

Copfilter

An add-on
for the
IPCop Firewall

© 2005 Markus Madlener

Table of Contents

<u>Chapter</u>	<u>Page</u>
Table of Contents	2
Copfilter - a Virus and Spam filtering IPCop add-on	3
Introduction	3
IPCop Firewall	3
Copfilter Features	5
Email Scanning	5
Internet traffic Scanning	5
Network	5
Monitoring	5
Administration and Management	5
Updates	6
User Notifications emails	6
Email Reports (for the System Administrator)	6
Software	6
Licensing	7
Security	7
Requirements	7
Software versions as of this writing	8
Main programs	8
Tools used by the Main programs	8
Clients	9
Test files	9
Installation	10
Preparation	10
Copy the package to the firewall	10
Install the package on the firewall	11
Quick configuration	14
Configuration	17
Status	18
Email Settings	19
Monitoring	20
POP3 Scanning	22
SMTP Scanning	25
HTTP Scanning	30
FTP Scanning	34
AntiSpam	35
AntiVirus	41
TESTING	44
Setup	45
Setup_util script command line parameters	45

Copfilter - a Virus and Spam filtering IPCop add-on

Copyright © 2005 Markus Madlener

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copfilter is distributed under the terms of the GNU General Public License.

This software is supplied AS IS. Copfilter disclaims all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. Copfilter assumes no liability for damages, direct or consequential, which may result from the use of this software.

Introduction

Copfilter's main goal is to provide a free and easy to use solution to filter and scan traffic from any insecure network, like the internet, for Viruses and Spam. It has been designed as a preconfigured and easy to install add-on for an IPCop firewall.

Copfilter is a package of various Open Source traffic filtering software and tools, customized and built to work together smoothly. All included proxies filter traffic transparently, which means that no client reconfiguration is necessary.

It scans POP3 and SMTP emails for Viruses and Spam. Instead of a Virus infected emails, users will receive Virus notification messages containing details about the originally sent emails, which can also be quarantined if desired.

Spam emails will be tagged as Spam by inserting the following text into the subject field: *** Spam ***

With this procedure any email client will be able to use its own message filtering rules to automatically delete or move these Spam messages into a different folder for a later review.

HTTP and FTP traffic will also be scanned for Viruses. If a Virus is found, access to that web page or file will be denied.

IPCop Firewall

IPCop is an Open Source Linux Firewall Distribution project. Its main goal is to provide a secure and stable Firewall, which is easy to configure and maintain. IPCop has a web interface and it provides easy upgrade and patch management.

Depending on the used hardware and user experience, IPCop can be installed and configured in a matter of about 15 minutes or less.

Main IPCop features:

- Secure, stable and highly configurable Linux based firewall
- Runs on Uni- and Multi-processor systems
- IPTables based firewall
- Build system uses LFS (Linux from Scratch)
- Easy configuration through the Web-based GUI Administration System (ssl secured)
- CPU/Memory/Disk/Traffic Graphs, System/Proxy/Firewall Logs

- IPCop Linux Updates Area
- Backup/restore configuration
- Built with ProPolice to prevent stack smashing attacks in all applications.
- Multiple language support

- HTTP Web Proxy (Squid) to speed up web access
- SSH server for Remote Access
- DHCP server - provides dhcp services to its clients
- NTP Server - provides time services to its clients
- Caching DNS to help speed up Domain Name queries
- Intrusion detection (Snort) to detect external attacks on your network
- IPSec based VPN Support (FreeSWAN) with x509 certificates

- Traffic Shaping capabilities to prioritize network traffic
- TCP/UDP port forwarding
- Port Address Translation which is a type of Network Address Translation (NAT)
http://de.wikipedia.org/wiki/Network_Address_Translation
- DMZ Pinhole support
- Dynamic DNS Support (dyndns.org, no-ip.com, zoneedit.com,..)

- Interface Support - up to 4 network adapters, partitioning your network into 4 zones

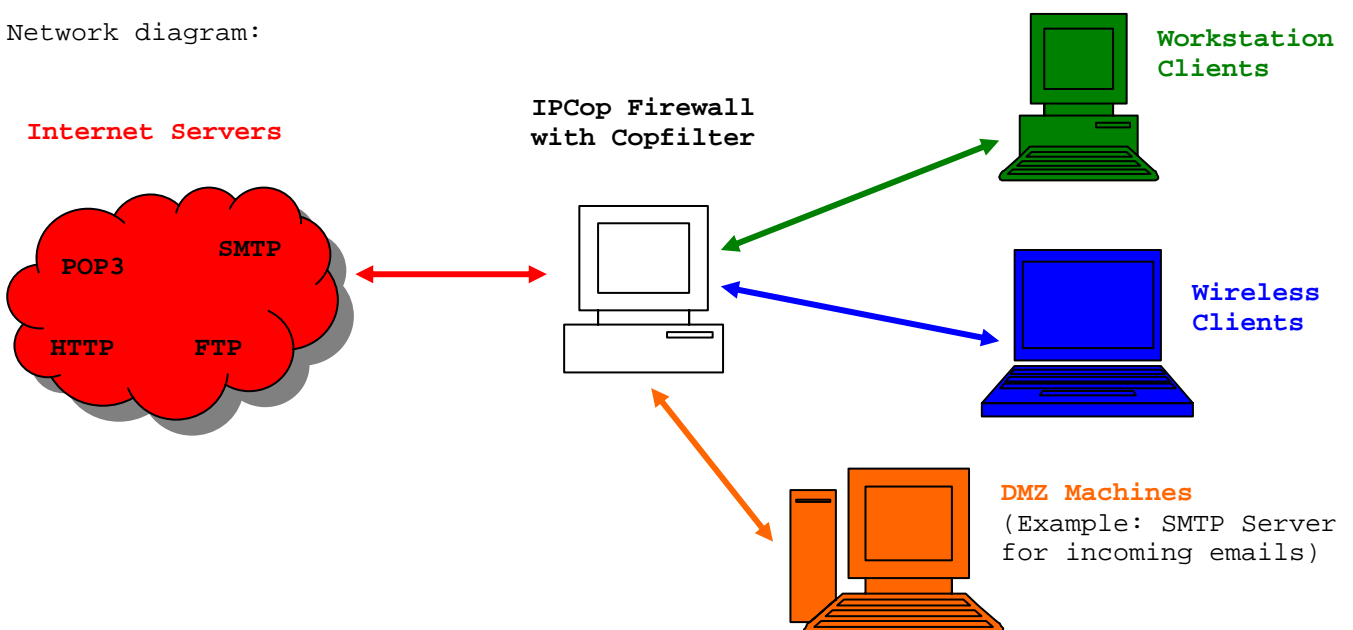
- GREEN** - internal safe network which is protected from the Internet
- BLUE** - wireless network for WLAN clients
- ORANGE** - DMZ (demilitarized zone) for publicly accessible servers, partially protected from the Internet
- RED** - internet unsafe network

ISP

- External **RED** interface supports Analog/ISDN/ADSL modem
- Supports PPP, PPTP, PPPoE, Ethernet
- DHCP client - IPCop is able to obtain its IP address from your ISP

For more information please visit the IPCop website at <http://www.IPCop.org>.
An installation manual can be found at <http://www.IPCop.org/1.4.0/en/install/html>.

Network diagram:



IPCop review in german: <http://www.heise.de/security/artikel/38011>

Copfilter Features

Email Scanning

- Virus and Spam scanning of incoming POP3 emails
- Virus and Spam scanning of incoming and outgoing SMTP emails
- Email sanitizing by removing dangerous html tags from HTML email messages
- Attachment scanning by renaming dangerous attachments (.pif .vbs ..) from email messages
- Adds a note to every email header indicating that the email was scanned
- Email discarding and/or quarantining, depending on a predefined Spam score level or if a Virus was found

Internet traffic Scanning

- Virus scanning of HTTP traffic, with no "trickle" effect, but continuous, non-blocking downloads
- Virus scanning of FTP traffic, with "trickle effect", a download delay is noticeable (file gets downloaded and scanned in the background, while browser only receives a few bytes until complete file has been scanned)
- Removes ads, banners, pop-ups and other obnoxious Internet junk from HTTP Traffic

Network

- All services work transparently, no re-configuration on any client is necessary!!
- Highly configurable, scanning can be turned on or off for every attached network
- Any type of email client (Outlook, Thunderbird, Evolution,..) on any OS (Win32, Linux, MacOS,..) can be used
- (RED) IP Alias support for mail server MX entries other than the default assigned ip address

Monitoring

- Detailed information about every installed service (CPU/Memory usage, uptime etc.)
- Service monitoring, if a service should fail, it will automatically be restarted (with email notification)
- Individual Service control - start/stop every services from the monitoring Web GUI

Administration and Management

- Copfilter AntiSpam Whitelist management through Web GUI and by sending an email (with pre-defined commands) (spam scanning will be skipped on the reply emails)
- Automatic outgoing email whitelisting, adds recipient (To: field) email address of outgoing email to the Whitelist, if a reply email to the original email arrives, Spam scanning will be skipped
- Copfilter Daily Spam Digest recipient management through Web GUI
- Ability to automatically download Spam and ham emails from an IMAP folder to train the integrated Bayesian filter (dramatically improves Spam recognition, important for false positives and false negatives)
- HTTP Whitelist management through a configuration file
- Uninstall, backup, restore and restore-to-default-configuration capability
- Virus and Spam Quarantine, option to resend, delete messages and/or add the sender email address to the Whitelist
- Customizable levels of when email messages should be quarantined or discarded
- Ability to send test Virus/spam/bad attachment emails directly from the Web GUI to test Copfilter functionality

- Links to test HTTP and FTP Viruses are included as well
- Copfilter installation and configuration can be done in less than 5 minutes. Just copy the installation file to the IPCop firewall, extract and execute the included install script (no IPCop addon server required)
- Based on the Linux Firewall Distribution IPCop which is very easy to install. Download the Iso-Image, burn the CD, answer a few screens and your new firewall is up and running in less than 15 minutes!
- Detailed documentation
- Ease to use and highly configurable Web-based graphical user interface (Web GUI)
- Free, Open Source and GPL licensed :-)

Updates

- Automatic AntiVirus signature updates
- Automatic AntiSpam ruleset updates
- Latest available Copfilter version is displayed in the Web GUI (Web GUI retrieves this information by reading the <http://www.copfilter.org> website)

User Notifications emails

- Instead of a Virus infected email, the user receives a notification that a Virus infected email has been sent to him, including details like sender, subject, email header, etc of the original message
- Optionally sends a copy of these user notifications to an administrator
- All Spam messages will be tagged in the subject: *** Spam *** for further client processing
- Daily digest containing all sender email addresses of all received Spam in 24h, optionally a user can send an email to automatically add an email address to the Whitelist

Email Reports (for the System Administrator)

about

- Virus signature updates
- Antispam ruleset updates
- IMAP BAYES Training results
- Failed services and if the automatic restart has been successful

Software

- Only uses Open Source software (except for optional Virus scanner F-Prot)
- Enhanced Spam capabilities: Bayesian filtering, Spam Rulesets, Razor, Dcc, SURBL and DNS Blocklists
- Is able to use an open source AND/OR a commercial Virus scanner (for POP3/SMTP/FTP: ClamAV and/or F-Prot - for HTTP: ClamAV only)
- All proxies run as a non-root user
- Init scripts included which can start/stop/reconfigure the proxies (some can be started in debug mode)
- Log directory with log files from all services (accessible through Web GUI)
- Supports multi languages based on the IPCop language setting languages available - depends on translations which have been already done

Licensing

Copfilter is licensed under the terms of the GNU General Public License Version (GPL). Its documentation is licensed under terms of the GNU Free Documentation License Version (GFDL).

GNU General Public License Version 2, June 1991

<http://www.gnu.org/copyleft/gpl.html>

Inofficial German translation

<http://www.gnu.de/gpl-ger.html>

GNU Free Documentation License Version 1.2, November 2002

<http://www.gnu.org/copyleft/fdl.html>

Inofficial German translation (Version 1.1)

<http://nautix.sourceforge.net/docs/fdl.de.html>

Security

From a security point of view, adding filters, Virus scanners and proxies to the firewall will highly reduce the firewall's overall security. Every additional application or software on a firewall could be a potential security hole. That's why the main target audience for Copfilter is the average home user or a smaller business with a lower demand on security than a huge corporate network serving hundreds of clients, although depending on their security requirements, Copfilter may serve them as well.

Copfilter is NOT an official IPCop Add-on. It has not been approved or reviewed by the IPCop development team. It comes with NO warranty or guarantee, so it should be used at everyone's own risk. Copfilter adds firewall rules, proxies, filters and Virus scanners to the IPCop machine, which reduces security! I am sure that there are lots of ways to break Copfilter, so if security is an issue, it should NOT be used.

Requirements

Software:

IPCop version 1.4.x

Hardware (recommended minimum hardware):

- a CPU with 350 Mhz, 256MB RAM
- if no Spam filtering is used then a machine with 128MB RAM should be sufficient

If a faster machine is being used, email scanning and traffic filtering will be faster as well.

Short description of the software is being used within Copfilter

- | | |
|-----------------|--|
| P3Scan | - a transparent POP3 Proxy server |
| ProxSMTP | - a transparent SMTP Proxy server |
| HAVP | - a transparent HTTP Proxy server (HTTP Antivirus Proxy) with continuous, non-blocking downloads and smooth scanning of dynamic and password protected HTTP traffic |
| Frox | - a transparent FTP Proxy server |
| Privoxy | - a HTTP Proxy with advanced filtering capabilities for protecting privacy, managing cookies, controlling access, and removing ads, banners, pop-ups and other obnoxious Internet junk |

- Clam AntiVirus** - a GPL Virus scanner with built-in support for Zip, Gzip, Bzip2 and automatic updating
- F-Prot Antivir** - for Linux Workstations (free for home users), Virus scanner is not included, but supported!
- F-Prot Antivir** - for x86 Mail Servers (corporate use) this Virus scanner is not included, but supported!
- Spam Assassin** - a mail filter to identify Spam
- Vipul's Razor** - a distributed, collaborative, Spam detection and filtering network, used by Spam Assassin
- DCC** - a cooperative, distributed system intended to detect "bulk" mail
- Renattach** - a stream filter that can identify and rename potentially dangerous e-mail attachments
- RulesDuJour** - a bash script which automatically downloads new versions of Spam Assassin rulesets
- Monit** - Monitoring Utility - automatically restarts a failed service, includes a service manager

Software versions as of this writing

Main programs

P3Scan	POP3 Proxy	2.1.99dev http://p3scan.sourceforge.net
ProxSMTP	SMTP Proxy	1.2.1 http://memberwebs.com/nielsen/software/proxsmtp
HAVP	HTTP Proxy	0.69 http://havp.sourceforge.net
Frox	FTP Proxy	0.7.18 http://frox.sourceforge.net
Privoxy	Webfilter	3.0.3 http://www.privoxy.org
Spam Assassin	Spamtool	3.0.4 http://www.spamassassin.org

Tools used by the Main programs

RulesDuJour	Bash script	1.21 http://www.exit0.us/index.php?pagename=RulesDuJour
Webuserprefs	Web GUI	0.6 http://sourceforge.net/projects/webuserprefs
PHP	Scripting language	4.4.0 http://www.php.net
Razor	Spam tool	2.75 http://razor.sourceforge.net
Dcc	Spam tool	1.3.12 http://www.rhyolite.com/anti-spam/dcc
Renattach	Attachment renamer	1.2.2 http://www.pc-tools.net/unix/renattach



P3Pmail	Mail sanitizer	1.3 http://p3scan.sourceforge.net/#p3pmail
Anomy	Mail sanitizer	1.70 http://mailtools.anomy.net
Ripmime	Mail ripper	1.4.0.5 http://www.pldaniels.com/ripmime
Formail	Mail formatter	1.102 http://www.procmail.org
ClamAV	Virus scanner	0.86.2 http://clamav.sourceforge.net
F-Prot	Virus scanner	4.6.0
Home use		http://www.f-prot.com/products/home_use/linux
Corporate use		http://www.f-prot.com/products/corporate_users/unix/linux/mailserver.html
Prices		http://www.f-prot.com/products/prices/price_unix_ms.html

Clients

Fetchmail	POP3 client	6.2.5 http://www.catb.org/~esr/fetchmail/
SMTPclient	SMTP client	1.0.0 ftp://ftp.ossdp.org/pkg/tool/smtpclient/smtpclient-1.0.0.tar.gz
SendEmail	SMTP client	1.42 http://caspian.dotconf.net/menu/Software/SendEmail (+ auth patch)
Wget	HTTP download tool	1.9.1 http://www.gnu.org/software/wget/wget.html
Ncftpget	FTP client	3.1.9 http://www.ncftpd.com

Test files

Eicar Test Virus <http://www.eicar.com>

Email address and Website

Website: <http://www.copfilter.org>
 Email address: copfilter@gmx.net
 Support email: copfilter-main@lists.sourceforge.net

Please do not publish my email address online like in forums, boards, except in the form (copfilter-main@lists.sourceforge.net) presented above. This helps reduce my Spam mail, thanks!

