FortiGate 结合 Openssl + freeradius

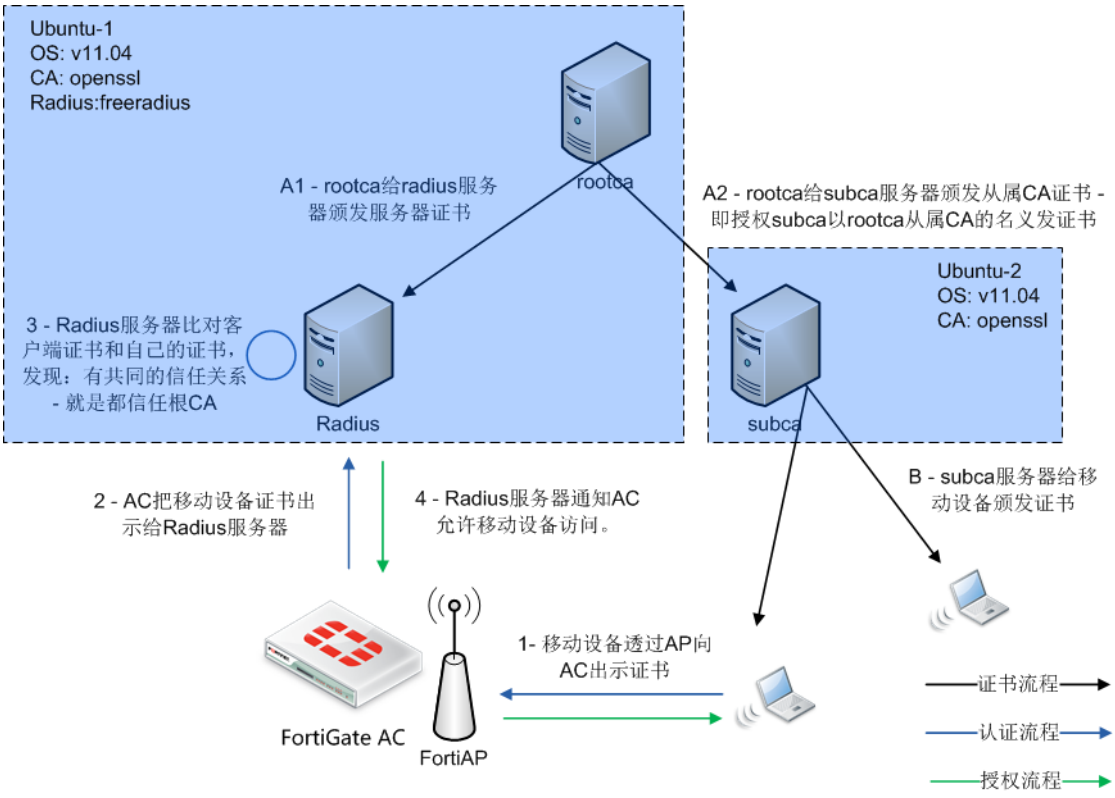
实现多级 CA 环境下的无线用户 EAP-TLS 认证

一、 EAP-TLS 简介

简而言之，使用数字证书来保护 radius 认证，与 802.1x 结合，可以用数字证书认证无线上网用户，是最安全的无线认证方法之一。

参考：http://zh.wikipedia.org/wiki/EAP#EAP-TLS

二、 实验环境



* Radius 服务性的认证模式：EAP-TLS，仅对证书信任关系判断，不需要查询数据库或LDAP的认证信息。
** 一旦信任关系建立，则Radius服务器不需要到CA服务器去查询任何信息，故CA服务器可离线。

