概要

この章では、WebVPN サービス モジュール の概要、機能、およびリモート アクセスのモードについて説明します。内容は、次のとおりです。

Web VPN の概要

WebVPN サービス モジュール は、Catalyst 6500 シリーズ スイッチに搭載できるレイヤ 4 ～ 7 サービス モジュールです。Web VPN により、エンド ユーザは Web ブラウザを使用してセキュアなリモート アクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェアのクライアントは不要です。Web VPN を使用すると、HTTPS インターネット サイトに接続できるほとんどのコンピュータ上で、広範囲の Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。Web VPN は、Secure Socket Layer Protocol およびそれを継承する Transport Layer Security（SSL/TLS1）を使用して、リモート エンド ユーザと、中央サイトに設定したサポート対象の特定の内部リソース間にセキュアな接続を提供します。WebVPN サービス モジュール により、プロキシが必要な接続が認識されると、HTTP サーバが認証サブシステムと通信し、エンド 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、エンド ユーザに WebVPN リソースへのアクセスを提供します。エンド ユーザは、内部ネットワークのリソースに直接アクセスすることはできません。

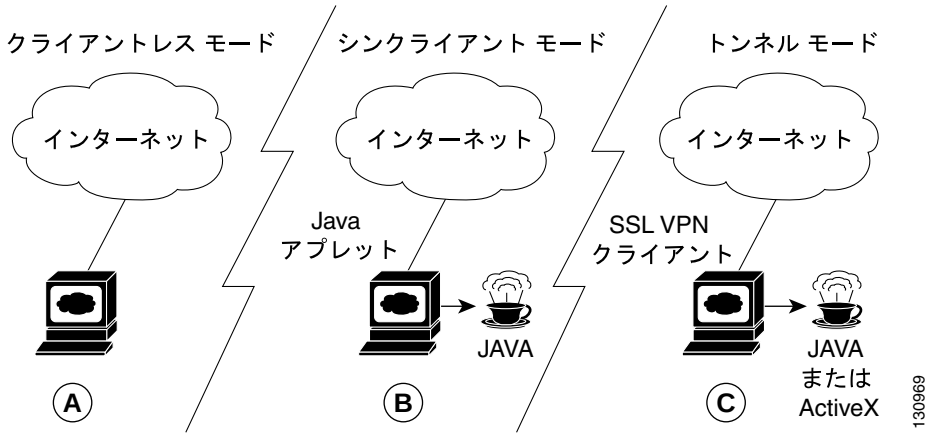
WebVPN サービス モジュール 上の接続は、リモート アクセス IPsec 接続とはまったく異なります。WebVPN 接続では、WebVPN サービス モジュール は、エンド ユーザの Web ブラウザとターゲット Web サーバ間のプロキシとして動作します。WebVPN のエンド ユーザが SSL 対応 Web サーバに接続すると、WebVPN サービス モジュール がセキュアな接続を確立し、サーバの SSL 証明書を評価します。エンド ユーザのブラウザは、提示された証明書を受信できないので、証明書を評価したり、確認することはできません。

リモート アクセスのモード

エンド ユーザのログインおよび認証は、Web ブラウザにより、HTTP リクエストを使用して、セキュア ゲートウェイに対して実行されます。これにより、クッキーにより参照されるセッションが作成されます。認証されると、エンド ユーザに対して、WebVPN ネットワークにアクセスできるポータル ページが表示されます。ブラウザから送信されるリクエストにはすべて、認証クッキーが含まれます。ポータル ページにより、内部ネットワーク上の使用可能なすべてのリソースが提供されます。たとえば、ポータル ページにより、シンクライアントの Java アプレット（TCP ポート転送用）またはトンネリング クライアントをダウンロードおよびインストールできるリンクを、エンド ユーザに提供できます。

図 1-1 に、リモート アクセス モードの概要を示します。

図 1-1　リモート アクセス モードの概要



A	クライアントレス モード	B	シンクライアント モード	C	トンネル モード
• ブラウザ ベース（クライアントレス） • Web 対応アプリケーション、ファイル共有（CIFS）、Outlook Web Access（OWA） • ゲートウェイが、アドレスまたはプロトコルの変換、コンテンツの解析と書き換えを実行		• TCP ポート転送 • Java アプレットを使用 • アプリケーション サポートを拡張 • Telnet、E メール、SSH、Meeting Maker、Sametime • スタティックなポート ベース アプリケーション		• 「クライアントレス」IPsec のように動作 • Java または ActiveX によりロードされたクライアントのトンネリング（約 500 kB） • アプリケーションを認識しない ― すべての IP ベース アプリケーションをサポート • スケーラブル • 管理者がインストレーションを許可	

