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

- 「クライアントレス SSL VPN セキュリティ対策」（P.11-1）
- 「クライアントレス SSL VPN サーバ証明書の確認」（P.11-3）
- 「プラグインへのブラウザ アクセスの設定」（P.11-7）
- 「ポート転送の設定」（P.11-12）
- 「ファイル アクセスの設定」（P.11-19）
- 「SharePoint アクセスのためのクロックの精度の確認」（P.11-20）
- 「仮想デスクトップ インフラストラクチャ（VDI）」（P.11-20）
- 「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」（P.11-24）

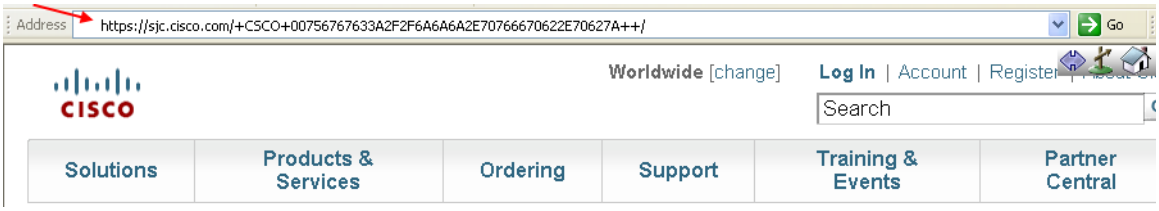
改訂日：2014 年 3 月 12 日

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 を書き換えます。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 11-1　ユーザが入力した URL の例

図 11-2　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



手順の詳細

ステップ 1　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。

ステップ 2　グループ ポリシーを開き、[General] > [More Options] > [Web ACL] を選択して [Manage] をクリックします。

ステップ 3　次のいずれかを行う場合、Web ACL を作成します。

- プライベート ネットワーク内の特定のターゲットだけにアクセスを許可する。
- プライベート ネットワークへのアクセスだけを許可する、インターネット アクセスを拒否する、または信頼できるサイトへのアクセスだけを許可する。

ステップ 4　クライアントレス SSL VPN アクセス用に設定しているすべてのポリシー（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 を割り当てます。Web ACL を DAP に割り当てるには、DAP レコードを編集し、[Network ACL Filters] タブで Web ACL を選択します。

ステップ 5　ブラウザベースの接続の確立時に表示される *ポータル* ページ上の URL エントリをオフに切り替えます。グループ ポリシーのポータル フレームと DAP の [Functions] タブの両方の [URL Entry] の横にある [Disable] をクリックします。DAP 上の URL エントリをオフに切り替えるには、ASDM を使用して DAP レコードを編集し、[Functions] タブをクリックして、[URL Entry] の横にある [Disable] をオンにします。

ステップ 6　ユーザに、ポータル ページの上のネイティブ ブラウザの Address フィールドに外部 URL を入力するか、別のブラウザ ウィンドウを開いて、外部サイトにアクセスするかを指示します。

クライアントレス SSL VPN アクセスの設定

クライアントレス SSL VPN アクセスを設定する場合、次の操作が可能です。

- クライアントレス SSL VPN セッション向けに ASA インターフェイスをイネーブルにする、またはオフに切り替える。
- クライアントレス SSL VPN 接続で使用するポートを選択する。
- 同時クライアントレス SSL VPN セッションの最大数を設定する。

手順の詳細

ステップ 1　クライアントレス アクセス用のグループ ポリシーを設定または作成するには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] ペインを選択します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] の順に進みます。

a. 各 ASA インターフェイスの [Allow Access] をイネーブルにするか、オフに切り替えます。

インターフェイスのカラムには、設定されているインターフェイスのリストが表示されます。[WebVPN Enabled] フィールドに、インターフェイスのクライアントレス SSL VPN のステータスが表示されます。[Yes] の隣に緑のチェックマークが入っていると、クライアントレス SSL VPN はイネーブルになっています。[No] の横の赤色の丸は、クライアントレス SSL VPN がオフに切り替えられていることを示します。

b. [Port Setting] をクリックし、クライアントレス SSL セッションに使用するポート番号（1 ～ 65535）を入力します。デフォルト値は 443 です。ポート番号を変更すると、現在のすべてのクライアントレス SSL VPN 接続が切断されるため、現在のユーザは再接続する必要があります。また、ASDM セッションへの再接続を求めるメッセージが表示されます。

