ポリシー グループ

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

内部サーバ上の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 に関するポリシーを作成して適用するには、グループ ポリシーを割り当てる必要があります。

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。ASA の内部認証サーバ、外部 RADIUS または LDAP サーバを使用して、ユーザをグループ ポリシーに割り当てることができます。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 用接続プロファイルの属性

次の表は、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」が「トンネル グループ」と呼ばれていました。接続プロファイルは、tunnel-group コマンドを使用して設定します。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 *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。

コマンド	機能
secondary-pre-fill-username	このトンネル グループにセカンダリ ユーザ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

次の表に、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。グループ ポリシー属性とユーザ属性の設定手順については、クライアントレス SSL VPN セッションのグループ ポリシー属性の設定 （4 ページ） または 特定ユーザのクライアントレス SSL VPN アクセスの設定 （14 ページ）を参照してください。

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。

コマンド	機能
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。
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。
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。

クライアントレス SSL VPN セッションのグループ ポリシー属性の設定

クライアントレス SSL VPN によって、ユーザは、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。クライアントレス SSL VPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。クライアントレス SSL VPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間のセキュアな接続を提供します。ASA はプロキシする必要がある接続を識別し、HTTP サーバは認証サブシステムと対話してユーザを認証します。デフォルトでは、クライアントレス SSL VPN はディセーブルになっています。

特定の内部グループ ポリシー用のクライアントレス SSL VPN のコンフィギュレーションをカスタマイズできます。

（注） グローバル コンフィギュレーション モードから入る webvpn モードでは、クライアントレス SSL VPN セッションのグローバル設定を構成できます。この項で説明する webvpn モード（グループ ポリシー コンフィギュレーション モードから入ります）を使用すると、クライアントレス SSL VPN セッションに固有のグループ ポリシーのコンフィギュレーションをカスタマイズできます。

グループ ポリシー webvpn コンフィギュレーション モードでは、すべての機能の設定を継承するか、または次のパラメータをカスタマイズするかどうかを指定できます。各パラメータについては、後述の項で説明します。

- customizations
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- auto-signon
- deny message
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

多くの場合、クライアントレス SSL VPN の設定の一部として webvpn 属性を定義した後、グループ ポリシーの webvpn 属性を設定するときにこれらの定義を特定のグループに適用します。グループ ポリシー コンフィギュレーション モードで **webvpn** コマンドを使用して、グループ ポリシー webvpn コンフィギュレーション モードに入ります。グループ ポリシー用の webvpn コマンドは、ファイル、URL、および TCP アプリケーションへのクライアントレス SSL VPN セッション経由のアクセスを定義します。ACL およびフィルタリングするトラフィックのタイプも指定します。クライアントレス SSL VPN は、デフォルトではディセーブルになっています。

グループ ポリシー webvpn コンフィギュレーション モードで入力されたすべてのコマンドを削除するには、このコマンドの **no** 形式を入力します。これらの webvpn コマンドは、設定元のユーザ名またはグループ ポリシーに適用されます。

webvpn

no webvpn

次の例は、FirstGroup というグループ ポリシーのグループ ポリシー webvpn コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

拒否メッセージの指定

グループポリシー webvpn コンフィギュレーション モードで **deny-message** コマンドを入力すると、クライアントレス SSL VPN セッション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できます。

```
hostname(config-group-webvpn)# deny-message value "message"
hostname(config-group-webvpn)# no deny-message value "message"
hostname(config-group-webvpn)# deny-message none
```

no deny-message value コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

no deny-message none コマンドは、接続プロファイル ポリシーのコンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

メッセージは、特殊文字、スペース、および句読点を含む英数字で最大491文字まで指定できますが、囲みの引用符はカウントされません。テキストは、ログイン時にリモートユーザのブラウザに表示されます。**deny-message value** コマンドに文字列を入力するときは、コマンドがラップする場合でも続けて入力します。

