WFilter-NGF 上网行为管理系统

产品白皮书

目录

1 产品概述

“WFilter 上网行为管理系统”（简称 WFilter NGF）是基于 Linux 的上网行为管理系统、下一代防火墙。无需安装客户端即可实现全网的上网行为管理，而且自带高性能防火墙，保护局域网网络安全。

自 2004 年起，我公司一直专注于上网行为管理领域十余年，自主研发的 WFilter 系列产品（上网行为管理软件、上网行为管理系统、上网行为管理硬件），在产品的功能、性能和细节都远远超过同类产品。

2 为什么选择 WFilter NGF 行为管理系统？

- ✧ 专注于上网行为管理十余年，功能和性能远超同类产品。
- ✧ 上网行为管理、流控、防火墙、入侵防御、VPN 等 N 合一。
- ✧ 友好的 Web 界面，无需专业技术即可操作使用。
- ✧ 强大的实时管控功能，每一个上网连接都可视可控。
- ✧ 为上网行为管理而生，支持多种管控手段，可以基于 IP、MAC、域账号进行记录和管控。
- ✧ 特色功能：上网记录，AD 域集成，千万级网址库，详尽的统计报表。

3 WFilter NGF 给用户带来的价值

3.1 保护信息安全

WFilter NGF 可以对上网内容进行监控审计，可以提供上网记录、流量统计、SSL 解密等功能：

1. 支持记录多种上网内容，包括网页浏览记录、邮件记录、论坛发帖等。
2. SSL 拦截解密，可以截获 SSL 邮件、HTTPS 网页内容。
3. 详细的统计报表，多种预置报表模版。

WFilter NGF 还支持“DDOS 防护”、“入侵防御”等网络安全防护功能，可以阻止来自内外网的网络攻击，从保障内网的网络信息安全。

3.2 提高工作效率

WFilter NGF 的上网行为管理模块，提供了企业级的上网行为管理：

1. 支持多种管控手段，可以基于网段、IP 地址、账号、MAC 地址设置策略。
2. 多种上网认证方式，支持 AD 域、Web 认证、Radius 认证等方式。
3. 千万级网址库，支持 60 余种网站分类，满足各类管理需要。
4. 全面、精准的协议识别，可以完全禁止迅雷、bt 等复杂的 P2P 协议，支持两千余种常见协议。

3.3 优化网络带宽

WFilter 上网行为管理系统集成了一系列的方案来帮助您优化局域网的上网带宽，包括：带宽优化模块，IP 限速模块，多线均衡模块，上网行为管理。您可以做到：

1. 根据需要申请多条外线，并且启用多线均衡模块来进行分流和负载均衡。
2. 利用带宽优化模块来处理业务的优先级，使业务数据和 VIP 数据优先通过，并且设置 P2P、视频、下载为较低的优先级。
3. 有需要的话，按部门进行带宽分配。使各部门之间不互相影响。
4. 配置上网行为管理策略，工作时间段禁止 P2P 下载和在线视频，节省带宽资源。

3.4 虚拟远程组网

WFilter 上网行为管理系统集成了 SD-WAN、IPSec、SSL VPN、WebVPN、PPTP 等多种虚拟组网和远程办公拨入方案，可以通过互联网组建安全高效的虚拟局域网，使您能快捷方便的搭建异地办公、在家办公环境。

4 功能简介

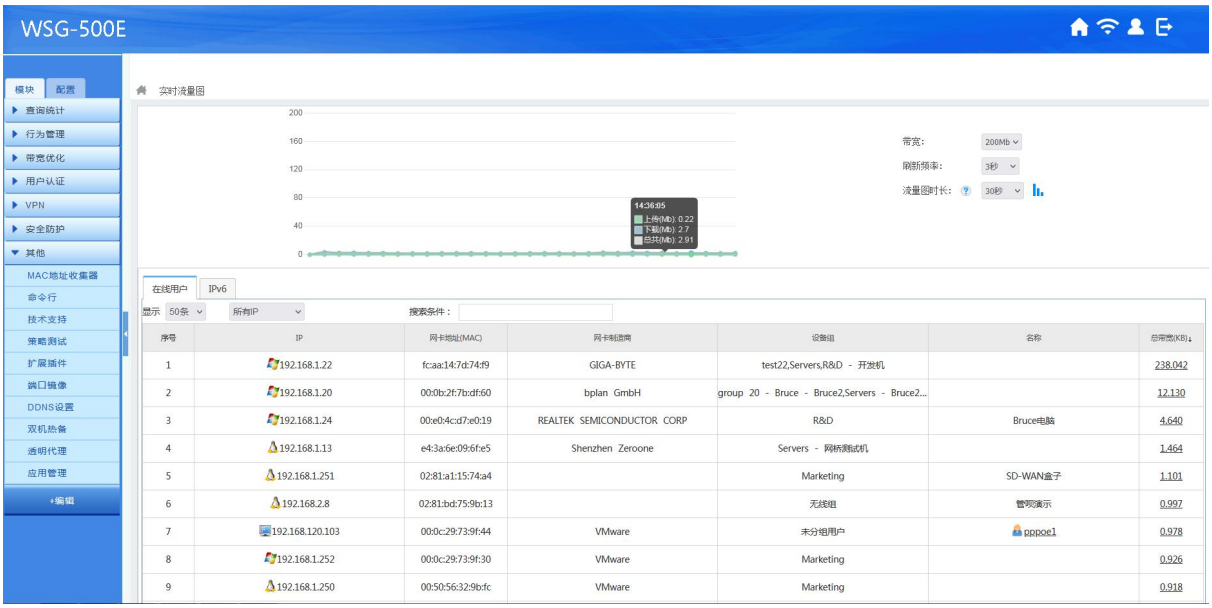
4.1 实时检测和控制

- ✓ 强大的实时监视和控制，所有连接尽在眼底。
- ✓ 显示客户机的 IP/MAC/账号信息，操作系统类型。

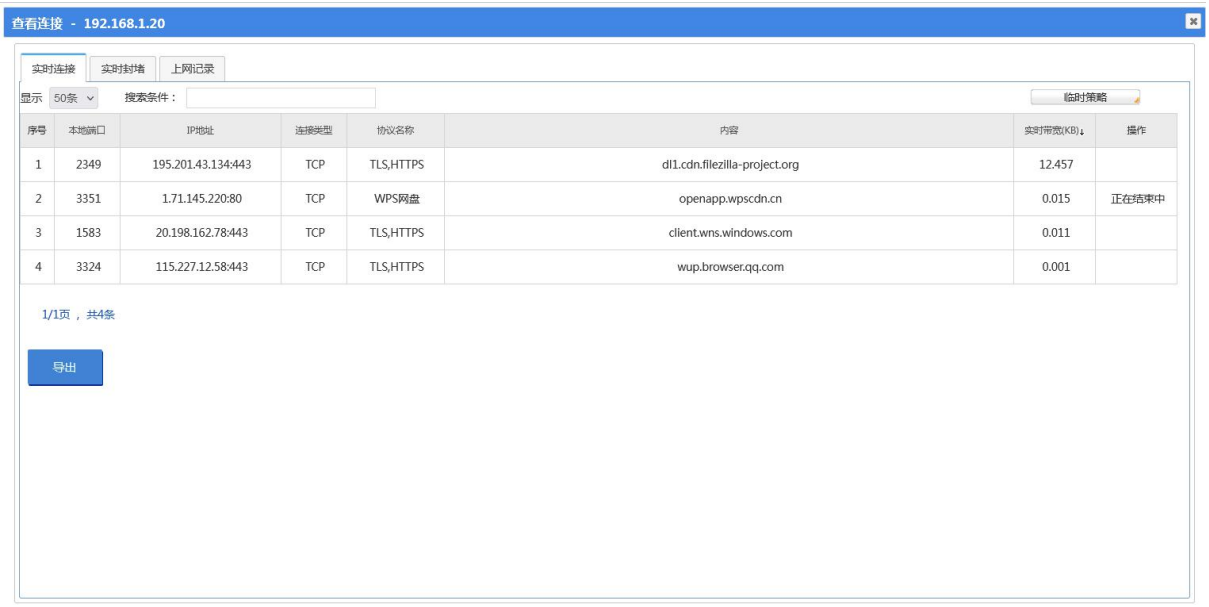
✓ 实时带宽检测和连接监控，并且可以显示域名、QQ 号等信息。

✓ 一键断开连接，设置惩罚策略。

4.1.1 在线设备列表



4.1.2 查看设备的实时链接



4.1.3 断开链接和设置惩罚策略

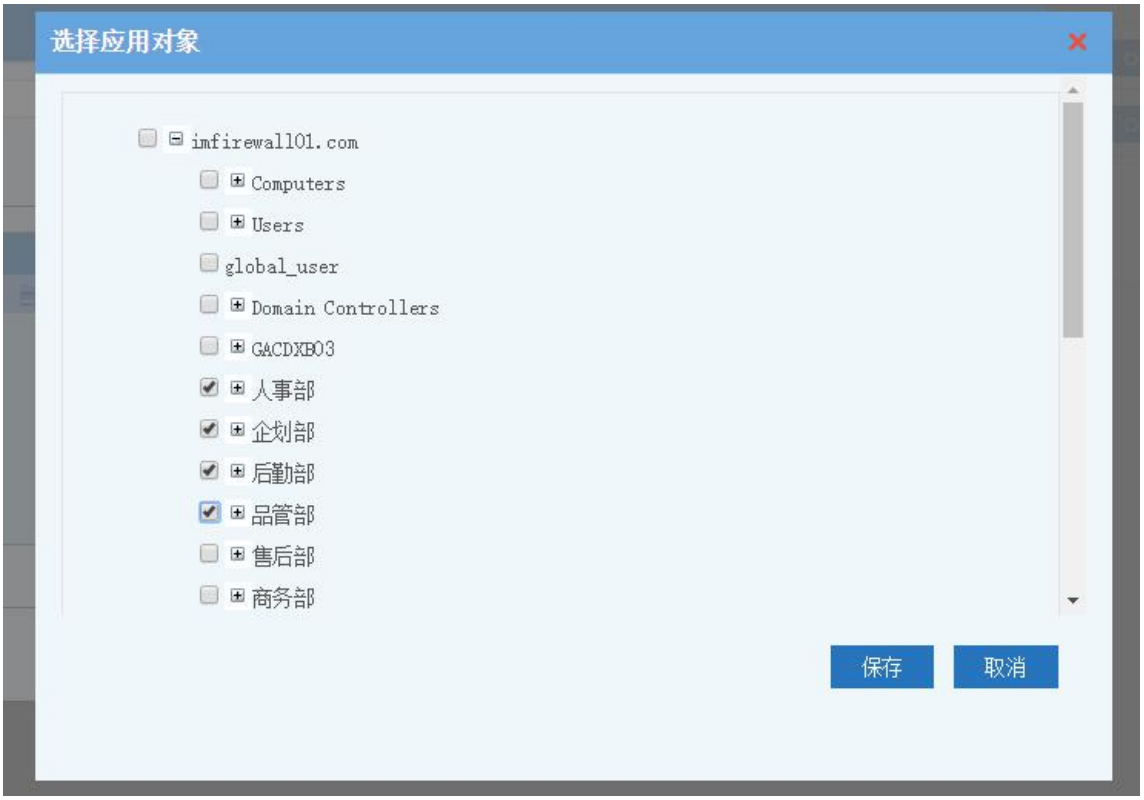
4.2 上网行为管理

- ✓ 网页过滤、应用过滤、IP-MAC 绑定、网页推送、聊天过滤等。
- ✓ 支持多种管控手段，可以基于网段、IP 地址、域账号、MAC 地址设置策略。
- ✓ 多种上网认证方式，支持短信实名认证，AD 域、Web 认证、Radius 认证等方式。
- ✓ 可以和 AD 域集成，基于域账号记录和设置上网策略。
- ✓ 千万级网址库，支持 60 余种网站分类，满足各类管理需要。
- ✓ 全面、精准的协议识别，支持两千余种常见协议。

