

The Perfect Linux Firewall Part II -- IPCop & Copfilter

Author: Joseph Guarino - [Evolutionary IT](#)

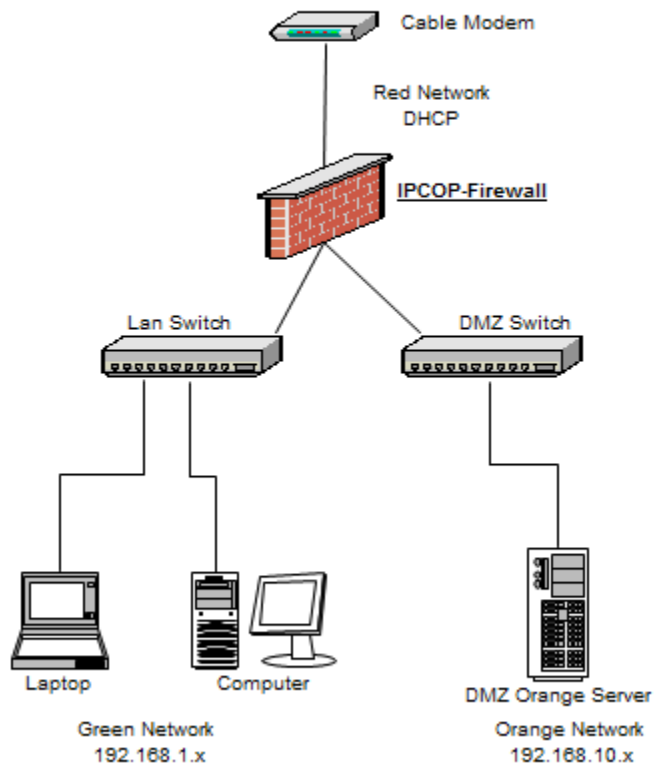
Version 2.x

This document is the second segment in a series on installing IPCop firewall. We will be creating a "DMZ" for hosting your own web server or mail server and the Copfilter proxy for filtering your application layer ingress and egress network traffic. This is intended to be a rough overview on creating a IPCop firewall with Copfilter and comes without warranty of any kind.

Using your IPCop for web hosting/mail hosting

Given the instructions from the previous article, you should have a full installation of IPCop running. The current focus remains two-fold: to get your server in the Orange (DMZ) segment of your IPCop Network and opening up the ports on your firewall to allow web traffic to it.

Example IPCop Network



Additionally, our second goal in this article will be securing our (application layer) web traffic, email and personal privacy with a wonderful add-in, called Copfilter.

As we detailed in part one, I suggested the 192.168.10.x network for our "Orange" DMZ segment. In this part of the network I will place hosts that I want visible to the outside world. Port forwarding will permit the flow of traffic from external RED (DHCP interface/network) to DMZ ORANGE network.

Orange Network Requirements

- Installed and configured server with the Distro of your choice with the email (SMTP & POP3 or IMAP and webserver of your choice. [Free & Open Source Software \(FOSS\)](#) is all about choice so pick what fits your needs..
- This orange network server must have a static IP address and not be on DHCP. For the sake of this article, we are using the static IP of 192.168.10.25 for our single internal ORANGE hosting server.

Secure your Orange Network Hosts

- Security is a process not any one tool or technology. Rather, it is many tools, technologies and processes. Consider a holistic view.
- Remember to consistently patch and monitor logs patches are an important measure to mitigate known vulnerabilities.
- Make sure you fully patched, secured and backed up any host before you expose it to the Internet.
- The best security is a layered approach so consider using a [HID \(Host Intrusion Detection\)](#), [chroot](#), [xinetd](#) and [Tcpwrappers](#) to name a few.
- Shut down any unnecessary network services on this node.
- Join the mailing lists or RSS feed for the Free/Open Source applications you are using and general security mailing lists so you are sure to be aware of vulnerabilities and issues that might arise. Also check out CERT for a general mailing list or RSS feed on security vulnerabilities. <http://www.us-cert.gov/current/>

Secure your Green Network

- Don't have a false sense of security just because you have strong and extensive IPCop/Copfilter configuration. Be sure to secure ALL of your machines. Consider a holistic view of security.

- Consistently patch your internal green nodes
- Have a Anti-Virus/Malware Scanner and Anti-Spyware Defense. In my view that extends to ALL Operating Systems.
- Enable a software firewall on your machines.

Hosting a server on a dynamic connection

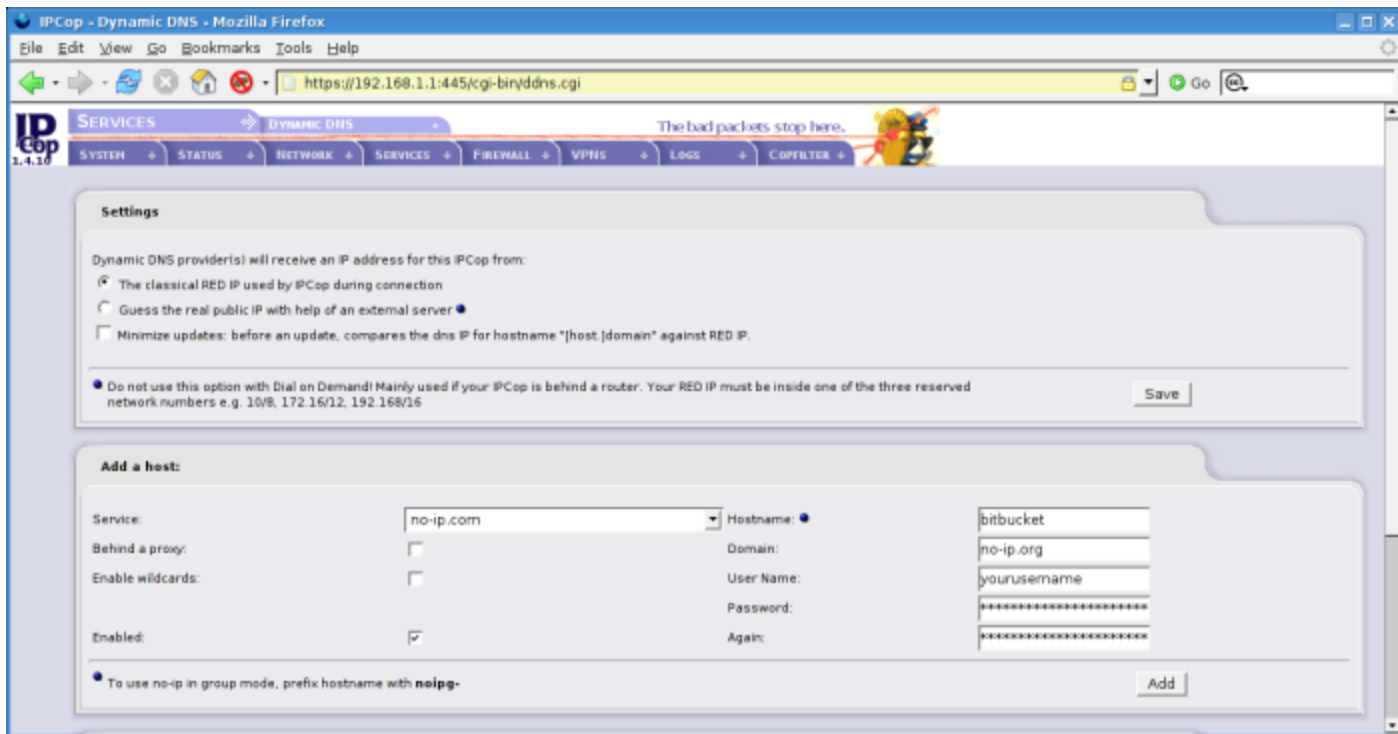
As you are using a cable modem that gives your RED IPCop network interface a dynamic DHCP address, you will need to set up Dynamic DNS services to resolve to this host via a human usable form, other than IP Address.

