CHAPTER 16

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
activex-relay	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。
auto-sign-on	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。
customization	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。
deny-message	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。
file-browsing	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。
file-entry	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。
filter	webtype アクセス リストの名前を設定します。
hidden-shares	非表示の CIFS 共有ファイルの可視性を制御します。
homepage	ログイン時に表示される Web ページの URL を設定します。
html-content-filter	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。
http-comp	圧縮を設定します。
http-proxy	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 **http-proxy** 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。
keep-alive-ignore	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。
port-forward	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。
post-max-size	ポストするオブジェクトの最大サイズを設定します。
smart-tunnel	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
sso-server	SSO サーバの名前を設定します。
storage-objects	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。
svc	SSL VPN クライアント属性を設定します。
unix-auth-gid	UNIX グループ ID を設定します。
unix-auth-uid	UNIX ユーザ ID を設定します。
upload-max-size	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。
url-entry	ユーザが HTTP/HTTPS URL を入力する機能を制御します。
url-list	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。
user-storage	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 アクセスに適格なアプリケーションの追加
- スマート トンネル アクセスに適格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。

  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る。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 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	**smart-tunnel auto-start** *list* または **smart-tunnel enable** *list* または **smart-tunnel disable** または **no smart-tunnel [auto-start list | enable list | disable]**	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。 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。 スマート トンネル アクセスを使用禁止にします。 **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。
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	**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	**[no] smart-tunnel network** *network name* **ip** *ip netmask*	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。*network name* は、トンネル ポリシーに適用する名前です。*ip* は、ネットワークの IP アドレスです。*netmask* 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	**[no] smart-tunnel network** *network name* **host** *host mask*	*.cisco.com などのホスト名マスクを確立します。
ステップ 4	**[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified}** *network name* **| tunnelall]** または **[no] smart-tunnel tunnel-policy {excludespecified | tunnelspecified}** *network* **name | tunnelall]**	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。*network name* は、トンネリングされるネットワークのリストです。*tunnelall* は、すべてをトンネリング（暗号化）します。*tunnelspecified* は、network name で指定されたネットワークだけをトンネリングします。*excludespecified* は、network name 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
[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* **| tunnelall]** または **[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified}** *network name* **| tunnelall]**	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。*network name* は、トンネリングされるネットワークのリストです。*tunnelall* は、すべてをトンネリング（暗号化）します。tunnelspecified は、network name で指定されたネットワークだけをトンネリングします。excludespecified は、network name 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
ciscoasa(config-webvpn)# [no] smart-tunnel network *network name* **ip** *ip netmask* **ciscoasa(config-webvpn)# [no] smart-tunnel network** *network name* **host** *host mask*	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。 *network name*：トンネル ポリシーを適用するネットワークの名前 *ip address*：ネットワークの IP アドレス *netmask*：ネットワークのネットマスク *host mask*：ホスト名マスク（*.cisco.com など）
例： ciscoasa(config-webvpn)# **smart-tunnel network inventory ip 10.5.2.2** ciscoasa(config-webvpn)# **smart-tunnel network inventory host www.example.com**	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 www.example.com（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）。
ciscoasa(config-group-webvpn)# **smart-tunnel tunnel-policy tunnelspecified inventory**	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。
（オプション） ciscoasa(config-group-webvpn)# **homepage value http://www.example.com** ciscoasa(config-group-webvpn)# h**omepage use-smart-tunnel**	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。
（オプション） ciscoasa(config-webvpn)# **smart-tunnel notification-icon**	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。

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
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。
smart-tunnel auto-sign-on *list* [*use-domain*] [**realm** *realm-string*] [**port** *port-num*]{**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}	サーバ リストに追加する各サーバに対して使用します。 • *list*：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。 • use-domain（オプション）：認証で必要な場合は、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。 • *realm*：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。 • *port*：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。 • *ip :* 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。 • *ip-address*[*netmask*]：自動認証先のホストのサブネットワークを指定します。 • *host*：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。 • *hostname-mask*：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） [**no**] **smart-tunnel auto-sign-on** *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}	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
show running-config webvpn smart-tunnel	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。
config-webvpn	config-webvpn コンフィギュレーション モードに切り替えます。
smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0	サブネット内のすべてのホストを追加し、認証で必要な場合に Windows ドメインをユーザ名に追加します。
（オプション） **no smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0**	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。
no smart-tunnel auto-sign-on HR	ASA 設定からリスト全体を削除します。
smart-tunnel auto-sign-on intranet host *.example.com	ドメイン内のすべてのホストを intranet 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。
no smart-tunnel auto-sign-on intranet host *.example.com	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	**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	**group-policy webvpn** または **username webvpn**	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	**smart-tunnel auto-sign-on enable**	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） [**no**] **smart-tunnel auto-sign-on enable** *list* [**domain** *domain*]	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。 • *list*：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）*domain*：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、**use-domain** キーワードをリスト エントリに入力します。
ステップ 5	**show running-config webvpn smart-tunnel**	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	**smart-tunnel auto-sign-on enable HR**	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	**smart-tunnel auto-sign-on enable HR domain CISCO**	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) **no smart-tunnel auto-sign-on enable HR**	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てもいなくても、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	**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	**group-policy webvpn** または **username webvpn**	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	**smart-tunnel auto-start** *list* 例： hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **smart-tunnel auto-start apps1**	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。*list* は、すでに存在するスマート トンネル リストの名前です。 apps1 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	**show running-config webvpn smart-tunnel**	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) **no smart-tunnel**	**smart-tunnel** 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	**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	**group-policy webvpn** または **username webvpn**	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	**smart-tunnel [enable** *list* **| disable]** 例： hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **smart-tunnel enable apps1**	スマート トンネル アクセスをイネーブルにします。*list* 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。 apps1 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	**show running-config webvpn smart-tunnel**	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) **no smart-tunnel**	**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) **smart-tunnel disable**	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、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。

手順の詳細

	コマンド	目的
ステップ 1	**[no] smart-tunnel notification-icon**	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。 **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。 (注)　このコマンドの no 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。 (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。
ステップ 2	***.webvpn.**	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。

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。

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	**crypto ca import**	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	**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	**rewrite**	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	**disable**	**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。

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	**webvpn** 例： `hostname(config)# webvpn`	クライアントレス SSL VPN コンフィギュレーション モードに入ります。

ステップ 2	**portal-access-rule** *priority* [{**permit** | **deny** [**code** *code*]} {**any** | **user-agent match** *string*}
	
	例：
	`hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*`
	
	`hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match "*my agent*"`
		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。
		
		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。

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。