Installation

The Copfilter installation and Web GUI language will be the same as what you in the IPCop Web GUI, so if you want a different language change this settings in System -> GUI Settings

Preparation

- Enable SSH on your IPCop machine through the IPCop admin web pages (necessary for file transfer)

IPCop Web GUI -> SYSTEM -> SSH ACCESS

- Enable Squid on your IPCop machine through the admin web pages (needed for Privoxy to work)

IPCop Web GUI -> SERVICES -> Proxy

- You will need a secure copy (scp) client to copy the package to your IPCop firewall and a secure shell client (ssh) to actually install the package if working on Unix, you should have ssh and scp already installed, if not you have to install these programs from the linux distribution you are using, or compile them yourself

If working on windows you could use (both Open Source and free):

Graphical secure copy client:

WinSCP <http://winscp.sourceforge.net/eng/>

Graphical secure shell client:

Putty <http://www.chiark.greenend.org.uk/~sgtatham/putty>

Putty includes a command line secure copy client called pscp.exe

- Download the latest Copfilter version from <http://www.copfilter.org>. **Do not try to extract this tar file on windows** (your Virus scanner will warn you about 4 Test Virus files in the archive), instead copy it to the IPCop machine by doing the following:

Copy the package to the firewall

Copy the package to the IPCop firewall using a secure copy client (scp) on a Unix or Linux machine (type the following command in one line!):

```
scp -P 222 <Copfilterpackage_name> root@<your_IPCop's_machine_ipaddress>:/root
```

(Notice that port 222 needs to be used!)

OR on a windows machine using WinSCP

Start WinSCP and create a new session in the WinSCP login screen, then drag and drop the Copfilter installation file to the IPCop /root and click on copy when asked to confirm

OR on a windows using Putty's pscp

```
pscp -P 222 <package_name> root@<your_IPCop's_machine_ipaddress>:/root
```

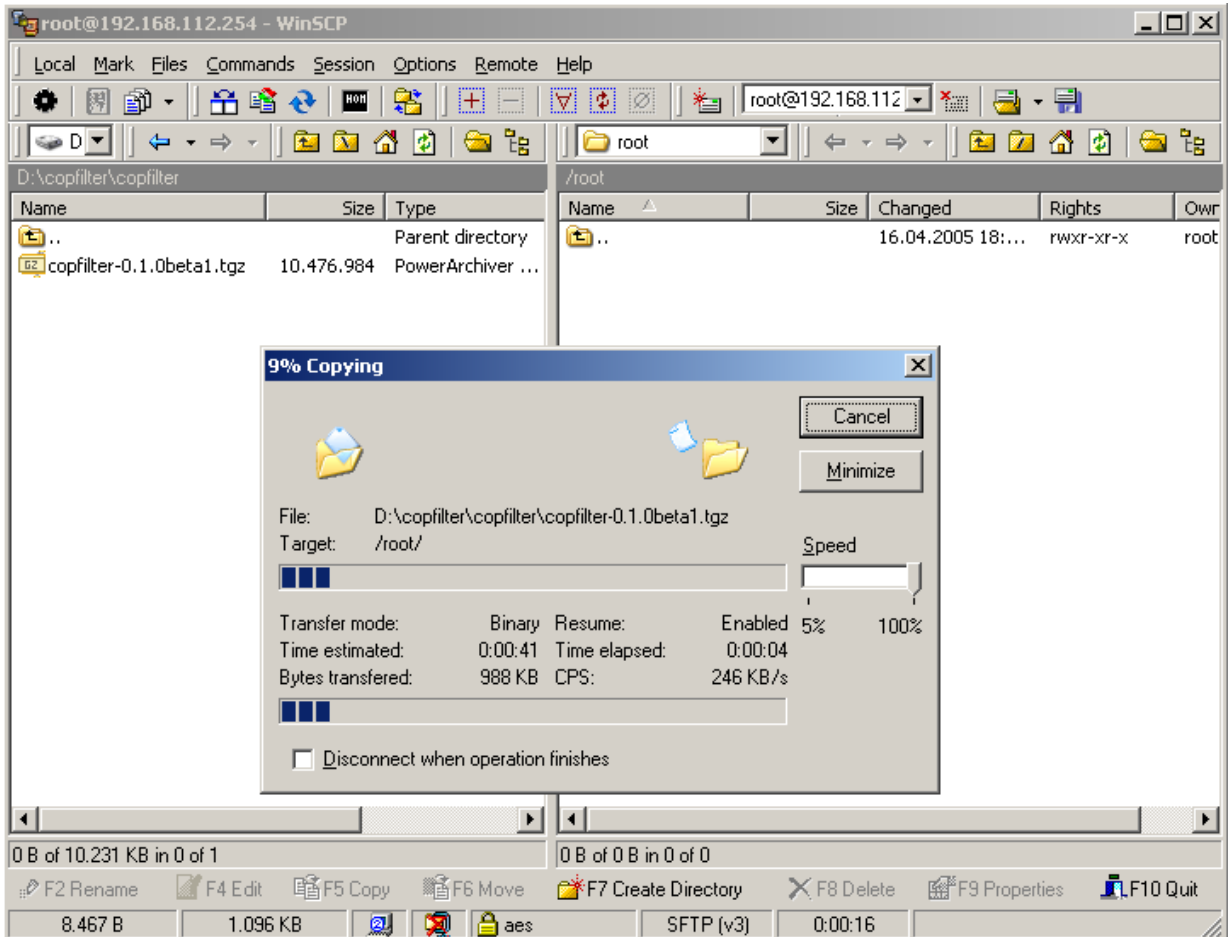


Fig. 1: copy the package to the firewall using WinSCP (assuming 192.168.112.254 is your IPCop's IP address)

Install the package on the firewall

1. Login to the IPCop machine with a SSH client

Example with Putty:

Start putty

- Enter the IP-Address of your IPCop machine into the "Host Name (or IP address)" field
- Enter the ssh port of your IPCop machine into the "Port" field, this is usually: "222"
- Enter a session name in "Saved Sessions", for example "IPCop"
- Click on "Save"
- Click on "Open" to start the ssh session to your IPCop machine

You should now have an open terminal session with Putty

2. If you are updating, first uninstall the old version

Note:

Everything which was Copfilter related will be deleted without confirmation, you might want to create backup before uninstalling:

```
/var/log/Copfilter/default/setup_util -b
```

to uninstall:

```
/var/log/Copfilter/default/setup_util -u
```

3. Extract the package

```
cd /root
tar xzvf Copfilter-0.1.0.tgz
```

(version number could be different than in this example)

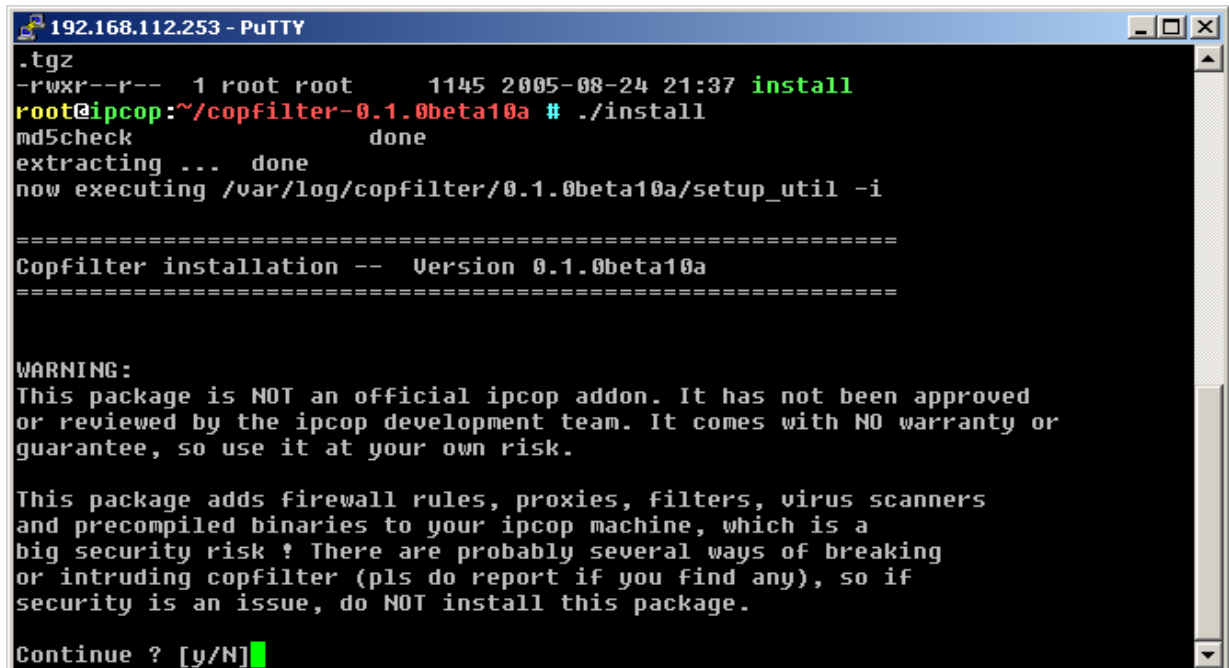
4. Change to the directory and install the new package

```
cd Copfilter-0.1.0
./install
```

This script will automatically extract the setup tar file and will also automatically execute `/var/log/Copfilter/default/setup_util -i`
If it fails and you get these error messages:

```
gzip: stdin: unexpected end of file Copfilter-0.1.0beta2/install
tar: Unexpected EOF in archive
tar: Unexpected EOF in archive
tar: Error is not recoverable: exiting now
```

Then this means that you have not correctly downloaded the full file, try to re-download the file and then try again



```
192.168.112.253 - PuTTY
.tgz
-rwxr--r-- 1 root root 1145 2005-08-24 21:37 install
root@ipcop:~/copfilter-0.1.0beta10a # ./install
md5check done
extracting ... done
now executing /var/log/copfilter/0.1.0beta10a/setup_util -i

=====
Copfilter installation -- Version 0.1.0beta10a
=====

WARNING:
This package is NOT an official ipcop addon. It has not been approved
or reviewed by the ipcop development team. It comes with NO warranty or
guarantee, so use it at your own risk.

This package adds firewall rules, proxies, filters, virus scanners
and precompiled binaries to your ipcop machine, which is a
big security risk ! There are probably several ways of breaking
or intruding copfilter (pls do report if you find any), so if
security is an issue, do NOT install this package.

Continue ? [y/N]
```

Fig. 2: Running the Installation Script in a Putty Session

```
192.168.112.253 - PuTTY
Continue ? [y/N]y
Ok, now installing copfilter on your machine..
extracting tar file for /usr/local/bin helper scripts           ok
adding startup scripts to /etc/rc.d/rc.local                   ok
adding copfilter startup scripts to /etc/rc.d/rc.firewall.local ok
adding copfilter users and groups                             ok
changing ownerships                                          ok
linking init scripts to /etc/rc.d/init.d/                     ok
modifying crontab                                           ok
linking unzip to /usr/local/bin                               ok
linking wget to /usr/local/bin                               ok
installing copfilter webgui for ipcop >= 1.4.4              ok
installing copfilter webgui for email white/black lists     ok
inserting webgui entry into header.pl                        ok
adding copfilter documentation to /home/httpd/html/copfilterdoc ok
Modifying /etc/httpd/conf/httpd.conf and restarting httpd   ok
deleting link to copfilter installation directory from /root  ok
creating default link                                       ok
creating a new razor account (this could take a minute)..   ok

Copfilter 0.1.0beta10a installation completed successfully !

Don't forget to:
1. Enter your Email Address and Smtп Server in the Copfilter webgui
   IPCop webgui -> Services -> Copfilter
2. Read the documentation: README
   (in webgui or /root/copfilter/doc)
3. Configure Copfilter webgui: configure AND press >>Save Settings<< in each
   section and then press >>Restart All Services to start all programs
4. If desired run tests from the webgui or from
   /root/copfilter/tests/make_all_tests.sh

Pls report errors and questions to
>>copfilter-main at lists dot sourceforge dot net<<
>>hello at test dot com<< is an email address and would mean hello@test.com
or visit the official copfilter forum (link is at the bottom of the webgui)
root@ipcop:~/copfilter-0.1.0beta10a #
```

Fig. 3: Screen Output of the Installation Script after a successful Installation

If you are a Home User, you could also install the F-Prot Virus Scanner (free for Home Use) so that your email will be scanned by 2 different Virus Scanners which increases security. This package only includes ClamAV Virus Scanner and you can optionally install F-Prot with the included installation script:

Home Users please read

http://www.f-prot.com/products/home_use/linux

Corporate Users please read

http://www.f-prot.com/products/corporate_users/unix/index.html

Only proceed to the next step if you fulfill the requirements as a Home User!

Download (from above URL) and copy the downloaded file (for example fp-linux-ws-4.3.3.tar.gz) to the IPCop machine into the /root/Copfilter directory, change to the Copfilter directory

```
cd /root/Copfilter
```

and execute

```
./setup_util -f fp-linux-ws-4.3.3.tar.gz
```

After installing F-Prot, additional options will appear in the Web GUI -> Anti-Virus section from where it can be activated to scan emails

Quick configuration

(for details please see the next section)

Open your web browser and go to your IPCop web configuration interface a new menu will appear under Services/Copfilter with which you can now configure Copfilter

Most important:

go to Copfilter -> Email and configure your email address and your SMTP server and click on save settings

The Email Address field is often misunderstood, this field is not a list of email addresses which will be scanned for Viruses, in fact all emails, no matter what email address is used will be scanned transparently, there is no list of email addresses to be scanned, since all emails will be recognized automatically.

The email address in this field will only be used as a recipient for Virus notification updates and a few other notifications

You can now test, if emails sent you are being scanned, by clicking on the buttons (available in the Copfilter -> Test&Debug Web GUI):

1. "Send Test Virus Email"
2. "Send Test Spam Email"
3. "Send Test Email+bad Attachment"

You should then receive:

1. a Virus notification message
2. a email with the subject tagged as *** Spam ***
3. an email with an ***renamed*** exe attachment called "**test_attachment.exe.bad**" - you can still rename the attachment to what it original was, but the purpose of this procedure is to prevent users "blind-clicking" on any exe attachment. If the exe attachment is renamed to .bad nothing will happen.

Please also visit the 2 websites (links are in the Web GUI)

For more information on the "Test&Debug" Web GUI please refer to Chapter "Testing" on page 44 of this manual.

