

WFilter NG Firewall

1 Introduction.....	2
2 Highlights.....	2
3 Benefits.....	3
3.1 Bandwidth Optimization.....	3
3.2 Increase Productivity.....	3
3.3 Data Loss Prevention.....	3
4 Features.....	4
4.1 Real-time monitoring and control.....	4
4.1.1 Online Devices.....	4
4.1.2 Live Connections.....	5
4.1.3 Terminate & Punish.....	5
4.2 Access Control.....	6
4.2.1 Set policy by devices or users.....	6
4.2.2 Web Filtering.....	8
4.2.3 Application Control.....	8
4.2.4 IP-MAC Binding.....	9
4.2.5 Mail Filter.....	9
4.2.6 SSL Inspection.....	10
4.3 Internet Usage Recording and Reports.....	11
4.3.1 Web Surf History.....	12
4.3.2 Email History.....	13
4.3.3 Reports.....	14
4.4 Bandwidth Optimization.....	14
4.4.1 Optimize Rules.....	15
4.4.2 Rate Limit.....	15
4.4.3 Multi-WAN.....	15
4.5 User Authentication.....	16
4.5.1 AD Integration.....	16
4.5.2 Web Auth.....	17
4.5.3 PPPoE.....	18
4.5.4 ISP Management.....	19
4.6 VPN.....	20
4.7 Security.....	21
4.7.1 DDos Protection.....	21
4.7.2 Intrusion Protection.....	22
4.7.3 Indicators of Compromise.....	23
4.8 Extensions.....	24
4.8.1 MAC Detector.....	24

5 Deployment.....	25
5.1 Gateway.....	25
5.2 Bridge.....	25

1 Introduction

WFilter NG Firewall(NGF) is a linux-based next generation firewall system. Designed for business networks, it can help you to monitor and filter internet access activities, optimize bandwidth usage, and protect network security.

Since 2004, IMFirewall Software has been focused on business network security for over ten years. Our products(WFilter internet content filter, WFilter NG firewall) provide competitive internet content security and network security solutions for business networks.

2 Highlights

- ✧ Real-time monitoring and control. Put every connection under control.
- ✧ Internet Usage Monitoring: recording of web and email activities, various statistics and reports, SSL inspection.
- ✧ Powerful Internet Filtering Features: connection tracking, URL category filtering, application control, messenger filter ...
- ✧ Bandwidth Shaper and Optimizer: multi-wan load balancing, advanced routing, packet priority, bandwidth shaper.
- ✧ VPN: pptp server, ipsec tunnels.
- ✧ Continuous research and development for over ten years.

3 Benefits

3.1 Bandwidth Optimization

WFilter NG Firewall provides a set of solutions for bandwidth optimization, including:

1. Set traffic priority
2. Bandwidth Allocator
3. Multiple WANs load-balancing and routing
4. Internet access policy

For better internet experience, you're recommended to:

1. Apply multiple DSL lines according to your requirement, then enable the Muti-WAN module to set load balancing and advanced routing.
2. Enable the Bandwidth Priority Module to set traffic priority, and let business traffic to be delivered first.
3. Enable the Bandwidth Shaper Module to allocate bandwidth for client devices or groups.
4. Set internet access policy with Access Policy Modules, and block unneeded traffic during working hours to save bandwidth.

3.2 Increase Productivity

WFilter NGF provides enterprise-level internet access control features:

1. Set internet access policy by network, ip address, mac address or username.
2. Various types of user authentication: AD integration, web auth, radius server ...
3. Support up to 60+ web categories and 2000+ protocols.
4. Identify protocols by signature matching. P2P applications can all be completely blocked.

3.3 Data Loss Prevention

WFilter NGF can provide recording of web and email activities, internet usage statistics

and reports, SSL inspection.

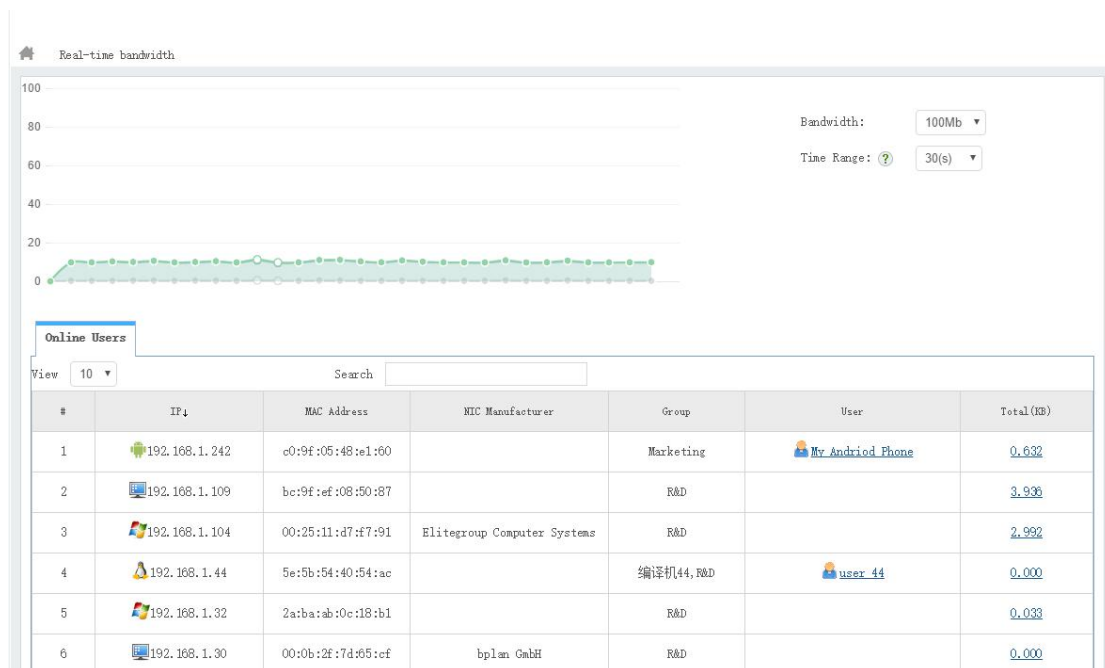
1. Recording of web and email usage.
2. SSL inspection of SMTP/POP3/IMAP over ssl and HTTP over SSL.
3. Internet usage statistics and reports.
4. Blocking online file storage and sharing services.