ステップ 3　[Configuration] > [Remote Access VPN] > [Advanced] > [Maximum VPN Sessions] の順に進み、[Maximum Other VPN Sessions] フィールドで許可するクライアントレス SSL VPN セッションの最大数を入力します。

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。

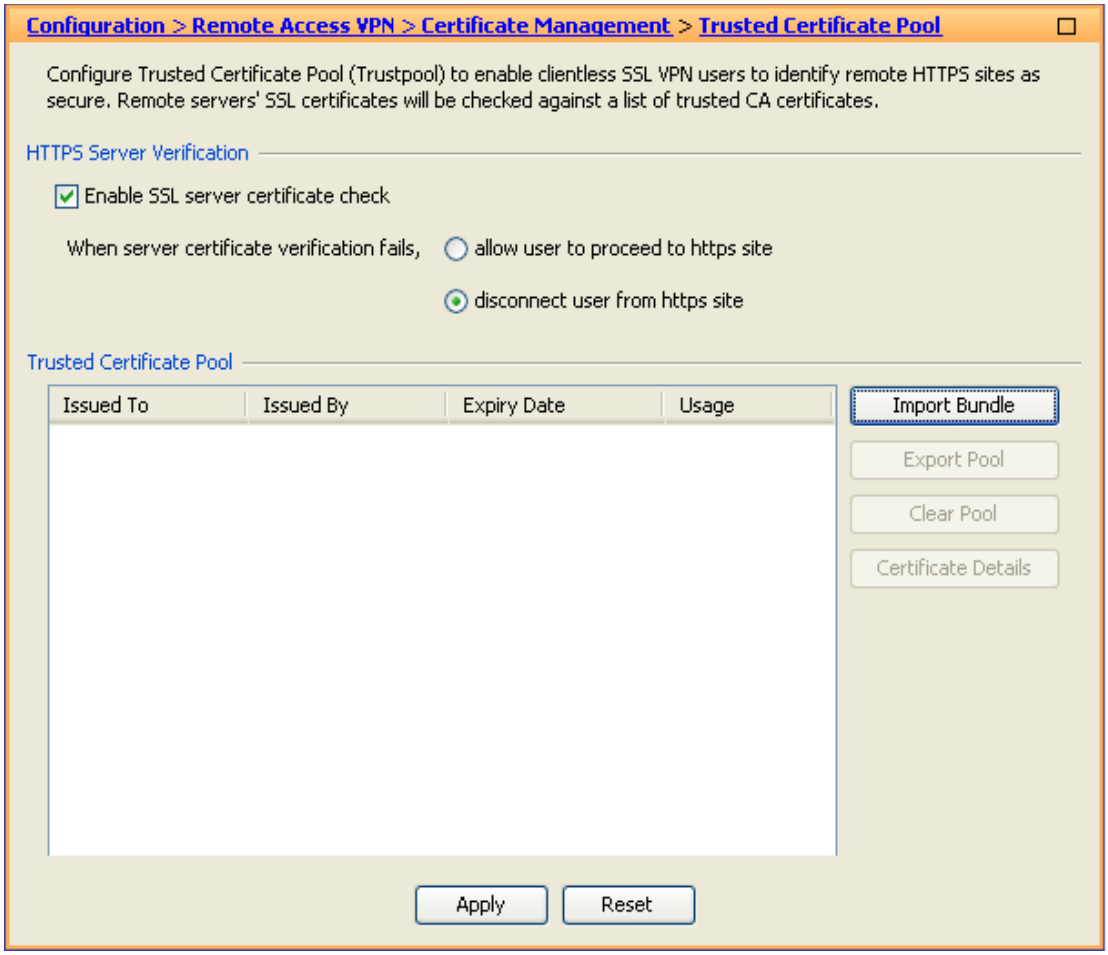
ASA は信頼できるプール証明書の管理機能を trustpool の形式で提供します。これは、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には Web ブラウザに備わっているものと同様のデフォルトの一連の証明書が含まれています。管理者が実行するまでは動作しません。