4.2.1 基于用户组、账号设置策略

基于设备组选择应用对象

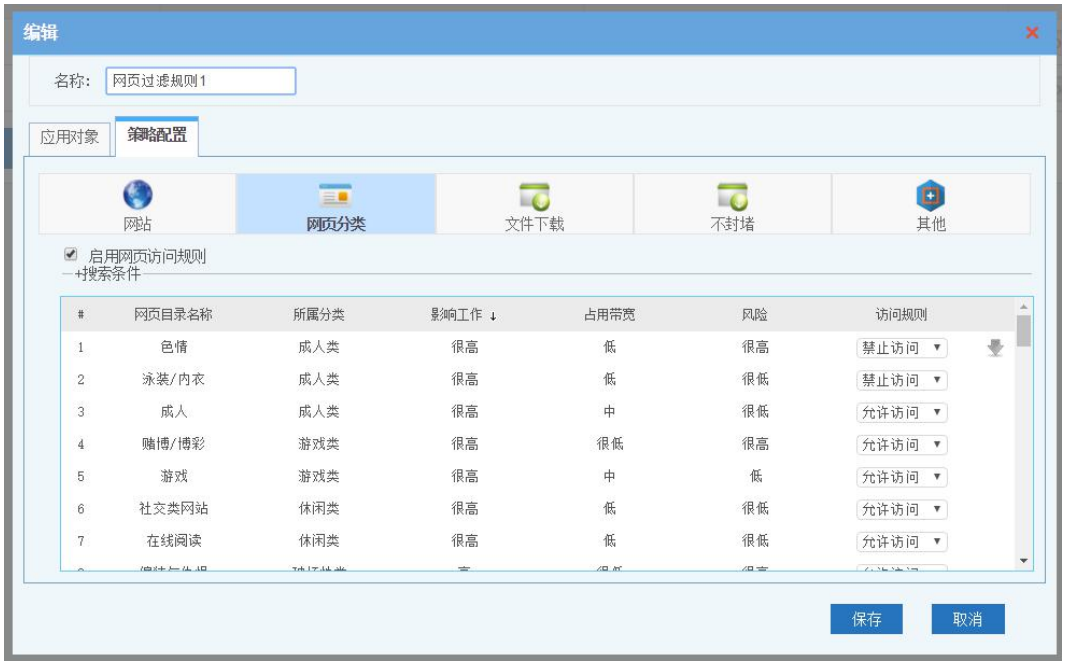
基于账号选择应用对象



时间段配置

4.2.2 网页过滤策略配置

可以基于网站分类进行屏蔽，设置网站黑白名单，根据文件类型屏蔽下载。



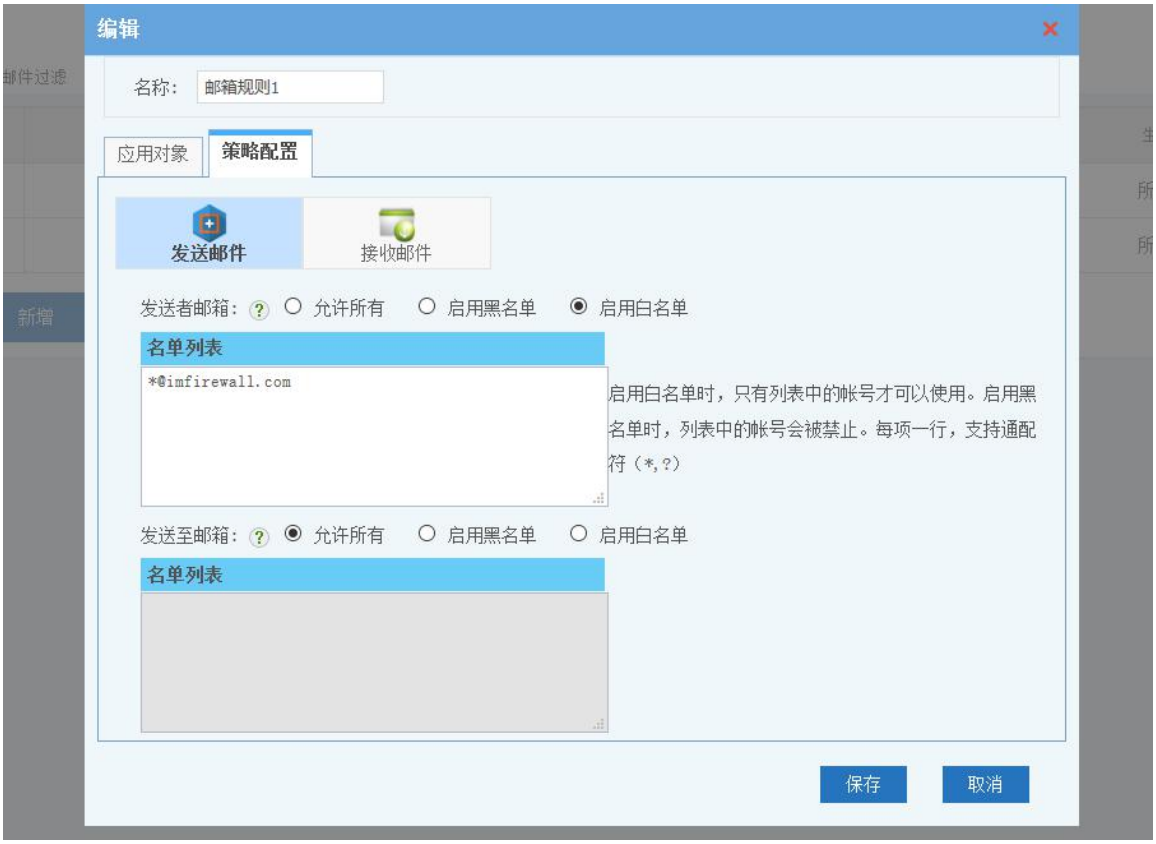
4.2.3 应用过滤策略

4.2.4 SSL 监控

该 SSL 监控模块，可以充当 SSL 的中间人进行证书拦截，从而解析出 SSL 加密的数据内容。

4.2.5 邮件过滤

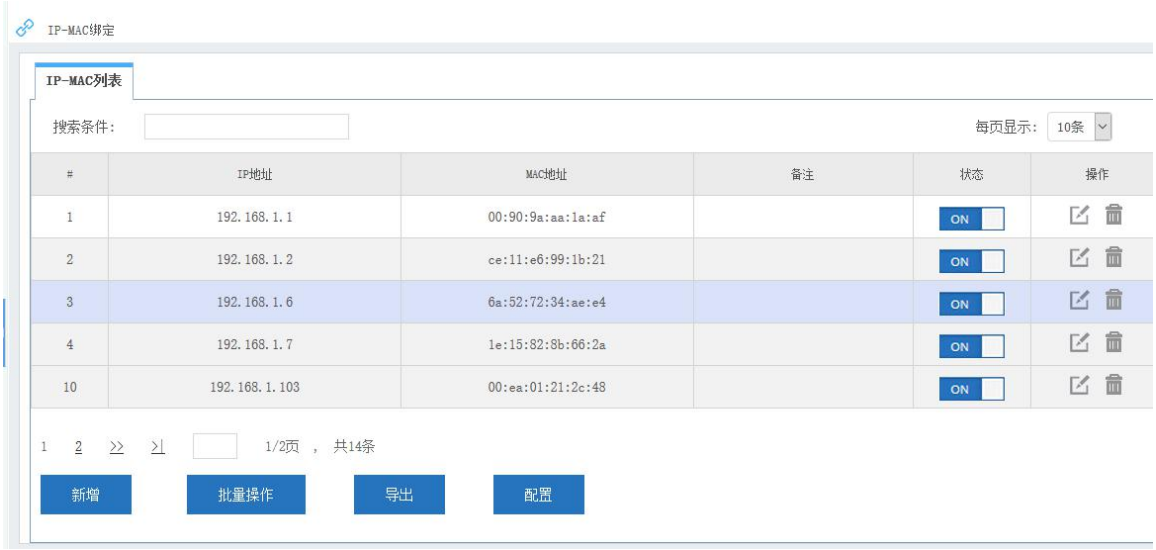
对客户端邮件的发件人、发送至、接收邮箱进行黑白名单过滤。

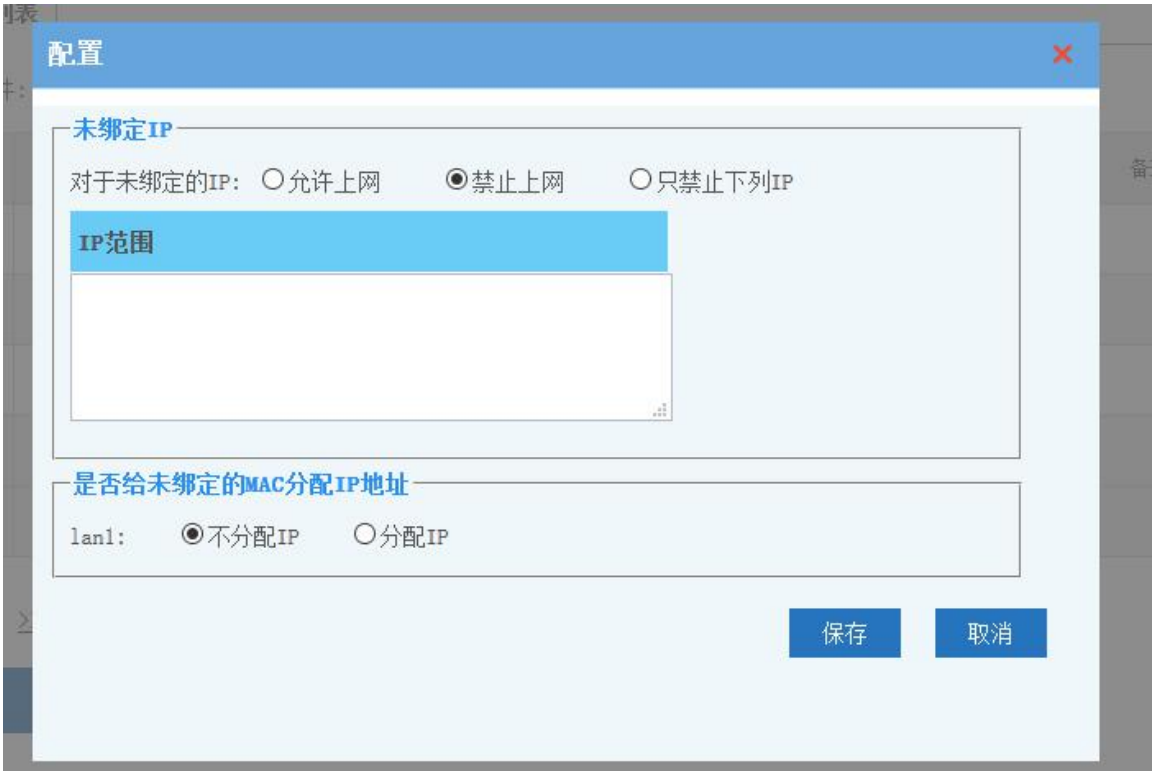


4.2.6 静态 IP 分配，IP-MAC 绑定

专业的 IP-MAC 绑定模块，可以实现如下功能：

