Secure Web Applianceでの復号化証明書の設定

内容

概要

前提条件

- 要件
- 使用するコンポーネント

HTTPS復号化

SWAでの復号化証明書の設定

- ルート証明書とキーのアップロード
- HTTPSプロキシ用の証明書およびキーの生成

証明書のインポート

- SWAへのアップストリームプロキシ証明書のインポート
- 別のSWAへのSWA証明書のインポート
- WindowsクライアントでのSWA証明書のインポート
- MacクライアントでのSWA証明書のインポート
- Ubuntu/DebianでのSWA証明書のインポート
- CentOS 6でのSWA証明書のインポート
- CentOS 5でのSWA証明書のインポート
- Mozilla FirefoxでのSWA証明書のインポート
- Google ChromeでのSWA証明書のインポート
- Microsoft Edge/Internet ExplorerでのSWA証明書のインポート
- SafariでのSWA証明書のインポート
- グループポリシーからクライアントへのSWA証明書のインポート

関連コンテンツ

概要

このドキュメントでは、Secure Web Appliance(SWA)およびプロキシクライアントでHTTPS暗号化証明書を設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SWAへの管理アクセス
- SWAのグラフィックユーザインターフェイス(GUI)へのアクセス

使用するコンポーネント

本書の内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

HTTPS復号化

SWA Hypertext Transfer Protocol Secure(HTTPS)復号化では、アプライアンスにアップロードしたルート証明書と秘密キーファイルを使用してトラフィックを暗号化します。アプライアンスにアップロードするルート証明書と秘密鍵のファイルは、PEM形式である必要があります。



注:DER形式はサポートされていません。

ルート認証局が署名した中間証明書をアップロードすることもできます。SWAは、サーバ証明書を表す証明書を作成すると、アップロードされた証明書を偽装した証明書とともにクライアントアプリケーションに送信します。この方法では、クライアントアプリケーションが信頼するルート認証局(CA)によって中間証明書が署名されている限り、アプリケーションは偽装サーバ証明書を信頼します。

SWAでの復号化証明書の設定

SWAは既存の証明書と秘密キーを使用してHTTPS復号化を行うことができます。ただし、すべてのx.509証明書が機能するとは限らないため、使用する必要がある証明書の種類について混乱が生じる可能性があります。

証明書には、サーバ証明書とルート証明書の2つの主要なタイプがあります。 すべての x.509 証明書に、証明書のタイプを識別する Basic Constraints フィールドが含まれています。

- Subject Type=End Entity：サーバ証明書
- Subject Type=CA：ルート証明書

ルート証明書とキーのアップロード

ステップ 1： GUIで、Security Servicesに移動し、HTTPS Proxyを選択します。
ステップ 2：Edit Settings をクリックします。
ステップ 3：Use Uploaded Certificate and Keyをクリックします。
ステップ 4：CertificateフィールドのBrowseをクリックし、ローカルマシンに保存されている証明書ファイルに移動します。



注：アップロードするファイルに複数の証明書または鍵が含まれている場合、Webプロキシはファイル内の最初の証明書または鍵を使用します。

ステップ 5：KeyフィールドにあるBrowseをクリックして、秘密キーファイルに移動します。



注：キーの長さは、512、1024、または2048ビットである必要があります。

手順 6：キーが暗号化されている場合は、Key is Encryptedを選択します。
手順 7：Upload Filesをクリックして、証明書とキーファイルをSecure Web Applianceに転送します。アップロードされた証明書情報は、Edit HTTPS Proxy Settingsページに表示されます。
ステップ8: (オプション) Download Certificateをクリックして、ネットワーク上のクライアントアプリケーションに転送します。