如上图所示，使用两台 ubuntu linux 服务器，Ubuntu-1 作为 rootca 和 radius 服务器；Ubuntu-2 作为 subca。

FortiOS：v4.3.6。

三、 安装 openssl 及 freeradius

sudo apt-get install openssl

sudo apt-get install freeradius

四、 openssl 环境准备

1. 在 ubuntu1 和 ubuntu2 的当前用户文件夹（例如/home/jeff/）下创建 openssl 工作数据存放文件夹，例如/home/jeff/certs/。
2. 将附件的设置文件 myopenssl.cnf 存放在/home/jeff/certs/目录下。注意修改一下配置文件中的 dir 路径。


myopenssl.cnf

3. 注意事项：Radius 服务器端证书的 extendedKeyUsage 属性必须包含服务器身份认证（1.3.6.1.5.5.7.3.1）；移动设备证书的 extendedKeyUsage 属性必须包含客户端身份验证 (1.3.6.1.5.5.7.3.2)。myopenssl.cnf 中已经包括相关设置。

五、 在 Ubuntu-1 上建立根 CA（密码：1234）

4. 生成根 CA 私钥（需要指定 Common Name）

cd /home/jeff/certs

openssl req -newkey rsa:1024 -sha1 -config ./myopenssl.cnf -keyout rootkey.pem -out rootreq.pem -days 3650

5. 生成证书，并用私钥签名

openssl x509 -req -in rootreq.pem -sha1 -extfile ./myopenssl.cnf -extensions v3_ca -signkey rootkey.pem -out rootcert.pem -days 3650

6. 组合证书与私钥，形成 CA 根证书

cat rootcert.pem rootkey.pem > root.pem

7. 显示根证书

openssl x509 -text -noout -in root.pem

六、 在 Ubuntu-2 上建立二级 CA（密码：5678）

8. 在 Ubuntu-2 上创建二级 CA 私钥（需要指定 Common Name）

```
cd /home/jeff/certs

openssl req -newkey rsa:1024 -sha1 -config ./myopenssl.cnf -keyout subcakey.pem
-out subcareq.pem  -days 3650
```

9. 将 subcakey.pem 复制到 Ubuntu-1 上，生成二级 CA 证书，并用根 CA 证书签名

```
openssl x509 -req -in subcareq.pem -sha1 -extfile ./myopenssl.cnf  -extensions v3_ca
-CA root.pem -CAkey root.pem  -CAcreateserial -out subcacert.pem  -days 3650
```

10. 将 subcacert.pem 和 rootcert.pem 复制回 Ubuntu-2 上，组合二级 CA 证书与二级 CA 私钥，形成二级 CA 证书

```
cat subcacert.pem subcakey.pem rootcert.pem > subca.pem
```

11. 显示二级 CA 证书

```
openssl x509 -text -noout -in subca.pem
```

七、 在 Ubuntu-1 上，使用根 CA 为 openradius 颁发服务器证书（密码：abcd）

12. 创建服务器证书私钥（需要指定 Common Name）

```
openssl req -newkey rsa:1024 -sha1 -config ./myopenssl.cnf  -keyout serverkey.pem
-out serverreq.pem  -days 365
```

13. 创建服务器证书，并签名

```
openssl x509 -req -in serverreq.pem -sha1 -extfile ./myopenssl.cnf  -extensions
server_cert -CA root.pem -CAkey root.pem  -CAcreateserial -out
servercert.pem  -days 365
```

14. 组合私钥与证书，形成服务器证书

```
 cat servercert.pem serverkey.pem rootcert.pem > server.pem
```

15. 显示服务器证书

```
openssl x509 -text -noout -in server.pem
```

八、 在 Ubuntu-2 上，使用二级 CA 为 Wifi 客户端颁发证书（密码：efgh）

16. 创建客户端证书私钥（需要指定 Common Name）

```
openssl req -newkey rsa:1024 -sha1 -config ./myopenssl.cnf    -keyout clientkey.pem -out clientreq.pem  -days 365
```

17. 创建客户端证书，并签名

```
openssl x509 -req -in clientreq.pem -sha1 -extfile ./myopenssl.cnf  -extensions client_cert -CA subca.pem -CAkey subca.pem -CAcreateserial -out clientcert.pem  -days 365
```

18. 组合私钥与证书，形成客户端证书

```
cat clientcert.pem clientkey.pem subcacert.pem rootcert.pem > client.pem
```

