NARI

DialKeeper-2000 安全拨号认证网关

服务器端配置手册

注意：

本文档中的内容是南瑞 DialKeeper-2000 安全拨号认证网关服务器端配置手册的内容。

南瑞安全拨号认证网关服务器端配置手册

Version2.1　2009-9-11

南瑞集团公司信息系统分公司

本资料将定期更新，如预获取最新相关信息，

请访问南瑞集团公司网站：http://www.nari-china.com

您的意见和建议请发送至：zhangtao@nari-china.com

南瑞集团公司信息系统分公司

南京南瑞路 8 号，210003

电话（TEL）:025-83096601(市场部)

025-83096702　025-83096715(技术支持)

传真（FAX）:025-83096701

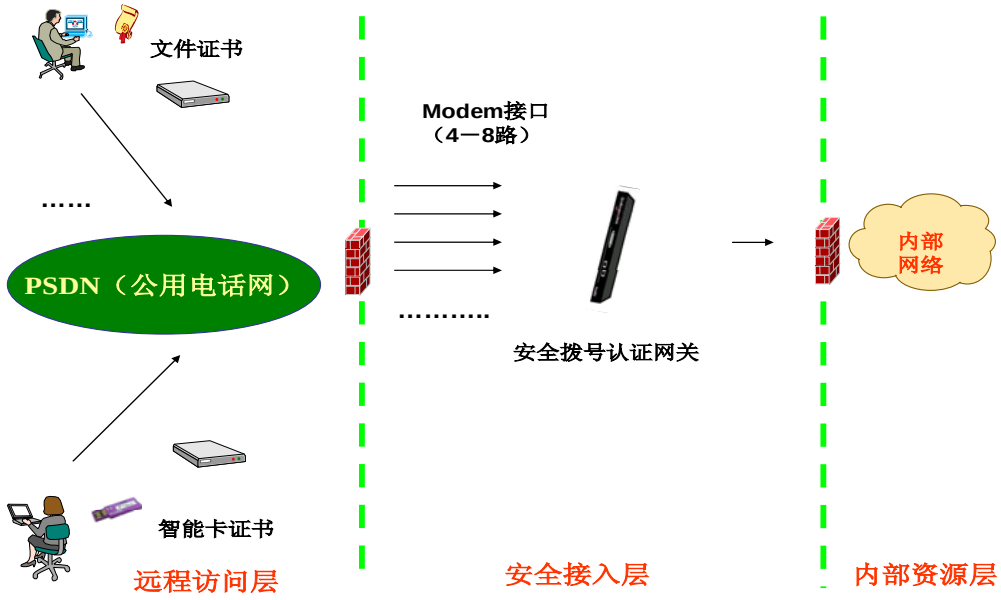
目录

图片索引

一、服务器配置环境与配置流程说明

1.1 服务器配置环境简介

DialKeeper-2000 安全拨号认证网关基于嵌入式操作系统开发，其在网络中的拓扑结构如下所示：



图表 1 安全拨号网关的部署位置

如上图所示，安全拨号认证网关处于内外网之间的关键路径上，对外提供拨号接口，用户使用数字证书，首先通过公用电话网拨号到此装置，然后通过此装置进行认证、授权，在权限范围内对电力内部网络进行相应的访问操作。

系统采用安全 web 进行相关的配置操作，用户可以通过配置计算机网卡为私有地址 1.2.3.0/24, 即可进行配置。（如配置地址为 1.2.3.3 ,掩码 255.255.255.0）

打开IE浏览器，访问 **https://1.2.3.4** ，并以默认用户名admin、密码 123456(可由管理员进行修改)进行登录。

1.2 快速配置导引

拨号网关的设置比较简单，一般配置流程如下（详细的设置请参见第二、三、四章的设置介绍）：

1.进入“系统”→ “日期设置”，检验是否当前系统时间正确，否则需进行正确地设置

2.进入“系统”→ “网卡配置”，按照实际的连接内网交换机需要，配置和启用 eth0-eth3 的网卡，**如果是基于跨 VLAN 环境访问，需要在路由配置页面中进行路由配置**。

3.进入“访问控制”→“内网资源”，设置欲访问的内网资源，一般可针对单台主机、某网段、特点端口或所有端口等进行设置，详细配置见2.2.1 内网资源配置

4.进入“访问控制”→ “用户组配置”，根据访问人员角色，如不同的维护厂家，新建不同的用户组

5.进入“访问控制”→ “用户配置”，新建访问人员的证书中 common name 名称，并和第 4 步的用户组关联

6.进入“证书管理”，删除原来预置的 Ca 证书及服务器证书，

7.参照第 5 步设置的证书人员名称，在第三方 Ca（如调度 Ca 系统或本光盘附带的第三方证书工具）中进行相应名称证书的签发，由第三方 Ca 签发 P12 服务器证书，并将第三方的 Ca 证书及 P12 服务器证书导入到系统中

8.客户端进行连接及证书设置，具体过程参见客户端配置手册文档，略。

二、服务器端配置界面功能介绍

2.1 系统

主要是针对服务器系统的一些基本配置信息的设置。

2.1.1 日期设置

对拨号网关的时间进行校核，一般本产品出厂前已经经过设置，用户只需要检查一下即可。界面如下图所示：

图表 2 系统-日期设置

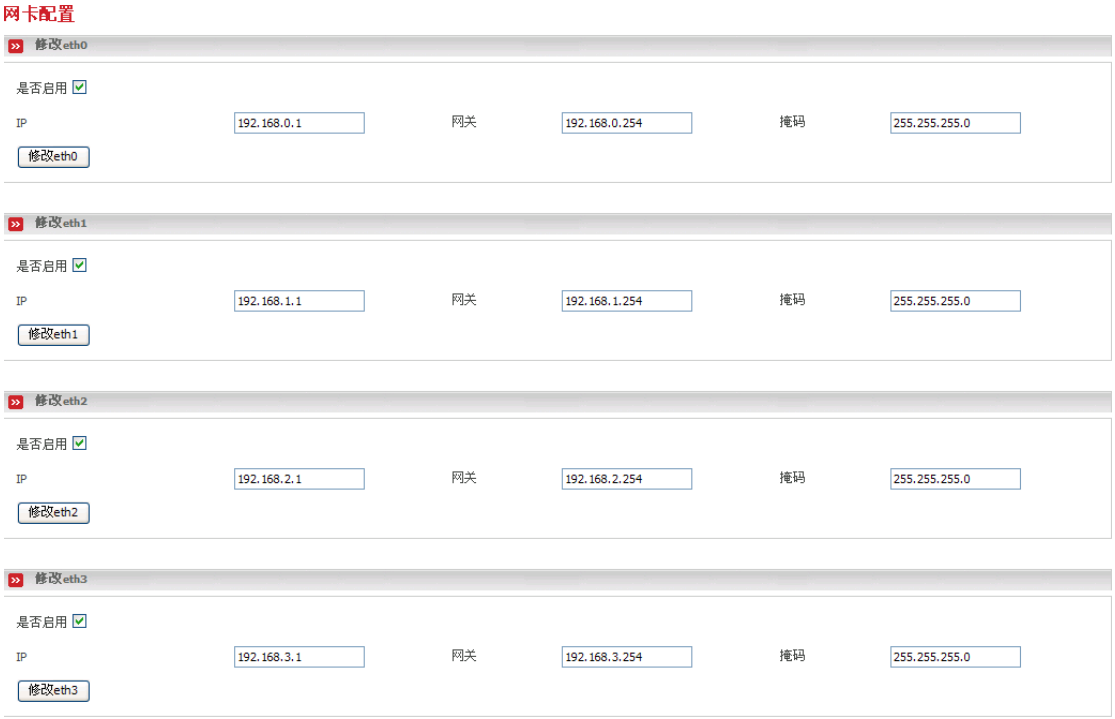
首先，界面上会显示默认的系统时间，如需进行调整，则对年、月、日等进行修改并点击保存按钮进行修改。

2.1.2 网卡配置

对拨号网关 IP 地址、掩码、网关进行设置并选择是否启用。本系统最多支持 4 个网卡，也就是内网支持 4 个不同网段，这对于交换机多 VLAN 的设置是很有用的。

如下图所示，填写地址后，选择“是否启用”按钮，点击“修改 ethx”按钮进行修改，

注意：每个网卡都需要单独点击设置。



图表 3 系统-网卡配置

2.1.3 路由表配置

需要访问的内网资源不和拨号装置几个网口不在同一网段是可以通过增加路由的方法来进行配置。

图表 4 系统-路由表配置

2.1.4 密码

修改安全 web 配置的管理员密码，用户名默认 admin 不变。

图表 5 系统-修改管理员密码

2.1.5 服务器 modem 测试

图表 6 服务器 modem 设置

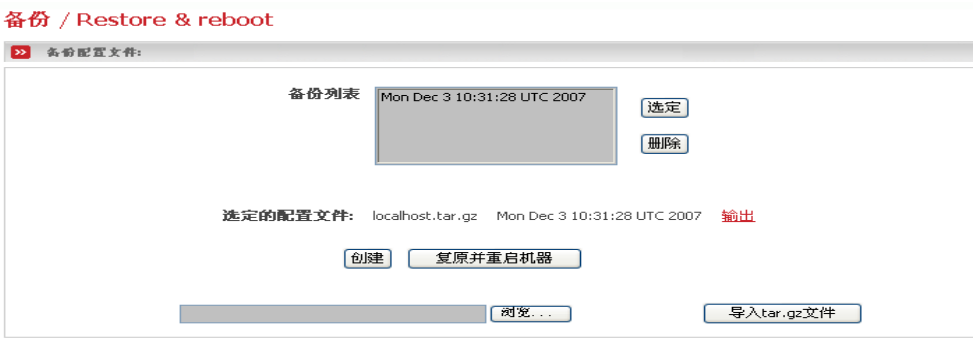
可以通过测试按钮诊断 modem 硬件的状态是否正常，注意，由于拨号网关具有多种型号，如 4 路 Modem / 8 路 Modem ，等，因此测试时应选择 0－3，0－7 等 Modem 序号进行测试。