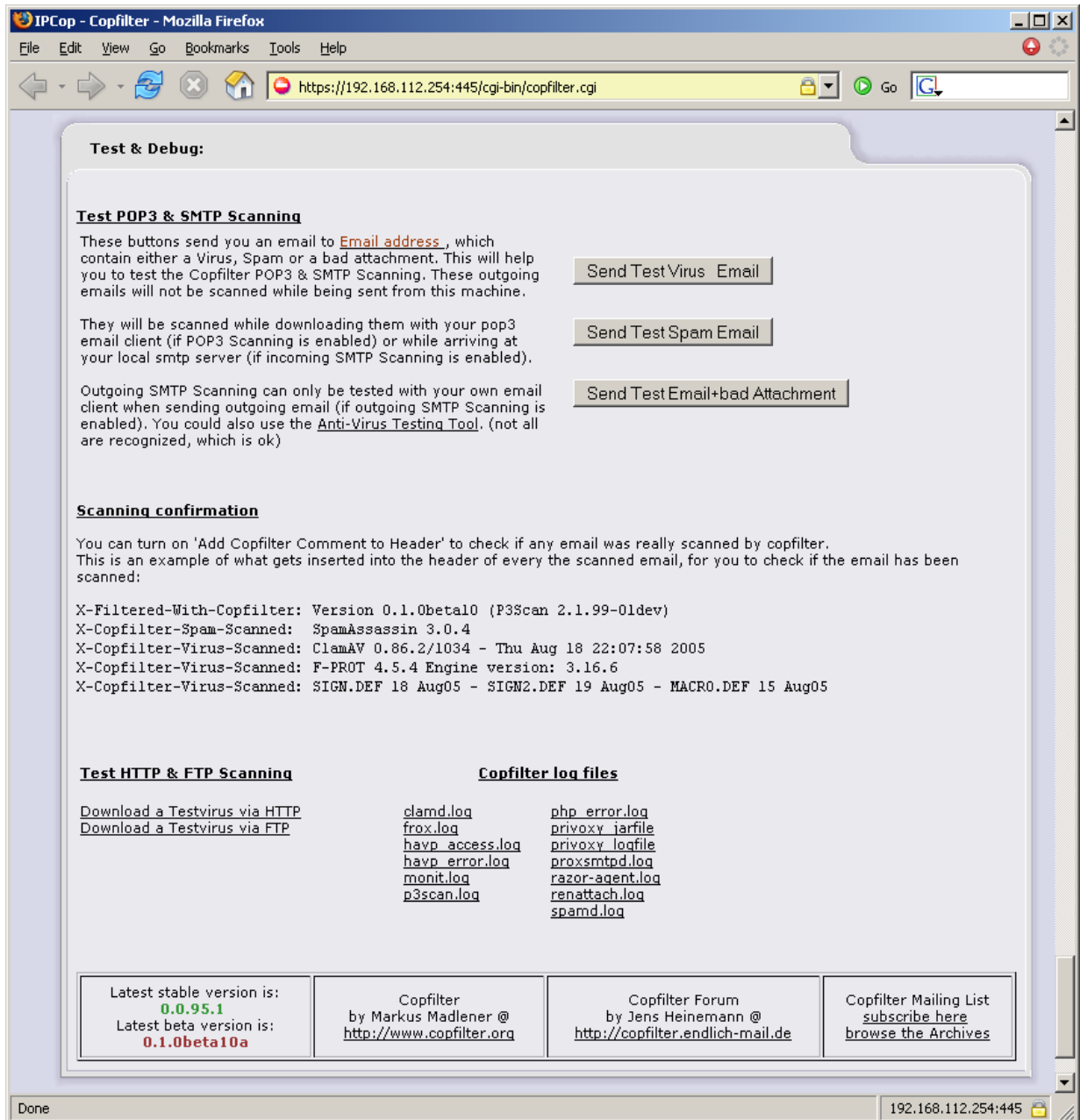


Fig. 4: The Test & Debug Web GUI



Fig. 4a: A typical Copfilter Notification email

Download a Test Virus via HTTP

http://www.eicar.org/anti_virus_test_file.htm

Download a Test Virus via FTP

<http://www.trendmicro.com/en/security/test/overview.htm>

and check if access to those files is denied - if above tests were successful you can now safely use email/HTTP/FTP

Configuration

To access the Copfilter Web-GUI start your browser and enter the IP address (of the green IPCop interface) or Hostname of your IPCop server along with a port director of either 445 (https/secure) or 81(redirected to 445):

`https://IPCop:445` or `https://192.168.112.254:445` or

`http://IPCop:81` or `http://192.168.112.254:81`

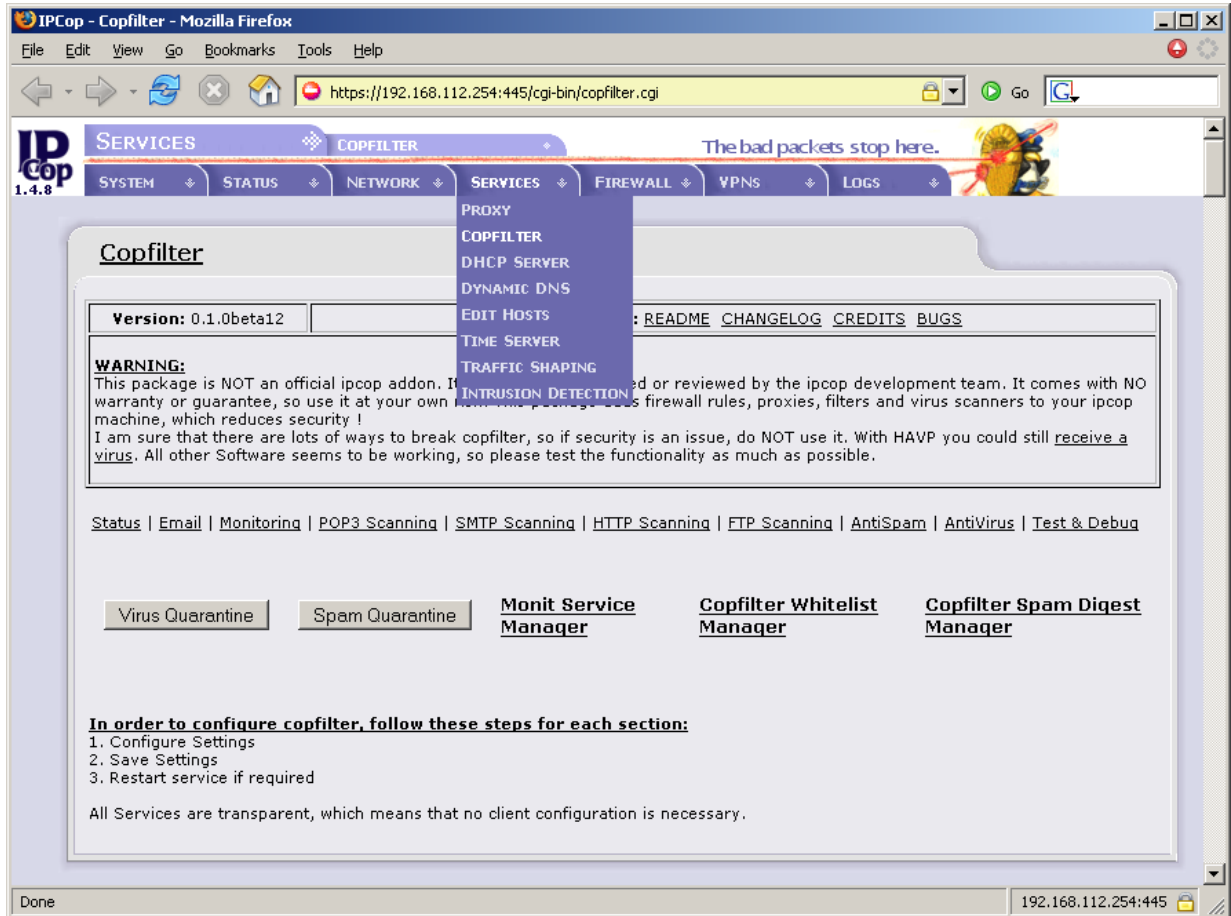


Fig. 5: The Copfilter Web GUI

Note:

If the Web GUI has vanished (for example when updating IPCop) execute the following command to read the menu:

```
/var/log/copfilter/default/setup_util -a
```

Status

Options:

No options can be configured.

This window will give you access to the Copfilter documentation. The currently installed Copfilter version is displayed as well as this warning message:

WARNING: This package is NOT an official IPCop add-on. It has not been approved or reviewed by the IPCop development team. It comes with NO warranty or guarantee, so use it at your own risk. This package adds firewall rules, proxies, filters and Virus scanners to your IPCop machine. Do NOT use Copfilter if security is an issue. With HAVP you could still receive a Virus.

Next follows a section with information regarding the status of each of the currently installed programs, including:

- product name
- short description
- associated daemon
- version number
- daemon status, if any daemons are running their PID numbers are shown
- ability to manually stop or start the daemon

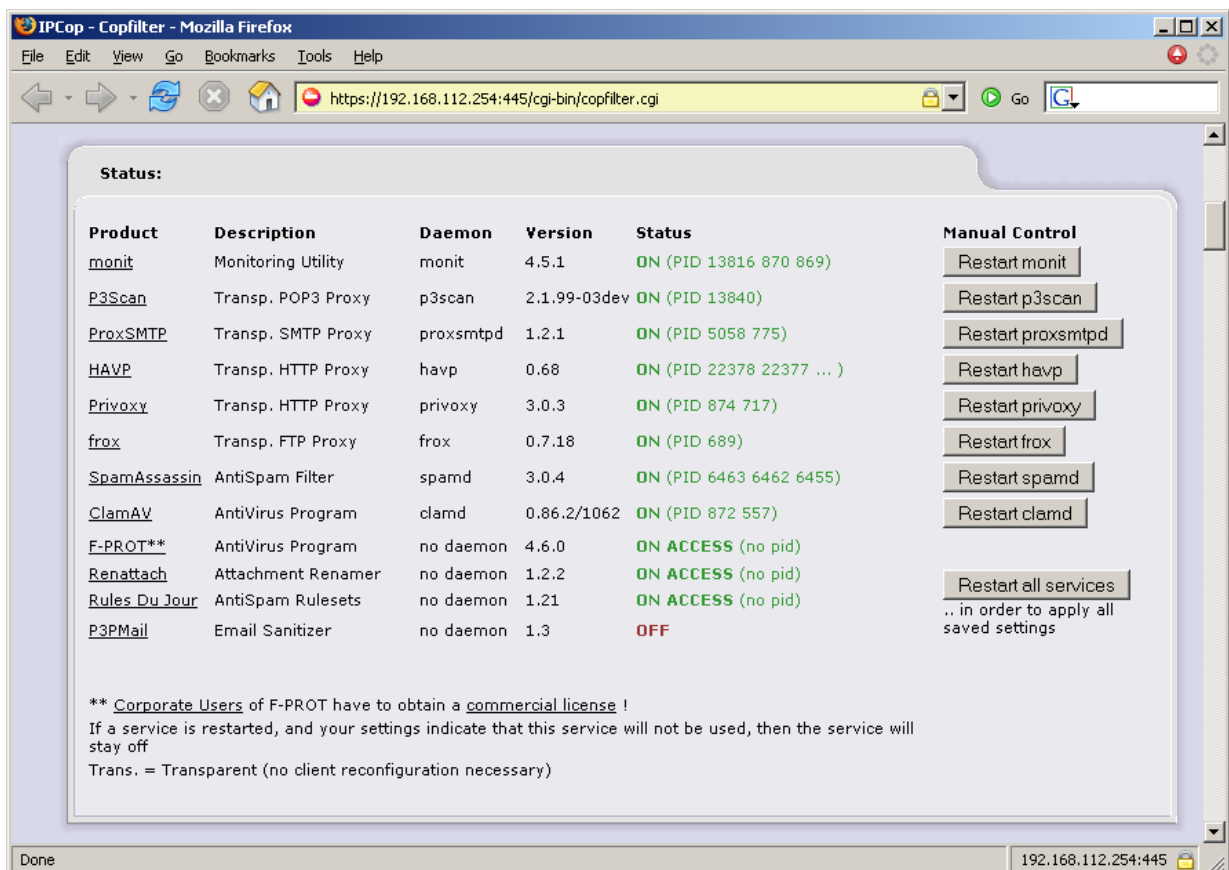


Fig. 6: The Copfilter Web GUI showing the status of the installed Services

Three additional buttons are available for accessing:

- Virus Quarantine
- Spam Quarantine
- Monit Service Manager
- Copfilter Whitelist Manager
- Copfilter Spam Digest Manager

Notes:

If a service is stopped or started manually, then monitoring for that service will stop, to re-enable monitoring of all enabled services, restart the monit service

F-PROT is a commercial program. It is free for Home Users only. Corporate Users have to obtain a license!

If a service is restarted, and your settings indicate that this service will not be used, then the service will stay off.

The abbreviation Trans. stands for Transparent and it means that no client reconfiguration necessary to use this service.

Email Settings

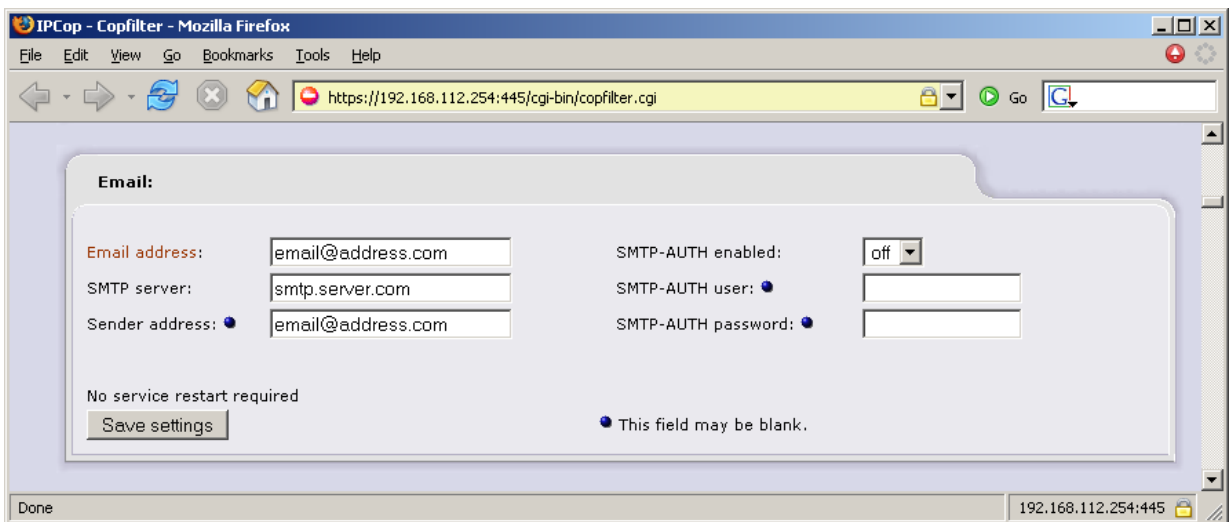


Fig. 7: Configure your email settings in the Copfilter Web GUI

Options:

Enter your email address, the SMTP server, the sender address and configure SMTP-auth if your SMTP server requires it.

Email Address: Enter your email address here, you will then receive various notifications regarding the result of Copfilter service procedures.

SMTP server: This is the address of your Internet Provider's SMTP server. You can also use your own SMTP server if it is located on your internal network.

Sender Address: This is the email address which will be used to send emails from. It will appear as the sender email address when you receive emails from Copfilter. If you don't know what to enter, leave it blank and Copfilter will automatically use your Email Address as your sender address.

If your SMTP server supports SMTP-AUTH you can enable it here (switch it to "on"), and enter the appropriate username and password.

The following notification will be sent to the Email Address mentioned above:

- Virus signature updates
- Antispam ruleset updates
- Imap BAYES Training results
- Failed services and if the automatic restart has been successful
- Copy of Virus notification messages if this has been activated

Notes:

No service restart is required.

