CHAPTER 13

ポリシー グループ

スマート トンネル アクセスの設定

次の項では、クライアントレス SSL VPN セッションでスマート トンネル アクセスをイネーブルにする方法、それらのアクセスを提供するアプリケーションの指定、および使用上の注意について説明します。

スマート トンネル アクセスの設定

スマート トンネル アクセスを設定するには、スマート トンネル リストを作成します。このリストには、スマート トンネル アクセスに適した 1 つ以上のアプリケーション、およびこのリストに関連付けられたエンドポイント オペレーティング システムを含めます。各グループ ポリシーまたはローカル ユーザ ポリシーでは 1 つのスマート トンネル リストがサポートされているため、ブラウザベースではないアプリケーションをサポート対象とするために、グループ化してスマート トンネル リストに加える必要があります。リストを作成したら、1 つ以上のグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。

次の項では、スマート トンネルおよびその設定方法について説明します。

- 「スマート トンネルについて」
- 「スマート トンネルを使用する理由」
- 「スマート トンネルの設定（Lotus の例）」
- 「トンネリングするアプリケーションの設定の簡略化」
- 「スマート トンネル リストについて」
- 「スマート トンネル自動サインオン サーバ リストの作成」
- 「スマート トンネル自動サインオン サーバ リストへのサーバの追加」
- 「スマート トンネル アクセスのイネーブル化とオフへの切り替え」

スマート トンネルについて

スマート トンネルは、TCP ベースのアプリケーションとプライベート サイト間の接続です。このスマート トンネルは、セキュリティ アプライアンスをパスウェイとして、また、ASA をプロキシ サーバとして使用するクライアントレス（ブラウザベース）SSL VPN セッションを使用します。スマート トンネル アクセスを許可するアプリケーションを特定し、各アプリケーションのローカル パスを指定できます。Microsoft Windows で実行するアプリケーションの場合は、チェックサムの SHA-1 ハッシュの一致を、スマート トンネル アクセスを許可する条件として要求もできます。

Lotus SameTime および Microsoft Outlook は、スマート トンネル アクセスを許可するアプリケーションの例です。

スマート トンネルを設定するには、アプリケーションがクライアントであるか、Web 対応アプリケーションであるかに応じて、次の手順のいずれかを実行する必要があります。

- クライアント アプリケーションの 1 つ以上のスマート トンネル リストを作成し、スマート トンネル アクセスを必要とするグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。
- スマート トンネル アクセスに適格な Web 対応アプリケーションの URL を指定する 1 つ以上のブックマーク リスト エントリを作成し、スマート トンネル アクセスを必要とするグループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てます。

また、クライアントレス SSL VPN セッションを介したスマート トンネル接続でのログイン クレデンシャルの送信を自動化する Web 対応アプリケーションのリストも作成できます。

スマート トンネルを使用する理由

スマート トンネル アクセスでは、クライアントの TCP ベースのアプリケーションは、ブラウザベースの VPN 接続を使用してサービスにアクセスできます。この方法では、プラグインやレガシー テクノロジーであるポート転送と比較して、ユーザには次のような利点があります。

- スマート トンネルは、プラグインよりもパフォーマンスが向上します。
- ポート転送とは異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続を要求しないことにより、ユーザ エクスペリエンスが簡略化されます。
- ポート転送とは異なり、スマート トンネルでは、ユーザは管理者特権を持つ必要がありません。

プラグインの利点は、クライアント アプリケーションをリモート コンピュータにインストールする必要がないという点です。

前提条件

ASA Release 9.0 のスマート トンネルでサポートされているプラットフォームおよびブラウザについては、『*Supported VPN Platforms, Cisco ASA Series*』を参照してください。

次の要件と制限事項が Windows でのスマート トンネル アクセスには適用されます。

- Windows では ActiveX または Oracle Java ランタイム環境（JRE）4 Update 15 以降（JRE 6 以降を推奨）をブラウザでイネーブルにしておく必要がある。
- Winsock 2 の TCP ベースのアプリケーションだけ、スマート トンネル アクセスに適する。
- Mac OS X の場合に限り、Java Web Start をブラウザでイネーブルにしておく必要がある。

