SANGFOR SSL 快速安装手册

技术支持说明

为了让您在安装，调试、配置、维护和学习 SANGFOR 设备时，能及时、快速、有效的获得技术支持服务，我们建议您：

1. 参考本快速安装手册图文指导，帮助你快速的完成部署、安装 SANGFOR 设备。如果快速安装手册不能满足您的需要，您可以到 http://bbs.sangfor.com.cn 获得电子版的完整版用户手册或者其他技术资料，以便你获得更详尽的信息。
2. 致电您的产品销售商（合同签约商），寻求技术支持。为了更快速的响应您的服务要求和保证服务质量，您所在地的 SANGFOR 的产品销售商配备有经过厂家认证的技术工程师，会向您提供快捷的电话咨询、远程调试及必要的上门技术服务。
3. 在不紧急的情况下，您可以访问 SANGFOR 技术论坛，寻求技术问题的解决方案和办法。
4. 致电 SANGFOR 客服中心，确认最适合您的服务方式和服务提供方，客服中心会在您的技术问题得到解决后，帮助您获得有效的服务信息和服务途径，以便您在后续的产品使用和维护中最有效的享受技术支持服务，及时、有效的解决产品使用中的问题。

SANGFOR 技术论坛：http://bbs.sangfor.com.cn

公司网址：www.sangfor.com.cn

技术支持服务热线： 400-630-6430（手机、固话均可拨打）

邮箱：support@sangfor.com.cn

返修查询，在线咨询，欢迎您关注深信服官方技术服务微信：

目录

技术支持说明.....1
目录.....2
声明.....3
前言.....4
第 1 章 SSL 系列硬件设备的安装.....5
1.1.环境要求.....5
1.2.电源.....5
1.3.产品接口说明.....5
1.4.配置与管理.....6
1.5.设备接线方式.....8
第 2 章 SSL 系列硬件设备的部署.....10
2.1.网关模式.....10
2.2.单臂模式.....15
第 3 章 SSL VPN 接入配置案例.....18
3.1.客户环境与需求.....18
3.2.配置思路.....18
3.3.SSL VPN 总部设备配置步骤.....19
3.4.SSL VPN 客户端自动登录配置步骤.....23
3.5 应用封装.....25
第 4 章 密码安全风险提示.....30
4.1 修改控制台登录密码.....30

声明

SANGFOR 及  图标为深圳市深信服电子科技有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

前言

本手册仅介绍 SSL 设备安装部署的配置指导和最基本使用方法，如需要更详细配置介绍，请登录深信服技术支持论坛下载详细电子版用户手册。深信服技术支持论坛地址 http://bbs.sangfor.com.cn。

本手册以深信服 VPN 2050 为例进行说明。各型号产品硬件规格存在一定差异，但是设备配置以及基本使用方法一致，本手册适用于所有型号的 SSL 设备。

第 1 章 SSL 系列硬件设备的安装

本部分主要介绍了 SANGFOR SSL 系列产品的硬件安装。硬件安装正确之后，您可以进行配置和调试。

1.1.环境要求

SSL 系列硬件设备可在如下的环境下使用：

🗁输入电压：110V~230V

🗁温度：0～45℃

🗁湿度：5～90％

为保证系统能长期稳定地运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

1.2.电源

SANGFOR SSL 系列硬件设备使用交流 110V 到 230V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

1.3.产品接口说明

图 1 SANGFOR SSL VPN 网关面板（以 VPN-2050 为例）

从左到右的接口分别是:

CONSOLE：双机热备接口

ETH0 ： 设备 LAN 口

EHT1： 设备 DMZ 口

ETH2： 设备 WAN1 口

ETH3 ： 设备 WAN2 口

1.图片仅供参考，不同型号的产品外观请以实物为准。

2.如果设备存在 ETH4 等接口，则对应关系依次类推，ETH4-WAN3，ETH5-WAN4 等。

1.4.配置与管理

设备出厂的默认 IP 见下表：

接口	IP 地址
ETH0（LAN）	10.254.254.254/24 或 10.111.222.33/30
ETH1（DMZ）	10.254.253.254/24

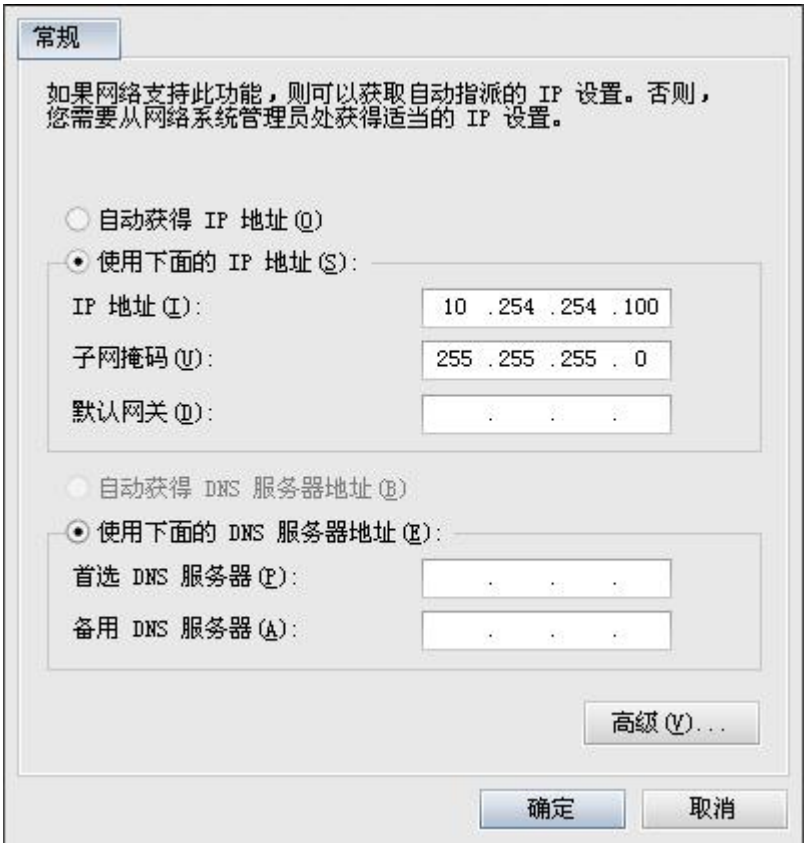
SSL 设备支持 HTTPS 管理，使用 4430 端口登录，如果使用初始地址登录，那么登录的 URL 地址为： https://10.254.254.254:4430 或者用 eth0 口的子接口地址输入 https://10.111.222.33:4430 登录，但是需要将电脑的 ip 地址更改为 10.111.222.34 子网掩码 255.255.255.252

