深圳市启博网络有限公司

启博 VPN / 防火墙用户手册

商标、版权声明


为深圳市启博网络有限公司注册商标，本产品的所有部分，包括配件、软件，其版权都归深圳市启博网络有限公司所有，未经深圳市启博网络有限公司许可，不得任意仿制、拷贝、誊抄或转译，除非另有约定，本手册所提到的产品规格和软件信息仅供参考，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如内容更新，恕不另行通知，用户可随时登录我们的网站 http://www.vpnsoft.net 查阅。

目录

1. 产品概述

感谢您选用深圳市启博网络有限公司出品的 MR 系列 VPN 防火墙网关，本手册以启博 MR-5400 为例进行设置，由于各型号产品硬件和软件规格存在差异，有涉及产品规格的问题需要和深圳市启博网络有限公司销售部联系确认。

1.1. 产品概述

启博 MR-5400（包括含 MR-5200/6100/7100/8100 等）是针对大中型企业量身定制的多功能一体化 VPN 防火墙网关，集成 VPN、防火墙、带宽控制、上网行为管理等功能，主要用于解决企业业务系统（如财务软件、ERP、进销存、OA、邮件系统等）的远程互联、移动办公、远程监控、工业控制等，设备内置启博目录服务寻址技术，不需要客户申请固定 IP 或动态域名，通过启博 VPN 的简单设置即可以把企业分布在不同地域的工作人员，连成一个大的局域网

1.2. 支持的标准和协议

- IEEE 802.3 10Base-T
- IEEE 802.3u 100Base-TX
- CSMA/CD、pppoE、PPP、IP、ARP、DHCP、TCP、UDP、HTTP、FTP、DNS、PPTP、L2TP、IPSEC、ESP、GRE

1.3. 工作环境

温度

- 0°至 50°（工作）
- -40°至 70°（储存）

湿度

- 10% 至 90% RH 无凝结（工作）
- 5% 至 95% RH 无凝结（储存）

2. 硬件安装

2.1. 系统要求

- 标准的个人计算机
- 具备至少 1 个以内网网络适配器（网卡和网线）
- 操作系统：微软 Windows，linux 或 MAC 操作系统
- 具备标准的 WEB 浏览器

2.2. 恢复默认

如果你想恢复出厂设置，请在启博 VPN 网关通电情况下，接上显示器和键盘，选择第 4 项 Restore Factory Defaults ,设备会自动重启并恢复出厂设置。

2.3.硬件安装过程

- 给设备接上电源并打开设备上的电源开关，设备上的 PWR 灯会亮起。
- 把连接外网的网线（也称进线）接到 VPN 网关的 WAN1 口（或 WAN2 口），连接电脑的网线接到 LAN1 接口。
- 连接好后，检查 PWR 提示灯及对应插网线的接口（WAN 和 LAN）网口指示灯是否点亮。

- 小提示：外网线包括 ADSL Modem(俗称：猫)接出来的网线，或者互联网运营商（电信、联通、移动、长宽等）直接拉进户的网线。

3. 登入设备

你可以通过基于 WEB 浏览器的配置来管理 VPN 网关。要通过 web 浏览器配置 VPN 网关，至少要一台合理配置的电脑，通过以内网或者无线网络连接到 VPN 网关，**启博 MR 系列 VPN 网关的默认 IP 是 192.168.10.1，子网掩码 255.255.255.0，DHCP 服务器默认是开启的**。在设置 VPN 网关之前，确保电脑的设置是从 VPN 网关自动获取 IP 地址，参照下面的步骤来设置

3.1. Windows XP

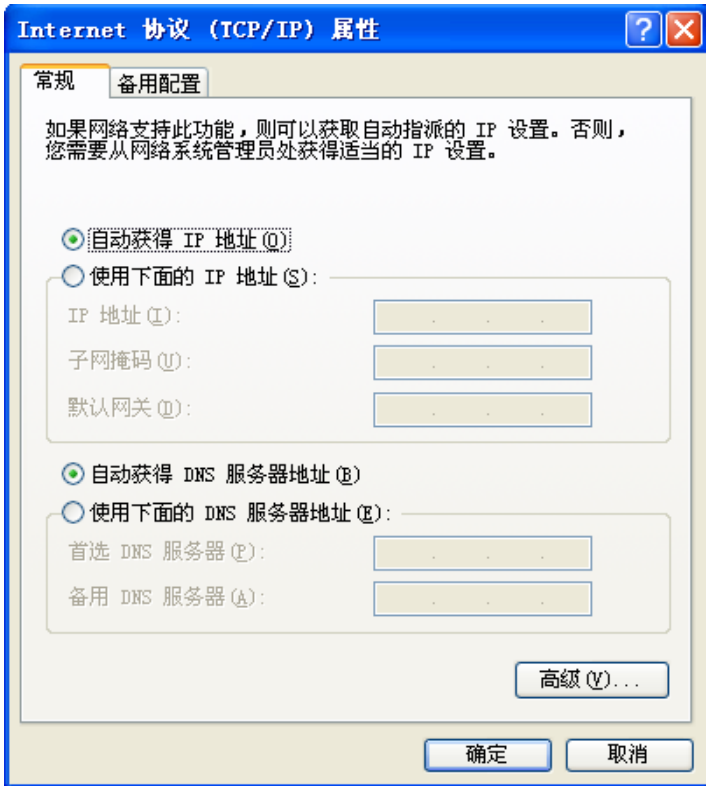
请按照下述步骤来配置你的电脑

1、**在桌面上找到网上邻居图标，鼠标右键点击，选择属性**

2、选择**本地连接**，右键点击**属性**

3、点击选择 **Internet 协议（TCP/IP）**， 再点击属性按钮

4、选择自动获得 IP 地址和自动获得 DNS 服务器地址，然后点击确定，关闭 Internet 协议（TCP/IP）属性窗口

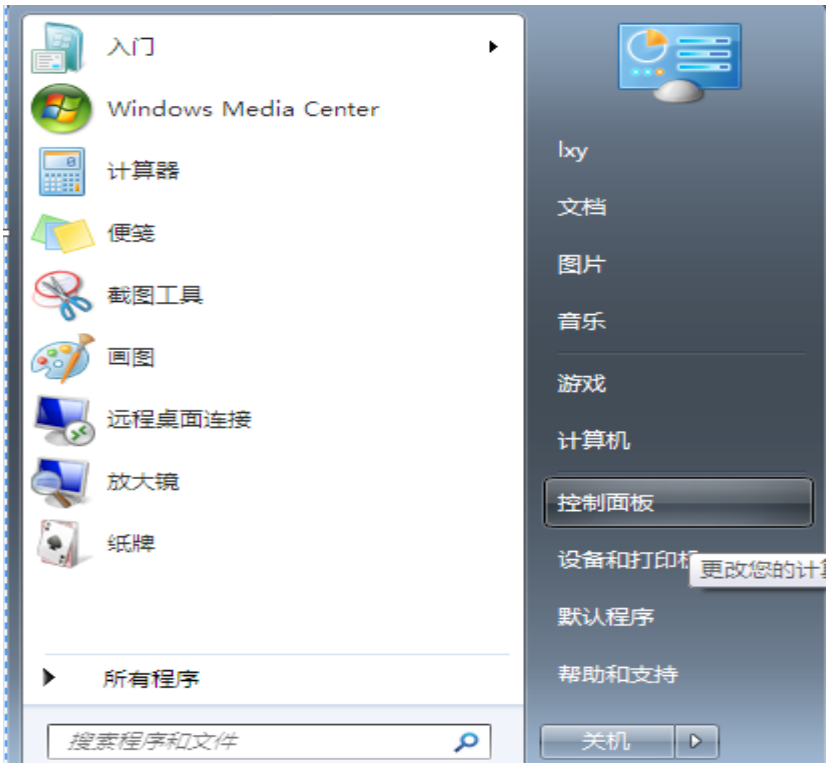


5、点击确定，关闭本地连接属性窗口后生效

3.2. Windows Vista/Windows 7

请按照下述步骤来配置你的电脑

1、**开始---控制面板**

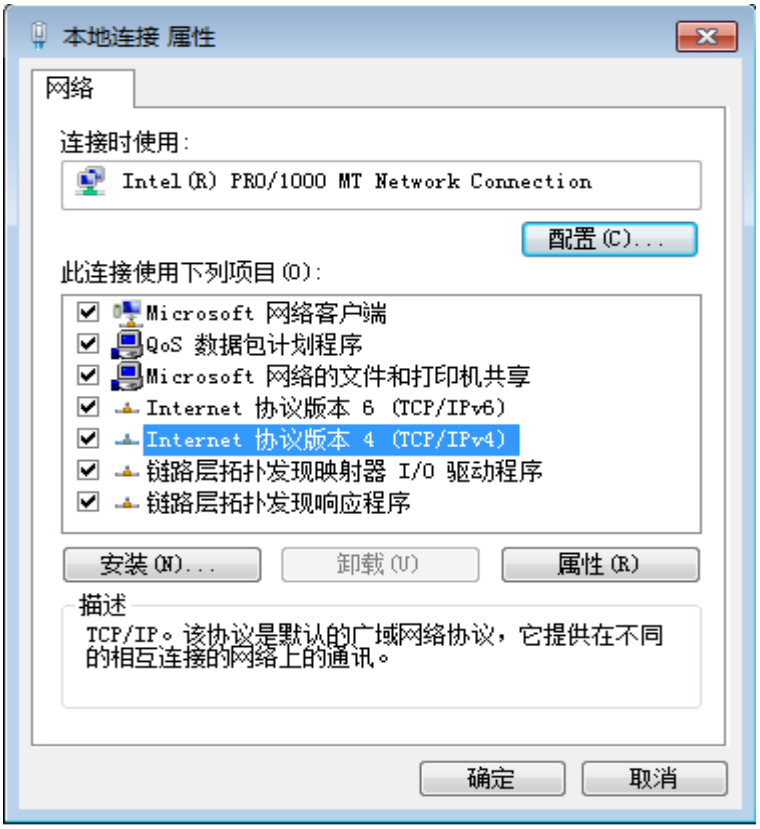


2、点击 **查看网络状态和任务**

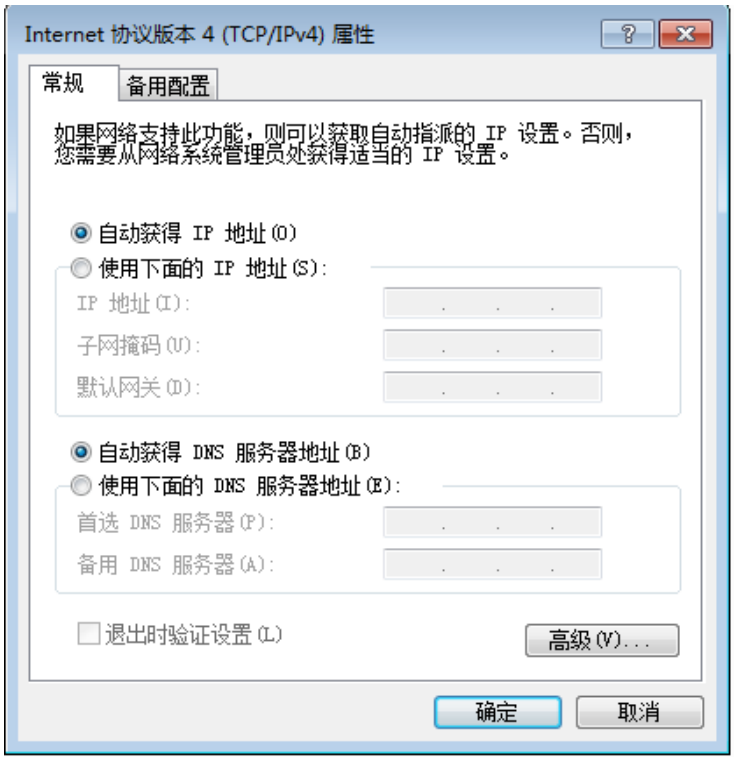
3、点击窗口最左边的**更改适配器设置**

4、右键点击 本地连接

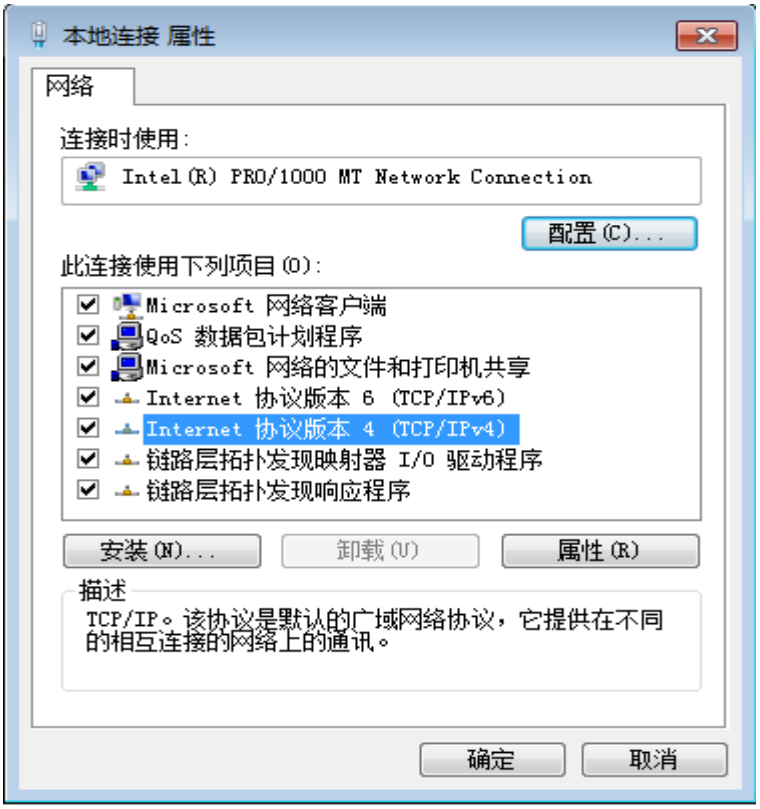
5、点击 **Internet 协议版本 4（TCP/IP）,然后点击属性按钮**



6、选择自动获得 IP 地址和自动获得 DNS 服务器地址，然后点击确定关闭 Internet 协议（TCP/IP）属性窗口



7、点击 确定 关闭本地连接窗口

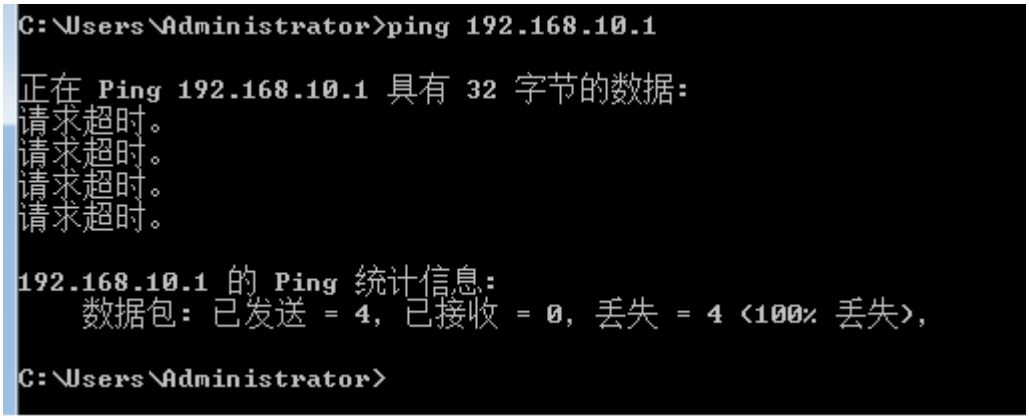


3.3. 用 VPN 网关检查电脑的 IP 和连接

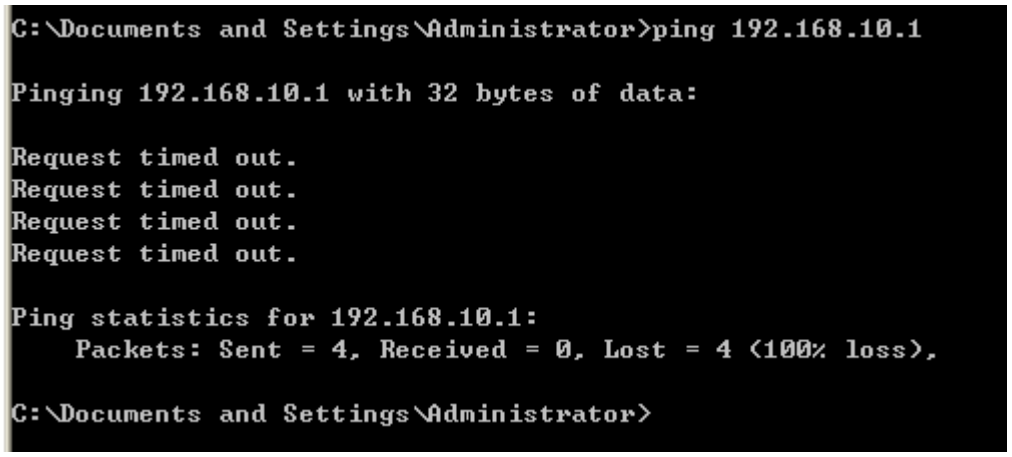
设置完 TCP/IP 协议后，用 Ping 命令来验证电脑是否可以与 VPN 网关通信，要执行 Ping 命令，打开 DOS 窗口，在 DOS 提示里 Ping 启博 VPN 网关的 IP 地址
在桌面左下方，开始--运行，输入 cmd 并回车，在 DOS 提示示，输入下述命令并回车，如果命令窗口返回类似于下面的内容。

那么 VPN 网关与电脑之间的连接就成功的建立了。

如果电脑和 VPN 设备连接有问题或电脑的本地连接设置不正确，将返回下述内容



或者



这里要确认你的电脑的网络设置是否正确，并且检查电脑与 VPN 网关之间的线路连接。

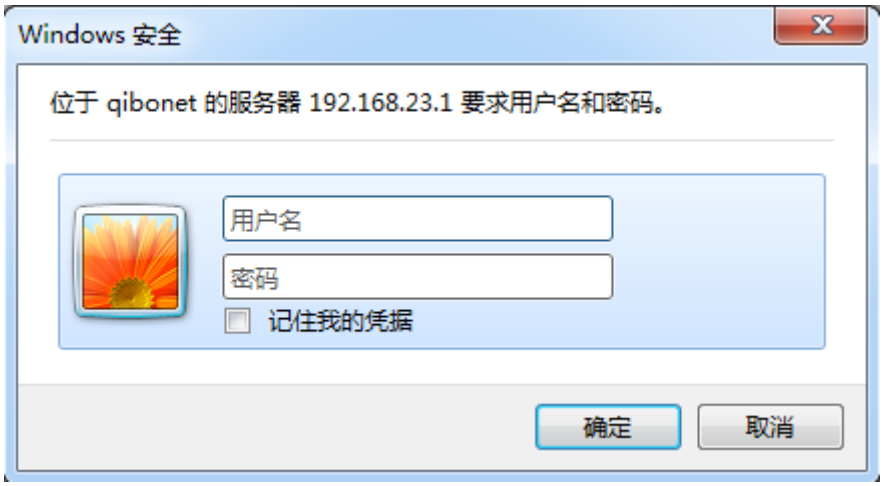
3.4. 登入

启博 VPN 网关提供基于浏览器（IE、firefox、chrome、腾讯 TT 等）的配置界面，这种配置方案适宜于任何 Windows、Linux(unix)、苹果系统等。

1、打开桌面上的 Internet Explorer 浏览器或其他浏览器，在地址栏里输入 https://192.168.10.1:10443 ,点击回车键

2、在下一个页面提示，选择 “继续浏览此网站”，这里需要说明的，这个安全提示是因为 https 协议本身的原因，它需要一个被微软公司认证过的证书，这个证书的费有时会贵过设备本身，https 协议本身就是一个安全协议，我们一般可以忽略这个提示。

3、在弹出的窗口中输入用户名：admin　密码：netadmin 注意都为小写，按下确认键。如果你需要经常配置 VPN 网关，可以勾选记住我的凭据。



使用默认的密码有时会有安全隐患，建议定期更换设备密码。

4、确定之后则成功登陆启博 VPN 网关配置界面。

这里有显示产品名称，设备型号，软件版本号，VPN 接入授权数、以及硬件信息、网络接口信息等。

4. 配置指南

4.1. 系统

4.1.1. 网络设置

系统->网络设置-> 第一步是选择宽带上网的方式，通常 PPPoE 拨号上网方式比较多，我们这里以 PPPOE（ADSL 拨号上网）为例,如下图所示：

- 以太网 STATIC：静态 IP 地址上网方式选择。
- 以太网 DHCP：动态 IP 地址上网方式选择， 如长城宽带、有线通，天威宽带等。
- PPPoE ：拨号上网方式选择，大多数用户用这种方式。
- GATEWAY:透明模式上网方式，有时也叫桥接模式、单臂接入或旁路接入

