基本的なクライアントレス SSL VPN のコンフィギュレーション

改訂日：2014 年 3 月 12 日

クライアントレス SSL VPN セキュリティ対策

デフォルトでは、ASA はすべての Web リソース（HTTPS、CIFS、RDP、プラグインなど）に対するすべてのポータル トラフィックを許可します。クライアントレス SSL VPN は、ASA だけに意味のあるものに各 URL をリライトします。ユーザは、要求した Web サイトに接続されていることを確認するために、この URL を使用できません。フィッシング Web サイトからの危険にユーザがさらされるのを防ぐには、クライアントレス アクセスに設定しているポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に Web ACL を割り当ててポータルからのトラフィック フローを制御します。これらのポリシーの URL エントリをオフに切り替えて、何にアクセスできるかについてユーザが混乱しないようにすることをお勧めします。

図 14-1　　ユーザが入力した URL の例

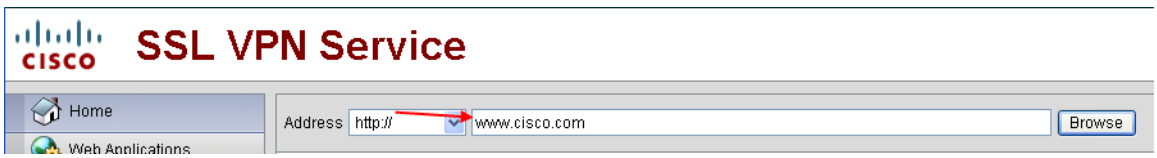
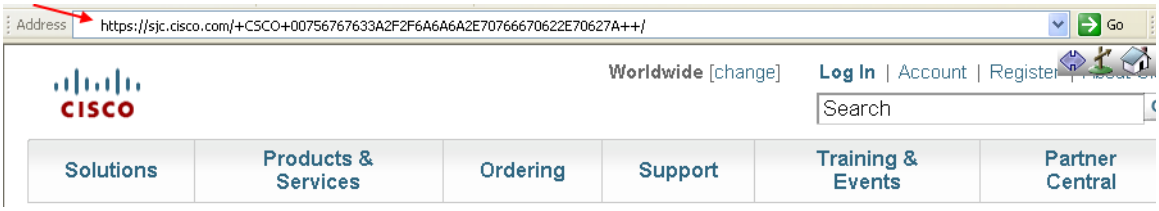


図 14-2　セキュリティ アプライアンスによって書き換えられ、ブラウザ ウィンドウに表示された同じ URL



ポータル ページでの URL エントリのオフへの切り替え

ユーザがブラウザ ベースの接続を確立したときにポータル ページが開きます。

前提条件

クライアントレス SSL VPN アクセスを必要とするすべてのユーザのグループ ポリシーを設定し、そのグループ ポリシーに対してだけクライアントレス SSL VPN をイネーブルにします。

手順の詳細

	コマンド	目的
ステップ 1	`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。
ステップ 2	`url-entry`	ユーザが HTTP/HTTPS URL を入力する機能を制御します。
ステップ 3	（オプション）`url-entry disable`	URL エントリをオフに切り替えます。

クライアントレス SSL VPN サーバ証明書の確認

クライアントレス SSL VPN 経由でリモート SSL 対応サーバに接続する場合は、リモート サーバを信頼できること、また、接続先が実際にサーバであることを認識することが重要です。ASA 9.0 には、クライアントレス SSL VPN の信頼できる認証局（CA）証明書のリストに対する SSL サーバ証明書の検証のためのサポートが追加されています。

HTTPS プロトコルを使用して Web ブラウザ経由でリモート サーバに接続する場合、サーバはサーバ自体を識別するために認証局（CA）が署名したデジタル証明書を提供します。Web ブラウザには、サーバ証明書の有効性を検証するために使用される一連の CA 証明書が含まれています。これは、公開キー インフラストラクチャ（PKI）の 1 つの形式です。

ASA は信頼できるプール証明書の管理機能を trustpool の形式で提供します。これは、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には Web ブラウザに備わっているものと同様のデフォルトの一連の証明書が含まれています。**`crypto ca import default`** コマンドを発行して、管理者が実行するまでは動作しません。

（注）　ASA trustpool は Cisco IOS trustpool と似ていますが、同じではありません。

プラグインへのブラウザ アクセスの設定

次の項では、クライアントレス SSL VPN のブラウザ アクセス用のブラウザ プラグインの統合について説明します。

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。ASA により、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

プラグインをフラッシュ デバイスにインストールすると、ASA は次の処理を実行します。

- （シスコが配布したプラグインのみ）URL で指定した jar ファイルを解凍する。
- ASA ファイル システムにファイルを書き込む。
- ASDM の URL 属性の横にあるドロップダウン リストに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、メイン メニュー オプションと、ポータル ページの [Address] フィールドの横にあるドロップダウン リストについてのオプションを追加します。

表 14-1 に、次の項で説明するプラグインを追加したときの、ポータル ページのメイン メニューと [Address] フィールドの変更点を示します。

表 14-1　クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
ica	Citrix MetaFrame Services	ica://
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	Secure Shell	ssh://
	Telnet services（v1 および v2 をサポート）	telnet://
vnc	Virtual Network Computing services	vnc://

* 推奨されないプラグイン。

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン リストに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

プラグインは、シングル サインオン（SSO）をサポートします。実装の詳細については、「HTTP Form プロトコルを使用した SSO の設定」（P.18-12）を参照してください。

前提条件

- プラグインへのリモート アクセスを提供するには、ASA でクライアントレス SSL VPN をイネーブルにする必要があります。
- プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマーク エントリを追加します。また、ブックマークを追加するときに、SSO サポートを指定します。
- リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。
- プラグインには、ActiveX または Oracle Java ランタイム環境（JRE）が必要です。バージョン要件については、「compatibility matrix」を参照してください。

制限

（注）　Remote Desktop Protocol プラグインでは、セッション ブローカを使用したロード バランシングはサポートされていません。プロトコルによるセッション ブローカからのリダイレクションの処理方法のため、接続に失敗します。セッション ブローカが使用されていない場合、プラグインは動作します。

- プラグインは、シングル サインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを開くときに入力したクレデンシャルと*同じ*クレデンシャルを使用します。プラグインはマクロ置換をサポートしないため、内部ドメイン パスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。
- ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。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。
- ステートフル フェールオーバーではなくステートレス フェールオーバーを使用する場合は、ブックマーク、カスタマイゼーション、ダイナミック アクセス ポリシーなどのクライアントレス機能はフェールオーバー ASA ペア間で同期されません。フェールオーバーの発生時に、これらの機能は動作しません。

プラグインのためのセキュリティ アプライアンスの準備

プラグインをインストールする前に、ASA で次のような準備を行います。

前提条件

クライアントレス SSL VPN が ASA インターフェイスでイネーブルになっていることを確認します。

制限

SSL 証明書の一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、ASA と通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