设备默认关闭了远程维护功能，即仅允许从 ETH0 登录控制台页面。

如何登录 SSL 设备控制台页面？

将电脑网卡与 SSL 设备 ETH0 口接在同一个二层交换机或者直接将 ETH0 口和电脑网卡用网线连接，通过 WEB 界面来配置 SANGFOR SSL 设备。方法如下：

首先为本机器配置一个 10.254.254.X 网段的 IP（如配置 10.254.254.100），掩码配置为 255.255.255.0，配置如图：



然后在 IE 浏览器中输入网关的默认登录 IP 及端口 https://10.254.254.254:4430，页面如下：

在登录框输入『用户名』和『密码』，点击登录按钮即可登录 SSL 设备进行配置，默认情况下的用户名和密码均为 admin。

如果需要查看当前网关的版本号，点击查看版本，即显示当前设备的版本信息。

1.5.设备接线方式

在背板上连接电源线，打开电源开关，此时前面板的 Power 灯(绿色，电源指示灯)和 Alarm 灯(红色，告警灯)会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

请用标准的 RJ-45 以太网线将 LAN 口与内部局域网连接，对 SSL 系列硬件设备进行配置。

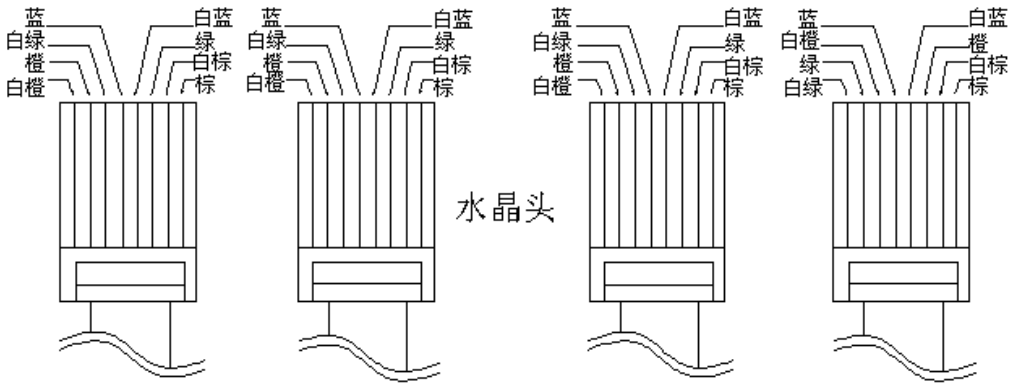
路由模式部署时，请用标准的 RJ-45 以太网交叉线（568A-568B）将 WAN1 口与 Internet 接入设备相连接，如路由器、光纤收发器或 ADSL Modem 等。

多线路的 SSL 系列硬件设备可以支持多条 Internet 线路，此时将 WAN2 口与第二条 Internet 接入设备相连，WAN3 口与第三条 Internet 线路相连，依此类推。

使用标准 RJ-45 以太网直通线（568A-568A）将 DMZ 口与 DMZ 区的网络连接，一般而言，DMZ 区放置对外提供服务的 WEB 服务器、EMAIL 服务器等。SSL 系列硬件设备可以为这些服务器提供安全保护。

SSL 系列硬件设备正常工作时 POWER 灯常亮，WAN 口和 LAN 口 LINK 灯长亮，ACT 灯在有数据流量时会不停闪烁。ALARM 红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不能熄灭，请与深信服客户服务中心联系。

WAN 口直接连接 MODEM 应使用直通线(568A-568A)、连接路由器应使用交叉线(568A-568B)；LAN 口连接交换机应使用直通线、直接连接电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，如下图：



直连网线线序图示　　交叉网线线序图示

第 2 章 SSL 系列硬件设备的部署

本部分主要介绍了 SANGFOR SSL VPN 系列产品的部署方式和配置方法。SANGFOR SSL 硬件支持两种部署方式，为网关模式、单臂模式。部署完成后，可以对 SSL VPN 设备进行配置。