制約事項

- スマート トンネルは、Microsoft Windows を実行しているコンピュータとセキュリティ アプライアンス間に配置されたプロキシだけをサポートする。スマート トンネルは、Windows でシステム全体のパラメータを設定する Internet Explorer 設定を使用します。この設定がプロキシ情報を含む場合があります。
  - Windows コンピュータで、プロキシが ASA にアクセスする必要がある場合は、クライアントのブラウザにスタティック プロキシ エントリが必要であり、接続先のホストがクライアントのプロキシ例外のリストに含まれている必要があります。
  - Windows コンピュータで、プロキシが ASA にアクセスする必要がなく、プロキシがホスト アプリケーションにアクセスする必要がある場合は、ASA がクライアントのプロキシ例外のリストに含まれている必要があります。

  プロキシ システムはスタティック プロキシ エントリまたは自動設定のクライアントの設定、または PAC ファイルによって定義できます。現在、スマート トンネルでは、スタティック プロキシ設定だけがサポートされています。
- スマート トンネルでは、Kerberos Constrained Delegation（KCD）はサポートされない。
- Windows の場合、コマンド プロンプトから開始したアプリケーションにスマート トンネル アクセスを追加する場合は、スマート トンネル リストの 1 つのエントリの [Process Name] に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要があります。これは「cmd.exe」がアプリケーションの親であるためです。
- HTTP ベースのリモート アクセスによって、いくつかのサブネットが VPN ゲートウェイへのユーザ アクセスをブロックすることがある。これを修正するには、Web とエンドユーザの場所との間のトラフィックをルーティングするために ASA の前にプロキシを配置します。このプロキシが CONNECT 方式をサポートしている必要があります。認証が必要なプロキシの場合、スマート トンネルは、基本ダイジェスト認証タイプだけをサポートします。
- スマート トンネルが開始されると、ASA は、ブラウザ プロセスが同じである場合に VPN セッション経由ですべてのブラウザ トラフィックをデフォルトで送信する。また、tunnel-all ポリシーが適用されている場合にのみ、ASA は同じ処理を行います。ユーザがブラウザ プロセスの別のインスタンスを開始すると、VPN セッション経由ですべてのトラフィックが送信されます。ブラウザ プロセスが同じで、セキュリティ アプライアンスが URL へのアクセスを提供しない場合、ユーザはその URL を開くことはできません。回避策として、tunnel-all ではないトンネル ポリシーを割り当てます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されない。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。
- スマート トンネルの Mac バージョンは、POST ブックマーク、フォームベースの自動サインオン、または POST マクロ置換をサポートしない。
- Mac OS ユーザの場合、ポータル ページから起動されたアプリケーションだけがスマート トンネル セッションを確立できる。この要件には、Firefox に対するスマート トンネルのサポートも含まれます。スマート トンネルを最初に使用する際に、Firefox を使用して Firefox の別のインスタンスを起動するには、csco_st という名前のユーザ プロファイルが必要です。このユーザ プロファイルが存在しない場合、セッションでは、作成するようにユーザに要求します。
- Mac OS X では、SSL ライブラリにダイナミックにリンクされた、TCP を使用するアプリケーションをスマート トンネルで使用できる。

- Mac OS X では、スマート トンネルは次をサポートしない。
  - プロキシ サービス
  - 自動サインオン
  - 2 つのレベルの名前スペースを使用するアプリケーション
  - Telnet、SSH、cURL などのコンソールベースのアプリケーション
  - dlopen または dlsym を使用して libsocket コールを見つけ出すアプリケーション
  - libsocket コールを見つけ出すスタティックにリンクされたアプリケーション
- Mac OS X では、プロセスへのフル パスが必要である。また、このパスは大文字と小文字が区別されます。各ユーザ名のパスを指定しないようにするには、部分パスの前にチルダ（~）を入力します（例：~/bin/vnc）。

スマート トンネルの設定（Lotus の例）

（注） この例では、アプリケーションでのスマート トンネル サポートを追加するために必要な最小限の指示だけを示します。詳細については、以降の各項にあるフィールドの説明を参照してください。

手順の詳細

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] を選択します。

ステップ 2　アプリケーションを追加するスマート トンネル リストをダブルクリックするか、または [Add] をクリックしてアプリケーションのリストを作成し、[List Name] フィールドにそのリストの名前を入力して [Add] をクリックします。