注：每一路 modem 支持一个拨号连接。

2.1.6 备份

备份功能可以快速备份拨号网关的配置（可导出），并可以利用先前备份重新恢复系统以前的设置，还可以恢复到默认的出厂设置状态。

1、创建与导出备份包文件



图表 7 备份到文件功能

创建备份包：点击“创建”按钮后，系统将创建一个当前系统配置备份包文件（*.tar.gz），并且显示在“备份列表”窗口中。

导出备份包：在列表中选中以时间命名的备份包，然后点击“选定”，再点击“输出”即可把文件导出到您的机器。

2、导入备份包与恢复系统设置

1. 点击“浏览”选择之前备份到磁盘上的备份包文件(*.tar.gz。
2. 点击“导入.tar.gz” 按钮 (备份设置将会显示在Backup Set窗口中)。
3. 直接关闭、开启电源进行系统复位，恢复系统设置到指定的日期。

2.1.7 注销登录

如上图所示，点击注销按钮，即可注销本次配置登录，退出系统。

2.1.8 关机

图表 8 关机重启示意图

在本节您可以通过点击相应的按钮进行关机和重起拨号网关，或者直接关闭电源。

2.2 访问控制

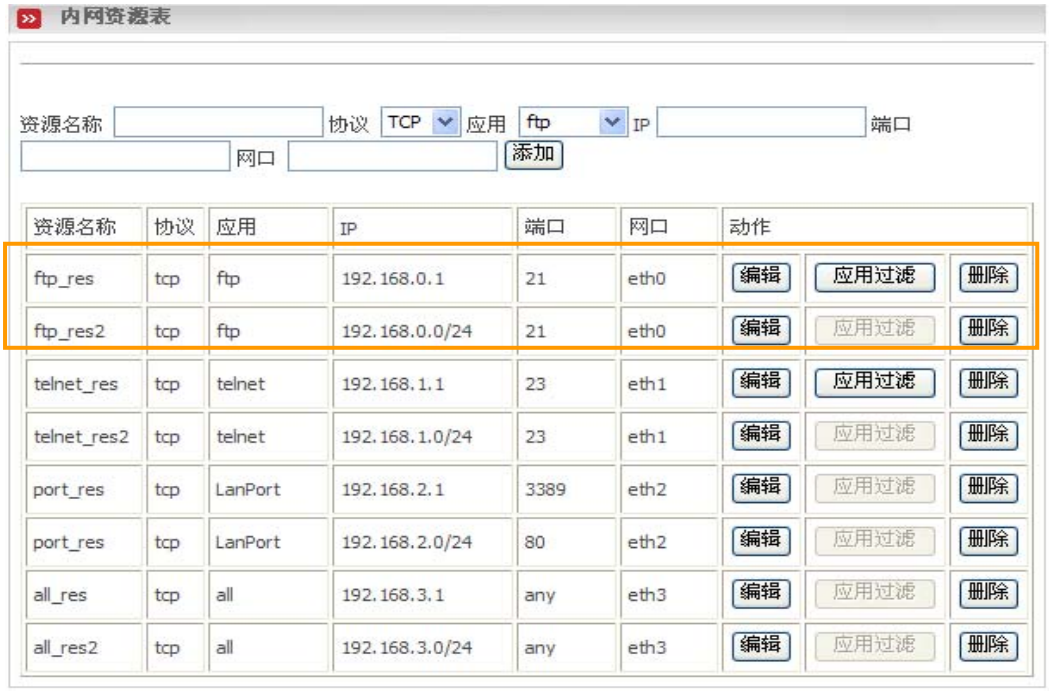
对用户可以访问的网络层资源和应用协议进行安全控制，按照内网资源设定、用户组配置、用户配置的顺序进行。

注意：添加的网络层资源是允许用户访问的内容，而添加的应用层资源过滤是禁止用户访问的内容。

2.2.1 内网资源设置

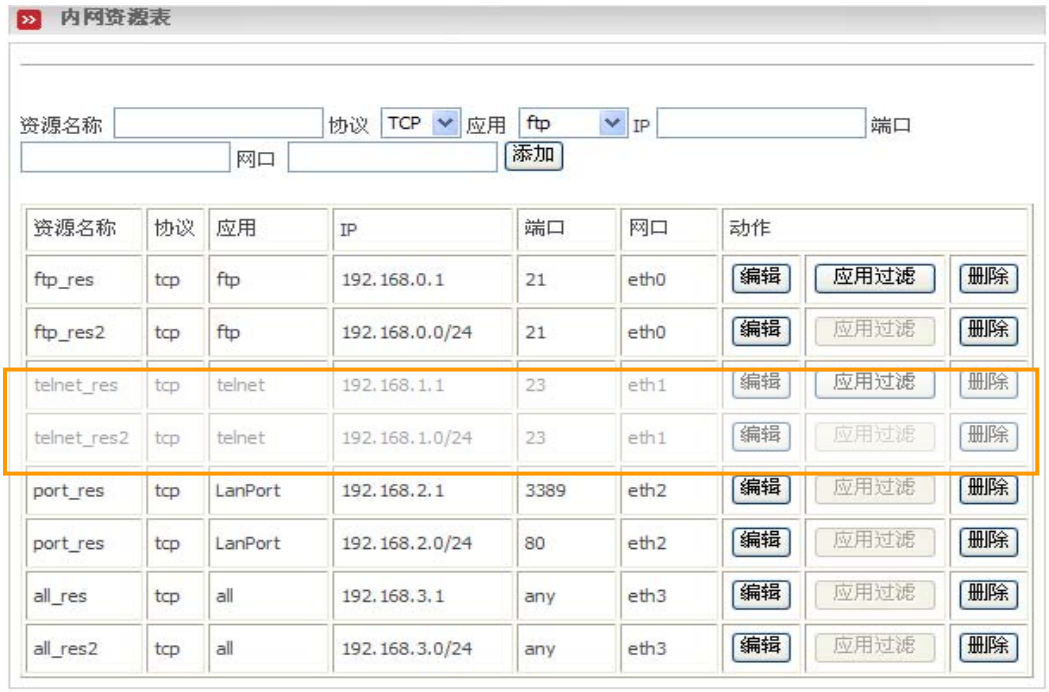
通过本页面可以进行内网资源属性的配置，可以针对某一台主机的资源设置（并同时设置应用过滤）、也可以针对某一个网段内的主机资源设置。内网资源设置可分为以下几种情况：

