ASA：ASDM を使用したスマート トンネルの設定例

内容

概要

スマート トンネルとは、TCP ベースのアプリケーションとプライベート サイトとの間の接続のことです。経路としてセキュリティ アプライアンスを使用したクライアントレス (ブラウザ ベース) の SSL VPN セッションを、プロキシ サーバとしてセキュリティ アプライアンスを使用します。スマート トンネル アクセスを付与するアプリケーションを指定し、各アプリケーションへのローカル経路を指定することができます。Microsoft Windows で実行されるアプリケーションでは、スマート トンネル アクセスを付与する条件として、チェックサムの SHA-1 ハッシュを一致させるように要求することもできます。

Lotus SameTime や *Microsoft Outlook Express* は、スマート トンネル アクセスを付与する可能性があるアプリケーションの例です。

アプリケーションがクライアントであるかどうか、または Web 対応アプリケーションであるかどうかによって、スマート トンネル設定では、次の手順のいずれか 1 つが必要です。

- クライアント アプリケーションの場合、1 つまたは複数のスマート トンネル リストを作成し、そのリストを、スマート トンネル アクセスを提供するグループ ポリシーまたはローカル ユーザ ポリシーに割り当てます。

- スマート トンネル アクセスが可能な Web 対応アプリケーションの場合、その URL を指定する 1 つまたは複数のブックマーク リスト エントリを作成し、そのリストを、スマート トンネル アクセスを提供する DAP、グループ ポリシー、またはローカル ユーザ ポリシーに割り当てます。クライアントレス SSL VPN セッションを介して、スマート トンネル接続でログイン クレデンシャルの発行が自動化される、Web 対応アプリケーションをリストに載せることもできます。

このドキュメントは、スマート トンネル機能が既存の構成で設定できるよう、Cisco AnyConnect SSL VPN Client の設定がすでに行われており、適切に動作することが前提となっています。Cisco AnyConnect SSL VPN Client の設定の詳細については、『ASA 8.x：ASA で AnyConnect VPN Client のスプリット トンネリングを許可する場合の設定例』）を参照してください。

注： ASA 8.xの「ASDM 6.0(2)を使用したASAの設定」セクションで説明されている手順4.bから4.lを確認してください。*ASA で AnyConnect VPN Client のスプリット トンネリングを許可するための設定例*』の「ASDM 6.0(2) を使用した ASA 設定」セクションで説明されている手順 *4.b から 4.l を実行しないようにしてください。*

このドキュメントでは、Cisco ASA 5500 シリーズの適応型セキュリティ アプライアンスにスマート トンネルを設定する方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 8.0(2) を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Microsoft Installer バージョン 3.1 によって Microsoft Vista、Windows XP SP2、または Windows 2000 Professional SP4 が動作している PC
- Cisco Adaptive Security Device Manager（ASDM）バージョン 6.0(2)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

スマート トンネル アクセスの設定

スマート トンネル テーブルには、スマート トンネル リストが表示されます。各リストでは、スマート トンネル アクセスと、それに関連するオペレーティング システム（OS）で使用可能な 1 つまたは複数のアプリケーションが指定されています。 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、スマート トンネル リストでサポートされるよう、非ブラウザ ベースのアプリケーションをグループ化する必要があります。リストの設定に続いて、それを 1 つまたは複数のグループ ポリシーまたはローカル ユーザ ポリシーに割り当てることができます。

スマート トンネルのウィンドウ（[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] [Smart Tunnels]）を使用すると、次の手順を完了できます。

- **スマート トンネル リストの追加とリストへのアプリケーションの追加**スマート トンネル リストを追加し、アプリケーションをリストに追加するには、次の手順を実行します。[Add] をクリックします。[Add Smart Tunnel List] ダイアログボックスが表示されます。リストの名前を入力し、[**Add**] をクリックします。ASDM によって、[Add Smart Tunnel Entry] ダイアログボックスが開かれ、これによって、スマート トンネルの属性をリストに割り当てることができます。スマート トンネルに必要な属性を割り当てた後で、[OK] をクリックします。ASDM によって、リストにある属性が表示されます。リスト全体の作業を完了するには、必要に応じてこれらの手順を繰り返し、[Add Smart Tunnel List] ダイアログボックスで [OK] をクリックします。
- **スマート トンネル リストの変更**スマート トンネル リストを変更するには、次の手順を実行します。リストをダブルクリックするか、またはテーブルにあるリストを選択し、[Edit] をクリックします。[Add] をクリックし、スマート トンネル属性の新しいセットをリストに挿入するか、または、リストにあるエントリを選択し、[Edit] または [Delete] をクリックします。
- **リストの削除**リストを削除するには、テーブルにあるリストを選択し、[Delete] をクリックします。
- **ブックマークの追加**設定およびスマート トンネル リストの割り当てに続いて、サービスのブックマークを追加し、[Add Bookmark] ダイアログボックスまたは [Edit Bookmark] ダイアログボックスで [Enable Smart Tunnel] **オプションをクリックして、スマート トンネルを使いやすいように設定できます。**