NOTE – Some ISPs block TCP port 80 (HTTP) 110 (POP3) and 25 (SMTP). To navigate around this, you can purchase port forwarding services from some of these dynamic DNS providers, run services on different non-blocked ports or upgrade to another provider. For the sake of this article we assume you have no ISP blocked ports.

Setting up Dynamic DNS

Along with your dynamically assigned IP address (RED), you will want to use a Dynamic DNS service to be able to allow external access to your external web/mail. Setting up Dynamic DNS with IPCop is easily achieved. Simply pick a Dynamic DNS provider listed in the IPCop DYNDNS settings.

- Go into your IPCop settings in Service Pulldown -- **Services** >> **Dynamic DNS** and under >> **Add a host**. Pick one of these supported DYNDNS providers.
- Open up your favorite browser and go to the DYNDNS provider you have chosen from the list above and register with them.
- Return to your IPCop web administration GUI and add the information in to your IPCop settings in Service Pulldown -- **Services** >> **Dynamic DNS**.
- Now return to your IPCop web administration GUI and fill in the information as listed below and then click **Add**. It will then display under “œcurrent hosts”.



What is Copfilter

An amazing project by open source developer Markus Madlener, to extend his IPCop's capabilities to the application layer (see OSI Model). Copfilter greatly enhances the capabilities of the already powerful IPCop by offering the jaw dropping and impressive large list of capabilities:

- **POP3/SMTP Scanning** - via P3Scan and ProxSMTP which allow for scanning of incoming and outgoing Email.
- **HTTP Scanning** - via HAVP which is a powerful HTTP scanning engine for scanning and securing your web traffic.
- **FTP Scanning** - via frox which allows for proxying of FTP traffic.
- **Privacy Protection** - via Privoxy which is an extremely powerful HTTP privacy protection filter which filters and or removes cookies, web ads, pop-ups and other annoying Internet junk.
- **Antivirus Scanning** - via ClamAV or F-Prot which can be used to scan your traffic for the ever prevalent malware. Please note F-Prot is a commercial product and you have to acquire a license to use it. This article utilizes the FOSS email scanner ClamAV.
- **AntiSpam** - via Spam Assassin, Vipul's Razor, DCC, renattach, RulesDuJour which coupled together make a very effective anti-spam defense.

- **Process Monitoring** - via Monit which allows you to monitor all of these processes and restart them as needed.

Why Copfilter?

You might ask yourself, if I have a IPCop firewall why would I need Copfilter? As a network security mechanism, the firewall has undergone a serious metamorphosis from a simple packet filter that only understood little of what it carried across the wire, to fully stateful inspection mechanisms that understand layer 5-7. This a far cry from the days of a simple packet filtering router or even a stripped down set of ipchains. And as security is not one technology, process or technique alone, but many of them, Copfilter is another powerful mechanism of defense in protecting your application layer.

Installing Copfilter

IPCop does not contain add-on binaries by default so they need to be copied via SCP to your IPCop. Then you will be logging in securely via SSH to your IPCop to install these binaries.

Turn on SSH on your IPCop

- Via the Webgui -> **System** -> **Ssh Access**
- Then click **Save**

NOTE - It is recommended that you shut off SSH access after you finish copying this code as SSH has many exploits.

Enable Squid on your IPCop

Via the Webgui go to -> **Services** -> **Proxy**

- **Enabled on Green**
- **Transparent on Green**
- Then click **Save.**

SSH and SCP Clients

Depending on your OS you may or may not have a native SCP or SSH client on your machine. Note the port number as TCP port 222 and NOT the default SSH/SCP port.

GNU/Linux, Unix, BSD & OSX Clients - Command Line #

Command Line *SCP*

```
scp -P 222 <Copfilterpackage_version.tar.gz  
root@ipcop_green_address>:/root
```

Command Line *SSH*

```
ssh -p 222 -l root ipcop_green_address
```

Graphical SCP/SSH -->

If you are wary of the command line or not interested, alternatively, there are several GUI clients in almost every OS. I will not address each and every one as they are so easy to use, simply requiring a drag and drop, or point and click operation.

OS X Clients -->

Cyberduck

<http://cyberduck.ch/>

Fugu

<http://rsug.itd.umich.edu/software/fugu/>

Windows -->

WinSCP - SCP Client

<http://www.winscp.net/>

Putty " SSH Client

<http://www.putty.nl/>

OpenSSH for Windows

<http://sshwindows.sourceforge.net/>

**NIX -->*

gFtp

<http://gftp.seul.org/>

Installing Copfilter

After you have SCP copied the Copfilter-x.x.tgz file to /root on your IPCop as detailed above you are now ready to install it.

SSH into your IPCop with whatever client you possess on your respective Operating System.

MD-What?

Takes an MD5 to assure that the code you downloaded is not altered or corrupted by an external source. Doing this is a simple step verifying that what you have the original, legitimate binary.