手順の詳細

	コマンド	目的
ステップ 1	`show running-config`	クライアントレス SSL VPN が ASA でイネーブルかどうかを示します。
ステップ 2	ASA インターフェイスに SSL 証明書をインストールします。	リモート ユーザ接続の完全修飾ドメイン名（FQDN）を指定します。

クライアントレス SSL VPN アクセスに提供するプラグインのタイプを指定する項に進んでください。

- 「シスコによって再配布されたプラグインのインストール」（P.14-5）
- 「Citrix XenApp Server へのアクセスの提供」（P.14-7）

シスコによって再配布されたプラグインのインストール

シスコでは、Java ベースのオープン ソース コンポーネントを再配布しています。これは、クライアントレス SSL VPN セッションで Web ブラウザのプラグインとしてアクセスされるコンポーネントで、次のものがあります。

前提条件

ASA のインターフェイス上でクライアントレス SSL VPN がイネーブルになっていることを確認します。そのためには、**show running-config** コマンドを入力します。

表 14-2　シスコが再配布しているプラグイン

プロトコル	説明	再配布しているプラグインのソース *
RDP	Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。 リモート デスクトップ ActiveX コントロールをサポートします。 RDP および RDP2 の両方をサポートするこのプラグインを使用することをお勧めします。RDP および RDP2 の 5.1 までのバージョンのみがサポートされています。バージョン 5.2 以降はサポートされていません。	http://properjavardp.sourceforge.net/
RDP2	Windows Vista および Windows 2003 R2 でホストされる Microsoft Terminal Services にアクセスします。 リモート デスクトップ ActiveX コントロールをサポートします。 （注）　この古いプラグインは、RDP2 だけをサポートします。このプラグインを使用することは推奨しません。代わりに、上記の RDP プラグインを使用してください。	http://properjavardp.sourceforge.net/

表 14-2　シスコが再配布しているプラグイン

プロトコル	説明	再配布しているプラグインのソース *
SSH	Secure Shell-Telnet プラグインにより、リモート ユーザはリモート コンピュータへの Secure Shell（v1 または v2）または Telnet 接続を確立できます。 （注）　キーボード インタラクティブ認証は JavaSSH ではサポートされていないため、（異なる認証メカニズムの実装に使用される）SSH プラグインではサポートされません。	http://javassh.org/
VNC	Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有（VNC サーバまたはサービスとも呼ばれる）をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。このバージョンでは、テキストのデフォルトの色が変更されています。また、フランス語と日本語のヘルプ ファイルもアップデートされています。	http://www.tightvnc.com/

*展開の設定と制限については、プラグインのマニュアルを参照してください。

これらのプラグインは、「Cisco Adaptive Security Appliance Software Download」サイトで入手できます。

手順の詳細

（注）　ASA は、**import webvpn plug-in protocol** コマンドをコンフィギュレーションに保持しません。その代わりに、csco-config/97/plugin ディレクトリの内容を自動的にロードします。セカンダリ ASA は、プライマリ ASA からプラグインを取得します。

	コマンド	目的

ステップ 1	**import webvpn plug-in** *protocol* [**rdp** | **rdp2** | [**ssh** | **telnet**] | **vnc**] *URL*
	
	例：
	`hostname#` **`import webvpn plug-in protocol ssh,telnet tftp://local_tftp_server/plugins/ssh-plugin.jar`**
	
	`Accessing tftp://local_tftp_server/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`Writing file disk0:/csco_config/97/plugin/ssh...`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`238510 bytes copied in 3.650 secs (79503 bytes/sec)`
		ASA のフラッシュ デバイスにプラグインをインストールします。*protocol* は次のいずれかの値になります。**ssh**、**telnet** は、セキュア シェル サービスと Telnet サービスの*両方*へのプラグイン アクセスを提供します。
		（注）　SSH 用と Telnet 用にこのコマンドをそれぞれ入力しないでください。ssh,telnet ストリングを入力する場合は、両者の間にスペースは挿入しません。
		
		URL は、プラグイン .jar ファイルへのリモート パスです。TFTP または FTP サーバのホスト名またはアドレス、およびプラグインへのパスを入力します。

	コマンド	目的
ステップ 2	（オプション） **revert webvpn plug-in protocol** *protocol* 例： hostname# **revert webvpn plug-in protocol rdp**	プラグインに対するクライアントレス SSL VPN のサポートをオフに切り替えて削除し、ASA のフラッシュ デバイスからも削除します。

Citrix XenApp Server へのアクセスの提供

サードパーティのプラグインに、クライアントレス SSL VPN ブラウザ アクセスを提供する方法の例として、この項では、Citrix XenApp Server Client にクライアントレス SSL VPN のサポートを追加する方法について説明します。

ASA に Citrix プラグインがインストールされている場合、クライアントレス SSL VPN ユーザは、ASA への接続を使用して、Citrix XenApp サービスにアクセスできます。

ステートフル フェールオーバーでは、Citrix プラグインを使用して確立したセッションは保持されません。Citrix のユーザは、フェールオーバー後に再認証を行う必要があります。

Citrix プラグインへのアクセスを提供するには、次の項で説明する手順に従ってください。

- クライアントレス SSL VPN アクセスのための Citrix XenApp Server の準備
- Citrix プラグインの作成とインストール

クライアントレス SSL VPN アクセスのための Citrix XenApp Server の準備

（Citrix）「セキュア ゲートウェイ」を使用しないモードで動作するように、Citrix Web Interface ソフトウェアを設定する必要があります。この設定をしないと、Citrix クライアントは Citrix XenApp Server に接続できません。

（注）　プラグインに対するサポートをまだ提供していない場合は、「プラグインのためのセキュリティ アプライアンスの準備」（P.14-4）の説明に従い作業を行った後に、この項を参照してください。

Citrix プラグインの作成とインストール

手順の詳細

ステップ 1　シスコのソフトウェア ダウンロード Web サイトから ica-plugin.zip ファイルをダウンロードします。

このファイルには、Citrix プラグインを使用するためにシスコがカスタマイズしたファイルが含まれています。

ステップ 2　Citrix のサイトから Citrix Java クライアントをダウンロードします。

Citrix Web サイトのダウンロード領域で **[Citrix Receiver]** と **[Receiver for Other Platforms]** を選択し、**[Find]** をクリックします。**[Receiver for Java]** ハイパーリンクをクリックしアーカイブをダウンロードします。

ステップ 3　アーカイブから次のファイルを抽出し、それらを ica-plugin.zip ファイルに追加します。

- JICA-configN.jar
- JICAEngN.jar

ステップ 4　Citrix Java クライアントに含まれている EULA によって、Web サーバ上にクライアントを配置するための権限が与えられていることを確認します。

ステップ 5　ASDM を使用するか、または特権 EXEC モードで次の CLI コマンドを入力して、プラグインをインストールします。

import webvpn plug-in protocol ica *URL*

URL はホスト名または IP アドレス、および ica-plugin.zip ファイルへのパスです。

（注）　Citrix セッションに SSO サポートを提供する場合は、ブックマークの追加は必須です。次のように、ブックマークで便利な表示を提供する URL パラメータを使用することを推奨します。

ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

ステップ 6　SSL VPN クライアントレス セッションを確立し、ブックマークをクリックするか、Citrix サーバの URL を入力します。

必要に応じて、『Client for Java Administrator's Guide』を参照してください。

セキュリティ アプライアンスにインストールされているプラグインの表示

手順の詳細

	コマンド	目的
ステップ 1	**show import webvpn plug-in** **例：** hostname# **show import webvpn plug** ssh rdp vnc ica	クライアントレス SSL VPN のユーザが使用できる Java ベースのクライアント アプリケーションを一覧表示します。
ステップ 2	**show import webvpn plug detail** **例：** hostname **show import webvpn plug** post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tues, 29 Apr 2008 19:57:03 GMT rdp fHeyReIOUwDCgAL9HdTs PnjdBoo= Tues, 15 Sep 2009 23:23:56 GMT rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT	プラグインのハッシュおよび日付を含めます。

ポート転送の設定

次の項では、ポート転送とその設定方法について説明します。

ポート転送に関する情報

ポート転送により、ユーザはクライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションにアクセスできます。TCP ベースのアプリケーションには次のようなものがあります。

- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP（FTP over SSH）
- SSH
- Telnet
- Windows Terminal Service
- XDDTS

その他の TCP ベースのアプリケーションも動作する可能性はありますが、シスコではテストを行っていません。UDP を使用するプロトコルは動作しません。

ポート転送は、クライアントレス SSL VPN 接続を介して TCP ベースのアプリケーションをサポートするためのレガシー テクノロジーです。ポート転送テクノロジーをサポートする設定を事前に構築している場合は、ポート転送の使用を選択することもできます。

ポート転送の代替方法として次のことを検討してください。

- スマート トンネル アクセスを使用すると、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。
- ポート転送およびスマート トンネル アクセスとは異なり、プラグインでは、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ありません。

ASA でポート転送を設定する場合は、アプリケーションが使用するポートを指定します。スマート トンネル アクセスを設定する場合は、実行ファイルまたはそのパスの名前を指定します。

前提条件

- リモート ホストで、次のいずれかの 32 ビット バージョンが実行されている必要があります。
  - Microsoft Windows Vista、Windows XP SP2 または SP3、または Windows 2000 SP4
  - Apple Mac OS X 10.4 または 10.5 と Safari 2.0.4(419.3)
  - Fedora Core 4
- また、リモート ホストで Oracle Java ランタイム環境（JRE）5 以降が動作している必要もあります。
- Mac OS X 10.5.3 上の Safari のブラウザベースのユーザは、Safari での URL の解釈方法に従って、使用するクライアント証明書を、1 回目は末尾にスラッシュを含め、もう 1 回はスラッシュを含めずに、ASA の URL を使用して指定する必要があります。次に例を示します。
  - https://example.com/
  - https://example.com

  詳細については、『Safari, Mac OS X 10.5.3: Changes in client certificate authentication』を参照してください。
- ポート転送またはスマート トンネルを使用する Microsoft Windows Vista 以降のユーザは、ASA の URL を信頼済みサイト ゾーンに追加する。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動し、**[Tools] > [Internet Options] > [Security]** タブを選択する必要があります。Vista（以降の）ユーザは保護モードをオフに切り替えるとスマート トンネル アクセスを使用することもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法の使用はお勧めしません。
- ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートするために、リモート コンピュータに Oracle Java ランタイム環境（JRE）1.5.x 以降がインストールされていることを確認します。JRE 1.4.x が実行中で、ユーザがデジタル証明書で認証される場合、JRE が Web ブラウザの証明書ストアにアクセスできないため、アプリケーションは起動しません。

制限

- ポート転送は、スタティック TCP ポートを使用する TCP アプリケーションのみをサポートしています。ダイナミック ポートまたは複数の TCP ポートを使用するアプリケーションはサポートしていません。たとえば、ポート 22 を使用する SecureFTP は、クライアントレス SSL VPN のポート転送を介して動作しますが、ポート 20 と 21 を使用する標準 FTP は動作しません。
- ポート転送は、UDP を使用するプロトコルをサポートしていません。
- ポート転送は Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。しかし、Microsoft Outlook Exchange Server と連携することにより、Microsoft Office Outlook のスマート トンネル サポートを設定することができます。
- ステートフル フェールオーバーでは、Application Access（ポート転送またはスマート トンネル アクセス）を使用して確立したセッションは保持されません。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。
- ポート転送は、携帯情報端末（PDA）への接続はサポートしていません。
- ポート転送を使用するには、Java アプレットをダウンロードしてローカル クライアントを設定する必要があります。これには、ローカル システムに対する管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

Java アプレットは、エンド ユーザの HTML インターフェイスにあるアプレット独自のウィンドウに表示されます。このウィンドウには、ユーザが使用できる転送ポートのリストの内容、アクティブなポート、および送受信されたトラフィック量（バイト単位）が表示されます。

- ローカル IP アドレス 127.0.0.1 が使用されており、ASA からのクライアントレス SSL VPN 接続によって更新できない場合、ポート転送アプレットはローカル ポートとリモート ポートを同一として表示します。その結果、ASA は、127.0.0.2、127.0.0.3 など、ローカル プロキシ ID の新しい IP アドレスを作成します。hosts ファイルを変更して異なるループバックを使用できるため、リモート ポートはアプレットでローカル ポートとして使用されます。接続するには、ポートを指定せずにホスト名を指定して Telnet を使用します。正しいローカル IP アドレスをローカル ホスト ファイルで使用できます。

ポート転送用の DNS の設定

ポート転送では、リモート サーバのドメイン名またはその IP アドレスを ASA に転送して、解決および接続を行います。つまり、ポート転送アプレットは、アプリケーションからの要求を受け入れて、その要求を ASA に転送します。ASA は適切な DNS クエリーを作成し、ポート転送アプレットの代わりに接続を確立します。ポート転送アプレットは、ASA に対する DNS クエリーだけを作成します。ポート転送アプレットはホスト ファイルをアップデートして、ポート転送アプリケーションが DNS クエリーを実行したときに、クエリーがループバック アドレスにリダイレクトされるようにします。次のように、DNS 要求をポート転送アプレットから受け入れるように、ASA を設定します。

	コマンド	目的
ステップ 1	**dns server-group**	DNS サーバ グループ モードを開始します。 example.com という名前の DNS サーバ グループを設定します。

ステップ 2	**domain-name**
	
	例：
	`hostname(config)# dns server-group example.com`
	`hostname(config-dns-server-group)# domain-name example.com`
		ドメイン名を指定します。デフォルトのドメイン名設定は DefaultDNS です。

ステップ 3	**name-server** 例： `hostname(config-dns-server-group)# name-server 192.168.10.10`	ドメイン名を IP アドレスに解決します。
ステップ 4	**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。