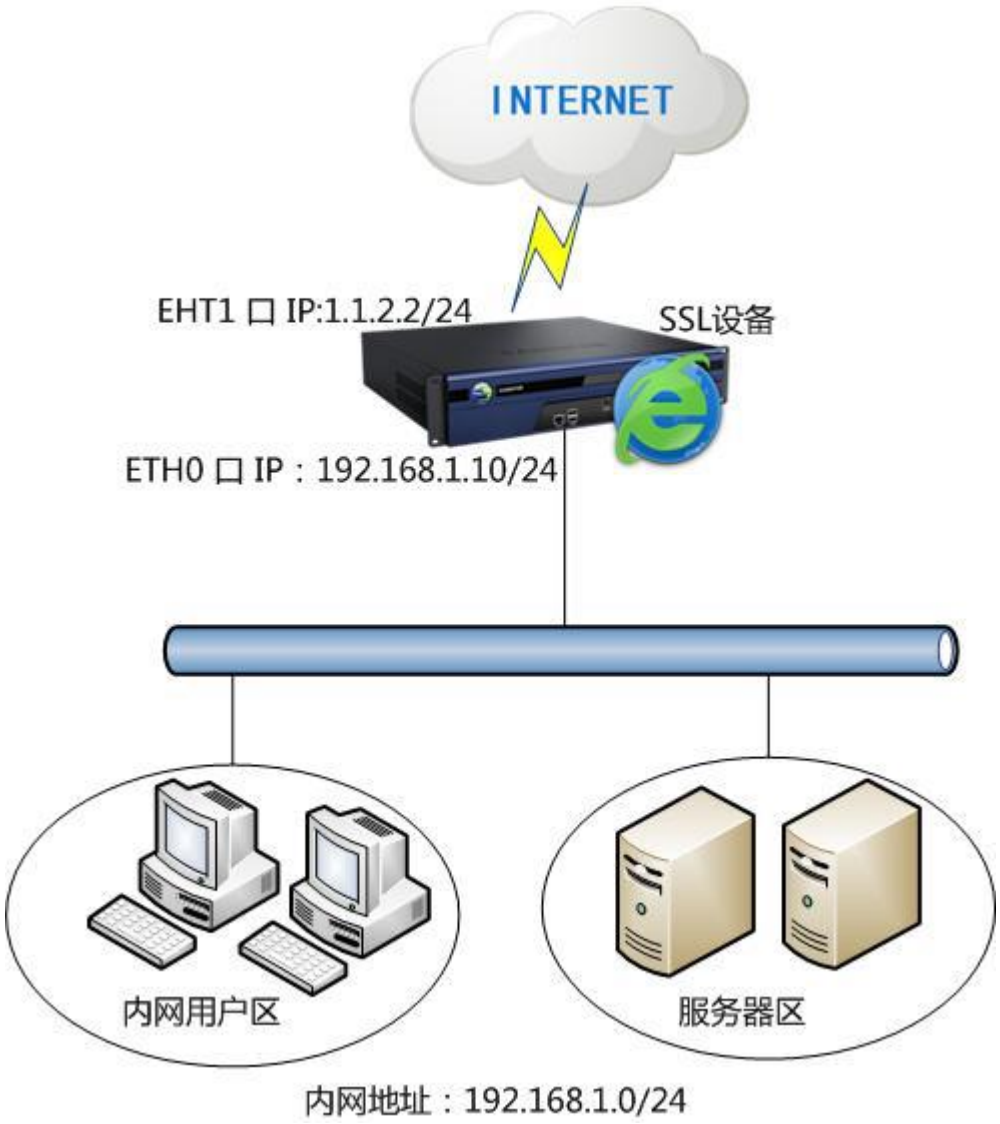
2.1.网关模式

2.1.1.SSL 网关模式介绍

网关模式下可以将 SSL 设备当成路由器或者简单防火墙来部署，需要设置内网口、外网口 IP 地址。可以设置代理上网，端口映射等规则，具备简单防火墙的功能。

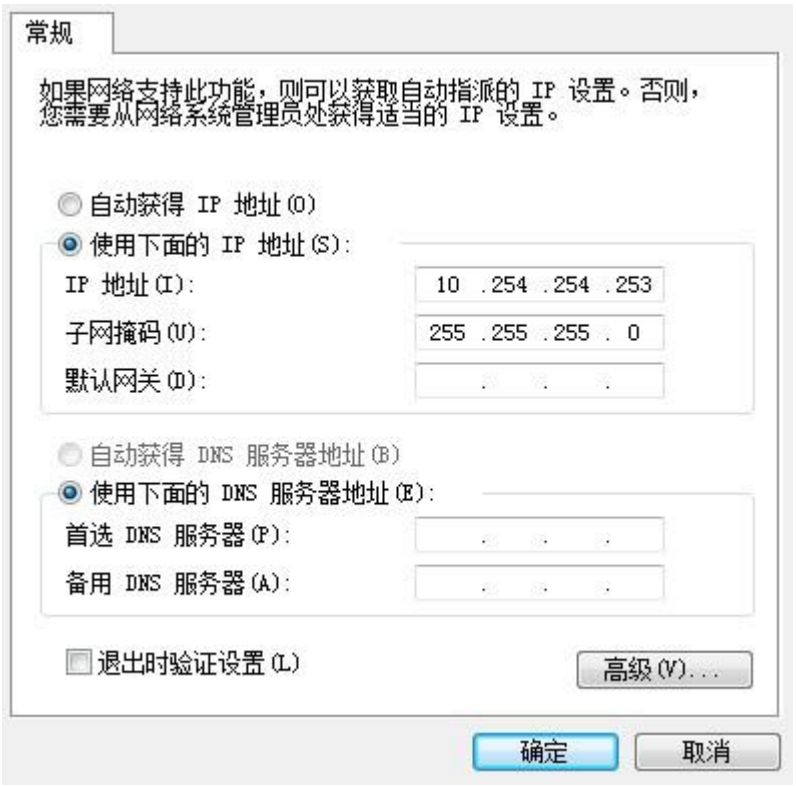
2.1.2.SSL 网关模式部署案例

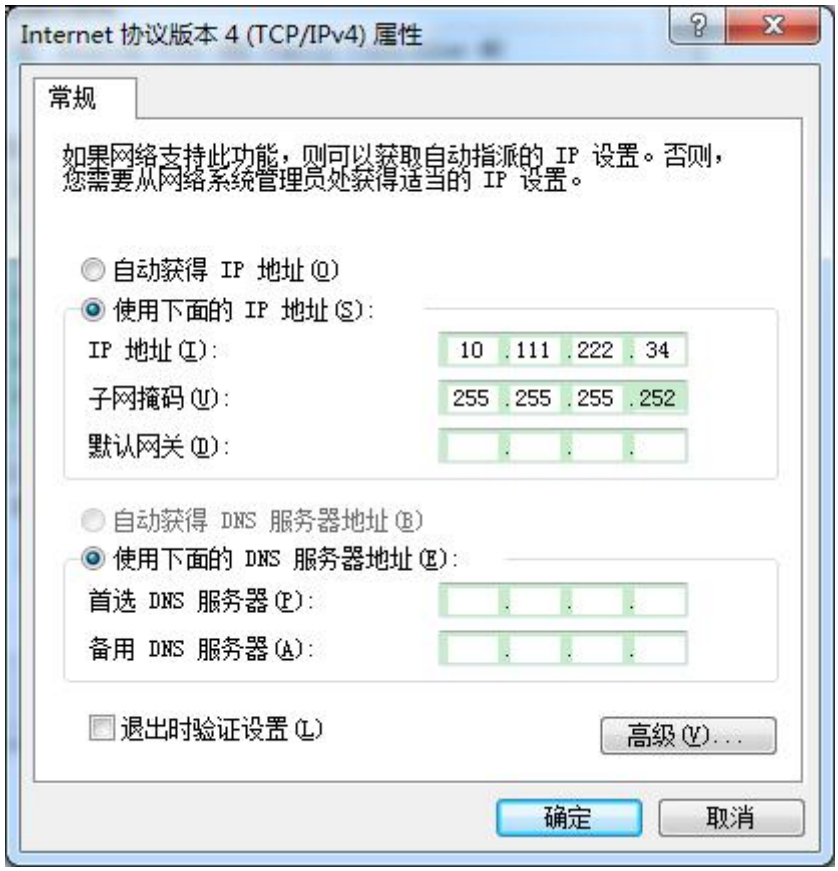
客户环境与需求：某客户网络拓扑如下，客户有一条运营商链路，原有一个路由器做出口。希望用 SSL 设备网关模式部署在网络出口，代理内网用户和服务器上网，并提供 SSL VPN 接入功能。



