视频安全接入系统
（单向导入前置/单向导入后置）
用户手册

珠海经济特区伟思有限公司

1.00 版

2021 年 4 月发行

信息反馈

珠海伟思欢迎您通过尽可能多的渠道向我们提供尽可能多的信息，您的意见和问题都会得到我们的重视和妥善处理。请将反馈信息投递到下述地址：

地址：珠海市唐家湾软件园路 1 号南方软件园 B3 一层

邮编：519080

电话：0756—3391616（总机）

传真：0756—3391618

注意！倘若本产品上之产品序号有所破损或无法辨识者，则该项产品恕不保修！

目 录

第一章 产品说明

1.1. 产品介绍

视频安全接入系统(单向导入前置/单向导入后置)是为企业级中心节点设计的多功能安全隔离系统，考虑到企业级节点在用户数量、应用类型、安全性以及管理的特殊需求，视频安全接入系统主要特点包括：

- 作为企业级节点，安全隔离系统必须具备更高的数据交换能力，视频安全接入系统为企业级用户提供业内领先的数据交换处理性能，在 FTP、HTTP 文件上传/下载等应用中采用数据交换分发技术、断点续传技术，大幅提高文件传输效率，达到业内最高的交换性能。
- 据统计，企业级节点是各类网络攻击的主要目标，伟思视频安全接入系统具备高安全性和抗攻击性特性，采用内置 IDS 入侵检测与联动系统，实现对攻击的自动防御。
- 具备流量控制功能，满足企业级节点对内网客户端的流量管理需求。
- 视频安全接入系统具备第三方日志输出与集中管理功能，能够实现与企业级网管中心的集成，方便管理员进行高效的网络管理。

1.2. 设备组成

视频安全接入系统的 LED、网络接口和串口位于机箱前部的面板，AC 电源插头和开关位于机箱后部的面板右侧。

表 1　网口

网口	说明
可信端	可信端接口用于连接内部可信网络的设备，如内网交换机。
不可信端	不可信端接口用于连接外部不可信网络的设备，如外网交换机、路由器和防火墙等。
管理口	管理口用于对本设备做管理配置用

CONSOLE	串口可接终端机作为高级设置之用。

表格 2　显示灯状态

LED	状态
POWER	绿灯亮，表示电源正常。
HDD1	当开机启动时红灯闪烁，表示可信端系统启动正常。
HDD2	当开机启动时红灯闪烁，表示不可信端系统启动正常。
可信端	绿色 LED(连续)：连接到内网的设备状态良好。 红色 LED(闪烁)：这个端口正在发送或接收数据。
不可信端	绿色 LED(连续)：连接到外网的设备状态良好。 红色 LED(闪烁)：这个端口正在发送或接收数据。

1.3. 运行环境

为保证系统能长期稳定的运行，视频安全接入系统应安装在标准的 19 英寸的机柜里，保证电源有良好的接地措施、防尘措施、保持运行环境的空气通畅和室温稳定。

视频安全接入系统运行环境应满足以下标准：

输入	200V 4A 50Hz
温度	-10℃～50 ℃
湿度	5%～90%
电源	220V 交流电

1.4. 安装步骤

1. 连接电源线到视频安全接入系统后面的电源插口，然后插入另一端的电源插头到 220V 电插座。

2. 开启视频安全接入系统后面的电源开关和前面设备开关。

3. 连接网线的一端到视频安全接入系统的可信端口，连接另一端到内网交换机的网

口。

4. 连接网线的一端到视频安全接入系统的不可信端口，连接另一端到外网设备的网口，例如外网交换机、路由器、防火墙等。

5. 用管理主机连接管理口登录视频安全接入系统并进行适当的配置。

6. 测试网络的连通性和访问服务是否正常。

第二章 产品配置

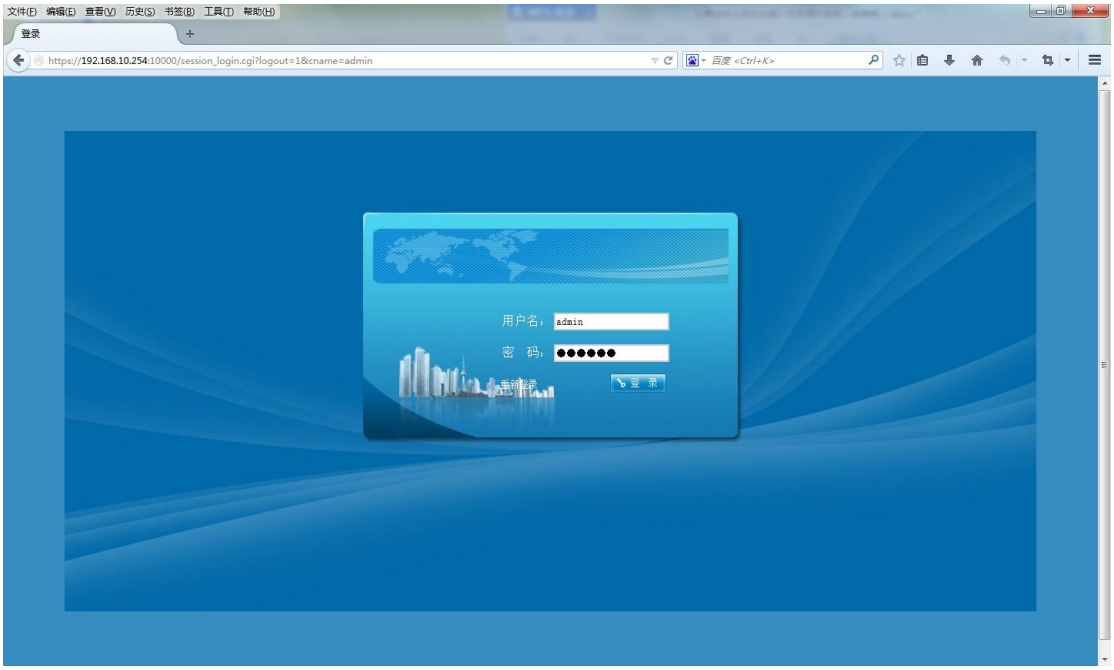
2.1. 摘要

视频安全接入系统有一个基于 Web 设计的配置界面能使视频安全接入系统更加容易配置。这一章会解释配置界面所有的功能。建议采用火狐浏览器。采用 SSL 连接，10000 端口。您能通过访问管理口地址 https://192.168.10.254:10000 打开配置界面。

配置界面上主要有十一个主目录：系统信息、网络配置、对象管理、策略模版、用户管理、行为审计、防火墙、VPN 管理、系统管理、设备日志、中心端管理。子目录会出现当您点击其中一个主目录。

2.2. 如何访问配置界面

为了要访问视频安全接入系统配置界面，先启动火狐浏览器，并且输入视频安全接入系统的管理口默认 IP 地址（https://192.168.10.254:10000）到地址栏，然后按下 Enter 键。一个登录界面会出现要求输入用户名和密码。输入“admin”到用户名输入栏里，并且输入“admin*2017”到密码输入栏里，然后点击“确定”按钮。



2.3. 系统信息

2.3.1 系统信息

第一个出现的页面是系统信息。这个页面显示视频安全接入系统目前的状态和设置。

系统信息：

主机名：设备名称

系统时间：系统显示的时间

设备名称：留空

固件版本：当前系统的版本号

应用识别库版本：视频协议库的版本

开机时间：系统从开机到当前的总时间

双机模式：显示双机热备的状态

接口信息：

显示管理口、可信端、不可信端的部署名、IP 地址和网口状态

资源信息：

CPU 负载：CPU 的占用率

内存占用：显示内存的占用率

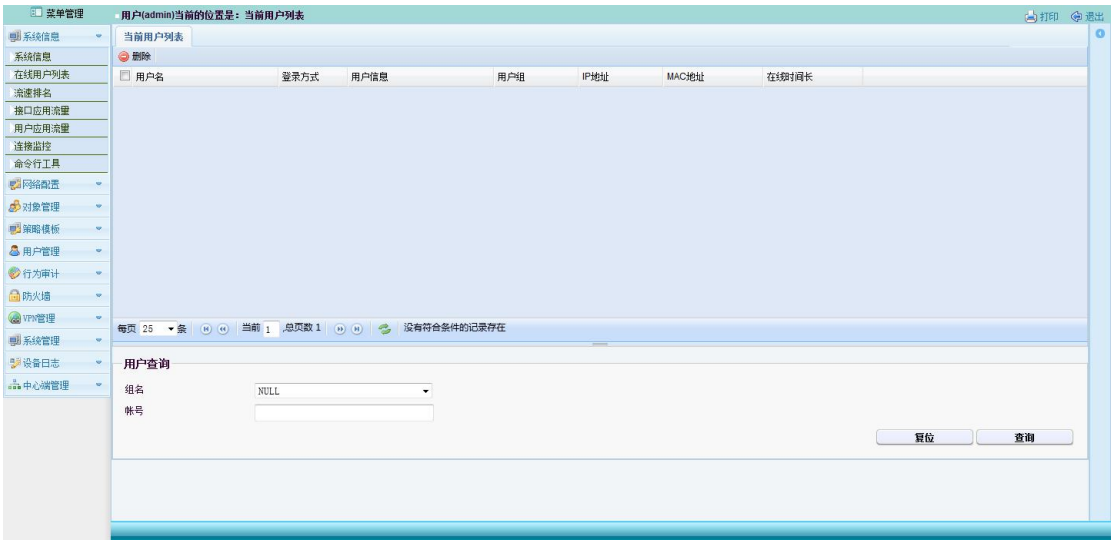
磁盘占用：显示磁盘的占用率

会话数：系统会话总数

在线用户数：显示目前在线的用户数量

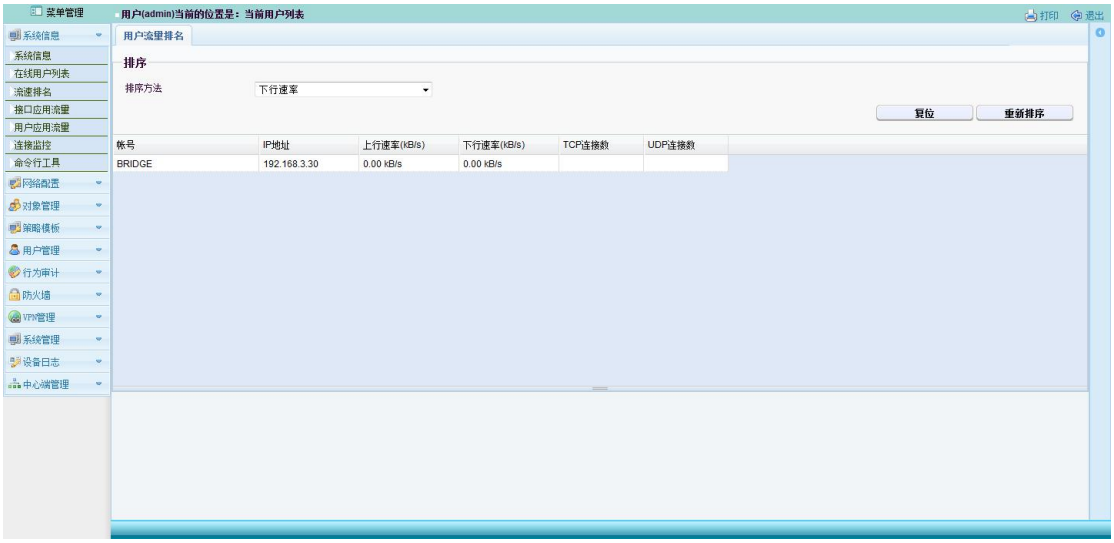
2.3.2 在线用户列表

显示当前认证用户中的在线用户信息列表。



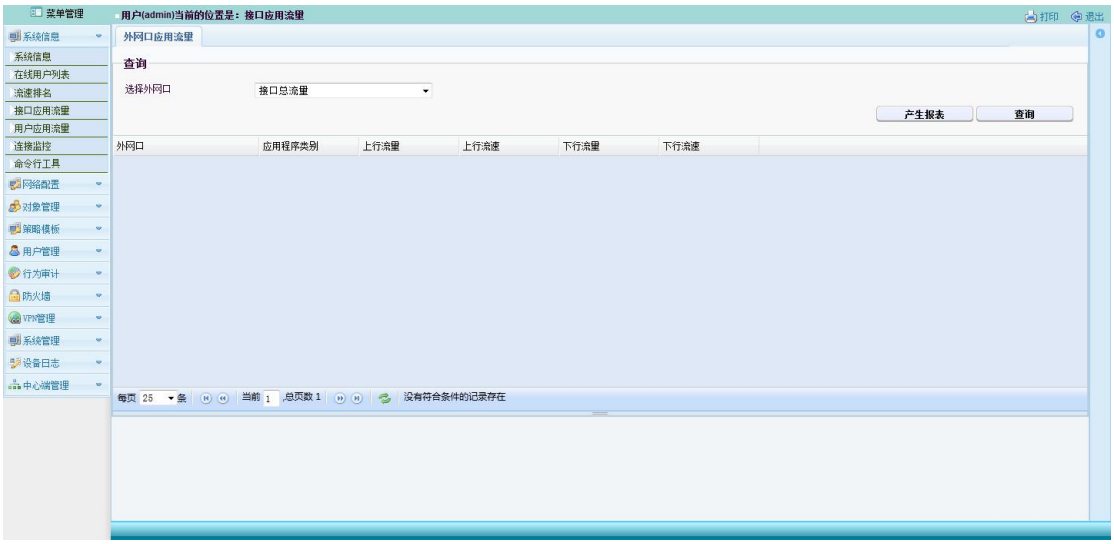
2.3.3 用户流量排名

显示当前认证用户的用户信息列表。



2.3.4 接口应用流量

查询 WAN 口各种应用的流量信息，包括总的上下行流量，当前上下行流速。

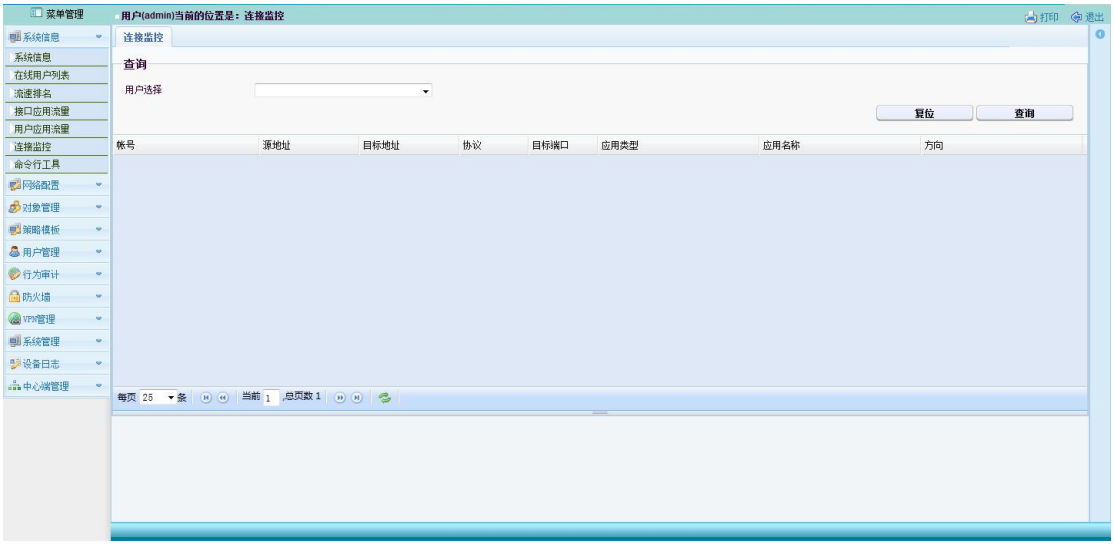


2.3.5 用户应用流量

显示在线用户的各种类别的应用程序的使用情况。

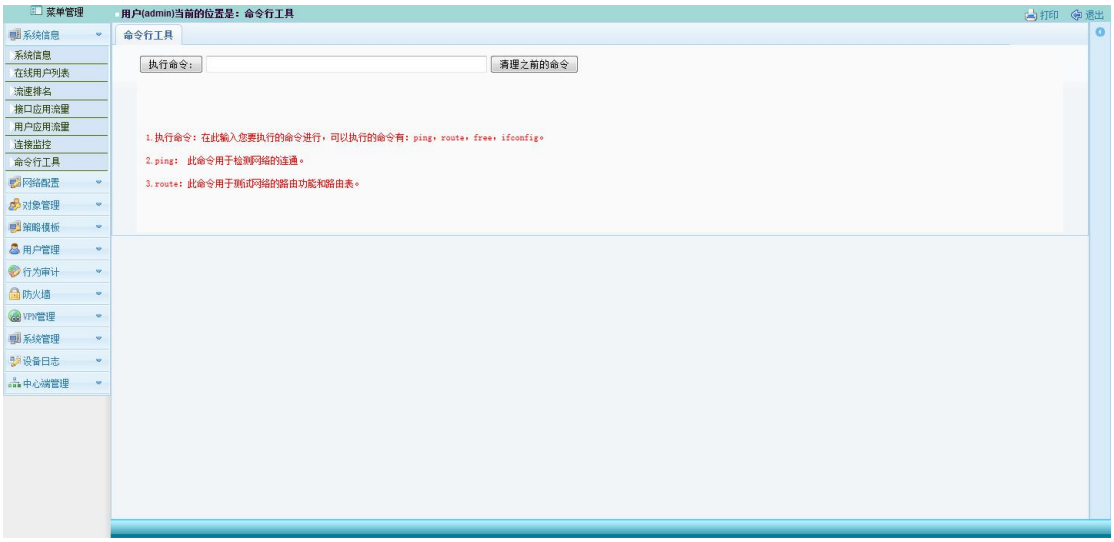
2.3.6 连接监控

查询当前的认证用户的连接信息。



2.3.7 命令行工具

在设备里使用命令行工具用来诊断各种网络问题。

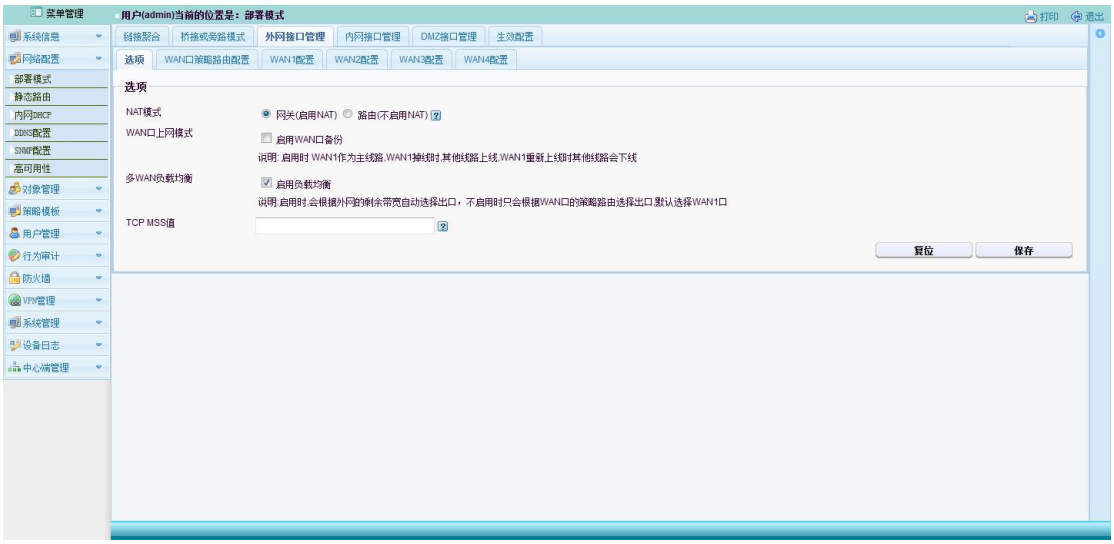


在执行命令右边的框中输入可执行的 Linux 命令 ping、route、free 或 ifconfig

2.4. 网络配置

2.4.1 部署模式

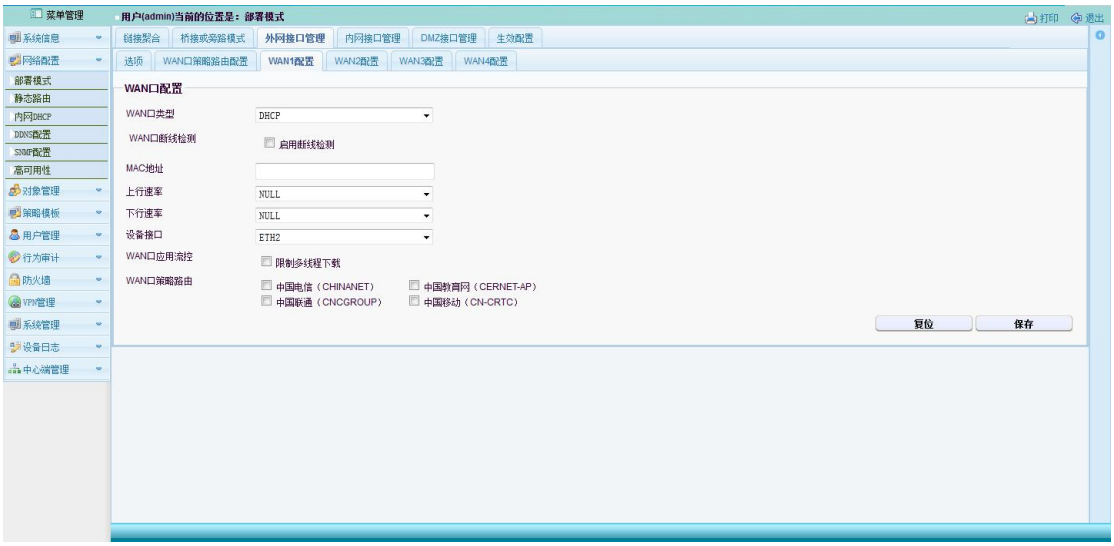
外网接口管理：



WAN 口类型：在下拉菜单中可以选择“关闭”、“DHTC”和“静态路由”。

WAN 口类型（DHTC）：

WAN 口断线检测：



设置完成后点击“保存”按钮保存配置，或者点击“复位”按钮恢复默认值。

WAN 口类型（静态路由）：

在这里可以自定义 IP 地址、网关 IP、和 DNS。填写 IP 时一行一个 IP，且 IP 和子网掩码用“/”分隔。例如：192.168.0.254/255.255.255.0。