Monitoring

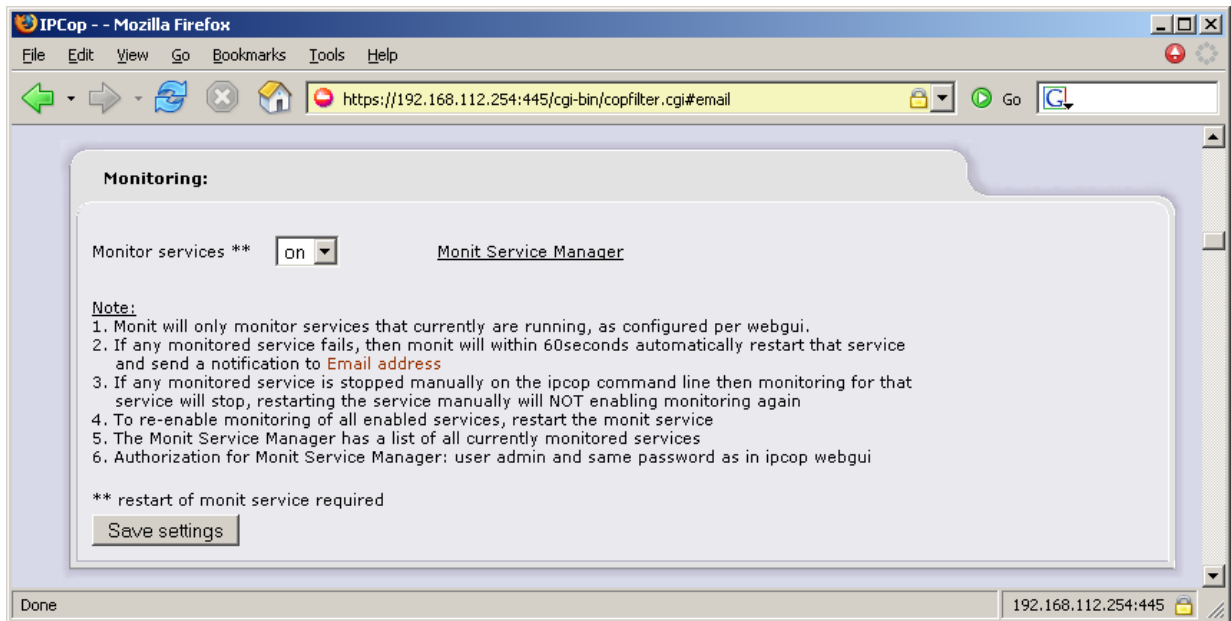


Fig. 8: Monit Service Manager Settings within the Copfilter Web GUI

Options:

Monitor all enabled services

This will enable monitoring for all enabled services which are being used

Note:

1. Monit will only monitor services that currently are running, as configured per Web GUI.
2. If any monitored service fails, then Monit will within 60seconds automatically restart that service and send a notification to Email address
3. If any monitored service is stopped manually on the IPCop command line then monitoring for that service will stop, restarting the service manually will NOT enable monitoring again
4. To re-enable monitoring of all enabled services, restart the Monit service
5. The Monit Service Manager has a list of all currently monitored services
6. Authorization for Monit Service Manager: user "admin" and same password as in IPCop Web GUI

**** Restart of Monit service required**

Notes:

Clicking on the "Save settings" button will automatically restart the necessary services in order to apply your settings. Enable "Skip Service Restart" if you wish to skip restarting the service.

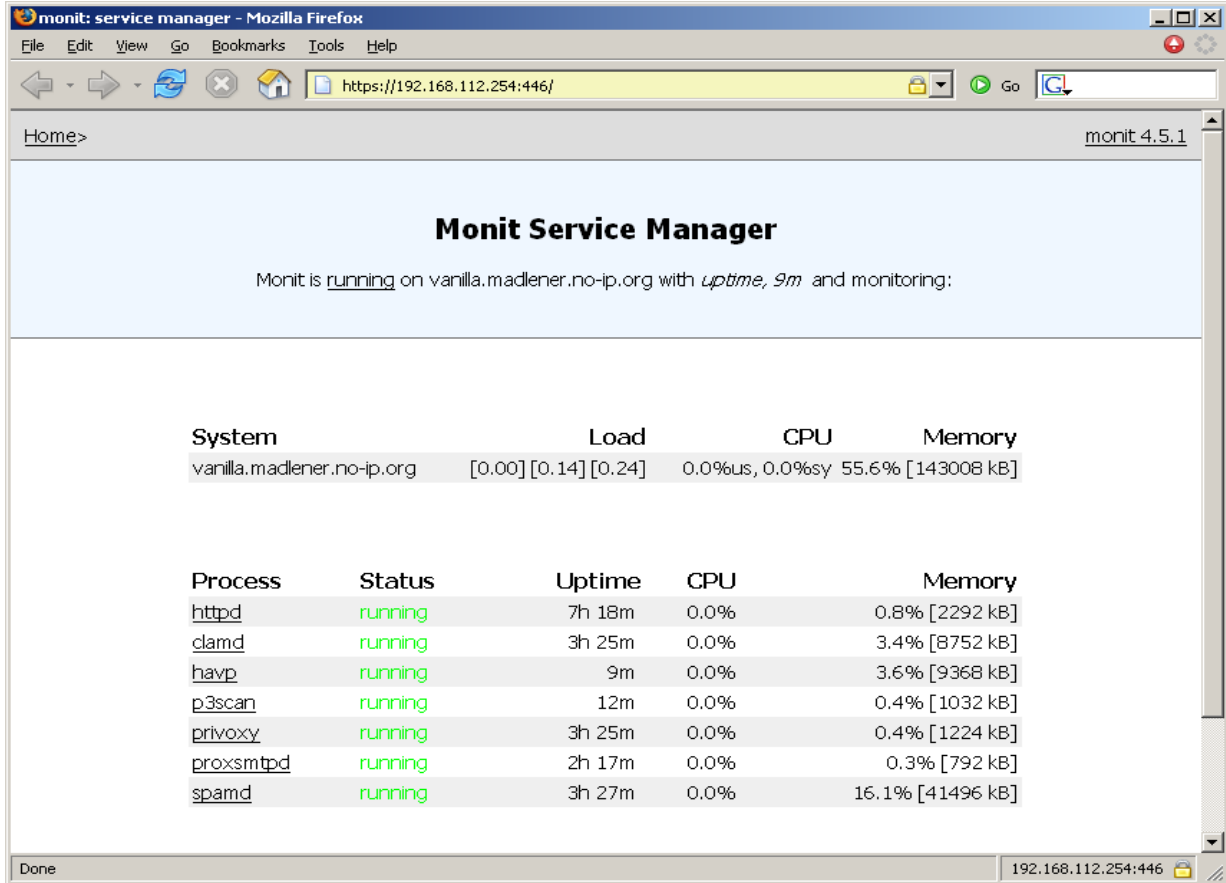
The following link to another Web GUI is available to retrieve information and to manage the monitored services:

Monit Service Manager:

<https://192.168.112.254:446/>

(assuming, 192.168.112.254 is your IPCop's IP address)

Fig. 9: The Monit Service Manager showing the Status of all monitored services



POP3 Scanning

Fig. 10: POP3 Scanning Settings within the Copfilter Web GUI

POP3 Scanning (P3Scan):

<p>Enable P3Scan to analyze outgoing traffic on GREEN** <input type="button" value="on"/></p> <p>Add Copfilter <u>Comment</u> to Email Header <input type="button" value="on"/></p> <p>Quarantine spam emails if ... *** <input type="button" value="on"/></p> <p>... if score is greater than: <input type="button" value="12"/></p>	<p>Stop virus emails and send virus <u>notifications</u> instead <input type="button" value="on"/></p> <p>Tag Spam in emails and <u>modify the subject</u> <input type="button" value="on"/></p> <p><u>Rename</u> bad attachments in emails which are <u>dangerous</u> <input type="button" value="on"/></p> <p>Sanitize and clean emails containing HTML * <input type="button" value="off"/></p> <p>Send a copy of virus <u>notification</u> to <u>Email address</u> <input type="button" value="on"/></p> <p>Use Copfilter <u>Whitelist ++</u> <input type="button" value="on"/></p> <p>Quarantine virus infected emails *** <input type="button" value="on"/></p> <p>Remove emails in quarantine if older than (in days) <input type="text" value="7"/></p>
--	---

Note:
If you wish to use POP3S (pop3-ssl) then configure your email client to fetch email via pop3 on port 995 (WITHOUT SSL !) P3Scan will then automatically open a pop3s (pop3 ssl secured) connection to your email server

* UNSTABLE, Sanitize function (P3PMail) will remove dangerous HTML tags (like pictures) from email messages. If an email contains a non-RFC compliant MIME attachment, P3PMail will damage it (CRC Errors). It is safer to turn this option OFF.
** Restart of p3scan service required
*** Users receive a notification. The POP3 Protocol does not allow email discarding during POP3 retrieval (so notifications cannot be disabled)
++ If sender address is in whitelist, spam scanning will be skipped.

Options:

Enable P3Scan to filter outgoing traffic on **GREEN****
 Enable P3Scan to filter outgoing traffic on **BLUE****
 Enable P3Scan to filter outgoing traffic on **ORANGE****

If a client in the GREEN, BLUE or ORANGE network initiates a POP3 session, which means that he tries to retrieve email from his POP3 server, then this POP3 traffic will be filtered according to the above settings. **BLUE** and **ORANGE** interface options will only appear if these interfaces exist.

If you wish to use POP3S (pop3-ssl) then leave the current settings of your email client just the way they are and only change the PORT number of your POP3 email server from 110 to 995 (**DO NOT ACTIVATE SSL!**) P3Scan will then automatically open an encrypted pop3s (pop3 ssl secured) connection from your IPCop machine to your POP3 email server and forward the emails to you.

Stop Virus emails and send Virus notifications instead

With these options you can enable or disable Virus scanning of incoming POP3 email. This will only work if either ClamAV or F-Prot (if installed) are enabled.

If a Virus is found in an email, the user will receive a Virus notification message with

- information about the detected Virus
- email delivery information (original sender, subject, recipients, date,..)
- the complete unmodified header
- if Virus quarantining has been enabled, the filename containing the original message will be shown

Depending on the quarantine settings the administrator would then be able to access the original file.

Tag Spam in emails and modify the subject

With these options you can enable or disable Spam scanning. If an email gets detected as Spam its subject field will be tagged with ***** Spam *****. The user will still receive this email, with no further modifications of the original email. With this procedure any email client will be able to use its own message rules to automatically delete or move these Spam messages.

Rename dangerous email attachments

With these options you can enable or disable attachment renaming. Emails with bad attachment will be tagged in the subject field with ***** renamed attachment *****. The attachment will be renamed to "originalattachmentname_originalextension.bad". This list of bad attachments can be viewed in the Web GUI -> Copfilter AntiSpam for more information

Sanitize and clean emails containing HTML

This option will modify an email so that it is safe for viewing, the modification depend on the used sanitizer. P3PMail for example removes all dangerous html tags.

Add Copfilter Comment to Header

If this option is enable Copfilter will add email headers of every email, an example:

```
X-Filtered-With: Copfilter Version 0.1.0beta1 (P3Scan 2.1.99-00dev)
X-Spam-Scanned: SpamAssassin 3.0.2
X-Virus-Scanned: ClamAV 0.83/833 - Sat Apr 16 04:31:36 2005
X-Virus-Scanned: F-PROT 4.5.4 Engine version: 3.16.6
X-Virus-Scanned: SIGN.DEF 15 Apr05 - SIGN2.DEF 16 Apr05 - MACRO.DEF 15 Apr05
```

The X-AntiVirus line will only appear if Virus scanning was enabled.

The X-AntiSpam line will only appear if Spam scanning was enabled.

The following lines will appear in the header if appropriate

X-Copfilter:Sender is in whitelist, skipped SpamAssassin

X-Copfilter:Client is part of our network, skipped SpamAssassin

Send a copy of Virus notification to Email address

This allows an administrator to get a copy of every Virus notification message.

Use Copfilter Whitelist

If sender address is in Copfilter Whitelist, Spam scanning will be skipped.



This Email Header will be inserted:

X-Copfilter:Sender is in whitelist, skipped SpamAssassin

This does not affect Virus scanning, meaning that all emails whitelisted email address will still be scanned for Viruses.

Quarantine Spam emails if ...

... if score is greater than: 5-40

Emails containing a Spam score greater than the configured value will be quarantined. Users will receive a notification. The POP3 Protocol does not allow email discarding during POP3 retrieval (so these notifications cannot be disabled)

Quarantine Virus infected emails

This option will save an original copy of a Virus infected email in the quarantine. If it is set to off then all infected emails will be deleted immediately.

Remove emails in quarantine if older than (in days)

Any emails in the POP3 quarantine will be deleted if they are older than this amount of days.

Notes:

Clicking on the "Save settings" button will automatically restart the necessary services in order to apply your settings. Enable "Skip Service Restart" if you wish to skip restarting the service.

Restart of p3scan service is required if one of the following options has been modified (the option "Skip Service Restart" can be checked none of below options have been changed):

- Enable P3Scan to filter outgoing traffic on GREEN**
- Enable P3Scan to filter outgoing traffic on BLUE**
- Enable P3Scan to filter outgoing traffic on ORANGE**

SMTP Scanning

SMTP Scanning (ProxSMTP):

<p>Enable ProxSMTP to analyze outgoing traffic on GREEN** <input type="checkbox" value="on"/></p> <p>Add Copfilter <u>Comment</u> to Email Header <input type="checkbox" value="on"/></p> <p>Enable ProxSMTP to analyze incoming traffic on RED and forward to internal Email Server** *** <input type="checkbox" value="off"/></p> <p>Email Server is located in network <input type="checkbox" value="GREEN"/></p> <p>Email Server IP Address <input type="text" value="1.1.1.1"/></p> <p>Red IP Alias Address (if this is empty the current RED IP Address will be used) <input type="text" value="2.2.2.2"/></p> <p>Add email addresses from outgoing email to Copfilter**** <u>Whitelist</u> <input type="checkbox" value="on"/></p> <p>Disable all spam scanning on outgoing email from internal network <input type="checkbox" value="on"/></p> <p>Quarantine spam emails if ... <input type="checkbox" value="on"/></p> <p>... if score is greater than: <input type="text" value="15"/></p> <p>Send user a copy of quarantined spam email <input type="checkbox" value="off"/></p>	<p>Stop virus emails and send virus <u>notifications</u> instead (see below) <input type="checkbox" value="on"/></p> <p>Tag Spam in emails and <u>modify the subject</u> <input type="checkbox" value="on"/></p> <p><u>Rename</u> bad attachments in emails which are <u>dangerous</u> <input type="checkbox" value="on"/></p> <p>Sanitize and clean emails containing HTML * <input type="checkbox" value="off"/></p> <p>Send user a <u>virus notification</u> with information about the originally sent email containing the virus <input type="checkbox" value="off"/></p> <p>Send a copy of virus <u>notification</u> to <u>Email address</u> <input type="checkbox" value="on"/></p> <p>Discard (delete) all SMTP virus emails (virus quaranting and virus notifications will be disabled) <input type="checkbox" value="off"/></p> <p>Discard (delete) all SMTP spam emails if ... <input type="checkbox" value="off"/></p> <p>... if score is greater than: (spam quaranting above this score will be disabled) <input type="text" value="15"/></p> <p>Discard (delete) all SMTP emails with bad attachments <input type="checkbox" value="off"/></p> <p>Enable Copfilter <u>Whitelist</u> modifications via <u>email</u>***** <input type="checkbox" value="on"/></p> <p>Use Copfilter <u>Whitelist</u> and <u>Blacklist</u> ++ <input type="checkbox" value="on"/></p> <p>Quarantine virus infected emails <input type="checkbox" value="off"/></p> <p>Remove emails in quarantine if older than (in days) <input type="text" value="7"/></p>
---	---

* UNSTABLE, Sanitize function (P3PMail) will remove dangerous HTML tags (like pictures) from email messages. If an email contains a non-RFC compliant MIME attachment, P3PMail will damage it (CRC Errors). It is safer to turn this option OFF.
 ** Restart of proxsmtpd service required
 *** **This will open port 25 on your firewall !!**
All incoming emails will be resent from your ipcop firwall to your mail server, which means that if you allow relaying from your ipcop's ip address, you mail server will become an open relay !!
Please use for example this [site](#) to test if your server is an open relay.
Do not enter any port 25 forwarding rules in IPCop
 **** except when sender=recipient, internal email address should not be added into the whitelist, as all incoming email to this address would then be whitelisted
 ***** send email to any external address (email will be discarded), with the following text in the body: (multiple lines possible)
 copfilter_add_to_whitelist youraddress@domain.com
 copfilter_remove_from_whitelist adress@domain.com
 ++ If sender address is in whitelist, spam scanning will be skipped. If sender address is in blacklist, email will be discarded.