スマート トンネル アクセスを使用すると、クライアント TCP ベースのアプリケーションで、ブラウザ ベースの VPN 接続を使用して、サービスを接続できます。プラグインおよび従来のテクノロジーのポート転送と比較して、ユーザに対して次の利点が提供されます。

- スマート トンネルでは、プラグインよりも優れたパフォーマンスが提供されます。
- ポート転送と異なり、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が不要のため、ユーザの使用感を簡素化できます。
- ポート転送と異なり、スマート トンネルでは、ユーザに管理権限が不要です。

スマート トンネルの要件、制約事項、および制限事項

一般的な要件と制限事項

スマート トンネルには、次のような一般的な要件および制限事項があります。

- スマート トンネル接続を開始するリモート ホストでは、32 ビット版の Microsoft Windows Vista、Windows XP、または Windows 2000、あるいは Mac OS 10.4 または 10.5 を実行している必要があります。

- スマート トンネルの自動サインオンは、Windows の Microsoft Internet Explorer のみでサポートされます。
- ブラウザは、Java と Microsoft ActiveX の一方または両方でイネーブルである必要があります。
- スマート トンネルでは、Microsoft Windows およびセキュリティ アプライアンスが実行されているコンピュータ間にあるプロキシのみがサポートされます。スマート トンネルでは、Internet Explorer の設定が使用されます（つまり、Windows のシステム全体での使用が意図されています）。 リモート コンピュータで、セキュリティ アプライアンスへの到達が必要な場合、接続の終端の URL は、プロキシ サービスから除外されている URL のリストにある必要があります。プロキシ設定により、ASA に定義されているトラフィックがプロキシを介して通信されるよう指定されている場合、すべてのスモール チャネル トラフィックはプロキシを介して通信されます。HTTP ベースのリモート アクセス シナリオでは、サブネットによって、VPN ゲートウェイへのユーザ アクセスが提供されない場合があります。この場合、Web とエンド ユーザとの間のトラフィックを通信するために ASA の正面に置かれるプロキシによって、Web アクセスが提供されます。ただし、VPN ユーザのみが、ASA の正面に置かれるプロキシを設定できます。これを行う場合、これらのプロキシによって、接続方式がサポートされることを確認してください。認証が必要なプロキシでは、スマート トンネルによって、基本ダイジェスト認証タイプのみがサポートされます。
- スマート トンネルの起動時に、セキュリティ アプライアンスによって、クライアントレス セッションの開始にユーザが使用したブラウザ プロセスから、すべてのトラフィックがトンネル内を通過されます。ユーザがブラウザ プロセスの別のインスタンスを起動すると、すべてのトラフィックがトンネルに渡されます。ブラウザ プロセスが同じで、セキュリティ アプライアンスによって指定された URL へのアクセスが提供されない場合、ユーザはその URL を開くことができません。回避策として、ユーザは、クライアントレス セッションの確立に使用されたブラウザと異なるブラウザを使用できます。
- ステートフル フェールオーバーでは、スマート トンネル接続は残されません。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。

Windows の要件と制限事項

次の要件と制限事項は、Windows のみに適用されます。

- Winsock 2 のみで、TCP ベースのアプリケーションから、スマート トンネル アクセスを行うことができます。
- セキュリティ アプライアンスでは、Microsoft Outlook Exchange（MAPI）プロキシはサポートされません。ポート転送でもスマート トンネルでも、MAPI はサポートされません。MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモート ユーザは AnyConnect を使用する必要があります。
- スマート トンネルまたはポート転送を使用する Microsoft Windows Vista のユーザは、ASA の URL を信頼済みサイト ゾーンに追加する必要があります。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を開始し、[Tools] > [Internet Options] を選択し、[Security] タブをクリックします。Vista ユーザは、スマート トンネル アクセスを活用するために、保護モードをディセーブルにすることもできます。ただし、攻撃に対する脆弱性が大きくなるため、シスコではこの方法を採用しないことを推奨します。

Mac OS の要件と制限事項

次の要件と制限事項は、Mac OS のみに適用されます。

- Safari 3.1.1 またはそれ以降か Firefox 3.0 またはそれ以降
- Sun JRE 1.5 またはそれ以降
- ポータル ページから開始されたアプリケーションのみがスマート トンネル接続を確立できます。この要件には、Firefox のスマート トンネル サポートが含まれます。スマート トンネルを最初に使用しているときに Firefox の別のインスタンスを開始するために Firefox を使用する場合、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 プロファイルがない場合、セッションからユーザに対し、プロファイルを作成する旨のプロンプトが表示されます。
- SSL ライブラリに動的にリンクされている TCP を使用するアプリケーションは、スマート トンネル経由で動作できます。
- Mac OS 上では、次の機能およびアプリケーションは、スマート トンネルではサポートされません。プロキシ サービス自動サインオン2 レベルのネーム スペースが使用されるアプリケーションTelnet、SSH、および cURL などのコンソール ベースのアプリケーションlibsocket コールを探す dlopen または dlsym を使用したアプリケーションlibsocket コールを探すために静的にリンクされているアプリケーション

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

スマート トンネル リストの追加または編集

[Add Smart Tunnel List] ダイアログボックスを使用すると、セキュリティ アプライアンス設定にスマート トンネル エントリのリストを追加できます。[Edit Smart Tunnel List] ダイアログボックスを使用すると、リストの内容を変更できます。