19. 显示客户端证书

```
openssl x509 -text -noout -in client.pem
```

20. *.pem 的证书是 BASE64 形式的，要转成 PKCS12 才能装到 Windows 上。转换命令如下（需要设置导出密码，为 xyz）：

```
openssl pkcs12 -export -in clientcert.pem -inkey clientkey.pem -out client.pfx
```

21. 将 client.pfx 复制到 Windows PC 上，导入 IE 浏览器的个人证书区。注意导入密码是 xyz

九、 配置 freeradius（Ubuntu-1）

22. 配置 radiusd.conf

```
cd /etc/freeradius

sudo gedit radiusd.conf
```

1）确认 eap 没有被注释掉

```
$INCLUDE eap.conf
```

2）修改 log 段，启用认证日志

```
auth = yes
```

23. 将服务器证书 server.pem（带私钥）和根 CA 证书 rootcert.pem（不带私钥）复制到 freeradius 的证书目录下

```
sudo cp /home/jeff/certs/server.pem /etc/freeradius/certs/
```

sudo cp /home/jeff/certs/rootcert.pem /etc/freeradius/certs/

需要修改/etc/freeradius/certs/的权限，否则 freeradius 不能读取证书

sudo cd /etc/freeradius/certs

sudo chmod -R ug+rwx .

24. 配置 eap.conf，启用 eap-tls

cd /etc/freeradius

sudo gedit eap.conf

关键语句如下：

```
eap {
        default_eap_type = tls                          #认证类型：tls
        tls {
            certdir = ${confdir}/certs                  #服务器证书目录
            cadir = ${confdir}/certs                    #CA 证书目录
            private_key_password = abcd                 #服务器私钥密码
            private_key_file = ${certdir}/server.pem    #服务器私钥文件
            certificate_file = ${certdir}/server.pem    #服务器证书文件
            CA_file = ${cadir}/rootcert.pem             #CA 证书文件
            }
        }
```

25. 配置 clients.conf

cd /etc/freeradius

sudo gedit clients.conf

```
client 192.168.1.99{                                    #FortiGate 地址
        secret          =123456                         #预共享密钥
        shortname       =fortigate                      #别名
}
```