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

HTTP サーバ検証のイネーブル化

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択します。

図 11-3　ASDM での HTTPS サーバ検証のイネーブル化



ステップ 2　[Enable SSL Certificate Check] チェックボックスをオンにします。

ステップ 3　[Disconnect User From HTTPS Site] をクリックして、サーバが検証できなかった場合に切断します。または、[Allow User to Proceed to HTTPS Site] をクリックして、チェックが失敗した場合でも、ユーザが接続を継続できるようにします。

ステップ 4　[Apply] をクリックして変更内容を保存します。

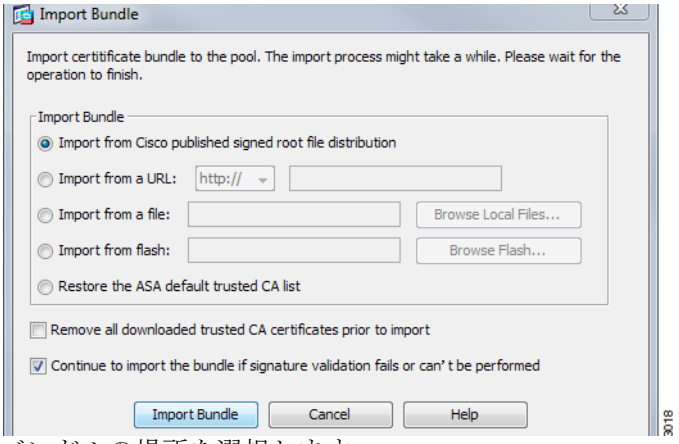
証明書のバンドルのインポート

次の形式のいずれかで、さまざまな場所から個々の証明書または証明書のバンドルをインポートできます。

- pkcs7 構造でラップされた DER 形式の x509 証明書。
- PEM 形式（PEM ヘッダーに囲まれた）の連結した x509 証明書のファイル。

ステップ 1　ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択します。

ステップ 2　[Import Bundle] をクリックします。



ステップ 3　バンドルの場所を選択します。

- バンドルがコンピュータに保存されている場合は、[Import From a File] をクリックし、[Browse Local Files] をクリックして、バンドルを選択します。
- バンドルが ASA フラッシュ ファイル システムに保存されている場合は、[Import From Flash] をクリックし、[Browse Flash] をクリックして、ファイルを選択します。
- バンドルがサーバでホストされている場合は、[Import From a URL] をクリックして、リストからプロトコルを選択し、フィールドに URL を入力します。
- シグニチャの確認が失敗したり、実行できない場合にバンドルのインポートを継続することにより、バンドルをインポートして、後で個々の証明書のエラーを修正することができます。証明書のいずれかに失敗した場合はバンドル全体が失敗するように、チェックボックスをオフにします。

ステップ 4　[Import Bundle] をクリックします。または、[Cancel] をクリックして変更を破棄します。

（注）　[Remove All Downloaded Trusted CA Certificates Prior to Import] チェックボックスをオンにして、新しいバンドルをインポートする前に trustpool をクリアします。

trustpool のエクスポート

trustpool を正しく設定したら、プールをエクスポートする必要があります。これにより、このポイントまで（たとえばエクスポート後に trustpool に追加された証明書を削除する場合など）trustpool を復元できます。ASA フラッシュ ファイル システムまたはローカル ファイル システムにプールをエクスポートできます。

ASDM で、[Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Export Pool] をクリックします。