フィールド

[List Name]：アプリケーションまたはプログラムのリストでの固有名を入力します。名前の文字数には制限はありません。スペースは使用しないでください。スマート トンネル リストの設定に続いて、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 ユーザ ポリシーの [Smart Tunnel List] 属性の隣に、リスト名が表示されます。設定する予定の他のリストから、内容や目的を区別することができる名前を割り当てます。

スマート トンネル エントリの追加または編集

[Add Smart Tunnel Entry] ダイアログボックスまたは [Edit Smart Tunnel Entry] ダイアログボックスを使用すると、スマート トンネル リストにアプリケーションの属性を指定できます。

- **[Application ID]：スマート トンネル リストのエントリに名前を付ける文字列を入力します。**文字列は OS で固有です。通常は、スマート トンネル アクセスが付与されるよう、アプリケーションに名前が付けられます。異なるパスまたはハッシュ値を指定するために選択するアプリケーションの複数のバージョンがサポートされるようにするには、この属性を使用して、各リスト エントリによってサポートされる OS と、アプリケーションの名前およびバージョンを指定し、エントリを区別できます。文字列には、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。**文字列には、最大 128 文字まで使用できます。Windows では、スマート トンネル アクセスのアプリケーシ

ョンが許可されるには、リモート ホストのアプリケーション パスの右側のこの値に完全に一致することが必要です。Windows のファイル名のみを指定する場合、スマート トンネル アクセスのアプリケーションを許可するために、SSL VPN によって、リモート ホスト上の場所は制限されません。別の場所にインストールされたアプリケーションのパスおよびユーザの場合、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、文字列の右側が入力する値と一致する限り、パスに置くことができます。スマート トンネル アクセスのアプリケーションが、リモート ホストの複数のパスの 1 つにある場合に、これを認可するには、アプリケーションの名前および拡張機能のみをこのフィールドに指定するか、または各パスに固有のスマート トンネル エントリを作成します。Windows では、コマンド プロンプトから開始され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、「cmd.exe」がアプリケーションの親であるため、スマート トンネル リストの 1 つのエントリのプロセス名に「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。Mac OS では、プロセスへのフル パスが必要で、大文字と小文字が区別されます。各ユーザ名のパスの指定を回避するには、パスの一部の前にチルド記号 (~) を挿入します (たとえば、~/bin/vnc) 。

- **[OS] : アプリケーションのホスト OS を指定するには、[Windows] または [Mac] をクリックします。**
- **[Hash] : (オプションで Windows のみに適用可) この値を取得するには、SHA-1 アルゴリズムを使用するハッシュを計算するユーティリティに、実行可能ファイルのチェックサムを入力します。**このようなユーティリティの一例として、Microsoft File Checksum Integrity Verifier(FCIV)があります。このユーティリティは、File Checksum Integrity Verifierユーティリティの可用性と説明で利用できます。FCIV のインストール後、スペースが含まれていないパスでハッシュされるアプリケーションの一時コピー (たとえば、c:/fciv.exe) を置き、コマンド ラインで fciv.exe -sha1 アプリケーションを入力 (たとえば、fciv.exe -sha1 c:\msimn.exe) して、SHA-1 ハッシュを表示します。SHA-1 ハッシュは、常に 40 の 16 進数の文字です。アプリケーションでスマート トンネル アクセスを認可する前に、クライアントレス SSL VPN によって、アプリケーション ID に一致するアプリケーションのハッシュが計算されます。結果がハッシュの値と一致すると、アプリケーションに対してスマート トンネル アクセスが許可されます。ハッシュを入力すると、SSL VPN によって、アプリケーション ID に指定した文字列と一致する不当なファイルが許可されないよう、妥当な保証が提供されます。チェックサムは、各バージョンまたはアプリケーションのパッチによって異なるため、入力したハッシュは、ある 1 つのバージョンまたはリモート ホストのパッチのみと照合できます。アプリケーションの複数のバージョンのハッシュを指定するには、各ハッシュ値に固有のスマート トンネルを作成します。**注 : ハッシュ値を入力**し、スマートトンネルアクセスを使用するアプリケーションの将来のバージョンまたはパッチをサポートする場合は、スマートトンネルリストを将来更新する必要があります。スマート トンネル アクセスに突然問題が発生した場合、ハッシュ値が含まれているアプリケーションが、アプリケーション アップグレードの最新の状態ではないことを示す可能性があります。この問題は、ハッシュを入力しないことによって回避できます。
- スマート トンネル リストを設定した場合は、それを、次のように、アクティブになるグループ ポリシーまたはローカル ユーザ ポリシーに割り当てる必要があります。リストをグループ ポリシーに割り当てるには、[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。リストをグループ ポリシーに割り当てるには、[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。