4 Features

4.1 Real-time monitoring and control

- ✓ Real-time bandwidth and connections monitoring. Put every connection under control.
- ✓ List of live clients, with bandwidth, IP, MAC, username and OS information.
- ✓ List of live connections, with target port, ip and domain information.
- ✓ One click to kill live connections or set temporary punishing policy.

4.1.1 Online Devices



4.1.2 Live Connections

All Connections - 192.168.1.109

Live Connections Blocking Events

View 10 Search Unblock and reset

#	Local Port	Content	Type	Protocol	Content	Bandwidth(KB)↓	Action
1	52621	180.101.217.140:443	TCP	TLS,HTTPS	qcloud.dpfile.com	11.381	
2	52636	59.56.18.215:443	TCP	TLS,HTTPS	pl.meituan.net	1.588	
3	52639	218.92.1.12:443	TCP	TLS,HTTPS	p0.meituan.net	1.402	
4	52550	103.37.152.74:443	TCP	SSL,HTTPS	report.meituan.com	1.146	
5	52637	115.159.129.148:443	TCP	TLS,HTTPS	catdot.dianping.com	0.345	
6	52506	115.159.130.100:443	TCP	SSL,HTTPS		0.049	
7	52640	114.80.165.113:443	TCP	TLS,HTTPS	mapi.dianping.com	0.011	
8	52642	180.153.8.37:80	TCP	Web(HTTP)	180.153.8.37:80	0.000	
9	52441	61.155.221.227:80	TCP			0.000	
10	52641	180.153.8.37:80	TCP	Web(HTTP)	180.153.8.37:80	0.000	

4.1.3 Terminate & Punish

Action

Kill this connection only

Block 192.168.1.109 Alipay for 1 minute

Block 192.168.1.109 all internet access for 24 hours

Message(?):

Add to Punish Group for 1 hour

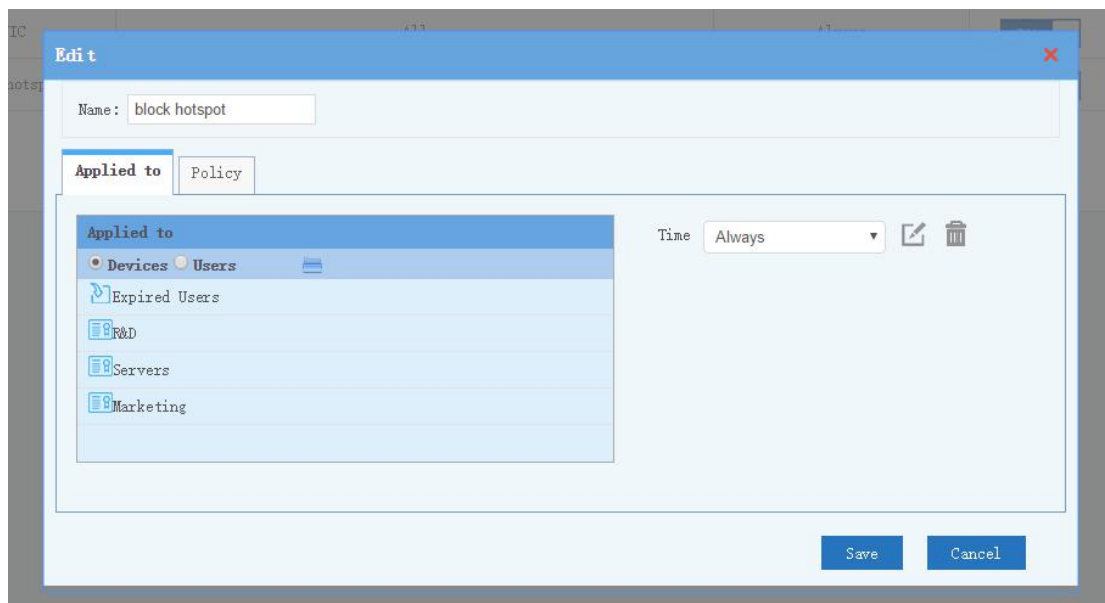
Save Cancel

4.2 Access Control

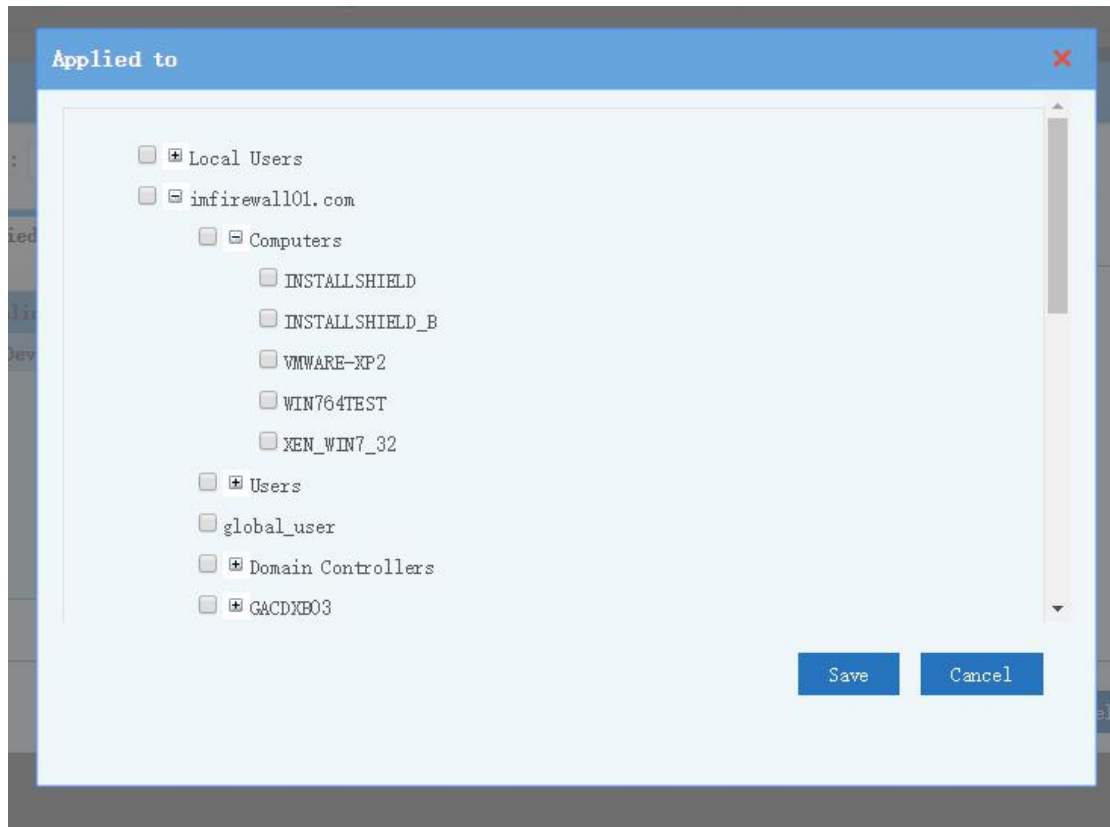
- ✓ Web filter, application control, IM filter, mail filter, IP-MAC binding...
- ✓ Set internet access policy by network, ip address, mac address or username.
- ✓ Various types of user authentication: AD integration, web auth, radius server ...
- ✓ Support up to 60+ web categories and 2000+ protocols.
- ✓ Identify protocols by signature matching. P2P applications can all be completely blocked.

