# 华御上网行为管理软件 V8. 2

# 操作手册

北京华御科技有限公司

**2015 年 3 月**

# 目 录

# 第1部分 设备登陆

## 1.1 接线方式

请按照如下步骤进行设备的接线：

1. 在后面板电源插座上插上电源线，打开电源开关，前面板的绿色指示灯会点亮。大约 1-2 分钟后设备正常工作。
2. 用标准 RJ-45 以太网线将 LAN 口与内部局域网连接。
3. 用标准 RJ-45 以太网线将 WAN 口与 Internet 接入设备相连接，如路由器、光纤收发器等。
4. 桥接模式：LAN1 和 WAN1 为网桥 1，LAN2 和 WAN2 为网桥 2、……、LANm 和 WANm 为网桥 m。每个桥之间是独立通信的，桥之间不能传递数据。
5. 路由模式：可以接入多条出口线路，每个端口之间在策略允许的情况下可以通信。

## 1.2 设备登录

1. 系统出厂默认是网桥模式 LAN1 和 WAN1 为网桥 1，地址为 192.168.0.1/24
2. 通过网线将电脑的网口与设备的 LAN1 口相连接，电脑 IP 地址配置为：192.168.0.2/24
3. 登录设备，打开浏览器输入 **https://192.168.0.1:9090**，默认用户名:admin 密码:bjhuayu


图 1：设备登陆

## 1.3 密码恢复

如果管理员密码丢失，请按以下步骤恢复系统默认密码：

1. 进入 Console 连接，使用 root 用户（username：root，password：bjhuayu）登录。
2. 选择 Reset WEBUI Password，进入密码恢复菜单，然后输入 yes，再回车。
3. 密码恢复成功，网管密码恢复到出厂设置（username：admin，password：bjhuayu）。

## 1.4 设备状态

登录设备后，首先将进入到设备首页，即设备状态页面。设备状态页面包含了设备版本信息、设备资源、实时网络流量、前十名服务实时速率分布、前十名用户实时速率排名、前十名站点排名、最近五次事件日志等七项内容。如下图：

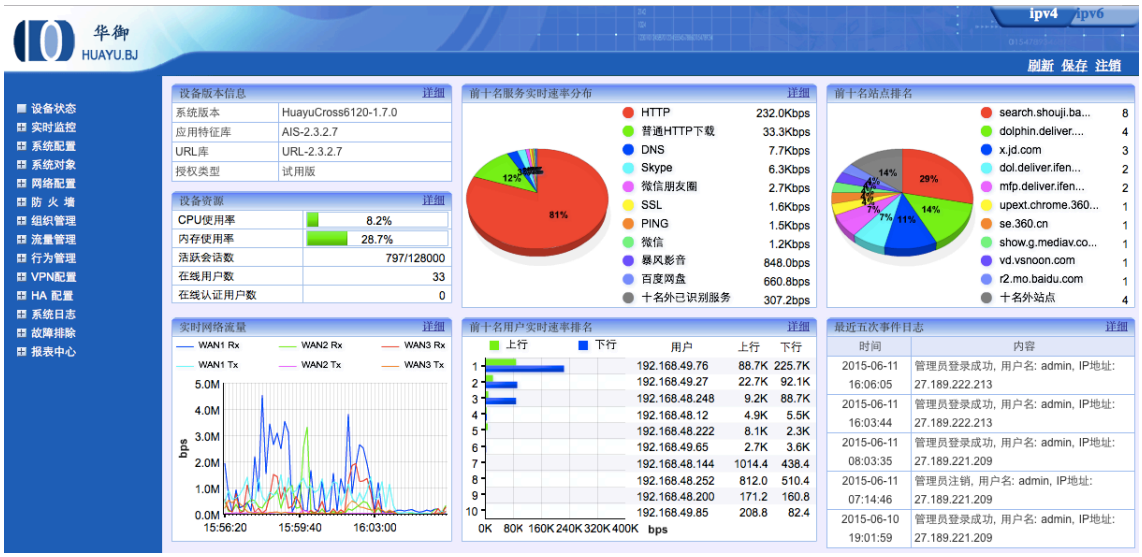



图 2：设备状态

- “设备版本信息”描述了系统固件、应用特征的版本、URL 库的版本和授权类型的信息。。
- “设备资源”动态显示了 CPU 使用率、内存使用率、活跃会话数、在线用户数和在线认证用户数的信息
- “实时网络流量”动态显示了当前 UP 的 WAN 口的速率。
- “前十名服务实时流量分布”动态显示了以总速率排名的前十名服务。
- “前十名用户实时流量排名”动态显示了以总速率排名的前十名用户。
- “前十名站点排名”动态显示了以被访问次数排名的前十名网站。
- “最近五次事件日志”动态显示了最近五次的事件日志。点击<详细>按钮，可以连接到“事件日志”页面，查看和搜索更多的事件日志。

# 第2部分 实时监控

实时监控部分用于查看设备实时的工作状态，包括设备资源、物理接口、服务监控、用户监控、上网行为、在线用户、防共享上网、当前黑名单、应用限额用户部分。

## 2.1 设备资源

设备资源包括了 CPU 使用率、内存使用率、活跃会话数、在线用户数、在线认证用户数、磁盘信息等共六部分。如下图：

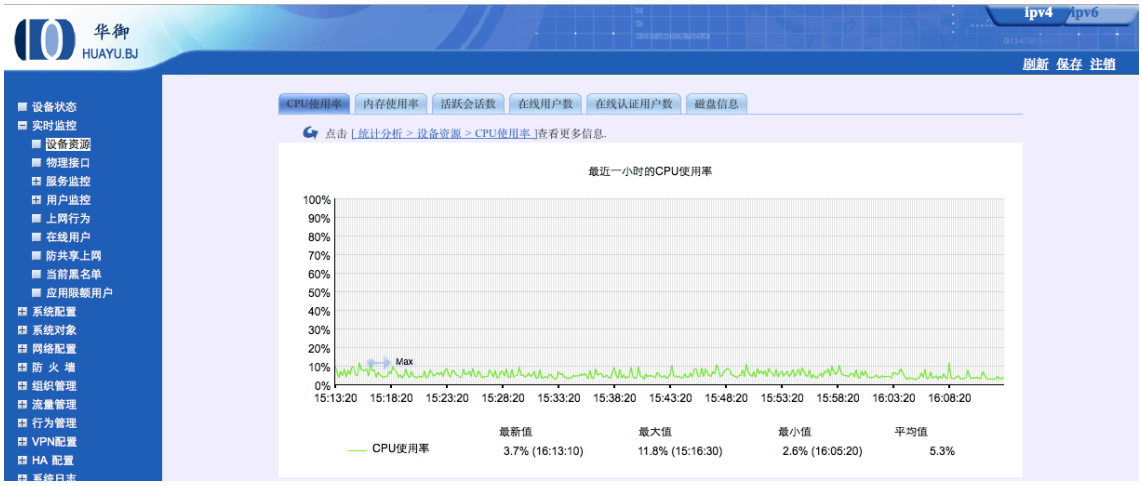



图 3：CPU 使用图

各分页详细说明如下：

- CPU 使用率：查看最近一小时 CPU 使用率；
- 内存使用率：查看最近一小时内存使用率；
- 活跃会话数：查看最近一小时活跃会话数的统计趋势图；
- 在线用户数：查看最近一小时在线用户数的统计趋势图；
- 在线认证用户数：查看最近一小时在线认证用户数的统计趋势图；

点击左侧导航底部的［报表中心］>>［内置报表中心］可以进入报表中心查看各参数的历史统计信息。

## 2.2 物理接口

物理接口页面的内容含两部分：所有端口的全局信息、每个端口的速率趋势图。

**第一**：物理接口的全局信息，如下图：


图 4：物理接口图

全局信息包括了以下内容：

- 柱状图显示了每个物理接口收发速率。
- 表格显示了每个接口的收发数据的统计信息，每个物理接口上面一行对应该接口接收数据的统计信息，下面一行对应该接口发送数据的统计信息。
- 表格中的古蓝色圆饼代表该端口为连接状态，灰色圆饼代表该端口为未连接状态。

单个物理接口的统计信息包括了总的速率、接收速率、发送速率，如下图：

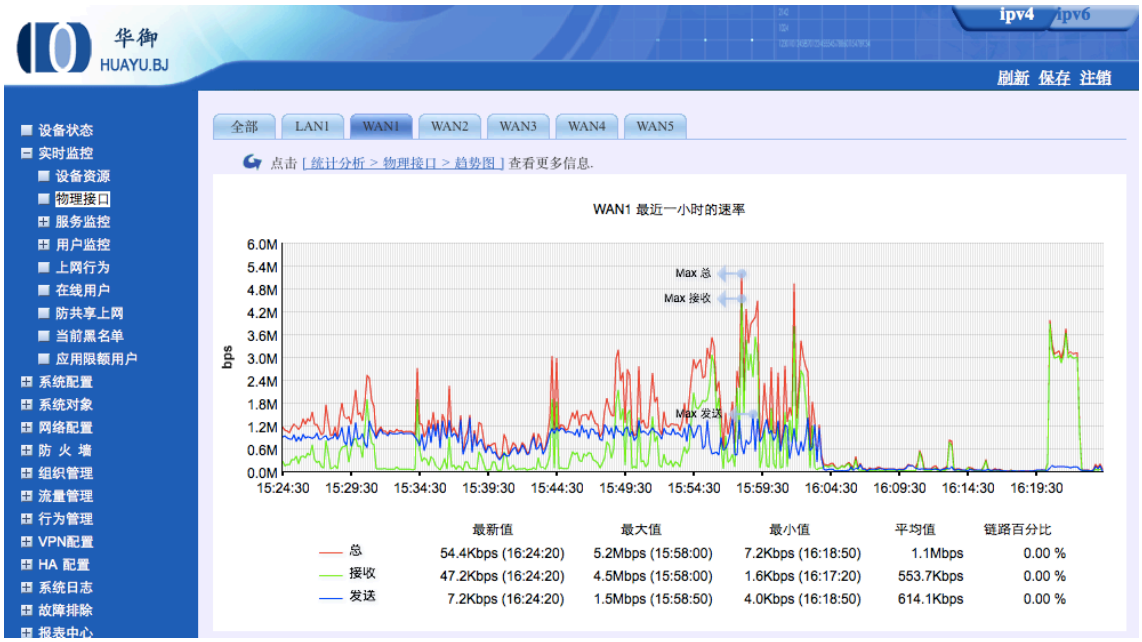



图 5：单个物理接口图

每个接口分页的下方都显示了当前值、最近一小时的最大值、最小值、平均值及每个值对应的时间点。点击页面下方的［报表中心］可以进入报表中心查看各端口的历史统计信息。

## 2.3 服务监控

服务监控页面显示了前十名服务趋叠加势图、服务组趋势图、活跃服务、所有服务四部分。

### 2.3.1 服务趋势叠加图

服务趋势叠加图如下：

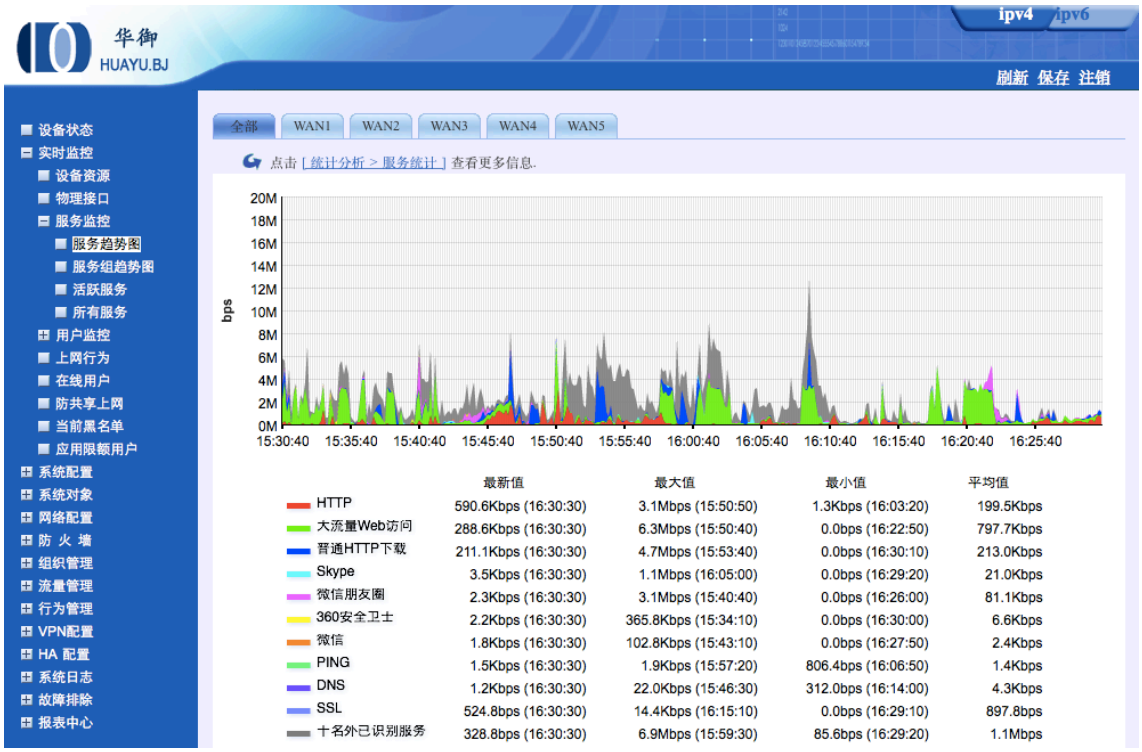



图 6：服务趋势图

这里显示了所有服务的叠加趋势图，其中列出了前十名和十名以外的识别的服务。

### 2.3.2 服务组趋势图

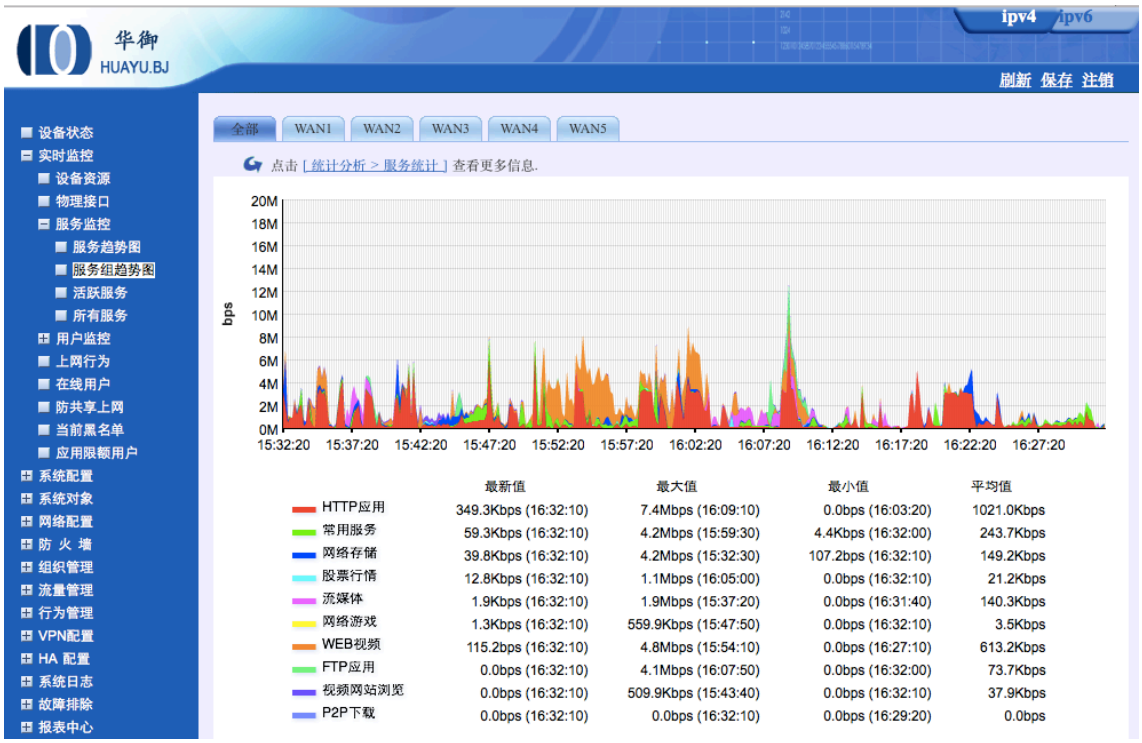



图 7：服务组趋势图

显示了所有服务组的叠加趋势图，一共有自定义普通服务、自定义特征识别、常用服务、HTTP 下载、P2P 下载、WEB 视频、流媒体、即时通讯、网络电话、网络游戏、股票交易、网上银行、其他服务等 13 种类型。

### 2.3.3 活跃服务统计


图 8：活跃服务图

**参数说明：**

- 最新速率： 表示某服务最后一个采样点的速率值。上箭头后面的值表示上行速率，下箭头后面的值表示下行速率。
- 最近一小时总流量：表示某服务最近一小时传输的流量叠加值。上箭头后面的值表示上行流量，下箭头后面的值表示下行流量。
- 最近一小时平均速率：表示某服务最近一小时的平均速率。上箭头后面的值表示上行速率，下箭头后面的值表示下行速率。

点击对应服务操作栏的<趋势图>按钮，查看该服务最近一小时的速率趋势图。点击<在线用户>，查看正在使用该服务的用户的信息。

### 2.3.4 所有服务统计

“所有服务”将分类显示所有的服务统计值，如下图：


| 序号 | 服务名称 | 最新速率(bps) | 最近一小时总流量(Byte) | 最近一小时平均速率(bps) | 操作 |
|---|---|---|---|---|---|
| 1 | TCP_ALL | ↓186.1K | ↓ 395.8M | ↓900.7K | 趋势图 |
| 2 | UDP_ALL | ↓ 3.1K | ↓ 91.2M | ↓207.6K | 趋势图 |
| 3 | DNS | ↑ 3.1K, ↓ 2.6K | ↑ 1.2M, ↓ 711.9K | ↑ 2.7K, ↓ 1.6K | 趋势图 |
| 4 | HTTP | ↑ 12.5K, ↓56.1K | ↑ 12.3M, ↓ 75.3M | ↑ 28.0K, ↓171.4K | 趋势图 |
| 5 | PING | ↑ 768.0, ↓704.0 | ↑ 337.3K, ↓ 309.2K | ↑ 767.6, ↓703.7 | 趋势图 |
| 6 | ICMP_Timeout | 0.0 | 0 | 0.0 | 趋势图 |
| 7 | ICMP_Unreach | 0.0 | 0 | 0.0 | 趋势图 |
| 8 | ICMP_ALL | ↓704.0 | ↓ 508.6K | ↓ 1.1K | 趋势图 |
| 9 | SMTP | 0.0 | ↑ 63.7K, ↓ 4.1K | ↑ 144.9, ↓ 9.4 | 趋势图 |
| 10 | POP3 | 0.0 | 0 | 0.0 | 趋势图 |
| 11 | Lotus_Notes | 0.0 | 0 | 0.0 | 趋势图 |
| 12 | IMAP | 0.0 | ↑ 857.0K, ↓ 12.0M | ↑ 1.9K, ↓27.3K | 趋势图 |
| 13 | TFTP | 0.0 | 0 | 0.0 | 趋势图 |
| 14 | SSL | 0.0 | ↑ 188.3K, ↓ 230.9K | ↑ 428.5, ↓525.4 | 趋势图 |
| 15 | SNMP | 0.0 | 0 | 0.0 | 趋势图 |
| 16 | SQL | 0.0 | 0 | 0.0 | 趋势图 |
| 17 | MySQL | 0.0 | 0 | 0.0 | 趋势图 |
| 18 | NTP | 0.0 | 0 | 0.0 | 趋势图 |

图 9：所有服务图

## 2.4 用户监控

用户监控页面显示了前五十名用户的实时传输速率、新建会话速率和活跃会话数。

### 2.4.1 流量分析

前五十名用户的实时传输速率统计图如下：

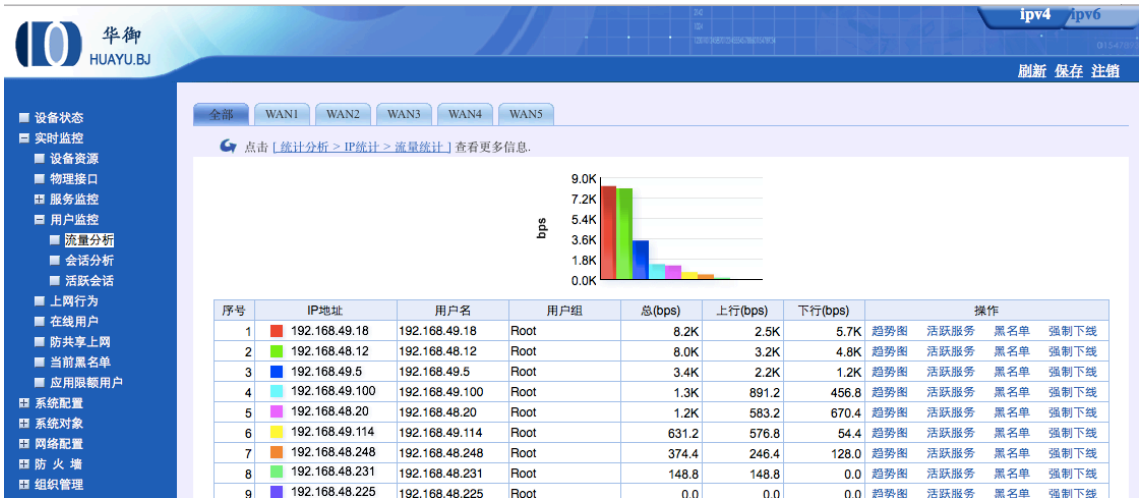



图 10：流量分析图

点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

点击<黑名单>按钮，将该用户快速加入到和名单。

点击<强制下线>按钮，将该用户将被强制下线。

点击页面上方的“报表中心”可以进入报表中心查看更多关于用户的历史统计信息。

## 2.4.2 会话分析

前五十名用户的新建会话的统计图如下：


图 11：会话分析图

点击<趋势图>按钮，查看该用户最近一小时的速率趋势图。

点击<活跃服务>按钮，查看该用户当前使用的服务的信息。

点击<黑名单>按钮，将该用户快速加入到和名单。

点击<强制下线>按钮，将该用户将被强制下线。

点击页面上方的“报表中心”可以进入报表中心查看更多关于用户的历史统计信息。

### 2.4.3 活跃会话

前五十名用户的当前活跃会话统计图如下：


图 12：活跃会话图

## 2.5 上网行为

实时显示当前的用户行为，包括访问网站、搜索引擎、邮件、IM 聊天、发帖网评、账户登录、外发文件、外发信息、Telnet 命令、其他的实时记录。可以设定 5s、10s、20s、30s、60s 的时间间隔进行过滤，如下图所示：


图 13：实时上网行为图

## 2.6 在线用户

查看当前的在线用户、可通过用户名、所属组、IP 地址、MAC 地址、时间范围查询用户，通过下方的选项卡可以查看所有在线的“已认证且在组织结构中”的用户、“已认证但不在组织结构中”的用户、“未通过认证用户”。在未启用认证的情况下，所有的用户都在已认证但不在组织结构中，如果启用认证后，可以在已认证且在组织结构中找到这些在线的用户。


图 14：在线用户图

## 2.7 防共享上网

通过防共享上网，可以查看当共享上网的用户信息。也可以通过用户名、所属组等信息来检索。


图 15：防共享上网图

## 2.8 当前黑名单

查看或查询进入黑名单的用户，对黑名单中的用户进行检索，或修改相应策略；可以通过【手动添加】按钮链接到添加黑名单用户的策略。设置黑名单的方法，可通过【行为管理】>【上网策略】>【黑名单策略】进行设置，也可以通过【用户监控】、【在线用户】中进行手动添加用户到黑名单，如下图所示：


图 16：当前黑名单

注：设置黑名单时，用户必须加入到组织结构中，才可以进行设定。

## 2.9 应用限额用户

查看超过应用限额的用户，可以临时配额来调整应用限额值，也可以减除对应用户的限制。如下图所示：


图 17：应用限额用户

下图显示，选择应用限额中的用户后，点击临时配额，进行配额值得调整。

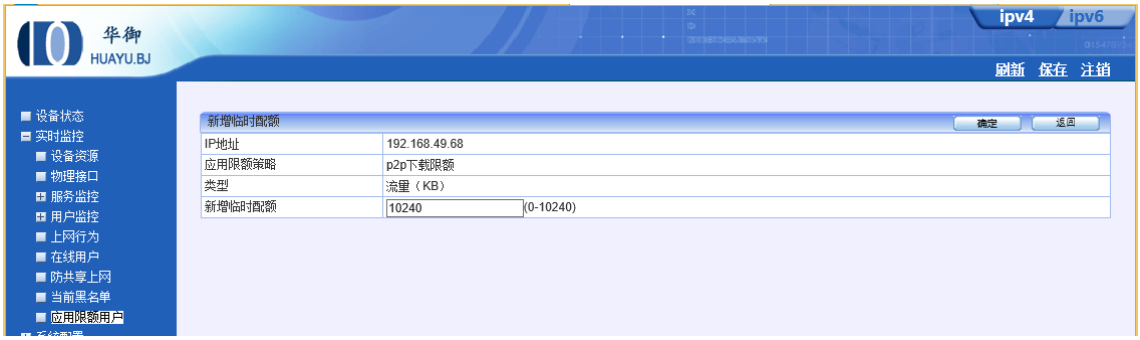

华御
HUAYU.BJ
ipv4
ipv6
刷新 保存 注销
设备状态
实时监控
设备资源
物理接口
服务监控
用户监控
上网行为
在线用户
防共享上网
当前黑名单
应用限额用户
新增临时配额
确定
返回
IP地址
192.168.49.68
应用限额策略
p2p下载限额
类型
流量（KB）
新增临时配额
10240
(0-10240)

图 18：新增临时限额

# 第3部分 系统配置

“系统配置”主要包括设备工作模式、系统维护、系统管理员、网络配置、网管策略、重启操作、关机操作、网络工具、系统信息等。

## 3.1 设备工作模式

“设备工作模式”用来设置设备的工作模式，可以设定为网桥模式、路由模式和旁路模式，默认为网桥模式。用户可根据网络中的实际情况选择相应的接入模式。

注：改变设备的工作模式，配置的静态路由将被清空。

### 3.1.1 网桥模式部署

设备不需要进行 NAT 网络地址转换时，通常采用网桥模式部署，网桥模式无需改变现有网络拓扑接口，“设备”视为一条带过滤功能的网线使用，把“设备”接在原有网关及内网用户之间，通常部署在配置 NAT 设备的下方。如下图所示：

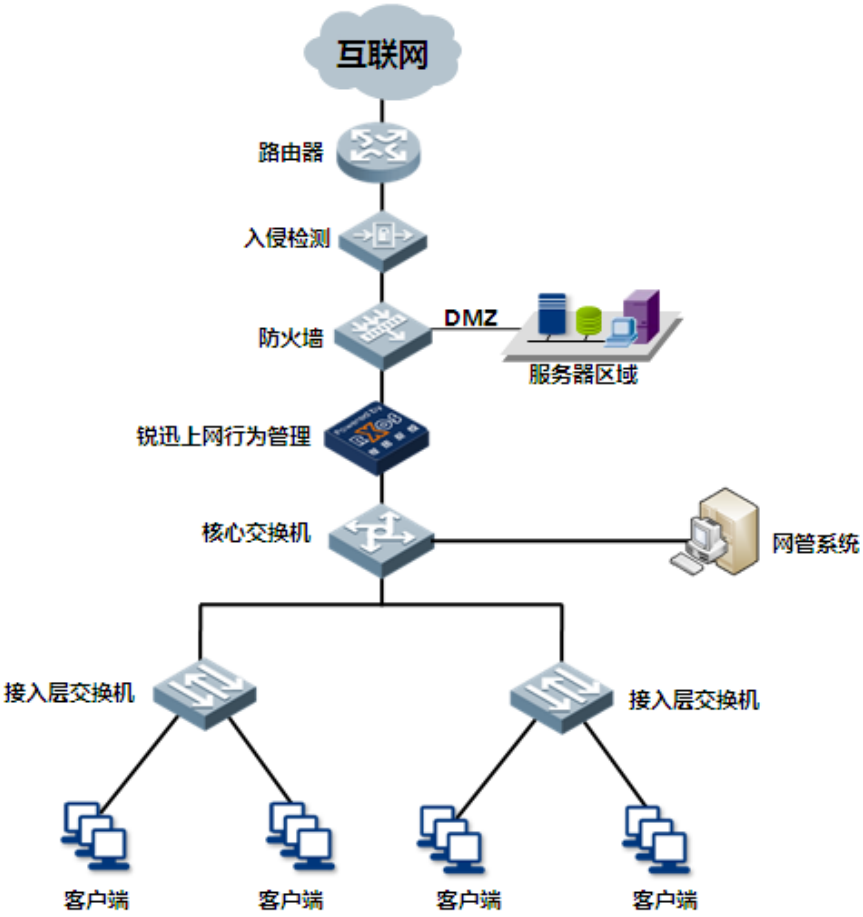



图 19：网桥部署拓扑

1. 设备处于网桥模式时，所有数据流经过设备的流量将透明转发，设备可进行上网策略配置及审计，默认无任何策略，用户可以正常上网，所有经过的流量将进行审计。
2. 配置网桥 IP 和网关，主要用于管理 Cross 设备，WEB 认证用、自动升级特征库和 URL 库等，可在”系统配置-工作模式“中配置，如下图所示：


图 20：设备工作模式

### 3.1.2 路由模式部署

Cross 设备具备地址转换功能，可以直接作为 Internet 出口网关，进行 NAT 地址、端口映射等。此时需要将设备配置为路由模式部署，LAN1 口连接下行交换机，WAN1 口连接运营商提供的线缆，可以是光口或电口，如下图所示：