	コマンド	目的
ステップ 5	**tunnel-group webvpn**	トンネルグループ 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 6	(デフォルトのドメイン名 [DefaultDNS] 以外のドメイン名を使用している場合にだけ必要) **dns-group** 例： asa2(config-dns-server-group)# **exit** asa2(config)# **tunnel-group DefaultWEBVPNGroup webvpn-attributes** asa2(config-tunnel-webvpn)# **dns-group example.com**	そのトンネル グループで使用されるドメイン名を指定します。デフォルトでは、セキュリティ アプライアンスがクライアントレス接続のデフォルトのトンネル グループとしてデフォルトのクライアントレス SSL VPN グループを割り当てます。ASA がこのトンネル グループを使用して設定をクライアントレス接続に割り当てる場合は、この手順を実行します。それ以外の場合は、クライアントレス接続に対して設定されたトンネルごとにこの手順を実行します。

アプリケーションのポート転送適格化

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、*ポート転送リスト*をサポートしています。それぞれのリストでは、アクセスを提供するアプリケーションが使用するローカル ポートとリモート ポートを指定します。各グループ ポリシーまたはユーザ名は 1 つのポート転送リストのみをサポートするため、サポートされる CA のセットをグループ化してリストを作成する必要があります。ASA コンフィギュレーションにすでに存在するポート転送リストのエントリを表示するには、次のコマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**show run webvpn port-forward**	ASA 設定にすでに存在するポート転送リスト エントリを表示します。
ステップ 2	**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。

	コマンド	目的
ステップ 3	**port-forward {<list name> <local port> <remote server> <remote port> <description>}** 例： hostname(config)# **webvpn** hostname(config-webvpn)# **port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail** hostname(config-webvpn)# **port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail** hostname(config-webvpn)# **port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH** hostname(config-webvpn)# **port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet**	ポート転送のエントリをリストに追加します。 • *list_name*：クライアントレス SSL VPN セッションのユーザがアクセスするアプリケーションのセット（理論的には、転送 TCP ポートのセット）の名前です。名前を認識しない場合、ASA は、ユーザが入力した名前を使用してリストを作成します。認識した場合は、そのポート転送のエントリをリストに追加します。最大 64 文字です。 • *local_port*：ユーザのコンピュータで実行しているアプリケーションの TCP トラフィックをリッスンするポートです。ローカル ポートの番号は、各ポート転送リストに対して一度だけ使用できます。1 ～ 65535 の範囲のポート番号、またはポート名を入力します。既存サービスとの競合を避けるために、1024 よりも大きいポート番号を使用します。 • *remote_server*：アプリケーションに対するリモート サーバの DNS 名または IP アドレスです。IP アドレスは IPv4 または IPv6 形式で指定できます。特定の IP アドレス用にクライアント アプリケーションを設定しなくて済むように、DNS 名を指定することをお勧めします。 （注）　DNS 名は、前の項で説明した手順に従って、トンネルを確立し、IP アドレスに解決するためにトンネル グループに割り当てられた DNS 名と一致する必要があります。その項で説明した **domain-name** **group** および **dns-group** の両方のコマンドに対するデフォルト設定は DefaultDNS です。 • *remote_port*：このアプリケーションが接続するリモート サーバのポートです。これは、アプリケーションで使用する実際のポートです。1 ～ 65535 の範囲のポート番号、またはポート名を入力します。 • *description*：エンド ユーザの Port Forwarding Java アプレット画面に表示されるアプリケーション名または簡単な説明です。最大 64 文字です。 これらのアプリケーションへのアクセスを提供する SalesGroupPorts という名前のポート転送リストを作成する方法を示します。

	コマンド	目的
ステップ 4	(オプション) **no port-forward <list name> <local port>**	リストとローカル ポートの両方を指定して、リストからエントリを削除します。

ポート転送リストの設定に続けて、次の項で説明するように、そのリストをグループ ポリシーまたはユーザ名に割り当てます。

ポート転送リストの割り当て

クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションの名前付きリストを追加または編集できます。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ポート転送アクセスを開始する。

(注)　これらのオプションは、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。

前提条件

port-forward enable <list_name> コマンドを開始する前に、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 Applications]** を使用して、ポート転送を手動で開始する必要があります。

手順の詳細

これらのコマンドは、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、後者のコマンドの場合は、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 **port-forward** 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	**port-forward auto-start <list name>**	ユーザのログイン時に自動的にポート転送を開始します。
	port-forward enable <list name>	ユーザのログイン時にポート転送をイネーブルにします。
	port-forward disable	ポート転送を禁止します。
	no port-forward [**auto-start** **<list name>** | **enable** **<list name>** | **disable**]	**port-forward** コマンドをグループ 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し、[**no**] **port-forward** コマンドをデフォルト グループ ポリシーから継承します。**no port-forward** 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は削除対象をその名前の **port-forward** コマンドに限定します。

ポート転送の自動化

ユーザのログイン時にポート転送を自動的に開始するには、次のコマンドを入力します。

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** **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	**port-forward auto-start <list name>** 例： hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **port-forward auto-start apps1**	ユーザのログイン時に自動的にポート転送を開始します。 *list_name* は 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ポート転送リストの名前です。複数のポート転送リストをグループ ポリシーまたはユーザ名に割り当てることはできません。 apps1 という名前のポート転送リストをグループ ポリシーに割り当てます。

	コマンド	目的
ステップ 4	**show run webvpn port-forward**	ASA 設定に存在するポート転送リスト エントリを表示します。
ステップ 5	（オプション） **no port-forward**	**port-forward** 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。

ポート転送のイネーブル化と切り替え

デフォルトでは、ポート転送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	**port-forward [enable <list name> | disable]** 例： hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **port-forward enable apps1**	ポート転送をイネーブルにします。前の表の **port-forward auto-start** ***list_name*** を入力した場合は、ポート転送を手動で開始する必要はありません。 *list_name* は、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ポート転送リストの名前です。複数のポート転送リストをグループ ポリシーまたはユーザ名に割り当てることはできません。 apps1 という名前のポート転送リストをグループ ポリシーに割り当てます。
ステップ 2	**show running-config port-forward**	ポート転送リストのエントリを表示します。
ステップ 3	（オプション） **no port-forward**	port-forward 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。
ステップ 4	（オプション） **port-forward disable**	ポート転送をオフに切り替えます。

ファイル アクセスの設定

クライアントレス SSL VPN は、リモート ユーザに HTTPS ポータル ページを提供しています。このページは、ASA で実行するプロキシ CIFS クライアントまたは FTP クライアント（あるいはその両方）と連動しています。クライアントレス SSL VPN は、CIFS または FTP を使用して、ユーザが認証の要件を満たしているファイルのプロパティがアクセスを制限しない限り、ネットワーク上のファイルへのネットワーク アクセスをユーザに提供します。CIFS クライアントおよび FTP クライアントは透過的です。クライアントレス SSL VPN から送信されるポータル ページでは、ファイル システムに直接アクセスしているかのように見えます。