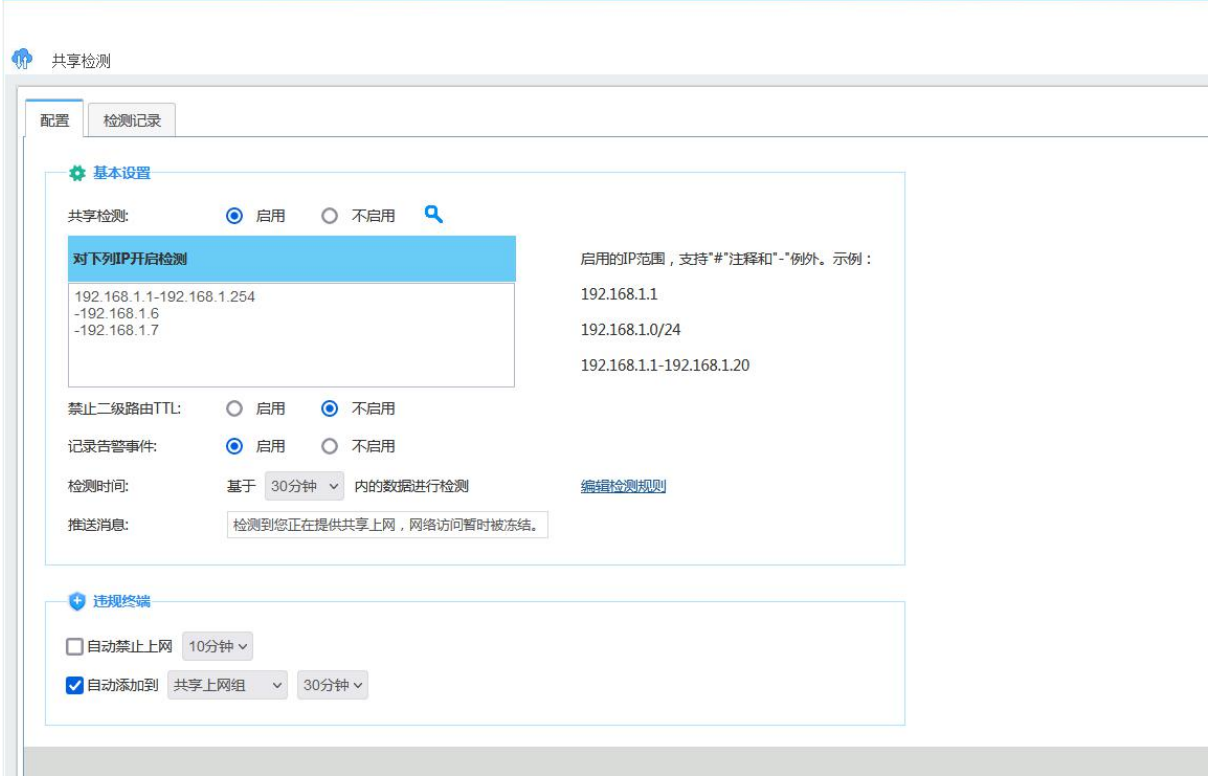
- 静态 IP 地址分配
- 跨网段 IP-MAC 绑定
- 网桥模式下的 IP-MAC 绑定和静态地址分配
- 没有绑定条目数的限制，可以实现海量绑定



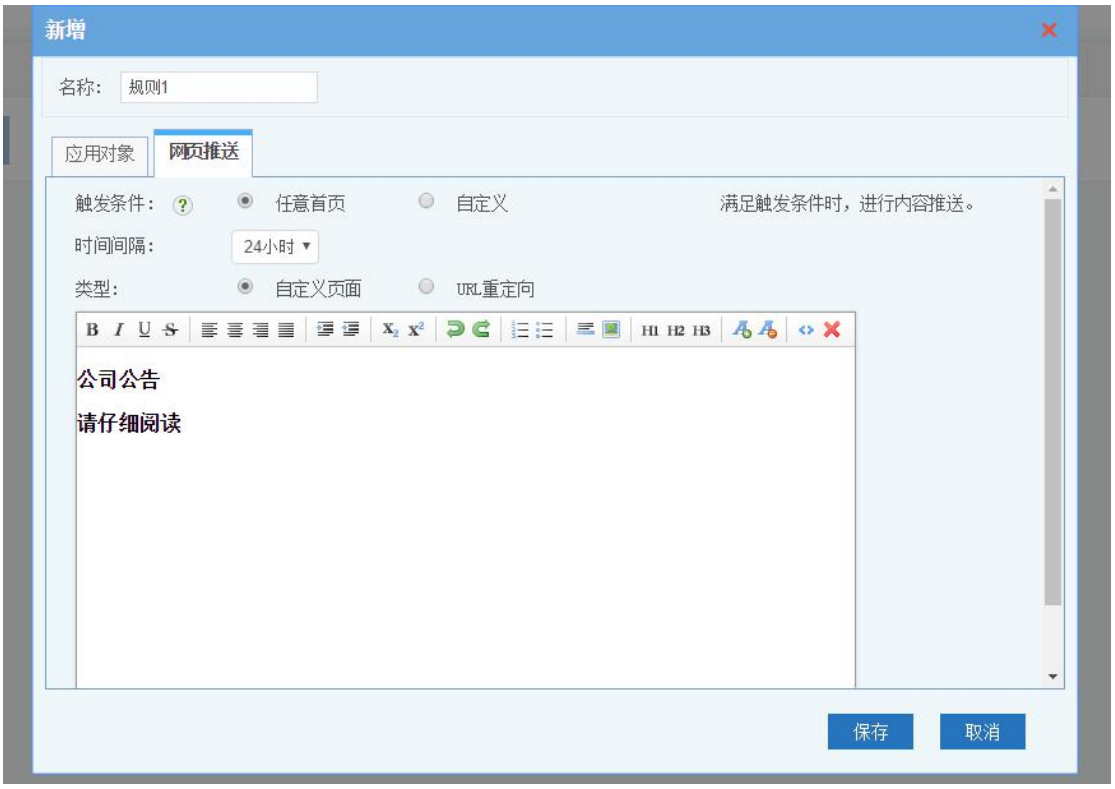


4.2.7 共享检测

共享检测模块可以检测局域网内的网络共享服务，包括二级路由、随身 WiFi 等网络共享行为。并且可以对发现的违规设备设置禁止上网等惩罚策略。



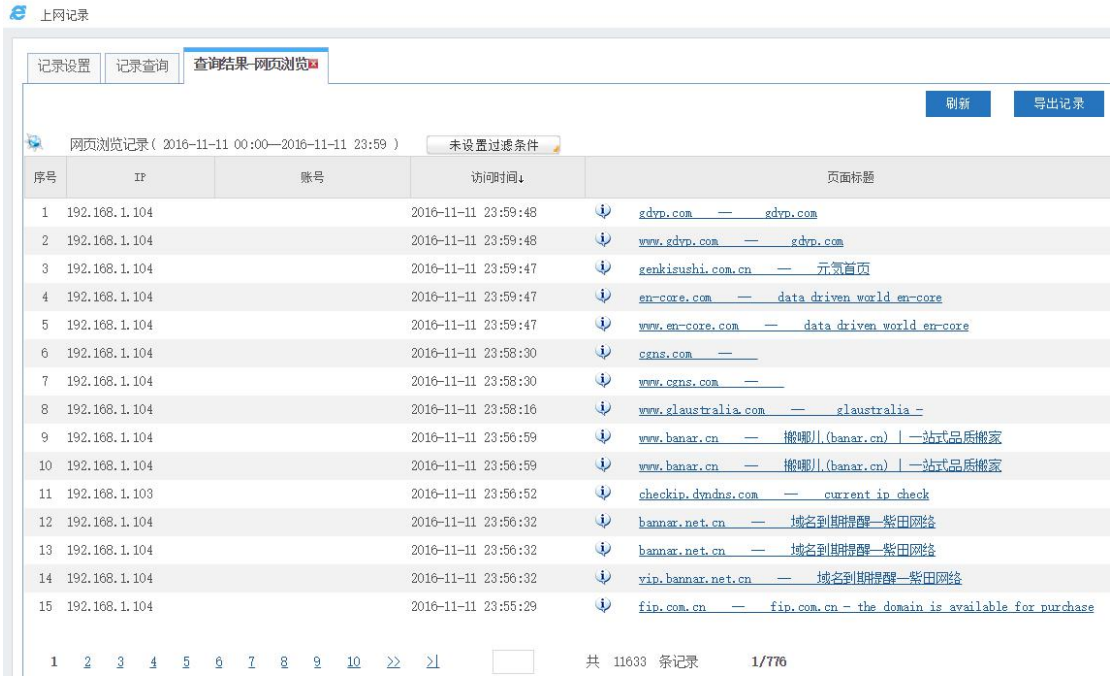
4.2.8 网页推送



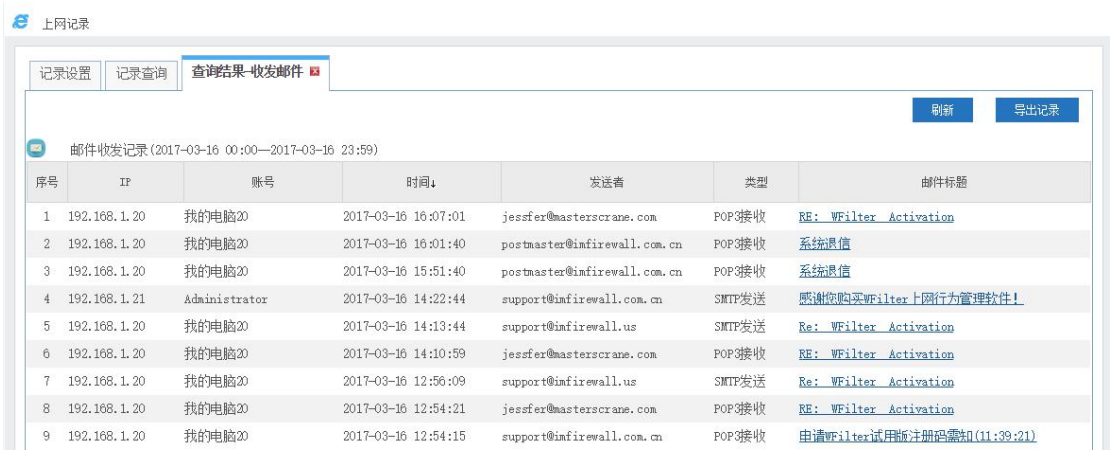
4.3 上网内容监控审计、统计报表

- ✓ 支持记录多种上网内容，包括网页浏览、邮件记录、文件传输、论坛发帖等。
- ✓ SSL 拦截解密，可以截获 SSL 邮件、HTTPS 网页内容。
- ✓ 详细的统计报表，多种预置报表模版。

