The Perfect Linux Firewall Part II -- IPCop & Copfilter

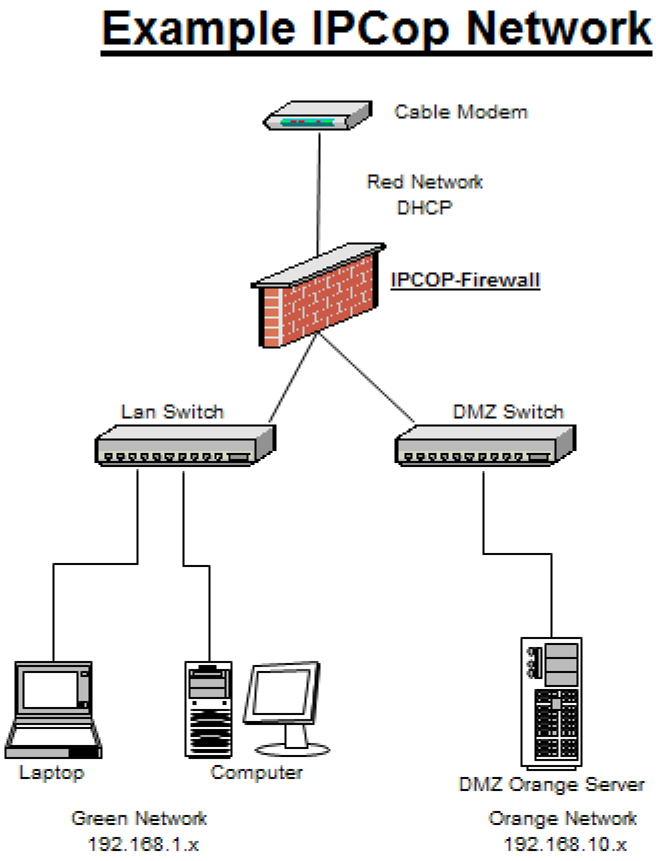
Author: Joseph Guarino - Evolutionary IT

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.



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

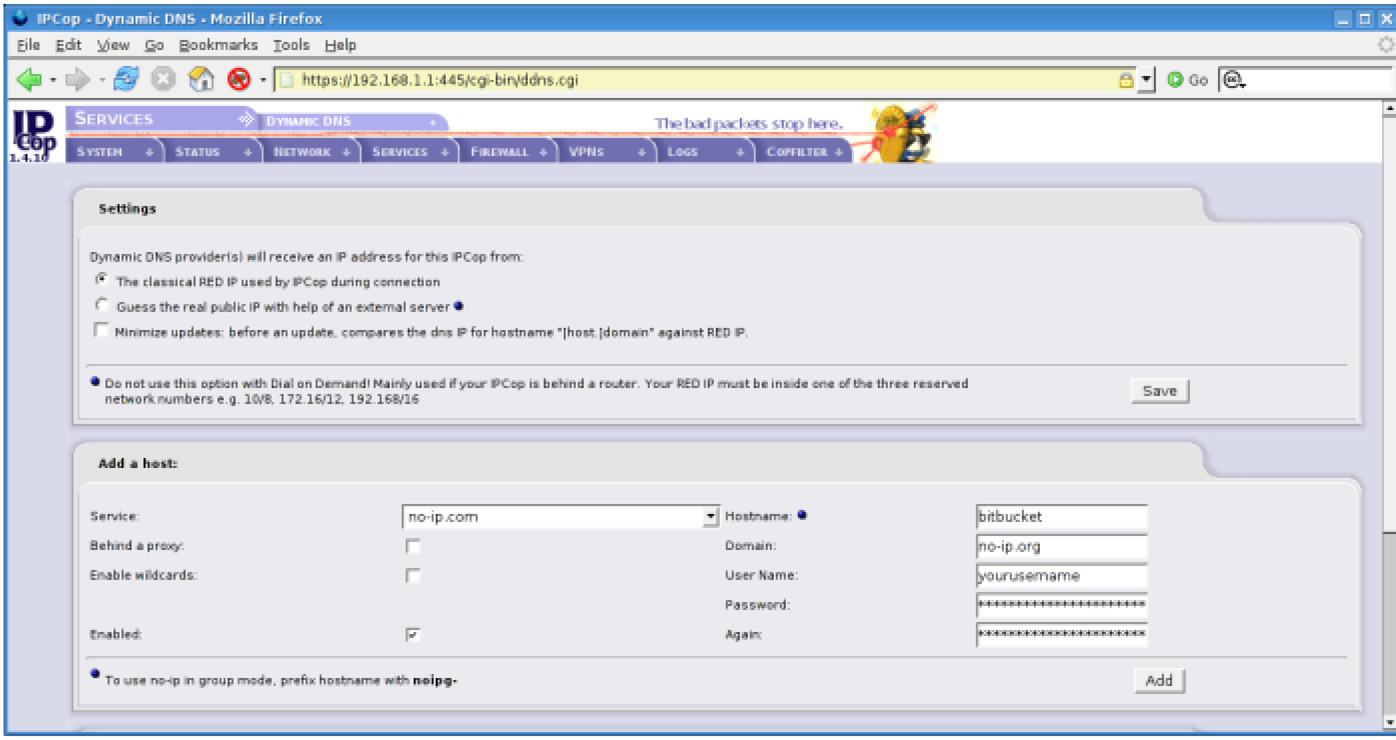
As you are using a cable modem that gives your RED IPCop network interface a dynamic DHCP address, you will need to set up Dynamic DNS services to resolve to this host via a human usable form, other than IP Address.

