



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



(注) シスコは、ASA バージョン 9.17(1) で有効なクライアントレス SSL VPN の非推奨機能を発表しました。9.17(1) より前のリリースでは、限定的なサポートが継続されます。より堅牢で新しいソリューション（たとえば、リモート Duo ネットワークゲートウェイ、AnyConnect、リモートブラウザの分離機能など）への移行オプションに関する詳細なガイダンスを提供します。

- [各 URL の書き換え \(1 ページ\)](#)
- [ポータル ページでの URL エントリのオフへの切り替え \(2 ページ\)](#)
- [信頼できる証明書のプール \(2 ページ\)](#)
- [プラグインへのブラウザ アクセスの設定 \(5 ページ\)](#)
- [ポート転送の設定 \(11 ページ\)](#)
- [ファイル アクセスの設定 \(18 ページ\)](#)
- [SharePoint アクセスのためのクロックの正確性の確保 \(21 ページ\)](#)
- [Virtual Desktop Infrastructure \(VDI\) \(21 ページ\)](#)
- [SSL を使用した内部サーバーへのアクセス \(24 ページ\)](#)
- [クライアント/サーバー プラグインへのブラウザ アクセスの設定 \(31 ページ\)](#)

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。ユーザーは、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ー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ーが混乱しないようにすることをお勧めします。

図 1: ユーザーが入力した 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



ポータル ページでの URL エントリのオフへの切り替え

ユーザーがブラウザ 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。

始める前に

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ーのグループ 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

ステップ 1 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。

webvpn

ステップ 2 ユーザーが HTTP/HTTPS URL を入力する機能を制御します。

url-entry

ステップ 3 (任意) URL エントリをオフに切り替えます。

url-entry disable

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、crypto ca import default コマンドを発行して、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 サーバーに接続する場合、サーバー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、サーバー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 対応サーバーに接続する場合は、そのリモートサーバーが信頼できるか、および適切なリモートサーバー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 サーバー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。

trustpool 証明書の自動インポートの設定

スマートライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA は、サーバー証明書の発行階層が変更された場合に証明書の検証をサポートするようになりました。カスタマーが証明書階層の変更を調整する必要はありません。CA サーバーの自己署名証明書が変更された場合に、Smart Call Home がアクティブな状態を維持できるように、定期的な trustpool バンドルの更新を自動化できます。この機能はマルチコンテキスト展開ではサポートされません。

trustpool の証明書バンドルを自動的にインポートするには、ASA がバンドルのダウンロードとインポートに使用する URL を指定する必要があります。次のコマンドを入力すると、デフォルトの Cisco URL とデフォルトの時間 (22 時間) を使用して、毎日一定の間隔でインポートが実行されます。

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

また、次のコマンドを使用して、カスタム URL による自動インポートをイネーブルにできます。

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

オフピーク時またはその他の都合のよい時間帯に柔軟にダウンロードを設定できるようにするには、次のコマンドを入力して、カスタム時間によるインポートをイネーブルにします。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

カスタム URL とカスタム時間の両方による自動インポートを設定するには、次のコマンドを使用する必要があります。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

trustpool ポリシーのステータスの表示

trustpool ポリシーの現在のステータスを表示するには、次のコマンドを使用します。

```
show crypto ca trustpool policy
```

このコマンドは次のような情報を返します。

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
  State: Not in progress
  Last import result: Not attempted N/A
  Current Jitter: 0

Trustpool auto import statistics:
  Last import result: N/A
  Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

Trustpool revocation checking is disabled.
CRL cache time: 60 seconds
CRL next update field: required and enforced
Auto import of trustpool is enabled
Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
Download time: 22:00:00

Policy Overrides:
  None configured
```

CA Trustpool のクリア

trustpool ポリシーをデフォルト状態にリセットするには、次のコマンドを使用します。