ユーザがファイルのリストを要求すると、クライアントレス SSL VPN は、そのリストが含まれるサーバの IP アドレスをマスター ブラウザに指定されているサーバに照会します。ASA はリストを入手してポータル ページ上のリモート ユーザに送信します。

クライアントレス SSL VPN は、ユーザの認証要件とファイルのプロパティに応じて、ユーザが次の CIFS および FTP の機能を呼び出すことができるようにします。

- ドメインとワークグループ、ドメインまたはワークグループ内のサーバ、サーバ内部の共有、および共有部分またはディレクトリ内のファイルのナビゲートとリスト。
- ディレクトリの作成。
- ファイルのダウンロード、アップロード、リネーム、移動、および削除。

ASA は、通常、ASA と同じネットワーク上か、またはこのネットワークからアクセス可能な場所のマスター ブラウザ、WINS サーバ、または DNS サーバを使用して、リモート ユーザがクライアントレス SSL VPN セッション中に表示されるポータル ページのメニュー上またはツールバー上の **[Browse Networks]** をクリックしたときに、ネットワークでサーバのリストを照会します。

マスター ブラウザまたは DNS サーバは、ASA 上の CIFS/FTP クライアントに、クライアントレス SSL VPN がリモート ユーザに提供する、ネットワーク上のリソースのリストを表示します。

(注)　ファイル アクセスを設定する前に、ユーザ アクセス用のサーバに共有を設定する必要があります。

CIFS ファイル アクセスの要件と制限事項

`\\server\share\subfolder\personal` *フォルダ*にアクセスするには、最低限、共有自体を含むすべての親フォルダに対する読み取り権限がユーザに必要です。

CIFS ディレクトリとローカル デスクトップとの間でファイルをコピー アンド ペーストするには、**[Download]** または **[Upload]** を使用します。[Copy] ボタンおよび [Paste] ボタンはリモート間のアクションのみで使用でき、ローカルからリモートまたはリモートからローカルへのアクションには使用できません。

CIFS ブラウズ サーバ機能は、2 バイト文字の共有名（13 文字を超える共有名）をサポートしていません。これは、表示されるフォルダのリストに影響を与えるだけで、フォルダへのユーザ アクセスには影響しません。回避策として、2 バイトの共有名を使用する CIFS フォルダのブックマークを事前に設定するか、ユーザが cifs://server/<long-folder-name> 形式でフォルダの URL またはブックマークを入力します。次に例を示します。

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

ファイル アクセスのサポートの追加

次の手順を実行して、ファイル アクセスを設定します。

(注)　この手順では、マスター ブラウザおよび WINS サーバを指定する方法について説明します。代わりに、ASDM を使用して、ファイル共有へのアクセスを提供する URL リストとエントリを設定することもできます。

ASDM での共有の追加には、マスター ブラウザまたは WINS サーバは必要ありません。ただし、Browse Networks リンクへのサポートは提供されません。**nbns-server** コマンドを入力するときは、ホスト名または IP アドレスを使用して ServerA を参照できます。ホスト名を使用する場合、ASA はホスト名を IP アドレスに解決するように DNS サーバに要求します。

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	**tunnel-group webvpn**	トンネルグループ 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	**nbns-server {**IPaddress **|** hostname**} [master] [timeout timeout] [retry retries]** 例： hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.20 master** hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.41** hostname(config-tunnel-webvpn)# **nbns-server 192.168.1.47**	各 NetBIOS ネーム サーバ（NBNS）のネットワークまたはドメインをブラウズします。 • **master** は、マスター ブラウザに指定されるコンピュータです。マスター ブラウザは、コンピュータおよび共有リソースのリストを維持します。コマンドのマスター部分を入力せずにこのコマンドで指定する任意の NBNS サーバは、Windows Internet Naming Server（WINS）である必要があります。まずマスター ブラウザを指定してから、WINS サーバを指定してください。マスター ブラウザを含め、接続プロファイル用のサーバは最大 3 つまで指定できます。 • *timeout* は、ASA が、クエリーを再度サーバに送信する前に待機する秒数です。このとき、サーバが 1 つしかない場合は同じサーバに送信し、サーバが複数存在する場合は別のサーバに送信します。デフォルトのタイムアウトは 2 秒で、指定できる範囲は 1 ～ 30 秒です。 • *retries* は、NBNS サーバに対するクエリーのリトライ回数です。ASA は、この回数だけサーバのリストを再利用してからエラー メッセージを送信します。デフォルト値は 2 で、指定できる範囲は 1 ～ 10 です。
ステップ 4	hostname# **show tunnel-group webvpn-attributes**	接続プロファイル コンフィギュレーションにすでに存在する NBNS サーバを表示します。

	コマンド	目的
ステップ 5	（オプション） **character-encoding *charset*** 例： hostname(config)# **webvpn** hostname(config-webvpn)# **character-encoding shift_jis** hostname(config-webvpn)# **customization DfltCustomization** hostname(config-webvpn-custom)# **page style background-color:white**	クライアントレス SSL VPN ポータル ページをリモート ユーザに送信するために符号化する文字セットを指定します。デフォルトでは、リモート ブラウザ上の符号化タイプ セットでクライアントレス SSL VPN ポータル ページの文字セットが決定されるため、ユーザは、ブラウザで符号化を適切に実行するために必要となる場合に限り、文字の符号化を設定する必要があります。 *charset* は、最大 40 文字からなる文字列で、http://www.iana.org/assignments/character-sets で指定されたいずれかの有効文字セットと同じです。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 （注）　character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。次の例に示すように日本語の Shift_JIS 文字エンコーディングを使用する場合などは、webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してフォント ファミリを置換し、これらの値の設定を補足するか、または webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォント ファミリを削除する必要があります。 日本語 Shift_JIS 文字をサポートする character-encoding 属性を設定し、フォント ファミリを削除し、デフォルトの背景色を保持します。
ステップ 6	（オプション） **file-encoding {server-name | server-ip-address} *charset*** 例： hostname(config-webvpn)# **file-encoding 10.86.5.174 cp860**	特定の CIFS サーバのクライアントレス SSL VPN ポータル ページの符号化を指定します。このため、これ以外の文字の符合化が必要な各 CIFS サーバに対し、異なるファイル符号化値を使用できます。 CIFS サーバ 10.86.5.174 の file-encoding 属性を設定して、IBM860（エイリアス「CP860」）文字をサポートします。

これらのコマンドの詳しい説明については、コマンド リファレンスを参照してください。

SharePoint アクセスのためのクロックの精度の確認

ASA のクライアントレス SSL VPN サーバは、クッキーを使用して、エンドポイントの Microsoft Word などのアプリケーションと対話します。ASA で設定されたクッキーの有効期間により、ASA の時間が正しくない場合、SharePoint サーバ上の文書にアクセスするときに Word が正しく機能しなくなる可能性があります。このような誤作動を回避するには、ASA クロックを正しく設定します。NTP サーバとダイナミックに同期化されるように ASA を設定することをお勧めします。手順については、一般的な操作のコンフィギュレーション ガイドの日付と時刻の設定の項を参照してください。