Linux/UNIX MD5

Md5sum is available in GNU/Linux and Unix by default

md5sum Copfilter-x.x.tgz and compare the output to what is listed on the download link as the MD5.

Microsoft Windows

Windows users can use the easy to use and GPLd wxChecksums or MD5Summer. Both are FOSS software which is freedom geared and light on cost.

Apple OS X

Apple users will need to open up a terminal window and type md5 Copfilter-x.x.tgz to verify the file.

Extract and Install the Binary

- cd /root
- tar xzvf Copfilter-x.x.tgz (change x to your version number)
- cd Copfilter-x.x.x
- ./install

Follow the prompts and you are all done. Reboot your IPCop and to be safe empty your browsers cache. After rebooting your IPCop you should see the Copfilter navigation item on the right most top part of the screen (next to the IPCop penguin).

Initial Copfilter Configuration

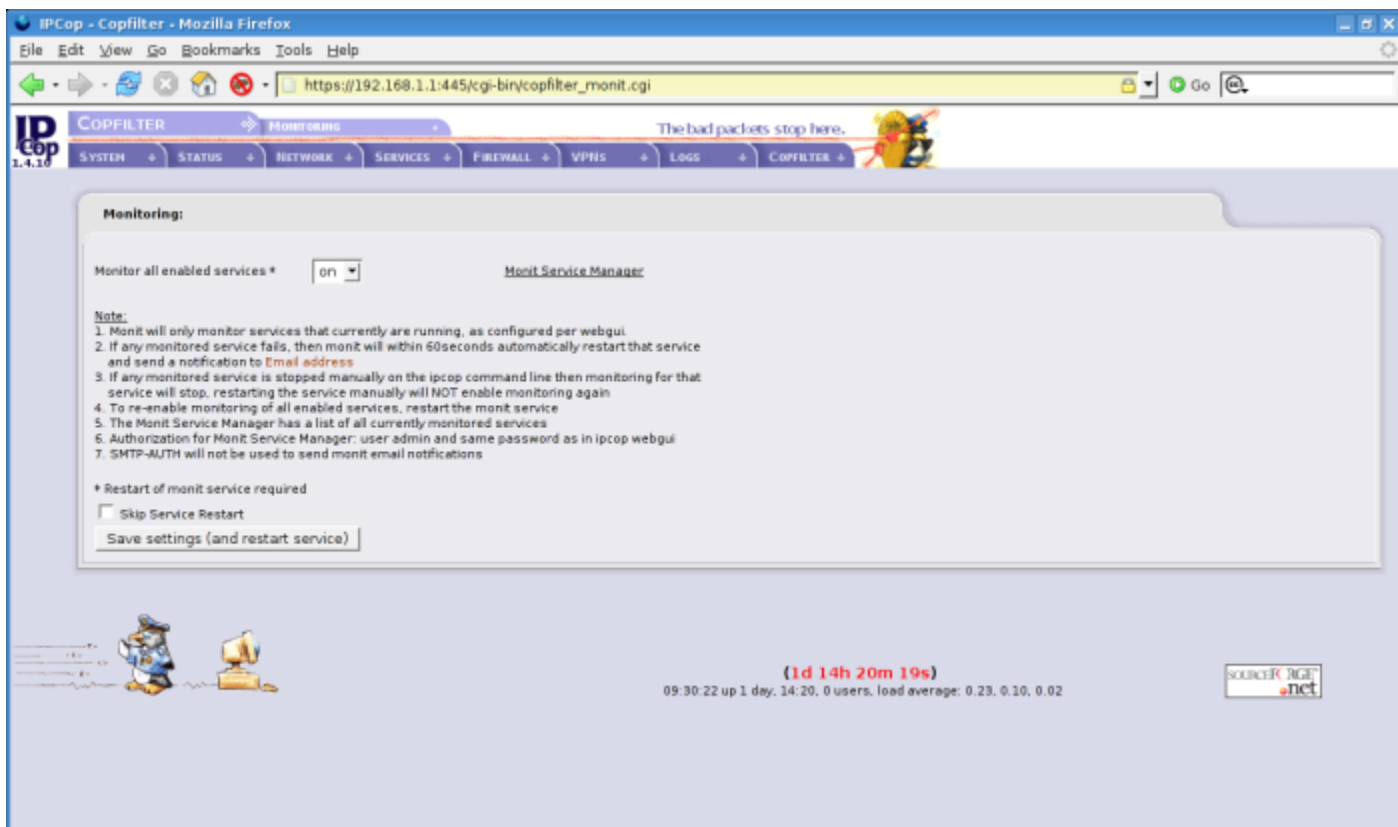
Go to Copfilter -> **Email** and configure your email address, SMTP server and then save those settings. The email address is your (root or administrator) email address and it will be used to notify you of updates and other important Copfilter messages.

IMPORTANT - It is strongly recommended that you READ the Copfilter documentation to have an in-depth understanding of the configuration options that you choose to implement. RTFM before you design and definitely before you deploy.

Monit - Monitoring Copfilter

This service enables you to monitor the core services of the Copfilter application. It provides you some resilience by automatically restarting applications should they fail.

Your Configuration Monitoring



The screenshot shows the IPCop Copfilter web interface in Mozilla Firefox. The browser address bar shows the URL: `https://192.168.1.1:445/cgi-bin/copfilter_monit.cgi`. The interface has a navigation menu with tabs for SYSTEM, STATUS, NETWORK, SERVICES, FIREWALL, VPNs, LOGS, and COPFILTER. The 'Monitoring' tab is active. The main content area is titled 'Monitoring:' and contains the following settings:

- Monitor all enabled services * ON OFF
- [Monit Service Manager](#)
- Note:**
 1. Monit will only monitor services that currently are running, as configured per webgui.
 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 webgui
 7. SMTP-AUTH will not be used to send monit email notifications
- * Restart of monit service required
- Skip Service Restart
-

At the bottom of the page, there is a status bar showing system uptime: `{1d 14h 20m 19s}` and system load: `09:30:22 up 1 day, 14:20, 0 users, load average: 0.23, 0.10, 0.02`. There is also a small logo for 'SEARCH ENGINE nct' in the bottom right corner.

