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

各 URL の書き換え

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 *1*：ユーザが入力した *URL* の例

図 *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

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 エントリの横にある [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

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]** に移動します。

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]** に移動し、[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。

信頼できる証明書のプール

ASA は trustpool に信頼できる証明書をグループ化します。trustpool 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一連のデフォルト証明書が含まれています。これらの証明書は、管理者がアクティブ化するまで機能しません。

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、サーバは自身を証明するために認証局（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。

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、そのリモートサーバが信頼できるか、および適切なリモート サーバに接続しているかを確認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。

[Configuration] > **[Remote Access VPN]** > **[Certificate Management]** > **[Trusted Certificate Pool]** で、https サイトへの SSL 接続に対して証明書検証を有効にすることができます。また、信頼できる証明書プール内の証明書も管理できます。

（注） ASA trustpool は Cisco IOS trustpool に類似していますが、同一のものではありません。

HTTP サーバ検証の有効化

手順

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

ステップ 3 サーバを検証できなかった場合は、[Disconnect User From HTTPS Site] をクリックして切断します。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。

手順

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。

- 署名検証が失敗したり、バンドルをインポートできない場合に、バンドルをインポートするように設定して、後で個別の証明書エラーを修正します。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。

手順

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。

信頼できる証明書プールのポリシーの編集

手順

ステップ 1 [Revocation Check]：プール内の証明書が失効しているかどうかをチェックするように設定し、さらに、失効のチェックに失敗した場合に、CLR または OCSP のいずれを使用するか、および証明書を無効にするかどうかを選択するように設定します。

ステップ 2 [Certificate Matching Rules]：失効または期限切れのチェックから除外する証明書マップを選択します。証明書マップは、AnyConnect またはクライアントレス SSL 接続プロファイル（別名「トンネル グループ」）に証明書をリンクします。

これらの証明書マップの詳細については、証明書/接続プロファイル マップのルール を参照してください。

ステップ 3 [CRL Options]：CRL キャッシュの更新頻度を 1 ～ 1440 分（24 時間）の間隔で指定します。

ステップ 4 [Automatic Import]：シスコでは、信頼済み CA の「デフォルト」のリストを定期的に更新しています。[Enable Automatic Import] をオンにして、デフォルト設定を保持するように指定した場合、ASA は 24 時間ごとにシスコのサイトで信頼済み CA の最新リストをチェックします。リストが変更されると、ASA は新しいデフォルトの信頼済み CA リストをダウンロードしてインポートします。

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。

信頼できる証明書プールのポリシーの編集

手順

ステップ 1 [Revocation Check]：プール内の証明書が失効しているかどうかをチェックするように設定し、さらに、失効のチェックに失敗した場合に、CLR または OCSP のいずれを使用するか、および証明書を無効にするかどうかを選択するように設定します。

ステップ 2 [Certificate Matching Rules]：失効または期限切れのチェックから除外する証明書マップを選択します。証明書マップは、AnyConnect またはクライアントレス SSL 接続プロファイル（別名「トンネル グループ」）に証明書をリンクします。

これらの証明書マップの詳細については、証明書/接続プロファイル マップのルール を参照してください。

ステップ 3 [CRL Options]：CRL キャッシュの更新頻度を 1 ～ 1440 分（24 時間）の間隔で指定します。

ステップ 4 [Automatic Import]：シスコでは、信頼済み CA の「デフォルト」のリストを定期的に更新しています。[Enable Automatic Import] をオンにして、デフォルト設定を保持するように指定した場合、ASA は 24 時間ごとにシスコのサイトで信頼済み CA の最新リストをチェックします。リストが変更されると、ASA は新しいデフォルトの信頼済み CA リストをダウンロードしてインポートします。

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

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 では、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。

- （Cisco 配布のプラグイン限定）URL で指定された jar ファイルのアンパック
- 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、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。

次に、以降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 メニューとアドレス フィールドの変更点を示します。

表 *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	セキュア シェル	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。

プラグインに伴う前提条件

- プラグインへのリモート アクセスを実現するには、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。
- プラグインを使用するには、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、『サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ』の互換性マトリクスを参照してください。

プラグインの使用上の制限

（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、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

始める前に

ASA インターフェイス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。

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

ステップ 1 クライアントレス SSL VPN が ASA で有効になっているかどうかを示します。

show running-config

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て、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。

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。

始める前に

ASA のインターフェイス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 *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。 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。	

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。 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

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。

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されたセッションが保持されません。フェールオーバー後に Citrix ユーザを再認証する必要があります。