4.2.1 Set policy by devices or users

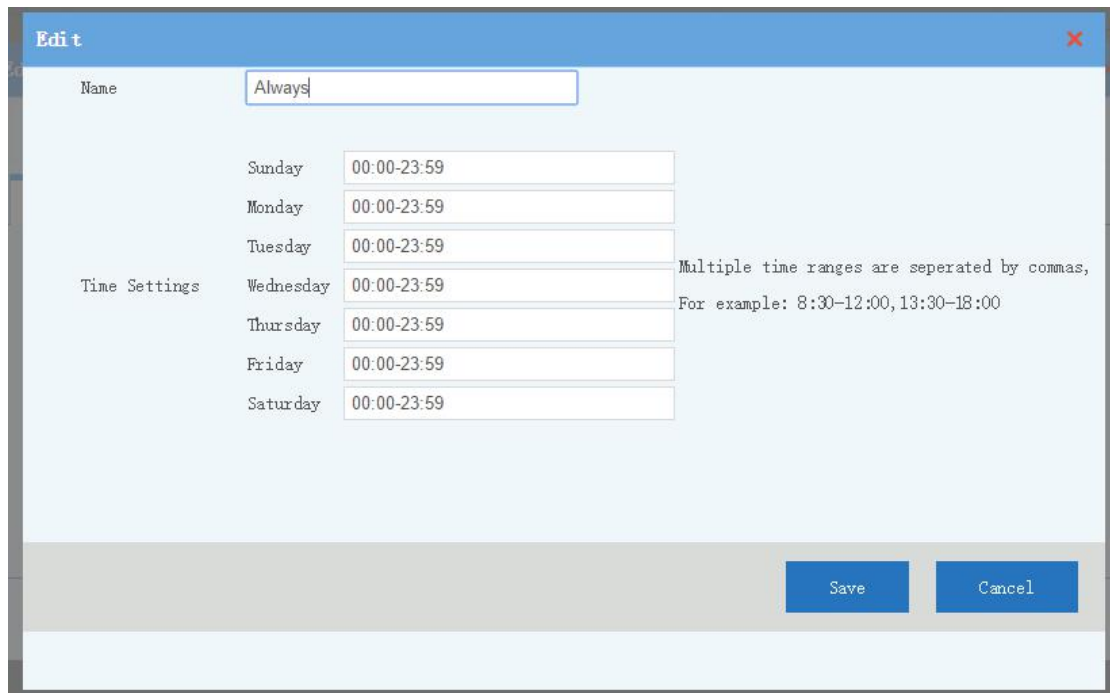
By devices



By Users

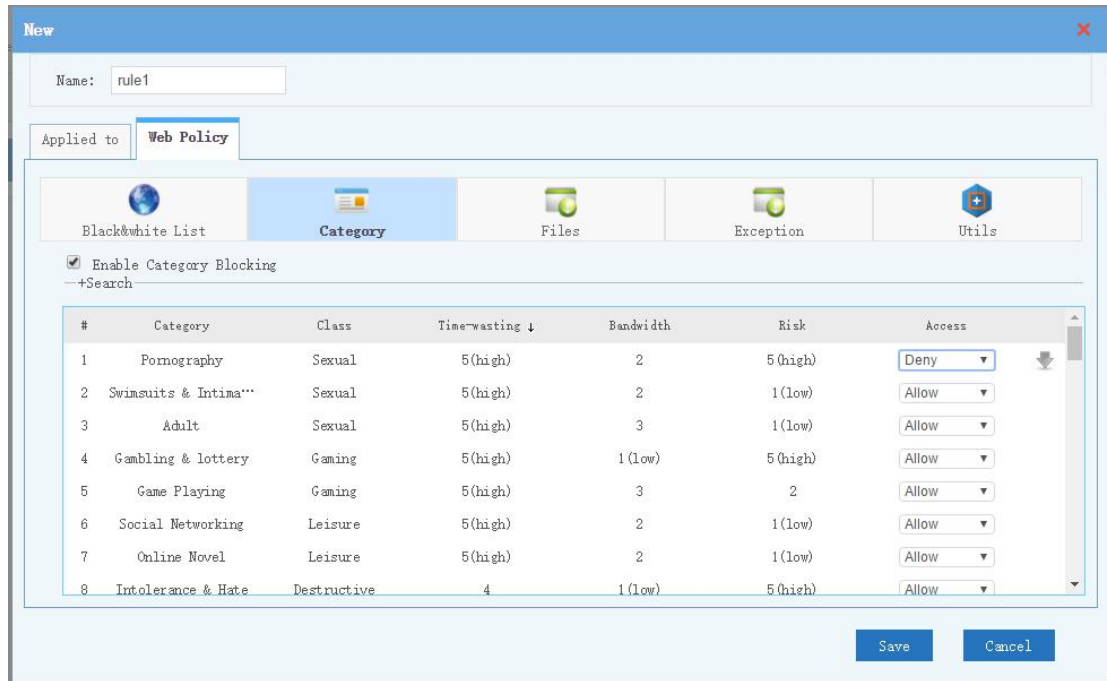


Time Settings

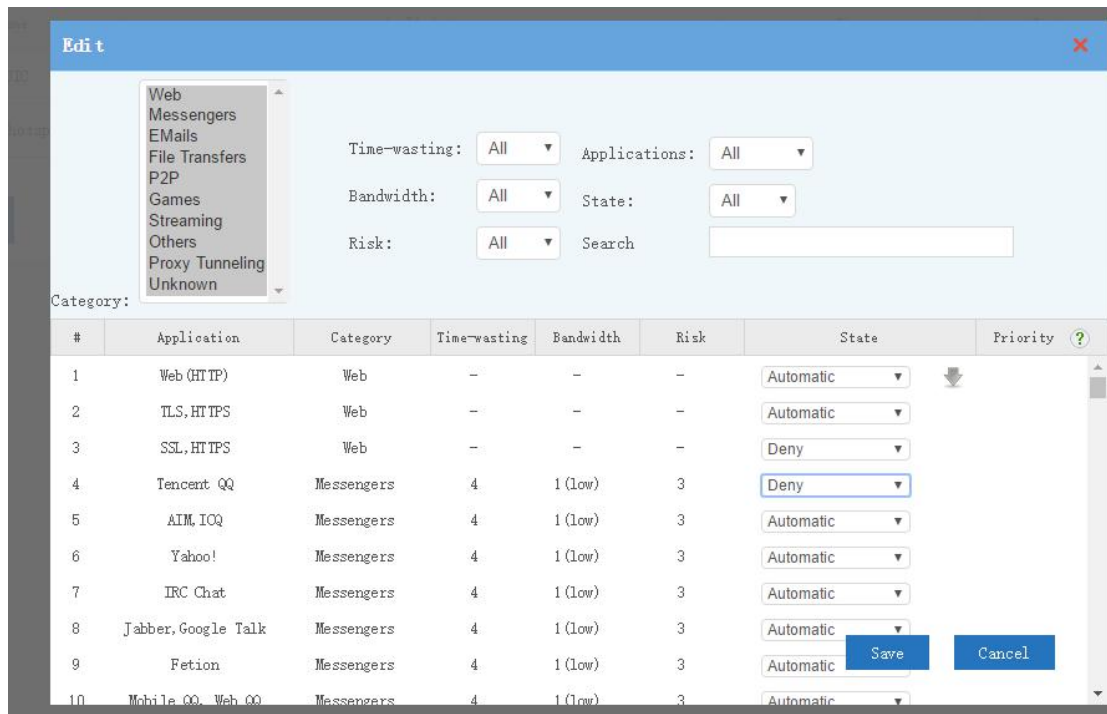


4.2.2 Web Filtering

Filter websites by category, website black&white list, block file downloading by type.



4.2.3 Application Control



4.2.4 IP-MAC Binding

IP-MAC Binding

Config

Block ip not in the below list

IP-MAC List

Search:

View: 10 ▾

#	IP	HWaddr	Remark	State	Action
1	192.168.1.20	00:0b:2f:7b:df:f0		ON <input type="checkbox"/>	
2	192.168.1.11	00:50:56:c0:10:c8		ON <input type="checkbox"/>	
3	192.168.1.134	6e:df:bf:57:fa:22		ON <input type="checkbox"/>	
4	192.168.1.109	bc:9f:ef:08:50:87		ON <input type="checkbox"/>	
5	192.168.1.131	46:cc:2f:f5:7b:eb		ON <input type="checkbox"/>	

1/1 , Total 5 record(s)

[New](#) [Scan & Remove](#) [Export](#)


4.2.5 Mail Filter


Filter POP3/SMTP/IMAP accounts.

New ✕

Name:

Applied to: **Policy**


Outgoing Emails


Incoming Emails

Sender: Allow all Block Listed Allow Listed Only

Address List

When white list is enabled, only emails in the white list are available. When black list is enabled, all black-listed emails will be blocked. One address per line, wildcard(*) is supported.

Mail to: Allow all Block Listed Allow Listed Only

Address List

4.2.6 SSL Inspection

When enabled, you will be able to monitor and filter the contents of HTTPS websites and SSL emails(SMTP/POP3/IMAP over SSL)

New

Name: rule1

Applied to | **SSL Policy**

Services : Web POP3 IMAP SMTP

More port(s)

Remote IP: Exclude below list Below IPs only

Remote IP ?

Services to be intercepted.
More port(s) to be intercepted, one port per line, eg:
8080

One IP segment or domain per line,
example:
192.168.1.0/24,172.10.0.0/16,*.google.com

Save Cancel

4.3 Internet Usage Recording and Reports

- ✓ Record web, email, FTP activities, IP-mac history.
- ✓ SSL inspection of https websites and ssl emails.
- ✓ Various statistics and reports.

New
✕

Name:

Applied to SSL Policy

Services : Web POP3 IMAP SMTP

More port(s)

Remote IP: Exclude below list Below IPs only

Remote IP ?

Services to be intercepted.

