在安全Web设备中配置解密证书

目录

简介

先决条件

- 要求
- 使用的组件

HTTPS解密

在SWA中配置解密证书

- 上传根证书和密钥
- 为HTTPS代理生成证书和密钥

导入证书

- 将上游代理证书导入SWA
- 将SWA证书导入另一个SWA
- 在Windows客户端中导入SWA证书
- 在Mac客户端中导入SWA证书
- 在Ubuntu/Debian中导入SWA证书
- 在CentOS 6中导入SWA证书
- 在CentOS 5中导入SWA证书
- 在Mozilla Firefox中导入SWA证书
- 在Google Chrome中导入SWA证书
- 在Microsoft Edge/Internet Explorer中导入SWA证书
- 在Safari中导入SWA证书
- 将SWA证书从组策略导入到客户端

相关内容

简介

本文档介绍在安全网络设备(SWA)和代理客户端中配置HTTPS加密证书的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 对SWA的管理访问
- 访问SWA的图形用户界面(GUI)

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

HTTPS解密

SWA超文本传输协议安全(HTTPS)解密使用您上传到设备的根证书和私钥文件来加密流量。上传到设备的根证书和私钥文件必须是PEM格式。



注意：不支持DER格式。

您还可以上传根证书颁发机构签名的中间证书。当SWA创建代表服务器证书的证书时，它将上传的证书与模拟的证书一起发送到客户端应用。这样，只要中间证书由客户端应用信任的根证书颁发机构(CA)签名，应用就会信任伪装的服务器证书。

在SWA中配置解密证书

SWA可以使用现有证书和私钥进行HTTPS解密。但是，由于并非所有x.509证书都起作用，因此可能会对必须使用的证书类型造成混淆。

证书有两种主要类型：服务器证书和根证书。所有x.509证书都包含用于标识证书类型的“基本限制”字段：

- Subject Type=End Entity -Server Certificate
- Subject Type=CA — 根证书

上传根证书和密钥

第1步：从GUI中，导航到Security Services，然后选择HTTPS Proxy。
步骤2.单击Edit Settings。
步骤3.单击使用上传的证书和密钥。
步骤4.单击Browse the Certificate字段导航到本地计算机上存储的证书文件。



注意：如果上传的文件包含多个证书或密钥，则Web代理使用文件中的第一个证书或密钥。

第5步：点击Key字段中的Browse，导航到私钥文件。



注意：密钥长度必须为512、1024或2048位。

第6步：如果密钥已加密，请选择Key is Encrypted。
步骤7.单击Upload Files将证书和密钥文件传输到安全Web设备。上传的证书信息显示在编辑HTTPS代理设置页面。
第8步（可选）点击Download Certificate以传输到网络上的客户端应用程序。

步骤9.提交并提交更改。

为HTTPS代理生成证书和密钥

第1步：从GUI中，导航到Security Services，然后选择HTTPS Proxy。
步骤2.单击Edit Settings。
步骤3.选择Use Generated Certificate and Key。
步骤4.单击Generate New Certificate and Key。
第5步：在Generate Certificate and Key对话框中，输入要在根证书中显示的信息。可以在Common Name字段中输入除正斜杠(/)之外的任何ASCII字符。
步骤6.点击Generate。
步骤7.生成的证书信息显示在Edit HTTPS Proxy Settings页面。
第8步（可选）点击Download Certificate，以便您可以将其传输到网络上的客户端应用。
第9步（可选）点击Download Certificate Signing Request链接，以便您可以向CA提交证书签名请求(CSR)。
第10步（可选）从CA收到签名证书后，将证书上传到安全网络设备。您可以在设备上生成证书后随时执行此操作。
步骤11.提交并提交更改。

导入证书

将上游代理证书导入SWA

如果SWA配置为使用上游代理，并且上游代理配置为进行HTTPS解密，则必须将上游代理加密证书导入到SWA。您可以管理受信任证书列表并向其添加证书，并从其上以功能方式删除证书。

第1步：从GUI中，选择Network，然后选择Certificate Management。
第2步：在Certificate Management页面上点击Manage Trusted Root Certificates。
第3步：要添加具有签名颁发机构（而不是思科识别的列表）的自定义受信任根证书，请点击Import，然后提交证书文件。