Citrix プラグインの作成とインストール

始める前に

セキュリティ アプリケーションをプラグイン用に準備する必要があります。

（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。

手順

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] の順に選択し、[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て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）と 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

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。

ポート転送の前提条件

- 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）8u131 b11、7u141 b11、6u151 b10 以降がインストールされていることを確認します。
- macOS 10.12 上で Safari を使用しているブラウザベースのユーザは、ASA の URL と共に使用するためにクライアント証明書を特定する必要があります。Safari の URL 解釈方法により、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指定します。次に例を示します。
  - https://example.com/
  - https://example.com
- ポート転送またはスマート トンネルを使用する Microsoft Windows 7 SP1 以降のユーザは、ASA の URL を信頼済みサイト ゾーンに追加します。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。Windows 7 SP1（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。

ポート転送に関する制限事項

- 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 接続によってそれを更新できない場合、ポート転送アプレットでは、ローカル ポートとリモート ポートが同一のものとして表示されます。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

ポート転送機能は、解決および接続のために、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。

手順

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 設定でクライアントレス接続に対してデフォルトのクライアントレス SSL VPN グループ エントリを使用する場合は、そのエントリを強調表示し、[Edit] をクリックします。エントリを使用しない場合は、設定でクライアント接続に対して使用する接続プロファイルを強調表示し、[Edit] をクリックします。