1. 单台主机或网段 ftp 服务，图表 9 中资源名称为 ftp_res, ftp_res2 两个资源



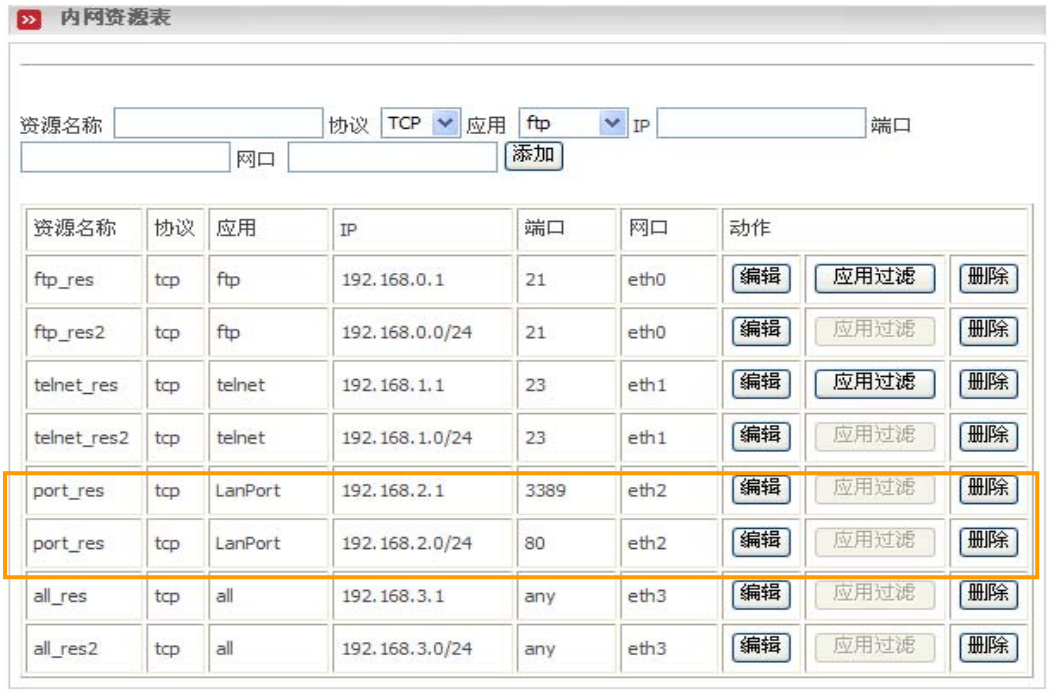
图表 9 单台主机或网段 ftp 服务

2. 单台主机或网段 telnet 服务，图表 100 中资源名称为 telnet_res, telnet_res2 两个资源



图表 10 单台主机或网段 telnet 服务

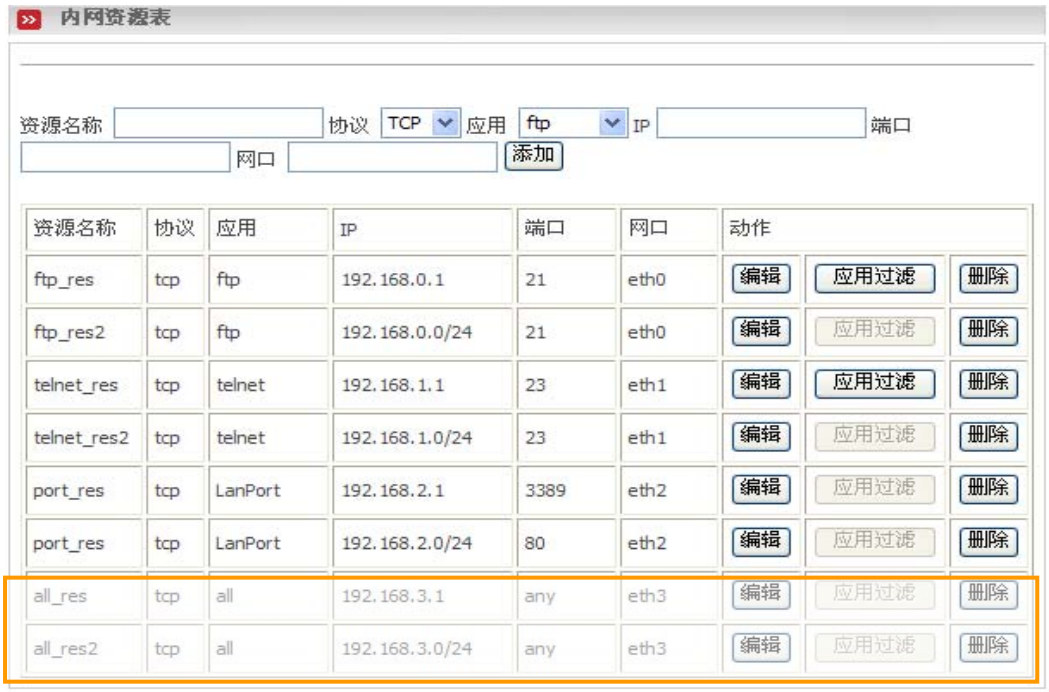
3. 单台主机或网段某个端口的应用，图表 11 中资源名称为 port_res, port_res 两个资源



图表 11 单台主机或网段某个端口的应用

4. 单台主机或网段所有端口应用，图表 12 中资源名称为 all_res, all_res2 两个资源

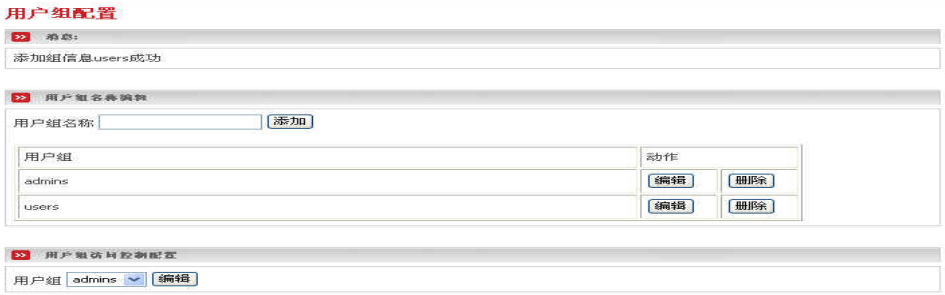
如下是针对如上情况的截图：



图表 12 内网资源设置

2.2.2 用户组及应用过滤配置

添加网络层资源后，还需要对系统的用户组进行设置，以对不同角色用户进行区分，如下图所示，增加了不同用户组。也可以根据实际需要增加 group1,group2,….等不同用户组来设置不同权限。

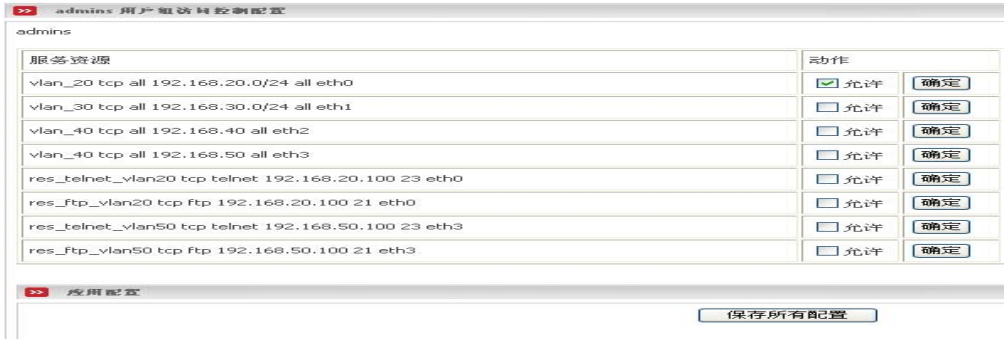


图表 133 用户组编辑

在 admin 用户组访问控制配置中，选择相应编辑的组然后点击“编辑”，即进入了对此用户组的配置，如下图：

图表 144 用户组访问控制配置

点击编辑后，这里会显示 2.4.1 中添加的内网资源规则，不同的用户组可以选择不同的内网资源，使其可以有权限通过此进行访问内网相应资源。一个组可以选定多条规则。



图表 155 用户组访问控制配置

勾选“允许”按钮，并点击“确定”和“保存所有配置”，保存设定的规则。

注意：每条资源都要分别进行点击进行确定！

此时，同时可以对应用过滤信息进行配置，点击“内网资源”页面，选中相应条目的“应用过滤”进行编辑:

图表 166 应用过滤资源配置

如上图所示，我们添加了一条针对 users 用户组的应用过滤，使此用户组用户在 telnet 192.168.0.8 服务器时，禁止其执行“kill process1”的命令，也就是不允许其杀死进程 process1，以保护系统。

2.2.3 用户配置及属性察看

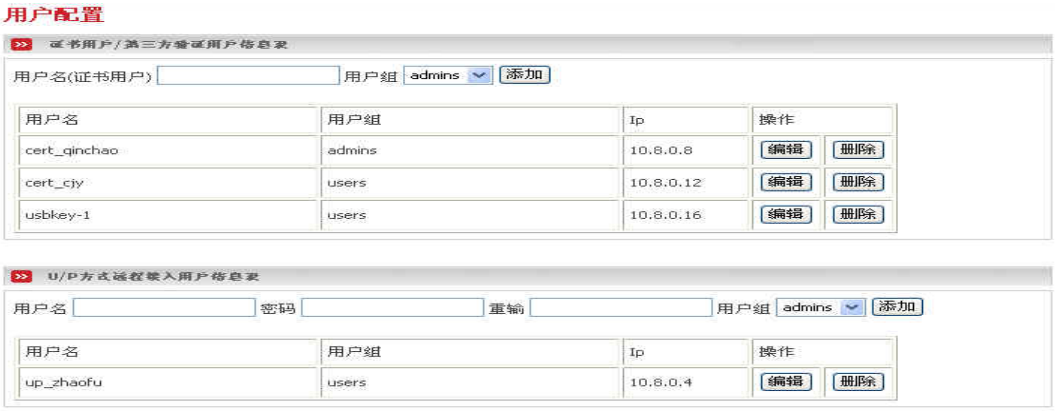
对用户的属性进行配置，目前主要有两类用户：

1. 证书验证用户：指由第三方 CA 签发的证书用户，包括采用 P12 文件证书的用户，也包括采用智能卡验证的证书用户。此时服务器证书也由第三方 CA 签发（详见“安全接入”

