



ポリシー グループ

2014年4月14日

リソース アクセスのためのクライアントレス **SSL VPN** ポリシーの作成と適用

内部サーバにあるリソースへのアクセスを制御するクライアントレス SSL VPN ポリシーを作成および適用するには、次のタスクを実行します。

- [グループポリシーへのユーザの割り当て](#)

グループポリシーへのユーザの割り当て

ユーザをグループポリシーに割り当てると、複数のユーザにポリシーを適用することで設定が容易になります。ユーザをグループポリシーに割り当てするには、ASA の内部認証サーバ、外部 RADIUS または LDAP サーバを使用できます。グループポリシーで設定を簡素化する方法の詳細な説明については、第4章の「接続プロファイル、グループポリシー、およびユーザ」を参照してください。

クライアントレス **SSL VPN** の接続プロファイルの属性の設定

表 16-1 は、クライアントレス SSL VPN に固有の接続プロファイル属性のリストです。これらの属性に加えて、すべての VPN 接続に共通の一般接続プロファイルの属性を設定します。接続プロファイルの設定に関する手順ごとの情報については、第4章の「接続プロファイル、グループポリシー、およびユーザ」を参照してください。



(注)

以前のリリースでは、「接続プロファイル」は「トンネルグループ」と呼ばれていました。**tunnel-group** コマンドを使用して接続プロファイルを設定します。この章では、この2つの用語が同義的によく使用されています。

表 16-1 クライアントレス SSL VPN 用接続プロファイルの属性

コマンド	機能
authentication	認証方式を設定します。
customization	適用するすでに定義済みのカスタマイゼーションの名前を指定します。
exit	トンネルグループのクライアントレス SSL VPN 属性コンフィギュレーションモードを終了します。
nbns-server	CIFS 名前解決に使用する NetBIOS ネーム サービス サーバ (nbns-server) の名前を指定します。
group-alias	サーバが接続プロファイルの参照に使用できる代替名を指定します。
group-url	1 つ以上のグループ URL を指定します。この属性で URL を確立すると、ユーザがその URL を使用してアクセスするときにこのグループが自動的に選択されます。
dns-group	DNS サーバ名、ドメイン名、ネームサーバ、リトライの回数、およびタイムアウト値を指定する DNS サーバグループを指定します。
help	トンネルグループコンフィギュレーションコマンドのヘルプを提供します。
hic-fail-group-policy	Cisco Secure Desktop Manager を使用して、グループベースポリシー属性を「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合は、VPN 機能ポリシーを指定します。
no	属性値のペアを削除します。
override-svc-download	AnyConnect VPN クライアントをリモートユーザにダウンロードするために、設定されているグループポリシー属性またはユーザ名属性のダウンロードが上書きされます。
pre-fill-username	このトンネルグループにユーザ名と証明書のバインディングを設定します。
proxy-auth	特定のプロキシ認証トンネルグループとしてこのトンネルグループを識別します。
radius-reject-message	認証が拒否されたときに、ログイン画面に RADIUS 拒否メッセージを表示します。
secondary-pre-fill-username	このトンネルグループにセカンダリユーザー名と証明書のバインディングを設定します。
without-csd	トンネルグループの CSD をオフに切り替えます。

クライアントレス SSL VPN のグループポリシー属性とユーザ属性の設定

表 16-2 に、クライアントレス SSL VPN のグループポリシー属性とユーザ属性のリストを示します。設定グループポリシーとユーザ属性の段階を追った手順については、『Cisco ASA シリーズ VPN CLI コンフィギュレーションガイド』の「グループポリシー属性とユーザ属性の設定」または「接続プロファイル、グループポリシー、およびユーザ」を参照してください。

