

F5 SSL 证书部署指南



沃通电子认证服务有限公司

WoSignCA Limited

目 录

一、 安装 SSL 证书的环境.....	3
1.1 SSI 证书安装环境简介.....	3
1.2 网络环境要求.....	3
二、 SSL 证书的安装.....	3
2.1 获取 SSI 证书.....	3
2.2 解压证书文件.....	3
2.3 安装 SSL 证书.....	3
2.4 测试 SSL 证书.....	6
三、 SSL 证书的备份.....	6
四、 SSL 证书的恢复.....	6

技术支持联系方式

技术支持邮箱：support@wosign.com
技术支持热线电话：0755-26027828 / 0755-26027859
技术支持网页：<https://bbs.wosign.com>
公司官网地址：<https://www.wosign.com>

一、安装 SSL 证书的环境

1.1 SSI 证书安装环境简介

F5 设备一台，

SSL 证书一张（备注：本指南使用 s.wosign.com 域名 OV SSL 证书进行操作,通用其它版本证书）

1.2 网络环境要求

请确保站点是一个合法的外网可以访问的域名地址，可以正常通过或 <http://xxx> 进行正常访问。

二、SSL 证书的安装

2.1 获取 SSI 证书

成功在沃通申请证书后，会得到一个有密码的压缩包文件，输入证书密码后解压得到四个文件：for Apache、for IIS、for Nginx、for Other Server，这个是证书的几种格式，F5 上需要用到 for Apache 格式的证书。

 for Apache.zip	← 解压此文件	2016/12/7 9:41	好压 ZIP 压缩文件
 for IIS.zip		2016/12/7 9:41	好压 ZIP 压缩文件
 for Nginx.zip		2016/12/7 9:41	好压 ZIP 压缩文件
 for Other Server.zip		2016/12/7 9:41	好压 ZIP 压缩文件

图 1

2.2 解压证书文件

解压 Apache 文件可以看到 2 个文件。包括公钥、证书链，如图 2

 root_bundle.crt	← 证书链	2016/12/7 9:41	安全证书
 test.wosign.com.crt	← 公钥	2016/12/7 9:41	安全证书

图 2

2.3 安装 SSL 证书

1、导入证书公钥

如果是导入已经存在的域，则根据之前其他 F5 上的命名规则填写名称，如果为新建则使用如下命名规则，域名_ssl_版本和根证书_域名_版本，例如：login_ssl_v3 和 parent_login_v3，Import Type 选择“certificate”，找到 test.wosign.com.crt 公钥,选择“Import”

SSL Certificate/Key Source	
Import Type	Certificate
Certificate Name	<input type="radio"/> Create New <input type="radio"/> Overwrite Existing <input type="text"/> 填写证书名称
Certificate Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text <input type="button" value="选择文件"/> 未选择文件