ステップ 1　[Export to a File] をクリックします。

ステップ 2　[Browse Local Files] をクリックします。

ステップ 3　trustpool を保存するフォルダを選択します。

ステップ 4　[File Name] ボックスに、trustpool の一意の覚えやすい名前を入力します。

ステップ 5　[Select] をクリックします。

ステップ 6　[Export Pool] をクリックして、ファイルを保存します。または、[Cancel] をクリックして保存を停止します。

証明書の削除

すべての証明書を削除するには、ASDM で [Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Clear Pool] をクリックします。

（注）　trustpool をクリアする前に、現在の設定を復元できるように、現在の trustpool をエクスポートする必要があります。

デフォルトの信頼できる認証局リストの復元

デフォルトの信頼できる認証局（CA）リストを復元するには、ASDM で [Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Restore Default Trusted CA List] をクリックし、[Import Bundle] をクリックします。

trustpool の更新

次のいずれかの条件が満たされる場合は、trustpool を更新する必要があります。

- trustpool の証明書が期限切れまたは再発行されている。
- 公開された CA 証明書のバンドルに、特定のアプリケーションで必要な追加の証明書が含まれている。

完全な更新によって、trustpool のすべての証明書が置き換えられます。

実用的な更新では、新しい証明書を追加したり、既存の証明書を置き換えることができます。

証明書のバンドルの削除

trustpool をクリアすると、デフォルトのバンドルではないすべての証明書が削除されます。

デフォルトのバンドルは削除できません。trustpool をクリアするには、ASDM で [Configuration] > [Remote Access VPN] > [Certificate Management] > [Trusted Certificate Pool] を選択し、[Clear Pool] をクリックします。

Java Code Signer

コード署名により、デジタル署名が、実行可能なコードそのものに追加されます。このデジタル署名には、さまざまな情報が保持されています。署名以降にそのコードが変更されていないことを保証するだけでなく、署名者を認証する場合に使用することもできます。

コード署名者証明書は、関連付けられている秘密キーがデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

Java オブジェクト署名で使用する、設定された証明書をドロップダウン リストから選択します。

Java Code Signer を設定するには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Java Code Signer] を選択します。

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。[Java Trustpoint] ペインでは、指定されたトラストポイントの場所から PKCS12 証明書とキー関連情報を使用するようにクライアントレス SSL VPN Java オブジェクト署名機能を設定できます。

トラストポイントをインポートするには、[Configuration] > [Properties] > [Certificate] > [Trustpoint] > [Import] を選択します。

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。

- 「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.11-8）
- 「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.11-9）
- 「Citrix XenApp Server へのアクセスの提供」（P.11-11）

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 ファイルを解凍します。
- ASA ファイル システムにファイルを書き込みます。
- 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、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 リストにメイン メニュー オプションとオプションを追加します。

表 11-1 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。

* 推奨されないプラグイン。

表 11-1　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://

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.15-5）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、互換性マトリクスを参照してください。

制約事項

（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。

制約事項

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。

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.11-9）
- 「Citrix XenApp Server へのアクセスの提供」（P.11-11）

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 11-2　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 のバージョン 5.1 へのバージョンアップだけ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/
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 ソフトウェアのダウンロード サイトで入手できます。

手順の詳細

ステップ 1　ASA との ASDM セッションを確立するために使用するコンピュータに、plugins という名前の一時ディレクトリを作成し、シスコの Web サイトから、必要なプラグインを [plugins] ディレクトリにダウンロードします。

ステップ 2　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Client-Server Plug-ins] を選択します。

このペインには、クライアントレス SSL セッションで使用可能な現在ロードされているプラグインが表示されます。これらのプラグインのハッシュおよび日付も表示されます。

ステップ 3　[Import] をクリックします。

[Import Client-Server Plug-in] ダイアログボックスが開きます。

ステップ 4　[Import Client-Server Plug-in] ダイアログボックスのフィールド値を入力するには、次の説明を参考にしてください。

- [Plug-in Name]：次のいずれかの値を入力します。
  - **ica**。Citrix MetaFrame または Web Interface サービスへのプラグイン アクセスを提供する場合に指定します。
  - Remote Desktop Protocol サービスへのプラグイン アクセスを提供するには、**rdp** を入力します。
  - セキュア シェル サービスと Telnet サービスの*両方*にプラグイン アクセスを提供するには、**ssh,telnet** を入力します。
  - Virtual Network Computing サービスにプラグイン アクセスを提供するには、**vnc** を入力します。