4.3.1 网页浏览历史



4.3.2 收发邮件监控



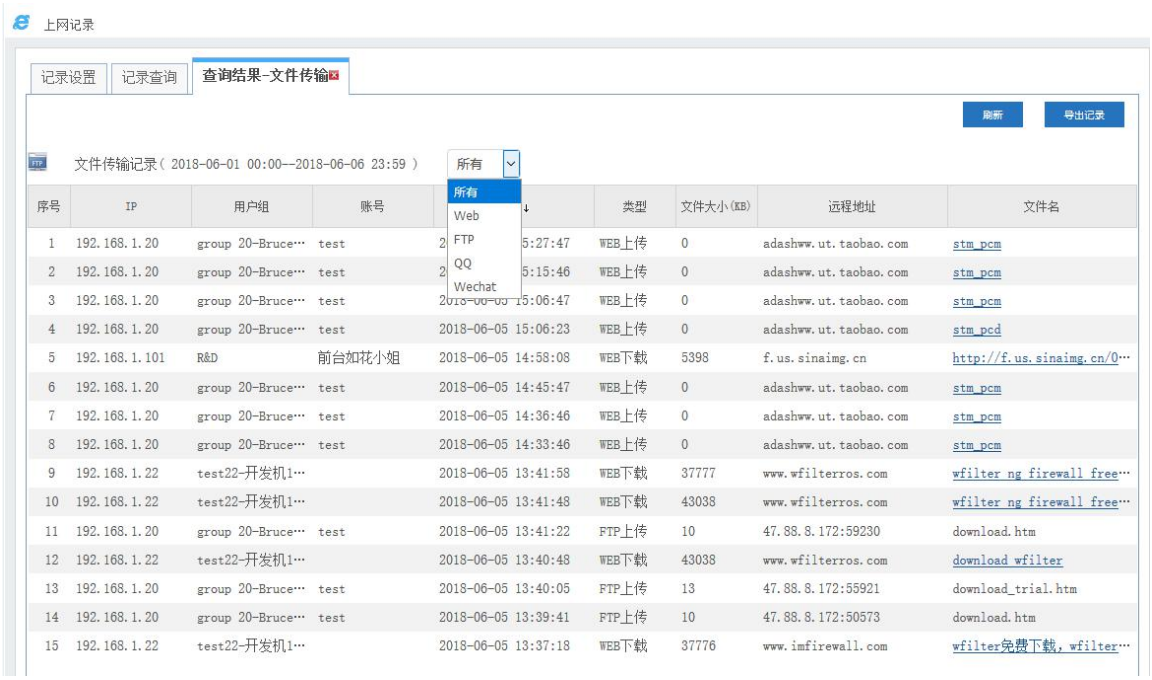

查看邮件内容
导出记录
发件人：
support@imfirewall.com.cn
日期：
Thu, 16 Mar 2017 11:39:21 +0800
收件人：
抄送：
邮件标题
申请WFilter试用版注册码需知(11:39:21)
附件：
内容：
您好：
感谢试用WFilter（超级嗅探狗）。
在申请试用版注册码前，请先查看WFilter的“系统配置”---“配置检测” 里面“监听网卡”的检测结果。
如果检测结果是“只能监控到自己” 那说明软件没有部署成功，那么试用版注册码没有任何用处，请和我们在线技术支持联系。我们会根据您的网络结构，提供一个最佳的部署方案，从而让软件实现监控，并提供试用版注册码，供您全面测试。
如果您的“系统配置”--“配置检测”的监听网卡检测正常，也请和我们在线技术支持联系获取注册码进行全面测试。
技术支持QQ：416537809
技术支持热线：400-018-0186

4.3.3 论坛发帖监控

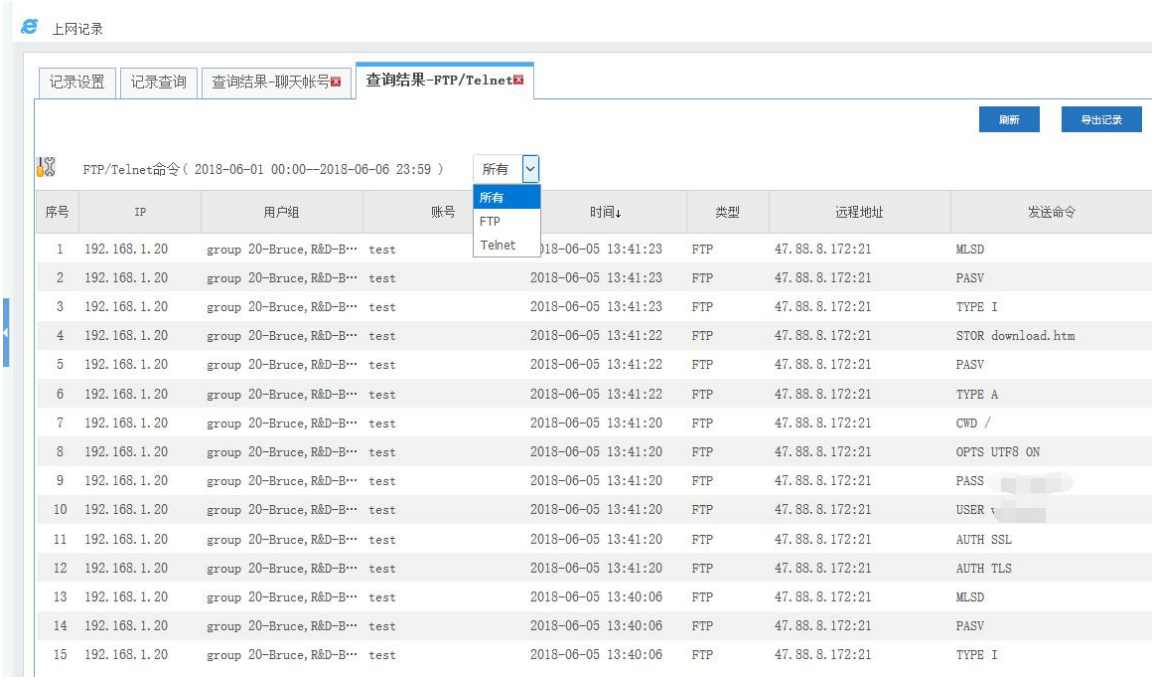

帮助
上网记录
记录设置
记录查询
查询结果-收发邮件
查询结果-网页粘贴
刷新
导出记录
网页粘贴记录(2017-03-16 00:00—2017-03-16 23:59)
未设置过滤条件
序号 IP 账号 访问时间 页面标题 大小(KB)
1 192.168.1.20 我的电脑20 2017-03-16 17:16:54 www.imfirewall.com — 很多客户机的mac地址都监控不到？ - w… 0.27
2 192.168.1.20 我的电脑20 2017-03-16 17:15:48 bbs.tianya.cn — 听伟哥讲《山海经》——讲那个逆天的上古世… 1.33
共 2 条记录 1/1


网页粘贴内容
查看网页粘贴内容
查看原始文件
序号 项目 粘贴内容 长度（B）
链接 听伟哥讲《山海经》——讲那个逆天的上古世界(第17页) 煮酒论史 天涯论坛 天涯社区
1 params.artId 421662 6
2 params.item no05 4
3 params.appId bbs 3
4 params.appBlock no05 4
5 params.postId 421662 6
6 params.preUrl http://bbs.tianya.cn/post-no05-421662-1.shtml 45
7 params.preTitle 听伟哥讲《山海经》——讲那个逆天的上古世界 63
8 params.preUserId 108004514 9
9 params.preUserName 听伟哥讲山海经 21
10 params.prePostTime 1455853800000 13