表 16-2 クライアントレス SSL VPN のグループポリシー属性とユーザ属性

コマンド	機能
<code>activex-relay</code>	クライアントレス SSL VPN セッションを確立したユーザが、ブラウザを使用して Microsoft Office アプリケーションを起動できるようになります。アプリケーションは、セッションを使用して ActiveX のダウンロードとアップロードを行います。ActiveX のリレーは、クライアントレス SSL VPN セッションを終了するまで有効なままです。
<code>auto-sign-on</code>	自動サインオンの値を設定します。設定ではクライアントレス SSL VPN への接続にユーザ名およびパスワードのクレデンシャルが 1 回のみ必要です。
<code>customization</code>	カスタマイゼーションオブジェクトをグループポリシーまたはユーザに割り当てます。
<code>deny-message</code>	クライアントレス SSL VPN に正常にログインできるが VPN 特権を持たないリモートユーザに送信するメッセージを指定します。
<code>file-browsing</code>	ファイルサーバとファイル共有の CIFS ファイルブラウジングをイネーブルにします。ブラウズには、NBNS (マスターブラウザまたは WINS) が必要です。
<code>file-entry</code>	アクセスするファイルサーバ名の入力をユーザに許可します。
<code>filter</code>	webtype アクセスリストの名前を設定します。
<code>hidden-shares</code>	非表示の CIFS 共有ファイルの可視性を制御します。
<code>homepage</code>	ログイン時に表示される Web ページの URL を設定します。
<code>html-content-filter</code>	このグループポリシー用の HTML からフィルタリングするコンテンツとオブジェクトを設定します。
<code>http-comp</code>	圧縮を設定します。
<code>http-proxy</code>	HTTP 要求の処理に外部プロキシサーバを使用するように ASA を設定します。 (注) プロキシ NTLM 認証は <code>http-proxy</code> ではサポートされていません。認証なしのプロキシと基本認証だけがサポートされています。
<code>keep-alive-ignore</code>	セッションタイマーのアップデートを無視するオブジェクトの最大サイズを設定します。
<code>port-forward</code>	転送するクライアントレス SSL VPN TCP ポートのリストを適用します。ユーザインターフェイスにこのリストのアプリケーションが表示されます。
<code>post-max-size</code>	ポストするオブジェクトの最大サイズを設定します。
<code>smart-tunnel</code>	スマートトンネルを使用するプログラムと複数のスマートトンネルパラメータのリストを設定します。

表 16-2 クライアントレス SSL VPN のグループポリシー属性とユーザ属性 (続き)

コマンド	機能
<code>sso-server</code>	SSO サーバの名前を設定します。
<code>storage-objects</code>	セッションとセッションの間に保存されたデータのストレージオブジェクトを設定します。
<code>svc</code>	SSL VPN クライアント属性を設定します。
<code>unix-auth-gid</code>	UNIX グループ ID を設定します。
<code>unix-auth-uid</code>	UNIX ユーザ ID を設定します。
<code>upload-max-size</code>	アップロードするオブジェクトの最大サイズを設定します。
<code>url-entry</code>	ユーザが HTTP/HTTPS URL を入力する機能を制御します。
<code>url-list</code>	エンドユーザのアクセス用にクライアントレス SSL VPN のポータルページに表示されるサーバと URL のリストを適用します。
<code>user-storage</code>	セッション間のユーザ データを保存する場所を設定します。

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](#)
- [スマートトンネルアクセスに適切なアプリケーションの追加](#)
- [スマートトンネルアクセスに適切なアプリケーションの追加](#)
- [スマートトンネルリストについて](#)
- [スマートトンネルのトンネルポリシーの設定および適用](#)
- [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 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。

ActiveX ページでは、関連するグループポリシーに **activex-relay** コマンドを入力しておくことが必要です。コマンドを入力しているか、ポリシーにスマートトンネルリストを割り当てていて、エンドポイントのブラウザのプロキシ例外リストでプロキシが指定されている場合、このリストに「shutdown.webvpn.relay.」エントリを追加する必要があります。

- 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。

制限

- 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、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。
- 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。

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。

制限

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。

手順の詳細

次の `smart tunnel` コマンドは、各グループポリシーとユーザ名で使用可能です。各グループポリシーとユーザ名のコンフィギュレーションは、一度にこれらのコマンドの1つだけサポートします。そのため、1つのコマンドを入力すると、ASA が、該当のグループポリシーまたはユーザ名のコンフィギュレーションに存在するコマンドを新しいコマンドで置き換えます。または、最後のコマンドの場合、グループポリシーまたはユーザ名にすでに存在する `smart-tunnel` コマンドが単純に削除されます。