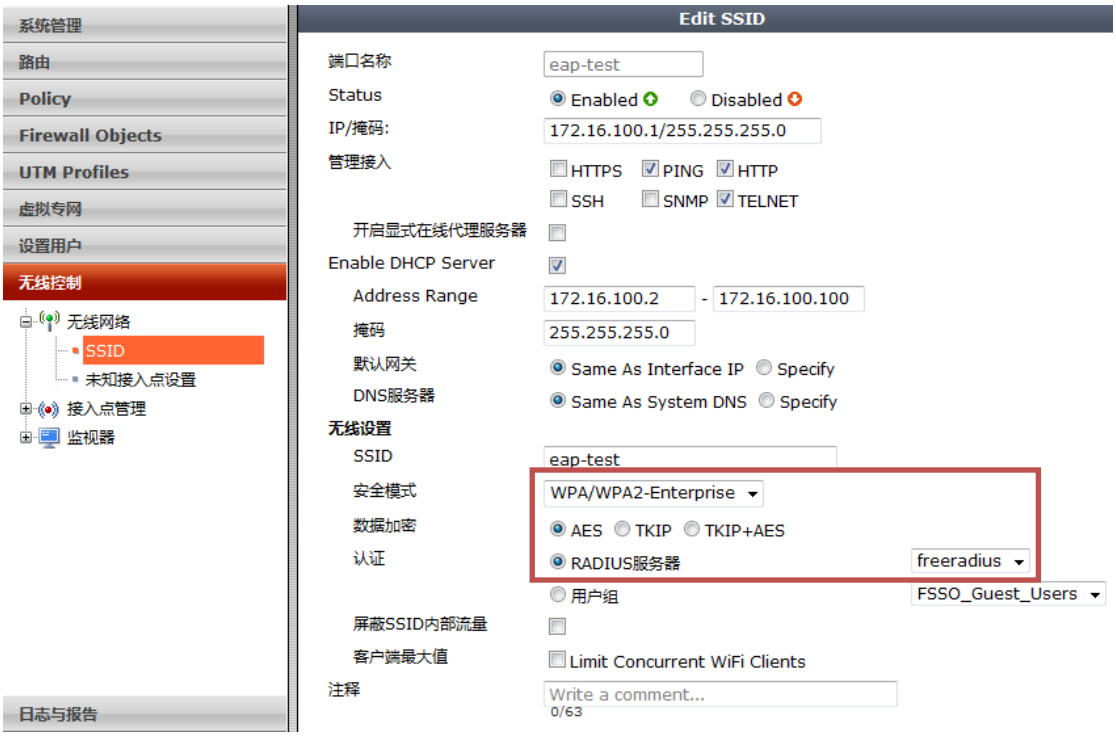
26. 重启 freeradius 服务

sudo service freeradius restart

十、 配置 FortiGate