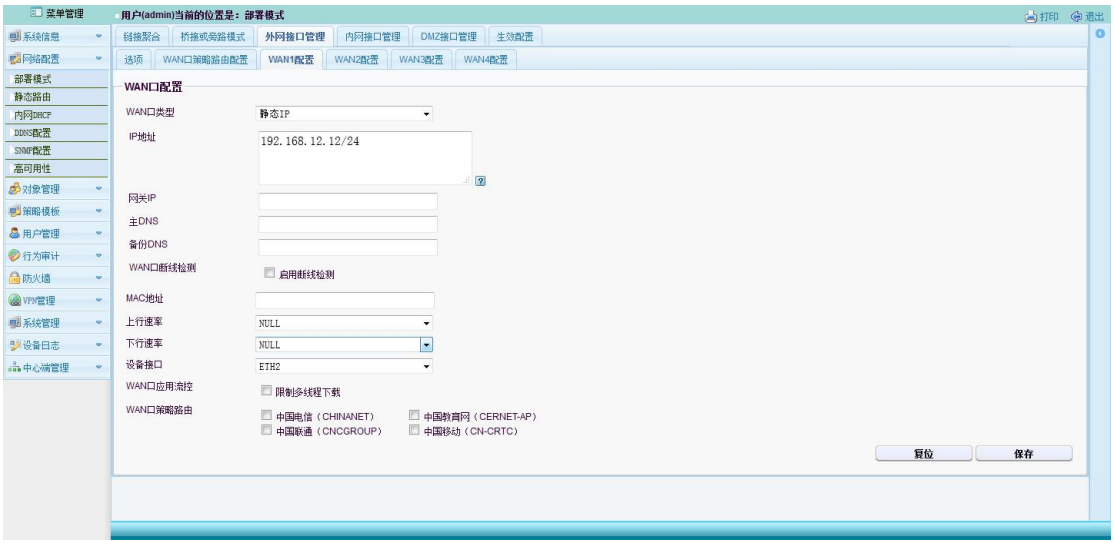
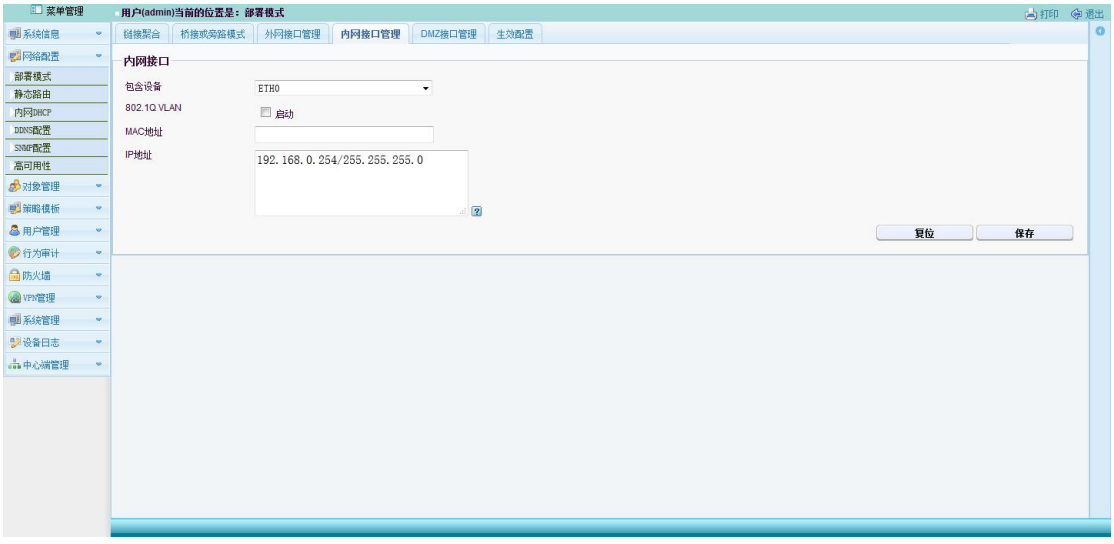


图 4.1.3

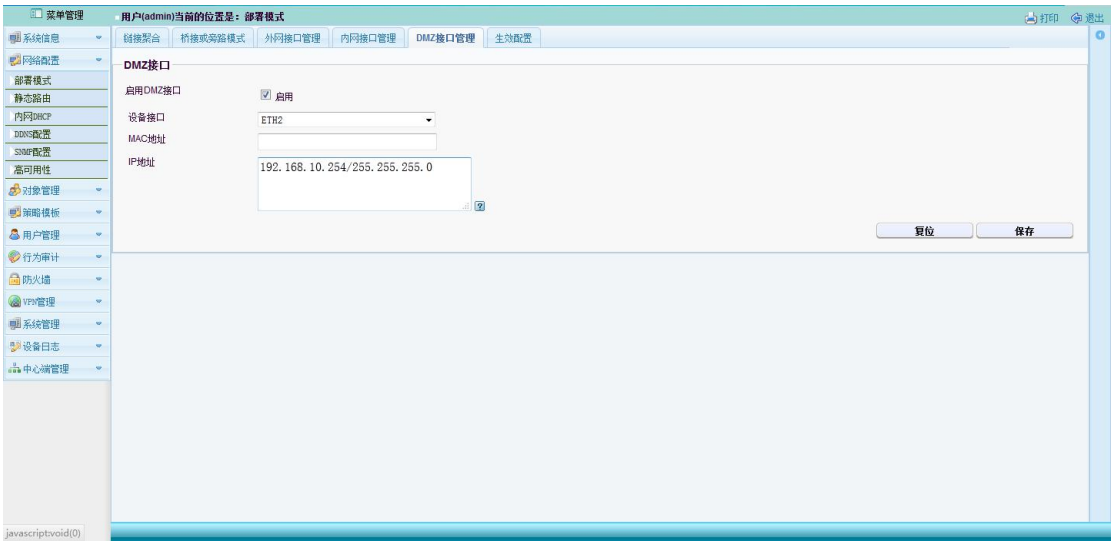
- MAC 地址：在这里可以设置本设备的 MAC 地址。
- 上行速率：在下拉菜单中可以选择“512K”—“100M”的限制速率。
- 下行速率：在下拉菜单中可以选择“512K”—“100M”的限制速率。
- 设备接口：在下拉菜单中可以选择把该接口设置为“管理口”。
- WAN 口策略路由：这里可多选中国电信、中国教育网、中国联通和中国移动，选择时在待选的选项前面的方框中点击即打勾。选择符合的策略路由可以加快访问速度。
- 设置完成后点击“保存”按钮保存配置，或者点击“复位”按钮恢复默认值。

内网接口管理：



- 包含设备：在下拉菜单中可以选择设置该接口为“不可信端接口”和“管理口”
- MAC 地址：自定义该接口网卡的 MAC 地址。
- IP 地址：自定义该接口的 IP 地址。填写 IP 时一行一个 IP，且 IP 和子网掩码用“/”分隔。例如：192.168.0.254/255.255.255.0。设置完成后点击“保存”按钮保存配置，或者点击“复位”按钮恢复默认值。

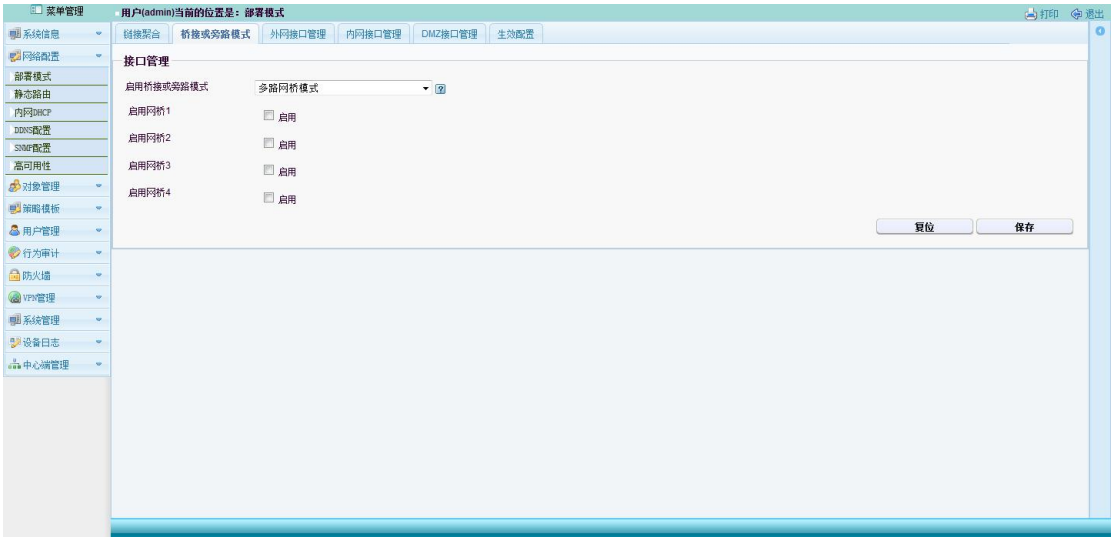
管理口：



- 启用管理接口：点击勾选“启用”，启用该管理口。
- 设备接口：默认选择管理口。在下拉菜单中可以选择设置为“不可信端”接口。
- MAC 地址：自定义该接口网卡的 MAC 地址。
- IP 地址：自定义该接口的 IP 地址。填写 IP 时一行一个 IP，且 IP 和子网掩码用“/”分隔。例如：192.168.0.254/255.255.255.0。设置完成后点击“保存”按钮保存配置，或者点击“复位”按钮恢复默认值。

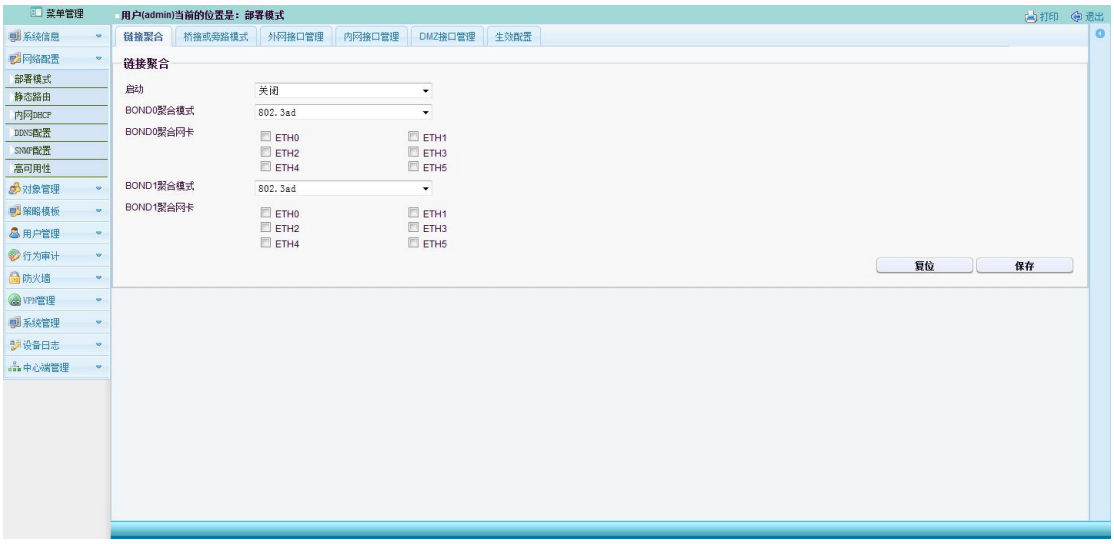
部署模式：

此页面可以选择启用或者关闭视频网闸模式、网闸模式、认证模式、快速转发模式、开发模式、SNMP 认证。



设置完成后点击“保存”按钮保存配置，或者点击“复位”按钮恢复默认值。

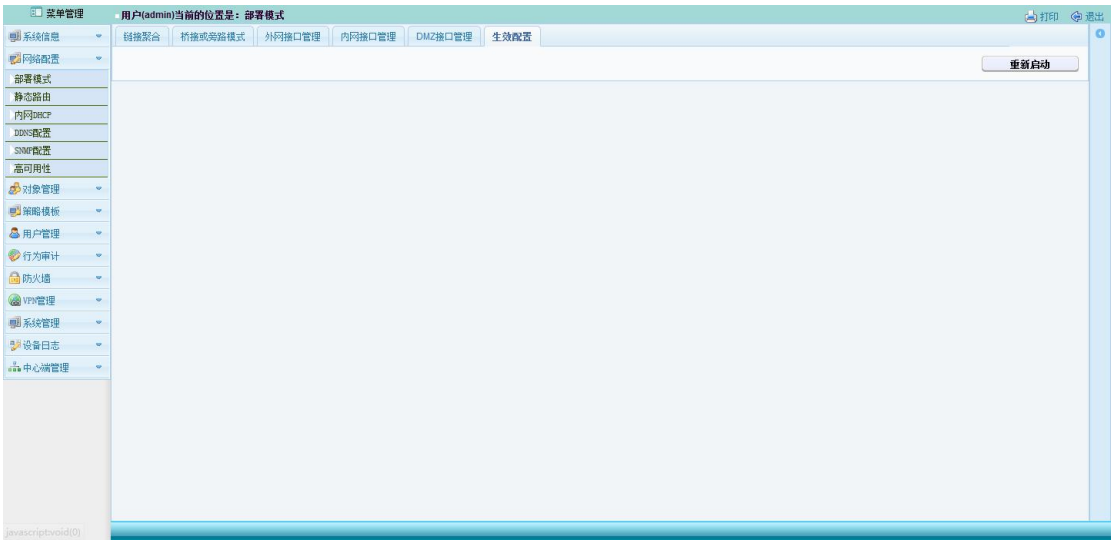
链接聚合：



- 启动：在下拉菜单中可以选择“启动”或者“关闭”链路聚合
- 聚合模式：在下拉菜单中有 802.3ad、active-backup、balance-rr、balance-tlb、balance-xor、broadcast 6 种模式可供选择。
- 聚合网卡：在这可勾选需要进行聚合的端口。
- 设置完成后点击“保存”按钮保存配置，或者点击“复位”按钮恢复默认值。

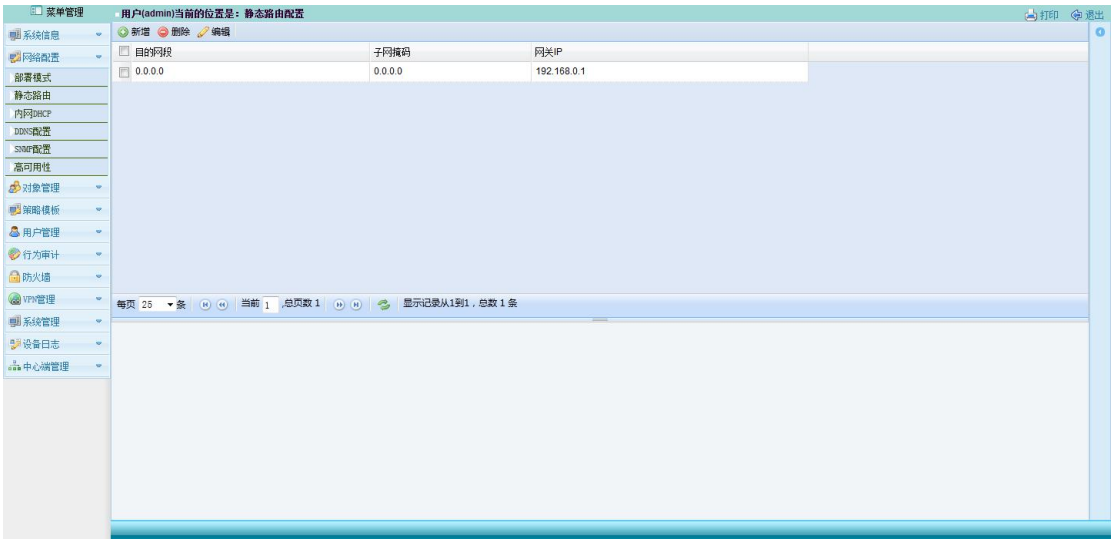
生效配置：

在该页面具有“重新启动”按钮，可以重新启动设备。



2.4.2 静态路由

本项菜单是设置本设备到其他网段的路由表。根据网络情况，指定好目标地址和掩码及网关，保存即可生效。



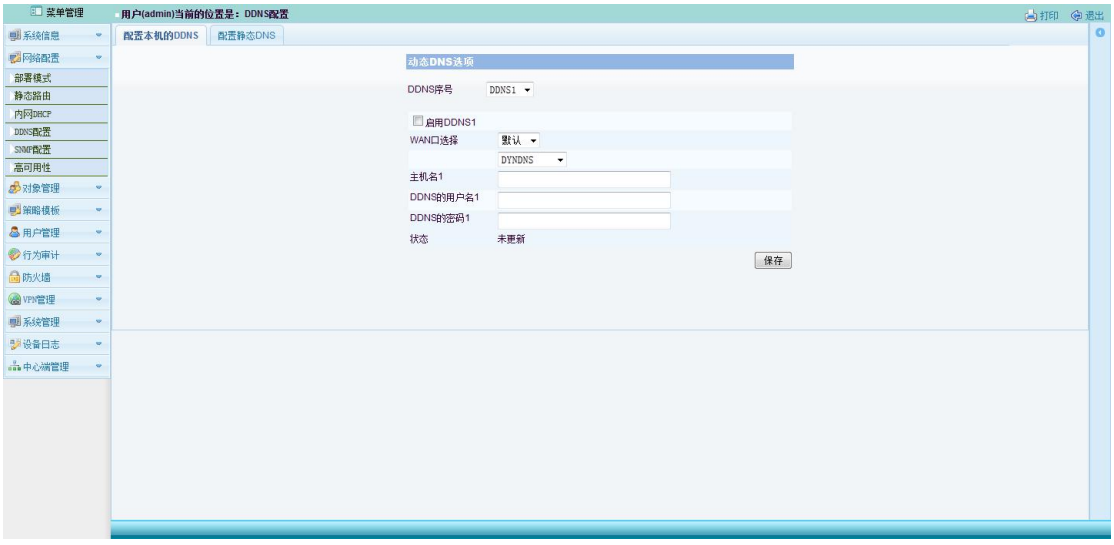
2.4.3 内网 DHCP

内部网络自动分配 IP 地址让用户和内部网络管理员作为对所有计算机做中央管理的手段。DHCP 设置范围不要与 PPTP 范围和固定 IP 冲突或重复。

2.4.4 DDNS 配置

本项菜单是设置绑定本设备的动态或静态 DNS。

配置本机的 DDNS：同时支持 4 种 DDNS 同时捆绑，设备出厂即已绑好 2 种，DDNS1 默认为本公司提供的 .COM 后缀的域名，规则为：序列号..COM (注：序列号为 2 位英文+7 位数字的组合，帖在设备电源接口或网口附近)；如设备恢复出厂值，则本项要重新配置，启用 DDNS1 并输入序列号保存即可，其他选项默认。



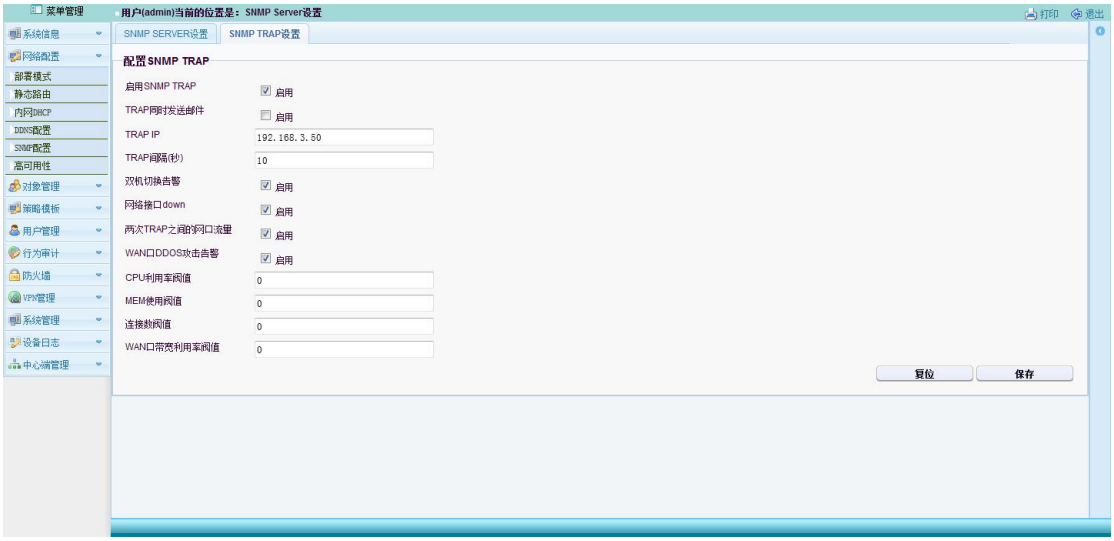
配置静态 DNS：根据需要指定 IP 和域名之间对应的关系，前提是 IP 是静态或不经常变动的，指定后内网通过本设备做 DNS，就可解析相应的域名。

2.4.5 SNMP 配置

SNMP 是一个从网络上的设备收集管理信息的公用通信协议。设备的管理者收集这些信息并记录在管理信息库（MIB ）中。这些信息报告设备的特性、数据吞吐量、通信超载和错误等。用户可以用 SNMP 服务来简化网络的管理和维护。本设备有自定义 oid=.1.3.6.1.4.1.12345678.5 可以获得自定义的设备信息。

SNMP SERVER 设置：

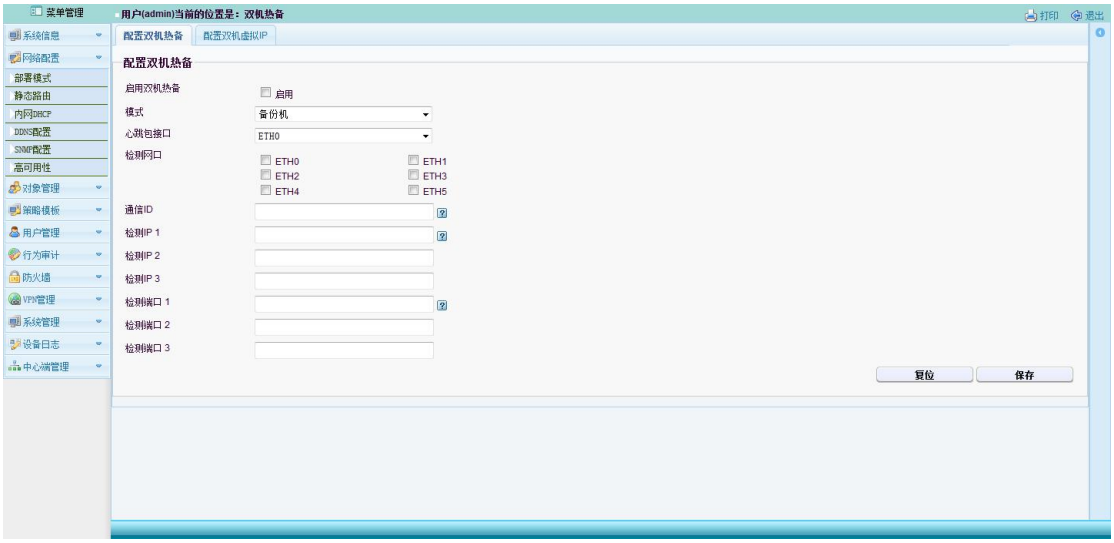
SNMP TRAP 设置：



2.4.6 高可用性

启用双机热备需要先配置虚拟 IP。主机和备份机的虚拟必须一样。在用户看来，虚拟 IP 就是双机热备系统的 IP 地址。开始时是主机的虚拟 IP 生效，系统通过心跳口检测两台设备的状态，如果主机宕机，则虚拟 IP 会自动转移到从机。主机恢复正常会自动转回主机，转移时间在两秒左右，不会影响系统的使用。有些双机系统会需要一些虚拟 IP 上的静态路由，可以在虚拟 IP 中加上路由 IP。