ステップ 9：変更を送信して確定します。

HTTPSプロキシ用の証明書およびキーの生成

ステップ 1： GUIで、Security Servicesに移動し、HTTPS Proxyを選択します。

ステップ 2：Edit Settings をクリックします。
ステップ 3：Use Generated certificate and keyを選択します。
ステップ 4：Generate New Certificate and Keyをクリックします。
ステップ 5：Generate Certificate and Keyダイアログボックスで、ルート証明書に表示する情報を入力します。Common Nameフィールドには、スラッシュ(/)以外の任意のASCII文字を入力できます。
手順 6：[Generate] をクリックします。
手順 7：生成された証明書情報は、「HTTPSプロキシ設定の編集」ページに表示されます。
ステップ8: (オプション) Download Certificateをクリックし、ネットワーク上のクライアントアプリケーションに証明書を転送できるようにします。
ステップ9: (オプション) 証明書署名要求(CSR)をCAに送信するには、Download Certificate Signing Requestリンクをクリックします。
ステップ10: (オプション) CAから署名付き証明書を受信した後、その証明書をセキュアWebアプライアンス(HTTPS)にアップロードします。この操作は、アプライアンスで証明書を生成した後にいつでも実行できます。
ステップ 11：変更を送信して確定します。

証明書のインポート

SWAへのアップストリームプロキシ証明書のインポート

SWAがアップストリームプロキシを使用するように設定され、アップストリームプロキシがHTTPS復号用に設定されている場合、アップストリームプロキシ暗号化証明書をSWAにインポートする必要があります。信頼できる証明書リストを管理して証明書を追加し、証明書を機能的に削除することができます。

ステップ 1：GUIから、Networkを選択し、Certificate Managementを選択します。
ステップ 2：Certificate ManagementページでManage Trusted Root Certificatesをクリックします。
ステップ 3： シスコが認識するリストではなく、署名権限を持つカスタムの信頼できるルート証明書を追加するには、Importをクリックしてから証明書ファイルを送信します。

ステップ 4：変更を送信して確定します。

別のSWAへのSWA証明書のインポート

HTTPSプロキシ用にHTTPS証明書とキーを1つのSWAにアップロードし、元のファイルにアクセスできる場合は、コンフィギュレーションファイルから別のSWAにインポートできます。

ステップ 1：両方のSWAのGUIから、System Administrationを選択し、Configuration Fileをクリックします。

ステップ 2： ローカルコンピュータでDownloadファイルをクリックして、表示または保存します。

ステップ 3： Configuration FilesでEncrypt passwordsを選択します。

ステップ4: (オプション) Use a user-defined file nameを選択し、必要な名前をコンフィギュレーションファイルに追加します。

ステップ 5：Current Configurationの下にあるSubmitをクリックして、設定.xmlファイルをダウンロードします。

手順 6：ダウンロードしたファイルをテキストエディタまたはXML工ディタで開きます。

手順 7：証明書を使用してSWAからこれらのタグをコピーし、タグ内のすべてのデータをコピーして、他のSWAのコンフィギュレーションファイルで置き換えます。

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>
<prox_config_uploaded_cert>....</prox_config_uploaded_key>
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

ステップ 8：変更内容を移行先SWAの.xmlファイルに保存します。

ステップ 9： 編集後の.xml設定ファイルをインポートしてインポートし直し、移行先のSWAに戻すには、GUIでSystem Administration を選択し、Configuration Fileをクリックします。

ステップ 10：Load Configurationセクションで、Load a configuration file from local computerをクリックします。

ステップ 11：Choose fileをクリックし、編集した.xmlコンフィギュレーションファイルを選択します。

ステップ 12：Loadをクリックし、証明書とキーを使用して新しいコンフィギュレーションファイルをインポートします。

ステップ 13：システムからプロンプトが表示されたら、Commitを使用して変更を確定します。

WindowsクライアントでのSWA証明書のインポート

Microsoft Windowsオペレーティングシステムがインストールされたクライアントコンピュータで、SWA HTTPSプロキシ証明書を信頼できるものとしてインポートするには、次の手順を確認します。

ステップ 1：タスクバーからStartをクリックして、Manage computer certificatesと入力します。
ステップ 2：Certificates-Local Computerページで、Trusted Root Certificationを展開し、Certificatesフォルダを右クリックします。
ステップ 3：All Tasksをクリックし、Importを選択します。
ステップ 4：Certificate Import WizardページでNextをクリックします。
ステップ 5： SWA証明書ファイルをインポートするには、Browseをクリックし、SWAからダウンロードした証明書を選択します。



