

WFilter 上网行为管理系统

产品白皮书

目录

1	产品概述.....	2
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	网络带宽优化.....	3
3.2	提高工作效率.....	3
3.3	保护信息安全.....	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	聊天黑白名单.....	9
4.2.5	静态 IP 分配, IP-MAC 绑定	10
4.2.6	网页推送.....	10
4.3	上网内容监控审计、统计报表.....	11
4.3.1	网页浏览历史.....	11
4.3.2	收发邮件监控.....	11
4.3.3	论坛发帖监控.....	12

4.3.4	报表概览和列表.....	13
4.4	带宽优化.....	13
4.4.1	带宽优化策略.....	14
4.4.2	IP 限速策略.....	14
4.4.3	多线均衡策略.....	14
4.5	用户认证.....	16
4.5.1	域账号集成.....	16
4.5.2	Web 认证和微信认证.....	16
4.5.3	微信认证.....	17
4.5.4	PPPoE 认证.....	17
4.5.5	运营管理.....	18
4.6	VPN.....	19
4.7	多种扩展插件.....	19
4.7.1	插件管理.....	20
4.7.2	MAC 地址收集器.....	20
4.7.3	随身 WiFi 和私接路由检测.....	20
5	典型部署方案.....	21

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、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 网络带宽优化

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。

3.2 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 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：

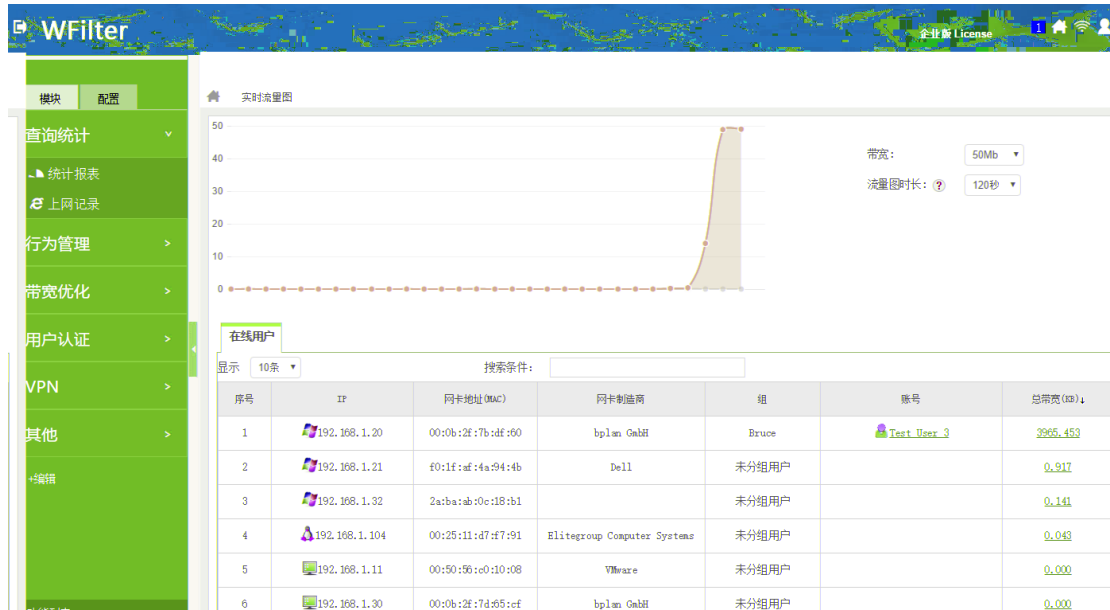
1. 支持记录多种上网内容，包括网页浏览记录、邮件记录、论坛发帖等。
2. SSL 拦截解密，可以截获 SSL 邮件、HTTPS 网页内容。
3. 详细的统计报表，多种预置报表模版。

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

The screenshot shows the 'View Connections' (查看连接) window for the IP address 192.168.1.21. It features a 'Real-time Connections' (实时连接) tab and a table listing active connections. The table includes columns for connection ID, local port, content, connection type, protocol name, content, real-time bandwidth, and actions.

序号	本地端口	内容	连接类型	协议名称	内容	实时带宽(KB)	操作
1	53134	180.97.33.107:443	TCP	TLS, HTTPS	www.baidu.com	17.285	
2	53136	111.221.29.253:443	TCP	TLS, HTTPS	settings-win.data.microsoft.com	1.124	✘
3	53131	65.55.44.109:443	TCP	TLS, HTTPS	vortex-win.data.microsoft.com	0.510	
4	53110	180.97.33.107:443	TCP	TLS, HTTPS	sp3.baidu.com	0.260	
5	4024	123.151.13.213:8000	UDP	Tencent QQ	416537809	0.059	
6	0	114.114.114.114:0	IP			0.033	
7	53113	180.97.33.107:443	TCP	TLS, HTTPS	sp2.baidu.com	0.009	
8	50856	114.114.114.114:53	UDP	DNS		0.000	
9	53111	180.97.33.108:443	TCP	TLS, HTTPS	sp1.baidu.com	0.000	
10	53027	184.168.193.33:80	TCP	Web (HTTP)	www.imfirewall.us	0.000	