步骤4.提交并提交更改。

将SWA证书导入另一个SWA

如果您上传了用于HTTPS代理的一个SWA中的HTTPS证书和密钥，并且原始文件可访问，则可以从配置文件将其导入到另一个SWA。

步骤1.从两个SWA的GUI中选择System Administration，然后点击Configuration File。

步骤2.单击Download file on the local computer to view or save。

步骤3.在配置文件中选择Encrypt passwords。

第4.（可选）选择Use a user-defined file name并将所需名称添加到配置文件。

第5步：点击Current Configuration下的Submit以下载configuration.xml文件。

步骤6.使用文本编辑器或XML编辑器打开下载的文件。

步骤7.使用证书从SWA复制这些标记，复制标记内的所有数据，并将它们替换在其他SWA的配置文件中：

```
<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>
```

步骤8.将更改保存在目标SWA的.xml文件中。

第9步：要将编辑的。xml配置文件导入到目标SWA，请从GUI中选择System Administration，然后单击Configuration File。

步骤10.在Load Configuration部分，点击Load a configuration file from local computer。

步骤11.单击Choose file并选择edited.xml配置文件。

步骤12.单击Load以导入包含证书和密钥的新配置文件。

步骤13.如果系统提示您，请提交更改。

在Windows客户端中导入SWA证书

要将SWA HTTPS代理证书导入为具有Microsoft Windows操作系统的客户端计算机中的受信任证书，请查看以下步骤：

步骤1.从任务栏点击Start（开始），然后键入Manage computer certificates。
第2步：在Certificates-Local Computer页面上，展开Trusted Root Certification，然后右键单击Certificates文件夹文件夹。
步骤3.单击All Tasks并选择Import。
第4步：从证书导入向导(Certificate Import Wizard)页面，点击下一步(Next)。
第5步：要导入SWA证书文件，请点击浏览，然后选择从SWA下载的证书。



提示：要下载SWA证书，请参阅上传根证书和密钥或为HTTPS代理生成证书和密钥部分的步骤8。

步骤6.单击Place all certificates in the following复选框。
步骤7.选择Trusted Root Certification Authorities（受信任的根证书颁发机构），然后点击Next。
第 8 步： 点击完成。

或者，您可以运行此命令将证书导入到受信任的根证书颁发机构。

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



注意：您必须将<Path to SWA Certificate/CertificateName.crt>替换为当前下载的证书路径和文件名。

在Mac客户端中导入SWA证书

步骤1.将HTTPS代理证书从SWA下载到Mac OS客户端。
步骤2.将文件扩展名重命名为.crt。
步骤3.运行以下命令将证书导入为受信任证书：

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



注意：您必须将其替换为当前下载的证书路径和文件名。

在Ubuntu/Debian中导入SWA证书

步骤1.从SWA下载HTTPS代理证书。
步骤2.在文本编辑器中打开证书文件并复制所有内容。
第3步：在/usr/local/share/ca-certificates/以.crt为扩展名创建新文件。
步骤4.使用所需的文本编辑器编辑文件，并将复制的文本粘贴到新文件中，然后保存。
步骤5.运行此命令以刷新操作系统中的证书。

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



提示：如果证书存储在客户端本地，您可以将证书复制到/usr/local/share/ca-certificates/并运行sudo update-ca-certificates。



注意：在某些版本中，您必须使用以下命令安装ca-certificates软件包：sudo apt-get install -y ca-certificates。

在CentOS 6中导入SWA证书

步骤1.从SWA下载HTTPS代理证书。
步骤2.在文本编辑器中打开证书文件并复制文件中的所有内容。
第3步：在/etc/pki/ca-trust/source/anchos/with a.crt扩展名中创建新文件。
步骤4.使用所需的文本编辑器编辑文件，并将过去复制的文本复制到新文件中，然后保存。
步骤5.安装ca-certificates软件包：

```
yum install ca-certificates
```

