CHAPTER 15

クライアントレス SSL VPN ユーザ

概要

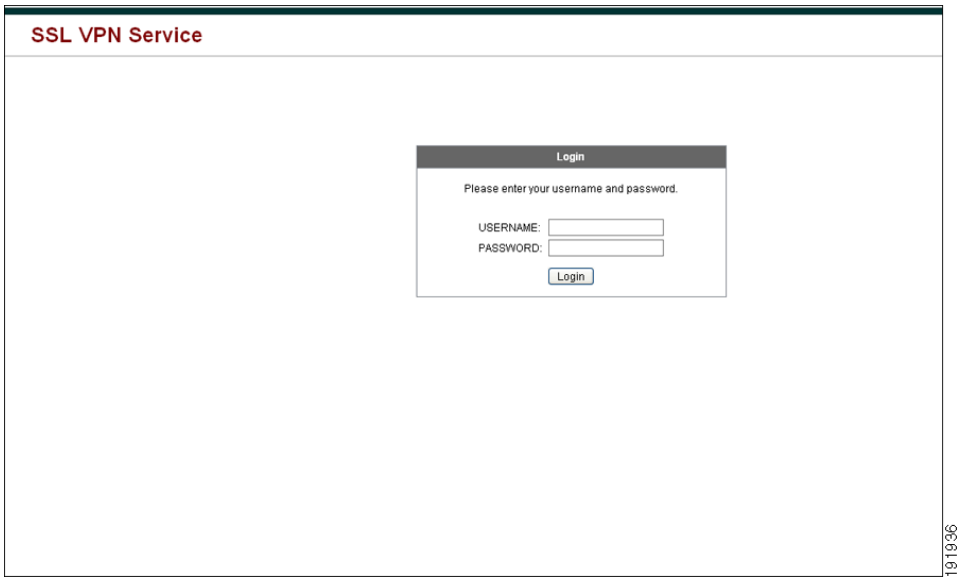
この項では、ユーザがクライアントレス SSL VPN の使用を開始するために、ユーザに伝える必要のある情報を明確にします。説明する項目は次のとおりです。

- 「パスワードの管理」（P.15-3）
- 「自動サインオンの使用」（P.15-9）
- 「セキュリティのヒントの通知」（P.15-11）
- 「クライアントレス SSL VPN の機能を使用するためのリモート システムの設定」（P.15-12）

エンドユーザ インターフェイスの定義

クライアントレス SSL VPN エンドユーザ インターフェイスは一連の HTML パネルで構成されます。ユーザは、ASA インターフェイスの IP アドレスを https://*address* 形式で入力することにより、クライアントレス SSL VPN にログインします。最初に表示されるパネルは、ログイン画面（図 15-1）です。

図 15-1　クライアントレス SSL VPN の [Login] 画面



クライアントレス SSL VPN ホーム ページの表示

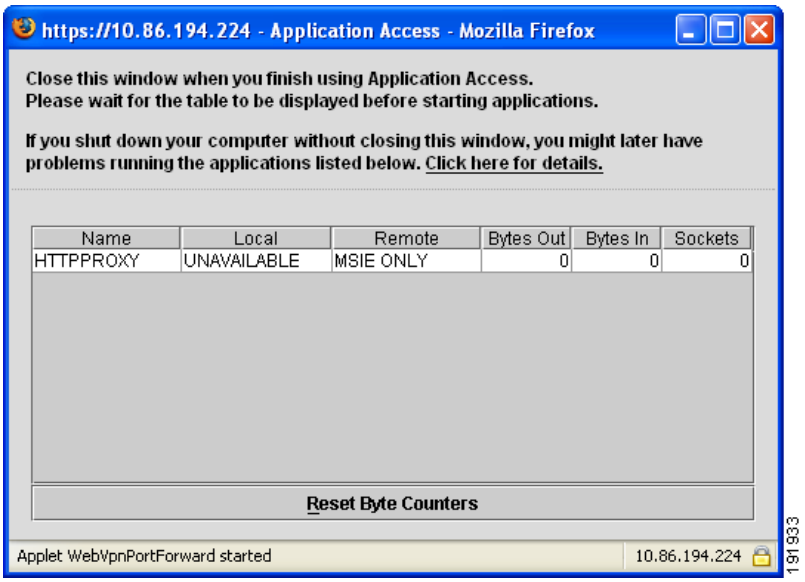
ユーザがログインすると、ポータル ページが開きます。

ホーム ページには設定済みのクライアントレス SSL VPN 機能がすべて表示され、選択済みのロゴ、テキスト、および色が外観に反映されています。このサンプル ホーム ページには、特定のファイル共有の指定機能以外のすべてのクライアントレス SSL VPN 機能が表示されています。ユーザはこのホーム ページを使用して、ネットワークのブラウズ、URL の入力、特定の Web サイトへのアクセス、および Application Access（ポート転送とスマート トンネル）による TCP アプリケーションへのアクセスを実行できます。

クライアントレス SSL VPN の Application Access パネルの表示

ポート転送またはスマート トンネルを開始するには、[Application Access] ボックスの [Go] ボタンをクリックします。[Application Access] ウィンドウが開きます（図 15-2）。