4.1.3 断开链接和设置惩罚策略

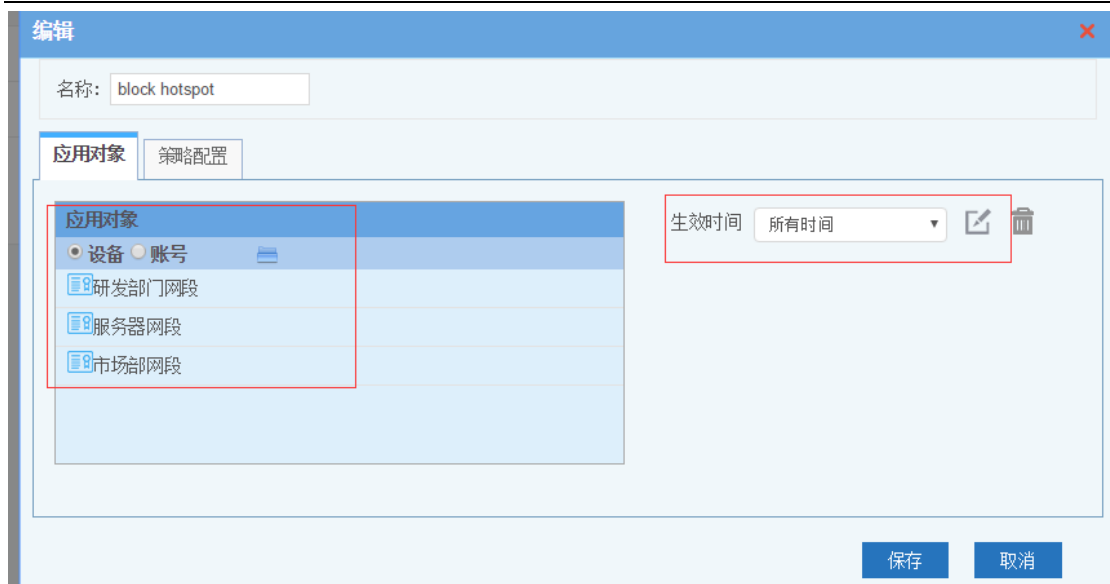


4.2 上网行为管理

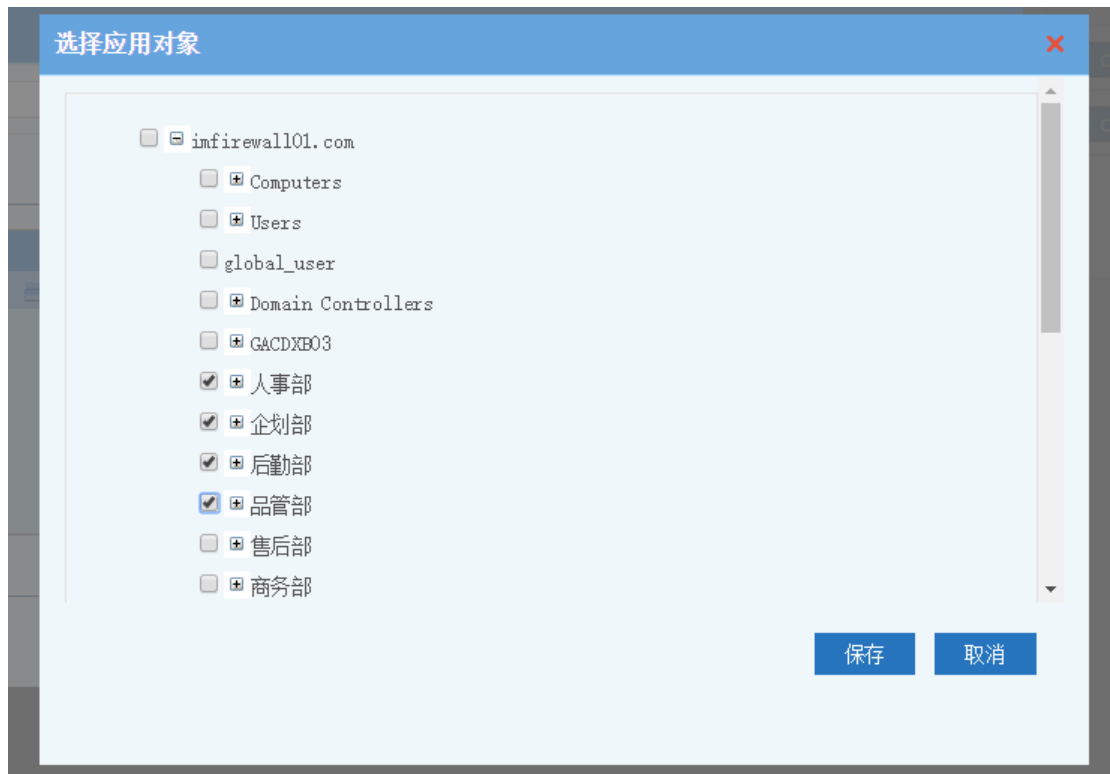
- ✓ 网页过滤、应用过滤、IP-MAC 绑定、网页推送、聊天过滤等。
- ✓ 支持多种管控手段，可以基于网段、IP 地址、域账号、MAC 地址设置策略。
- ✓ 多种上网认证方式，支持 AD 域、Web 认证、Radius 认证等方式。
- ✓ 可以和 AD 域集成，基于域账号记录和设置上网策略。
- ✓ 千万级网址库，支持 60 余种网站分类，满足各类管理需要。
- ✓ 全面、精准的协议识别，支持两千余种常见协议。