配置方法：

第一步：首先将设备开机，用网线接设备的 EHT0 口（LAN），将电脑网卡的 IP 配置成 10.254.254.253，或者将电脑网卡的 ip 地址配置为 10.111.222.34 子网掩码 255.255.255.252 界面如下：





第二步：打开 IE 浏览器，输入 https://10.254.254.254:4430 或者 https://10.111.222.33:4430，即可到登录界面，输入设备出厂默认的账号密码 admin/admin，界面如下：

第三步：内、外网接口配置，进入『系统设置』→『网络配置』，部署模式选择网关模式，配置好内网接口，界面如下：

外网接口配置，在配置内网接口的下面，显示外网线路，点击相应的线路进行配置，界面如下：

第四步：本案例中还需要 SSL 设备代理内网用户和服务器上网，所以还需要设置代理上网。进入『防火墙设置』→『NAT 设置』→『代理上网设置』，选择新增，配置需要代理上网的内网网段，界面如下：

以上步骤设置完毕，则可以将设备 LAN 口接到交换机，WAN 口接公网链路。部署完毕。

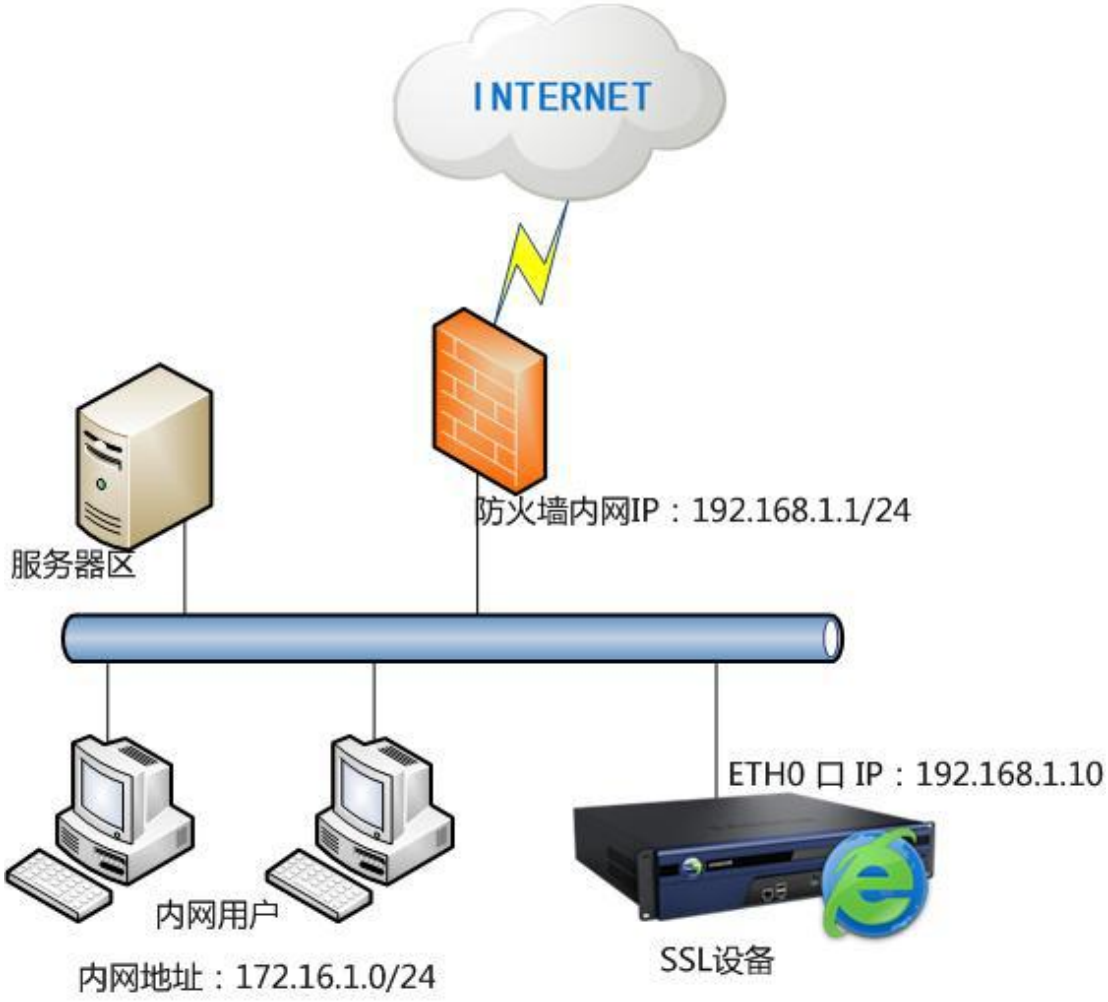
2.2.单臂模式

2.2.1.SSL 单臂模式介绍

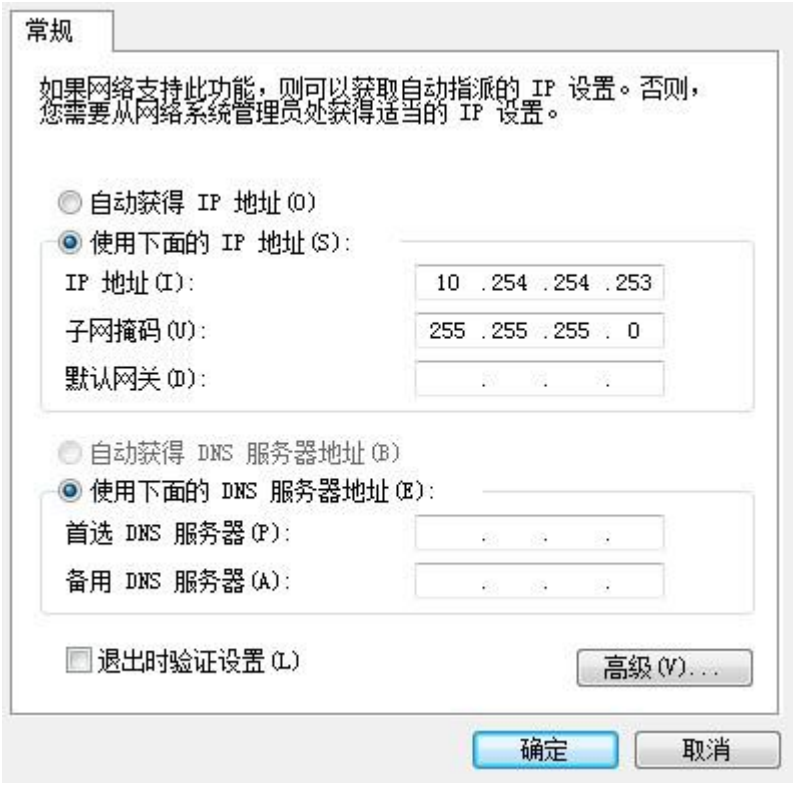
单臂模式为常用部署方式，不需要改变网络结构。接设备一个 LAN 口到内网交换机即可。SSL 单臂模式主要实现 SSL VPN 接入功能。