- Go to **Copfilter >> Monitoring**
- Monitor all enabled services **ON**
- Then click on **Save settings** (and restart service)

Copfilter Configuration Options

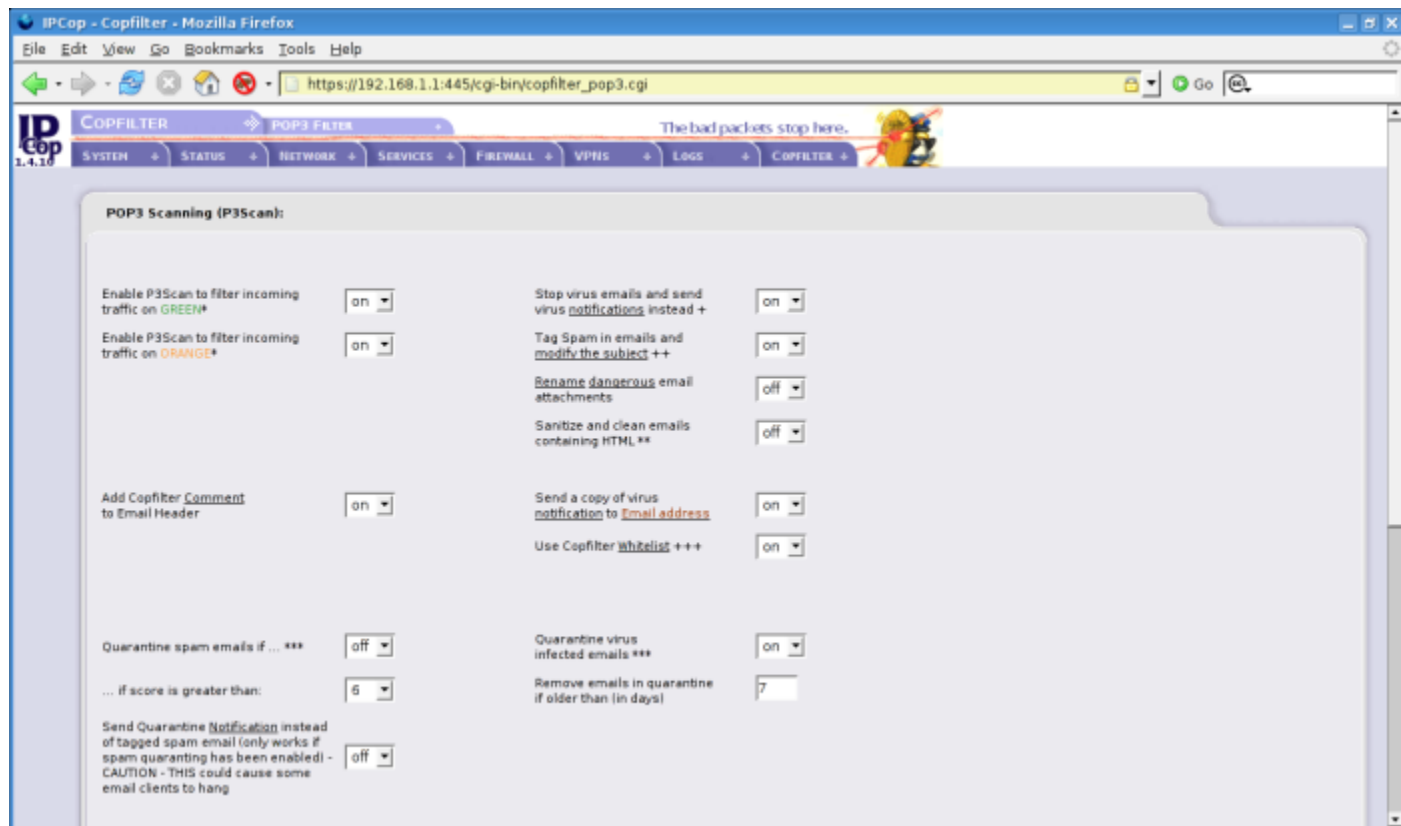
In controlling the three network services we are going to have ingress (ingoing) and egress (outgoing) control of in our IPCop/Copfilter configuration we have many granular options. Copfilter is going to be filtering our HTTP traffic, POP3, and SMTP traffic. The wonder of the Copfilter add-on is the plethora of options one can chose to deploy our configuration is of course only one of the many.

Copfilter - POP3 configuration - P3Scan

The Post Office Protocol Version 3 is the industry standard for receiving email. The goal of our configuration is to block spam/malware from being received via our email clients.

To access these setting go to **Copfilter >> POP3 configuration**

P3Scan Configuration



The following options detail those to be turned ON and all others will be left in the default OFF configuration.

- Enable P3scan on incoming traffic on Green ON
- Enable P3scan on incoming traffic on Orange ON
- Add Copfilter Comment to Email Header
- Quarantine Spam if ... *** OFF
- Tag Spam in Emails and modify the subject ON
- Stop Virus email and send virus notification instead ON
- Send a copy of virus notification to Email address ON
- Quarantine virus infected emails ON
- Remove emails in quarantine if older than (in days) 7
- Then click on Save settings (and restart service)

The net effect of this configuration will be an aggressive stance on scanning, dropping and notifying you of the spam/malware, before it reaches your internal network.