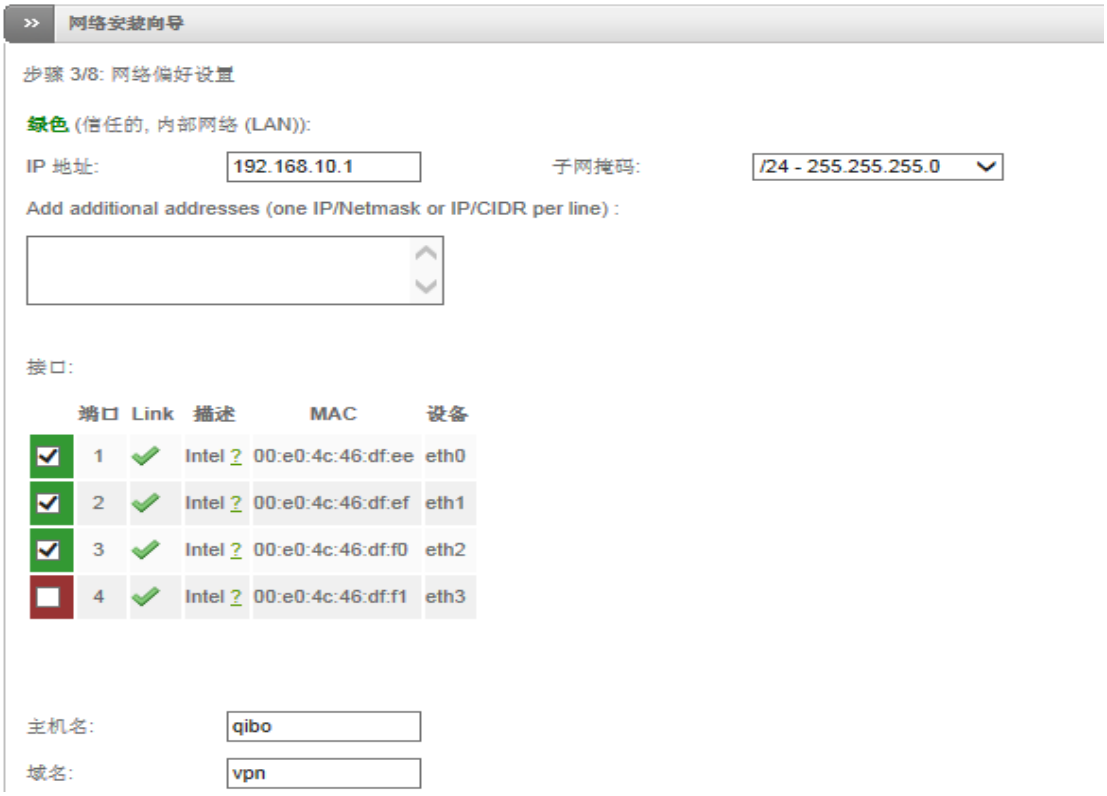
点前进 >>> 按钮继续下一步的配置。

此页面根据你的网络类型选择即可.如下图所示：

网络设置

点前进 >>> 按钮继续下一步的配置。

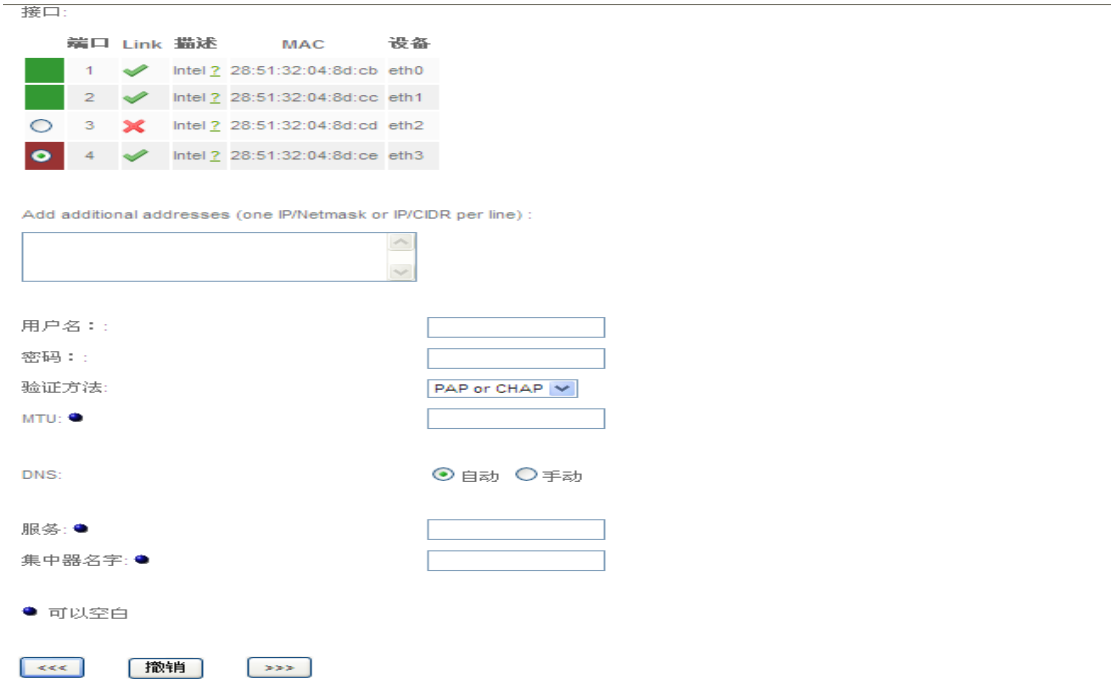
网络设置



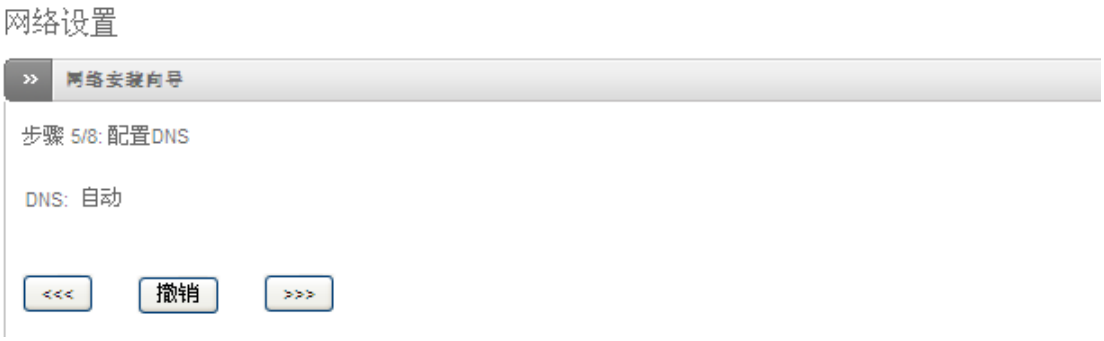
- IP 地址：VPN 设备的 LAN 接口 IP 地址，也是我们通过浏览器进入 VPN 设备的地址。
- 子网掩码：VPN 设备的 LAN 口子网掩码，它决定了 VPN 设备下内部网络的 IP 地址范围。
- Add additional address：这个是可选项，如果需要内网多网段的用户，可以在此设置多个网段，如 192.168.8.1/24 , 192.168.9.1/24 等一行一个。

点前进 >>> 按钮继续下一步的配置。

此页面是设置宽带上网用户名和密码,认证方式用默认. MTU 可以手动输入接口的 MTU 大小的自定义值，建议用默认留空，除非 ISP 指定。DNS 选择自动。其它的可为空。如下图所示：

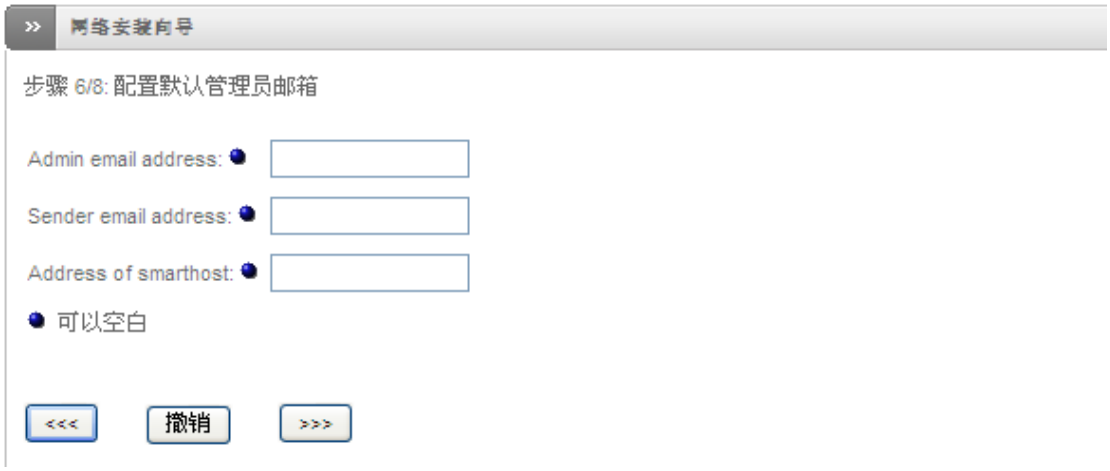


点前进 >>> 按钮继续下一步的配置。
如上一步 DNS 选择的是自动,那么这里就直接点前进按钮继续下一步的配置，如下图所示：



点前进 >>> 按钮继续下一步的配置。
这里是填写管理员的邮箱，主要用于接收一些系统提示邮件，可做配置,也可不做配置,直接进入到一下步，如下图所示：

网络设置



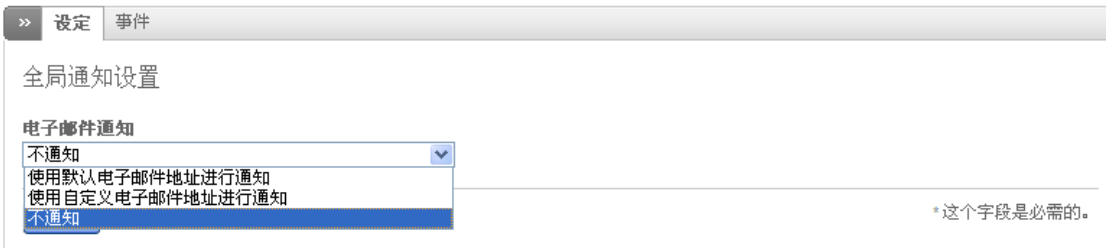
点前进 >>> 按钮继续下一步的配置。
这里单击“OK 应用配置”，如下图所示：

网络设置

到此网络设置完成，设备会自动重新启动一次。

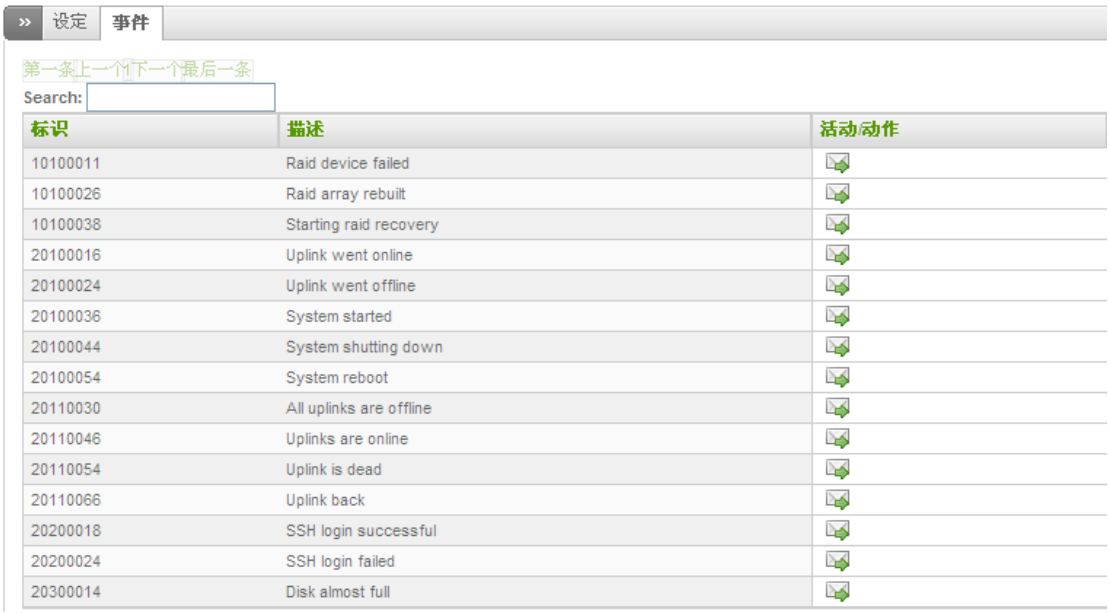
4.1.2. 事件通知

系统 > 事件通知,选择好记得单击“保存”按钮，如下图所示:



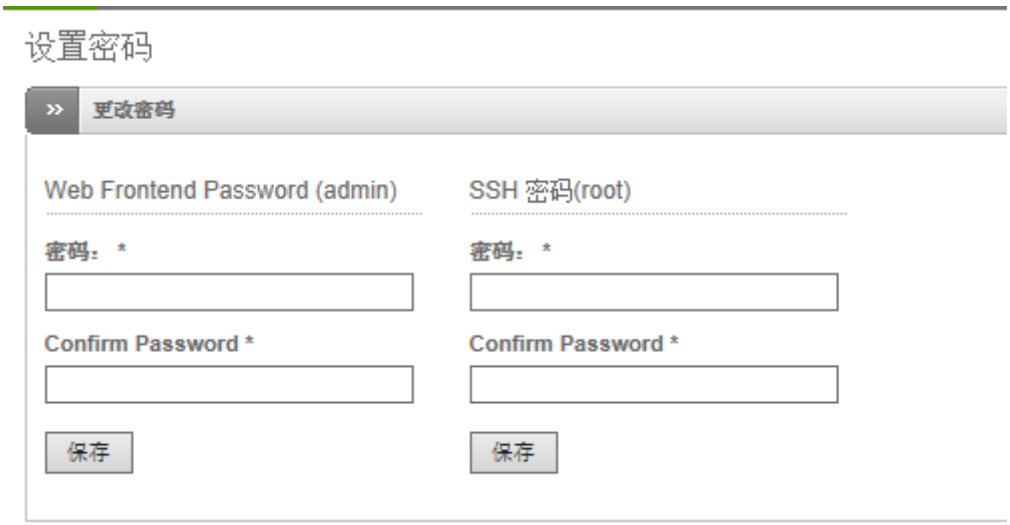
事 件

系统-> 事件通知-> 事件，如下图所示：



4.1.3. 设置密码

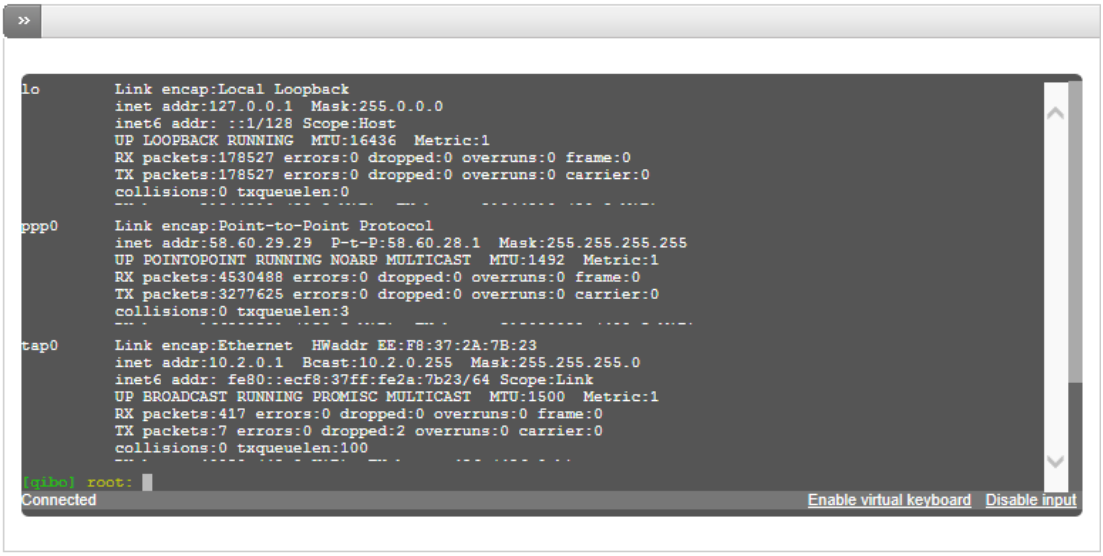
系统->设置密码，可以把设备默认的用户名和密码更改为你所容易记住的用户名和密码，如下图所示：其中 web frontend password 是指通过网页访问启博 VPN 网关使用的密码；ssh 密码是指通过 SSH 命令行方式访问启博 VPN 使用的密码。



4.1.4. 运行命令

系统 > 运行命令,如下图所示:这里可以登录系统后台，做一些简单的调试工作，方法是输入 login,回车，根据提示符输入密码，

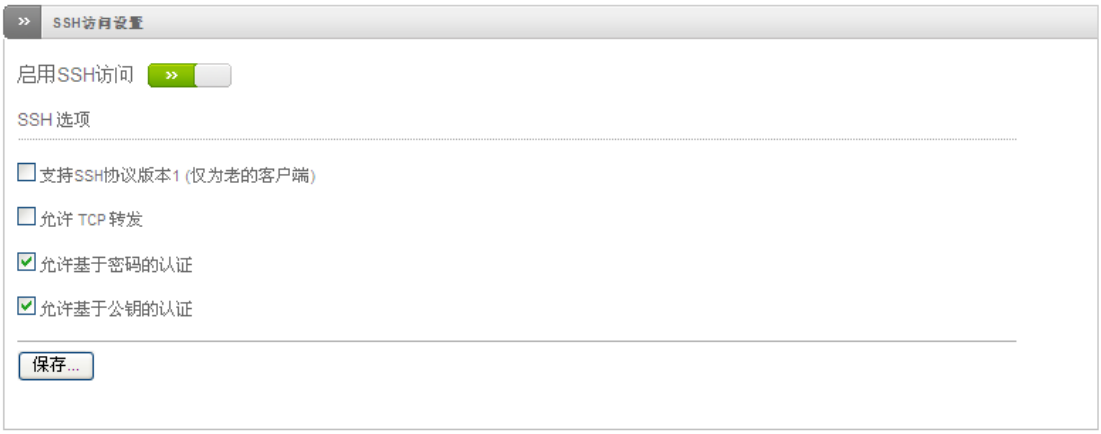
运行命令



4.1.5. SSH 访问

系统 > SSH 访问,如下图所示：

SSH 访问

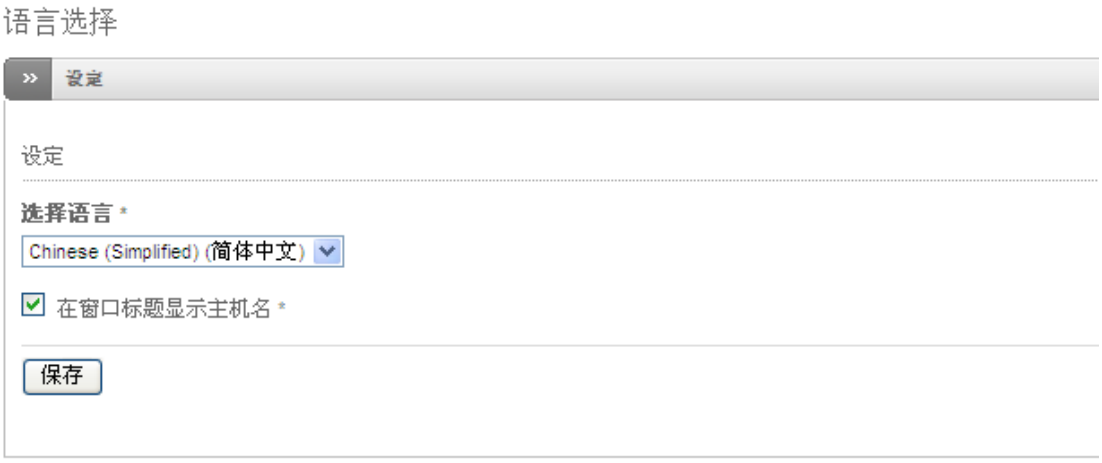


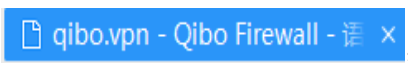
有时候我们需要登录启博 VPN 后台做一些调整或设置，SSH 是我们常用的访问后台的一种方式。如果是需要通过外网使用 SSH 访问该设备，还需要通过在防火墙--系统访问里添加相应的防火墙规则才可以通过 WAN 接口 ssh 远程登录 VPN 网关。