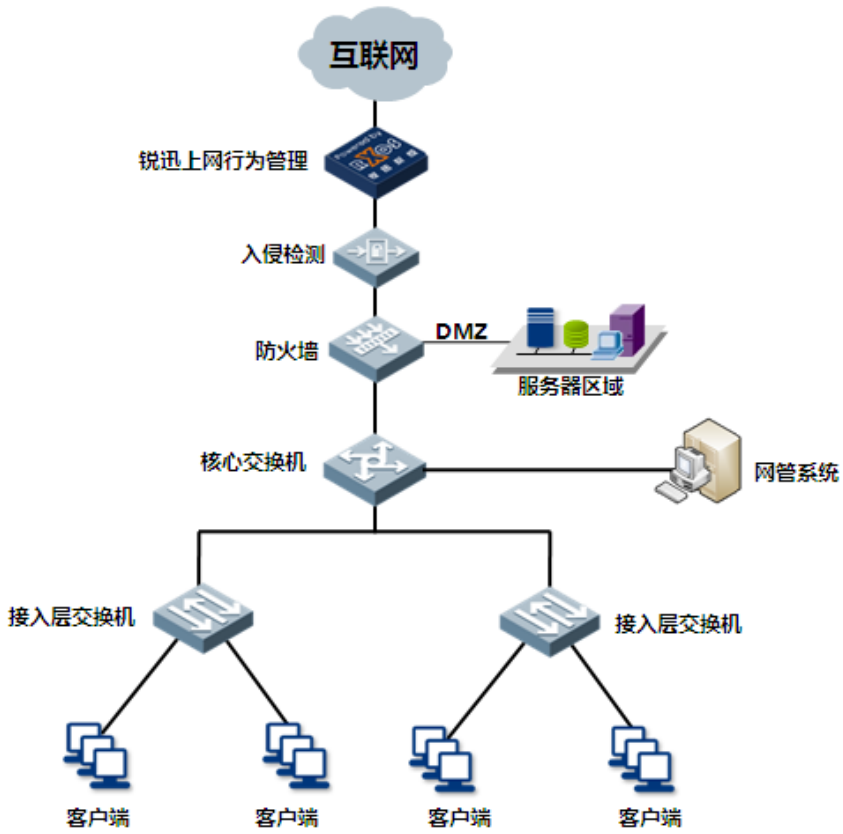



图 21：网关模式部署拓扑

在路由模式下，需要根据实际的上网方式进行不同的配置，通常互联网接入包括：拨号上网、分配固定地址上网两种方式，下面分别介绍如何进行两种上网方式的配置

#### 3.1.2.1 拨号上网配置

当采用拨号上网时，可通过如下方法进行配置：

**第一**：首先在”系统配置-工作模式”页面,配置好 LAN 接口的 IP 地址，然后点击确定，如下图所示：

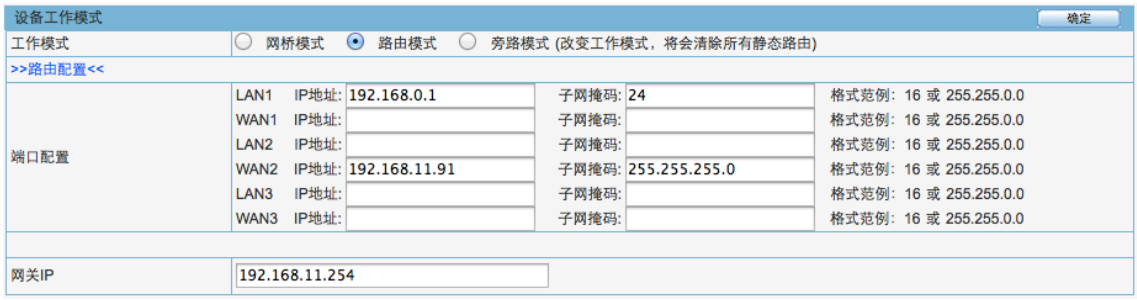



图 22：设备工作模式-路由模式

**第二：**在“网络配置-接口配置-PPPOE”页面,选择外网接口(对应 Cross 设备的 WAN1 或者其他 WAN 口)，配置好拨号账号和密码，点击确定。


图 23：新增 PPPOE 配置

**第三：**在“网络配置-路由配置-静态路由”页面,新增一条默认路由,下一跳指向 pppoe 接口。如果内网是跨三层交换机,有多个内网网段的情况下,还需要配置回程路由,如果内网无三层交换机,可跳过第(4)步骤。


图 24：新增静态路由配置

**第四：**在“网络配置-路由配置-静态路由”页面,新增回程路由,目的 IP，输入内网中的网段，下一跳指向三层交换机上联 Cross 设备接口（LAN1 口）的地址。


图 25：新增静态路由配置

**第五：**在“防火墙-NAT 规则-内网代理”新增规则，流量方向必须选 LAN 口-PPPOE 拨号的接口，如刚创建的 PPPOE 接口名称为 adsl，其他默认。


图 26：新增内网代理规则

### 3.1.2.2 固定地址上网配置

**第一：**首先在"系统配置-工作模式"页面，配置好 LAN 和 WAN(运营商提供的固定 IP)接口的 IP 地址,网关 IP 地址,如下图,点击确定


图 27：设备工作模式

如果内网是跨三层交换机,有多个内网网段的情况下,还需要配置回程路由,如果内网无三层交换机,那么第(2)步骤可以跳过。

**第二：**在"网络配置-路由配置-静态路由"页面,新增回程路由,目的 IP，输入内网中的网段，下一跳指向三层交换机上联 Cross 设备接口（LAN1 口）的地址。


图 28：新增静态路由

**第三：**在"防火墙-NAT 规则-内网代理"新增一条规则,流量方向必须选 LAN1 口-WAN1 的接口,有多个公网 IP，转换后源地址选地址范围。

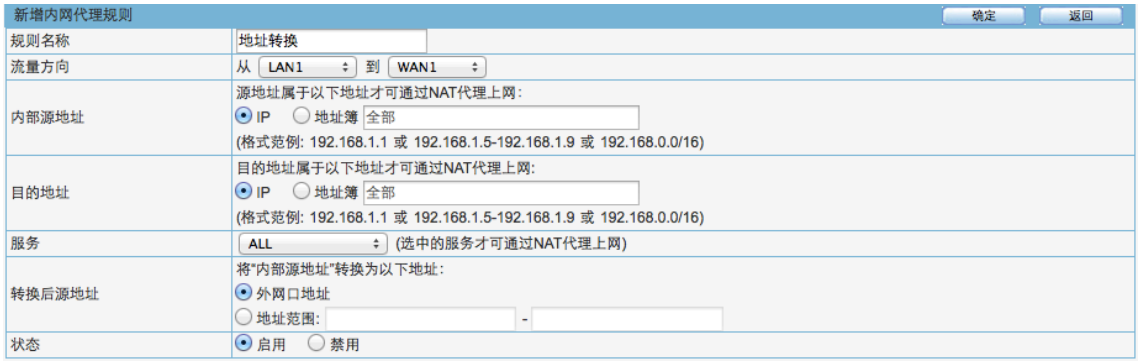



图 29：新增 NAT 配置

### 3.1.3 多互联网出口负载均衡配置

1、首先在”系统配置-工作模式”页面，配置好 LAN1、WAN1 和 WAN2 接口的 IP 地址,网关 IP 地址,如下图

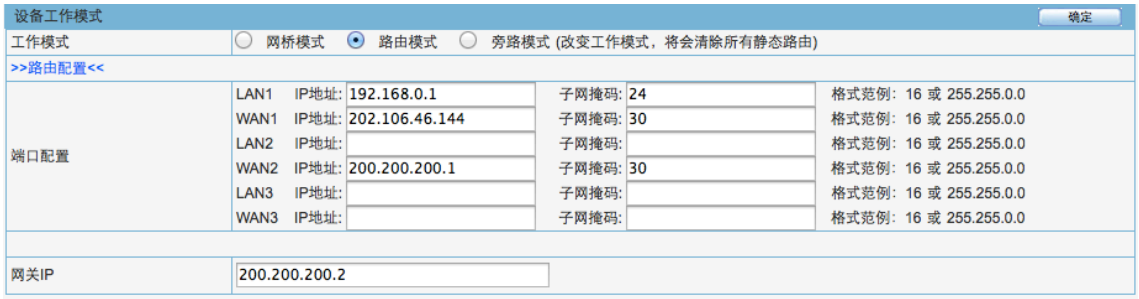



图 30：工作模式配置

如果内网是三层交换机,有多个内网网段的情况下,还需要配置回程路由,如果内网无三层交换机,那么第(2)步骤可以跳过。

2、在“网络配置-路由配置-静态路由”页面,新增回程路由,下一跳指向三层交换机上联接口的地址。


图 31：静态路由配置

3、在“网络配置-路由配置-均衡策略”页面，新增策略，如果是 1 条电信，1 条网通的线路，建议选择最佳路径算法，如果 2 条都是电信，建议选择总流量算法。

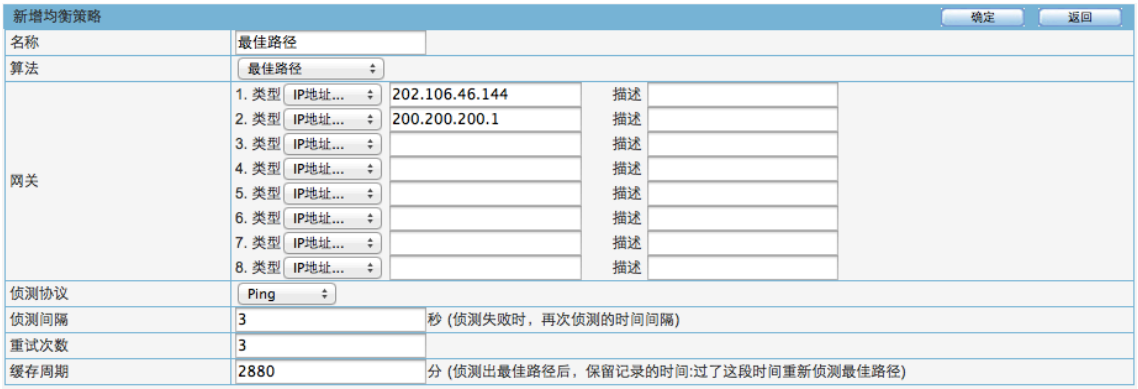



图 32：新增均衡策略-最佳路径算法

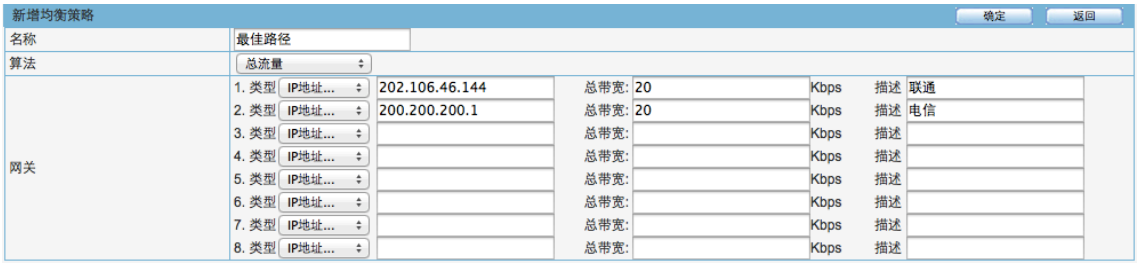



图 33：新增均衡策略-总流量算法

4、如果 2 条链路,1 条失效立马切换到另 1 条线路,必须配置链路健康检查,在“网络配置-路由配置-链路健康检查”页面,新增策略,建好 2 条线路的侦测。

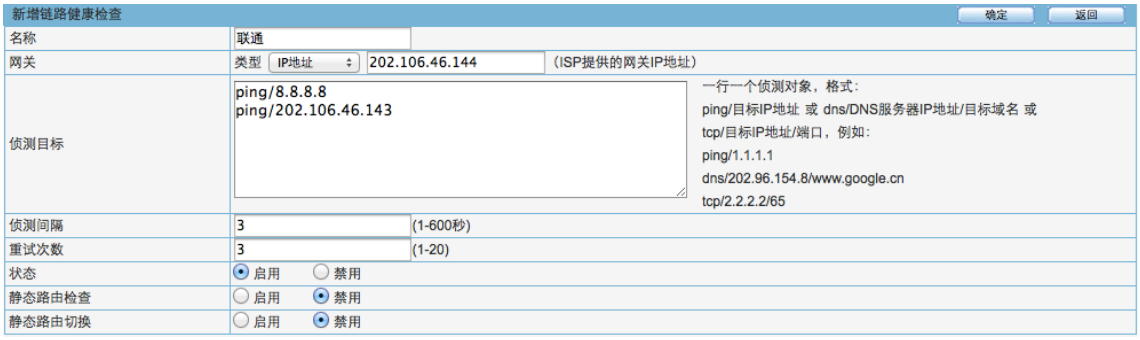



图 34：新建链路健康状况检查

5、在“网络配置-路由配置-策略路由”页面,新增策略,引用刚创建的均衡策略。


图 35：新增策略路由

注:均衡策略算法根据实际环境配置,如果 2 条都是电信线路,可以选择总流量或者下行流量进行负载,如果 1 条电信、1 条网通都是相同带宽,可以选择最佳路径,也可以实现一部分用户走 1 条线路,另一些用户走第 2 条线路,根据实际需要进行配置。

6、在“防火墙-NAT 规则-内网代理”新增二条规则,流量方向必须选 LAN1 口-WAN1、LAN1-WAN2,有多个公网 IP,转换后源地址选地址范围。

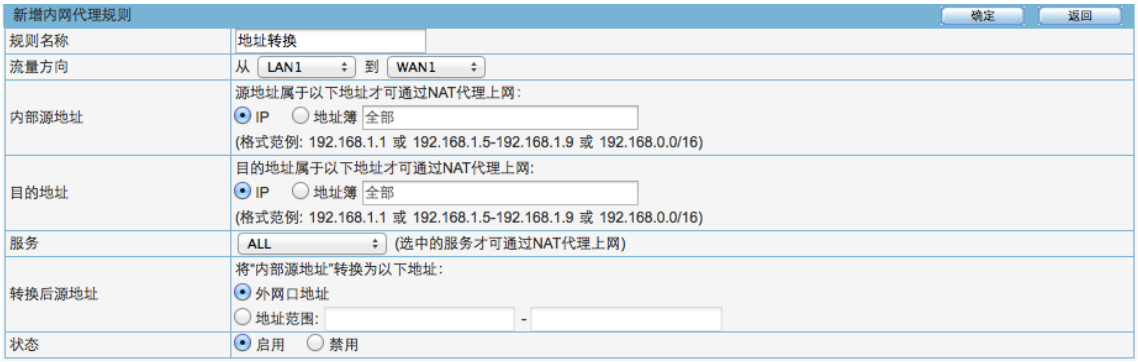



图 36：新增 NAT 配置

## 3.2 系统维护

### 3.2.1 系统升级

用于升级设备的系统文件包括：系统固件、应用特征库、URL 库、授权文件，点击相应升级选项后，将【浏览】按钮，点击后选择升级文件后点击确定完成升级。


图 37：系统升级

注：系统升级包升级后，重启方可生效。其他文件升级后立即生效。

### 3.2.2 自动升级

用于配置应用特征库、URL 库的自动升级，勾选启动自动升级后，再服务器那里填写能够自动升级的服务器地址，再升级延迟区域可以选择升级延迟的时间。如下图所示：


图 38：自动升级配置

### 3.2.3 备份与恢复

**功能描述：**该功能能够将系统的所有配置进行备份与恢复。

**配置路径：**【系统配置】>【系统维护】>【备份与恢复】

进入【备份与恢复】页面，如下图，选择相应配置

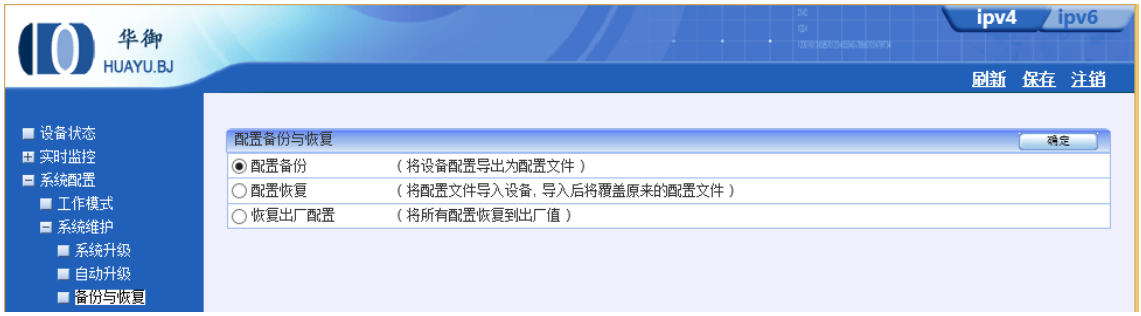



图 39：配置备份与恢复

- 配置备份：系统会将所有的配置以文件的形式存储，然后可将这个配置文件导出到 PC。
- 配置恢复：导入一个配置文件（备份到 PC 的.conf 的压缩文件），导入后会覆盖原来的配置文件，**设备将自动重启**。
- 恢复出厂配置：将设备的配置恢复到出厂值，**设备将自动重启**。

### 3.2.4 重启与关机

**功能描述：**重启或关闭设备

**配置路径：**【系统配置】>【系统维护】>【重启/关闭】

配置描述：进入【重启/关闭】页面，选择重启或关机，再点击<确定>按钮，可重启或关闭设备。如下图：

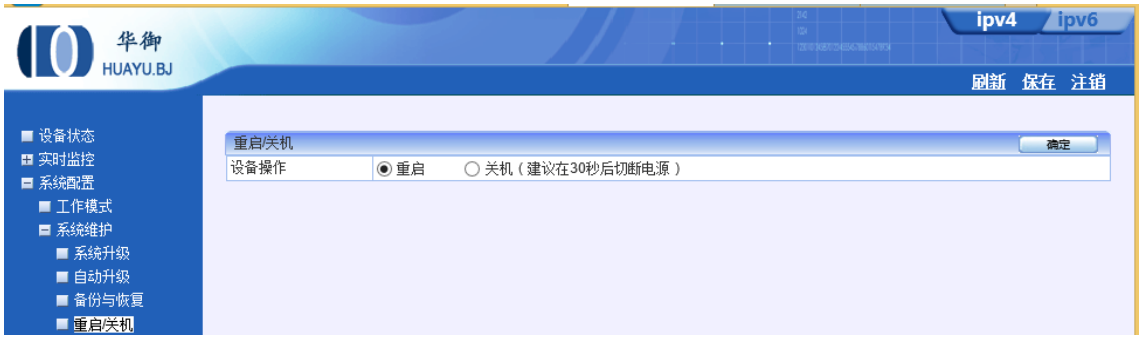



图 40：设备重启或关机

注：设备关机，最好等 20 秒后再切断电源。设备重启的时间为 40s 左右；

## 3.3 系统管理员

**功能描述：**配置登陆系统的管理员用户名、口令、权限策略。

**配置路径：**【系统配置】>【系统管理员】

**配置描述：**进入【系统管理员】页面，可以看到当前的管理员列表，系统默认包括 admin、

guest、reporter 三个用户，每种用户预设了不同的权限，如下图，可以通过点击修改对用户的口令、权限、用户的备注信息。


图 41：系统管理员配置

**系统用户及权限说明：**

1、 系统默认配置了三个管理设备的用户：

- admin：角色为超级管理员，默认密码为 bjhuayu；
- guest：角色为 Guest（访客），默认密码为 guest*PWD；
- reporter：角色为审计管理员，默认密码为 reporter*PWD；

2、系统默认配置了三种权限

- 超级管理员：具有全部编辑、读取权限；
- Guest：仅具读取权限；
- 审计管理员：具有 Reporter 全部的权限；

3、 系统默认的管理员(admin、guest、reporter)不能删除，可修改密码，及备注信息。

4、 系统默认的角色（超级管理员、Guest、审计管理员）不能删除，

5、 新增的用户可以修改密码，可以被删除。

6、 密码的长度为 6-16 位，可以为任何值，但不能为中文。

7、 新增的角色，可以修改，可以被删除。

7、 拥有查看或者配置设备，并且有管理 Reporter 权限的管理员，先登录了设备后，可以不用再次登录即可管理 Reporter。当先登录 Reporter，必须要再次登录才可以管理设备。

### 3.3.1 系统用户登录方式

第一：admin、guest 用户登录

打开浏览器输入 https://192.168.0.1:9090，在出现的登录页面输入用户名与密码进行登录。（其中 192.168.0.1 为设备 IP 地址，如修改，填写修改后的 ip 地址）

第二：reporter 用户登录

打开浏览器输入 http://192.168.0.1:9091，在出现的登录页面输入用户名与密码进行登录。（其中 192.168.0.1 为设备 IP 地址，如修改，填写修改后的 ip 地址）

### 3.3.2 修改默认管理员信息

第一：以管理员身份（admin）登录系统，

第二：点击【系统配置】> 【系统管理员】，将出现系统用户列表页面，如下图所示：


第三：选择相应的用户，点击<修改>选项，如下图所示：

可进行管理员密码修改，用户辅助信息（真实姓名、公司部门等）修改，新增角色信息。


第四：点击<确定>按钮，保存修改。

### 3.3.3 新增用户并分配角色

第一：以管理员身份（admin）登录系统，

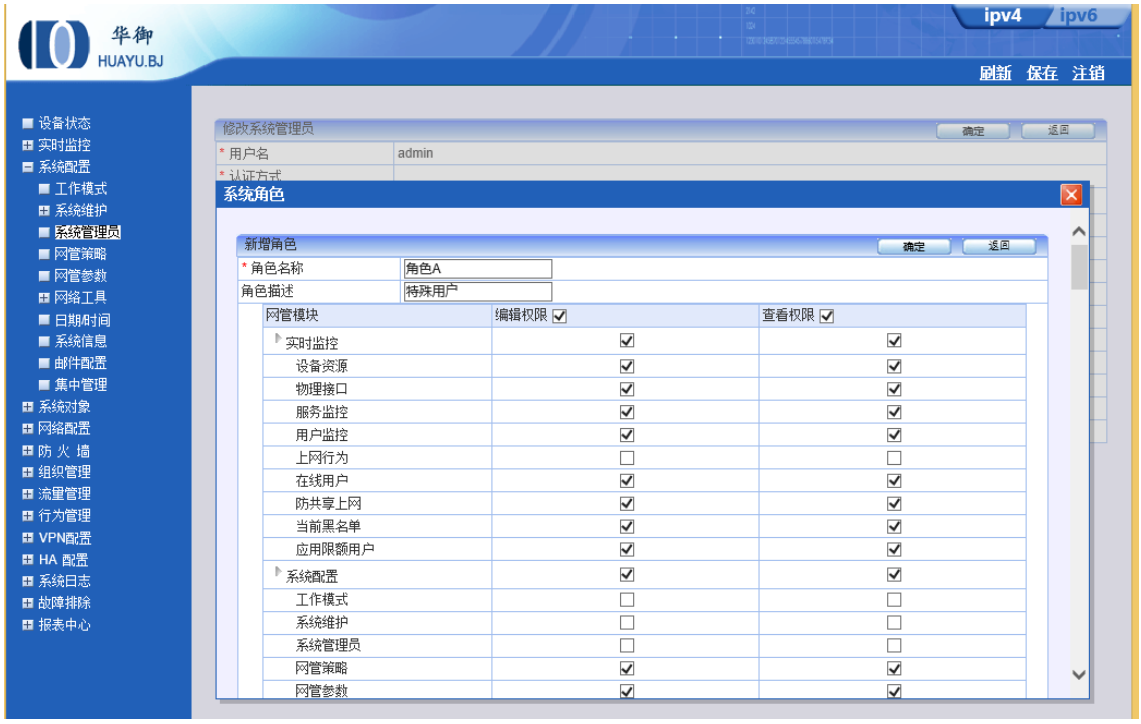
第二：点击【系统配置】> 【系统管理员】，将出现系统用户列表页面，如下图所示：


第三：点击<新增>按钮，增加用户，如下图所示：

设置用户名、认证方式选择口令认证、设置密码、用户详细信息。


第四：点击<系统角色>选项，如下图所示


第五：点击<新增>按钮，如下图所示，输入角色的名称，角色描述，修改需要分配给新用户的权限。然后点击<确定>进行保存。




第六：在角色地方，选择刚才新建的角色即可，如下图所示：


第七：修改完成之后，点击<确定>按钮，将返回用户列表，此时可以看到刚才新建的用户 user1，如下图所示：

## 3.4 网管策略

**功能描述：**设置网管策略，可允许部分 IP 能网管设备，以限制非法用户访问设备。

**配置路径：**【系统配置】>【网管策略】

**配置描述：**进入【网管策略】页面，如下图所示，点击新增，输入规则名称，在 IP 地址栏中输入可以管理的 IP 地址。策略类型选择为“根据下面策略进行控制”时，如果允许网管设备的 IP 里没有配置任何 IP 地址，则所有 IP 都可以网管设备；如果配置了 IP 地址，则只有这些 IP 可以网管设备。

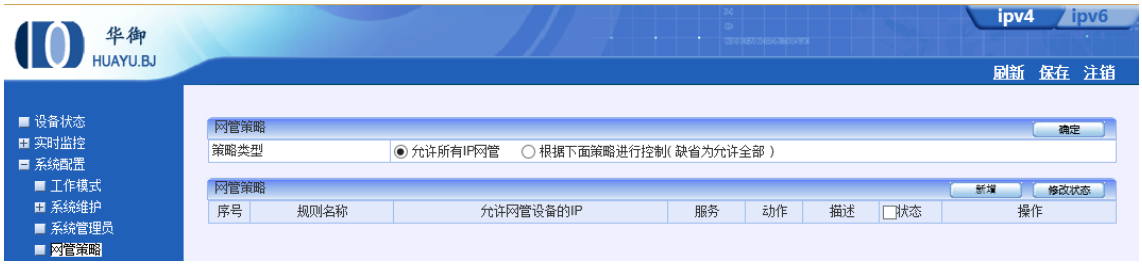



图 42：系统网管策略

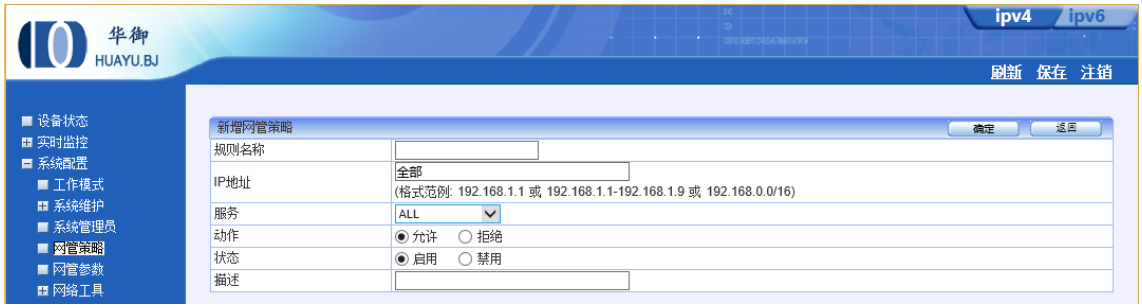



图 43：新增网管策略

## 3.5 网管参数

**功能描述：配置**对设备访问方式、访问端口、登陆超时、管理员登陆最大次数，管理员超出登陆次数惩罚时间。

**配置路径：**【系统配置】>【网管参数】，设置相应值之后，点击确定后生效。

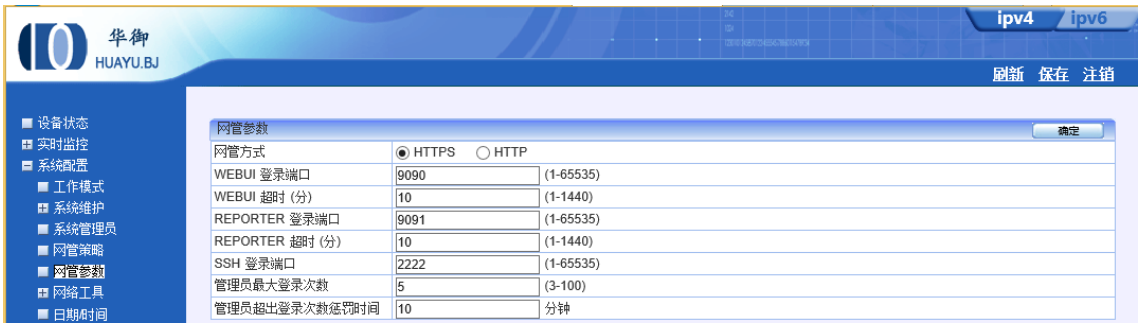



图 44：网管参数配置

## 3.6 网管工具

“网络工具”包括 Ping 和 Tracerute，可以实现通过设备进行 ping、Traceroute 相应地址进行测试。如下图所示：

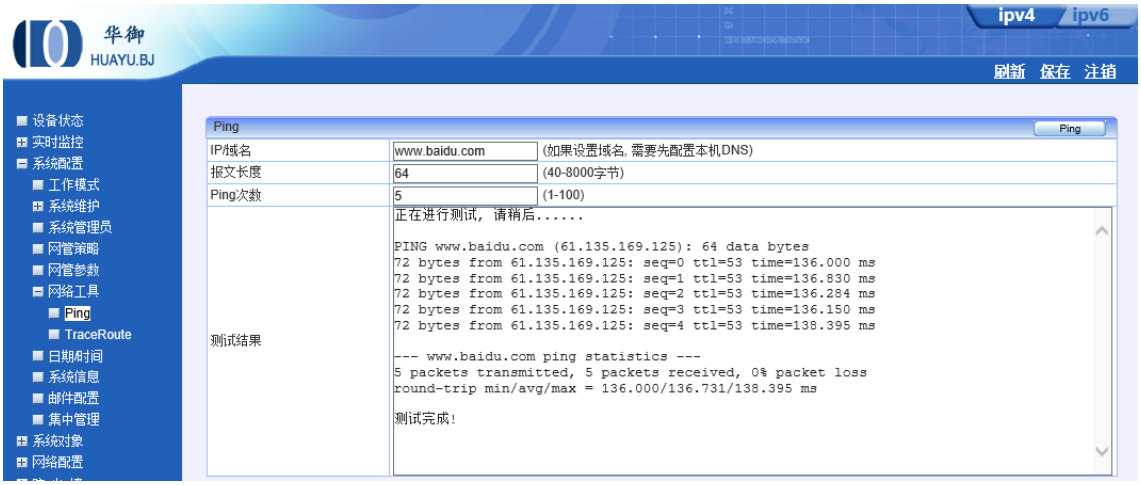



图 45：Ping 网络工具

参数说明：

- IP/域名：目的 IP 地址或者域名，如果设置域名，需要先配置本机 DNS。
- 超时设置：1-10 秒，缺省 10 秒。
- 最小 TTL：1-255，缺省 1。
- 最大 TTL：1-255，缺省 10。

## 3.7 系统时间

**功能描述：**用于设定设备的系统时间。

**配置路径：**【系统配置】>【系统时间】，设置界面如下图：


图 46：系统日期时间配置

如需启用 SNTP 则勾选“自动与 SNTP 服务器同步”，然后可配置 SNTP 服务器和同步间隔。

## 3.8 系统信息

**功能描述：**设备基本信息描述。

**配置路径：**【系统配置】>【系统信息】，配置页面如下：

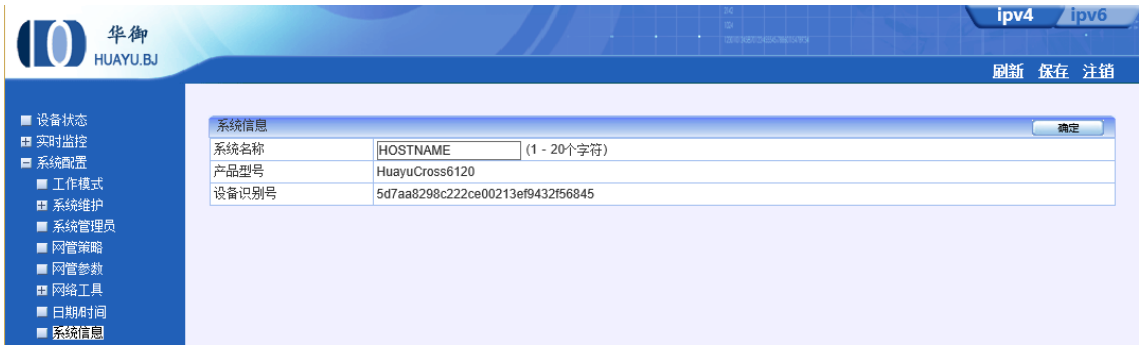



图 47：系统信息配置

## 3.9 邮件配置

**功能描述：**配置设备发送告警邮件的参数。

**配置路径：**【系统配置】>【邮件配置】，配置页面如下：

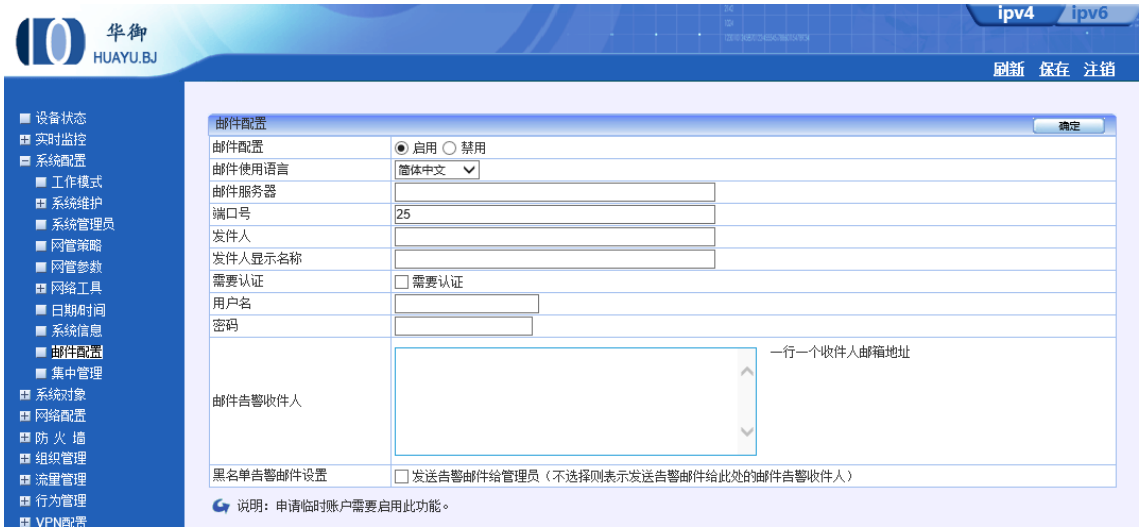



图 48：邮件配置

参数说明：

- 邮件使用语言：发送邮件时使用的语言。
- 邮件服务器：设置邮件发服务器地址。
- 端口号：设置邮件端口号。
- 发件人：设置告警邮件的发送者。
- 发件人显示名：设置告警邮件发送者显示的姓名。
- 需要认证：选择是否需要进行密码安全认证。
- 用户名：需要安全认证时，必须填入用户名。
- 密码：需要安全认证时，必须填入用户密码。
- 邮件告警收件人：设置告警邮件的收件人邮箱地址，可以设置多个，一行一个收件人地址。

