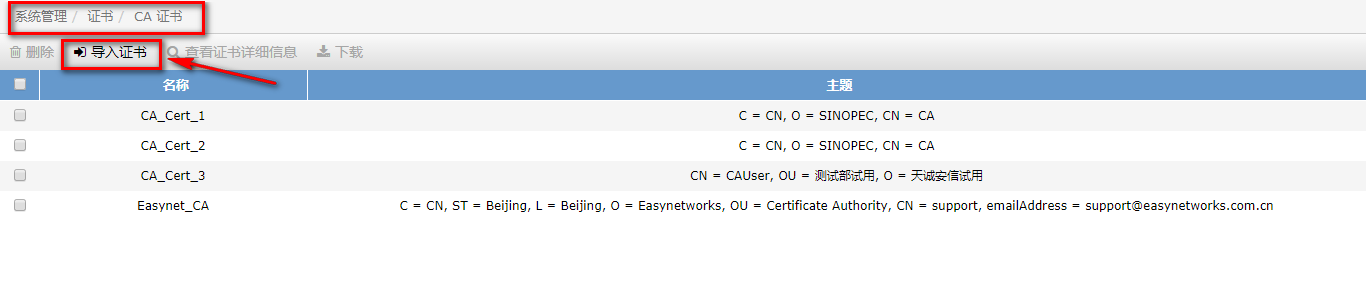
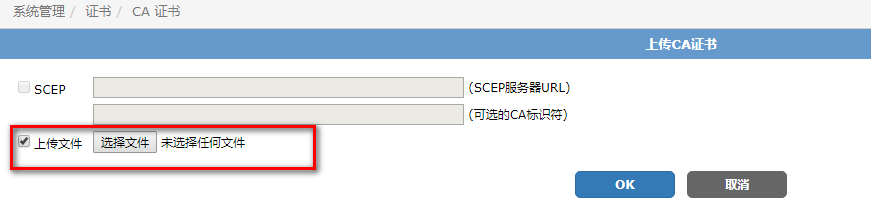
# 第一章 通过证书认证用户

# 根CA导入

根证书和二级根证书都是通过“系统管理>证书>CA证书”界面导入的。如下图所示：



选择“导入证书”。如下图所示，选择“上传文件”