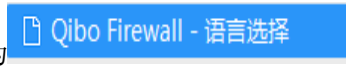
注意：开放 ssh 服务，有一定的危险性，建议使用时才打开，使用完就关闭它。

4.1.6. 语言选择

系统 > 语言选择 > 在这里，你可以选择你喜欢的语言，可选择英语和简体中文两种语言，如下图所示：



小提示：在窗口标题是否显示主机名，如果勾选了的显示是： 

；如果是不勾选，则显示为 

4.1.7. 系统备份

系统 > 系统备份，这里可以把所有配置信息做备份，如下图所示：

点击新建备份，来对当前 VPN 网关的系统配置做一备份，以备将来还原所用。

同时我们也可以在这里把以前的正确配置导入到设备中，如下图示

如果我们清空设备里的所有配置，将设备恢复到刚出厂的时候状态，可以通过下面的恢复出厂按钮来实现

自 动 备 份

系统 > 系统备份 > 自动备份，如需启用，一定要把启用打“√”根据需要进行设置即可。如下图所示：

4.1.8. 关机

系统->关机,可通过这里，关闭设备或重启设备，如下图所示：

VPN 网关就像我们个人电脑，有时工作时间太了，重启一次可以运行的更快，我们这里可以手动重启设备，或者制定设备自动重启计划，让设备在设定的时间自动重启。

4.1.9. 产品授权信息

系统 > 授权信息，如下图所示：

4.2. 状 态

4.2.1. 系统状态

系统状态里可以查看系统服务运行状态，内存、磁盘使用情况，设备运行时间及当前登录用户，引导模块信息及当前系统的内核版本情况。如下图示：

4.2.2. 网络状态

网络状态主要是显示 VPN 网关设备接口连接情况，DHCP 地址分配信息、系统路由表信息及 ARP 表入口。

网络链接状态信息

接口 | 当前的动态租约 | NIC状态 | 路由表条目 | ARP 表入口

» 接口

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 100
    link/ether 00:e0:4c:46:df:ee brd ff:ff:ff:ff:ff:ff
    inet6 fe80::2e0:4cff:fe46:dfee/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 100
    link/ether 00:e0:4c:46:df:ef brd ff:ff:ff:ff:ff:ff
    inet6 fe80::2e0:4cff:fe46:dfef/64 scope link
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 100
    link/ether 00:e0:4c:46:df:f0 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::2e0:4cff:fe46:dff0/64 scope link
       valid_lft forever preferred_lft forever
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 100
    link/ether 00:e0:4c:46:df:f1 brd ff:ff:ff:ff:ff:ff
    inet 1.1.1.1/24 brd 1.1.1.255 scope global eth3
    inet6 fe80::2e0:4cff:fe46:dff1/64 scope link
       valid_lft forever preferred_lft forever
1113: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 00:e0:4c:46:df:ee brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/24 brd 192.168.10.255 scope global br0
14: tap0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 100
    link/ether 12:7d:c2:df:87:51 brd ff:ff:ff:ff:ff:ff
    inet 10.2.0.1/24 brd 10.2.0.255 scope global tap0
    inet6 fe80::107d:c2ff:fedf:8751/64 scope link
       valid_lft forever preferred_lft forever
15: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1492 qdisc pfifo_fast state UNKNOWN qlen 3
    link/ppp
    inet 58.60.67.137 peer 58.60.64.1/32 scope global ppp0
```

4.2.3. 实时流量

可以显示当前网络中，流量最大的前 20 台电脑的 IP 地址及实时上传和下载速率，我们可根据这里的显示内容找出来哪些人的电脑在占用大量带宽。进而对其进行限制或警告，保证单位宽带的合理利用。

网络流量曲线图

» Green graph

IP 地址	上传(KB/秒)	下载(KB/秒)	总值(KB/秒)
192.168.10.253	13.605	6.603	20.208
192.168.10.249	1.957	4.027	5.984
192.168.10.108	0.428	0.185	0.613
192.168.10.254	0.496	1.822	2.318
192.168.10.251	0.122	0.473	0.595
192.168.10.252	0.000	0.005	0.005
192.168.10.250	0.000	0.000	0.000

4.2.4. 代理访问

采用代理方式访问互联网的情况，需要启用后面的代理功能才有效。

代理访问曲线图

4.2.5. 连接状态

这里可以查看局域网中的电脑连接互联网的情况，可以看到内网 IP、源端口、目的地 IP、目的地端口、协议、状态及到期时间。

连接状态

使用iptables连接跟踪

标签: 局域网 互联网 DMZ 无线 Qibo Firewall VPN (IPsec)

源IP	源端口	目的地IP	目的地端口	协议	状态	到期
192.168.10.253	61675	101.226.140.159	443 (HTTPS)	tcp	ESTABLISHED	119:59:59
192.168.10.108	4790	183.60.48.250	80 (HTTP)	tcp	ESTABLISHED	119:59:59
127.0.0.1	54295	127.0.0.1	32000	tcp	ESTABLISHED	119:59:59
192.168.10.108	4826	42.156.152.79	16000	tcp	ESTABLISHED	119:59:59
192.168.10.253	58379	14.17.33.218	80 (HTTP)	tcp	ESTABLISHED	119:59:59
192.168.10.254	3967	119.147.32.233	80 (HTTP)	tcp	ESTABLISHED	119:59:59
192.168.10.254	3960	120.196.212.94	80 (HTTP)	tcp	ESTABLISHED	119:59:59
192.168.10.108	4766	183.60.48.250	80 (HTTP)	tcp	ESTABLISHED	119:59:59
192.168.10.254	4539	14.17.41.165	443 (HTTPS)	tcp	ESTABLISHED	119:59:58
192.168.10.253	55449	120.196.212.86	80 (HTTP)	tcp	ESTABLISHED	119:59:58
192.168.10.108	4778	183.60.48.250	80 (HTTP)	tcp	ESTABLISHED	119:59:57
192.168.10.108	4752	183.60.48.250	80 (HTTP)	tcp	ESTABLISHED	119:59:55
192.168.10.253	55519	120.196.212.86	80 (HTTP)	tcp	ESTABLISHED	119:59:53
192.168.10.251	1088	115.29.11.219	5222	tcp	ESTABLISHED	119:59:51
192.168.10.254	4007	42.156.152.146	16000	tcp	ESTABLISHED	119:59:50

4.2.6. SSL VPN 连接

这里显示该台启博 VPN 网关，做为 SSL VPN 服务器端，异地远程连到到这台设备上的 VPN 连接信息。

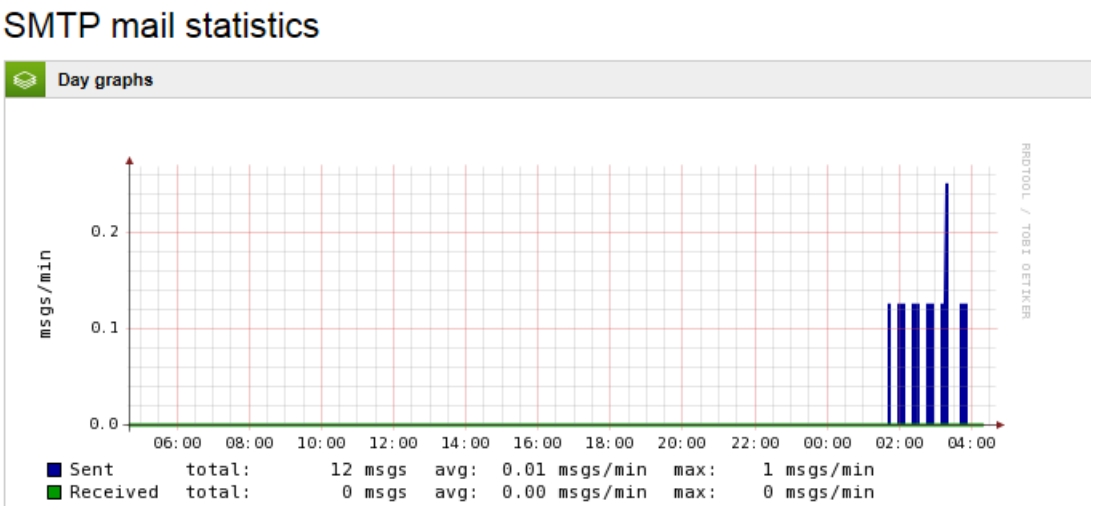
SSL VPN连接状态及控制

连接状态及控制

用户	已分配IP地址	实际IP地址	接收 / 发送	从 开始已连接	运行时间	活动/动作