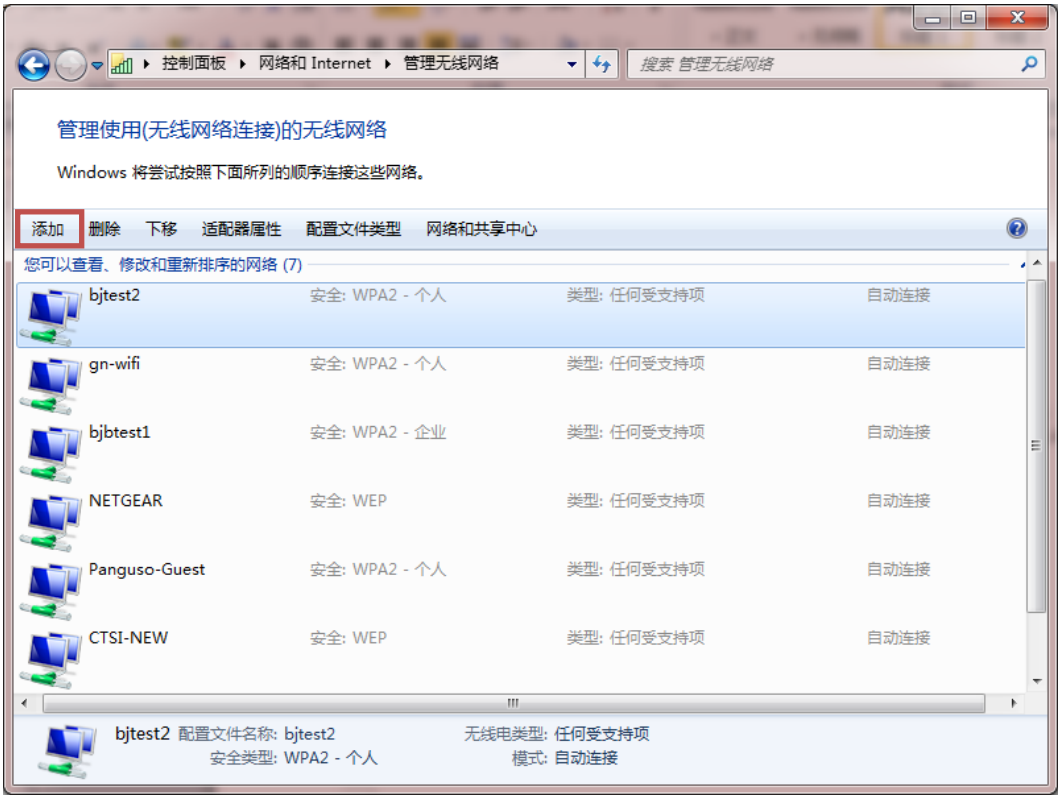
27. 配置 Radius 服务器

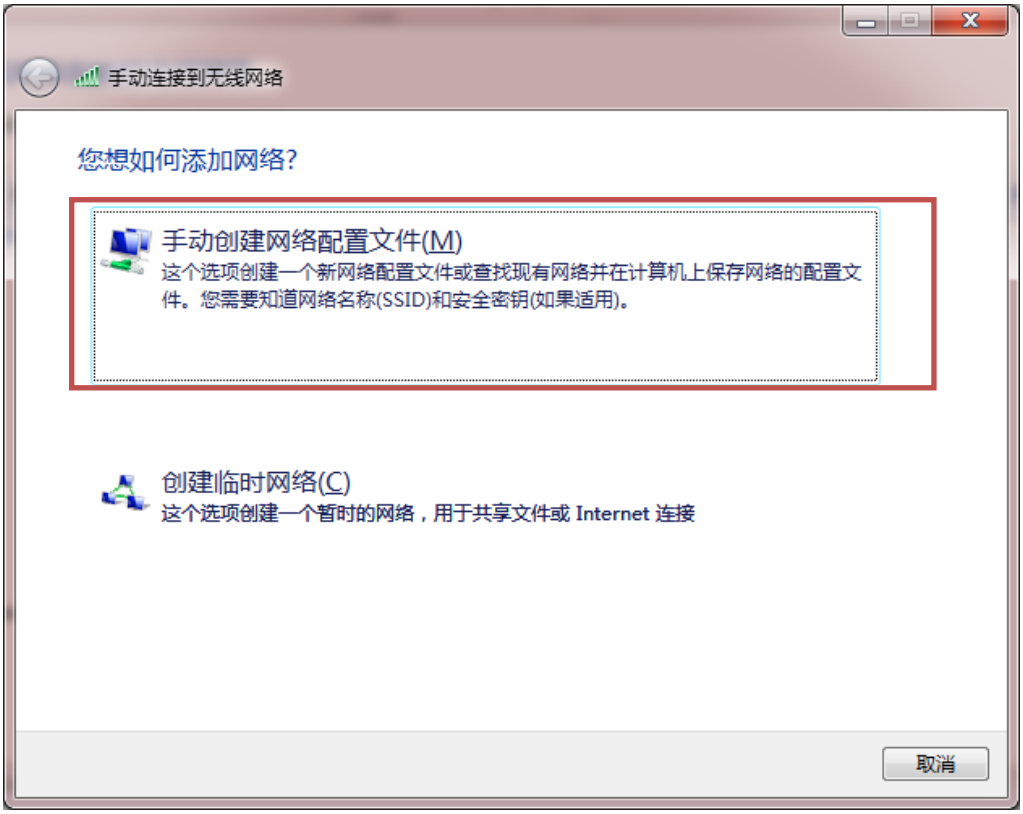
28. 配置 SSID，设置为 WPA/WPA2-Enterprise 安全模式

