生成第三方证书的CSR并且下载被释放的证书到WLC

目录

简介

本文档说明如何生成证书签名请求 (CSR) 以获取第三方证书，以及如何将非链接证书下载到无线局域网 (WLAN) 控制器 (WLC)。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解如何配置 WLC、轻量接入点 (LAP) 和无线客户端卡以执行基本操作
- 了解如何使用针对安全套接字层 (SSL) 的 OpenSSL 应用程序

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 4.2.61.0 的 Cisco 4400 WLC
- 适用于 Microsoft Windows 的 OpenSSL 应用程序**注意：** 因为 WLC 当前不支持 Openssl 1.0，因此 Openssl 0.9.8 是必需的。
- 特定于第三方证书颁发机构 (CA) 的注册工具

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

默认情况下，WLC 使用内置的自签名 SSL 证书。在处于下列情况之一时，WLC 使用此 SSL 证书：

- 当客户端尝试使用基于 SSL 的 Web 身份验证连接到 WLAN 网络时
- 当用户尝试使用安全 HTTP (HTTPS)（WebAdmin 身份验证）登录 WLC 时

无论是哪种情况，在第一次尝试访问 WLC 时，您都会收到如下所示的 Web 浏览器安全警报：

系统会提示您接受来自 WLC 的证书，因为客户端没有安装在 WLC 上的证书的受信任根证书。WLC 上的 SSL 证书不在客户端系统信任的证书列表中。有两种方法可以停止生成此 Web 浏览器安全警报告弹出窗口：

- 使用 WLC 上的自签名 SSL 证书并将客户端站点配置为接受此证书。将 WLC 上的自签名证书包括在客户端站点上受信任的证书列表中。
- 生成 CSR，并安装客户端已为其安装受信任根证书的源（第三方 CA，例如 VeriSign）所签名的证书。您可以使用类似 OpenSSL 的程序从 WLC 脱机执行此操作。有关 OpenSSL 的详细信息，请参阅 OpenSSL 项目 。

本文档说明如何生成第三方证书的 CSR 以及如何将非链接 Web 身份验证证书下载到 WLC。

对链接证书的支持

早于 5.1.151.0 的 WLC 软件版本不支持链接证书。为了解决此问题，可以使用下列选项之一：

- 从 CA 获取非链接证书，这意味着签名根是受信任的。
- 将所有有效的中间 CA 根证书（受信任或不受信任）都安装到客户端上。

有了版本 5.1.151.0 及更高版本，WLC 将支持链接证书进行 Web 身份验证。Web 身份验证证书可以是以下任何一种证书：

- 串连
- 释放
- 自动生成的

有关如何使用 WLC 上的链接证书的信息，请参阅生成第三方证书的 CSR 并将链接证书下载到 WLC。

CSR

证书是用来标识服务器、公司或某个其他实体并将其身份与公钥相关联的电子文档。

CA 是验证身份并颁发证书的实体。CA 颁发的证书将特定的公钥绑定到证书所标识的实体的名称（例如，服务器或设备的名称）。只有证书认证的公钥才能与证书所标识的实体拥有的相应私钥一

起使用。证书可以帮助防止使用伪造的公钥进行假冒。

CSR 是申请人向 CA 发送的用于申请数字身份证书的消息。通常，第三方 CA 公司（如 Entrust 或 VeriSign）需要先获得 CSR 然后才能创建数字证书。

CSR 生成与您计划安装外部证书的设备无关。因此，CSR 和私钥文件可以在任何单独的 Windows 或 UNIX 计算机上生成。在这种情况下，CSR 生成与交换机或设备无关。

由于 WLC 不生成 CSR，您必须使用第三方应用程序（例如 OpenSSL）以生成 WLC 的 CSR。

生成 CSR 部分讨论为了生成私钥和 CSR 而必须在 OpenSSL 应用程序中发出的命令。

完成以下步骤以从 CA 获得第三方证书：

1. 生成私钥/公钥对。
2. 使用公钥生成 CSR。
3. 向 CA 提交 CSR。
4. 检索 CA 生成的证书。
5. 将证书和私钥组合到 pkcs12 文件中。
6. 将 pkcs12 文件转换为保密增强型邮件 (PEM) 编码文件。
7. 将新的第三方证书（.pem 文件）下载到 WLC。

