

# WFilter-NGF 上网行为管理系统

## 产品白皮书

### 目录

1 产品概述.....	3
2 为什么选择 WFilter NGF 行为管理系统? .....	3
3 WFilter NGF 给用户带来的价值.....	3
3.1 保护信息安全.....	3
3.2 提高工作效率.....	4
3.3 优化网络带宽.....	4
3.4 虚拟远程组网.....	4
4 功能简介.....	4
4.1 实时检测和控制.....	4
4.1.1 在线设备列表.....	5
4.1.2 查看设备的实时链接.....	5
4.1.3 断开链接和设置惩罚策略.....	6
4.2 上网行为管理.....	6
4.2.1 基于用户组、账号设置策略.....	6
4.2.2 网页过滤策略配置.....	8
4.2.3 应用过滤策略.....	9
4.2.4 SSL 监控.....	9
4.2.5 邮件过滤.....	10
4.2.6 静态 IP 分配, IP-MAC 绑定.....	10
4.2.7 共享检测.....	12
4.2.8 网页推送.....	13
4.3 上网内容监控审计、统计报表.....	13
4.3.1 网页浏览历史.....	14
4.3.2 收发邮件监控.....	14
4.3.3 论坛发帖监控.....	15
4.3.4 文件传输记录.....	16
4.3.5 FTP/Telnet 记录.....	16
4.3.6 报表概览和列表.....	17
4.4 带宽优化.....	17
4.4.1 带宽优化策略.....	18
4.4.2 IP 限速策略.....	18
4.4.3 多线均衡策略.....	19

---

4.5 用户认证.....	20
4.5.1 域账号集成.....	20
4.5.2 Web 用户名认证.....	21
4.5.3 短信认证.....	21
4.5.4 钉钉和企业微信认证.....	22
4.5.5 二维码认证.....	23
4.5.6 PPPoE 认证.....	24
4.5.7 运营管理.....	25
4.6 VPN、SD-WAN.....	26
4.7 安全防护.....	27
4.7.1 DDOS 防护.....	27
4.7.2 入侵防御.....	27
4.7.3 木马检测.....	29
4.7.4 主动防御.....	29
4.8 多种扩展插件.....	30
4.8.1 插件管理.....	31
4.8.2 MAC 地址收集器.....	31
4.8.3 网络健康度检测.....	31
4.8.4 随身 WiFi 和私接路由检测.....	32
5 典型部署方案.....	33

# 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

序号	IP	网卡地址(MAC)	网卡制造商	设备组	名称	总带宽(KB)
1	192.168.1.22	fcac:14:7d:74:f9	GIGA-BYTE	test22,Servers,R&D - 开发机		238,042
2	192.168.1.20	00:0b:2f:7b:df:60	bplan GmbH	group 20 - Bruce - Bruce2,Servers - Bruce2...		12,130
3	192.168.1.24	00:e0:4c:d7:e0:19	REALTEK SEMICONDUCTOR CORP	R&D	Bruce电脑	4,640
4	192.168.1.13	e4:3a:6e:09:6f:e5	Shenzhen Zeroone	Servers - 网络测试机		1,464
5	192.168.1.251	02:81:a1:15:74:a4		Marketing	SD-WAN盒子	1,101
6	192.168.2.8	02:81:bd:75:9b:13		无线组	管理演示	0,997
7	192.168.120.103	00:0c:29:73:9f:44	VMware	未分组用户	pppoe1	0,978
8	192.168.1.252	00:0c:29:73:9f:40	VMware	Marketing		0,926
9	192.168.1.250	00:50:56:32:9b:fc	VMware	Marketing		0,918

### 4.1.2 查看设备的实时链接

序号	本地端口	IP地址	连接类型	协议名称	内容	实时带宽(KB)	操作
1	2349	195.201.43.134:443	TCP	TLS,HTTPS	d11.cdn.filezilla-project.org	12.457	
2	3351	1.71.145.220:80	TCP	WPS网盘	openapp.wpscdn.cn	0.015	正在结束中
3	1583	20.198.162.78:443	TCP	TLS,HTTPS	client.wns.windows.com	0.011	
4	3324	115.227.12.58:443	TCP	TLS,HTTPS	wup.browser.qq.com	0.001	

### 4.1.3 断开链接和设置惩罚策略

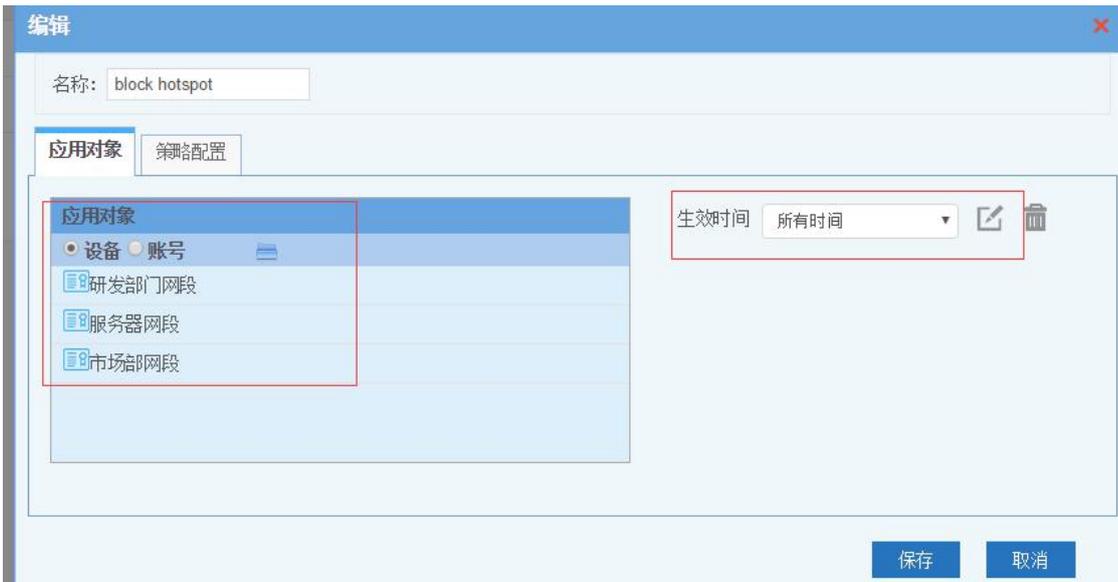


## 4.2 上网行为管理

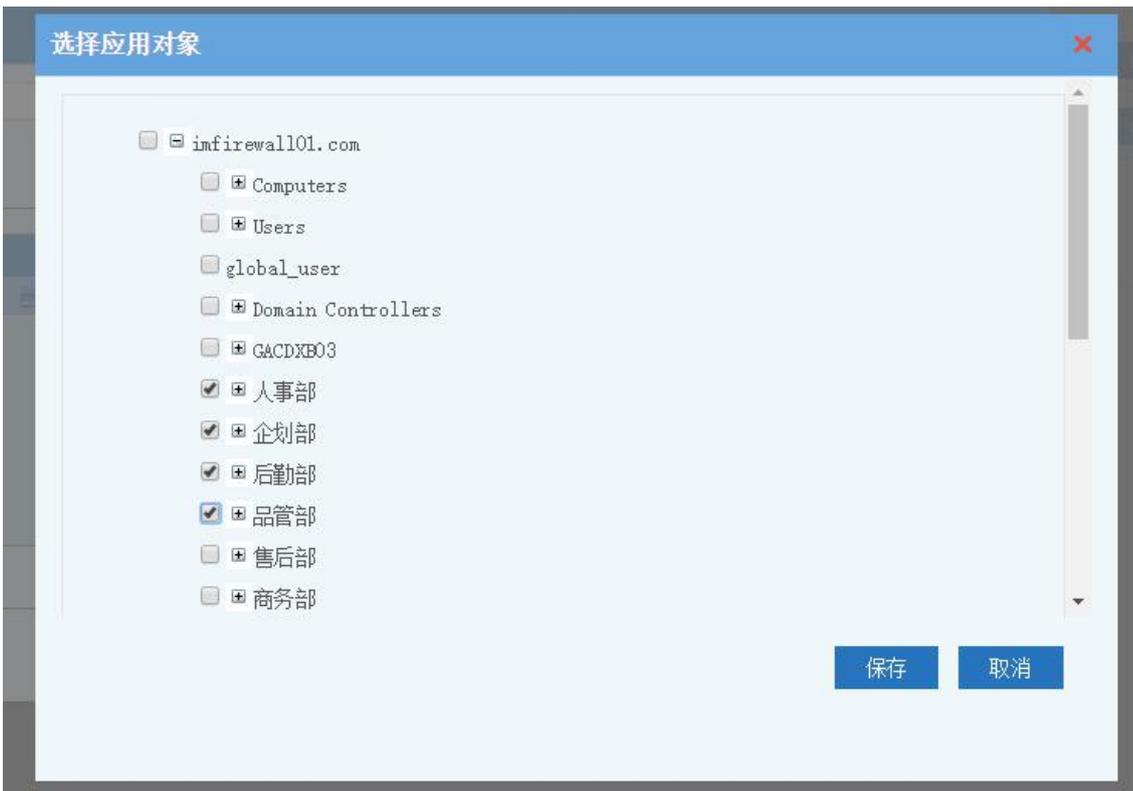
- ✓ 网页过滤、应用过滤、IP-MAC 绑定、网页推送、聊天过滤等。
- ✓ 支持多种管控手段，可以基于网段、IP 地址、域账号、MAC 地址设置策略。
- ✓ 多种上网认证方式，支持短信实名认证，AD 域、Web 认证、Radius 认证等方式。
- ✓ 可以和 AD 域集成，基于域账号记录和设置上网策略。
- ✓ 千万级网址库，支持 60 余种网站分类，满足各类管理需要。
- ✓ 全面、精准的协议识别，支持两千余种常见协议。