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.」

次の例の最初のコマンドは、group2 という名前の内部グループ ポリシーを作成します。後続のコマンドは、そのポリシーに関連付けられている webvpn 拒否メッセージが含まれた属性を変更します。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
 you have not been granted rights to use the VPN features. Contact your administrator
for more information."
hostname(config-group-webvpn)
```

クライアントレス SSL VPN セッションのグループ ポリシー フィルタ属性の設定

webvpn モードで **html-content-filter** コマンドを使用して、このグループ ポリシーのクライアントレス SSL VPN セッションからの Java、ActiveX、イメージ、スクリプト、クッキーをフィルタリングするかどうかを指定します。HTML フィルタリングは、デフォルトでディセーブルです。

コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**none** キーワードを指定して **html-content-filter** コマンドを発行して作成したヌル値を含めて、すべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループポリシーから継承できるようになります。HTML コンテンツ フィルタを継承しないようにするには、**none** キーワードを指定して **html-content-filter** コマンドを入力します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

```
hostname(config-group-webvpn)# html-content-filter {java | images | scripts |
 cookies | none}

hostname(config-group-webvpn)# no html-content-filter [java | images | scripts
 | cookies | none]
```

下記の表に、このコマンドで使用するキーワードの意味を示します。

表 *2 : filter* コマンドのキーワード

キーワード	意味
cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを提供します。
images	イメージへの参照を削除します（<IMG> タグを削除します）。
java	Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および<OBJECT> の <OBJECT>各タグを削除します）。
none	フィルタリングを行わないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
scripts	スクリプティングへの参照を削除します（<SCRIPT> タグを削除します）。 <SCRIPT> tags).

次の例は、FirstGroup という名前のグループ ポリシーに対して JAVA と ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
hostname(config-group-webvpn)#
```

ユーザ ホームページの指定

グループ ポリシー webvpn コンフィギュレーション モードで **homepage** コマンドを使用して、このグループのユーザがログインしたときに表示される Web ページの URL を指定します。デフォルトのホームページはありません。

homepage none コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。ホームページを継承しないようにするには、**homepage none** コマンドを入力します。

none キーワードは、クライアントレス SSL VPN セッションのホームページがないことを示します。これにより、ヌル値が設定されてホームページが拒否され、ホームページが継承されなくなります。

キーワード **value** の後ろの *url-string* 変数で、ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

```
hostname(config-group-webvpn)# homepage {value url-string | none}
hostname(config-group-webvpn)# no homepage
hostname(config-group-webvpn)#
```

自動サインオンの設定

auto-signon コマンドは、クライアントレス SSL VPN セッションのユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のためにログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名がグループに優先し、グループがグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、使用する認証の対象範囲によって異なります。

特定サーバへの特定ユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URI を指定してこのコマンドの **no** 形式を使用します。すべてのサーバに対して認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、グループ ポリシーから値を継承できます。

次の例では、グループ ポリシー webvpn コンフィギュレーション モードで入力し、基本認証を使用して、10.1.1.0 から 10.1.1.255 の範囲の IP アドレスを持つサーバへの anyuser という名前のユーザの自動サインオンを設定します。

次のコマンド例では、基本認証または NTLM 認証を使用して、クライアントレス SSL VPN セッションのユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
```

```
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/*
 auth-type all
hostname(config-group-webvpn)#
```

次のコマンド例では、基本認証または NTLM 認証を使用して、クライアントレス SSL VPN セッションのユーザに対し、サブネット マスク 255.255.255.0 を使用する IP アドレス 10.1.1.0 のサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type all
hostname(config-group-webvpn)#
```

クライアントレス SSL VPN セッション用の ACL の指定

webvpn モードで **filter** コマンドを使用し、このグループ ポリシーまたはユーザ名に対してクライアントレス SSL VPN セッションで使用する ACL の名前を指定します。**filter** コマンドを入力して指定するまで、クライアントレス SSL VPN ACL は適用されません。

filter none コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。フィルタの値を継承しないようにするには、**filter value none** コマンドを入力します。

filter コマンドを入力して指定するまで、クライアントレス SSL VPN セッションの ACL は適用されません。

ACL を設定して、このグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを入力して、これらの ACL をクライアントレス SSL VPN トラフィックに適用します。

```
hostname(config-group-webvpn)# filter {value ACLname | none}
hostname(config-group-webvpn)# no filter
```

none キーワードは、**webvpntype** ACL がないことを示します。これにより、ヌル値が設定されて ACL が拒否され、別のグループ ポリシーから ACL が継承されなくなります。