たとえば、[Smart Tunnels] ペインで [Add] をクリックし、[List Name] フィールドに **Lotus** と入力して [Add] をクリックします。

ステップ 3　[Add or Edit Smart Tunnel List] ダイアログボックスで [Add] をクリックします。

ステップ 4　[Application ID] フィールドに、スマート トンネル リスト内のエントリに対する一意のインデックスとして使用する文字列を入力しします。

ステップ 5　[Process Name] ダイアログボックスに、ファイル名とアプリケーションの拡張子を入力します。

表 13-1 に、[Application ID] 文字列の例と、Lotus をサポートするために必要となる関連付けられたパスを示します。

表 13-1　スマート トンネルの例 : Lotus 6.0 Thick Client with Domino Server 6.5.5

アプリケーション ID の例	必要最小限のプロセス名
lotusnotes	notes.exe
lotusnlnotes	nlnotes.exe
lotusntaskldr	ntaskldr.exe
lotusnfileret	nfileret.exe

ステップ 6　[OS] の横の [Windows] を選択します。

ステップ 7　[OK] をクリックします。

ステップ 8　リストに追加するアプリケーションごとに、ステップ 3 ～ 7 を繰り返します。

ステップ 9　[Add or Edit Smart Tunnel List] ダイアログボックスで [OK] をクリックします。

ステップ 10　次のようにして、関連付けられたアプリケーションへのスマート トンネル アクセスを許可するグループ ポリシーとローカル ユーザ ポリシーにリストを割り当てます。

- グループ ポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add] または [Edit] > [Portal] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。
- ローカル ユーザ ポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] または [Edit] > [VPN Policy] > [Clientless SSL VPN] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。

トンネリングするアプリケーションの設定の簡略化

スマート トンネル アプリケーション リストは、基本的に、トンネルへのアクセスを許可するアプリケーションのフィルタです。デフォルトでは、ブラウザによって開始されるすべてのプロセスに対してアクセスが許可されます。スマート トンネル対応ブックマークによって、クライアントレス セッションでは Web ブラウザによって開始されるプロセスのみにアクセスが許可されます。ブラウザ以外のアプリケーションでは、管理者はすべてのアプリケーションをトンネリングすることを選択して、エンド ユーザがどのアプリケーションを起動するかを知る必要性をなくすことができます。表 13-2 にアクセスを許可されるプロセスの状況を示します。

表 13-2　スマート トンネル アプリケーションのアクセスと対応ブックマーク

状況	スマート トンネル対応ブックマーク	スマート トンネル アプリケーション アクセス
アプリケーション リストが指定される	アプリケーション リストのプロセス名と一致する任意のプロセスにアクセス権が付与されます。	アプリケーション リストのプロセス名と一致するプロセスのみにアクセス権が付与されます。
スマート トンネルをオフに切り替える	すべてのプロセス（およびその子プロセス）にアクセス権が付与されます。	プロセスにアクセス権は付与されません。
[Smart Tunnel all Applications] チェックボックスをオンにします。	すべてのプロセス（およびその子プロセス）にアクセス権が付与されます。 (注)　スマート トンネル以外の Web ページによって開始されたプロセスも含まれます（Web ページが同じブラウザ プロセスによって処理される場合）。	ブラウザを開始したユーザが所有するすべてのプロセスにアクセス権が付与されますが、その子プロセスには付与されません。

制約事項

この設定は、Windows プラットフォームのみに適用されます。

手順の詳細

ステップ 1　[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択します。

ステップ 2　[User Account] ウィンドウで、編集するユーザ名を強調表示します。

ステップ 3　[Edit] をクリックします。[Edit User Account] ウィンドウが表示されます。

ステップ 4　[Edit User Account] ウィンドウの左側のサイドバーで、[VPN Policy] > [Clientless SSL VPN] をクリックします。

ステップ 5　次のいずれかの操作を行います。

- [smart tunnel_all_applications] チェックボックスをオンにします。リストを作成しなくても、または外部アプリケーションについてエンド ユーザが起動する可能性がある実行ファイルを知らなくても、すべてのアプリケーションがトンネリングされます。
- または、次のトンネル ポリシー オプションから選択します。
  - [Smart Tunnel Policy] パラメータの [Inherit] チェックボックスをオフにします。
  - ネットワーク リストから選択し、トンネル オプションの 1 つを指定します。指定されたネットワークに対してスマート トンネルを使用する、指定されたネットワークに対してスマート トンネルを使用しない、またはすべてのネットワーク トラフィックに対してトンネルを使用する、のいずれかです。