### 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

**编辑**

名称:

时间段配置

周日	<input type="text"/>
周一	<input type="text" value="08:30-12:00,13:00-17:30"/>
周二	<input type="text" value="08:30-12:00,13:00-17:30"/>
周三	<input type="text" value="08:30-12:00,13:00-17:30"/>
周四	<input type="text" value="08:30-12:00,13:00-17:30"/>
周五	<input type="text" value="08:30-12:00,13:00-17:30"/>
周六	<input type="text"/>

多个时间段用“,”连接:  
如:08:30-12:00,13:30-18:00

### 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。

**编辑**

名称:

应用对象: **策略配置**

网站  网页分类  文件下载  不封堵  其他

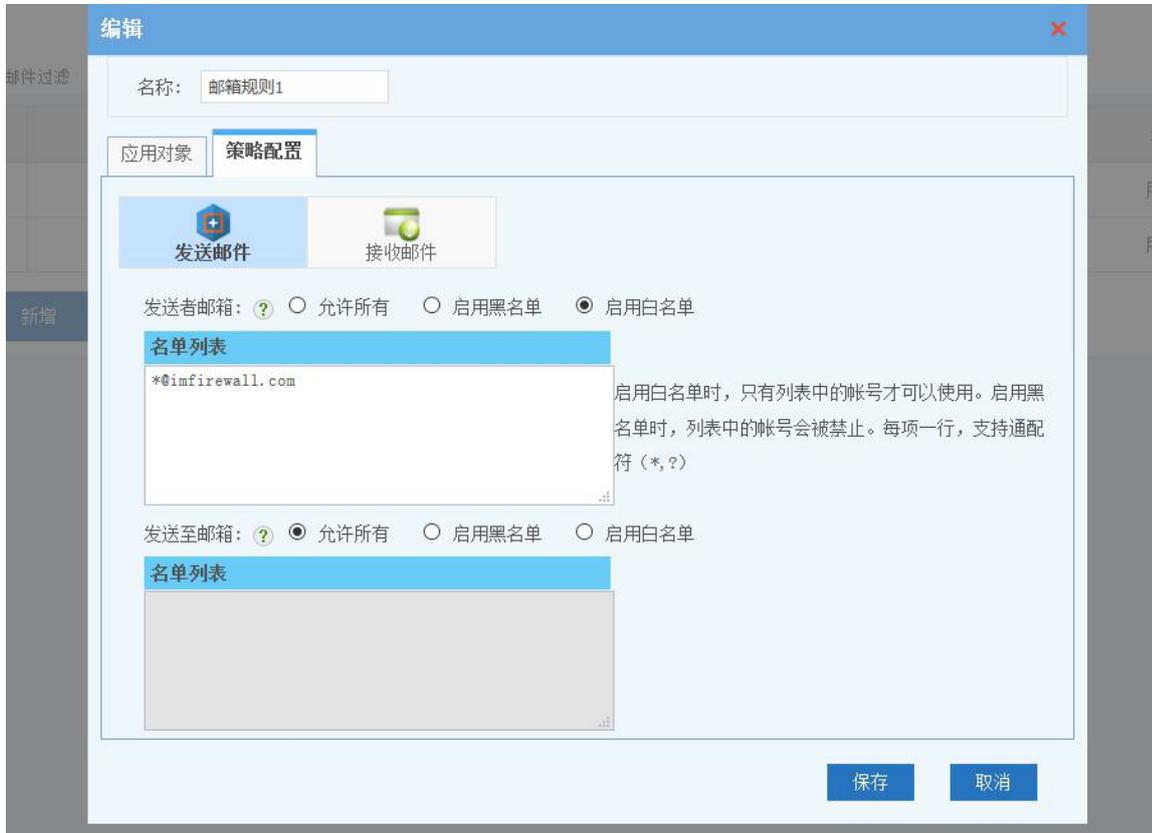
启用网页访问规则  
- 搜索条件

#	网页目录名称	所属分类	影响工作 ↓	占用带宽	风险	访问规则
1	色情	成人类	很高	低	很高	禁止访问 ▼
2	泳装/内衣	成人类	很高	低	很低	禁止访问 ▼
3	成人	成人类	很高	中	很低	允许访问 ▼
4	赌博/博彩	游戏类	很高	很低	很高	允许访问 ▼
5	游戏	游戏类	很高	中	低	允许访问 ▼
6	社交类网站	休闲类	很高	低	很低	允许访问 ▼
7	在线阅读	休闲类	很高	低	很低	允许访问 ▼



## 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

IP-MAC绑定

IP-MAC列表

搜索条件:

每页显示: 10条

#	IP地址	MAC地址	备注	状态	操作
1	192.168.1.1	00:90:9a:aa:1a:af		ON <input type="checkbox"/>	
2	192.168.1.2	ce:11:e6:99:1b:21		ON <input type="checkbox"/>	
3	192.168.1.6	6a:52:72:34:ae:e4		ON <input type="checkbox"/>	
4	192.168.1.7	1e:15:82:8b:66:2a		ON <input type="checkbox"/>	
10	192.168.1.103	00:ea:01:21:2c:48		ON <input type="checkbox"/>	

1 2 >> << 1/2页, 共14条

[新增](#) [批量操作](#) [导出](#) [配置](#)