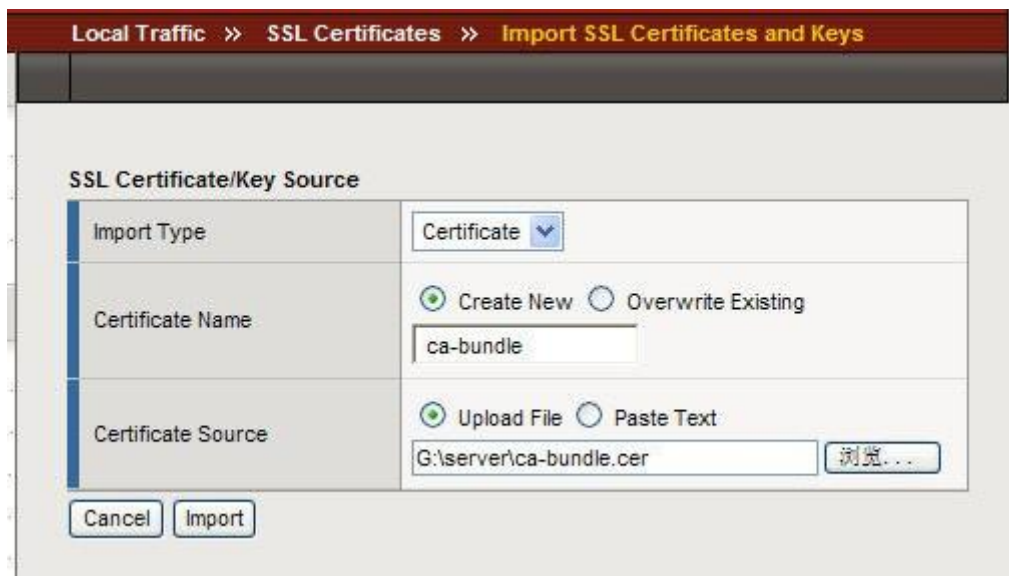
2、导入证书的私钥

Key 文件为生成 csr 时生成的文件，如果是导入已经存在的域，则根据之前其他 F5 上的命名规则填写名称，如果为新建则必须与证书名称相同，例如：证书名称为 login_ssl_v3，key 的名称也与证书名相同，Import Type 选择“key”，找到 test.wosign.com.key 私钥,选择“Import”

SSL Certificate/Key Source	
Import Type	Key
Key Name	<input type="radio"/> Create New <input type="radio"/> Overwrite Existing <input type="text"/> 名称必须与SSL证书名称相同
Key Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text <input type="button" value="选择文件"/> 未选择文件

3、导入 CA 中级证书

选择 Local Traffic-> SSL Certificates 在 SSL Certificate List 主界面点击右上角“Import”，将压缩包的 root_bundle.crt 使用“Certificate”方式导入。



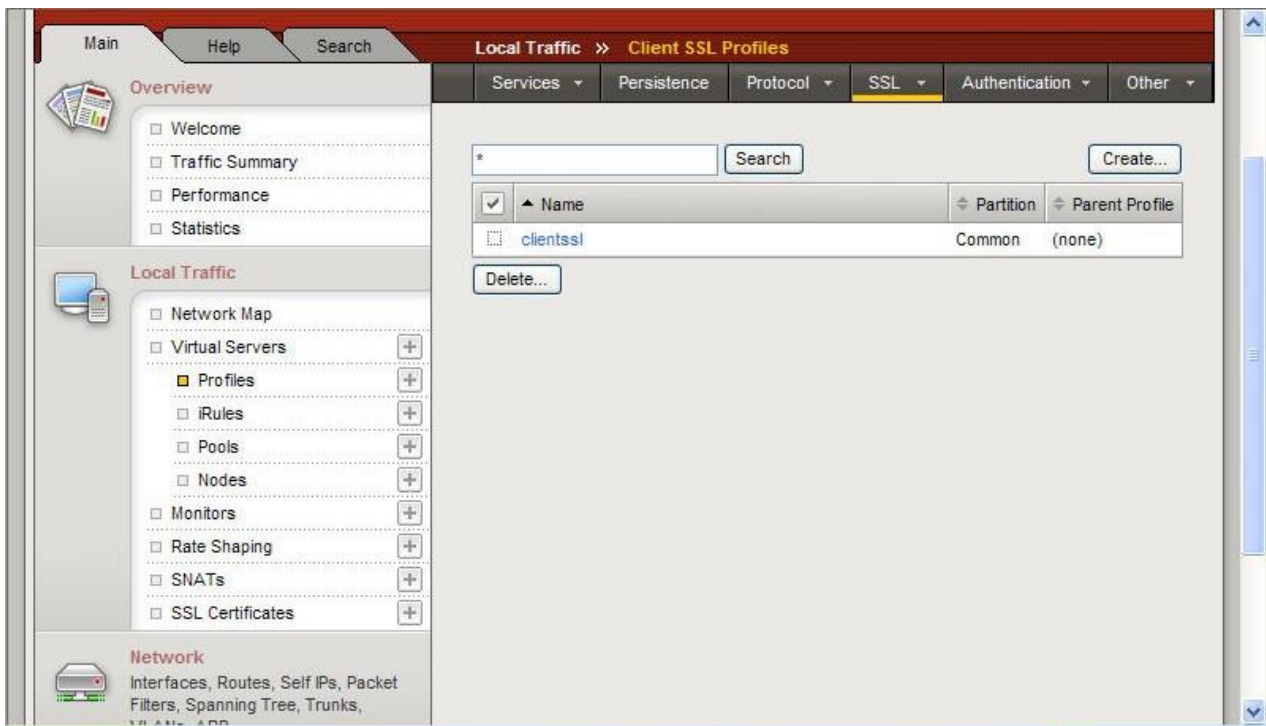
导入成功后，F5 将自动识别导入的证书为 Certificate Bundle。