	コマンド	目的
ステップ 1	<code>smart-tunnel auto-start list</code> または <code>smart-tunnel enable list</code> または <code>smart-tunnel disable</code> または <code>no smart-tunnel [auto-start list enable list disable]</code>	<p>ユーザのログイン時にスマートトンネルアクセスを自動的に開始します。</p> <p>ユーザ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します。ただし、ユーザがクライアントレス SSL VPN ポータルページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマートトンネルアクセスを開始する必要があります。</p> <p>スマートトンネルアクセスを使用禁止にします。</p> <p>smart-tunnel コマンドがグループポリシーまたはユーザ名コンフィギュレーションから削除され、[no] smart-tunnel コマンドがデフォルトグループポリシーから継承されます。no smart-tunnel コマンドの後にあるキーワードはオプションですが、これらのキーワードにより削除対象をその名前の smart-tunnel コマンドに限定します。</p>
ステップ 2	必要なオプションについては、「 スマートトンネルアクセスの自動化 」を参照してください。	

スマートトンネルポリシーの設定および適用

スマートトンネルポリシーは、グループポリシーまたはユーザ名単位の設定が必要です。各グループポリシーまたはユーザ名は、グローバルに設定されたネットワークのリストを参照します。スマートトンネルをオンにすると、トンネル外部のトラフィックに、ネットワーク（ホストのセット）を設定する CLI および指定されたスマートトンネルネットワークを使用してユーザに対してポリシーを適用する CLI の 2 つの CLI を使用できます。次のコマンドによって、スマートトンネルポリシーを設定するために使用するホストのリストが作成されます。

手順の詳細

	コマンド	目的
ステップ 1	<code>webvpn</code>	クライアントレス SSL VPN コンフィギュレーションモードに切り替えます。
ステップ 2	<code>[no] smart-tunnel network network name ip ip netmask</code>	スマートトンネルポリシー設定のために使用するホストのリストを作成します。 <i>network name</i> は、トンネルポリシーに適用する名前です。 <i>ip</i> は、ネットワークの IP アドレスです。 <i>netmask</i> は、ネットワークのネットマスクです。

	コマンド	目的
ステップ 3	<code>[no] smart-tunnel network network name host host mask</code>	*.cisco.com などのホスト名マスクを確立します。
ステップ 4	<code>[no] smart-tunnel tunnel-policy [excludespecified tunnelspecified] network name tunnelall]</code> または <code>[no] smart-tunnel tunnel-policy [excludespecified tunnelspecified] network name tunnelall]</code>	特定のグループポリシーまたはユーザポリシーにスマートトンネルポリシーを適用します。 <i>network name</i> は、トンネリングされるネットワークのリストです。 <i>tunnelall</i> は、すべてをトンネリング (暗号化) します。 <i>tunnelspecified</i> は、 <i>network name</i> で指定されたネットワークだけをトンネリングします。 <i>excludespecified</i> は、 <i>network name</i> で指定されたネットワークの外部のネットワークだけをトンネリングします。

スマートトンネルのトンネルポリシーの設定および適用

SSL VPN クライアントでのスプリットトンネル設定と同様に、スマートトンネルポリシーはグループポリシーおよびユーザ名単位の設定です。各グループポリシーおよびユーザ名は、グローバルに設定されたネットワークのリストを参照します。

コマンド	目的
<code>[no] smart-tunnel tunnel-policy [excludespecified tunnelspecified] network name tunnelall]</code> または <code>[no] smart-tunnel tunnel-policy [excludespecified tunnelspecified] network name tunnelall]</code>	グローバルに設定されたネットワークのリストを参照します。 <i>network name</i> は、トンネリングされるネットワークのリストです。 <i>tunnelall</i> は、すべてをトンネリング (暗号化) します。 <i>tunnelspecified</i> は、 <i>network name</i> で指定されたネットワークだけをトンネリングします。 <i>excludespecified</i> は、 <i>network name</i> で指定されたネットワークの外部のネットワークだけをトンネリングします。