2.2.2.SSL 单臂模式部署案例

客户环境与需求：某客户拓扑如下，内网用户和服务器均通过公网 INTERNET 上网。客户希望 SSL 设备单臂模式部署到三层交换机，最终实现 SSL VPN 接入功能。



第一步：首先将设备开机，用网线接设备的 EHT0 口（LAN），将电脑网卡的 IP 配置成 10.254.254.253 或者是 10.111.222.34 子网掩码 255.255.255.252，界面如下：



第二步：打开 IE 浏览器，输入 https://10.254.254.254:4430 或者输入 https://10.111.222.33:4430，即可到登录界面，输入设备出厂默认的账号密码 admin/admin，界面如下：

第三步：进入『系统设置』→『网络配置』，部署模式选择单臂模式，设置好 LAN 口

IP 地址，掩码和网关。界面如下：

第四步：由于 SSL 设备部署在内网，该设备作为总部实现 SSL VPN 接入功能，需要在前置防火墙做端口映射给 SSL 设备。SSL 设备建立 VPN 的端口是 TCP 443。各个厂家设置方法有所不同，此处不截图说明。

以上步骤设置完毕，则可以将 SSL 设备 LAN 口接到交换机，检查从内网是否可以登录设备，部署完毕。

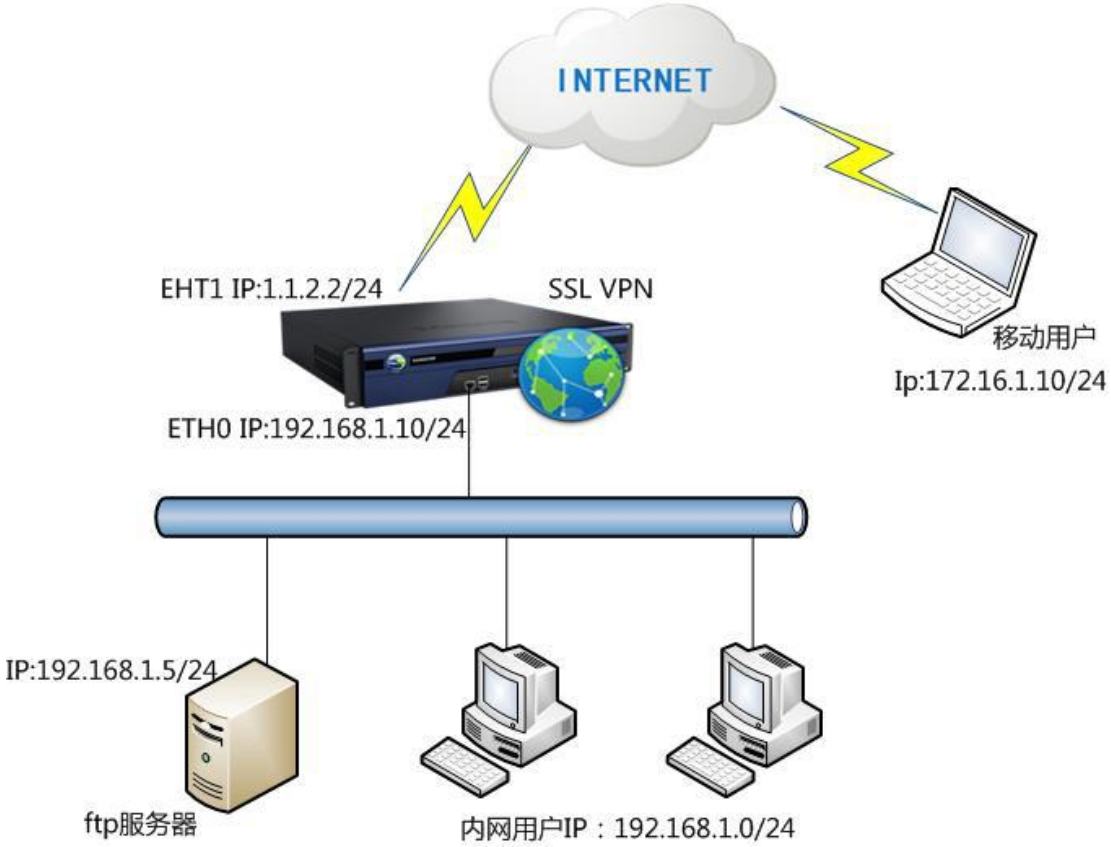
1. 443 为 SSL 设备出厂默认的 VPN 监听端口，可以做修改，如做了修改，则端口映射需要映射实际的监听端口。

2.单臂模式必须将设备 LAN 口接到内网交换机。

第 3 章 SSL VPN 接入配置案例

3.1.客户环境与需求

某客户拓扑如下，SSL VPN 网关模式部署在客户网络出口处，代理内网用户和服务器上网，公司有移动办公人员希望通过 SSL VPN 接入访问公司内网的 ftp 服务。并在客户端实现自动登录 SSL VPN。