More port(s) to be intercepted, one port per line, eg:
8080

One IP segment or domain per line, example:
192.168.1.0/24,172.10.0.0/16,*.google.com

Save

Cancel

4.3.1 Web Surf History

Internet Usage

Recording Policy
Usage Query
Report — Web Surf
Report — Web Surf

Reload

Export

Record Web Surfing (2017-03-17 00:00—2017-03-17 23:59) No Filter

#	IP	Users	Visit Time	Web Title
211	192.168.1.104		2017-03-17 14:26:51	motashin.com - متاشين :: برنال متاشين : سيمكو جشمه اطلاع رساني جهان اسلام
212	192.168.1.104		2017-03-17 14:26:51	www.biofeedbackanalytics.com - אמוני ביפידוק באינטרנט
213	192.168.1.104		2017-03-17 14:26:51	biofeedbackanalytics.com - אמוני ביפידוק באינטרנט
214	192.168.1.104		2017-03-17 14:26:49	neonieruchomosci.pl - neonieruchomości - zielona góra, poznań...
215	192.168.1.104		2017-03-17 14:26:49	www.horizont-n.pl
216	192.168.1.104		2017-03-17 14:26:49	www.ipsglobal.org
217	192.168.1.104		2017-03-17 14:26:49	www.centeredlearning.de - centered learning - karriere und weit...
218	192.168.1.104		2017-03-17 14:26:49	www.bhmedia.vn - bhmedia - công ty cổ phần truyền thông đại chúng...
219	192.168.1.104		2017-03-17 14:26:49	www.lichman-nieruchomosci.com - domy i mieszkania na sprzedaż ...
220	192.168.1.104		2017-03-17 14:26:39	www.lichman-nieruchomosci.com - domy i mieszkania na sprzedaż ...
221	192.168.1.104		2017-03-17 14:26:39	www.centeredlearning.de - centered learning - karriere und weit...
222	192.168.1.104		2017-03-17 14:26:39	neonieruchomosci.pl - neonieruchomości - zielona góra, poznań...
223	192.168.1.104		2017-03-17 14:26:39	www.horizont-n.pl
224	192.168.1.104		2017-03-17 14:26:26	euromanna.pl - strona główna
225	192.168.1.104		2017-03-17 14:26:26	www.euromanna.pl - strona główna

⏪ ⏩ 13 14 15 16 17 18 19 20 21 22 ⏩ ⏪

15/640

Total 9586 record(s)

4.3.2 Email History

Internet Usage

Recording Policy | Usage Query | Report —Web Surf | Report —Web Surf | **Report —Emails**

Reload | Export

Email History (2017-03-16 00:00—2017-03-17 23:59)

#	IP	Users	Time	Sender	Type	Subject
46	192.168.1.21	Administrator	2017-03-16 10:00:33	support@imfirewall.com.cn	POP3 In	
47	192.168.1.21	Administrator	2017-03-16 10:00:33	support@imfirewall.com.cn	POP3 In	
48	192.168.1.21	Administrator	2017-03-16 10:00:33	support@imfirewall.com.cn	POP3 In	
49	192.168.1.21	Administrator	2017-03-16 10:00:32	support@imfirewall.com.cn	POP3 In	
50	192.168.1.21	Administrator	2017-03-16 10:00:32	ebates@mail.ebates.cn	POP3 In	【海淘】Raymond, Rado, Hamilton 独家折扣+福利...
51	192.168.1.21	Administrator	2017-03-16 10:00:31	support@imfirewall.com.cn	POP3 In	
52	192.168.1.21	Administrator	2017-03-16 10:00:25	service@newsletter.chinabyte.com	POP3 In	1
53	192.168.1.21	Administrator	2017-03-16 10:00:25	service@newsletter0.chinabyte.com	POP3 In	
54	192.168.1.21	Administrator	2017-03-16 10:00:25	bdwenjuan@baidu.com	POP3 In	百度官方邀请: 客户满意度调研 (有奖)
55	192.168.1.21	Administrator	2017-03-16 10:00:16	forums@tomshardware.com	POP3 In	Reply Received for website blocking fo...
56	192.168.1.21	Administrator	2017-03-16 10:00:08	kkemedy@eberman.com	POP3 In	No love failure risk
57	192.168.1.21	Administrator	2017-03-16 10:00:08	jessfer@masterscrane.com	POP3 In	RE: WFilter Activation
58	192.168.1.21	Administrator	2017-03-16 10:00:08	jessfer@masterscrane.com	POP3 In	WFilter Activation
59	192.168.1.20	我的电脑20	2017-03-16 09:56:40	kkemedy@eberman.com	POP3 In	No love failure risk
60	192.168.1.20	我的电脑20	2017-03-16 09:56:40	jessfer@masterscrane.com	POP3 In	RE: WFilter Activation

Navigation: < << 2 3 4 5 >> > Total 67 record(s) 4/5

View Email Content

Export

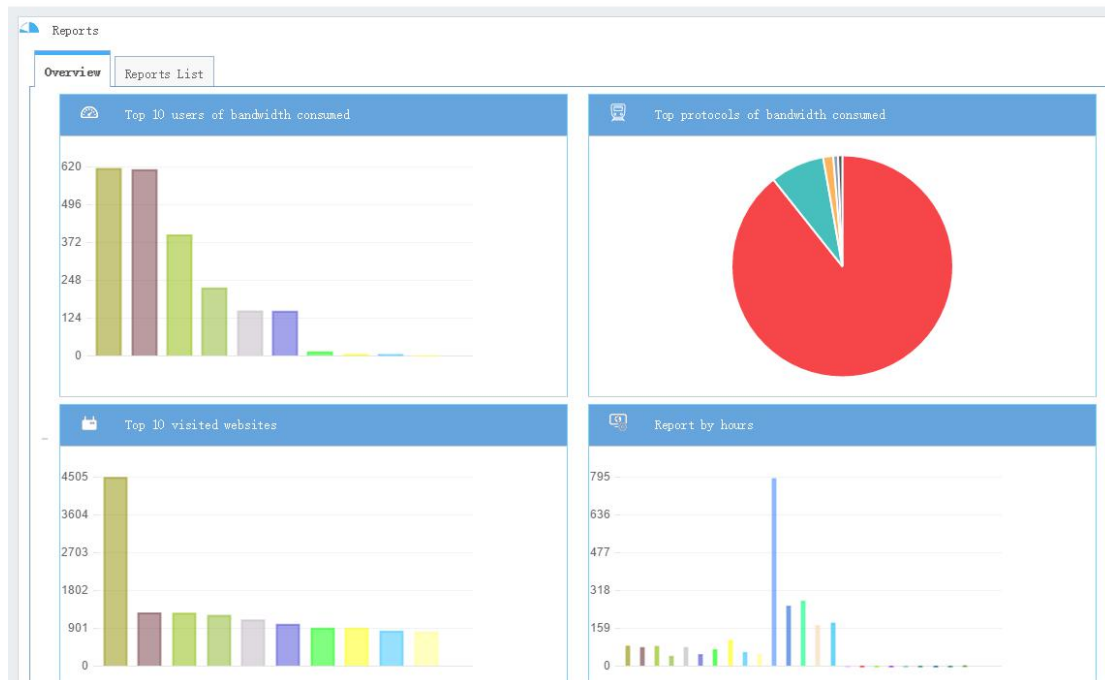
From: Tom's Hardware <forums@tomshardware.com>
 Date: Wed, 15 Mar 2017 12:59:11 +0100
 To: sales@imfirewall.us
 Cc:
 Subject: Reply Received for website blocking for network
 Attachment:
 Body: DISPLAYMAIL INTXT