```
clear configure crypto ca trustpool
```

トラストポイント証明書の自動インポートはデフォルトでオフになるので、次のコマンドを使用して機能をディセーブにします。

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。
- 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。

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ー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があります。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ーがポータル 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ーが選択して [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、サーバー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 サーバーの属性で 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。ユーザー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。リモートユーザーは、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、リモートユーザー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	<p>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。</p> <p>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。</p> <p>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。</p>	http://properjavardp.sourceforge.net/
RDP2	<p>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。</p> <p>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。</p> <p>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。</p>	
SSH	<p>Secure Shell-Telnet プラグインにより、リモート ユーザーはリモート 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。</p> <p>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。</p>	http://javassh.org/
VNC	<p>Virtual Network Computing プラグインを使用すると、リモート ユーザーはリモート デスクトップ共有 (VNC サーバー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、モニター、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。</p>	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](http://www.cisco.com/go/asa) サイトで入手できます。



- (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、`cisco-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。

手順

ステップ 1 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。

import webvpn plug-in protocol [rdp | rdp2] [ssh | telnet] | vnc *URL*

- (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** を入力する場合、両者の間にスペースは挿入しません。これによって、Secure Shell サービスと Telnet サービスの両方にプラグイン アクセスを提供します。

例：

次に、TFTP または FTP サーバーのホスト名またはアドレスと、URL がプラグイン .jar ファイルへのリモートパスであるプラグインへのパスを入力する例を示します。

```
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:/cisco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

ステップ 2 (任意) 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。

revert webvpn plug-in protocol *protocol*

例：

```
hostname# revert webvpn plug-in protocol rdp
```

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 ユーザーは、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 ユーザー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 サーバー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 サーバーの 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

ステップ 1 クライアントレス SSL VPN のユーザーが使用できる 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。

例：

```
hostname# show import webvpn plug
ssh
rdp
vnc
ica
```

ステップ 2 プラグインのハッシュおよび日付を含めます。

例：

```
hostname show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tues, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTs PnjdBoo= Tues, 15 Sep 2009 23:23:56 GMT
```

ポート転送の設定

ポート転送により、ユーザー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、ユーザー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ー接続を要求しないことにより、ユーザー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、ユーザー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ーは、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 以降のユーザーは、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）ユーザー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。ユーザー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、ユーザー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、エンドユーザーの 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、ユーザー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、リモートサーバー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。ポート転送アプレットから DNS 要求を受け入れるように、次のように ASA を設定します。

手順

ステップ 1 DNS サーバー グループ モードを開始して、`example.com` という名前の DNS サーバー グループを設定します。

例：

```
hostname (config) # dns server-group example.com
```

ステップ 2 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。

例：

```
hostname (config-dns-server-group) # domain-name example.com
```

ステップ 3 ドメイン名を IP アドレスに解決します。

例：

```
hostname (config-dns-server-group) # name-server 192.168.10.10
```

ステップ 4 クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。

webvpn

ステップ 5 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。

tunnel-group webvpn

ステップ 6 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。

例：

```
asa2 (config-dns-server-group) # exit  
asa2 (config) # tunnel-group DefaultWEBVPNGroup webvpn-attributes  
asa2 (config-tunnel-webvpn) # dns-group example.com
```

ポート転送に対するアプリケーションの適格化

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、アプリケーションがアクセスの提供に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ー名は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。

手順

ステップ 1 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。

```
show run webvpn port-forward
```

ステップ 2 クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。

```
webvpn
```

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ー名に割り当てます。

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ー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ー名ごとに、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ー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。

- ユーザー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。

始める前に

port-forward enable list name コマンドを開始する前に、ユーザーは、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。

これらのコマンドは、各グループポリシーとユーザー名で使用可能です。各グループポリシーとユーザー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せん。そのため、1つのコマンドが入力されると、ASA は、該当のグループポリシーまたはユーザー名のコンフィギュレーションに存在するコマンドを新しいコマンドと置き換えます。最後

のコマンドの場合は、グループポリシーまたはユーザー名のコンフィギュレーションにすでに存在する **port-forward** コマンドが削除されるだけです。

手順

ステップ 1 ユーザーのログイン時に自動的にポート フォワーディングを開始します。

```
port-forward auto-start <list name>
```

ステップ 2 ユーザー ログイン時のポート フォワーディングを許可または禁止します。

```
port-forward enable <list name>
```

```
port-forward disable
```

ステップ 3 (任意) **port-forward** コマンドがグループポリシーまたはユーザー名のコンフィギュレーションから削除され、[no] **port-forward** コマンドがデフォルト グループ ポリシーから継承されます。no **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により削除対象をその名前の **port-forward** コマンドに限定します。

```
no port-forward [ auto-start <list name> | enable <list name> | disable ]
```