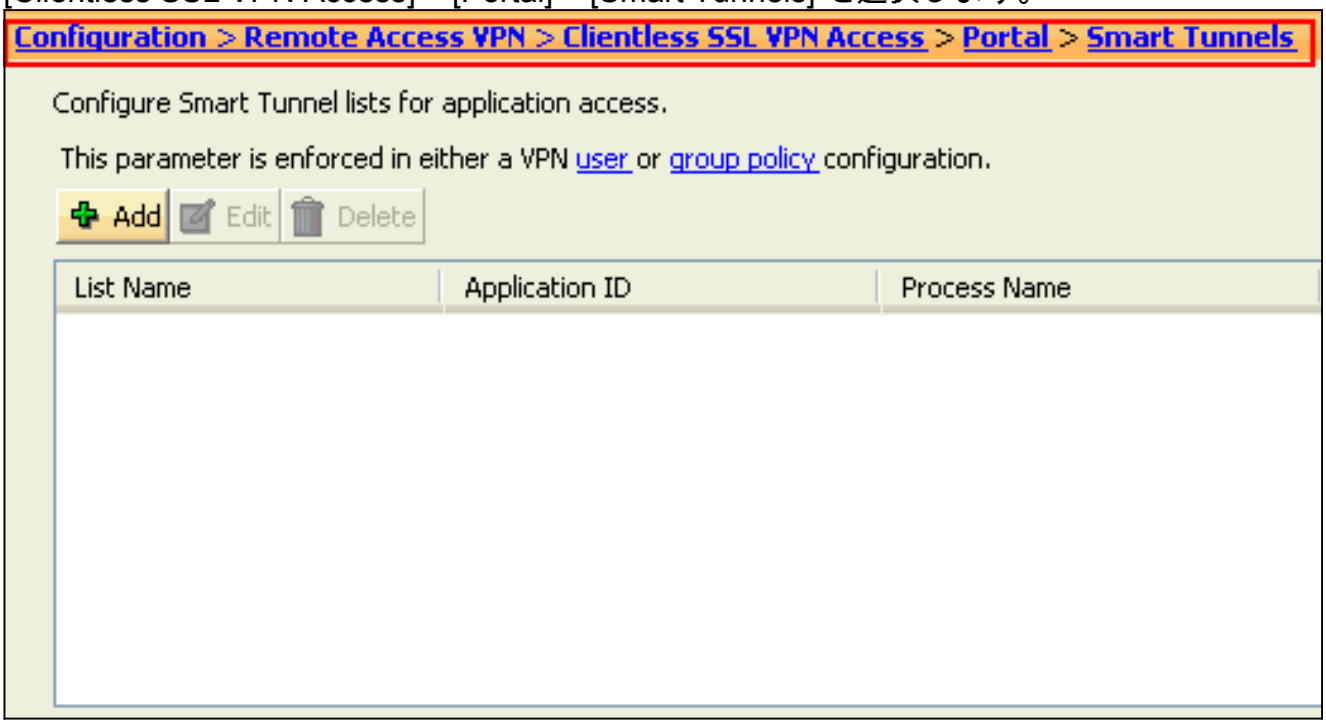
ASDM 6.0(2) を使用した ASA スマート トンネルの設定 (Lotus の例)