tom's HARDWARE
THE AUTHORITY ON TECH

Hello Tina_Jiang,

nigelvey has posted a new reply to the question you've been following "[website blocking for network](#)"

4.3.3 Reports



The screenshot displays the 'Reports List' page with a table of reports:

#	Report Type	Report Alias	Action
1	Activity	Top 20 visited websites	🔍 📄 🗑️
2	Activity	report by users	🔍 📄 🗑️
3	Activity	Report by groups	🔍 📄 🗑️
4	Activity	指定域用户统计	🔍 📄 🗑️
5	Bandwidth	Top 20 websites of bandwidth consumed	🔍 📄 🗑️
6	Bandwidth	占用流量最多的20个IP	🔍 📄 🗑️
7	Bandwidth	占用流量最多的10种协议	🔍 📄 🗑️
8	Trend	Trend of web visits	🔍 📄 🗑️
9	Trend	Trend of bandwidth	🔍 📄 🗑️
10	Trend	Trend of visits to news websites	🔍 📄 🗑️
11	Trend	Trend of visits to job search websites	🔍 📄 🗑️
12	Trend	Trend of visits to streaming websites	🔍 📄 🗑️
13	Trend	Trend of visits to microblogging websites	🔍 📄 🗑️

At the bottom of the table, there is a 'New' button and a help icon (?).

4.4 Bandwidth Optimization

- ✓ Packet with higher priority goes first. This feature ensures important traffic won't be delayed.

- ✓ Set bandwidth priority by protocols or domains. Online streaming won't delay web browsing.
- ✓ Multi-wan load balancing and advanced routing. Maximum your WAN lines usage.
- ✓ Set bandwidth rate-limit by IP, group, username.

4.4.1 Optimize Rules

You can set priority based on IP, users group, usernames, protocols and domains.

Priority

#	Name	Applied to	Time	Content	Reorder	State	Action
1	Mail	all	All Time	By Protocol Categ...	⬆️⬇️⬆️	ON <input type="checkbox"/>	✎️ 🗑️
2	Web	all	All Time	By Protocol	⬆️⬇️⬆️	ON <input type="checkbox"/>	✎️ 🗑️
3	P2P & Streaming	all	All Time	By Protocol Categ...	⬆️⬇️⬆️	ON <input type="checkbox"/>	✎️ 🗑️

New

4.4.2 Rate Limit

Limit bandwidth rate based on IP, group and user account.

New

Name: rule1

Applied to: Policy

Up Down

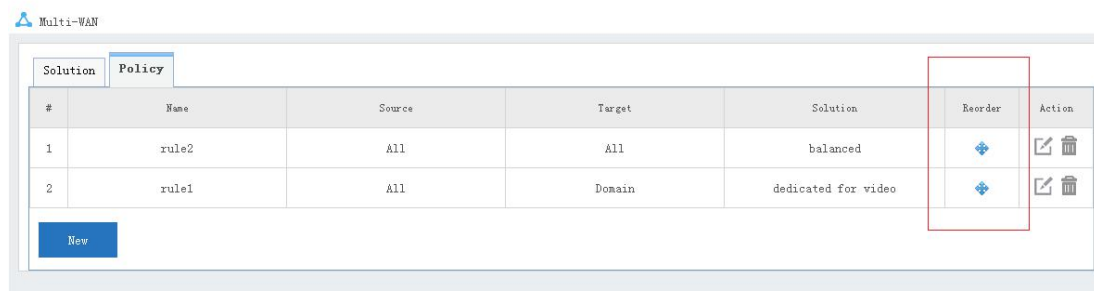
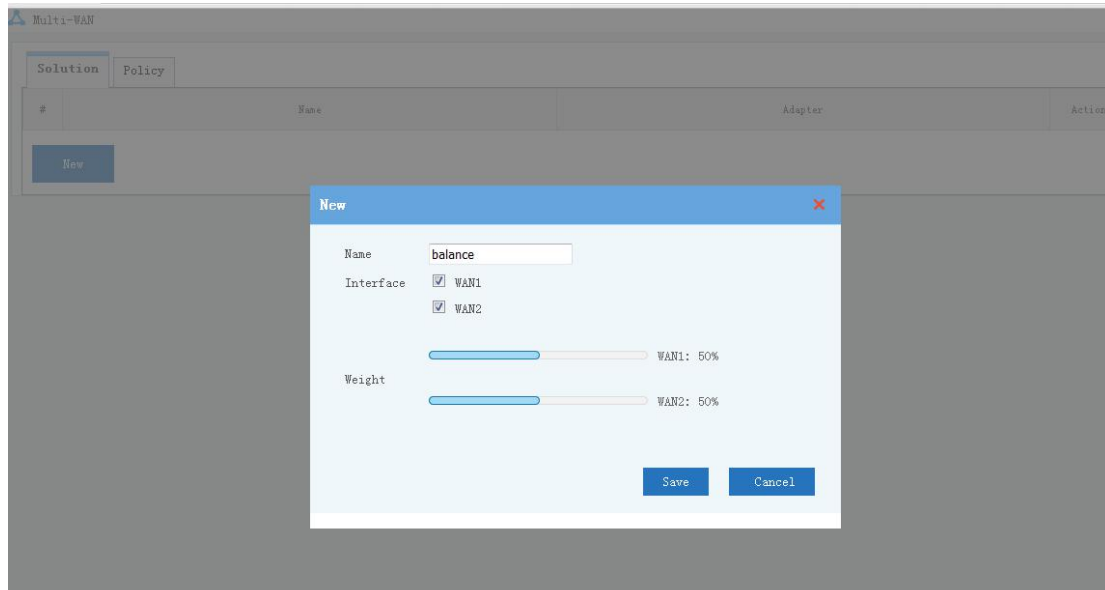
Limit total down bandwidth to ? - 20 Mbit ▾

Set client maximum rate to ? Down 2 Mbit ▾

Save Cancel

4.4.3 Multi-WAN

Set load balancing and advanced routing when you have multiple WAN interfaces.