キーワード **value** の後ろの *ACLname* 文字列で、設定した ACL の名前を指定します。

（注） クライアントレス SSL VPN セッションは、**vpn-filter** コマンドで定義されている ACL を使用しません。

次の例は、FirstGroup という名前のグループ ポリシーで acl_in という ACL を呼び出すフィルタの設定方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
hostname(config-group-webvpn)#
```

URL リストの適用

グループ ポリシーのクライアントレス SSL VPN ホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して、1 つ以上の名前付きリストを作成する必要があります。特定のグループ ポリシーにクライアントレス SSL VPN セッションのサーバと URL のリストを適用して、特定のグループ ポリシーのリスト内にある URL にアクセスできるようにするには、グループ ポリシー webvpn コンフィギュレーション モードで **url-list** コマンドを実行する際に、作成するリスト（複数可）の名前を使用します。デフォルトの URL リストはありません。

url-list none コマンドを使用して作成したヌル値を含めてリストを削除するには**,** このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。URL リストが継承されないようにするには、**url-list none** コマンドを使用します。コマンドを 2 回使用すると、先行する設定が上書きされます。

```
hostname(config-group-webvpn)# url-list {value name | none} [index]
hostname(config-group-webvpn)# no url-list
```

下記の表に、**url-list** コマンドのパラメータとその意味を示します。

表 *3 : url-list* コマンドのキーワードと変数

パラメータ	意味
index	ホームページ上の表示のプライオリティを指定します。
none	URL リストにヌル値を設定します。デフォルトまたは指定したグループ ポリシーからリストが継承されないようにします。
value name	設定済み URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

次の例では、FirstGroup という名前のグループ ポリシーに FirstGroupURLs という URL リストを設定し、これがホームページに表示される最初の URL リストになるように指定します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
```

```
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
hostname(config-group-webvpn)#
```

グループ ポリシーの ActiveX Relay のイネーブル化

ActiveX Relay を使用すると、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 Microsoft Office ドキュメント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。

クライアントレス SSL VPN セッションで ActiveX コントロールをイネーブルまたはディセーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードで次のコマンドを入力します。

activex-relay {**enable** | **disable**}

デフォルト グループ ポリシーから **activex-relay** コマンドを継承するには、次のコマンドを入力します。

no activex-relay

次のコマンドは、特定のグループ ポリシーに関連付けられているクライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

グループ ポリシーに対するクライアントレス SSL VPN セッションでのアプリケーション アクセスのイネーブル化

このグループ ポリシーでアプリケーション アクセスをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート フォワーディングは、デフォルトではディセーブルになっています。

グループ ポリシー webvpn コンフィギュレーション モードで **port-forward** コマンドを入力して、アプリケーション アクセスをイネーブルにする前に、クライアントレス SSL VPN セッションでユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

port-forward none コマンドを発行して作成したヌル値を含めて、グループ ポリシー コンフィギュレーションからポート フォワーディング属性を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、別のグループ ポリシーからリストを継承できようになります。ポート フォワーディング リストを継承しないようにするには、**none** キーワードを指定して **port-forward** コマンドを入力します。**none** キーワードは、フィルタリングが実行されないことを示します。これにより、ヌル値が設定されてフィルタリングが拒否され、フィルタリング値が継承されなくなります。

このコマンドの構文は次のとおりです。

```
hostname(config-group-webvpn)# port-forward {value listname | none}
hostname(config-group-webvpn)# no port-forward
```

キーワード **value** の後ろの *listname* 文字列で、クライアントレス SSL VPN セッションのユーザがアクセスできるアプリケーションのリストを指定します。webvpn コンフィギュレーション モードで port-forward コマンドを入力し、このリストを定義します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

次の例は、FirstGroup という名前の内部グループ ポリシーに ports1 というポート フォワーディング リストを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
hostname(config-group-webvpn)#
```

ポート フォワーディング表示名の設定

グループ ポリシー webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用して、特定のユーザまたはグループ ポリシーでエンド ユーザへの TCP ポート フォワーディングを識別する表示名を設定します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するには**,** このコマンドの **no** 形式を入力します。**no** オプションを指定すると、デフォルト名 Application Access が復元されます。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。このコマンドの構文は次のとおりです。

```
hostname(config-group-webvpn)# port-forward-name {value name | none}
hostname(config-group-webvpn)# no port-forward-name
```

次の例は、FirstGroup という内部グループ ポリシーに Remote Access TCP Applications という名前を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP
Applications
hostname(config-group-webvpn)#
```

セッション タイマー更新時に無視する最大オブジェクト サイズの設定

ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回路が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定サイズ以下のメッセージをすべてキープアライブ メッセージと見なして、セッション タイマーの更新時にトラフィックと見なさないように ASA に指定できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

