在安全Web裝置中配置解密證書

目錄

簡介

必要條件

- 需求
- 採用元件

HTTPS解密

在SWA中配置解密證書

- 上傳根憑證和金鑰
- 為HTTPS代理生成證書和金鑰

匯入證書

- 將上游代理證書匯入到SWA
- 將SWA證書匯入到其他SWA
- 在Windows客戶端中匯入SWA證書
- 在Mac客戶端中匯入SWA證書
- 在Ubuntu/Debian中匯入SWA證書
- 在CentOS 6中匯入SWA證書
- 在CentOS 5中匯入SWA證書
- 在Mozilla Firefox中匯入SWA證書
- 在Google Chrome中匯入SWA證書
- 在Microsoft Edge/Internet Explorer中匯入SWA證書
- 在Safari中匯入SWA證書
- 將SWA證書從組策略匯入到客戶端

相關內容

簡介

本檔案介紹在安全網路裝置(SWA)和代理使用者端中設定HTTPS加密憑證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 對SWA的管理訪問
- 訪問SWA的圖形使用者介面(GUI)

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

HTTPS解密

SWA超文本傳輸協定安全(HTTPS)解密使用您上傳到裝置的根證書和私鑰檔案來加密流量。上傳到裝置的根證書和私鑰檔案必須是PEM格式。



附註：不支援DER格式。

您還可以上傳根憑證授權機構簽名的中間憑證。當SWA創建代表伺服器證書的證書時，它將上傳的證書與模擬的證書一起傳送到客戶端應用程式。這樣，只要中間證書由客戶端應用程式信任的根證書頒發機構(CA)簽名，應用程式就信任偽伺服器證書。

在SWA中配置解密證書

SWA可以使用現有證書和私鑰進行HTTPS解密。但是，可能會混淆必須使用的證書型別，因為並非所有x.509證書都工作。

證書主要有兩種型別：伺服器證書和根證書。所有x.509證書都包含標識證書型別的「基本約束」欄位：

- Subject Type=End Entity — 伺服器證書
- Subject Type=CA — 根證書

上傳根憑證和金鑰

步驟1.在GUI中，導覽至Security Services，然後選擇HTTPS Proxy。
步驟2.按一下Edit Settings。
步驟3.按一下Use Uploaded Certificate and Key。
步驟4.按一下Browse the Certificate欄位，以導覽至儲存在本機電腦上的憑證檔案。



附註：如果您上傳的檔案包含多個憑證或金鑰，Web代理會使用檔案中的第一個憑證或金鑰。

步驟5.在Key欄位中按一下Browse，以導覽至私鑰檔案。



附註：金鑰長度必須為512、1024或2048位。

步驟6.如果密鑰已加密，請選擇Key is Encrypted。
步驟7.單擊Upload Files以將證書和金鑰檔案傳輸到Secure Web Appliance。上載的證書資訊顯示在編輯HTTPS代理設定頁面上。
步驟8.(可選)按一下Download Certificate，將憑證傳輸至網路上的使用者端應用程式。

步驟9. Submit和Commit更改。

為HTTPS代理生成證書和金鑰

步驟1.在GUI中，導覽至Security Services，然後選擇HTTPS Proxy。
步驟2.按一下Edit Settings。
步驟3.選擇Use Generated Certificate and Key。
步驟4.按一下Generate New Certificate and Key。
步驟5.在「Generate Certificate and Key」對話框中，輸入要在根憑證中顯示的資訊。您可以在Common Name欄位中輸入除正斜槓(/)之外的任何ASCII字元。
步驟6.按一下Generate。
步驟7.生成的證書資訊顯示在Edit HTTPS Proxy Settings頁面上。
步驟8.(可選)按一下Download Certificate，以便將其傳送到網路上的使用者端應用程式。
步驟9.（可選）按一下Download Certificate Signing Request連結，以便您可以向CA提交憑證簽署請求(CSR)。
步驟10.（可選）收到來自CA的簽署憑證後，將其上傳到安全網路裝置。您可以在裝置上生成證書後隨時執行此操作。
步驟11. Submit和Commit更改。

匯入證書

將上游代理證書匯入到SWA

如果SWA配置為使用上游代理，並且上游代理配置為進行HTTPS解密，則必須將上游代理加密證書匯入到SWA。您可以管理受信任的證書清單，向其中新增證書並從其中以功能方式刪除證書。