配置

**未绑定IP**

对于未绑定的IP:  允许上网  禁止上网  只禁止下列IP

**IP范围**

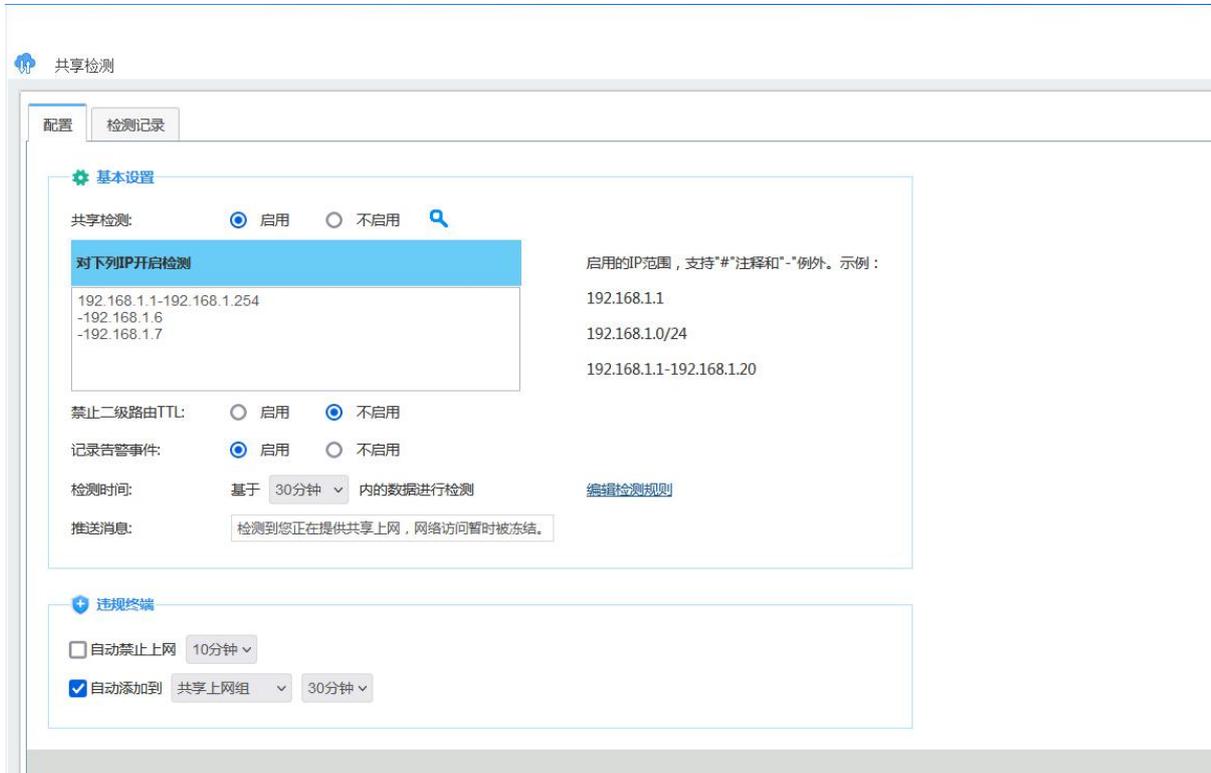
**是否给未绑定的MAC分配IP地址**

lan1:  不分配IP  分配IP

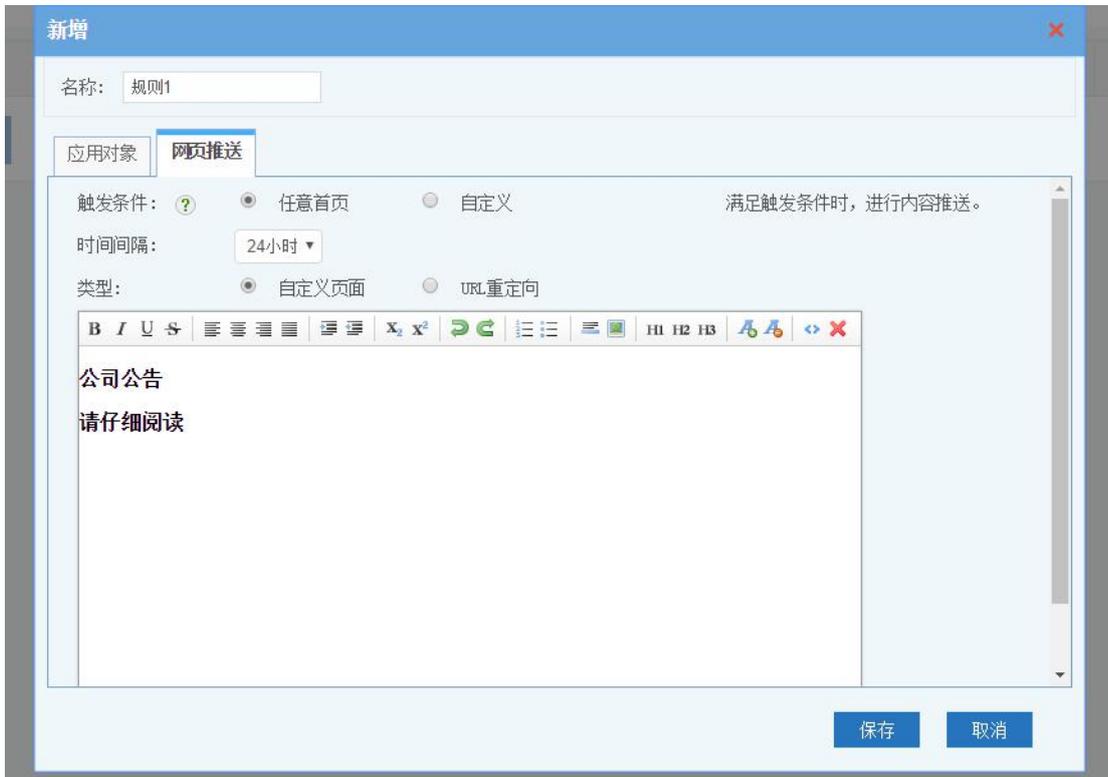
[保存](#) [取消](#)

## 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

上网记录

记录设置 | 记录查询 | 查询结果-网页浏览

刷新 | 导出记录

网页浏览记录 ( 2016-11-11 00:00—2016-11-11 23:59 ) 未设置过滤条件

序号	IP	账号	访问时间	页面标题
1	192.168.1.104		2016-11-11 23:59:48	gdvp.com — gdvp.com
2	192.168.1.104		2016-11-11 23:59:48	www.gdvp.com — gdvp.com
3	192.168.1.104		2016-11-11 23:59:47	genkisushi.com.cn — 元気首页
4	192.168.1.104		2016-11-11 23:59:47	en-core.com — data driven world en-core
5	192.168.1.104		2016-11-11 23:59:47	www.en-core.com — data driven world en-core
6	192.168.1.104		2016-11-11 23:58:30	cgns.com —
7	192.168.1.104		2016-11-11 23:58:30	www.cgns.com —
8	192.168.1.104		2016-11-11 23:58:16	www.glaustralia.com — glaustralia -
9	192.168.1.104		2016-11-11 23:56:59	www.banar.cn — 搬哪儿(banar.cn)   一站式品质搬家
10	192.168.1.104		2016-11-11 23:56:59	www.banar.cn — 搬哪儿(banar.cn)   一站式品质搬家
11	192.168.1.103		2016-11-11 23:56:52	checkip.dydns.com — current ip check
12	192.168.1.104		2016-11-11 23:56:32	banar.net.cn — 域名到期提醒—紫田网络
13	192.168.1.104		2016-11-11 23:56:32	banar.net.cn — 域名到期提醒—紫田网络
14	192.168.1.104		2016-11-11 23:56:32	vip.banar.net.cn — 域名到期提醒—紫田网络
15	192.168.1.104		2016-11-11 23:55:29	fip.com.cn — fip.com.cn - the domain is available for purchase

1 2 3 4 5 6 7 8 9 10 >> >| 共 11633 条记录 1/776

### 4.3.2 收发邮件监控

上网记录

记录设置 | 记录查询 | 查询结果-收发邮件

刷新 | 导出记录

邮件收发记录 (2017-03-16 00:00—2017-03-16 23:59)

序号	IP	账号	时间	发件者	类型	邮件标题
1	192.168.1.20	我的电脑20	2017-03-16 16:07:01	jessfer@masterscrane.com	POP3接收	RE: WFilter Activation
2	192.168.1.20	我的电脑20	2017-03-16 16:01:40	postmaster@imfirewall.com.cn	POP3接收	系统退信
3	192.168.1.20	我的电脑20	2017-03-16 15:51:40	postmaster@imfirewall.com.cn	POP3接收	系统退信
4	192.168.1.21	Administrator	2017-03-16 14:22:44	support@imfirewall.com.cn	SMTP发送	感谢您购买WFilter上网行为管理软件！
5	192.168.1.20	我的电脑20	2017-03-16 14:13:44	support@imfirewall.us	SMTP发送	Re: WFilter Activation
6	192.168.1.20	我的电脑20	2017-03-16 14:10:59	jessfer@masterscrane.com	POP3接收	RE: WFilter Activation
7	192.168.1.20	我的电脑20	2017-03-16 12:56:09	support@imfirewall.us	SMTP发送	Re: WFilter Activation
8	192.168.1.20	我的电脑20	2017-03-16 12:54:21	jessfer@masterscrane.com	POP3接收	RE: WFilter Activation
9	192.168.1.20	我的电脑20	2017-03-16 12:54:15	support@imfirewall.com.cn	POP3接收	申请WFilter试用版注册码通知(11:39:21)



### 4.3.3 论坛发帖监控



### 4.3.4 文件传输记录

上网记录

记录设置 记录查询 查询结果-文件传输

文件传输记录 ( 2018-06-01 00:00--2018-06-06 23:59 )

