をクリックして、目的のグループを選択するか、新しいグループを作成します。
Authentication Server Group	認証サーバ グループ。リストは、プライオリティ順に表示されます。認証は最初のグループを使用して試行され、ユーザが認証または拒否されるまで、リスト内のグループが順に使用されます。ゲートウェイ自体でユーザが定義されている場合は、LOCAL グループを使用します。 AAA サーバ グループの名前を入力します。複数のエントリはカンマで区切ります。[選択（Select）] をクリックして、グループを選択するか、新しいグループを作成します。
認証ドメイン（Authentication Domain）	SSL VPN リモート ユーザ認証のリストまたは方式。リストも方式も指定しない場合、ゲートウェイではリモート ユーザ認証にグローバル AAA パラメータが使用されます。
Accounting Server Group	アカウンティング サーバ グループ。AAA サーバー グループ ポリシー オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

SSL VPN Configuration ウィザード：[Portal Page Customization] ページ（IOS）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

SSL VPN Configuration ウィザードのこの手順を使用して、リモート ユーザが SSL VPN に接続すると表示されるポータル ページの外観を定義します。リモートユーザーは、このポータル ページから SSL VPN ネットワーク上で使用可能なすべての Web サイトにアクセスできます。

ナビゲーション パス

（デバイスビュー）ASA デバイスでリモートアクセス SSL VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用（17 ページ）を参照）。次に、このページが表示されるまで [次へ（Next）] をクリックします。

関連項目

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（42 ページ）

フィールド リファレンス

表 *10 : SSL VPN Configuration* ウィザード：*[Portal Page Customization]* ページ

要素	説明
Title	ページの上部に表示されるテキスト。[Title Color] フィールドと [Text Color] フィールド内の [Primary] 設定を使用して色を制御します。
ロゴ	タイトルの隣に表示されるグラフィック。[None]、[Default]、または [Custom] を選択します。カスタムグラフィックを設定するには、目的のグラフィックを Cisco Security Manager サーバーにコピーし、[参照（Browse）] をクリックしてファイルを選択する必要があります。サポートされるグラフィック タイプは、GIF、JPG、および PNG で、最大サイズは 100 KB です。
ログイン メッセージ（Login Message）	ログインプロンプトのすぐ上に表示されるテキスト。[Title Color] フィールドと [Text Color] フィールド内の [Secondary] 設定を使用して色を制御します。

要素	説明
Title Color テキストの色	タイトルとログイン領域に使用される色とテキスト。 • [Primary]：タイトル、ログイン ボックスのタイトル、およびこれらの領域のテキスト。 • [Secondary]：ログイン ボックスのユーザ名とパスワード、およびこの領域のテキスト。 [選択（Select）] をクリックして背景色を選択します。テキストでは、テキスト リストから [Black] または [White] を選択します。
プレビュー	選択内容に基づいたポータル ページの外観のプレビュー。

Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco IOS、FWSM、IPS、および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、Remote Access VPN Configuration ウィザードを使用して、IOS デバイスおよび PIX 6.3 デバイスで IPSec VPN を作成または編集する方法について説明します。

ヒント このウィザードの [Defaults] ページ（ウィザードの最後のステップ）では、VPN で使用する共有ポリシーを選択できます。この機能を使用する場合、必要なすべての共有ポリシーがデータベースに設定および送信されていることを最初に確認する必要があります。共有ポリシーと VPN ポリシーのデフォルトの設定については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定を参照してください。

関連項目

- リモート アクセス IPSec VPN について （2 ページ）
- 各リモートアクセス VPN テクノロジーでサポートされるデバイスについて （10 ページ）

ステップ 1 [Device] ビューで、目的の IOS または PIX 6.3 デバイスを選択します。

ステップ 2 ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [構成ウィザード（Configuration Wizard）] を選択します。

ステップ 3 [リモートアクセスIPSec VPN（Remote Access IPSec VPN）] オプションボタンを選択します。

ステップ 4 [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックします。[User Group Policy] ページが開きます。

ステップ 5 [利用可能なユーザーグループ（Available User Groups）] リストから必要なユーザ グループを選択して、[>>] をクリックします。

- 必要なユーザーグループがリストにない場合、[作成（Create）]（+）をクリックして [ユーザーグループの追加（Add User Groups）] ダイアログボックスを開きます。このダイアログボックスでは、ユーザー グループ オブジェクトを作成または編集できます。[Add User Group]/[Edit User Group] ダイアログボックスを参照してください。
- 既存のユーザーグループをいずれかのリストで選択して [編集（Edit）]（鉛筆）をクリックすると、ユーザーグループを編集できます。
- ユーザーグループの選択を解除するには、ユーザーグループを選択して、[<<] をクリックします。

ステップ 6 [次へ（Next）] をクリックします。[Defaults] ページが開きます。

ステップ 7 VPN に割り当てる共有ポリシーを選択します。最初から選択されているポリシーは、[Security Manager Administration] の [VPN Defaults] ページで設定されているポリシーです。デフォルトを使用することも、使用可能なポリシーがある場合は別のポリシーを選択することもできます。これらのポリシーデフォルトの詳細については、Remote Access VPN Configuration ウィザード：[Defaults] ページ （40 ページ）を参照してください。

ステップ 8 [終了（Finish）] をクリックして変更を保存します。

作成したポリシーを調べて、実装するオプションを追加で設定します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。