步驟1。在GUI中選擇Network，然後選擇Certificate Management。
步驟2.在Certificate Management頁面上按一下Manage Trusted Root Certificates。
步驟3.要添加具有簽名授權而非思科識別清單上的自定義受信任根證書，請按一下Import，然後提交證書檔案。

步驟4. Submit和Commit更改。

將SWA證書匯入到其他SWA

如果您已上載一個HTTPS代理的SWA中的HTTPS證書和金鑰，且原始檔案可訪問，則可以從配置檔案將其匯入到另一個SWA。

步驟1.在兩個SWA的GUI中選擇System Administration，然後單擊Configuration File。

步驟2.按一下Download file on the local computer to view or save。

步驟3.在組態檔中選擇Encrypt passwords。

步驟4.（可選）選擇使用使用者定義的檔名並將所需名稱新增到配置檔案。

步驟5.按一下Current Configuration底下的Submit以下載configuration .xml檔案。

步驟6.使用文本編輯器或XML編輯器開啟下載的檔案。

步驟7.使用證書從SWA複製這些標籤，複製標籤內的所有資料，並將它們替換在其他SWA的配置檔案中：

```
<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>
```

步驟8.將更改儲存到目標SWA的.xml檔案中。

步驟9.要將編輯的.xml配置檔案匯入回目標SWA，請從GUI中選擇System Administration，然後按一下Configuration File。

步驟10.在Load Configuration部分，按一下Load a configuration file from local computer。

步驟11.按一下Choose file，然後選擇edited.xml組態檔。

步驟12.按一下Load，以匯入包含憑證和金鑰的新組態檔。

步驟13.如果系統提示您，請提交更改。

在Windows客戶端中匯入SWA證書

要將SWA HTTPS代理證書匯入為具有Microsoft Windows作業系統的客戶端電腦中的受信任證書，請檢視以下步驟：

步驟1.從工作列按一下「開始」，然後鍵入「管理電腦證書」。
步驟2.在Certificates-Local Computer頁面上，展開Trusted Root Certification，然後按一下右鍵Certificates文件夾資料夾。
步驟3.單擊All Tasks並選擇Import。
步驟4.在「Certificate Import Wizard（證書匯入嚮導）」頁面中，按一下Next(下一步)。
步驟5.要匯入SWA證書檔案，請按一下Browse並選擇您從SWA下載的證書。



提示：要下載SWA證書，請參閱上傳根證書和金鑰或為HTTPS代理生成證書和金鑰部分的步驟8。

步驟6.單擊Place all certificates in the following複選框。
步驟7.選擇Trusted Root Certification Authorities，然後點選Next。
步驟8.單擊完成。

或者，您可以運行此命令以將證書匯入到受信任的根證書頒發機構。

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



附註：您必須將<Path to SWA Certificate/CertificateName.crt>替換為當前下載的證書路徑和檔名。

在Mac客戶端中匯入SWA證書

步驟1.將HTTPS代理證書從SWA下載到Mac OS客戶端。
步驟2.將副檔名重新命名為.crt。
步驟3.運行以下命令將證書匯入為受信任證書：

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



附註：您必須將其替換為當前下載的證書路徑和檔名。

在Ubuntu/Debian中匯入SWA證書

步驟1.從SWA下載HTTPS代理證書。
步驟2.在文本編輯器中開啟證書檔案並複製所有內容。
步驟3.在/usr/local/share/ca-certificates/中建立一個以.crt為擴展名的新檔案。
步驟4.使用所需的文本編輯器編輯檔案，並將複製的文本貼上到新檔案中，然後儲存。
步驟5.運行此命令以刷新作業系統中的證書。

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



提示：如果您的憑證儲存在使用者端本地，可將憑證複製到/usr/local/share/ca-certificates/並執行sudo update-ca-certificates。



附註：在某些版本中，必須使用以下命令安裝ca-certificates軟體包：sudo apt-get install -y ca-certificates。

在CentOS 6中匯入SWA證書

步驟1.從SWA下載HTTPS代理證書。
步驟2.在文字編輯器中開啟憑證檔案，並複製檔案中的所有內容。
步驟3.在/etc/pki/ca-trust/source/anchors/中,以.crt副檔名建立一個新檔案。
步驟4.使用所需的文本編輯器編輯檔案，並將過去複製的文本儲存到新檔案中，然後儲存。
步驟5.安裝ca-certificates程式包：

```
yum install ca-certificates
```