スマート トンネル アクセスに適格なアプリケーションの追加

各 ASA のクライアントレス SSL VPN コンフィギュレーションは、*スマート トンネル リスト*をサポートしています。各リストは、スマート トンネル アクセスに適格な 1 つ以上のアプリケーションを示します。各グループ ポリシーまたはユーザ名は 1 つのスマート トンネル リストのみをサポートするため、サポートされる各アプリケーションのセットをスマート トンネル リストにグループ化する必要があります。

[Add or Edit Smart Tunnel Entry] ダイアログボックスでは、スマート トンネル リストにあるアプリケーションの属性を指定できます。

ステップ 1　[Configuration] > [Remote Access VPN] >[Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に進み、編集するスマート トンネル アプリケーション リストを選択するか、新しいリストを追加します。

ステップ 2　新しいリストの場合は、アプリケーションまたはプログラムのリストに付ける一意の名前を入力します。スペースは使用しないでください。

スマート トンネル リストのコンフィギュレーションに続いて、クライアントレス SSL VPN のグループ ポリシーとローカル ユーザ ポリシーの [Smart Tunnel List] 属性の横にリスト名が表示されます。他に設定する可能性があるリストと、内容および目的を区別できるような名前を付けてください。

ステップ 3　[Add] をクリックして、このスマート トンネル リストに必要な数のアプリケーションを追加します。パラメータについては次で説明します。

- [Application ID]：スマート トンネル リストのエントリに命名する文字列を入力します。このユーザ指定の名前は保存され、GUI に戻されます。文字列はオペレーティング システムに対して一意です。通常は、スマート トンネル アクセスを許可されるアプリケーションに付けられる名前です。異なるパスまたはハッシュ値を指定するアプリケーションの複数バージョンをサポートするには、この属性を使用してエントリを差別化し、オペレーティング システム、および各リスト エントリによってサポートされているアプリケーションの名前とバージョンの両方を指定します。文字列は最大 64 文字まで使用できます。
- [Process Name]：アプリケーションのファイル名またはパスを入力します。ストリングには最大 128 文字を使用できます。

  Windows では、アプリケーションにスマート トンネル アクセスを許可する場合に、この値とリモート ホストのアプリケーション パスの右側の値が完全に一致している必要があります。Windows でファイル名のみを指定すると、SSL VPN では、アプリケーションにスマート トンネル アクセスを許可する場合に、リモート ホストに対して場所の制限を強制しません。

  アプリケーションのパスを指定し、ユーザが別の場所にインストールした場合は、そのアプリケーションは許可されません。アプリケーションは、入力する値と文字列と右側の値が一致している限り、任意のパスに配置できます。

  アプリケーションがリモート ホストの複数のパスのいずれかにある場合に、アプリケーションにスマート トンネル アクセスを認可するには、このフィールドにアプリケーションの名前と拡張子だけを指定するか、またはパスごとに固有のスマート トンネル エントリを作成します。

（注） スマート トンネル アクセスで突然問題が発生する場合、[Process Name] 値がアップグレードされたアプリケーションに対して最新ではない可能性があります。たとえば、アプリケーションへのデフォルト パスは、そのアプリケーションおよび次のアップグレード版を製造する企業が買収されると変更されることがあります。

  Windows の場合、コマンド プロンプトから開始したアプリケーションにスマート トンネル アクセスを追加する場合は、スマート トンネル リストの 1 つのエントリの [Process Name] に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要があります。これは「cmd.exe」がアプリケーションの親であるためです。

- [OS]：[Windows] または [Mac] をクリックし、アプリケーションのホスト オペレーティング システムを指定します。
- [Hash]（任意、Windows にのみ該当）：この値を取得するには、アプリケーションのチェックサム（つまり、実行ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュを計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft ファイル チェックサム整合性検証（FCIV）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。FCIV のインストール後、スペースを含まないパス（c:/fciv.exe など）に、ハッシュするアプリケーションの一時コピーを置き、コマンドラインで **fciv.exe -sha1** *application* と入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。