4.2.1 基于用户组、账号设置策略

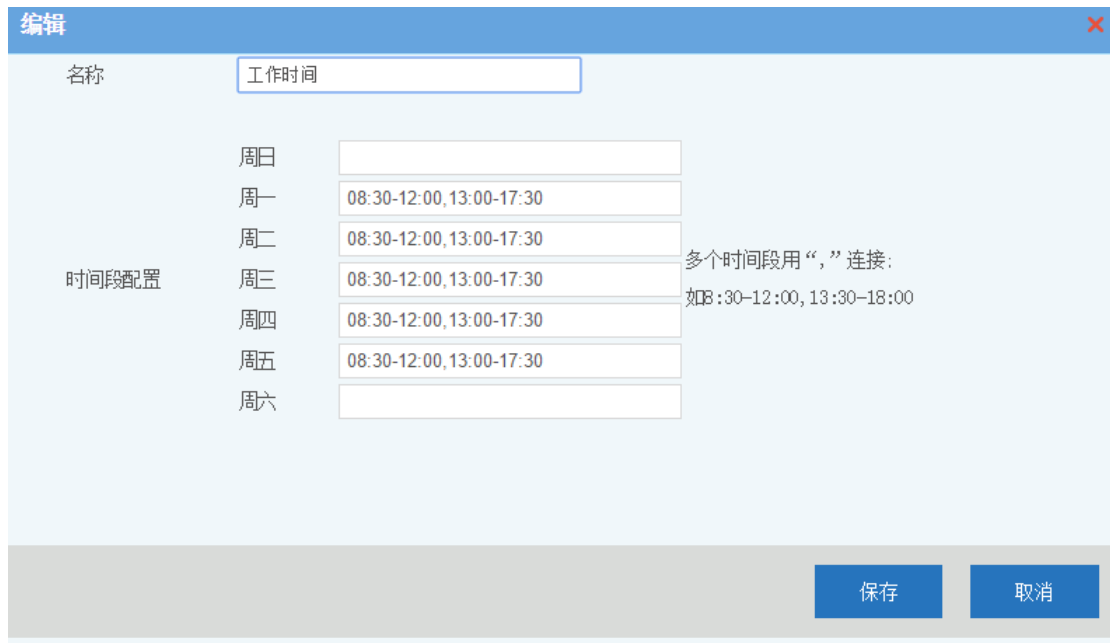
基于设备组选择应用对象



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

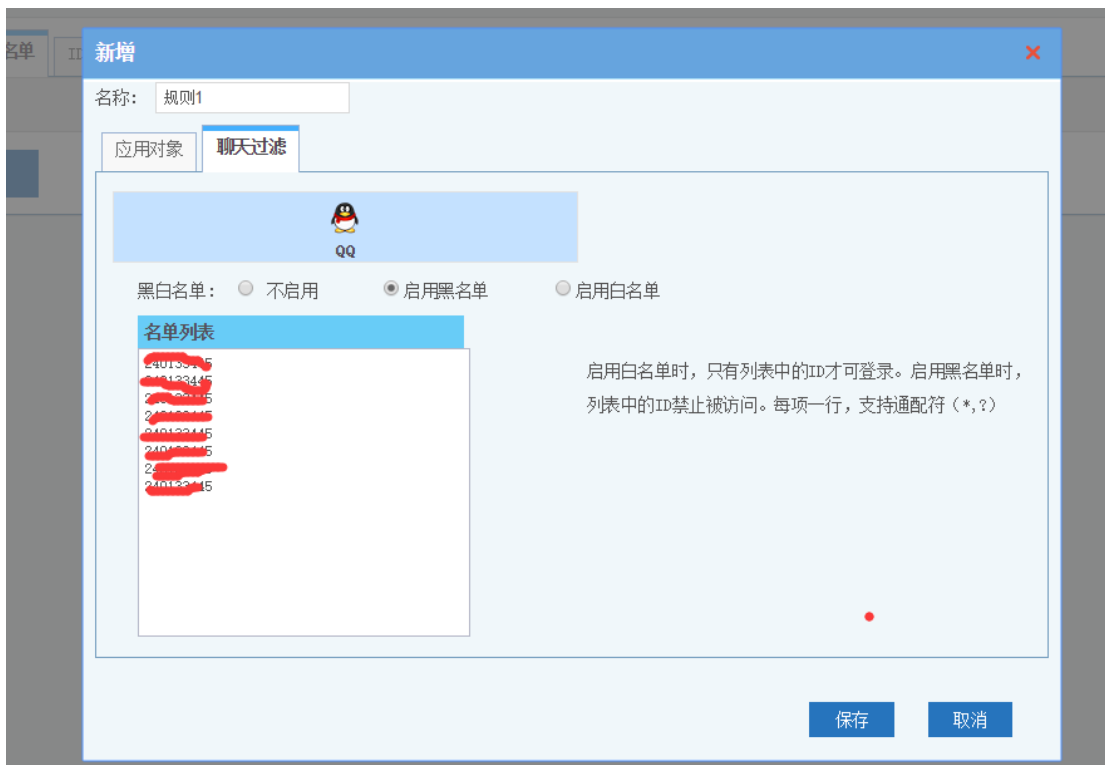
可以基于网站分类进行屏蔽，设置网站黑白名单，根据文件类型屏蔽下载。



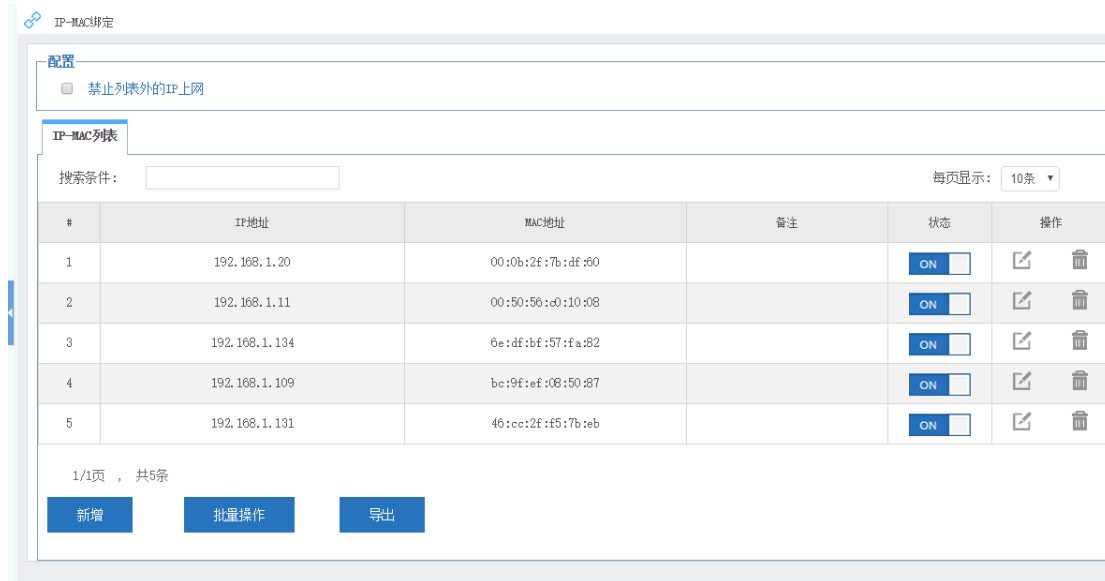
4.2.3 应用过滤策略



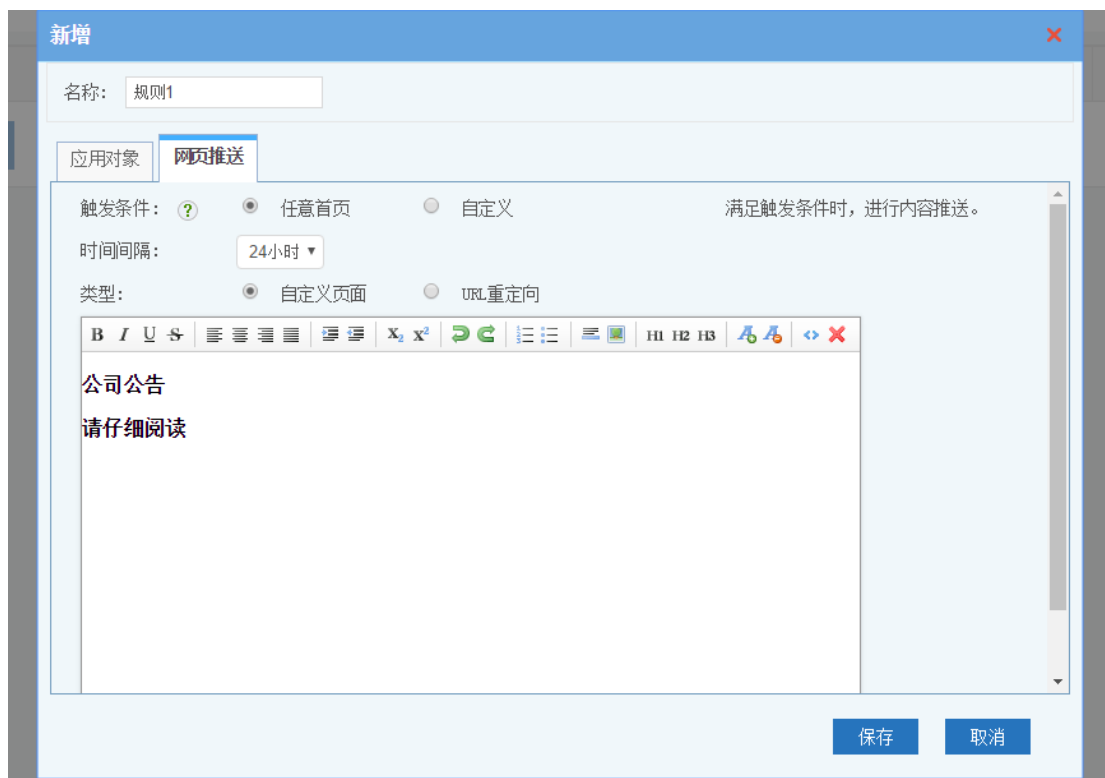
4.2.4 聊天黑白名单



4.2.5 静态 IP 分配, IP-MAC 绑定



4.2.6 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，包括网页浏览记录、邮件记录、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 — 元氮首页
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	cxns.com —
7	192.168.1.104		2016-11-11 23:58:30	www.cxns.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	ftp.com.cn — ftp.com.cn - the domain is available for purchase