図 15-2　クライアントレス SSL VPN の [Application Access] ウィンドウ



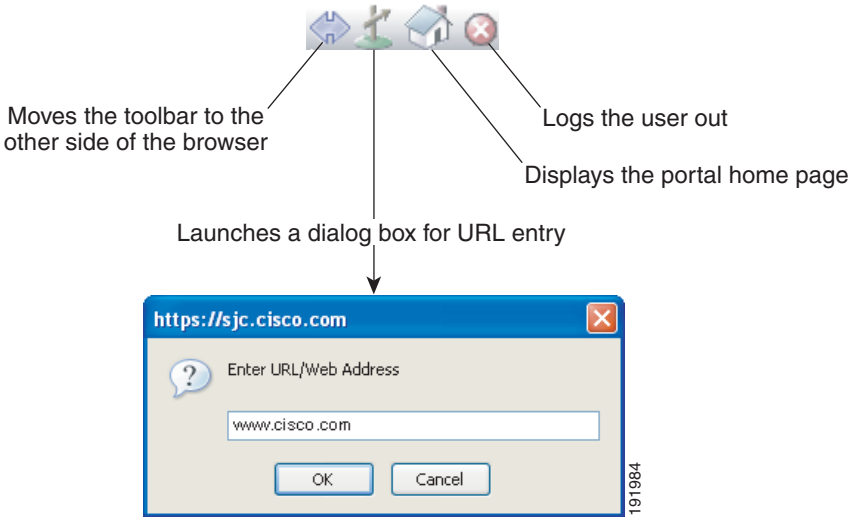
このウィンドウには、このクライアントレス SSL VPN 接続用に設定された TCP アプリケーションが表示されます。このパネルを開いたままでアプリケーションを使用する場合は、通常の方法でアプリケーションを起動します。

（注）　ステートフル フェールオーバーでは、Application Access を使用して確立したセッションは保持されません。ユーザはフェールオーバー後に再接続する必要があります。

フローティング ツールバーの表示

図 15-3 に示すフローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。

図 15-3　クライアントレス SSL VPN フローティング ツールバー



フローティング ツールバーの次の特性に注意してください。

- ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。
- ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。
- ツールバーを閉じると、ASA はクライアントレス SSL VPN セッションを終了するよう促すメッセージを表示します。

クライアントレス SSL VPN の使用方法については、表 15-1（P.15-11）を参照してください。

パスワードの管理

オプションで、パスワードの期限切れが近づくとエンド ユーザに警告するように ASA を設定できます。

ASA では、RADIUS および LDAP プロトコルのパスワード管理をサポートします。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPsec リモート アクセスと SSL VPN トンネル グループのパスワード管理を設定できます。パスワード管理を設定すると、ASA は、リモート ユーザのログイン時に、現在のパスワードの期限切れが近づいていること、または期限が切れていることを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このコマンドは、そのような通知をサポートする AAA サーバに対して有効です。

ASA のリリース 7.1 以降では通常、LDAP による認証時、または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPsec VPN クライアント
- クライアントレス SSL VPN

RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバのみに対して通信しているように見えます。

前提条件

- ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

  認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。

  Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
  Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。制約事項
- MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。
- Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポート*されません*。
- LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。
- RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

手順の詳細

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] > [Add or Edit] > [Advanced] > [General] > [Password Management] に移動します。

ステップ 2　[Enable password management] オプションをクリックします。

シスコの認証スキームの SiteMinder への追加

SiteMinder による SSO を使用するための ASA の設定に加え、Java プラグインとして提供されているシスコの認証スキーム（シスコの Web サイトからダウンロード）を使用するようにユーザの CA SiteMinder ポリシー サーバを設定する必要もあります。

前提条件

SiteMinder ポリシー サーバを設定するには、SiteMinder の経験が必要です。

手順の詳細

この項では、手順のすべてではなく、一般的なタスクを取り上げます。

ステップ 1　SiteMinder Administration ユーティリティを使用して、次の特定の引数を使用できるようにカスタム認証スキームを作成します。

- [Library] フィールドに、**smjavaapi** と入力します。
- [Secret] フィールドに、ASA に設定したものと同じ秘密キーを入力します。

  コマンドライン インターフェイスで **policy-server-secret** コマンドを使用して、ASA に秘密キーを設定します。
- [Parameter] フィールドに、**CiscoAuthAPI** と入力します。

ステップ 2　Cisco.com にログインして、http://www.cisco.com/cisco/software/navigator.html から **cisco_vpn_auth.jar** ファイルをダウンロードして、SiteMinder サーバのデフォルトのライブラリ ディレクトリにコピーします。この .jar ファイルは、Cisco ASA CD にも含まれています。

SAML POST SSO サーバの設定

サーバ ソフトウェア ベンダーが提供する SAML サーバのマニュアルに従って、SAML サーバを Relying Party モードで設定します。

手順の詳細

ステップ 1　アサーティング パーティ（ASA）を表す SAML サーバ パラメータを設定します。

- Recipient consumer URL（ASA で設定する assertion consumer URL と同一）
- Issuer ID（通常はアプライアンスのホスト名である文字列）
- Profile type：Browser Post Profile