Fig. 11: SMTP Scanning Settings within the Copfilter Web GUI

Options:

Enable ProxSMTP to filter outgoing traffic on **GREEN***
Enable ProxSMTP to filter outgoing traffic on **BLUE***
Enable ProxSMTP to filter outgoing traffic on **ORANGE***

If a client in **GREEN**, **ORANGE** or **BLUE** initiates a SMTP session, which means that he tries to send an email from his SMTP server, then this SMTP traffic will be scanned. According to the above settings **BLUE** and **ORANGE** interface options will only appear if these interfaces exist.

Stop Virus emails and opt. send Virus notifications instead (see below)

This will only work if either ClamAV or F-Prot (if installed) are enabled as well. With these options you can enable or disable Virus scanning. If a Virus is found in an email, the user will receive a Virus notification message with

- information about the detected Virus
- email delivery information (original sender, subject, recipients, date,..)
- the complete unmodified header
- if email quarantining has been enabled, the filename containing the original message will be shown

Depending on the quarantine settings the administrator would then be able to access the original file.

Tag Spam in emails and modify the subject

With these options you can enable or disable Spam scanning. If an email gets detected as Spam it's subject field will be tagged with ***** Spam *****. The user will still receive this email, with no further modifications of the original email. With this procedure any email client will be able to use its own message rules to automatically delete or move these Spam messages.

Rename dangerous email attachments

With these options you can enable or disable attachment renaming. Emails with bad attachment will be tagged in the subject field with ***** renamed attachment *****. The attachment will be renamed to "originalattachmentname_originalextension.bad"

This list of bad attachments can be viewed in the Web GUI -> Copfilter AntiSpam for more information

Sanitize and clean emails containing HTML

This option will modify an email so that it is safe for viewing, the modification depend on the used sanitizer. P3PMail for example removes all dangerous html tags.

Add Copfilter Comment to Header

If this option is enabled Copfilter will add email headers of every email, an example:

```
X-Filtered-With: Copfilter Version 0.1.0beta1 (P3Scan 2.1.99-00dev)
X-Spam-Scanned: SpamAssassin 3.0.2
X-Virus-Scanned: ClamAV 0.83/833 - Sat Apr 16 04:31:36 2005
X-Virus-Scanned: F-PROT 4.5.4 Engine version: 3.16.6
X-Virus-Scanned: SIGN.DEF 15 Apr05 - SIGN2.DEF 16 Apr05 - MACRO.DEF 15 Apr05
```

The X-AntiVirus line will only appear if Virus scanning was enabled.
The X-AntiSpam line will only appear if Spam scanning was enabled.

The following lines will appear in the header if appropriate

```
X-Copfilter:Sender is in whitelist, skipped SpamAssassin  
X-Copfilter:Client is part of our network, skipped SpamAssassin
```

Send user a Virus notification with information about the originally sent email containing the Virus

This option allows enabling or disabling the client Virus notifications.

Send a copy of Virus notification to Email address

This allows an administrator to get a copy of every Virus notification message.

Enable ProxSMTP to filter incoming traffic on RED and forward to internal Email Server

This option will enable scanning of incoming SMTP traffic. This is useful, if you are running your own SMTP server and you receive email via SMTP to your own mail server. For security reasons it is recommended to put the email server into the DMZ (**Orange**) network.

Do not enter a port forwarding in IPCop/Firewall/Portforwarding. The necessary rules are being maintained by Copfilter and will not be shown in the IPCop Web GUI. The rules which will be entered, will be shown upon starting proxsmtpd. Be aware that this option opens port 25 on your firewall which will then be transparently redirected to an internal email server.

This means, that your internal email server will be open on port 25 to the internet!

All incoming emails will be resent from your IPCop firwall to your mail server, which means that if you allow relaying from your IPCop's ip address, you mail server will become an open relay!! Please test, if your server is an open relay.

Email Server is located in network

Here you need to define the location of your Email Server

Email Server IP Address

All incoming email will be forwarded to this IP address

Red IP Alias Address (if this is empty the current RED IP Address will be used)

Here you have the option of defining an ip alias address, which would be an additional ip address you got from your provider, solely for email receipt.

Red IP Alias Ethernet Interface

Choose, which interface this new IP alias address should have.

Discard (delete) all SMTP Virus emails (virus quarantining and Virus notifications will be disabled)

All incoming SMTP email will be accepted and discarded (deleted) immediately, no Virus quarantining will occur, no Virus notifications will be sent

Discard (delete) all SMTP Spam emails if ...

... if score is greater than: (spam quarantining above this score will be disabled)

Emails containing a Spam score greater than the configured value will be discarded. No Spam quarantining above this score will occur.

Discard (delete) all SMTP emails with dangerous attachments

Emails with dangerous attachments will be accepted and immediately deleted.

Add email addresses from outgoing email to Copfilter Whitelist

This option will extract any Recipient Email Addresses from outgoing SMTP emails which originated from the **GREEN**, **ORANGE** and **BLUE** network. These addresses will then be entered into the Copfilter Whitelist, except when sender=recipient, internal email address should not be added into the whitelist, as all incoming email to this address would then be whitelisted. If you wish to only add email addresses, which originated in the GREEN network then copy this file

```
/var/log/Copfilter/default/opt/tools/bin/IpInSubnet.pl_add_email_address_to_whitelist_from_GREEN
```

to this file

```
/var/log/Copfilter/default/opt/tools/bin/IpInSubnet.pl
```

or simply edit /var/log/Copfilter/default/opt/tools/bin/IpInSubnet.pl and modify it for your needs

Disable all Spam scanning on outgoing email from internal network

If an email is sent from a computer located in the internal network (**GREEN** interface) then Spam scanning will be skipped and this Header will be inserted into the email:

```
X-Copfilter:Client is part of our network, skipped SpamAssassin
```

Enable Copfilter Whitelist modifications via email

Any user will be able to send an email containing whitelist commands to any external email address. Copfilter will intercept, extract the commands and discard the email.

The body of the email has to contain (multiple lines possible):

```
Copfilter_add_to_whitelist      youraddress@domain.com
```

```
Copfilter_remove_from_whitelist  adress@domain.com
```

Users can add email address to the whitelist only, blacklist commands will be ignored, any asterisk in an email address will not be valid, so no *@domain.com whitelist commands will be possible. Only the administrator is able to do this. This is because of security reasons, we don't want any user to blacklist any other users email

Use Copfilter Whitelist and Blacklist

All incoming emails which contain an email address (in the From field) from the Whitelist will not be scanned from Spam.

This Email Header will be inserted:

```
X-Copfilter:Sender is in Whitelist, skipped SpamAssassin
```

This does not affect Virus scanning, meaning that all emails whitelisted email address will still be scanned for Viruses. All incoming emails which contain an email address (in the From field) from the blacklist will be discarded immediately.



Quarantine Spam emails if ...

... if score is greater than: 5-40

Emails containing a Spam score greater than the configured value will be quarantined. Users will receive a notification. The POP3 Protocol does not allow email discarding during POP3 retrieval (so these notifications cannot be disabled)

Send user a copy of quarantined Spam email

If a Spam email has been quarantined the user will receive a copy.

Quarantine Virus infected emails

This option will save an original copy of a Virus infected email in the quarantine. If it is set to off then all infected emails will be deleted immediately.

Quarantine Virus infected emails

This option will save an original copy of a Virus infected email in the quarantine. If it is set to off then all Virus infected emails will be deleted.

Remove emails in quarantine if older than (in days)

Any emails in the SMTP quarantine will be deleted if they are older than this amount of days.

Notes:

Clicking on the Save settings button will automatically restart the necessary services in order to apply your settings. Enable "Skip Service Restart" if you wish to skip restarting the service. Restart of proxsmtpd service is required if one of the following options has been modified:

- Enable ProxSMTP to filter outgoing traffic on **GREEN**
- Enable ProxSMTP to filter outgoing traffic on **BLUE**
- Enable ProxSMTP to filter outgoing traffic on **ORANGE**
- Enable ProxSMTP to filter incoming traffic on **RED** and forward to internal Email Server

HTTP Scanning

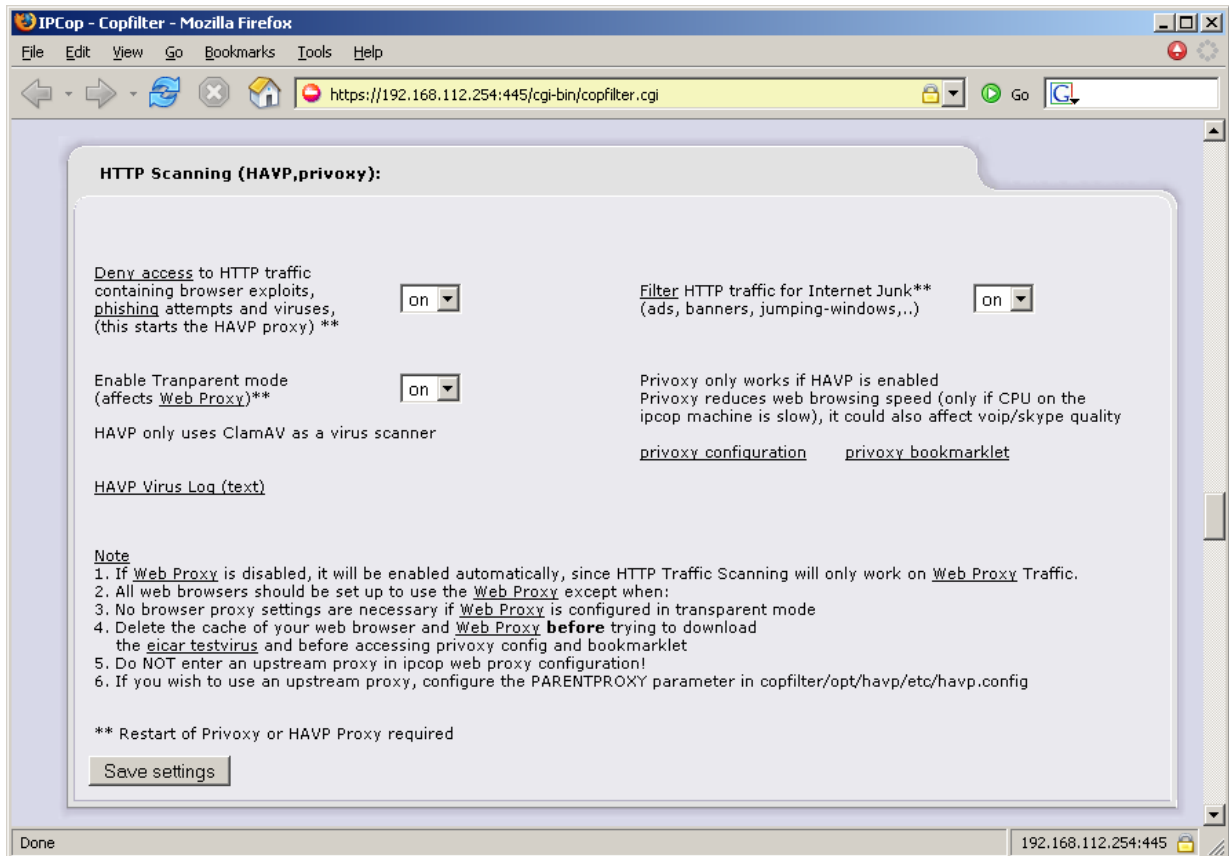


Fig. 12: HTTP Scanning Settings within the Copfilter Web GUI

Options:

Deny access to HTTP traffic containing browser exploits, phishing attempts and Viruses(this starts the HAVP Proxy)

This option will enable HTTP Virus scanning. If a Virus is found, access to that file will be denied and a webpage notifying you about the name of the Virus will appear instead.

HAVP only uses ClamAV as a Virus scanner. This will also work if ClamAV is disabled since it loads the ClamAV library when starting. For HTTP Scanning, the IPCop Proxy (squid) needs to be enabled. On english IPCop installations the web Proxy gets started automatically.

Enable Transparent mode (affects Web Proxy)

This will option will automatically enable the IPCop Webproxy in transparent mode (only on english installations)

HAVP Virus Log (text)

Some HAVP Virus statistics. If you enable Web Proxy logs, then theses logs will also display the IP address of computer, from which the Virus-infected webpage was requested.

Filter HTTP traffic for Internet Junk (ads, banners, jumping-windows,..)

This option activates the Privoxy internet junk filter. Privoxy only works if HAVP is enabled Privoxy reduces web browsing speed (only, if CPU on the IPCop machine is slow), it could also affect VoIP/Skype quality

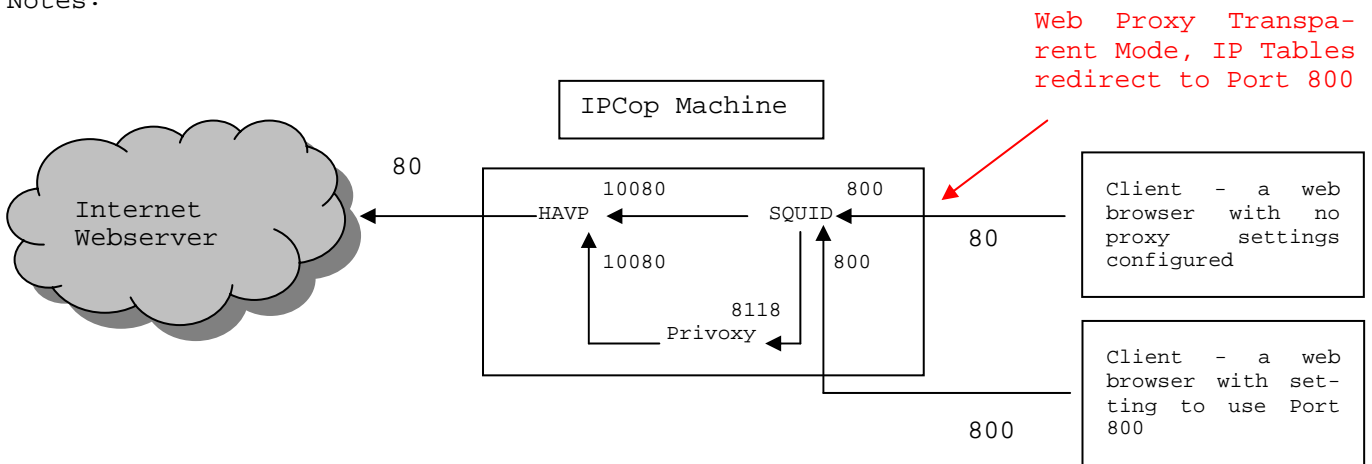
Privoxy configuration

This link will allow you to configure Privoxy settings

Privoxy bookmarklet

this link will allow you to quickly enable or disable privoxy, just in case a website isn't displayed correctly with privoxy turned on (you could as well change the Proxy settings) you can also set a bookmark to this link for quick access

Notes:



This has the following advantages:

- All transparent, no web browser client Proxy settings necessary
- Better web browsing performance since Privoxy filters out junk needed stuff first, before passing along to squid
- Maintains compatibility with other IPCop Add-ons such as COP+, Dansguardian, Advanced Proxy, Urlfilter

Privoxy works between HAVP and SQUID, if enabled. HAVP acts as parent Proxy to squid.