このドキュメントは、インターフェイス設定などの基本設定が完了していて、適切に動作していることを前提としています。

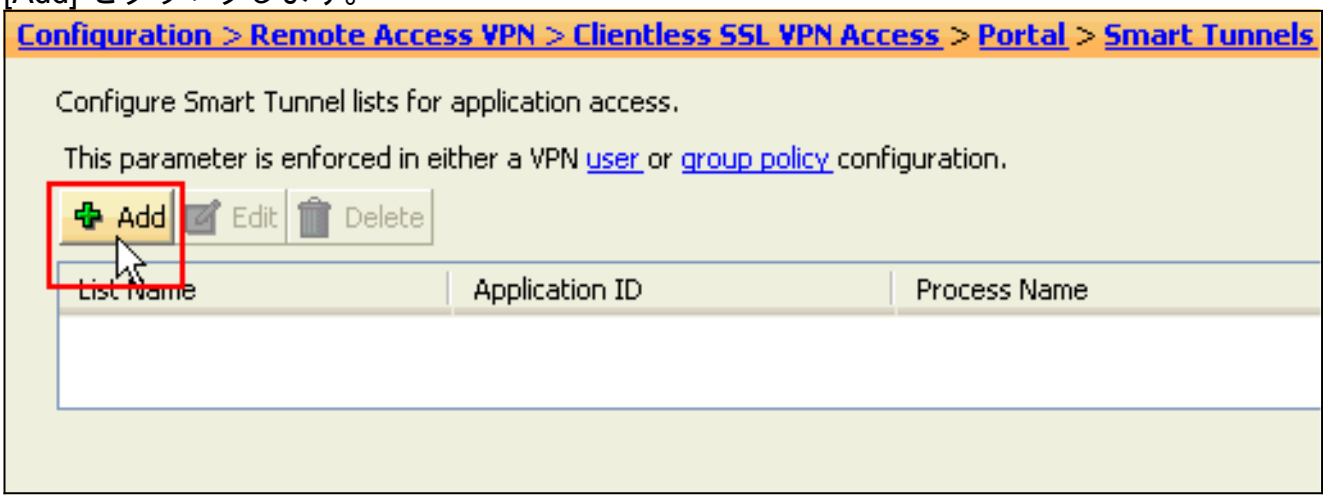
スマート トンネルを設定するには、次の手順を実行します。

注：この設定例では、スマートトンネルはLotusアプリケーション用に設定されています。

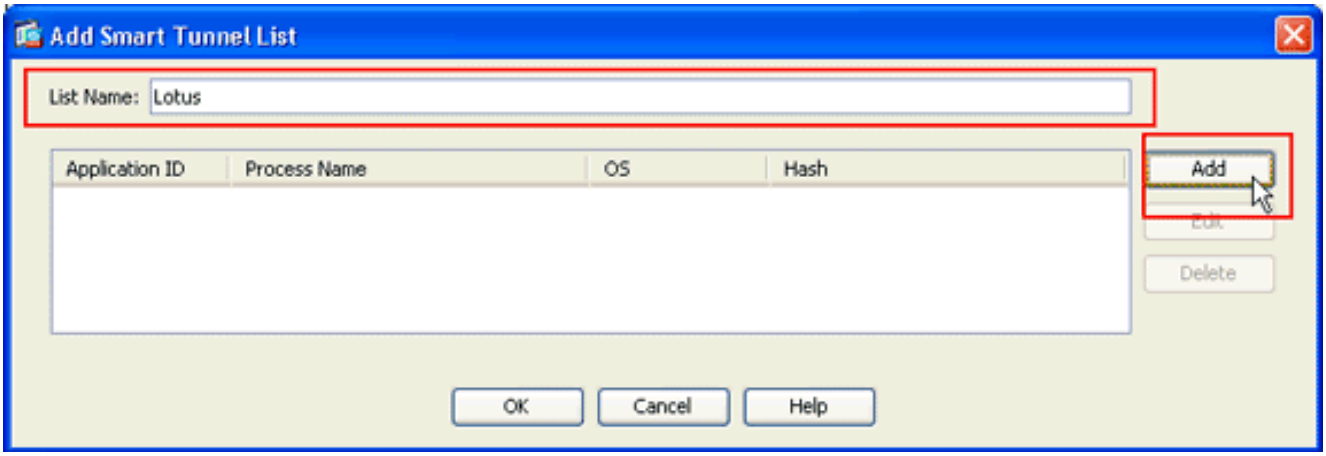
1. スマート トンネルの設定を開始するには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] を選択します。



