



ポリシーグループ

- [スマート トンネルアクセス \(1 ページ\)](#)
- [クライアントレス SSL VPN キャプチャツール \(15 ページ\)](#)
- [ポータルアクセスルールの設定 \(15 ページ\)](#)
- [クライアントレス SSL VPN のパフォーマンスの最適化 \(17 ページ\)](#)

スマート トンネル アクセス

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 \(2 ページ\)](#)
- [スマート トンネルの前提条件 \(3 ページ\)](#)
- [スマート トンネルのガイドライン \(3 ページ\)](#)
- [スマート トンネルの設定 \(Lotus の例\) \(5 ページ\)](#)
- [トンネリングするアプリケーションの設定の簡略化 \(6 ページ\)](#)
- [スマート トンネルリストについて \(11 ページ\)](#)
- [スマート トンネル自動サインオンサーバリストの作成 \(11 ページ\)](#)
- [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 \(12 ページ\)](#)

- [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 \(13 ページ\)](#)
- [スマートトンネルからのログオフの設定 \(14 ページ\)](#)

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では、セキュリティ アプライアンスをパスイェイ、ASA をプロキシサーバとするクライアントレス (ブラウザベース) SSL VPN セッションが使用されます。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 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切な 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。

スマートトンネルのメリット

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。

スマートトンネルの前提条件

スマートトンネルでサポートされるプラットフォームとブラウザについては、『[サポート対象のVPNプラットフォーム、Cisco ASA 5500 シリーズ](#)』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 ではブラウザで ActiveX または Oracle Java ランタイム環境（JRE 6 以降を推奨）を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。
- スマートトンネルは、IE の拡張保護モードと互換性がありません。

スマートトンネルのガイドライン

- 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せん。

- 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。
- 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。
- macOS 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 セッション接続を確立できる。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、`cscost` 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。
- macOS 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。
- macOS では、スマート トンネルは次をサポートしない。
 - サンドボックス化されたアプリケーション ([View] > [Columns] を使用してアクティビティ モニタで確認します)。そのため、macOS 10.14 および 10.15 はスマート トンネリングをサポートしていません。
 - 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
- macOS では、プロセスへのフルパスが必要です。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`) 。
- Mac デバイスや Windows デバイスの Chrome ブラウザでスマート トンネルをサポートするための新しいメソッドが用意されました。Chrome Smart Tunnel Extension は、Netscape プラグインアプリケーションプログラムインターフェイス (NPAPI) に代わるものです。NPAPI は、Chrome ではサポートされなくなりました。

この拡張プログラムをインストールしていない Chrome でスマート トンネルに対応したブックマークをクリックすると、ユーザは拡張プログラムを取得できるように Chrome ウェブストアにリダイレクトされます。Chrome を新規インストールする場合、ユーザは拡張プログラムを取得できるように Chrome ウェブストアに移動されます。この拡張プログラムは、スマート トンネルの実行に必要なバイナリを ASA からダウンロードします。

Chrome のデフォルトのダウンロード場所が、現在のユーザの「ダウンロード」フォルダを指している必要があります。または、Chrome のダウンロード設定が [Ask every time] である場合は、ユーザは尋ねられたときに「ダウンロード」フォルダを選択する必要があります。

スマートトンネルの使用時、通常のブックマークおよびアプリケーション設定は、新しい拡張機能のインストールとダウンロード場所指定のプロセス以外は変更されません。

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

- 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。

次の表に、[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 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

アプリケーション ID の例	必要最小限のプロセス名
lotuslnotes	lnotes.exe
lotusntaskldr	ntaskldr.exe
lotusfileret	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** アプリケーションごとにステップを繰り返してリストに追加します。
- 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] 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] 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。



(注) この設定は、Windows プラットフォームのみに適用されます。

次の表に、アクセスを許可されるプロセスの状況を示します。

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。

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
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する	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。 (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。

手順

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。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に移動し、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。以下に、JSON 配列に格納されるパラメータについて説明します。

- [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。string 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は、[Process Name] の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) 上に、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 (例 : **fciv.exe-sha1 c:\msimn.exe**)、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] の値と一致すると、アプリケーションのスマート トンネル アクセスが認定されます。

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にしています。チェックサムはアプリケーションのバージョンやパッチに応じて異なるため、[Hash] の入力値が、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ことがあります。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場合は、それぞれの [Hash] の値に一意的なスマート トンネル エントリを作成します。