Internet Junk

Ads, Banners, Web-Bugs, unsolicited Pop-Ups, Jumping-Windows, MS Internet Explorer exploits, HTML-annoyances, modifying web page content, and other obnoxious Internet Junk

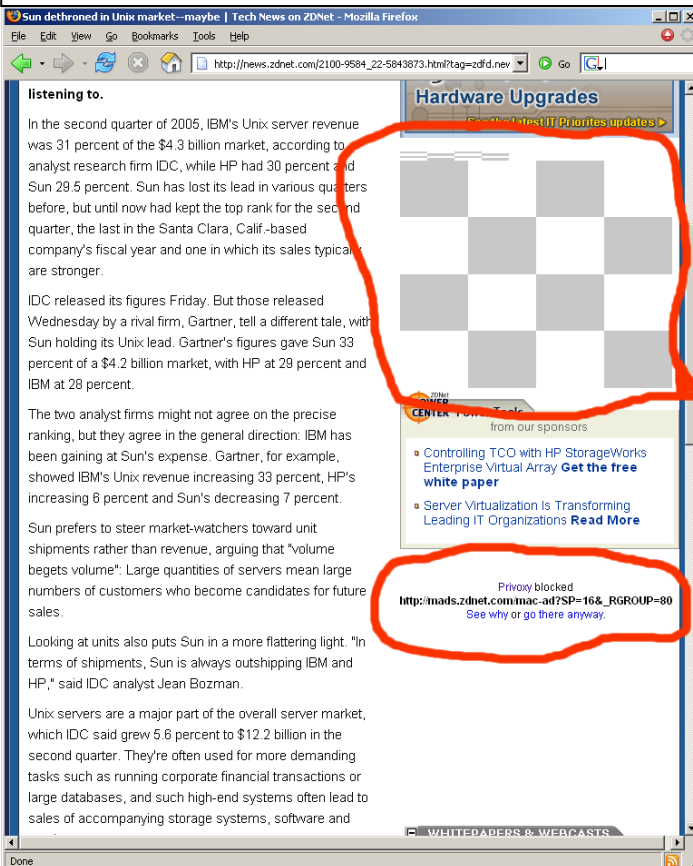
These settings can be customized here: `/var/log/copfilter/default/opt/privoxy/etc/`

Added section to Privoxy to easily whitelist domains:

- Enable Privoxy and point your browser to `config.privoxy.org`
- Then choose "View & change the current configuration"
- Then click on Edit right beside `"/var/log/copfilter/default/opt/privoxy/etc/user.action"`
- Then in the first section (scroll down one page) where you will see the domain `".Copfilter.org"`
- Click on the add button and add your domain in this manner `".yourdomain.com"` (don't forget the leading dot)



Fig. 13: A web page without (above) and with (below) active Privoxy



Note:

ONLY HTTP TRAFFIC ON PORT 80 WILL BE Virus SCANNED

Means, that if a web server is running on a port other than 80, then traffic to this web server will **NOT** be Virus scanned!

So, if you only want to allow Virus scanned HTTP traffic, then you need to block traffic to any other ports. This could, for example, be done with a different IPCop Add-On named BlockOutTraffic. This Add-On can be found here:

<http://firewalladdons.sourceforge.net/blockouttraffic.html>

Note:

Clicking on the "Save settings" button will automatically restart the necessary services in order to apply your settings. Enable "Skip Service Restart" if you wish to skip restarting the service. Restart of HAVP and Privoxy service is required if any settings have been changed.

Notes:

1. If Web Proxy is disabled, it will be enabled automatically, since HTTP Traffic scanning will only work on Web Proxy Traffic.
2. All Web Browsers should be set up to use the Web Proxy except if Web Proxy is configured in transparent mode (no Browser Proxy settings are necessary)
3. Delete the cache of your Web Browser and Web Proxy before trying to download the eicar Test Virus and before accessing Privoxy Config and Bookmarklet
4. Do NOT enter an upstream Proxy in IPCop Web Proxy configuration!
5. If you wish to use an upstream Proxy, configure the PARENTPROXY parameter in copfilter/opt/havp/etc/havp.config
6. Web Proxy logging will be enabled automatically, so that havp Virus logs will work

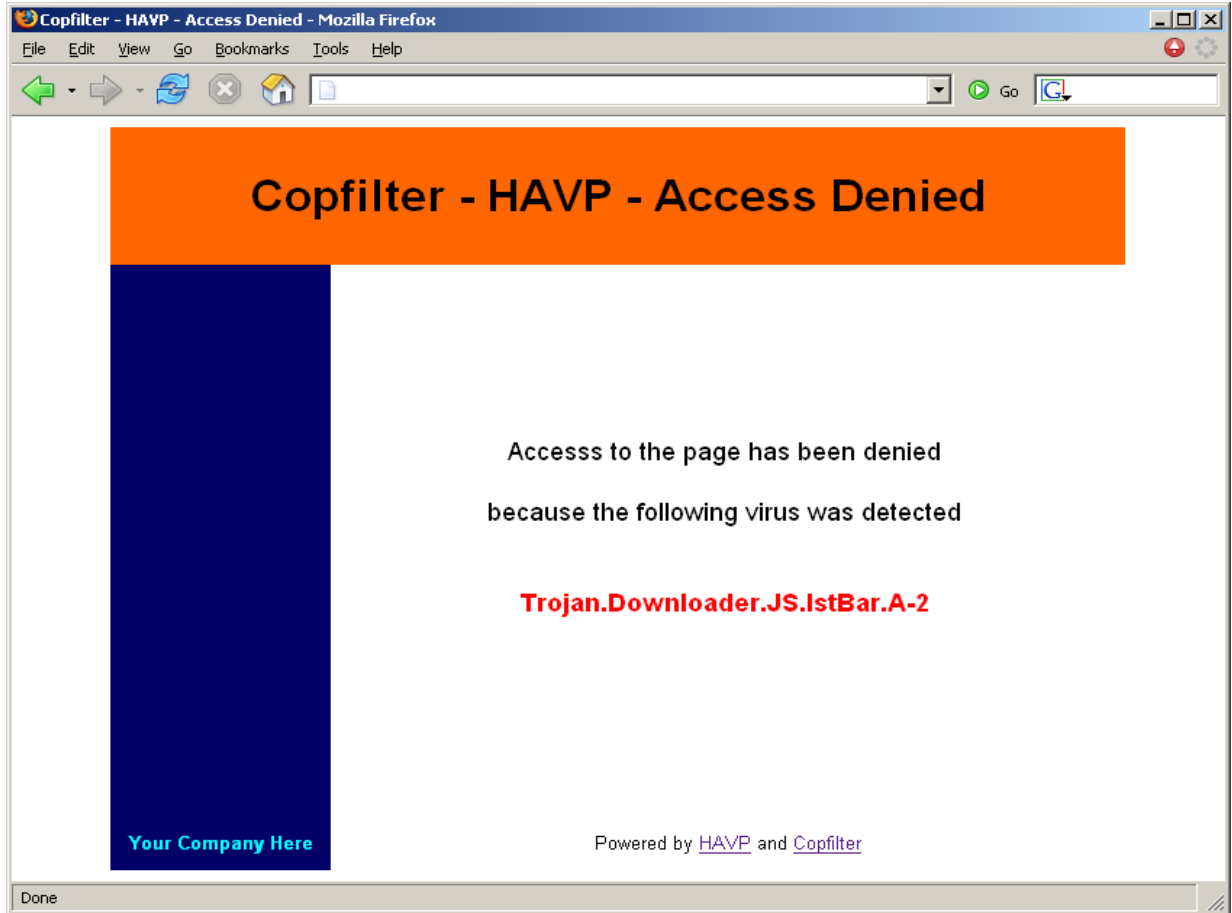


Fig. 14: HAVP in „action“

FTP Scanning

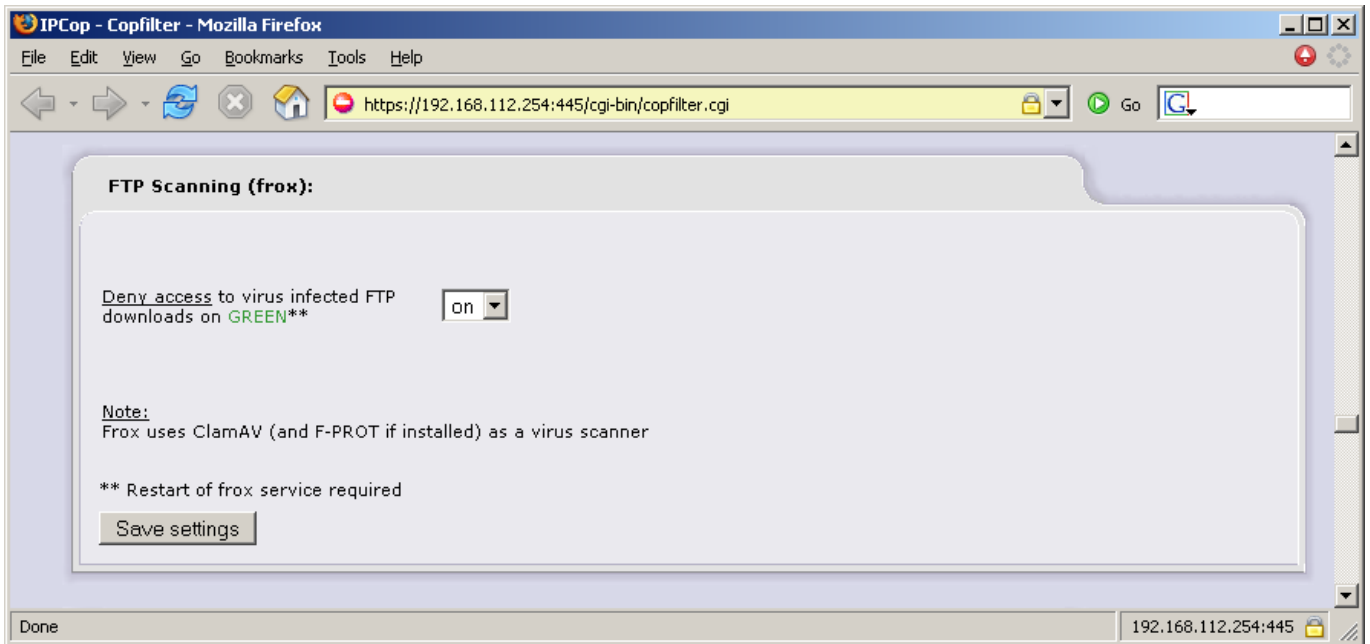


Fig. 15: FTP Scanning Settings within the Copfilter Web GUI

Options:

Deny access to Virus infected FTP downloads on **GREEN**

Deny access to Virus infected FTP downloads on **BLUE**

Deny access to Virus infected FTP downloads on **ORANGE**

BLUE and **ORANGE** interface options will only visible if these interfaces exist.

This will only work if either ClamAV or F-Prot (if installed) are enabled as well. This option enables FTP traffic scanning for Viruses. If a Virus is found, access to that file will be denied and your client will fail to download the file.

Be aware that when you try to download an ftp file. It might appear that your FTP client (for example a Web Browser or a command line FTP utility) is hanging. This is so because the FTP Proxy is already downloading the file in the background, and only sends a few bytes of this file to your FTP client. It will deliver the rest of the FTP file to your client only after it has fully downloaded and scanned the ftp file.

Again:

If you are using a Web Browser as an FTP client then you will receive the "save as" dialog only AFTER the FTP Proxy has successfully downloaded and scanned the FTP file. This could take a while so don't be confused if you do not get an immediate reply and if it seems that your web browser might be hanging. The FTP Proxy will send some bytes to your web browser from time to time to prevent it from running into a time-out.

Frox uses ClamAV as a Virus scanner and F-PROT if installed

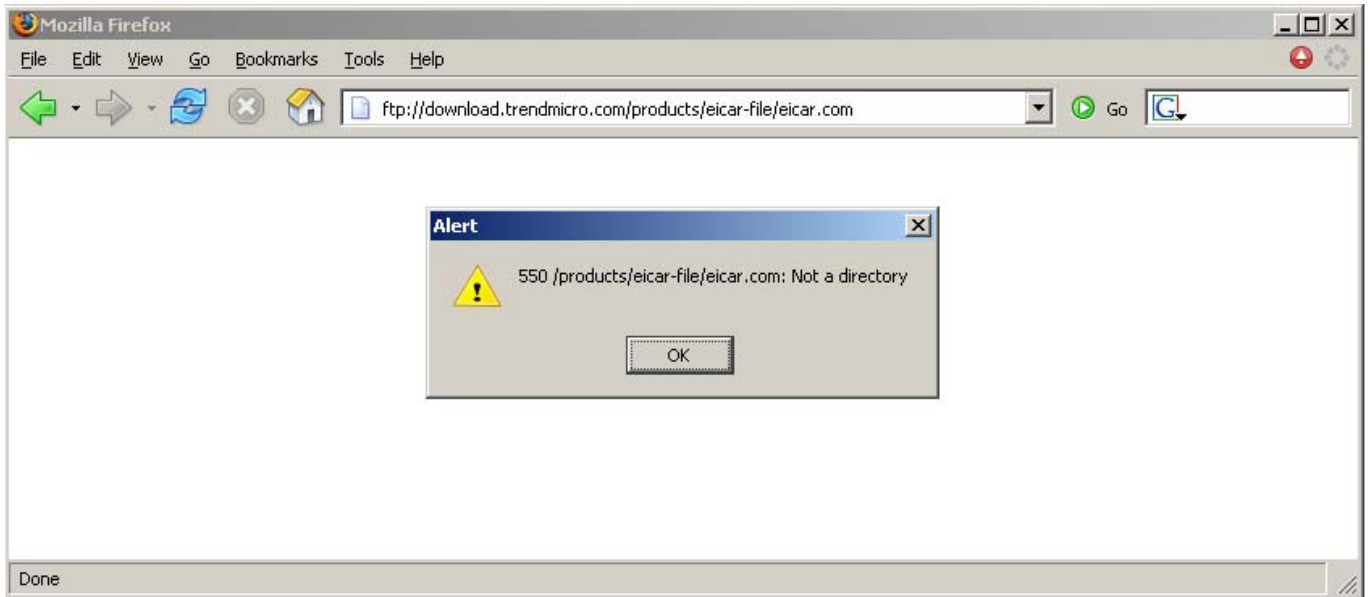


Fig. 15a: Frox in „action“

Notes:

Clicking on the Save settings button will automatically restart the necessary services in order to apply your settings. Enable "Skip Service Restart" if you wish to skip restarting the service. Restart of frox service is required if any setting has been changed.

AntiSpam

SpamAssassin Statistics (text)

This will show Spam/ham statistics including:

- number of Spam/ham messages received in each month of the year
- number of Spam/ham messages received in each day of the current month and current year
- scanning information about the last 200 received ham and Spam messages

SpamAssassin Statistics

- selectable year, month
 - > will show statistics of that month, with percentage comparisons of ham and Spam
- selectable year, month, day
 - > will show statistics of that day, with percentage comparisons of ham and Spam

Enable SpamAssassin (necessary to detect Spam)

Enable this option if you want to enable Spam detection, P3scan and ProxSMTP will not be able to detect Spam if this option is off.