（注）　このメニューの、記載のないオプションは実験的なものであるため、サポートされていません。

- [Select the location of the plugin file]：次のいずれかのオプションをクリックし、テキスト フィールドにパスを挿入します。
  - [Local computer]：関連する [Path] フィールドにプラグインの場所と名前を入力するか、[Browse Local Files] をクリックしてプラグインを選択し、プラグインを選択して [Select] をクリックします。
  - [Flash file system]：関連する [Path] フィールドにプラグインの場所と名前を入力するか、[Browse Flash] をクリックしてプラグインを選択し、プラグインを選択して [OK] をクリックします。
  - [Remote Server]：リモート サーバで実行されているサービスに応じて、関連付けられた [Path] 属性の横にあるドロップダウン メニューで [ftp]、[tftp]、または [HTTP] を選択します。隣にあるテキスト フィールドに、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。

ステップ 5　[Import Now] をクリックします。

ステップ 6　[Apply] をクリックします。

これで、以降のクライアントレス SSL VPN セッションでプラグインが使用できるようになりました。

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.11-8）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]、[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。

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」（P.11-12）
- ポート転送用の DNS の設定
- アプリケーションのポート転送適格化
- ポート転送エントリの追加と編集
- ポート転送リストの割り当て
- ポート転送のイネーブル化と切り替え

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る。
  - 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る。
- 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。

制約事項

- 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。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] の順にクリックします。

デフォルトのクライアントレス SSL VPN グループ エントリは、クライアントレス接続に使用されるデフォルトの接続プロファイルです。

ステップ 2　設定をクライアントレス接続にも使用する場合は、デフォルトのクライアントレス SSL VPN グループ エントリを強調表示し、[Edit] をクリックします。このエントリが使用されない場合は、クライアント接続のコンフィギュレーションで使用される接続プロファイルを強調表示し、[Edit] をクリックします。

[Basic] ウィンドウが開きます。

ステップ 3　[DNS] 領域にスキャンし、ドロップダウン リストから DNS サーバを選択します。ドメイン名をメモしておきます。使用する DNS サーバが ASDM に表示されている場合は、残りのステップを飛ばし、次のセクションに移動します。ポート転送リストのエントリを設定する際、リモート サーバの指定時には、同じドメイン名を入力する必要があります。コンフィギュレーションに DNS サーバがない場合は、残りのステップを続けます。