4.5 User Authentication

4.5.1 AD Integration

"AD Integration" enables you to integrate WFilter NG Firewall with Microsoft active directory, so you can:

1. Detect AD username of online devices.
2. Set internet access and bandwidth shaper policies based on AD users.
3. Record AD users internet activity.

AD Intergration ?

AD Intergration

AD Intergration Enable Disable

Domain Controller: 192.168.1.32 Sync

Port: 389

Domain Admin: administrator

Password: [Redacted]

Domain Name: imfirewall01.com

DC Location: WAN LAN

Advanced Settings

Interval of polling domain controller: 10 ?

Enable user entry timeout: 30 hour(s)

Automatically sync domain users: Everyday 00:00

Enable Debug Check Log

User Exception List ?

Users will be ignored, one account per line, wildcards(*,?) are supported.

4.5.2 Web Auth

Authenticate with username and password of local accounts and remote radius users.

Web Auth

User & Pass Auth | Third Party Auth | Settings

Enable ? Disable

IP Range: 192.168.1.1-192.168.1.254

One IP/Range per line.
For example:192.168.1.1
192.168.1.1-192.168.1.20

Local Auth Remote Auth ?

Landing Page: [Empty]

Port: 8080 Edit Auth Page Preview

Require re-authentication every 1440 minutes

Require re-authentication every 30 minutes of no internet activity

Save

SMS authentication, QR code authentication

Web Auth

User & Pass Auth Third Party Auth **Visitor Auth** Settings

Enable Disable

IP Range

172.16.0.1/16
192.168.28.0/24 #test
-192.168.28.253

One IP/Range per line. "#" starts a comment,
192.168.1.1
192.168.1.0/24
192.168.1.1-192.168.1.20
-192.168.1.10

Type

Settings

Visitors Name

Moderators

Moderators IP or MAC addresses

Landing Page

Port

Require re-authentication every minutes
 Require re-authentication every minutes of no internet activity

4.5.3 PPPoE

You can set multiple PPPoE services.

Edit

Interface

Service Name

IP Range -

Preferred DNS

Alternate DNS

Bandwidth Limit(KB/s) Up Down

Auth Type Local Auth Remote Auth

Radius

Radius Server

PreShared Key

Authentication Port

Accounting Port

Auth Protocols chap mschap mschap-v2 pap

4.5.4 ISP Management

"ISP Management" provides an integrated solution for ISP management, including below features:

1. Policy management: manage ISP bandwidth policies, support "rate limiting" and "weekly/monthly bandwidth cap".
2. User management: add/edit/delete client users, query users bandwidth statistics.
3. User portal: a portal for client users to check bandwidth statistics.
4. Supports "PPPoE" and "Web Auth" and "Static IP" authentication.
5. Supports "Web Push" to send alerts and statistics to clients.

The 'New' dialog box is used for creating a new user. It contains the following fields and options:

- Username: test3
- Password: [masked]
- Confirm Password: [masked]
- Valid Until: 2020-09-25
- Email(s): test3@imfirewall.com, test3@imfirewall.com.cn
- Policy: Monthly 30G(Bandwidth Cap)
- Access Type: PPPoE, Web, Static IP
- Bound to IP: 192.168.1.20

Buttons: Save, Cancel

The 'Settings' dialog box is used for configuring automatic user management. It contains the following settings:

- Automatic add users expiring in 30 days to group: Expiring Users
- Automatic add expired users to group: Expired Users

Buttons: Save, Cancel

ISP

Policy Users User Portal **Emails**

Email to valid users: Yes No

Send email on: First day for every month

Email to cap exceeded users: Yes No

Send email on: Every monday

Email to expiring users: Yes No

Send email when user:
 expires in 30 days
 expires in 14 days
 expires in 10 days
 expires in 7 days
 expires in 3 days
 expires in 1 day

4.6 VPN

- ✓ Support pptp, l2tp, openVPN, zerotier networks.
- ✓ Connect multiple networks together with ipsec tunnels.
- ✓ Various VPN user authentication: local accounts, active directory, radius server.

4.7 Security

4.7.1 DDos Protection

Anti DDOS

Anti DDOS

Settings

DDOS Protection: [?](#) Enable Disable [||](#)

DDOS Settings

- Disable Ping on WAN Interfaces
- Drop Fragmented Packets
- Drop Invalid Packets
- Enable Protection on Forwarding [?](#)
- Enable SYN Flood Protection Rate-burst - [?](#)
- Enable UDP Flood Protection Rate-burst -
- Enable ICMP Flood Protection Rate-burst -

Geo-IP Filter

Geo-IP Filter: Total **4** countries choosed.