ステップ 2　証明書を設定します。

ステップ 3　アサーティング パーティのアサーションには署名が必要なことを指定します。

ステップ 4　SAML サーバがユーザを特定する方法を、次のように選択します。

- Subject Name Type が DN
- Subject Name format が uid=<user>

HTTP Form プロトコルを使用した SSO の設定

この項では、SSO における HTTP Form プロトコルの使用について説明します。HTTP Form プロトコルは、SSO 認証を実行するための手段で、AAA 方式としても使用できます。このプロトコルは、クライアントレス SSL VPN のユーザおよび認証を行う Web サーバの間で認証情報を交換するセキュアな方法を提供します。RADIUS サーバや LDAP サーバなどの他の AAA サーバと組み合わせて使用することができます。

前提条件

HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

制約事項

これは、一般的なプロトコルとして、認証に使用する Web サーバ アプリケーションの次の条件に一致する場合にだけ適用できます。

- 認証クッキーは、正常な要求に対して設定され、未許可のログインに対して設定されないようにする必要があります。この場合、ASA は、成功した認証と失敗した認証を区別することはできません。

手順の詳細

ASA は、ここでも認証 Web サーバに対するクライアントレス SSL VPN のユーザのプロキシとして機能しますが、この場合は、要求に対して HTTP Form プロトコルと POST 方式を使用します。フォーム データを送受信するように ASA を設定する必要があります。図 15-4 は、次の SSO 認証手順を示しています。

ステップ 1　最初に、クライアントレス SSL VPN のユーザは、ユーザ名とパスワードを入力して ASA 上のクライアントレス SSL VPN サーバにログオンします。

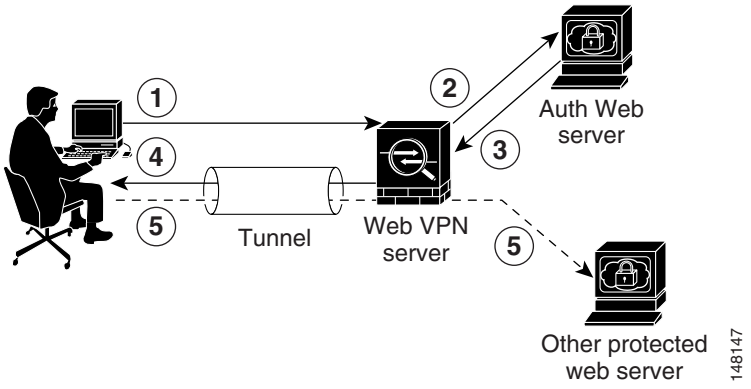
ステップ 2　ユーザのプロキシとして動作するクライアントレス SSL VPN サーバは、このフォーム データ（ユーザ名およびパスワード）を、POST 認証要求を使用して認証する Web サーバに転送します。

ステップ 3　認証する Web サーバがユーザのデータを承認した場合は、認証クッキーをユーザの代行で保存していたクライアントレス SSL VPN サーバに戻します。

ステップ 4　クライアントレス SSL VPN サーバはユーザまでのトンネルを確立します。

ステップ 5　これでユーザは、ユーザ名やパスワードを再入力しなくても、保護された SSO 環境内の他の Web サイトにアクセスできるようになります。

図 15-4　HTTP Form を使用した SSO 認証



ASA でユーザ名やパスワードなどの POST データを含めるようにフォーム パラメータを設定しても、Web サーバが要求する非表示のパラメータが追加されたことに、ユーザが最初に気付かない可能性があります。認証アプリケーションの中には、ユーザ側に表示されず、ユーザが入力することもない非表示データを要求するものもあります。ただし、認証 Web サーバが要求する非表示パラメータを見つけるのは可能です。これは、ASA を仲介役のプロキシとして使用せずに、ユーザのブラウザから Web サーバに直接認証要求を出す方法で行います。HTTP ヘッダー アナライザを使用して Web サーバの応答を分析すると、非表示パラメータが次のような形式で表示されます。

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

非表示パラメータには、必須のパラメータとオプションのパラメータとがあります。Web サーバが非表示パラメータのデータを要求すると、Web サーバはそのデータを省略するすべての認証 POST 要求を拒否します。ヘッダー アナライザは、非表示パラメータが必須かオプションかについては伝えないため、必須のパラメータが判別できるまではすべての非表示パラメータを含めておくことをお勧めします。

HTTP Form データの収集

この項では、必要な HTTP Form データを検出および収集する手順を示します。認証 Web サーバが要求するパラメータが何かわからない場合は、認証交換を分析するとパラメータ データを収集することができます。

前提条件

これらの手順では、ブラウザと HTTP ヘッダー アナライザが必要です。

手順の詳細

ステップ 1　ユーザのブラウザと HTTP ヘッダー アナライザを起動して、ASA を経由せずに Web サーバのログイン ページに直接接続します。

ステップ 2　Web サーバのログイン ページがユーザのブラウザにロードされてから、ログイン シーケンスを検証して交換時にクッキーが設定されているかどうか判別します。Web サーバによってログイン ページにクッキーがロードされている場合は、このログイン ページの URL を *start-URL* として設定します。

ステップ 3　Web サーバにログオンするためのユーザ名とパスワードを入力して、Enter を押します。この動作によって、ユーザが検証する認証 POST 要求が HTTP ヘッダー アナライザを使用して生成されます。

次に、ホストの HTTP ヘッダーおよび本文が記載された POST 要求の例を示します。

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05
-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIr
NT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmye
mco%2FHTTP/1.1

Host: www.example.com

(BODY)

SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%
2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