以降のセクションで、サポートされる 3 つのリモート アクセス モードについて説明します。

- クライアントレス モード（p.1-3）
- シンクライアント モード（p.1-3）
- トンネル モード（p.1-4）

クライアントレス モード

クライアントレス モードでは、エンド ユーザは、クライアント マシン上の 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。

クライアントレス モードでは、次のアプリケーションがサポートされます。

- Web ブラウジング（HTTP およびセキュア HTTP [HTTPS] を使用）— エンド ユーザは、ポータル ページ上の URL ボックスと Web サーバ リンクのリストを使用して、Web をブラウズできます。
- ファイル共有（Common Internet File System [CIFS] を使用）— エンド ユーザは、ポータル ページ上のファイル サーバ リンクのリストを使用して、次の操作を実行できます。
  - ネットワークのブラウズ（ドメインのリスト）
  - ドメインのブラウズ（サーバのリスト）
  - サーバのブラウズ（共有のリスト）
  - 共有ファイルのリスト
  - 新規ファイルの作成
  - ディレクトリの作成
  - ディレクトリの名前変更
  - ファイルの更新
  - ファイルのダウンロード
  - ファイルの削除
  - ファイルの名前変更
- Microsoft Outlook Web Access（OWA）2003 などの Web ベース E メール（HTTP および HTTPS を使用）および Web Distributed Authoring and Versioning（WebDAV）拡張機能 — エンド ユーザは、リンクを使用して Exchange サーバに接続し、Web ベース E メールを読むことができます。

シンクライアント 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、クライアントの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。

シンクライアント モードでは、エンド ユーザは、ポータル ページに提供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。Java アプレットは、ゲートウェイに設定するサービスに対して、クライアント マシン上の TCP プロキシとして動作します。

シンクライアント モードでサポートされるアプリケーションは、主に E メール ベース（SMTP、POP3、および IMAP4）アプリケーションです。

（注） TCP ポート転送プロキシが動作するのは、Sun 1.4 Java Virtual Machine（JVM）以降のリリースだけです。ブラウザが 1.4 JVM をダウンロードするように、HTML が指定されます。アプレットも JVM のバージョンをチェックし、互換性のないバージョンの場合、実行を拒否します。

Java アプレットは、エンド ユーザ クライアントから WebVPN ゲートウェイへの HTTP リクエストを開始します。HTTP リクエスト（POST または CONNECT）には、内部 E メール サーバの名前およびポート番号が含まれます。WebVPN ゲートウェイは、指定された内部 E メール サーバおよびポートへの TCP 接続を作成します。

Java アプレットは、すべてのクライアント接続について、新しい SSL 接続を開始します。

シンクライアント モードを使用する場合には、次の制約に注意してください。

- エンド ユーザに、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ります。
- ポートがダイナミックにネゴシエートされる FTP などのアプリケーションには、シンクライアント モードを使用できません。TCP ポート転送を使用できるのは、スタティック ポートだけです。
- アプリケーションをシームレスに動作させるには、エンド ユーザに管理者権限を提供する必要があります。エンド ユーザに管理者権限を提供しない場合、エンド ユーザは、アプリケーションを適正に動作させるために、クライアント プログラムの設定を手動で変更する必要があります。

トンネル モード

一般的なクライアントレス リモート アクセスの場合、エンド ユーザは SSL トンネルを確立し、アプリケーション レイヤで内部ネットワークとのデータ通信（Web および E メールなど）を行います。トンネル モードでは、エンド ユーザは SSL トンネルを使用して、ネットワーク（IP）レイヤでデータ通信を行います。したがって、トンネル モードでは、ほとんどの IP ベース アプリケーションがサポートされます。トンネル モードは、多数の一般的な企業アプリケーション（Microsoft Outlook、Microsoft Exchange、Lotus Notes E-mail、Telnet など）をサポートしています。

トンネル接続は、グループ ポリシー設定により判別されます。エンド ユーザの PC に、SSL VPN クライアント（SVC）がダウンロードおよびインストールされ、エンド ユーザが WebVPN ゲートウェイにログインした時点で、トンネル接続が確立されます。

デフォルトでは、SVC は、接続終了後にクライアントの PC から削除されます。任意に、クライアントの PC に SVC を常時インストールしておくこともできます。