  SHA-1 ハッシュは、常に 16 進数 40 文字です。

  クライアントレス SSL VPN は、アプリケーションにスマート トンネル アクセスの認可を与える前に、[Application ID] に一致するアプリケーションのハッシュを計算します。結果が [Hash] の値と一致すれば、アプリケーションにスマート トンネル アクセスの資格を与えます。

ハッシュを入力することにより、[Application ID] で指定した文字列に一致する不正ファイルに対して SSL VPN が資格を与えないようしています。チェックサムは、アプリケーションのバージョンまたはパッチによって異なるため、入力する [Hash] 値は、リモート ホストの 1 つのバージョンやパッチにしか一致しない可能性があります。複数のバージョンのアプリケーションにハッシュを指定するには、[Hash] 値ごとに固有のスマート トンネル エントリを作成します。

(注)　[Hash] 値を入力し、スマート トンネル アクセスで、アプリケーションの今後のバージョンまたはパッチをサポートする必要がある場合は、スマート トンネル リストを更新し続ける必要があります。スマート トンネル アクセスに突然問題が発生した場合は、[Hash] 値を含むアプリケーション リストが、アプリケーションのアップグレードによって最新の状態になっていない可能性があります。この問題は hash を入力しないことによって回避できます。

ステップ 4　[OK] をクリックしてアプリケーションを保存し、このスマート トンネル リストに必要な数だけアプリケーションを作成します。

ステップ 5　スマート トンネル リストの作成が終わったら、そのリストをアクティブにするには、次の手順に従って、グループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てる必要があります。

- グループ ポリシーにリストを割り当てるには、[Config] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add] または [Edit] > [Portal] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。
- ローカル ユーザ ポリシーにリストを割り当てるには、[Config] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] または [Edit] > [VPN Policy] > [Clientless SSL VPN] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストからスマート トンネル名を選択します。

表 13-3　スマート トンネル エントリの例

スマート トンネルのサポート	アプリケーション ID（一意の文字列であればどれでも OK）	プロセス名	OS
Mozilla Firefox	firefox	firefox.exe	Windows
Microsoft Outlook Express	outlook-express	msimn.exe	Windows
より制限的なオプション：実行ファイルが事前定義済みのパスにある場合は、Microsoft Outlook Express 専用。	outlook-express	\Program Files\Outlook Express\msimn.exe	Windows
Mac で新しいターミナル ウィンドウを開く（ワンタイムパスワードが実装されているので、それ以降、同じターミナル ウィンドウでのアプリケーションの起動は失敗します）。	terminal	Terminal	Mac
新しいウィンドウでスマート トンネルを開始	new-terminal	Terminal open -a MacTelnet	Mac
Mac ターミナル ウィンドウでアプリケーションを起動	curl	Terminal curl www.example.com	Mac

スマート トンネル リストについて

グループ ポリシーとユーザ名ごとに、次のいずれかを行うようにクライアントレス SSL VPN を設定できます。

- ユーザのログイン時に自動的にスマート トンネル アクセスを開始する。
- ユーザのログイン時にスマート トンネル アクセスをイネーブルにするが、ユーザはクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、スマート トンネル アクセスを手動で開始するようにユーザに要求する。

制約事項

スマート トンネル ログオン オプションは、各グループ ポリシーとユーザ名に対して互いに排他的です。1 つだけ使用してください。

スマート トンネル自動サインオン サーバ リストの作成

[Add Smart Tunnel Auto Sign-on Server List] ダイアログボックスで、スマート トンネルのセットアップ中にログイン クレデンシャルの送信を自動化するサーバのリストを追加または編集できます。スマート トンネルの自動サインオンは、Internet Explorer および Firefox で利用可能です。

ステップ 1　[Configuration] > [Remote Access VPN] >[Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に進み、[Smart Tunnel Auto Sign-on Server List] が展開されて表示されていることを確認します。

ステップ 2　[Add] をクリックして、他に設定する可能性があるリストと、内容および目的を区別できるようなリモート サーバのリストの一意の名前を入力します。文字列は最大 64 文字まで使用できます。スペースは使用しないでください。