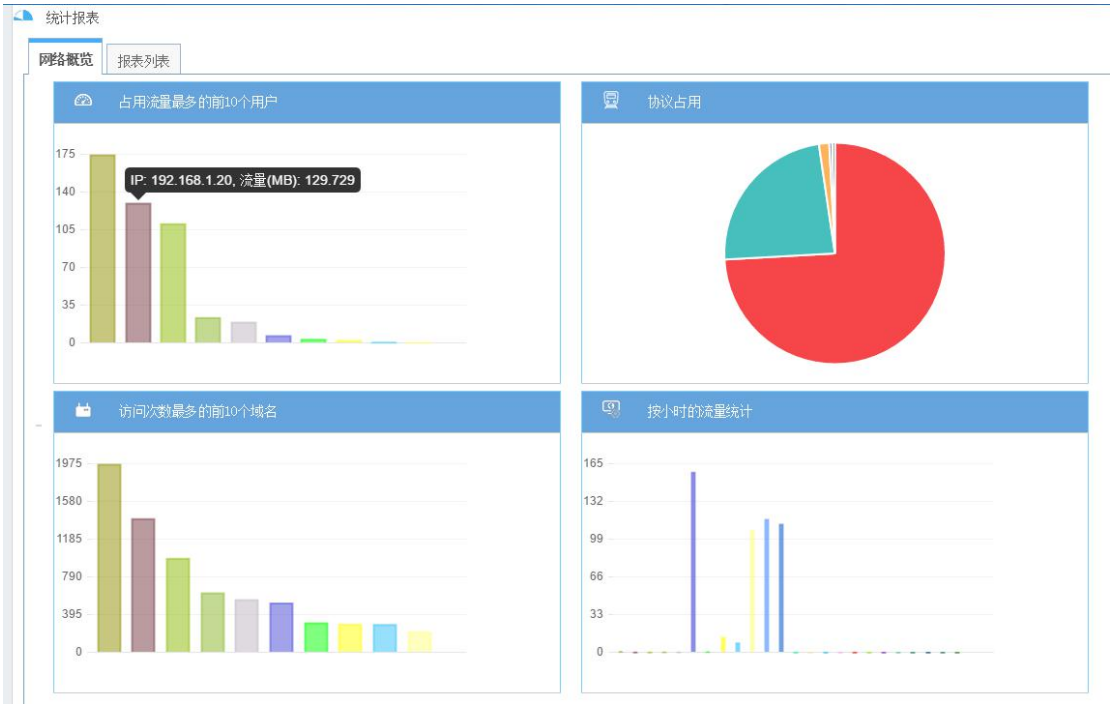
4.3.4 文件传输记录

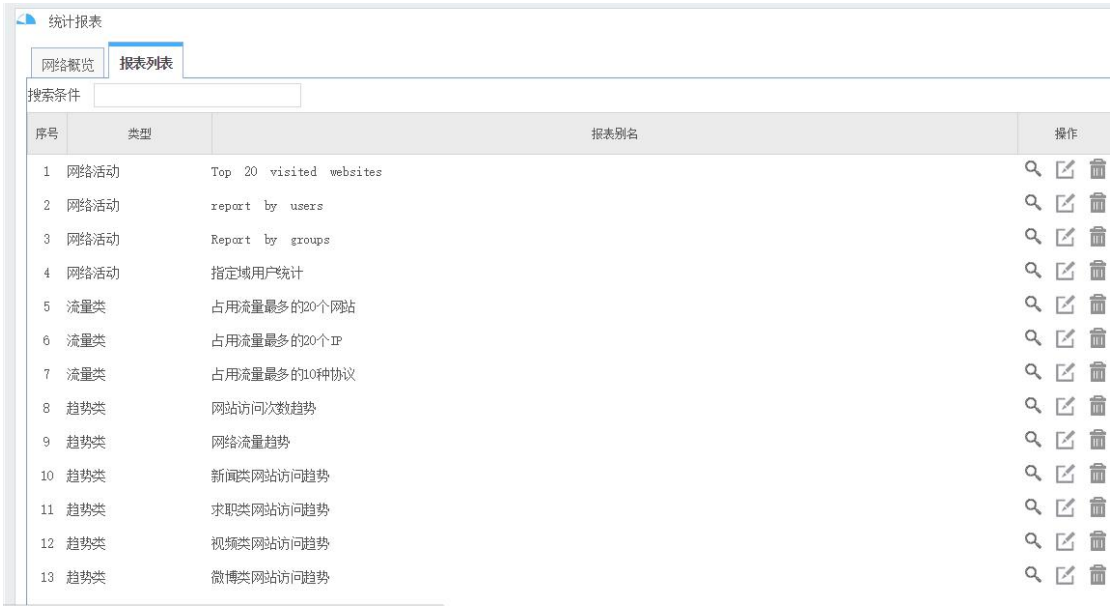


4.3.5 FTP/Telnet 记录



4.3.6 报表概览和列表





4.4 带宽优化

- ✓ 关键数据优先通过，确保业务流量。
- ✓ 基于协议类型设置优先级别，网页、视频互不影响。
- ✓ 多线均衡负载，多线分流。

✓ 基于 IP、用户组、账号进行限速。

4.4.1 带宽优化策略

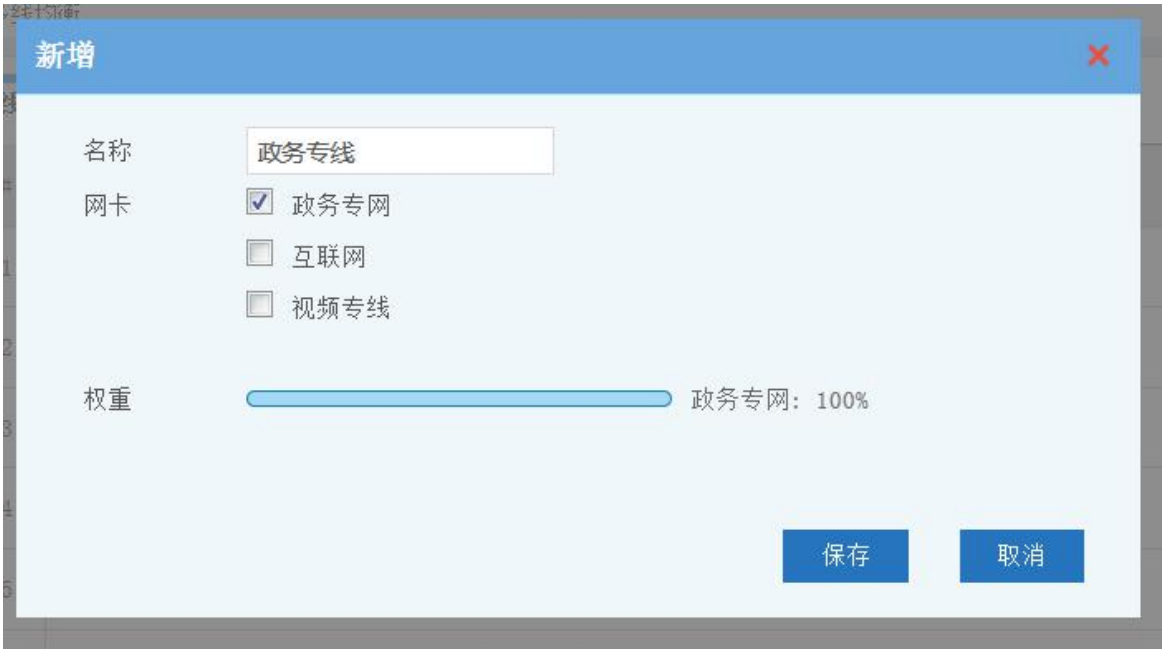
可以配置不同协议、用户组、账号的带宽优先级。

4.4.2 IP 限速策略

基于 IP 段、用户组、账号设置限速，可以同时给组以及组中的成员进行限速。还可以对不同的应用类型、网站类型进行限速。

4.4.3 多线均衡策略

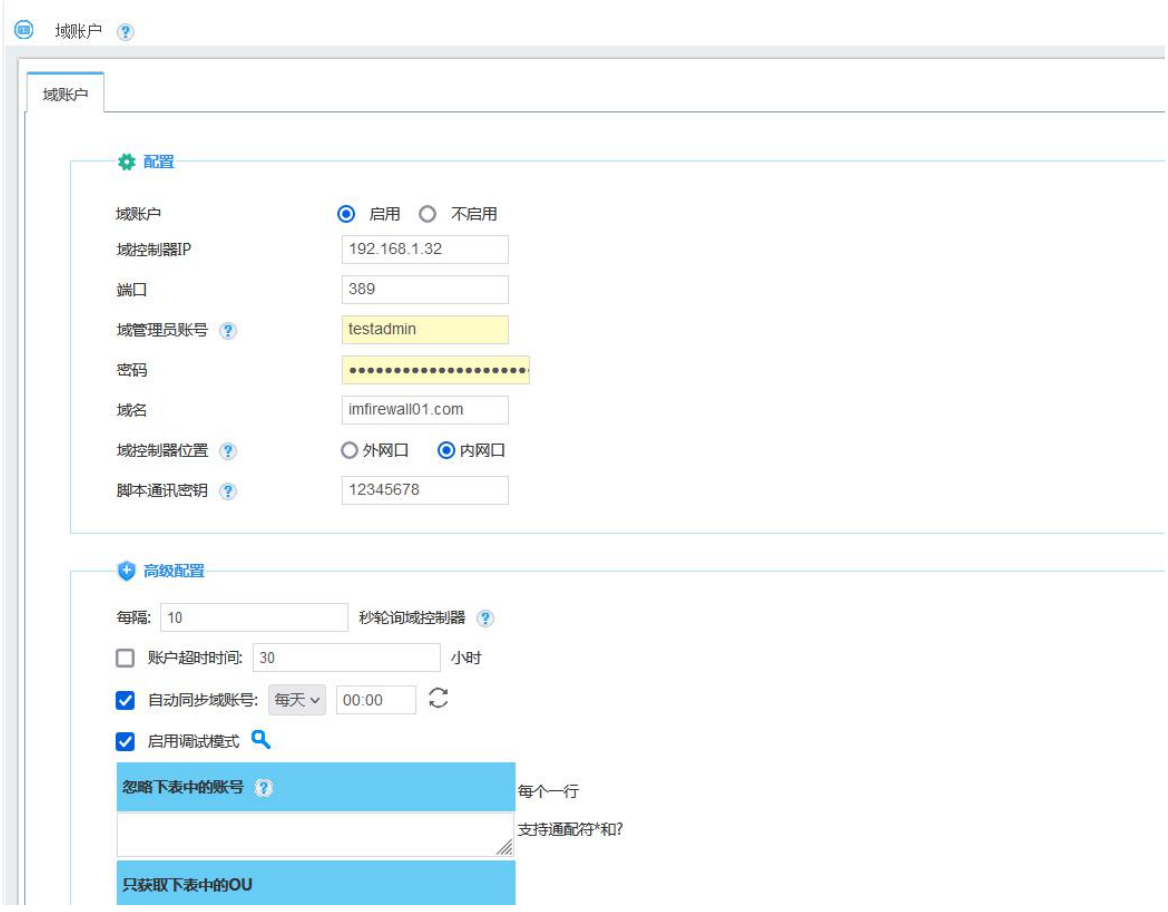
多条外线时，无需配置默认就可以进行运营商分流。您也可以根据需要配置自己的分流策略。可以基于国家地区、网站分类、应用分类来配置分流策略。