NOTE â€“ 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 â€œcurrent hostsâ€?.


IPCop - Dynamic DNS - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.1:445/cgi-bin/ddns.cgi
Go
IPCop 1.4.10
SERVICES
DYNAMIC DNS
The bad packets stop here.
SYSTEM
STATUS
NETWORK
SERVICES
FIREWALL
VPNS
LOGS
COPFILTER

Settings

Dynamic DNS provider(s) will receive an IP address for this IPCop from:

● The classical RED IP used by IPCop during connection

○ Guess the real public IP with help of an external server ●

□ Minimize updates: before an update, compares the dns IP for hostname "[host.]domain" against RED IP.

● Do not use this option with Dial on Demand! Mainly used if your IPCop is behind a router. Your RED IP must be inside one of the three reserved network numbers e.g. 10/8, 172.16/12, 192.168/16

Save

Add a host:

Service:	no-ip.com	Hostname: ●	bitbucket
Behind a proxy:	□	Domain:	no-ip.org
Enable wildcards:	□	User Name:	yourusername
		Password:	**********************
Enabled:	☑	Again:	**********************

● To use no-ip in group mode, prefix hostname with **noipg-**

Add

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 â€“ 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

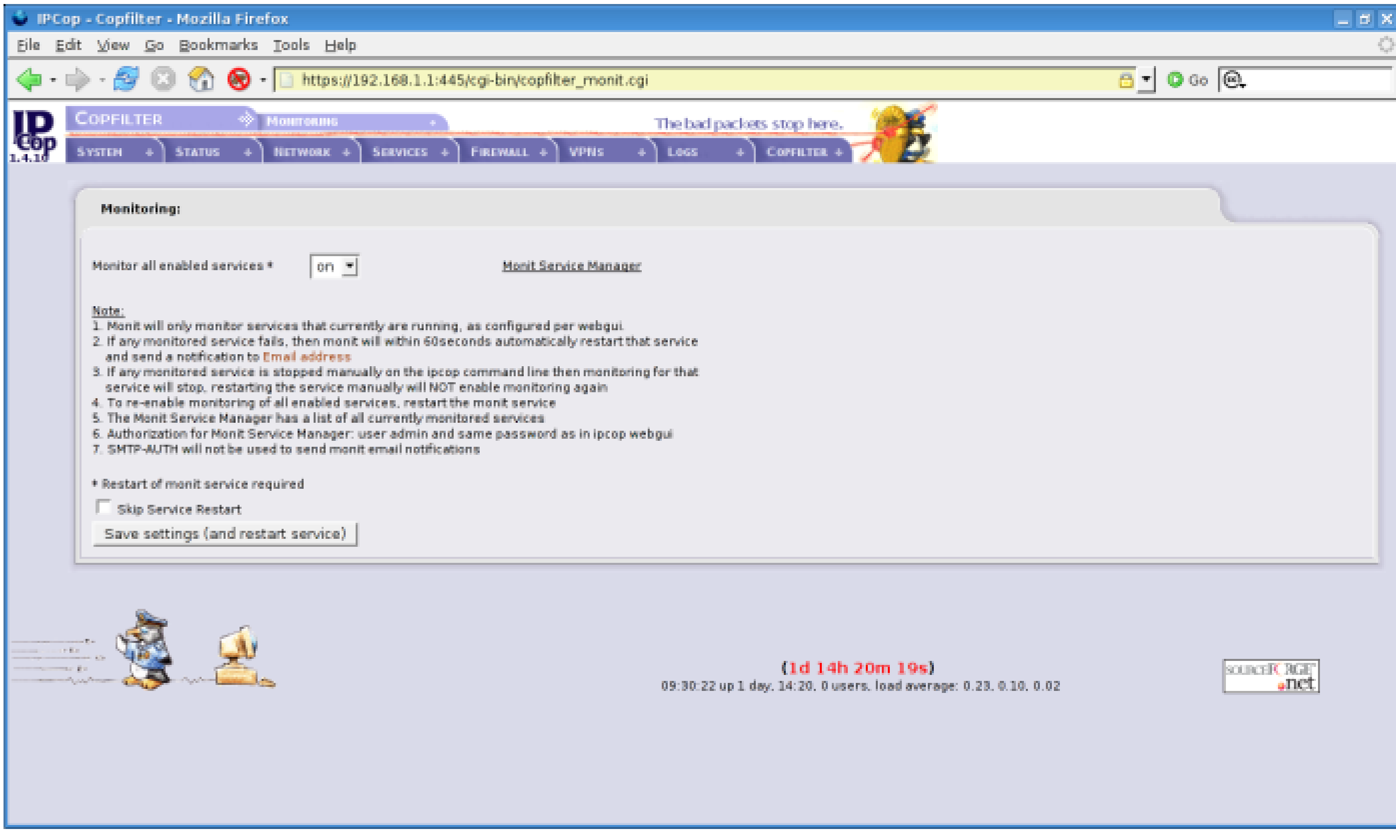
Go to Copfilter -> **Email** and configure your email address, SMTP server and then save those settings. The email address is your (root or administrator) email address and it will be used to notify you of updates and other important Copfilter messages.

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


IPCop - Copfilter - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.1:445/cgi-bin/copfilter_monit.cgi
Go
IPCop 1.4.10
Copfilter
Monitoring
The bad packets stop here.
System
Status
Network
Services
Firewall
VPNs
Logs
Copfilter
Monit Service Manager
SOURCEFORGE.net

Monitoring:

Monitor all enabled services * on

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

Save settings (and restart service)

(1d 14h 20m 19s)
09:30:22 up 1 day, 14:20, 0 users, load average: 0.23, 0.10, 0.02