ヒント:SWA証明書をダウンロードするには、「ルート証明書およびキーのアップロード」または「HTTPSプロキシの証明書およびキーの生成」セクションの「ステップ8」を参照してください。

手順 6：Place all certificates in the followingチェックボックスをクリックします。
手順 7：Trusted Root Certification Authoritiesを選択し、Nextをクリックします。
ステップ 8：[Finish] をクリックします。

または、次のコマンドを実行して、証明書を信頼されたルート証明機関にインポートすることもできます。

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```



注:<Path to SWA Certificate/CertificateName.crt>の部分は、ダウンロード済みの証明書のパスとファイル名に置き換える必要があります。

MacクライアントでのSWA証明書のインポート

ステップ 1：SWAからMac OSクライアントにHTTPSプロキシ証明書をダウンロードします。

ステップ 2：ファイル拡張子を.crtに変更します。
ステップ 3：次のコマンドを実行して、証明書を信頼できる証明書としてインポートします。

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```



注：このファイルは、ダウンロードした証明書のパスとファイル名で置き換える必要があります。

Ubuntu/DebianでのSWA証明書のインポート

ステップ 1：SWAからHTTPSプロキシ証明書をダウンロードします。
ステップ 2： テキストエディタで証明書ファイルを開き、すべての内容をコピーします。
ステップ 3： /usr/local/share/ca-certificates/に新しいファイルを作成し、拡張子を.crtにします。
ステップ 4：目的のテキストエディタでファイルを編集し、コピーしたテキストを新しいファイルに貼り付けて保存します。
ステップ 5： オペレーティングシステムの証明書を更新するには、次のコマンドを実行します。

```
sudo update-ca-certificates
```



ヒント：証明書がクライアントにローカルに保存されている場合は、証明書を/usr/local/share/ca-certificates/にコピーしてsudo update-ca-certificatesを実行できます。



注：バージョンによっては、sudo apt-get install -y ca-certificatesコマンドを使用してca-certificatesパッケージをインストールする必要があります。

CentOS 6でのSWA証明書のインポート

ステップ 1：SWAからHTTPSプロキシ証明書をダウンロードします。
ステップ 2： テキストエディタで証明書ファイルを開き、ファイル内のすべての内容をコピーします。
ステップ 3： /etc/pki/ca-trust/source/anchors/に、.crt拡張子を持つ新しいファイルを作成します。
ステップ 4：目的のテキストエディタでファイルを編集し、コピーしたテキストを新しいファイ

ルにコピーして保存します。
ステップ 5：ca-certificatesパッケージをインストールします。

```
yum install ca-certificates
```

手順 6： オペレーティングシステムで証明書を更新するには、次のコマンドを実行します。

```
update-ca-trust extract
```



ヒント：証明書がクライアントにローカルに保存されている場合は、証明書を/etc/pki/ca-trust/source/anchors/にコピーし、ca-certificatesをインストールした後にupdate-ca-trust extractを実行できます。

CentOS 5でのSWA証明書のインポート

ステップ 1：SWAからHTTPSプロキシ証明書をダウンロードします。
ステップ 2： テキストエディタで証明書ファイルを開き、ファイル内のすべての内容をコピーします。
ステップ 3： 現在のフォルダに、.crtという拡張子の付いた新しいファイル（SWA.crtなど）を作成します。
ステップ 4：目的のテキストエディタで/etc/pki/tls/certs/ca-bundle.crt を編集し、コピーしたテキストをファイルの最後に貼り付けて保存します。



ヒント：証明書がクライアントのローカルに保存されている場合（この例では、ファイル名はSWA.crt）、cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crtコマンドを使用してこの証明書を追加できます。

Mozilla FirefoxでのSWA証明書のインポート

ステップ 1：SWAからHTTPSプロキシ証明書をダウンロードします。
ステップ 2： ファイル拡張子を.crtに変更します。
ステップ 3： Firefoxを開き、メニュー（右上隅の3つのバー）をクリックします。
ステップ 4：Settingsを選択します（一部のバージョンではOptionsになっています）。
ステップ 5：左側のメニューでPrivacy & Securityをクリックし、Certificatesまでスクロールしま