コマンド	目的
<pre>ciscoasa(config-webvpn)# [no] smart-tunnel network network name ip ip netmask ciscoasa(config-webvpn)# [no] smart-tunnel network network name host host mask</pre>	<p>グループポリシーおよびユーザポリシーにトンネルポリシーを適用します。一方のコマンドによってホストが指定され、他方のコマンドによってネットワークIPが指定されます。1つのコマンドのみを使用します。</p> <p><i>network name</i> : トンネルポリシーを適用するネットワークの名前</p> <p><i>ip address</i> : ネットワークのIPアドレス</p> <p><i>netmask</i> : ネットワークのネットマスク</p> <p><i>host mask</i> : ホスト名マスク (*.cisco.com など)</p>
<p>例 :</p> <pre>ciscoasa(config-webvpn)# smart-tunnel network inventory ip 10.5.2.2 ciscoasa(config-webvpn)# smart-tunnel network inventory host www.example.com</pre>	<p>パートナーがログイン時に最初にクライアントレスポータルを介さずに内部インベントリサーバページにクライアントレスアクセスできるようにしたいとベンダーが考えている場合、スマートトンネルポリシー設定は適切なオプションです。1つのホストだけを含むトンネルポリシーを作成します (次の例では、インベントリページは <code>www.example.com</code> (10.5.2.2) でホストされており、ホストのIPアドレスと名前の両方を設定するものと仮定します)。</p>
<pre>ciscoasa(config-group-webvpn)# smart-tunnel tunnel-policy tunnelspecified inventory</pre> <p>(オプション)</p> <pre>ciscoasa(config-group-webvpn)# homepage value http://www.example.com ciscoasa(config-group-webvpn)# homepage use-smart-tunnel</pre>	<p>パートナーのグループポリシーに、指定したトンネルのトンネルポリシーを適用します。</p> <p>グループポリシーのホームページを指定して、そのページでスマートトンネルをイネーブルにします。スクリプトを記述したり何かをアップロードしなくても、管理者はどのページがスマートトンネル経由で接続するかを指定できます。</p>
<p>(オプション)</p> <pre>ciscoasa(config-webvpn)# smart-tunnel notification-icon</pre>	<p>スマートトンネルをイネーブルにした状態でブラウザによって開始されたすべてのプロセスはトンネルにアクセスできるため、デフォルトでは、スマートトンネルアプリケーションの設定は必須ではありません。ただし、ポータルが表示されないため、ログアウト通知アイコンをイネーブルにできます。</p>

スマートトンネル自動サインオンサーバリストの作成

コマンド	目的
<code>webvpn</code>	クライアントレス SSL VPN コンフィギュレーションモードに切り替えます。
<code>smart-tunnel auto-sign-on list [use-domain] [realm realm-string] [port port-num] {ip ip-address [netmask] host hostname-mask}</code>	<p>サーバリストに追加する各サーバに対して使用します。</p> <ul style="list-style-type: none"> <code>list</code> : リモートサーバのリストの名前を指定します。スペースを含む場合、名前の前後に引用符を使用します。文字列は最大 64 文字まで使用できます。コンフィギュレーション内にリストが存在しない場合、ASA はリストを作成します。存在する場合、リストにエントリを追加します。区別しやすい名前を割り当てます。 <code>use-domain</code> (オプション) : 認証が必要な場合は、Windows ドメインをユーザ名に追加します。このキーワードを入力する場合は、スマートトンネルリストを1つ以上のグループポリシーまたはユーザ名に割り当てるときにドメイン名を指定してください。 <code>realm</code> : 認証のレルムを設定します。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。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。 <code>port</code> : 自動サインオンを実行するポートを指定します。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。 <code>ip</code> : IP アドレスとネットマスクによってサーバを指定します。 <code>ip-address[netmask]</code> : 自動認証先のホストのサブネットワークを指定します。 <code>host</code> : ホスト名またはワイルドカードマスクによってサーバを指定します。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。 <code>hostname-mask</code> : 自動認証する対象のホスト名またはワイルドカードマスクを指定します。
(オプション) <code>[no] smart-tunnel auto-sign-on list [use-domain] [realm realm-string] [port port-num] {ip ip-address [netmask] host hostname-mask}</code>	ASA 設定に表示されるとおりにリストと IP アドレスまたはホスト名を指定して、サーバのリストからエントリを削除します。