トランザクションごとに無視する HTTP/HTTPS トラフィックの上限を指定するには、グループ ポリシー属性 webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

このコマンドの**no**形式を使用すると、コンフィギュレーションからこの指定が削除されます。

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

HTTP 圧縮の指定

グループポリシー webvpn モードで http-comp コマンドを入力し、特定のグループまたはユーザに対してクライアントレス SSL VPN セッションを介した HTTP データの圧縮をイネーブルにします。

```
hostname(config-group-webvpn)# http-comp {gzip | none}
hostname(config-group-webvpn)#
```

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-webvpn)# no http-comp {gzip | none}
hostname(config-group-webvpn)#
```

このコマンドの構文は次のとおりです。

- **gzip—**グループまたはユーザに対して圧縮をイネーブルにすることを指定します。これはデフォルト値です。
- **none—**そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

クライアントレス SSL VPN セッションの場合、グローバル コンフィギュレーション モードで設定された **compression** コマンドは、グループ ポリシー webvpn モードやユーザ名 webvpn モードで設定された **http-comp** コマンドよりも優先されます。

次に、グローバル ポリシー sales の圧縮をディセーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
```

```
hostname(config-group-webvpn)#
```

特定ユーザのクライアントレス SSL VPN アクセスの設定

次の各項では、特定のユーザのクライアントレス SSL VPN セッションの設定をカスタマイズする方法について説明します。ユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用して、ユーザ名 webvpn コンフィギュレーション モードを開始します。クライアントレス SSL VPN によって、ユーザは、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。クライアントレス SSL VPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできます。クライアントレス SSL VPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間のセキュアな接続を提供します。ASA はプロキシする必要がある接続を識別し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ユーザ名 webvpn コンフィギュレーション モードのコマンドによって、ファイル、URL、TCP アプリケーションへのクライアントレス SSL VPN セッション経由のアクセスを定義します。ACL およびフィルタリングするトラフィックのタイプも指定します。クライアントレス SSL VPN は、デフォルトではディセーブルになっています。これらの **webvpn** コマンドは、コマンドの設定を行ったユーザ名にのみ適用されます。プロンプトが変化して、ユーザ名 webvpn コンフィギュレーション モードに入ったことがわかります。

```
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

ユーザ名 webvpn コンフィギュレーション モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

```
hostname(config-username)# no webvpn
hostname(config-username)#
```

電子メール プロキシを使用するためにクライアントレス SSL VPN を設定する必要はありません。

（注） グローバル コンフィギュレーション モードから入る webvpn モードでは、クライアントレス SSL VPN セッションのグローバル設定を構成できます。この項で説明した、ユーザ名モードから入ったユーザ名 webvpn コンフィギュレーション モードを使用すると、特定のユーザのクライアントレス SSL VPN セッションのコンフィギュレーションをカスタマイズできます。

ユーザ名 webvpn コンフィギュレーション モードでは、次のパラメータをカスタマイズできます。各パラメータについては、後続の手順で説明します。

- customizations

- deny message
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- auto-signon
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

次の例は、username anyuser attributes に対してユーザ名 webvpn コンフィギュレーション モードを開始する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

HTML からフィルタリングするコンテンツとオブジェクトの指定

このユーザのクライアントレス SSL VPN セッションの Java、ActiveX、イメージ、スクリプト、クッキーをフィルタリングするには、ユーザ名 webvpn コンフィギュレーション モードで **html-content-filter** コマンドを入力します。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を入力します。**html-content-filter none** コマンドを発行して作成したヌル値を含めて、すべてのコンテンツ フィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプションを使用すると、グループ ポリシーから値を継承できます。HTML コンテンツ フィルタを継承しないようにするには、html-**html-content-filter none** コマンドを入力します。HTML フィルタリングは、デフォルトでディセーブルです。

次回このコマンドを使用すると、前回までの設定が上書きされます。

```
hostname(config-username-webvpn)# html-content-filter {java | images | scripts
 | cookies | none}

hostname(config-username-webvpn)# no html-content-filter [java | images | scripts
 | cookies | none]
```

このコマンドで使用するキーワードは、次のとおりです。

- **cookies**—イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを提供します。
- **images**—イメージへの参照を削除します（<IMG> タグを削除します）。

- **java—**Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> の <OBJECT>各タグを削除します）。
- **none—**フィルタリングを行わないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
- **scripts**：スクリプティングへの参照を削除します（<SCRIPT> タグを削除します）。 <SCRIPT> tags).

次の例は、anyuser という名前のユーザに、Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# html-content-filter java cookies images
hostname(config-username-webvpn)#
```