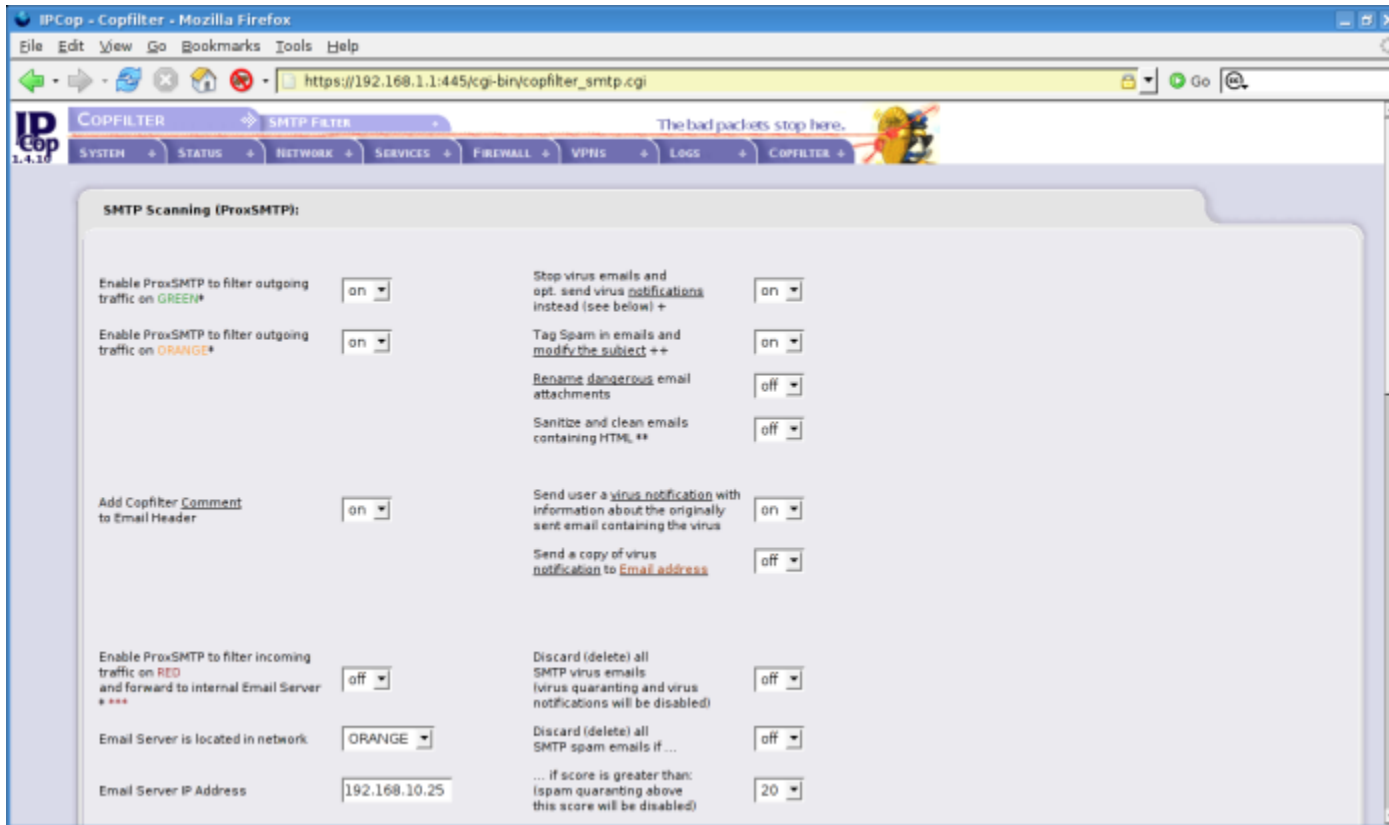
Copfilter - SMTP configuration - ProxSMTP

Simple mail transfer protocol is the standard for email transmission on the the Internet today. With the power of Copfilter one can get very granular on controlling the flow of mail message to and from our network. The goal of our configuration is to block spam/malware from being sent/received via our email clients.

To access these setting go to **Copfilter >> SMTP configuration**

The following options are to be turned ON and all others will be left in the default OFF configuration.

SMTP Filtering Configuration



- o Enable ProxSMTP to filter outgoing traffic on GREEN ON
- o Enable ProxSMTP to filter outgoing traffic on ORANGE ON
- o Add Copfilter Comment to Email Header ON
- o Enable ProxSMTP to filter incoming traffic on RED
- o Email Server is located in network ORANGE
- o Email Server IP Address 192.168.10.25
- o Red IP Alias Ethernet Interface - eth2:1
- o Tag Spam in emails and modify the subject ON
- o Stop virus emails and opt. Send virus notification instead ON
- o Send user a virus notification ON
- o Use Copfilter Whitelist and Blacklist ON
- o Remove emails in quarantine if older than (in days) 7
- o Then click on Save settings (and restart service)

NOTE - Choices of the ProxSMTP on RED interface entails 2 options:

- **RED scanning ON** - Copfilter manages the creation of Iptables rules so these are not needed to be created manually through IPCop.
- **RED scanning OFF** - Copfilter with portforwarding rule to orange mail server with scanning done at the server. I.e. you could do your ingress smtp scanning on the Email server itself & not with Copfilter.

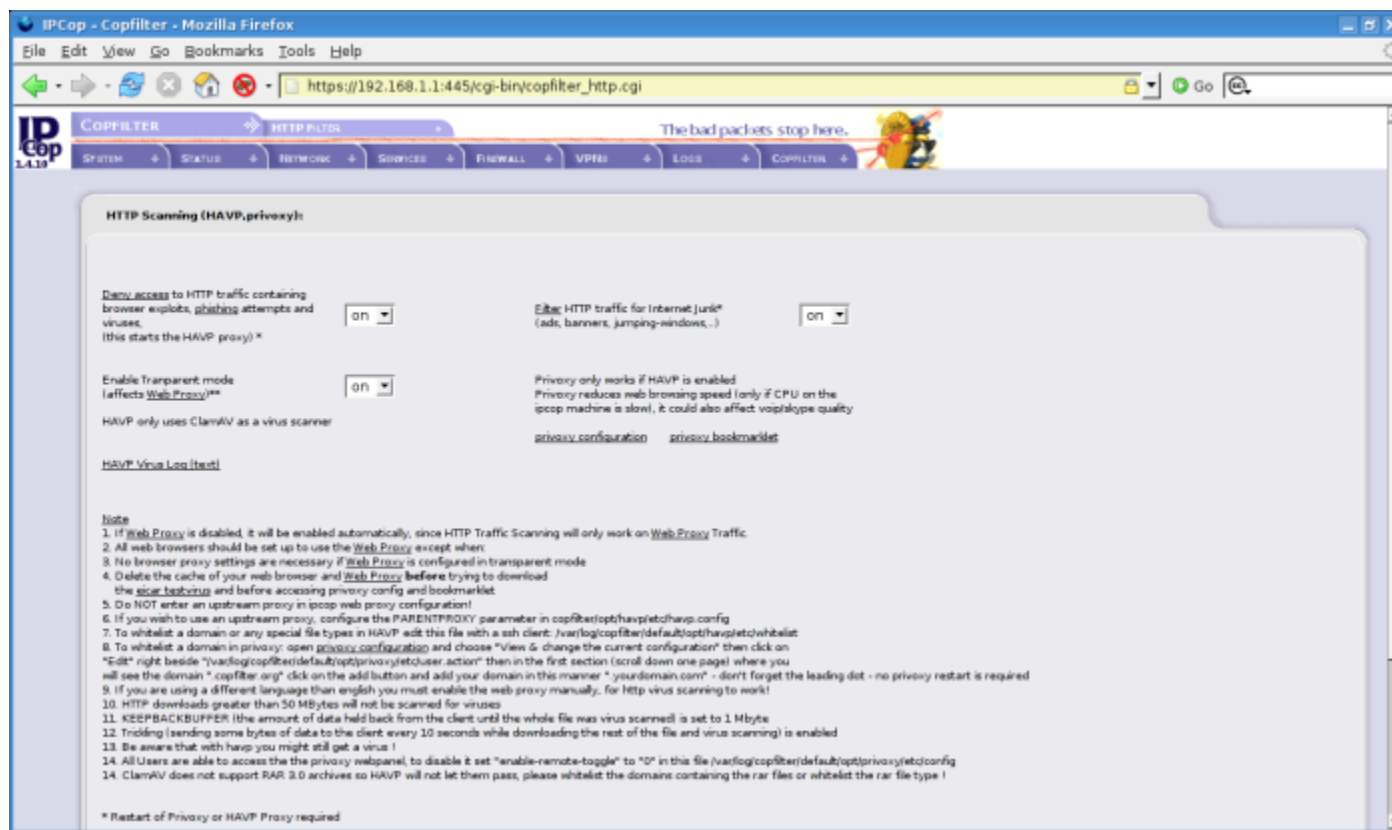
This configuration will be an proactive stance on the capturing, quarantining and deleting malware before it infect our trusted machines in the GREEN network. With quarantining ON it is recommended that an administrator be very responsive to the systems warnings about quarantine Spam, and process consistently, or it will be deleted on a weekly basis. I would not recommend keeping a Spam Quarantine setup if you are short on disk space and or want to increase this interval beyond one week. If you do you run the risk of filling up your disk. Also as whitelisting and blacklisting has been turned on remember to add in your whitelisted domains (trusted email sources) and blacklisted (domains you do not trust or want spam from).