仮想デスクトップ インフラストラクチャ（VDI）

ASA は、Citrix サーバおよび VMware VDI サーバへの接続をサポートします。

- Citrix の場合、ASA ではクライアントレス ポータルを介してユーザの実行中の Citrix レシーバへアクセスできます。
- VMware は、（スマート トンネル）のアプリケーションとして設定されます。

VDI サーバには、他のサーバ アプリケーションのように、クライアントレス ポータルのブックマークを介してアクセスできます。

制限事項

- 自動サインオンの場合、証明書またはスマート カードを使用する認証はサポートされません。これは、これらの認証形式では間にある ASA を許可しないためです。
- XML サービスは XenApp サーバおよび XenDesktop サーバにインストールし、設定する必要があります。
- スタンドアロン モバイル クライアントを使用している場合は、クライアント証明書の確認、二重認証、内部パスワードと CSD（Vault だけでなく、すべての CSD）はサポートされません。

Citrix モバイルのサポート

Citrix レシーバを実行しているモバイル ユーザは、次を実行して Citrix サーバに接続できます。

- AnyConnect で ASA に接続してから Citrix サーバに接続する。
- AnyConnect クライアントを使用せずに ASA を介して Citrix サーバに接続する。ログオン クレデンシャルには次を含めることができます。
  - Citrix ログオン画面の接続プロファイルのエイリアス（トンネル グループ エイリアスとも呼ばれる）。VDI サーバは、それぞれ別の権限と接続設定を備えた複数のグループ ポリシーを持つことができます。
  - RSA サーバが設定されている場合は RSA SecureID トークンの値。RSA サポートには、無効なエントリ用の次のトークンと、最初の PIN または期限切れ PIN 用の新しい PIN を入力するための次のトークンが含まれています。

サポートされているモバイル デバイス

- iPad：Citrix Receiver バージョン 4.x 以降
- iPhone/iTouch：Citrix Receiver バージョン 4.x 以降
- Android 2.x/3.x/4.0/4.1 電話機：Citrix Receiver バージョン 2.x 以降
- Android 4.0 電話機：Citrix Receiver バージョン 2.x 以降

制限事項

証明書の制限

- 証明書/スマートカード認証は自動サインオンの手段としてはサポートされていません。
- クライアント証明書の確認および CSD はサポートされていません。
- 証明書の Md5 署名は、iOS の既知の問題であるセキュリティ上の問題（http://support.citrix.com/article/CTX132798）から動作していません。
- SHA2 シグニチャは Citrix Web サイト（http://www.citrix.com/）の説明に従って Windows を除き、サポートされていません。
- 1024 以上のキー サイズはサポートされていません。

その他の制限

- HTTP リダイレクトはサポートされません。Citrix レシーバ アプリケーションはリダイレクトでは機能しません。
- XML サービスは XenApp サーバおよび XenDesktop サーバにインストールし、設定する必要があります。

Citrix Mobile Receiver のユーザ ログオンについて

Citrix サーバに接続しているモバイル ユーザのログオンは、ASA が Citrix サーバを VDI サーバとして設定したか、または VDI プロキシ サーバとして設定したかによって異なります。

Citrix サーバが VDI サーバとして設定されている場合:

1. AnyConnect Secure Mobility Client を使用し、VPN クレデンシャルで ASA に接続します。
2. Citrix Mobile Receiver を使用し、Citrix サーバ クレデンシャルで Citrix サーバに接続します（シングルサインオンを設定している場合は、Citrix クレデンシャルは不要です）。

ASA が VDI プロキシ サーバとして設定されている場合:

1. Citrix Mobile Receiver を使用し、VPN と Citrix サーバの両方のクレデンシャルを入力して ASA に接続します。最初の接続後、正しく設定されている場合は、以降の接続に必要なのは VPN クレデンシャルだけです。

Citrix サーバをプロキシする ASA の設定

ASA を Citrix サーバのプロキシとして動作するように設定し、ASA への接続が Citrix サーバへの接続であるかのようにユーザに見せることができます。ASDM の VDI プロキシがイネーブルになっている場合は AnyConnect クライアントは不要です。次の手順は、エンド ユーザーから Citrix に接続する方法の概要を示します。

1. モバイル ユーザが Citrix レシーバを起動し、ASA の URL に接続します。
2. Citrix のログイン画面で、XenApp サーバのクレデンシャルと VPN クレデンシャルを指定します。
3. 以降、Citrix サーバに接続する場合に必要になるのは、VPN クレデンシャルだけです。

XenDesktop および XenApp のプロキシとして ASA を使用すると Citrix アクセス ゲートウェイは必要なくなります。XenApp サーバ情報が ASA に記録され、ASDM に表示されます。

Citrix サーバのアドレスおよびログイン クレデンシャルを設定し、グループ ポリシーまたはユーザ名にその VDI サーバを割り当てます。ユーザ名とグループ ポリシーの両方を設定した場合は、ユーザ名の設定によってグループ ポリシー設定がオーバーライドされます。

その他の情報

http://www.youtube.com/watch?v=JMM2RzppaG8：このビデオでは、その ASA を Citrix プロキシとして使用する利点について説明します。

グループ ポリシーへの VDI サーバの割り当て

VDI サーバを設定し、グループ ポリシーに割り当てる方法は次のとおりです。

- [VDI Access] ペインで VDI サーバを追加し、サーバにグループ ポリシーを割り当てる。
- グループ ポリシーに VDI サーバを追加する。

ユーザ名とグループ ポリシーが両方とも設定されている場合、ユーザ名の設定は、グループ ポリシーに優先します。次を入力します。

```
configure terminal
    group-policy DfltGrpPolicy attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>
configure terminal
    username <username> attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>]
```

構文オプションは、次のように定義されます。

- type：VDI のタイプ。Citrix Receiver タイプの場合、この値は *citrix* にする必要があります。
- url：http または https、ホスト名、ポート番号、および XML サービスへのパスを含む XenApp または XenDesktop サーバの完全な URL。
- username：仮想化インフラストラクチャ サーバにログインするためのユーザ名。この値は、クライアントレス マクロにすることができます。
- password：仮想化インフラストラクチャ サーバにログインするためのパスワード。この値は、クライアントレス マクロにすることができます。

- domain：仮想化インフラストラクチャ サーバにログインするためのドメイン。この値は、クライアントレス マクロにすることができます。

内部サーバにアクセスするための SSL の使用

	コマンド	目的
ステップ 1	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。
ステップ 2	url-entry disable	URL エントリをオフに切り替えます。

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、内部サイトにある特定のサポートされている内部リソースとの間でセキュアな接続を提供します。

- 「クライアントレス SSL VPN セッションでの HTTPS の使用」（P.14-23）
- 「クライアントレス SSL VPN ポートと ASDM ポートの設定」（P.14-24）
- 「プロキシ サーバのサポートの設定」（P.14-24）
- 「SSL/TLS 暗号化プロトコルの設定」（P.14-27）