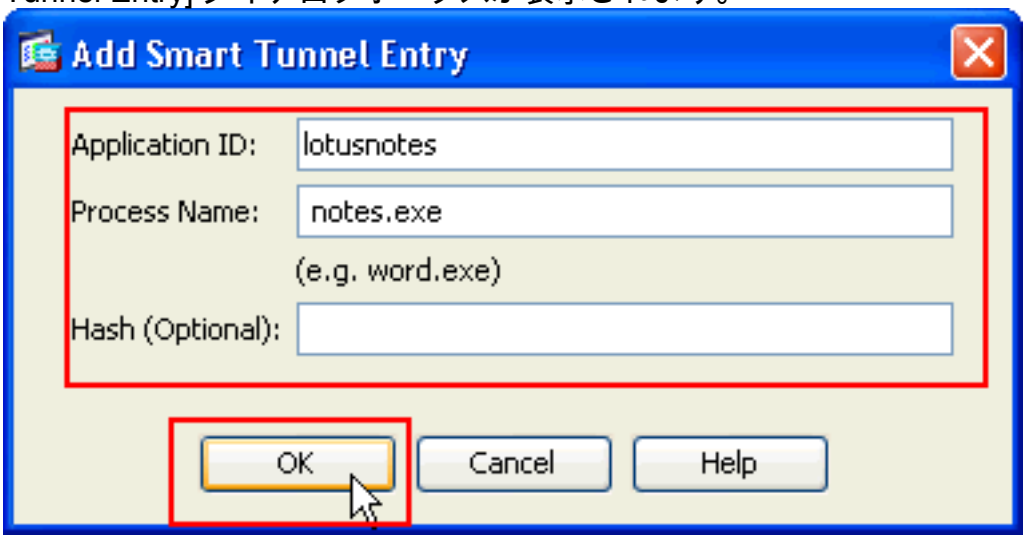
2. [Add] をクリックします。



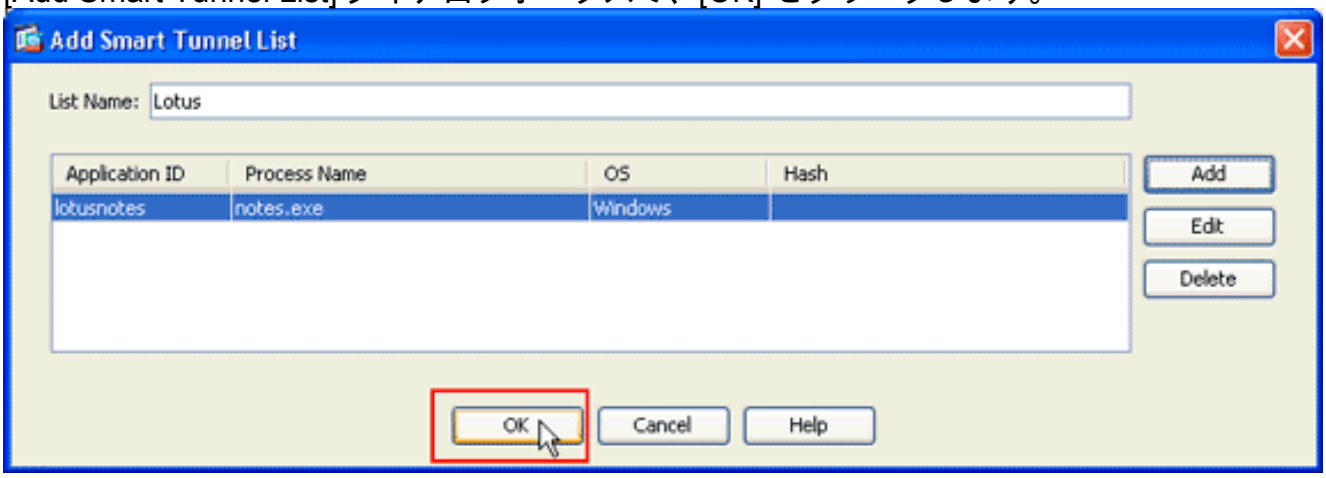
[Add Smart Tunnel List] ダイアログボックスが表示されます。



3. [Add Smart Tunnel List] ダイアログボックスで、[Add] をクリックします。[Add Smart Tunnel Entry] ダイアログボックスが表示されます。

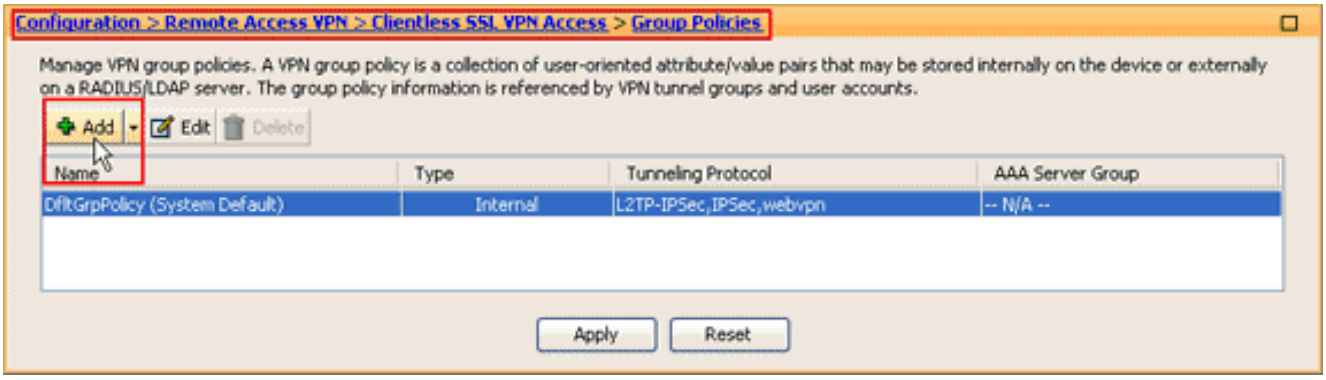


4. [Application ID] フィールドで、スマート トンネル リスト内のエントリを指定する文字列を入力します。
5. アプリケーションのファイル名および拡張子を入力し、[OK] をクリックします。
6. [Add Smart Tunnel List] ダイアログボックスで、[OK] をクリックします。