す。
手順 6： [View Certificate] をクリックします。
手順 7： Authoritiesタブをクリックし、次にImportをクリックします。
ステップ 8：証明書ファイルを選択し、Openをクリックします。
ステップ 9：[OK] をクリックします。

Google ChromeでのSWA証明書のインポート

ステップ 1：SWAからHTTPSプロキシ証明書をダウンロードします。
ステップ 2： ファイル拡張子を.crtに変更します。
ステップ 3： Google Chromeを開き、Customize and control Google Chromeをクリックします（右上隅の3つのドット）。
ステップ 4：[Settings] を選択します。
ステップ 5：左側のメニューからPrivacy and Securityをクリックします。
手順 6： Securityを選択します。
手順 7： Manage certificatesまでスクロールして、右側のボタンをクリックします。
ステップ 8：Trusted Root Certification Authoritiesタブを選択し、Importをクリックします。
ステップ 9：証明書ファイルを選択し、Openをクリックします。
ステップ 10：[OK] をクリックします。



注：オペレーティングシステムにSWA証明書をインストールする場合、Google Chromeはその証明書を信頼するため、ブラウザに証明書を個別にインポートする必要はありません。

Microsoft Edge/Internet ExplorerでのSWA証明書のインポート

Microsoft EdgeおよびInternet Explorer(IE)は、オペレーティングシステムの証明書を使用します。SWA証明書をオペレーティングシステムにインストールする場合は、証明書をブラウザに個別にインポートする必要はありません。

SafariでのSWA証明書のインポート

ステップ 1：SWAからHTTPSプロキシ証明書をダウンロードします。
ステップ 2： ファイル拡張子を.crtに変更します。
ステップ 3： 起動パッドでKeychain Accessを選択します。
ステップ 4：FileメニューからAdd Keychainをクリックします。
ステップ 5： SWA証明書ファイルを選択し、Addをクリックします。
手順 6： Securityを選択します。

手順 7： Manage certificatesまでスクロールして、右側のボタンをクリックします。
ステップ 8：Trusted Root Certification Authoritiesタブを選択し、Importをクリックします。
ステップ 9：証明書ファイルを選択し、Openをクリックします。
ステップ 10：[OK] をクリックします。

グループポリシーからクライアントへのSWA証明書のインポート

Active Directoryからグループポリシーによって証明書をクライアントコンピュータに配布するには、次の手順を実行します。

ステップ 1：SWAからHTTPSプロキシ証明書をダウンロードします。
ステップ 2： ファイル拡張子を.crtに変更します。
ステップ 3： 証明書ファイルをドメインコントローラにコピーします。
ステップ 4： ドメインコントローラで、Startをクリックし、Group Policy Managementスナップインを開きます。
ステップ 5： 目的のグループポリシーオブジェクト(GPO)を検索するか、クライアントにインポートするSWA証明書を含む新しいGPOを作成します。
手順 6： GPOを右クリックし、Editをクリックします。
手順 7： 左側のメニューから、Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policiesの順に選択します。
ステップ 8：Trusted Root Certification Authoritiesを右クリックし、Importをクリックします。
ステップ 9： Welcome to the Certificate Import Wizardページで Nextをクリックします。
ステップ 10： インポートするSWA証明書ファイルを選択し、Nextをクリックします。
ステップ 11： Place all certificates in the following storeをクリックし、次にNextをクリックします。
ステップ 12： 表示された情報が正しいことを確認し、Finishをクリックします。

注：状況によっては、クライアントを再起動するか、gpupdate /forceを実行してActive Directoryクライアントマシンに変更を適用する必要があります。

関連コンテンツ

- AsyncOS 14.5 for Cisco Secure Web Applianceユーザガイド – GD（一般導入）
- グループポリシーを使用して証明書をクライアントコンピューターに配布する| Microsoft Learn
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。