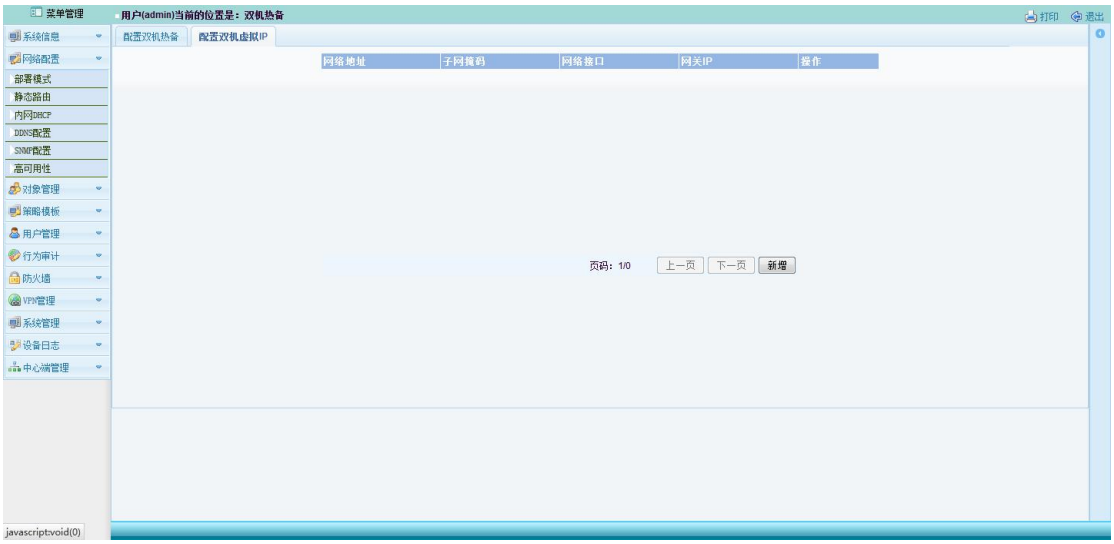
配置双机热备：



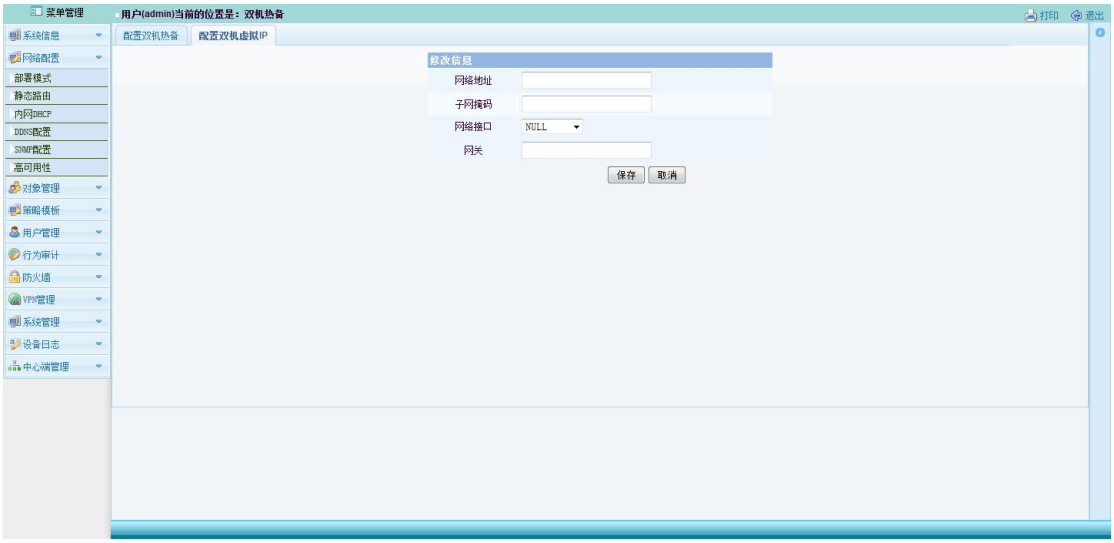
配置双机虚拟 IP：

在此页面添加虚拟 IP，启用双机热备后，虚拟地址池中的地址会生效，并绑定在主机

上，但主机出现故障，或网络出现问题时，虚拟地址会转移到从机上。



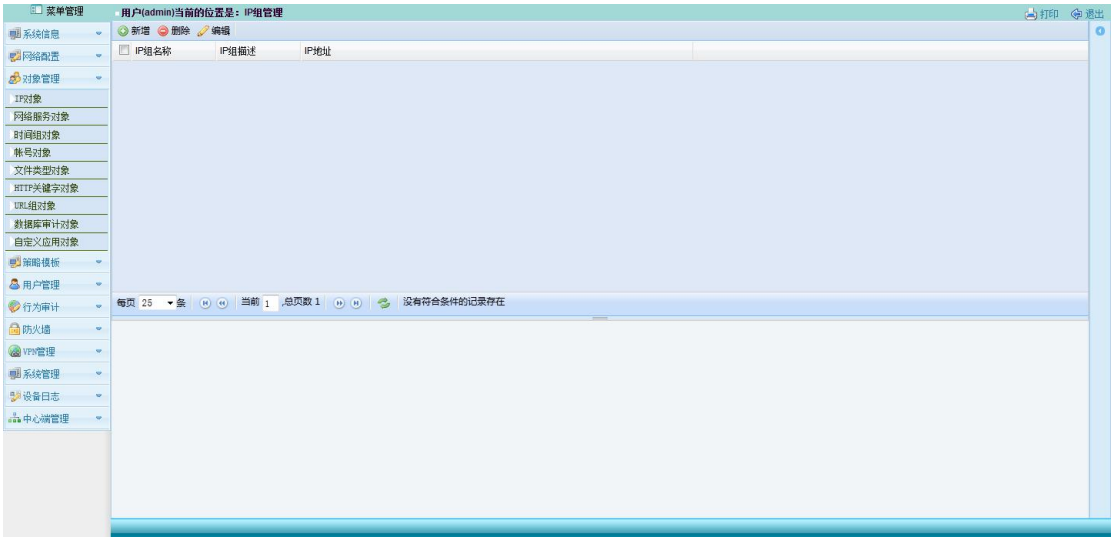
点击“新增”之后跳到此页面。



2.5. 对象管理

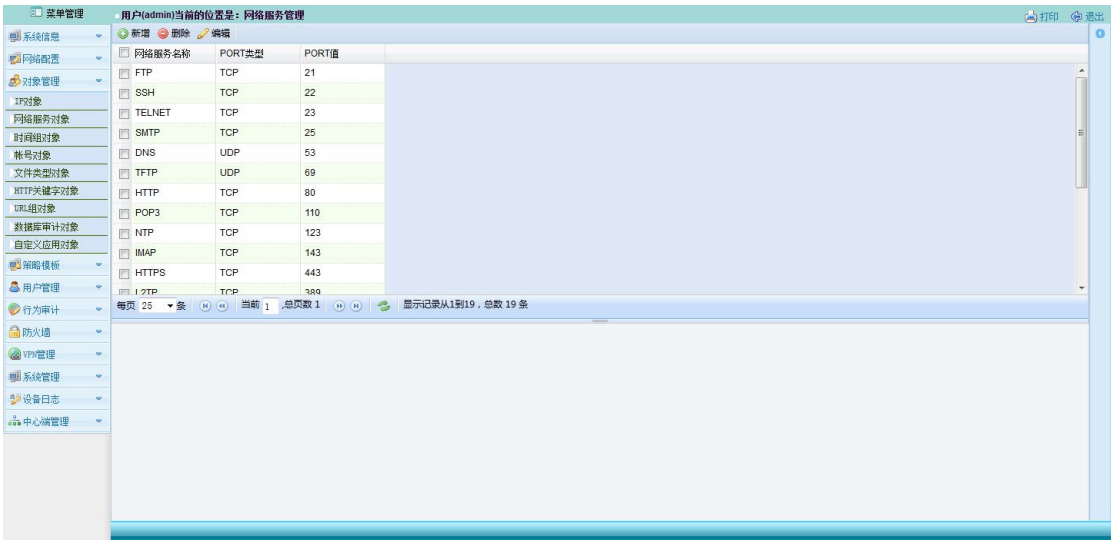
2.5.1 IP 对象

IP 对象应用在【过滤策略】->【IP/PORT 过滤】，【防火墙】->【NAT 配置】,【防火墙】->【数据包控制】中。



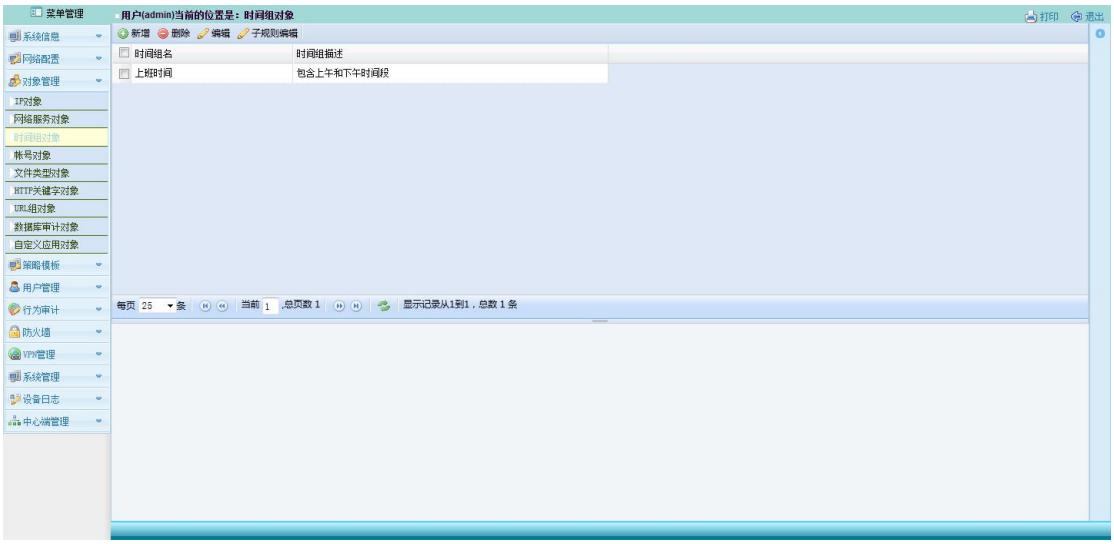
2.5.2 网络服务对象

网络服务对象对象应用在【过滤策略】->【IP/PORT 过滤】,【防火墙】->【数据包控制】中。



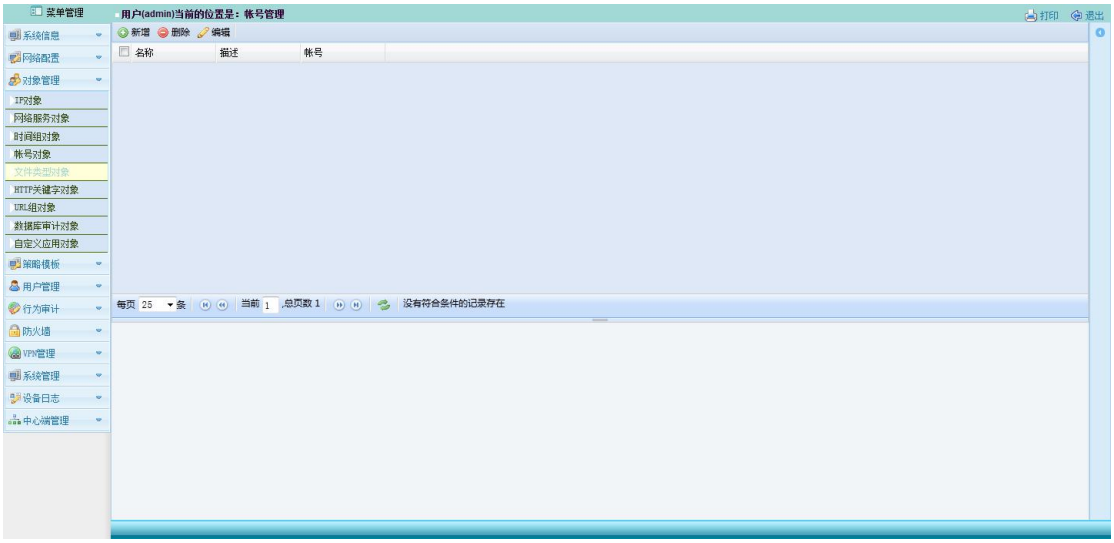
2.5.3 时间组对象

时间对象应用在所有的策略模板中，表示策略在相应的时间段内生效。和用户管理中表示在相应的时间段内允许登录。



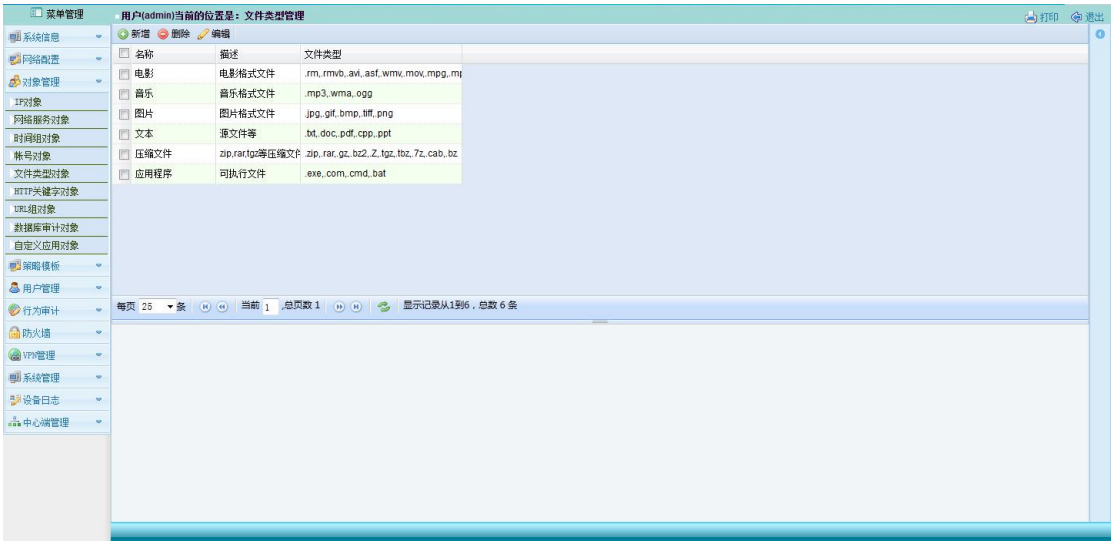
2.5.4 账号对象

账号对象应用在【过滤策略】->【账号过滤】中。



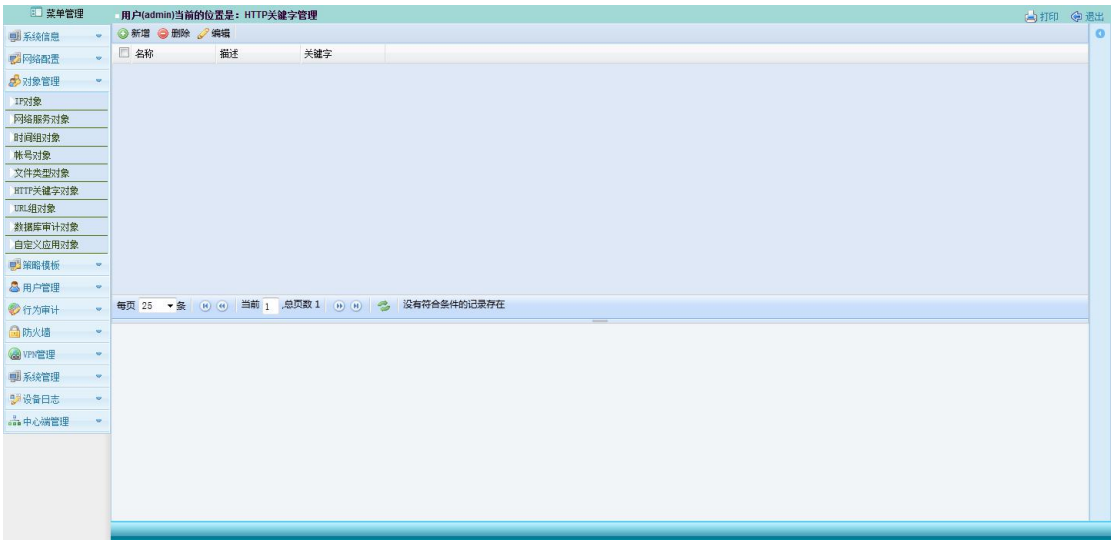
2.5.5 文件类型对象

文件类型对象应用在【过滤策略】->【文件过滤】中，识别方法方式主要主要通过文件名后缀。



2.5.6 HTTP 关键字对象

关键字对象应用在【过滤策略】->【HTTP 关键字过滤】中，主要识别内容是 http 发帖，邮件等，同时支持 UTF8，BIG5 和 GBK。

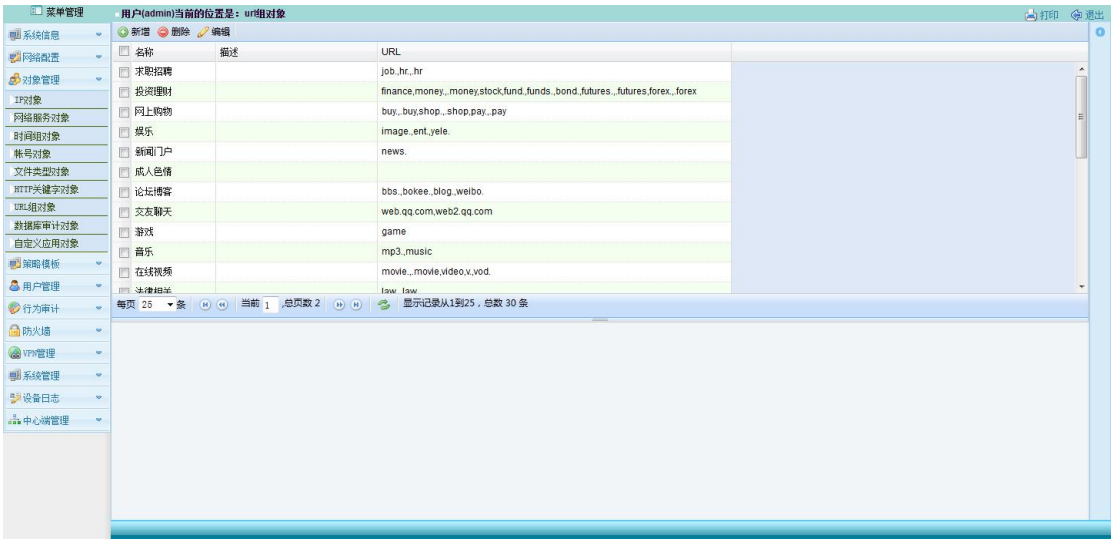


2.5.7 URL 组对象

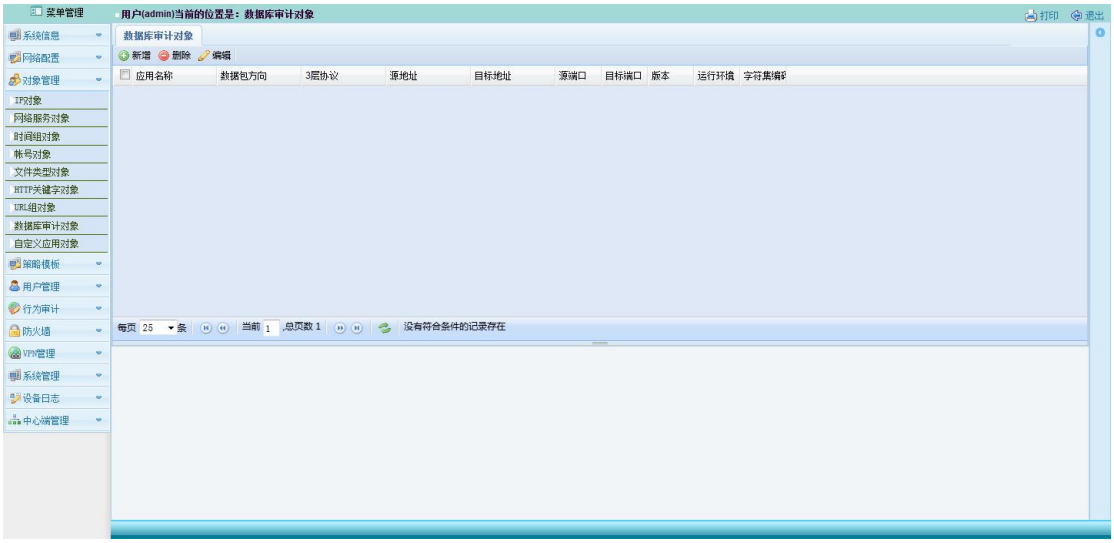
URL 对象应用在【过滤策略】->【URL 过滤】中系统内置了 33 种网站类别，包括大量的内置 URL，同时用户可以在已有类别上添加自己的 URL 信息，也可以创建新的类别。

URL 添加支持部分匹配。比如加入 .qq.com ，则 www.qq.com 或者 news.qq.com 都会

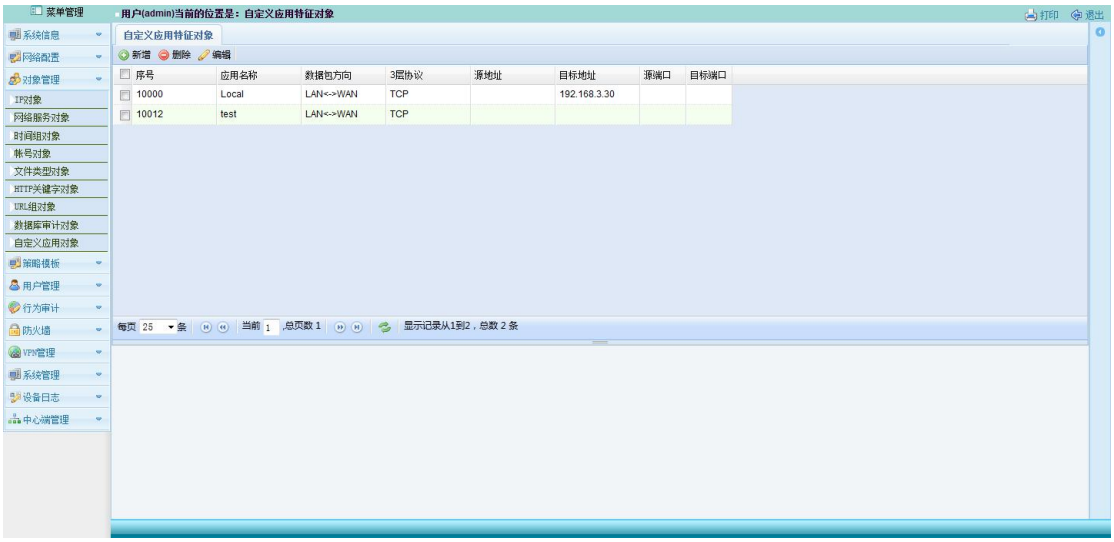
匹配。



2.5.8 数据库审计对象



2.5.9 自定义应用对象



2.6. 策略模版

策略模块是用户行为管理的核心模块。包括过滤策略，流控策略。审计策略，提醒策略。每个模板可以包括多个功能块，用户可以将大量的功能需求集中在一个模板中，用户管理时只需要选择相应的模板就可以完成权限的管理，比普通防火墙，流控等产品的 ACL 规则，清晰方便许多。

2.6.1 过滤策略

一个过滤策略模板可以 6 种过滤策略，分别是 IP 端口过滤，应用过滤，URL 过滤，HTTP 关键字过滤，文件过滤，账号过滤。每种过滤策略支持自己的 ACL 规则。系统内置了一些策略模板，用户可以仿照这些模板创建自己的模板，也可以在系统模板上进行修改。

使用方法：

点击新增按钮输入模板名和模板说明，点击保存。选择新建的模板，点击子规则编辑，打开过滤规则编辑页面。根据需要依次编辑相应的规则。每种类型的规则都支持优先级设置，生效时间段设置，运行或通过，日志和邮件告警等功能。