## 3.10 集中管理

**功能描述：**配置设备是否加入集中管理平台。

**配置路径：**【系统配置】>【集中管理】，配置页面如下：


图 49：集中管理配置

参数说明：

- 启用集中管理：配置设备是否加入集中管理，加入后即成为集中管理的客户端或网点。
- 中兴端 IP 地址：配置集中管理的中心端的 IP 地址。
- 通讯端口：配置与中心端通信的端口号，默认是 1194。须与中心端配置的通讯端口一致。
- 网点编号：配置设备在中心端的区域结构中显示的网点编号。
- 数据加密密钥：与中心端通信时的数据是加密的，此处配置的密钥与中心端上该网点密钥一致。
- 已获取的虚拟 IP：中兴端分配给设备的虚拟 IP 地址。
- 与中兴端连接状态：显示与中心端的连接状态。“连接”表示与中心端的数据通道连接正常，“断开”表示与中心端的数据通道连接已断开。“最后响应时间”表示最后一次与中心端通信的时间。

# 第4部分 系统对象

“系统对象”包括地址薄、网络服务、时间计划、URL 库、关键字、文件类型等。

## 4.1 地址薄

**功能描述：**用于定义一个包含某些 IP 地址的 IP 地址组，这个 IP 组可以是任意的一个 IP、一段 IP 或者 IP 范围的任意组合。“地址簿”可在【网络配置】、【流量管理】、【行为管理】定义的规则中引用。

**配置路径：**【系统对象】>【地址簿】,如下图所示

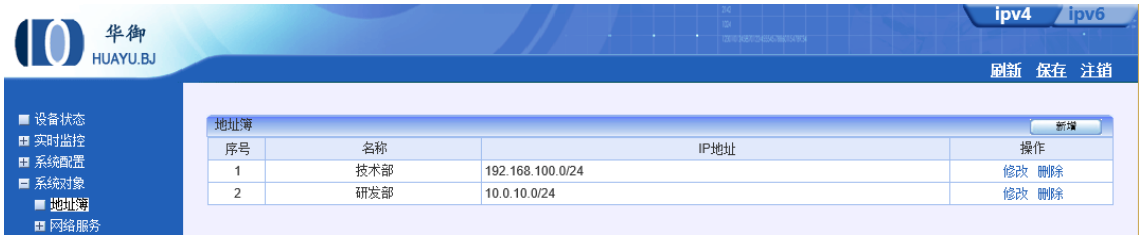



图 50：地址薄列表

**操作方法：**点击表格右上角的<新增>按钮，增加地址簿，并填入地址簿的第一个 IP/IP 段/IP 范围。点击删除、修改按钮可删除或修改地址薄中的内容。

注：如果某地址簿已经被引用，则不能被删除。删除前必须先解除引用。

## 4.2 网络服务

网络服务共分为：内置服务、自定义普通服务、自定义特征识别、自定义论坛网评识别、协议剥离。这些服务在【流量管理】中将被引用。其中自定义普通服务和常用服务为基于端口的服务，其余的都是基于内容识别的服务。

### 4.2.1 内置服务

可以查看系统中包含识别的网络应用，如下图所示：


图 51：内置服务列表

### 4.2.2 自定义普通服务

可以通过 TCP、UDP 端口号、ICMP 协议、IP 协议号，来进行定义，如下图所示：


图 52：自定义普通服务

### 4.2.3 自定义特征识别

进入之后可以看到自定义特征识别的列表，点击上方的新增，可以新增自定义特征识别。


图 53：自定义应用特征设别

参数说明：

- 协议类型：选择本条规则的协议类型，可选择 TCP、UDP 或者 TCP+UDP
- 目的端口：可选择所有端口或者指定的端口范围
- IP 地址：可选择所有 IP 或者指定的 IP 地址
- 数据长度：不计算 TCP/UDP 的头部，即 Payload 的长度。符合设定长度的报文才会被匹配。
- 特征字符串：报文的特征，用正则表达式来表示。
- 优先级：默认低于系统定义的特征。

### 4.2.4 自定义论坛/网页评论特征

进入后，可以看到自定义论坛/网页评论特征列表，点击左上角的<新增>按钮，将出现下图所示：

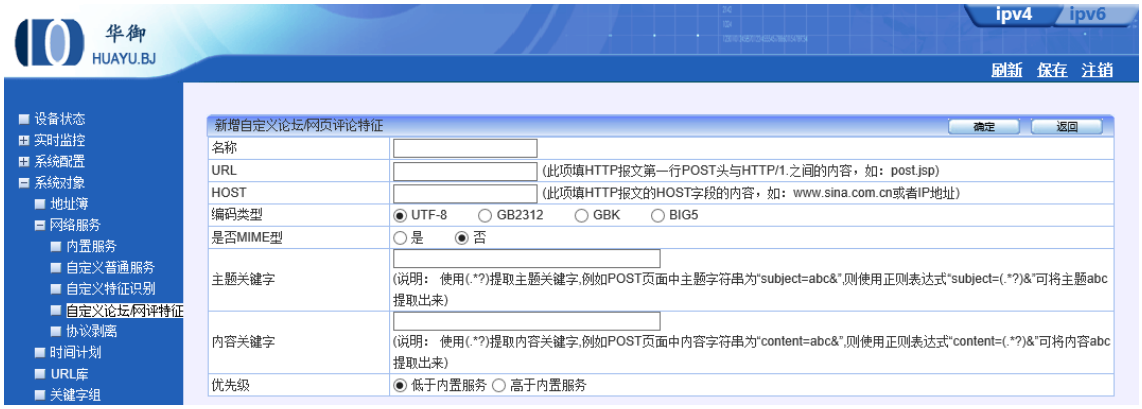



图 54：自定义论坛/网评特征识别

参数说明：

- URL：此项填 HTTP 报文第一行 POST 头与 HTTP/1.之间的内容，如：post.jsp
- HOST：此项填 HTTP 报文的 HOST 字段的内容，如：www.sina.com.cn 或者 IP 地址；
- 编码类型：可选择四种编码中的其中 1 种；
- 是否 MIME 型：选择是或者否。
- 主题关键字：使用正则表达式来提取主题关键词。
- 内容关键字：使用正则表达式来提取内容关键词。
- 优先级：选择低于内置服务或高于内置服务。

### 4.2.5 协议剥离

当经过的数据包中封装了特殊的协议时，可以通过协议剥离来正常识别网络中的流量，系统默认支持对 L2TP 协议剥离、GRE 协议剥离，除此之外提供了自定义协议剥离接口，管理员可以自定义协议剥离。如下图所示：


图 55：协议剥离

## 4.3 时间计划

**功能描述：**用于定义时间段，然后可在【防火墙】、【流量管理】、【行为管理】中引用，以控制这些策略生效或失效的时间，从而可对各种策略分时间段管理。

**配置路径：**【系统对象】>【时间计划】

**配置描述：**进入【时间计划】页面，可以看到当前已配置的时间计划，如下图所示：


图 56：时间计划列表

点击<新增>按钮，可以增加时间计划，如下图所示：点击<新增时间计划>可选择周一到周日中的任意时间段，增加好之后，可以在时间分布预览中看到定义的时间段。

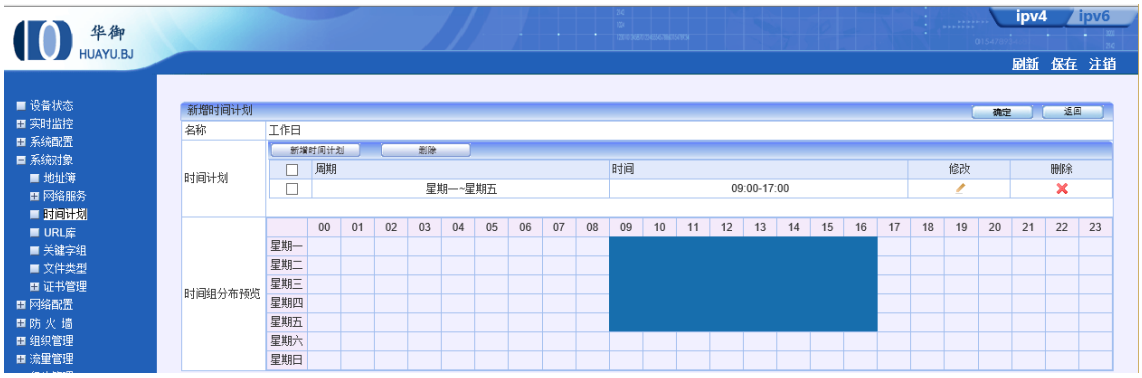



图 57：新增时间计划

## 4.4 URL 库

**功能描述：**用于查看系统 URL 的分类和自定义的 URL 库。URL 库可用于【行为管理 > 上网策略对象 > 上网权限策略】，实现对 URL 的过滤。

**配置路径：**【系统对象】>【URL 库】

**配置描述：**进入【URL 库】页面，可以看到当前的内置 URL 库，如下图所示：


图 58：内置 URL 库列表

**自定义 URL 库：**当管理员需要怎对特殊的网站进行控制，可以点击自定义 URL 库，先进行定义，如下图所示，新建 URL 库时，输入名称，描述（选填），URL 进行增加。

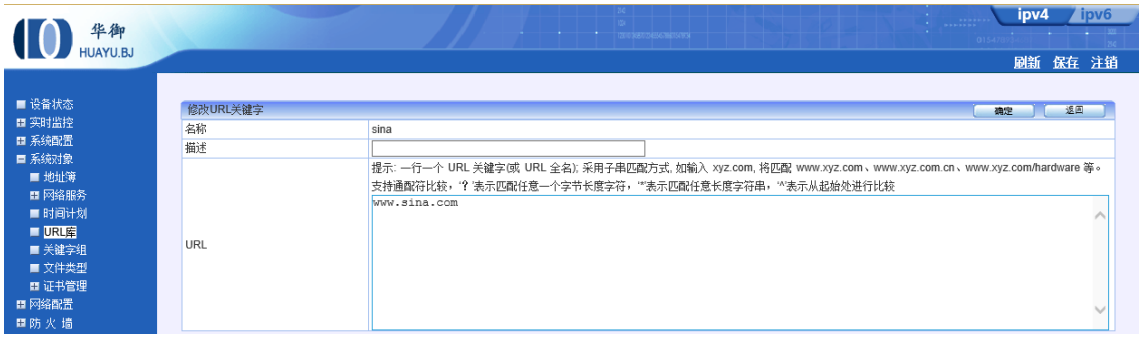



图 59：自定义 URL 库

在“URL”输入框内填写 URL，一行一个 URL 关键字(或 URL 全名)。采用子串匹配方式，如配置 xyz.com，将匹配 www.xyz.com、www.xyz.com.cn、www.xyz.com/hardware 等。

## 4.5 关键字组

**功能描述：**用于设置关键字，并把关键字分组，这些关键字组可用于【上网行为管理】中限制某些关键字的搜索和上传。

**配置路径：**【系统对象】>【关键字组】

**配置描述：**进入【关键字组】页面，可以看到当前已定义的关键字组，然后点击新增按钮增加关键词，如下图所示：

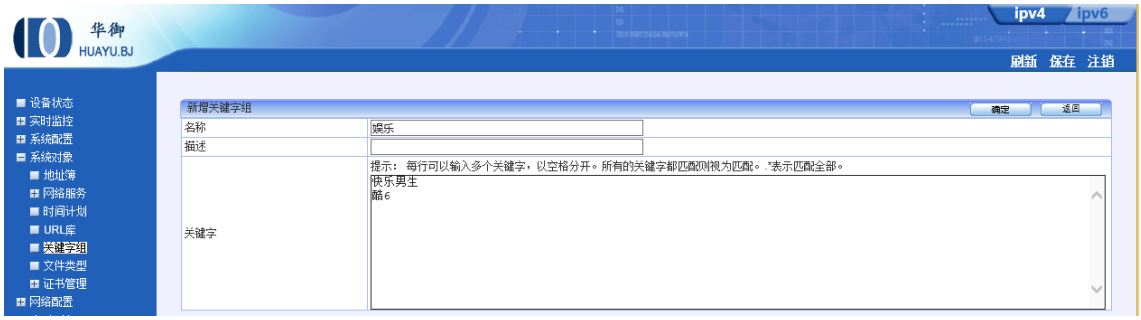



图 60：新增关键字组

## 4.6 文件类型

**功能描述：**用于定义文件类型，并把文件类型分组。这些文件类型可用于【上网行为管理】中限制这些类型的文件的上传和下载。

**配置路径：**【系统对象】>【文件类型】

**配置描述：**进入【文件类型】页面，可以看到当前已定义的文件类型分组。点击<新增>按钮来增加文件类型，如下图所示：

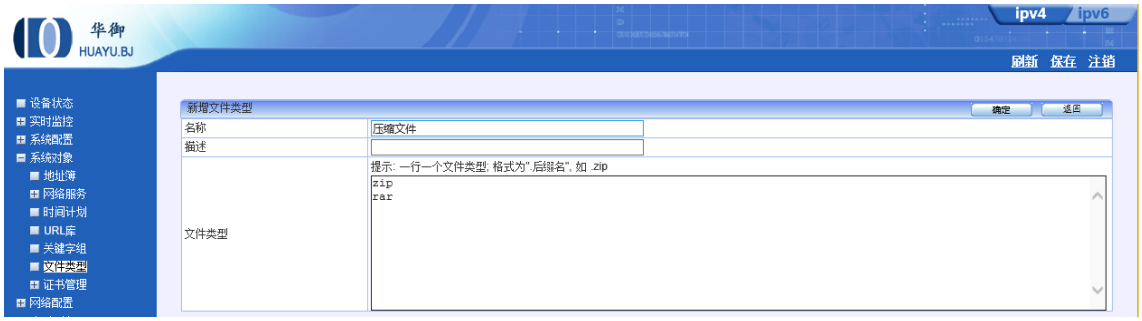



图 61：新增文件类型

# 第5部分 网络配置

“网络配置”包括：物理接口、配置 IP 地址、路由配置、本地 DNS、ARP 表、GRE 隧道、PPPOE 和 DHCP 配置。

## 5.1 接口配置

包括物理接口、VLAN 接口、PPPoE、GRE 隧道 四部分。

### 5.1.1 物理接口

**功能描述：**物理接口指和产品面板上一一对应的数据接口，不同产品型号接口数目不一样。

**配置路径：**【网络配置】>【接口配置】>【物理接口】，配置页面如下图所示：

**配置描述：**

第一：进入【物理接口】页面，如下图：


图 62：物理接口列表

**提示：**物理接口的状态为“未连接”时，工作速率为 0 M。

**第二：**点击操作栏的<修改>按钮，对物理接口的参数进行配置，如下图所示：

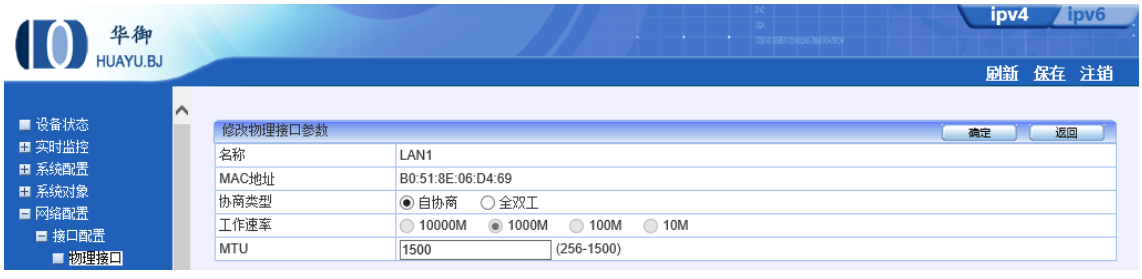



图 63：修改物理接口参数

### 5.1.2 链路聚合

**功能描述：**将 2 个或多个物理端口组合在一起成为一条逻辑的路径从而增加在设备和网络节

点之间的带宽。

**配置路径：**【网络配置】>【接口配置】>【链路聚合】，配置页面如下图所示：

**配置描述：**

**第一：**进入【链路聚合】页面，如下图所示，查看当前聚合的链路。


图 64：链路聚合列表

**第二：**点击<新增>按钮，进入链路聚合新增选项，如下图所示，选择物理接口，选择均衡算法（轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应）、侦测目标。


图 65：新增链路汇聚

**注：**修改“均衡算法”原先配置的静态路由将清空，请重新配置静态路由。

### 5.1.3 VLAN 接口

**功能描述：**通过配置 802.1Q 的 VLAN 接口地址，来实现 VLAN 间的数据转发，设备产品支持连接二层交换机的 TRUNK 口。

**配置路径：**【网络配置】>【接口配置】>【VLAN 接口】

**第一：**进入【VLAN 接口】界面，可以看到当前已经建立的 VLAN 接口。如下图：


图 66：VLAN 接口列表

接口名称是物理接口和 VLAN ID 的组合。例如，WAN4.20 表示物理接口为 WAN4，VLAN ID 为 20 的 VLAN 接口。然后在【网络配置>配置 IP 地址】处，可以为 VLAN 接口配置 IP 地址。

**第二：**点击<新增>按钮，增加 VLAN 接口。如下图：

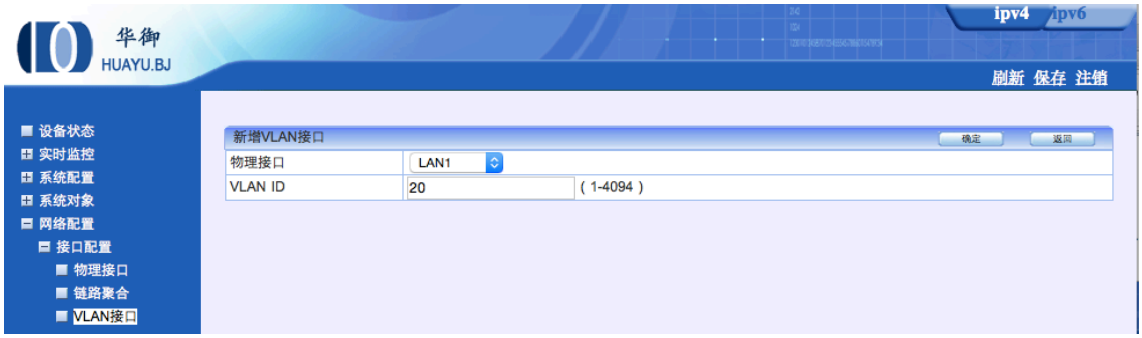



图 67：新增 VLAN 接口

### 5.1.4 PPPoE

**功能描述：**配置 PPPoE 拨号账号，实现 PPPoE 拨号。

**配置路径：**【网络配置】>【接口配置】>【PPPoE】

**配置描述：**进入【PPPoE】界面，可以看到当前已经建立的 PPPoE 配置。如下图所示，点击<新增>按钮，在出现的对话框中，输入名称，选择拨号的端口，输入拨号用户名与密码，然后点击确定。


图 68：PPPOE 配置列表

### 5.1.5 DHCP 客户端

**功能描述：**如果 WAN 口的地址为 DHCP 动态分配的，在此处可以启用 WAN 口的 DHCP 客户端功能。

**配置路径：**【网络配置】>【接口配置】>【DHCP 客户端】

**配置描述：**进入【DHCP 客户端】界面，可以看到当前 DHCP 客户端配置。如下图：


图 69：WAN 口 DHCP 客户端配置

### 5.1.6 GRE 隧道

**功能描述：**配置 GRE 隧道，用于在两台 Cross 设备之间建立隧道

**配置路径：**【网络配置】>【接口配置】>【GRE】

**配置描述：**

**第一：**进入【GRE】界面，可以看到当前已经建立的 GRE 配置。如下图：


图 70：GRE 隧道列表

**第二：**点击<新增>按钮，增加 GRE 隧道配置。如下图：


图 71：GRE 隧道配置

**参数说明：**

- 隧道名称：为 GRE 隧道取的名字。
- 隧道IP：隧道的标识地址，可设置任意 IP，隧道两端的标识地址应该配置为同一网段。
- 子网掩码：隧道IP的子网掩码
- 源地址：隧道的源端地址，与本端发出 GRE 报文的接口地址相同或同网段
- 目的地址：隧道的目的端地址，与对端接收 GRE 报文的接口地址相同或同网段

注：配置完 GRE 隧道后，在【网络配置 > 路由配置】添加路由，选择 GRE 隧道。

## 5.2 配置 IP 地址

**功能描述：**用于给设备的接口或网桥配置 IP 地址。在单网桥模式下，可对网桥和其它独立的网口配置 IP 地址；在路由模式下可为每个接口配置 IP 地址。

**配置路径：**【网络配置】>【配置 IP 地址】

**配置描述：**

第一：进入【配置 IP 地址】页面，可查看当前配置的 IP 地址信息，如下图所示：


图 72：配置 IP 地址列表

**第二：**点击<新增>按钮，为接口增加 IP 地址。新增页面的物理接口名称随工作模式的改变而不同，单网桥时物理接口名称为 Bridge1、LAN2、WAN2，……；双网桥时物理接口名称为：Bridge1 和 Bridge1，……；路由模式时时物理接口名称为 LAN1、LAN2、WAN1、WAN2，……。下图是四个网口，单网桥模式下新增 IP 地址的页面：


图 73：新增 IP 地址

**注：**1、可对物理接口、VLAN 接口、网桥配置 IP 地址。

2、不同的接口不能配置相同网段的 IP 地址。

3、每个接口可配置多个不同网段的 IP 地址。

## 5.3 静态路由

**功能描述：**配置静态路由。

**配置路径：**【网络配置】>【路由配置】>【静态路由】

**配置描述：**

**第一：**进入【静态路由】页面，如下图所示：


图 74：静态路由列表

**第二：**进入点击<新增>按钮，增加静态路由。如下图：


图 75 新增静态路由

网关可以选择为“IP 地址”、“GRE 隧道”或者“PPPoE”。选择 GRE 隧道和 PPPoE，需先分别到【网络配置 > GRE 隧道】和【网络配置 > PPPoE 】页面配置 GRE 隧道 PPPoE 拨号。

**注：**直连路由不可以修改和删除。<删除所有>按钮表示删除所有静态路由。

## 5.4 策略路由

### 5.4.1 多链路负载均衡配置

**功能描述：**策略路由主要用户链路负载均衡配置。

**配置描述：**配置链路负载均衡的方法请按照下面所示方法配置。

**第一：**在”系统配置-工作模式”页面，配置好 LAN1、WAN1 和 WAN2 接口的 IP 地址,网关 IP 地址,如下图

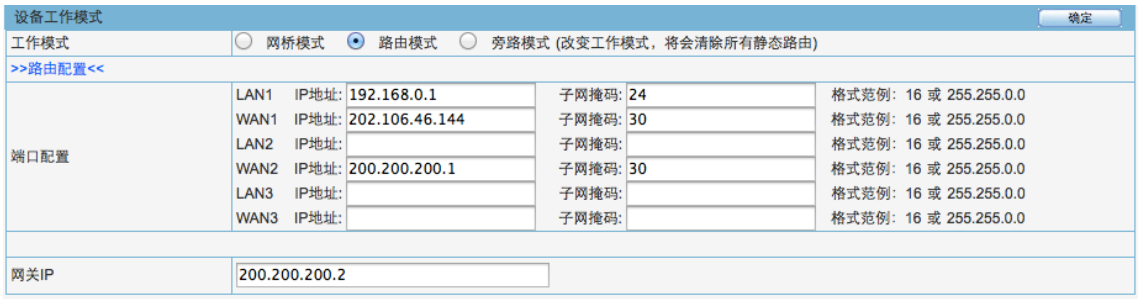



图 76：设备工作模式

如果内网是三层交换机,有多个内网网段的情况下,还需要配置回程路由,如果内网无三层交换机,那么第(2)步骤可以跳过。

**第二：**在“网络配置-路由配置-静态路由”页面,新增回程路由,下一跳指向三层交换机上联接口的地址。


图 77：新增静态路由

**第三：**在“网络配置 > 策略路由 > 均衡策略”页面，新增策略，如果是 1 条电信，1 条网通的线路，建议选择最佳路径算法，如果 2 条都是电信，建议选择总流量算法。

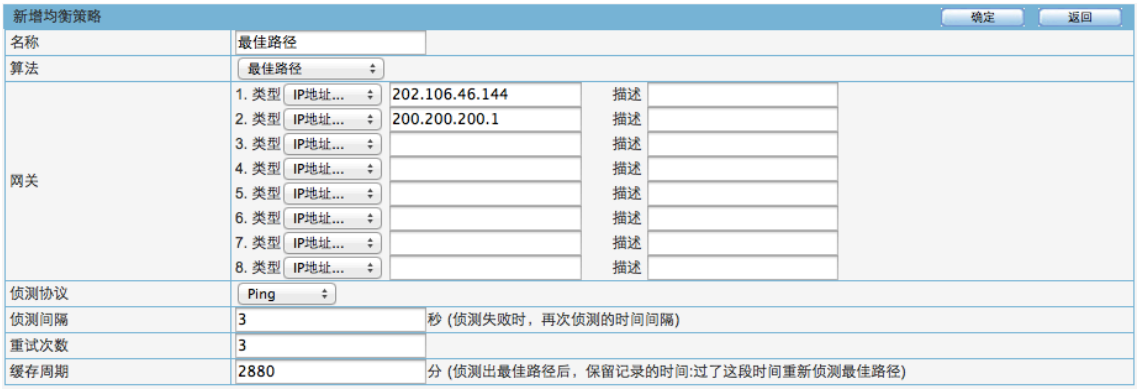



图 78：新增均衡策略


图 79：新增均衡策略

**第四：**如果 2 条链路,1 条失效立马切换到另 1 条线路,必须配置链路健康检查,在“网络配置 > 策略路由 > 链路健康检查”页面,新增策略,建好 2 条线路的侦测。

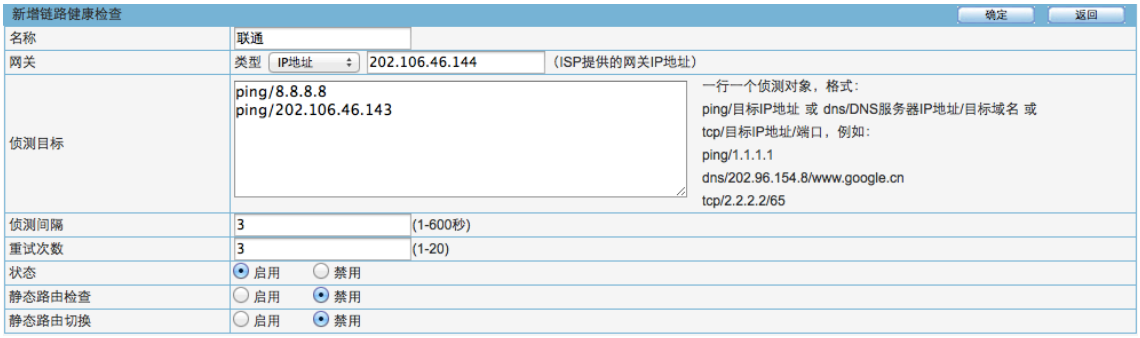



图 80：新增链路健康检查

**第五：**在“网络配置 > 策略路由 > 策略路由”页面,新增策略,引用刚创建的均衡策略。

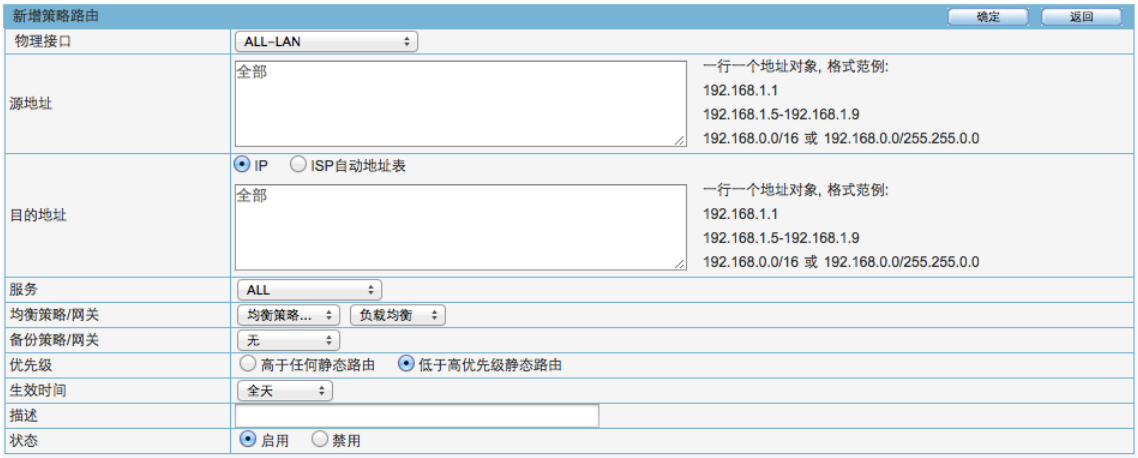



图 81：新增策略路由

注:均衡策略算法根据实际环境配置,如果 2 条都是电信线路,可以选择总流量或者下行流量进行负载,如果 1 条电信、1 条网通都是相同带宽,可以选择最佳路径,也可以实现一部分用户走 1 条线路,另一些用户走第 2 条线路,根据实际需要进行配置。

### 5.4.2 持续路由

**功能描述：**持续路由，某些银行网站使用策略路由时，可能会出现无法登录的问题，此时需

要使用持续路由。持续路由是指当要建立连接时，首先依照“均衡策略”设定的算法进行选路。当决定使用某条链路后，才参考“持续路由”设定的规则，决定是否固定使用这条链路。

**第一：**进入【持续路由】页面，可以看到当前配置的持续路由规则。如下图所示：


图 82：持续路由列表

超时时间：固定使用某条链路的最大等待时间，默认为 60 秒。根据“均衡策略”选定使用某条链路后，并且“持续路由”规则决定要固定使用这条链路，但在 60 秒内都没有报文再次使用这条“持续路由”规则进行选路，则新的报文再次选路时，需要首先依照“均衡策略”设定的算法进行重新选路，再参考“持续路由”设定的规则决定是否固定使用那条链路。

**第二：**进入点击<新增>按钮，增加持续路由规则。如下图：


图 83：新增持续路由

**参数说明：**

- 名称：持续路由规则的名称。
- 源地址：匹配报文的源地址，可以选择为地址簿或者输入 IP 地址。输入 IP 地址的格式范例：192.168.1.1、192.168.1.5-192.168.1.9、192.168.0.0/16 或 192.168.0.0/255.255.0.0。

- 目的地址：匹配报文的目的地址，可以选择为地址簿或者输入 IP 地址。输入 IP 地址的格式范例：192.168.1.1、192.168.1.5-192.168.1.9、192.168.0.0/16 或 192.168.0.0/255.255.0.0。
- 动作：选择为“使用持续路由”或“不使用持续路由”。

## 5.5 DNS 配置

**功能描述：**配置设备的 DNS 服务器，以便于设备自身能访问互联网。

**配置路径：**【网络配置】>【本机 DNS】

**配置描述：**进入【DNS 配置】页面，配置 DNS 服务器。如下图所示：

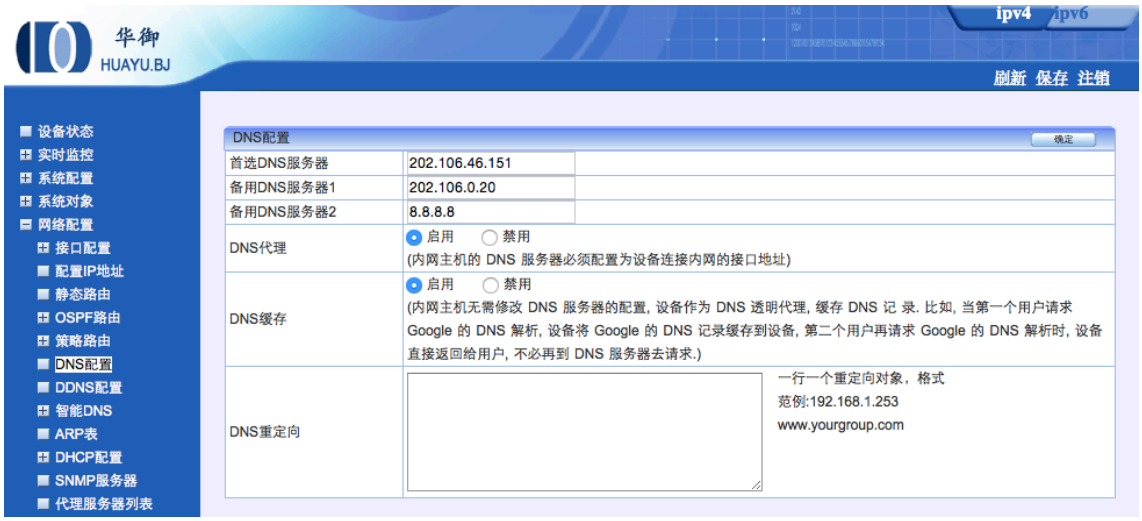



图 84：DNS 配置

参数说明:

- 首选 DNS 服务器/备份 DNS 服务 1/备份 DNS 服务 2:配置设备的 DNS 服务器的 IP 地址。
- DNS 代理:内网的 DNS 代理功能。内网主机的 DNS 服务器必须配置为设备连接内网的 LAN 口的 IP 地址。
- DNS 缓存:内网的 DNS 缓存器。内网主机无需修改 DNS 服务器的配置,设备作为 DNS 透明代理，缓存 DNS 记 录。 比如，当第一个用户请求 Google 的 DNS 解析,设备将 Google 的 DNS 记 录缓存到设备，第二个用户再请求 Google 的 DNS 解析时，设备直接返回给用户，不必再到 DNS

## 5.6 DDNS 配置

**功能描述:** DDNS 可以捕获用户每次变化的 IP 地址,然后将其与域名相对应,这样其他上网用

户就可以通过域名来访问。

**配置路径:**【网络配置】>【DDNS 配置】 配置描述:进入【DDNS 配置】页面,配置 DNS 服务器。如下图所示:


图 85：DDNS 配置

参数说明:

- 服务提供者:提供 DDNS 服务的服务器域名,可选择为 [花生壳(www.oray.net)] 或 [DynDns( www.dyndns.com )]。
- 用户名:在 DDNS 服务商那里注册的用户名。
- 密码:在 DDNS 服务商那里注册的用户名对应的密码。
- DDNS 状态:当前 DDNS 的工作状态。
- 域名信息:为本用户名分配的域名,以后不论 IP 地址如何变化,则会自动对应到该域名信息。

**注：**首先需要在 DDNS 服务商那里注册一个可用的用户名，然后 DDNS 服务就会为该用户名分配一个域名。当启用 DDNS 功能后,DDNS 服务会将动态变化的 IP 对应到该域名。

## 5.7 ARP 表

**功能描述：**查看 ARP 表，配置静态 ARP。

**配置路径：**【网络配置】>【ARP 表】

**配置描述：**

**第一：**进入【ARP 表】页面，可查看到当前 ARP。如下图：


图 86：ARP 表

类型为“动态”代表自动学习到的 ARP 条目；为“静态”代表将固定的 IP 和 MAC 绑定在一起。

**第二：**当选“静态”列的复选框，再点击<转为静态>，可以将动态学习到的 ARP 转换为静态 ARP。当类型为“静态”时，对应 ARP 条目的“静态”列的复选框消失。勾选表头的“静态”复选框，可以选中所有的动态 ARP 条目。

**第三：**点击<新增>按钮，可添加静态 ARP 条目，如下图：


图 87：新增静态 ARP

## 5.8 DHCP 配置

**功能描述：**配置 DHCP 基本参数。

**配置路径：**【网络配置】>【DHCP 配置】>【基本参数】

**配置描述：**

**第一：**进入【基本参数】页面，可以看到当前已建立的 DHCP 配置。如下图：


图 88：DHCP 配置

**第二：**进入点击<新增>按钮，增加 DHCP 配置。如下图：


图 89：DHCP 基本参数

**参数说明：**

- 接口名称：选择启用 DHCP 服务的接口名称。
- 首选 DNS 服务器/备用 DNS 服务器：配置 DHCP 客户端所获得的 DNS 配置信息。
- IP 地址池：配置 DHCP 客户端所获得的 IP 地址的范围。一行一个地址，格式范例：192.168.2.2 或 192.16.2.2-192.168.2.253。地址范围必须与接口地址同网段，多个范围间地址不能重叠。
- 固定 IP ：可根据 MAC 绑定 IP， 即根据 MAC 地址把固定的 IP 地址分配给对应的客户端。一行一个固定 IP，固定 IP 的地址必须在 IP 地址池范围内，名称不能为中文。格式范例：名称/IP/MAC, 如 Tom/192.168.1.1/00:19:21:3f:a1:11
- 子网掩码：配置 DHCP 客户端所获得的 IP 地址的掩码。

- 网管 IP：配置 DHCP 客户端所获得的网关 IP 地址。一般为第一行选择的接口的 IP。
- 租用期限：设置 DHCP 获得的 IP 地址的有效期，默认为永远有效。

**注：**

1、配置 IP 地址池时，一行一个地址范围，起始地址与结束地址间以英文中线(-)隔开。

2、地址范围必须与 LAN 口地址同网段，不要包含网络地址及网段广播地址，多个范围间地址不能重叠。

3、固定 IP 地址应包含在 IP 地址池中。

4、每个接口都可以启用 DHCP，包括桥接口，如 bridge1。

## 5.9 DHCP 中继

**功能描述：**配置 DHCP 中继。

**配置路径：**【网络配置】>【DHCP 配置】>【DHCP 中继】

**配置描述：**

**第一：**进入【DHCP 中继】页面，可以看到当前已建立的 DHCP 中继配置。如下图：


图 90：DHCP 中继列表

**第二：**进入点击<新增>按钮，增加 DHCP 中继配置。如下图：


图 91：新增 DHCP 中继

**参数说明：**

- 中继接口：LAN 口是连接内网主机方向的端口，WAN 口是连接 DHCP 服务器方向的端口。
- DHCP Server IP：DHCP 服务器 IP 地址。

## 5.10 已分配 IP 地址

显示当前 DHCP 分配的 IP 总数，所分配的 IP 地址、计算机名称、MAC 地址及分配的 IP 地址到

期时间。

## 5.11 SNMP 服务器

**功能描述：**当设备作为 SNMP 服务器时，配置允许访问该 SNMP 服务器的 SNMP 客户端 IP 地址。

**配置路径：**【网络配置】>【SNMP 服务器】

**配置描述：**进入【SNMP 服务器】页面，配置允许访问该 SNMP 服务器的 SNMP 客户端 IP 地址。如下图

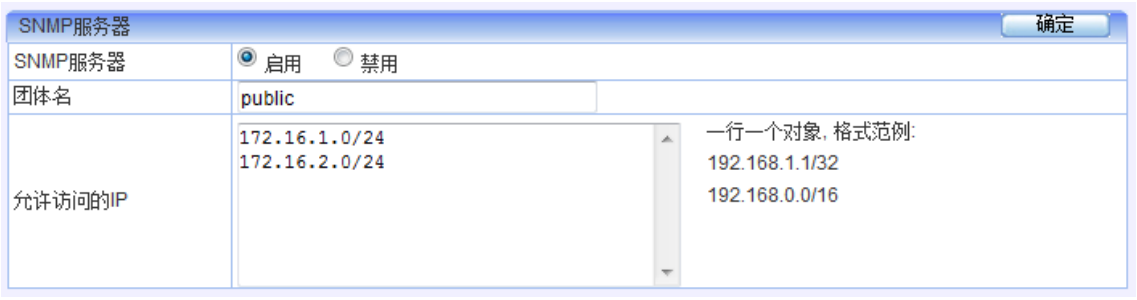



图 92：SNMP 服务器配置

## 5.12 代理服务器列表

当内网使用了代理时，所有的数据报文都被重新封装，原来的特征库将不能识别这部分被代理封装的报文。系统对此处配置的代理服务器地址将先封装头再进行特征分析。若对所有报文都进行这样的分析，将消耗大量性能，所以通过次方法来减少对性能的无谓消耗。

**功能描述：**配置代理服务器的 IP 地址。

**配置路径：**【网络配置】>【代理服务器列表】

**配置描述：**进入【代理服务器列表】页面，代理服务器的 IP 地址。如下图：

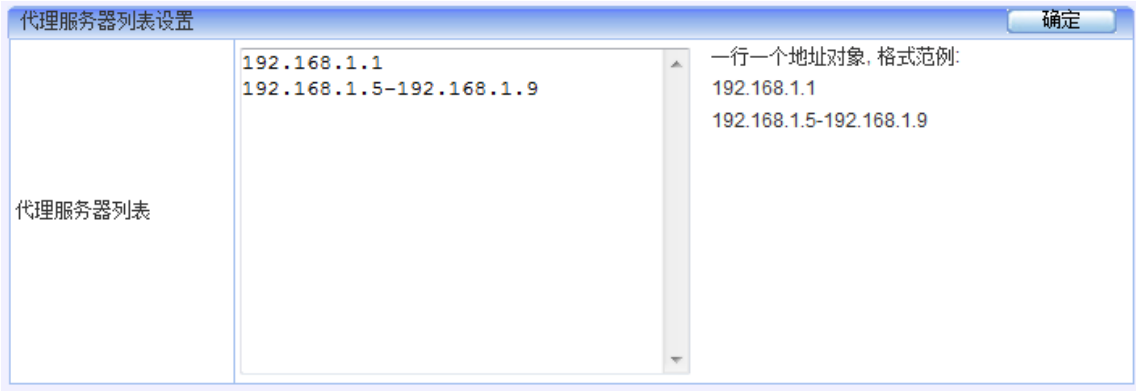



图 93：代理服务器列表设置

## 5.13 代理配置

**功能描述：** 对于 SSL 网页的分析和审计,默认是关闭的,若需要分析和审计需要设定相关的参数，此处设定需要做分析和审计的 SSL 域名以及开启 SSL 代理。

**配置路径:**【网络配置 > 代理配置】

**配置描述:**

**第一：**进入【代理配置】页面，配置需要代理的 SSL 页面的域名。如下图:


图 94：SSL 透明代理规则

**参数说明:**

- SSL 透明代理规则： ［以下域名做代理］表示在域名列表里面的域名需要进行 SSL 代理，以便于对这些 SSL 网站内容进行分析和审计。［以下域名不做代理］表示除了在域名列表以外的域名需要进行 SSL 代理，以便于对这些 SSL 网站内容进行分析和审计。
- 域名列表框：设定需要或不需要做 SSL 代理的域名,一行一个域名,可输入多个域名。

**第二：**点击［代理配置］选项，用于开启或关闭 SSL 代理。

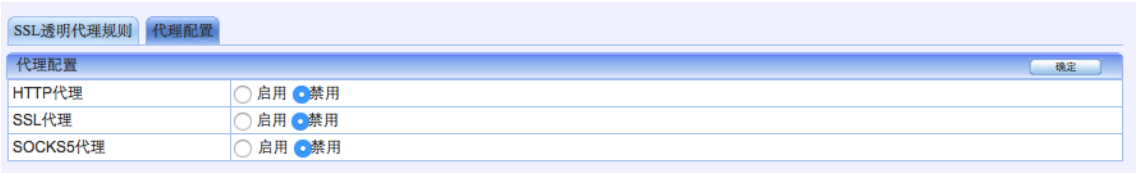



图 95：代理配置

# 第6部分 防火墙

“防火墙”设置包括安全策略、NAT 规则。防 DOS 攻击、ARP 欺骗防护、应用层网关、加速老化、移动终端管理部分。

## 6.1 安全策略

**功能描述：**安全策略定义了对数据流的控制规则；可以通过指定报文的源地址、目的地址、服务、时间段等参数来控制信息流。安全策略的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，所以同一组策略中，序号小的优先级高。

**配置路径：**【防火墙】>【安全策略】

**配置描述：**

**第一：**进入【安全策略】页面，如下图：


图 96 安全策略列表

点击<删除所有>，将删除所有的安全策略。

点击<删除本组>，将删除本组的安全策略，如删除 LAN2→WAN2 的所有安全策略。

点击<删除>，删除本条安全策略。

点击<修改>，修改本条安全策略的参数，但不能修改本条安全策略的方向。

点击<插入>，在当前位置之前插入一条安全策略

点击<移动>，改变对应安全策略的序号，从而改变安全策略的优先级。

改变状态栏复选框的值，再点击<修改状态>，可修改安全策略的状态（“勾选”表示启用，“不勾选”表示禁用）。点击表头的“状态”复选框，可以改变所有安全策略的状态。

**第二：**点击<新增>按钮，新增安全策略，如下图：


图 97：新增安全策略规则

**参数说明：**

- 策略方向：代表数据流的方向。
- 源地址：数据流的源地址，可输入 IP 地址或选择地址簿。地址簿在【系统对象 > 地址簿】中配置。
- 目的地址：数据流的目的地址，可输入 IP 地址或选择地址簿。
- 服务：数据流的服务类型。
- 生效时间：本策略的有效时间段。
- 动作：安全策略允许、拒绝服务的动作
- 状态：启用或禁用本规则，默认启用

## 6.2 NAT 规则

“NAT 规则”包括三种 NAT 方式，包括：内网代理、一对一地址转换、端口映射。

### 6.2.1 内网代理

**功能描述：**作为内部网络的代理网关，转换内部主机上网数据流的源 IP 地址。内部网络的所有主机均可共享一个或者多个合法外部 IP 地址实现对 Internet 的访问。

内网代理的匹配原则是按顺序从前往后匹配，从第一条开始顺序匹配，遇到第一个匹配的条目就停止，所以序号小的优先级高。

**配置路径：**【防火墙】>【NAT规则】>【内网代理】

**配置描述：**

**第一：**进入【内网代理】页面，如下图：

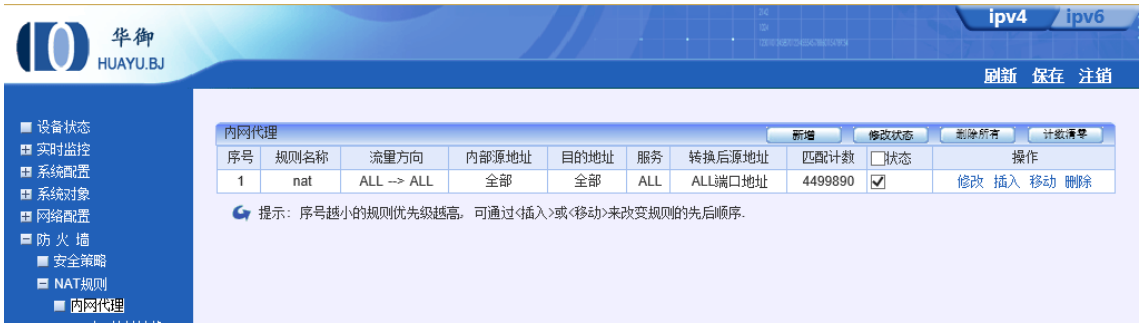



图 98：内网 NAT 列表

点击<删除所有>，将删除所有的内网代理规则。

点击<删除>，删除本条规则。

点击<修改>，修改本条规则的参数，但不能修改流量方向。

点击<插入>，在当前位置之前插入一条规则。

点击<移动>，改变对应规则的序号，从而改变规则的优先级。

改变状态栏复选框的值，再点击<修改状态>，可改变规则状态（“勾选”表示启用，“不勾选”表示禁用）。点击表头的“状态”复选框，可以改变所有规则的状态。

**第二：**点击<新增>按钮，新增规则，如下图：

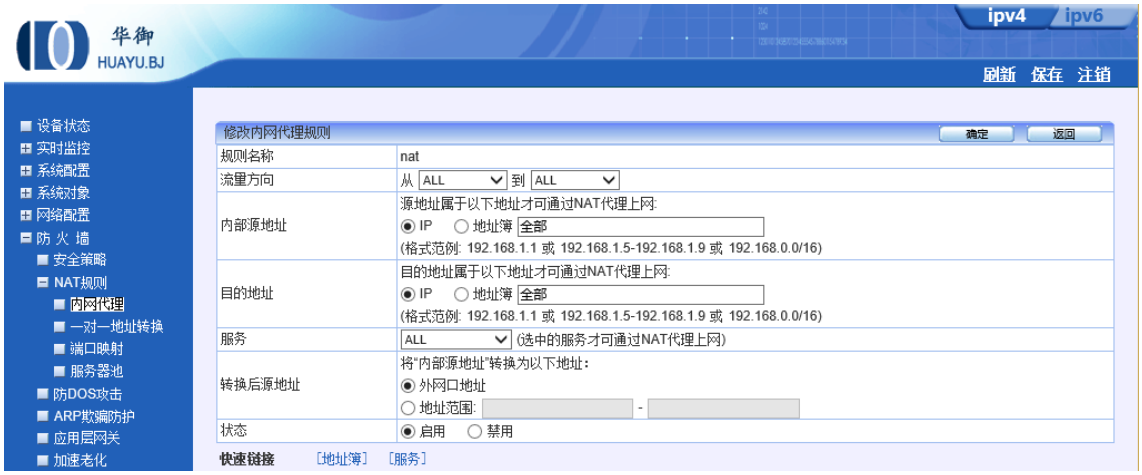



图 99：新增 NAT 配置

**参数说明：**

- 规则名称：内网代理规则的名称。
- 流量方向：代表数据流的方向，方向必须从内网端口（LAN1、LAN2）到外网端口（WAN1、WAN2）。
- 内部源地址：内网主机发出的数据流的源地址，可输入 IP 地址或选择地址簿。地址簿在【系统对象 > 地址簿】中配置。
- 目的地址：数据流的目的地址，可输入 IP 地址或选择地址簿。

**提示：**内网代理规则遵循从上向下匹配的原则，如果一个规则匹配了，就不会再向下匹配了，所以请注意规则的先后顺序。先定义的规则，位置排在前面，可通过<插入>或<移动>来改变规则的先后。

- 服务：选中的服务才可通过 NAT 转换上网。
- 转换后源地址：数据流从设备出去时的源 IP 地址，可选择外网口地址（如 WAN1 接口地址）或输入一个地址范围
- 状态：启用或禁用本规则，默认启用。

## 6.2.2 一对一地址转换

**功能描述：**

将内网的私有 IP 转换为公有 IP，一个私有 IP 只能对应一个公有 IP，主要用于对内网服务器的转换。

**配置路径：**【防火墙】>【NAT规则】>【一对一地址转换】

**配置描述：**

**第一：**进入【一对一地址转换】页面，如下图：


图 100：一对一地址转换

点击<删除所有>，将删除所有的内网代理规则。

点击<删除>，删除本条规则。

点击<修改>，修改本条规则的参数，但外网口不能修改。

改变状态栏复选框的值，再点击<修改状态>，可改变规则状态（“勾选”表示启用，“不勾选”表示禁用）。点击表头的“状态”复选框，可以改变所有规则的状态。

**第二：**点击<新增>按钮，新增规则，如下图：

**提示：**一次可以配置多个连续的转换 IP，但“内部 IP 地址”与“对外映射 IP 地址”的个数要相等。



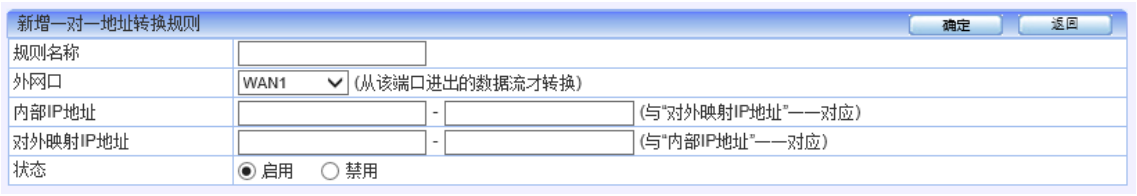



图 101：新增一对一地址转换

**参数说明：**

- 规则名称：一对一地址转换规则的名称
- 外网口：连接外网的物理接口，如 WAN1、WAN2
- 内部 IP 地址：内网主机的IP地址范围，与“对外映射 IP 地址”一一对应
- 对外映射 IP 地址：对外网映射的公网IP地址范围，与“内部 IP 地址”一一对应
- 状态：启用或禁用本规则，默认启用

### 6.2.3 端口映射

**功能描述：**如果内网有服务器需要向 Internet 提供服务，且只提供某些端口的服务，那么就需要在网关上做端口映射。

**配置路径：**【防火墙】>【NAT规则】>【端口映射】

**配置描述：**进入【端口映射】页面，点击<新增>按钮，如下图所示：


图 102：新增端口映射规则

## 6.3 防 DOS 攻击

**功能描述：**防止DOS功能,防止本设备被DOS攻击，通过最大连接数限制的方式进行。

**配置路径：**【防火墙】>【防DOS攻击】

**配置描述**：进入【防DOS攻击】页面，如下图所示：

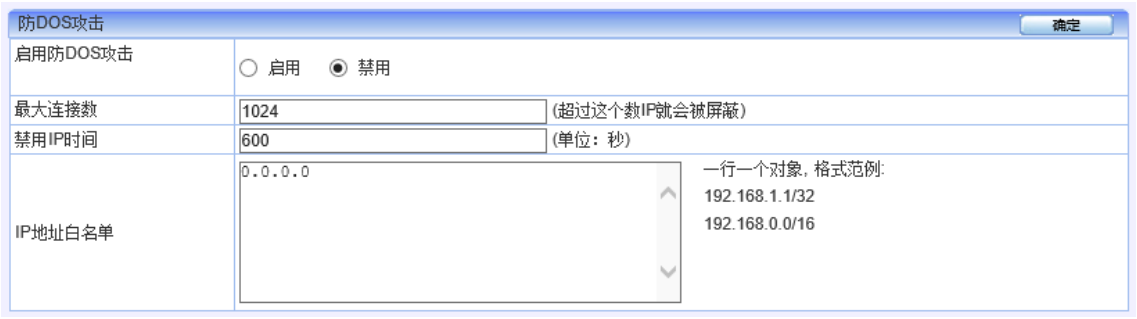



图 103：防 DOS 攻击

# 第7部分 组织管理

组织管理可以通过分组维护用户和组的信息，从而建立起和本单位实际组织结构相一致的组织信息。用户和组的维护功能包括新建、删除、更新、改变所属关系、绑定 MAC 地址。

## 7.1 组织结构查看

**功能描述：**在针对用户和组操作时，应首先浏览、定位、选中当前要操作的用户或组。

**配置路径：**【行为管理】>【组织管理】>【组织结构】

**配置描述：**

**第一：**进入【组织结构】页面，在下图中，点击左边的组织结构中的节点，右边的列表中将显示该组织的成员，可以通过右面列表中的复选框选择要操作的用户或组。如下图：


图 104：组织结构

左边是当前所有用户组的树型结构，默认有一个 Root 根组，所有建立的组和用户都在根组之下。右边是左边已定为的组所包含的所有直属用户和子组。名称列图标为两个人的表示子组，图标为一个人且颜色为彩色的表示在线用户，图标为一个人且颜色为黑白的表示离线用户。

**第二：**若想查看或编辑当前组下面的用户和子组，点击右边列表中名称列子组或用户应的链接。

## 7.2 修改根组

**功能描述：**修改根组的名称、认证超时、强制继承、公用账号

**配置路径：**【行为管理】>【组织管理】>【组织结构】

**配置描述：**进入【组织结构】页面，点击顶部的<修改根组>按钮，弹出“修改根组”页面，

如下图：

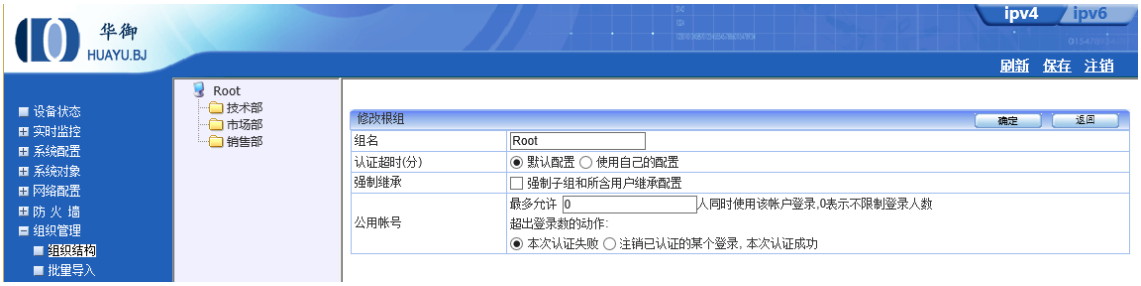



图 105：修改根组

**参数说明：**

- 组名：根组的名称，默认 Root，可填入需要修改的名称。
- 认证超时：可以选择默认配置，认证超时时间为 10 分钟，也可选择使用自己的配置。选择自己的配置后，在后面出现的认证超时表单中填入超时时间，单位是分钟。
- 强制继承：强制子组和所含用户继承配置，默认未启用。启用后，所有的用户和子组的配置将被继承。
- 公用账号：表示可以多人同时使用同一账号登录，0 表示不限制登录人数。当超出登录人数时，处理方法包括：本次登录失败、注销已认证的某个登录，本次认证成功。

## 7.3 新增子组

**功能描述：**新增子组，并设置子组的名称、所属组、http代理、认证超时、离线用户自动删除、共用账号。

**配置路径：**【行为管理】>【组织管理】>【组织结构】

**配置描述：**进入【组织结构】页面，浏览定位相应的组，点击顶部的<新增子组>按钮，弹出“新增子组”页面，如下图：

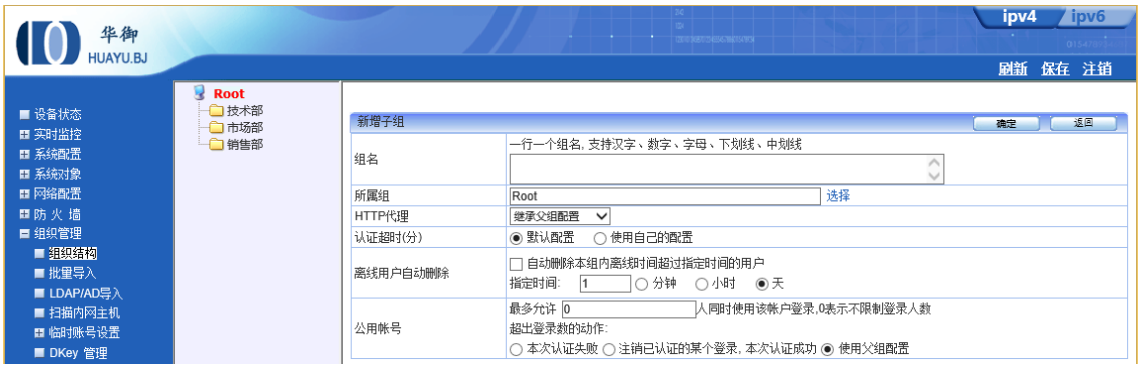



图 106：新增子组

**参数说明：**

- 组名：子组的名称，一次可以创建多个子组，一行一个组名，支持汉字、数字、字母、下划线、中划线。
- 所属组：默认已经填好刚才进入新增页面时的父组，也可以点击后面的<选择>，就出现选择用户组的框，可改变父组。
- HTTP 代理：选择是否启用 HTTP 代理，如果启用，选择使用自己的配置，在后面的 HTTP 代理前面打钩。
- 认证超时：可以选择默认配置，认证超时时间为 10 分钟，也可选择使用自己的配置。选择自己的配置后，在后面出现的认证超时表单中填入超时时间，单位是分钟。
- 离线用户自动删除：配置离线用户超过多上时间将被系统自动删除。
- 公用账号：表示可以多人同时使用同一账号登录，0 表示不限制登录人数。当超出登录人数时，处理方法包括：本次登录失败、注销已认证的某个登录，本次认证成功。

## 7.4 新增普通用户

**功能描述：**新增普通用户，并设置用户的名称、所属组、用户类型、绑定检查等。

**配置路径：**【行为管理】>【组织管理】>【组织结构】

**配置描述：**进入【组织结构】页面，浏览定位相应的组，点击顶部的<新增用户>按钮，弹出“新增用户”页面，用户类型选择“普通用户”。如下图：


图 107：新增普通用户

**参数说明：**

- 用户名：用户名称。
- 显示名：用户的别名，如果是以用户的 IP、MAC、主机名等为用户名，在显示名处可填入用户真实的姓名，在统计的时候就会看到真实的姓名，方便记忆。
- 所属组：默认已经填好刚才进入新增页面时的父组，也可以点击后面的<选择>，就出现选择用户组的框，可改变父组。
- 用户类型：普通用户表示不需密码认证的用户，认证用户表示在上网之前需要输入用户名和密码认证的用户。
- 绑定检查：用来绑定 IP、MAC、IP+MAC 和 VLAN ID，以保证过滤策略的准确有效。普通用户和认证用户的绑定含义不尽相同，后面将详细描述。
- 状态：正常或冻结。正常表示该用户可用，冻结表示暂时不可用。

## 7.5 新增认证用户

**功能描述：**新增普通用户，并设置子组的上网策略和黑名单控制。

**配置路径：**【行为管理】>【组织管理】>【组织结构】

**配置描述：**进入【组织结构】页面，浏览定位相应的组，点击顶部的<新增用户>按钮，弹出“新增用户”页面，“用户类型”选择“认证用户”。如下图：

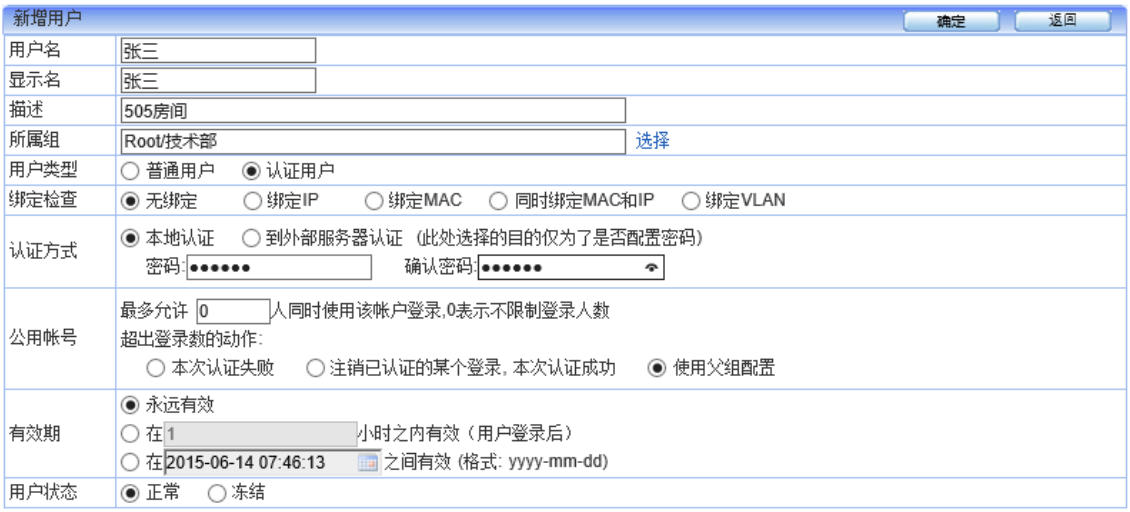



图 108：新增认证用户

**参数说明：**

- 用户名：用户名称。
- 显示名：用户的别名，如果是以用户的 IP、MAC、主机名等为用户名，在显示名处可填入用户真实的姓名，在统计的时候就会看到真实的姓名，方便记忆。
- 所属组：默认已经填好刚才进入新增页面时的父组，也可以点击后面的<选择>，就出现选择用户组的框，可改变父组。
- 用户类型：普通用户表示不需密码认证的用户。认证用户表示在上网之前需要输入用户名和密码认证的用户。
- 绑定检查：用来绑定 IP、MAC、IP+MAC 和 VLAN ID，以保证过滤策略的准确有效。普通用户和认证用户的绑定含义不尽相同，后面将详细描述。
- 认证方式：包括本地认证、到服务器去认证。本地认证表示在账号放于设备本地，这时候需要为用户设置密码。到服务器去认证，表示到外部服务器去认证，不用设置密码。外部服务器包括：Radius 服务器、LDAP 服务器、AD 服务器、POP3 服务。
- 公用账号：表示可以多人同时使用同一账号登录，0 表示不限制登录人数。当超出登录人数时，处理方法包括：本次登录失败、注销已认证的某个登录，本次认证成功。
- 有效期：用户有效期，当有效期到了，就自动将该用户从设备中删除。默认为“永远有效”。
- 状态：正常或冻结。正常表示该用户可用，冻结表示暂时不可用。

## 7.6 组织结构导出

在配置好用户后，可以通过组织结构导出来备份组织结构，便于管理人员后期管理。选择【组织管理】->【组织架构】->【导出按钮】,选择需要导出的用户或者用户组,如图:


图 109：组织结构导出

选择<导出>按钮,选择文件保存位置即可。

## 7.7 移动用户或组

当需要调整用户或者组的隶属关系，可以通过移动用户或组的功能进行调整，点击“【组织管理】->【组织结构】,选择需要移动的用户或者组,点击“移动”按钮，在“目的组”处选择需要移动的最终隶属组,点击“选择”按钮,如下图所示:


图 110：移动用户组

## 7.8 批量导入

如果用户较多，可以通过批量导入的方式进行导入，避免管理员逐个建立用户的麻烦。点击【组织管理】>【批量导入】,如下图所示:

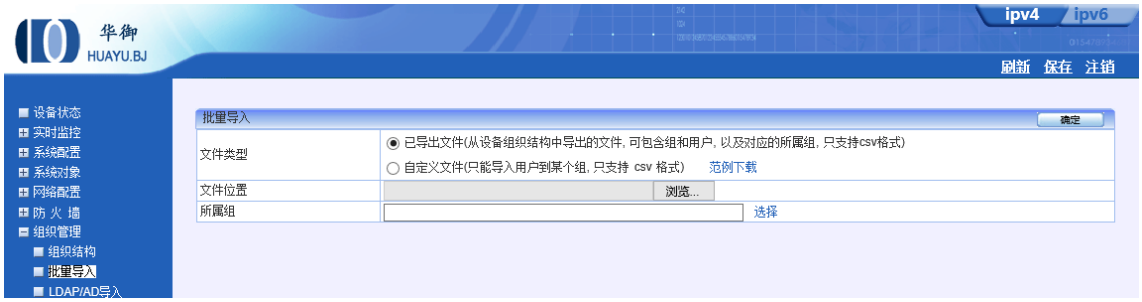



图 111：批量用户导入

## 7.9 LDAP / AD 导入

如果配置了与 LDAP 或 AD 域结合，可以通过此功能导入 LDAP / AD 中的用户，【组织管理】>【LDAP / AD 导入】,如下图所示:


配置参数说明如下:

- 服务器类型：可选择 Active Directoty 或 Open Ldap 、Lotus LDAP 和 Other LDAP，如果是微软的 AD 域，请选择 Active Directory
- 服务器地址：填入服务器的 IP 地址
- 服务器端口：LDAP/AD 服务的端口,默认值 389。

- 导入入口（BaseDN）:确定导入用户数据的导入点,由域名和用户组名组成。格式为:[ CN=2 级用户组名称,CN=1 级用户组名称,DC=N 级域名,...,dc=2 级域名,dc=1 级域名]，如果不指定 CN 将导入整个 AD 域架构，如下图所示：


如果只想导入 Computers 组中的用户，导入入口可设置如下图所示：


- 用户查找: [匿名查询]指不需要进行认证,即可进行用户导入;[本地用户查询]必须要输入 LDAP/AD 域 里的任何一个用户名及密码,并成功进行认证后,才能进行用户导入。
- 用户名属性字段：默认设置为 SAMAccountName；
- 显示名属性字段：默认为 dislayName；
- 自动更新：可设定定时与 LDAP 服务器同步数据。
- 其余字段设置为默认即可。

# 第8部分 流量管理

流量管理可以用于：

1、精确识别各种互联网应用，包括各种对带宽占用较大的主流 P2P 软件与在线视频软件；

2、基于应用或用户对流量进行管理，对指定类型的流量进行限速，避免占用过多网络带宽；

3、对关键业务提供带宽资源保障，保留足够可用带宽，保障服务质量；

## 8.1 线路带宽配置

用于配置互联网出口带宽，根据运营商实际给定的带宽值填写，此处配置好之后，在设定策略的时候可以通过百分比来分配带宽。

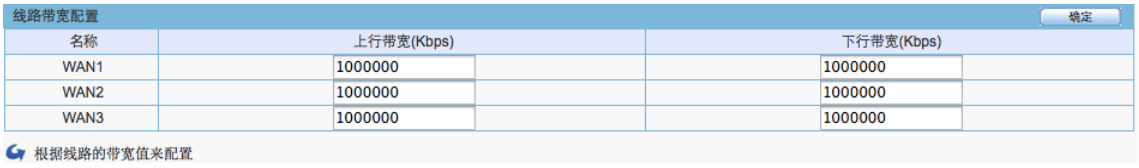



图 112 线路带宽配置

## 8.2 基于策略的流控

用于全局的基于用户与对应七层应用的流控策略控制，配置完立即生效，策略规则匹配原则是按顺序从前往后匹配，从上往下顺序匹配，遇到第一匹配的条目就停止，所以同一组策略中，序号小的优先执行，可以通过插入、移动来调整顺序，此处如果使用 URL 阻断策略时，需要防止到最下方。


图 113：策略留空规则列表


图 114：修改策略规则

**配置说明：**

- 生效线路：流控规则的生效线路
- 内网地址：可输入 IP 地址、选择地址簿或用户组。地址簿需要在【系统对象>地址簿】中预先配置好，用户组在【组织管理>组织结构】中预先配置后在此处可选择。
- 外网地址：可输入目的 IP 地址、选择地址簿或用户组，通常无需配置；
- 服务 / URL / 文件类型：可以选择七层应用或应用组、URL 分类或自定义 URL、文件类型；
- 流控行为：包括“阻断流量”、“限制通道”、“保障通道”，其中详细配置选项包括，
- 优先级：保障带宽时，优先级较高的报文优先传送。可将核心业务应用、重要人物的流量配置为高优先级；同时将 P2P、网络电视、WEB 视频等非核心的、占用带宽资源较多的应用配置为低优先级。
- 最大带宽：为某些用户或特定应用指定最大带宽，百分比为占用本线路带宽值的比例。
- 保障带宽：结合最大带宽和优先级，根据需要为某些关键应用或者 VIP 客户保障一定带宽。当网络繁忙时，这些关键应用或者 VIP 客户至少可以得到设定的保障带宽，并还可以租借空闲的或低优先级流量的带宽；当网络空闲时，低优先级的流量亦可使用当前空闲带宽。从而保证了带宽的合理、高效的使用。百分比为占用本线路带宽值的比例。
- 预留带宽：为某种特定应用或某些重点客户预留一定带宽，以保证在不同时间段、不同的网络使用环境中某种流量都能得到同样的带宽。预留带宽不能被其他数据流使用，百

分比为占用本线路带宽值的比例。

- 生效时间：本规则的有效时间段，细化至分钟，可在“时间计划”中预先定义好。

## 8.3 基于用户的流控

网络中 80%的带宽被 20%的人占用，为了防止这一情况出现，体现网络公平，可以对全网中每个主机进行带宽、会话控制、分类服务进行限制以及分时段管理。策略规则匹配的原则是从上往下匹配，如下图所示：


用户流控规则列表

新增 修改状态 删除所有 计数清零

| 序号 | 规则名称 | 地址 | 最大带宽(Kbps) | 会话数 | 带宽细分配 | 生效时间 | 匹配计数 | 状态 | 操作 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 工作日每... | 全部 | ↑ 512, ↓ 512 | ↑ 200, ↓ 200 | 禁用 | 工作时间 | 4313 | ☑ | 修改 插入 移动 删除 |
| 2 | 非工作时... | 全部 | ↑ 512, ↓ 512 | ↑ 300, ↓ 300 | 禁用 | 全天 | 5233 | ☑ | 修改 插入 移动 删除 |

提示: 序号越小的规则优先级越高, 可通过<插入>或<移动>来改变规则的先后顺序.

图 115：基于用户的流控规则列表

## 8.4 配置策略常见注意事项

1、如果需要阻断 URL，建议在行为管理策略中配置，流控对 URL 阻断会现实无法访问此网站；

2、如果在基于策略的流控中选择对 URL 阻断或者流控，那么所有服务（如 P2P、Web 视频）都会匹配这一条，而且默认的服务是允许的，因此阻断服务如 Web 视频或者 P2P 下载的服务，必须配置在 URL 流控的上方才可生效；

3、有阻断的策略，建议开启阻断记录，方便排查问题；

4、配置完成后，发现策略无效果，查看匹配计数，无匹配计数请检查生效线路，IP、服务、URL 以及生效时间有无配置错误，策略是否启用。如果是某一项应用没有祈祷控制效果，请把该应用的名称、版本号上报，方便及时对该应用进行更新。

5、应用服务中对某些 P2P 下载的阻断和流控需要选择多种服务才能起作用，比如迅雷等下载，迅雷有自己的私有协议还有加密协议，对此种协议的阻断需要阻断如下集中应用：P2P 下载中的迅雷、BT、HTTP 应用的多线程下载和伪 IE 下载阻断，这样能阻断和控制大部分迅雷和 BT，但是有一些极端环境中，迅雷还是会走我们没有识别到的部分加密协议，那么需要把“其他服务－其他 TCP 协议”也阻断掉，这个阻断可能会引发一些没有识别到重要的 TCP 应用也无法访问，阻断视情况而定。如果基于策略流控和基于用户流控都对某个 IP 的带宽限制，那么带宽限制小的生效；

6、对于限制单个用户的会话数也非常有必要，用户中毒、木马或者使用扫描工具会产生大量的上行会话，P2P 下载也会产生大量上下行会话，特别在教育行业，会话必须进行限制，建议值为 400-500，值太小会导致正常应用访问不了，太大达不到应有的效果，对于服务器不能限制会话数。

## 8.5 配置流控策略的步骤

- 清楚网络出口实际带宽大小；
- 设备上架后先分析用户网络流量的状况，在“设备状态页面”查看实时网络流量大小，前 10 名服务和前 10 名用户流量；
- 观察一段时间流量后，开始配置策略流控，配置的步骤为：
  - 先配置好实际的线路带宽大小；
  - 针对重要 IP、重要服务和服务器做保障带宽，保障的带宽值视带宽；
  - 针对 P2P 下载、WEB 视频以及流媒体做带宽限制或阻断；
  - 对“其他服务－其他 UDP”做一定的带宽限制（但不能过小，可能会影响部分游戏）
  - 最后配置一条默认策略，IP 和服务都是全部，带宽限制为总带宽的 80%－100%（必须，要想保障带宽起到很好的作用，必须最后配置这条）
  - 对于某些用户占用带宽资源比较大时，在基于用户流控对每个用户限制一个带宽值（1-2M），除非带宽很充裕可以适当调整，对于服务器的 IP 通常不做限制。
  - 提示：所有策略保障带宽的和加起来不能大于总的线路带宽。

# 第9部分 行为管理

行为管理部分用于配置上网认证、URL 过滤、关键字过滤、文件传输过滤等、网络准入、黑白名单等信息。

## 9.1 认证策略

**功能描述：**定义认证的条件、认证方式及使用的认证服务器。策略规则的匹配原则是按顺序从前往后匹配，

即从第一条规则开始顺序匹配，一旦遇到一条匹配的规则就停止，所以序号越小的规则优先级越高。

**配置路径：**【行为管理】>【认证策略】

**配置描述：**

第一：进入【认证策略】配置页面，如下图：


图 116 认证策略列表

点击<删除所有>，删除所有的认证策略。

点击<删除>，删除本条认证策略。

点击<修改>，修改本条认证策略。

点击<插入>，在当前位置插入一条认证策略。

点击<移动>，改变认证策略的序号。

改变状态栏复选框的值，再点击<修改状态>，可修改认证策略的状态(“勾选”表示启用，“不勾选”表示禁止。

用)。点击表头的“状态”复选框，可以改变所有认证策略的状态。

提示：

1、没有配置任何策略的情况下，系统默认以 IP 地址作为新用户名，自动加入到根组(Root)，并自动绑定 IP 地址。

第二：点击<新增>，新增认证策略，如下图：

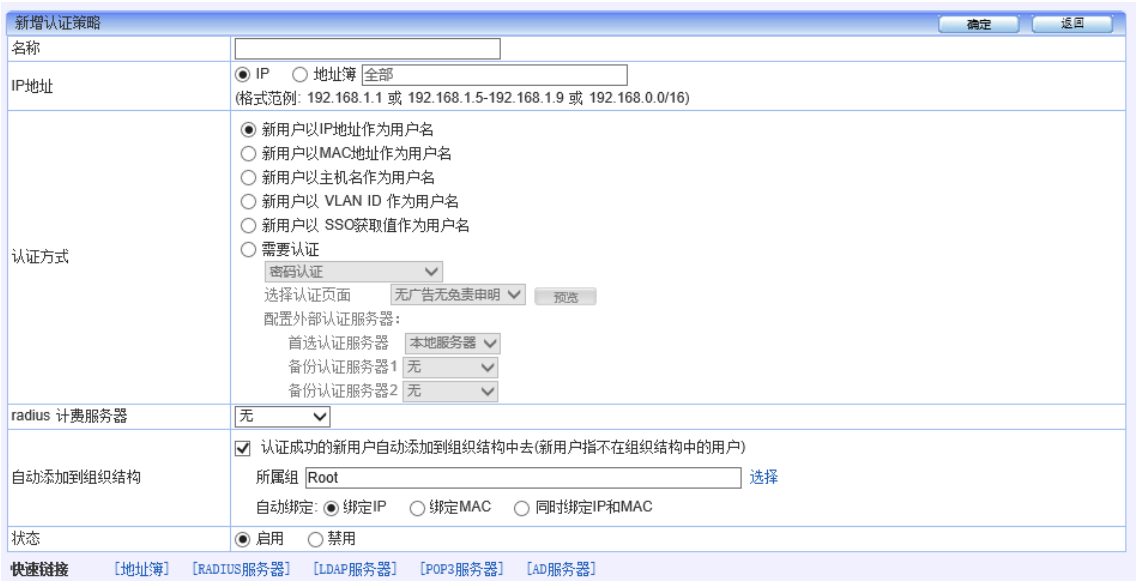



图 117：新增认证策略

**参数说明：**

- 名称：认证策略的名称。
- IP 地址：匹配认证条件的内网地址。
- 认证方式： 根据内网地址的 IP 地址来判断用户采取的认证方式，共有如下五种：
  - 新用户以 IP 地址作为用户名：内网用户不需要密码认证，并且当该用户不在组织结构中时，自动以用户的 IP 地址为用户名。
  - 新用户以 MAC 地址作为用户名：内网用户不需要密码认证，并且当该用户不在组织结构中时，自动以用户的 MAC 地址为用户名。
  - 新用户以主机名作为用户名：内网用户不需要密码认证，并且当该用户不在组织结构中时，自动以用户的主机名。
  - 新用户以 VLAN ID 作为用户名：内网用户不需要密码认证，并且当该用户不在组织结构中时，自动以用户的 VLAN ID 地址为用户名。
  - 到服务器去认证：内网用户需要用户名和密码认证，并选择认证服务器，一共可以选择三个服务器。首先去[首选认证服务器]进行认证；若未返回认证结果，再去[备份认证服务器 1]进行认证；若仍未返回认证结果，再去[备份认证服务器 2]进行认证。
- 自动添加到组织结构：认证成功的新用户自动添加到组织结构中去，新用户指不在

组织结构中的用户。“所属组”表示自动添加到那个组，点击输入框后面的<选择>按钮，可选择组。

- 自动绑定：在自动添加用户时，是否要配置绑定检查。随着选择认证方式不同，自动绑定选项也稍微有区别，具体如下：
  - 新用户以 IP 地址作为用户名：可以选择为“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“绑定 IP”。
  - 新用户以 MAC 地址作为用户名：可以选择为“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“绑定 MAC”。
  - 新用户以主机名作为用户名：可以选择为“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“绑定 IP”。
  - 新用户以 VLAN ID 作为用户名：只能且必须选择为“绑定 VLAN”。
  - 到服务器去认证：可以选择为“无绑定”、“绑定 IP”、“绑定 MAC”或“同时绑定 IP 和 MAC”，默认已选择“无绑定”。
  - 状态：启用或禁用本策略，默认启用。

## 9.2 上网策略

【上网策略对象】用于设置内网用户的上网策略，上网策略包括上网权限策略、终端提醒策略、准入策略、应用限额策略、黑名单策略、上网审计策略。

### 9.2.1 上网权限策略

**功能描述：**定义上网管理的策略，包括 URL 过滤、关键词过滤、文件传输过滤、邮件过滤、SSL 管理、其他类。

**配置路径：**【行为管理】>【上网策略】>【上网权限策略】

**配置描述：**

**第一：**进入【上网权限策略】配置页面，如下图：


图 118：上网权限策略列表

点击<删除所有>，删除所有的上网策略。

点击<删除>，删除本条上网策略。

点击<修改>，修改本条上网策略。

点击<插入>，在当前位置插入一条上网策略。

点击<移动>，改变上网策略的序号。

改变状态栏复选框的值，再点击<修改状态>，可修改认证策略的状态(“勾选”表示启用，“不勾选”表示禁用)。点击表头的“状态”复选框，可以改变所有认证策略的状态。

**第二：**点击<新增>，新增上网权限策略，如下图：


图 119：新增上网策略-URL 过滤

### 9.2.1.1 URL 过滤

URL 过滤可以对内置 URL 库、自定义 URL 库、七层应用进行阻断或允许。

1、选择内置 URL 库或自定义 URL 库时，右侧出现过滤的列表，在选定列表中选择相应项目，打钩后实现过滤。

2、选择应用控制时，选择相应的应用服务，在操作动作设置禁止或允许、在生效时间选择生效的时间范围，如下图所示：


图 120：新增上网策略-应用控制

### 9.2.1.2 关键字过滤

关键字过滤用于设置搜索引擎搜索的关键字、HTTP 上传的关键字、网页内容中包含的关键字进行过滤。

**第一**，打开【行为管理】>【上网策略】【上网权限策略】中的策略，点击左侧的【关键字过滤】。

**第二**，点击页面下方的快捷链接中的【关键字组】，打开关键字组的对话框，然后点击<新增>按钮，新增关键字。如下图所示，输入名称、描述、要过滤的关键字，之后点击确定。

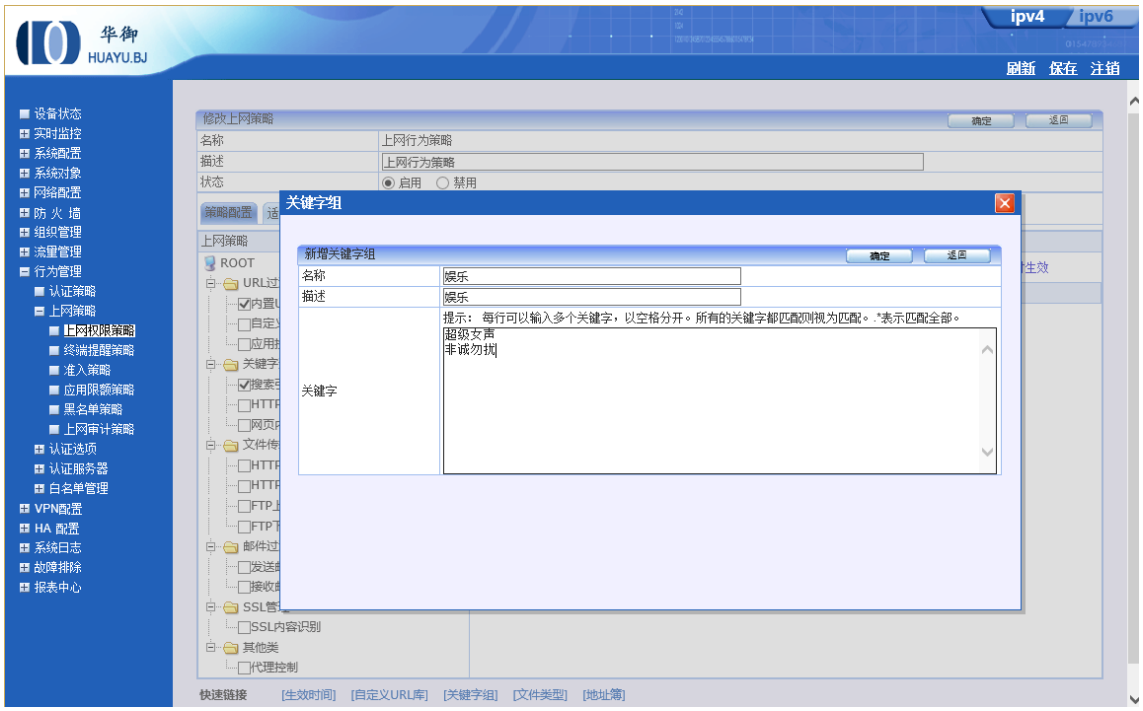



图 121：增加关键字组

**第三，**关闭刚才代开关键字组的对话框，将回到上网策略中。

**第四，**勾选关键字过滤中的【搜索引擎】【HTTP 上传】【网页内容】，在右侧出现的对应内容中，可以看刚才建立的关键字，选择动作允许或拒绝，生效时间选择全天或自定义好的时间，选定中对关键字勾选，点击确定后生效。搜索引擎将过滤百度、谷歌、hao 搜、搜狗等搜索引起搜索的关键字、HTTP 上传将过滤通过 http 协议上传的内容中的关键字、网页内容将过滤论坛、微博等上传的内容。


图 122：关键字过滤

### 9.2.1.3 文件传输过滤

**第一**，打开【行为管理】>【上网策略】【上网权限策略】中的策略，点击左侧的【文件传输过滤】，将对 HTTP、FTP 上传的文件类型进行过滤。

**第二**，点击页面下方的快捷链接中的【文件类型】，打开文件类型的对话框，然后点击<新增>按钮，新增文件类型。如下图所示，输入名称、描述、要过滤的文件类型，之后点击确定，

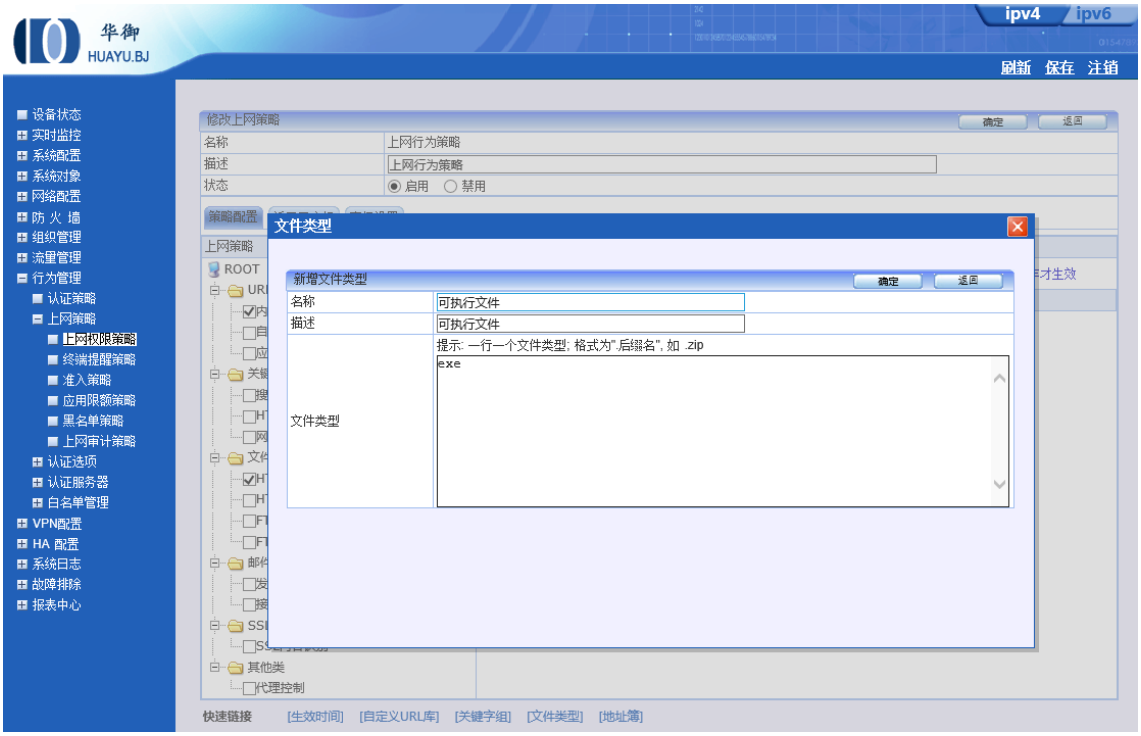



图 123：新增文件类型

**第三**，关闭刚才代开【文件类型】的对话框，将回到上网策略中。

**第四**，勾选【文件传输过滤】中的【HTTP 上传】【HTTP 下载】【FTP 上传】【FTP 下载】，在右侧出现的对应内容中，可以看刚才建立的文件类型，选择动作允许或拒绝，生效时间选择全天或自定义好的时间，选定中对关键字勾选，点击确定后生效。通过设置将过滤通过 HTTP 协议、FTP 协议上传或下载的文件类型，如下图所示：


图 124：文件传输过滤

### 9.2.1.4 邮件过滤

**第一**，打开【行为管理】>【上网策略】【上网权限策略】中的策略，点击左侧的【邮件过滤】，将对发送或接收邮件的地址、主题、内容、附件进行过滤。

**第二**，勾选【文件传输过滤】中的【发送邮件过滤】【接收邮件过滤】在右侧出现的对应内容中，可以对收发邮件的地址、主题和内容中的关键字、附件内容中的关键字和附件的文件类型、以及邮件内容大小、附件内容大小进行过滤，如下图所示：


图 125：邮件过滤

### 9.2.1.5 SSL 管理

**第一**，打开【行为管理】>【上网策略】【上网权限策略】中的策略，点击左侧的【SSL 内容识别】，将禁止终端通过 WEB 加密、邮件加密方式的流量通过。

**第二**，勾选【SSL 管理】中的【SSL 识别】在右侧出现的对应内容中，可以对加密 WEB 应用内容识别、加密邮件内容识别进行过滤，如下图所示，通过设置可以禁止采用 https 方式、加密邮件（邮件终端如 Foxmail 等设置加密邮件）的流量通过。


图 126：SSL 内容识别

### 9.2.1.6 其他类

**第一**，打开【行为管理】>【上网策略】【上网权限策略】中的策略，点击左侧的【其他类】，将禁止或允许终端通过 HTTP 代理、Socks、在 HTTP 协议和 SSL 协议标准端口使用的其他协议通过。

**第二**，勾选【其他类】中的【代理控制】在右侧出现的对应内容中，选择禁止或允许对应协议。


图 127：代理控制

## 9.2.2 终端提醒策略

**功能描述：**可定期对用户进行信息公告，通过定期 URL 重定向的方式。管理员可以自定义设置公告的内容，公告的时间等。

**配置路径：**【行为管理】>【上网策略】>【终端提醒策略】

**配置描述：**

**第一：**进入【终端提醒策略】配置页面，如下图：


图 128：终端提醒策略

**第二：**点击<新增>按钮，新建终端提醒策略，如下图所示;

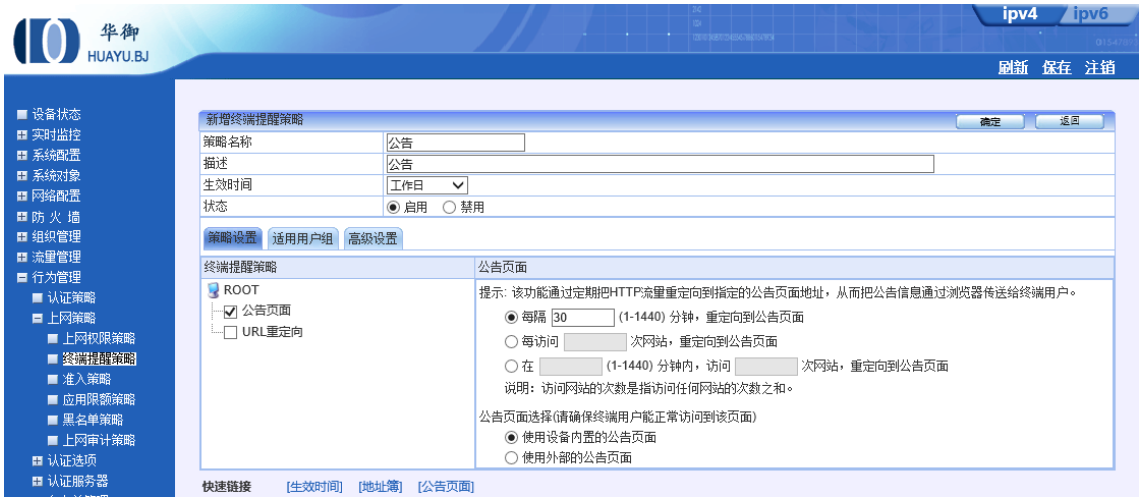



图 129：公告页规则配置

**参数说明：**

- 名称：终端提醒策略的名称。
- 描述：终端提醒策略的描述。
- 生效时间：选择生效的时间范围，可以提前时间计划中定义好时间策略。
- 状态：启用或禁用。
- 公告策略选型：选择设定每隔多少分钟重定向到公告页面，或每访问多少次网站重定向到公告页面，或在多少分钟内访问了多少次网站重定向到公告页面。
- 公告页：可选择内置的公告页，也可选择使用外部的公告页。

内置的公告页面设置，可以点击下方的快速链接中的公告页面进行设置，在本手册的后面会进行介绍。

### 9.2.3 准入策略

**功能描述：**可对终端的 IM 监控、操作系统规则、进程规则、文件规则、注册表规则等设定准入策略，从而实现对客户端的安全管理。

**配置路径：**【行为管理】>【上网策略】>【准入策略】

**配置描述：**进入【准入策略】配置页面，点击<新增>按钮，如下图：


图 130：准入策略

**参数说明：**

- 名称：准入策略的名称。
- 描述：准入策略的描述。
- 生效时间：选择生效的时间范围，可以提前时间计划中定义好时间策略。
- 状态：启用或禁用。
- 不支持准入的终端策略配置：可选择允许上网或视为检查失败，禁止上网（对于不支持运维准入/桌面安全系统的计算机及移动终端）。
- 准入策略中，可以选择 IM 监控规则、操作系统规则、进程规则、文件规则、注册表规则、其他规则中的一种或多种
- 适用用户组：选择使用的组织结构中建立的用户或用户组、IP 地址、地址薄。