ステップ 4　POST 要求を検証してプロトコル、ホストをコピーし、URL を入力して action-uri パラメータを設定します。

ステップ 5　POST 要求の本文を検証して、次の情報をコピーします。

a. ユーザ名パラメータ。上記の例では、このパラメータは *USERID* で、値 *anyuser* ではありません。

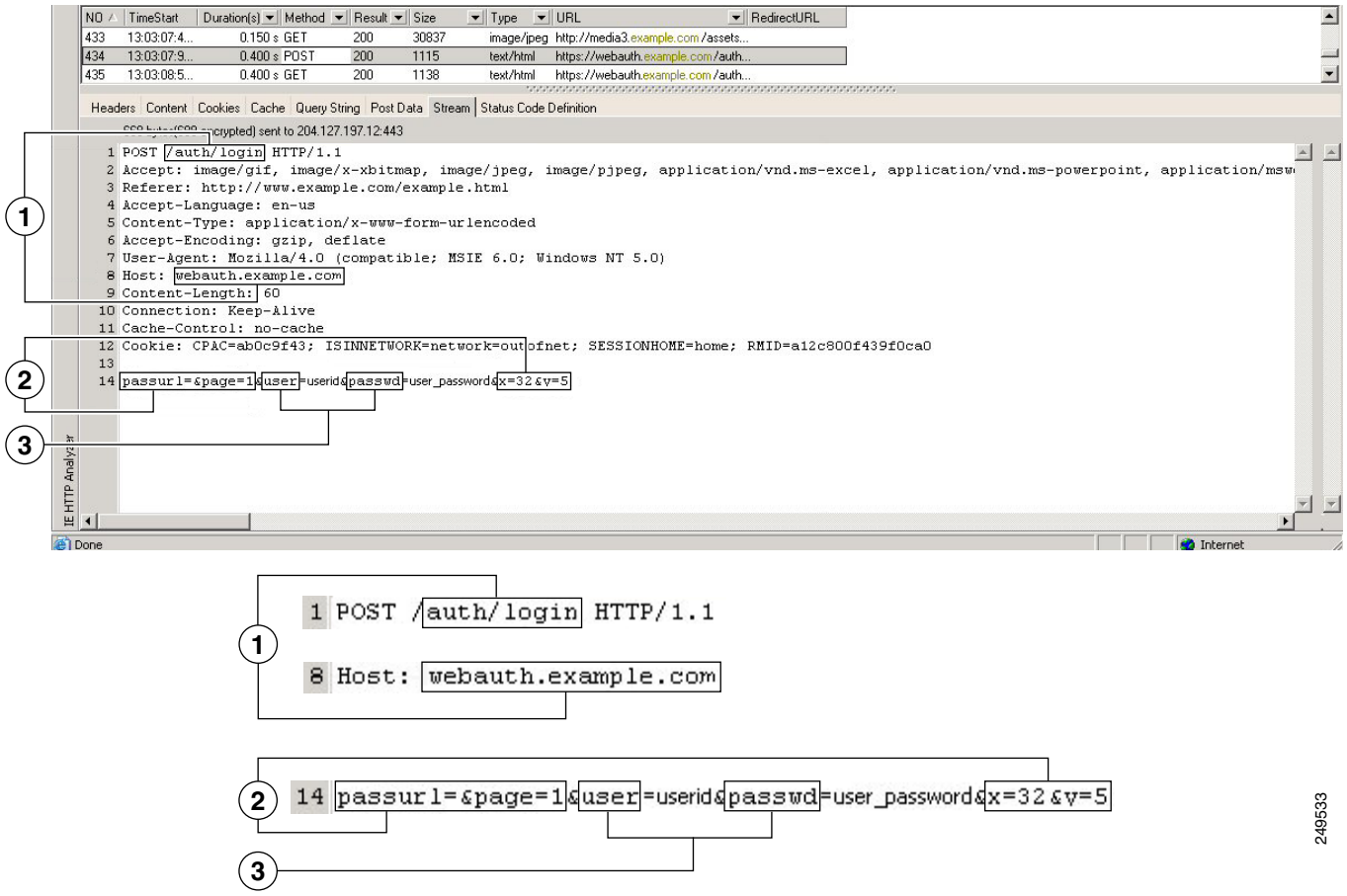
b. パスワード パラメータ。上記の例では、このパラメータは *USER_PASSWORD* です。

c. 非表示パラメータ。このパラメータは、POST 本文からユーザ名パラメータとパスワード パラメータを除くすべてです。前の例の非表示パラメータは次のとおりです。

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0

図 15-5 は、HTTP アナライザの出力例に表示される action URI、非表示、ユーザ名、パスワードの各種パラメータを強調して示したものです。これは一例です。出力は Web サイトによって大幅に異なることがあります。