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

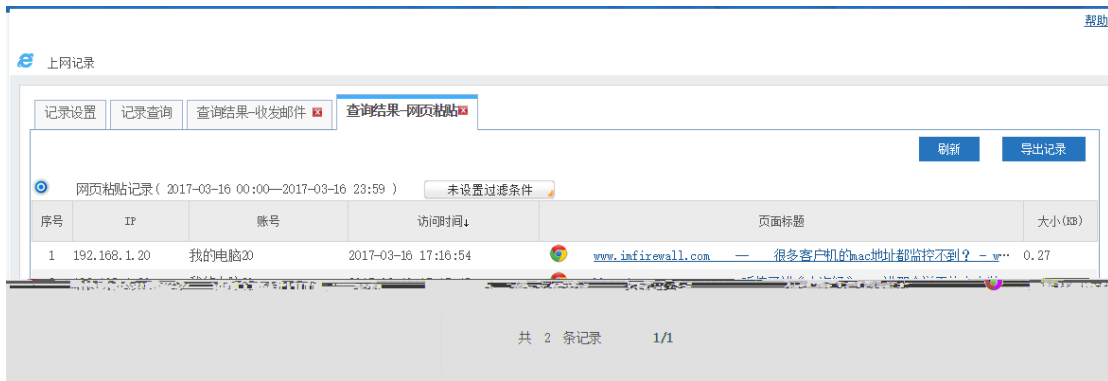
刷新 导出记录

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

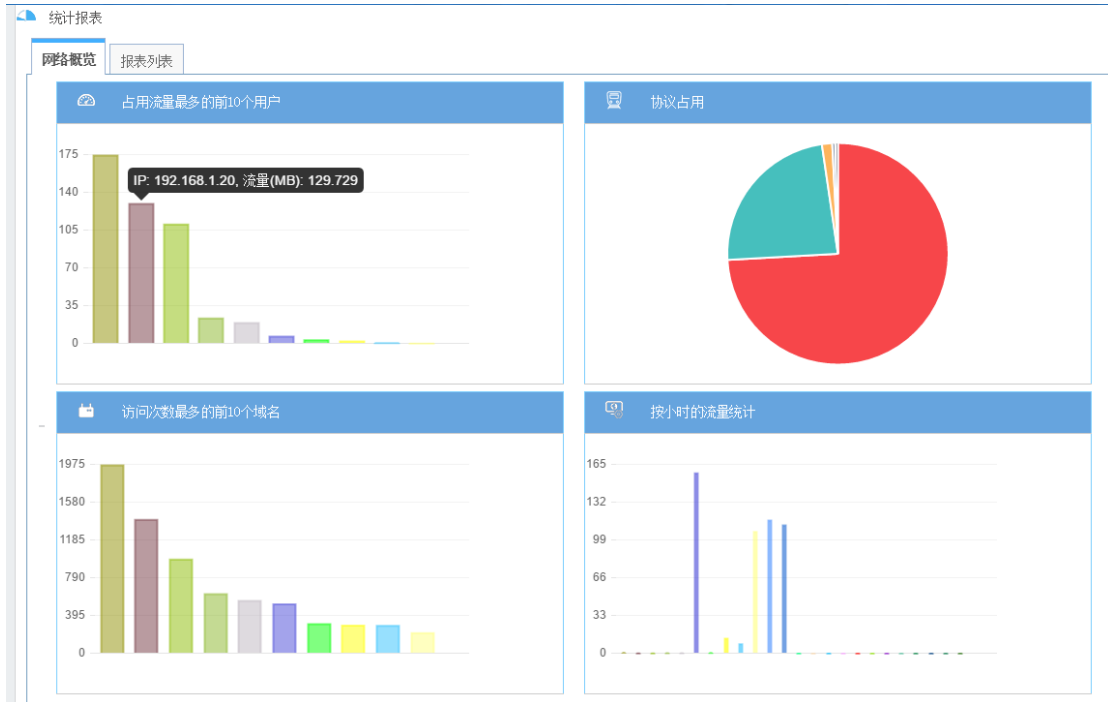
序号	IP	账号	时间↓	发送者	类型	邮件标题
1	192.168.1.20	我的电脑20	2017-03-16 16:07:01	jessfer@masterscrane.com	POP3接收	RE: WFilter Activation
2	192.168.1.20	我的电脑20	2017-03-16 16:01:40	postmaster@imfirewall.com.cn	POP3接收	系统退信
3	192.168.1.20	我的电脑20	2017-03-16 15:51:40	postmaster@imfirewall.com.cn	POP3接收	系统退信
4	192.168.1.21	Administrator	2017-03-16 14:22:44	support@imfirewall.com.cn	SMTP发送	感谢你购买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 报表概览和列表