コマンド	目的
<code>show running-config webvpn smart-tunnel</code>	スマートトンネル自動サインオンサーバリストを表示します。
<code>config-webvpn</code>	<code>config-webvpn</code> コンフィギュレーションモードに切り替えます。
<code>smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0</code>	サブネット内のすべてのホストを追加し、認証が必要な場合に Windows ドメインをユーザ名に追加します。
(オプション) <code>no smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0</code>	削除されるエントリがリストの唯一のエントリである場合は、リストからそのエントリを削除し、HR という名前のリストも削除します。
<code>no smart-tunnel auto-sign-on HR</code>	ASA 設定からリスト全体を削除します。
<code>smart-tunnel auto-sign-on intranet host *.example.com</code>	ドメイン内のすべてのホストを <code>intranet</code> という名前のスマートトンネル自動サインオンリストに追加します。
<code>no smart-tunnel auto-sign-on intranet host *.example.com</code>	リストからエントリを削除します。

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き、次の項で説明するように、そのリストを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てアクティブにする必要があります。

次の手順は、サーバリストにサーバを追加することです。

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。

前提条件

`smart-tunnel auto-sign-on list` コマンドを使用して、最初にサーバのリストを作成する必要があります。グループポリシーまたはユーザ名に割り当てることができるリストは1つだけです。

制限

- スマートトンネル自動サインオン機能は、Internet Explorer および Firefox を使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。
- Firefox では、管理者が正確なホスト名または IP アドレスを使用してホストを指定する必要があります（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、およびネットマスクは使用できません）。たとえば、Firefox では、`*.cisco.com` を入力したり、`email.cisco.com` をホストする自動サインオンを期待したりすることはできません。

手順の詳細

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル自動サインオンをイネーブルにするには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>webvpn</code>	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	<code>group-policy webvpn</code> または <code>username webvpn</code>	グループ ポリシーのクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。 ユーザ名のクライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 3	<code>smart-tunnel auto-sign-on enable</code>	スマート トンネル自動サインオン クライアントレス SSL VPN セッションをイネーブルにします。
ステップ 4	(オプション) <code>[no] smart-tunnel auto-sign-on enable list</code> <code>[domain domain]</code>	スマート トンネル自動サインオン クライアントレス SSL VPN セッションをオフに切り替えて、グループ ポリシーまたはユーザ名からこのセッションを削除して、デフォルトを使用します。 <ul style="list-style-type: none"> • <code>list</code> : ASA クライアントレス SSL VPN コンフィギュレーションにすでに存在するスマート トンネル自動サインオン リストの名前です。 • (オプション) <code>domain</code> : 認証中にユーザ名に追加されるドメインの名前です。ドメインを入力する場合、<code>use-domain</code> キーワードをリスト エントリに入力します。
ステップ 5	<code>show running-config webvpn smart-tunnel</code>	SSL VPN コンフィギュレーション内のスマート トンネル自動サインオン リストのエントリを表示します。
ステップ 6	<code>smart-tunnel auto-sign-on enable HR</code>	HR という名前のスマート トンネル自動サインオン リストをイネーブルにします。
ステップ 7	<code>smart-tunnel auto-sign-on enable HR domain CISCO</code>	HR という名前のスマート トンネル自動サインオン リストをイネーブルにし、認証中に CISCO という名前のドメインをユーザ名に追加します。
ステップ 8	(オプション) <code>no smart-tunnel auto-sign-on enable HR</code>	HR という名前のスマート トンネル自動サインオン リストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル自動サインオン リスト コマンドを継承します。