序号	IP	用户组	账号	时间	类型	文件大小(KB)	远程地址	文件名
1	192.168.1.20	group 20-Bruce...	test	2018-06-05 15:27:47	WEB上传	0	adashww.ut.taobao.com	stm_pcm
2	192.168.1.20	group 20-Bruce...	test	2018-06-05 15:15:46	WEB上传	0	adashww.ut.taobao.com	stm_pcm
3	192.168.1.20	group 20-Bruce...	test	2018-06-05 15:06:47	WEB上传	0	adashww.ut.taobao.com	stm_pcm
4	192.168.1.20	group 20-Bruce...	test	2018-06-05 15:06:23	WEB上传	0	adashww.ut.taobao.com	stm_pcm
5	192.168.1.101	R&D	前台如花小姐	2018-06-05 14:58:08	WEB下载	5398	f.us.sinaimg.cn	http://f.us.sinaimg.cn/0...
6	192.168.1.20	group 20-Bruce...	test	2018-06-05 14:45:47	WEB上传	0	adashww.ut.taobao.com	stm_pcm
7	192.168.1.20	group 20-Bruce...	test	2018-06-05 14:36:46	WEB上传	0	adashww.ut.taobao.com	stm_pcm
8	192.168.1.20	group 20-Bruce...	test	2018-06-05 14:33:46	WEB上传	0	adashww.ut.taobao.com	stm_pcm
9	192.168.1.22	test22-开发机1...		2018-06-05 13:41:58	WEB下载	37777	www.wfilterros.com	wfilter ng firewall free...
10	192.168.1.22	test22-开发机1...		2018-06-05 13:41:48	WEB下载	43038	www.wfilterros.com	wfilter ng firewall free...
11	192.168.1.20	group 20-Bruce...	test	2018-06-05 13:41:22	FTP上传	10	47.88.8.172:59230	download.htm
12	192.168.1.22	test22-开发机1...		2018-06-05 13:40:48	WEB下载	43038	www.wfilterros.com	download_wfilter
13	192.168.1.20	group 20-Bruce...	test	2018-06-05 13:40:05	FTP上传	13	47.88.8.172:55921	download_trial.htm
14	192.168.1.20	group 20-Bruce...	test	2018-06-05 13:39:41	FTP上传	10	47.88.8.172:50573	download.htm
15	192.168.1.22	test22-开发机1...		2018-06-05 13:37:18	WEB下载	37776	www.imfirewall.com	wfilter免费下载, wfilter...

### 4.3.5 FTP/Telnet 记录

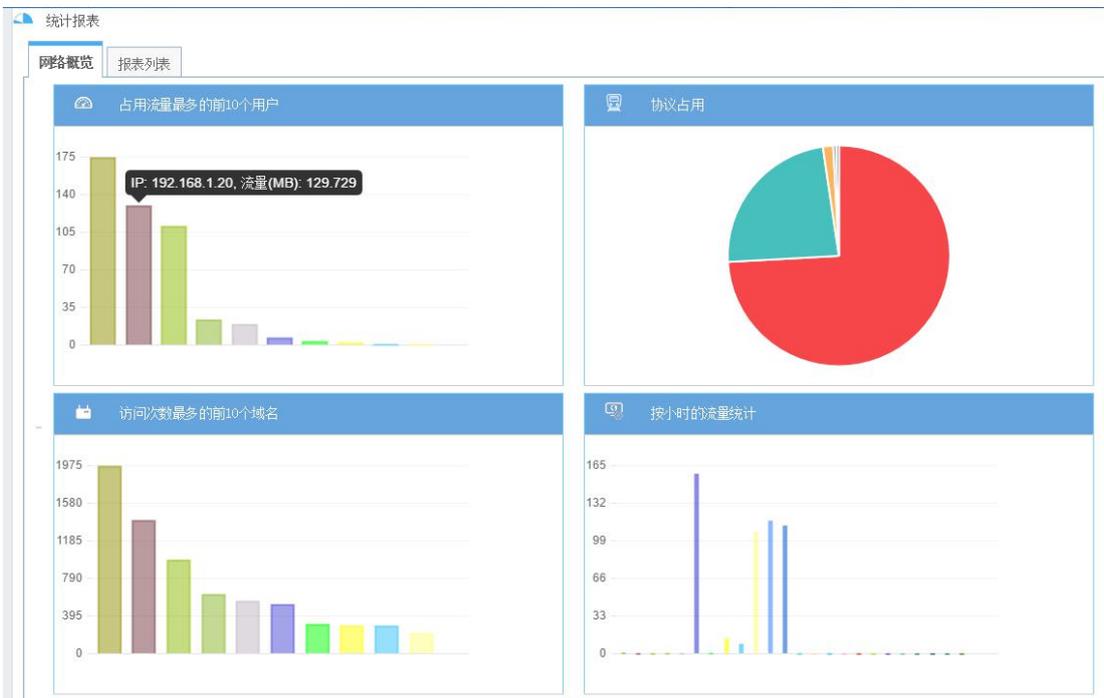
上网记录

记录设置 记录查询 查询结果-聊天帐号 查询结果-FTP/Telnet

FTP/Telnet命令 ( 2018-06-01 00:00--2018-06-06 23:59 )

序号	IP	用户组	账号	时间	类型	远程地址	发送命令
1	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:23	FTP	47.88.8.172:21	MLSD
2	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:23	FTP	47.88.8.172:21	PASV
3	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:23	FTP	47.88.8.172:21	TYPE I
4	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:22	FTP	47.88.8.172:21	STOR download.htm
5	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:22	FTP	47.88.8.172:21	PASV
6	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:22	FTP	47.88.8.172:21	TYPE A
7	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:20	FTP	47.88.8.172:21	CWD /
8	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:20	FTP	47.88.8.172:21	OPTS UTF8 ON
9	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:20	FTP	47.88.8.172:21	PASS
10	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:20	FTP	47.88.8.172:21	USER
11	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:20	FTP	47.88.8.172:21	AUTH SSL
12	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:41:20	FTP	47.88.8.172:21	AUTH TLS
13	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:40:06	FTP	47.88.8.172:21	MLSD
14	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:40:06	FTP	47.88.8.172:21	PASV
15	192.168.1.20	group 20-Bruce, R&D-B...	test	2018-06-05 13:40:06	FTP	47.88.8.172:21	TYPE I

### 4.3.6 报表概览和列表



序号	类型	报表别名	操作
1	网络活动	Top 20 visited websites	🔍 ✎ 🗑️
2	网络活动	report by users	🔍 ✎ 🗑️
3	网络活动	Report by groups	🔍 ✎ 🗑️
4	网络活动	指定域用户统计	🔍 ✎ 🗑️
5	流量类	占用流量最多的20个网站	🔍 ✎ 🗑️
6	流量类	占用流量最多的20个IP	🔍 ✎ 🗑️
7	流量类	占用流量最多的10种协议	🔍 ✎ 🗑️
8	趋势类	网站访问次数趋势	🔍 ✎ 🗑️
9	趋势类	网络流量趋势	🔍 ✎ 🗑️
10	趋势类	新闻类网站访问趋势	🔍 ✎ 🗑️
11	趋势类	求职类网站访问趋势	🔍 ✎ 🗑️
12	趋势类	视频类网站访问趋势	🔍 ✎ 🗑️
13	趋势类	微博类网站访问趋势	🔍 ✎ 🗑️

### 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。

带宽优化

序号	名称	应用对象	生效时间	内容	排序	状态	操作
1	规则1	group 20	所有时间	不限制	+	<input checked="" type="checkbox"/>	
2	Mail	所有	所有时间	指定协议分类	+	<input checked="" type="checkbox"/>	
3	Web	所有	所有时间	指定协议名称	+	<input checked="" type="checkbox"/>	
4	P2P & Streaming	所有	所有时间	指定协议分类	+	<input checked="" type="checkbox"/>	

新增

### 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。

编辑

名称: 实验室限速

应用对象: 限速规则

数据类型: 所有

上行

限制上行总带宽为: 0 - 100 Mbit

限制单IP上行最大值: 5 Mbit

下行

限制下行总带宽为: 0 - 100 Mbit

限制单IP下载最大值: 5 Mbit

连接数限制

TCP最大连接数: 不限制

保存 取消

### 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。

新增

名称: 政务专线

网卡:  政务专网  
 互联网  
 视频专线

权重: 政务专网: 100%

保存 取消

多线程均衡

线路方案 分流规则

#	名称	本地IP	远程IP	远程端口	线路方案	排序	状态	操作
1	政务	所有	172.16.2.0/24	所有	政务专线	+	ON	✎ ✖ 🔍
2	rule1	所有	所有	所有	互联网	+	OFF	✎ ✖ 🔍
3	规则7	所有	所有	所有	Solution1	+	ON	✎ ✖ 🔍
4	规则3	所有	所有	TCP 22, 21	政务专线	+	OFF	✎ ✖ 🔍
5	运营商分流	所有	所有	所有	运营商分流		OFF	🔍
6	负载均衡	所有	所有	所有	负载均衡		ON	🔍

新增

## 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。

域账户 ?