beijing	10.2.0.2	123.117.83.109	5 KiB / 6.9 KiB	Fri Jan 30 11:24:27 2015	11m	kill

4.2.7. 发送邮件统计

通过该 VPN 网关发送邮件的一个大致统计。



4.2.8. 邮件队列

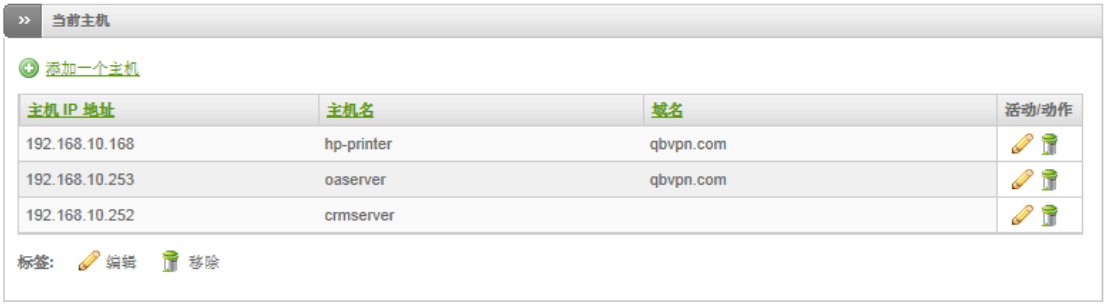
当前还没有发送或没有发送成功的邮件条目。

4.3. 网 络

4.3.1. 主机设置

主机配置功能类似于 DNS 服务器，我们可以预定义一些条目来实现满足测试的需要，或者在 DNS 服务器工作不正常时，做为 DNS 服务器的补充，矫正一些不正常的 DNS 解析，尤其在 VPN 的网络里可以起到通过机器名对服务器访问。

主机配置



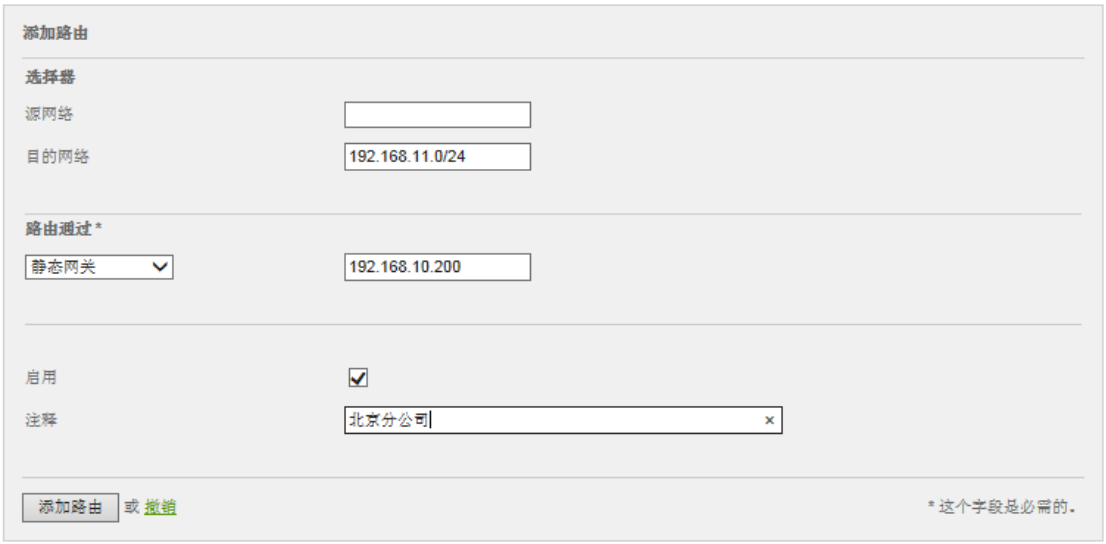
例如我们这里定义了 oaserver.qbvpn.com 这个域名对应的 IP 是 192.168.10.253，我们做一下 Ping 测试

从返回结果来看，刚才定义主机设置工作正常。

4.3.2. 路由

4.3.2.1. 静态路由

我们可以根据需要设定一些静态路由表，达到访问的需要。



- 源网络：是指发起方的网段
- 目的网络：是指目的地址的网段，如 192.168.11.0/24
- 路由通过：是指下一跳的地址，可以是一个 IP 或 vpn 用户名或某一上行线路
- 启用：只有选中该项后本条目所设置的静态路由规则才能生效。
- 注释：对本条目路由规则做一下备注说明

4.3.2.2. 策略路由

策略路由多应用于多条上行宽带时，为不同的内网 IP 设置不同的网络出口，比如有中国电信、中国联通、中国移动三条宽带时，我们可根据不同的目的地址，选择不同的网络出口，电信的服务器走电信的线路，联通的服务器走联通的线路，移动的服务器走移动的线路。

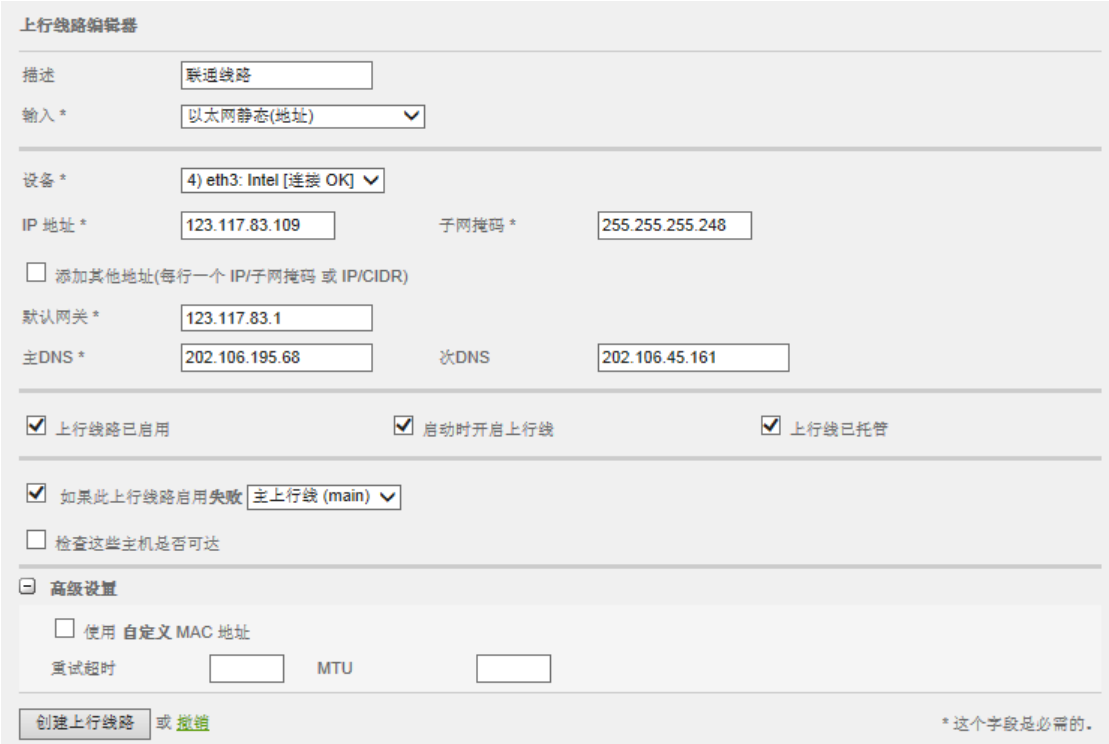
我们新建一条策略路由，让目的地址为电信的访问通过中国电信的线路出去。

- 源：指源地址，可以为任意、网络接口、VPN 用户、网络/IP、MAC 地址等。
- 目标：指我们要访问的目标地址为任意、VPN 用户、网络/IP。
- 服务：里面有些常用的服务定义可供选择。
- 协议：可选任意、TCP、UDP、TCP+UDP、ESP、GRE、ICMP 等。
- 目的地端口：所要访问用到的目的地端口，可以输多个，一行一个。
- 经由途径：策略路由的出口，可以为静态网关、上行线路、VPN 用户。
- 服务类型：可根据需要进行选择，非专业用户可以直接用未定义即可。
- 注释：对这条策略路由进行备注说明。
- 启用：只有选中该项后本条目所设置的静态路由规则才能生效。
- 记录所有接受的包：记录所有受这条路由策略影响的数据包，可能会造成日志文件太多，非特殊需要，不建议选择。

4.3.3. 接 口

网络 -> 接口 -> 上行线路编辑器，在这里可以修改上网设置的参数.也可以这里创建新的上网线路，如下图所示：

我们创建一条上行线路，取名为联通线路，上网方式为以太网静态（地址）。



- 输入：宽带的连接类型，一定不能选错。
- 设备：是指新添加的宽带接在 VPN 网关的哪个网络接口上面。
- 如果此上行线路启用失败：用于如果此宽带连接出错时，该宽带上的流量转到另一条线路上去，启动线路备份的作用。
- 使用自定义 MAC：有些 ISP 运营商会绑定上网设备的 MAC 地址，有里需要进行 MAC 克隆才能上网。

4.4. 服务

4.4.1. DHCP 服务器

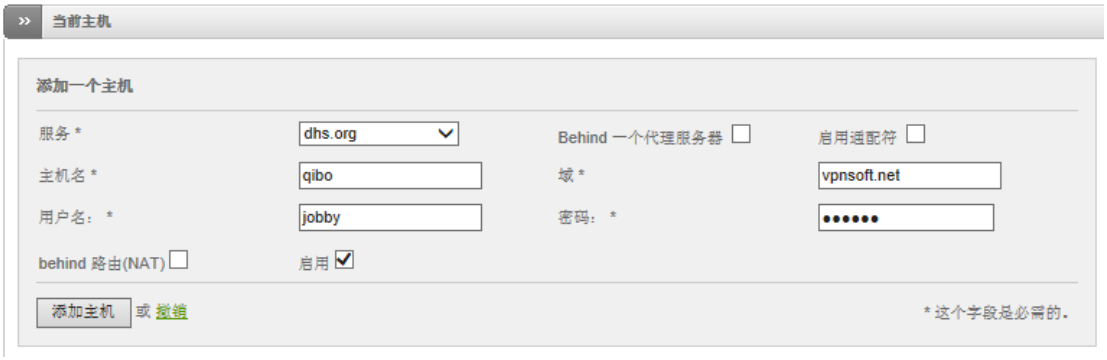
服务 > DHCP 服务器,如果启用那么要把启用选项打“√”配置完记得单击“全部保存”配置界面如下图所示：

固定租约：有时我们需要给某些设备分配固定的 IP 地址，避免由于 IP 地址变化造成管理的不便，我们可以根据设备的 MAC 地址给他们分配一下固定的 IP 地址，这样这台设备每次都可以获取到相同的 IP 地址了。

4.4.2. 动态域名

服务->动态域名，添加完记得单击“添加主机”，配置界面如下图所示：

动态域名



- 服务：选择动态域名的服务商。
- 主机名：比如 qibo.vpnsoft.net 的主机名就是 qibo 。
- 域：比如 qibo.vpnsoft.net 的域就是 vpnsoft.net 。
- 用户名：申请该动态域名时所使用的用户名。
- 密码：申请该动态域名帐号时所使用的密码。

4.4.3. Clam 防病毒

服务->Clam 防病毒，此项为另付费项目，配置界面如下图所示：

4.4.4. 系统时间

服务->系统时间,设置界面如下图所示:

这里主要注意时区一定要选择对，系统会自动较正设备时间，如果是其他原因设备时间不准确时，可以使用下面的手动调整来设置系统时间。特别是 VPN 应用时，涉及到加密解密时一定要保证系统时间的准确，否则会出现证书出错，vpn 无法连接。

4.4.5. 邮件过滤

服务->邮件过滤,如下图所示:

4.4.6. 入侵防御系统

服务->入侵防御,如需启用点一下“启用入侵防御系统”，如下图所示:

启博 VPN 网关集成入侵检测系统（IDS）和预防防御系统 SNORT，它是基于 iptables，自动拦截掉不必要的或不信任的来源连接。

4.4.7. 网络流控分析

服务->网络流控,如有需要可启用,如下图所示:

4.4.8. SNMP 服务器

SNMP 是用来监视网络连接的设备，例如，去控制内网中的基础网络的状态。,如下图

所示:

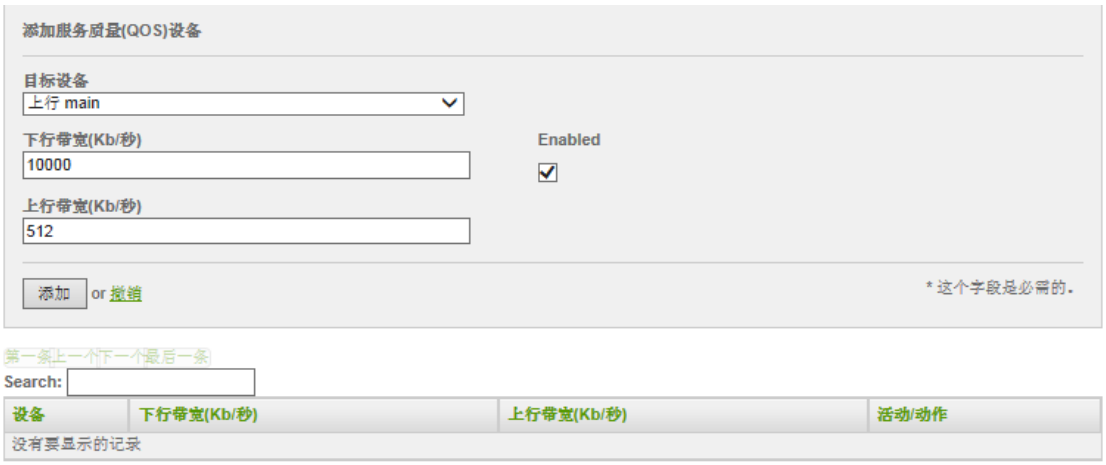
- 团体字符串：从 SNMP 客户端读取数据所需要的密钥
- 位置：字符串标识符，可以为任何字符，但是建议描述本台设备以区别于其它设备。
- 优先于全局通知电子邮件地址：勾选后，默认以下面所输入的电子邮件做为 snmp 服务器联系的邮件地址。

4.4.9. 智能 QoS

智能 QoS（Quality of Service，服务质量）是用来解决网络延迟和阻塞等问题的一种技术。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行，如下图所示:

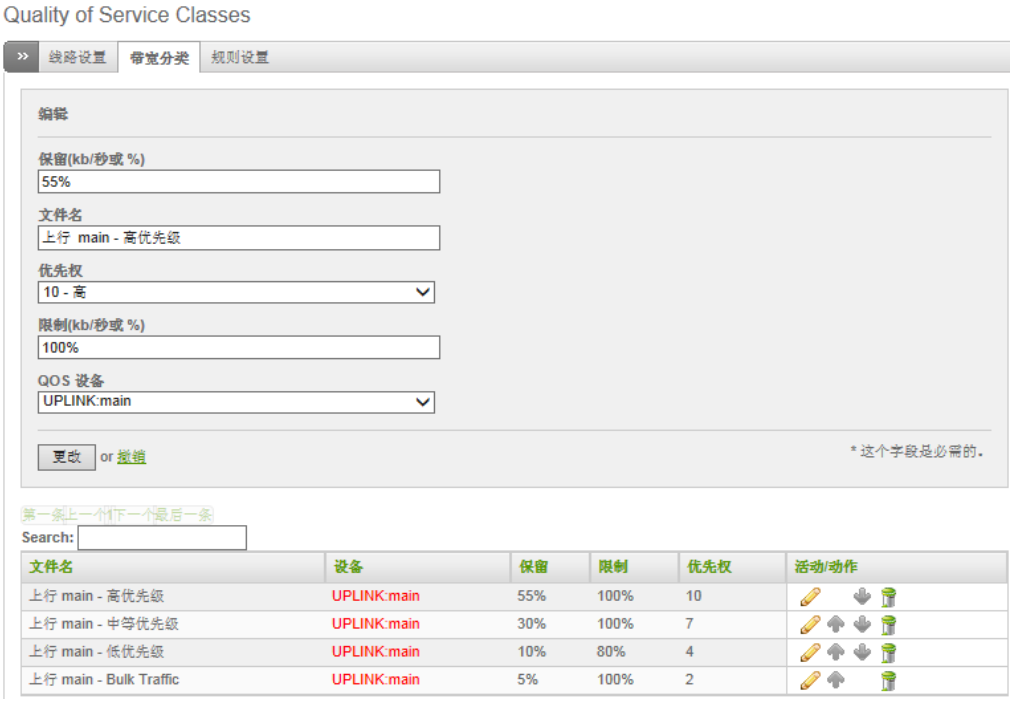
4.4.9.1. 线路设置

比如我们以下行 10M 上行 512Kb 的宽带，定义参数如下：



4.4.9.2. 带宽分类

根据需要调整不同应用分配的所占宽带的网速比例，可根据需要自行设置。



4.4.9.3. 规则设置

举例给 http 服务，即网页浏览优先流畅，只需按下图设置

4.5. 防火墙

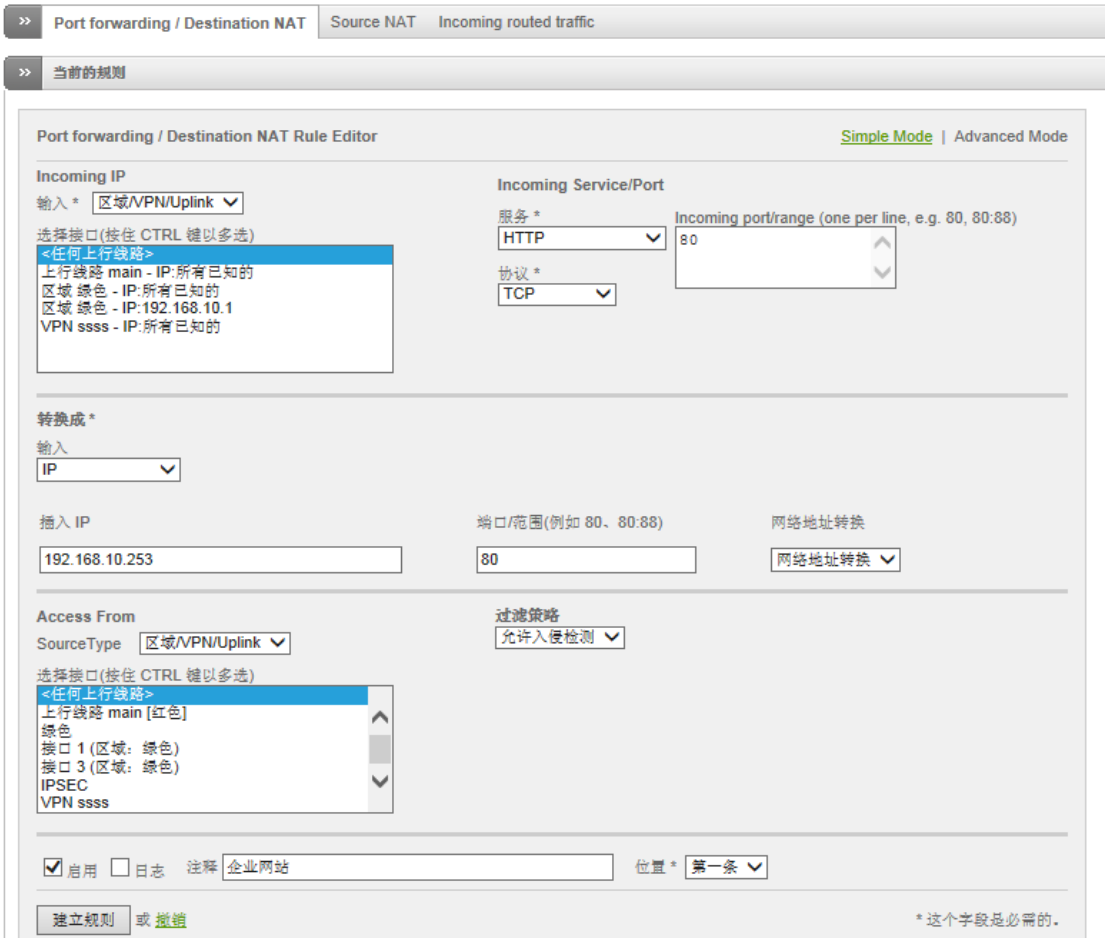
4.5.1. 转发规则

用于管理互联网通过上行线路访问启博VPN网关的应用程序或访问VPN网关后的服务器的进入和流出数据。如下图示

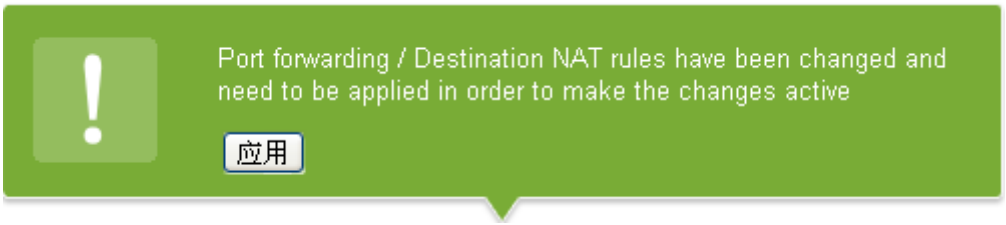
4.5.1.1. Portfording/Destination NAT

Portfording/Destination NAT（端口转发/目标地址转换），当内部需要提供对外服务时（如

对外发布 web 网站），外部地址发起主动连接，由 VPN 网关接收这个连接，然后将连接转换到内部，此过程是由带有公网 IP 的网关替代内部服务来接收外部的连接，然后在内部做地址转换，主要用于内部服务对外发布。



一旦规则被创建后，必须将规则应用到设备，点击“**应用**”按钮。如下图所示：

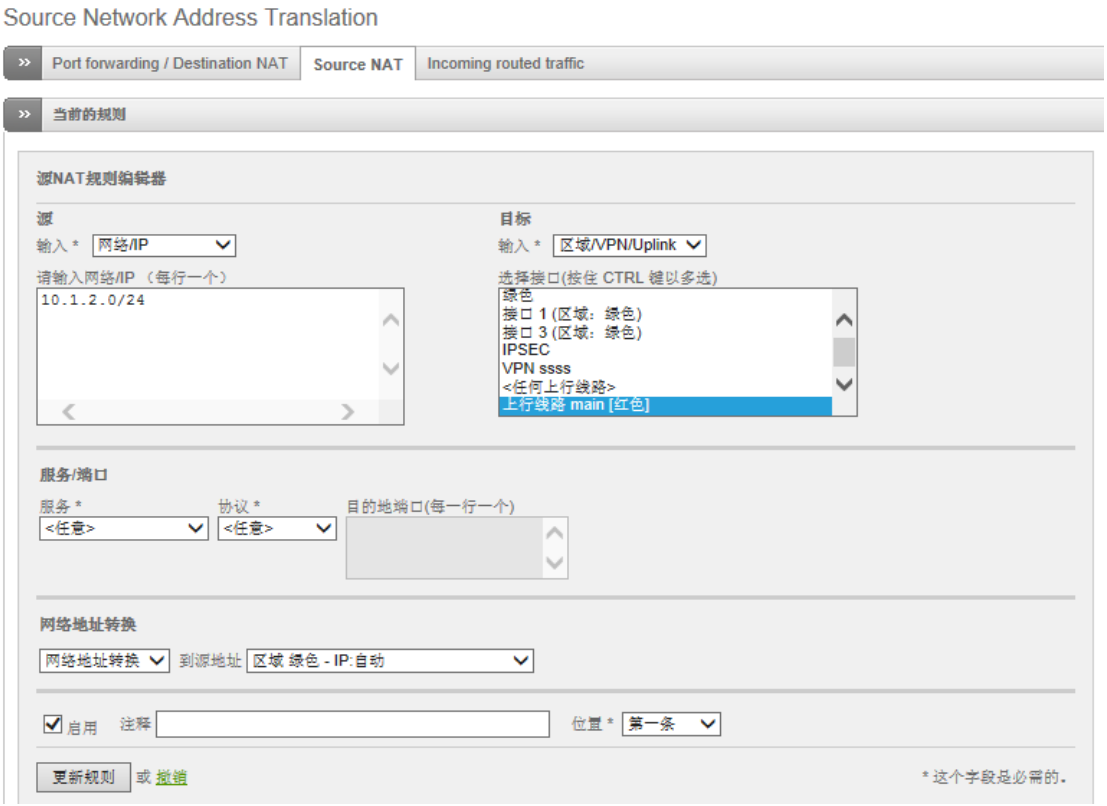


4.5.1.2. Source NAT

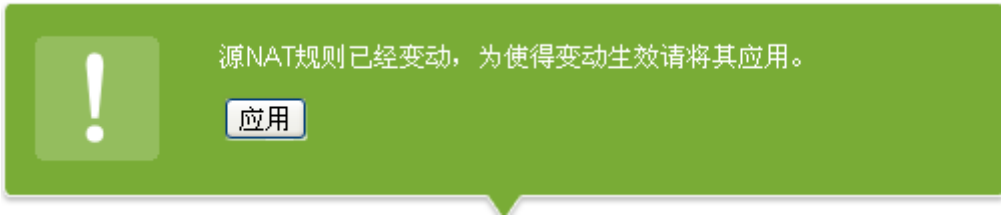
Source NAT(源网络地址转换)内部地址要访问公网上的服务时（如 web 访问），内部地址会主动发起连接，由 VPN 网关上的网关对内部地址做个地址转换，将内部地址的私有 IP 转换为公网的公有 IP，网关的这个地址转换称为 Source NAT，主要用于内部共

享 IP 访问外部。

此页面根据需求进行相应的配置即可。配置完记得单击“**建立规则**”界面如下图所示：



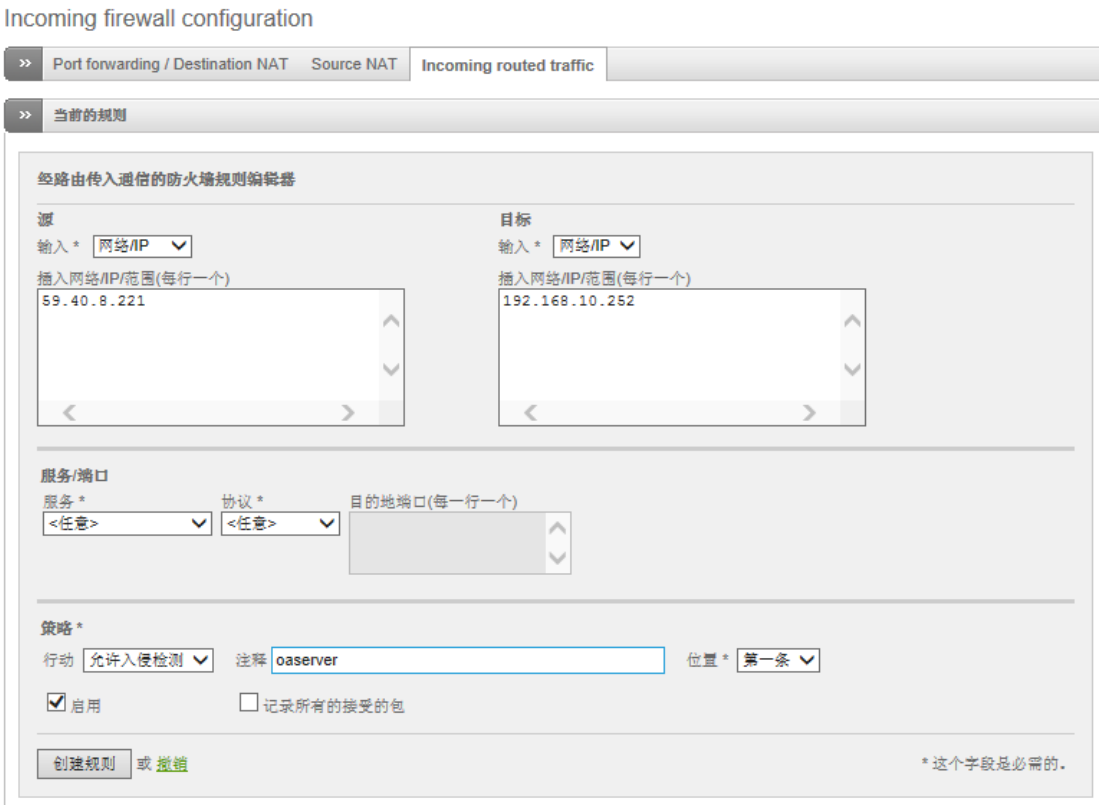
一旦规则被创建后，必须将规则应用到设备，点击“**应用**”按钮。如下图所示：



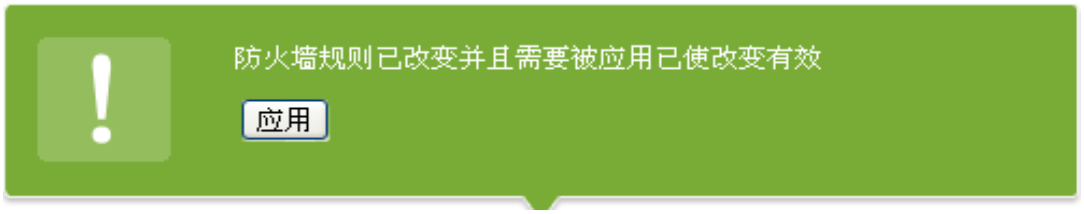
4.5.1.3. Incoming routed traffic

Incoming routed traffic(入站路由流量) 主要用于外网多地址管理，比如光纤上网的客户，经常有多个公网 IP 地址，可以将每一个公网 IP 地址和内网中的一台服务器进行一对一映射，对外提供服务,如下图所示:

此页面根据需求进行相应的配置即可。举例我们把其中的一个公网 IP 地址：59.40.8.221 映射给 192.168.10.252 的 OA 服务器，我们单击“创建规则”如下图所示：



一旦规则被创建后，必须将规则应用到设备，点击“应用”按钮。如下图所示：



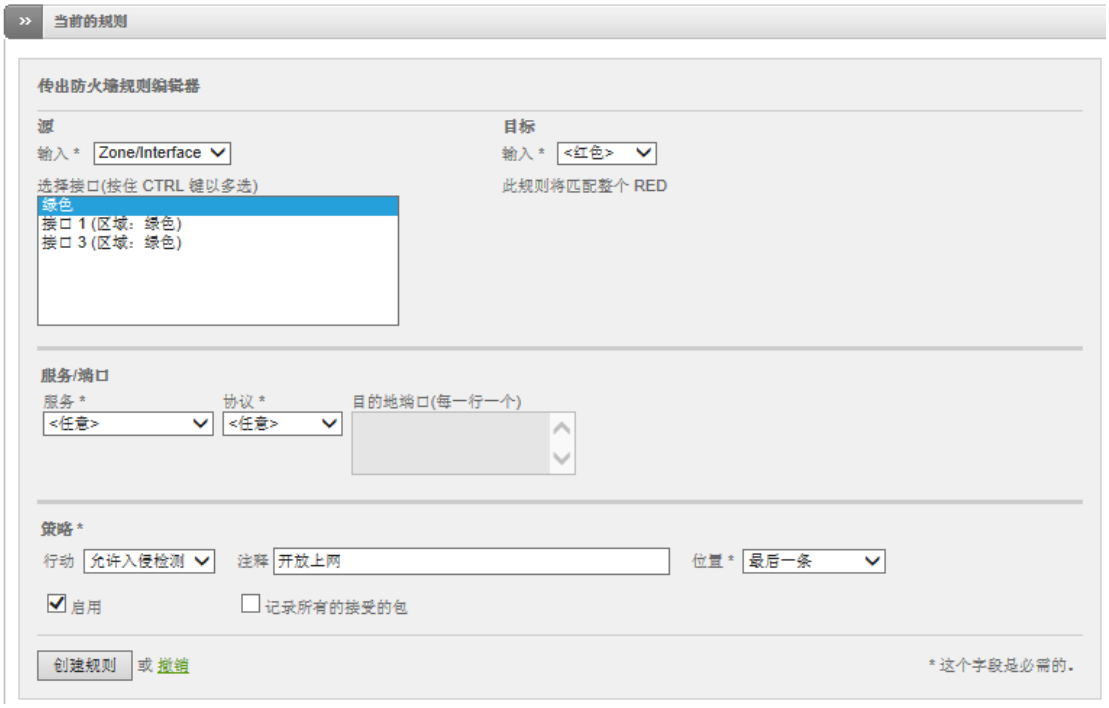
4.5.2. 流出访问

流出访问是指允许内网计算机用户访问外部互联网的规则，启博 VPN 防火墙只开放了常用的 80、53、21、443、25、110 等常用访问，如里需要开通其他服务，可自行添加规则。