说明： 启用邮件告警时，要先配置邮件服务器账号，在【系统管理】->【高级配置】->【邮件告警配置】中设置。

下面说明相应的规则：

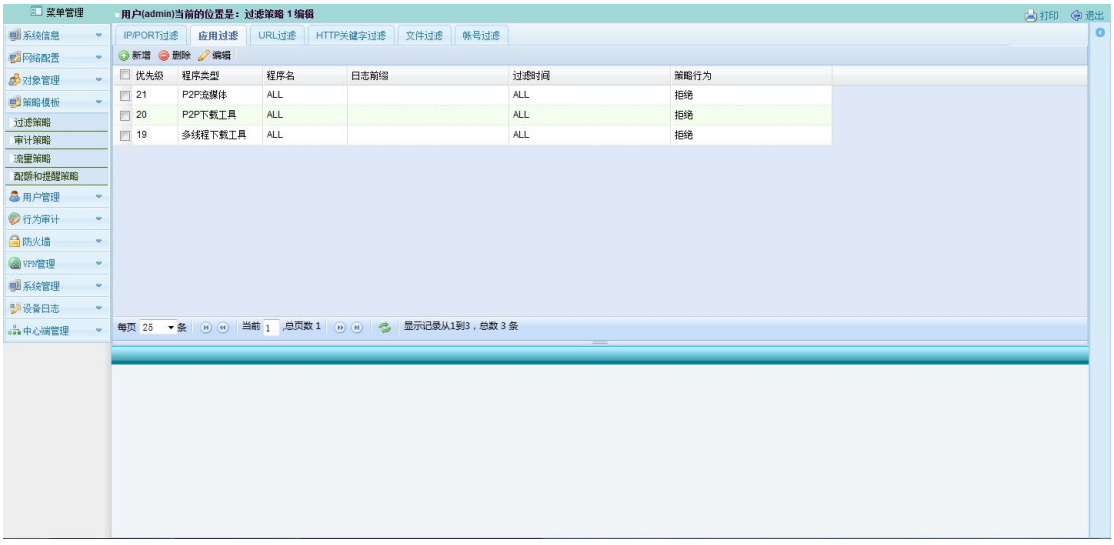
IP/PORT 过滤：

所有过滤规则里都有优先级项，优先级是一个数字，数字越大，优先级越高，规则列表里会根据优先级自动排序。

目标 IP，目标端口：可以选择在 IP，或服务对象里创建的对象，点击后面的图标可以直接编辑。

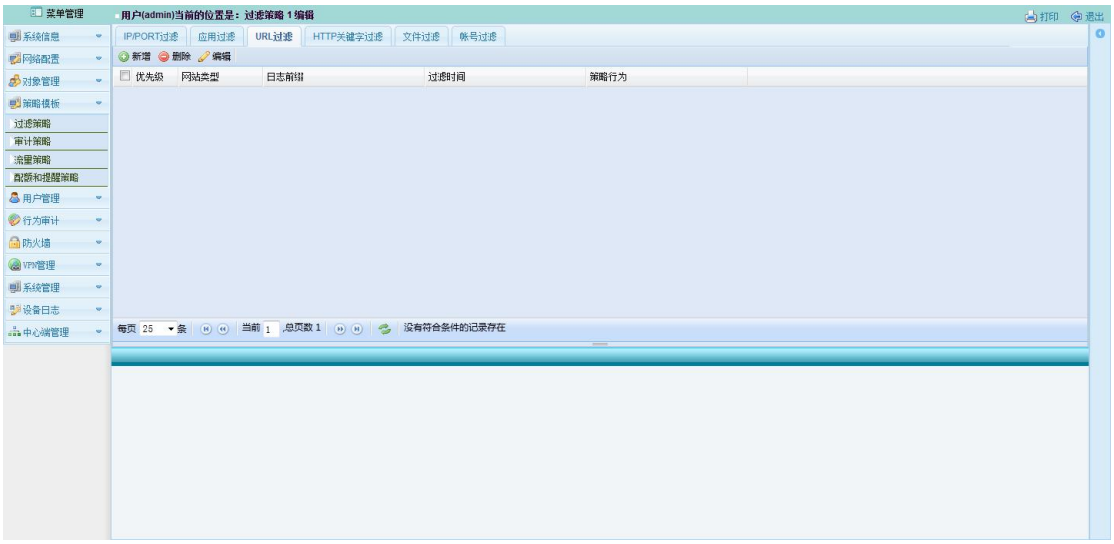
应用过滤：

系统内置了 700 多种应用识别特征，分为 20 多类应用。涵盖了大多数知名网络应用程序。可以对上网用户进行精细管理。



URL 组过滤：

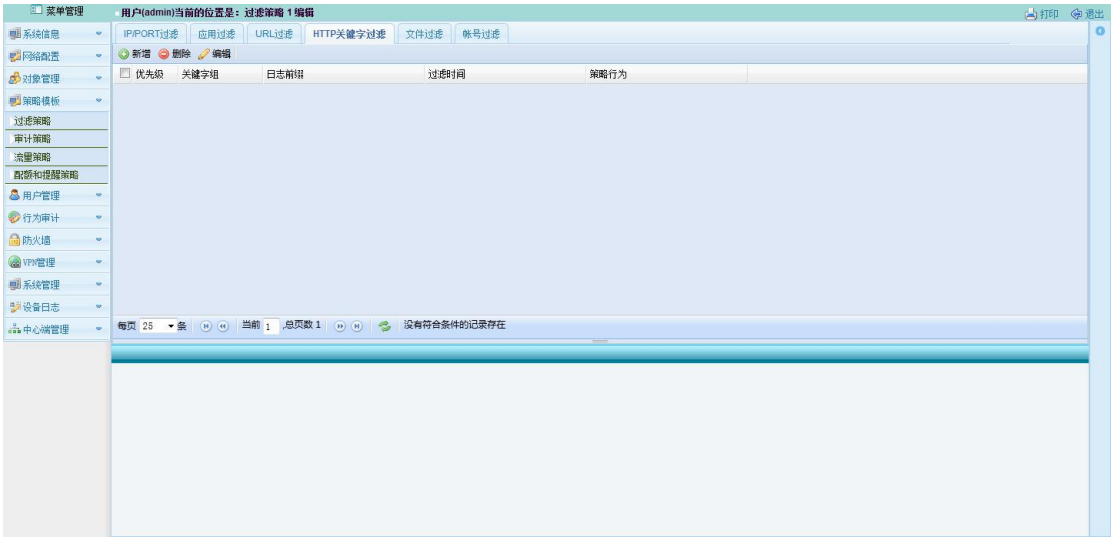
URL 组选择可以选择运行访问或拒绝访问的网站类型。



HTTP 关键字过滤：

过滤上行的 HTTP 关键字，例如发帖，web 邮件，网页搜索等，默认拒绝时是弹出拒绝页面。

在【系统管理】->【高级配置】中可以设置是弹出拒绝页面，还是直接拒绝。

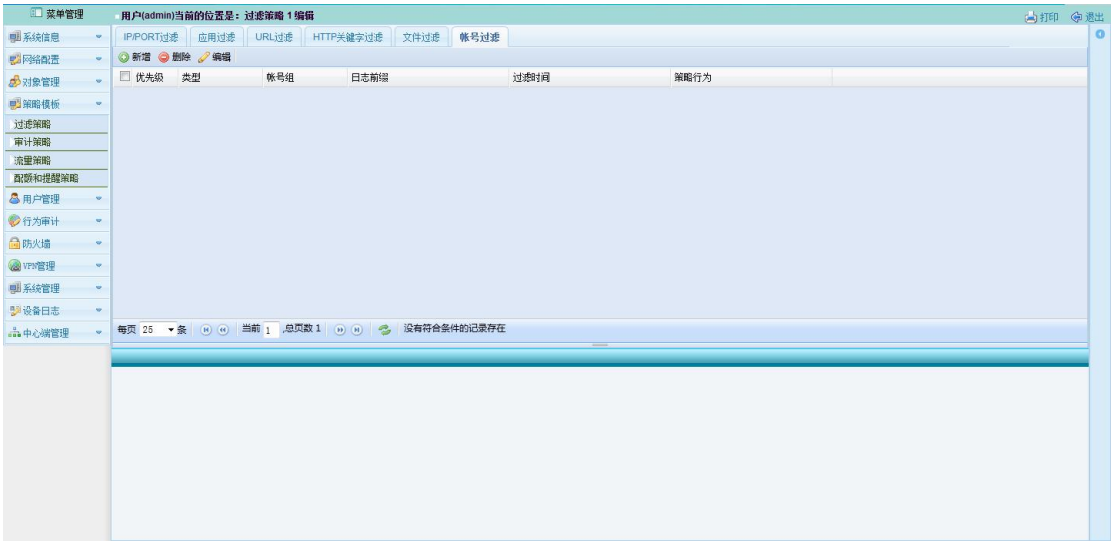


文件过滤：

文件过滤分为上行文件，和下行文件。包括浏览器上传下载的文件，比如 web 邮件的附件，ftp 的文件，SMTP 发送的附件，POP3 接受的附件等。

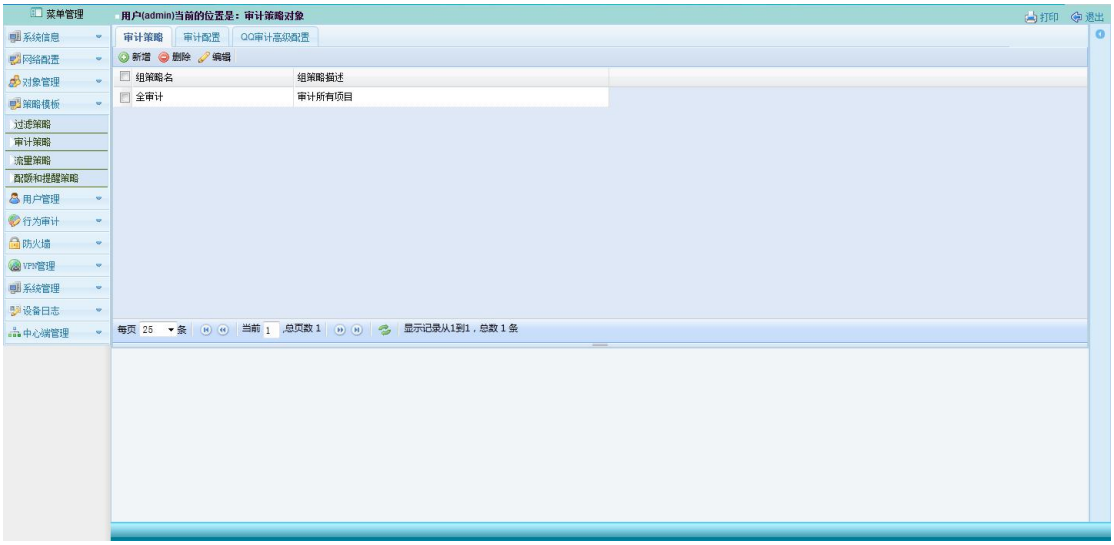
帐号过滤：

账号过滤当前版本主要支持聊天账号的过滤，比如只允许特点的 QQ 账号登陆。



2.6.2 审计策略

审计是内网管理的另一个重要功能。当前系统支持 12 种审计类别，审计到的数据会记录到设备的数据库中，在【行为审计】->【内容审计查询】中可以搜索审计到的用户数据。

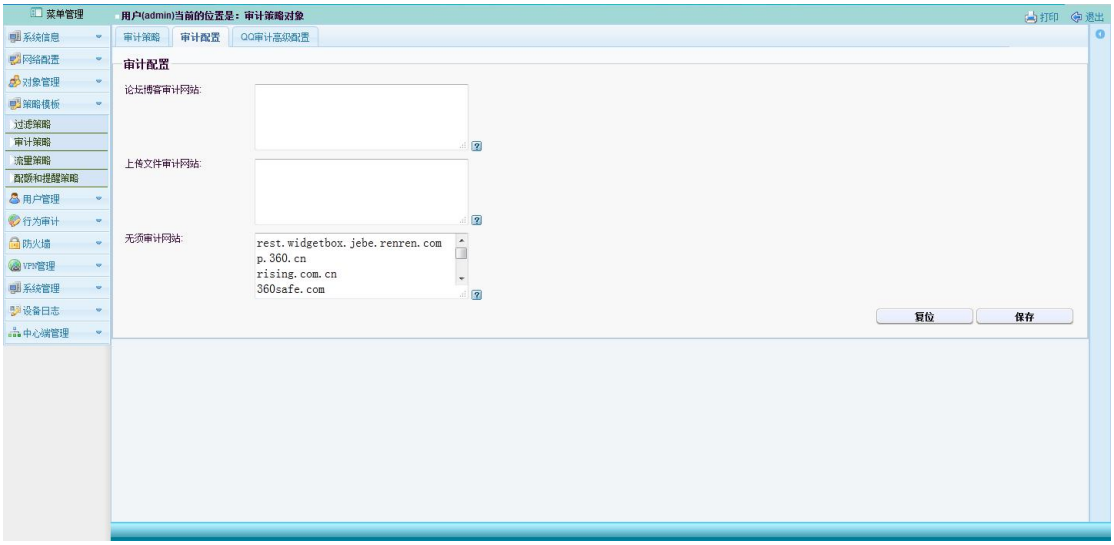


审计配置：

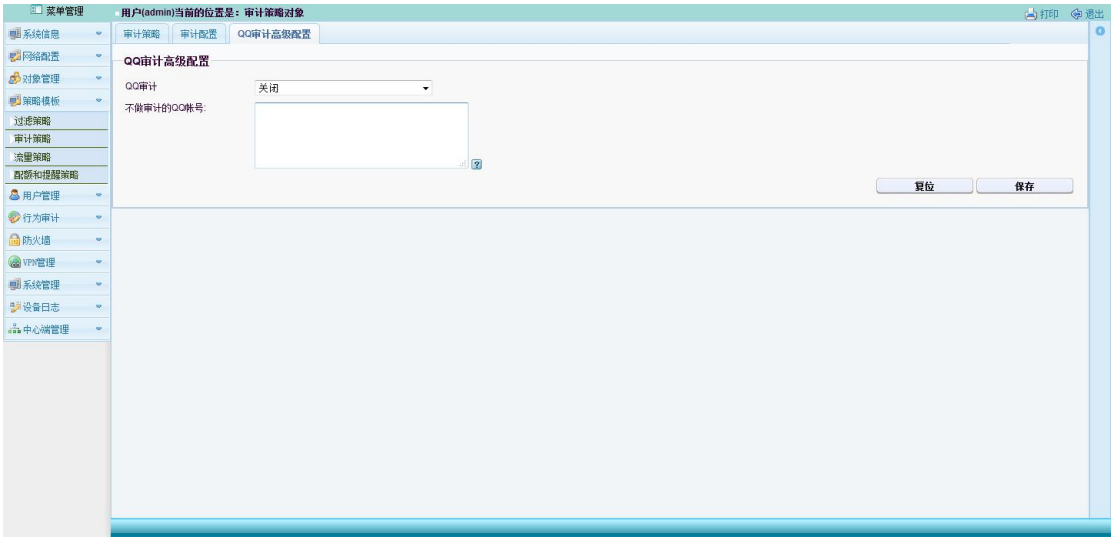
论坛博客审计网站：系统有内置的论坛博客网站，如果用户需要审计一些特点的网站，这些没有包括在当前设备中，则设备可能不会将这些网络数据当成论坛博客进行审计。此时可以将这些网站添加到这里。

需要说明的是当前设备支持智能论坛博客识别（需开启 POST 包审计），设备不认识的网站也可能被正确识别。

上传文件审计网站： 在 HTTP 审计时，系统默认只对 WEBMAIL 网站进行审计，用户需要审计一些特定的网站的时候，需要在这里添加。



QQ 审计高级配置：



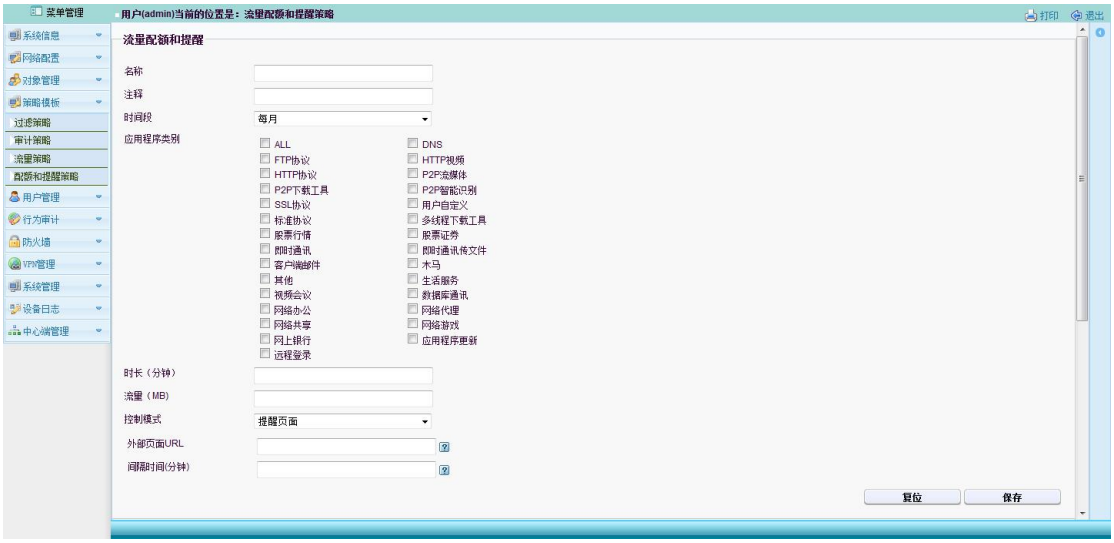
2.6.3 流量策略

流量策略也是针对用户的，可以控制用户某种类型或几种类型的网络访问的流量大小，控制模式是以占用用户允许带宽的百分比来实现的。比如可以控制 P2P 下载占用用户运行带宽的 60%，应用程序类别，可以选择 ALL。也可以复选多个类别。

2.6.4 配额和提醒策略

包括用户网络资源配额功能和提醒功能。

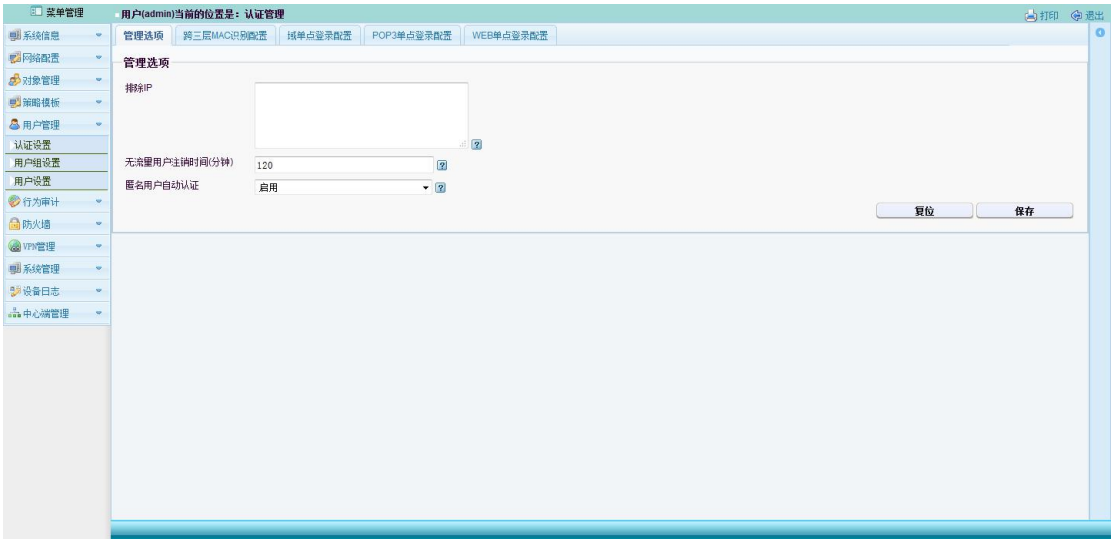
- 配额功能： 在某些应用使用多长时间或多少流量后禁止用户继续使用。
- 提醒策略： 在某些应用使用多长时间或多少流量后弹出提醒页面。
- 时间段： 可以选择配额从什么时候开始计算，包括有当月，当日，本次上线。
- 应用类别： 也是可以选择 ALL，或复选其他几项。
- 时长或流量可以同时存在，谁先到达都会触发策略。
- 控制方式： 包括弹出公告页面（ 在【系统管理】->【高级配置】->【编辑公告页面】 中可以编辑），弹出提醒页面，或者直接拒绝。
- 间隔时间： 如果控制方式是弹出公告或提醒页面，可以控制下次的弹出时间。



2.7. 用户管理

2.7.1 认证设置

管理选项：



用户认证控制选项 ：

排除 IP： 即相应的 IP 不管理，不审计。

无流量用户注销时间： 默认是 120 分钟，即 120 分钟没有流量会注销用户。

匿名用户管理：

匿名用户是指没有被本地用户管理的用户，也就是不在【用户设置】列表里的上网用户。匿名用户由【用户组设置】〖允许匿名登录网段〗来管理，在匿名登录网段范围内的上网用户，会成为这个组的用户。匿名用户有两种方式登录：

1.用户上网时会弹出认证页面，点击匿名登录即可登录。

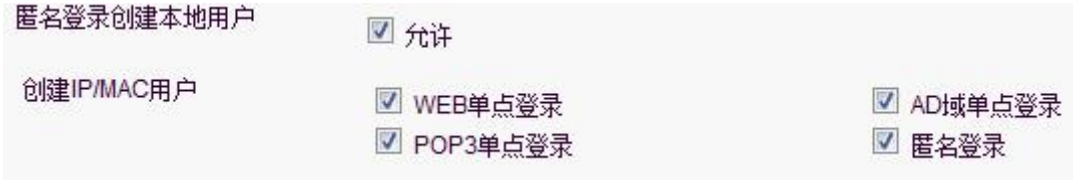
2.〖匿名用户自动认证〗选择启用，则用户上网时不会弹出认证页面，设备会自动运行登录这个用户登录。用户的权限由所属的用户组来管理，如果所有的运行匿名登录网段都不包含这个上网用户的 IP,则此用户无法登录。登录后的的匿名用户会在当前用户列表里显示如：

用户名	登录方式	用户信息	用户组
192.168.0.220	anonymous		default

匿名用户还可以自动创建为本地用户，启用【用户组设置】〖匿名登录创建本地用〗，此时登录匿名用户会在本地用户（【用户认证】）列表里创建一个 IP/MAC 绑定用户如：

192.168.100.243	00:13:e8:2d:29:05	ipmac	dhcp用户组

需要说明的是单点登录的用户在没有创建本地用户时也属于匿名用户，同样由【用户组设置】〖允许匿名登录网段〗来管理。不同的是匿名登录用户自动创建的用户只能是 IP/MAC 用户。单点登录则可以创建本地实名用户，也可以创建 IP/MAC 绑定用户 。如下图所示如果选择了 AD 域，POP3，WEB 单点登录则会创建单点登录的 IP/MAC 用户，这种情况下用户下次无需单点登录也可以以 MAC/IP 认证的方式完成认证。

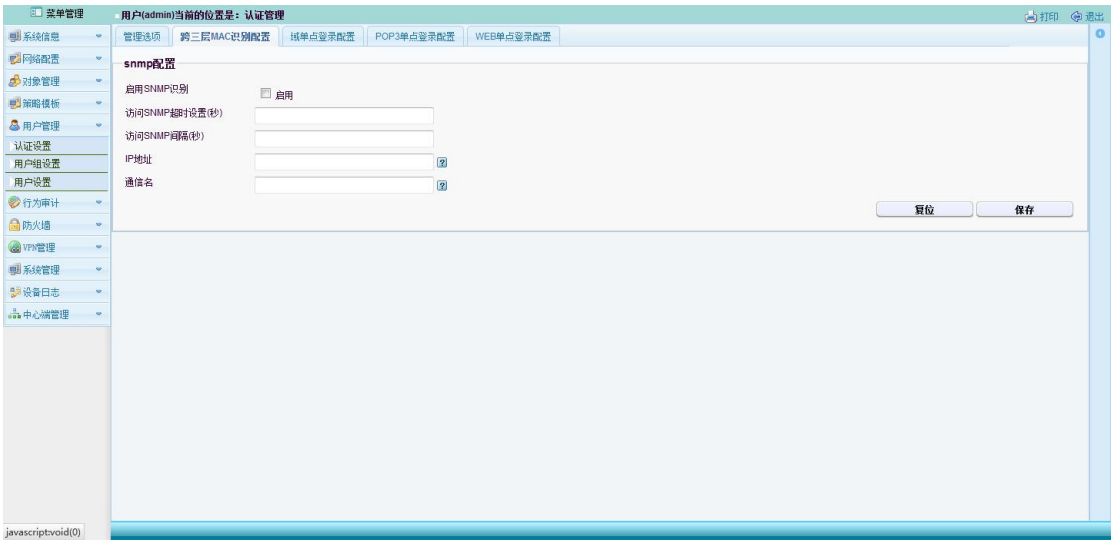


通过匿名用户和单点登录的使用，使得安全设备的部署变得非常方便。

跨三层 MAC 识别配置：

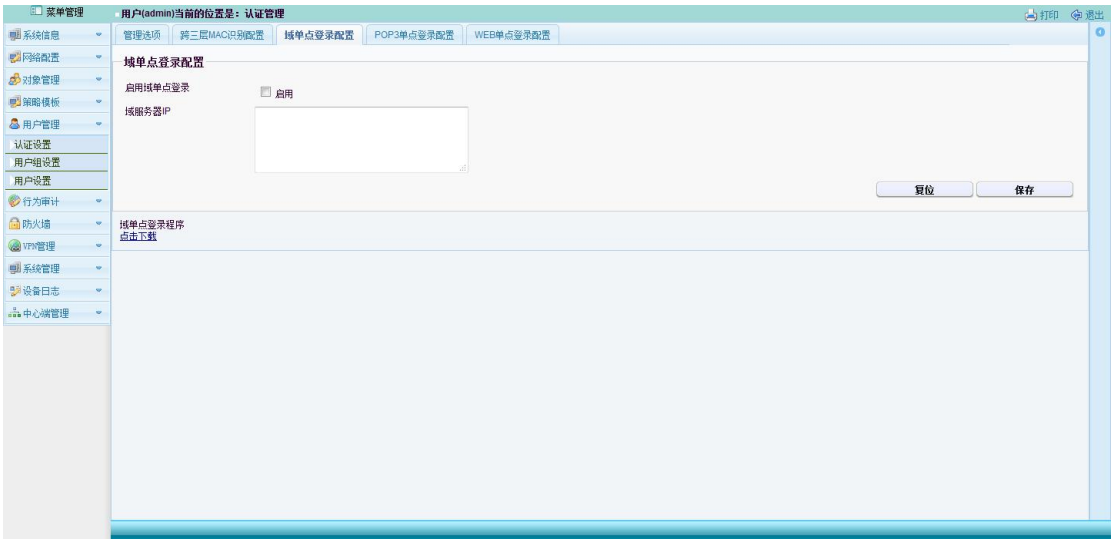
一般企业中经常会使用 MAC/IP 绑定用户，这种类型的用户管理，安全程度不高，但使用方便，这种情况下，如果企业使用的是三层交换机，则无法绑定用户的 MAC。