4.5 用户认证

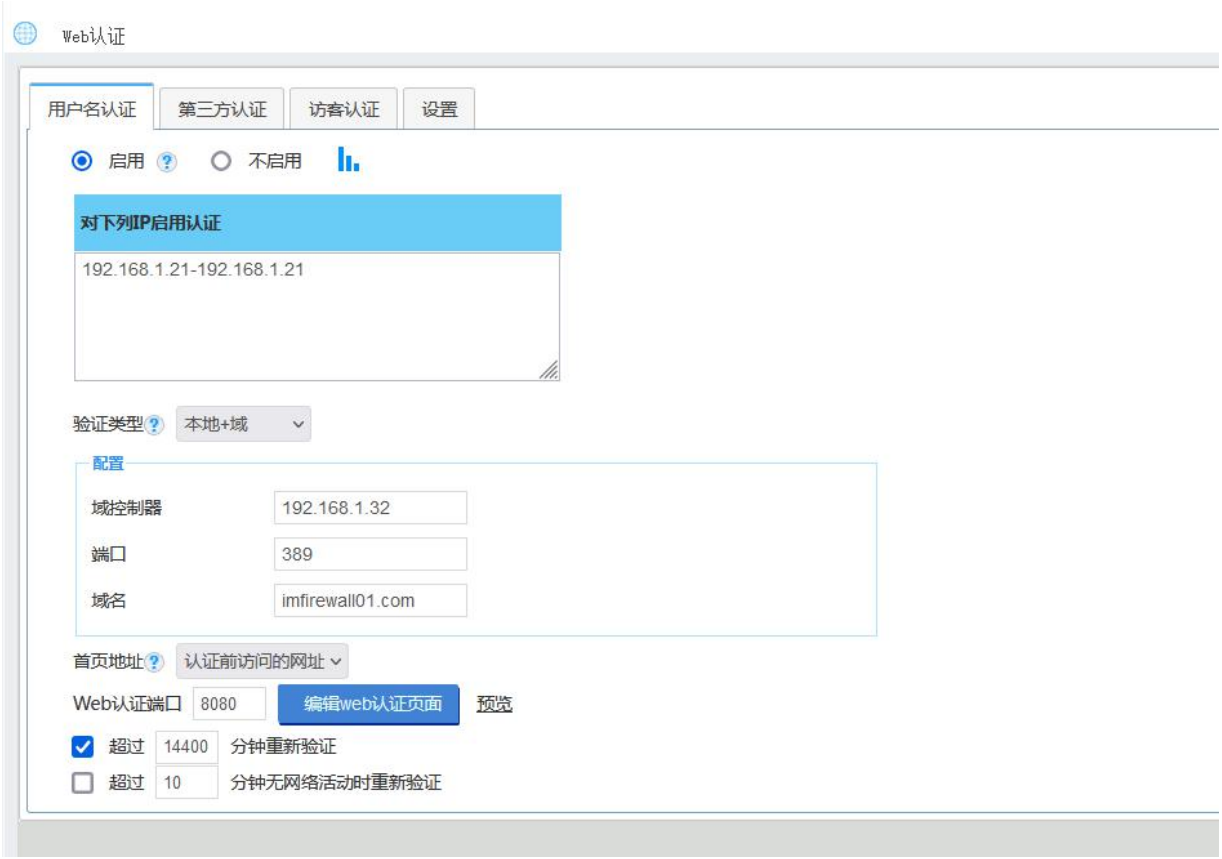
4.5.1 域账号集成

可以和微软的 AD 域集成，基于域账号设置上网策略和记录上网行为。



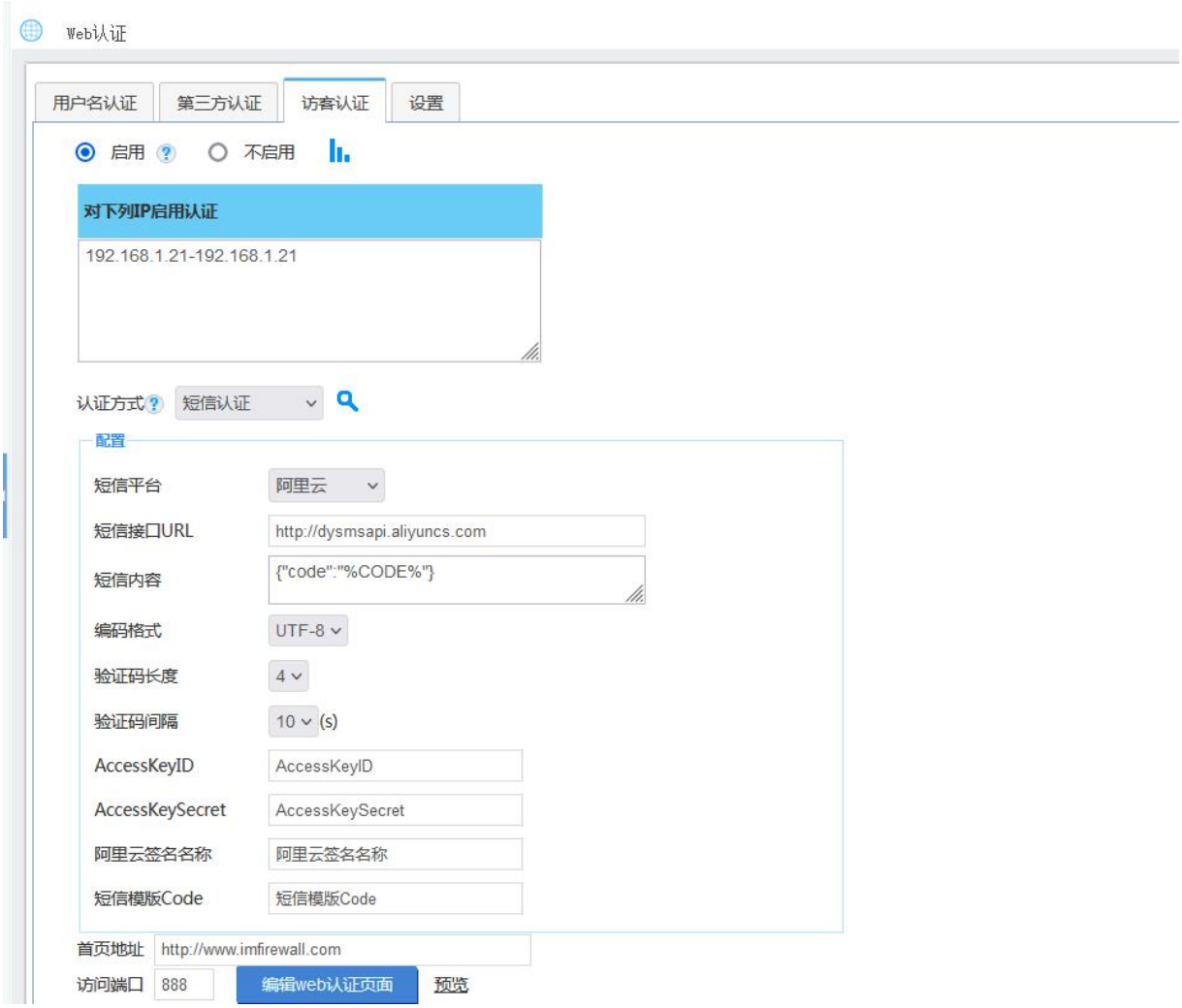
4.5.2 Web 用户名认证

基于用户名的 Web 认证，可以进行本地认证、邮箱认证、LDAP 认证、远程 Radius 认证、混合认证等。



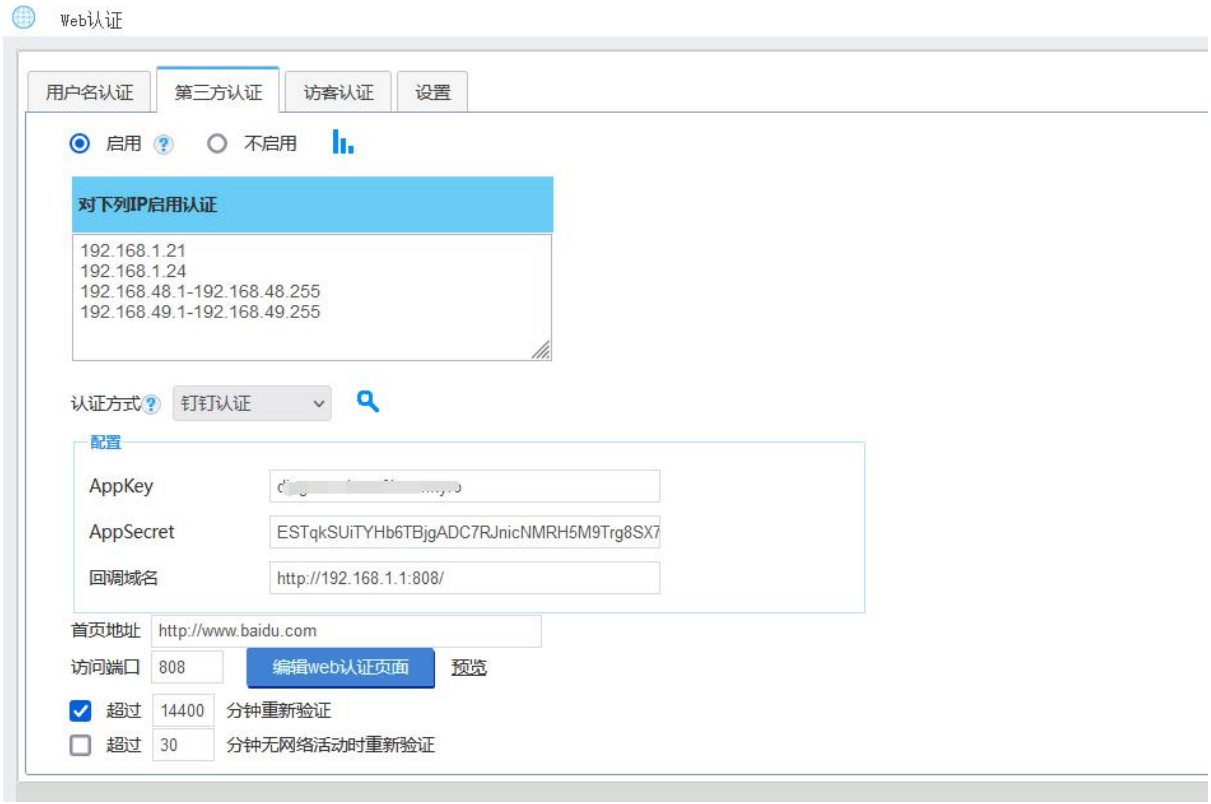
4.5.3 短信认证

输入手机号获取短信验证码后上网，可以和多种短信平台集成。



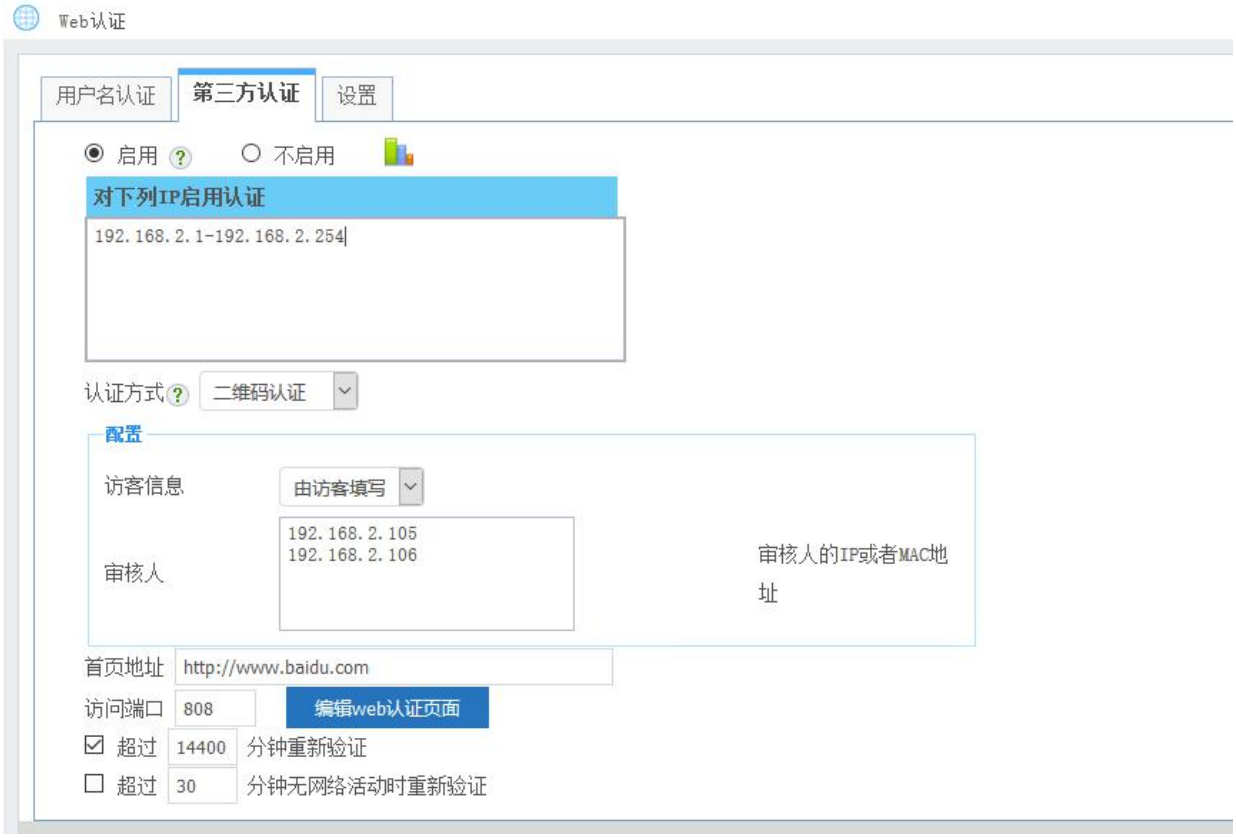
4.5.4 钉钉和企业微信认证

用钉钉或者企业微信扫描二维码进行实名认证。



4.5.5 二维码认证

访客上网需要出示二维码经过审核人的人工审核才能放行。