IP Whitelist

192.168.1.24

One ip or subnet per line. For example:
192.168.1.20
192.168.1.20/24

4.7.2 Intrusion Protection

IPS

Threat history

Settings

IPS Protection: Enable Disable

IPS Settings

WAN Attacks: Record only

LAN Attacks: Record only

Alert: Alert on all attacks

Rules Set: [os-linux,os-mobile,os-other,os-solaris,...](#) [Edit](#)

Network

Interfaces: Customize eth0 eth1 eth2 eth3

Variables: Customize [Edit](#)

IP Whitelist

IP Whitelist

One ip or subnet per line. For example:

192.168.1.20

192.168.1.20/24

Edit				
Rules Set				
#	Class	Rule name	State	Action
1	System	os-linux	ON <input type="checkbox"/>	
2	System	os-mobile	ON <input type="checkbox"/>	
3	System	os-other	ON <input type="checkbox"/>	
4	System	os-solaris	ON <input type="checkbox"/>	
5	System	os-windows	ON <input type="checkbox"/>	
6	Protocol	protocol-dns	ON <input type="checkbox"/>	
7	Protocol	protocol-finger	ON <input type="checkbox"/>	
8	Protocol	protocol-ftp	ON <input type="checkbox"/>	
9	Protocol	protocol-icmp	ON <input type="checkbox"/>	
10	Protocol	protocol-imap	ON <input type="checkbox"/>	

1 2 3 4 >> ≥| 1/4 , Total 33 record(s)

4.7.3 Indicators of Compromise

Indicators of compromise

Indicators of compromise | Detection history

Settings

IOCs: Enable Disable

IOCs Settings

Upon detected: Record only

Alert: Add alert events

Rules Set: [malware-backdoor,malware-cnc,malwa...](#) [Edit](#)

IP Whitelist

192.168.1.24

One ip or subnet per line. For example:
192.168.1.20
192.168.1.20/24

4.8 Extensions

- ✓ Scan of network client devices.
- ✓ Detection of NAT sharing.
- ✓ Scan of local proxy servers.
- ✓ Discovery of DHCP servers.
- ✓ More extensions for downloading. You also can build extensions by yourself.

4.8.1 MAC Detector

"MAC Detector" can gather client's physical MAC addresses via SNMP protocol.

MAC Detector

MAC Detector: Enable Disable

Debug: Enable Disable [Check Log](#)

Polling Interval: 60s

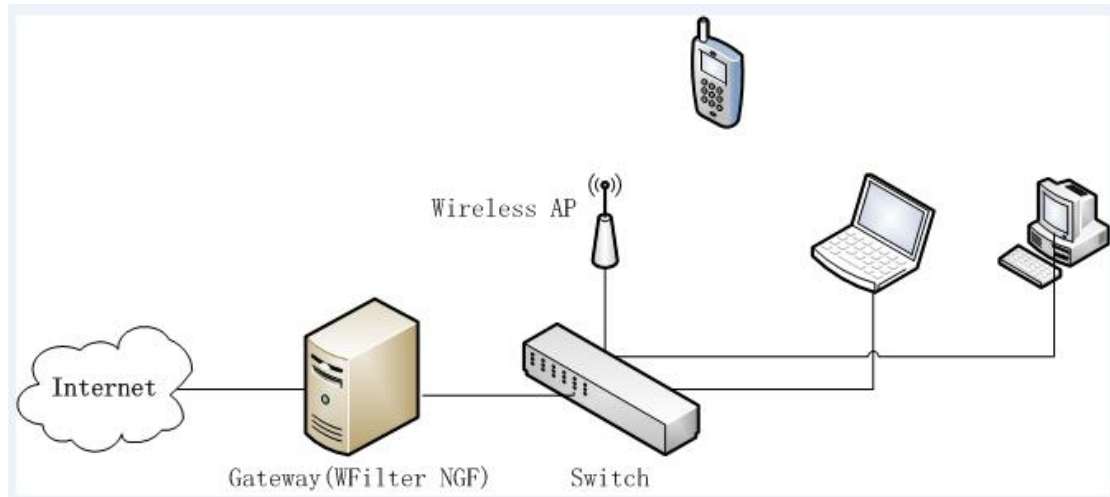
SNMP Queries

#	SNMP Commands List	Result Format	Action
1	snmpwalk -v 2c -c public 192.168.1.2 ipNetToMediaPhysAddress	IP-MIB::ipNetToMediaPhysAddress\.\d+.*	

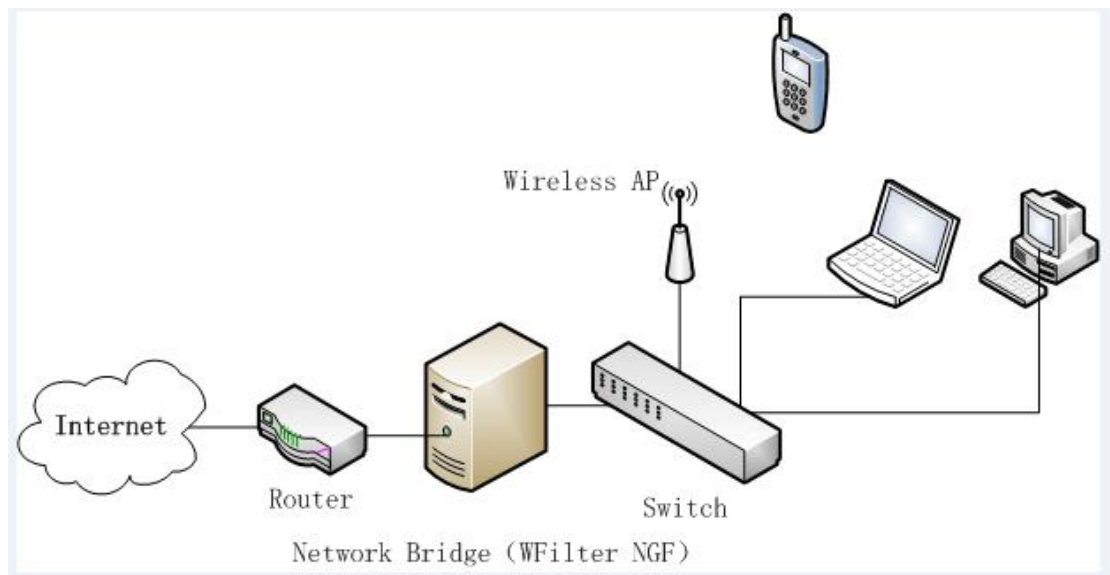
[Add](#) [Test](#) [Save](#)

5 Deployment

5.1 Gateway



5.2 Bridge



Business Name: IMFirewall Software Co., Ltd

Email: support@imfirewall.com.cn

Website: <http://www.wfilterngf.com>