启用跨三层 MAC 识别，则上网用户即使在三层交换机下面，一样可以完成 MAC 的绑定。实现这个功能需要启用三层交换的 SNMP 功能，通过 SNMP 获得上网用户的 MAC 地址。



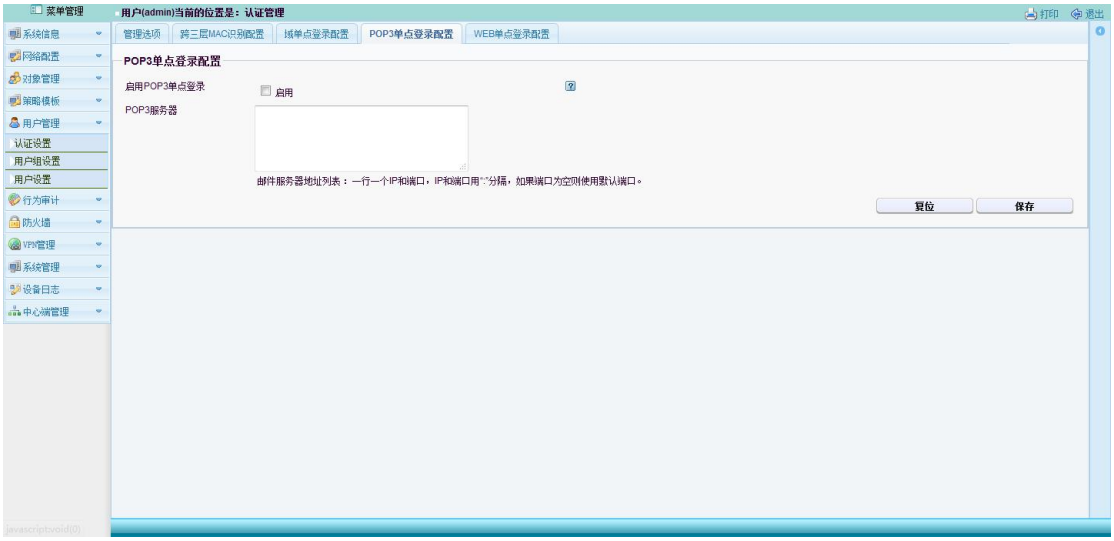
域单点登录配置：

域单点登录是和 WindowsAD 认证集成。该功能需要管理员首先从视频安全接入系统中下载客户端，并将其配置导入所使用的 AD 域服务器中，上网用户在登录 AD 域时，自动完成在视频安全接入系统上得登录。



POP3 单点登录配置：

POP3 单点登录启用时，用户只需打开 OUTLOOK 或 FOXMAIL 等邮件客户端软件收一下邮件就可以完成安全设备的登录。

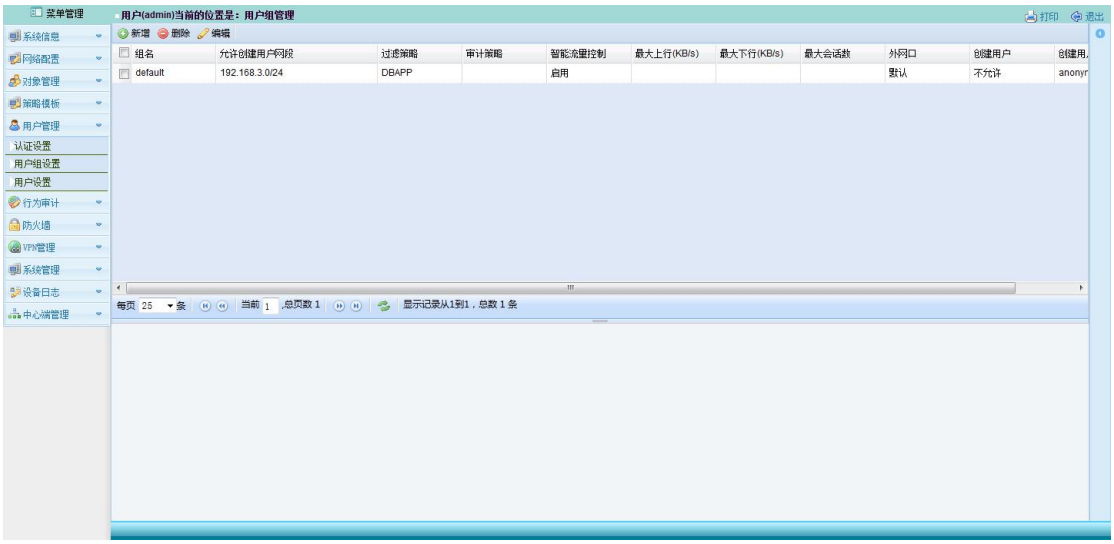


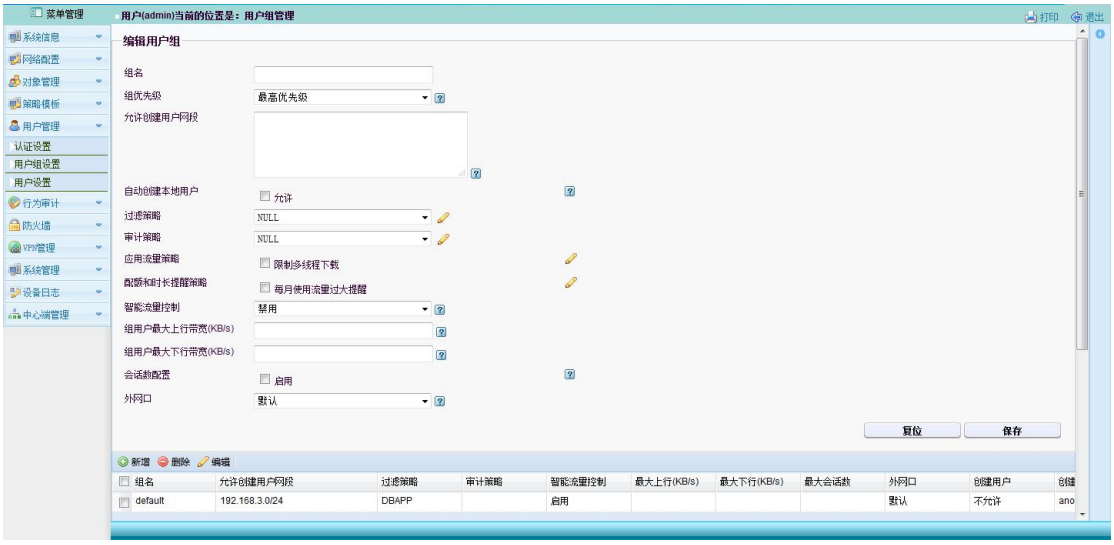
Web 单点登录配置：

如果用户需要登录某些 WEB 服务器时，可以与安全设备绑定，自动在设备上登录。

2.7.2 用户组设置

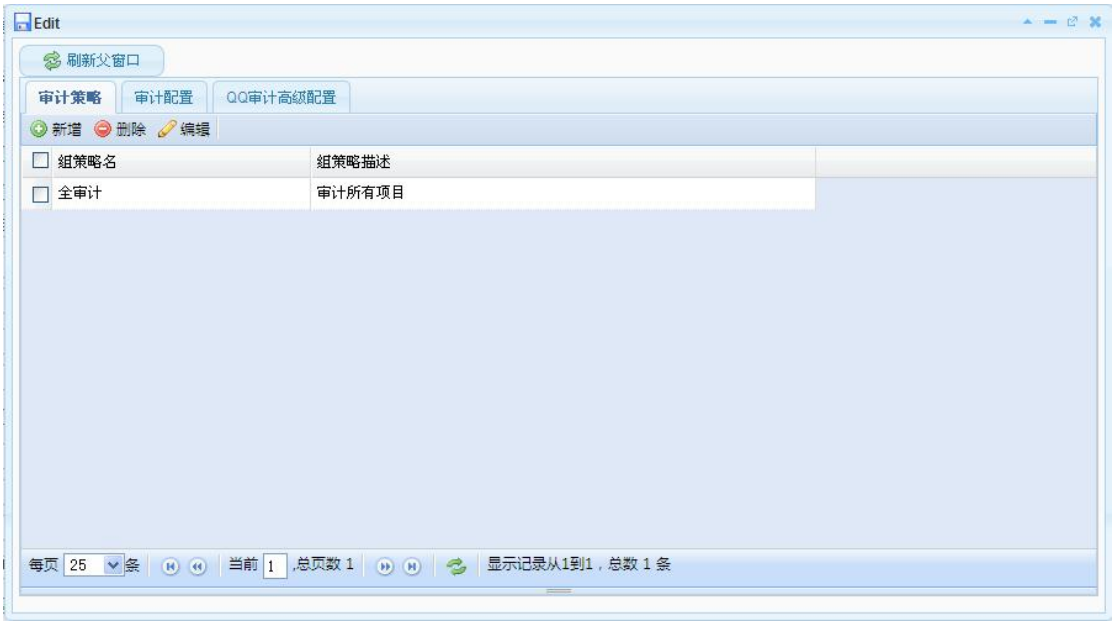
使用用户组功能可以方便用户管理。在用户组中选择过滤规则、审计规则、流量控制等自动生效于组中的用户，可以对用户组中的用户启用智能流量控制。智能流控启用时，要配置好 WAN 口的流量，智能流控系统会自动为用户分配一个相应的带宽，保证带宽的合理应用。

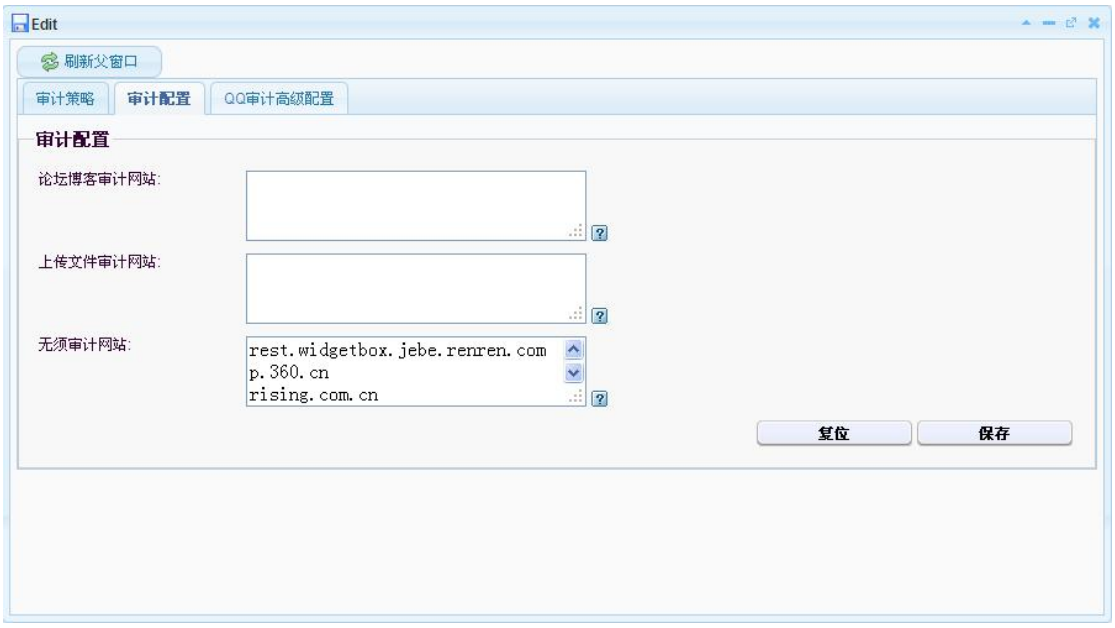




点击“编辑笔”会弹出过滤策略、审计策略、应用流量策略、配额和时长提醒策略


Edit
刷新父窗口
新增
删除
编辑
子规则编辑
策略组名
策略组描述
禁止P2P下载
封堵P2P等下载工具，仅允许单线程下载，提升正常上网速度
工作时间禁止无关网络使用
禁止在上班时间聊天、游戏、娱乐、炒股等
不允许加密通讯
阻断加密应用提高网络可见性，如SSL、远程登录、传文件等
严格限制
仅允许基本上网应用：浏览网站、收发邮件等
只允许即时通讯
只允许使用即时通讯,其他拒绝
只允许邮件
只允许使用客户端邮件或网页邮箱,其他拒绝
只允许邮件和即时通信
允许使用pop3邮件和web邮箱和即时通信,其他拒绝
每页 25 条
当前 1 ,总页数 1
显示记录从1到7，总数 7 条

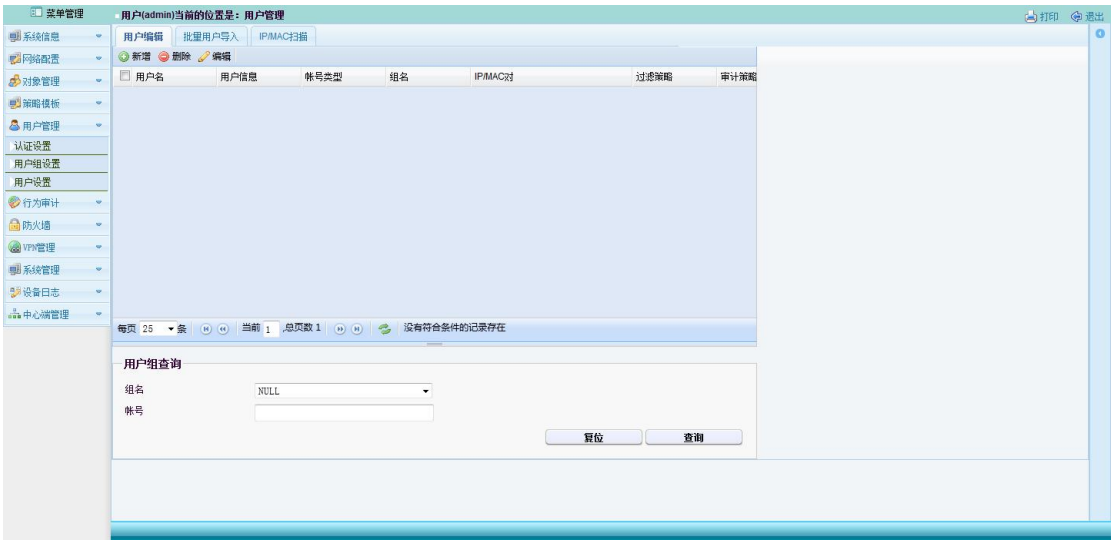

Edit
刷新父窗口
审计策略
审计配置
QQ审计高级配置
新增
删除
编辑
组策略名
组策略描述
全审计
审计所有项目
每页 25 条
当前 1 ,总页数 1
显示记录从1到1，总数 1 条

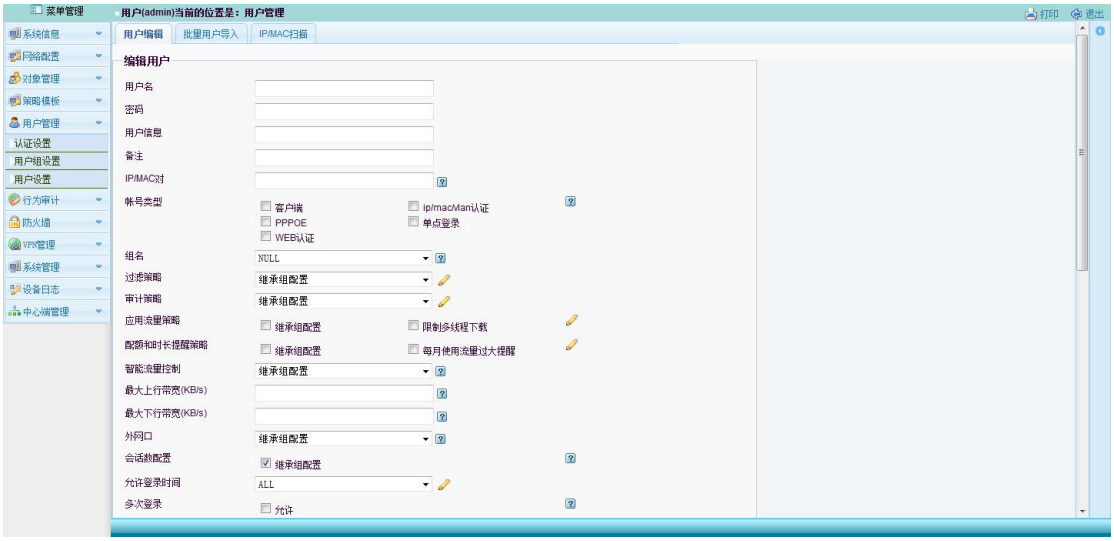

Edit
刷新父窗口
审计策略
审计配置
QQ审计高级配置
审计配置
论坛博客审计网站:
上传文件审计网站:
无须审计网站:
rest.widgetbox.jebe.renren.com
p.360.cn
rising.com.cn
复位
保存


Edit
刷新父窗口
审计策略
审计配置
QQ审计高级配置
QQ审计高级配置
QQ审计
关闭
不做审计的QQ帐号:
复位
保存

2.7.3 用户管理

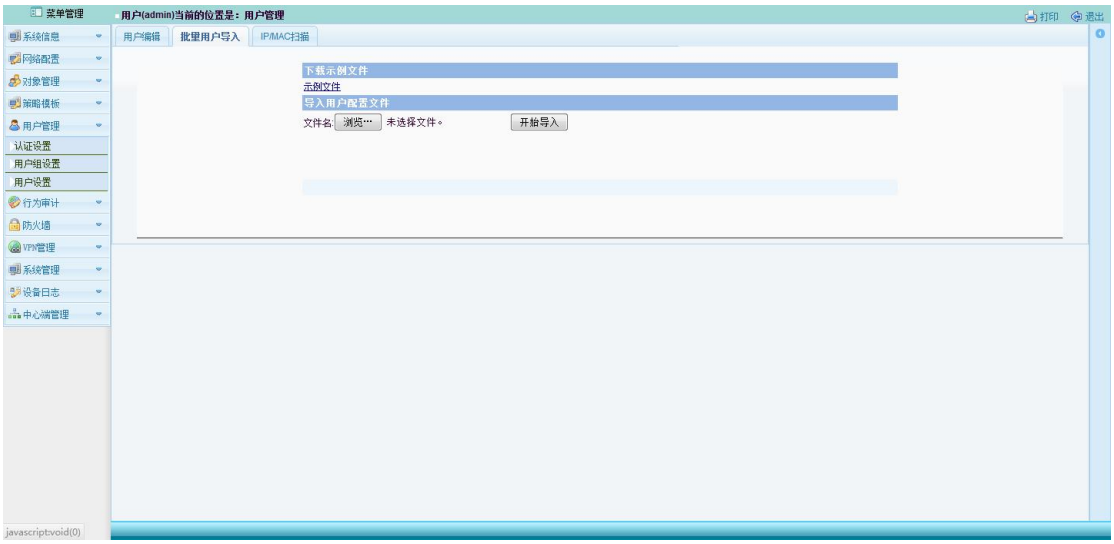
用户编辑：



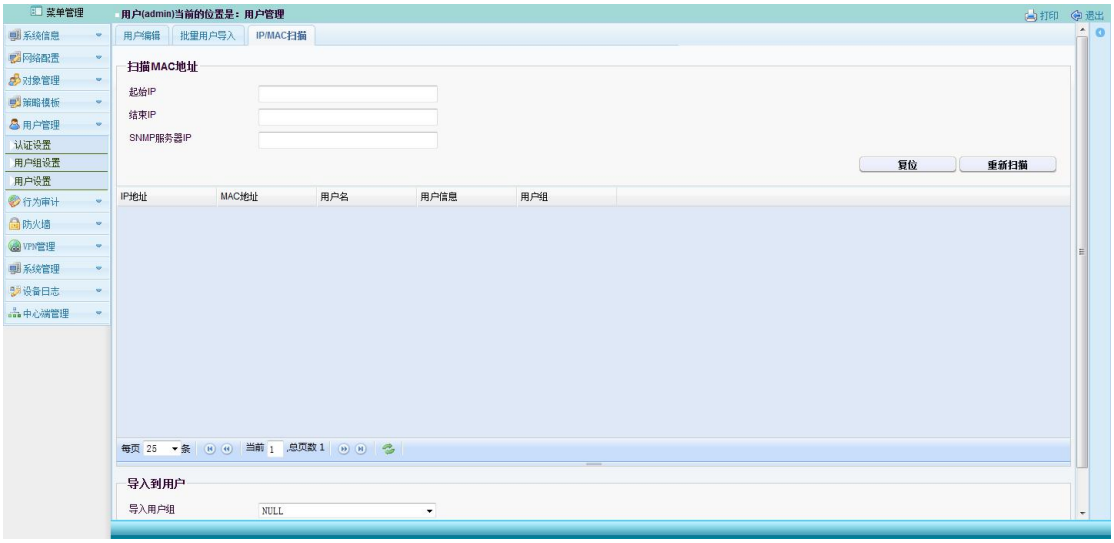


编辑用户的属性，所有为空的属性默认继承组属性，如果想修改用户的属性，也可以重新配置，同时可以选择批量用户导入和 ARP 扫描导入，ARP 扫描导入时可以选择导入组，已有用户不受影响，如果希望修改用户信息，可以在导入后手工修改。

批量用户导入：



IP/MAC 扫描：

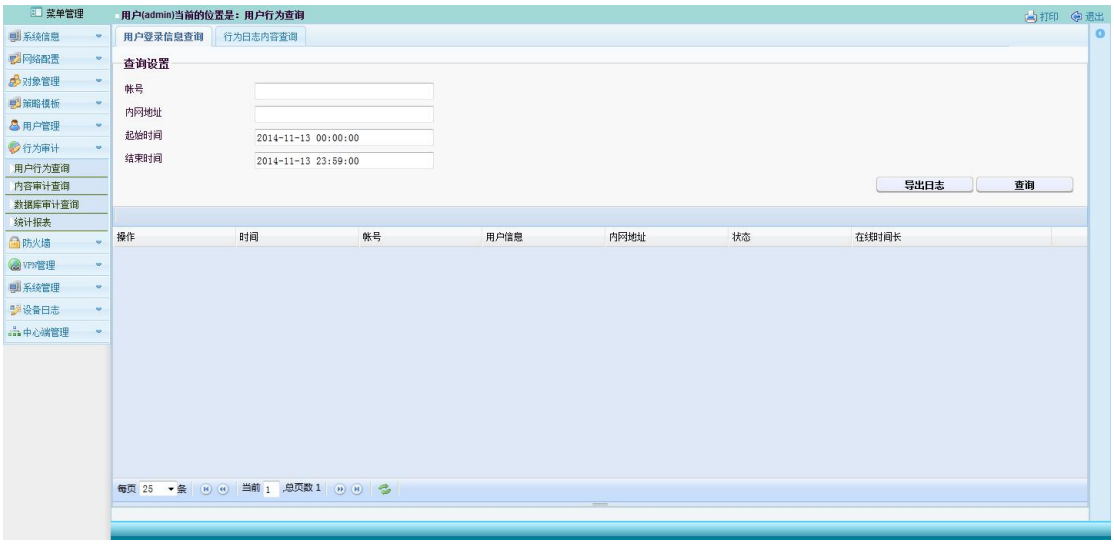


2.8. 行为审计

上网行为都被记录在视频安全接入系统的数据库中，通过本菜单可以对记录的行为进行查询。审计数据可以通过各种查询条件进行查询，查询到的数据可以通过点击详细信息按钮查看详细信息。