4、配置服务器证书

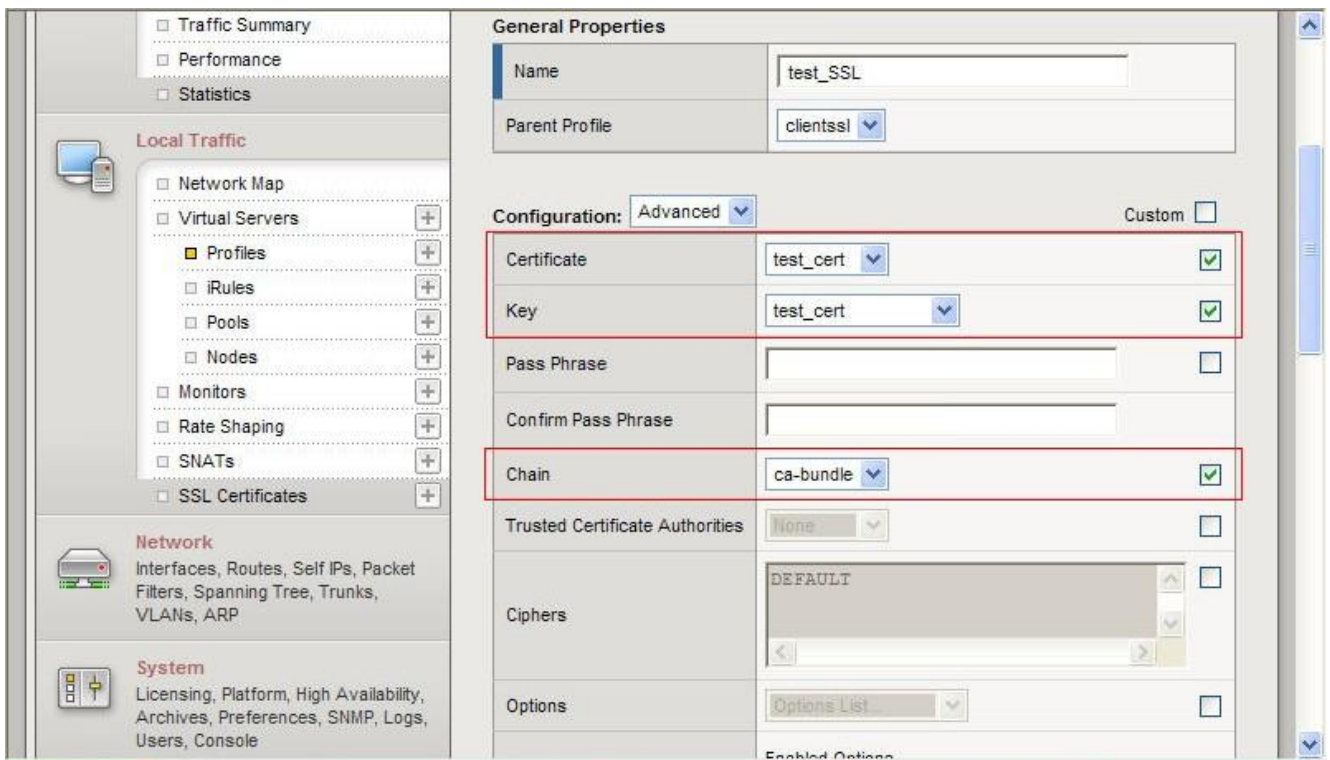
选择“Local Traffic” - “Virtual Servers” - “Profiles”

选择“Profile”中，“SSL”下的“Client”进入“Client SSL Profile”设置

如果您需要为站点配置一个全新的 SSL 证书，则需要新建一个 Client SSL Profile。如果您需要为一个已有证书的站点更新服务器证书，则仅需点击已存在的 Profile，进行编辑更新操作即可。



在新建的 Profile 中，选择当前 Profile 所使用的证书（Certificate）、私钥（key），以及在 Chain 处，设置与该证书应用相关联的证书链（之前导入的中级 CA 证书）。完成后，选择“Update”保存。



在证书成功配置后，需要创建一个 443 端口的 Virtual Server，并加载上面的 Client SS Profile 对应该站点启用 SSL 证书。

2.4 测试 SSL 证书

在浏览器地址栏输入：<https://s.wosign.com> (申请证书的域名) 测试您的 SSL 证书是否安装成功，如果成功，则浏览器地址栏后方会显示一个安全锁标志。测试站点证书的安装配置。

三、SSL 证书的备份

请保存好收到的证书压缩包文件和私钥文件，以防丢失。

四、SSL 证书的恢复

重复 2.3 操作即可。