ステップ 4　[DNS] 領域で [Manage] をクリックします。

[Configure DNS Server Groups] ウィンドウが開きます。

ステップ 5　[Configure Multiple DNS Server Groups] をクリックします。

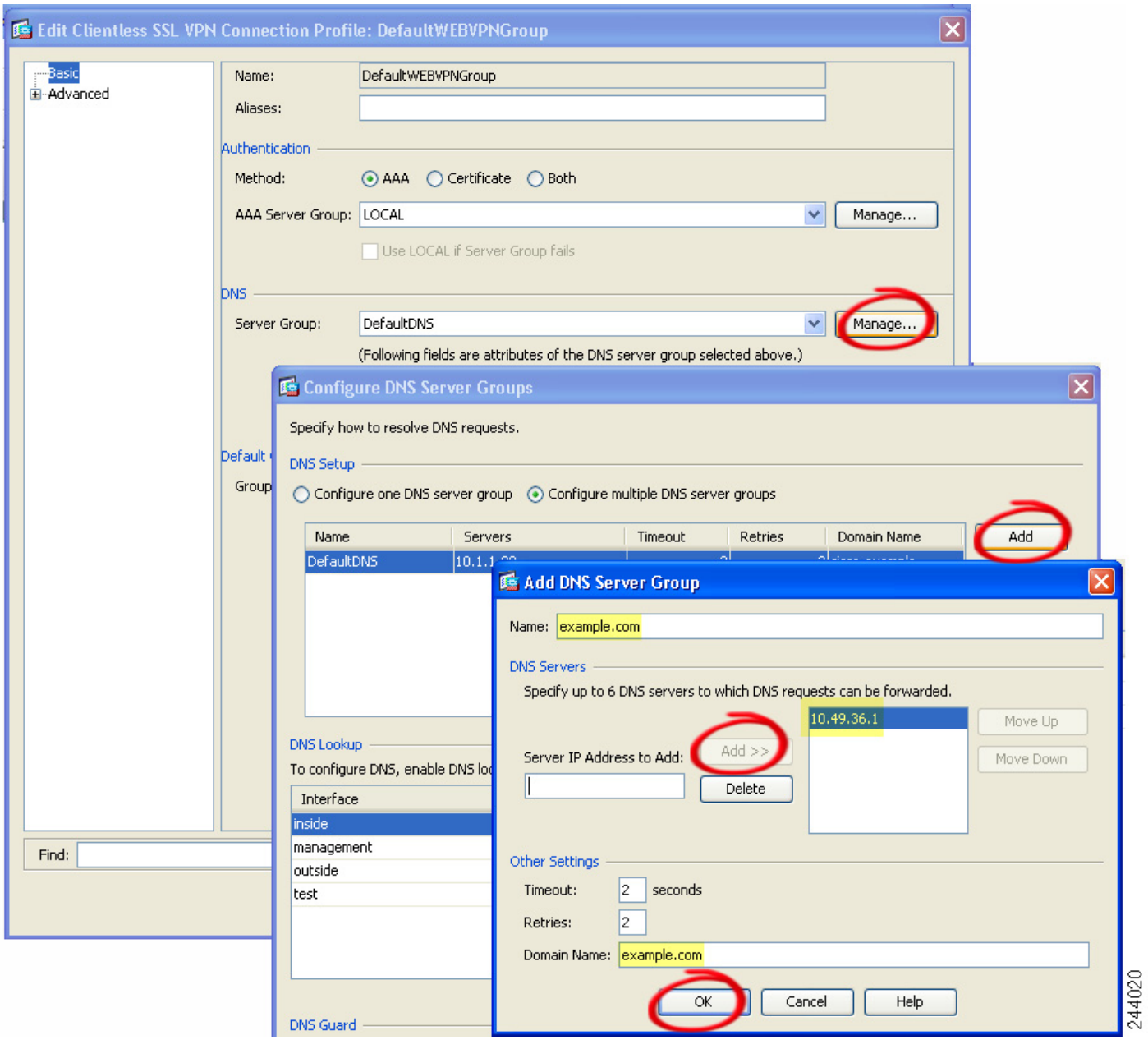
ウィンドウに、DNS サーバのエントリの一覧表が表示されます。

ステップ 6　[Add] をクリックします。

[Add DNS Server Group] ウィンドウが開きます。

ステップ 7　[Name] フィールドに新しいサーバ グループ名を入力し、IP アドレスとドメイン名を入力します（図 11-4 を参照）。

図 11-4　ポート転送の DNS サーバ値の例



入力したドメイン名を書き留めます。後ほど、ポート転送エントリを設定する際、リモートサーバを指定するために必要になります。

ステップ 8　[Connection Profiles] ウィンドウが再度アクティブになるまで、[OK] をクリックします。

ステップ 9　クライアントレス接続の設定で使用される、残りすべての接続プロファイルについて、手順 2 ～8 を繰り返します。

ステップ 10　[Apply] をクリックします。

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。

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。

ポート転送エントリの追加と編集

[Add/Edit Port Forwarding Entry] ダイアログボックスでは、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 アプリケーションを指定できます。これらのウィンドウで属性に値を割り当てるには、次の手順を実行します。