步骤6.运行以下命令以刷新操作系统中的证书：

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



提示：如果证书存储在客户端本地，则可以在安装ca-certificates后，将证书复制到/etc/pki/ca-trust/source/anchos/和update-ca-trust extract。

在CentOS 5中导入SWA证书

步骤1.从SWA下载HTTPS代理证书。
步骤2.在文本编辑器中打开证书文件并复制文件中的所有内容。
步骤3.在当前文件夹中创建扩展名为.crt的新文件（例如SWA.crt）。
第4步：使用所需的文本编辑器编辑/etc/pki/tls/certs/ca-bundle.crt，将复制的文本粘贴到文件末尾，然后保存。



提示：如果证书存储在客户端本地（在本示例中，文件名为SWA.crt），则可以使用以下命令附加证书：cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt。

在Mozilla Firefox中导入SWA证书

步骤1.从SWA下载HTTPS代理证书。
步骤2.将文件扩展名重命名为.crt。
步骤3.打开Firefox并点击Menu（右上角三个条）。

第4步：选择设置（在某些版本中为选项）。
第5步：点击左侧菜单中的Privacy & Security，然后滚动到Certificates。
步骤6.单击View Certificates。
步骤7.单击Authorities选项卡，然后单击Import。
第8步：选择证书文件并点击打开。
步骤9.单击确定。

在Google Chrome中导入SWA证书

步骤1.从SWA下载HTTPS代理证书。
步骤2.将文件扩展名重命名为.crt。
步骤3.打开Google Chrome并点击自定义和控制Google Chrome（右上角三个点）。
步骤4.选择设置。
步骤5.从左侧菜单中点击Privacy and Security。
步骤6.选择Security。
步骤7.滚动到Manage certificates（管理证书），然后点击右侧的按钮。
步骤8.选择Trusted Root Certification Authorities选项卡，然后点击Import。
步骤9.选择证书文件并点击打开。
步骤10.单击OK。



注意：如果您在操作系统中安装SWA证书，Google Chrome会信任该证书，因此无需将证书单独导入到浏览器中。

在Microsoft Edge/Internet Explorer中导入SWA证书

Microsoft Edge和Internet Explorer(IE)使用操作系统证书。如果您在操作系统中安装SWA证书，则无需将证书单独导入到浏览器中。

在Safari中导入SWA证书

步骤1.从SWA下载HTTPS代理证书。
步骤2.将文件扩展名重命名为.crt。
步骤3.在启动板中，选择Keychain Access。
步骤4.从“文件”菜单中，单击添加密钥链。
第5步：选择SWA证书文件，然后点击添加。
步骤6.选择Security。
步骤7.滚动到Manage certificates（管理证书），然后点击右侧的按钮。
步骤8.选择Trusted Root Certification Authorities选项卡，然后点击Import。

步骤9.选择证书文件并点击打开。
步骤10.单击OK。

将SWA证书从组策略导入到客户端

要通过组策略从Active Directory将证书分发到客户端计算机，请执行以下步骤：

步骤1.从SWA下载HTTPS代理证书。
步骤2.将文件扩展名重命名为.crt。
步骤3.将证书文件复制到您的域控制器。
步骤4.在域控制器上，单击开始并打开组策略管理管理单元。
第5步：查找所需的组策略对象(GPO)或创建新的GPO，以包含要导入到客户端的SWA证书。
步骤6.右键单击GPO，然后单击Edit。
步骤7.从左侧菜单中，导航到计算机配置>策略> Windows设置> 安全设置> 公钥策略。
步骤8.右键点击Trusted Root Certification Authorities，然后点击Import。
步骤9.在Welcome to the Certificate Import Wizard页上点击Next。
第10步：选择SWA证书文件以便导入，然后点击下一步。
步骤11.单击将所有证书放入以下存储，然后点击下一步。
步骤12.检查提供的信息是否准确，然后点击完成。

注意：在某些情况下，必须重新启动客户端或运行gpupdate /force才能在Active Directory客户端计算机上应用更改。

相关内容

- 思科安全网络设备AsyncOS 14.5用户指南 — GD（通用部署）
- 使用组策略将证书分发到客户端计算机 | Microsoft学习
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。