ユーザ ホームページの指定

このユーザがクライアントレス SSL VPN セッションにログインしたときに表示される Web ページの URL を指定するには、ユーザ名 webvpn コンフィギュレーション モードで **homepage** コマンドを入力します。**homepage none** コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、グループ ポリシーから値を継承できます。ホームページを継承しないようにするには、**homepage none** コマンドを入力します。

none キーワードは、クライアントレス SSL VPN ホームページがないことを示します。これにより、ヌル値が設定されてホームページが拒否され、ホームページが継承されなくなります。

キーワード **value** の後ろの *url-string* 変数で、ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

デフォルトのホームページはありません。

```
hostname(config-username-webvpn)# homepage {value url-string | none}
hostname(config-username-webvpn)# no homepage
hostname(config-username-webvpn)#
```

次の例は、anyuser という名前のユーザのホームページとして www.example.com を指定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# homepage value www.example.com
hostname(config-username-webvpn)#
```

拒否メッセージの指定

ユーザ名 webvpn コンフィギュレーション モードで **deny-message** コマンドを入力すると、クライアントレス SSL VPN セッション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できます。

```
hostname(config-username-webvpn)# deny-message value "message"
hostname(config-username-webvpn)# no deny-message value "message"
hostname(config-username-webvpn)# deny-message none
```

no deny-message value コマンドは、リモート ユーザがメッセージを受信しないように、メッセージ文字列を削除します。

no deny-message none コマンドは、接続プロファイル ポリシーのコンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

メッセージは、特殊文字、スペース、および句読点を含む英数字で最大491 文字まで指定できますが、囲みの引用符はカウントされません。テキストは、ログイン時にリモートユーザのブラウザに表示されます。**deny-message value** コマンドに文字列を入力するときは、コマンドがラップする場合でも続けて入力します。

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.」

次の例の最初のコマンドは、ユーザ名モードに入り、anyuser という名前のユーザに属性を設定します。後続のコマンドは、ユーザ名 webvpn コンフィギュレーション モードに入り、そのユーザに関連付けられている拒否メッセージを変更します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# deny-message value "Your login credentials are OK.
However, you have not been granted rights to use the VPN features. Contact your
administrator for more information."
hostname(config-username-webvpn)
```

URL リストの適用

クライアントレス SSL VPN セッションを確立したユーザのホームページに URL のリストを表示するように指定できます。最初に、グローバル コンフィギュレーション モードで **url-list** コマンドを入力して、1 つ以上の名前付きリストを作成する必要があります。クライアントレス SSL VPN の特定のユーザにサーバと URL のリストを適用するには、ユーザ名 webvpn コンフィギュレーション モードで **url-list** コマンドを入力します。

url-list none コマンドを使用して作成したヌル値を含めてリストを削除するには**,** このコマンドの **no** 形式を入力します。**no** オプションを使用すると、グループ ポリシーから値を継承できます。URL リストが継承されないようにするには、**url-list none** コマンドを入力します。

```
hostname(config-username-webvpn)# url-list {listname displayname url | none}
hostname(config-username-webvpn)# no url-list
```

このコマンドで使用するキーワードと変数は、次のとおりです。

- *displayname*：URL の名前を指定します。この名前は、クライアントレス SSL VPN セッションのポータル ページに表示されます。
- listname：URL をグループ化する名前を指定します。
- **none**：URL のリストが存在しないことを示します。ヌル値を設定して、URL リストを拒否します。URL リストの値を継承しないようにします。
- *url*：クライアントレス SSL VPN のユーザがアクセスできる URL を指定します。

デフォルトの URL リストはありません。

次回このコマンドを使用すると、前回までの設定が上書きされます。

次の例は、anyuser という名前のユーザに AnyuserURLs という URL リストを設定する方法を示しています。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# url-list value AnyuserURLs
hostname(config-username-webvpn)#
```

ユーザの ActiveX Relay のイネーブル化

ActiveX Relay を使用すると、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 Microsoft Office ドキュメント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。

クライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルまたはディセーブルにするには、ユーザ名 webvpn コンフィギュレーション モードで次のコマンドを入力します。

activex-relay {enable | disable}

グループ ポリシーから **activex-relay** コマンドを継承するには、次のコマンドを入力します。

no activex-relay

次のコマンドは、特定のユーザ名に関連付けられているクライアントレス SSL VPN セッションの ActiveX コントロールをイネーブルにします。