ポート転送の自動化

ユーザー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

ステップ 1 クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。

```
webvpn
```

ステップ 2 グループ ポリシーまたはユーザー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。

```
group-policy webvpn または username webvpn
```

ステップ 3 ユーザーのログイン時に自動的にポート フォワーディングを開始します。

```
port-forward auto-start list_name
```

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の既存の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ー名に割り当てることはできません。

例 :

次のコマンドは、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。

```
hostname (config-group-policy) # webvpn
hostname (config-group-webvpn) # port-forward auto-start apps1
```


ステップ4 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。

```
show run webvpn port-forward
```

ステップ5 (任意) グループ ポリシーまたはユーザー名から port-forward コマンドを削除し、デフォルトに戻します。

```
no port-forward
```

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。

手順

ステップ1 ポート フォワーディングを有効にします。

port-forward auto-start *list_name* を入力した場合は、手動でポート フォワーディングを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既存のポート フォワーディング リストの名前です)。複数のポート フォワーディング リストをグループ ポリシーまたはユーザー名に割り当てることはできません。

```
port-forward [enable <list name> | disable]
```

例 :

次のコマンドは、apps1 という名前のポート フォワーディング リストをグループ ポリシーに割り当てます。

```
hostname(config-group-policy)# webvpn  
hostname(config-group-webvpn)# port-forward enable apps1
```

ステップ2 ポート フォワーディング リストのエントリを表示します。

```
show running-config port-forward
```

ステップ3 (任意) グループ ポリシーまたはユーザー名から port-forward コマンドを削除し、デフォルトに戻します。

```
no port-forward
```

ステップ4 (任意) ポート フォワーディングをオフに切り替えます。

```
port-forward disable
```

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 ユーザーに 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、ユーザー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 アクセスをユーザーに提供します。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。

ユーザー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ーの 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ーに照会します。ASA はリストを取得して、ポータル ページ上のリモート ユーザーに送信します。

クライアントレス SSL VPN は、ユーザーの認証要件とファイルのプロパティに応じて、ユーザーが次の CIFS および FTP の機能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ー、サーバー内部の共有、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 ユーザーがクリックすると、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 サーバー、または DNS サーバーを使用して、サーバー 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 サーバーは、クライアントレス SSL VPN がリモート ユーザー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、ユーザー アクセス用のサーバー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

ユーザーが \\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 サーバー機能は、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ー 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、ユーザーが `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 サーバー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 サーバーは必要ありません。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 サーバーに要求します。

手順

ステップ 1 クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。

```
webvpn
```

ステップ 2 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。

```
tunnel-group webvpn
```

ステップ 3 各 NetBIOS ネーム サーバー (NBNS) のネットワークまたはドメインをブラウズします。

```
nbns-server {IPaddress | hostname} [master] [timeout timeout] [retry retries]
```

- **master** は、マスターブラウザとして指定す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 サーバーは、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 サーバー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ーは最大 3 つまで指定できます。

- *timeout* は、ASA がクエリーを再度サーバーに送信する前に待機する秒数です。このとき、サーバーが1つだけの場合は同じサーバーに送信され、サーバーが複数存在する場合は別のサーバーに送信されます。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 サーバー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ー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。

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
```

ステップ4 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 サーバーを表示します。

show tunnel-group webvpn-attributes

ステップ5 (任意) 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ー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、ユーザーは、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。

character-encoding charset

charset は、最大 40 文字からなる文字列で、<http://www.iana.org/assignments/character-sets> で指定されている有効文字セットのいずれかと同じです。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ー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ーを置換し、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ーを削除する必要があります。

例：

次に、日本語 Shift_JIS 文字をサポートする *character-encoding* 属性を設定し、フォントファミリーを削除し、デフォルトの背景色を保持する例を示します。

```
hostname (config) # webvpn
hostname (config-webvpn) # character-encoding shift_jis
hostname (config-webvpn) # customization DfltCustomization
hostname (config-webvpn-custom) # page style background-color:white
```

ステップ6 (任意) 特定の CIFS サーバー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号化が必要な各 CIFS サーバーに対し、異なるファイル符号化値を使用できます。

file-encoding {*server-name* | *server-ip-address*} *charset*

例：

次に、CIFS サーバー 10.86.5.174 のファイルエンコーディング属性を設定して、IBM860（エイリアス「CP860」）文字をサポートする例を示します。