スマート トンネルの自動サインオン リストを作成した後は、クライアントレス SSL VPN グループ ポリシーおよびローカル ポリシー コンフィギュレーションの下の [Auto Sign-on Server List] 属性の横に、リスト名が表示されます。

スマート トンネル自動サインオン サーバ リストへのサーバの追加

次の手順では、スマート トンネル接続での自動サインオンを提供するサーバのリストにサーバを追加し、そのリストをグループ ポリシーまたはローカル ユーザに割り当てる方法について説明します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に進み、リストのいずれかを選択して、[Edit] をクリックします。

ステップ 2　[Tunnel Auto Sign-On Server List] ダイアログで [Add] ボタンをクリックして、スマート トンネル サーバをもう 1 つ追加します。

ステップ 3　自動認証を行うサーバのホスト名または IP アドレスを入力します。

- [Hostname] を選択する場合、自動認証を行うホスト名またはワイルドカード マスクを入力します。次のワイルドカード文字を使用できます。
  - *：任意の数の文字を一致させる、またはどの文字も一致させない。
  - ?：単一の文字を一致させる。

- [ ] : かっこ内に指定された範囲内の、任意の 1 文字を一致させる。
- たとえば、*.example.com と入力します。このオプションを使用すると、IP アドレスのダイナミックな変更からコンフィギュレーションを保護します。

- [IP Address] を選択する場合、IP アドレスを入力します。

（注） Firefox では、ワイルドカードを使用したホスト マスク、IP アドレスを使用したサブネット、またはネットマスクをサポートしていません。正確なホスト名または IP アドレスを使用する必要があります。たとえば、Firefox では、*.cisco.com を入力した場合、email.cisco.com をホストする自動サインオンは失敗します。

ステップ 4　[Windows Domain]（オプション）: 認証で必要な場合、クリックして Windows ドメインをユーザ名に追加します。このオプションを使用する場合は、1 つ以上のグループ ポリシーまたはローカル ユーザ ポリシーにスマート トンネル リストを割り当てる際に、ドメイン名を指定する必要があります。

ステップ 5　[HTTP-based Auto Sign-On]（オプション）

- [Authentication Realm] : レルムは Web サイトの保護領域に関連付けられ、認証時に認証プロンプトまたは HTTP ヘッダーのいずれかでブラウザに再度渡されます。ここで自動サインオンが設定され、レルムの文字列が指定されたら、ユーザはレルムの文字列を Web アプリケーション（Outlook Web Access など）で設定し、Web アプリケーションにサインオンすることなくアクセスできます。

  イントラネットの Web ページのソース コードで使用されるアドレス形式を使用します。ブラウザ アクセス用にスマート トンネル自動サインオンを設定しており、一部の Web ページでホスト名が使用され、他の Web ページで IP アドレスが使用されている場合、あるいはどちらが使用されているかわからない場合は、両方を異なるスマート トンネル自動サインオン エントリで指定します。それ以外の場合、Web ページのリンクで、指定されたフォーマットとは異なるフォーマットが使用されると、ユーザがリンクをクリックしても開きません。

（注） 対応するレルムがわからない場合、管理者はログインを一度実行し、プロンプト ダイアログから文字列を取得する必要があります。

- [Port Number] : 対応するホストのポート番号を指定します。Firefox では、ポート番号が指定されていない場合、自動サインオンはデフォルトのポート番号 80 および 443 でそれぞれアクセスされた HTTP および HTTPS に対して実行されます。

ステップ 6　[OK] をクリックします。

ステップ 7　スマート トンネル自動サインオン サーバ リストのコンフィギュレーションに続いて、そのリストをアクティブにするには、グループ ポリシーまたはローカル ユーザ ポリシーにそのリストを割り当てる必要があります。

- グループ ポリシーにリストを割り当てるには、次の手順を実行します。
  1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] の順に進み、グループ ポリシーを開きます。
  2. [Portal] タブを選択し、[Smart Tunnel] 領域を見つけ、[Auto Sign-on Server List] 属性の横にあるドロップダウン リストから自動サインオン サーバ リストを選択します。

- ローカル ユーザ ポリシーにリストを割り当てるには、次の手順を実行します。
  1. [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択し、自動サインオン サーバ リストに割り当てるローカル ユーザを編集します。
  2. [VPN Policy] > [Clientless SSL VPN] 順に進み、[Smart Tunnel] 領域の下の [Auto Sign-on Server] 設定を探します。
  3. [Inherit] をオフにし、[Auto Sign-on Server List] 属性の横にあるドロップダウン リストからサーバ リストを選択します。