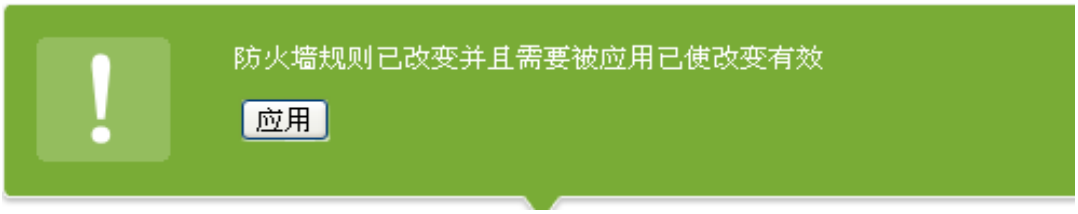
流出访问

首先要开启对外防火墙,然后单击“添加一个新的防火墙规则”如下图所示:

流出访问



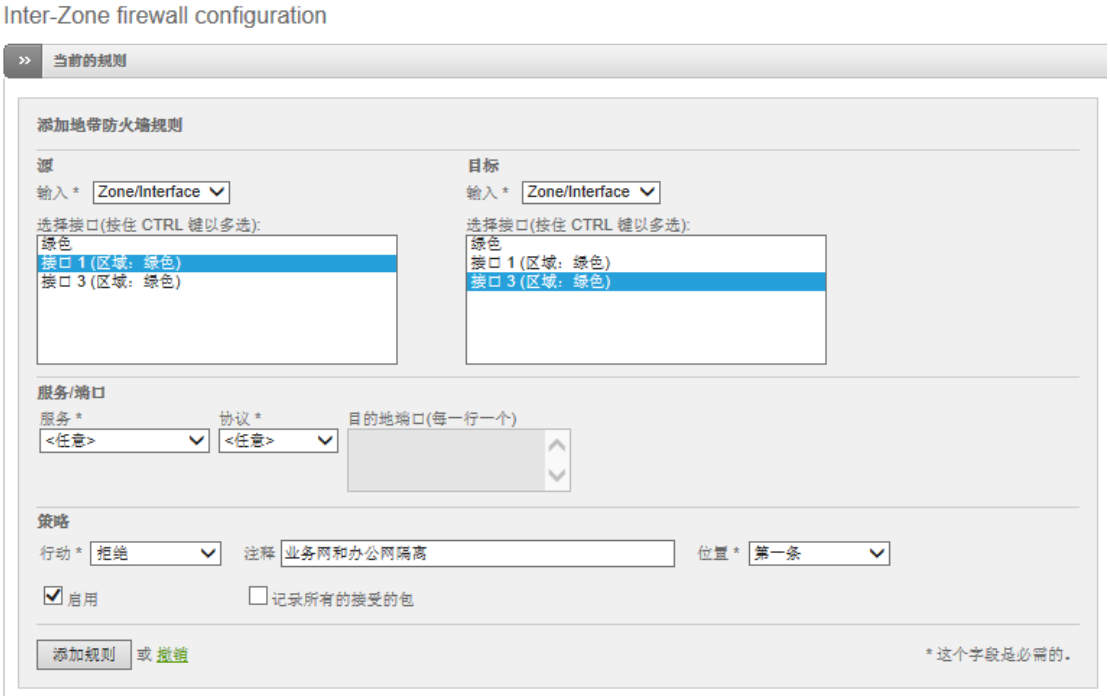
规则被创建后，必须将规则应用到设备，点击“**应用**”按钮。如下图所示：



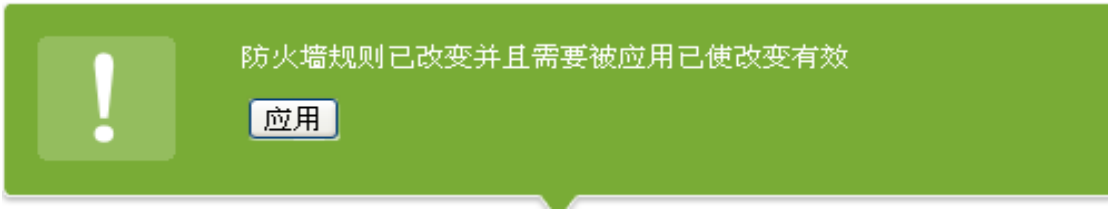
4.5.3. 区间访问

区间防火墙，主要是用于内网区域之间或内网 IP 之间的防火墙规则，首先要打开地区间防火墙，然后单击“添加一个新的地区间防火墙规则”如下图所示：

此页面根据需求进行相应的配置即可。配置完记得单击“**添加规则**”界面如下图所示：

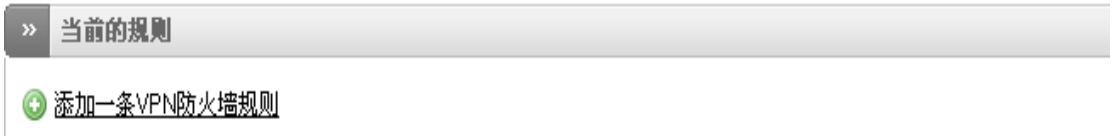


规则被创建后，必须将规则应用到设备，点击“应用”按钮。如下图所示：

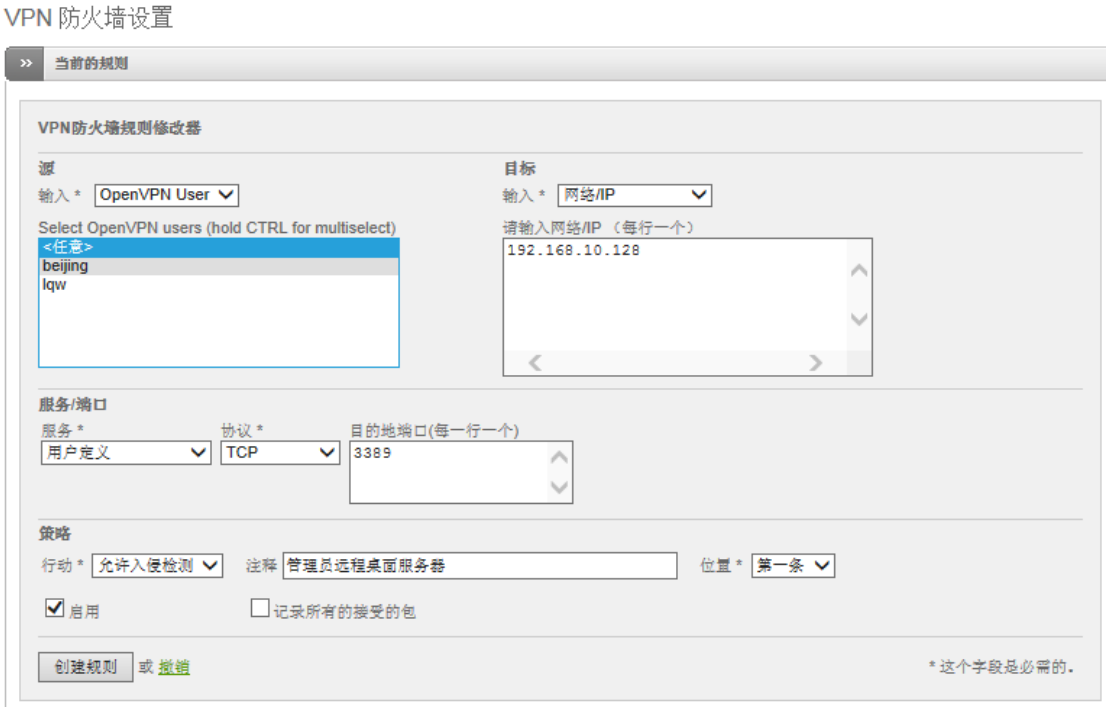


4.5.4. VPN 访问

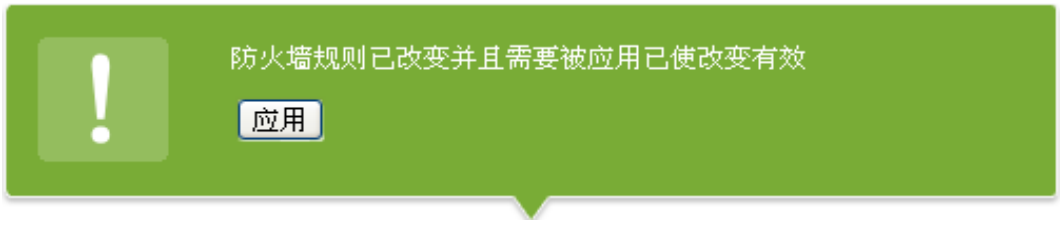
VPN 防火墙，用于 VPN 用户和内网区域或其它区域之间的防火墙规则,如果需要对 VPN 访问内网做细致权限管理，可以使用 VPN 防火墙设置。



此页面根据需求进行相应的配置即可。配置完记得单击“创建规则”界面如下图所示：

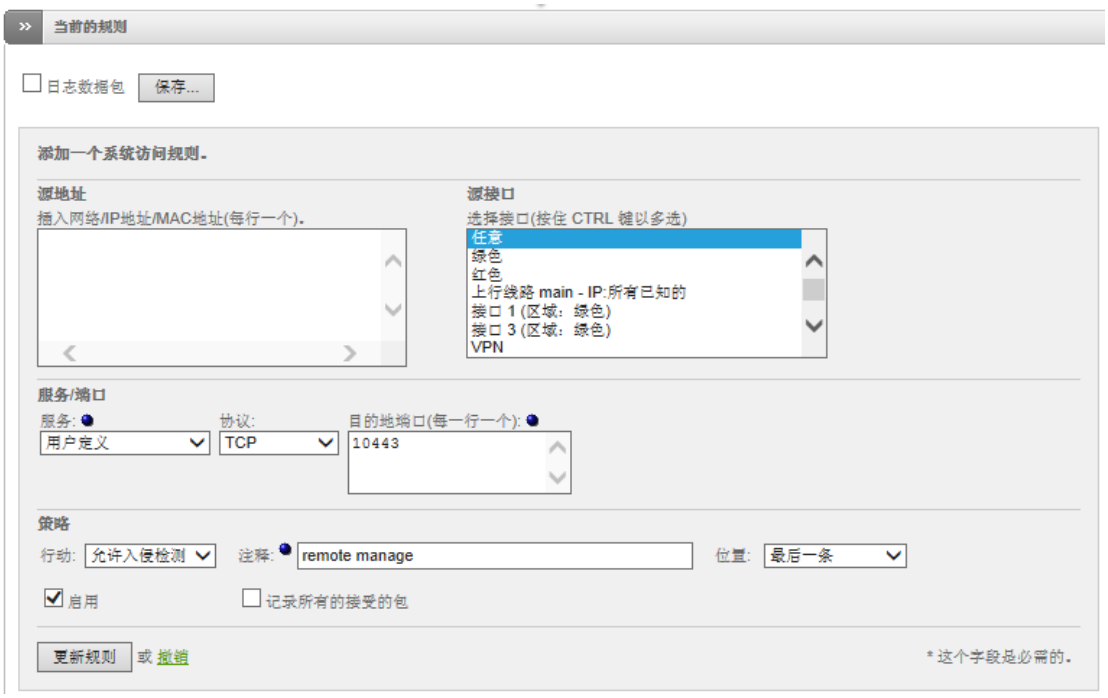


规则被创建后，必须将规则应用到设备，点击“应用”按钮。如下图所示：



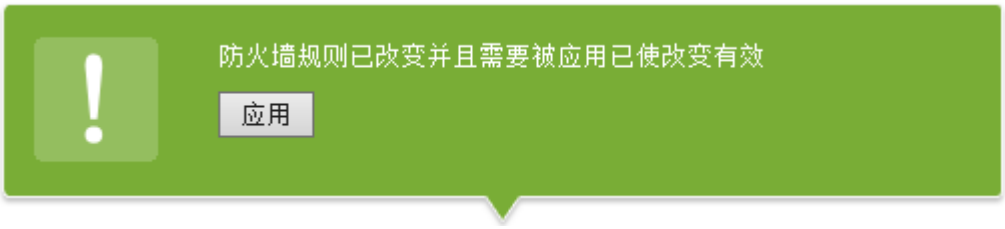
4.5.5. 系统访问规则

防火墙 > 系统防问,这里是添加管理该系统的规则，例如我们经常用到在家里或其他地方想管理公司的 VPN 设备，我们可以单击“添加一个新的系统访问规则”，如下图所示：



- 源地址：发起连接方的使用的 IP 地址。
- 源接口：发接连接方连接启博 VPN 网关时，使用的 VPN 网关网络接口。
- 服务/端口：要访问的服务名称，协议，端口号。
- 行动：允许入侵检测、允许、拒绝、丢弃四个选择根据需要选择。
- 注释：对该条规则的注解说明
- 位置：这条规则位于规则列表中的序列位置。
- 启用：只有启用了该条规则才生效。
- 记录所有的接受的包：日志文件会记录有关这条规则的所有日志信息。

规则被创建后，必须将规则应用到设备，点击“**应用**”按钮，配置才升效。如下图所示：



这样就可以远程管理 VPN 网关了。

4.5.6. IP/MAC 绑定

IP/MAC 绑定是防止 IP 盗用，通过 MAC 地址控制方式实现控制内网设备上网的一种常用手段，启博 VPN 网关支持 IP/MAC 地址绑定功能。

- 没有绑定 MAC 和 IP 机器无法上网。
- 绑定了 MAC 和 IP 地址的机器可以上网，但是如果修改了 IP 或 MAC 就不能上网。
- 只有 IP 和 MAC 地址严格对应了，才可以上网。

4. 6. 代理

4.6.1. HTTP 代理

4.6.1.1. 参数设置

参数设置，开启 HTTP 代理服务，如下图所示：

此页面为开启 HTTP 代理服务的界面，根据需求进行相应的配置即可，配置好点击“ **保存**”，然后点击“ **应用**”更改继续。

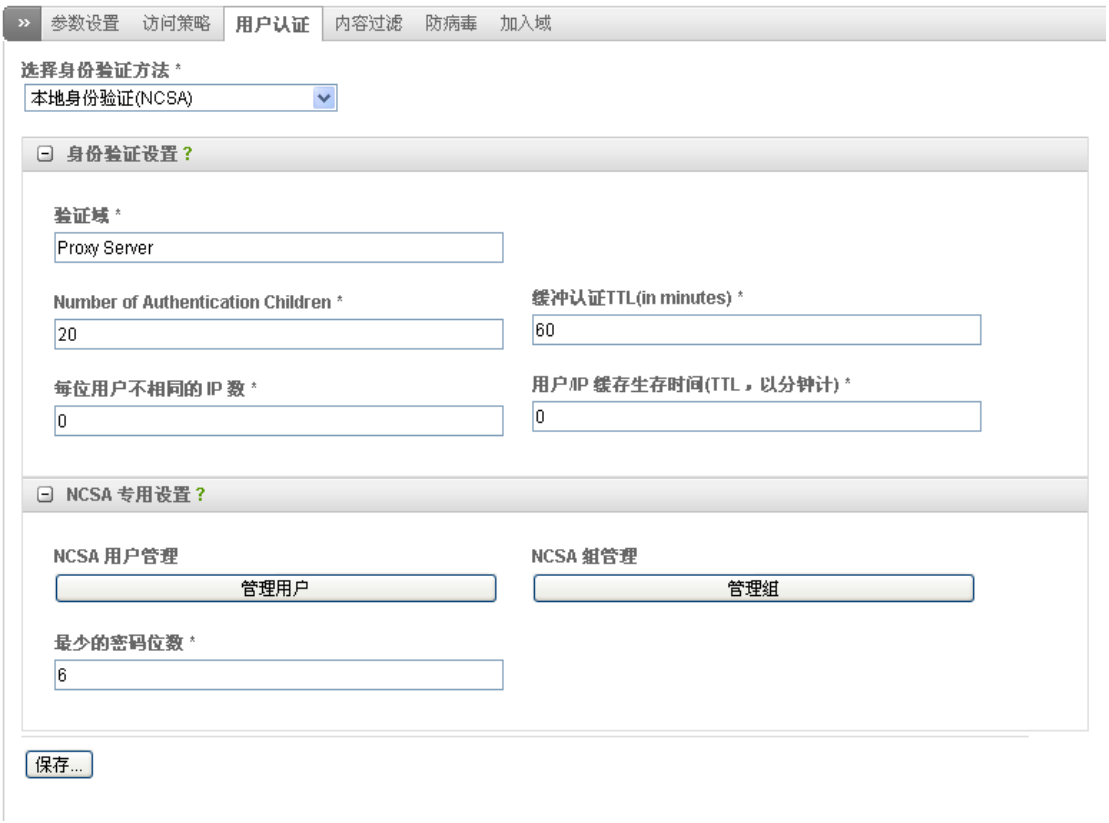
4.6.1.2. 访问策略

代理 > HTTP > 访问策略，单击“添加访问策略”。

此页面根据需求进行相应的配置即可。配置完记得单击“**创建策略**”界面如下图所示：

4.6.1.3. 用户认证

代理 > HTTP > 用户认证，根据所需进行设置，设置完记得单击“**保存**”按钮，界面如下图所示：

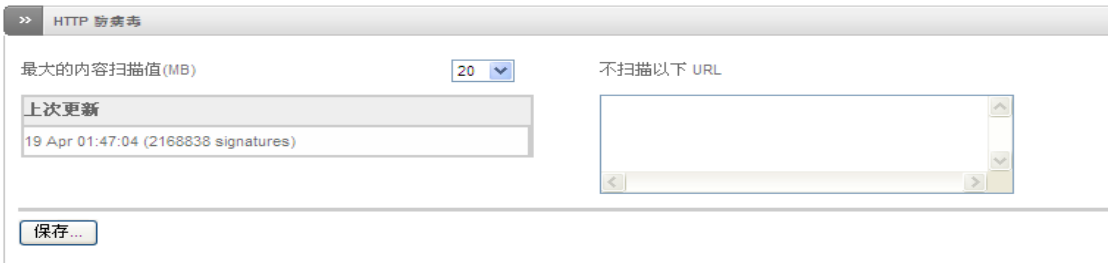


4.6.1.4. 内容过滤

代理 > HTTP > 内容过滤，根据需要，单击活动动作进行编辑，如下图所示：

4.6.1.5. 防病毒

代理 > HTTP > 防病毒,如下图所示:



4.6.1.6. 加入域

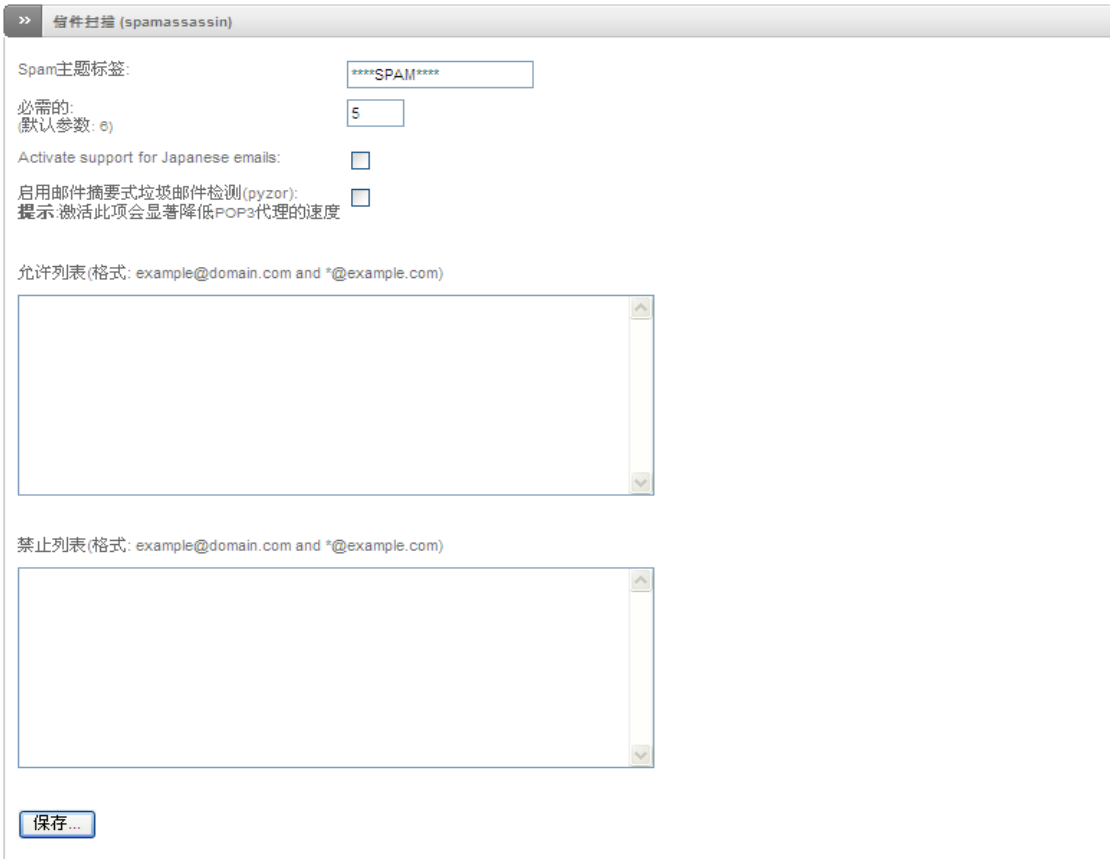
代理 > HTTP > 加入域,如下图所示:

4.6.2. POP3 代理

4.6.2.1. 全局设置

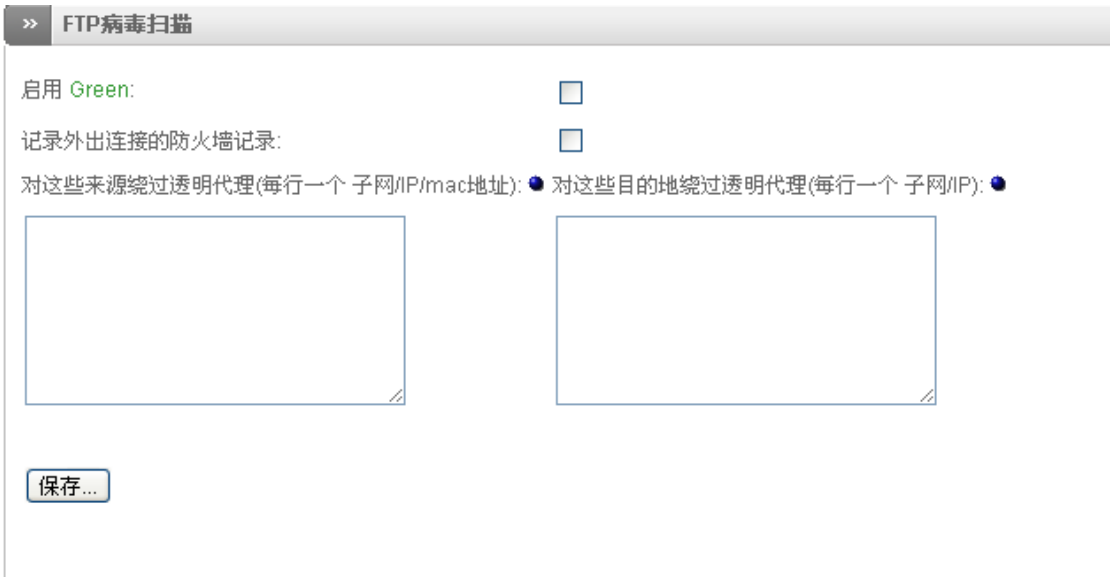
4.6.2.2. 垃圾邮件过滤器

代理 > POP3 > 垃圾邮件过滤器,根据需求进行设置，如下图所示：



4.6.3. FTP 代理

代理 > FTP,根据需求进行设置,界面如下图所示:



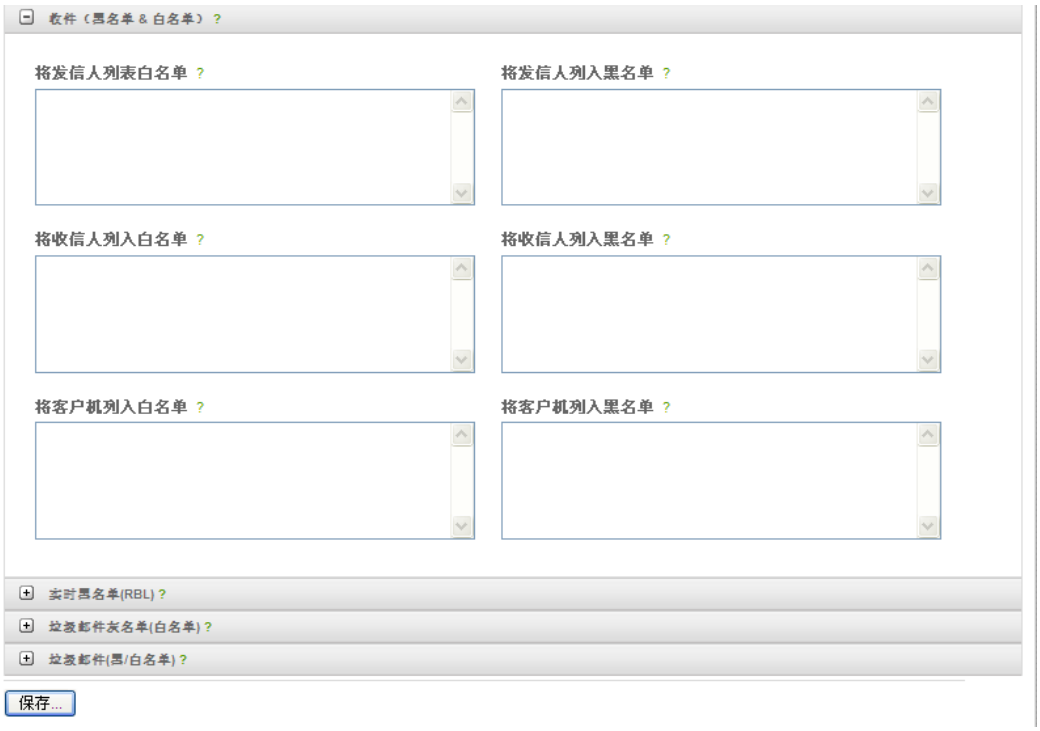
4.6.4. SMTP 代理

4.6.4.1. 参数设置

代理 > SMTP > 参数设置，单击“启用 SMTP 代理”。根据需要进行设置，界面如下所示：

4.6.4.2. 黑名单&白名单

SMTP > Black-&whitelists,根据需要进行设置，如下图所示：



4.6.4.3. Incoming Domain

Incoming Domain(入站域名)，入站域名设置后，要发送邮件需要转发到 VPN 网关下的邮件服务器，通常是位于 DMZ 区域，它需要声明 SMTP 代理所接受的域名同时相应域名的邮件将被转发，可以指定多个邮件服务器通过不同的域名。

4.6.4.4. Mail Routing

此功能是将发送的邮件抄送一份给一个指定的邮箱或将接收到的邮件抄送一份给一个指定的邮箱，像当于邮件审查。

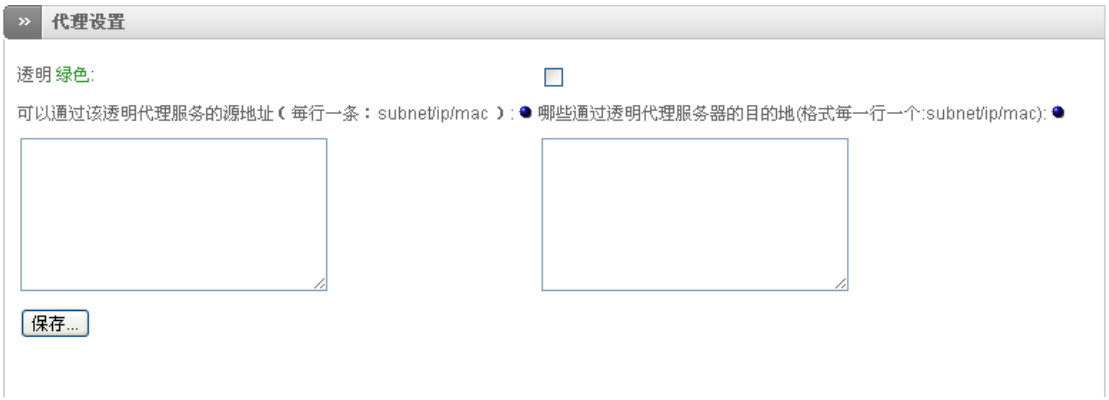
4.6.4.5. 高级设置

SMTP->高级设置，如下图所示：

4.6.5. DNS 代理

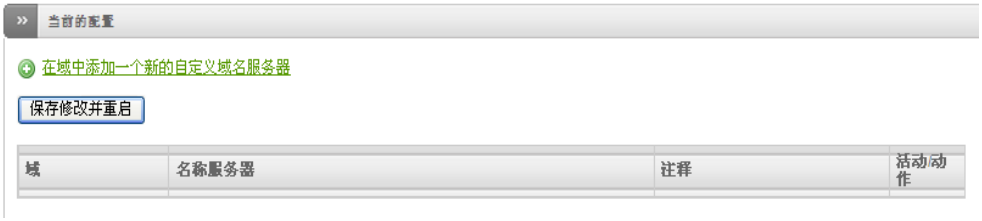
4.6.5.1. 代理设置

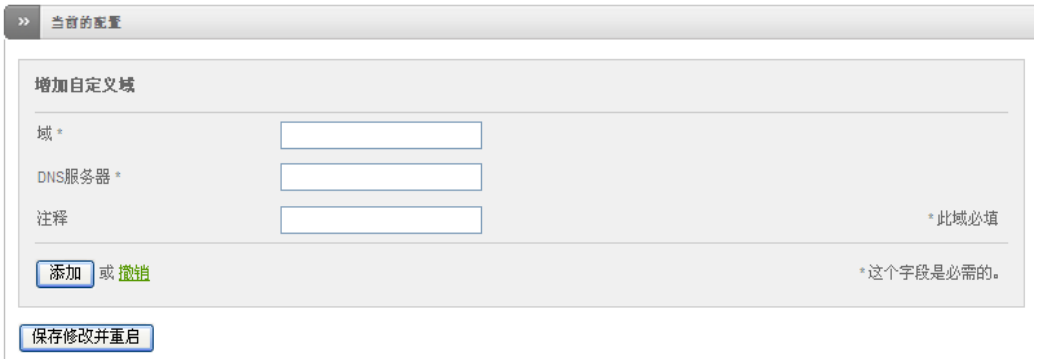
DNS->代理设置，根据需要进行设置，界面如下所示：



4.6.5.2. DNS Routing

DNS -> DNS Routing,单击“在域中添加一个新的自定义域名服务器”，根据需要进行设置就好了，配置好单击“保存修改并重启”如下图所示：





4.6.5.3. 反间谍软件

DNS > 反间谍软件,如有需求把启用打上“√”， 根据需要进行设置，如下图所示：

4.7. VPN 配置

4.7.1. SSL VPN 服务器

4.7.1.1. 全局设置

如果 VPN 产品部署在总部,从主菜单中，选择 VPN > SSL VPN 服务器,需要把开启 VPN 服务器选项打上“ √ ”,vpn subnet:是设备子网,可根据个人喜好进去修改,也可使用默认的.如下图所示：

- 开启 VPN 服务器：VPN 服务器的功能开关，打勾启用 VPN 功能，去掉勾关闭 VPN 功

能。

- 桥模式：桥模式开关，如果开启桥模式，VPN 服务器虚拟网卡和 VPN 网关 LAN 接口网卡进行桥接。
- 动态 IP 池开始地址：桥模式下，vpn 客户端可使用的地址池开始 IP 地址。
- 动态 IP 池结束地址：桥模式下，vpn 客户端可使用的地址池结束 IP 地址。
- VPN subnet：非桥接模式下，VPN 网络的网段，如 10.2.0.0/24 。

4.7.1.2. 帐户配置

接下来是创建账户,点击添加账户,添加账号关键的参数是：用户名和密码，这是远程客户端接入的凭证.创建好记得点“保存”.要不然系统是不作保存的。

点击添加帐户，来增加新的 VPN 接入帐户

4.7.1.3. 高级设置

接下来是高级设置，这里的端口号和协议便用默认的就可以了,全局推送选项根据实际进行填写,身份验证设置选择 PSK(用户名/密码)选项。

- 端口：VPN 连接时使用的端口号，默认为 1194，可以修改成其它未被使用的端口。
- 协议：VPN 封装协议，分 UDP 和 TCP 两种，客户端和服务器端要保持一致即可。
- 阻止来自隧道的 DHCP 应答：勾选此项，阻止来自于 VPN 另一端的 DHCP 服务应答，避免也本地 DHCP 服务器冲突。
- 允许客户端之间互联：勾选此项 VPN 客户端之间可以相互通信，反之则不能相互通信。
- 相同帐号允许多人同时连接：勾选此项，将允许多人共用一个 VPN 帐号进行连接。
- 推送这些网络：是指向 VPN 客户端推送服务器端内网网段路由，可以为多个网段。
- 推送这些域名服务器：将 VPN 内网中的域服务器地址推送给客户端。
- 推送域：向 VPN 客户端推送域名。

身份验证设置：

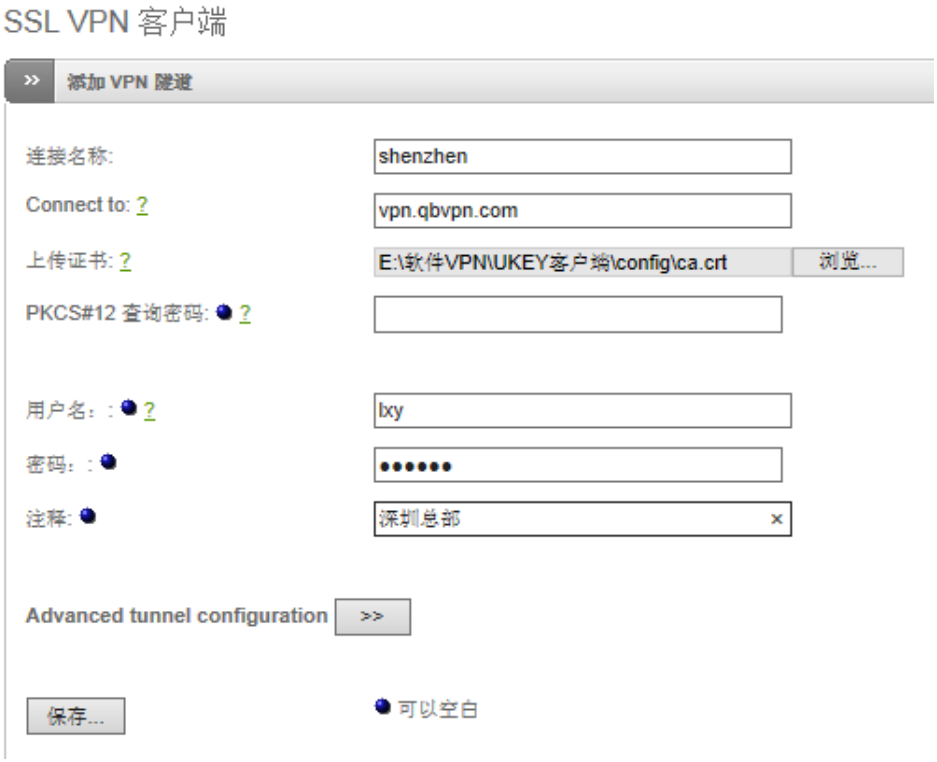
这里是对 VPN 客户端接入 VPN 服务器采用的哪种身份验证方式，一般选择 PSK(用户名/

密码)方式。

到此 SSL VPN 服务器的配置完成。

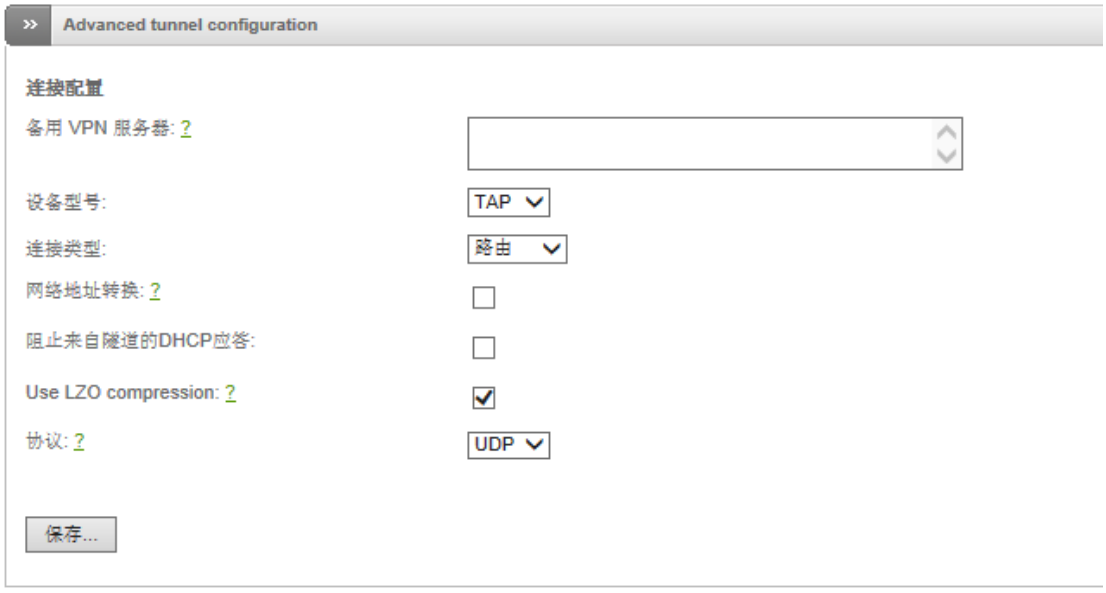
4.7.2. VPN 客户端

如果 VPN 产品部署在分部,从主菜单中，选择 VPN > SSL VPN 客户端,选择添加 VPN 隧道按钮开始创建客户端 vpn 账户,连接名称可随意填写，Connect to（域名）与在系统 > 网络设置里填写的一致,用户名和密码必须填写你在 VPN 服务器 > 账号里创建的,最后点击“保存”。