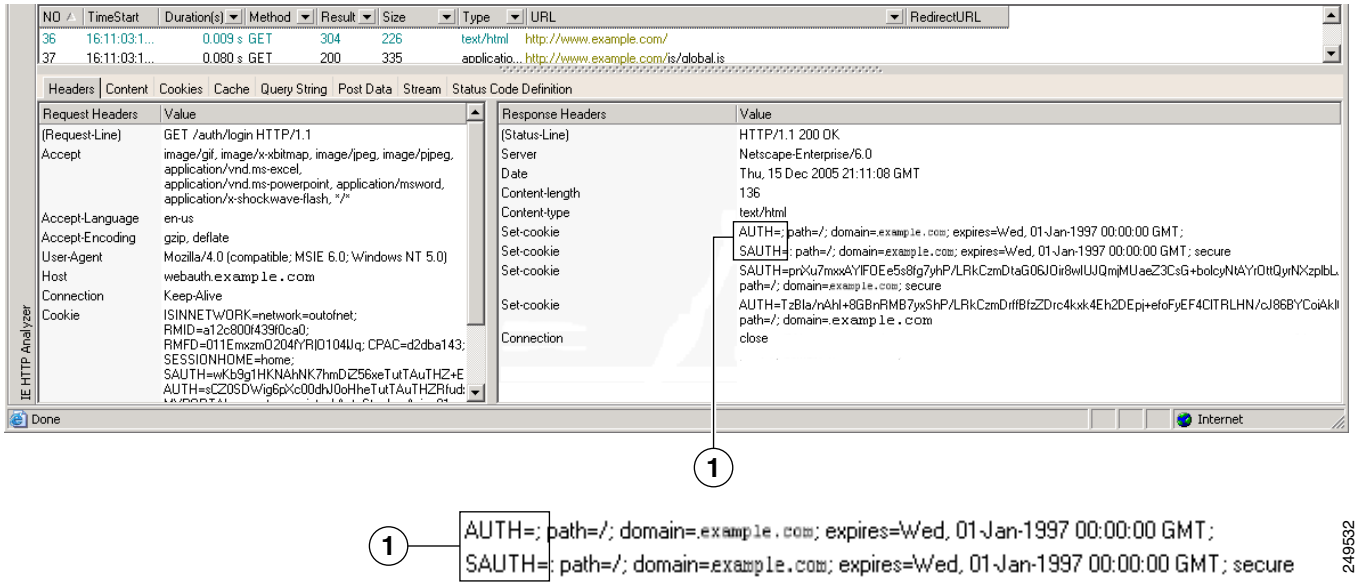
図 15-5　action-uri、非表示、ユーザ名、パスワードの各種パラメータ



ステップ 6　Web サーバへのログオンが成功したら、HTTP ヘッダー アナライザを使用して、サーバからユーザのブラウザに設定されているクッキー名を見つけ出すことによって、サーバの応答を検証します。これは **auth-cookie-name** パラメータです。

次のサーバ応答ヘッダーでは、SMSESSION がセッションのクッキーの名前です。必要なのはこの名前だけです。値は不要です。図 15-6 に、HTTP アナライザによる認可クッキーの出力例を示します。これは一例です。出力は Web サイトによって大幅に異なることがあります。

図 15-6　HTTP アナライザの出力例に表示された認可クッキー



1	認可クッキー

ステップ 7　場合によっては、認証の成否にかかわらず同じクッキーがサーバによって設定される可能性があり、このようなクッキーは、SSO の目的上、認められません。クッキーが異なっていることを確認するには、無効なログイン クレデンシャルを使用してステップ 1 からステップ 6 を繰り返し、「失敗」クッキーと「成功した」クッキーとを比較します。これで、HTTP Form プロトコルによる SSO を ASA に設定するために必要なパラメータ データを入手できました。

自動サインオンの使用

[Auto Sign-on] ウィンドウまたはタブでは、クライアントレス SSL VPN ユーザの自動サインオンを設定または編集できます。自動サインオンは、内部ネットワークに SSO 方式をまだ展開していない場合に使用できる簡素化された単一サインオン方式です。特定の内部サーバに対して自動サインオンを設定すると、ASA は、クライアントレス SSL VPN ユーザが ASA へのログオンで入力したログイン クレデンシャル（ユーザ名とパスワード）をそれら特定の内部サーバに渡します。特定の範囲のサーバの特定の認証方式に応答するように、ASA を設定します。ASA が応答するように設定可能な認証方式は、Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべてを使用する認証で構成されます。

ユーザ名とパスワードのルックアップが ASA で失敗した場合は、空の文字列で置き換えられ、動作は自動サインオンが不可の場合の状態に戻されます。

自動サインオンは、特定の内部サーバに SSO を設定する直接的な方法です。この項では、自動サインオンを行うように SSO をセットアップする手順について説明します。Computer Associates SiteMinder SSO サーバを使用して SSO をすでに導入している場合、または Security Assertion Markup Language（SAML）Browser Post Profile SSO がある場合。このソリューションをサポートするように ASA を設定するには、「SSO サーバ」（P.12-7）を参照してください。

次のフィールドが表示されます。

- [IP Address]：次の [Mask] と組み合わせて、認証されるサーバの IP アドレスの範囲を [Add/Edit Auto Sign-on] ダイアログボックスで設定されたとおりに表示します。サーバは、サーバの URI またはサーバの IP アドレスとマスクで指定できます。
- [Mask]：前の [IP Address] と組み合わせて、[Add/Edit Auto Sign-on] ダイアログボックスで自動サインオンをサポートするように設定されたサーバの IP アドレスの範囲を表示します。
- [URI]：[Add/Edit Auto Sign-on] ダイアログボックスで設定されたサーバを識別する URI マスクを表示します。
- [Authentication Type]：[Add/Edit Auto Sign-on] ダイアログボックスで設定された認証のタイプ（Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべて）を表示します。

