防火墙、IPS、LB产品是否涉及SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱漏洞（有补充+更新ssl服务策略名称为test）

漏洞相关 **王奎银** 2022-02-11 发表

漏洞相关信息

漏洞编号： 无

漏洞名称： SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱漏洞

产品型号及版本： 防火墙、IPS、LB产品

漏洞描述

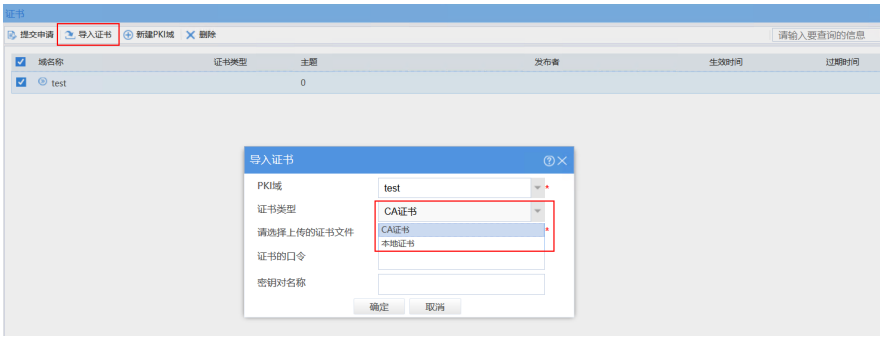
当服务器SSL/TLS的瞬时Diffie-Hellman公共密钥小于等于1024位时，存在可以恢复纯文本信息的风险

漏洞解决方案

1，配置SSL服务器端策略需要引用PKI域，首先新建PKI域。

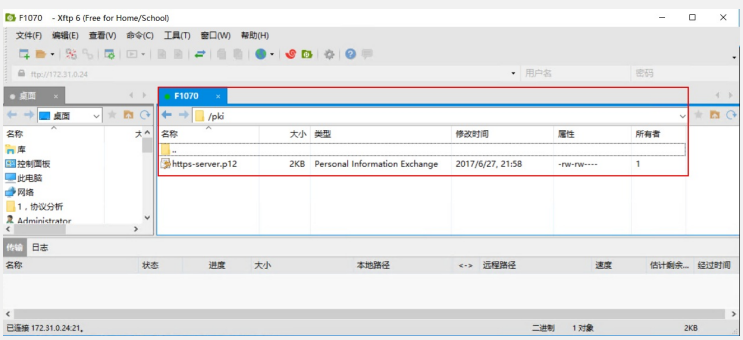
如下图所示，在防火墙Web界面【对象/PKI/证书】菜单栏中点击【新建PKI域】按钮，新建一个名称为“test”的PKI域。

2，然后为新建的PKI域导入CA证书和本地证书



3，证书可以通过 Microsoft Active Directory 证书服务 或者 Linux OpenSSL 来进行获取。如果需要权威CA证书，则需要向权威CA机构付费获取。防火墙flash包含一个自签名证书，https和sslvpn默认使用的就是这个自签名证书，可以将这个证书导出将公钥和私钥分离后分别作为CA证书和本地证书导入创建的PKI域，操作如下：

3.1，使用FTP或者SFTP的方式从防火墙的/**pki**/文件夹下获取对应的**https-server.p12**证书文件放置桌面。



3.2，双击证书文件，将导出的证书再导入到本地PC中，用来分离出不含私钥的CA证书。

3.3，由于防火墙自带的自签名证书没有对私钥进行口令保护，所以这里无须输入密码，直接点击“下一步”