步驟6.運行以下命令以刷新作業系統中的證書：

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



提示：如果您將憑證儲存在使用者端本地，則可以將憑證複製到/etc/pki/ca-trust/source/anchos/，並在安裝ca-certificates後執行update-ca-trust。

在CentOS 5中匯入SWA證書

步驟1.從SWA下載HTTPS代理證書。
步驟2.在文本編輯器中開啟證書檔案並複製檔案中的所有內容。
步驟3.在當前資料夾中建立副檔名為.crt(例如SWA.crt)的新檔案。
步驟4.使用所需的文字編輯器編輯/etc/pki/tls/certs/ca-bundle.crt，將複製文字貼上到檔案末尾，然後儲存。



提示：如果您將憑證儲存在使用者端本地(在本範例中，檔案名稱為SWA.crt)，則可以使用以下命令附加憑證：cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt。

在Mozilla Firefox中匯入SWA證書

步驟1.從SWA下載HTTPS代理證書。
步驟2.將副檔名重新命名為.crt。
步驟3.開啟Firefox，然後按一下Menu（右上角有三個條）。

步驟4.選擇Settings(在某些版本中為Options)。
步驟5.按一下左側功能表中的Privacy & Security，然後滾動到Certificates。
步驟6.按一下View Certificates。
步驟7.按一下Authorities索引標籤，然後Import。
步驟8.選擇憑證檔案，然後按一下Open。
步驟9.按一下OK。

在Google Chrome中匯入SWA證書

步驟1.從SWA下載HTTPS代理證書。
步驟2.將副檔名重新命名為.crt。
步驟3.開啟Google Chrome，然後單擊「Customize and control Google Chrome」（右上角三個點）。
步驟4.選擇Settings。
步驟5.從左側選單中按一下Privacy and Security。
步驟6.選擇Security。
步驟7.滾動至Manage certificates，然後點選右側按鈕。
步驟8.選擇Trusted Root Certification Authorities選項卡，然後點選Import。
步驟9.選擇憑證檔案，然後按一下Open。
步驟10.按一下OK。



附註：如果在作業系統中安裝SWA證書，Google Chrome會信任該證書，因此無需將證書單獨匯入到瀏覽器。

在Microsoft Edge/Internet Explorer中匯入SWA證書

Microsoft Edge和Internet Explorer(IE)使用作業系統證書。如果在作業系統中安裝SWA證書，則無需將證書單獨匯入到瀏覽器。

在Safari中匯入SWA證書

步驟1.從SWA下載HTTPS代理證書。
步驟2.將副檔名重新命名為.crt。
步驟3.在啟動板中，選擇Keychain Access。
步驟4.在「File」菜單中，按一下「Add Keychain」。
步驟5.選擇SWA證書檔案，然後點選Add。
步驟6.選擇Security。
步驟7.滾動至Manage certificates，然後點選右側按鈕。

步驟8.選擇Trusted Root Certification Authorities選項卡，然後點選Import。
步驟9.選擇憑證檔案，然後按一下Open。
步驟10.按一下OK。

將SWA證書從組策略匯入到客戶端

要通過Active Directory中的組策略將證書分發到客戶端電腦，請執行以下步驟：

步驟1.從SWA下載HTTPS代理證書。
步驟2.將副檔名重新命名為.crt。
步驟3.將憑證檔案複製到您的網域控制器。
步驟4.在域控制器上，按一下開始並開啟組策略管理管理單元。
步驟5.查找所需的組策略對象(GPO)，或建立新的GPO以包含要匯入到客戶端的SWA證書。
步驟6.按一下右鍵GPO，然後按一下Edit。
步驟7.從左側選單中，導航到電腦配置> 策略> Windows設定> 安全設定> 公鑰策略。
步驟8.右鍵點選Trusted Root Certification Authorities，然後點選Import。
步驟9.在「Welcome to the Certificate Import Wizard(歡迎使用證書匯入嚮導)」頁面上單擊Next。
步驟10.選擇SWA證書檔案以進行匯入，然後按一下下一步。
步驟11.單擊將所有證書放入以下儲存區，然後單擊Next。
步驟12.驗證所提供的資訊是否準確，然後按一下完成。

附註：在某些情況下，必須重新啟動客戶端或運行gpupdate /force才能在Active Directory客戶端電腦上應用更改。

相關內容

- Cisco Secure Web Appliance - GD（常規部署）AsyncOS 14.5使用手冊
- 使用組策略將證書分發到客戶端電腦 | Microsoft學習
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。