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

Copfilter Configuration Options

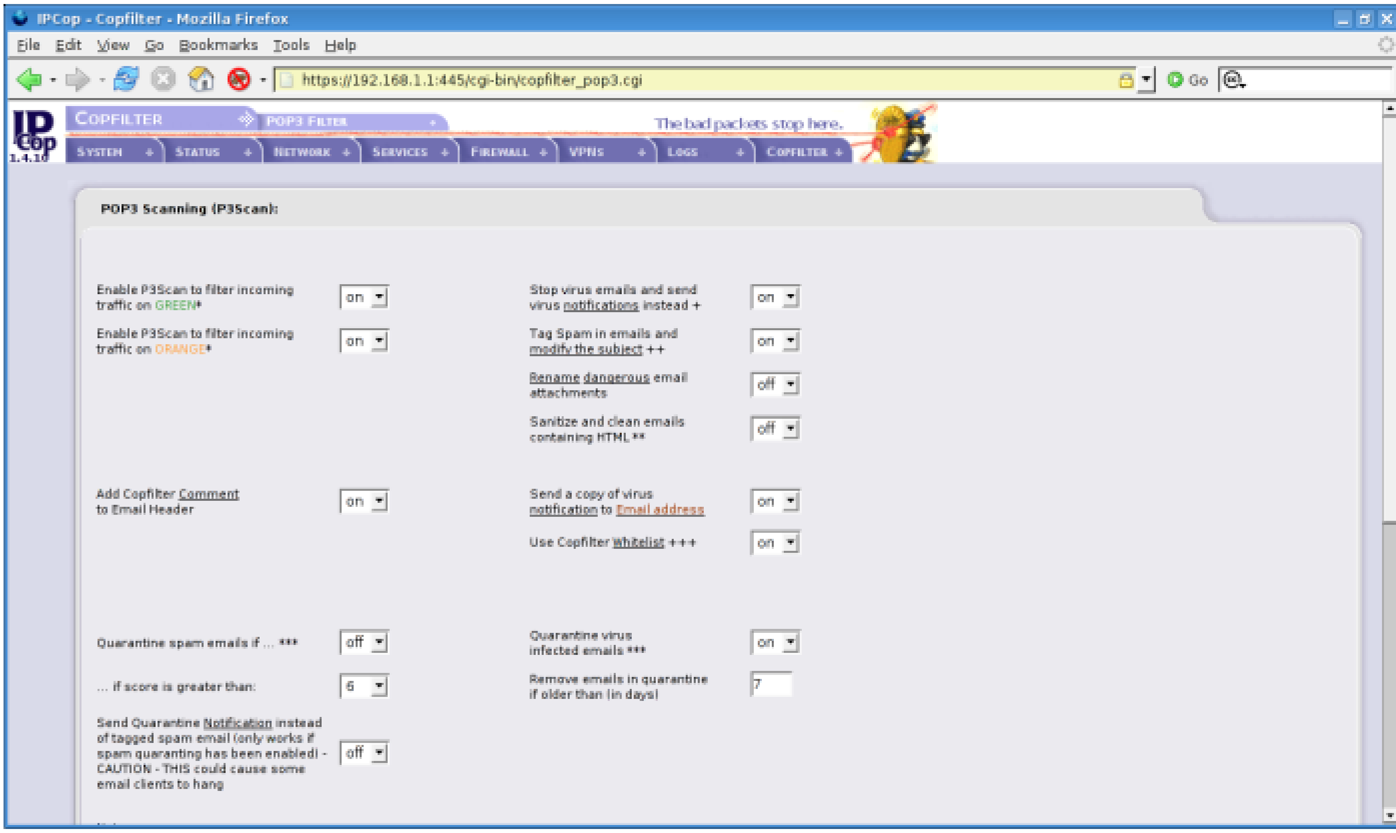
In controlling the three network services we are going to have ingress (ingoing) and egress (outgoing) control of in our IPCop/Copfilter configuration we have many granular options. Copfilter is going to be filtering our HTTP traffic, POP3, and SMTP traffic. The wonder of the Copfilter add-on is the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


IPCop - Copfilter - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.1:445/cgi-bin/copfilter_pop3.cgi
Go
IPCop 1.4.10
COPFILTER
POP3 FILTER
The bad packets stop here.
SYSTEM
STATUS
NETWORK
SERVICES
FIREWALL
VPNS
LOGS
COPFILTER

POP3 Scanning (P3Scan):