HTTP Scanning - HAVP/Privoxy

HyperText Transfer Protocol is the protocol we use when we are surfing the Internet. HAVP (HTTP Antivirus Proxy) is a proxy server with the ClamAV anti-virus scanner. This will be crucial in your configuration to scan incoming HTTP traffic and keep malware off your machines.

To access these setting go to **Copfilter >> HTTP Filter**

HTTP Configuration



The following options are to be turned ON and all others will be left in the default OFF configuration.

- Deny access to HTTP traffic ON
- Enable Transparent mode ON
- Filter HTTP traffic for Internet Junk ON
- Then click on Save settings (and restart service)

This configuration will allow for malware to be filtered out at our IPCop box, such as browser exploits, phishing attempts and viruses. Additionally, ads, banners and other Internet advertising junk with Privoxy.

With web banners and such that are blocked you will either see the item labeled "Advertisement" or an image of a checkered pattern indicating it has been blocked. If you hate ads as much as do I you can get an add-on for Firefox called Adblock that will allow client side blocking as well. Adblock

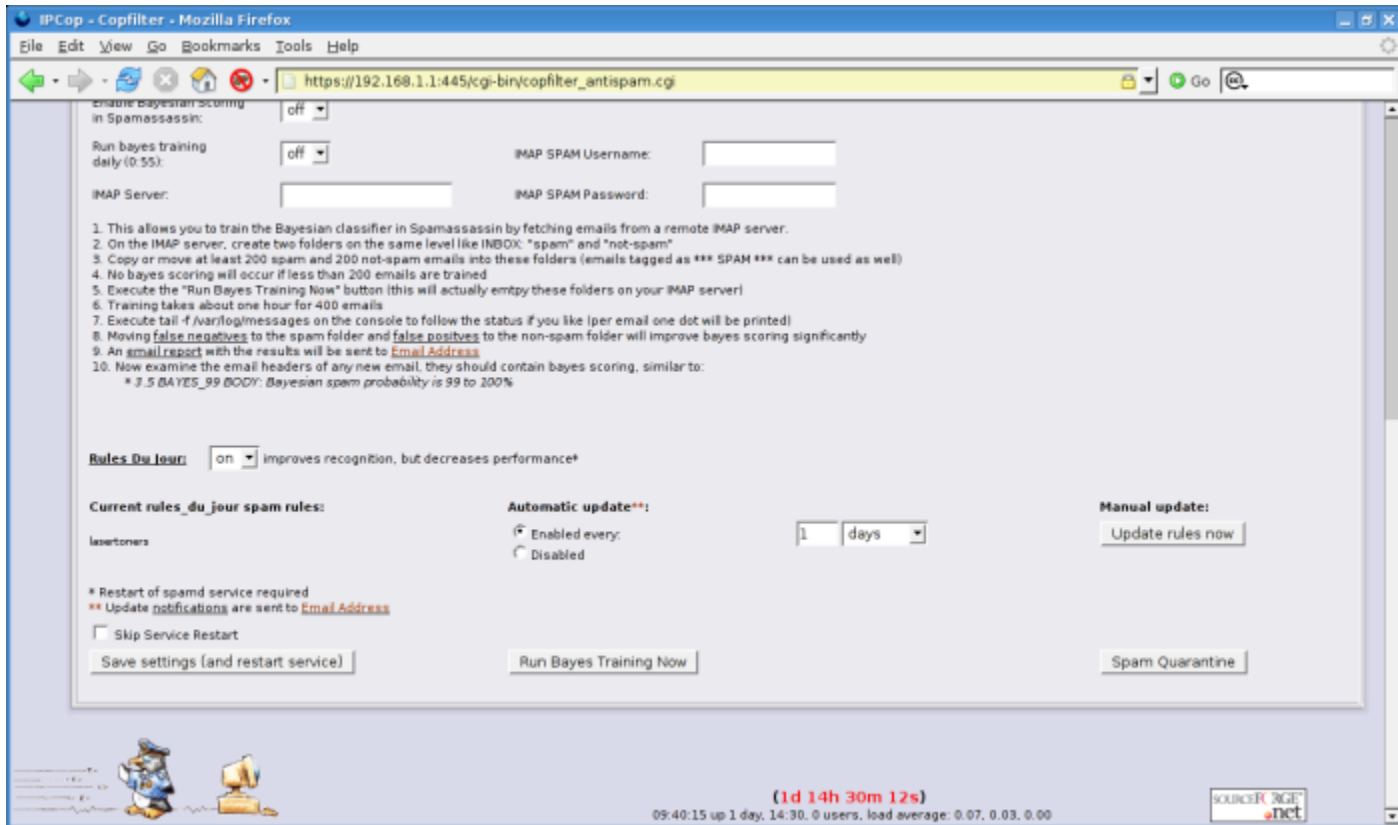
AntiSpam - SpamAssassin and Rules Du Jour

Spam Assassin will help your email server identify and filter Spam before it reaches your email client inbox. SpamAssassin uses Bayesian filtering, DNS blocklist, header and text analysis and collaborative filtering databases to keep your Spam at a minimum. Please note that the more filtering you do before delivering to the client the higher the load on the server.