スマート トンネル アクセスのイネーブル化とオフへの切り替え

デフォルトでは、スマート トンネルはオフになっています。

スマート トンネル アクセスをイネーブルにしている場合、ユーザは、クライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、スマート トンネル アクセスを手動で開始する必要があります。

スマート トンネルからのログオフの設定

ここでは、スマート トンネルからの適切なログオフ方法について説明します。すべてのブラウザ ウィンドウを閉じるか、通知アイコンを右クリックしてログアウトを確認すると、スマート トンネルからログオフできます。

（注） ポータルにあるログアウト ボタンを使用することを強くお勧めします。この方法は、クライアントレス SSL VPN 用であり、スマート トンネルが使用されているかどうかに関係なくログオフが行われます。通知アイコンは、ブラウザを使用しないスタンドアロン アプリケーションを使用する場合に限り使用する必要があります。

ペアレント プロセスの終了

この方法では、ログオフを示すためにすべてのブラウザを閉じることが必要です。スマート トンネルのライフタイムは現在、プロセスのライフタイムの開始に結び付けられています。たとえば、Internet Explorer からスマート トンネルと開始した場合、iexplore.exe が実行されていないとスマート トンネルがオフになります。スマート トンネルは、ユーザがログアウトせずにすべてのブラウザを閉じた場合でも、VPN セッションが終了したと判断します。

（注） 場合によっては、ブラウザ プロセスがエラーの結果として、意図的にではなく残っていることがあります。また、Secure Desktop を使用しているときに、ユーザが Secure Desktop 内ですべてのブラウザを閉じてもブラウザ プロセスが別のデスクトップで実行されている場合があります。したがって、スマート トンネルは、現在のデスクトップで表示されているウィンドウがない場合にすべてのブラウザ インスタンスが終了したと見なします。

通知アイコンの利用

ブラウザを閉じてもセッションが失われないようにするために、ペアレント プロセスの終了時にログオフをオフに切り替えることもできます。この方法では、システム トレイの通知アイコンを使用してログアウトします。アイコンは、ユーザがアイコンをクリックしてログアウトするまで維持されます。ユーザがログアウトする前にセッションの期限が切れた場合、アイコンは、次回に接続を試行するまで維持されます。セッション ステータスがシステム トレイで更新されるまで時間がかかることがあります。

(注)　このアイコンが、SSL VPN からログアウトする別の方法です。これは、VPN セッション ステータスのインジケータではありません。

手順の詳細

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] を選択します。

ステップ 2　[Click on smart-tunnel logoff icon in the system tray] オプション ボタンをイネーブルにします。

ステップ 3　ウィンドウの [Smart Tunnel Networks] 部分で、[Add] をオンにして、アイコンを含めるネットワークの IP アドレスとホスト名の両方を入力します。

(注)　アイコンを右クリックすると、SSL VPN からのログアウトをユーザに求める単一のメニュー項目が表示されます。

プロキシ バイパスの使用

ユーザはプロキシ バイパスを使用するように ASA を設定できます。これは、プロキシ バイパスが提供する特別なコンテンツ リライト機能を使用した方が、アプリケーションや Web リソースをより有効活用できる場合に設定します。プロキシ バイパスはコンテンツのリライトに代わる手法であり、元のコンテンツの変更を最小限に抑えます。多くの場合、カスタム Web アプリケーションでこれを使用すると有効です。

プロキシ バイパスには複数のエントリを設定できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートにより、プロキシ バイパス ルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシ バイパスを設定する場合、ネットワーク コンフィギュレーションによっては、これらのポートが ASA にアクセスできるようにするために、ファイアウォール コンフィギュレーションの変更が必要になることがあります。この制限を回避するには、パス マスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスは、URL で .com や .org、またはその他のタイプのドメイン名の後に続く全体です。たとえば、www.example.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.example.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、*（ワイルドカード）を /hr* のように使用して、コマンドを複数回使用しないようにできます。

ASA がコンテンツ リライトをほとんどまたはまったく実行しない場合のルールを設定できます。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Proxy Bypass] の順に進みます。