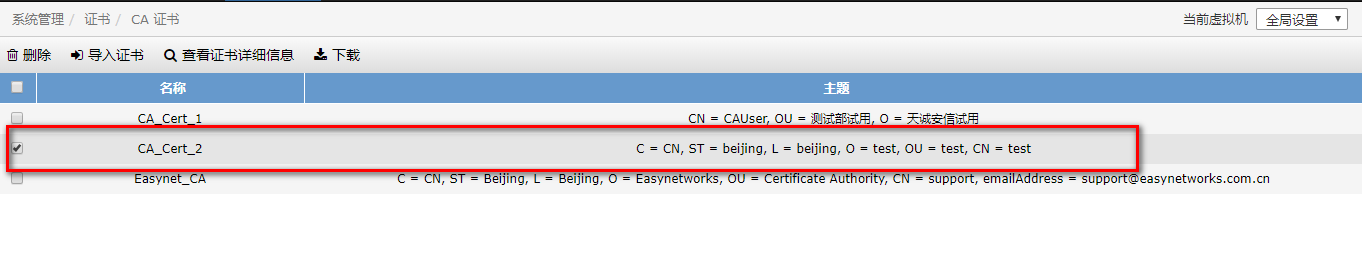


导入成功后，可以在“系统管理>证书>CA证书”中看到所导入证书。在本例中”CA\_Cert\_3”就是所导入的证书文件。

该文件是根CA



导入后效果如下



# 创建证书用户和用户组

首先在命令行下创建证书用户。

define user peer

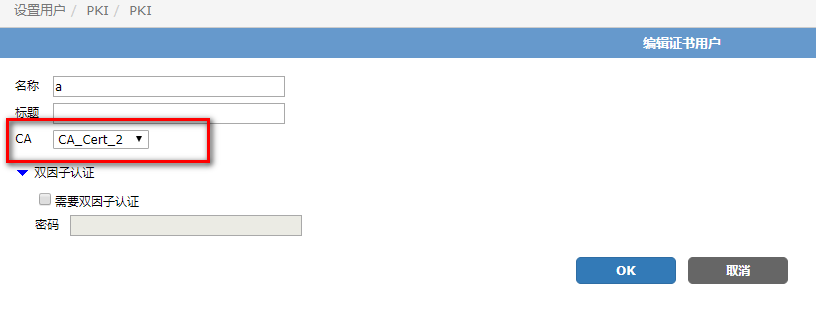
edit "a" ------名称可以随意指定

set ca "CA\_Cert\_2" ------此处指定所要用到的根证书

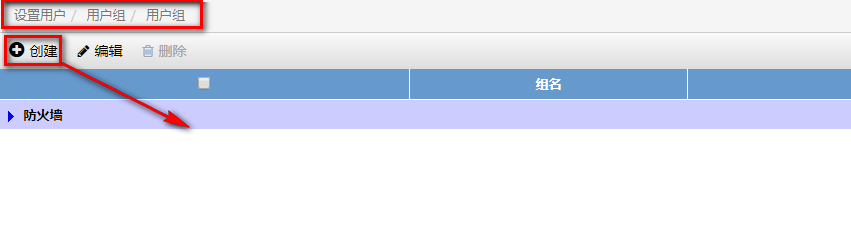
next

end

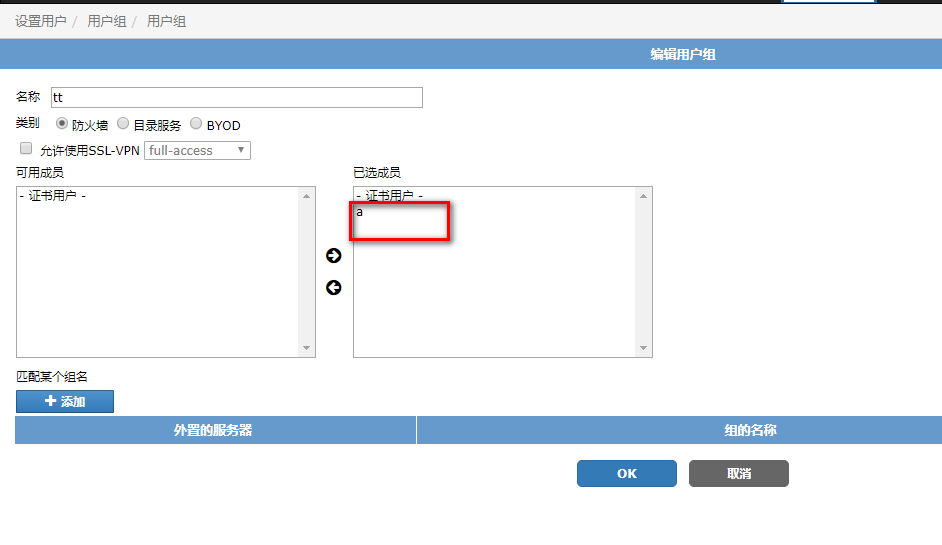
用户被创建后，图形界面中就会显示出“设置用户/PKI/PKI”。如下图所示，这部分内容就是我们命令行下设置的。如果我们希望证书认证管理员时，加上密码认证，也就是双因子认证，可以在该界面设置双因子认证。