- **Rules Du Jour** is a simple back script which will download new versions of Spam Assassin rules. This is very helpful in keeping your anti-spam defense in optimal shape.
- **Razor** is a distributed, collaborative spam detection and filtering network.
- **DCC** or Distributed Checksum Clearinghouse is an anti-spam content filter.
- **DNSBL** are DNS Blacklists or ban lists based upon DNS entries of known spammers or known nodes/networks that once emanated Spam.

To access these setting go to **Copfilter** >> **AntiSpam** configuration

AntiSpam Configuration



The following options are to be turned ON and all others will be left in the default OFF configuration.

- Enable Spamassassin ON
- Score required to identify email as spam 6
- Send daily spam digest ON
- Razor, DCC, DNSBL ON
- Rules Du Jour - ON
- Automatic Update Enable every 1 days
- Then click on Save settings (and restart service)

AntiVirus - ClamAV

ClamAV is an amazing FOSS project virus scanner. Within Copfilter this is used to virus scan email and web traffic for malware.

To access these settings go to Copfilter >> Antivirus

Copfilter - Antivirus Configuration

IPCop - Copfilter - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.1:445/cgi-bin/copfilter_antivirus.cgi
COPFILTER ANTIVIRUS The bad packets stop here.
SYSTEM STATUS NETWORK SERVICES FIREWALL VPNs LOGS COPFILTER
AntiVirus (ClamAV):
ClamAV: on * Treat an encrypted archives as viruses * off ClamAV Statistics Text (immediate updates) Scaph (weekly updates, starts after one week)
Current virus signatures:
ClamAV 0.88/1280
Tue Feb 7 05:11:53 2006
Feb 7 05:45 daily.cvd
Jan 6 04:30 main.cvd
Automatic update**:
Enabled every: 24 hours
Disabled
Manual update:
Update clamd now
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, MSL, MSP, MST, NWS, OCX, PCD, PIP, REG, SCR, SCT, SHB, SHS, URL, VB, VBE, VBS, WSC, WSF, WSH (manual configuration in renattach.conf)
* Restart of clamd service required
** Update notifications are sent to Email Address
Skip Service Restart
Save settings (and restart service) Virus Quarantine
09:38:50 up 1 day, 14:29, 0 users, load average: 0.00, 0.02, 0.00
SOURCEFIRE net

- ClamAV ON
- Automatic Update - Enable every 24 hours
- Then click on Save settings (and restart service)

The effect of these settings is that ClamAV is going to update its virus definitions on its own and be available for scanning your SMTP/POP3 and HTTP traffic.

Allowing traffic between Different Networks

Please note that there are certain default rules that IPCop implements on your network and be aware of the implications. See the following link for further details.

By default the configuration uses the /etc/rc.d/rc.firewall.local and changes can be made through web GUI or via SSH. Any good firewall

by default setup to deny any external connections behind its trusted networks. In IPCop speak that means that there is no ingress (incoming) access by default from the RED interface/network to any other Network. By default access from ORANGE to RED is Open so there is no need for any special configuration in this example. If you for whatever reason need access from your Orange "DMZ" to Internal GREEN you can define rules via DMZ Pinholes.

IPCop Port Forwarding - HTTP

As detailed above SMTP and POP3 rules are created by Copfilter are automatically created. As for HTTP (RED to ORANGE) it is NOT so you have to create it in Port Forwarding as below. If you would like to open other ports to external access (ex. FTP, SSH) please be aware the services should be hardened and security as much as possible (see layered approach I detail above).

The screenshot displays the IPCop web interface for port forwarding configuration. The browser window title is "IPCop - Port forwarding configuration - Mozilla Firefox". The address bar shows the URL "https://192.168.1.1:445/cgi-bin/portfw.cgi". The page header includes the IPCop logo and navigation tabs for FIREWALL, PORT FORWARDING, SYSTEM, STATUS, NETWORK, SERVICES, FIREWALL, VPNs, LOGS, and COPFILTER. The main content area is titled "Add a new rule:" and contains a form with the following fields: Protocol (TCP), Alias IP (DEFAULT IP), Destination IP (192.168.10.25), Source port (80), and Destination port (80). There is also a Remark field and an Enabled checkbox. Below the form are "Add" and "Reset" buttons. A note below the form states "This field may be blank." Below the form is a section titled "Current rules:" which contains a table with columns for Proto, Source, Destination, Remark, and Action. The table is currently empty. At the bottom of the page, there is a status bar showing "Connected (0d 8h 22m 18s)" and "11:39:22 up 8:22, 0 users, load average: 0.00, 0.00, 0.00". The browser's status bar at the bottom shows "Done" and the IP address "192.168.10.1:445".

Copfilter Test & Log

The most obvious way is via surf the web. Send and receive a test email. The Copfilter Test & Log page can help you ascertain if your configuration is proper. The tests listed are very self-explanatory in