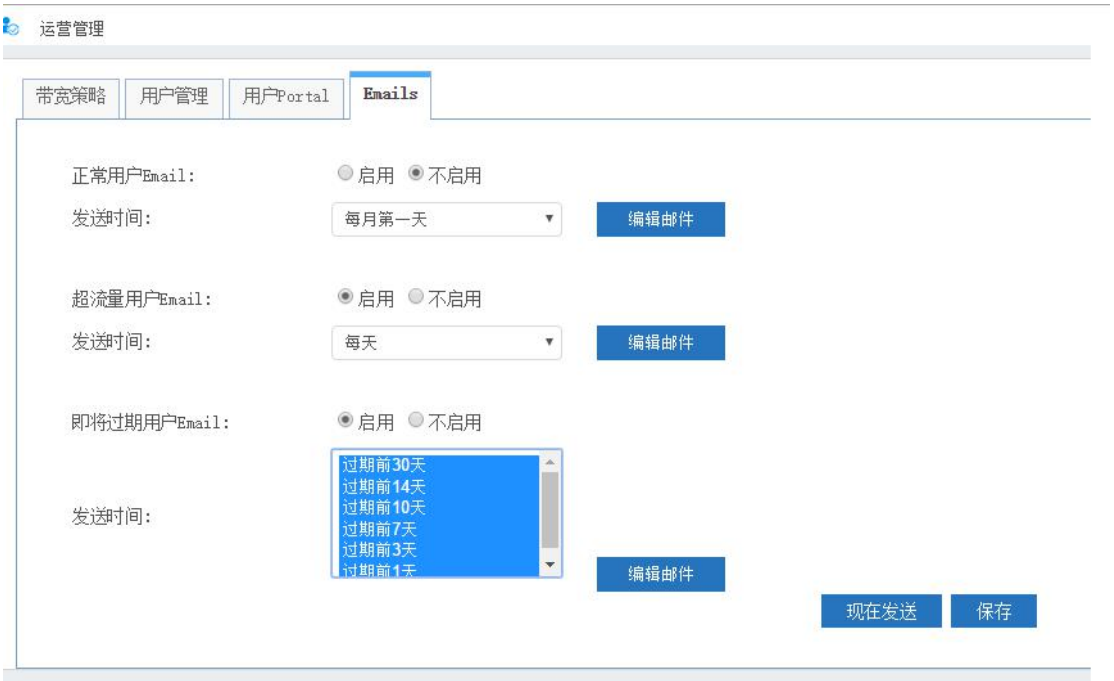


4.5.6 PPPoE 认证

支持建立多个 PPPoE 服务，支持本地认证和远程 Radius 认证。

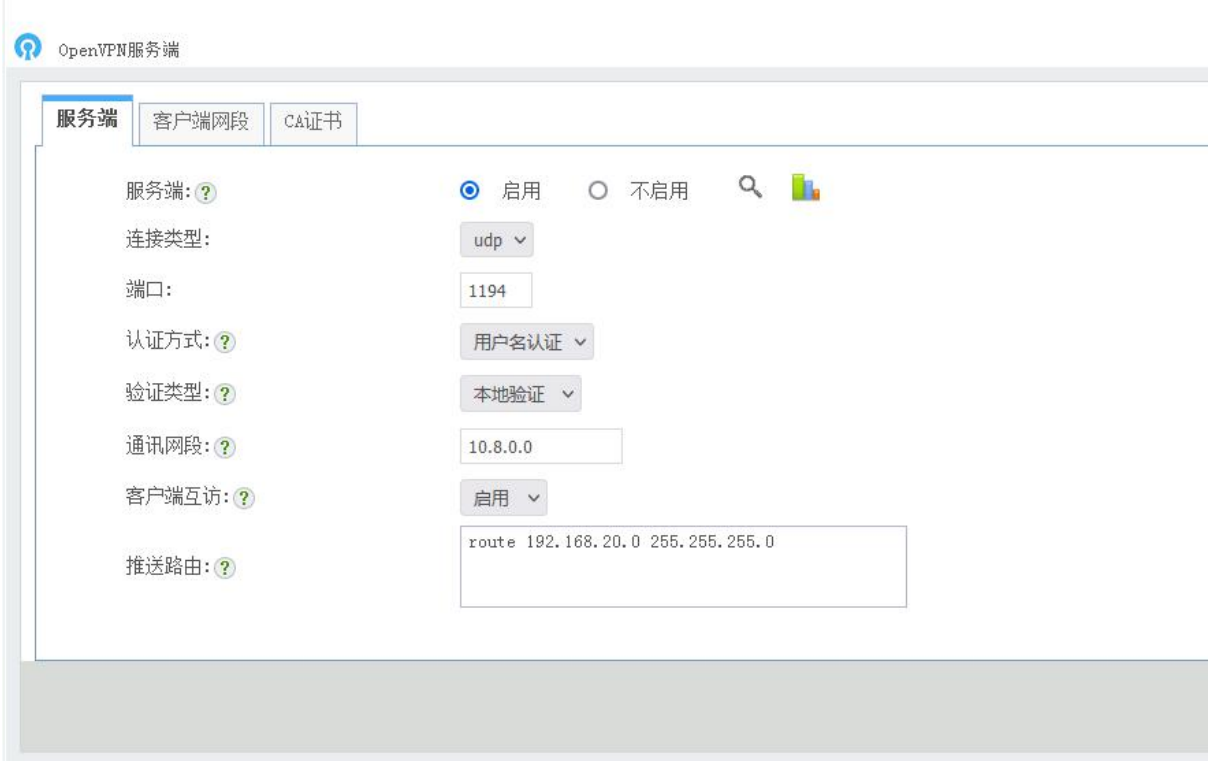
4.5.7 运营管理

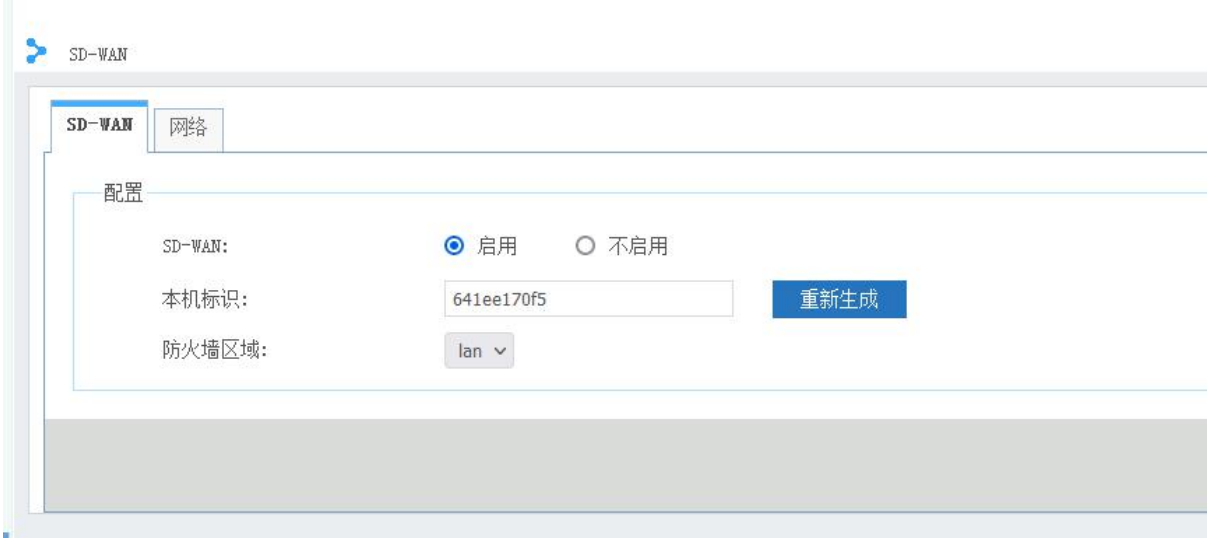
该模块给酒店、小区用户提供了集成的运行管理功能。包括：策略管理，用户管理，用户 Portal，Email 通知等功能。



4.6 VPN、SD-WAN

- ✓ 支持 PPTP、IPSec、OpenVPN、WebVPN 等多种主流 VPN 接入。
- ✓ 支持多达 100 条 IPSec 隧道。
- ✓ 多种认证方式：本地账号认证、域账号认证、第三方 Radius 认证等。
- ✓ 支持 SD-WAN。