Enable P3Scan to filter incoming traffic on GREEN*	on	Stop virus emails and send virus notifications instead +	on
Enable P3Scan to filter incoming traffic on ORANGE*	on	Tag Spam in emails and modify the subject ++	on
		Rename dangerous email attachments	off
		Sanitize and clean emails containing HTML **	off
Add Copfilter Comment to Email Header	on	Send a copy of virus notification to Email address	on
		Use Copfilter Whitelist +++	on
Quarantine spam emails if ... ***	off	Quarantine virus infected emails ***	on
... if score is greater than:	6	Remove emails in quarantine if older than (in days)	7
Send Quarantine Notification instead of tagged spam email (only works if spam quaranting has been enabled) - CAUTION - THIS could cause some email clients to hang	off		

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.

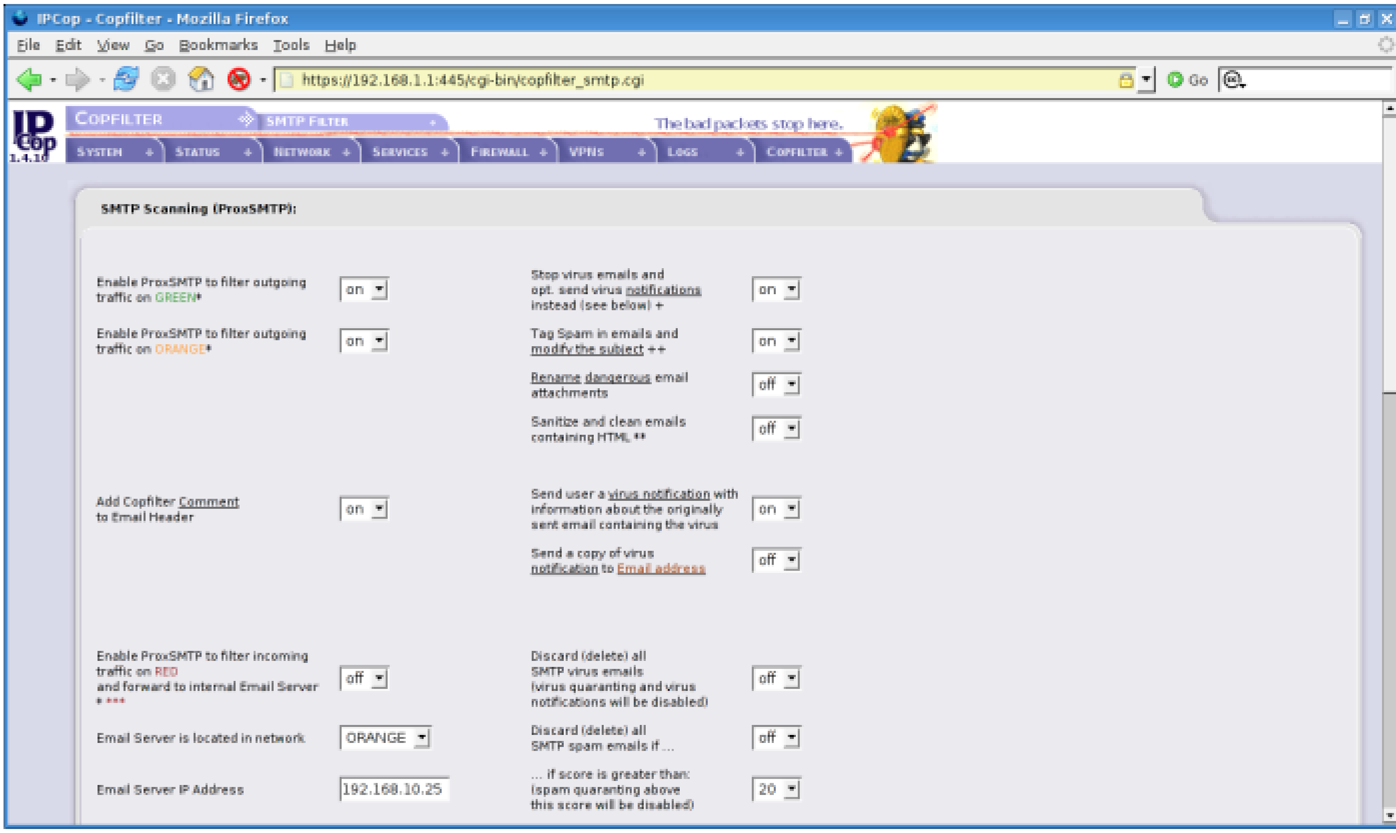
Copfilter - SMTP configuration - ProxSMTP