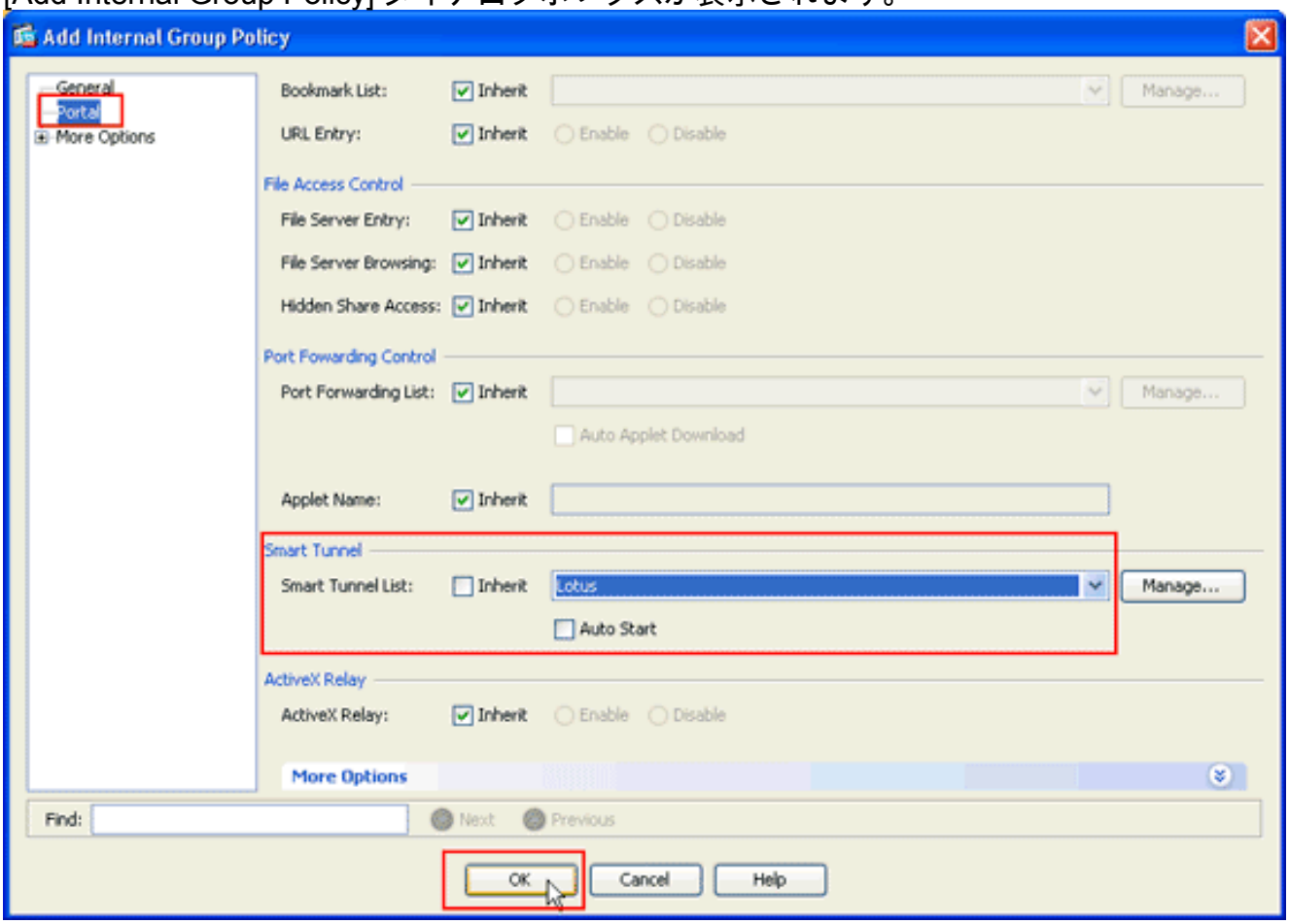


注：同等のCLI設定コマンドを次に示します。

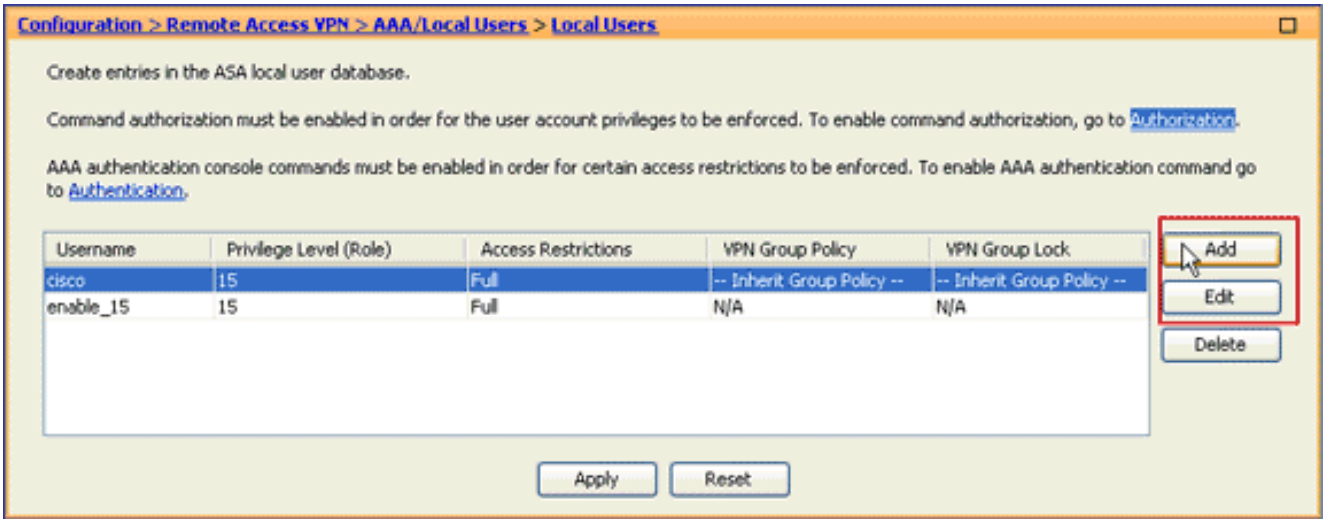
7. 次のようにして、関連付けられているアプリケーションにスマート トンネル アクセスを提供するグループ ポリシーまたはローカル ユーザ ポリシーにリストを割り当てます。グループ ポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] を選択し、[Add] または [Edit] **を選択します**。