→“证书管理”中证书生成的有关内容)。

注意：此用户名称和用户数字证书中的 common name 相同，因此在申请证书时务必注意保持该名称的一致性。

2. 用户名口令验证用户：即配置页面上的 U/P（Username/Password）方式。同时，客户端配置时选择“用户名口令”方式进行认证。



图表 177 用户属性配置

设置或添加用户就可以将用户和特定的角色用户组关联。

选择用户名称，并点击确定按钮，进行用户访问控制信息（网络层和应用层）的查看。如下图所示：

图表 188 查看用户属性

2.2.4 远程登陆控制

图表 19 远程登陆控制

此功能是分配给拨号网关厂家进行远程维护装置用，默认为关闭状态，须由管理员配置启用后生效。

2.3 安全接入

安全接入提供了接入状态显示及证书管理功能，如下所示：

2.3.1 接入状态显示

图表 190 接入服务配置

当用户连接上后，可以看到用户的连接状态，如上图所示，包括用户名称、分配虚拟 IP，真实 IP，流量信息，连接建立初始时间，连接时间等等。

2.3.2 证书管理

使用数字证书对系统进行设置，支持第三方 CA 功能（使用本系统光盘中自带的“证书工具”软件或使用南瑞信息公司的调度证书系统进行证书签发）。

图表 201 选择第三方 CA

注：“证书工具”软件使用参见附录 1 第三方 CA 工具证书签发说明，南瑞信息公司调度证书系统使用参见有关的用户手册和文档。

步骤 1：删除旧证书

点击 CA 证书及服务器证书后的“垃圾桶”图标，进行装置出厂时预置旧证书的删除。

步骤 2：导入服务器 pfx 证书

安全拨号网关支持 PKCS#12 格式的 pfx 证书直接导入，请参考附录中的“第三方 CA 工具使用”中关于 p12-server 证书生成的有关内容；如果是调度 CA,则直接生成类型为“程序证书”的 pfx 证书即可。

如下图所示，点击浏览，选择对应的 pfx 证书，并输入证书的保护口令，然后点击“上传 PKCS#12 证书”按钮，进行证书上传。

图表 212 由外界导入拨号网关服务器证书

这种方式和拨号网关自己生成证书只要选择一种就可以了，一般推荐后一种方式。

步骤 3：导入系统根证书

将证书工具生成的根证书或者南瑞调度证书系统的根证书导入到拨号网关内，方法和步骤 2 类似，点击“证书管理”菜单，然后点击右下方的“浏览”按钮，选定服务器证书，然后点击“上传 CA 证书”按钮，便完成了所有操作。

注：多级根证书的使用参见附录 3 的有关说明。

2.3.3 客户端安全检查配置

通过客户端安全检查配置，可以对待接入客户端的接入标准进行设置，只有符合安全要求的客户端才允许进行接入，以便更好的保护内网系统的安全，防止网络攻击和病毒的侵害。

注：如有特殊需要，可选择旁路功能，暂不进行客户端接入检测，让用户顺利接入，如下图所示：

图表 223 客户端安全检查配置-旁路功能

1、客户端安全检查配置

选择检查范围，目前本系统提供了系统版本、防火墙、杀毒软件三种检查模式，可以根据不同的安全要求和角度进行设定。这里至少要选择一种方式，选择后点击“确定”进行保存。

图表 234 客户端安全检查-检查范围设置

2、客户端操作系统版本号

提供了三个版本的接入，若在客户端安全检查配置中设定了要检查客户端操作系统版本，那么在这里要选择上至少一种，只有在这里选择的操作系统版本才能够接入。

图表 245 客户端安全检查-操作系统类型设置

3、客户端防火墙

提供了五种防火墙的接入，若在客户端安全检查配置中设定了要检查客户端防火墙，那么在这里要选择上至少一种，只有客户端那里安装了在这里选择的防火墙才能够接入。

图表 256 客户端安全检查-客户端防火墙设置

4、客户端反病毒软件

提供了六种杀毒软件的接入，若在客户端安全检查配置中设定了要检查客户端杀毒软件，那么在这里要选择上至少一种，只有客户端那里安装了在这里选择的杀毒软件才能够接入。

图表 27 客户端杀毒软件设置

2.4 日志

DK2000 服务器系统提供了完备的系统审计日志查询，服务器管理员可以通过这些日志方便的查看系统运行的状况，帮助解决出现的问题。主要有安全接入日志、系统日志 TELNET 审计日志、FTP 审计日志、日志设置。

2.4.1 功能介绍

安全接入日志指针对用户的接入行为，记录的详细日志信息。系统日志包含了系统所有的进程启动，停止，拨号服务信息等日志。telnet 和 ftp 的审计日志对用户的接入行为尤其是非法的操作进行了详细审计。

通过分别点击日志菜单中的各子菜单，可以查看各模块的安全日志信息。如下为安全接入日志信息：

时间戳	日志类型	日志有效信息
Wed Nov 7 19:01:53 2007	通信信息	验证证书成功: depth=1, /C=86/ST=JS/L=NanJing/O=nari/OU=nari-info/CN=dk2000-ca/emailAddress=dk2000-ca@nari-china.com
Wed Nov 7 19:01:53 2007	通信信息	验证证书成功: depth=0, /C=86/ST=js/L=nanjing/O=nari-info/OU=nari/CN=cert_zhangsan/emailAddress=cert_zhangsan@nari-china.com
Wed Nov 7 19:04:18 2007	人员操作	用户: cert_zhangsan 退出系统登陆
Wed Nov 7 19:04:18 2007	人员操作	用户: cert_zhangsan 退出系统登陆
Wed Nov 7 19:04:18 2007	人员操作	用户: cert_zhangsan 退出系统登陆
Wed Nov 7 19:06:34 2007	通信信息	验证证书成功: depth=1, /C=86/ST=JS/L=NanJing/O=nari/OU=nari-info/CN=dk2000-ca/emailAddress=dk2000-ca@nari-china.com

图表 28 日志信息察看

2.4.2 日志设置

进入 web 的“日志/日志设置”就是如下图 2.64 界面，日志设置提供了对日志显示方式、远端日志等功能的置。下面对界面中各个功能进行介绍。

1、 日志查看选项

含有两项，其中

每页显示行数，指定 web 中每行显示多少行日志（日志文件中每行日志记录一个事件）。

反序事件输出，选上此选项后每页日志将从上到下依次显示，时间上最近的发生的日志、时间上较前发生的日志…，不选择此项将相反。

2、 远端日志：可以将 DialKeeper2000 服务器端的日志记录在远程计算机上，选择启用后，需要提供远端计算机的名称或者 IP 地址。

附：远程日志服务器的配置

假设有一台机器专门用来做为日志服务器，那么 DialKeeper 相对来说就是日志客户机，这样在 DialKeeper 这一端（客户机）设置了远程日志后，还需要在日志服务器端进行相应的设置。若日志服务器是 Windows 操作系统的话需要安装专门的日志接受软件；若日志服务器安装的是 linux 操作系统，则可以通过相应的配置使其做为日志服务器，专门用来记录日志，配置过程如下：

- 编辑服务器的日志配置文件/etc/syslogd.conf，添加如下一行：

  *.info /var/log/everyinfo

  其中/var/log/everyinfo 为日志存放文件，可以根据您的需要进行更改。

- 编辑服务器的/etc/sysconfig/syslog，把 SYSLOGD_OPTIONS 的值加上-r，变成"-r -m 0"，然后重起 syslog：/etc/rc.d/init.d/syslog restart

- 确认 syslog 开起 514/udp(通过如下命令查看)

  # cat /etc/services |grep syslog

  正确显示应该是：

  syslog 514/udp

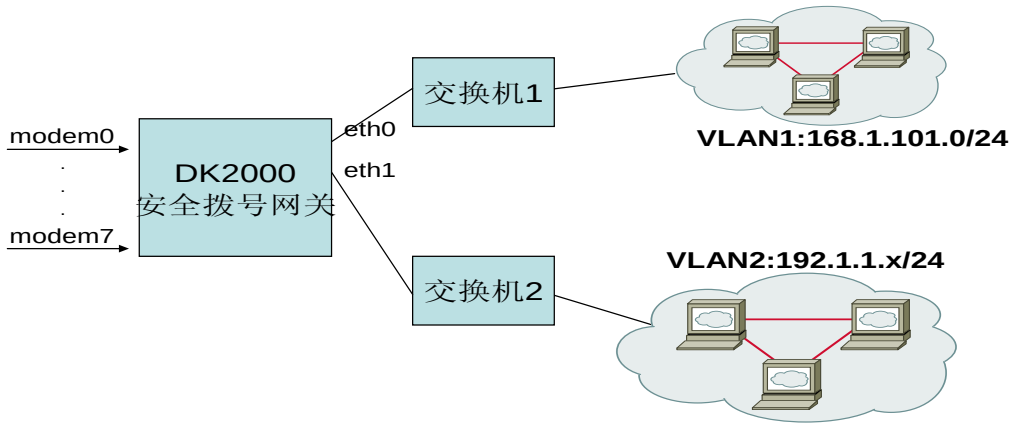
图表 29 日志设置功能

三、服务器端典型设置介绍

本章将结合一个典型的使用样例（二个内网网段的情况），进行详尽的说明。

3.1 典型网络拓扑结构

某电力公司的实时系统外网拨号出口部署了 DialKeeper-2000 网关，其网络拓扑结构图如下所示：



图表 3026 典型设置一网络拓扑结构

内网有两个 vlan 中的机器需要通过拨号网关进行安全访问，两个 vlan 的网段分别是 168.1.101.0/24、192.1.1.x/24（在本说明中分别被称为 1 号区、2 号区），在这两个网段内部都提供 telnet 服务，客户要用到这些服务。

3.2 应用环境访问权限

管理员希望将系统用户分成两个组：Admins（超级用户组）和 Users（普通用户组）。有两个用户，分别名称为 cert_zhangsan, up_lisi,分别属于 Admins 和 Users,并准备对他们分别进行证书验证和用户名口令验证。