制約事項

- 認証が不要なサーバ、または ASA とは異なるクレデンシャルを使用するサーバでは、自動サインオンをイネーブルにしないでください。自動サインオンがイネーブルの場合、ASA は、ユーザ ストレージにあるクレデンシャルに関係なく、ユーザが ASA へのログオンで入力したログイン クレデンシャルを渡します。
- 一定範囲のサーバに対して 1 つの方式（HTTP Basic など）を設定する場合に、その中の 1 台のサーバが異なる方式（NTLM など）で認証を試みると、ASA はユーザのログイン クレデンシャルをそのサーバに渡しません。

手順の詳細

ステップ 1　クリックして自動サインオン命令を追加または編集します。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。

ステップ 2　[Auto Sign-on] テーブルで選択した自動サインオン命令を削除する場合にクリックします。

ステップ 3　[IP Block] をクリックして、IP アドレスとマスクを使用して内部サーバの範囲を指定します。

- [IP Address]：自動サインオンを設定する範囲の最初のサーバの IP アドレスを入力します。
- [Mask]：[subnet mask] メニューで、自動サインオンをサポートするサーバのサーバ アドレス範囲を定義するサブネット マスクを選択します。

ステップ 4　[URI] をクリックして、URI によって自動サインオンをサポートするサーバを指定し、このボタンの横にあるフィールドに URI を入力します。

ステップ 5　サーバに割り当てられる認証方式を決定します。指定された範囲のサーバの場合には、Basic HTTP 認証要求、NTLM 認証要求、FTP と CIFS の認証要求、またはこれら方式のいずれかを使用する要求に応答するように、ASA を設定できます。

- [Basic]：サーバが Basic（HTTP）認証をサポートする場合は、このボタンをクリックします。
- [NTLM]：サーバが NTLMv1 認証をサポートする場合は、このボタンをクリックします。
- [FTP/CIFS]：サーバが FTP と CIFS の認証をサポートする場合は、このボタンをクリックします。
- [Basic, NTLM, and FTP/CIFS]：サーバが上のすべての方式をサポートする場合は、このボタンをクリックします。

ユーザ名とパスワードの要求

ネットワークによっては、リモート セッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、クライアントレス SSL VPN、メール サーバ、ファイル サーバ、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。

表 15-1 に、クライアントレス SSL VPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 15-1　クライアントレス SSL VPN セッションのユーザに提供するユーザ名とパスワード

ログイン ユーザ名/パスワード タイプ	目的	入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN の起動
ファイル サーバ	リモート ファイル サーバへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	クライアントレス SSL VPN 経由によるリモート メール サーバへのアクセス	電子メール メッセージの送受信

セキュリティのヒントの通知

ユーザはいつでもツールバーの [Logout] アイコンをクリックして、クライアントレス SSL VPN セッションを閉じることができます（ブラウザ ウィンドウを閉じてもセッションは閉じません）。

クライアントレス SSL VPN は、企業ネットワーク上のリモート PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。クライアントレス SSL VPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信は暗号化されていないため、プライベートではありません。

「クライアントレス SSL VPN セキュリティ対策」（P.1）に、セッション内で実行する手順に応じて、ユーザと通信するための追加のヒントを示します。

クライアントレス SSL VPN の機能を使用するためのリモート システムの設定

この項では、クライアントレス SSL VPN を使用するようにリモート システムを設定する方法について説明します。

ユーザ アカウントを別々に設定でき、各ユーザは異なるクライアントレス SSL VPN の機能を使用できます。

クライアントレス SSL VPN の起動

次のようなサポートされている接続を使用して、インターネットに接続できます。

- 家庭の DSL、ケーブル、ダイヤルアップ。
- 公共のキオスク。
- ホテルのホットスポット。
- 空港の無線ノード。
- インターネット カフェ。

（注）　クライアントレス SSL VPN がサポートする Web ブラウザのリストについては、『*Supported VPN Platforms, Cisco ASA Series*』を参照してください。

前提条件

- ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
- クライアントレス SSL VPN の URL が必要です。URL は、https://*address* の形式の https アドレスである必要があります。*address* は、SSL VPN がイネーブルである ASA（またはロードバランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、https://cisco.example.com などです。
- クライアントレス SSL VPN のユーザ名とパスワードが必要です。

制約事項

- クライアントレス SSL VPN ではローカル印刷がサポートされていますが、VPN 経由による企業ネットワーク上のプリンタへの印刷はサポートされていません。

クライアントレス SSL VPN フローティング ツールバーの使用

フローティング ツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。

フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。[Close] ボタンをクリックすると、ASA によってクライアントレス SSL VPN セッションを閉じることを求めるメッセージが表示されます。

ヒント　テキストをテキスト フィールドに貼り付けるには、Ctrl を押した状態で V を押します（クライアントレス SSL VPN セッション中は、表示されるツールバー上での右クリックはオフになっています）。

制約事項

ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。

Web のブラウズ

クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。「セキュリティのヒントの通知」を参照してください。

クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。

- クライアントレス SSL VPN のタイトル バーが各 Web ページの上部に表示される。
- Web サイトへのアクセス方法：
  - クライアントレス SSL VPN [Home] ページ上の [Enter Web Address] フィールドに URL を入力する
  - クライアントレス SSL VPN [Home] ページ上にある設定済みの Web サイト リンクをクリックする
  - 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN [Home] ページ上にリンクとして表示されるものに限られる