2.8.1 用户行为查询

用户登录信息查询：



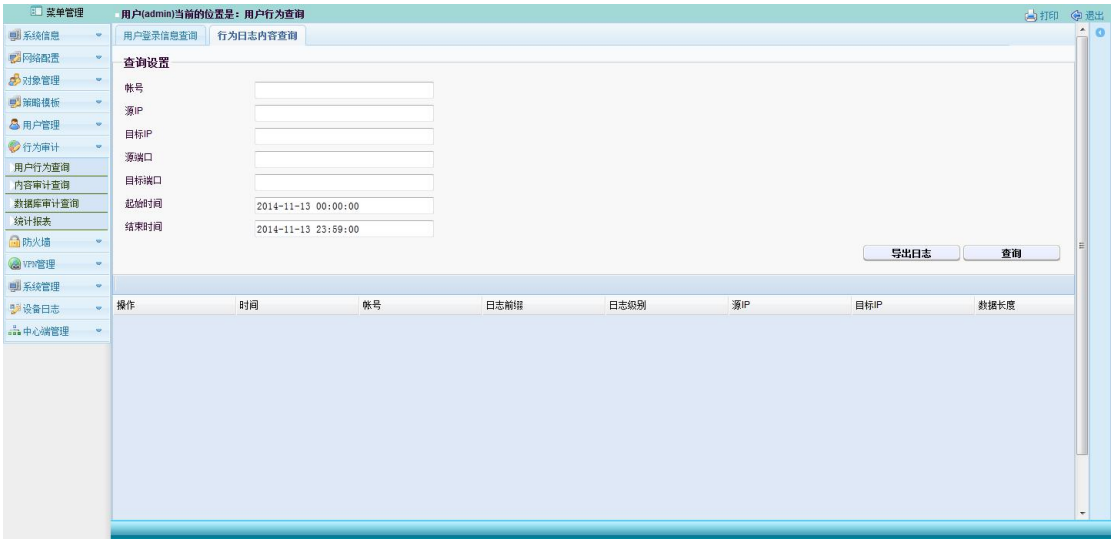
- 用户行为查询：包括上网用户的登录信息和行为日志。
- 用户登录信息记录上网用户的登录，下线，登录时长等信息。

行为日志内容查询：

行为日志是指在【过滤策略】中设置为〖日志〗的策略所记录的信息。日志记录可以生产为〖详细日志〗或〖简略日志〗，在【系统管理】->【高级配置】中设置。

详细日志会记录被策略匹配的完整的数据包。

简略日志只记录 IP, 端口，应用名等信息。

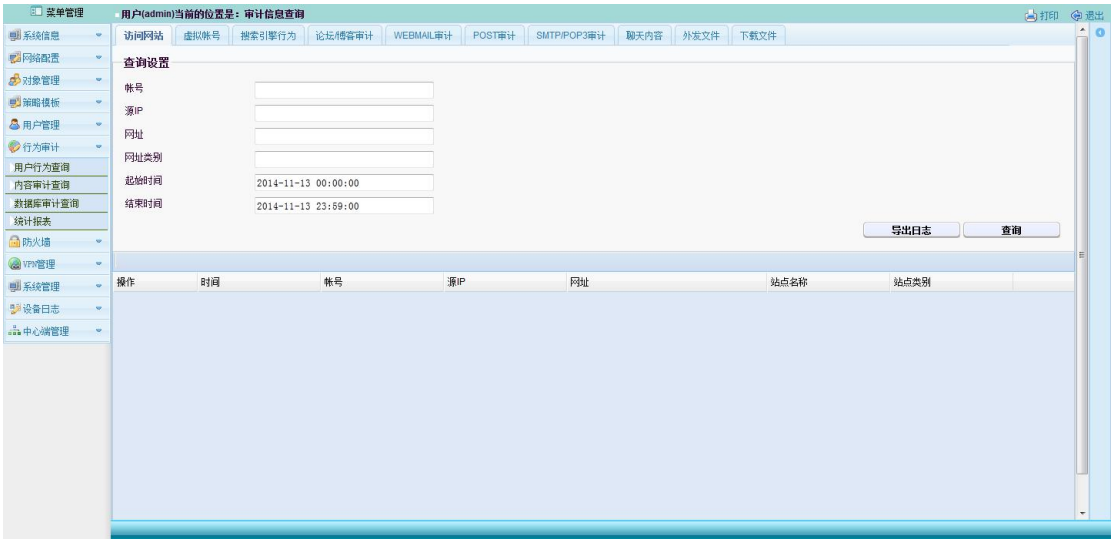


2.8.2 内容审计查询

内容审计的数据是通过【审计策略】产生的审计信息。

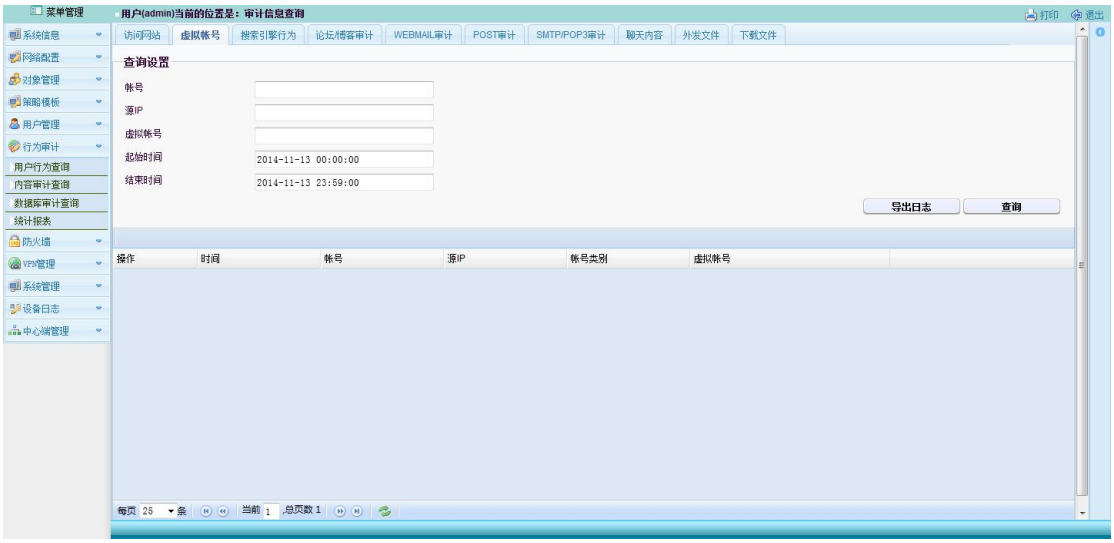
访问网站：

访问网站默认记录访问首页和相应 HTML 网页的信息。记录方式可以在【系统管理】->【高级配置】中设置。



虚拟帐号查询：

记录上网用户的 QQ，MSN，飞信等账号的登录情况。



搜索引擎行为：

记录百度，谷歌等搜索引擎的使用情况。

论坛/博客审计：

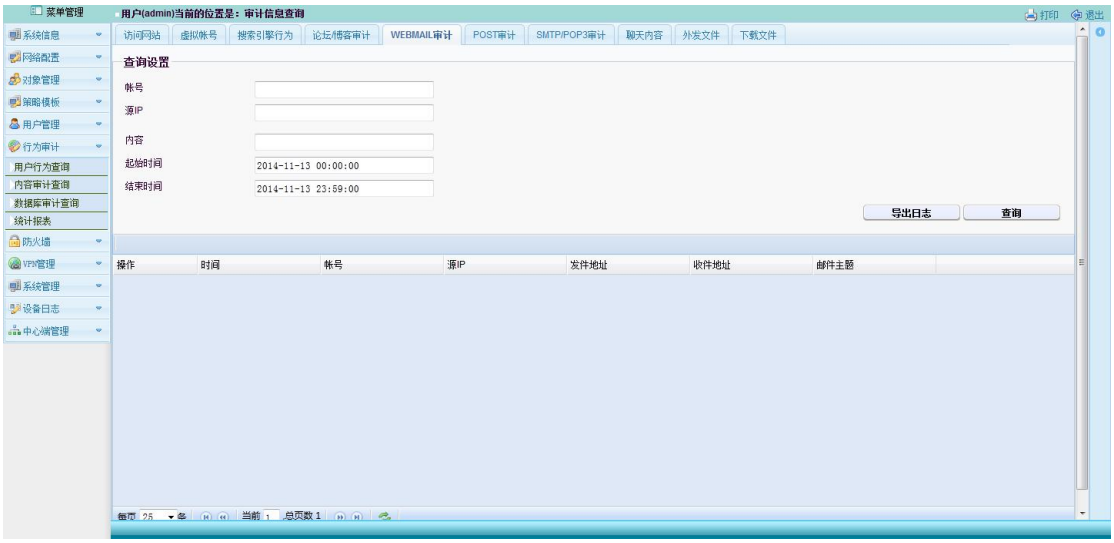
审计常用论坛博客的信息，管理员也可以自定义论坛博客的网站，和审计关键字等信息（【审计策略】->【审计配置】）。

WEBMAIL 审计：

邮件审计分为 web 邮件和客户端邮件。WEB 邮件目的是审计常用的 WEB 邮箱，不支持 SSL 的邮箱比如 GMAIL。如果管理员需要审计所有的邮件，可以关闭 WEB 邮箱（【过滤策略】->【URL 过滤】），只允许使用客户端邮件。审计的内容包括草稿，附件等所有的信息。

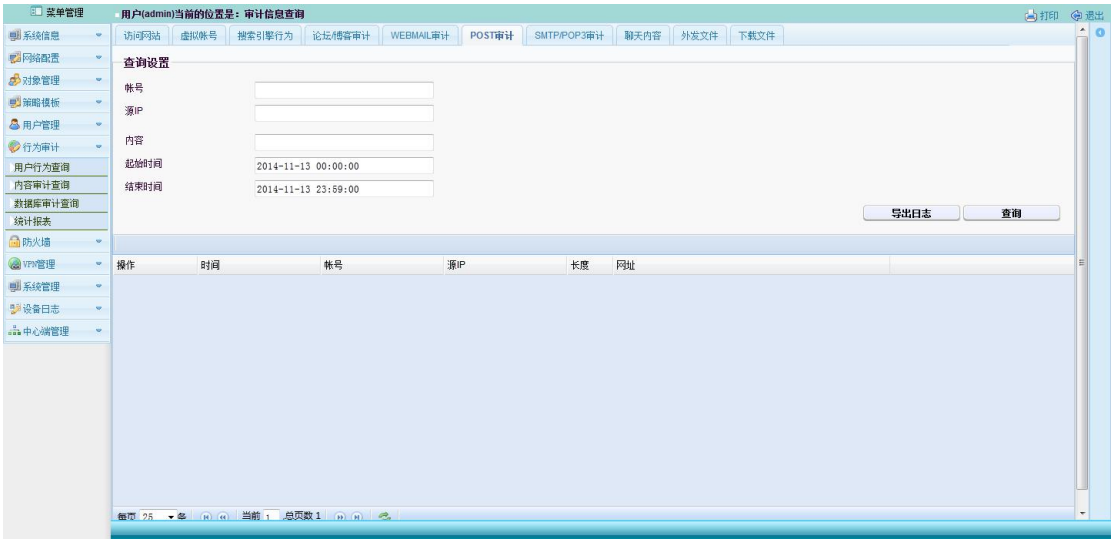
说明： 如果审计的收件人地址为空，说明是审计的是草稿。如果发送的有附件，审计时间较长，可能最大延迟 5 分钟才审计到。审计到的附件同时会显示在〖外发文件审计〗

中。



POST 审计：

POST 包审计： 因为网络上得 POST 包比较多，默认策略里是不审计 POST 包，对审计要求比较严格的企业单位可以开启 POST 包审计，这样用户所有的 HTTP 发送信息都会被审计到。



SMTP/POP3 审计：

客户端邮件审计支持 OUTLOOK、FOXMAIL 等所有标准 SMTP/POP3 的审计，支持 SSL 加密邮件的审计。

聊天内容审计：

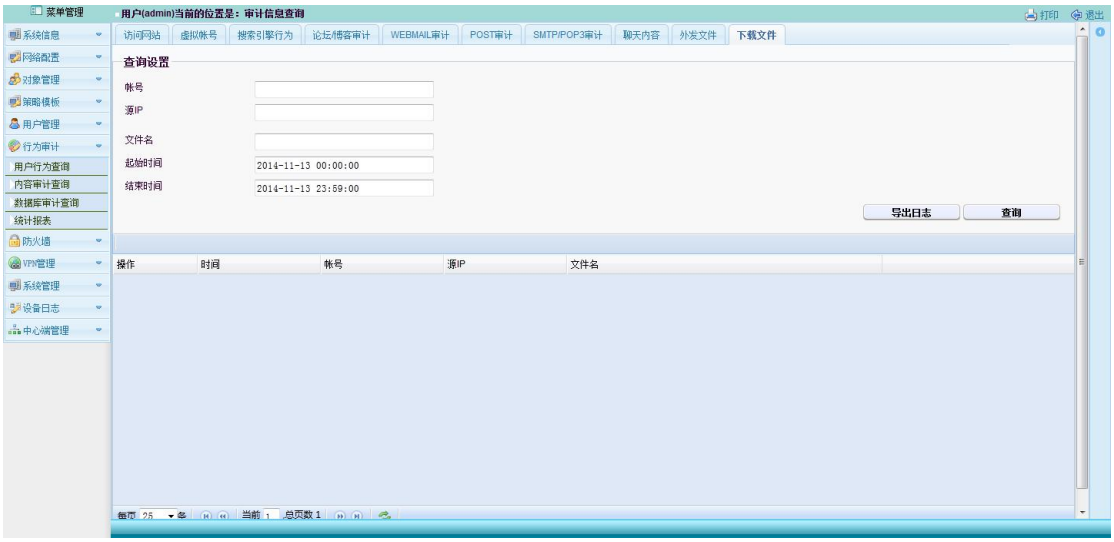
聊天内容支持 QQ、MSN 的审计。

外发文件审计：

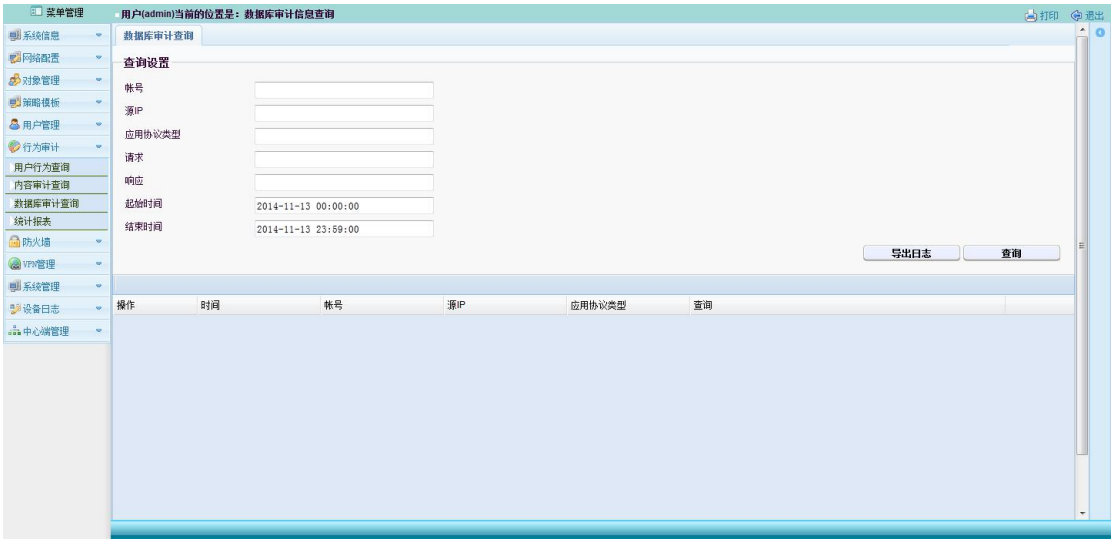
邮件发送的附件，或用户自定义网站（在【审计策略】->【审计配置】）发送的文件进行审计。


菜单管理
用户(admin)当前的位置是：审计信息查询
打印
退出
系统信息
网络配置
对象管理
策略模板
用户管理
行为审计
用户行为查询
内容审计查询
数据库审计查询
统计报表
防火墙
VPN管理
系统管理
设备日志
中心端管理
访问网站
虚拟帐号
搜索引擎行为
论坛/博客审计
WEBMAIL审计
POST审计
SMTP/POP3审计
聊天内容
外发文件
下载文件
查询设置
帐号
源IP
文件名
起始时间
2014-11-13 00:00:00
结束时间
2014-11-13 23:59:00
导出日志
查询
操作
时间
帐号
源IP
文件名
每页 25
当前 1
总页数 1

下载文件审计：


菜单管理
用户(admin)当前的位置是：审计信息查询
打印
退出
系统信息
网络配置
对象管理
策略模板
用户管理
行为审计
用户行为查询
内容审计查询
数据库审计查询
统计报表
防火墙
VPN管理
系统管理
设备日志
中心端管理
访问网站
虚拟帐号
搜索引擎行为
论坛/博客审计
WEBMAIL审计
POST审计
SMTP/POP3审计
聊天内容
外发文件
下载文件
查询设置
帐号
源IP
文件名
起始时间
2014-11-13 00:00:00
结束时间
2014-11-13 23:59:00
导出日志
查询
操作
时间
帐号
源IP
文件名
每页 25
当前 1
总页数 1

2.8.3 数据库审计查询

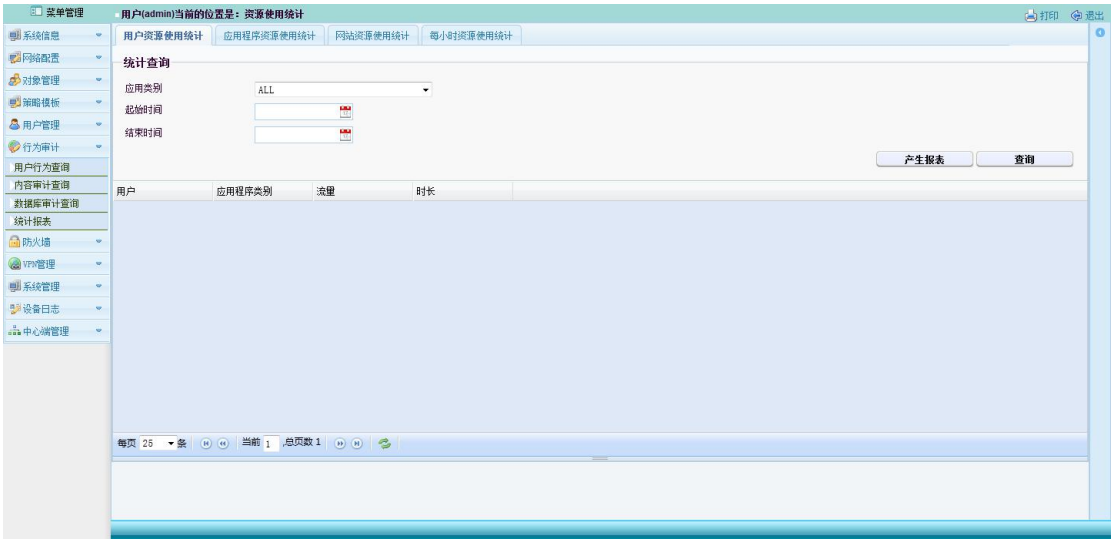


2.8.4 统计报表

统计各种资源使用情况，提供查询条件，产生报表，包括饼装图，走势图等。

用户资源使用统计：

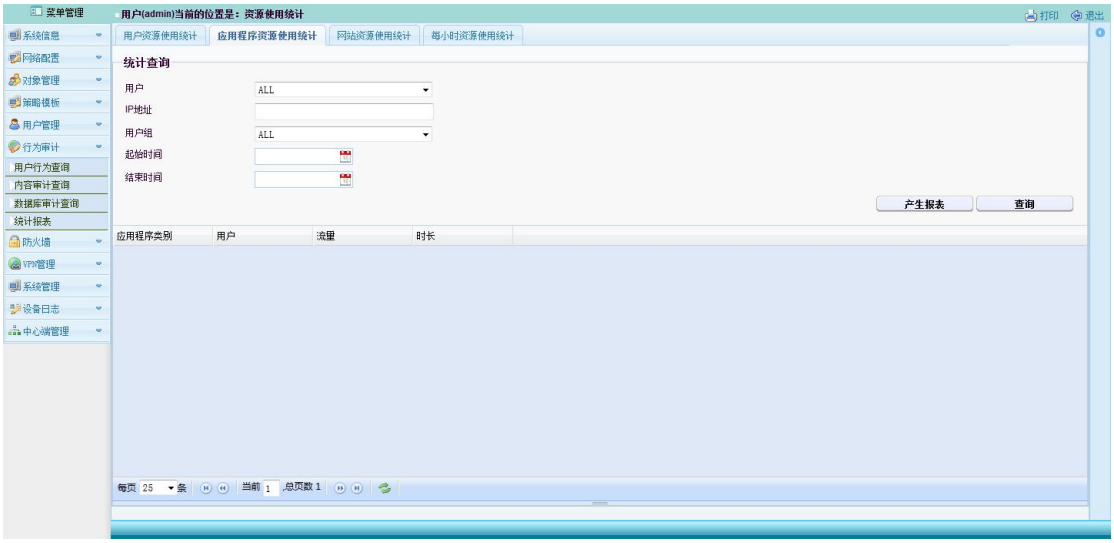
统计用户各种应用类别的总使用时间，和使用流量，依据流量自动排序。可以查询总的流量，或某个类别的流量。



应用程序资源使用统计：

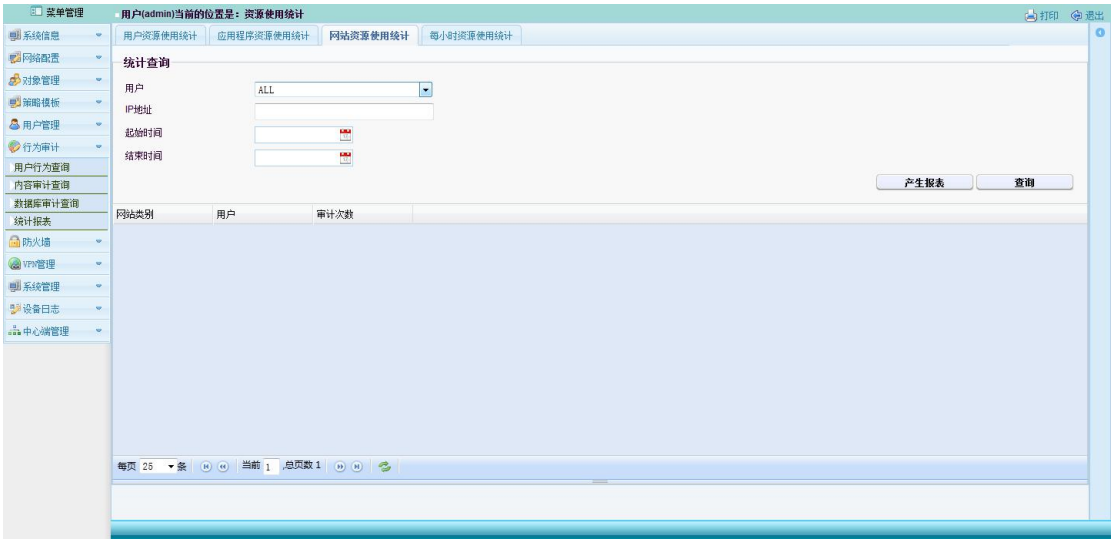
可以查询每个用户一段时间内，各种应用的流量，使用时长。也可查询一组或所有用户一段时间内，各种应用的总流量，总时长。