然后是创建用户组。在菜单项中找到“设置用户/用户组/用户组”，如下图所示。



选择创建。名称可以随便定义，本例中设置为tt。将证书用户a选到右侧去，如下图所示。注意一个问题，这个用户组里只能证书用户，不能放其他用户。

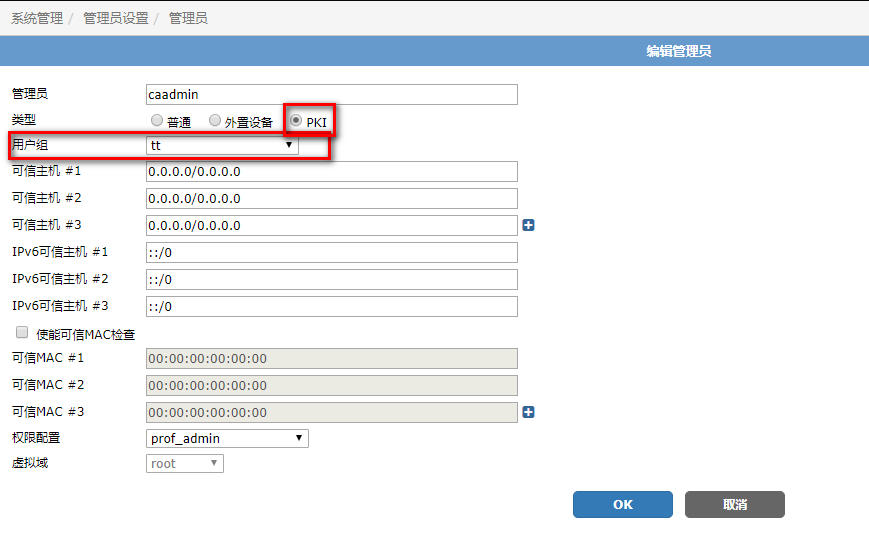


# 设置管理员

找到“系统管理/管理员设置/管理员”，点击“创建”，如下图所示。



创建管理员的界面如下图。管理员名称可以随意输入。类型选择为“PKI”。权限设置根据需求来选择，本例中选择prof\_admin。



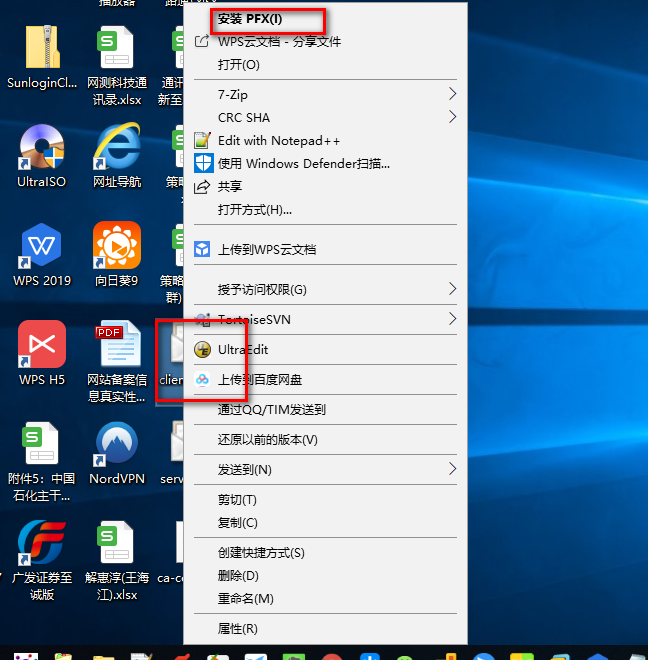
# 使用证书管理员进行登录。

首先将浏览器导入证书。证书来源可以是在浏览器中生成请求，然后在CA证书服务器上批准，然后安装。也可以直接使用带私钥证书PFX，本例中使用test0908.pfx如下图所示。