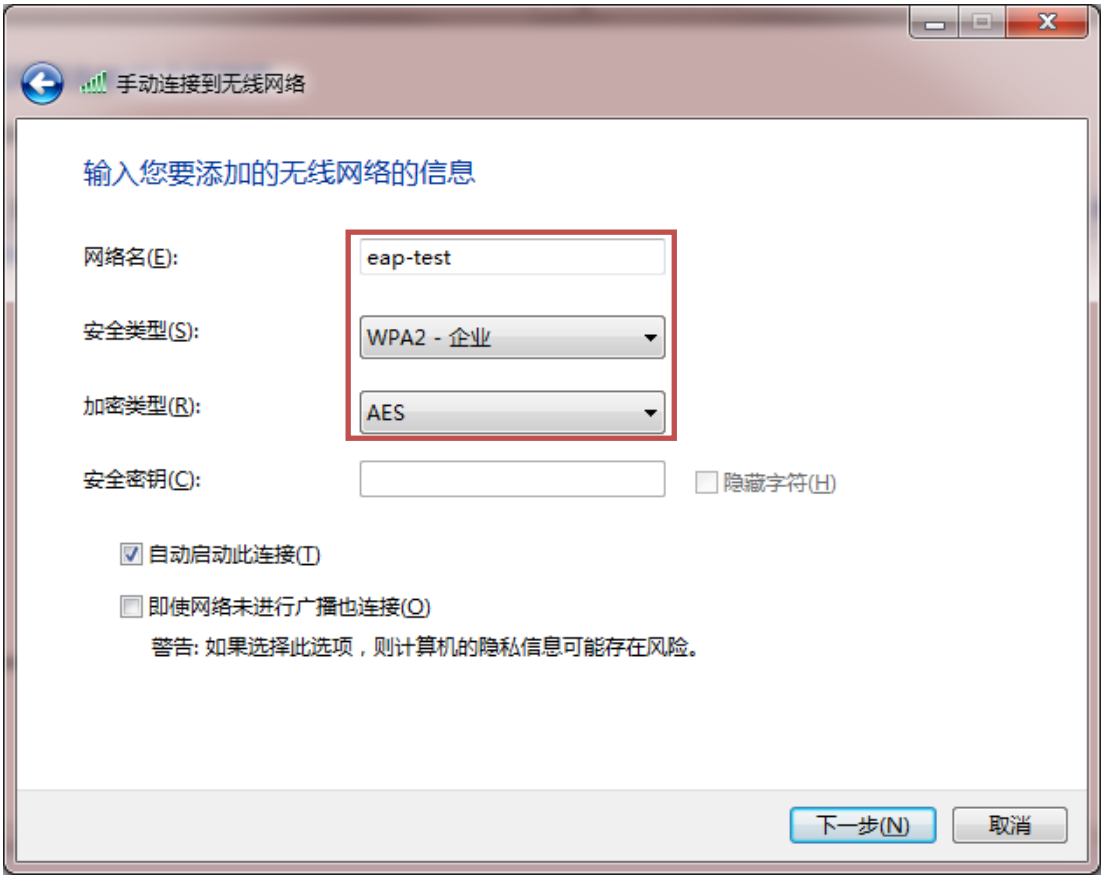


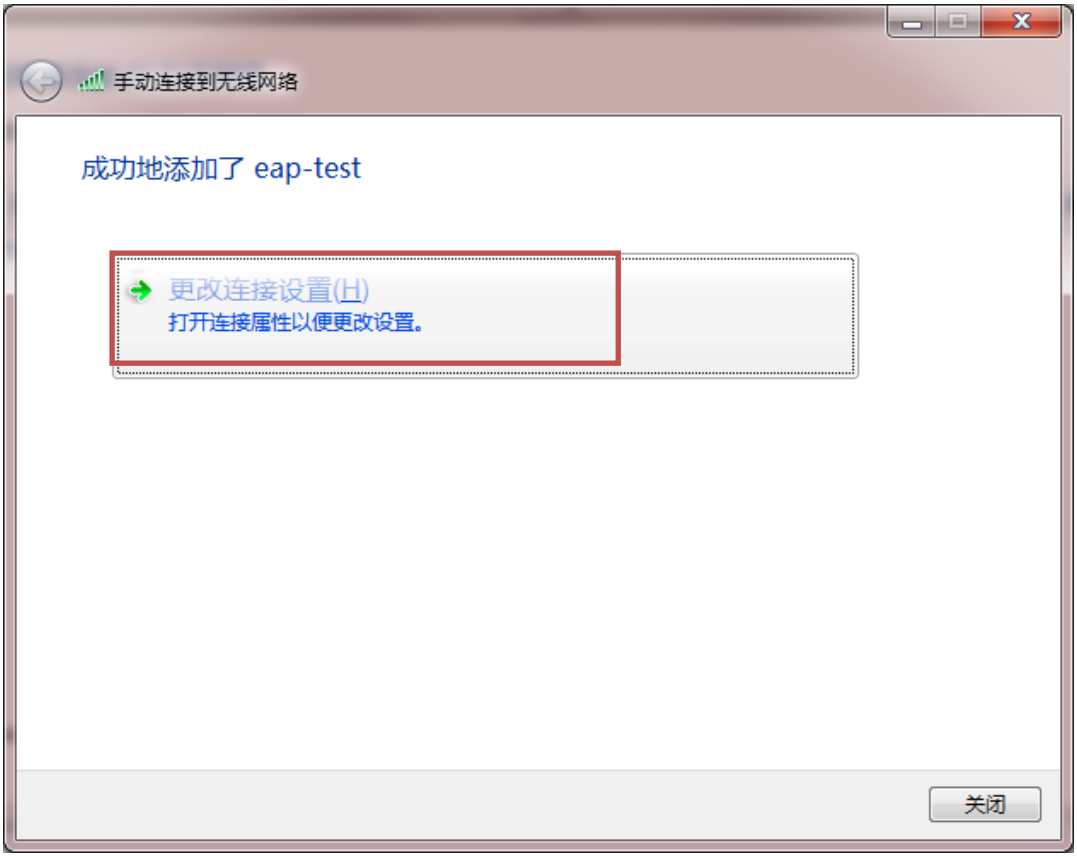
十一、 Windows wifi 设置

29. 手动添加无线网络

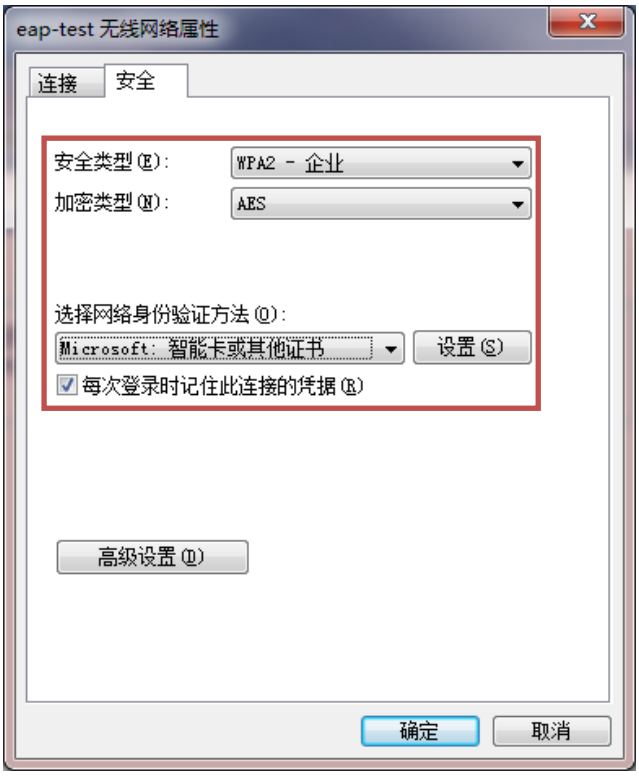