クライアントレス SSL VPN セッションでの HTTPS の使用

前提条件

Web ブラウザには、ASA のアドレスを *https:// address* 形式で入力します。*address* は ASA インターフェイスの IP アドレスまたは DNS ホスト名です。

制限

- ユーザの接続先の ASA インターフェイス上でクライアントレス SSL VPN セッションをイネーブルにする必要があります。
- ASA またはロードバランシング クラスタへのアクセスに HTTPS を使用する必要があります。

	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	**enable** <クライアントレス SSL VPN セッションに使用するインターフェイスの名前> 例： hostname(config)# **webvpn** hostname(config-webvpn)# **enable outside**	outside という名前のインターフェイス上でクライアントレス SSL VPN セッションをイネーブルにします。

クライアントレス SSL VPN ポートと ASDM ポートの設定

バージョン 8.0(2) 以降、ASA は、クライアントレス SSL VPN セッションと ASDM 管理セッションの両方を、外部インターフェイスのポート 443 で同時にサポートするようになりました。さまざまなインターフェイスでこれらのアプリケーションを設定できます。

	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	**port** *port_number* 例： hostname(config)# **http server enable** hostname(config)# **http 192.168.3.0 255.255.255.0 outside** hostname(config)# **webvpn** hostname(config-webvpn)# **port 444** hostname(config-webvpn)# **enable outside**	クライアントレス SSL VPN の SSL リスニング ポートを変更します。 外部インターフェイスのポート 444 上でクライアントレス SSL VPN をイネーブルにします。このコンフィギュレーションでは、リモート ユーザは、ブラウザに https://<outside_ip>:444 を入力してクライアントレス SSL VPN セッションを開始します。
ステップ 3	**http server enable** 例： hostname(config)# **http server enable** hostname(config)# **http 192.168.3.0 255.255.255.0 outside** hostname(config)# **webvpn** hostname(config-webvpn)# **enable outside**	（特権モード）ASDM のリスニング ポートを変更します。 HTTPS ASDM セッションが外部インターフェイスのポート 444 を使用することを指定します。クライアントレス SSL VPN も外部インターフェイスでイネーブルになり、デフォルト ポート（443）を使用します。このコンフィギュレーションでは、リモート ユーザは https://<outside_ip>:444 を入力して ASDM セッションを開始します。

プロキシ サーバのサポートの設定

ASA は HTTPS 接続を終了して、HTTP および HTTPS 要求をプロキシ サーバに転送できます。これらのサーバは、ユーザとパブリック ネットワークまたはプライベート ネットワーク間を中継する機能を果たします。組織が管理するプロキシ サーバを経由したネットワークへのアクセスを必須にすると、セキュアなネットワーク アクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

HTTP および HTTPS プロキシ サービスに対するサポートを設定する場合、プリセット クレデンシャルを割り当てて、基本認証に対する各要求とともに送信できます。HTTP および HTTPS 要求から除外する URL を指定することもできます。

制限

プロキシ自動設定（PAC）ファイルを HTTP プロキシ サーバからダウンロードするように指定できますが、PAC ファイルを指定するときにプロキシ認証を使用しない場合があります。

	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	**http-proxy および https-proxy**	外部プロキシ サーバを使用して HTTP および HTTPS 要求を処理するように 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。
ステップ 3	**http-proxy** *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]	HTTP プロキシを設定します。
ステップ 4	**https-proxy** *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]	HTTPS プロキシを設定します。
ステップ 5	**http-proxy pac** *url*	PAC ファイル URL を設定します。
ステップ 6	（オプション） exclude	URL をプロキシ サーバに送信される可能性がある URL から除外します。
ステップ 7	*host*	外部プロキシ サーバのホスト名または IP アドレスを指定します。
ステップ 8	pac	ASA にダウンロードされた、各 URL のプロキシを識別するために JavaScript 機能を使用するプロキシ自動コンフィギュレーション ファイル。
ステップ 9	（任意。ユーザ名を指定した場合にのみ使用可能） password	基本的なプロキシ認証を提供するためにパスワードとともに各プロキシ要求と一緒に送信します。
ステップ 10	*password*	各 HTTP または HTTPS 要求とともにプロキシ サーバに送信するパスワード。
ステップ 11	（オプション） *port*	プロキシ サーバが使用するポート番号を指定します。デフォルトの HTTP ポートは 80 です。デフォルトの HTTPS ポートは 443 です。代替値を指定しない場合、ASA はこれらの各ポートを使用します。範囲は 1 ～ 65535 です。

	コマンド	目的
ステップ 12	*url*	**exclude** を入力した場合は、プロキシ サーバに送信される可能性がある URL から除外する URL またはカンマで区切った複数の URL のリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 – * は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。 – **?**は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 – [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。 – [**!***x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。
ステップ 13	**http-proxy pac** を入力した場合、**http://** に続けてプロキシ自動設定ファイルの URL を入力します（**http://** の部分を省略すると、CLI はコマンドを無視します）。	—
ステップ 14	（オプション） username	基本的なプロキシ認証のためにユーザ名とともに各 HTTP プロキシ要求と一緒に送信します。このキーワードは、**http-proxy** *host* コマンドでのみサポートされています。
ステップ 15	*username*	各 HTTP または HTTPS 要求とともにプロキシ サーバに送信するユーザ名。
ステップ 16	例： hostname(config-webvpn)# **http-proxy 209.165.201.1 user jsmith password mysecretdonttell** hostname(config-webvpn)	次の設定の HTTP プロキシ サーバの使用を設定する方法を示します。IP アドレスが 209.165.201.1 で、デフォルト ポートを使用し、各 HTTP 要求とともにユーザ名とパスワードを送信する。
ステップ 17	例： hostname(config-webvpn)# **http-proxy 209.165.201.1 exclude www.example.com username jsmith password mysecretdonttell** hostname(config-webvpn)	同じコマンドの例を示しますが、前の例とは異なり、この例では、ASA が HTTP 要求で www.example.com という特定の URL を受信した場合には、プロキシ サーバに渡すのではなく自分自身で要求を解決します。
ステップ 18	例： hostname(config-webvpn)# **http-proxy pac http://www.example.com/pac** hostname(config-webvpn)	ブラウザにプロキシ自動設定ファイルを提供する URL を指定する方法を示します。

ASA クライアントレス SSL VPN コンフィギュレーションは、それぞれ 1 つの **http-proxy** コマンドと 1 つの **https-proxy** コマンドのみサポートしています。たとえば、**http-proxy** コマンドの 1 インスタンスが実行コンフィギュレーションにすでに存在する場合に別のコマンドを入力すると、CLI が前のインスタンスを上書きします。

（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。

SSL/TLS 暗号化プロトコルの設定

ポート転送には、Oracle Java ランタイム環境（JRE）が必要です。クライアントレス SSL VPN のユーザがいくつかの SSL バージョンに接続する場合、ポート転送は機能しません。サポートされている JRE バージョンについては、「compatibility matrix」を参照してください。