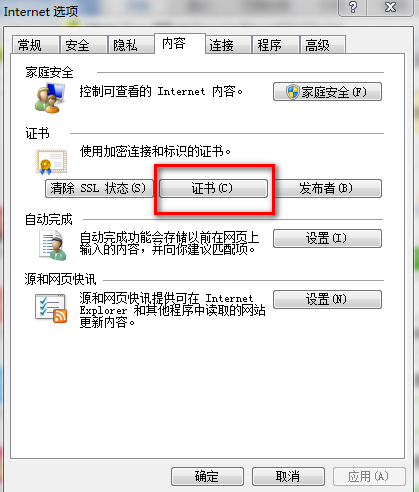
证书如下，密码是空。



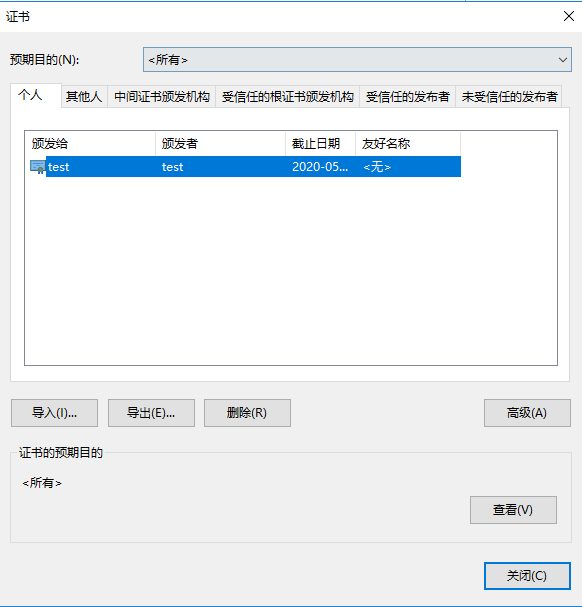
将该文件保存到桌面，然后选择右键安装。



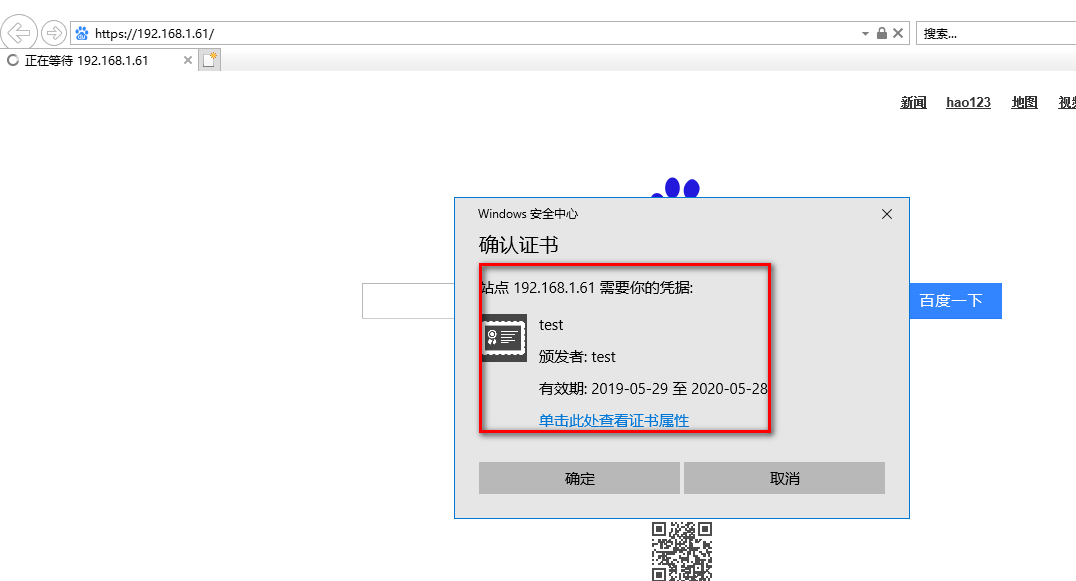
导入成功后，可以在IE浏览器中看到该证书。选择“Internet选项”，然后选择“内容”，最后选择“证书”