3.2.配置思路

1. 按照第 2 章的内容将 SSL 设备配置上架。
2. 外网需要访问内部资源，首先要建立 VPN 连接。
3. 配置 SSL VPN 客户端自动登录。

3.3.SSL VPN 总部设备配置步骤

第一步：将深信服 SSL 设备配置成网关模式并且上架，详细请参考 2.1 章节。

第二步：配置 SSL VPN 接入选项，进入『系统设置』→『SSL VPN 选项』→『系统选项』，选择接入选项，配置接入端口及 WEBAGENT，配置界面如下，

1.443 为设备默认的标准协议端口，如果更改了端口，则访问 SSL 登录页面时需要在主机地址后面添加端口来登录，如无必要，请勿修改。

2.SSL VPN 网关设备如果在没有固定公网 IP 的时候，可以使用 WebAgent 动态寻址。

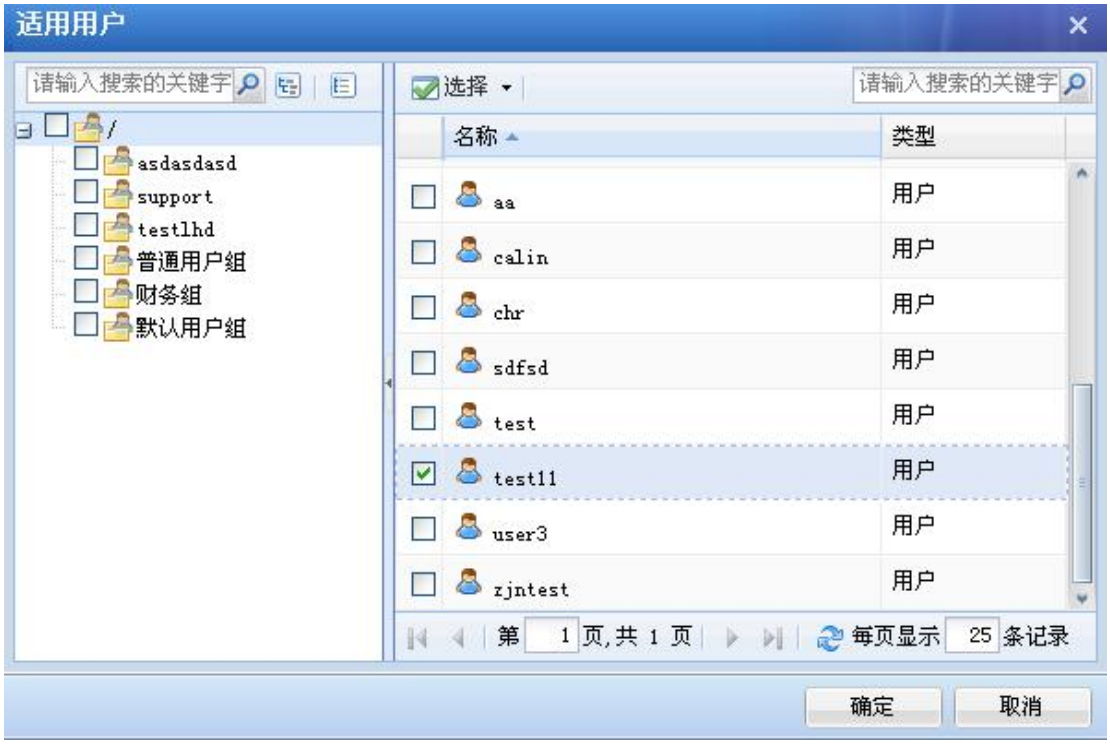
第三步：客户端选项配置，进入『系统设置』→『SSL VPN 选项』→『系统选项』，选择客户端选项，本案例配置界面如下：

第四步：新建用户，『SSL VPN 设置』→『用户管理』→，点击新建用户，配置完以后点保存，本案例配置界面如下：

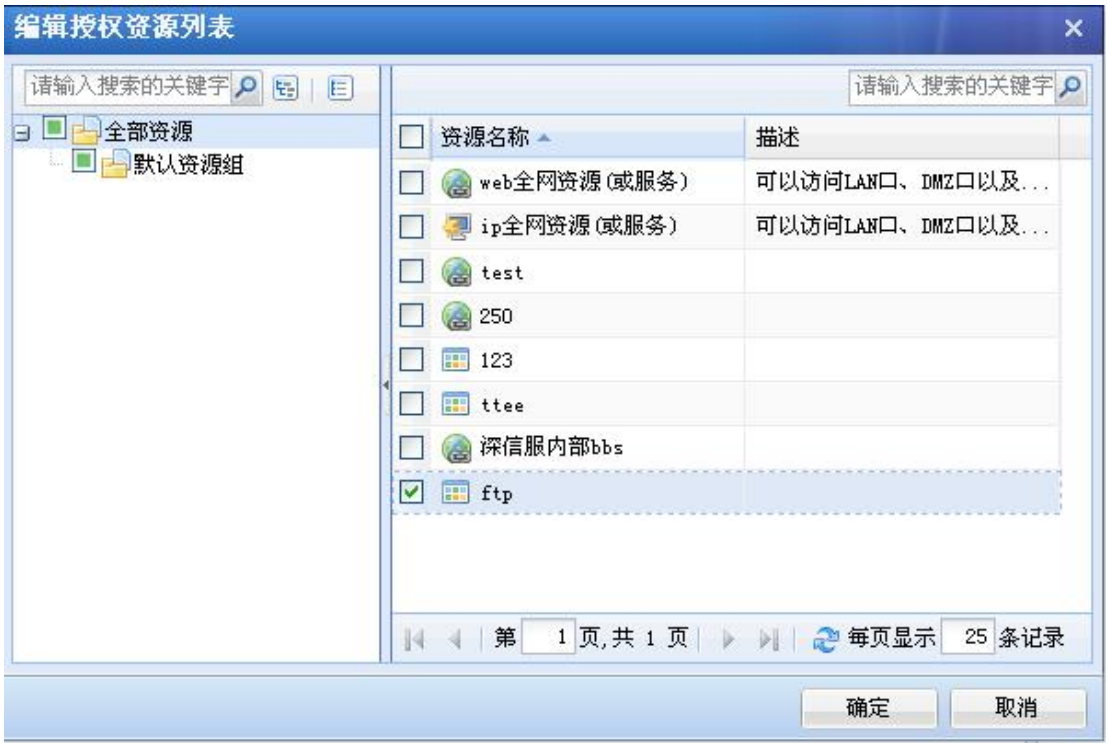
第五步：新增资源，进入『SSL VPN 设置』→『资源管理』，点击新建，选择 TCP 应用，设置资源名称，选择资源类型，配置界面如下：