```
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
```

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 サーバーは、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 サーバー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 サーバー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 サーバーおよび VMware VDI サーバー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ーの実行中の 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 サーバーには、他のサーバー 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 サーバーおよび XenDesktop サーバーにインストールし、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ーは、次を実行して Citrix サーバーに接続できません。

- AnyConnect で ASA に接続してから Citrix サーバーに接続する。
- AnyConnect クライアントを使用せずに ASA を介して Citrix サーバーに接続する。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 サーバーは、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 サーバー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 サーバーおよび XenDesktop サーバーにインストールし、設定する必要があります。

Citrix Mobile Receiver のユーザー ログオンについて

Citrix サーバーに接続しているモバイルユーザーのログオンは、ASA が Citrix サーバーを VDI サーバーとして設定したか、または VDI プロキシサーバーとして設定したかによって異なります。

Citrix サーバーが VDI サーバー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 サーバー クレデンシャルで Citrix サーバーに接続します（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 プロキシサーバーとして設定されている場合：

1. Citrix Mobile Receiver を使用し、VPN と Citrix サーバー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 サーバーをプロキシするための ASA の設定

ASA を Citrix サーバー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 サーバーへの接続であるかのようにユーザー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。

手順

- ステップ 1** モバイルユーザーが 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 サーバー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 サーバーに接続する場合に必要なのは、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 サーバー情報が ASA に記録され、ASDM に表示されます。

Citrix サーバー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ー名にその VDI サーバーを割り当てます。ユーザー名とグループポリシーの両方を設定した場合は、ユーザー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。

グループポリシーへの VDI サーバーの割り当て

VDI サーバーを設定し、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 サーバーを追加し、サーバー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 サーバーを追加する。

ユーザー名とグループポリシーが両方とも設定されている場合、ユーザー名の設定は、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 サーバーの完全な URL。
- **username** : 仮想化インフラストラクチャサーバーにログインするためのユーザー名。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ー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ー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。

SSL を使用した内部サーバーへのアクセス

手順

ステップ 1 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。

webvpn

ステップ 2 URL エントリをオフに切り替えます。

url-entry disable

クライアントレス SSL VPN は SSL とその後継である TLS1 を使用して、内部サーバーでサポートされている特定の内部リソースと、リモートユーザーとの間のセキュアな接続を実現します。

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) 以降の ASA では、外部インターフェイスのポート 443 で、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が同時にサポートされ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。

手順

ステップ 1 クライアントレス SSL VPN コンフィギュレーションモードに切り替えます。

```
webvpn
```

ステップ 2 クライアントレス SSL VPN の SSL リスニングポートを変更します。

```
port port_number
```

例：

次の例では、外部インターフェイスのポート 444 でクライアント SSL VPN を有効にします。このコンフィギュレーションでは、リモートユーザーは、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。

```
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
```

ステップ 3 (特権モード) ASDM のリスニングポートを変更します。

```
http server enable
```

例：

この例では、HTTPS ASDM セッションが外部インターフェイスのポート 444 を使用するよう指定します。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、リモートユーザーは `https://<outside_ip>:444` を入力して ASDM セッションを開始します。

```
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
```

クライアントレス SSL VPN セッションでの HTTPS の使用

HTTPS の設定に加えて、Web サイトをプロトコルダウングレード攻撃や cookie ハイジャックから保護するのに役立つ Web セキュリティ ポリシーメカニズムである HTTP Strict-Transport-Security (HSTS) を有効にします。HSTS は、UA およびブラウザを HTTPS Web

サイトにリダイレクトし、次のディレクティブを送信することにより指定したタイムアウト期限が切れるまで Web サーバーに安全に接続します。