个人证书中的test就是所导入的证书



然后用浏览器打开防火墙管理界面



这里是提示使用什么证书，在本例中选择test

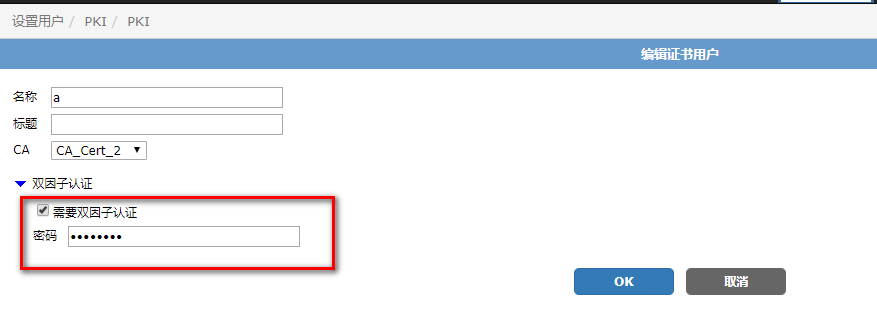
然后会提示服务器发放证书，如下图所示。选择继续浏览此网站。



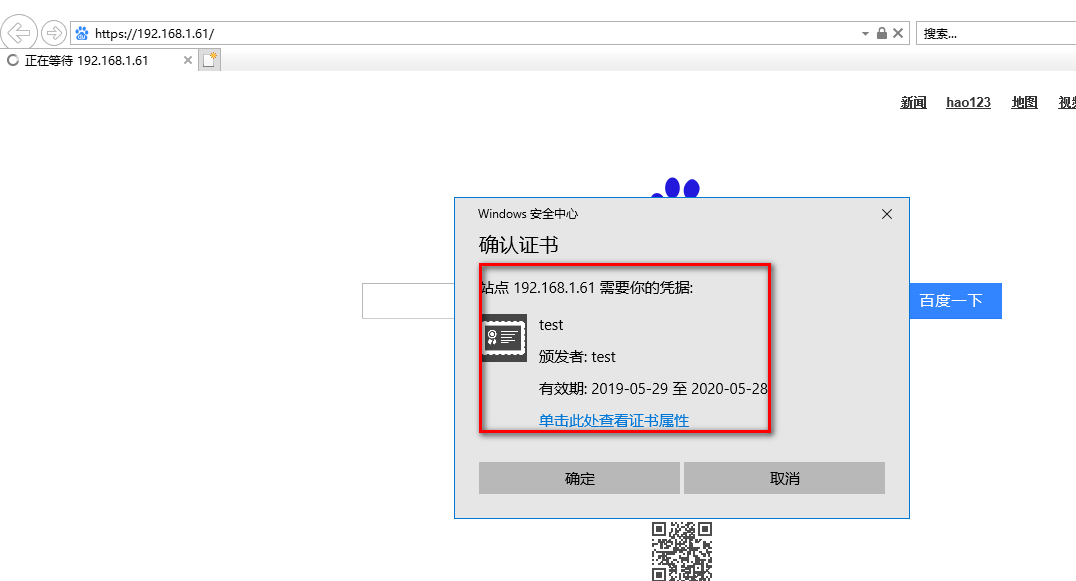
然后我们就可以成功地登录到防火墙了。

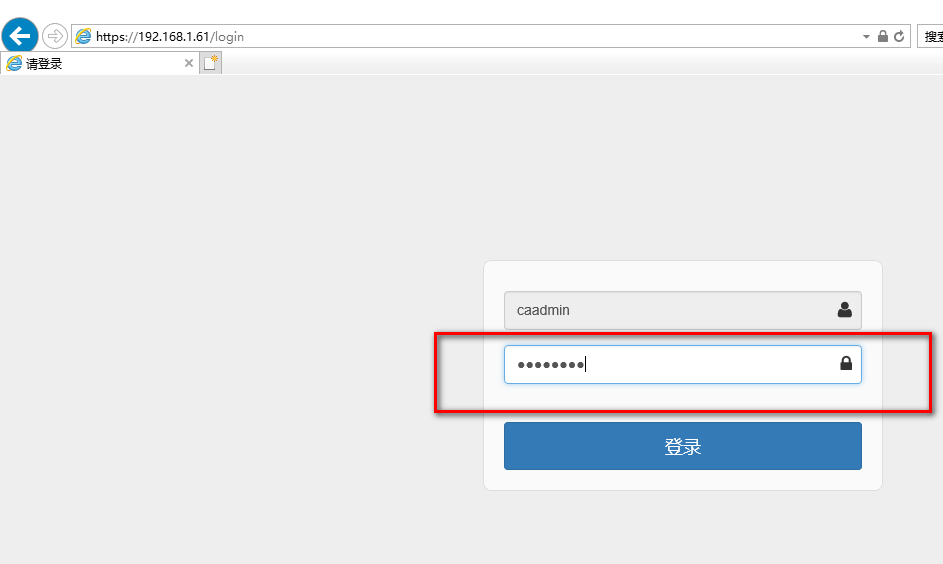
# 双因子认证客户端

所有步骤都如上，但是在CA用户，增加双因子认证选项，设置密码为12345678



当用户登录时会提示提交证书和输入密码





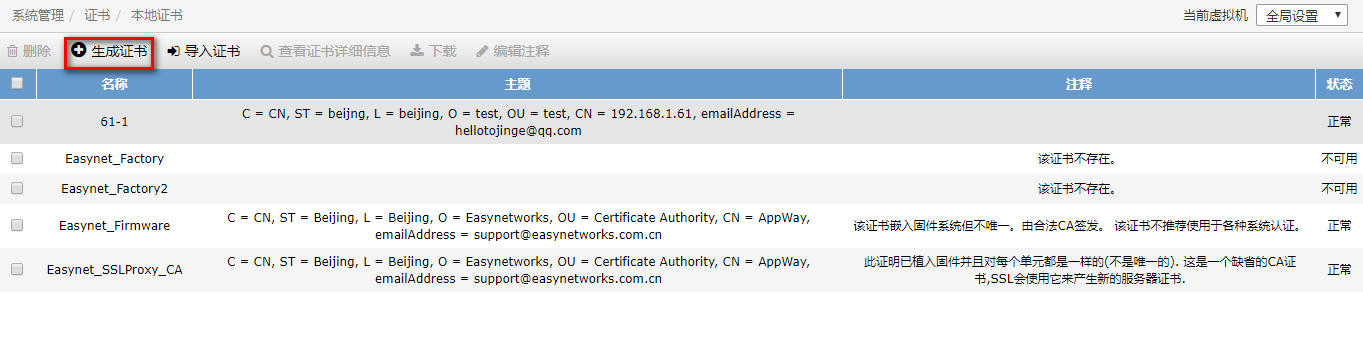