生成 CSR

完成以下步骤以生成 CSR 并将该 CSR 提交给第三方 CA：

1. 安装并打开 OpenSSL 应用程序。**注意：** 因为 WLC 当前不支持 Openssl 1.0，因此 Openssl 0.9.8 是必需的。在 Windows 中，默认情况下 openssl.exe 位于 c:\openssl\bin。
2. 发出以下命令：`OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem` **注意：** WLC 支持的最大密钥大小为 **2048** 位。在您发出此命令后，系统将提示您输入一些信息：国家/地区名称、州、城市等等。
3. 提供必填信息。您需要正确提供的最重要信息是公用名称。请确保用于创建证书的主机名（公用名称）与 WLC 上的虚拟接口 IP 的域名系统 (DNS) 主机名条目匹配，并且该名称也实际存在于 DNS 中。另外，您对 VIP 接口进行更改后，必须重新启动系统才能使此更改生效。**注意：** 必须在 WLC 中的 **Interfaces > Edit** 下输入虚拟接口的 DNS 主机名。这在已启用 Web 身份验证时用于验证证书的源。请重新启动控制器以使此更改生效。在提供所有必需的详细资料后，最终将获得两个文件：名为 mykey.pem 的新私钥名为 myreq.pem 的 CSR这些文件存储在安装 OpenSSL 的默认目录（在本示例中为 c:\openssl\bin）中。文件 myreq.pem 是包含 CSR 信息的文件。必须将该信息提交到第三方 CA，以使第三方 CA 能够生成数字证书。下面是当您使用 OpenSSL 应用程序发出此命令时的示例命令输出：

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................................................................++++++
.....................................................++++++ writing new private key to
'mykey.pem' ----- You are about to be asked to enter information that will be incorporated
into your certificate request. What you are about to enter is what is called a
Distinguished Name or a DN. There are quite a few fields but you can leave some blank For
some fields there will be a default value, If you enter '.', the field will be left blank.
----- Country Name (2 letter code) [AU]:US State or Province Name (full name) [Some-
State]:CA Locality Name (eg, city) []:San Jose Organization Name (eg, company) [Internet
Widgits Pty Ltd]:ABC Organizational Unit Name (eg, section) []:CDE Common Name (eg, YOUR
name) []:XYZ.ABC Email Address []:Test@abc.com Please enter the following 'extra'
```

attributes to be sent with your certificate request A challenge password []:**Test123** An optional company name []: OpenSSL> **注意：** 请记住质询口令并保存密钥文件。当您导入第三方 CA 发送的数字签名证书时，很可能需要该口令（除非第三方 CA 将新口令与它为您或您的组织生成的数字证书一起发送）。

4. 既然您的 CSR 已准备就绪，请将 CSR 信息复制并粘贴到任何 CA 注册工具。为了将信息复制并粘贴到注册表中，请在不添加额外字符的文本编辑器中打开该文件。Cisco 建议您使用 Microsoft Notepad 或 UNIX vi。有关如何通过注册工具提交 CSR 的详细信息，请参阅第三方 CA 的网站。您将 CSR 提交给第三方 CA 后，第三方 CA 会对证书进行数字签名，然后通过电子邮件发送回签名证书。
5. 将您从 CA 接收到签名证书信息复制到一个文件中。本示例将该文件命名为 CA.pem。
6. 将 CA.pem 证书与私钥结合使用，然后将该文件转换为 .pem 文件。在 OpenSSL 应用程序中发出以下命令：openssl>**pkcs12 -export -in CA.pem -inkey mykey.pem -out CA.p12 -clcerts -passin pass:check123 -passout pass:check123** *!--- This command should be on one line.* openssl>**pkcs12 -in CA.p12 -out final.pem -passin pass:check123 -passout pass:check123** **注意：** 在此命令中，您必须为参数 **- passin** 和 **- passout** 输入口令。为 **- passout** 参数配置的口令必须与在 WLC 上配置的 **certpassword** 参数匹配。在本示例中，为 **-passin** 和 **-passout** 参数配置的口令为 **check123**。本文档的将第三方证书下载到 WLC 部分中过程的第 4 步讨论如何配置 **certpassword** 参数。**final.pem** 是通过 TFTP 传输到 Cisco WLC 的文件。既然您已有了来自第三方 CA 的证书，您需要将该证书下载到 WLC。

将第三方证书下载到 WLC

使用 TFTP 服务器加载新证书。要使用 TFTP，请遵循下列指导原则：

- 如果通过服务端口加载证书，则 TFTP 服务器必须与 WLC 位于同一子网中，因为服务端口不可路由；但是，如果通过分布式系统 (DS) 网络端口加载证书，则 TFTP 服务器可以位于任何子网中。
- TFTP 服务器与 Cisco Wireless Control System (WCS) 运行于同一台计算机上，因为 WCS 和 TFTP 服务器使用同一通信端口。

完成以下步骤以加载外部生成的 HTTPS 证书：

1. 将 final.pem 文件移到 TFTP 服务器上的默认目录。
2. 在命令行界面 (CLI) 中，发出 **transfer download start** 命令以查看当前下载设置，并在提示符处输入 **n**。示例如下：>**transfer download start**
   Mode..... TFTP Data
   Type..... Admin Cert TFTP Server
   IP..... xxx.xxx.xxx.xxx TFTP
   Path..... <directory path> TFTP
   Filename..... Are you sure you want to start? (y/n) **n** Transfer Canceled
3. 发出以下命令以更改下载设置：>**transfer download mode tftp** >**transfer download datatype webauthcert** >**transfer download serverip** *<TFTP server IP address>* >**transfer download path** *<absolute TFTP server path to the update file>* >**transfer download filename** *final.pem*
4. 输入 .pem 文件的口令，以使操作系统可以解密 SSL 密钥和证书。>**transfer download certpassword** *password* >Setting password to *password* **注意：** 请确保 **certpassword** 与生成 CSR 部分的第 6 步讨论的 **-passout** 参数口令相同。在本示例中，**certpassword** 必须为 **check123**。
5. 发出 **transfer download start** 命令以查看更新的设置。然后在提示符处输入 **y** 以确认当前下载设置并开始证书和密钥下载。示例如下：(Cisco Controller) >**transfer download start**
   Mode..... TFTP Data
   Type..... Admin Cert TFTP Server