访问控制权限分配如下：

1. Admins 用户组可以访问 1 号区的所有 telnet 服务，不能访问 2 号区。
2. Users 用户组不能访问 1 号区，只能访问 2 号区的 telnet 服务。

用户	用户组	可访问网络层资源	备注

cert_zhangsan	admins	1 号区	采用证书验证
up_lisI	users	2 号区	采用用户名口令验证

图表 31 典型设置－用户访问权限一览表

3.3 详细配置过程介绍

下面结合具体的配置界面等进行详细配置过程介绍。

步骤 1：准备配置

从包装盒中打开拨号号网关，接上电源开机，并等待片刻至系统启动完毕。

将配置用计算机 IP 地址设置为 1.2.3.100, 掩码 255.255.255.0, 并用交叉网线连接拨号网关的 eth0 网口，ping 1.2.3.4 ,如果能 ping 通，则可以进行后续配置，否则检查网线。

步骤 2：进入系统，进行系统初始设置

1.输入https://1.2.3.4 ，打开默认安全web页面进行初始配置，输入admin,123456 登陆系统。

2.进入系统->日期设置，如有需要，进行校准系统日期时间，并保存。

3.进入系统->网卡设置，分别设置 eth0 ,eth1 地址并和 vlan1,vlan2 处于同一网段中，168.1.101.100、192.1.1.100，掩码都是 255.255.255.0,并分别勾选启用框进行网卡启用。

4.进入系统->密码设置，增加一个拨号用户名，如 nariuser, 密码 xxxxx。

5.进入系统->服务器 modem 设置，设置系统 modem 个数为 4 个。

步骤 3：进行系统访问控制设置

1. 进入访问控制->内网资源菜单，添加两个资源,各字段属性如下：

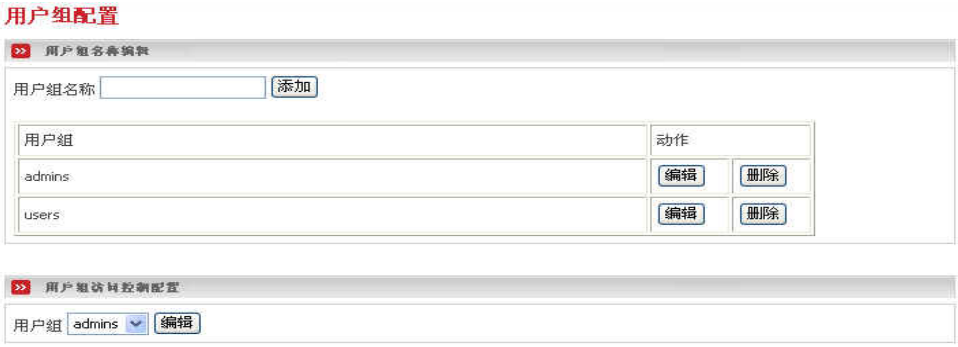
资源名称 test1 协议： tcp 应用 all IP：168.1.101.0/24 端口 ：23 网口：eth0

资源名称 test2 协议： tcp 应用 all IP：192.1.1.0/24 端口 ：23 网口：eth1

如下所示：

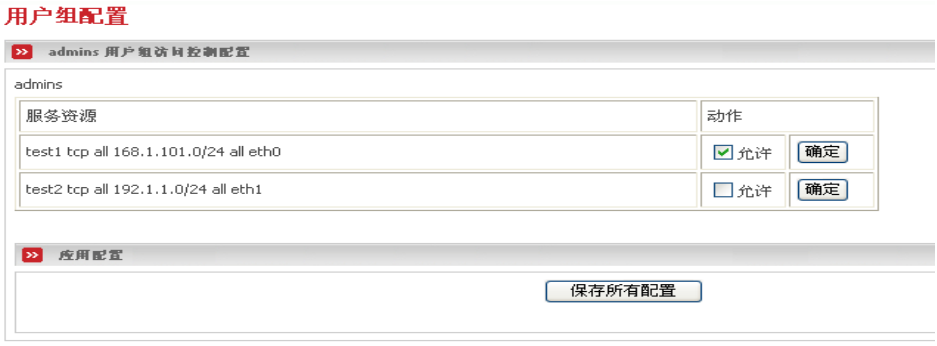
图表 272 典型设置－内网资源设置

2. 进入访问控制->用户组配置，添加用户组 admins 和 users。选中下拉框中的用户组 admins，并点击“编辑”按钮：



图表 283 典型设置－编辑用户组访问控制 1

进入如下选择界面：



图表 294 典型设置－编辑用户组访问控制 2

勾选相应的资源，并点击确定，最后点击“保存所有配置”，为 admins 用户组设置两条访问控制规则：test1

同样，回到用户组配置页面，选中下拉框中的 users 用户，然后，勾选对应于 test2 的那条访问控制规则。

注意：每次退出前都必须点击“保存所有配置”按钮进行规则的保存。

3. 进入访问控制->用户配置，进行用户的配置， 首先进行证书用户“cert_zhangsan”的添加,添加到 admins 用户组：

图表 305 典型设置－添加证书用户

然后，进行 U/P 方式验证的用户 up_lisi 验证，创建到 users 用户组：

图表 316 典型设置－添加 U/P 用户

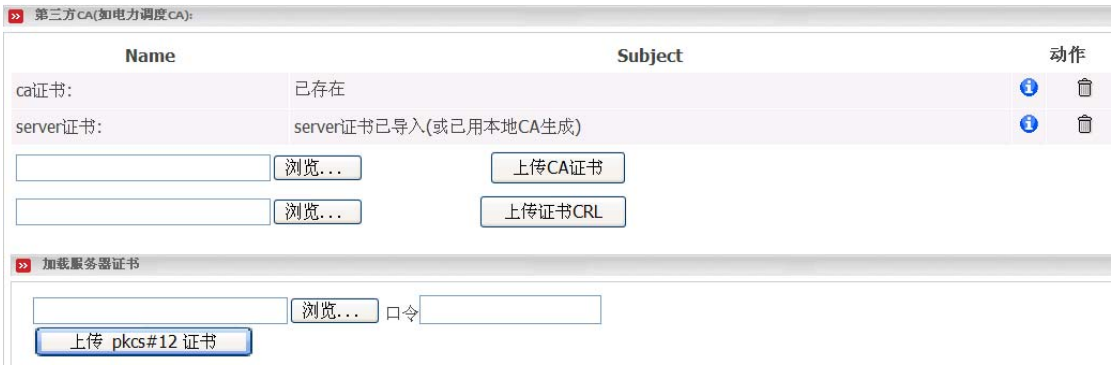
可以进入访问控制->用户配置中的下半部界面核对用户的访问控制规则

图表 327 典型设置－检查设置 1

步骤 4：进行安全接入设置

1. 进入安全接入->证书管理，选择第三方 CA，点击确定。

注：由于服务器出厂时预置了临时 CA 证书和服务器证书，因此，分别点击删除按钮（垃圾桶按钮）进行删除



图表 338 典型设置－证书配置

然后，点击界面上的“生成证书请求”按钮进行服务器证书请求生成，将生成的文件改名成 newreq.pem 并提交到证书工具中签发成服务器证书，然后，再通过界面上的“上传 server 证书”按钮导入服务器证书。再点击“上传 CA 证书”按钮导入 CA 证书。（证书生成详见附录 1、2、3）。