# 交叉认证

所谓交叉认证，就是不仅仅是防火墙认证用户，用户也认证防火墙。除了第一章的内容外，还需要完成以下步骤

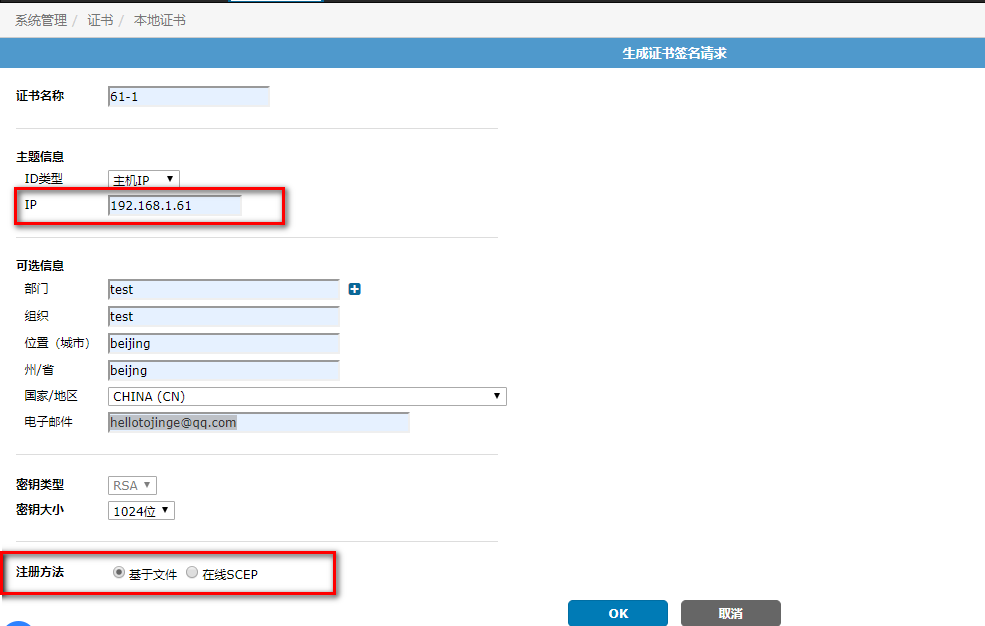
1. 给防火墙签发证书
2. 给客户端导入根CA

# 防火墙生成证书请求

在“系统管理/证书/本地证书”中，点击生成证书



生成证书配置如下：





点击下载，得到证书

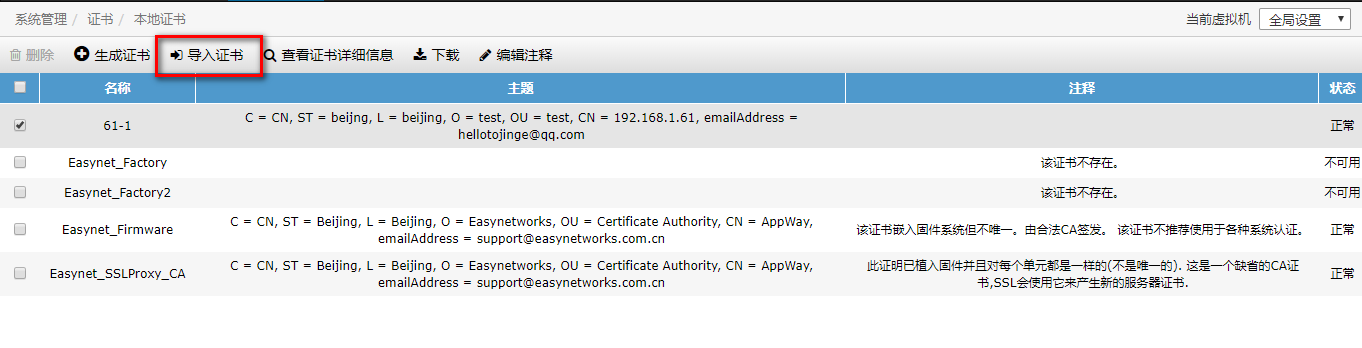


# 根据请求，签发证书

将61-1.csr发送给证书服务器，进行签名，得到



然后将其导入防火墙。如下图所示，选择“导入证书”



# 防火墙设置使用该证书

防火墙上配置使用该证书，用于发给客户端做验证用。

define system global

set admin-server-cert "61-1"