```
hostname(config-username-policy)# webvpn
hostname(config-username-webvpn)# activex-relay enable
hostname(config-username-webvpn)
```

クライアントレス SSL VPN セッションでのアプリケーション アクセスのイネーブル化

このユーザのアプリケーション アクセスをイネーブルにするには、ユーザ名 webvpn コンフィギュレーション モードで **port-forward** コマンドを入力します。ポート フォワーディングは、デフォルトではディセーブルになっています。

port-forward none コマンドを発行して作成したヌル値を含めて、コンフィギュレーションからポート フォワーディング属性を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、グループ ポリシーからリストを継承できるようになります。フィルタリングを拒否してポート フォワーディング リストを継承しないようにするには、**none** キーワードを指定して **port-forward** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward {value listname | none}
hostname(config-username-webvpn)# no port-forward
hostname(config-username-webvpn)#
```

キーワード **value** の後ろの *listname* 文字列で、クライアントレス SSL VPN のユーザがアクセスできるアプリケーションのリストを指定します。コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

ユーザ名 webvpn コンフィギュレーション モードで **port-forward** コマンドを入力して、アプリケーション アクセスをイネーブルにする前に、クライアントレス SSL VPN セッションでユーザが使用できるアプリケーションのリストを定義する必要があります。グローバル コンフィギュレーション モードで **port-forward** コマンドを入力して、このリストを定義します。

次の例は、ports1 というポート フォワーディング リストを設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward value ports1
hostname(config-username-webvpn)#
```

ポート フォワーディング表示名の設定

ユーザ名 webvpn コンフィギュレーション モードで **port-forward-name** コマンドを使用し、特定のユーザ用にエンド ユーザへの TCP ポート フォワーディングを識別する表示名を設定します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するには**,** このコマンドの **no** 形式を入力します。**no** オプションを指定すると、デフォルト名 Application Access が復元されます。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。

```
hostname(config-username-webvpn)# port-forward-name {value name | none}
hostname(config-username-webvpn)# no port-forward-name
```

次の例は、ポート転送名 test を設定する方法を示しています。

```
hostname(config-group-policy)# webvpn
```

```
hostname(config-username-webvpn)# port-forward-name value test
hostname(config-username-webvpn)#
```

セッション タイマー更新時に無視する最大オブジェクト サイズの設定

ネットワーク デバイスは、短いキープアライブ メッセージを交換して、デバイス間の仮想回路が引き続きアクティブであることを確認します。これらのメッセージの長さは異なる可能性があります。**keep-alive-ignore** コマンドを使用すると、指定サイズ以下のメッセージをすべてキープアライブ メッセージと見なして、セッション タイマーの更新時にトラフィックと見なさないように ASA に指定できます。範囲は 0 ～ 900 KB です。デフォルトは 4 KB です。

トランザクションごとに無視する HTTP/HTTPS トラフィックの上限を指定するには、グループ ポリシー属性 webvpn コンフィギュレーション モードで **keep-alive-ignore** コマンドを使用します。

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

このコマンドの**no**形式を使用すると、コンフィギュレーションからこの指定が削除されます。

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

次の例では、無視するオブジェクトの最大サイズを 5 KB に設定します。

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

自動サインオンの設定

NTLM、基本 HTTP 認証、またはその両方を使用する内部サーバに、クライアントレス SSL VPN の特定ユーザのログイン クレデンシャルを自動的に渡すには、ユーザ名 webvpn コンフィギュレーション モードで **auto-signon** コマンドを使用します。

auto-signon コマンドは、クライアントレス SSL VPN セッションのユーザ用のシングル サインオン方式です。NTLM 認証、基本認証、またはその両方を使用する認証のためにログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

自動サインオン機能は、webvpn コンフィギュレーション、webvpn グループ コンフィギュレーション、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。ユーザ名がグループに優先し、グループがグローバルに優先するという標準的な優先動作が適用されます。選択するモードは、使用する認証の対象範囲によって異なります。

特定サーバへの特定ユーザの自動サインオンをディセーブルにするには、元の IP ブロックまたは URI を指定してこのコマンドの **no** 形式を使用します。すべてのサーバに対して認証をディセーブルにするには、引数を指定しないで **no** 形式を使用します。**no** オプションを使用すると、グループ ポリシーから値を継承できます。

次のコマンド例では、基本認証または NTLM 認証を使用して、anyuser という名前のクライアントレス SSL VPN のユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow uri https://*.example.com/*
 auth-type all
```