附录

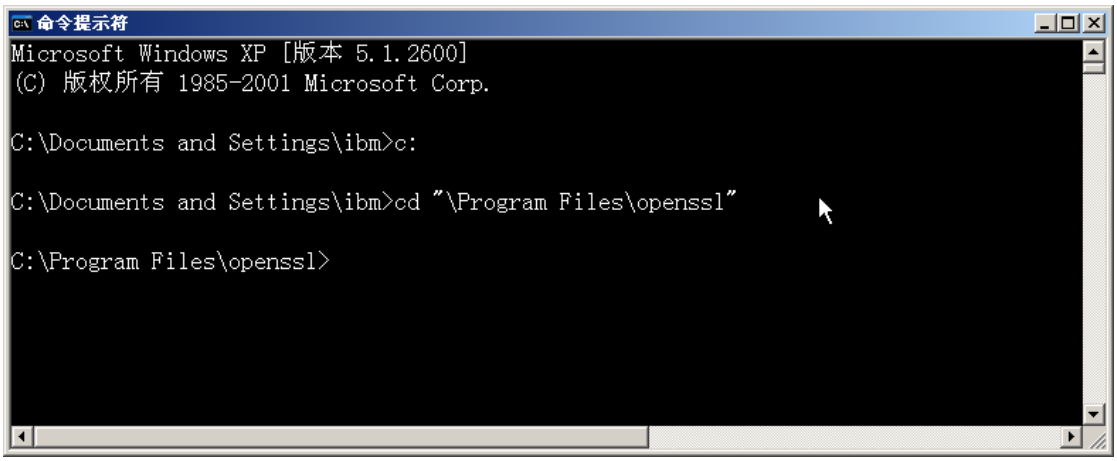
附录 1：第三方 CA 工具使用说明

注：这里仅介绍配套光盘中的命令行证书工具的使用，南瑞信息调度证书系统的使用参见有关使用手册及说明书，这里不再赘述。

1） 小型证书系统的建立

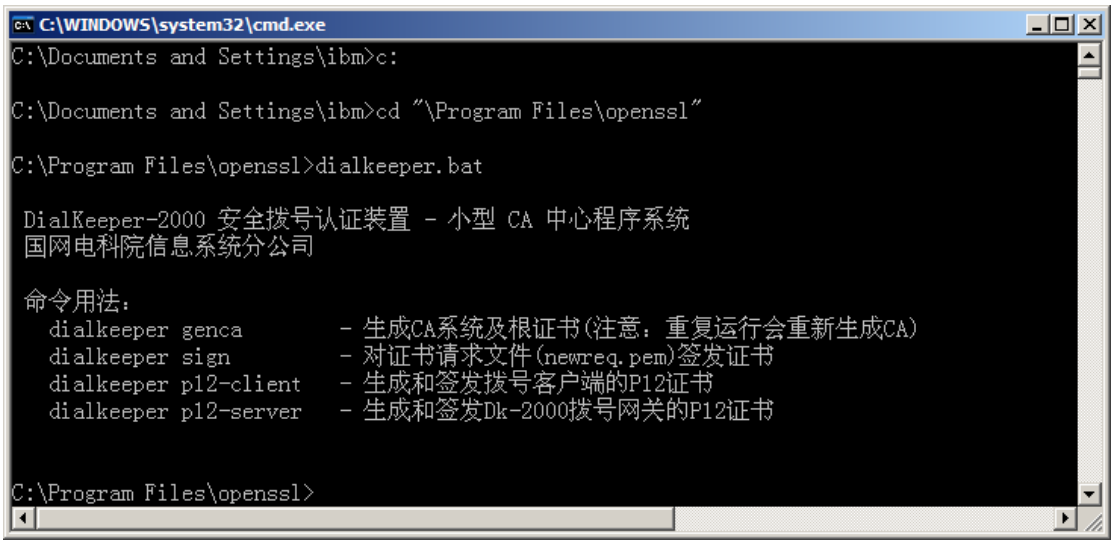
安全拨号网关和拨号客户端都需要申请证书并在通讯时进行相互认证，为使用户使用方便，拨号网关光盘中自带了小型证书系统工具进行各种证书的生成。

1. 将拨号认证网关中证书工具目录下的 openssl 目录复制到 C:\Program Files 目录下；
2. 启动 windows 系统自带的命令行终端（DOS 界面）；
3. 进入在第 1 步操作中复制的目录，即证书系统的主目录中，命令如下图所示：



图表 3934 进入证书工具主目录

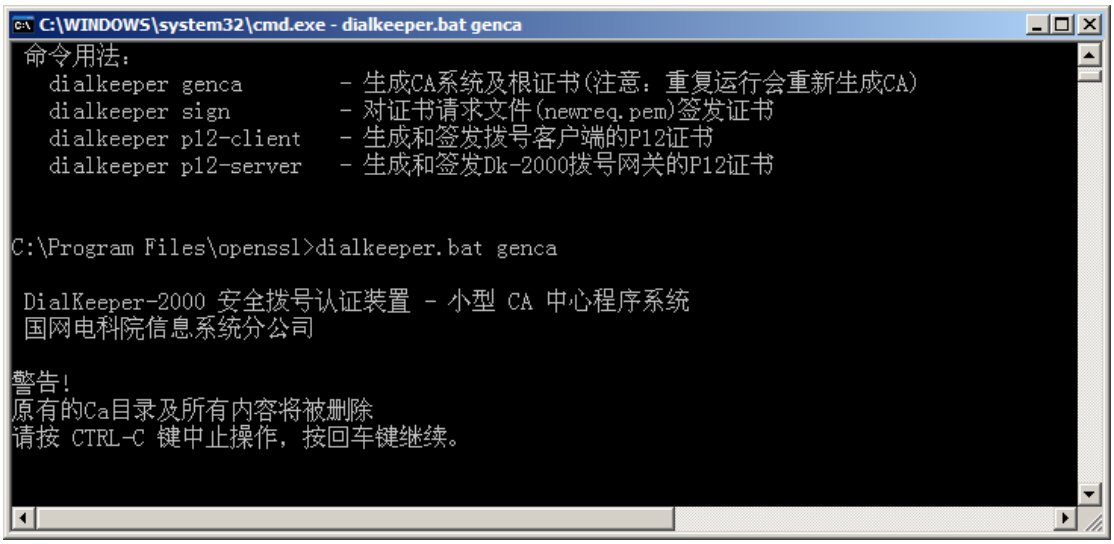
4. 不带参数运行证书工具命令，结果如下图所示：



图表 350 不带参数运行证书工具时输出的提示信息

从这里可以看到证书工具所能进行的操作都有哪些。其中第一个就是我们每次要建立一个全新的证书系统时要做的操作，也是我们接下来要做的。

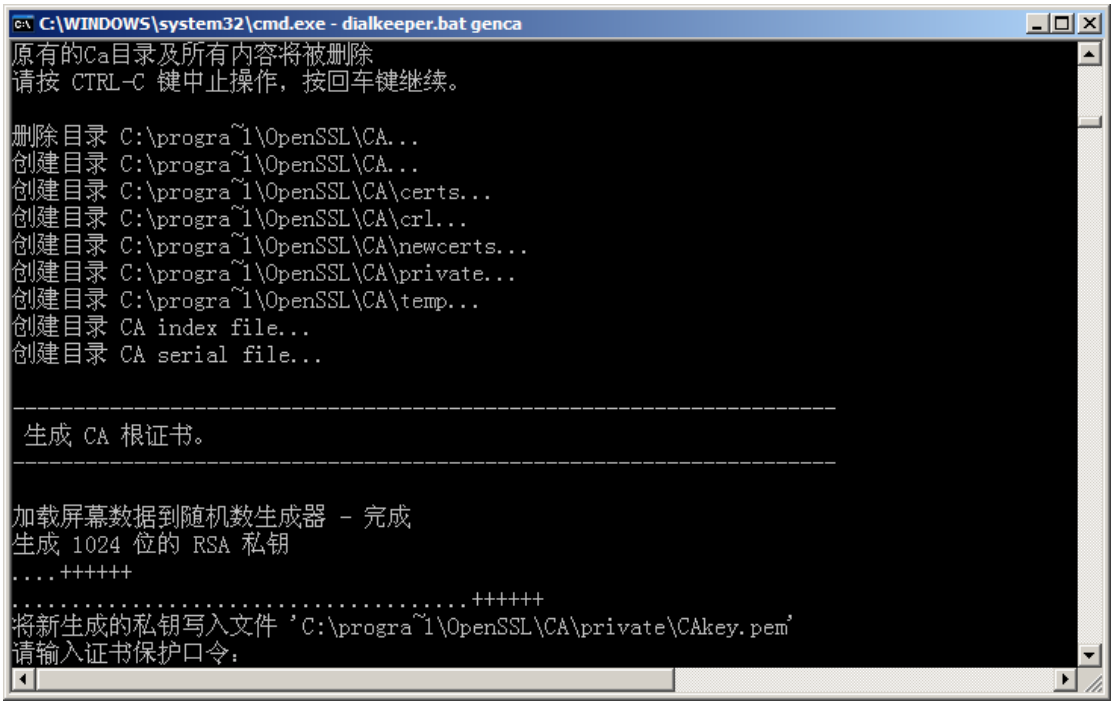
5. 执行 dialkeeper.bat genca 命令，开始初始化证书系统及签发 CA 根证书：



图表 361 执行 dialkeeper.bat genca 命令

根据提示，若你想取消该操作，只需要按下 Ctrl-C 键就可以了。

6. 按回车键继续（原有的证书系统内容将会被覆盖）：



图表 372 证书系统初始化过程及提示输入保护口令

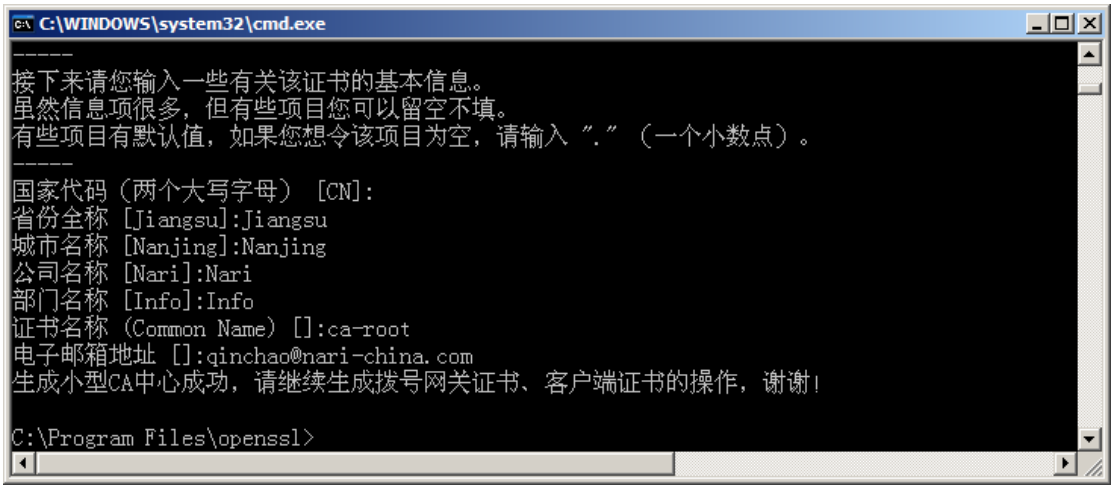
7. 这时该工具将自动建立一个新的证书系统结构，并生成 CA 根证书。之后就会提示我们输入一个 CA 根证书的保护口令。