统计报表

网络概览 报表列表

搜索条件

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	+	ON <input type="checkbox"/>	
2	Mail	所有	所有时间	指定协议分类	+	ON <input type="checkbox"/>	
	指定协议名称	<input type="text"/>	3	Web	所有	ON <input type="checkbox"/>	
	指定协议分类	<input type="text"/>	4	P2P & Streaming	所有	ON <input 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。

新增

名称: 规则1

应用对象: 限速规则

上行 下行

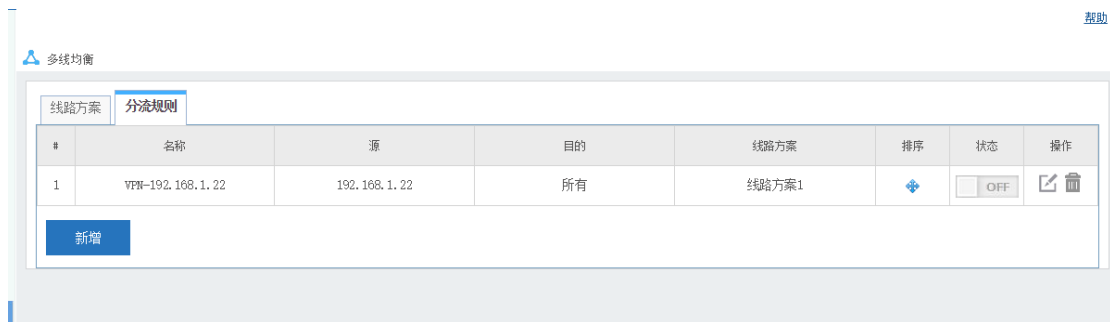
限制下行总带宽为 - Mbit

设置单IP最大带宽为 下行 Mbit

保存 取消

4.4.3 多线均衡策略

多线时，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。



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。

The screenshot shows the '域账户' (Domain Account) configuration page in the IMFirewall management system. The page is divided into two main sections: '域账户' and '高级配置' (Advanced Configuration).

域账户 Section:

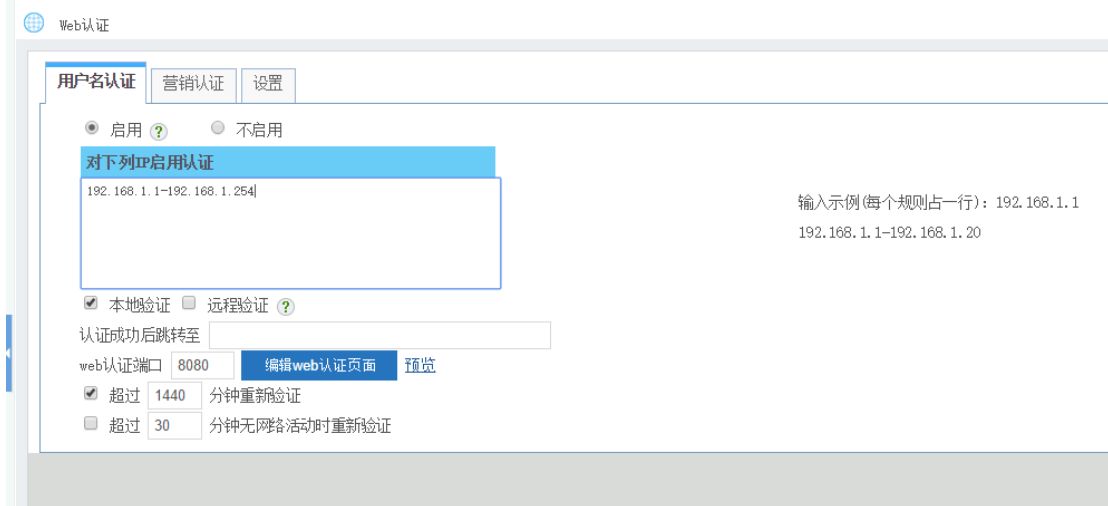
- 域账户:** Radio buttons for '启用' (Enabled) and '不启用' (Disabled). '启用' is selected.
- 域控制器IP:** Text input field containing '192.168.1.32'. A blue button '立即同步域账号' (Sync Domain Accounts Immediately) is to the right.
- 端口:** Text input field containing '389'.
- 域管理员账号:** Text input field containing 'administrator'.
- 密码:** Password input field with masked characters.
- 域名:** Text input field containing 'imfirewall01.com'.
- 域控制器位置:** Radio buttons for '外网' (External Network) and '内网' (Internal Network). '内网' is selected.

高级配置 Section:

- 每隔:** Text input field containing '10'. A label '秒轮询域控制器' (Poll domain controller every...) is next to it.
- 账户超时时间:** Checked checkbox. Text input field containing '30'. Label '小时' (Hours) is next to it.
- 自动同步域账号:** Checked checkbox. Text input field containing '每天' (Every day) and '00:00'.
- 启用调试模式:** Unchecked checkbox. Label '查看日志' (View logs) is next to it.
- 忽略下表中的账号:** A blue button with a question mark icon. Below it is an empty table with a scrollable area.
- 每个一行:** Text label.
- 支持通配符*和?:** Text label.