说明：应用时长是根据用户来统计的，总时长加在一起会显得比较大，这属于正常情况。



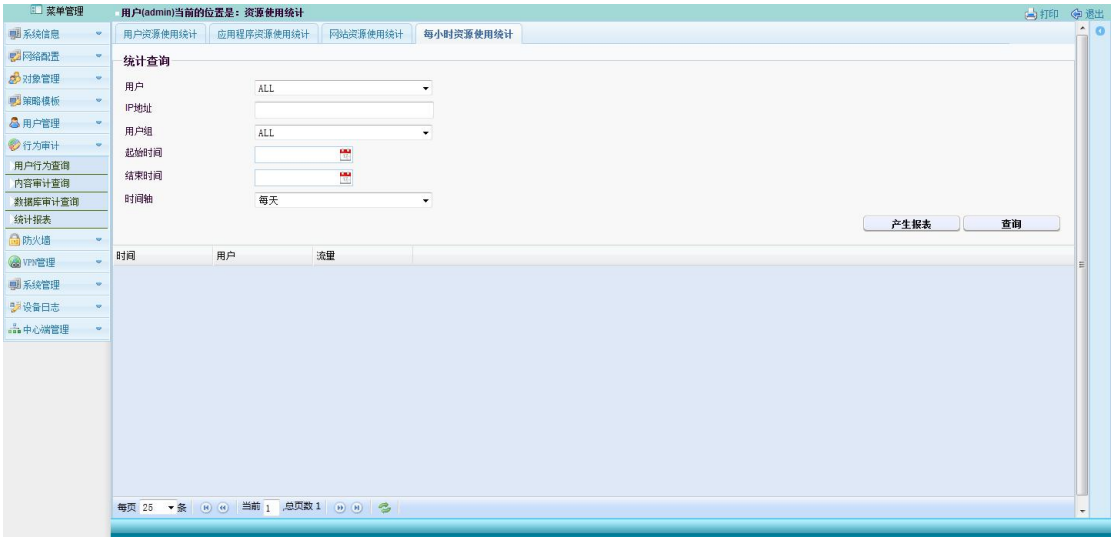
网站资源使用统计：

统计一段时间内某个用户或所有用户不同类别网站的访问次数。



每小时资源使用统计：

每小时或每天的用户流量走势图。



2.9. 防火墙

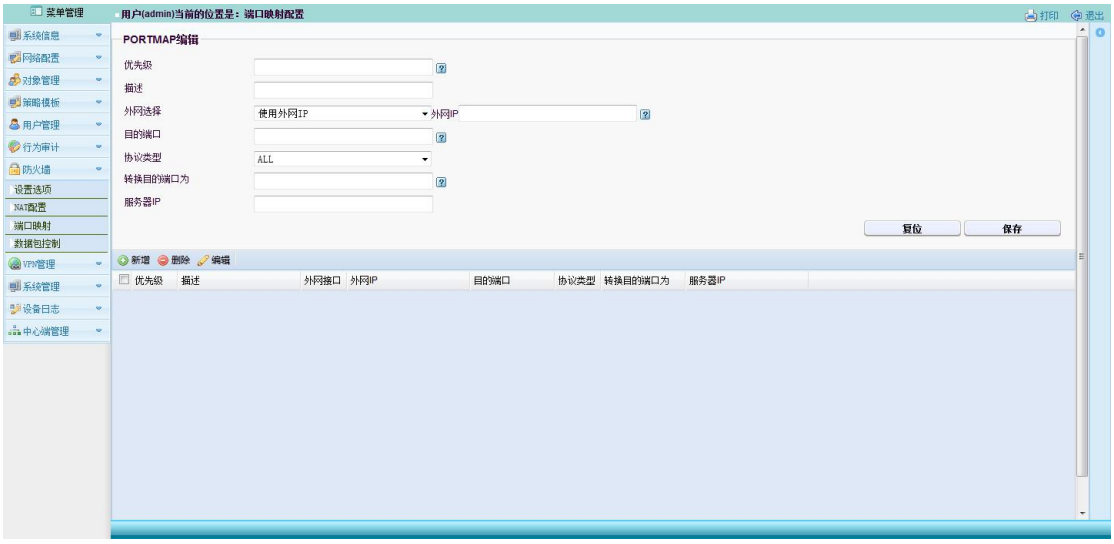
防火墙的几种控制策略，可以与用户管理一起使用，每种策略都支持优先级管理。优先级高则策略先执行，优先级低则后执行。

2.9.1 NAT 配置

手工配置源地址转换规则，可以根据源地址，目标地址或出口，对数据包进行相应的源地址转换。

2.9.2 端口映射

对进入设备的数据包进行目标地址转换。可以根据网络的接口，访问的接口 IP，目的端口等选择转发到某个 IP 的特定端口。端口映射支持数据回流，内网用户可以像外网用户一样通过域名来访问内部服务器。



- 〖外网接口〗中可以选择映射接口，如果接口中有多个 IP，只希望其中的一个 IP 完成映射，可以选择使用外网 IP, 然后在外网 IP 中填入一个 IP 地址。
- 目的端口：访问接口上得端口。
- 转换目的端口：内网服务器的端口。
- 服务器 IP：内网服务器 IP。

说明：由于内网的用户需要认证才能上网，服务器 IP，也需要完成认证，或者可以将服务器 IP 添加到【认证设置】〖排除 IP〗中。

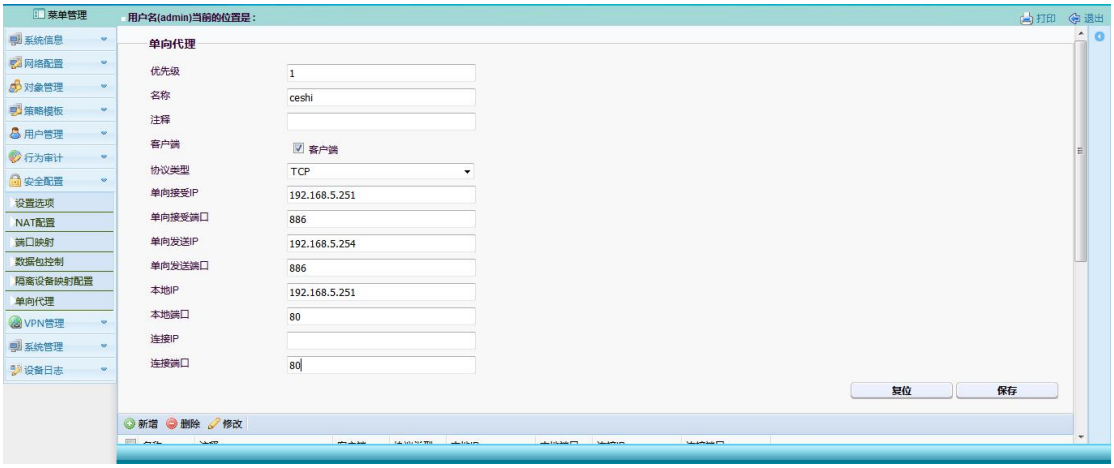
2.9.3 数据包控制

对出入设备的数据包根据 IP 和端口进行控制，支持状态检测。IP 和端口需要在对象管理的 IP 管理和服务管理里先定义。

2.10. TCP 转 UDP

2.10.1 客户端配置

进入“安全配置”->“单向代理”页面，点击“新增”



客户端：勾选则作为客户端，不勾选则作为服务器；

协议类型：应用服务器的协议，支持 tcp、udp；

单向接受 IP（通道监听 IP）：前置机侦听 IP；

单向接受端口（通道监听端口）：前置机侦听端口，与网闸 UDP 映射端口保持一致；

单向发送 IP（对端通道 IP）：即网闸 IP；

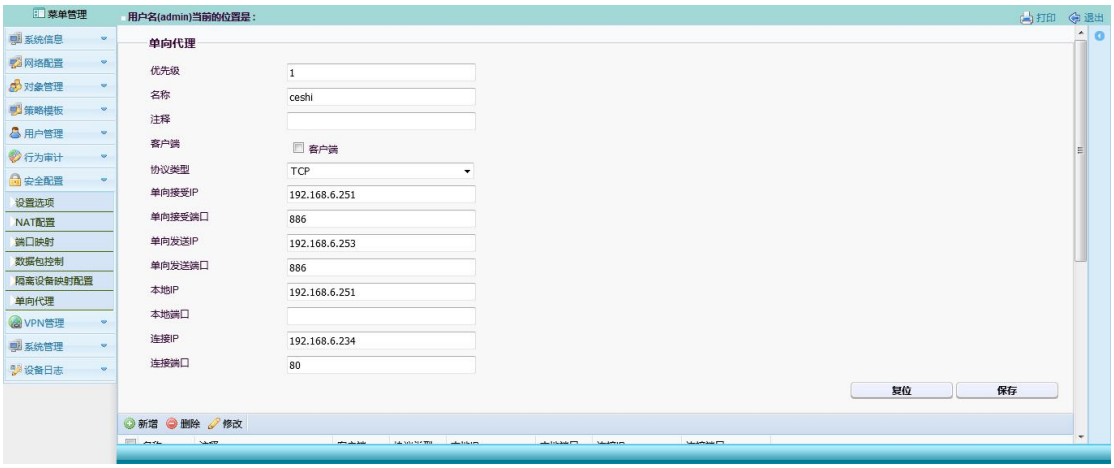
单向发送端口（对端通道端口）：即网闸端口，与单向接受端口保持一致；

本地 IP：前置机服务 IP；

本地端口：前置机服务端口；

2.10.2 服务端配置

进入“安全配置”->“单向代理”页面，点击“新增”



客户端：勾选则作为客户端，不勾选则作为服务器；

协议类型：应用服务器的协议，支持 tcp、udp；

单向接受 IP（通道监听 IP）：后置机侦听 IP，与网闸 UDP 映射端口保持一致；

单向接受端口（通道监听端口）：后置机侦听端口；

单向发送 IP（对端通道 IP）：即网闸 IP；

单向发送端口（对端通道端口）：即网闸端口，与单向接受端口保持一致；

本地 IP：后置机服务 IP；

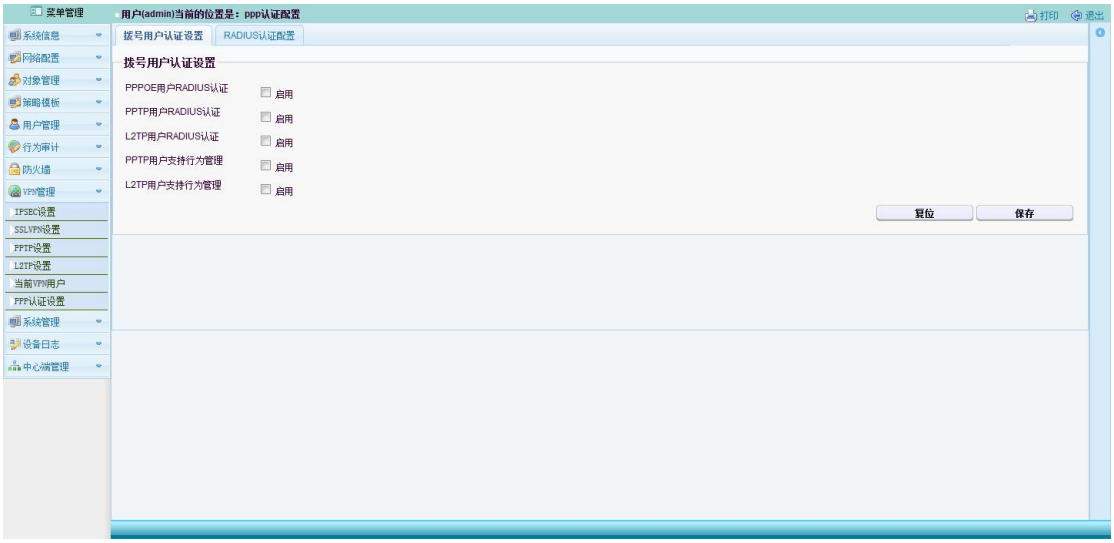
连接 IP：即服务器 IP；

连接端口：即服务器端口。

2.11. VPN 管理

2.11.1 PPP 认证设置

设置 PPP 连接用户（包括 PPPOE,PPTP,L2TP）的认证模式和管理模式。



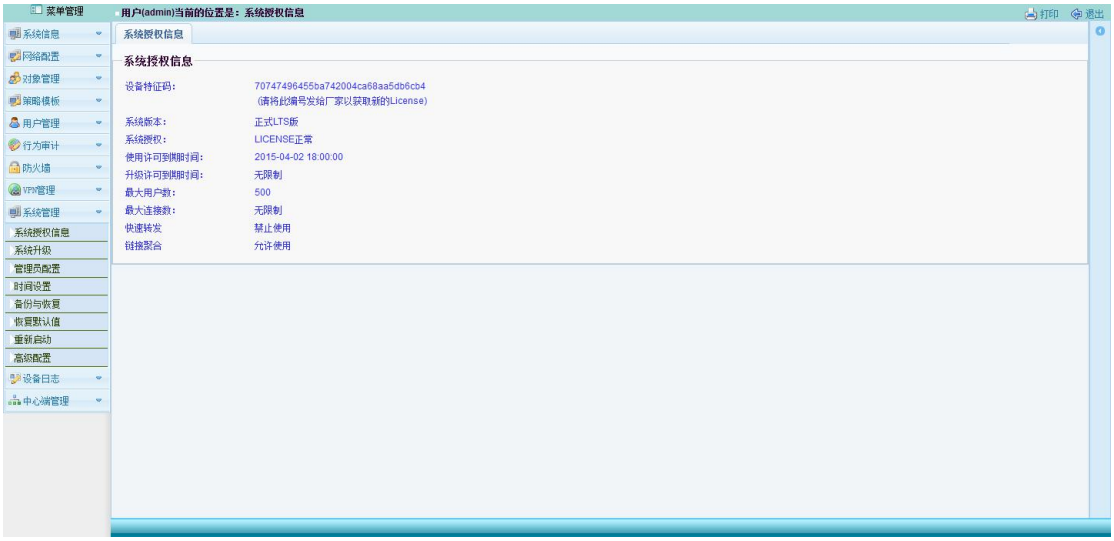
如果启用了相应的 RADIUS 认证，需要在右边的 RADIUS 认证中配置好 RADIUS 服务器，则上网用户认证不通过本地完成认证。与单点登录类似，如果配置〖支持行为管理〗用户可以自动创建。

说明：启用 RADIUS 认证需要在 DDNS 里配置一个设备主机名。

2.12. 系统管理

2.12.1 系统授权信息

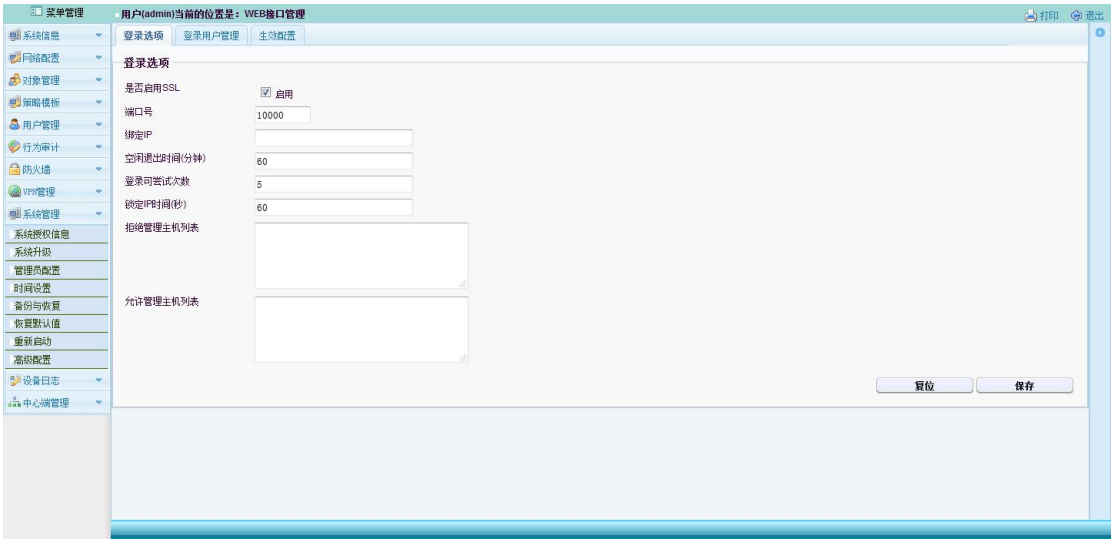
该页面显示系统的授权信息，具有：设备特征码（用于系统注册）、系统版本（目前系统的版本号）、系统授权（提示目前 LICENSE 的状态）使用许可到期时间、升级许可到期时间、最大连接数、快速转发是否、链接聚合状态。



2.12.2 管理员配置

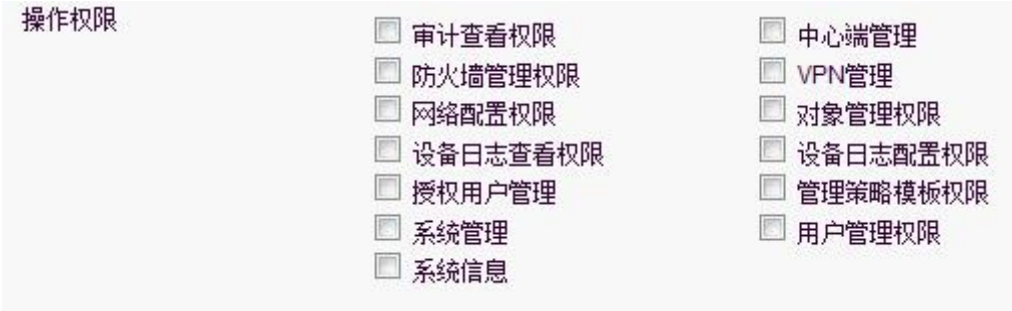
登录选项：

管理员登录时的安全控制。



登录用户管理：

理员账号的管理，可以创建，删除管理员，编辑管理员的权限。

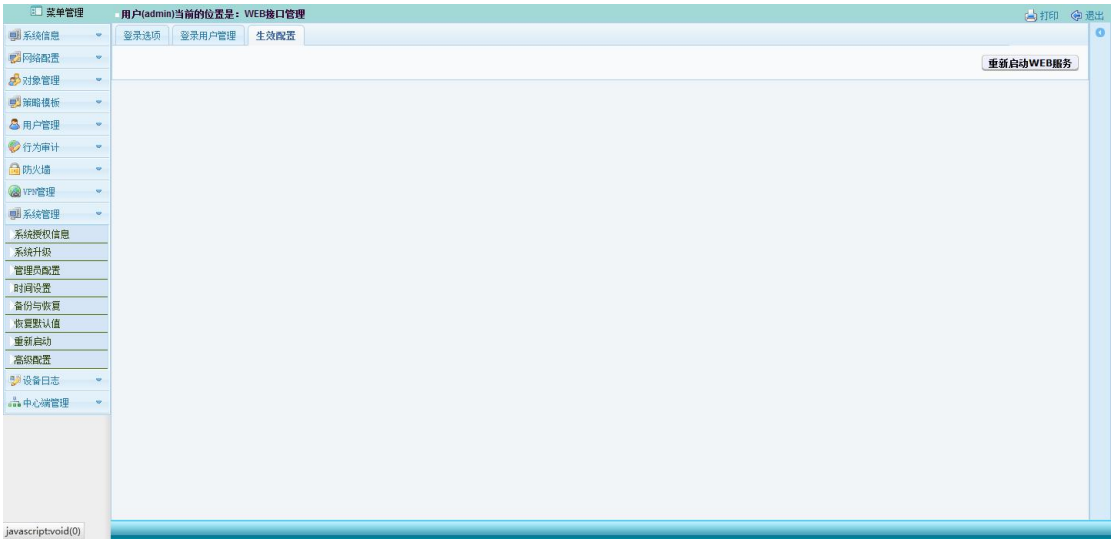


说明： 管理员配置保存后并不自动生效，需要点击右边的〖生效配置〗。

点击“新建”按钮可设置管理员操作权限。

生效配置：

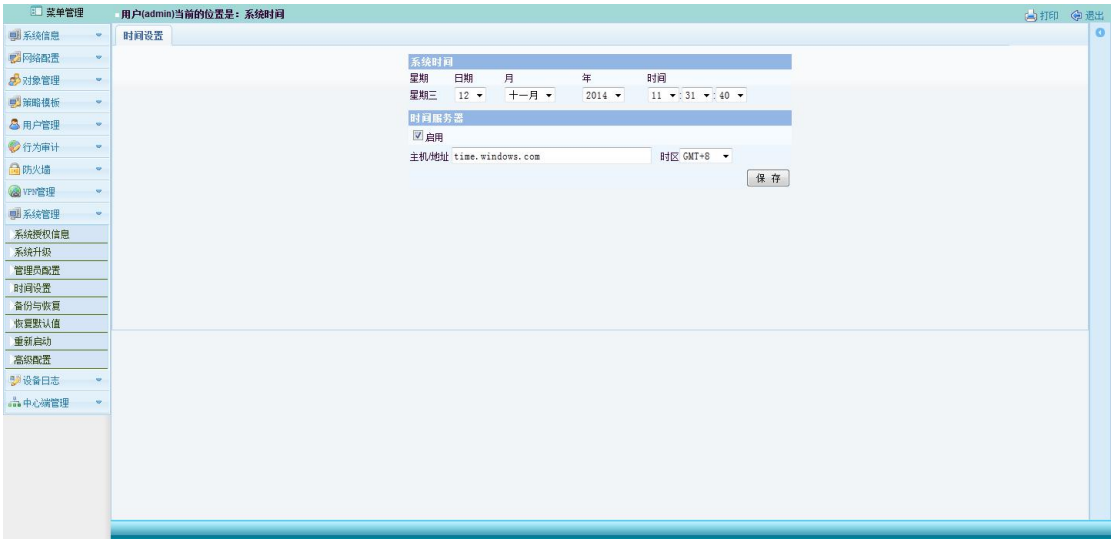
点击“重新启动 WEB 服务”，使刚刚编辑过的管理员配置信息生效。



2.12.3 时间设置

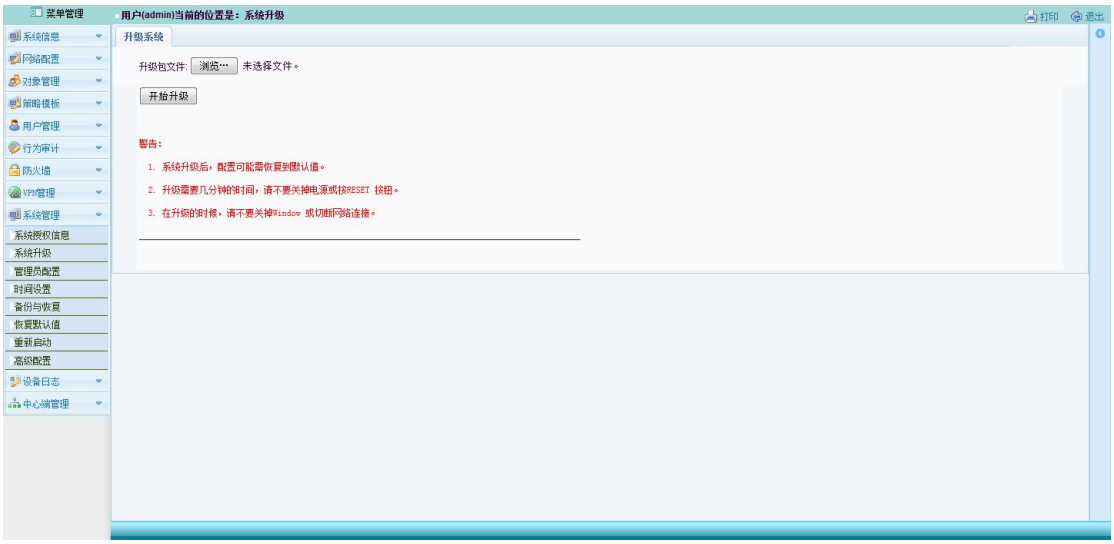
视频安全接入系统利用时间设置时间戳到每件日志事件，自动地更新内容过滤目录，或为其它内部的原因。