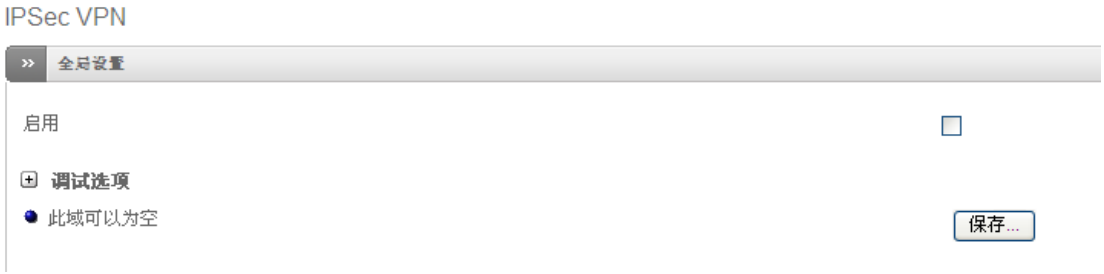
- 连接名称：可以任意填写，主要用于区别不同的 VPN 连接，只要不重复就可以了。
- Connect to: 是输入 VPN 服务器端的 IP 地址或域名。
- 上传证书：VPN 服务器所使用的 ca 证书。
- PKCS#12 查询密码：此项留空即可。
- 用户名：在 VPN 服务器端所建的帐户名密码。
- 密码：上一项用户名所输入帐户对应的密码。
- 注释：用于对此 VPN 连接进行备注说明。

高级设置



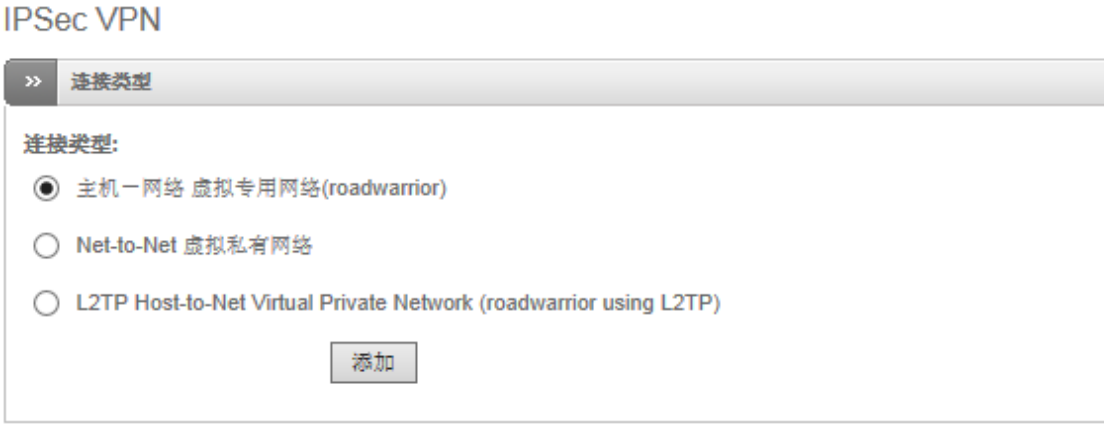
4.7.3. IPSEC VPN

从主菜单中，选择 VPN > IPSEC VPN，然后把启用选项打上“√”记得点击“保存”。



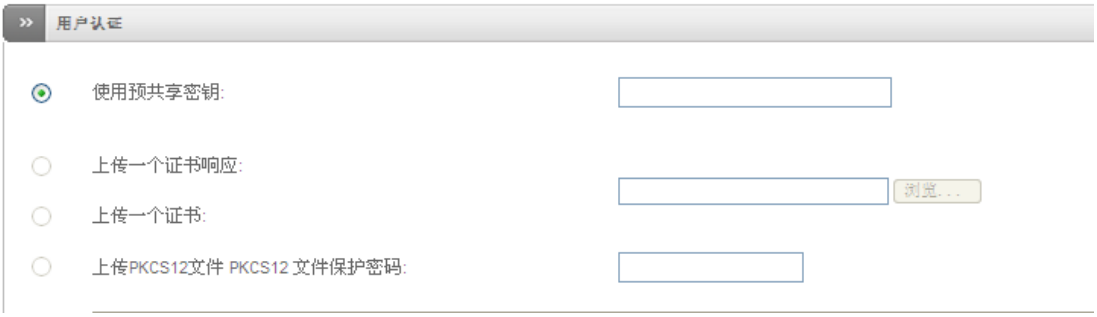
添加一个 VPN 连接,单击“添加”按钮创建一个新的连接。

这里根据你的连接类型选择，一般选择 Net-to-Net 虚拟私有网络，单击“添加”。



文件名可随意填写,启用选项必须打“√”,本地里基本不用作修改,远程里需要填写远程主机/ＩＰ协议和远程子网,ID 可填可不填, Dead peer detection action 默认就可以。

这里默认就可以了,不用作任何更改.然后单击“保存”按钮。

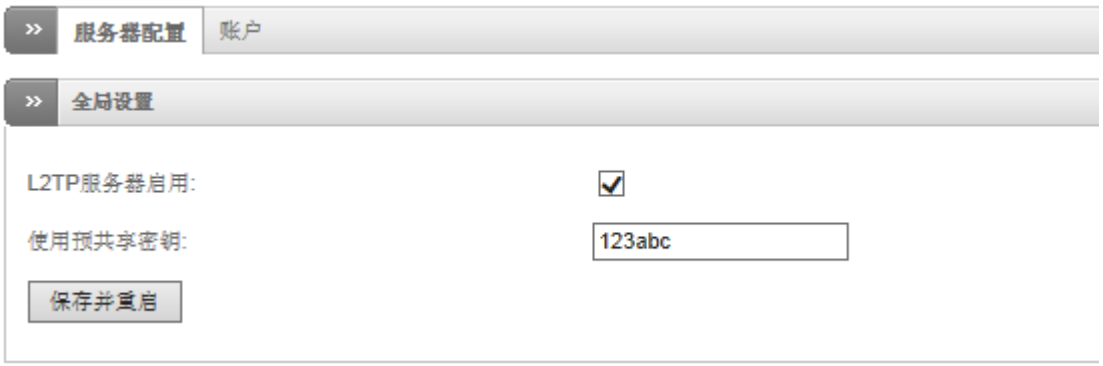


到此 IPSEC VPN 的配置完成。

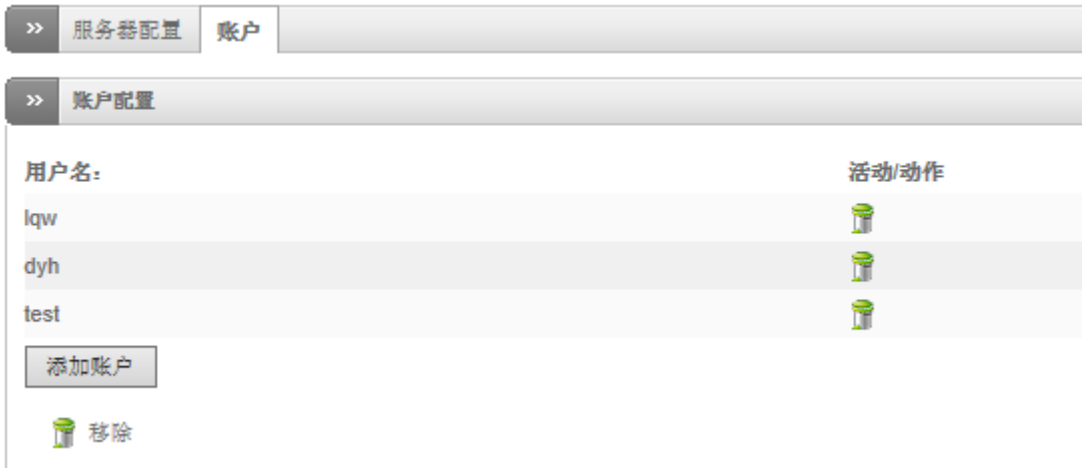
4.7.4. L2TP/IPsec 服务器

L2TP/IPsec 服务器是启博 VPN 网关专门安卓(Android)和苹果(Apple)用户远程接入量身定制功能，可以很好的解决智能手机用户和平板用户的远程接入问题。

4.7.4.1. 全局设置



帐户设置



4.7.4.2. 连接状态及控制

4.8. EPN

EPN 是启博公司推出的新一代 VPN 技术，是一项增值服务，需付费使用。EPN 具有强大的穿透能力，可以穿透多级路由,EPN 能适用包括铁通、广电、长城宽带、歌华、e 家宽等没有公网 IP 的网络。将 VPN 设备设置为不同的网段，EPN 组网后即可让 VPN 设备之间互通。另外启博 EPN 支持 PC 客户端和安卓手机客户端连接，使用非常方便，并大大降低了传统 VPN 的实施复杂度。

4.8.1. 基本设置

- 启用：EPN 功能开关，勾选启用 EPN 功能可用，去掉勾选则 EPN 功能失效。
- 本机名称：可以任意输入英文、数字或英文数字组合，不支持中文及特殊符号。
- 本机组网密码：可以是任意的数字及字母，其他设备连接此设备时需要提供给对方，否则对方连接不上。
- 客户端桥接模式：启用则 EPN 的 PC 端连接上 EPN 后，可以通过网上邻居看到 EPN 设备端的内网所有机器，实现 windows 网上邻居的作用，主要用于一些特殊应用场合。

- 设备子网互通：是指连接到该设备的其他 EPN 设备下设备或 PC 可以互通，类似于客户端互访功能

服务状态　是显示当前 EPN 的工作状态，以及 EPN 的序列号情况

- 当前状态：显示该设备是否与 EPN 云服务端是否连接成功，只有成功连接云服务器后，其他设备才能与该设备进行连接。分为已连接和离线两种状态。
- 本机序列号：是指该设备的 EPN 序列号，一台设备有一个唯一的序列号，并且终身有效，无法修改。
- 最大接入数：是指该 EPN 序列号的最多接入许可数，包括 EPN 设备、PC 电脑、手机等的数量总和。
- 服务有效期至：是指该 EPN 序列号的截至有效期，过期 EPN 服务自动停止将无法使用。需付费另行开通 EPN 服务。

4.8.2. 组网管理

组网管理是设置需要连接的设备信息，例如我们要连接北京分公司的 EPN 网关，则在这里添加名称：北京分公司，序列号是北京分公司网关的 EPN 序列号和北京的组网密码，MTU 值默任是 1360，其中北京的 EPN 序列号和组网密码需要向北京分公司索取或到北京 EPN 网关上查询。

✧ **注意：如果 A 和 B 两台设备相连，只需要 A 添加 B 或 B 添加 A 即可，不需要互相添加，这一点和传统 VPN 有区别！！！**

- 名称：是对要连接的网关信息的描述，可以为任意字符，支持中文。
- 序列号：是要连接的设备的 EPN 序列号，需向对方索取。
- 组网密码：是要连接的设备上设置的 EPN 组网密码，需向对方索取
- MTU 值：默认值是 1360 ，不建议修改。
- 加密：EPN 连接后数据的传输时是否采用加密，一般勾选加密。

4.8.3. 组网状态

组网状态显示和本设备已连接的其他设备及安卓移动端连接情况

- 对端名称：接入端的设备名称，一般是显示在组网管理中输入的对应 EPN 序列号的名

称，对端的 EPN 设备上的组网状态里，名称显示为本端 EPN 设备端设置的本机名称（**见下图**）；对于手机端连接后则显示为 CLIENT。

- 序列号：显示接入设备的 EPN 序列号，安卓移动端则显示为该安卓设备的硬件标识符。
- 网络：接入的 VPN 设备 LAN 接口 IP 地址及子网掩码、MTU 值信息。
- 当前速率：本端和对端之间当前数据传输的速率，分为接收和分送两种情况。
- 类型：根据对端的网络类型会显示为其他设备中转、内网 P2P、公网 P2P。
- 在线时长：EPN 已连接的时间，以秒为单位。
- 状态：是接 EPN 设备连接连接的情况，如果正常连接会显示已连接，否则会给出相应的错误提示信息。

4.8.4. 客户端帐号

客户端帐号管理是添加或删除 PC 端通过 EPN 连接的用户名和密码。

- 帐号：PC 端 EPN 连接时使用的用户名，可以为字母或数字。
- 密码：PC 端 EPN 连接时使用的密码。可以为字母或数字及英文标点附号。
- IP 地址：是分配给该帐号的 VPN 的虚拟 IP 地址，此帐号不管什么时间连接都会获取相同的 IP 地址。（**注意：如果启用了客户端桥模式后，这里输入的 IP 必须是和 EPN 网关 LAN 接口相同网段的 IP 地址**）
- 备注：是对该帐号的说明或描述信息，支持中文输入 。

4.8.5. 客户端连接

这里显示的是 PC 端 EPN 连接到该设备的情况

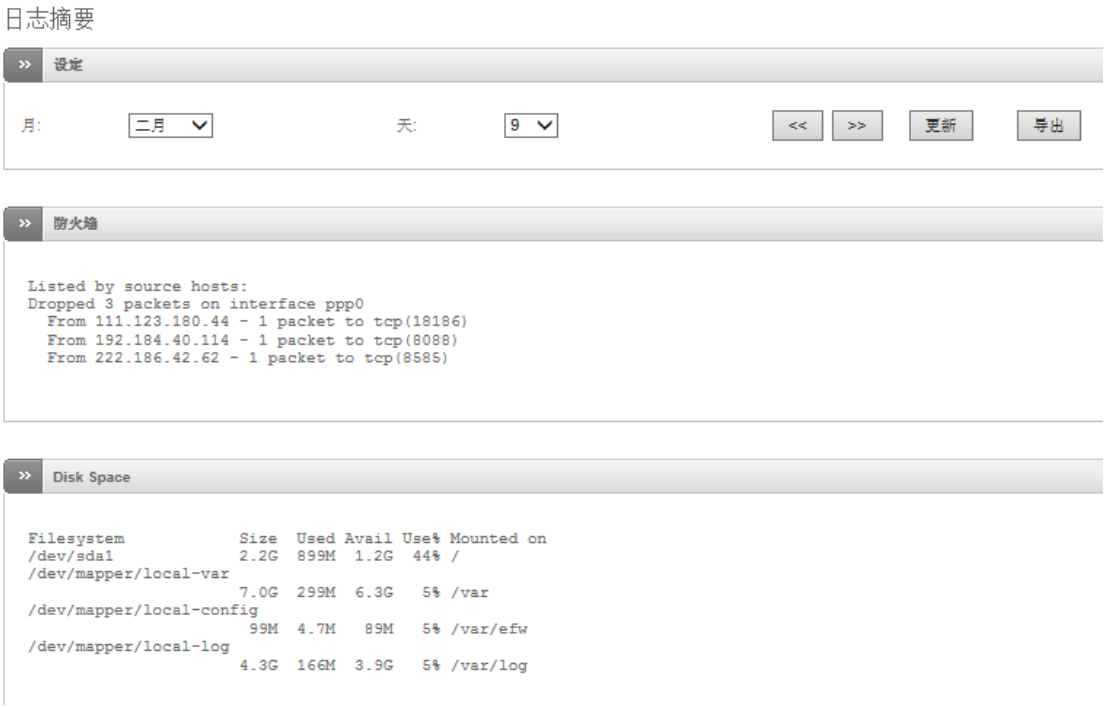
可以显示接入的帐号，分配的内部 IP、来源 IP，当前发送速率和当前接收数率，网络类型，以及连接时长（这里计时以秒为单位）。

4. 9. 日志

4.9.1. 实时日志

在这里可以查看到设备的运行状态的日志记录，下面是部分日志，如下所示：

4.9.2. 日志摘要



4.9.3. 系统日志

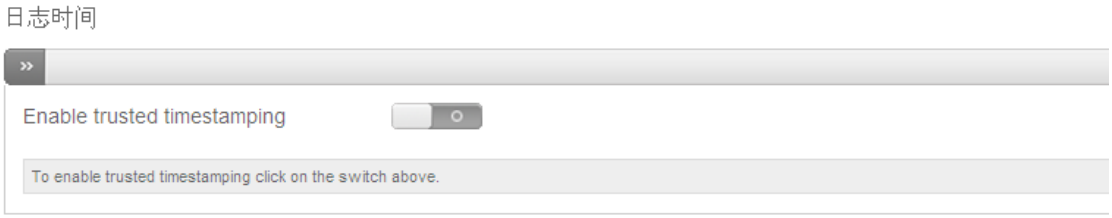
4.9.4. 服务日志

4.9.5. 防火墙日志

4.9.6. 代理日志

4.9.7. 日志设置

4.9.8. 日志时间



5. SSL VPN 配置部分

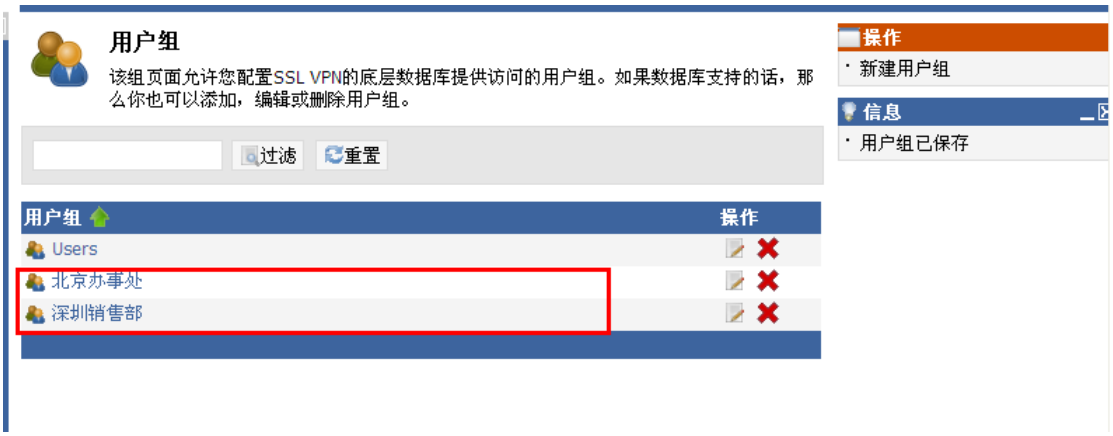
5.1. 基本配置

输入设备地址 https://192.168.10.1 ，登录设备，注意这里是 https 不是 http

输入帐号和密码，进入系统中，系统初始的管理员帐号：admin 密码：netadmin (全部是小写字母)

首先在接入管理里，建两个用户组和两个用户，如图：

这里建了北京办事处和深圳销售部，分别保存，如图：



再建立两个用户 lqw 和 mfh ，其中 lqw 划分到 深圳销售部用户组里，mfh 划分到北京办事处的组里

5.2. 应用发布：

5.2.1. B/S 模式软件发布

用户建好之后，就可以发布应用了
这里首先发布一个 OA 的应用，选择“应用发布----WEB 推送”，

新建 Web 推送，如图：

点击向后，设置要推送的名称和资料描述，如图：

点击向后，设置推送服务器的目标网址：


新建Web推送
以下向导将引导您完成，创建一个新的Web推送配置，并且分配给它一个或多个规则。
Step 3 - Web 推送具体细节
请提供此Web推送的其他信息.
目标网址
http://192.168.23.253
${}
向前
向后
取消


Step 5 - Web 推送规则选择
选择要添加此Web 推送的规则.
选择的规则
Everyone
添加
移除
设置
OA用户
显示私有规则
向前
向后
取消


新建Web推送
以下向导将引导您完成，创建一个新的Web推送配置，并且分配给它一个或多个规则。
Web 推送新建完成
Web 推送创建过程已完成.请查看下面的信息.
Web 推送已建立.
分配Web 推送规则.
所有步骤已完成.点击退出向导完成.
退出向导

5.2.2. 文件共享类发布：


新建规则
下面的向导将引导您创建一个新的规则，并授予它的主体（用户或组）
Step 1 - 规则详情
请输入规则名称.
名称:
文件共享
描述:
文件共享
向后
取消

新建网上邻居共享，比如新建一个共享文档，“营销资料”


管理控制台
全局设置
系统设置
应用扩展
证书管理
属性
接入管理
用户管理
用户组
规则设置
访问权限
认证计划
IP地址限制
应用发布