Copfilter Whitelist Manager

A link to the Copfilter Whitelist Manager, which is a Blacklist as well

Copfilter Spam Digest Manager

A link to the Spam Digest Manager. Here you can enter the email addresses which should receive a Spam digest notification message. Copfilter will search for those email addresses in the Spam quarantine and send a digest notification message to each email address including brief information about the Spam messages that email address has received, this is done once a day (at about midnight)

Score required to identify email as Spam (subject will be modified)**

The threshold at which a email will be marked as Spam.

Razor, DCC, DNSBL (improves recognition, decreases performance)**

Enable or disable additional Spam checks which need to connect to the internet (dns lookup queries). This option greatly increases detection but email receiveal will be delayed (between 10-120sec depending on the email)

Send daily Spam digest (only from emails in Spam quarantine from the last 24h) to recipients in Digest Manager see the description above

German Rules**

This option will add additional german Spam checks.

SpamAssassin Bayes:

Enable Bayesian Scoring in SpamAssassin:

Turn this on if you want bayes scoring in SpamAssassin (it will be active after the first bayes training) After training the Bayes classifier, examine the email headers of any new email, they should contain bayes scoring, similar to:

```
* 3.5 BAYES_99 BODY: Bayesian Spam probability is 99 to 100%
```

Run bayes training daily (0:55):

This allows you to train the Bayesian classifier in SpamAssassin by fetching emails from a remote IMAP server. On the IMAP server, create two folders on the same level like INBOX: "spam" and "not-spam". Copy or move at least 200 Spam and 200 non-spam emails into these folders (emails tagged as *** Spam *** can be used as well). All SpamAssassin related tags will be ignored while training.

If you have additional email header fields which should be ignored (for example if you ISP adds some email headers then you should add these to /var/log/Copfilter/default/opt/mail-spamassassin/etc/mail/spamassassin/local.cf and use the bayes_ignore_header parameter). No bayes scoring will occur if less than 200 emails are trained. Training takes about one hour for 400 emails. Execute tail -f /var/log/messages on the console to follow the status if you like (per email one dot will be printed)

Moving false negatives to the Spam folder and false positives to the non-spam folder will improve bayes scoring significantly. An email report with the results will be sent to Email Address

AntiSpam (SpamAssassin, P3PMail, Renattach, RulesDuJour):

SpamAssassin Statistics [SpamAssassin Statistics \(text\)](#)

Year: Month:
 Year: Month: Day:

SpamAssassin:

Score required to identify email as spam (subject will be modified)** **Razor, DCC, DNSBL****
(improves recognition, decreases performance)

Send daily spam digest (only from emails in spam quarantine from the last 24h) to recipients in Digest Manager **German Rules****

SpamAssassin Bayes:

Enable Bayesian Scoring in Spamassassin:
 Run bayes training daily (0:55): **IMAP SPAM Username:**
IMAP Server: **IMAP SPAM Password:**

1. This allows you to train the Bayesian classifier in Spamassassin by fetching emails from a remote IMAP server.
2. On the IMAP server, create two folders on the same level like INBOX: "spam" and "not-spam"
3. Copy or move at least 200 spam and 200 not-spam emails into these folders (emails tagged as *** SPAM *** can be used as well)
4. No bayes scoring will occur if less than 200 emails are trained
5. Execute the "Run Bayes Training Now" button (this will actually empty these folders on your IMAP server)
6. Training takes about one hour for 400 emails
7. Execute tail -f /var/log/messages on the console to follow the status if you like (per email one dot will be printed)
8. Moving false negatives to the spam folder and false positives to the non-spam folder will improve bayes scoring significantly
9. An email report with the results will be sent to [Email Address](#)
10. Now examine the email headers of any new email, they should contain bayes scoring, similar to:
 * 3.5 BAYES_99 BODY: Bayesian spam probability is 99 to 100%

Attachment renamer (renattach):
 Files with the following extensions will be renamed, if bad attachment scanning has been enabled.
 ADE, ADP, BAS, BAT, CHM, CMD, COM, CPL, CRT, EML, EXE, HLP, HTA, INF, INS, ISP, JS, JSE, LNK, MDB, MDE, MSC, MSH, MSI, MSP, MST, NWS, OCX, PCD, PIF, REG, SCR, SCT, SHB, SHS, URL, VB, VBE, VBS, WSC, WSF, WSH (manual configuration in renattach.conf)

Rules Du Jour: improves recognition, but decreases performance**

Current rules_du_jour spam rules: **Automatic update*:** **Manual update:**

sare_adult sare_bayes sare_evilnum Enabled every:
 sare_evilnum sare_evilnum sare_genisubj Disabled
 sare_genisubj sare_header sare_html
 sare_obfu sare_oem sare_random
 sare_specific sare_spoof sare_uri sare_bml
 sare_redirect sare_fraud
 bogus-virus-warnings casino chickenpox
 lasertoners medtable_obfu nigeria_german
 nigeria_newgen obfuscated random
 rbl-combo sexmail sober_g sober_p
 tripwire worm_found

** Restart of spamd service required
 * Update notifications are sent to [Email Address](#)

Fig. 16: AntiSpam Settings within the Copfilter Web GUI

IMAP Server:

```
IMAP Spam Username:      )
                        ) self explaining, see below
IMAP Spam Password:     )
```

The Spam or ham messages need to train the bayesian classifier in SpamAssassin need to reside on an IMAP server in a "spam" and "no-spam" folder at the same level as "inbox". These options will be used to login into the IMAP server and retrieve those messages. After a successful download the messages will be deleted from those folders.

Rules Du Jour: improves recognition, but decreases performance*

Enabling rules du jour will enable SpamAssassin to use lots of Spam detection rulesets.

Current rules_du_jour Spam rules:

A list of currently used Spam detection rulesets

Automatic update:

Turn this on, if you want Copfilter to automatically download updates of Spam detection rulesets. This may happen once in one or two months.

Manual update:

Manually start the Spam detection ruleset update.

Run Bayes Training Now

Execute the "Run Bayes Training Now" button (this will actually empty these folders on your IMAP server)

Clicking on the "Save settings" button will automatically restart the necessary services in order to apply your settings. Enable "Skip Service Restart" if you wish to skip restarting the service. Restart of Spamd service is required if any setting of these settings have been changed:

- Enable SpamAssassin (necessary to detect Spam)
- Score required to identify email as Spam (subject will be modified)
- Razor, DCC, DNSBL (improves recognition, decreases performance)
- German Rules
- Rules Du Jour

The "Spam Quarantine" button will show a list of email messages, which were quarantined, because they were identified as Spam.

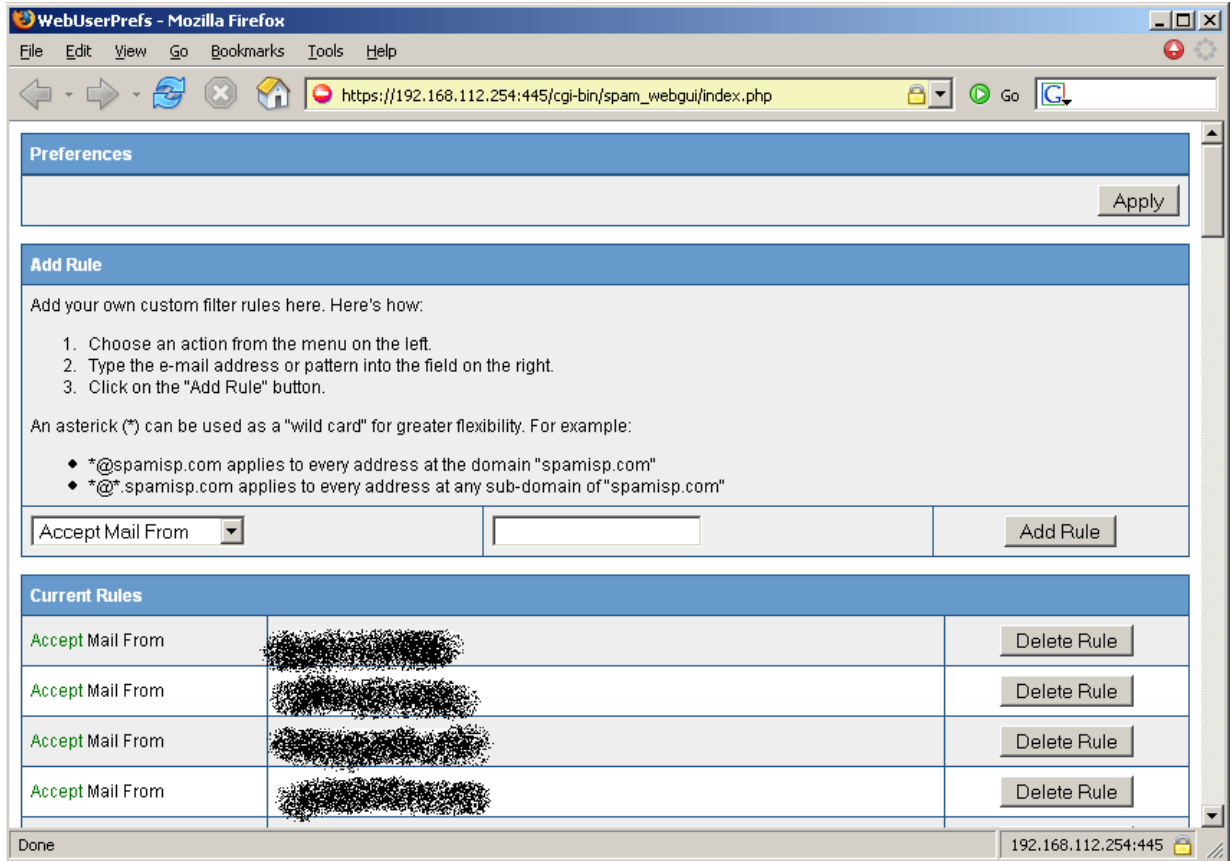


Fig. 17: The Copfilter Whitelist/Blacklist Manager

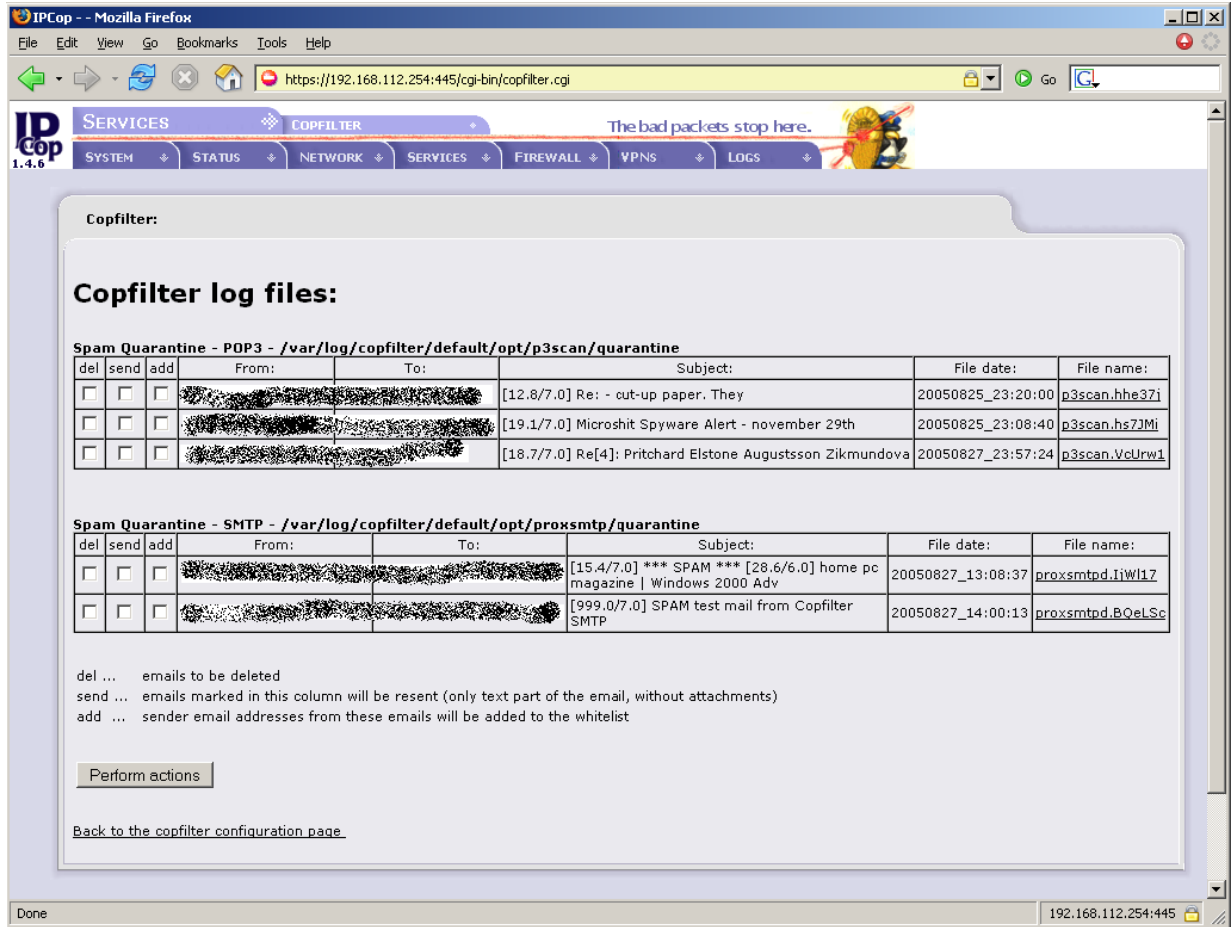


Fig. 18: The Spam Quarantine list, accessible through the Copfilter Web GUI

AntiVirus

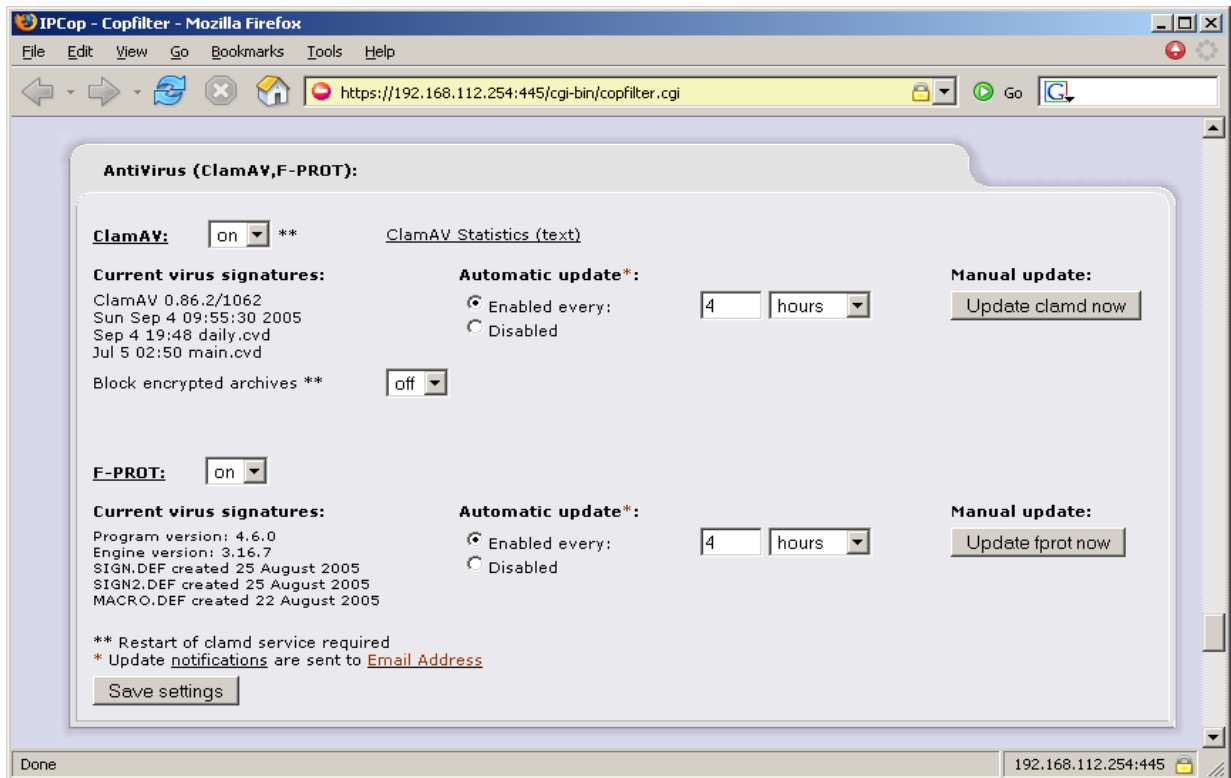


Fig. 19: AntiVirus Settings within the Copfilter Web GUI

ClamAV:

Turn ClamAV on to enable Virus scanning. P3Scan and Proxsmtpd will not be able to detect Viruses if this setting is off.