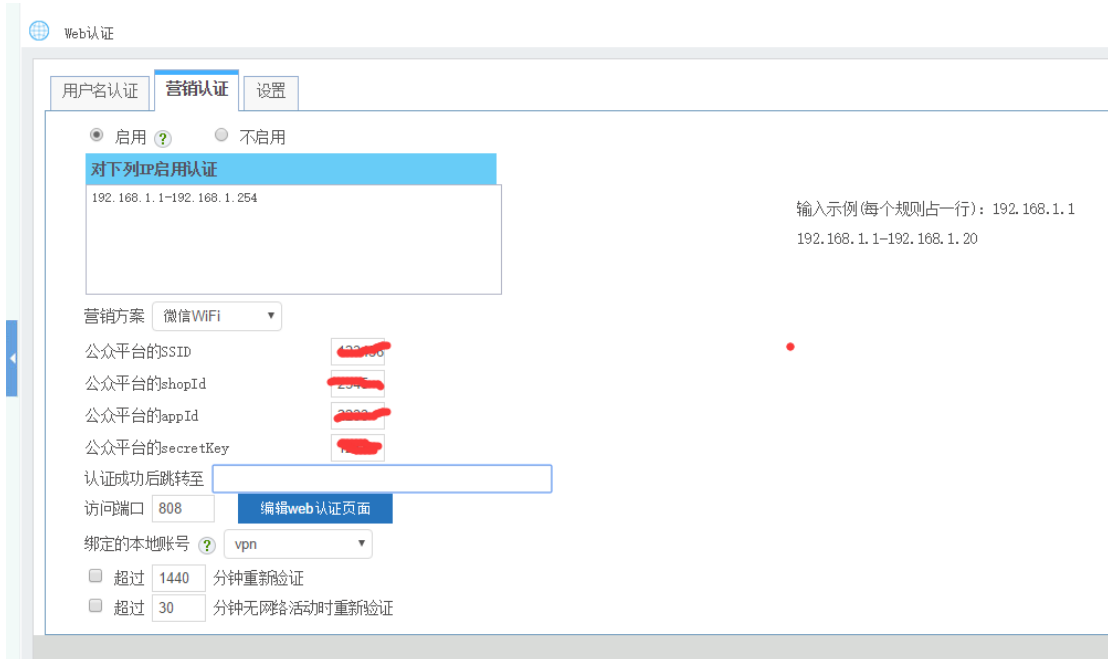
4.5.2 Web 认证和微信认证

基于用户名的 Web 认证，可以进行本地认证和远程 Radius 认证。



4.5.3 微信认证

关注微信公众号进行上网，可以和微信公众号集成。



4.5.4 PPPoE 认证

支持建立多个 PPPoE 服务，支持本地认证和远程 Radius 认证。

The screenshot shows a configuration window titled "编辑" (Edit) with a close button in the top right corner. The window contains the following fields and options:

- 监听网段 (Listening Segment): lan1 (dropdown)
- 服务名称 (Service Name): (empty text box)
- 客户机IP范围 (Client IP Range): 192.168.20.1 - 192.168.20.200
- 主dns (Primary DNS): 114.114.114.114
- 备用dns (Secondary DNS): (empty text box)
- 限速 (KB/s) (Speed Limit): 上行 (Upstream) and 下行 (Downstream) (empty text boxes)
- 认证方式 (Authentication Method): 本地认证 (Local Authentication) 远程认证 (Remote Authentication)
- 支持的协议 (Supported Protocols): chap mschap mschap-v2 pap

At the bottom right, there are two buttons: "保存" (Save) and "取消" (Cancel).

4.5.5 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。

The screenshot shows a configuration window titled "编辑" (Edit) with a close button in the top right corner. The window contains the following fields and options:

- 用户名 (Username): Bruce2
- 密码 (Password): (masked with dots)
- 确认密码 (Confirm Password): (masked with dots)
- 到期日期 (Expiration Date): 2017-05-04
- 联系邮箱 (Contact Email): wgeng@debian2.com, myliu@debian2.com
- 实时带宽 (Real-time Bandwidth): 实时限速2M (dropdown)
- 累计流量 (Accumulated Traffic): 累计流量每周1G (dropdown)
- 验证方式 (Authentication Method): PPPoE Web 静态IP (Static IP)

At the bottom, there is a note: "注意：修改用户属性会断开该用户的当前PPP连接。" (Note: Modifying user attributes will disconnect the user's current PPP connection.)

At the bottom right, there are two buttons: "保存" (Save) and "取消" (Cancel).