(注) [Hash] に値を入力して、スマート トンネル アクセスで今後のアプリケーションのバージョンや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 アクセスで突然問題が発生する場合は、[Hash] の値を含んでいるアプリケーション リストが、アプリケーションのアップグレードに対して最新ではない可能性があります。ハッシュを入力しないことで、この問題を回避できます。

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 TunnelList] 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 2: 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。ただし、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る。



(注) 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。

手順

- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] の順に移動し、[Smart Tunnel Auto Sign-on Server List] が展開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、リモートサーバのリストの一意の名前を入力します。設定する可能性がある他のリストと内容や目的を区別できるような名前を指定してください。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。

次のタスク



(注) 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。

手順

ステップ 1 [Configuration]>[Remote Access VPN]>[Clientless SSL VPN Access]>[Portal]>[Smart Tunnels] に移動し、いずれかのリストを選択して、[Edit] をクリックします。

ステップ 2 [Add Smart Tunnel Auto Sign-On Server List] ダイアログで [Add] ボタンをクリックし、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ません。
- ? : 単一の文字を一致させます。
- [] : かつ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) : 認証が必要な場合、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لم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。

- [PortNumber] : 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 サーバリストを割り当てるローカル ユーザを編集します。
 2. [VPN Policy] > [Clientless SSL VPN] の順に進み、[Smart Tunnel] 領域の下の [Auto Sign-on Server] 設定を探します。
 3. [Inherit] をオフにして、[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た場合、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。

親プロセスが終了した場合のスマートトンネルからのログオフの設定

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を開始した場合、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。

通知アイコンを使用したスマートトンネルからのログオフの設定

ブラウザを閉じて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

-
- 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。
-

クライアントレス SSL VPN キャプチャ ツール

クライアントレス SSL VPN CLI には、WebVPN 接続では正しく表示されない Web サイトに関する情報を記録できるキャプチャツールが含まれています。このツールが記録するデータは、シスコカスタマーサポートの担当者が問題のトラブルシューティングを行う際に役立ちます。

クライアントレス SSL VPN キャプチャ ツールの出力には次の 2 つのファイルが含まれます。

- Web ページのアクティビティに応じて mangled.1,2,3,4... など。mangle ファイルは、クライアントレス SSL VPN 接続のページを転送する VPN コンセントレータの html のアクションを記録します。
- Web ページのアクティビティに応じて original.1,2,3,4... など。元のファイルは、URL が VPN コンセントレータに送信したファイルです。

キャプチャ ツールによってファイル出力を開き、表示するには、[Administration] > [File Management] に移動します。出力ファイルを圧縮し、シスコサポート担当者に送信します。



- (注) クライアントレス SSL VPN キャプチャ ツールを使用すると、VPN コンセントレータのパフォーマンスが影響を受けます。出力ファイルを生成した後に、キャプチャ ツールを必ずオフに切り替えます。
-

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 ポリシーを設定できます。ASA はクライアントレス 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。

手順

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" を検出しようとはしますが、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。

クライアントレス SSL VPN のパフォーマンスの最適化

ASA には、クライアントレス SSL VPN のパフォーマンスと機能を最適化する複数の方法があります。パフォーマンスの改善には、Web オブジェクトのキャッシングと圧縮が含まれます。機能性の調整には、コンテンツ変換およびプロキシバイパスの制限の設定が含まれます。その他に、APCF でコンテンツ変換を調整することもできます。

コンテンツ変換の設定

デフォルトでは、ASA は、コンテンツ変換およびリライト エンジンを通じてすべてのクライアントレス SSL VPN トラフィックを処理します。これには、JavaScript や Java などの高度な要素からプロキシHTTPへのトラフィックも含まれますが、そのようなトラフィックでは、ユーザがアプリケーションに SSL VPN デバイス内部からアクセスしているのか、それらのデバイスに依存せずにアクセスしているのかに応じて、セマンティックやアクセス コントロールのルールが異なる場合があります。

Web リソースによっては、高度に個別の処理が要求される場合があります。次の項では、このような処理を提供する機能について説明します。組織や関係する Web コンテンツの要件に応じてこれらの機能のいずれかを使用する場合があります。

プロキシバイパスの使用

プロキシバイパスを使用するように ASA を設定できます。この設定は、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行います。プロキシバイパスはコンテンツの書き換え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の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。

手順

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。
-