# 使用证书认证SSL VPN

## 一、首先获得以下三种证书

1、根证书，直接找用户要即可



2、给防火墙签发的证书

首先在防火墙界面生成一个证书请求



填写下面内容，选择“基于文件”



将生成的文件发送给CA管理员。签名后导入即可。



1. 客户端证书



前者是私钥，后者证书请求。将client.csr发送给CA管理员进行签名，得到



如果得到的”.cer”文件，那么直接将后缀改成“.crt”。

客户端证书采用OPENSSL来制作：

1，生成客户端私钥

openssl genrsa -des3 -out client.key 1024

2，生成客户端证书请求

openssl req -new -key client.key -out client.csr

## 防火墙端配置

1、进入“VPN/SSL/设置”里，设置启用ssl-vpn，然后服务器证书选择CA管理员所签发的证书，然后选择“要求客户端认证”。这两个步骤是关键。后面的配置就和普通ssl vpn配置没有任何区别了。



1. 新建账号test，设置密码。如下图所示。



1. 建立用户组。在“设置用户/用户组”选择新建用户组。注意，要选择“允许使用SSL-VPN”，这样就把该用户组与SSLVPN绑定了。



1. 设置路由。缺省状态下，给ssl vpn用户分配的地址是10.0.0.1-10.0.0.10。所以要给ssl.root增加一个路由，就是10.0.0.0/24网段。如下图所示。



1. 添加策略。策略分为两条，一个是认证策略，一个是控制策略。

认证策略是从“拨入接口”到内网，动作设置为“SSL VPN”，用户认证选择我们前面所建的用户组t，服务选择为ANY，时间设置为“always”



流量策略是ssl vpn隧道接口与内网接口之间建立，动作是Accept。如下图所示。



## 客户端配置

建议windows10作为客户端。首先安装客户端软件。

<http://update.easynetworks.com.cn/download/sslvpn/ksoft-installer.exe>

安装完毕后，会进入该界面。在此处设置“拨号目标IP地址:10443”



选择，进入配置界面

CA证书指的是根证书。

用户证书是用户申请后被签发的证书

用户密钥是用户生成私钥。



然后输入用户私钥的密码“123456”



完成以上操作后，点击连接，然后在提示下，输入用户名test，密码123456。

灯变成绿色，表明vpn通道建成。



注意：完成通道建立后，会自动缩小到屏幕的右下角，图标如下。