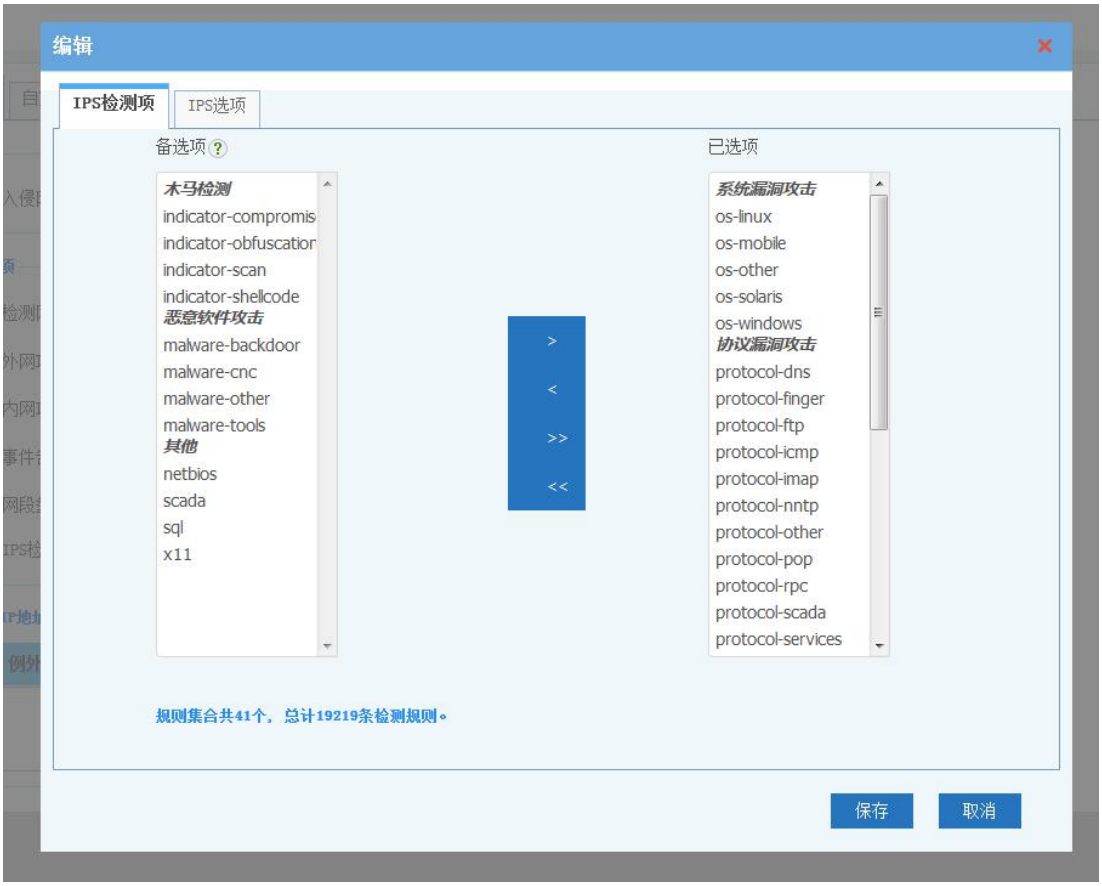
4.7 安全防护

4.7.1 DDOS 防护

该模块可以包含网络不受外网的 DDOS 攻击。

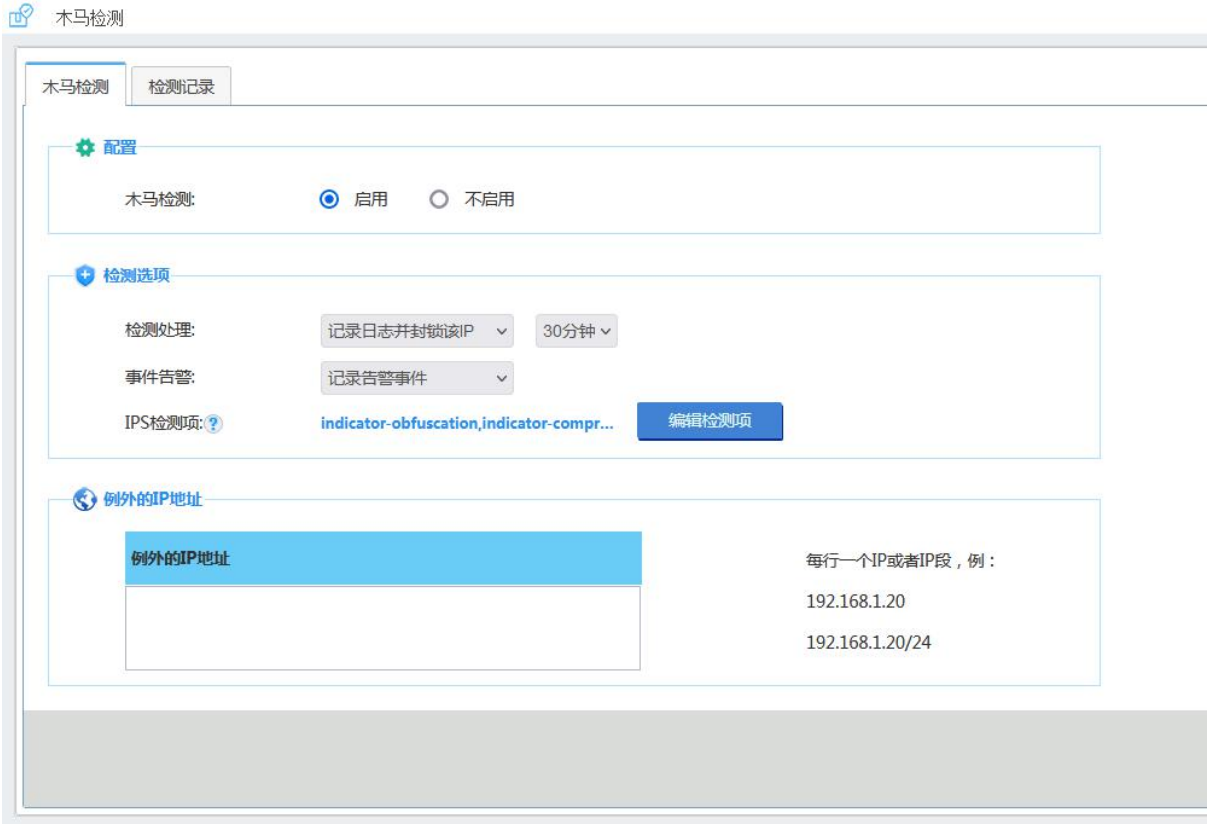
4.7.2 入侵防御

“入侵防御”模块可以检测来自内、外网的恶意攻击行为，触发告警并且封锁 IP 地址，从而保护内网的网络安全。



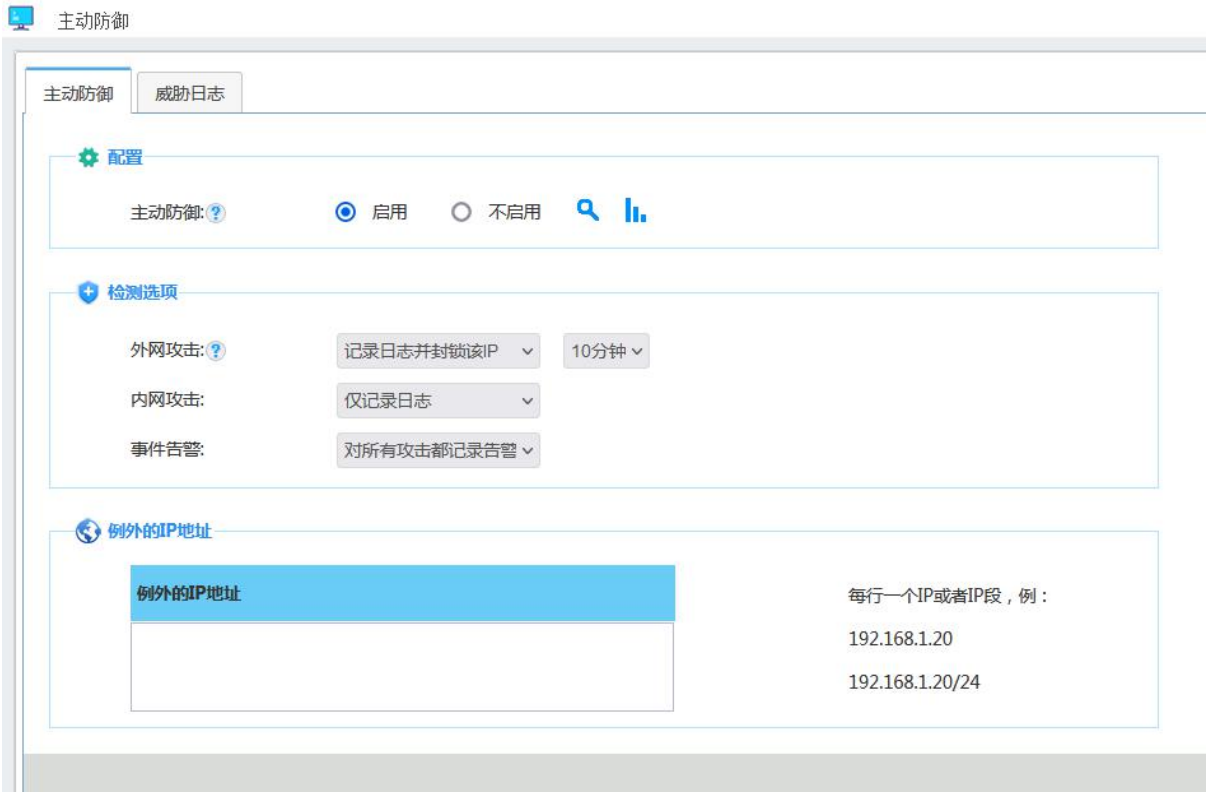
4.7.3 木马检测

“木马检测”模块用于检测内网的木马病毒等，可以触发告警并且封锁 IP 地址，从而保护内网的网络安全。



4.7.4 主动防御

“主动防御”模块通过 AI 技术智能检测和防护攻击，可以有效的检测和阻止网络扫描、DDoS 攻击等。



4.8 多种扩展插件

- ✓ 一键扫描网内设备
- ✓ 私接路由和随身 wifi 检测
- ✓ 代理服务器扫描
- ✓ DHCP 服务器扫描
- ✓ 网络健康度检测等。

4.8.1 插件管理

4.8.2 MAC 地址收集器

该模块可以从三层交换机获取 MAC 地址信息，从而监控到 MAC 地址，基于 MAC 地址配置策略和记录上网行为。

4.8.3 网络健康度检测

可以检测局域网内的 ARP 攻击、IP 地址冲突、广播风暴和环路、可疑主机等各种

网络异常。

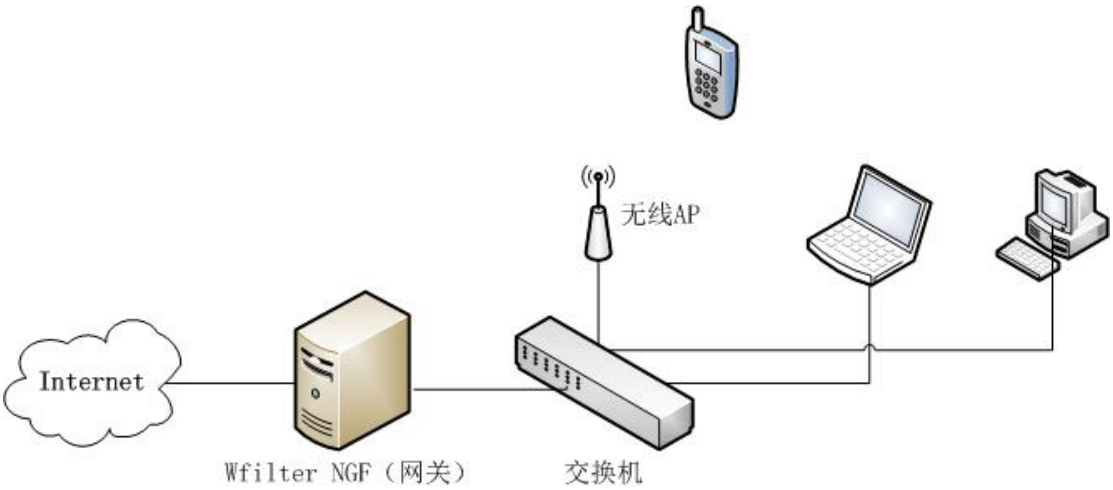
4.8.4 随身 WiFi 和私接路由检测

可以检测出网内的非法共享，并且设置惩罚策略。

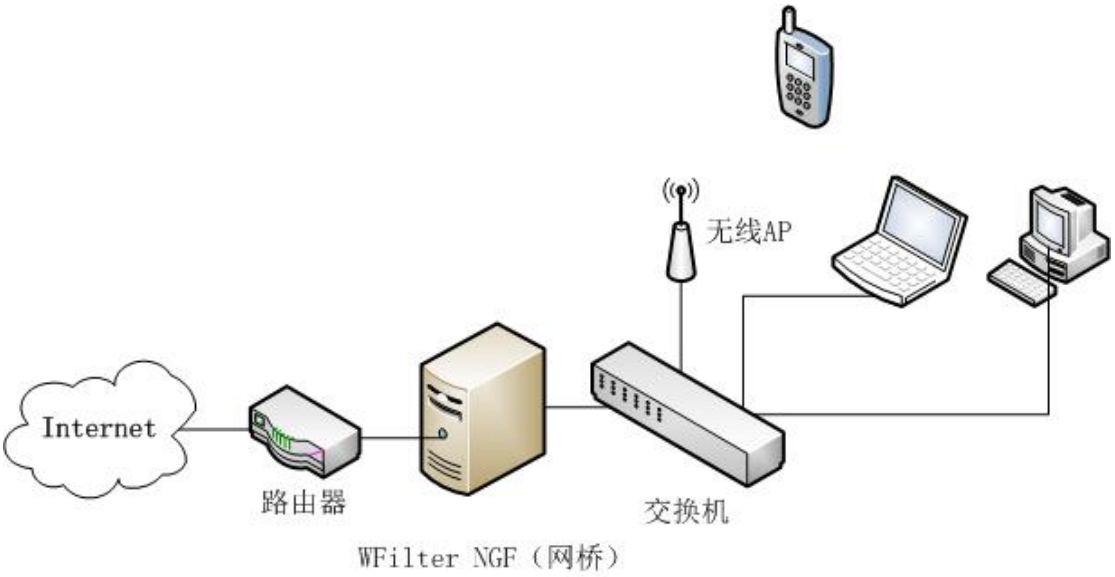
5 典型部署方案

WFilter NGF 支持网关、网桥、旁路三种部署模式。

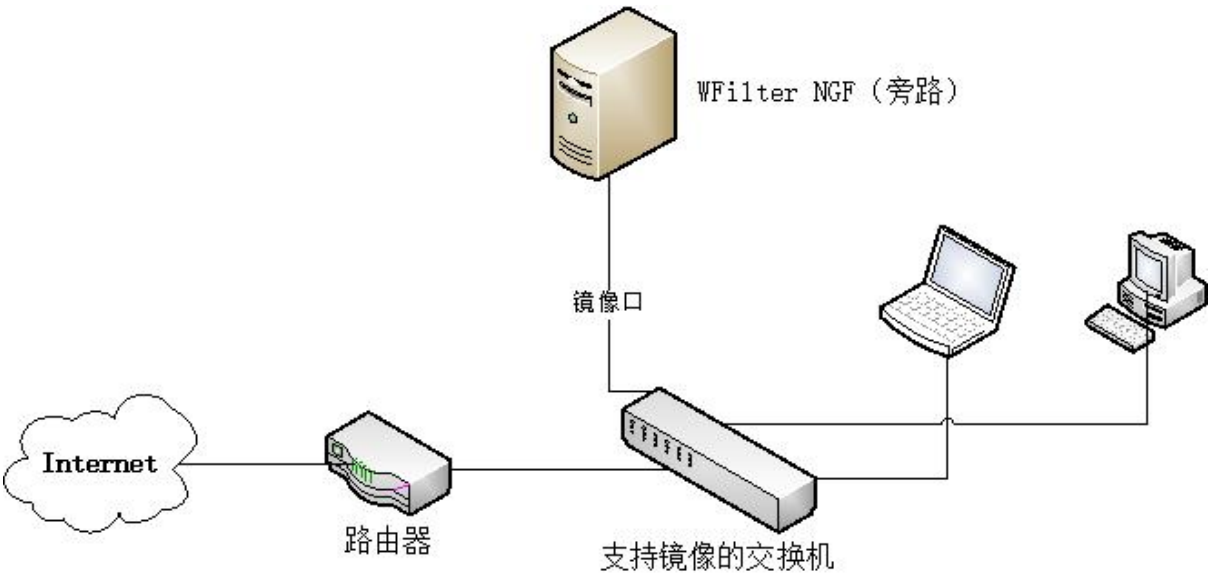
1. 网关部署模式



2. 网桥部署模式



3. 旁路部署模式



公司名称： 南京笨驴信息技术有限公司

公司地址： 江苏省南京市红山路 88 号常发广场 3 号楼 909(邮编:210028)

电话： 400-018-0186 025-84632168

电子邮件： support@imfirewall.com.cn

中文网址： http://www.imfirewall.com

English： http://www.wfiltericf.com