域账户

**配置**

域账户  启用  不启用

域控制器IP

端口

域管理员账号 ?

密码

域名

域控制器位置 ?  外网口  内网口

脚本通讯密钥 ?

**高级配置**

每隔:  秒轮询域控制器 ?

账户超时时间:  小时

自动同步域账号: 每天 00:00

启用调试模式

忽略下表中的账号 ? 每个一行  
支持通配符\*和?

只获取下表中的OU

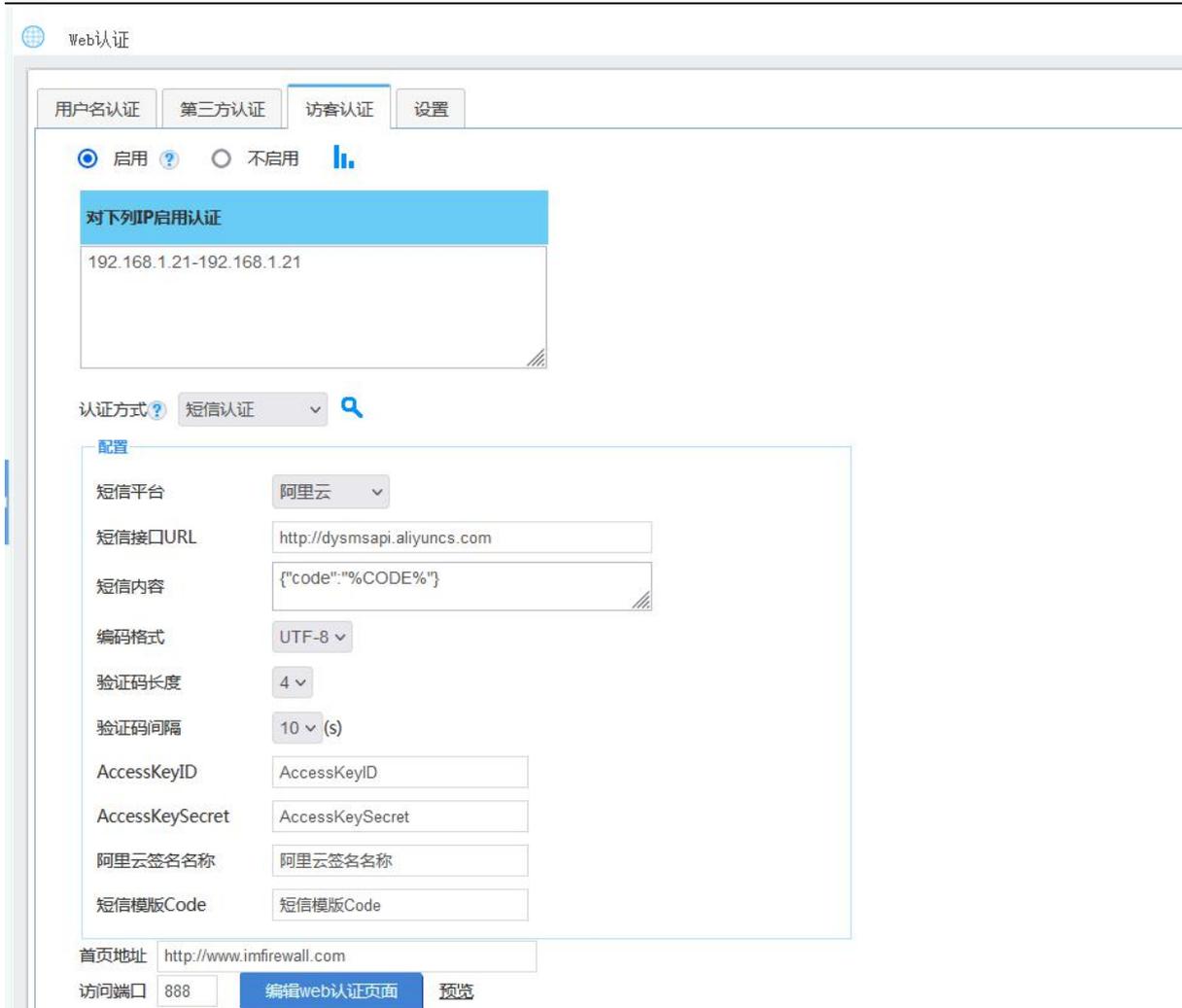
## 4.5.2 Web 用户名认证

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。

The screenshot shows the 'Web认证' (Web Authentication) configuration page. It features several tabs: '用户名认证' (User Authentication), '第三方认证' (Third-party Authentication), '访客认证' (Guest Authentication), and '设置' (Settings). The '用户名认证' tab is active, showing options to '启用' (Enable) or '不启用' (Disable) the feature. Below this, there is a section for '对下列IP启用认证' (Enable authentication for the following IP addresses) with a text area containing '192.168.1.21-192.168.1.21'. The '验证类型' (Authentication Type) is set to '本地+域' (Local+Domain). A '配置' (Configuration) section includes fields for '域控制器' (Domain Controller) set to '192.168.1.32', '端口' (Port) set to '389', and '域名' (Domain Name) set to 'imfirewall01.com'. The '首页地址' (Home Address) is set to '认证前访问的网址' (Website visited before authentication). The 'Web认证端口' (Web Authentication Port) is '8080', with buttons for '编辑web认证页面' (Edit web authentication page) and '预览' (Preview). At the bottom, there are two checkboxes for session timeout: one checked for '超过 14400 分钟重新验证' (Over 14400 minutes, re-authenticate) and one unchecked for '超过 10 分钟无网络活动时重新验证' (Over 10 minutes of inactivity, re-authenticate).