Block encrypted archives**:

If this option is enabled, clamav will treat encrypted archives as if they were Viruses. This might be useful if a encrypted attachment contains a Virus (the password might be in the email itself, encouraging users to open the encrypted attachment)

ClamAV Statistics (Text) (immediate updates)

This will show Virus statistics including:

- List of most detected Viruses (with percentage value)
- text statistics, Viruses by hour/day/month and year
- exact number of Viruses received in each month of the year
- exact number of Viruses received in each day of the current month and current year
- list of the last 200 received Viruses
- Graph (weekly updates, starts after one week)

These statistics start after one week (the scripts will analyze only the rotated log files from logrotate, and the first rotation is in a week).

Current Virus signatures:

List of current ClamAv signatures with timestamps.

Automatic update:

Enable automatic Virus signature updating with this option

Manual update:

This allows a user to manually update the Virus signatures, for example in an event of a Virus outbreak

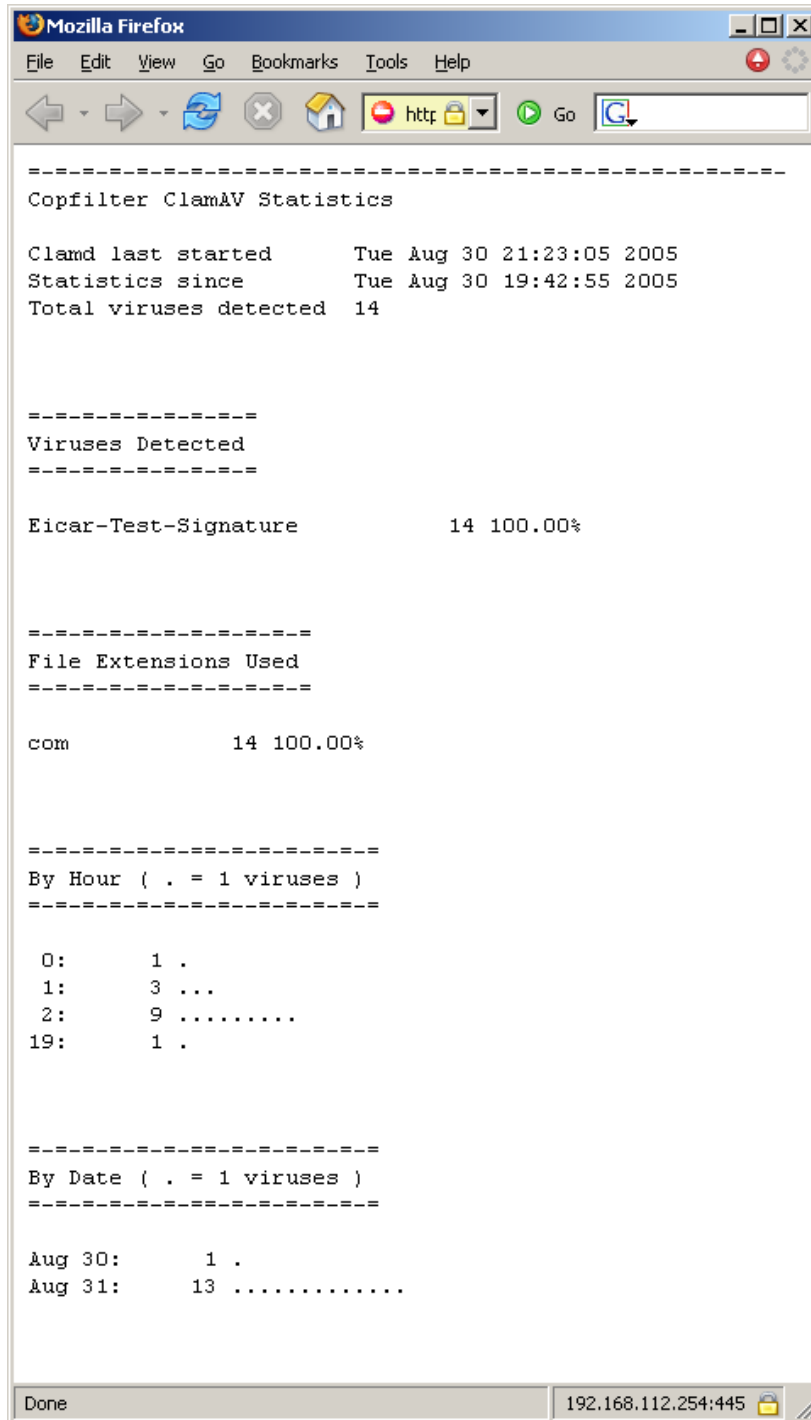


Fig. 20: Copfilter's ClamAV Statistics, accessible through the Web GUI

If f-prot has been installed these menu will appear:

F-PROT:

Current Virus signatures:

List of current clamav signatures with timestamps

Automatic update:**

Enable automatic Virus signature updating with this option

Manual update:

This allows a user to manually update the Virus signatures, for example in an event of a Virus outbreak.

Attachment Renamer (renattach):

Files with the following extensions will be renamed, if dangerous attachment scanning has been enabled:

ADE, ADP, BAS, BAT, CHM, CMD, COM, CPL, CRT, EML, EXE, HLP, HTA, INF, INS, ISP, JS, JSE, LNK, MDB, MDE, MSC, MSH, MSI, MSP, MST, NWS, OCX, PCD, PIF, REG, SCR, SCT, SHB, SHS, URL, VB, VBE, VBS, WSC, WSF, WSH (manual configuration in renattach.conf)

This is an information about attachment extensions which will be renamed, if attachment renaming has been enabled in P3Scan or ProxSMTP.

The "Virus Quarantine" button will show a list of unmodified email messages, which were quarantined, because they contained a Virus.

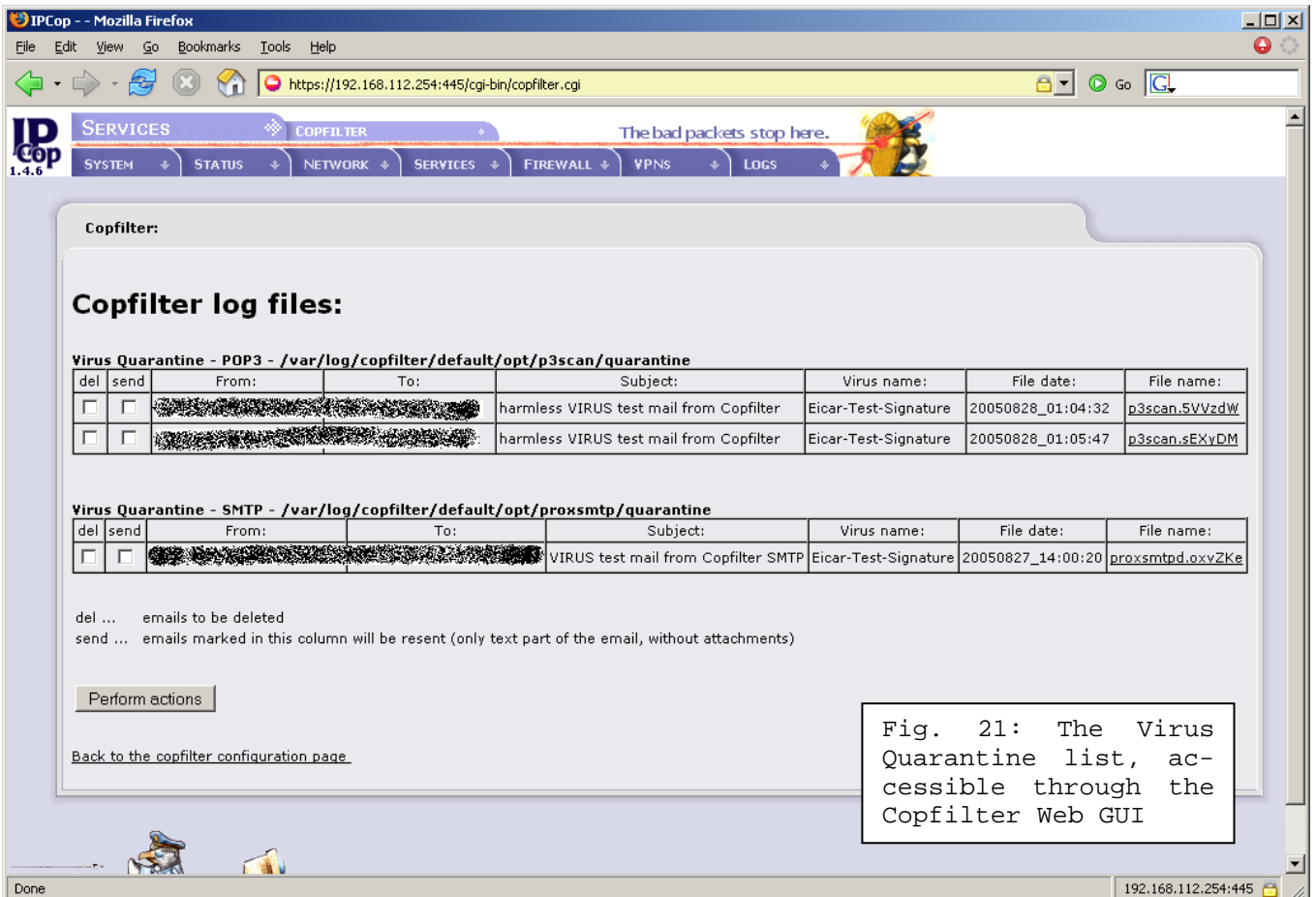


Fig. 21: The Virus Quarantine list, accessible through the Copfilter Web GUI

Notes:

Clicking on the Save settings button will automatically restart the necessary services in order to apply your settings. Enable "Skip Service Restart" if you wish to skip restarting the service. Restart of clamd service is required if clamav settings has been changed.

TESTING

Send Test Virus Email

Send Test Spam Email

Send Test Email+bad Attachment

These options send emails to the Email Address given on the Email Settings page, for testing purposes.

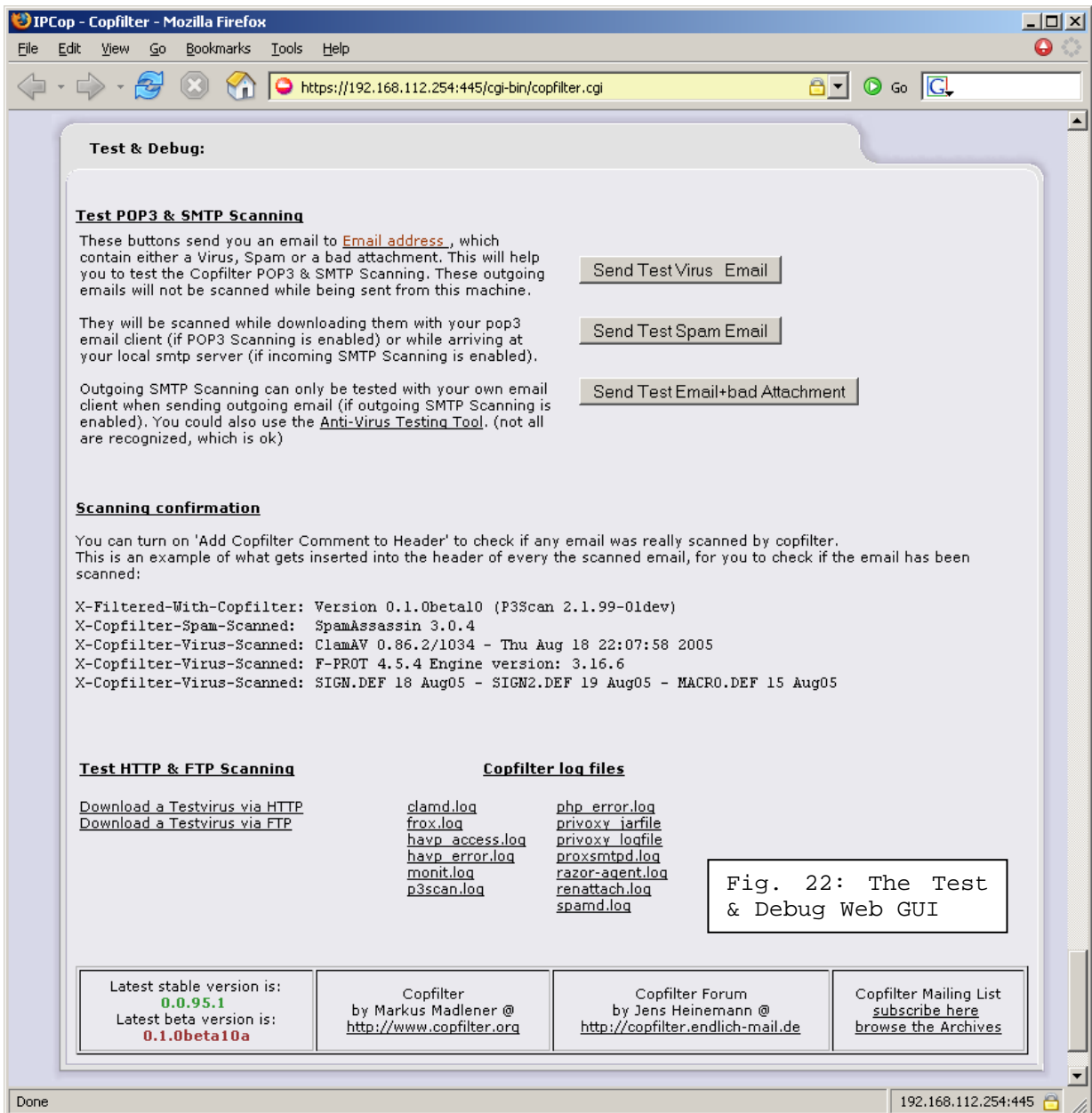


Fig. 22: The Test & Debug Web GUI

Please refer also to Chapter "Quick Installation" on Page 13 of this Manual.

Setup

Since the /var/log directory resides on the biggest partition on every IPCop installation, Copfilter will be installed into /var/log/Copfilter

Setup_util script command line parameters

Usage: setup_util OPTION

Options:

-a, --addmenu

add Copfilter menu to the Web GUI (already done with -i)

-b, --backup [FILE]

backup current settings & logfiles (optional: backup file)

-d, --default

restore default configuration

-i, --install [--force]

install (or reinstall) Copfilter (use force if already installed)

-f, --fprot FILE

install F-Prot, FILE:

download and copy F-Prot >GZIP-ed TAR file< to IPCop from this Url:

http://www.f-prot.com/download/home_user/download_fplinux.html

example: setup_util -f fp-linux-ws.tar.gz

-r, --restore [FILE]

restore configuration (optional: restore file)

-R, --regrazor

register razor



-u, --uninstall

uninstall Copfilter and F-Prot

-V, --version

print version information and exit

-x, --fixbackspace

fix backspace key in vi