Web 推送
网上邻居
应用程序
SSL 隧道
配置文件
系统
运行状态
消息队列
关机
网上邻居
在这里，你可以配置你的网络的地方。 SSL VPN可以提供到Windows（Samba/CIFS），本地和FTP文件系统的访问。
过滤
重置
名称
操作
网上邻居或许根本不存在，你被允许编辑。如果允许，你将能够创建一个新的网络的地方，点击 新建网上邻居 操作.
操作
新建网上邻居


向导
新建网上邻居
1. 资源详情
2. 网上邻居细节
3. 规则选择
4. 概要
您可以随时点击取消按钮退出安装。
当前用户: admin
SSL VPN; 0.9.1
新建网上邻居
下面的向导将引导您通过配置一个新的网上邻居，给其分配给一个或多个访问规则。
Step 1 - 网上邻居细节
请提供该网上邻居的名称和描述.
名称:
营销资料
描述:
营销资料
添加到收藏夹


向导
新建网上邻居
1. 资源详情
2. 网上邻居细节
3. 规则选择
4. 概要
您可以随时点击取消按钮退出安装。
当前用户: admin
SSL VPN; 0.9.1
版权所有; 2003-2020
& 深圳市迅博信息技术有限公司
新建网上邻居
下面的向导将引导您通过配置一个新的网上邻居，给其分配给一个或多个访问规则。
Step 2 - 网上邻居路径信息
请提供文件存储类型和相应的路径和这个网络的地方访问属性。如果，您选择 自动, 你可以输处一个路径按下面格式t "\\Server\Share"用于windows共享或者一个本地路径如 "C:\Documents and Settings" or "/home/joeb/share".相对路径也是支持的，如 (e.g. "./logs")，并且 URL也可以用于网上邻居如 (e.g. "ftp://upload.sourceforge.net/incoming").
类型:
Windows Network
主机:
192.168.23.200
端口:
0
路径:
customer
用户名:
szqibo
密码:
显示 隐藏
只读
显示文件夹
无删除
向前
向后
取消


新建网上邻居
下面的向导将引导您通过配置一个新的网上邻居，给其分配给一个或多个访问规则。
Step 3 - 网上邻居选择
选择你想连接这个网上邻居的规则.
选择的规则
Everyone
OA用户
添加
移除
设置
文件共享
显示私有规则
向前
向后
取消

新建网上邻居

下面的向导将引导您通过配置一个新的网上邻居，给其分配给一个或多个访问规则。

Step 4 - 网上邻居概要

阅读下面的信息，然后点击**完成** 创建网上邻居.

资源

网上邻居名称: 营销资料

策略

名称: 文件共享

向前 完成 取消

新建网上邻居

下面的向导将引导您通过配置一个新的网上邻居，给其分配给一个或多个访问规则。

创建网上邻居

网上邻居创建向导已经完成。请仔细阅读下面信息

- 创建网上邻居.
- 连接网上邻居的规则.

所有步骤已完成. 点击 **退出向导** 结束任务.

退出向导

5.2.3. C/S 模式软件发布：

新建应用程序发布

比如要远程应用用友软件，用友软件的服务器 IP 是 192.168.23.200，下面来具体设置，

应用发布--》应用程序


向导
新建应用
1. 应用扩展
2. 应用详情
3. 应用规则
4. 规则选择
5. 资源概要
您可以随时点击取消按钮退出安装。
当前用户: admin
SSL VPN; 0.9.1
新建应用
以下向导将引导您完成创建一个新的应用程序和它分配给一个或多个策略。
Step 2 - 应用详情
请提供此应用程序快捷方式的名称和描述。
名称:
用友U8
描述:
用友U8
添加到收藏夹
向前
向后
取消


向导
新建应用
1. 应用扩展
2. 应用详情
3. 应用规则
4. 规则选择
5. 资源概要
您可以随时点击取消按钮退出安装。
当前用户: admin
SSL VPN; 0.9.1
新建应用
以下向导将引导您完成创建一个新的应用程序和它分配给一个或多个策略。
Step 3 - 应用选项
请提供启动此应用程序的其它信息
General
Display
Local Resources
Programs
Experience
Hostname
192.168.23.200
Port
3389
Username
Password
Domain
Authentication Level
No Authentication
Credential Security Service Provider
Prompt for Credentials
Close tunnel on disconnect
向前
向后
取消


新建应用
以下向导将引导您完成创建一个新的应用程序和它分配给一个或多个策略。
Step 4 - 应用程序快捷规则选择
选择要附加此应用程序的快捷方式的规则.
选择的规则
OA用户
文件共享
添加
移除
设置
向上
向下
Everyone
显示私有规则
向前
向后
取消

5.3. 客户端设置

客户端登陆 SSL VPN，首次运行必须安装 SSL VPN 插件，SSL VPN 插件是 VPN 运行环境必须的，如果没有安装插件也是可以进入系统，但是运行 VPN 里系统中的应用无法执行。

下载完毕，点击安装

直接安装，全部按默认安装即可。

安装完毕后，重启或刷新一次浏览器，输入管理员分配的帐号和密码，登陆到 VPN 里就可以看到总公司管理员分配给自己的各种应用。

访问 B/S 类型的资源，例如我们点击 OA,，在此过程中如果出现警告信息，点确定，允许即可，并在前面总是信任那里打上勾，以后就不会提示了。如下图

访问 C/S 类的资源，例如我们点击”用友 T6”，在此过程中如果出现警告信息，点确定，允许即可，并在前面总是信任那里打上勾，以后就不会提示了。

用友软件的登陆的企业门户就出现了，输入用户名和密码，点确定


RDP7465 - 127.0.0.1:50901 - 远程桌面连接
用友T6-企业管理软件 - [企业流程]
用友T6
系统(S)
视图(V)
窗口(W)
工具(T)
服务专区
帮助(H)
企业流程
业务工作
保存 | 增删改
财务会计
总账
应收款管理
应付款管理
UFO报表
现金流量表
财务分析
出纳管理
供应链
采购管理
销售管理
库存管理
企业应用集成
企业应用集成
客户关系管理
CRM模块
上一级
最上级
采购管理
销售管理
库存管理
计划生产
简单生产
委外管理
财务核算
存货核算
企业应用平台

6. 附录一、常见问题解答（FAQ）

1、忘记启博 VPN 网关的登录密码，进不去设备的设置界面怎么办？
答：启博 VPN 网关默认用户名是小写的 admin ，密码是 netadmin ，可以尝试一下默认的用户名和密码能否进去，如果进不去，可以通过 SSH 方式，进入设备后台，输入如下命令 factory-default，按回车，设备会自动重启并清空里面所有的配置。如果你连 SSH 后台的密码也忘记了，你可以把启博 VPN 网关接上显示器和键盘，按上面的提示恢复出厂设置。如果是你感觉里面的配置内容很多，又不想简单清空里面的参数，可以向启博公司寻求帮助试试，电话: 400-618-3858，在线 QQ: 28838513

2、用户收到设备后，第一次如何设置上网？

答：如果你是 ADSL 宽带用户，网络---选择 RED 接口的类型， 选“PPPoE”，把 ADSL 宽带上网的帐号和密码输入到相应的文本框里，保存即可。（注，有些猫启用了路由拨号功能，请联系客服，改为纯猫模式。）

如果你是光纤固定 IP 方式上网用户，网络----选择 RED 接口的类型，选“以太网 STATIC”，把 ISP 运营商分配的 IP 地址、子网掩码、默认网关、DNS 输入保存即可。

如果你是用的小区宽带或天威视讯等小的运营商的网络，网络---选择 RED 接口的类型，选“以太网 DHCP”，保存即可。

3、启博 VPN 需要固定 IP 地址才能用吗？
答：启博 VPN 不需要固定 IP 地址就可以使用，但是对于公司的总部也就是中心端，需要有公网 IP 地址，这个公网 IP 可以是固定的也可以是动态的，中心端不能是私网 IP 的那种网络。
判断中心端的网络是否有公网 IP 地址的方法是，进行路由器，看一下运行状态里，外网那里拨号获取的地址是什么样的，一般以 10 开头或 100 开头的 IP 地址都是私网 IP，如果不确定，可以将这个 IP 地址和打开 http://www.ip138.com 上面显示的 IP 地址对比，如果是相同的就是合法的公网 IP，否则就是私网 IP。

4、启博 VPN 需要申请动态域名才能用吗？

答：启博 VPN 网关集成启博目录寻址服务和启博 DDNS 服务，用户不需要自己申请动态域名，直接用启博 VPN 网关自带的域名和目录服务就可以了。相比第三方的动态域名，启博 DDNS 是全商用、全封闭的寻址服务，只针对启博 VPN 的用户提供服务，不开放注册使用，不提供给第三方使用。有效的保证启博 DDNS 服务的稳定性和安全性。

5、启博 VPN 网关一定要替换我们现有的路由器吗？

答：启博 VPN 网关可以替换客户现有的路由器，也可以不替换现有路由器，直接放在现有

路由器下，把启博 VPN 网关当作一台 PC 机一样使用。

6、启博 VPN 网关当路由器用和放在路由器后有什么区别？

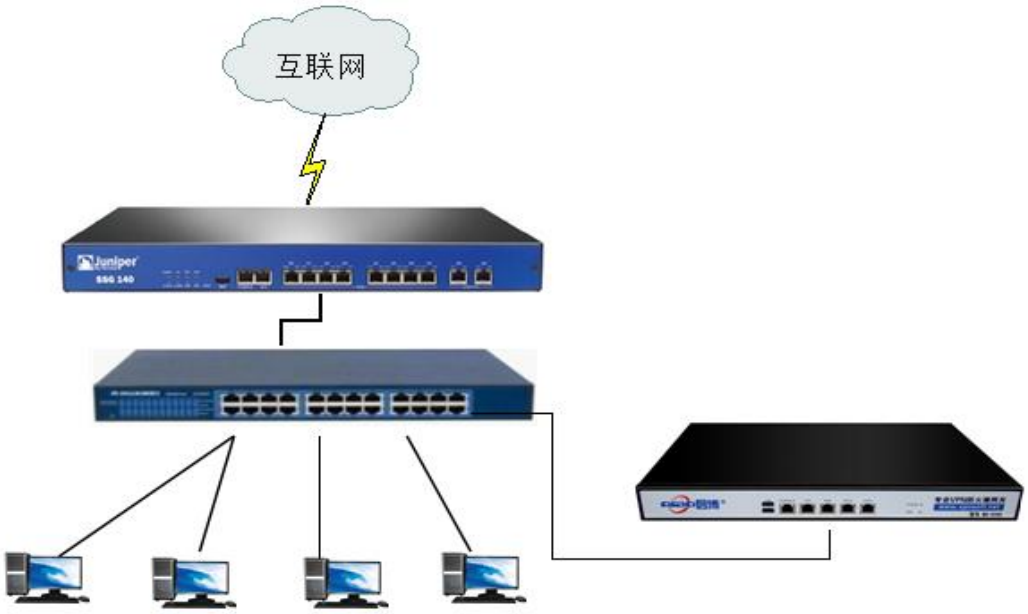