```
IP.................................. 172.16.1.1 TFTP Packet
Timeout............................. 6 TFTP Max Retries.............................
10 TFTP Path..................................... c:\OpenSSL\bin/ TFTP
Filename............................... final.pem This may take some time. Are you
sure you want to start? (y/N) y TFTP Webadmin cert transfer starting. Certificate
installed. Reboot the switch to use new certificate.
```

注意： 要安装用于对尝试使用 HTTPS 登录 WLC 的用户进行管理身份验证的第三方证书，请将 **transfer download datatype** 命令中的数据类型更改为 **webadmincert**，然后重复本过程的第 3 步到第 5 步。

6. 发出以下命令以启用 HTTPS：`>config network secureweb enable`
7. 将 SSL 证书、密钥和安全 Web 口令保存到 NVRAM，以便跨重新启动保留您的更改。`>save config Are you sure you want to save? (y/n) y Configuration Saved!`
8. 重新启动控制器。`>reset system Are you sure you would like to reset the system? (y/n) y System will now restart! The controller reboots.` **注意：** 如果已安装证书，则下载新证书的过程将清除旧证书。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

可以在 WLC 上使用 **show certificate summary** 命令来检查 WLC 是否按照预期使用第三方证书。示例如下：

```
(Cisco Controller) >show certificate summary Web Administration Certificate.................
3rd Party Web Authentication Certificate.................. 3rd Party Certificate compatibility
mode:.................. off
```

该输出确认已将第三方证书用作 Web 管理证书和 Web 身份验证证书。

用户下次尝试登录使用基于 SSL 的 Web 身份验证的 WLAN 网络时，如果已安装在 WLC 上的第三方证书位于客户端浏览器支持的受信任 CA 列表中，则系统将不会提示该用户接受 Web 安全警报。

故障排除

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

可以在 WLC 上使用 **debug pm pki enable** 命令。如果您将证书安装在 WLC 上，请运行此命令。

每当向/从控制器进行任何传输时，都可以启用 **debug transfer all enable** 命令，然后重新运行该传输以查看已进行传输的详细资料，这会很有帮助。传输可能会在输送期间失败（相应数量的位或字节未从服务器移到控制器），或者，文件到达控制器后，控制器无法识别内容，或者发现内容不适用于所需功能。

相关信息

- 无线 LAN 控制器 (WLC) 软件升级
- 生成第三方证书的CSR并且下载被串连的证书到WLC
- 无线 LAN 控制器 (WLC) 故障排除常见问题
- Cisco 无线 LAN 控制器配置指南 4.0 版

- 无线产品支持
- OpenSSL 项目
- 技术支持和文档 - Cisco Systems