前提条件

保護されている Web サイトのユーザ名とパスワードが必要です。

制約事項

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN [Home] ページ上にリンクとして表示されるものに限られる

ネットワークのブラウズ（ファイル管理）

ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。

（注）　コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。

前提条件

- 共有リモート アクセス用にファイル アクセス権を設定する必要があります。
- 保護されているファイル サーバのサーバ名とパスワードが必要です。
- フォルダとファイルが存在するドメイン、ワークグループ、およびサーバの名前が必要です。

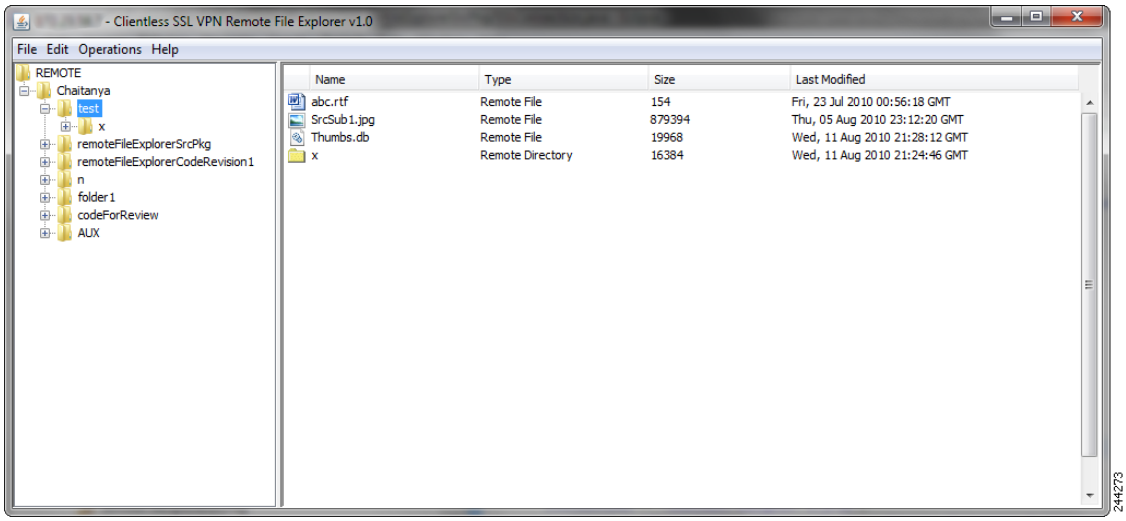
制約事項

クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。

Remote File Explorer の使用

ユーザは、Remote File Explorer を使用して、Web ブラウザから企業ネットワークをブラウズできます。ユーザが Cisco SSL VPN ポータル ページの [Remote File System] アイコンをクリックすると、ユーザのシステムでアプレットが起動し、ツリーおよびフォルダ ビューにリモート ファイル システムが表示されます。

図 15-7　Clientless SSL VPN Remote File Explorer



ユーザはブラウザで次を実行できます。

- リモート ファイル システムのブラウズ。
- ファイルの名前の変更。
- リモート ファイル システム内、およびリモートとローカルのファイル システム間でのファイルの移動またはコピー
- ファイルのバルク アップロードおよびダウンロードの実行。

（注）　この機能では、ユーザのマシンに Oracle Java ランタイム環境（JRE）1.4 以降がインストールされ、Web ブラウザで Java がイネーブルになっている必要があります。リモート ファイルの起動には、JRE 1.6 以降が必要です。

ファイルまたはフォルダの名前変更

ファイルまたはフォルダの名前を変更するには、次の手順を実行します。

ステップ 1　名前を変更するファイルまたはフォルダをクリックします。

ステップ 2　[Edit] > [Rename] を選択します。

ステップ 3　プロンプトが表示されたら、ダイアログに新しい名前を入力します。

ステップ 4　[OK] をクリックして、ファイルまたはフォルダの名前を変更します。または、名前を変更しない場合は [Cancel] をクリックします。

リモート サーバでのファイルやフォルダの移動またはコピー

リモート サーバでファイルやフォルダを移動またはコピーするには、次の手順を実行します。

ステップ 1　移動またはコピーするファイルやフォルダが含まれている送信元フォルダに移動します。

ステップ 2　ファイルまたはフォルダをクリックします。

ステップ 3　ファイルをコピーするには、[Edit] > [Copy] を選択します。また、ファイルを移動するには、[Edit] > [Cut] を選択します。

ステップ 4　宛先フォルダに移動します。

ステップ 5　[Edit] > [Paste] を選択します。

ローカル システム ドライブからリモート フォルダへのファイルのコピー

ローカル ファイル システムとリモート ファイル システム間でファイルをコピーするには、リモート ファイル ブラウザの右ペインとローカル ファイル マネージャ アプリケーション間でファイルをドラッグ アンド ドロップします。

ファイルのアップロードおよびダウンロード

ファイルをダウンロードするには、ブラウザでファイルをクリックし、[Operations] > [Download] を選択し、[Save] ダイアログで場所と名前を指定してファイルを保存します。

ファイルをアップロードするには、宛先フォルダをクリックし、[Operations] > [Upload] を選択し、[Open] ダイアログでファイルの場所と名前を指定します。