次のコマンド例では、サブネット マスク 255.255.255.0 を使用して、anyuser という名前のクライアントレス SSL VPN のユーザに対し、IP アドレス 10.1.1.0 を持つサーバへの基本認証または NTLM 認証による自動サインオンを設定します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
 auth-type all
hostname(config-username-webvpn)#
```

HTTP 圧縮の指定

ユーザ名 webvpn コンフィギュレーション モードで http-comp コマンドを入力し、特定のユーザに対してクライアントレス SSL VPN セッションを介した HTTP データの圧縮をイネーブルにします。

```
hostname(config-username-webvpn)# http-comp {gzip | none}
hostname(config-username-webvpn)#
```

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-username-webvpn)# no http-comp {gzip | none}
hostname(config-username-webvpn)#
```

このコマンドの構文は次のとおりです。

- **gzip—**グループまたはユーザに対して圧縮をイネーブルにすることを指定します。これはデフォルト値です。
- **none—**そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

クライアントレス SSL VPN セッションの場合、グローバル コンフィギュレーション モードで設定された **compression** コマンドは、グループ ポリシー webvpn モードやユーザ名 webvpn モードで設定された **http-comp** コマンドよりも優先されます。

次の例は、testuser というユーザ名で圧縮をディセーブルにしています。

```
hostname(config)# username testuser internal
hostname(config)# username testuser attributes
```

```
hostname(config-username)# webvpn
hostname(config-username-webvpn)# http-comp none
hostname(config-username-webvpn)#
```

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

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ウェイ、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。

  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。
- 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、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。
- 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）。
  - 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）。

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。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。

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、これらのコマンドを一度に1つだけサポートします。そのため、1つのコマンドが入力されると、ASAは、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と置き換えます。最後のコマンドの場合は、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 コマンドが削除されるだけです。

- **smart-tunnel auto-start** *list*

  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。

- **smart-tunnel enable** リスト

  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。

- **smart-tunnel disable**

  スマート トンネル アクセスを禁止します。

- **no smart-tunnel [auto-start list | enable list | disable]**

  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

ステップ 1 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。

webvpn

ステップ 2 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。

[no] smart-tunnel network *network name* **ip** *ip netmask*

- *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。

ステップ 3 *.cisco.com などのホスト名マスクを確立します。

[no] smart-tunnel network *network name* **host** *host mask*

ステップ 4 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。

[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* **| tunnelall]**

- *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、ネットワーク名で指定されたネットワークだけをトンネリングする。
- *excludespecified* は、ネットワーク名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する。

スマート トンネル トンネルポリシーの設定と適用

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。

手順

ステップ 1 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。

[no]smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* | *tunnelall]*

- *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、ネットワーク名で指定されたネットワークだけをトンネリングする。
- **excludespecified** は、ネットワーク名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する。

ステップ 2 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。

[no] smart-tunnel network *network name* **ip** *ip netmask*

または

[no] smart-tunnel network *network name* **host** *host mask*

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 つだけ使用してください。

- *network name* は、トンネル ポリシーを適用するネットワークの名前を指定します。
- *ip address* は、ネットワークの IP アドレスを指定します。
- *netmask* は、ネットワークのネットマスクを指定します。
- *host mask* は、ホスト名マスク（*.cisco.com など）を指定します。

例：

例：

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-webvpn)# smart-tunnel network inventory ip 10.5.2.2
or
ciscoasa(config-webvpn)# smart-tunnel network inventory host www.example.com
```

ステップ 3 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。

ciscoasa(config-group-webvpn)# **smart-tunnel tunnel-policy tunnelspecified inventory**

ステップ 4 （任意） 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。

例：

例：