```
http-headers: hsts-server; enable; max-age="31536000"; include-sub-domains; no preload
```

それぞれの説明は次のとおりです。

http-headers : ASA からブラウザに送信されるさまざまな HTTP ヘッダーを設定します。サブモードを設定するか、すべての **http-headers** 設定をリセットします。

- **hsts-client** : HSTS クライアントとして機能する HTTP サーバーからの HSTS ヘッダーの処理を開始します。
 - **enable** : HSTS ポリシーを有効または無効にすることができます。有効にすると、既知の HSTS ホストと HSTS ヘッダーに対して HSTS ポリシーが適用されます。
- **hsts-server** : ASA からブラウザに送信する HSTS ヘッダーを設定します。ASA はヘッダーを基に、HTTP ではなく HTTPS を使用したアクセスのみを許可するようブラウザに指示します。
 - **enable** : HSTS ポリシーを有効または無効にすることができます。有効にすると、既知の HSTS ホストと HSTS ヘッダーに対して HSTS ポリシーが適用されます。
 - **include-sub-domains** : ドメイン所有者は、Web ブラウザの HSTS プリロードリストに含める必要があるドメインを送信できます。



(注) HTTPS サイトからの追加リダイレクトを設定するには、(リダイレクト先のページではなく) リダイレクトに HSTS ヘッダーを保持しておく必要があります。

- **max-age** : (設定可能) Web サーバーが HSTS ホストとしてみなされ、HTTPS のみを使用してセキュアにアクセスされる必要のある時間を秒単位で指定します。デフォルトは 3153600 秒 (1 年) です。範囲は 0 ~ 2147483647 秒です。
- **preload** : ブラウザに対し、すでに UA およびブラウザに登録され、HSTS ホストとして取り扱う必要のあるドメインのリストの読み込みを指示します。プリロードされたリストの実装は UA およびブラウザに依存し、各 UA およびブラウザは他のディレクティブの振る舞いに対して追加の制限を指定することができます。たとえば、Chrome のプリロードリストは、HSTS の最大寿命が少なくとも 18 週 (10,886,400 秒) であることを指定します。
- **x-content-type-options** : 「X-Content-Type-Options: nosniff」応答ヘッダーの送信を有効にします。
- **x-xss-protection** : 「X-XSS-Protection: 1[; mode=block]」応答ヘッダーの送信を有効にします。
- **content-security-policy** : ASA からブラウザに WebVPN 接続用の「Content-Security-Policy」ヘッダーを送信することを有効または無効にでき、次のディレクティブを設定できます。

- **default-src** : 他の CSP ディレクティブのデフォルトソースリストを設定します。ここで、<sources> は URL (または URL のリスト) またはキーワードソース (*self*、*none* など) です。
- **frame-ancestors** : ユーザーエージェントが、*frame*、*iframe*、*object*、*embed*、または *applet* 要素、もしくは HTML 以外のリソースにおける同等の機能を使用したリソースの埋め込みを許可するかどうかを示します。ここで、<sources> は URL (または URL のリスト) またはキーワードソース (*self*、*none* など) です。

手順

ステップ 1 クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。

webvpn を入力します。

ステップ 2 *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。

enable interface-name と入力します。

ステップ 3 **http-headers** のサブモードを入力するか、**http-headers** を入力してすべての http-header 設定をリセットします。このコマンドは、ASA からブラウザに送信されるさまざまな HTTP ヘッダーを設定します。

ステップ 4 **hsts-client** または **hsts-server** を入力し、**enable** を入力します。

ステップ 5 **include-sub-domains** を入力します。

ステップ 6 **preload** を入力します。

ステップ 7 HSTS の有効時間 (秒数) を設定します。

hsts max-age max-age-in-seconds と入力します。

値の範囲は <0 ~ 31536000> 秒です。デフォルトは 10,886,400 (18 週) です。この制限に達すると、HSTS は有効ではなくなります。

例