この機能には次の制限があります。

- ユーザは、アクセスを許可されていないサブフォルダを表示できません。
- ユーザがアクセスを許可されていないファイルは、ブラウザに表示されても移動またはコピーできません。
- ネストされたフォルダの最大の深さは 32 です。
- ツリー ビューでは、ドラッグ アンド ドロップのコピーがサポートされていません。
- Remote File Explorer の複数のインスタンスの間でファイルを移動するときは、すべてのインスタンスが同じサーバを探索する必要があります（ルート共有）。
- Remote File Explorer は、1 つのフォルダに最大 1500 のファイルおよびフォルダを表示できます。フォルダがこの制限を超えた場合、フォルダは表示されません。

ポート転送の使用

(注)　ユーザは、アプリケーションを使用し終えたら、[Close] アイコンをクリックして必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がオフに切り替わる可能性があります。詳細については、「Application Access 使用時の hosts ファイル エラーからの回復」（P.18-1）を参照してください。

前提条件

- Mac OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。
- クライアント アプリケーションがインストールされている必要があります。
- ブラウザでクッキーをイネーブルにする必要があります。
- DNS 名を使用してサーバを指定する場合、ホスト ファイルの変更に必要になるため、PC に対する管理者アクセス権が必要です。
- Oracle Java ランタイム環境（JRE）バージョン 1.4.x と 1.5.x がインストールされている必要があります。

  JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。まれに、Java 例外エラーで、ポート転送アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。

  a. ブラウザのキャッシュをクリアして、ブラウザを閉じます。
  b. Java アイコンがコンピュータのタスク バーに表示されていないことを確認します。
  c. Java のインスタンスをすべて閉じます。
  d. クライアントレス SSL VPN セッションを確立し、ポート転送 Java アプレットを起動します。
- ブラウザで javascript をイネーブルにする必要があります。デフォルトでは有効に設定されています。
- 必要に応じて、クライアント アプリケーションを設定する必要があります。

（注）　Microsoft Outlook クライアントの場合、この設定手順は不要です。Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] フィールドの値をチェックします。[Remote Server] フィールドにサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。[Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。

制約事項

この機能を使用するには、Oracle Java ランタイム環境（JRE）をインストールしてローカル クライアントを設定する必要があります。これには、ローカル システムでの管理者の許可、または C:\windows\System32\drivers\etc の完全な制御が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

手順の詳細

クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。

1. クライアントレス SSL VPN セッションを開始して、[Home] ページの [Application Access] リンクをクリックします。[Application Access] ウィンドウが表示されます。
2. [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。
3. この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。

（注）　クライアントレス SSL VPN セッション上で実行しているアプリケーションで URL（電子メール メッセージ内のものなど）をクリックしても、サイトがそのセッションで開くわけではありません。サイトをセッション上で開くには、その URL を [Enter Clientless SSL VPN (URL) Address] フィールドに貼り付けます。

ポート転送を介した電子メールの使用

電子メールを使用するには、クライアントレス SSL VPN のホーム ページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。

（注）　IMAP クライアントの使用中にメール サーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。

前提条件

アプリケーション アクセスおよびその他のメール クライアントの要件を満たしている必要があります。

制約事項

Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。

クライアントレス SSL VPN は、Lotus Notes および Eudora などの、ポート転送を介したその他の SMTPS、POP3S、または IMAP4S 電子メール プログラムをサポートしますが、動作確認は行っていません。

Web アクセスを介した電子メールの使用

次の電子メール アプリケーションがサポートされています。

- Microsoft Outlook Web App to Exchange Server 2010

  OWA には、Internet Explorer 7 以降、または Firefox 3.01 以降が必要です。
- Microsoft Outlook Web Access to Exchange Server 2007、2003、および 2000

  最適な結果を得るために、Internet Explorer 8.x 以降または Firefox 8.x で OWA を使用してください。
- Louts iNotes

前提条件

Web ベースの電子メール製品がインストールされている必要があります。

制約事項

その他の Web ベースの電子メール アプリケーションも動作しますが、動作確認は行っていません。

電子メール プロキシを介した電子メールの使用

次のレガシー電子メール アプリケーションがサポートされています。

- Microsoft Outlook 2000 および 2002
- Microsoft Outlook Express 5.5 および 6.0

メール アプリケーションの使用方法と例については、「クライアントレス SSL VPN を介した電子メールの使用」（P.12-23）を参照してください。

前提条件

- SSL 対応メール アプリケーションがインストールされている必要があります。
- ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。
- メール アプリケーションが正しく設定されている必要があります。

制約事項

その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。

スマート トンネルの使用

スマート トンネルの使用に管理権限は必要ありません。

（注）　ポート フォワーダの場合と異なり、Java は自動的にダウンロードされません。

前提条件

- スマート トンネルには、Windows では ActiveX または JRE（1.4x および 1.5x）、Mac OS X では Java Web Start が必要です。
- ブラウザで Cookie をイネーブルにする必要があります。
- ブラウザで javascript をイネーブルにする必要があります。

制約事項

- Mac OS X では、フロントサイド プロキシはサポートされていません。
- 「スマート トンネル アクセスの設定」（P.13-1）で指定されているオペレーティング システムおよびブラウザだけがサポートされています。
- TCP ソケットベースのアプリケーションだけがサポートされています。