**准入策略：**

### 9.2.3.1 IM 监控规则

实现对 IM 中的 QQ、MSN、Skype、Yachoo、飞信、GItalk、阿里旺旺聊天内容、发送内容进行识别与监控

**第一：**打开【行为管理】>【上网策略】【准入策略】中的策略，点击左侧的【IM 监控规则】，如下图所示，勾选要识别 IM 聊天软件。

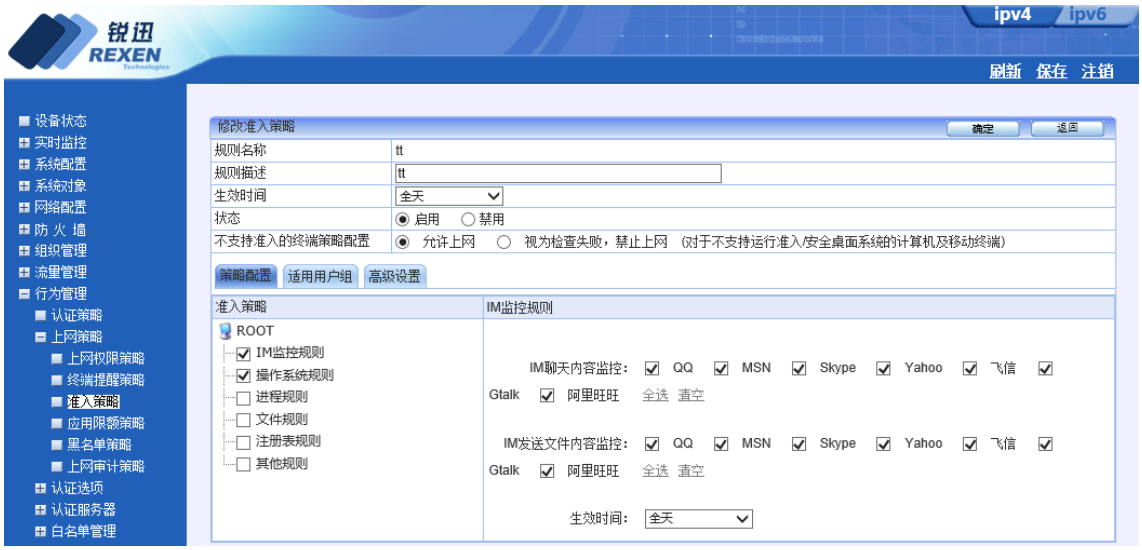



图 131：准入策略-IM 监控规则

**第二：**点击确定，保存该条准入策略

## 9.2.3.2 操作系统规则

实现对终端计算机操作系统及补丁包的准入管理。

**第一：**打开【行为管理】>【上网策略】【准入策略】中的策略，点击左侧的【操作系统规则】，如下图所示，勾选要操作系统及补丁的要求，在页面的地步，选择违反规则“禁止用户上网”或“发送日志”。


图 132：操作系统规则

**第二：**点击确定，保存该条准入策略

### 9.2.3.3 进程规则

实现对终端计算机进程的管理。

**第一：**打开【行为管理】>【上网策略】【准入策略】中的策略，点击左侧的【操作系统规则】，如下图所示：当前的进程规则。

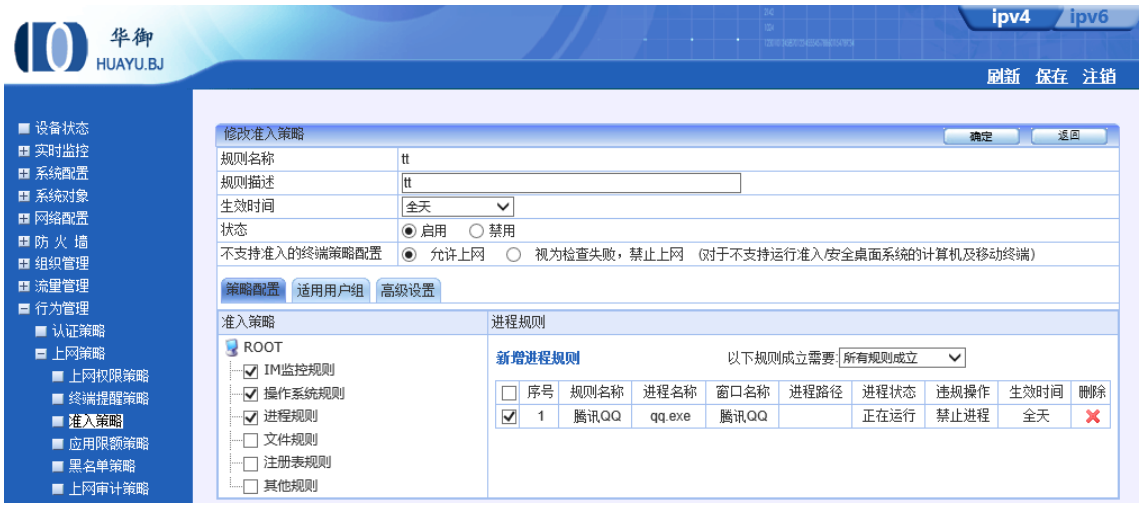



图 133：进程规则

**第二：**点击<新增进程规则>，打开新增进程规则，如下图所示

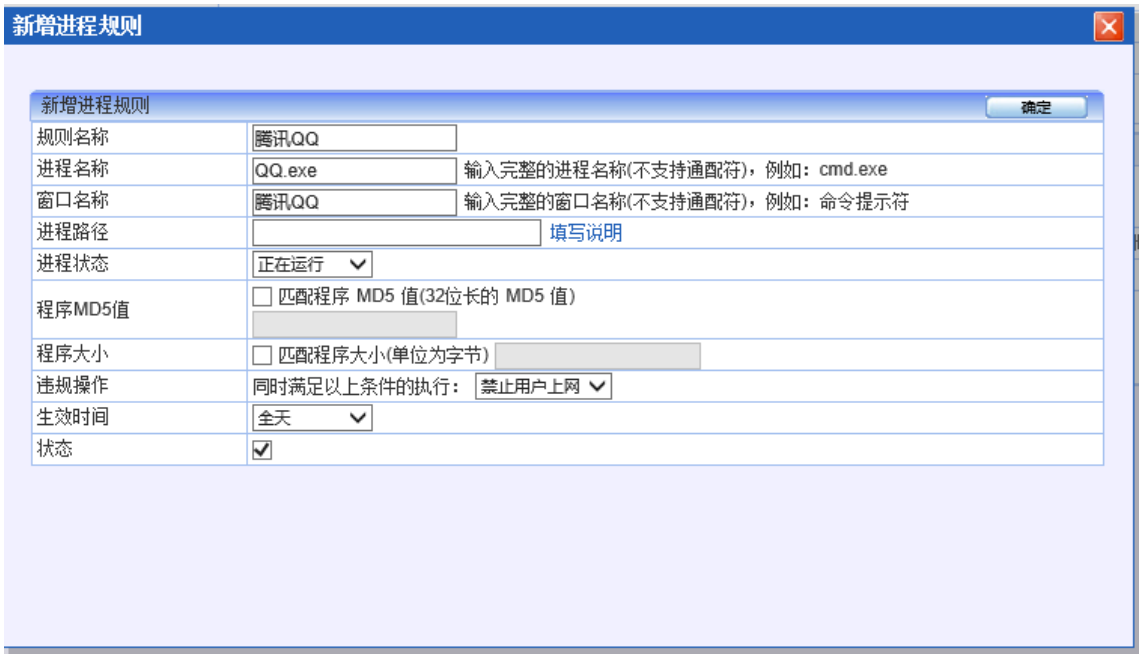



图 134 新增进程规则

**参数说明：**

- 名称：进程规则的名称。

- 进程名称：输入完整进程名称，例如 cmd.exe
- 窗口名称：输入完整的窗口名称，例如：命令提示符。
- 进程路径：此路径只适用于"开启进程"，其他操作不生效，配置时支持系统环境变量，

| 环境变量 | 对应路径 |
|---|---|
| %systemdriver% | C: |
| %systemroot% | C:\WINNT |
| %system% | C:\WINNT\system32 |
| %windir% | C:\WINNT |
| %userprofile% | C:\Documents and Settings\Administrator |
| %temp% | C:\Documents and Settings\Administrator\Local Settings\Temp |
| %program% | C:\Program Files |

- 进程状态：选择正在运行或没有运行。
- 程序 MD5 值：匹配程序 MD5 值(32 位长的 MD5 值)。
- 程序大小：匹配程序大小(单位为字节)。违规操作：同时满足以上条件的执行：禁止用户上网或禁止进程。
- 生效时间：选择生效的时间范围，可以提前时间计划中定义好时间策略。
- 状态：启用或禁用。

### 9.2.3.4 文件规则

实现对终端计算机文件的管理。

**第一**：打开【行为管理】>【上网策略】【准入策略】中的策略，点击左侧的【文件规则】， 如下图所示：当前的文件规则。

**第二**：点击<新增文件规则>，打开新增文件规则，如下图所示

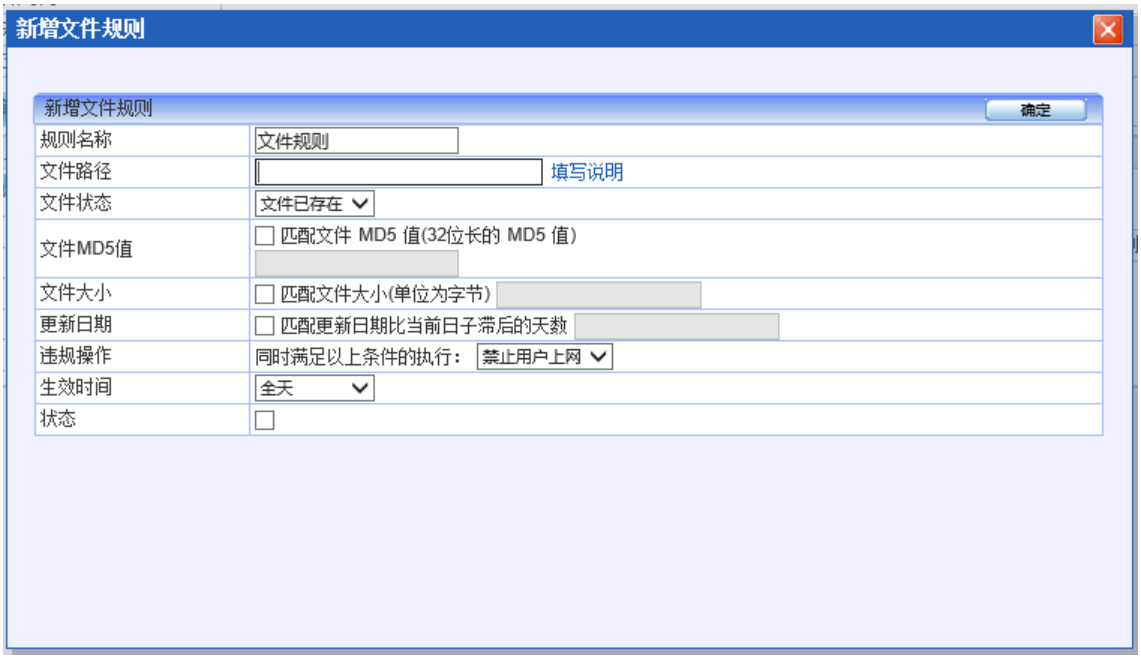



图 135：新增文件规则

**参数说明：**

- 名称：文件规则的名称。
- 文件路径：填写文件所在路径，点击填写说明，可以查看文件的路径填写说明，
- 文件 MD5 值：匹配文件 MD5 值(32 位长的 MD5 值)。
- 文件大小：匹配文件大小(单位为字节)。
- 更新日期：匹配更新日期比当前日子滞后的天数
- 违规操作：同时满足以上条件的执行：禁止用户上网或删除文件。
- 生效时间：选择生效的时间范围，可以提前时间计划中定义好时间策略。
- 状态：启用或禁用。

### 9.2.3.5 注册表规则

实现对终端计算机注册表的管理。

**第一：**打开【行为管理】>【上网策略】【准入策略】中的策略，点击左侧的【注册表规则】，如下图所示：当前的注册表规则。

**第二：**点击<新增注册表规则>，打开新增注册表规则，如下图所示

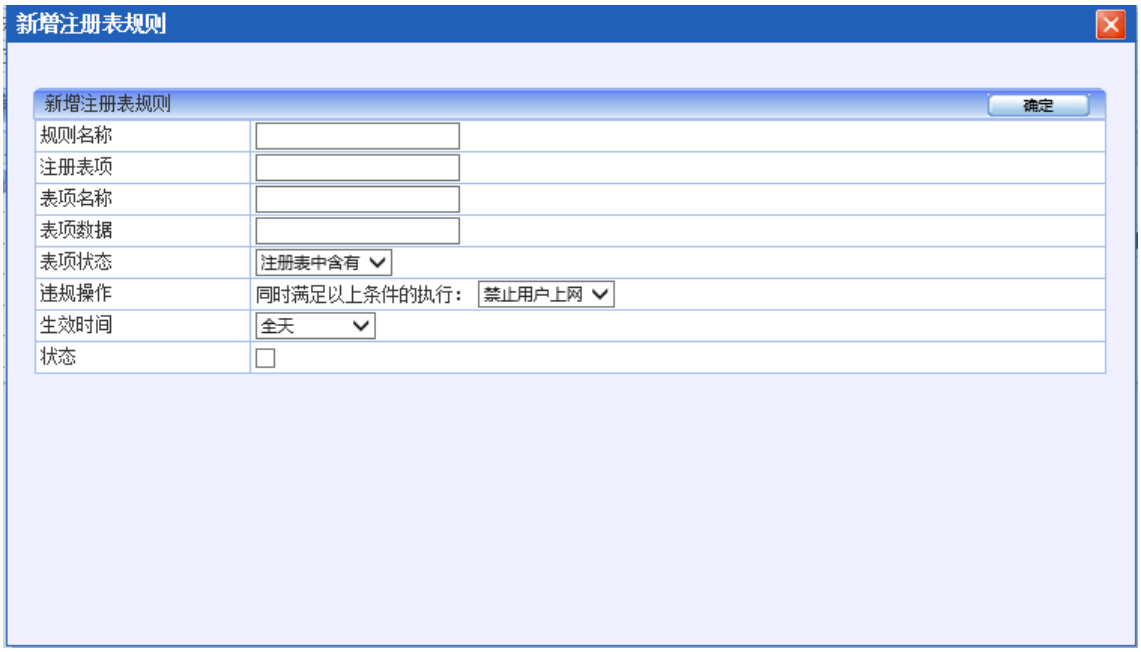



图 136：新增注册表规则

**参数说明：**

- 名称：注册表规则的名称。
- 注册表项：填写要设定的注册表项。
- 表项名称：填写要设定的注册表项名称。
- 表项名称：填写要设定的注册表项对应的数据。
- 表项状态：选择<注册表中含有>或<注册表中没有>。
- 违规操作：同时满足以上条件的执行：禁止用户上网或删除注册表项。
- 生效时间：选择生效的时间范围，可以提前时间计划中定义好时间策略。
- 状态：启用或禁用。

### 9.2.3.6 其他规则

实现对终端计算机超级管理员登陆管理以及 IP/MAC 地址绑定检查。

**第一**：打开【行为管理】>【上网策略】【准入策略】中的策略，点击左侧的【其他规则】， 如下图所示：

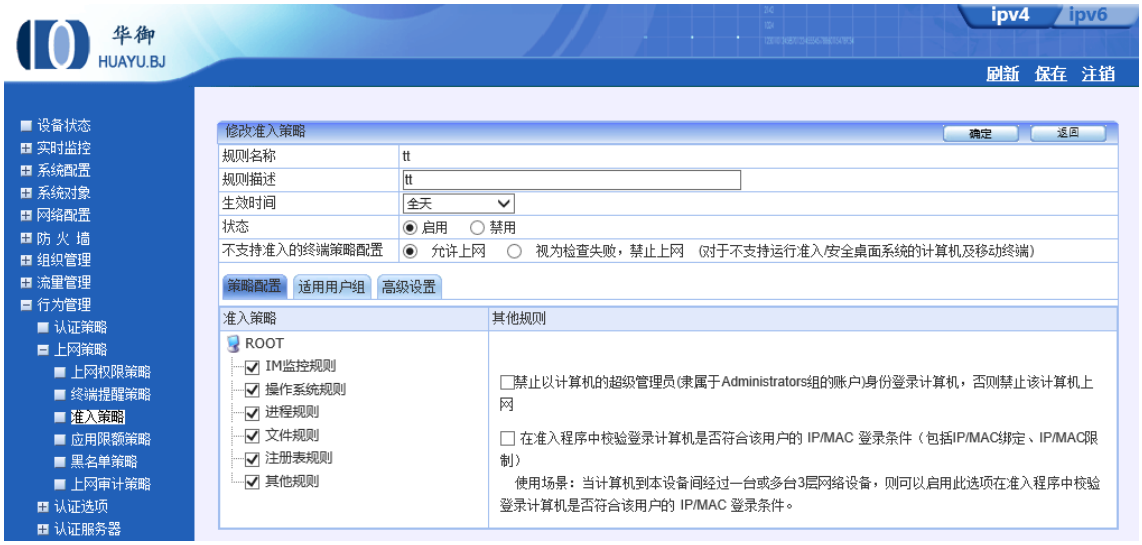



图 137：其他规则配置

**参数说明：**

- 禁止以计算机的超级管理员(隶属于 Administrators 组的账户)身份登录计算机，否则禁止该计算机上网。
- 在准入程序中校验登录计算机是否符合该用户的 IP/MAC 登录条件（包括 IP/MAC 绑定、IP/MAC 限制） 使用场景：当计算机到本设备间经过一台或多台 3 层网络设备，则可以启用此选项在准入程序中校验登录计算机是否符合该用户的 IP/MAC 登录条件。

### 9.2.4 准入客户端安装

准入配置生效后，计算机使用浏览器流量网站时，将出现如下提醒，如下图所示：

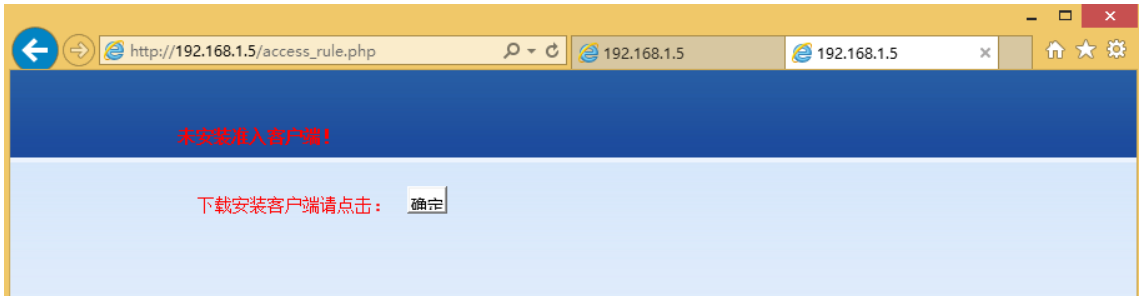



图 138：准入客户端安装提醒

点击<下载客户端>，正常安装后，计算机才能正常上网。

**第一：**安装的过程中，需要退出杀毒软件与防火墙。

**第二：**在弹出【你允许来自未知发布的以下程序对此计算机进行更改吗】的对话框，选择<是>选项，然后点击下一步进行安装。如下图，

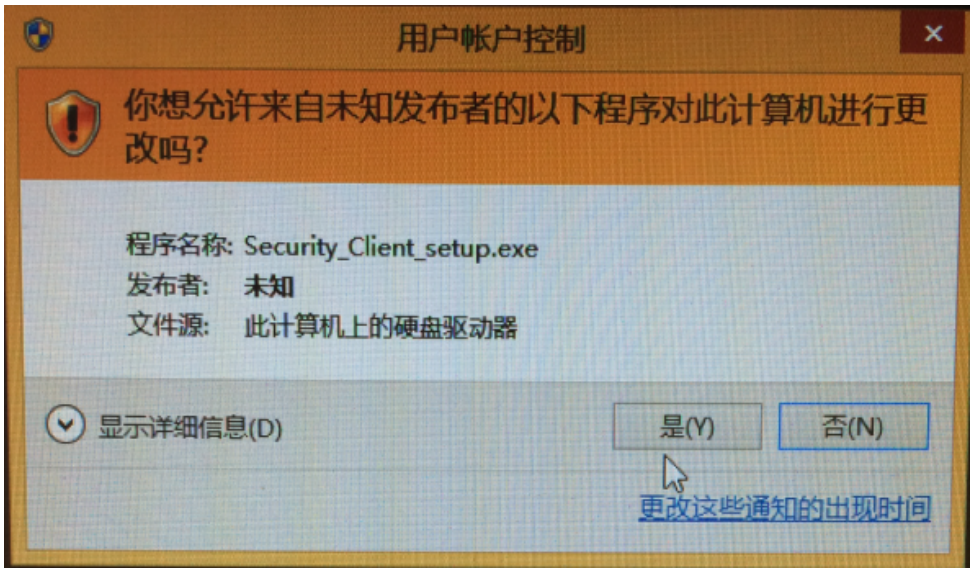



图 139：安装提示

**第三：**点击<下一步>，如下图

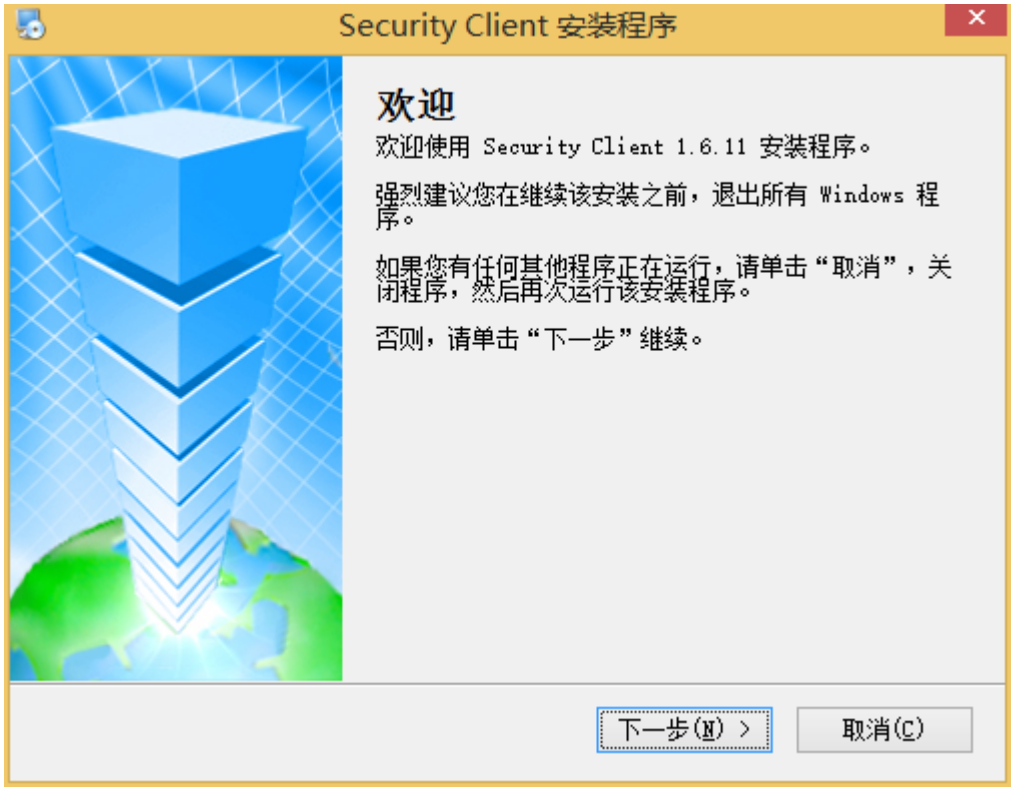



图 140：客户端安装

**第四：**点击<下一步>，如下图


图 141：客户端安装

**第五：**点击<下一步>，如下图


图 142：客户端安装

**第六：**点击<完成>，如下图，实现准入客户端的安装。


图 143：客户端安装

### 9.2.5 应用限额

**功能描述：**针对某个或某组用户限制一种或多种应用能使用多少流量或多少时长。

**配置路径：**【行为管理】>【上网策略】>【应用限额策略】

**配置描述：**进入【应用限额策略】界面，点击“新增”应用限额策略，如图：

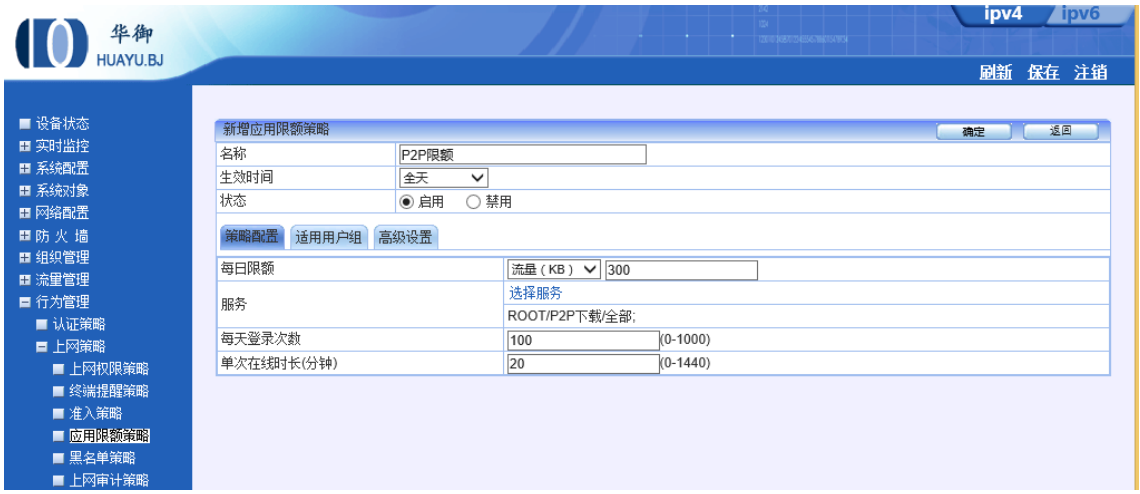



图 144：新增应用限额策略

**参数说明：**

- 名称：应用限额策略名称。
- 生效时间：选择生效的时间范围，可以提前时间计划中定义好时间策略。
- 状态：启用或禁用。
- 每日限额：当天可供规则内应用占用的带宽总量或使用时长。
- 服务：选择需要设置的一种或多种服务。
- 每天登陆次数：设定应用每天登陆的次数。
- 单次在线时长：设定应用单次在线的时长，单位为分钟。
- 适用用户组：选择需要针对哪些用户生效。

### 9.2.6 黑名单策略

为了防止网络资源的滥用和方便管理员管理用户，设备支持将超量使用网络资源(流量、带宽、会话)的用户加入黑名单，以示惩罚。对进入黑名单的用户可以采取惩罚机制，惩罚期限到了之后，该用户又可以正常使用网络。

**功能描述：**将超量使用网络资源(流量、带宽、会话)的用户加入黑名单，以示惩罚。

**配置路径：**【行为管理】>【上网策略】>【黑名单规则】

**配置描述：**进入【黑名单规则】配置页面，点击<新增>按钮，如下图：


图 145：新增黑名单策略

**参数说明：**

- 名称：黑名单规则的名称。
- 生效时间：在生效时间内才进行黑名单的控制；在生效时间外，不对用户的速率和会话进行限制，用户产生的流量也不记入黑名单的流量配额内。
- 状态：启用或禁用。
- 拒绝内部共享上网：启用后，系统将自动发现共享上网的用户，并加入到黑名单中。
- 每日流量配额：每天允许使用的流量值，总流量、上行流量、下行流量三个值独立计算。
- 每周流量配额：每天允许使用的流量值，总流量、上行流量、下行流量三个值独立计算。
- 每月流量配额：每天允许使用的流量值，总流量、上行流量、下行流量三个值独立计算。
- 每日最大上线时间：每日允许上线的时间，单位可按照分钟、小时来设置。
- 每周最大上线时间：每周允许上线的时间，单位可按照分钟、小时来设置。
- 每月最大上线时间：每月允许上线的时间，单位可按照分钟、小时来设置。
- 最大速率：连续多少分钟内，速率超过一定阀值，上行速率和下行速率分开计算。
- 最大会话数：连续多少分钟内，分钟会话数持续超过一定阀值，上行会话和下行会话分开计算。

- 新增最大会话数：连续多少分钟内，分钟新增会话数持续超过，上行会话和下行会话分开计算。
- 惩罚方式：当用户进入黑名单时的惩罚方式，包括：强制下线、修改带宽和会话。强制下线表示该用户不能上网，修改带宽和会话表示修改用户的带宽和会话值。
- 惩罚时长：用户进入黑名单的时间。当惩罚时间到了，用户又可以正常上网。
- 加倍惩罚：当用户在一段时间内(包括：在一周内、在一月内、在一季度内) 连续进入黑名单的次数超过预设阀值后，将被加倍惩罚。比如，惩罚时间将变为原来的 3 倍。
- 适用用户组：选择需要针对哪些用户生效。

### 9.2.7 上网审计策略

**功能描述：**过滤报表中心行为分析的记录内容，如：对某些用户只记录 WEB 记录和 FTP 记录等。

**配置路径：**【行为管理】>【上网策略】>【上网审计策略】

**配置描述：**进入【上网审计策略】页面，点击<新增>按钮，如下图所示：


图 146：上网审计策略

**参数说明：**

- 名称：上网审计策略名称。
- 生效时间：在生效时间内审计策略才生效。
- 状态：启用或禁用。
- WEB 记录：可复选“URL 地址”、“网页标题”、“论坛/微博发帖”、“搜索关键字”、“文件上传”、“外发信息”、“网页内容过滤”。 “URL 地址”记录 URL 的全址。

“网页标题”记录 WEB 页面的标题。“发帖信息”记录在论坛上发贴的内容。“搜索关键字”记录在搜索引擎上搜索的关键字。“文件上传”记录通过 WEB 上传的文件的记录。

- 账号登录：选择审计登录账号信息。
- 即时通讯：可复选“通信内容”和“文件上传”。
- 邮件记录：可复选“基本信息”、“邮件正文”和“邮件附件”。“基本信息”记录的信息包括：发件人、收件人、邮件主题、日期。 “邮件正文”记录邮件的基本信息和邮件正文的内容。“邮件附件”记录邮件的基本信息和邮件附件，附件将保存到硬盘中，可以下载到本地。
- FTP 记录：可复选“仅文件名”、“文件上传”。可记录 FTP 的登录信息，上传下载文件信息。
- Telnet 记录：启用 Telnet 记录。
- 会话记录：记录会话信息。
- 统计信息：可复选“流量记录”、“访问量记录”和“在线时长记录”。
- 告警记录：记录告警信息。

提示：带*号者会产生大量日志。

## 9.3 认证选项

### 9.3.1 跨三层 MAC 识别

**功能描述：**设备部署到三层交换机的上方后，数据经过三层交换机后，终端的 MAC 地址都将变成交换机的 MAC 地址，这样将无法还原真是的 MAC 地址，绑定 MAC 地址将失效，通过下面方法配置将实现跨三层绑定 MAC 地址。

**配置路径：**【行为管理】>【认证选项】>【跨三层 MAC 识别】

**配置描述：**

**第一：**进入【跨三层 MAC 识别】页面，如下图所示：

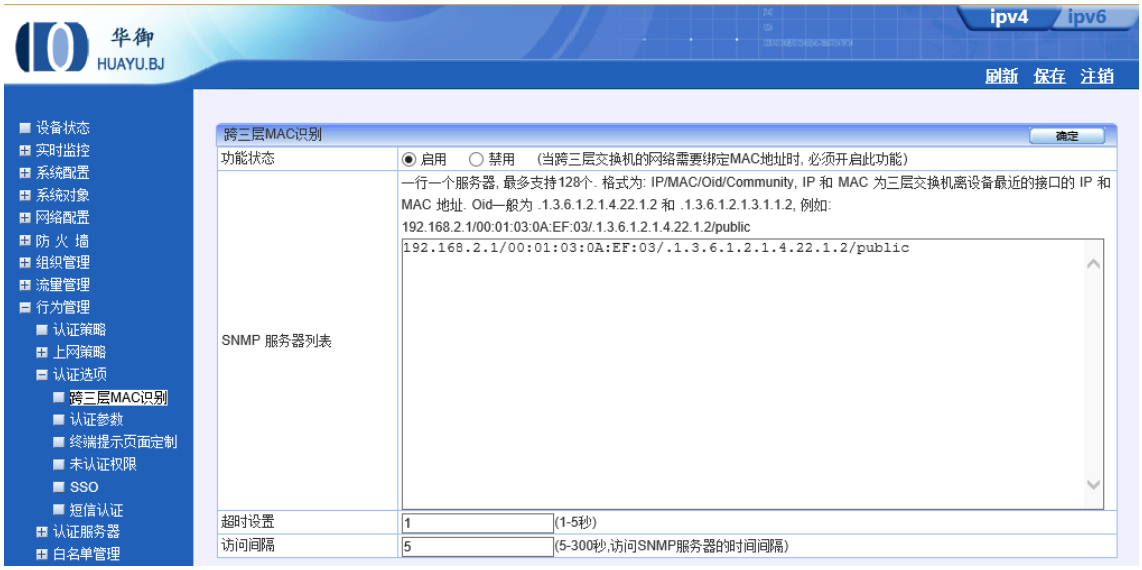



图 147：跨三层 MAC 识别

**第二：**启用功能状态

**第三：**输入交换机的 SNMP 信息，一行一个服务器，最多支持 128 个. 格式为: IP/MAC/Oid/Community, IP 和 MAC 为三层交换机离设备最近的接口的 IP 和 MAC 地址. Oid 一般为 .1.3.6.1.2.1.4.22.1.2 和 .1.3.6.1.2.1.3.1.1.2，例如: 192.168.2.1/00:01:03:0A:EF:03/.1.3.6.1.2.1.4.22.1.2/public。

第四：（下面这个操作在三层交换机上配置）开启三层交换机的 SNMP 协议，获取三层交换机的 community 值，交换机必须支持 SNMPV2 及以上的版本，下面给出 H3C、华为、思科交换机的配置

H3C 交换机配置

[Sysname]snmp-agent sys-info version v1v2c

[Sysname]snmp-agent community read public

华为交换机配置

snmp-agent community read public

snmp-agent sys-info version all

思科交换机配置

snmp-server community public ro

通过上面的配置，设置只读 community 名为 public；

### 9.3.2 认证参数

**功能描述：**设置客户端 WEB 认证窗口登录界面设置

**配置路径：**【行为管理】>【认证选项】>【认证参数】，配置页面如下：


图 148：认证参数

**参数说明：**

- 用户语言：选择认证界面显示的语言。
- 认证方式：现在认证过程使用的协议，有[HTTPS]和[HTTP]两种，默认[HTTP]。
- 认证端口：[HTTP]认证方式的认证端口，默认80。[HTTPS]认证方式的端口固定为443。
- 认证超时：认证成功后，在设定的时间内用户没有上网流量，认证用户自动下线。
- 其他认证选项：每天前置注销所有用户。
- 关闭登录页面退出登录：勾选启用。
- 公告信息：管理员可以设置一些信息公告给每个用户，将在认证客户端页面显示。
- 黑名公告信息：管理员可以设置一些信息公告给每个用户，将在用户进入黑名单时显示到客户端。
- 认证通过跳转，可选择认证通过后跳转到用户上网信息页面、最近请求页面、自定义页面。

### 9.3.3 终端提示页面定制

**功能描述：**设置客户端认证页面、认证成功、URL 禁止访问、准入策略、公告页面、黑名单通知的页面。

**配置路径：**【行为管理】>【认证选项】>【终端提示页面定制】，配置页面如下：


图 149：终端提示页面定制

**参数说明：**

- 认证页面：配置用户登录认证的页面。
- 认证成功：配置内置的认证成功返回的页面。
- URL禁止访问：配置URL被禁止访问时，出现的提醒页面。
- 准入策略：在安装了准入客户端，但未通过准入规则的情况下出现的提示页面。
- 公告页面：在【行为管理】>【上网策略】>【终端提醒策略】中定义好公告后，在此处修改公告页面的内容。
- 黑名单通知：当用户被加入黑名单时提示的页面定制。

### 9.3.4 未认证权限

**配置描述：**进入【未认证权限】页面，[当用户未通过认证时可以访问 DNS 和 Ping 服务]默认已勾选，即未通过认证的用户可以访问 DNS 和 Ping 服务。其它服务禁止访问，若未认证用户需要访问更多的服务，需要在[未认证权限策略]处添加策略。配置页面如下：