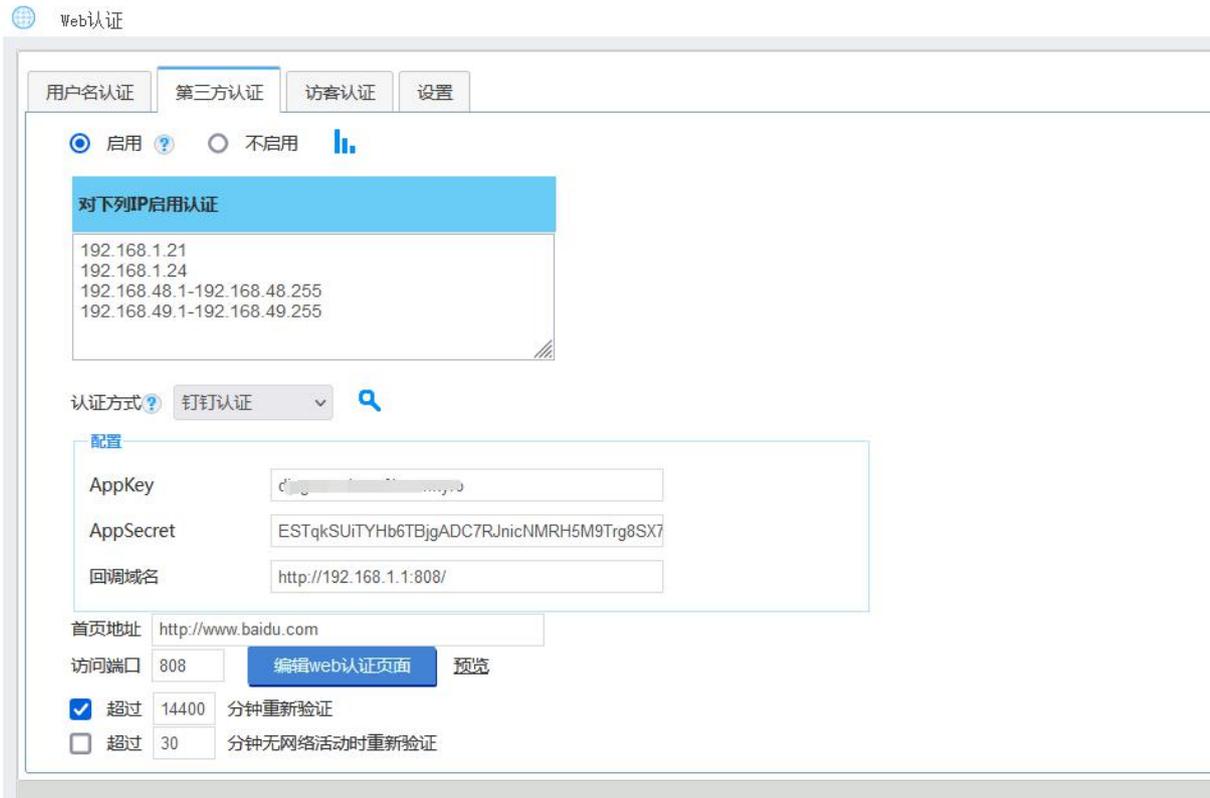
## 4.5.3 短信认证

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。

Web认证

用户名认证 第三方认证 设置

启用  不启用

对下列IP启用认证

192.168.2.1-192.168.2.254

认证方式

配置

访客信息

审核人   
 审核人的IP或者MAC地址

首页地址

访问端口

超过 14400 分钟重新验证

超过 30 分钟无网络活动时重新验证

## 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。

编辑

监听网段

服务名称

客户机IP范围  -

主dns

备用dns

限速(KB/s) 上行  下行

认证方式  本地认证  远程认证

支持的协议  chap  mschap  mschap-v2  pap

## 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。

### 编辑

用户名:

密码:

确认密码:

到期日期:

联系邮箱:

实时带宽:

累计流量:

验证方式:  PPPoE  Web  静态IP

注意: 修改用户属性会断开该用户的当前PPP连接。

### 运营管理

带宽策略 | 用户管理 | 用户Portal | **Emails**

正常用户Email:  启用  不启用

发送时间:

超流量用户Email:  启用  不启用

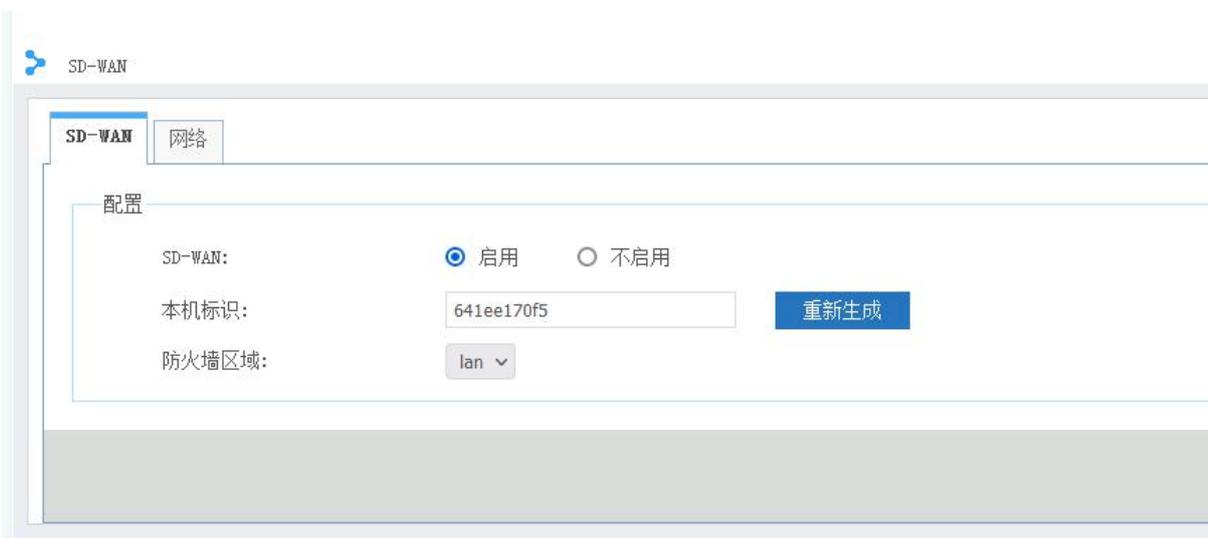
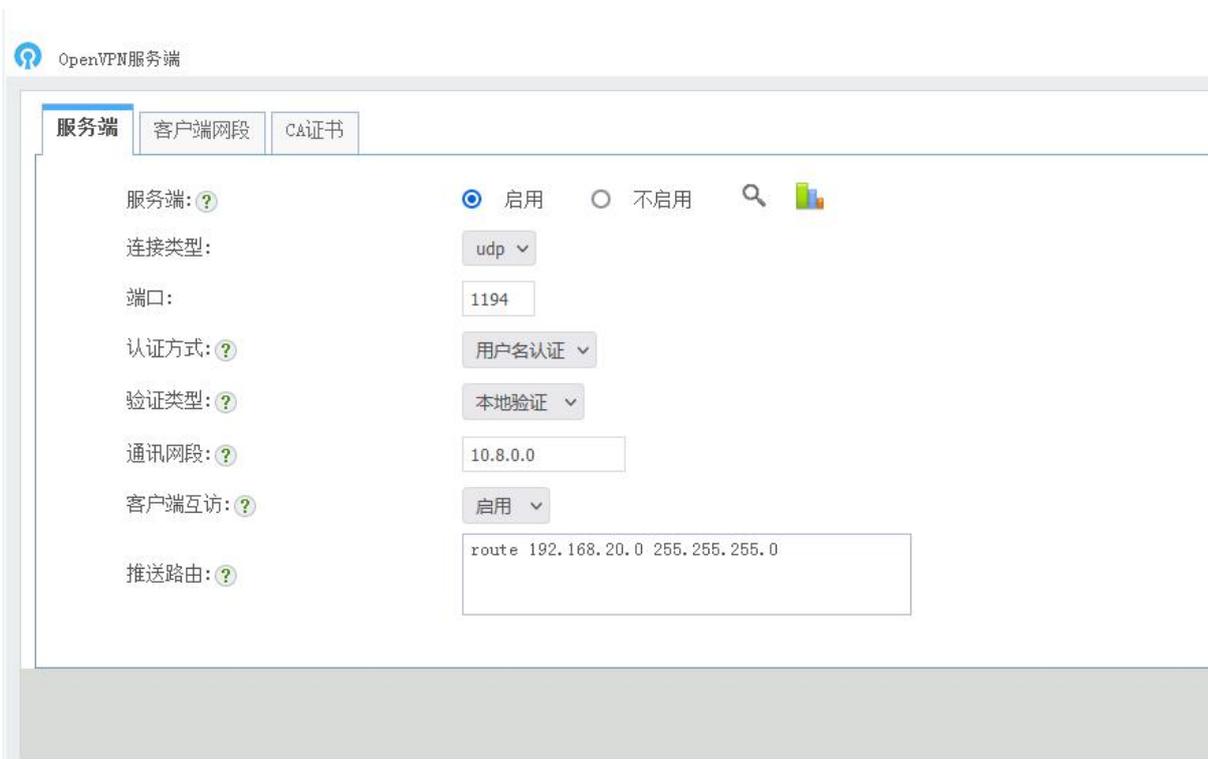
发送时间:

即将过期用户Email:  启用  不启用

发送时间:

## 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。

DDOS防护

配置

DDOS防护:  启用  不启用

DDOS防护选项

- 阻止WAN口Ping入
- 丢弃无效的数据包
- 阻止IP分片攻击
- 启用SYN-FLOOD防护 阈值 50 - 100
- 启用UDP-FLOOD防护 阈值 75 - 150
- 启用ICMP-FLOOD防护 阈值 100 - 200

IP地域限制

IP地域限制: 不启用

例外的IP地址

每行一个IP或者IP段, 例:

- 192.168.1.20
- 192.168.1.20/24

### 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。

入侵防御

入侵防御 | 自定义规则 | 记录查询

**配置**

入侵防御:  启用  不启用

**检测选项**

检测网卡: 自动选择

外网攻击: 记录日志并封锁IP 10分钟

内网攻击: 仅记录日志

事件告警: 对内网攻击记录告警事件

网段参数: 自动选择

IPS检测项: os-linux, os-mobile, os-other, os-so... [编辑检测项](#)

**例外的IP地址**

例外的IP地址

每行一个IP或者IP段，例：  
192.168.1.20  
192.168.1.20/24

编辑

IPS检测项 | IPS选项

**备选项**

- 木马检测
  - indicator-compromis
  - indicator-obfuscator
  - indicator-scan
  - indicator-shellcode
- 恶意软件攻击
  - malware-backdoor
  - malware-cnc
  - malware-other
  - malware-tools
- 其他
  - netbios
  - scada
  - sql
  - x11

**已选项**

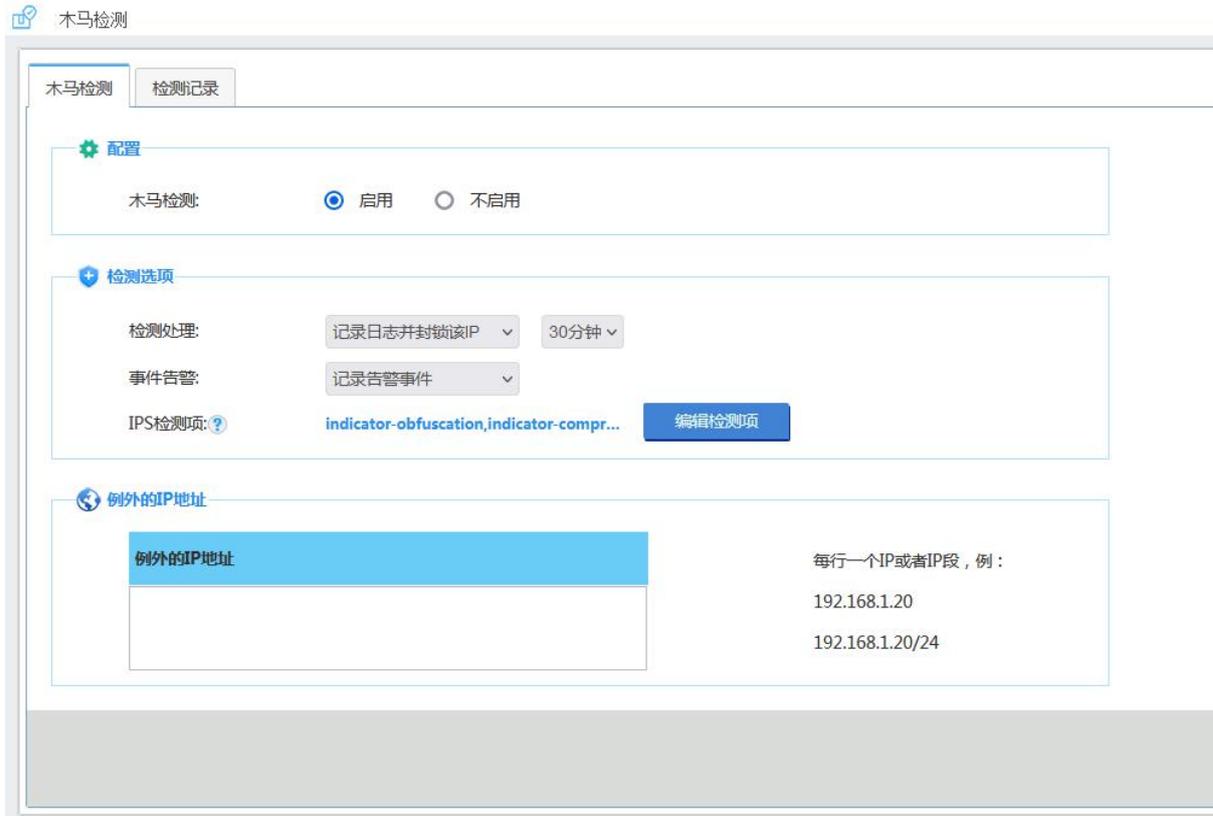
- 系统漏洞攻击
  - os-linux
  - os-mobile
  - os-other
  - os-solaris
  - os-windows
- 协议漏洞攻击
  - protocol-dns
  - protocol-finger
  - protocol-ftp
  - protocol-icmp
  - protocol-imap
  - protocol-nntp
  - protocol-other
  - protocol-pop
  - protocol-rpc
  - protocol-scada
  - protocol-services

规则集合共41个，总计19219条检测规则

[保存](#) [取消](#)

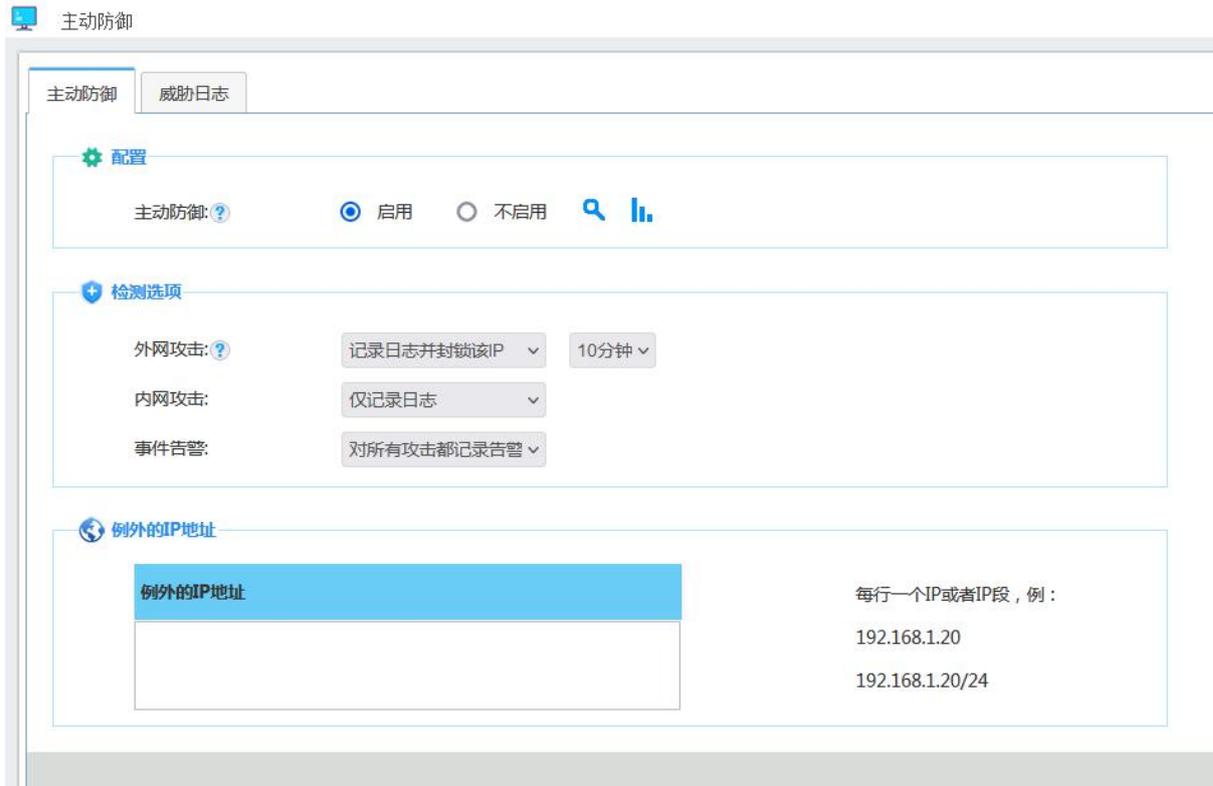
### 4.7.3 木马检测

“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

插件管理

显示 15条 搜索条件

序号	插件名称	插件描述	作者
1	随身wifi和私接路由检测	该插件可以检测局域网中私接路由、随身wifi、代理服务器等互联网共享行为。	<a href="#">imfirewall</a>
2	网络健康度监测	网络健康度监测	<a href="#">imfirewall</a>
3	批量ping工具	可以批量ping多个主机地址，支持自动运行；并且可以记录一段时间内的ping数据，并以图表格式显示。	<a href="#">imfirewall</a>
4	局域网扫描	“局域网扫描”插件可以扫描局域网电脑的IP地址、MAC地址、端口、netbios信息、ping值等信息。	<a href="#">imfirewall</a>
5	局域网DHCP服务器扫描	该插件可以扫描局域网内的DHCP服务器的信息。用此插件可以检测管理DHCP服务器的工作状况，也可以有...	<a href="#">imfirewall</a>
6	代理服务器扫描	该插件可以扫描网内的代理服务器，也可以指定IP范围进行代理扫描。	<a href="#">imfirewall</a>
7	Logo修改器	该插件可以自定义WFilter ROS的产品名称和Logo图标	<a href="#">imfirewall</a>