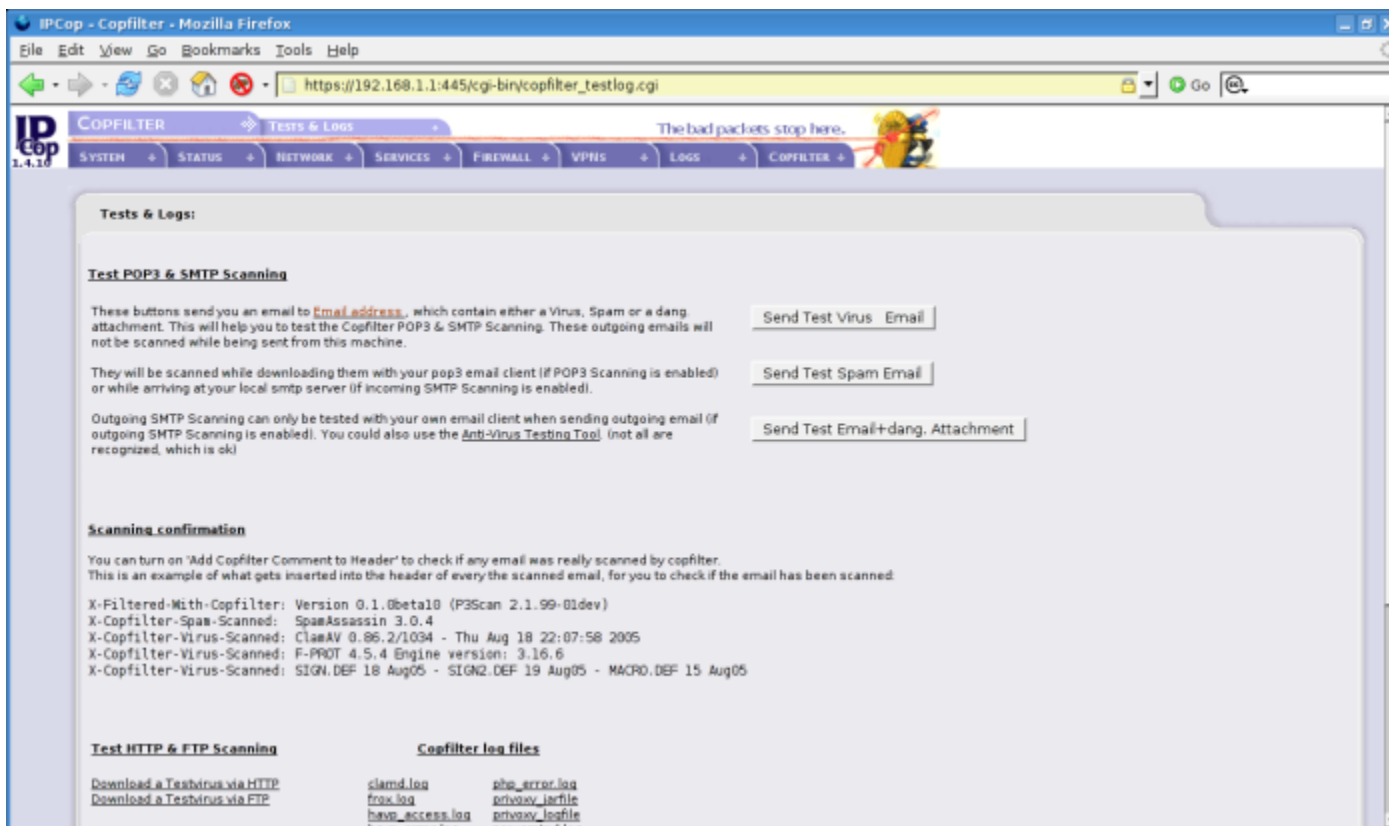
that you can examine your Email/Spam defense by clicking on the buttons in the Test POP3 & SMTP Scanning section. Below is the Test HTTP & FTP Scanning section which you can click on to verify the functionality of your HAVP HTTP virus scanner by clicking on the link to the Eicar "test" virus. This page will come up blocked with the default HAVP message to show you that your HTTP is now secured from common malware, phishing attempts, and other threats.

Sending and testing the variety of email options on the test page will allow you to verify your SMTP/POP3 configuration. If you can send and receive your emails and see the following in your email headers -- you are all set.

X-Filtered-With-Copfilter: Version 0.82 (ProxSMTP 1.3.91)

X-Copfilter-Virus-Scanned: ClamAV 0.88/1291 - Thu Feb 16 21:15:09 2006

Copfilter Test and Logs Screen



Lastly, your log files are to the right bottom of your Copfilter Test & Log page where you can see all the details of your Copfilter configuration.

Bravo! You are good to go! =) Now you can enjoy the fact you are much more secure than when you began this article!

If you like what you see, I welcome you to join our FOSS community. Free and Open Software (FOSS) does not sustain on developers alone but by the work of all sorts in technical writing, support, marketing, graphics, web developers and a multitude of other supporters like you! FOSS is built upon community, so join us and take part in reinventing computing in the positive directions from which we all collectively benefit.

In speaking with Markus I was able to ask him why he was motivated to create Copfilter and he answered, he said: "*I created Copfilter to help protect the computers of my friends and family and the greater Internet community.*" Markus I don't think there is a better way to describe the spirit of FOSS. Much thanks to Markus and the entire IPCop Team and all the other projects that made this possible!

::Check out the FOSS community Projects related to this article

IPCop Homepage --> <http://www.ipcop.org>

Copfilter Homepage --> <http://www.copfilter.org>

Copfilter Forum --> <http://copfilter.endlich-mail.de/>

Additional Related Links

http://www.ipcop.org/1.4.0/en/admin/html/services.html#services_dyn dns

<http://en.wikipedia.org/wiki/Malware>

<http://www.linuxdocs.org/sln/pop3s/>

<http://en.wikipedia.org/wiki/Pop3>

<http://en.wikipedia.org/wiki/Smtp>

<http://en.wikipedia.org/wiki/Http>

http://en.wikipedia.org/wiki/Osi_model

http://en.wikipedia.org/wiki/Port_forwarding

<http://en.wikipedia.org/wiki/Md5>

<http://www.tildeslash.com/monit>

<http://p3scan.sourceforge.net/>

<http://memberwebs.com/nielsen/software/proxsmtp>

<http://havp.sourceforge.net/>

<http://www.privoxy.org/>

<http://frox.sourceforge.net/>

<http://spamassassin.apache.org/>

<http://clamav.sourceforge.net/>

<http://www.pc-tools.net/unix/renattach>

<http://www.exit0.us/index.php?pagename=RulesDuJour>

<http://p3scan.sourceforge.net/#p3pmail>

<http://wiki.apache.org/spamassassin/DnsBlocklists>

http://wxchecksums.sourceforge.net/mainpage_en.html

<http://www.md5summer.org/>

<http://www.firefox.com/>

<http://adblock.mozdev.org/>

<http://www.us-cert.gov/current/>

[Evolutionary IT](#) is an independent provider of systems, network and security solutions. Please do feel free to email comments or suggestions. <http://www.evolutionaryit.com/> Many thanks for the help of my amazing sister [Antonina](#) in editing this article.



2006 Licensed under Creative Commons Attribution-NonCommercial_ShareAlike 2.5

Joseph Guarino -- Evolutionary IT -- www.evolutionaryit.com