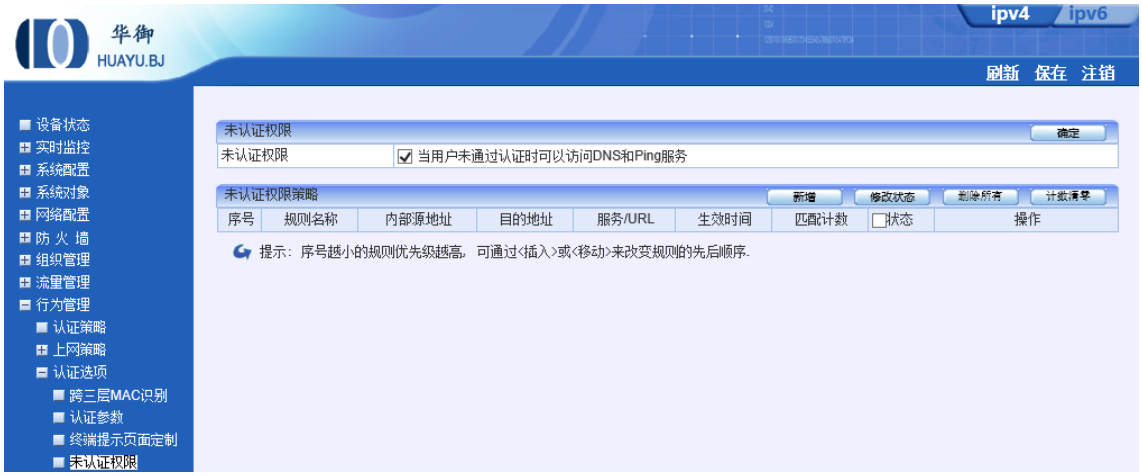



图 150：未认证权限

点击<删除所有>，将删除所有的策略。

改变状态栏复选框的值，再点击<修改状态>，可修改策略的状态(“勾选”表示启用，“不勾选”表示禁用)。

点击表头的“状态”复选框，可以改变所有策略的状态。

点击<修改>，修改本条策略的参数，但不能修改本条策略的方向。

点击<插入>，在当前位置之前插入一条策略。

点击<移动>，改变对应策略的序号，从而改变策略的优先级。

点击<删除>，删除本条策略。

点击<新增>，新增策略，如下图：


图 151：新增未认证权限规则

**参数说明：**

- 规则名称：输入新增“未认证权限规则”的名称。
- 内部源地址：数据流的源地址（内网主机地址），可输入 IP 地址或选择地址簿。地址簿在【系统对象>地址簿】中配置。
- 目的地址：数据流的目的地址，可输入 IP 地址或选择地址簿。

- 服务/URL：定义未认证可以使用的服务或 URL 地址。
- 生效时间：本策略的有效时间段。
- 状态：启用或禁用本规则，默认启用。

### 9.3.5 SSO

SSO 用于配置点单登陆，与其他认证服务器进行联动，避免多次认证，包括 AD SSO、PPPOESSO、WEB SSO、第三方设备、HTTP 单点登陆接口、PROXY SSO、SSO 镜像设置。

#### 9.3.5.1 AD SSO

**功能描述：**配置与 windows 的 AD 域单点认证

**配置路径：**【行为管理】>【认证选项】>【SSO】，点击页面顶部的<ADSSO>配置，如下图所示：

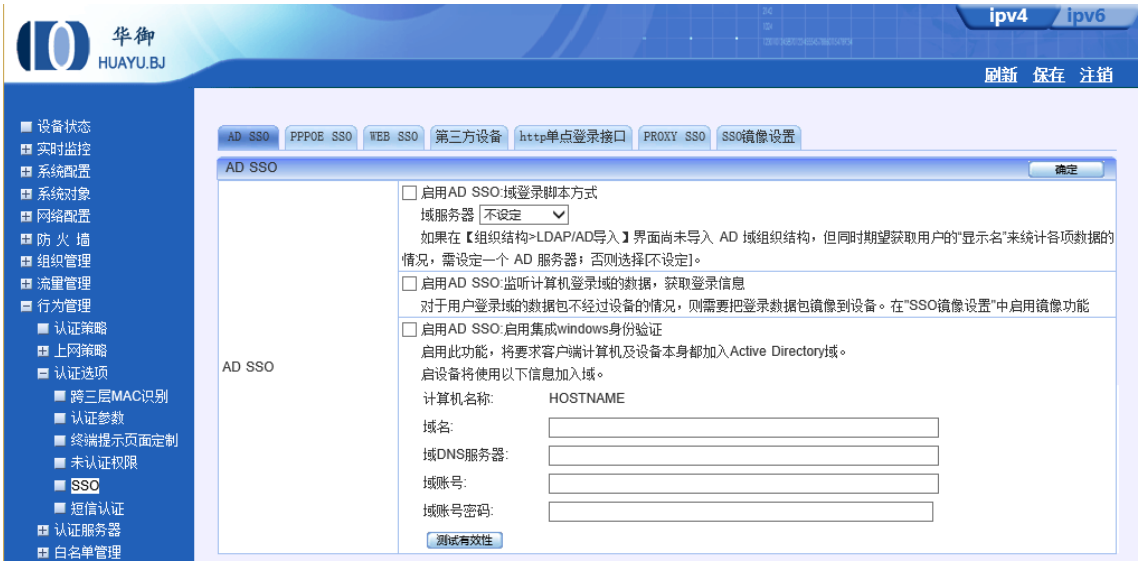



图 152：SSO 单点登录配置

**参数说明：**

- 启用AD SSO:域登录脚本方式：如果在【组织结构>LDAP/AD导入】界面尚未导入 AD 域组织结构，但同时期望获取用户的“显示名”来统计各项数据的情况，需设定一个 AD 服务器；否则选择[不设定]。
- 启用AD SSO:监听计算机登录域的数据，获取登录信息： 对于用户登录域的数据包不经过设备的情况，则需要把登录数据包镜像到设备。在"SSO镜像设置"中启用镜像功能。

- 启用AD SSO:启用集成windows身份验证：启用此功能，将要求客户端计算机及设备本身都加入Active Directory域。在下方填写给本设备分配的域信息。

### 9.3.5.2 PPPOE SSO

**功能描述：**配置与 PPPOE 单点认证

**配置路径：**【行为管理】>【认证选项】>【SSO】，点击页面顶部的<PPPOE SSO>配置，点击启用，如下图所示：


图 153：PPPOE SSO 配置

### 9.3.5.3 Web SSO

**功能描述：**配置与其他 Web 认证服务器的单点登陆认证

**配置路径：**【行为管理】>【认证选项】>【SSO】，点击页面顶部的<Web SSO>配置，如下图所示：


图 154：WEB SSO 配置

**参数说明：**

- 启用 Web 单点登录: 用户 WEB 认证的数据包不经过本设备，需要镜像 WEB 认证数据包到本设备，同时启用 Web 单点登录，并在"SSO 镜像设置"中启用镜像功能。
- Web 认证服务器地址：输入外部 web 认证服务器地址。
- 用户认证 POST 页面 URL：(例如: /cgi-bin/auth.php)
- 用户账号提取正则表达式：使用(.*?)提取用户账号,例如 POST 页面中用户账号字符串为“username=abc&”,则使用正则表达式“username=(.*?)&”可将用户账号 abc 提取出来。
- 认证结果：可选择，认证成功页面的 URL(例如: /auth_ok.php)、认证成功结果中的关键字(认证请求和认证结果在同一个 http 连接中)、认证失败结果中的关键字(认证请求和认证结果在同一个 http 连接中)的其中一种，然后在下面输入认证结果信息。

### 9.3.5.4 第三方设备

**功能描述：**配置与第三方设备的单点认证

**配置路径：**【行为管理】>【认证选项】>【SSO】，点击页面顶部的<第三方设备>配置，如下图所示，点击启用按钮设置。

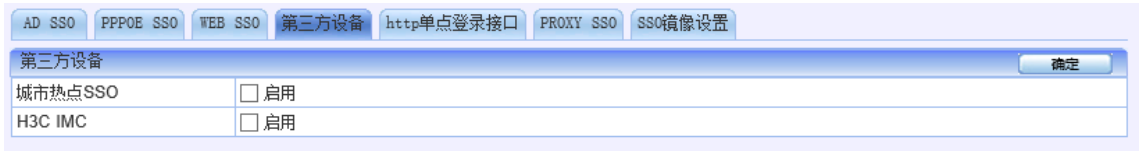



图 155：第三方设备 SSO 配置

### 9.3.5.5 Http 单点登陆接口

**功能描述：**启用此功能，为第三方设备认证设备提供 HTTP 单点登录接口。

**配置路径：**【行为管理】>【认证选项】>【SSO】，点击页面顶部的< Http 单点登陆接口 >配置，如下图所示：


图 156：HTTP 单点登录接口

点击启用，接口格式如下：

1. 用户登录接口

http://172.16.1.1/http_sso_page.php?login=1&username=abc&showname=abc&groupname=AAA&userip=172.16.1.100

2. 用户注销接口

http://172.16.1.1/http_sso_page.php?logout=1&userip=172.16.1.100

其中 username,showname,groupname 为 utf8 编码,并 urlencode 编码. 172.16.1.1 为设备地址,172.16.1.100 为上线用户 ip 地址。

### 9.3.6 短信认证

**功能描述：**启用此功能，为设备配置短信认证功能，包括 HTTP 协议方式、GSM 短信猫、CDMA 短信猫、电信运营商等方式。

**配置路径：**【行为管理】>【认证选项】>【短信认证】，如下图所示：

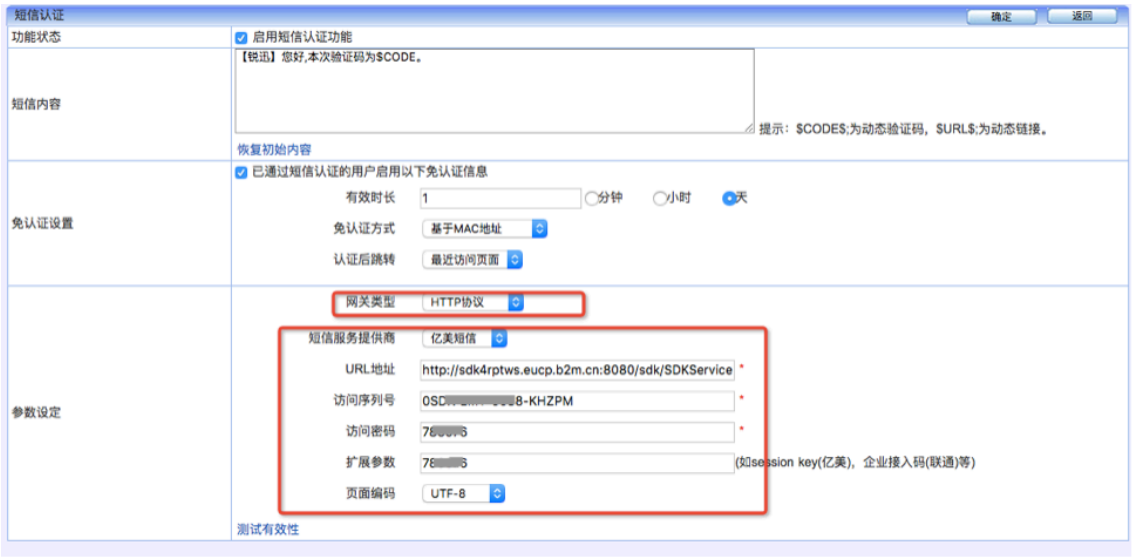

图 157：短信认证配置

**参数说明：**

- 功能转台:启用短信认证功能。
- 短信内容：输入手机客户接受到的短信信息，其中$CODE$;为动态验证码，$URL$;为动态链接。
- 免认证设置：已通过短信认证的用户启用以下免认证信息，设定有效时长、基于浏览器 Cookie 或基于 MAC 地址进行免认证、认真后跳转到最近访问页面或认证通过页面。
- 参数设定：可以选择 HTTP 协议方式、GSM 短信猫、CDMA 短信猫、电信运营商、自定义服务器的其中一种。

■ **第三方网关认证**

下面按照第三方网关举例说明，如下图所示，以亿美短信举例，选择的借口类型是 webservice，其中 URL 地址与访问序列号，需要和亿美官方确认，确保帐号中有费，访问密码和




备注：亿美 webservice 协议：http://sdk4rptws.eucp.b2m.cn:8080/sdk/SDKService?wsdl

扩展参数与访问密码相同。

■ **短信猫认证：**

可以选择不同运营商，举例电信的可以用 CDMA MODEM，WAVECOM 品牌，型号 M1206B，这款是 3G 的，需要支持 3G 的电信卡才能使用，将短信猫插入 USB 借口，短信认证，配置的方法如下图所示：

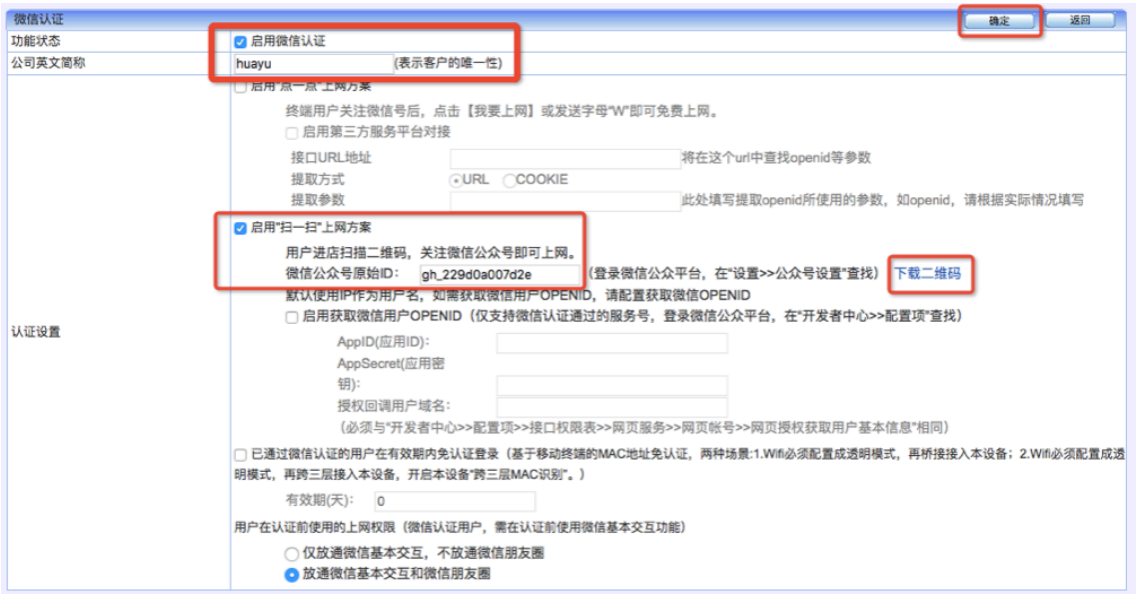

## 9.3.7 微信认证

1、注册微信公众号

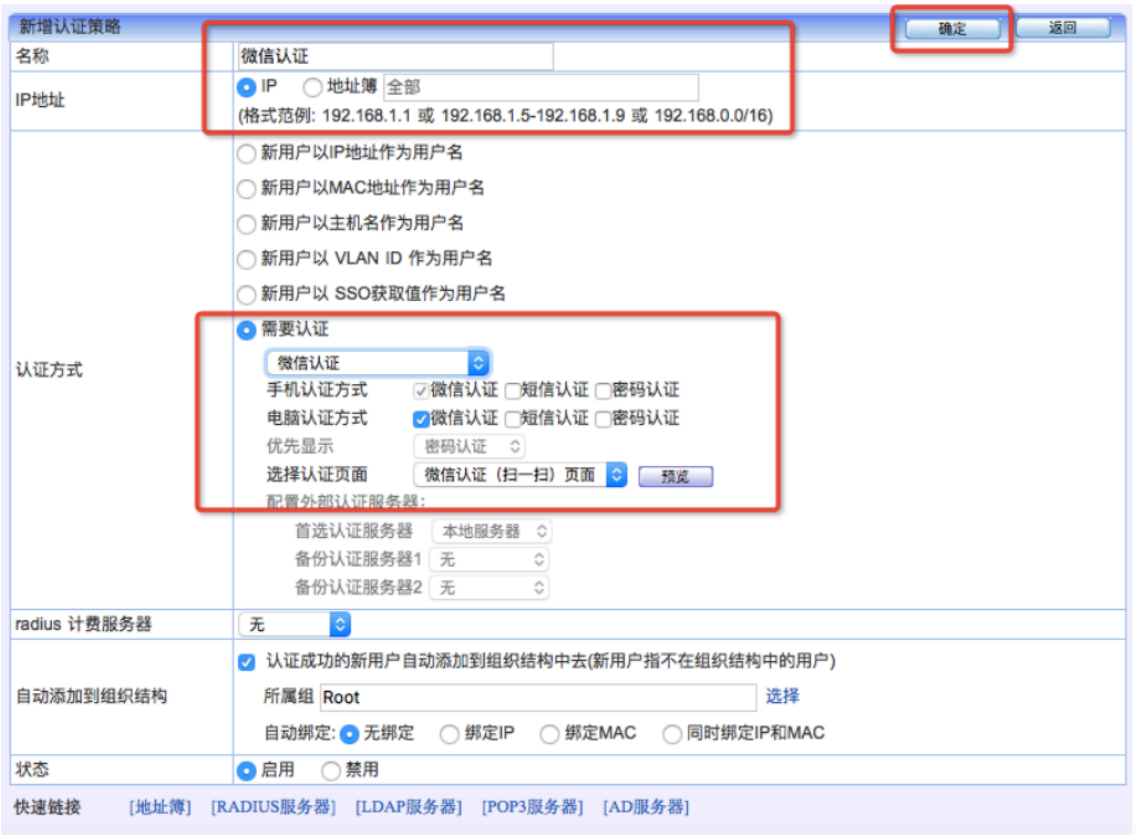
注册的时候**一定要选择订阅号**，如下图所示：


2、找到你的公众号原始 ID，如下图所示


3、配置微信认证，如下图所示，下载的二维码，可用于用户扫码。




4、新建一条认证策略［行为管理］>［认证策略］，如下图所示：




## 9.4 认证服务器

认证服务器包括 RADIUS 服务器、AD 服务器、LDAP 服务器、POP3 服务器和服务器测试。

### 9.4.1 RADIUS 服务器

**功能描述：**配置 RADIUS 认证服务器

**配置路径：**【行为管理】>【认证服务器】>【RADIUS 服务器】

**配置描述：**

**第一：**进入【RADIUS 服务器】页面，点击<新增>按钮，，配置 RADIUS 认证服务器，如下图：


图 158：新增 RADIUS 认证服务器

**参数说明：**

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP 地址：RADUIS 服务器 IP 地址。
- 认证端口：服务器中用于认证的端口号，缺省 1812。
- 计费端口：服务器中用于计费的端口号，缺省 1813。
- 间隔传送时间：设定定期传送的时间，单位为妙。
- 共享密钥：与 RADUIS 服务器交换数据时进行加密的密钥。
- 使用 radius 返回值作为用户组：点击启用。

### 9.4.2 AD 服务器

**功能描述：**配置 AD 认证服务器

**配置路径：**【行为管理】>【认证服务器】>【AD 服务器】

**配置描述：**

**第一：**进入【AD 服务器】页面，点击<新增>按钮，配置 AD 认证服务器，如下图：


图 159：新增 AD 域名认证服务器

**参数说明：**

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP 地址：AD 服务器 IP 地址。
- AD 域名：域控制器域名，例如 abc.com。
- 查找用户 DN：输入查找用户的用户名，如：administrator@huayu.com
- 查找用户名密码：查找用户在 AD 服务器中的密码。

### 9.4.3 LDAP 服务器

**功能描述：**配置 LDAP 认证服务器

**配置路径：**【行为管理】>【认证服务器】>【LDAP 服务器】

**配置描述：**

**第一：**进入【LDAP 服务器】页面，点击<新增>按钮，配置 LDAP 认证服务器，如下图：


图 160：新增 LDAP 认证服务器

**参数说明：**

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字。
- IP 地址：LDAP 服务器 IP 地址。
- 认证端口：服务器中用于认证的端口号，缺省为 389。
- DN：LDAP 服务器用通用名称标识符搜索具体条目时所使用的路径，如 cn=searcher,cn=software,dc=abc,dc=com，
- CN：识别在 LDAP 服务器中输入的个体的标识符，如 cn=cn 。
- 查找用户 DN：所查找用户的路径，如 cn=searcher,ou=group1,dc=abc,dc=com。

### 9.4.4 POP3 服务器

**功能描述：**配置 POP3 认证服务器

**配置路径：**【行为管理】>【认证服务器】>【POP3 服务器】

**配置描述：**

**第一：**进入【POP3 服务器】页面，点击<新增>按钮，配置 POP3 认证服务器，如下图：


图 161：新增 POP3 认证服务器

**参数说明：**

- 名称：合法的字符是数字(0-9)，字母(A-Z，a-z)和下划线，中划线及中文汉字
- IP/域名：POP3 服务器 IP 地址或域名

## 9.5 白名单

### 9.5.1 IP 白名单

**功能描述：**对于特殊的用户，他们的上网不希望受到各种控制策略的限制，也不希望上网的内容被记录。设备的白名单功能可以很好的满足这些需求。符合白名单规则的流量，将不受“防火墙规则、流控规则、认证策略规则、上网策略对象规则、黑名单规则”的控制；上网的流量值以及会话记录将被统计；但统计的流量将不计入黑名单规则的流量统计中；上网行为的内容（如发送的邮件、发送的帖子、访问的网页、即时通讯记录等）将全部不记录。

**配置路径：**【行为管理】>【白名单规则】>【IP 白名单】

**配置描述：**进入【IP 白名单】配置页面，点击<新增>按钮，增加 IP 白名单，如下图所示：

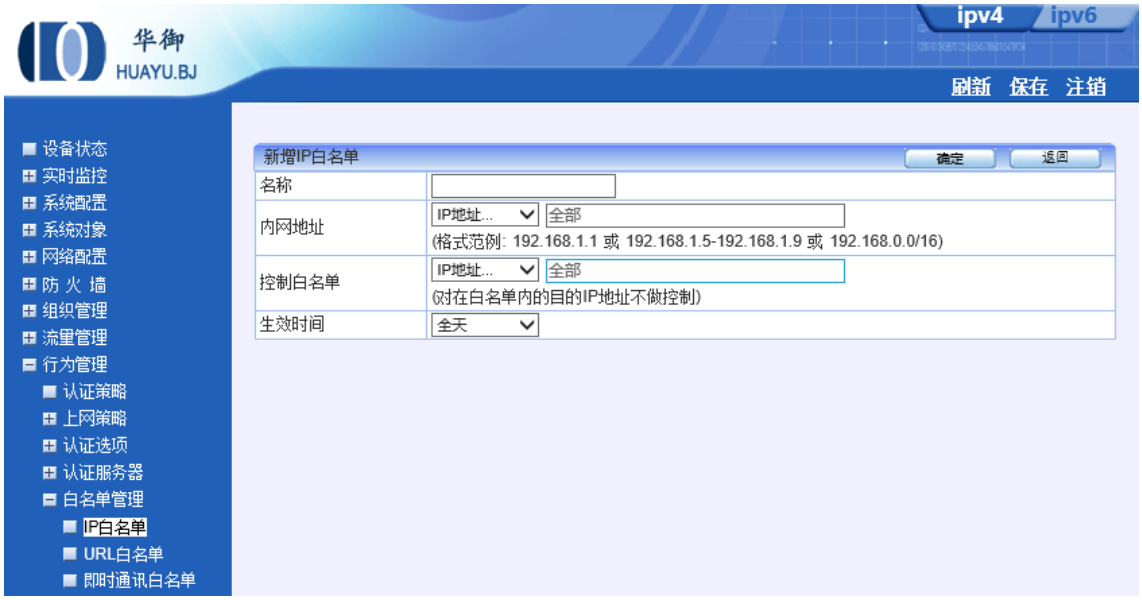



图 162：IP 白名单

**参数说明：**

- 名称：白名单规则的名称。
- 内网地址：不受控的用户的地址，有三种输入方式，详细说明如下：
  - IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；
  - 地址簿：引用已定义好的地址簿；
  - 用户组：引用组织结构中定义的用户组
- 控制白名单：不受控的外网地址，有两种输入方式，详细说明如下：
  - IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；
  - 地址簿：引用已定义好的地址簿；
- 生效时间：白名单规则的生效时间。生效时间以外，该规则不起作用。

### 9.5.2 URL 白名单

**功能描述：**针对指定用于放心指定的 URL 地址。URL 白名单包含的流量全部放行，不受任何策略的控制，也不被审计。

**配置路径：**【行为管理】>【白名单规则】>【URL 白名单】

**配置描述：**进入【URL 白名单】配置页面，点击<新增>按钮，增加 URL 白名单，如下图所示：

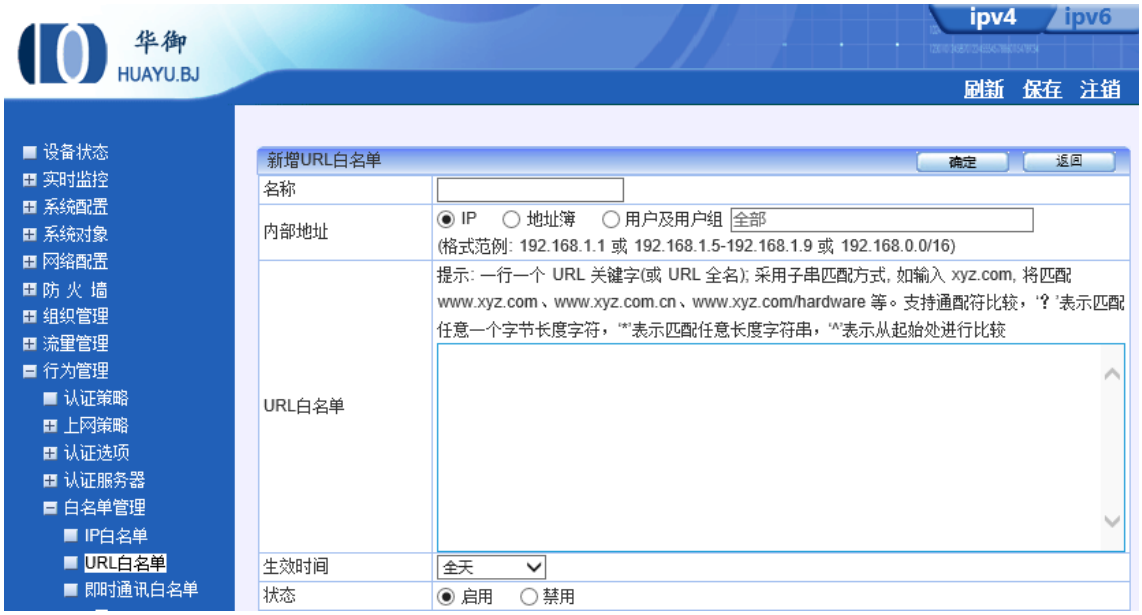



图 163：URL 白名单

**参数说明：**

- 名称：白名单规则的名称。
- 内网地址：针对 URL 白名单的用户的地址,有三种输入方式，详细说明如下：
  - IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；
  - 地址簿：引用已定义好的地址簿；
  - 用户组：引用组织结构中定义的用户组
- URL 白名单：不受控的 URL 地址,一行一个：
- 生效时间：白名单规则的生效时间。生效时间以外，该规则不起作用。
- 状态：启用或禁用，默认为启用。

### 9.5.3 即时通信白名单

**功能描述：**只有在'即时通讯白名单'策略里的账号才可登录和使用，但其通讯记录是否被审计由【报表中心>内容记录配置】页面的配置来决定。

**配置路径：**【行为管理】>【白名单规则】>【即时通信白名单】

**配置描述：**进入【即时通信白名单】配置页面，点击<新增>按钮，增加即时通信白名单，如下图所示：

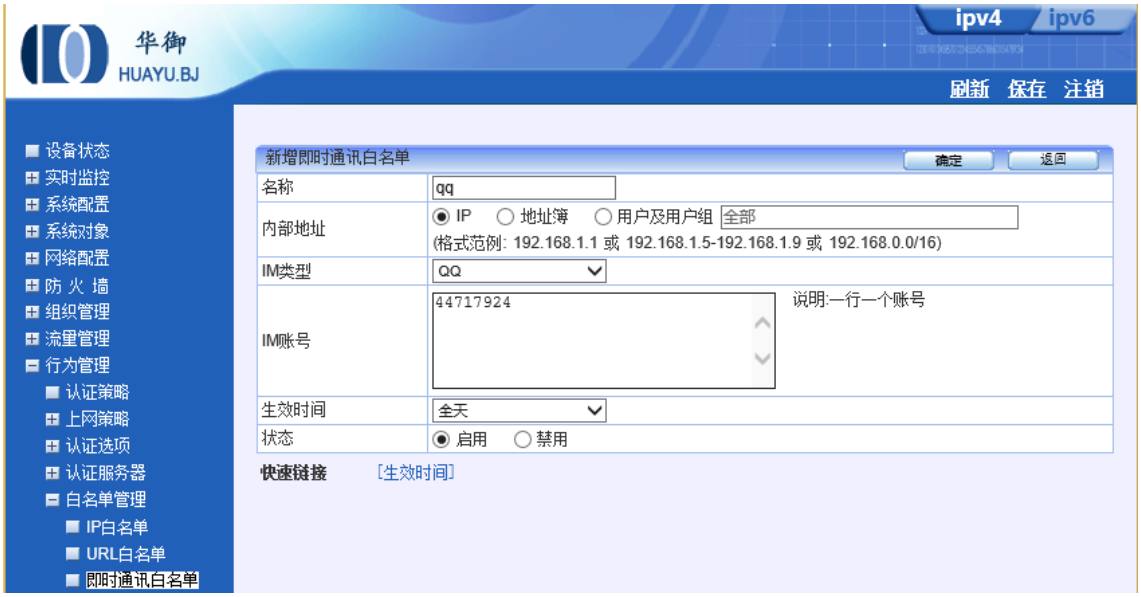



图 164：即时通讯白名单

**参数说明：**

- 名称：即时通信白名单规则的名称。
- 内网地址：针对 URL 白名单的用户的地址,有三种输入方式，详细说明如下：
  - IP 地址：可输入一个 IP 地址、一段 IP 地址、IP 子网；
  - 地址簿：引用已定义好的地址簿；
  - 用户组：引用组织结构中定义的用户组
- 即时通信类型：选择 QQ、MSN、yahoo、飞信、ICQ、Gtalk、阿里旺旺的其中一种。
- IM 账号：输入允许的 IM 账号。
- 生效时间：即时通信白名单规则的生效时间。生效时间以外，该规则不起作用。
- 状态：启用或禁用，默认为启用。

# 第10部分 VPN 配置

VPN 用于配置 IPsecVPN 和 SSL VPN，用于建立两点之间的虚拟索道，可以是总部与分公司的 Ipsec VPN 也可以是在家或出差连接公司的 SSL VPN。

## 10.1 IPSec VPN

### 10.1.1 IPsec 隧道

**功能描述：**配置 IPSec 隧道。

**配置路径：**【VPN】>【IPSec】>【IPSec 隧道】

**配置描述：**

**第一：**进入【IPSec 隧道】页面，可以看到当前已建立的 IPSec 隧道配置。如下图：


图 165：IPSec 隧道列表

**第二：**进入点击<新增>按钮，增加 IPSec 隧道。如下图：


图 166：新增 IPSec 隧道

**参数说明：**

- 本地网关：有三个选项
  - 固定IP地址：指行为管理设备 WAN 端下一跳 IP 地址和本端标识（E-mail地址）。
  - 域名格式:输入域名全称。
  - 电子邮件格式： 输入E-mail地址。
- 本地网关：指对端 VPN 设备连接 IP 或域名或对端为 VPN 拨号用户，必须有一端为为固定IP，同样有四个选项
  - 固定IP地址：指对端行为管理设备 IP 地址和对端标识。
  - 域名格式:输入域名全称。
  - 电子邮件格式： 输入E-mail地址。
  - 拨号用户：输入对端IP地址和对端标识
- 协商模式：配置 VPN 协商模式，两端协商模式必须一致。
- 预共享密钥：配置 VPN 连接的预共享密钥，两端预共享密钥必须一致。
- 点击<高级>按钮，可配置 IPSec 连接的更多详细参数，两端必须一致。

## 10.1.2 IPSec 规则

**功能描述：**配置 IPSec 规则。

**配置描述：**

**第一：**进入【IPSec 规则】页面，可以看到当前已建立的 IPSec 规则配置。如下图：


图 167：IPSec 规则列表

**第二：**进入点击<新增>按钮，增加 IPSec 规则。如下图：


图 168：新增 IPSec 规则

**参数说明：**

- 源地址：指需要匹配 VPN 规则的行为管理设备 LAN 端地址。
- 目标地址：指与哪些目标地址通讯时使用 VPN 隧道。
- 服务：被指定的服务将使用 VPN 隧道。
- 隧道名称：将此规则应用在合适的 VPN 隧道上。
- 方向：指规则应用的数据流方向。
- 状态：启用或禁用该规则。