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


IPCop - Copfilter - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.1:445/cgi-bin/copfilter_smtp.cgi
Go
IPCop 1.4.10
COPFILTER
SMTP FILTER
The bad packets stop here.
SYSTEM
STATUS
NETWORK
SERVICES
FIREWALL
VPNS
LOGS
COPFILTER

SMTP Scanning (ProxSMTP):

Enable ProxSMTP to filter outgoing traffic on GREEN*	on	Stop virus emails and opt. send virus notifications instead (see below) +	on
Enable ProxSMTP to filter outgoing traffic on ORANGE*	on	Tag Spam in emails and modify the subject ++	on
		Rename dangerous email attachments	off
		Sanitize and clean emails containing HTML **	off
Add Copfilter Comment to Email Header	on	Send user a virus notification with information about the originally sent email containing the virus	on
		Send a copy of virus notification to Email address	off
Enable ProxSMTP to filter incoming traffic on RED and forward to internal Email Server * ***	off	Discard (delete) all SMTP virus emails (virus quaranting and virus notifications will be disabled)	off
Email Server is located in network	ORANGE	Discard (delete) all SMTP spam emails if ...	off
Email Server IP Address	192.168.10.25	... if score is greater than: (spam quaranting above this score will be disabled)	20

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

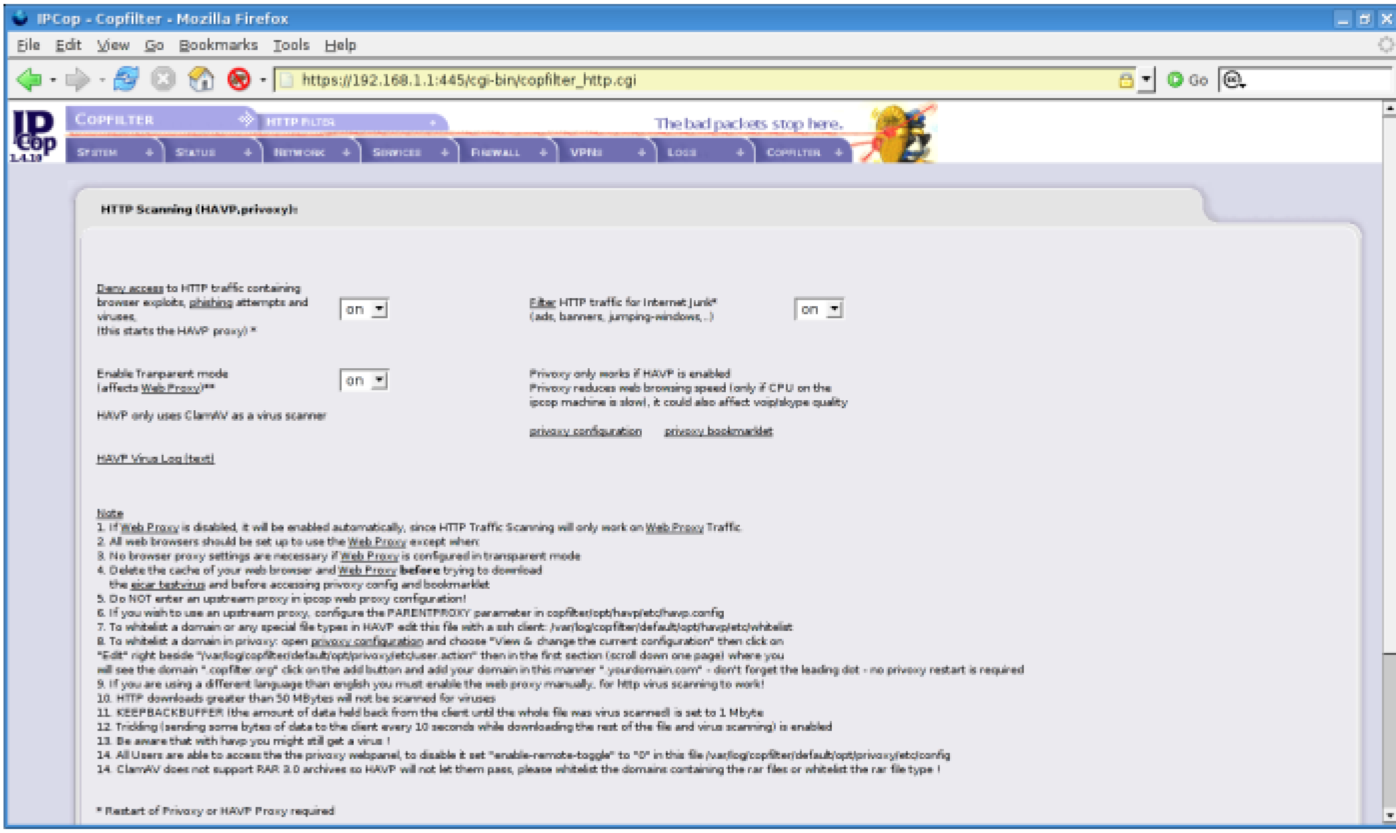
This configuration will be an proactive stance on the capturing, quarantining and deleting malware before it infect our trusted machines in the GREEN network. With quarantining ON it is recommended that an administrator be very responsive to the systems warnings about quarantine Spam, and process consistently, 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