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: 每月第一天

超流量用户Email: 启用 不启用

发送时间: 每天

即将过期用户Email: 启用 不启用

发送时间:

- 过期前30天
- 过期前14天
- 过期前10天
- 过期前7天
- 过期前3天
- 过期前1天

4.6 VPN

- ✓ 支持 PPTP、IPSec、OpenVPN 等多种主流 VPN 接入。
- ✓ 支持多达 50 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。

4.7 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
- ✓ Logo 修改器
- ✓ 网络健康度检测等。

4.7.1 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。	imfirewall
2	网络健康监测	网络健康监测	imfirewall
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。	imfirewall
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。	imfirewall
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…	imfirewall
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。	imfirewall
7	Logo修改器	该插件可以自定义WFilter ROS的产品名称和Logo图标	imfirewall

共 7 条记录 1/1

下载插件 新增插件 导入插件

4.7.2 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： 启用 不启用

调试日志： 记录 不记录 [查看日志](#)

轮询间隔：

SNMP配置

#	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+.*	  

添加 测试

保存

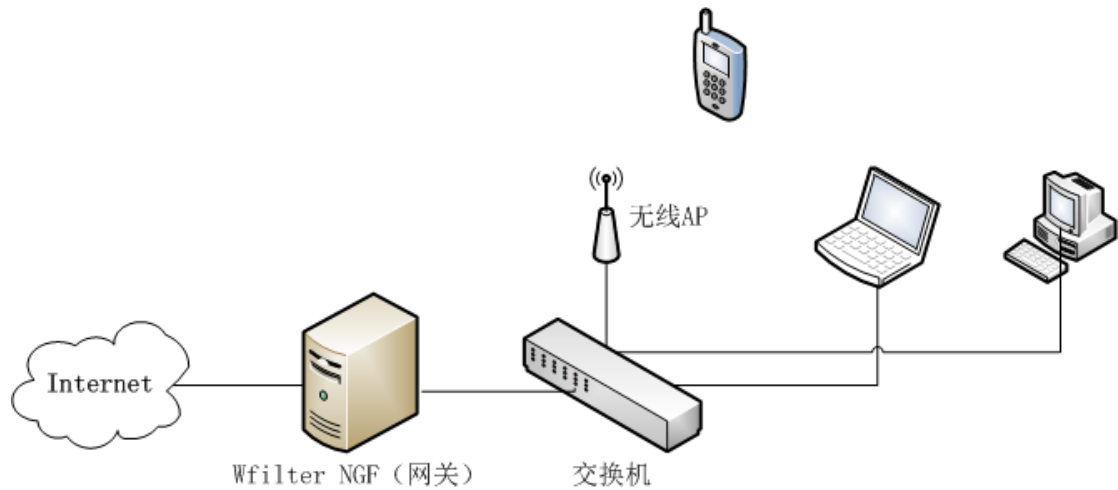
4.7.3 随身 WiFi 和私接路由检测

可以检测出网内的非法共享，并且设置惩罚策略。

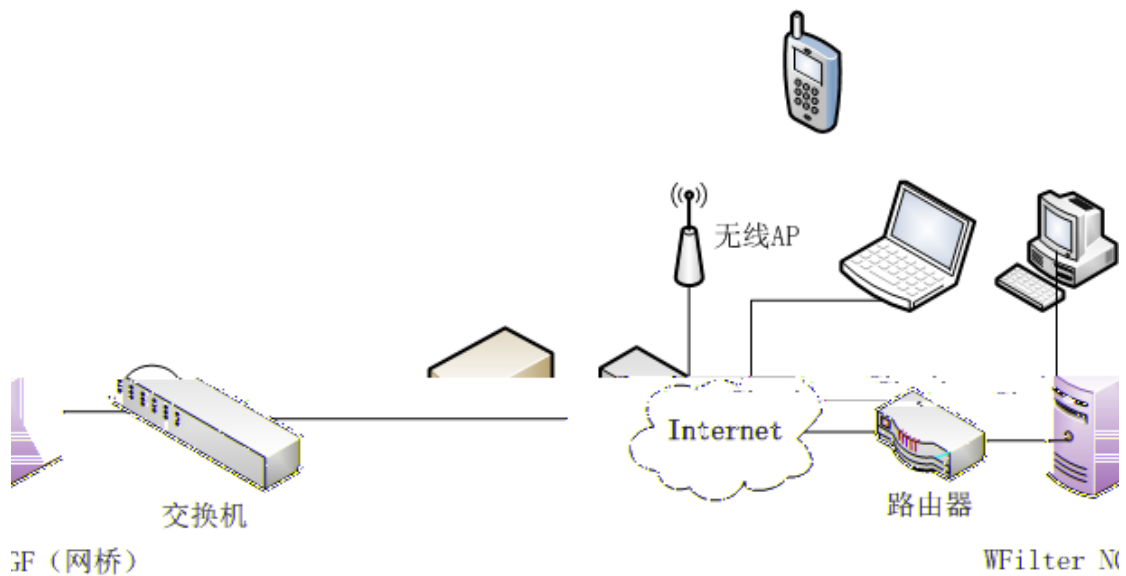


5 典型部署方案

1. 网关部署模式



2. 网桥部署模式



公司名称： 南京笨驴信息技术有限公司：

公司地址： 南京市瑞金路 21 号友谊商务大厦 202 (邮编:210007)

电话： 400-018-0186 025-84632168

传真： 025-84632168-806

电子邮件： support@imfirewall.com.cn

中文网址： <http://www.imfirewall.com>

English: <http://www.imfirewall.us>