配置资源地址，点击后面的添加按钮，配置完后点击确定，配置界面如下：

第六步：角色关联，即将资源和用户关联，进入『SSL VPN 设置』→『角色授权』，点击新建，选择新建角色，配置角色名称，选择关联用户，界面如下：



『进入编辑授权资源』页面，选择关联资源，界面如下：



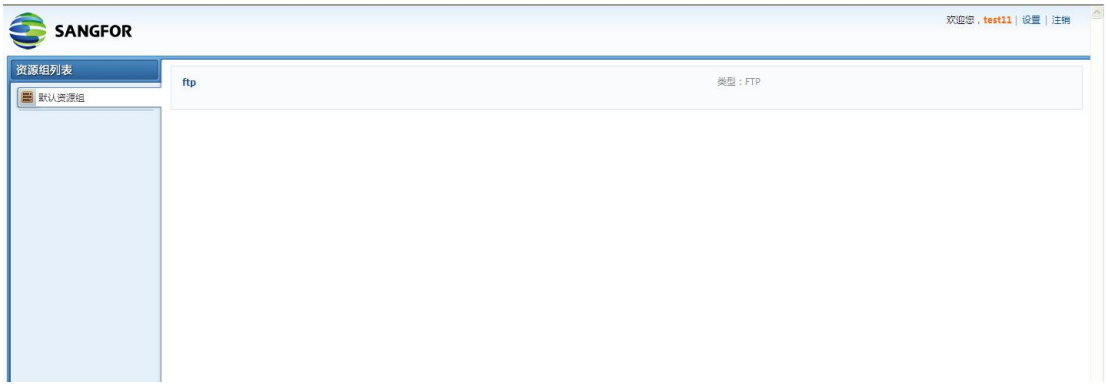
配置完以后点保存

所有配置完成以后，必须点击右上角的立即生效，否则配置不会更新到设备。

3.4.SSL VPN 客户端自动登录配置步骤

第一步：登录 SSL VPN，在浏览器上输入 SSL VPN 登录地址，登录界面如下：

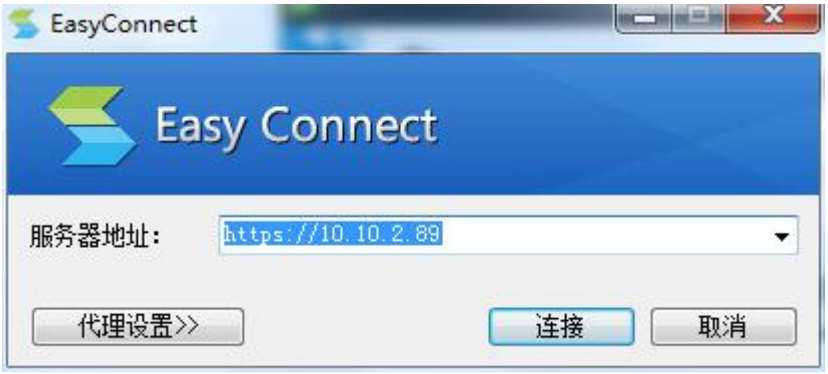
第二步：输入用户名密码，登录 SSL VPN，便可以看到资源列表，界面如下：



这时，用户可以根据需要访问资源。

第三步：首次登录 SSL VPN 后，会自动安装 SSLVPN 登录客户端，在客户端的“开始菜单”会如下图所示：

第二步：点击启动客户端，设置 SSL VPN 地址，点击连接



第四步： 配置登录的用户名和密码，选择自动登录，点击登录，界面如下

以上步骤完成，即完成客户端自动登录的所有配置，后续客户端再需要连接 SSL VPN 时，只需要打开客户端程序即可。

SSL VPN 支持 Windows 操作系统、Linux 操作系统和 Mac OS X 操作系统。

3.5 应用封装

『应用封装』将应用封装到 SSL VPN，以实现应用的安全接入和访问。

WEBUI 路径：『SSL VPN 设置』→『企业移动管理』→『应用封装』。如下图：

点击删除，用来删除所选择的应用。

点击编辑，用来编辑一条所选的应用。

『刷新间隔』，设置页面信息的刷新时间。点击立即刷新，则立即更新页面上显示的信息。如图：

查询中可选择[按名称]、[按类型]或[按状态]来查找应用。在输入搜索关键字中输入相应的关键字，点击后面的即可。

点击基础设置，用来设置应用封装的认证界面模板和所需的证书，如下图所示：

点击删除，用来选择所选择的规则。

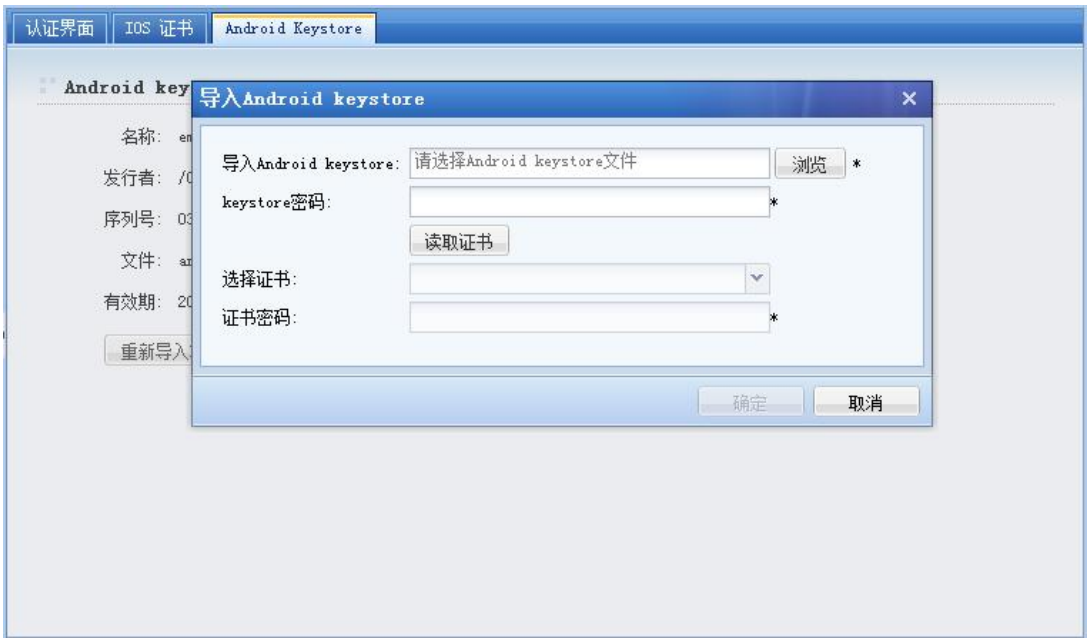
点击编辑，用来编辑一条所选的规则。

点击新建，新建 APP 登录 VPN 的认证界面模板（适合认证方式为：由用户自行填写），可根据实际情况上传 iPhone、iPad 、Android phone 、Android Pad 的图片。如图：