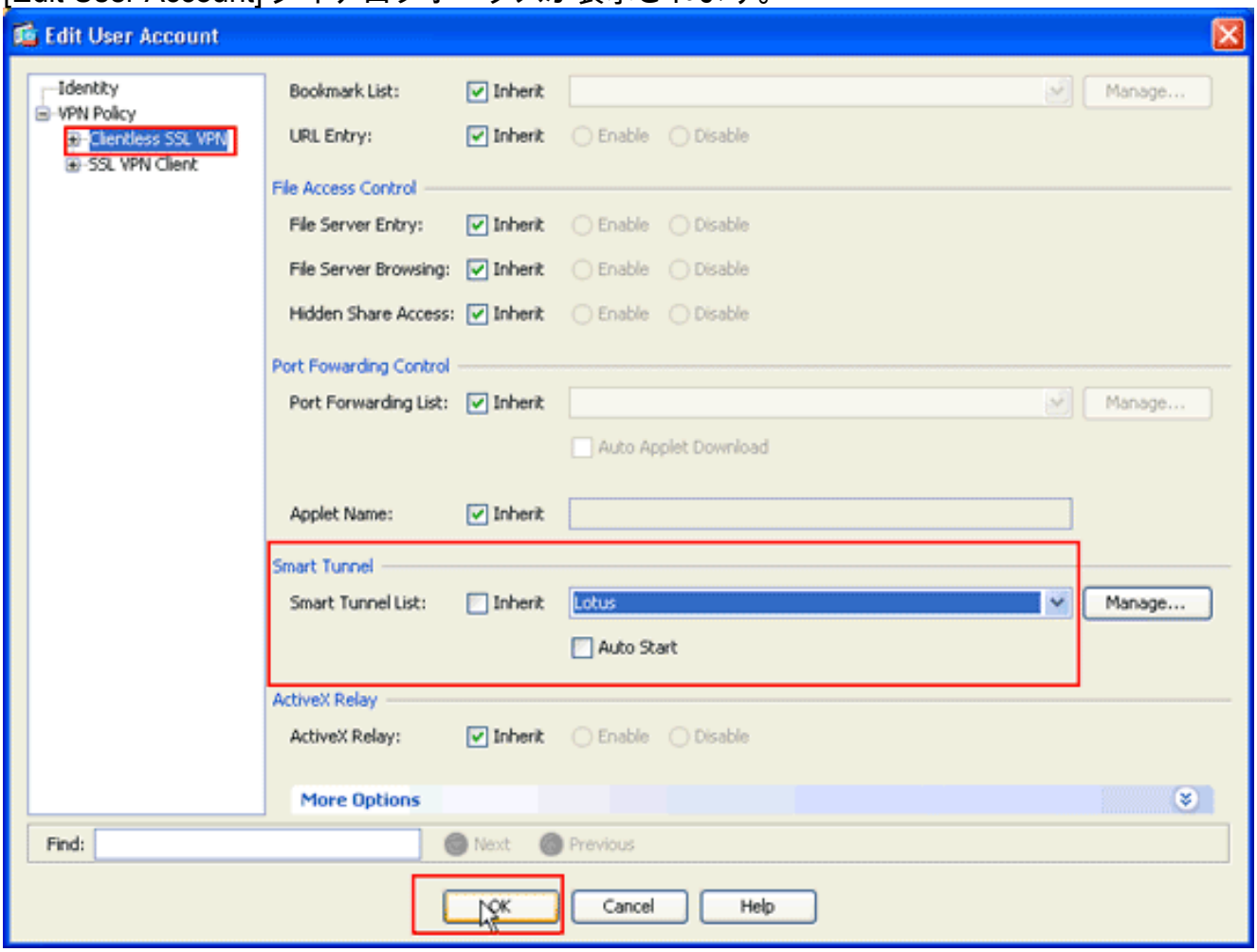
[Add Internal Group Policy] ダイアログボックスが表示されます。



8. [Add Internal Group Policy] ダイアログボックスで [Portal] をクリックし、[Smart Tunnel List] 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て、[OK] をクリックします。**注：この例**では、スマートトンネルリスト名としてLotusを使用しています。
9. 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] を選択し、[Add] をクリックして新しいユーザを設定するか、または [Edit] をクリックして既存ユーザを編集します。



[Edit User Account] ダイアログボックスが表示されます。



10. [Edit User Account] ダイアログボックスで [Clientless SSL VPN] をクリックし、[Smart Tunnel List] 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て、[OK] をクリックします。**注：この例**では、スマートトンネルリスト名としてLotusを使用しています。

スマート トンネル設定が完了しました。

トラブルシュート

クライアントレス ポータルでブックマークされたスマート トンネル URL を使用して接続できません。なぜこれが発生するのでしょうか。また、どうすれば解決できますか。

この問題は、Cisco Bug ID CSCsx05766（登録ユーザ専用）のために発生します。 この問題を解決するには、Java Runtime プラグインを、旧バージョンにダウングレードします。

WebVPN で設定されているスマート トンネル リンクの URL を変換できますか。

ASA でスマート トンネルを使用する場合は、URL を変換すること、およびブラウザのアドレスバーを非表示にすることはできません。ユーザは、スマート トンネルを使用するように Web VPN で設定されているリンクの URL を表示できます。このため、ユーザがポートを変更し、他のサービスを使用するためにサーバにアクセスすることが可能になります。

この問題を解決するには、WeType ACL を使用します。詳細は、『WebTypeアクセスコントロールリスト』を参照してください。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- ASDM を使用した ASA での SSL VPN Client（SVC）の設定例
- テクニカル サポートとドキュメント – Cisco Systems