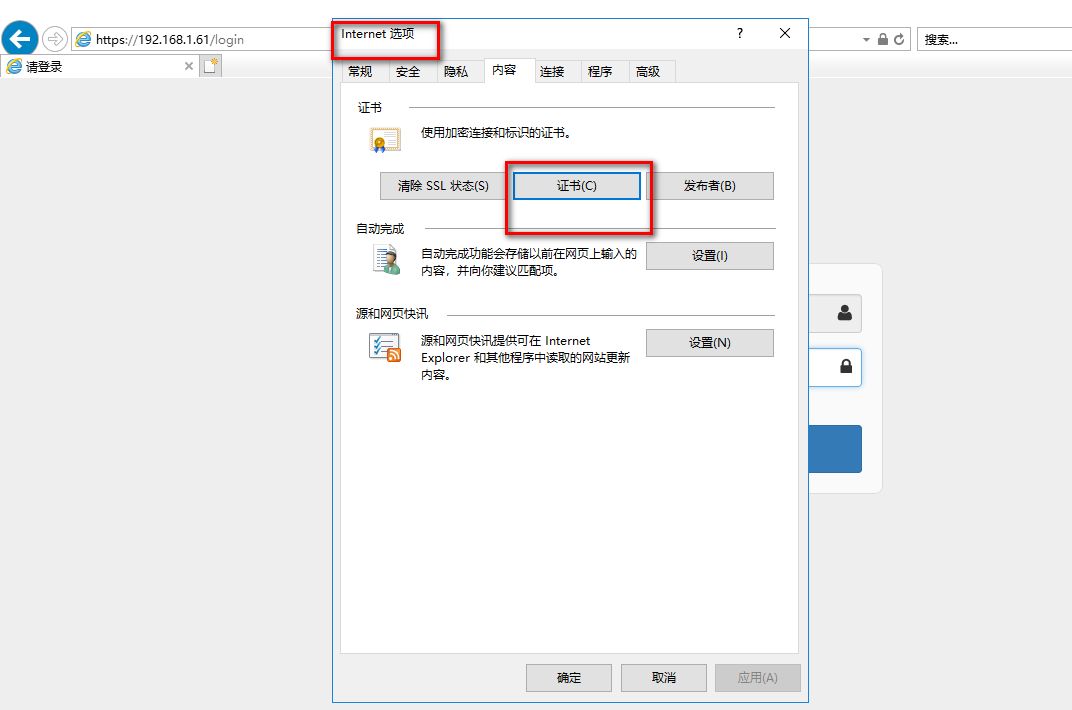
end

# 用户端导入根证书

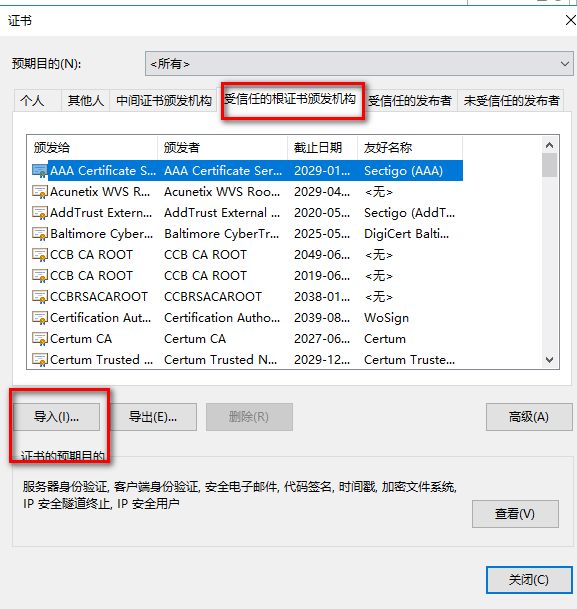
在用户端导入该根CA。



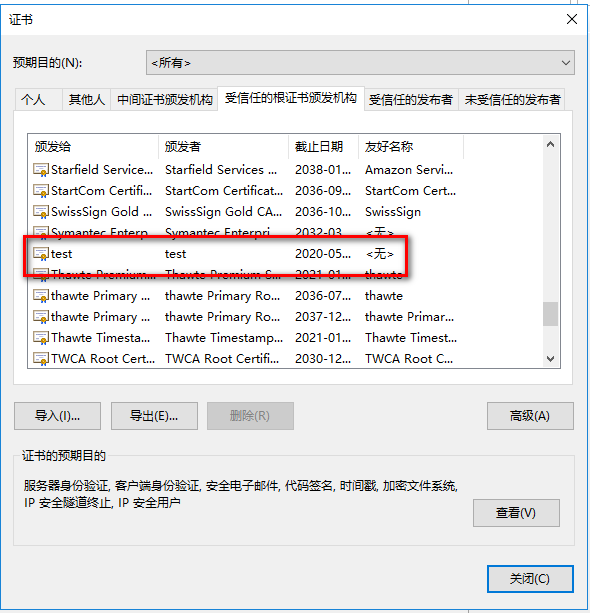
在IE的Internet选项中选择“内容”，然后选择“证书”



找到“受信任的根证书颁发机构”，选择“导入”，如下图所示。



导入完毕后，可以看到test这个根证书。



# 客户端登录

完成上述设置后，客户端访问防火墙就不会有证书存在问题的提示了。

# 

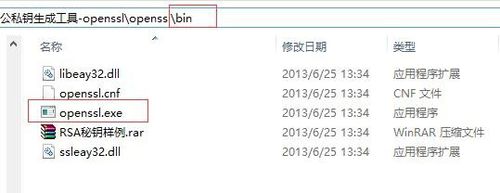
# Openssl 生成证书

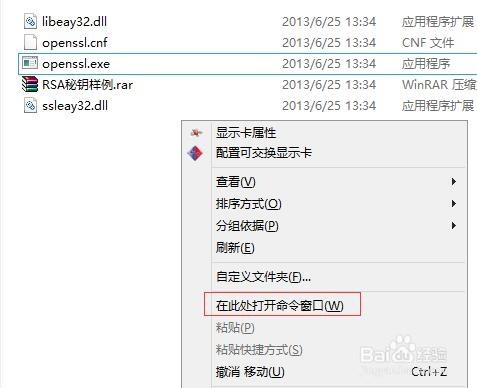
前面所用证书，都是通过openssl生成的。

# 安装OPENSSL

1、下载openssl工具到本地电脑，然后解压，进入bin目录

在当前目录，按住shift键右击，选择"在此处打开命令窗口"

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=1)