用手动设置系统时间或通过网络服务器自动设置本地时间。当选择使用 NTP 设置时间，视频安全接入系统会自动地连入提供正确时间的 NTP 服务器。同时要选择正确的时区。



2.12.4 系统升级

使用这个功能升级视频安全接入系统的固件到最新的版本。如果已经下载了固件到电脑上，那么点击“浏览”寻找这个文件，然后点击“开始升级”按钮。

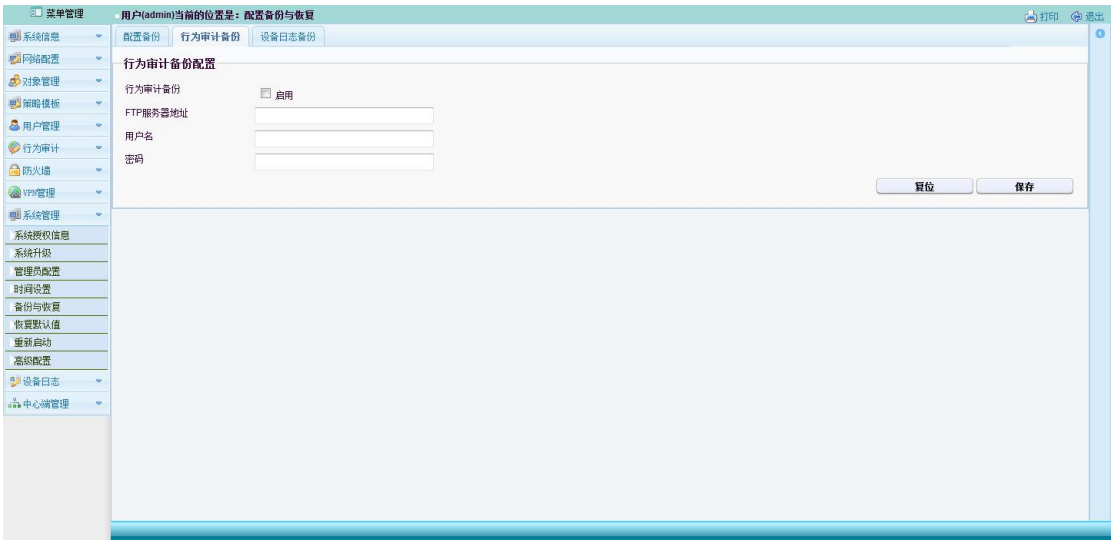


2.12.5 备份与恢复

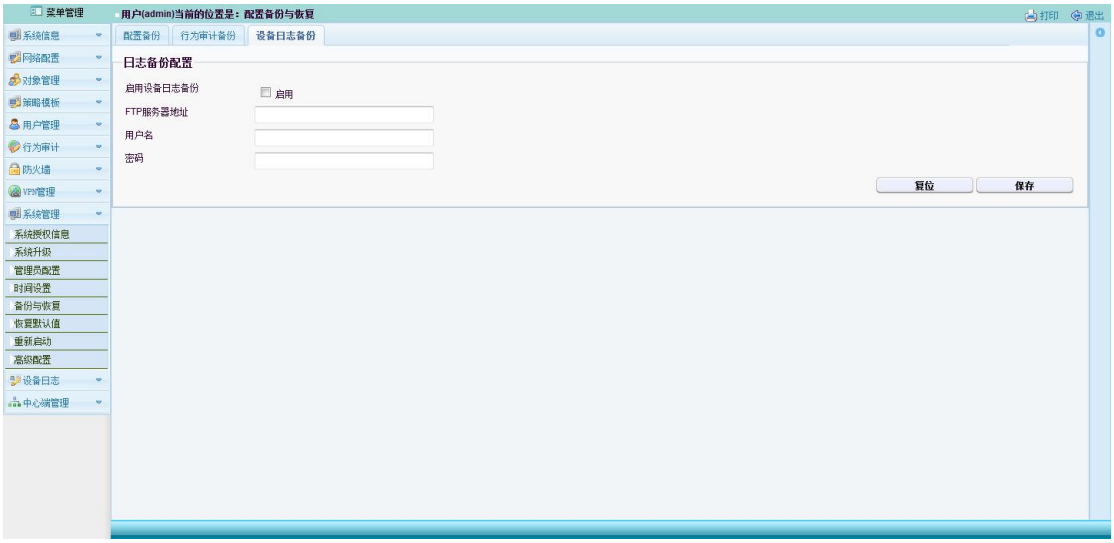
配置备份：

在这个页面，视频安全接入系统提供一个备份文件和恢复配置的功能。

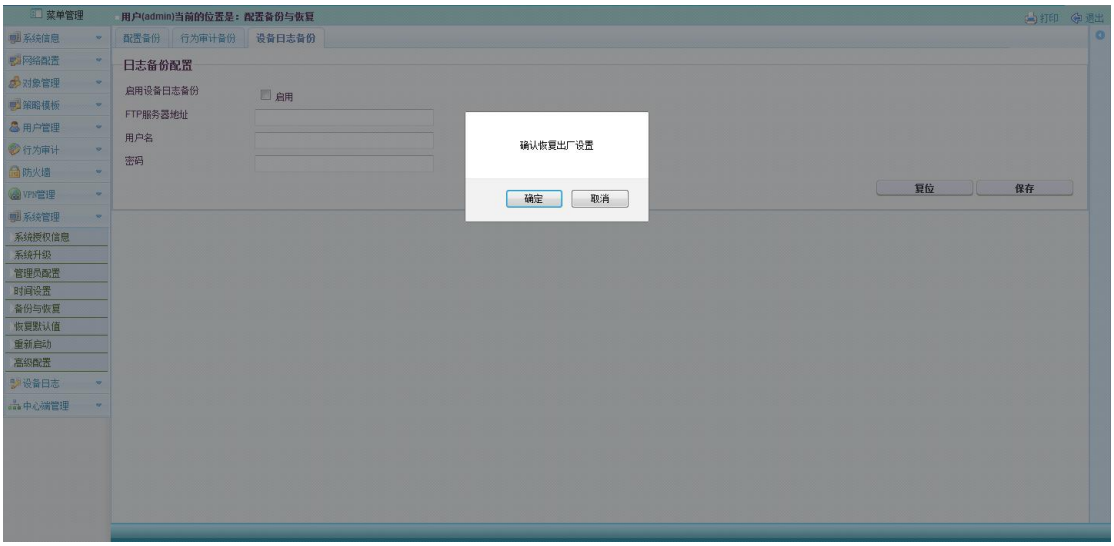
设置行为审计备份：


菜单管理
用户(admin)当前的位置是：配置备份与恢复
打印
退出
系统信息
网络配置
对象管理
策略模板
用户管理
行为审计
防火墙
VPN管理
系统管理
系统授权信息
系统升级
管理员配置
时间设置
备份与恢复
恢复默认值
重新启动
高级配置
设备日志
中心端管理
配置备份
行为审计备份
设备日志备份
行为审计备份配置
行为审计备份
启用
FTP服务器地址
用户名
密码
复位
保存

设置日志备份：

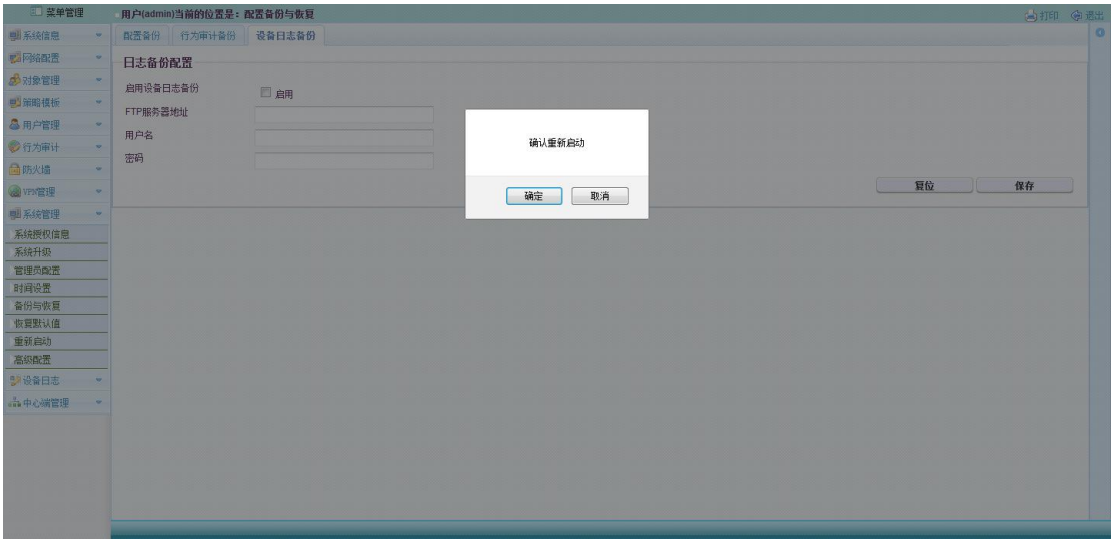

菜单管理
用户(admin)当前的位置是：配置备份与恢复
打印
退出
系统信息
网络配置
对象管理
策略模板
用户管理
行为审计
防火墙
VPN管理
系统管理
系统授权信息
系统升级
管理员配置
时间设置
备份与恢复
恢复默认值
重新启动
高级配置
设备日志
中心端管理
配置备份
行为审计备份
设备日志备份
日志备份配置
启用设备日志备份
启用
FTP服务器地址
用户名
密码
复位
保存

2.12.6 恢复默认值



出厂设置按钮能用来清除所有的配置信息和恢复视频安全接入系统的出厂设置。点击“恢复默认值”系统会弹出一个提示询问是否确定要回复设置到默认值。点击“确定”按钮继续，然后进入到另一个页面并显示系统正在恢复和系统正在重启。

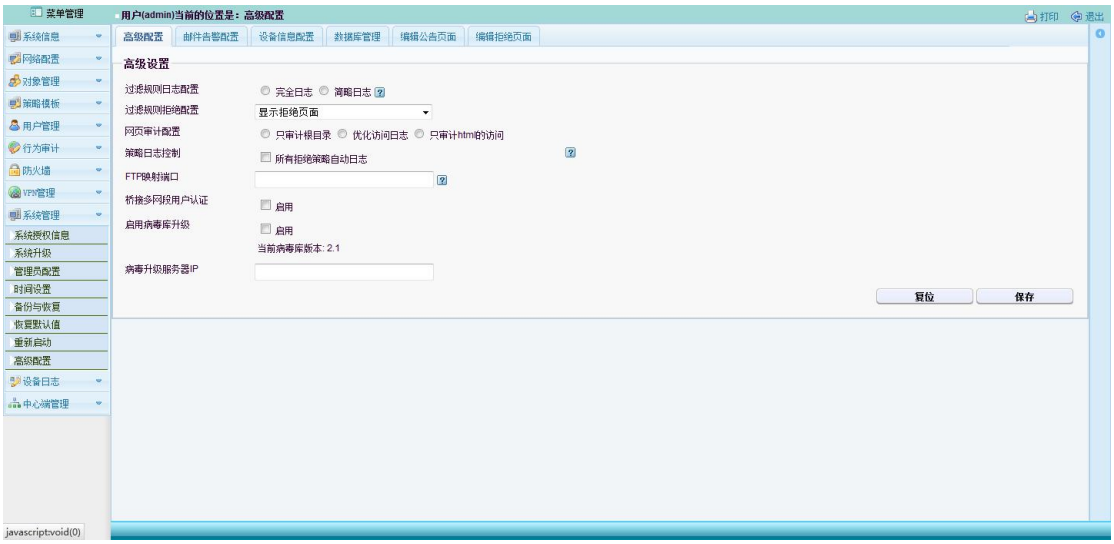
2.12.7 重新启动



重新启动按钮能在 web 页面重新启动系统，方便管理。点击“确定”按钮继续，然后进入到另一个页面并显示系统正在重启。

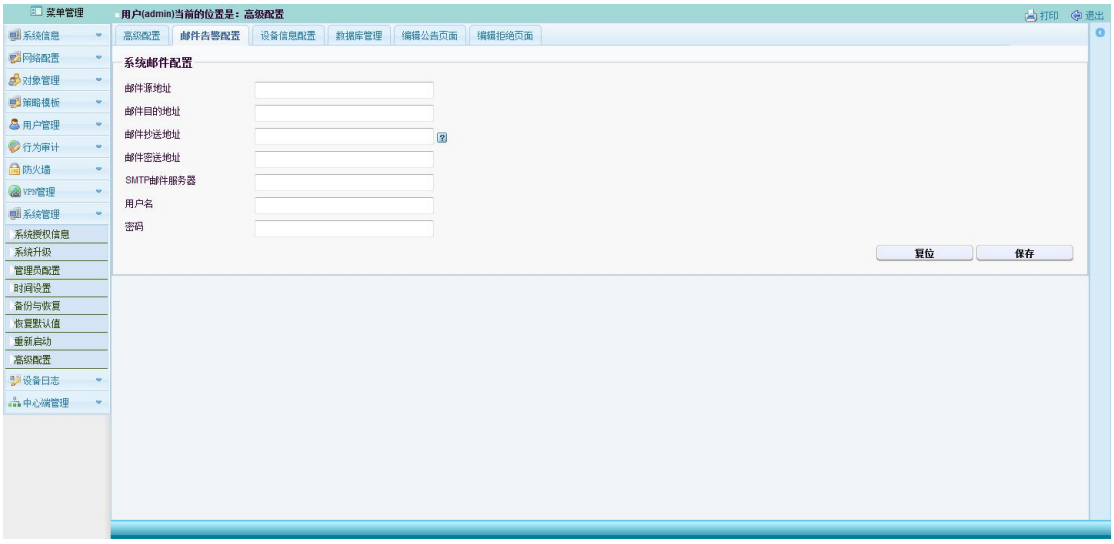
2.12.8 高级配置

高级配置分为高级配置选项，在前面的相关配置中已有介绍，用户一般无需修改。



邮件告警配置：

系统告警和策略告警都需要配置邮件发送信息。

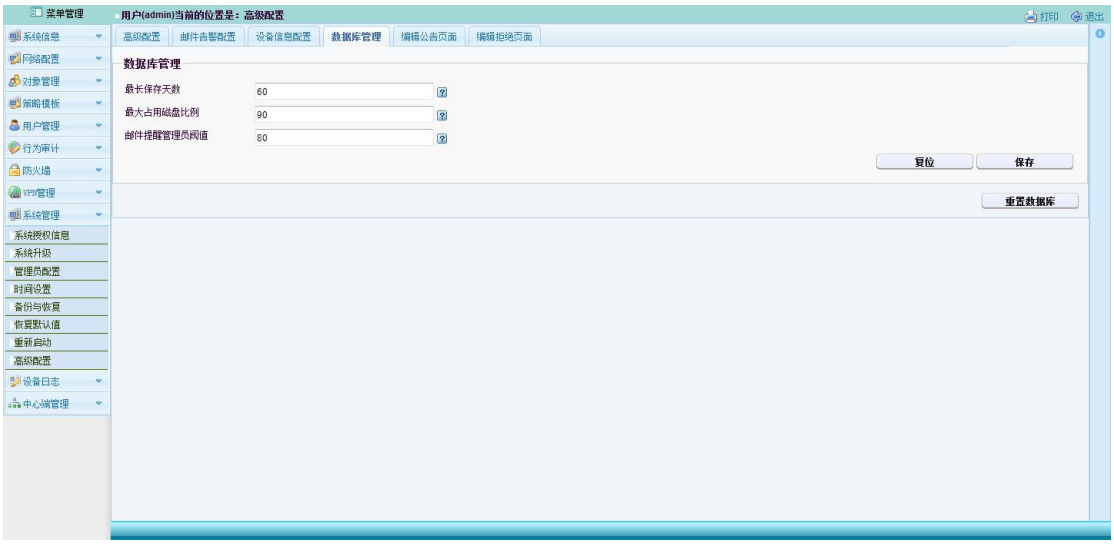


设备信息配置：

视频安全接入系统支持中心端管理，此时需要在设备信息配置里如果设备的一些基本信息，和中心端的 IP。中心端设备就可以对此设备进行管理。

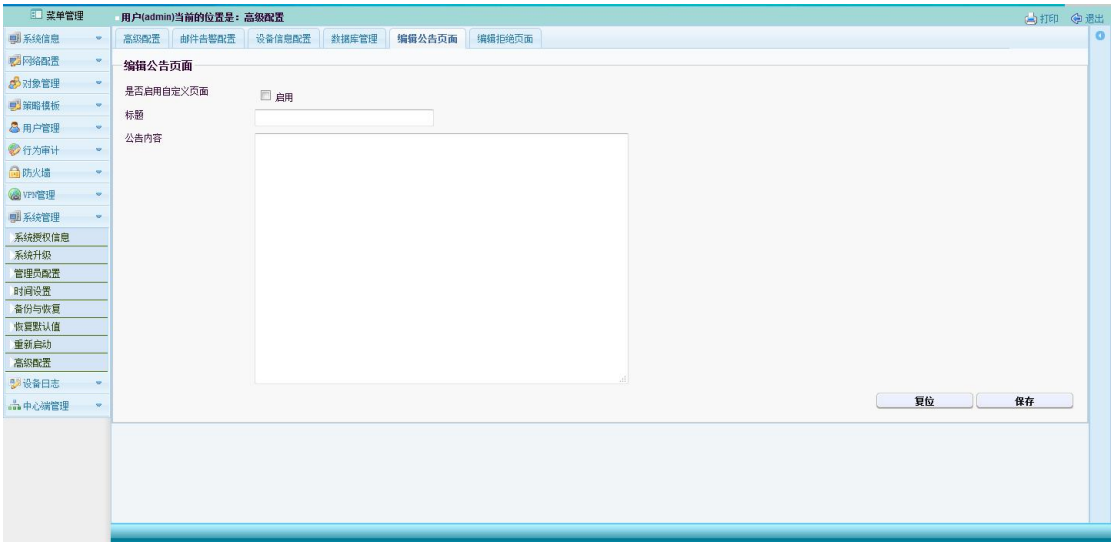
数据库管理：

在此页面可以对数据库进行管理操作。

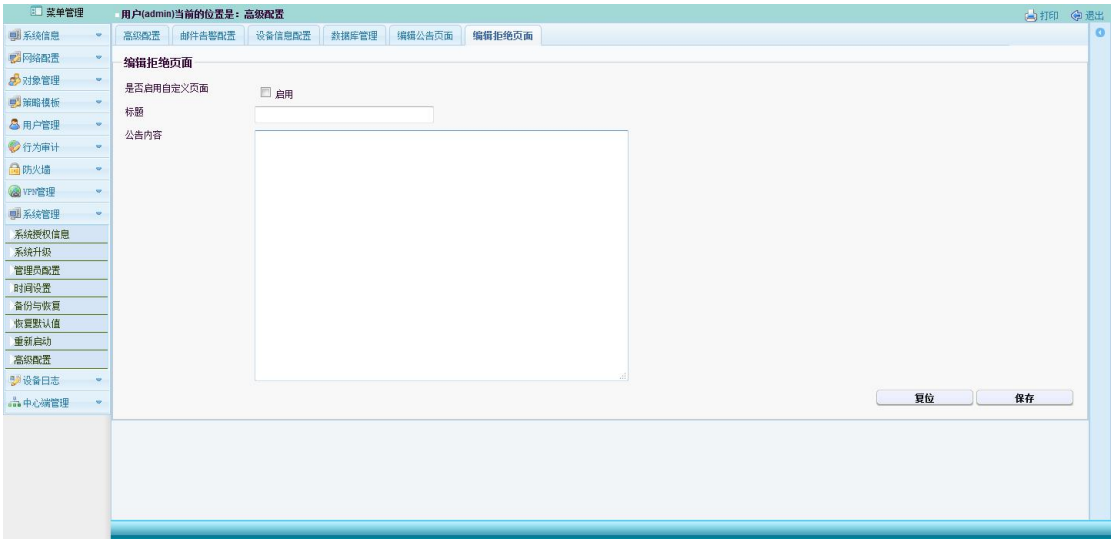


编辑公告页面：

此页面用来编辑公告信息。



编辑拒绝页面：



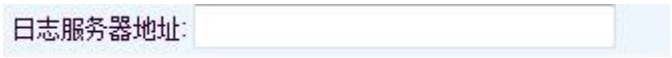
2.13. 设备日志

设备日志是指管理员操作日志，设备开关机日志，系统报警日志，软件的运行日志等。

2.13.1 日志配置

视频安全接入系统设备的日志支持上传功能，上传方式有多种，包括 SYSLOG,邮件，SNMPTRAP 等。这里可以配置什么类型的日志上传，通过什么方式上传。

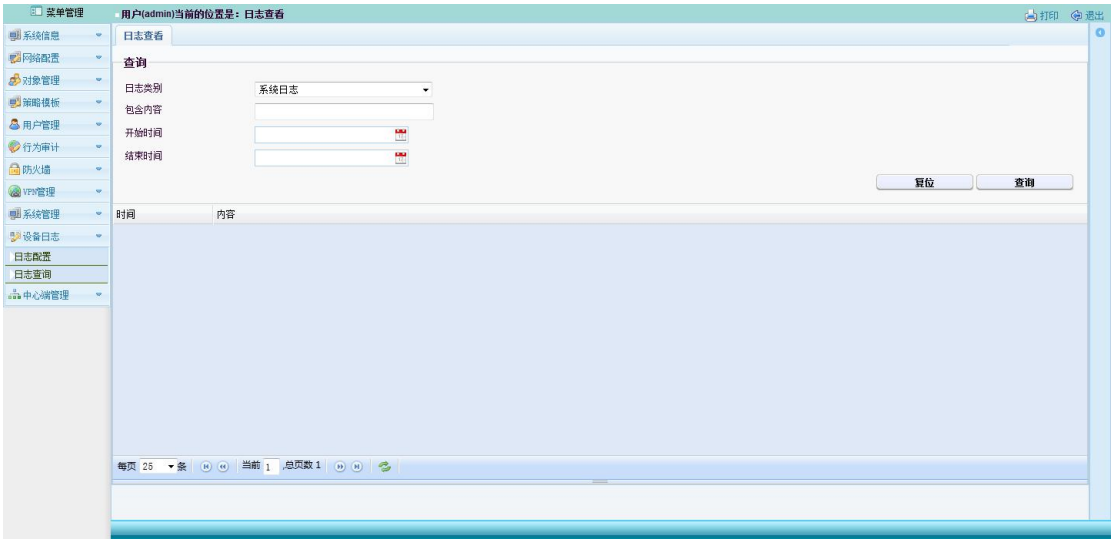
SYSLOG 上传配置： SYSLOG 服务器地址。



- 邮件上传配置:【系统管理】->【高级配置】->〖邮件告警配置〗
- SNMPTRAP 配置: 【网络配置】->【SNMP 配置】->〖SNMPTRAP 配置〗

2.13.2 日志查询

查询系统日志，操作日志，告警日志，和 VPN 的日志。



第三章 故障维修

当您安装或运行视频安全接入系统时发生了问题，请参考以下所提供的解决方法。阅读下面的说明，如果您不能在这里找到回答，请联系我们。

1. 无法开机：请检查是否接通电源。面板开关和电源开关是否打开。

2. 无法登录管理界面：请确认连接端口是否为可信端 NIC0 口，登录方式是否使用“https”IP 地址配置是否正确。

3. 如何将视频安全接入系统恢复出厂设置：登录管理界面，在“系统管理”选项，选择“恢复默认值”。

4. 网络接口指示灯不亮：请检查网络是否正常。交换机运行可能不正常，请试着把网线插到交换机的其它接口，或者插到另一台交换机上。