ステップ 2　プロキシ バイパスのインターフェイス名を選択します。

ステップ 3　プロキシ バイパス用のポートまたは URI を指定します。

- [Port]：（オプション ボタン）プロキシ バイパスにポートを使用します。有効なポート番号は 20000 ～ 21000 です。
- [Port]：（フィールド）ASA がプロキシ バイパス用に予約する大きな番号のポートを入力します。
- [Path Mask]：（オプション ボタン）プロキシ バイパスに URL を使用します。
- [Path Mask]：（フィールド）プロキシ バイパス用の URL を入力します。この URL には、正規表現を使用できます。

ステップ 4　プロキシ バイパスのターゲット URL を定義します。

- [URL]：（ドロップダウン リスト）プロトコルとして、http または https をクリックします。
- [URL]（テキスト フィールド）：プロキシ バイパスを適用する URL を入力します。

ステップ 5　リライトするコンテンツを指定します。選択肢は、なし、または XML、リンク、およびクッキーの組み合わせです。

- [XML]：XML コンテンツをリライトする場合に選択します。
- [Hostname]：リンクをリライトする場合に選択します。

ポータル アクセス ルールの設定

この拡張機能により、カスタマーは、HTTP ヘッダー内に存在するデータに基づいて、クライアントレス SSL VPN セッションを許可または拒否するグローバルなクライアントレス SSL VPN アクセス ポリシーを設定することができます。ASA がクライアントレス SSL VPN セッションを拒否する場合、ただちにエンドポイントにエラー コードを返します。

ASA は、このアクセス ポリシーを、エンドポイントが ASA に対して認証する前に評価します。その結果、拒否の場合は、エンドポイントからの追加の接続試行による ASA の処理リソースの消費はより少なくなります。

前提条件

ASA にログインし、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードでは、ASA は次のプロンプトを表示します。

```
hostname(config)#
```

手順の詳細

ステップ 1　ASDM を起動し、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Portal Access Rule] を選択します。

[Portal Access Rule] ウィンドウが開きます。

ステップ 2　[Add] をクリックしてポータル アクセス ルールを作成するか、既存のルールを選択して [Edit] をクリックします。

[Add Portal Access Rule] または [Edit Portal Access Rule] ダイアログボックスが開きます。

ステップ 3　1 ～ 65535 のルール番号を [Rule Priority] フィールドに入力します。

ルールは 1 ～ 65535 のプライオリティの順序で処理されます。

ステップ 4　[User Agent] フィールドに、HTTP ヘッダーで検索するユーザ エージェントの名前を入力します。

- 文字列を広範囲に指定するには、文字列をワイルドカード（*）で囲みます。たとえば、*Thunderbird* です。検索文字列でワイルドカードを使用することを推奨します。ワイルドカードを使用しないと、ルールがどの文字列とも一致しないか、予期したよりも大幅に少ない文字列としか一致しない場合があります。
- 文字列にスペースが含まれている場合、ASDM によって、ルールの保存時に文字列の最初と最後に自動的に引用符が追加されます。たとえば、`my agent` と入力した場合、ASDM によってこの文字列は `"my agent"` として保存されます。ASA では `my agent` の一致が検索されます。

  スペースを含む文字列に引用符を追加しないでください。ただし、文字列に追加した引用符を ASA で照合させる場合を除きます。たとえば、`"my agent"` と入力すると、ASDM はその文字列を `"\"my agent\'"` として保存するため、`"my agent"` を検出しようとしますが、`my agent` は見つかりません。
- スペースを含む文字列でワイルドカードを使用する場合は、文字列全体をワイルドカードで開始して終了します。たとえば、`*my agent*` です。ASDM によって、ルールの保存時に、その文字列は自動的に引用符で囲まれます。

ステップ 5　[Action] フィールドで、[Deny] または [Permit] を選択します。

ASA は、この設定に基づいて、クライアントレス SSL VPN 接続を拒否または許可します。

ステップ 6　HTTP メッセージ コードを [Returned HTTP Code] フィールドに入力します。

HTTP メッセージ番号 403 がフィールドにあらかじめ入力されており、これがポータル アクセス ルールのデフォルト値です。メッセージ コードの有効な範囲は 200 ～ 599 です。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。