前提条件

トンネルを確立し、IP アドレスに解決するには、「ポート転送リストの割り当て」（P.11-18）に記載のとおり、[Remote Server] パラメータに割り当てた DNS 名が、[Domain Name] および [Server Group] パラメータと一致する必要があります。[Domain] および [Server Group] パラメータのデフォルト設定は、いずれも DefaultDNS です。

手順の詳細

ステップ 1　[Add] をクリックします。

ステップ 2　アプリケーションが使用する TCP ポート番号を入力します。ローカル ポート番号は、1 つの listname に対して一度だけ使用できます。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

ステップ 3　リモート サーバのドメイン名または IP アドレスを入力します。特定の IP アドレスに対してクライアント アプリケーションを設定しなくて済むよう、ドメイン名を使用することをお勧めします。

ステップ 4　そのアプリケーション用の well-known ポート番号を入力します。

ステップ 5　アプリケーションの説明を入力します。最大で 64 文字まで指定可能です。

ステップ 6　（オプション）ポート転送リストを強調表示し、[Assign] をクリックして、選択したリストを 1 つ以上のグループ ポリシー、ダイナミック アクセス ポリシー、またはユーザ ポリシーに割り当てます。

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。
- ユーザのログイン時にポート転送アクセスをイネーブル化するが、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ようにユーザに要求する。

(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。

手順の詳細

[Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックスでは、次のものを追加または編集できます。

ステップ 1　リストの英数字の名前を指定します。最大で 64 文字まで指定可能です。

ステップ 2　アプリケーションのトラフィックを受信するローカル ポートを入力します。ローカル ポート番号は、1 つの listname に対して一度だけ使用できます。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

(注)　リモート サーバの IP アドレスまたは DNS 名を入力します。特定の IP アドレスに対してクライアント アプリケーションを設定しなくて済むよう、ドメイン名を使用することをお勧めします。

ステップ 3　アプリケーションのトラフィックを受信するリモート ポートを入力します。

ステップ 4　TCP アプリケーションの説明を入力します。最大で 64 文字まで指定可能です。

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。

ポート転送をイネーブルにした場合、ユーザはクライアントレス SSL VPN ポータル ページの [Application Access] > [Start 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。

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。

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 Receiver 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 アプリケーションなど、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 Receiver 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 Receiver 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 セキュア モビリティ クライアントを使用し、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 Receiver 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 Access Gateway 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。

VDI サーバの設定

1 サーバの場合：

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] を選択します。
2. [Enable VDI Server Proxy] チェックボックスをオンにし、VDI サーバを設定します。

複数のグループ ポリシーを VDI サーバに割り当てる場合：

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] を選択します。
2. [Configure All VDI Servers] チェックボックスをオンにします。
3. VDI サーバを追加し、1 つ以上のグループ ポリシーを割り当てます。

VDI プロキシ サーバの設定

1 グループ ポリシーが割り当てられた 1 つの VDI サーバ：

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] を選択します。
2. [Enable VDI Server Proxy] チェックボックスをオンにし、VDI サーバを設定します。

複数のグループ ポリシーを VDI サーバに割り当てる場合：

1. [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] の順に移動します。
2. [Configure All VDI Servers] チェックボックスをオンにします。
3. VDI サーバを追加し、1 つ以上のグループ ポリシーを割り当てます。

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。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] を参照します。

ステップ 2　DfltGrpPolicy を編集し、左側のメニューから [More Options] メニューを展開します。

ステップ 3　[VDI Access] を選択します。[Add] または [Edit] をクリックして、VDI サーバの詳細を表示します。

- [Server (Host Name or IP Address)]：XenApp または XenDesktop サーバのアドレス。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。
- [Port Number (Optional)]：Citrix サーバに接続するためのポート番号。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。
- [Active Directory Domain Name]：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。
- [Use SSL Connection]：サーバに SSL を使用して接続する場合、チェックボックスをオンにします。
- [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。

	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/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 ファイルを解凍します。
- 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みます。
- 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、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 リストにメイン メニュー オプションとオプションを追加します。

  表 11-3 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 11-3　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 の前にクライアントレス 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。