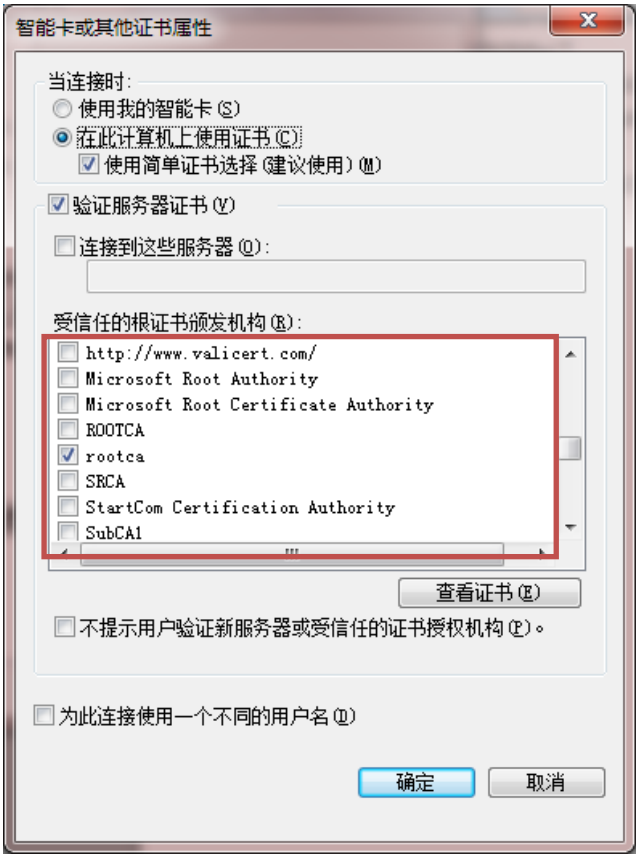

手动连接到无线网络
输入您要添加的无线网络的信息
网络名(E):
eap-test
安全类型(S):
WPA2 - 企业
加密类型(R):
AES
安全密钥(C):
隐藏字符(H)
自动启动此连接(T)
即使网络未进行广播也连接(O)
警告: 如果选择此选项，则计算机的隐私信息可能存在风险。
下一步(N)
取消