答：启博 VPN 网关当路由器用可以完整使用启博 VPN 所有功能，包括防火墙、VPN 功能、上网行为管理、流量控制等等。启博 VPN 放在路由器后，只用其中的 VPN 功能。
启博 VPN 当路由器比放在现有路由器后寻址稳定性稍好，有些客户网络管理很规范，防火墙、上网行为管理都部署的很好，用启博 VPN 网关放在路由器后也是很方便的，特别的是有固定 IP 地址的网络，使用效果也是不错的。
启博 VPN 当路由器用时需要接两条网线，一条是接外网，一条接内网；启博 VPN 放在路由器后，采用的是启博 VPN 的透明模式，只需要一条网线即可，不区分内网和外网。

7、我们是用的小区宽带，没有公网 IP 能用你们的 VPN 吗？

答：启博 VPN 只要求中心点也就是公司总部有合法的公网 IP 就可以了，如果你是做为 VPN 的分支端或客户端，不管用什么网络都是可以使用启博 VPN 的。如果的确是公司总部的网络没有公网 IP，请采用启博 VPN 双 NAT 版，详情可以登录启博官网进行了解（http://www.vpnsoft.net）。

7. 附录二、透明模式接入

有些客户在上 VPN 前，公司网络规划比较好，有专门的防火墙路由器和交换机，网络管理很规范，IT 部门人员也比较熟悉以前设备的维护管理，不太愿意换下以前的防火墙路由器使用 VPN 网关当路由器用，这样可以用启博 VPN 的透明模式的接法。
透明模式接法的优点是无需改变客户的现有网络结构，直接将 VPN 接在网络中的交换机上，网线接在 VPN 设备的 LAN 口上。网络拓朴图如下：



注意：网线一定要接在 VPN 网关的 LAN 口上，WAN 口上不用插线

假设路由器的 LAN 地址为：192.168.10.1，VPN 设备的网络参数配置如下：
第一步：


系统
状态
网络
服务
防火墙
网络设置
系统信息
网络设置
事件通知
设置密码
运行命令
SSH 访问
语言选择
系统备份
关机
授权信息
网络安装向导
步骤 1/8: 选择RED接口的类型
红色: 不信任, 互联网连接 (WAN)
以太网STATIC
以太网DHCP
PPPoE
ADSL (USB, PCI)
ISDN
ANALOG/UMTS Modem
GATEWAY
撤销
>>>

第二步：


网络设置
系统信息
网络设置
事件通知
设置密码
运行命令
SSH 访问
语言选择
系统备份
关机
授权信息
网络安装向导
步骤 3/8: 网络偏好设置
绿色 (信任的, 内部网络 (LAN)):
IP 地址:
192.168.10.254
子网掩码:
/24 - 255.255.255.0
Add additional addresses (one IP/Netmask or IP/CIDR per line) :
接口:
端口 Link 描述 MAC 设备
1 Intel ? 00:e0:4c:46:df:ee eth0
2 Intel ? 00:e0:4c:46:df:ef eth1
3 Intel ? 00:e0:4c:46:df:f0 eth2
4 Intel ? 00:e0:4c:46:df:f1 eth3

第三步：

第四步：

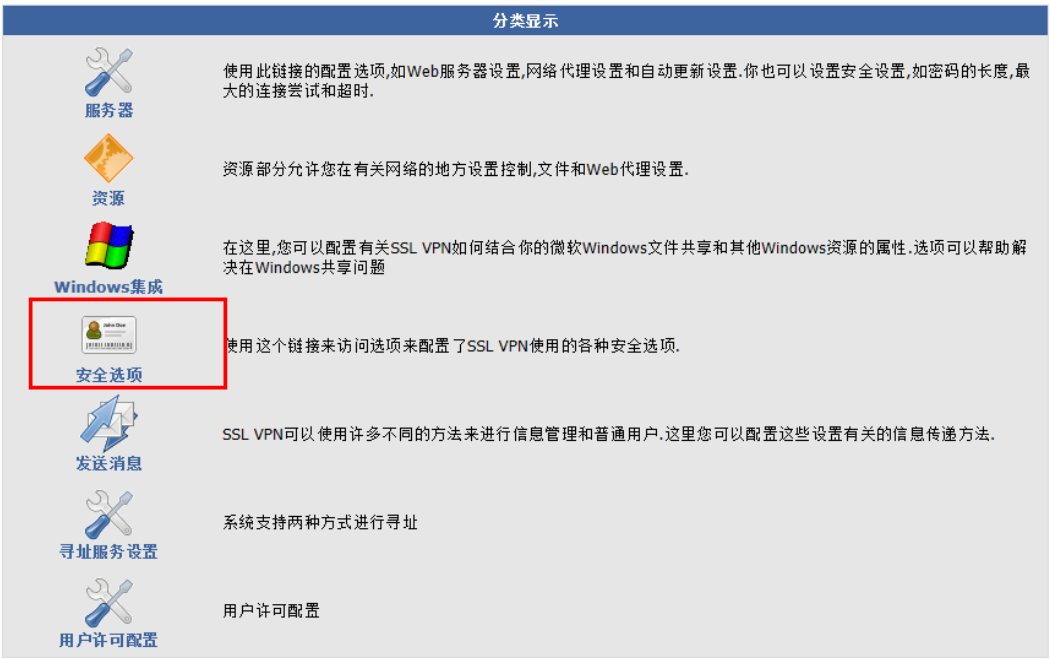
注意：VPN 设备的路由 IP 地址，是当前网络中任一空闲 IP 地址均可，不一定是按上图设置；默认网关就是路由器防火墙的地址，静态 DNS 为当地 ISP 的 DNS，如果实在不知道，也可以写成和默认网关相同的内容，DNS 必须输入两个。

8. 附录三：启博 SSL VPN 短信登陆使用方法

手机现在已经成了人们生活中的必备品，有些单位一些业务系统登陆，也采用了手机短信验证的方式，以提高系统的安全性，做为国内知名 VPN 厂商-----启博 VPN，以客户的需求为己任，公司全线 MS 系列 VPN 支持手机短信认证功能，并且针对签约的客户全部免费赠送手机短信认证模块。

启博 SSL VPN 手机认证内置多个短信认证网关，供用户选择，费用低，不需要购买硬件（如短信猫），节省客户的投资。下面就举例说明一下，启博 SSL VPN 短信认证的用法。特别说明，软件版本不同，操作可能有差异。

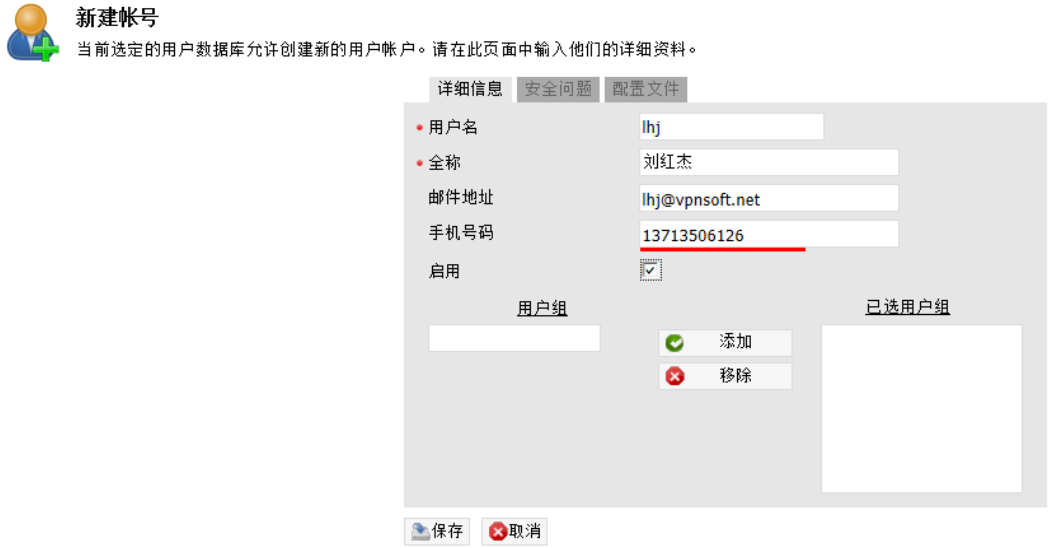
（一）、系统设置----安全选项，启用短信认证



短信认证 打勾即可

这里的短信需要先找短信运营商开通短信业务才可以。使用短信登录。

（二）、新建用户，并输入用户的手机号，**这里输入的手机号就是用户登陆 SSL VPN 时，接收短信用的，一定不能输错，如果输入错误将无法正常接收认证短信**，从而无法进入 VPN。



输入完毕，点击保存。

（三）、下面用新建的用户登录 VPN，在网址栏里输入 https://qibo.szsec.net ，即可看到下面登录页面，

输入新建的用户名和密码，然后点获取短信

正常是 60 秒以内，将收到一条如下内容的短信提示：

把收到的 6 位身份验证码输入到验证码的位置，点登录，就可以进入 VPN 了，

点击 OA ，即可进入通达 OA 系统。

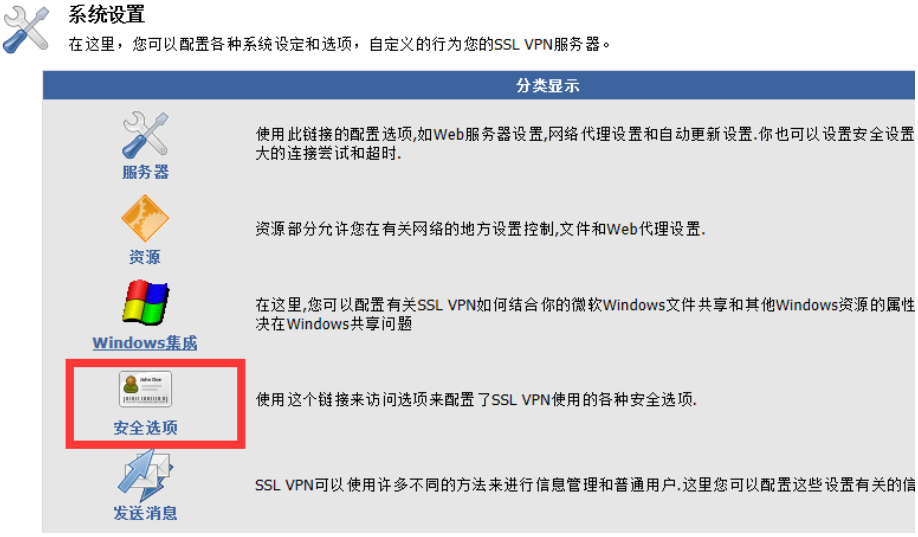
使用非常方便，如果是想取消手机短信验证，只需要管理员，在系统设置---安全选项中，启用“普通登录”方式即可。

9. 附录四：启博 SSL VPN 使用 UKEY 登录使用方法

使用启博 UKEY 登录 VPN 的好处，简化用户的登录，类似于网上银行，只要输入密码即可登录 VPN，但必须要有 UKEY 才能用 VPN，否则无法使用 VPN。最终用户不需要了解 UKEY 里的信息，只需输入管理员分给自己的密码就可使用 VPN，并用成功进入 VPN 后，用户可以自己使修改自己的密码，有很好的私密性。同时保证了 VPN 系统有更强的安全性。

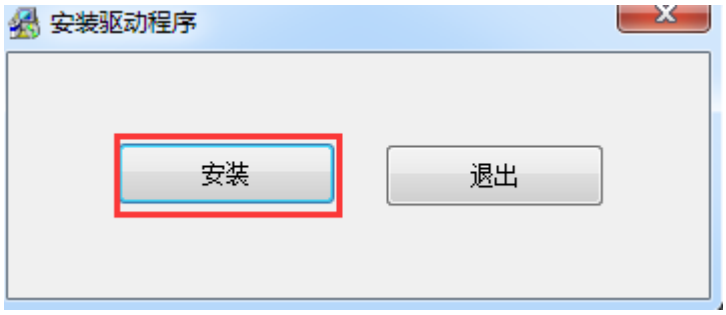
一、先建用户，在“接入管理”---“用户管理”---“新建帐号”

二、启用启博 SSL VPN 的 UKEY 登录方式，“系统管理”----“安全选项”



三、使用启博 UKEY 分发套件，分发 UKEY

第一次使用 UKE 分发套件时，需要安装 UKEY 驱动，包括使用 UKEY 登录系统时，也需要安装 UKEY，否则会提示出错的，无法进入 SSL VPN，安装很简单，只需要双击 keydriver.exe 文件，

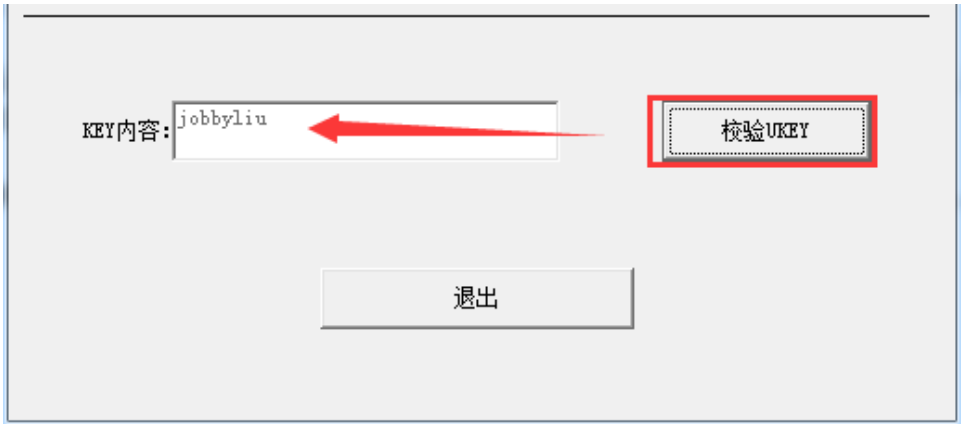


点击安装就可以了。

下面开始分发 UKEY，运行 UKEY 分发套件程序。

插入 UKEY，然后输入在 SSL VPN 新建的用户名称 jobbyliu ，再点击“写入 UKEY”，就会出现 UKEY 分发成功的提示。

有时候我们担心分发的是否成功，可以对已分发的 UKEY 进行校验，我们这里试一下，



就可以校验出 UKEY 里抽内容和我们输入的是否相同。

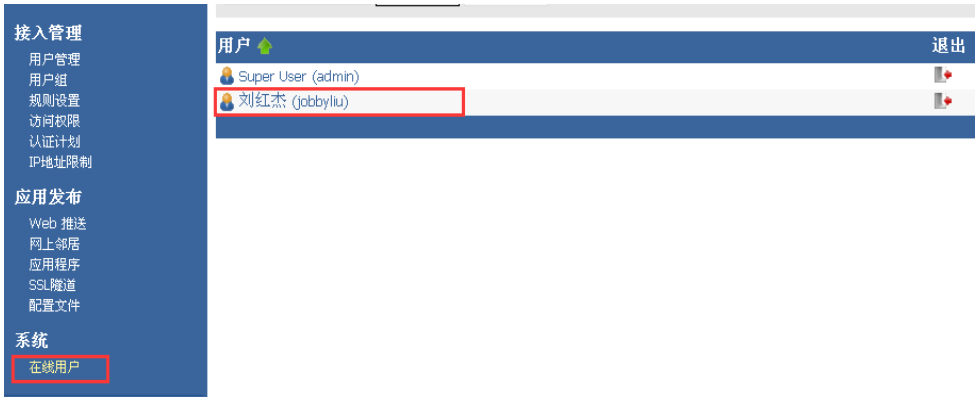
四、使用 UKEY 登录 SSL VPN

输入 SSL VPN 的登录地址，如 https://192.168.10.1 ,注意是 https ,就会出现 VPN 的登录页面。

首次登录时，需要按上面的提示，安装 SSL VPN 插件，和 UKEY 驱动，插件和驱动下载按默认方式安装就可以了，安装完毕，接入 UKEY

输入密码后，直接回车或点登录，即可登录 SSL VPN 了。

这时管理员，在后台的“在线用户”那里能看到刚登录的 UKEY 用户。



五、系统管理员后台管理

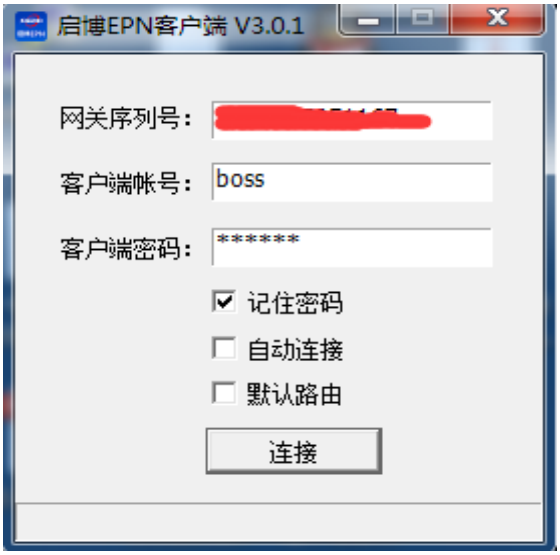
SSL VPN 启用了 UKEY 登录或短信登录方式后，管理员的登录地址需要通过指定的地址来登录，如果设备的地址是 192.168.10.1 ，这里可以输入 https://192.168.10.1/adminlogin.html，注意后面的 URL 部份，adminlogin.html 这时就可以显示出管理员的登录页面

10. 附录五：EPN 客户端使用说明

一、PC 端

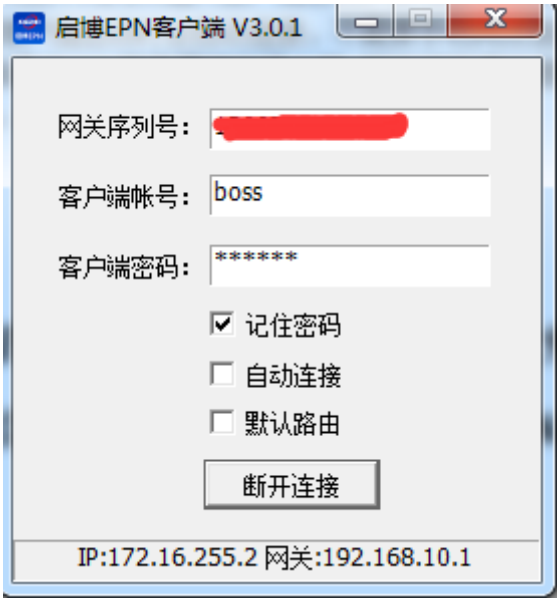
采用默认安装方式安装启博 EPN 客户端，安装成功后会在桌面上出现启博 EPN 的快捷方式，

如下图，双击启博 EPN 的快捷方式，显示下列窗口



- 网关序列号：是想要连接的设备的 EPN 序列号，可以在 VPN 设备的管理页面中查询到。
- 客户端帐号：连接到 EPN 网关的帐号，请向单位 IT 管理人员索取。
- 客记端密码：连接到 EPN 网关的密码，请向单位 IT 管理人员索取。
- 记住密码：下次使用时就不用再次输入客户端密码，系统会记住所输密码。
- 自动连接：下次 EPN 客户端启动时会自动连接，不需要手动再点连接按钮。
- 默认路由：EPN 客户端通过 EPN 服务器端代理上网，即实现所谓的借线或 VPN 代理功能。

连接成功后，如下图所示，如果连接失败，会有相应错误提示信息。



二、安卓端

安装文件请联系启博公司索取，按正常安卓文件安装方法安装即可，安装后会在手机屏幕上出现启博 EPN 快捷方式，

点击启博 EPN 快捷方式，

输入需要连接的 EPN 网关序列号和组网密码，点击连接，为了方便下次使用，可勾选 记住密码选项。显示下图表示 EPN 连接成功，如果连接失败会给出相应的提示信息。


63% 09:22
启博EPN
网关序列号：
网关组网密码：
记住密码
自动重连
已连接
断开