

知 H3C F1000-E-SI防火墙SSL VPN证书导入配置案例

SSL VPN 证书 认证 丁犁 2015-12-03 发表

客户现场使用F1000-E-SI部署SSL VPN功能，需要将CA证书服务器上生成的证书上传并加载到防火墙中。

第一步：

路径：VPN>证书管理>PKI实体

创建PKI实体，点击“新建”按钮



输入

PKI实体名称：123

通用名：123

其他信息根据现场需求自定义

点击“确定”



第二步：

路径：VPN > 证书管理 > PKI域

创建PKI域，点击“新建”



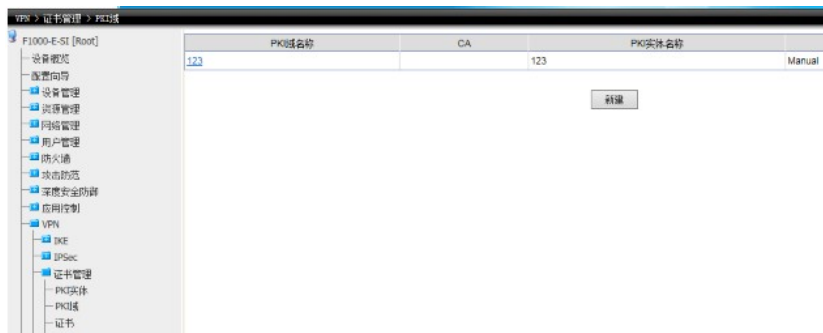
输入

PKI域名名称: 123

本端实体: 123 (第一步创建的PKI实体名称)

其他信息根据现场需求自定义

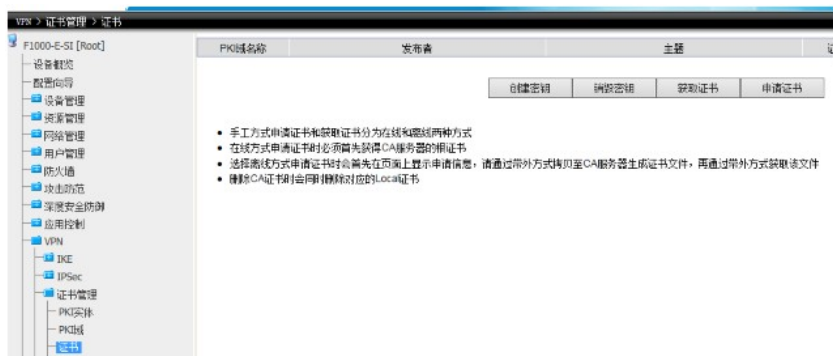
点击“确定”



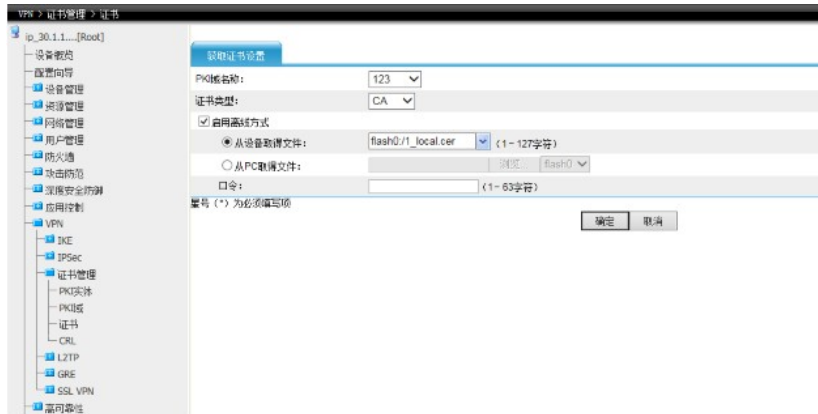
第三步:

路径: VPN > 证书管理 > 证书

点击“获取证书”



在获取证书设置中：
 选择第二步中创建的PKI域“123”
 证书类型选择“CA”
 选择“启用离线方式”
 从设备取得文件中选择flash中已经上传的证书文件“1_local.cer”
 点击“确认”



在获取证书设置中：
 选择第二步中创建的PKI域“123”
 证书类型选择“Local”
 选择“启用离线方式”
 从设备取得文件中选择flash中已经上传的证书文件“2003_local.pfx”
 口令中输入证书密码
 点击“确认”



根据上述步骤操作后，证书界面显示如下：



第四步：

路径：VPN > SSL VPN > 服务管理

在SSL中服务管理选择相关PKI域
 点击“确认”



通过上述四个步骤就完成SSL VPN的证书导入功能。