注意：该保护口令很重要，它是我们以后用该证书系统做签发证书操作时所必需的，请务必妥善保管。

输入一个保护口令（如 123456），重复输入一次以确认，并回车：

图表 383 输入证书系统保护口令并确认之后

8. 从这里开始我们要输入一些签发 CA 根证书所需要的基本信息：



图表 394 输入 CA 根证书基本信息，完成证书系统的建立

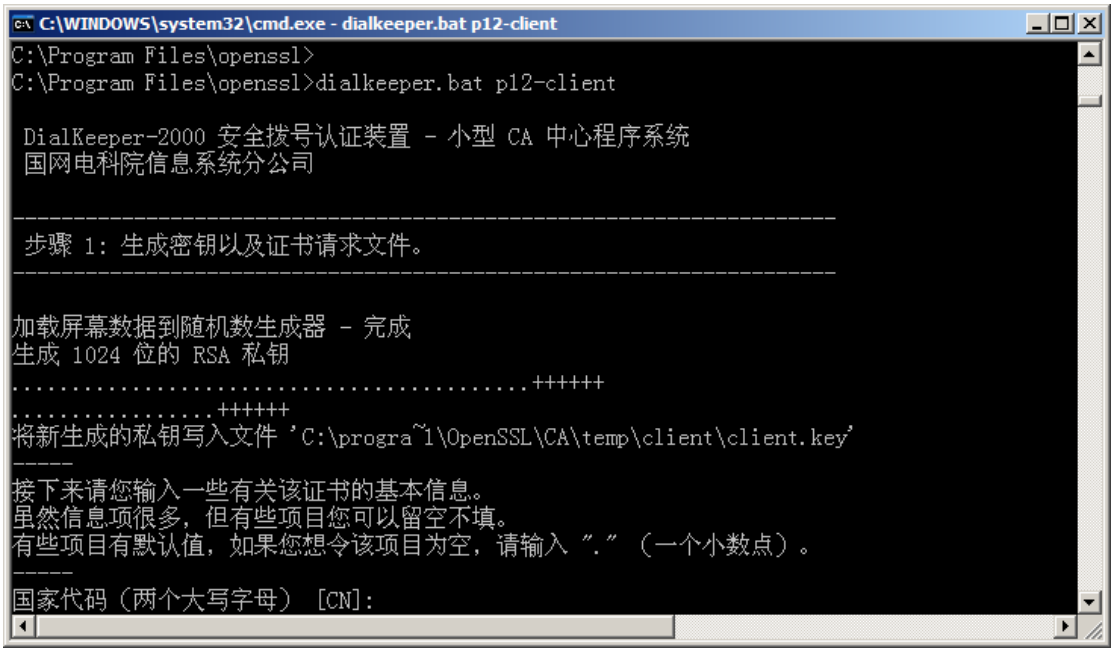
这些基本信息从前到后依次为：国家代码（CN 代表中国）、省份名称、城市名称、公司名称、部门名称、证书名称（Common Name）、电子邮件地址。在冒号之前的方括号中的字符串为该项的默认值。

这些基本信息都是可选的，不填也可以，但只有一项，即证书名称是必填项。同时要注意，证书名称被用来唯一标识一个证书系统中所签发的证书，所以在同一个证书系统中，一个证书名称只能对应唯一的一个证书（包括 CA 根证书，即我们在这步操作中所签发的证书）。

完成上述操作之后，我们就建立起了一个全新的证书系统。需要说明一下的是，CA 根证书的存放位置为当前目录下的 CA 子目录中，其中，CAcert.pem 为 CA 证书文件，private\CAkey.pem 为经过口令加密保护的 CA 公私钥对，保护口令即为我们在做上述操作的过程中所输入的口令。

2）签发客户端证书

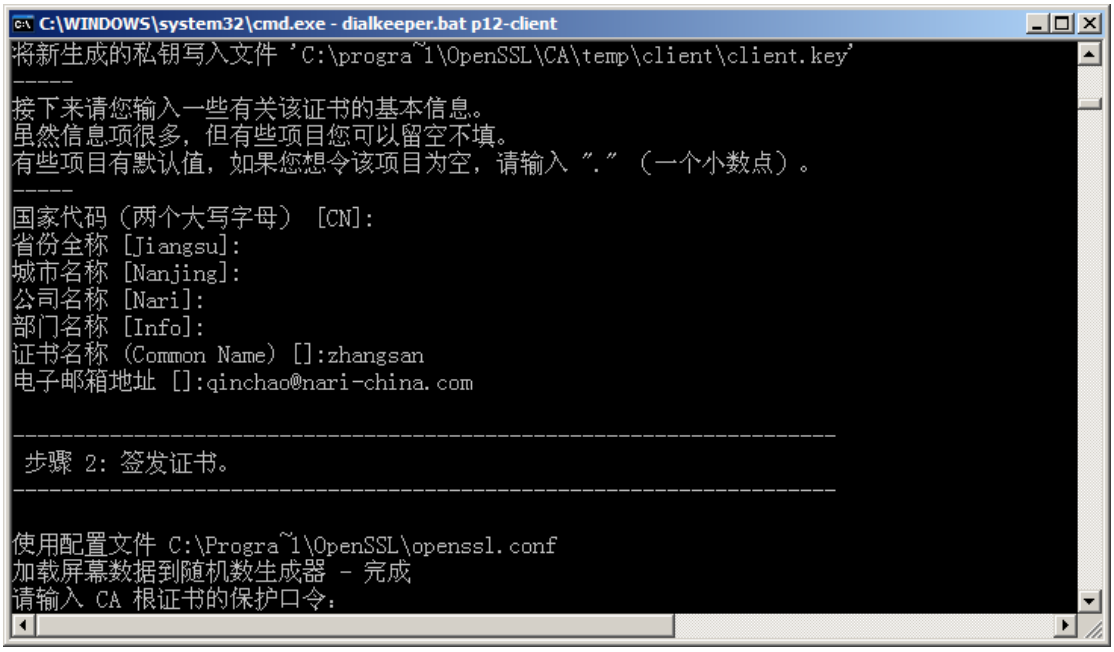
1. 进入证书工具主目录（具体做法参见上文），并执行命令 dialkeeper.bat p12-client：



图表 405 执行命令 dialkeeper.bat p12-client 以签发客户端证书

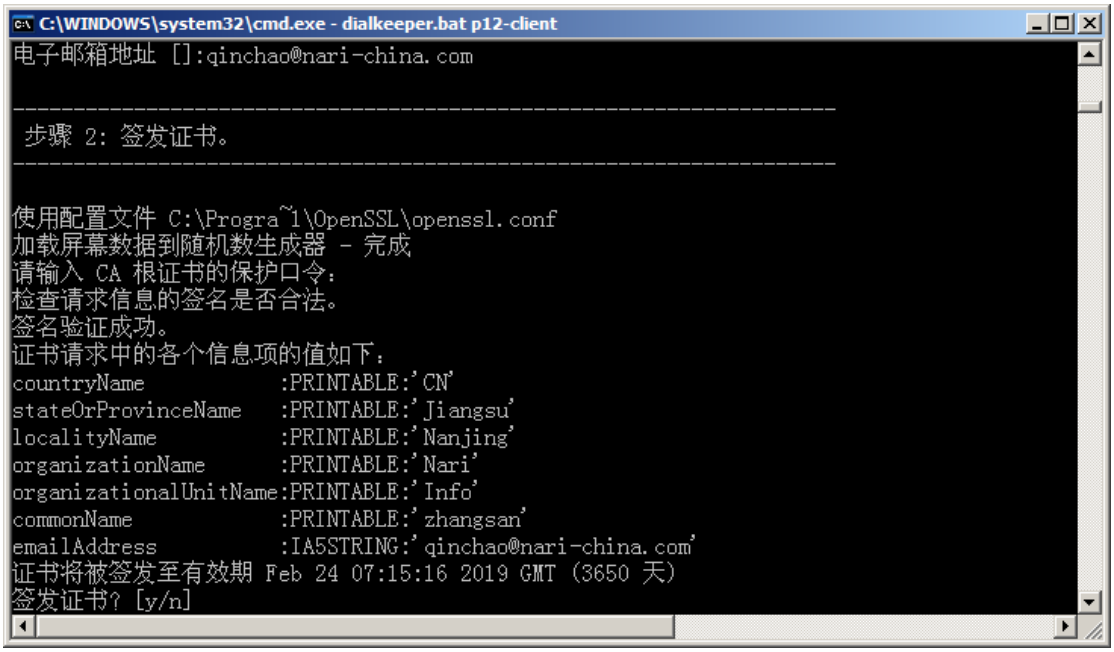
注意，生成的客户端证书会被放在当前目录下的 CA\temp\client 目录中。如果该目录中有之前生成的其他客户端证书的话，证书工具会提示你有已证书文件存在。当你确保已经备份过之前生成的证书文件之后，按回车键即可进行接下来的操作。