スマートトンネルアクセスの自動化

ユーザのログイン時にスマートトンネルアクセスを自動的に開始するには、次のコマンドを入力します。

要件

Mac OS X の場合は、自動開始設定が行われていなくても、ポータル の [Application Access] パネルにあるアプリケーションのリンクをクリックする必要があります。

手順の詳細

	コマンド	目的
ステップ 1	<code>webvpn</code>	クライアントレス SSL VPN コンフィギュレーションモードに切り替えます。
ステップ 2	<code>group-policy webvpn</code> または <code>username webvpn</code>	グループポリシーのクライアントレス SSL VPN コンフィギュレーションモードに切り替えます。 ユーザ名のクライアントレス SSL VPN コンフィギュレーションモードに切り替えます。
ステップ 3	<code>smart-tunnel auto-start list</code> 例： <code>hostname(config-group-policy)# webvpn</code> <code>hostname(config-group-webvpn)# smart-tunnel auto-start apps1</code>	ユーザのログイン時にスマートトンネルアクセスを自動的に開始します。 <i>list</i> は、すでに存在するスマートトンネルリストの名前です。 <code>apps1</code> という名前のスマートトンネルリストをグループポリシーに割り当てます。
ステップ 4	<code>show running-config webvpn smart-tunnel</code>	SSL VPN コンフィギュレーション内のスマートトンネルリストのエントリを表示します。
ステップ 5	(オプション) <code>no smart-tunnel</code>	<code>smart-tunnel</code> コマンドをグループポリシーまたはユーザ名から削除し、デフォルトに戻します。

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。

手順の詳細

	コマンド	目的
ステップ 1	<code>webvpn</code>	クライアントレス SSL VPN コンフィギュレーションモードに切り替えます。
ステップ 2	<code>group-policy webvpn</code> または <code>username webvpn</code>	グループポリシーのクライアントレス SSL VPN コンフィギュレーションモードに切り替えます。 ユーザ名のクライアントレス SSL VPN コンフィギュレーションモードに切り替えます。
ステップ 3	<code>smart-tunnel [enable list disable]</code> 例： <code>hostname(config-group-policy)# webvpn</code> <code>hostname(config-group-webvpn)# smart-tunnel enable apps1</code>	スマートトンネルアクセスをイネーブルにします。 <code>list</code> は、すでに存在するスマートトンネルリストの名前です。前の表の smart-tunnel auto-start list を入力した場合は、スマートトンネルアクセスを手動で開始する必要はありません。 <code>apps1</code> という名前のスマートトンネルリストをグループポリシーに割り当てます。
ステップ 4	<code>show running-config webvpn smart-tunnel</code>	SSL VPN コンフィギュレーション内のスマートトンネルリストのエントリを表示します。
ステップ 5	(オプション) <code>no smart-tunnel</code>	smart-tunnel コマンドをグループポリシーまたはローカルユーザポリシーから削除し、デフォルトのグループポリシーに戻します。
ステップ 6	(オプション) <code>smart-tunnel disable</code>	スマートトンネルアクセスをオフに切り替えます。

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を開始した場合、`ieexplore.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。

手順の詳細

	コマンド	目的
ステップ 1	<code>[no] smart-tunnel notification-icon</code>	<p>管理者が通知アイコンをグローバルでオンにすることを許可します。このコマンドは、ブラウザウィンドウを閉じることでログアウトを行うのではなく、ログアウトプロパティを設定し、ユーザにログアウトのためのログアウトアイコンが提示されるかどうかを制御します。また、このコマンドは通知アイコンをオンまたはオフにすると自動的にオンまたはオフになる親プロセスが終了する場合のログオフも制御します。</p> <p>notification-icon は、ログアウトのためにアイコンを使用するタイミングを指定するキーワードです。</p> <p>(注) このコマンドの <code>no</code> バージョンがデフォルトです。この場合、すべてのブラウザウィンドウを閉じることで SSL VPN セッションからログオフします。</p> <p>(注) ポータルのログアウトは引き続き有効であり、影響を受けません。</p>
ステップ 2	<code>*.webvpn.</code>	<p>プロキシを使用し、プロキシリストの例外に追加すると、アイコンの使用に関係なく、ログオフ時にスマートトンネルが必ず適切に閉じられるようにします。</p>