```
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
ciscoasa(config-webvpn)# smart-tunnel notification-icon
```

（注） 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。

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。

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

手順

ステップ 1 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。

webvpn

ステップ 2 サーバ リストに追加する各サーバに対して使用します。

smart-tunnel auto-sign-on *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*]{**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

- *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（任意）：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。

ステップ 3 （任意） 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。

no smart-tunnel auto-sign-on *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*]{**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

ステップ 4 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。

show running-config webvpn smart-tunnel

ステップ 5 config-webvpn コンフィギュレーション モードに切り替えます。

config-webvpn

ステップ 6 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。

smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0

ステップ 7 （任意）削除す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 use-domain ip 93.184.216.119 255.255.255.0

ステップ 8 ASA 設定からリスト全体を削除します。

no smart-tunnel auto-sign-on HR

ステップ 9 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。

smart-tunnel auto-sign-on intranet host *.example.com

ステップ 10 リストからエントリを削除します。

no smart-tunnel auto-sign-on intranet host *.example.com

（注） スマート トンネル自動サインオン サーバ リストを設定した後、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 ポリシーにリストを割り当てる必要があります。詳細については、を参照してください。 スマート トンネル自動サインオン サーバ リストへのサーバの追加 （31 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

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。

始める前に

- **smart-tunnel auto-sign-on** リスト コマンドを使用して、最初にサーバのリストを作成します。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。

（注） 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 を使用している場合は、正確なホスト名または IP アドレスを使用してホストが指定されていることを確認します（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

ステップ 1 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。

webvpn

ステップ 2 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。

group-policy webvpn

ステップ 3 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。

username webvpn

ステップ 4 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。

smart-tunnel auto-sign-on enable

ステップ 5 （任意） 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、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。

[**no**] **smart-tunnel auto-sign-on enable** *list* [**domain** *domain*]

- *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。
- （任意）*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 6 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。

show running-config webvpn smart-tunnel

ステップ 7 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。

smart-tunnel auto-sign-on enable HR

ステップ 8 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。

smart-tunnel auto-sign-on enable HR domain CISCO

ステップ 9 （任意） 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。

no smart-tunnel auto-sign-on enable HR

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、次の手順を実行します。

始める前に

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します。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

group-policy webvpn

ステップ 3 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。

username webvpn

ステップ 4 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。

smart-tunnel auto-start *list*

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。

例：

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-start apps1
```

これにより、apps1 という名前のスマート トンネル リストがグループ ポリシーに割り当てられます。

ステップ 5 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。

show running-config webvpn smart-tunnel

ステップ 6 グループ ポリシーまたはユーザ名から smart-tunnel コマンドを削除し、デフォルトに戻します。

no smart-tunnel

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

ステップ 1 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。

webvpn

ステップ 2 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。

group-policy webvpn

ステップ 3 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。

username webvpn

ステップ 4 スマート トンネル アクセスをイネーブルにします。

smart-tunnel [enable *list* **| disable]**

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。

例：

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel enable apps1
```

この例では、apps1 という名前のスマート トンネル リストがグループ ポリシーに割り当てられます。

ステップ 5 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。

show running-config webvpn smart-tunnel

ステップ 6 グループ ポリシーまたはローカル ユーザ ポリシーから smart-tunnel コマンドを削除し、デフォルトのグループ ポリシーに戻します。

no smart-tunnel

ステップ 7 スマート トンネル アクセスをオフに切り替えます。

smart-tunnel disable

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。

手順

ステップ 1 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。

[no] smart-tunnel notification-icon

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。

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。

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 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。

***.webvpn.**

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。

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。

始める前に

ASA にログオンし、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 によって `hostname(config)#` プロンプトが表示されます。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

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*"
```

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。

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。

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 エンジンを介し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。

リライト済み Java コンテンツの署名用証明書の設定

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

ステップ 1 証明書をインポートします。

crypto ca import

ステップ 2 証明書を採用します。

ava-trustpoint

例：

```
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
```

この例では、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 リライトのオフへの切り替え

一部のアプリケーションや Web リソース（公開 Web サイトなど）が ASA を通過しないようにしたい場合があります。そのような場合、ASA では、ASA を通過せずに特定のサイトやアプリケーションをブラウズできるようにするリライト 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。

手順

ステップ 1 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。

webvpn

ステップ 2 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。

rewrite

このコマンドは複数回使用できます。

ステップ 3 rewrite コマンドとともに使用します。

disable

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

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。

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

ステップ 1 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。

webvpn

ステップ 2 プロキシ バイパスを設定します。

proxy-bypass