『IOS 证书』：.ipa 的 app 封装需要导入 IOS 的企业签名证书如下图所示：

导入 IOS 证书，使用应用封装功能封装 IPA 应用，必需先上传 IOS 企业签名证书。

『Android 的 Keystore 证书』：.apk 的 APP 封装需要导入 Android 的 Keystore 证书，如图：



点击新建，新建封装，如下图：

点击浏览找到 apk 或者 ipa 的本地路径，点击上传上传对应的应用。

『应用名称』定义该应用的名称，可不修改。

『认证方式』用户使用 APP 时登录 vpn 的方式，包括匿名认证、公共帐号认证、用户名密码或证书认证。

『匿名登录』封装后的 APP 使用匿名用户登录 SSL VPN，需要在『SSL VPN 设置』→『认证设置』开启匿名登录功能，登录 APP 过程无认证界面。

『公共帐号认证』需填写 SSL VPN 的公有用户帐号和密码，封装后的 APP 使用该公有用户登录 SSL VPN，登录 APP 过程无认证界面。

『用户名密码或证书认证』主要是私有认证，封装后的 APP 有认证界面，需要用户填写认证信息，支持用户密码认证、证书认证、短信认证、令牌认证，及它们的组合认证。

『认证界面模板』封装后的 APP 登录 SSL VPN 的认证界面，只有在选择『用户名密码或证书认证』认证方式才有，用户可选择默认模板，也可在应用封装列表的【设置】中

新增自己的认证界面。

『VPN 地址』封装后的 APP 连接 SSL VPN 的地址，可为 IP，域名或 webagent 地址。

『Keystore 证书』用于重新签名已封装好的 Android 应用程序。可在此导入新的证书，或在【设置】中导入。若上传的是 IOS 的 APP，则此处为『IOS 企业签名证书』，另外 IOS 应用还需要每个 APP 都上传一份.mobileprovision。

『为安全应用共享会话 』当企业有多个 APP（封装时使用同证书签名）时，无需多次进行 VPN 认证，后一个 APP 使用前一个 APP 登录时的帐号信息，自动进行登录，且只占用一个授权。

『启用手势密码保护』已封装的 APP，从后台拉起或登录，都需输入正确的手势密码才能进入，以此保证应用的安全。

『启用文件加密』已封装的应用，落地文件加密处理，保证文件安全。提供【所有文件】、【常见的文档、数据库、配置文件 】和【配置排除】。

『SDK 版本号』默认标准版本，客户若有特殊需求，可提交快速响应需求单，填写定制单号封装 APP。

第 4 章 密码安全风险提示

为了防止其他无关人员或恶意攻击者通过默认账号密码登录和更改设备配置，请修改 SSL 设备登录的默认密码。SANGFOR SSL 设备有两类密码：

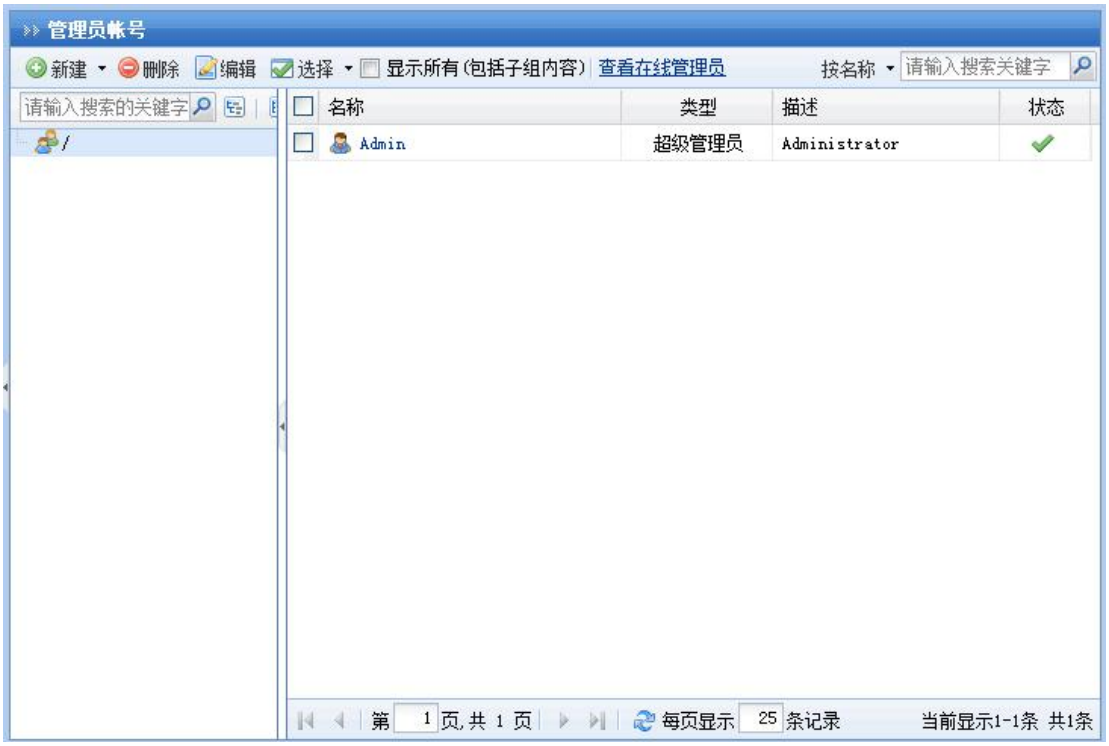
1. SSL 控制台登录密码。

2. SANGFOR 设备升级系统的登录密码。

SANGFOR 设备升级系统的登录密码与 SSL 设备控制台超级管理员 admin 的登录密码一致，修改了控制台的登录密码，即同时修改了 SANGFOR 设备升级系统的登录密码。

4.1 修改控制台登录密码

通过【系统设置】-【管理员账号】修改控制台登录密码，方法如下：



点击用户名“admin”，出现如下页面：

修改管理员密码，点击保存。

1. 如果有多个网络管理员需要登录设备，请给每位管理员设置登录账号，超级管理员 admin 的密码请勿广泛流传。

2.修改了控制台 admin 的密码后，SANGFOR 设备升级系统的登录密码也会做相应的修改。