## 10.2 PPTP

**功能描述：**配置 PPTP VPN

**配置路径：**【VPN】>【PPTP】

**配置描述：**

**第一：**进入【PPTP】页面，开始设置 PPTP的相关参数。如下图：


图 169：PPTP 配置

**参数说明：**

- PPTP 状态：启用或禁用 PPTP 服务器功能。
- 服务器 IP：本机作为 PPTP 服务器的接口 IP 地址。
- 首选 DNS 服务器：分配给 PPTP 客户端的首选 DNS 服务器。
- 备用 DNS 服务器：分配给 PPTP 客户端的备用 DNS 服务器。
- 认证方式：选择 Radius 认证，或 VPN 用户本地认证

**第二：**进入点击<新增>按钮，增加 PPTP IP 池。如下图：

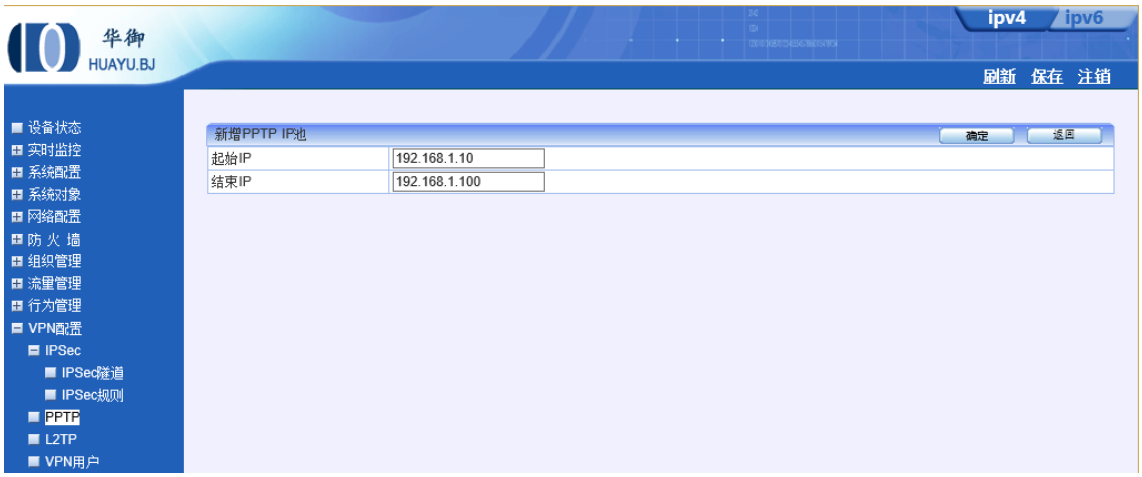



图 170：新增 PPTP IP 池

**参数说明：**

- 起始 IP：分配给 PPTP 客户端的 IP 地址段的起始地址。

- 结束 IP：分配给 PPTP 客户端的 IP 地址段的结束地址。

## 10.3 L2TP

**功能描述：**配置 L2TP VPN

**配置路径：**【VPN】>【L2TP】

**配置描述：**

**第一：**进入【L2TP】页面，开始设置 L2TP 的相关参数。如下图：


图 171：L2TP 配置

**参数说明：**

- L2TP 状态：启用或禁用，默认为启用。
- 服务器 IP：填写外网口 IP 地址。
- 域共享秘钥：L2TP IPSEC VPN 客户端预共享密钥。
- L2TP 本地 IP：L2TP VPN 客户端协商成功后的网关 IP。
- L2TP IP 范围：
  - 起始 IP：分配给 L2TP 客户端的 IP 地址段的起始地址。
  - 结束 IP：分配给 L2TP 客户端的 IP 地址段的起始地址。
- 首选 DNS 服务器：分配给 L2TP 客户端的首选 DNS 服务器。
- 备用 DNS 服务器：分配给 L2TP 客户端的首选 DNS 服务器。
- 认证方式：选择 Radius 认证，或 VPN 用户本地认证。

## 10.4 VPN 用户

**功能描述：**配置 VPN 的用户，该用户可应用于 PPTP VPN 和 IPSec VPN。

**配置路径：**【VPN】>【VPN 用户】

**配置描述：第一：**进入【VPN 用户】页面，可以看到当前已配置好的 VPN 用户。如下图:


图 172：VPN 用户列表

**第二：**进入点击<新增>按钮，增加 PPTP 用户。如下图：

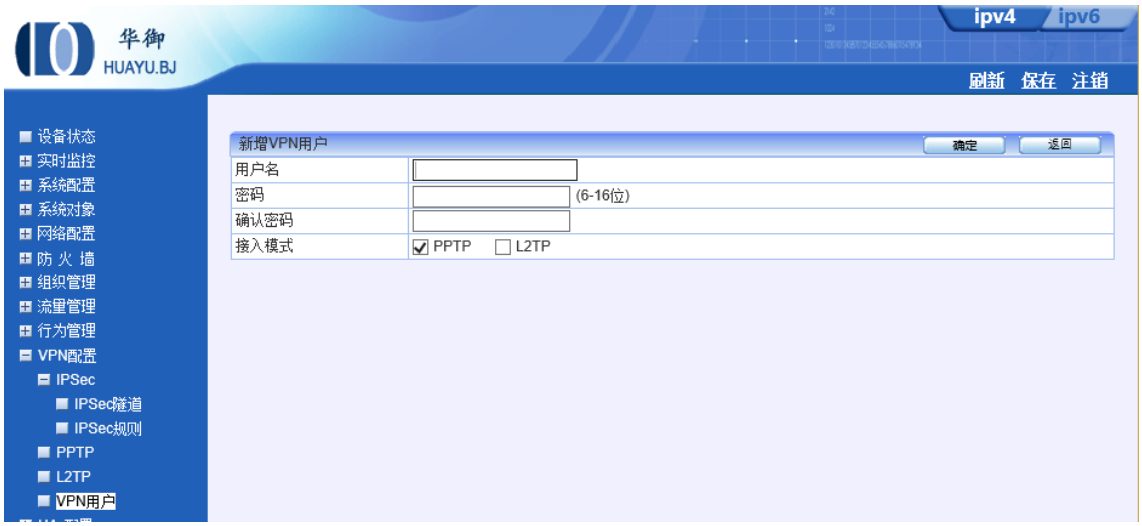



图 173：新增 VPN 用户

**参数说明：**

- 用户名：VPN 用户的名称；
- 密码：VPN 用户的密码；
- 确认密码：VPN 用户的确认密码；
- 接入模式：选择该用户可以应用于哪些 VPN 协议，可选择为 PPTP 或 L2TP 其中一种。

# 第11部分 HA 配置

## 11.1 HA 配置

如果您的网络是冗余网络拓扑接口，可以在网络中部署 2 台 Cross 上网行为管理设备，实现冗余备份，下面介绍以网桥模式 HA 配置，部署拓扑分下面两种;

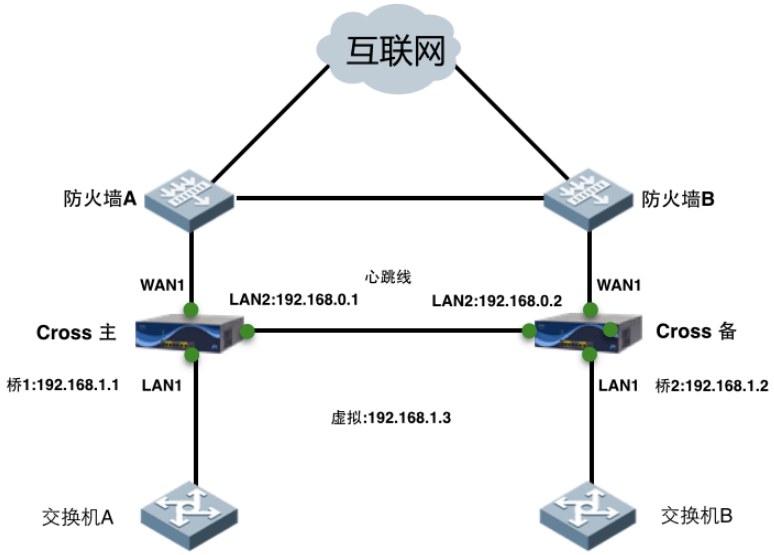



图 174：HA 配置 1

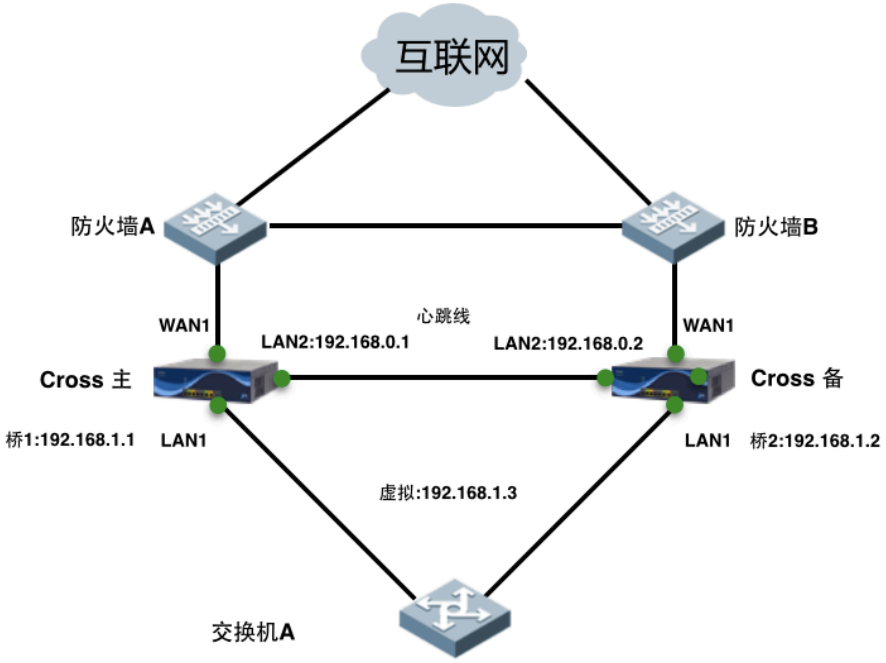



图 175：HA 配置图 2

**第一步:**配置主备设备的 IP 地址，主网桥 1：IP 地址 192.168.1.1/24；备网桥 1：IP 地址 192.168.1.2/24，虚拟 IP 地址定义为：192.168.1.3

**第二步:**配置心跳线 LAN2 地址，主设备配置成 192.168.0.1/24，备设备配置为 192.168.0.2/24

**第三步:**配置主备设备的节点名称,在"系统配置-系统信息"里修改主设备配置为 host1，备设备配置为 host2

**第四步:**配置 HA，启用主设备“自动同步”，“同步 IP”填备机 LAN2 接口的 IP 地址：192.168.0.2(主设备保存配置的时候将自动把配置同步到备机)

**第五步:**在主设备上配置心跳间隔 2s，死亡时间 6s，心跳端口选 LAN2.，对端节点名称写备份的节点 host2,主设备一栏写 host1192.168.1.3/24/192.168.1.255.强制抢占和链路健康检查视情况而定(注意,主设备一栏节点名称需要写要协商成主设备的节点名称,虚拟 IP 必须和 Bridge1IP 相同网段,但是不能和内网地址有冲突)。备份设备除了对端节点名写 hostname001,其他的和主设备一样.

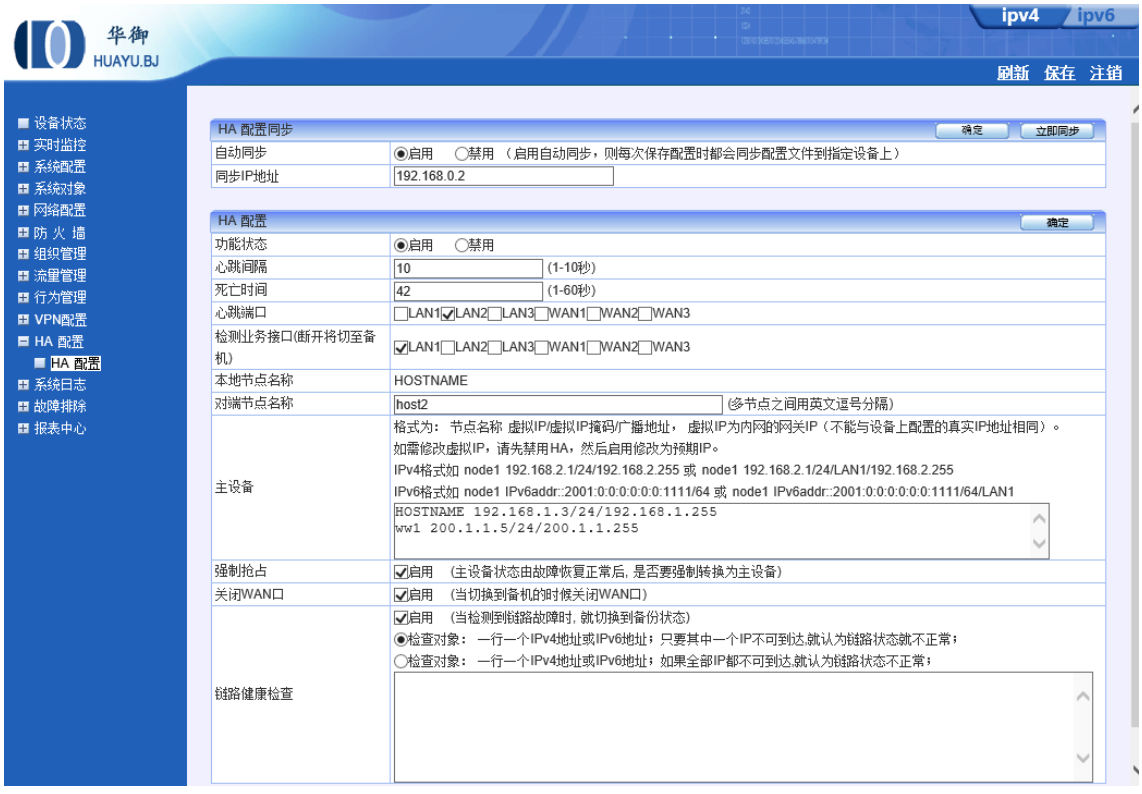



图 176：HA 配置

**第六步:**配置完后,先启用备份设备的 HA 功能,然后在立即开启主设备的 HA 功能,过几秒种 host1 这台就协商成主设备,host2 协商成备份设备,备份设备不转发数据,主设备可以有按钮一键切换到备份设备。

注意事项:(针对图一)

1.第一次 HA 上线的时候，先连接心跳线，并配置心跳线，然后登陆上去，把 pc 接到主设备 LAN1，WAN1 连接备机的 WAN1 口，登陆主机和备机，备机先开启 HA，然后主机开启 HA，协商好后,就可以插线了。

2.Cross 主备 LAN1 口都接在一个交换机上时，在协商好之前，备机不能插线，协商成一主一备后，备机插上线，以防协商过程中出现的短暂环路。

3.备机设备断电的情况下需要把接口线拔了,以防断电 bypass 出现的环路。

4.心跳线出现问题的情况下，2 台设备都会变成主的,需要把原来备机的线拔掉。

# 第12部分 系统日志

## 12.1 命令日志

**功能描述：**将管理员对设备配置的命令记录下来，以便查询。

**配置路径：**【系统日志】>【命令日志】

**配置描述：**

**第一：**进入【命令日志】页面，如下图：


图 177：命令日志

**查询条件：**

- 管理员：根据配置设备的管理员名称来查找。
- IP 地址：根据配置设备的管理员使用的 IP 地址来查找
- 命令内容：根据配置的命令的内容来查找
- 实行结果：根据配置的结果(失败/成功)来查找
- 时间范围：根据管理员配置设备时的时间范围来查找

默认显示所有命令日志。输入查询条件后，点击<查询>按钮，显示满足查询条件的命令日志。点击<清空>按钮，清空所有的命令日志。

## 12.2 事件日志

**功能描述：**设备提供事件日志，用于监视系统事件的发生。

**配置路径：**【系统日志】>【事件日志】

**配置描述：**

**第一：**进入【事件日志】页面，如下图：

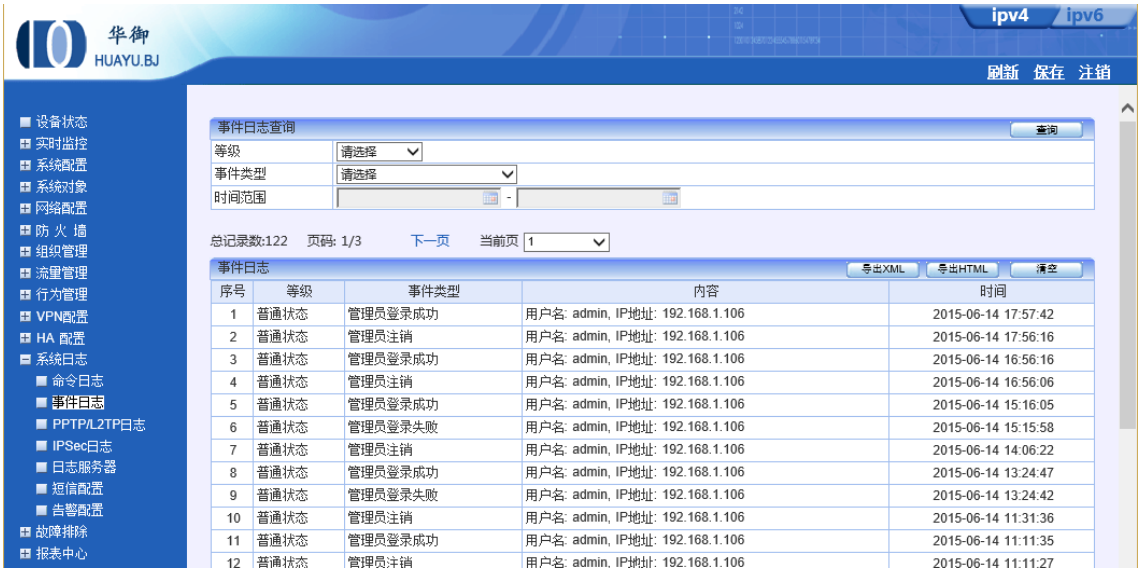



图 178：事件日志

事件日志的内容包括：管理员登录设备成功/失败、物理接口 UP/Down、设备启动成功、ARP 冲突、线路健康结果等等信息点击<清空>按钮，清空所有的命令日志。

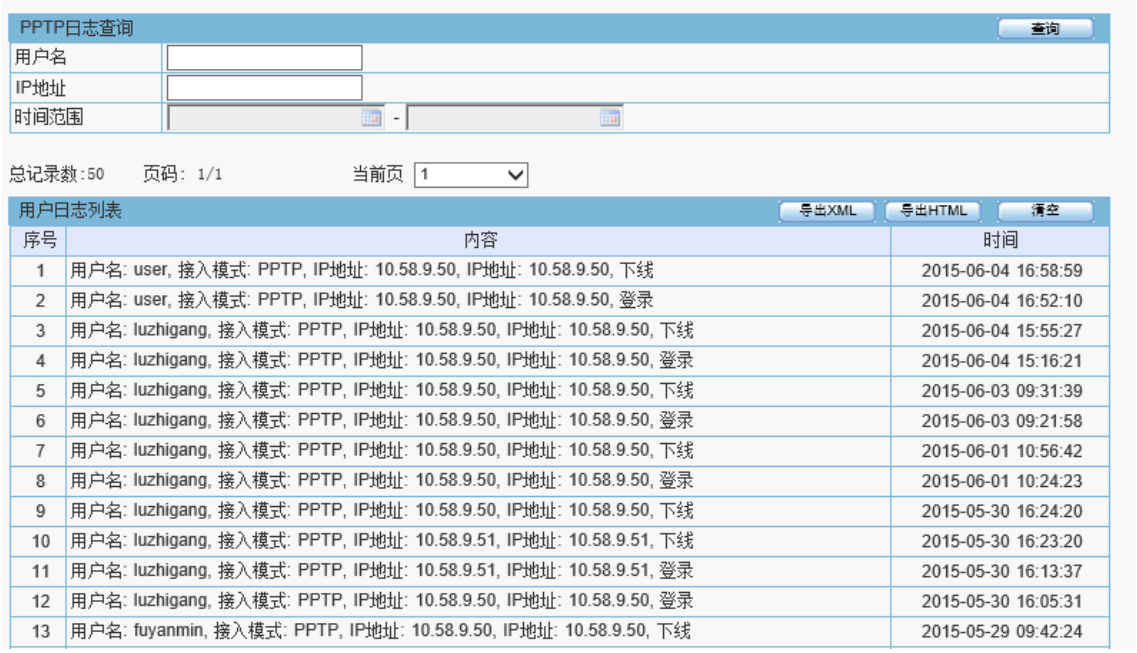
## 12.3 PPTP 日志

**功能描述：**用于记录 PPTP 拨号的日志。

**配置路径：**【系统日志】>【PPTP 日志】

**配置描述：**

**第一：**进入【PPTP 日志】页面，如下图


PPTP日志查询 查询

用户名

IP地址

时间范围 -

总记录数:50 页码: 1/1 当前页 1

用户日志列表 导出XML 导出HTML 清空

| 序号 | 内容 | 时间 |
|---|---|---|
| 1 | 用户名: user, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 下线 | 2015-06-04 16:58:59 |
| 2 | 用户名: user, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 登录 | 2015-06-04 16:52:10 |
| 3 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 下线 | 2015-06-04 15:55:27 |
| 4 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 登录 | 2015-06-04 15:16:21 |
| 5 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 下线 | 2015-06-03 09:31:39 |
| 6 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 登录 | 2015-06-03 09:21:58 |
| 7 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 下线 | 2015-06-01 10:56:42 |
| 8 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 登录 | 2015-06-01 10:24:23 |
| 9 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 下线 | 2015-05-30 16:24:20 |
| 10 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.51, IP地址: 10.58.9.51, 下线 | 2015-05-30 16:23:20 |
| 11 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.51, IP地址: 10.58.9.51, 登录 | 2015-05-30 16:13:37 |
| 12 | 用户名: luzhigang, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 登录 | 2015-05-30 16:05:31 |
| 13 | 用户名: fuyanmin, 接入模式: PPTP, IP地址: 10.58.9.50, IP地址: 10.58.9.50, 下线 | 2015-05-29 09:42:24 |

图 179：PPTP 日志

**查询条件：**

- 用户名：根据用户名称来查找。
- IP 地址：根据用户的 IP 地址来查找
- 时间范围：根据用户登录、认证、下线的时间范围来查找

默认显示所有 PPTP 日志。输入查询条件后，点击<查询>按钮，显示满足查询条件的用户日志。点击<清空>按钮，清空所有的用户日志。

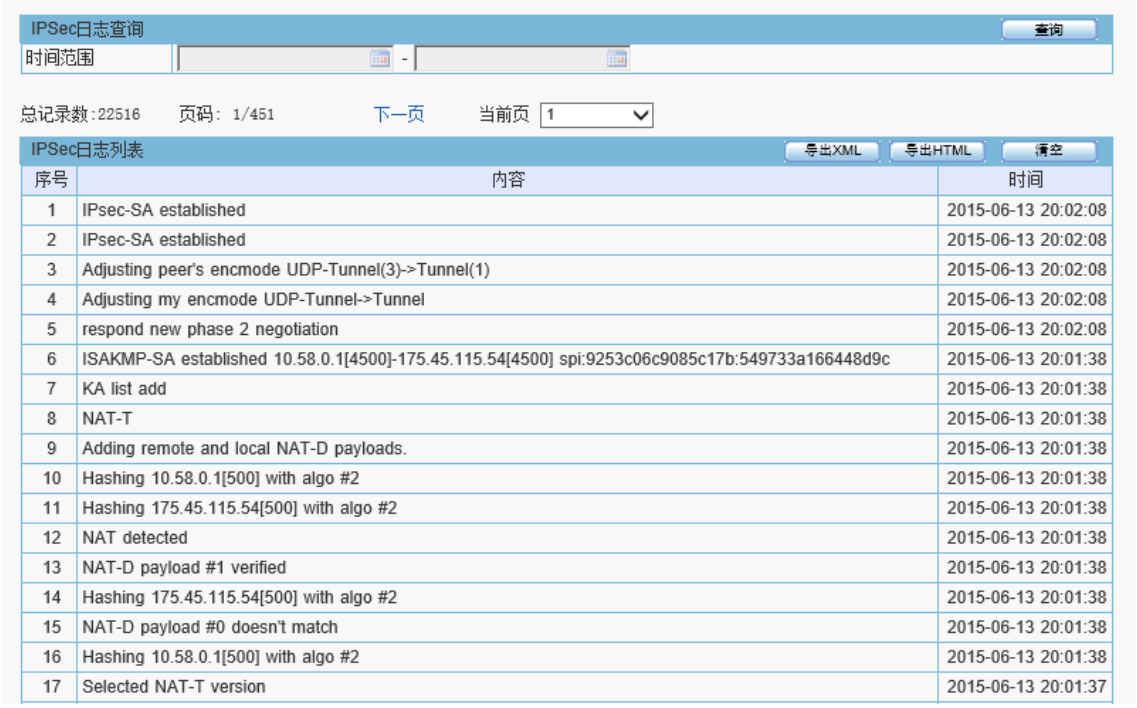
## 12.4 IPSec 日志

**功能描述：**记录 IPSec VPN 连接的日志。

**配置路径：**【系统日志】>【IPSec 日志】

配置描述：

第一：进入【IPSec 日志】页面，如下图




| 序号 | 内容 | 时间 |
|---|---|---|
| 1 | IPsec-SA established | 2015-06-13 20:02:08 |
| 2 | IPsec-SA established | 2015-06-13 20:02:08 |
| 3 | Adjusting peer's encmode UDP-Tunnel(3)->Tunnel(1) | 2015-06-13 20:02:08 |
| 4 | Adjusting my encmode UDP-Tunnel->Tunnel | 2015-06-13 20:02:08 |
| 5 | respond new phase 2 negotiation | 2015-06-13 20:02:08 |
| 6 | ISAKMP-SA established 10.58.0.1[4500]-175.45.115.54[4500] spi:9253c06c9085c17b:549733a166448d9c | 2015-06-13 20:01:38 |
| 7 | KA list add | 2015-06-13 20:01:38 |
| 8 | NAT-T | 2015-06-13 20:01:38 |
| 9 | Adding remote and local NAT-D payloads. | 2015-06-13 20:01:38 |
| 10 | Hashing 10.58.0.1[500] with algo #2 | 2015-06-13 20:01:38 |
| 11 | Hashing 175.45.115.54[500] with algo #2 | 2015-06-13 20:01:38 |
| 12 | NAT detected | 2015-06-13 20:01:38 |
| 13 | NAT-D payload #1 verified | 2015-06-13 20:01:38 |
| 14 | Hashing 175.45.115.54[500] with algo #2 | 2015-06-13 20:01:38 |
| 15 | NAT-D payload #0 doesn't match | 2015-06-13 20:01:38 |
| 16 | Hashing 10.58.0.1[500] with algo #2 | 2015-06-13 20:01:38 |
| 17 | Selected NAT-T version | 2015-06-13 20:01:37 |

图 180：IPSec 日志

## 12.5 日志服务器

**功能描述：**配置 Syslog 服务器。

**配置路径：**【系统日志】>【日志服务器】

**配置描述：**进入【日志服务器】页面，如下图


图 181：日志服务器

**参数说明：**

- 日志服务器：启用或禁用 Syslog 服务器，启用后设备将会向 Syslog 服务器发送

日志消息；

- 服务器地址：Syslog 服务器的 IP 地址；
- 服务器端口：与 Syslog 服务器通信的端口号，默认是 514。

## 12.6 短信配置

**功能描述：**配置发送短信日志中使用到的短信接收手机号。

**配置路径：**【系统日志】>【短信配置】

**配置描述：**进入【短信配置】页面，如下图，点击启用，并输入手机号码。


图 182：短信手机号配置

## 12.7 告警配置

对设备告警、违规网站、违规搜索、违规上环、违规邮箱、违规 IM、潜在危害等信息进行告警。

### 12.7.1 设备告警

**功能描述：**配置事件告警、黑名单告警、设备状态告警，并设定告警级别以及处理策略。

**配置路径：**【系统日志】>【告警配置】

**配置描述：**进入【告警配置】页面，如下图，


图 183：告警配置

**参数说明：**

- 事件告警：勾选启用，设定告警级别，处理策略；
- 黑名单告警：勾选启用，设定告警级别，处理策略；
- 监控告警：设置 CPU、内存、活跃会话、WAN 口总流量超过法制进行告警。

# 第13部分 故障排除

## 13.1 捕获数据包

**功能描述：**配置捕获数据报文的规则，然后可以捕获数据报文，进行故障排除分析。

**配置路径：**【故障排除】>【捕获数据包】

**配置描述：**进入【捕获数据包】页面，如下图：


图 184：捕获数据包

**参数说明：**

- 捕获报文个数：捕获报文的总个数；
- 物理接口：捕获在此接口收到的报文，“全部”代表设备所有的物理接口；
- 简易配置：根据报文源 IP、目的 IP、源端口、目的端口和协议类型来捕获报文；
- 高级配置：根据过滤正则表达式来进行报文的捕获。如要抓取单个 IP 地址的所有 TCP 包，则输入：host 1.1.1.1 and tcp；

配置好捕获规则后，点击<开始捕获>按钮，开始报文的捕获。点击<停止捕获>，停止报文的捕获。然后到【故障排除】>【查看数据包】页面去查看捕获到的数据包文件。

## 13.2 查看数据包

**功能描述：**查看已捕获的数据报文。

**配置路径：**【故障排除】>【查看数据包】

**配置描述：**进入【查看数据包】页面，如下图：


图 185：查看数据包

点击<下载>按钮后，即下载已捕获的的文件，然后可通过 Sniffer 或 Ethereal 等软件进行报文分析。

# 第14部分 报表中心

设备提供了内置报表中心，无需另外安装外置报表中心即可实现对实时监控、统计分析、行为分析的记录与查询功能。在内置报表中心，默认已开启对流量的实时监控、统计分析，行为分析等所有的记录。行为分析部分也可根据需要选择记录部分内容，具体配置方法参照【内容记录配置】。

## 14.1 内容记录配置

**功能描述：**过滤报表中心行为分析的记录内容，如：对某些用户只记录 URL 记录和 FTP 记录等。

**配置路径：**【报表中心】>【报表中心配置】

**配置描述：**

**第一：**进入【报表中心配置】页面，如下图：


图 186：报表中心配置

**参数说明：**

- 启动外置报表：选择启用或禁用外置报表中心。
- 网点名称：输入其他行为管理设备的名称。
- 外置报表IP地址：输入外置报表IP地址。
- 同步数据内容：选择全部或除去URL记录、除去会话记录、除去会话记录和URL记录。
- 同步报表方式：选择实时上传或定时上传。

- 启用内置报表中心：选择是或否。

## 14.2 内置报表中心

**功能描述：**打来内置报表中心，查看所有的历史流量、历史上网日志记录。

**配置路径：**【报表中心】>【内置报表中心】

**配置描述：**

**第一：**进入【内置报表中心】页面，如下图：

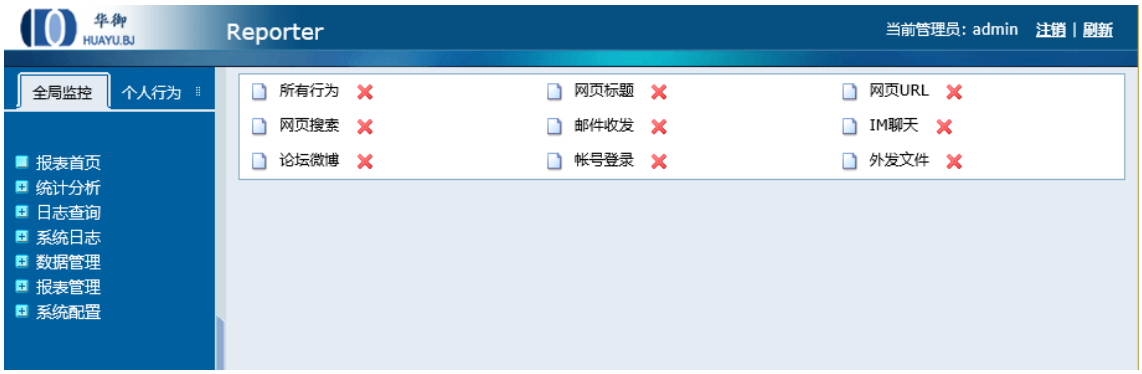



图 187：内置报表中心

第二：点击日志查询，查看所有上网行为，会话记录，告警记录，高级检索。


图 188：上网日志查询