通知アイコンの利用

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。

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、JavaScript および Java などの高度な要素からプロキシ HTTP へのトラフィックを含む、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アクセスするのに SSL VPN デバイス内部からアクセスしているか、これらに依存せずにアクセスしているかによって、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。

- [リライトされた Java コンテンツに署名するための証明書の設定](#)
- [コンテンツのリライトの切り替え](#)
- [プロキシバイパスの使用](#)

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。

リライトされた Java コンテンツに署名するための証明書の設定

クライアントレス SSL VPN が変換した Java オブジェクトは、その後、トラストポイントに関連付けられた PKCS12 デジタル証明書により署名されます。

手順の詳細

	コマンド	目的
ステップ 1	<code>crypto ca import</code>	証明書をインポートします。
ステップ 2	ava-trustpoint 例 : t hostname(config)# crypto ca import mytrustpoint pkcs12 mypassphrase Enter the base 64 encoded PKCS12. End with the word "quit" on a line by itself. [PKCS12 data omitted] quit INFO: Import PKCS12 operation completed successfully. hostname(config)# webvpn hostname(config)# java-trustpoint mytrustpoint	証明書を採用します。 mytrustpoint という名前のトラストポイントの作成、および Java オブジェクトに署名するための割り当てを示します。

コンテンツのリライトの切り替え

公開 Web サイトなどの一部のアプリケーションや Web リソースによっては、ASA を通過しない設定が求められる場合があります。このため、ASA では、特定のサイトやアプリケーションを ASA を通過せずにブラウズできるリライトルールを作成できます。これは、IPsec VPN 接続におけるスプリット トンネリングによく似ています。

	コマンド	目的
ステップ 1	<code>webvpn</code>	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	<code>rewrite</code>	クライアントレス SSL VPN トンネルの外部にアクセスするためのアプリケーションとリソースを指定します。このコマンドは複数回使用できます。
ステップ 3	<code>disable</code>	rewrite コマンドとともに使用します。セキュリティ アプライアンスはリライトルールを順序番号に従って検索するため、ルールの順序番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

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。

proxy-bypass コマンドは複数回使用できます。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。

手順の詳細

	コマンド	目的
ステップ 1	webvpn	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	proxy-bypass	プロキシバイパスを設定します。

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

	コマンド	目的
ステップ 1	<pre>webvpn</pre> <p>例:</p> <pre>hostname(config)# webvpn</pre>	クライアントレス SSL VPN コンフィギュレーションモードに入ります。
ステップ 2	<pre>portal-access-rule priority [{permit deny [code code]}] {any user-agent match string}</pre> <p>例:</p> <pre>hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*</pre> <pre>hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match "*my agent*"</pre>	<p>HTTP ヘッダー内の HTTP ヘッダー コードまたは文字列に基づいて、クライアントレス SSL VPN セッションの作成を許可または拒否します。</p> <p>2 番目の例では、スペースを含む文字列を指定するための適切な構文を示しています。文字列はワイルドカード (*) で囲み、さらに引用符 (") で囲みます。</p>

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性を最適化するいくつかの方法があります。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。次の項では、これらの機能について説明します。

- [キャッシングの設定](#)
- [コンテンツ変換の設定](#)

キャッシングの設定

キャッシングを行うとクライアントレス SSL VPN のパフォーマンスが向上します。頻繁に再利用されるオブジェクトをシステム キャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。また、クライアントレス SSL VPN とリモート サーバ間のトラフィックが軽減されるため、多くのアプリケーションが今までよりはるかに効率的に実行できるようになります。

デフォルトでは、キャッシングはイネーブルになっています。キャッシュモードでキャッシングコマンドを使用すると、ユーザの環境に応じてキャッシング動作をカスタマイズできます。