```
hostname (config-webvpn) # http-headers
hostname (config-webvpn-http-headers) # hsts-server or hsts-client
hostname (config-webvpn-http-headers-hsts-srv) # enable
hostname (config-webvpn-http-headers-hsts-srv) # include-sub-domains
hostname (config-webvpn-http-headers-hsts-srv) # preload
hostname (config-webvpn-http-headers-hsts-srv) # max-age 31536000
hostname (config-webvpn-http-headers-hsts-srv) # content-security-policy enable
hostname (config-webvpn-http-headers-hsts-srv-content-security-policy) # default-src
'self',http,https://example.com
hostname (config-webvpn-http-headers-hsts-server-content-security-policy) # frame-ancestors
'self',https://example.com
```

次のタスク

現在の設定を参照するには、**show running-config webvpn [hsts]** を使用します。

現在の設定をクリアするには、**clear configure webvpn** を使用します。

プロキシ サーバーのサポートの設定

ASA は HTTPS 接続を終了させて、HTTP および HTTPS 要求をプロキシ サーバーに転送できます。これらのサーバーは、ユーザーとパブリック 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 サーバー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。

始める前に

プロキシ自動設定 (PAC) ファイルを HTTP プロキシサーバー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。

手順

-
- ステップ 1** クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
- webvpn**
- ステップ 2** 外部プロキシサーバーを使用して HTTP および HTTPS 要求を処理するように ASA を設定します。
- http-proxy and https-proxy**
- (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 プロキシを設定します。
- http-proxy host [port] [exclude url] [username username {password password}]**
- ステップ 4** HTTPS プロキシを設定します。
- https-proxy host [port] [exclude url] [username username {password password}]**
- ステップ 5** PAC ファイル URL を設定します。
- http-proxy pac url**
- ステップ 6** (任意) URL をプロキシサーバーに送信される可能性がある URL から除外します。
- exclude**

ステップ 7 外部プロキシサーバーのホスト名または IP アドレスを指定します。

ホスト

ステップ 8 各 URL のプロキシを識別する JavaScript 関数を使用して ASA にプロキシ自動コンフィギュレーション ファイルをダウンロードします。

pac

ステップ 9 (任意) (ユーザー名を指定した場合に限り使用可能) 各プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供します。

password

ステップ 10 各 HTTP または HTTPS 要求とともにプロキシサーバーへのパスワードを送信します。

password

ステップ 11 (任意) プロキシサーバー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。代替の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。

port

ステップ 12 **exclude** を入力した場合は、プロキシサーバー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 までの範囲の任意の 1 文字と一致します。x は ANSI 文字セット内のある 1 文字を表し、y は別の 1 文字を表します。
- ![x-y] は、範囲外の任意の 1 文字と一致します。

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 (任意) 基本的なプロキシ認証のために各 HTTP プロキシ要求にユーザー名を付加します。このキーワードは、**http-proxy host** コマンドでのみサポートされます。

username

ステップ 15 各 HTTP または HTTPS 要求とともにプロキシサーバーへのユーザー名を送信します。

username

ステップ 16 次のように設定されている HTTP プロキシサーバーの使用について設定方法を示します : IP アドレスが 209.165.201.1、デフォルトポートを使用、各 HTTP 要求とともにユーザー名とパスワードを送信。

例：

```
hostname(config-webvpn)# http-proxy 209.165.201.1 user jsmith password
mysecretdonttell
```

ステップ 17 同じコマンドを示しますが、異なる点として、ASA は HTTP 要求で `www.example.com` という特定の URL を受信した場合、プロキシサーバーに渡すのではなく自身で要求を解決します。

例：

```
hostname(config-webvpn)# http-proxy 209.165.201.1 exclude www.example.com
username jsmith password mysecretdonttell
```

ステップ 18 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。

例：

```
hostname(config-webvpn)# http-proxy pac http://www.example.com/pac
```

ASA クライアントレス SSL VPN 設定は、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オーバーライドします。

(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

ポートフォワーディングには、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 のユーザーがいくつかの SSL バージョンに接続する場合、ポートフォワーディングは機能しません。サポートされている JRE バージョンについては、『[サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ](#)』を参照してください。

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付き SSL サーバー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 証明書をユーザーによって 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。

デジタル証明書認証の制限

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。

デジタル証明書による認証および認可については、一般的操作用コンフィギュレーションガイドの「証明書とユーザー 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/サーバー 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ー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があります。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 `cisco-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 クライアント	citrix://

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
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ーがポータル 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ーが選択して [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 サーバー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 サーバーの属性で 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、サーバー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せん。

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。ユーザー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 ユーザー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 ユーザーは、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。

新しい HTML ファイルを使用するための ASA の設定

手順

ステップ 1 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。

```
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#
```

ステップ 2 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。

```
export webvpn customization <file> <URL>
```

例 :

```
hostname# 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
```

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 :

この例では、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。

```
<full-customization>
  <mode>enable</mode>
  <url>/+CSCOU+/login.inc</url>
```

```
</full-customization>
```

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
```

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。