デジタル証明書による認証

SSL はデジタル証明書を使用して認証を行います。ASA は、ブート時に自己署名の SSL サーバ証明書を作成します。または、PKI コンテキストで発行された SSL 証明書を ASA にインストールできます。HTTPS の場合、この証明書をクライアントにインストールする必要があります。

制限

MS Outlook、MS Outlook Express、Eudora などの電子メール クライアントは、証明書ストアにアクセスできません。

デジタル証明書を使用する認証と認可については、一般的な操作のコンフィギュレーション ガイドの証明書とユーザ ログイン クレデンシャルの使用に関する項を参照してください。

クライアント/サーバ プラグインへのブラウザ アクセスの設定

[Client-Server Plug-in] テーブルには、ASA によってクライアントレス SSL VPN セッションのブラウザで使用できるようになるプラグインが表示されます。

プラグインを追加、変更、または削除するには、次のいずれかを実行します。

- プラグインを追加するには、**[Import]** をクリックします。[Import Plug-ins] ダイアログボックスが開きます。
- プラグインを削除するには、そのプラグインを選択して **[Delete]** をクリックします。

次の項では、クライアントレス SSL VPN のブラウザ アクセス用のブラウザ プラグインの統合について説明します。

- ブラウザ プラグインのインストールについて
- プラグインのためのセキュリティ アプライアンスの準備
- シスコによって再配布されたプラグインのインストール

ブラウザ プラグインのインストールについて

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。ASA により、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。通常、シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートは推奨しません。

プラグインをフラッシュ デバイスにインストールすると、ASA は次の処理を実行します。

- （シスコが配布したプラグインのみ）*URL* で指定した jar ファイルを解凍する。
- ASA ファイル システムの csco-config/97/plugin ディレクトリにファイルを書き込む。
- ASDM の URL 属性の横にあるドロップダウン リストに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、メイン メニュー オプションと、ポータル ページの [Address] フィールドの横にあるドロップダウン リストについてのオプションを追加します。

  表 14-3 に、次の項で説明するプラグインを追加したときの、ポータル ページのメイン メニューと [Address] フィールドの変更点を示します。

表 14-3　クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

（注）　セカンダリ ASA は、プライマリ ASA からプラグインを取得します。

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン リストに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

（注）　Java プラグインによっては、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインというステータスがレポートされることがあります。open-source プラグインは、ASA ではなくステータスをレポートします。

1 つ目のプラグインをインストールする前に、次の項の指示に従う必要があります。

前提条件

- セキュリティ アプライアンスでクライアントレス セッションがプロキシ サーバを使用するように設定している場合、プラグインは機能しません。

（注）　Remote Desktop Protocol プラグインでは、セッション ブローカを使用したロード バランシングはサポートされていません。プロトコルによるセッション ブローカからのリダイレクションの処理方法のため、接続に失敗します。セッション ブローカが使用されていない場合、プラグインは動作します。

- プラグインは、シングル サインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを開くときに入力したクレデンシャルと*同じ*クレデンシャルを使用します。プラグインはマクロ置換をサポートしないため、内部ドメイン パスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバの属性で SSO を実行するオプションはありません。
- プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバへのリンクを表示するためのブックマーク エントリを追加します。また、ブックマークを追加するときに、SSO サポートを指定します。
- リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。

要件

- シスコでは、GNU 一般公的使用許諾（GPL）に従い、変更を加えることなくプラグインを再配布しています。GPL により、これらのプラグインを直接改良できません。
- プラグインへのリモート アクセスを提供するには、ASA でクライアントレス SSL VPN をイネーブルにする必要があります。
- ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。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。
- プラグインには、ActiveX または Oracle Java ランタイム環境（JRE）1.4.2（以降）がブラウザでイネーブルになっている必要があります。64 ビット ブラウザには、RDP プラグインの ActiveX バージョンはありません。

RDP プラグイン ActiveX デバッグのクイック リファレンス

RDP プラグインをセットアップして使用するには、新しい環境変数を追加する必要があります。

ステップ 1　**[My Computer]** を右クリックし、[System Properties] を開いて **[Advanced]** タブを選択します。

ステップ 2　[Advanced] タブで、[Environment Variables] ボタンを選択します。

ステップ 3　[New User Variable] ダイアログボックスで、RF_DEBUG 変数を入力します。

ステップ 4　[User variables] セクションの新しい環境変数を確認します。

ステップ 5　バージョン 8.3 以前のクライアントレス SSL VPN のバージョンでクライアント コンピュータを使用していた場合、古い Cisco Portforwarder Control を削除してください。C:/WINDOWS/Downloaded Program Files ディレクトリを開いて、Portforwarder Control を右クリックして、**[Remove]** を選択します。

ステップ 6　Internet Explorer ブラウザのすべてのキャッシュをクリアします。

ステップ 7　クライアントレス SSL VPN セッションを起動して、RDP ActiveX プラグインを使用して RDP セッションを確立します。

これで Windows アプリケーションのイベント ビューアでイベントを確認できるようになります。

プラグインのためのセキュリティ アプライアンスの準備

ステップ 1　クライアントレス SSL VPN が ASA インターフェイスでイネーブルになっていることを確認します。

ステップ 2　リモート ユーザが完全修飾ドメイン名（FQDN）を使用して接続する ASA インターフェイスに SSL 証明書をインストールします。

（注）　SSL 証明書の一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、ASA と通信するために FQDN の使用を試行します。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

ASA で新しい HTML ファイルを使用するための設定

手順の詳細

	コマンド	目的
ステップ 1	**import webvpn webcontent <file> <url>** **例：** hostname# **import webvpn webcontent /+CSCOU+/login.inc tftp://209.165.200.225/login.inc** !!!!* Web resource `+CSCOU+/login.inc' was successfully initialized hostname#	ファイルおよびイメージを Web コンテンツとしてインポートします。
ステップ 2	**export webvpn customization <file> <URL>** **例：** hostname2# **export webvpn customization template tftp://209.165.200.225/sales_vpn_login** !!! %INFO: Customization object 'Template' was exported to tftp://10.21.50.120/sales_vpn_login	カスタマイゼーション テンプレートをエクスポートします。

	コマンド	目的

ステップ 3	ファイル内の full customization mode タグを enable に変更します。
	
	例：
	`<full-customization>`
	`<mode>enable</mode>`
	`<url>/+CSCOU+/login.inc</url>`
	`</full-customization>`
		ASA メモリに格納されているログイン ファイルの URL を指定します。

ステップ 4	ファイルを新しいカスタマイゼーション オブジェクトとしてインポートします。
	
	例：
	`hostname# import webvpn customization sales_vpn_login tftp://10.21.50.120/sales_vpn_login$`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`%INFO: customization object 'sales_vpn_login' was successfully imported`
		—

ステップ 5	接続プロファイル（トンネル グループ）にカスタマイゼーション オブジェクトを適用します。
	
	例：
	`hostname(config)# tunnel-group Sales webvpn-attributes`
	`hostname(config-tunnel-webvpn)#customization sales_vpn_login`
		—