共 7 条记录 1/1

## 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。

MAC地址收集器

MAC地址收集器

MAC地址收集器:  启用  不启用

调试日志:  记录  不记录 [查看日志](#)

轮询间隔:

#	SNMP查询命令	返回格式	操作
1	snmpwalk -v 2c -c public 192.168.1.2 ipNetToMediaPhysAddress	IP-MIB::ipNetToMediaPhysAddress.\d+.*	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>

## 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。

### 网络健康度监测

外网	
域名解析(wan1)	✔ 很快
连通状态(wan1)	✔ 很快

内网	
连通状态(lan1)	✔ 很快
IP地址冲突检测(lan1)	⚠ 异常
ARP攻击检测(lan1)	✔ 正常
广播风暴与环路检测(lan1)	✔ 正常
可疑主机检测(LAN)	✔ 正常

重新检测

#### 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。

nat\_discover

### 随身wifi和私接路由检测

192.168.1.170 (共发现3个客户机) 重新检测

-  Android 4.2.1 (魅族)
-  Windows NT 5.1
-  Android 4.1.2 (小米)

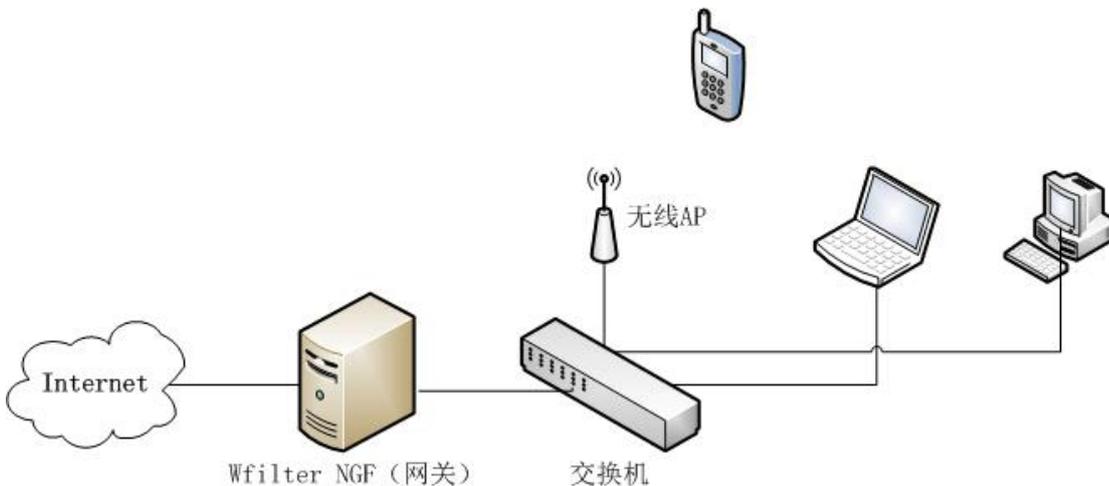
对选中的IP   确定



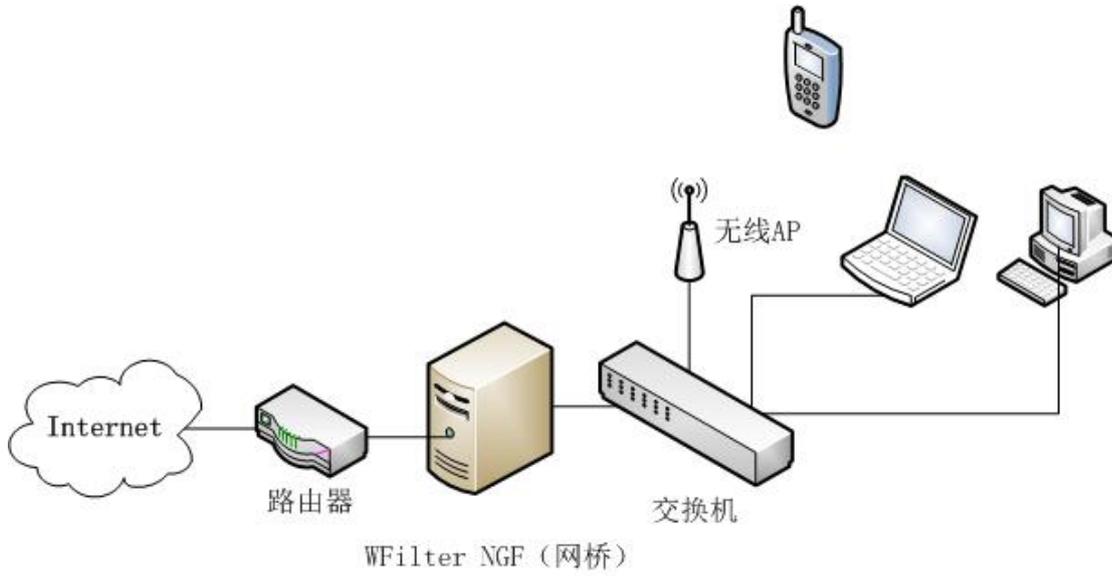
## 5 典型部署方案

WFilter NGF 支持网关、网桥、旁路三种部署模式。

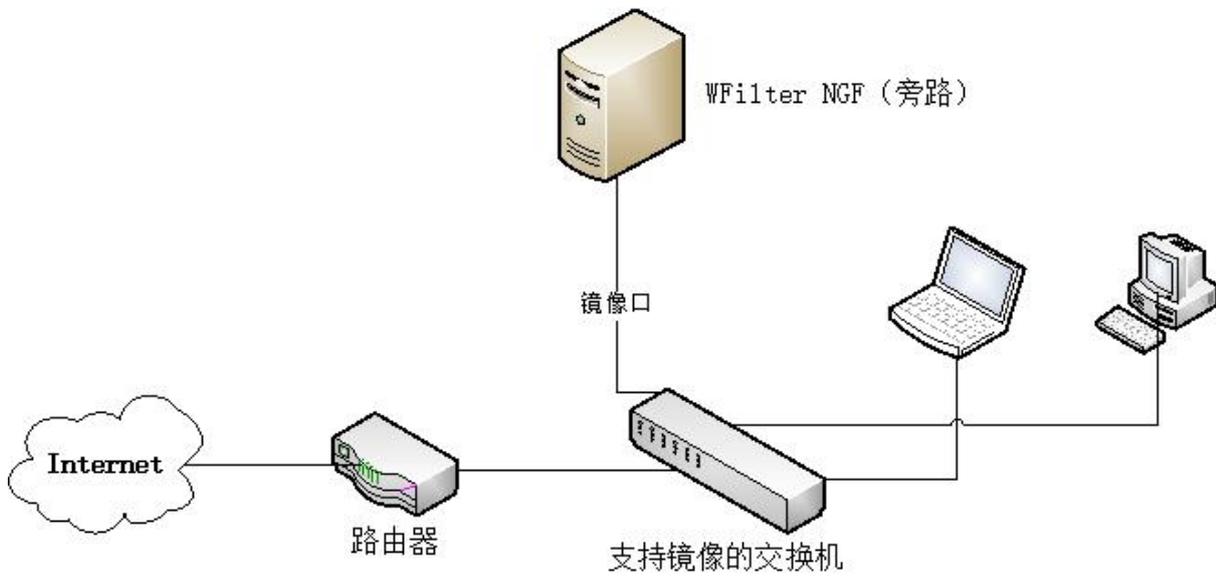
### 1. 网关部署模式



## 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](mailto:support@imfirewall.com.cn)

中文网址： <http://www.imfirewall.com>

English: <http://www.wfiltericf.com>