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。

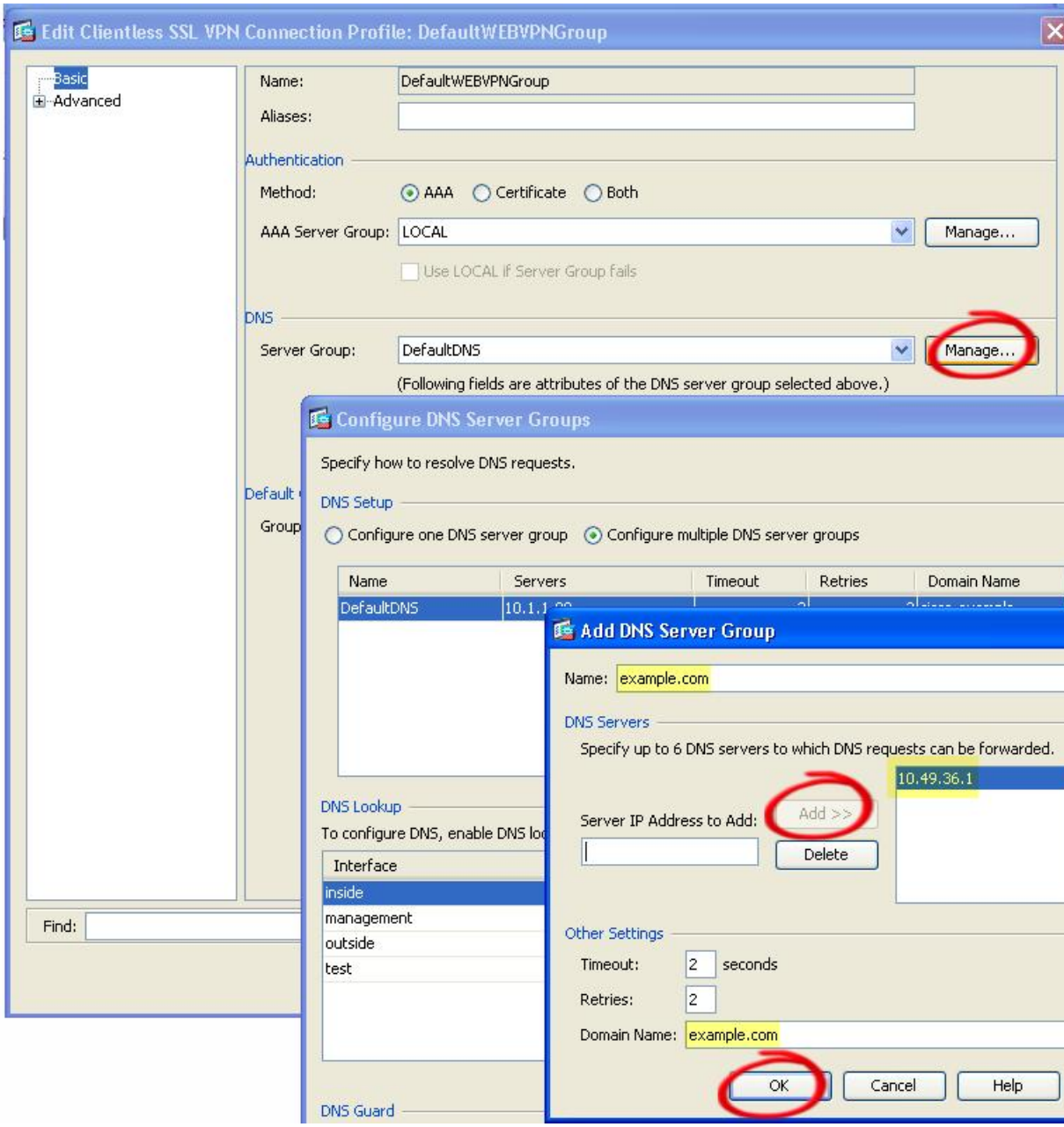
ステップ 4 [DNS] 領域で [Manage] をクリックします。

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

ステップ 6 [Add] をクリックします。

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 *3* : 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 設定でクライアントレス接続に使用する残りの接続プロファイルすべてに対して、手順を繰り返します。

ステップ 10 [適用（Apply）] をクリックします。

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。

始める前に

トンネルを確立して IP アドレスを解決するには、[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

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、リスト名ごとに 1 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 （任意） 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 フォワーディング 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。

（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。

- ユーザのログイン時に自動的にポート フォワーディング アクセスを開始する。
- ユーザのログイン時にポート フォワーディング アクセスをイネーブル化する。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 Applications] を使用して、ポート フォワーディングを手動で開始する必要がある。

手順

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、リスト名ごとに 1 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 フォワーディングのイネーブル化と切り替え

デフォルトでは、ポート フォワーディングはオフになっています。

ポート フォワーディング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、手動でポート フォワーディングを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 はリストを取得して、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。

ポータルページのメニュー内またはクライアントレス SSL VPN セッション中に表示されるツールバー上にある、[Browse Networks] をリモート ユーザがクリックすると、ASA は、通常、ASA と同じネットワーク上またはこのネットワークからアクセス可能な場所にある、マスターブラウザ、WINS サーバ、または DNS サーバを使用して、サーバ リストをネットワークに照会します。

マスター ブラウザまたは DNS サーバは、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、ASA 上の CIFS/FTP クライアントに表示します。

（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

ユーザが `\\server\share\subfolder\personal` フォルダにアクセスするには、少なくとも、共有自体を含めたすべての親フォルダに対する読み取り権限を持っている必要があります。

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。

Web フォルダからワークステーションのフォルダにファイルをドラッグ アンド ドロップすると、一時ファイルのように見えることがあります。ビューを更新し、転送されたファイルを表示するには、ワークステーションのフォルダを更新します。

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

（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ことを DNS サーバに要求します。

SharePoint アクセスのためのクロックの正確性の確保

ASA 上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 の時間が正しくないと、SharePoint サーバ上の文書にアクセスしたときに、ASA で設定されたクッキーの有効期間によって Word が正常に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 サーバと時間をダイナミックに同期させるように、ASA を設定することをお勧めします。手順については、一般的操作用コンフィギュレーション ガイドで「日付と時刻の設定」に関する項を参照してください。

Virtual Desktop Infrastructure（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。

VDI の制限事項

- 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。

Citrix の制限

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 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ための 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。

手順

ステップ 1 モバイル ユーザが Citrix Receiver を起動し、ASA の URL に接続します。

ステップ 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。

ステップ 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。

次のタスク

http://www.youtube.com/watch?v=JMM2RzppaG8：このビデオでは、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 サーバまたは VDI プロキシ サーバの設定

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [VDI Access] の順に選択します。

ステップ 2 1 つのサーバで、[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。

ステップ 3 VDI サーバに複数のグループ ポリシーを割り当てるには、[Configure All VDI Servers] をオンにします。

ステップ 4 [Add a VDI Server] を選択し、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。

手順

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。

ステップ 4 [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は、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。

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可能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。

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 では、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。

- （Cisco 配布のプラグイン限定）URL で指定された jar ファイルのアンパック
- 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、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。

次の表に、以降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 メニューとアドレス フィールドの変更点を示します。

表 *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。

ブラウザ プラグインのインストールの前提条件

- 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。

ブラウザ プラグインのインストールに関する要件

- 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 アクセスを実現するには、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。
- プラグインを使用するには、ブラウザで ActiveX または Oracle Java ランタイム環境（JRE）が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 プラグインのセットアップ

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。

手順

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

手順

ステップ 1 ASA インターフェイス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。

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。