2. 接下来要输入客户端证书的基本信息。所需要的信息跟初始化证书系统、签发根证书时所需信息相同，如下图：



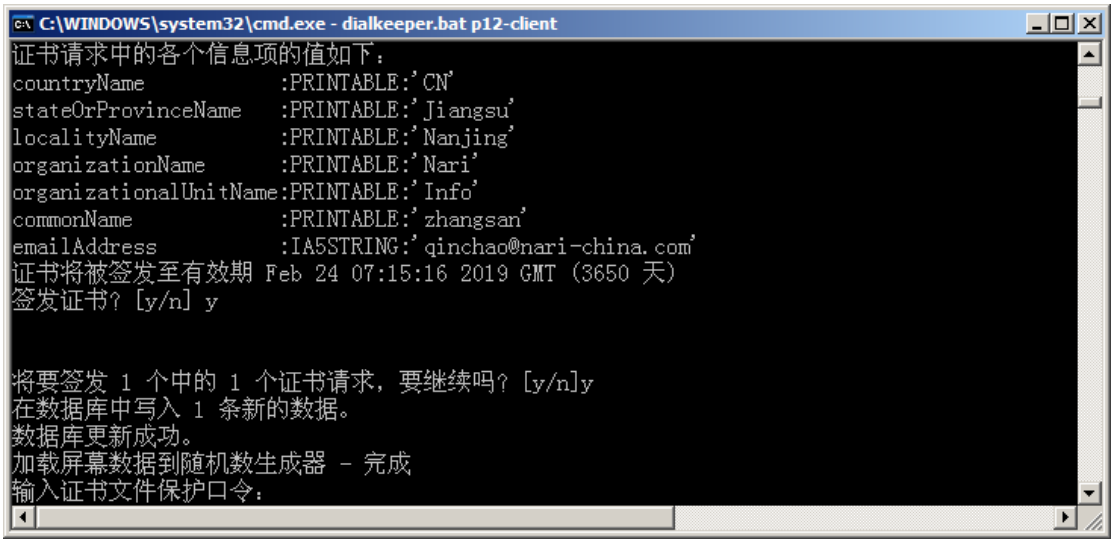
图表 416 输入客户端证书的基本信息

3. 这时，为了对客户端证书进行签发，就需要你输入证书系统的保护口令了。将证书系统初始化时所设置的保护口令输入进去，并按回车键，进入下一步：



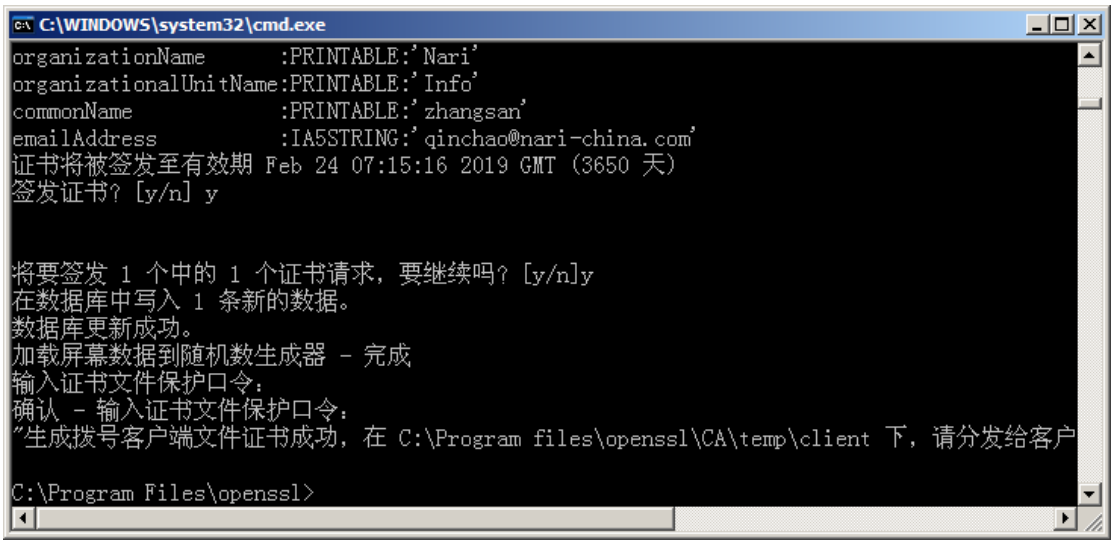
图表 427 确认之前输入的客户端证书基本信息

4. 当你确认完之前所输入的基本信息之后，即可连续输入两次 y 加回车键：



图表 438 确认提交证书签发请求

5. 这时，系统提示你输入该客户端证书的保护口令。这个口令即是用来保护当前正在签发的客户端证书的。请输入口令两次以确认：



图表 49 输入客户端证书保护口令

至此，我们就完成了一个客户端证书的签发工作。新签发出来的证书文件保存在当前目录下的 CA\temp\client 目录中，文件名为 client.pfx。请注意将该证书文件备份到 openssl 目录之外的其他地方，以免下次签发新的客户端证书时将该证书文件覆盖掉。

3）签发服务器证书

签发服务器证书的方法与签发客户端证书的方法非常相似，不同之处只有两点：

1. 要签发服务器证书，请使用命令 dialkeeper.bat p12-server;
2. 签发生成的服务器证书文件会存放在 CA\temp\server 子目录中。

4）使用该证书工具须注意的几点内容：

1. dialkeeper ca 命令用于 CA 的生成，因此，如果重复执行该命令，将清除以前生成的 CA 文件（并使以前颁发的证书失效）。
2. 由该证书工具生成的同一个证书系统中的所有证书都要有一个唯一的证书名，即 Common Name。

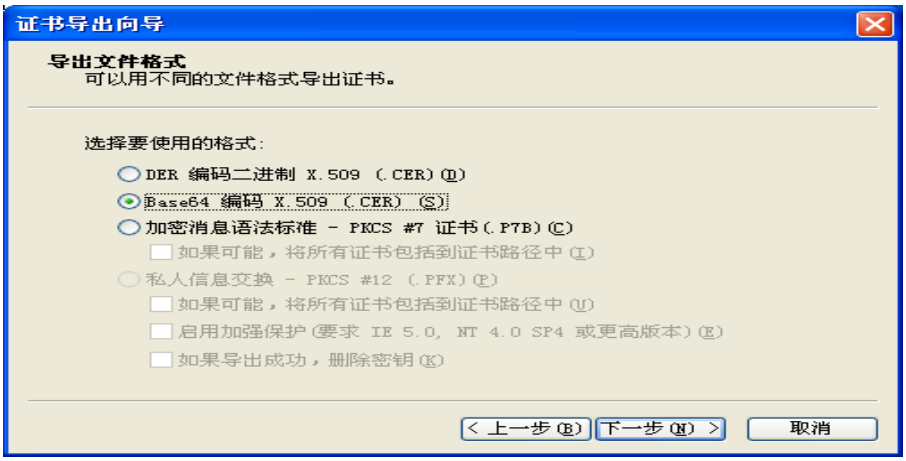
附录 2：证书格式转换说明

拨号网关的安全接入→ 证书管理中需要导入 server 证书和 CA 证书到网关内,目前默认证书必须为 PEM 格式(属于文本格式)，如下所示:

若证书是二进制格式的(如 DER 格式)，可采用如下方法将其导出 PEM 格式.

首先，在 Windows 下双击证书文件，点击“复制到文件”，会出现图 2.49 所示窗口。

选择 Base64 编码格式，再点击下一步

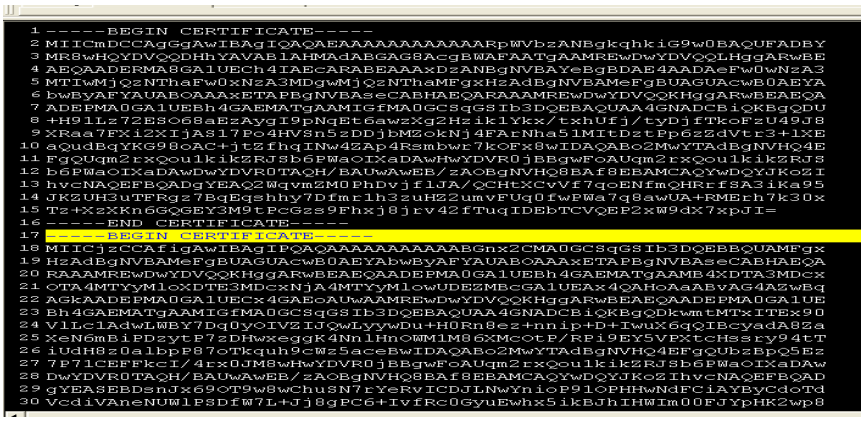


指定路径和文件名，并保存,然后使用此文件进行 CA 证书或服务器证书的导入。

附录 3：多级根证书使用说明

如果是多级 CA 的环境，那么在导入 CA 证书的时候需要进行适当的转换。

方法是在 Windows 下将两个根证书合成（合成前确定都是文本格式，否则要进行转换，见上所示），合成办法是在 UltraEdit 等工具中把两个证书文件内容，按照先从上级到下级 CA 证书的次序复制到同一个文件中。见下图 2.52，这里假设国调和江苏省调两级，那么黄色一行以上是国调根证书的内容，黄色一行（包括这一行）以下是江苏省调根证书内容。



确定好以上两点没有问题的话，就可以通过点击“浏览”选定好此证书，然后点击“上传 CA 证书”上传 CA 证书。

注意：在客户端配置的 CA 证书也必须是这样的格式。