手动连接到无线网络
成功地添加了 eap-test
更改连接设置(H)
打开连接属性以便更改设置。
关闭

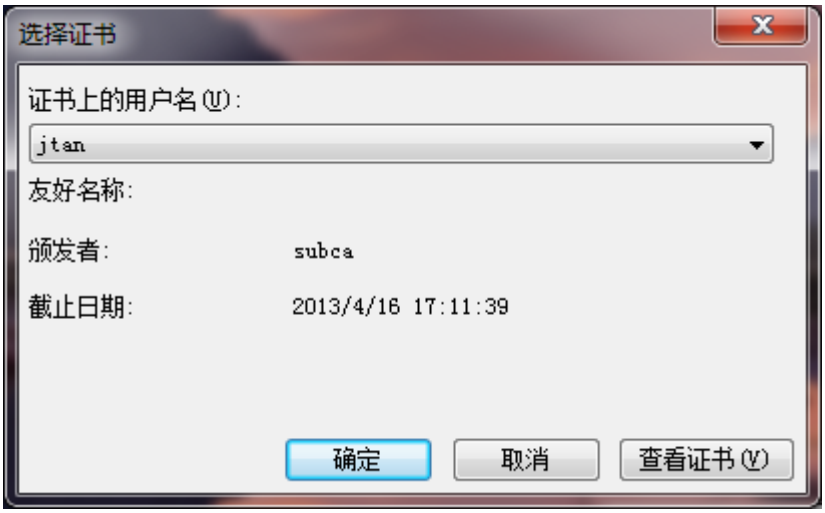
30. 使用 WPA2-企业安全类型，选择身份验证方法为“智能卡或其他证书”。



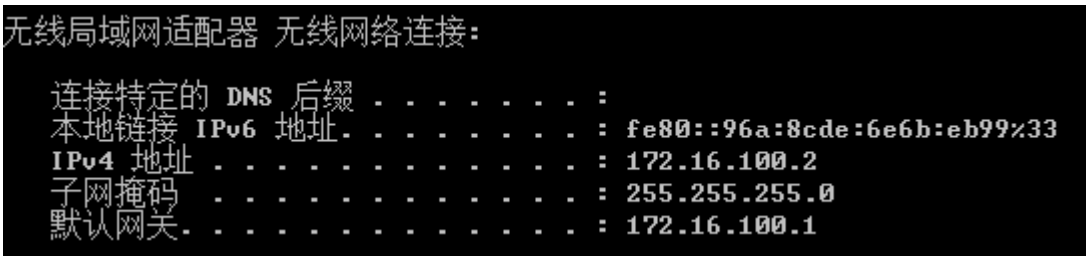
31. 点击设置，选择信任 rootca



32. 连接 eap-test，选择正确的证书

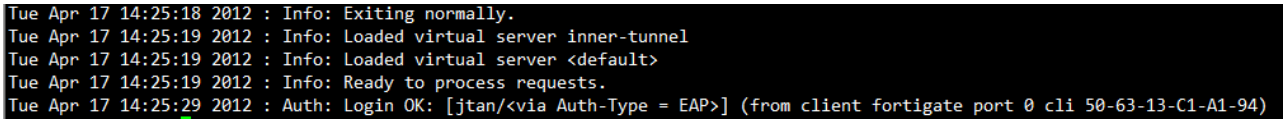


33. 成功连接



34. 查看 freeradius 日志

sudo more /var/log/freeradius/radius.log



如果认证或服务启动失败，也可以通过查询日志帮助排错。