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=2)

2、打开cmd命令窗口之后，可以看到，已经自动切换到当前的bin目录位置

输入openssl命令，进入openssl

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=3)

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=4)

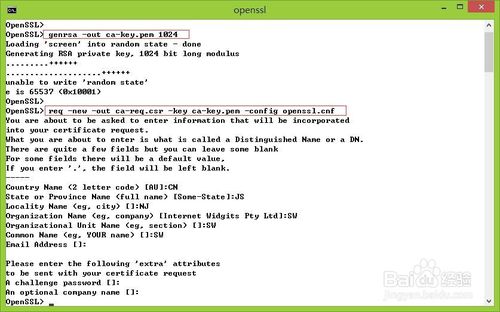
现在开始生成CA证书

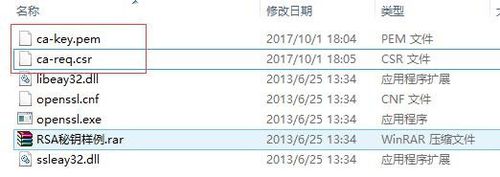
# 生成私钥和公钥

创建私钥：genrsa -out ca-key.pem 1024

创建证书请求：req -new -out ca-req.csr -key ca-key.pem -config openssl.cnf

执行之后，会在目录下生成ca-key.pem和ca-req.csr文件

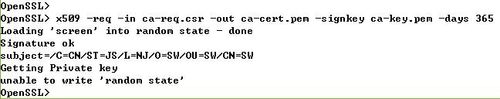
[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=5)

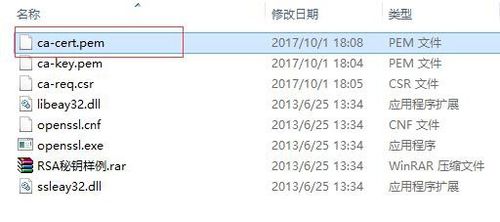
[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=6)

自签署证书：

x509 -req -in ca-req.csr -out ca-cert.pem -signkey ca-key.pem -days 365

执行完成之后会生成ca-cert.pem文件

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=7)

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=8)

# 生成server证书

创建私钥:

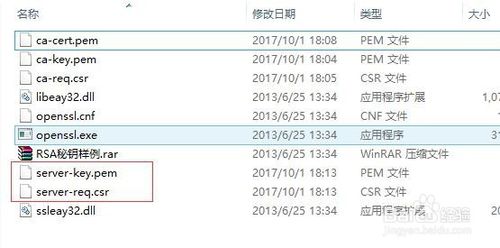
genrsa -out server-key.pem 1024

创建证书请求：

req -new -out server-req.csr -key server-key.pem -config openssl.cnf

执行完成生成server-key.pem和server-req.csr文件

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=9)

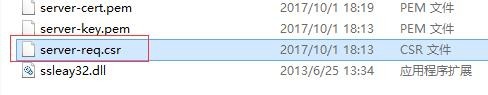
[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=10)

自签署证书：

x509 -req -in server-req.csr -out server-cert.pem -signkey server-key.pem -CA ca-cert.pem -CAkey ca-key.pem -CAcreateserial -days 365

执行完成生成server-cert.pem文件

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=11)

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=12)

在本例中用不到服务器证书。

# 生成客户端证书

生成client证书，与服务器生成证书差不多

创建私钥：

genrsa -out client-key.pem 1024

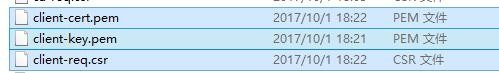
创建证书请求：

req -new -out client-req.csr -key client-key.pem -config openssl.cnf

自签署证书：

x509 -req -in client-req.csr -out client-cert.pem -signkey client-key.pem -CA ca-cert.pem -CAkey ca-key.pem -CAcreateserial -days 365

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=13)

[](http://jingyan.baidu.com/album/6c67b1d6be538c2787bb1e06.html?picindex=14)

生成带私钥的p12证书：

pkcs12 -export -in client-cert.pem -inkey client-key.pem -out client-key.p12

该证书是给客户端浏览器安装的

# 给防火墙证书进行签发

将第三章中的61-1.csr导入到openssl目录下，执行该命令进行签发

x509 -req -days 3650 -in 61-1.csr -CA ca-cert.pem -CAkey ca-key.pem -CAcreateserial -out 61-1.pem

61-1.pem就是签发的证书，导入到防火墙就可以使用了。

# 常见问题

1. 注意一下时间，证书时间和防火墙时间是否匹配。因为证书是有有效时间的。
2. 如果浏览器进行登录时，不能出现提交证书的页面。首先关闭所有浏览器，然后再打开。如果还不行，则清理ssl缓存。如果还不行，则重启防火墙。