IPCop - Copfilter - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.1:445/cgi-bin/copfilter_http.cgi
Go
IPCop 1.4.10
COPFILTER
HTTP FILTER
The bad packets stop here.
SYSTEM
STATUS
NETWORK
SERVICES
FIREWALL
VPNS
LOGS
COPFILTER

HTTP Scanning (HAVP,privoxy):

Deny access to HTTP traffic containing browser exploits, phishing attempts and viruses, (this starts the HAVP proxy) * on

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

Enable Tranparent mode (affects Web Proxy)** on

HAVP only uses ClamAV as a virus scanner

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 privoxy bookmarklet

HAVP Virus Log (text)

Note
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 when:
3. No browser proxy settings are necessary if Web Proxy is configured in transparent mode
4. Delete the cache of your web browser and Web Proxy **before** trying to download the eicar testvirus and before accessing privoxy config and bookmarklet
5. Do NOT enter an upstream proxy in ipcop web proxy configuration!
6. If you wish to use an upstream proxy, configure the PARENTPROXY parameter in copfilter/opt/havp/etc/havp.config
7. To whitelist a domain or any special file types in HAVP edit this file with a ssh client: /var/log/copfilter/default/opt/havp/etc/whitelist
8. To whitelist a domain in privoxy: open privoxy configuration and 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 - no privoxy restart is required
9. If you are using a different language than english you must enable the web proxy manually, for http virus scanning to work!
10. HTTP downloads greater than 50 MBytes will not be scanned for viruses
11. KEEPBACKBUFFER (the amount of data held back from the client until the whole file was virus scanned) is set to 1 Mbyte
12. Trickling (sending some bytes of data to the client every 10 seconds while downloading the rest of the file and virus scanning) is enabled
13. Be aware that with havp you might still get a virus !
14. All Users are able to access the the privoxy webpanel, to disable it set "enable-remote-toggle" to "0" in this file /var/log/copfilter/default/opt/privoxy/etc/config
14. ClamAV does not support RAR 3.0 archives so HAVP will not let them pass, please whitelist the domains containing the rar files or whitelist the rar file type !

* Restart of Privoxy or HAVP Proxy required

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

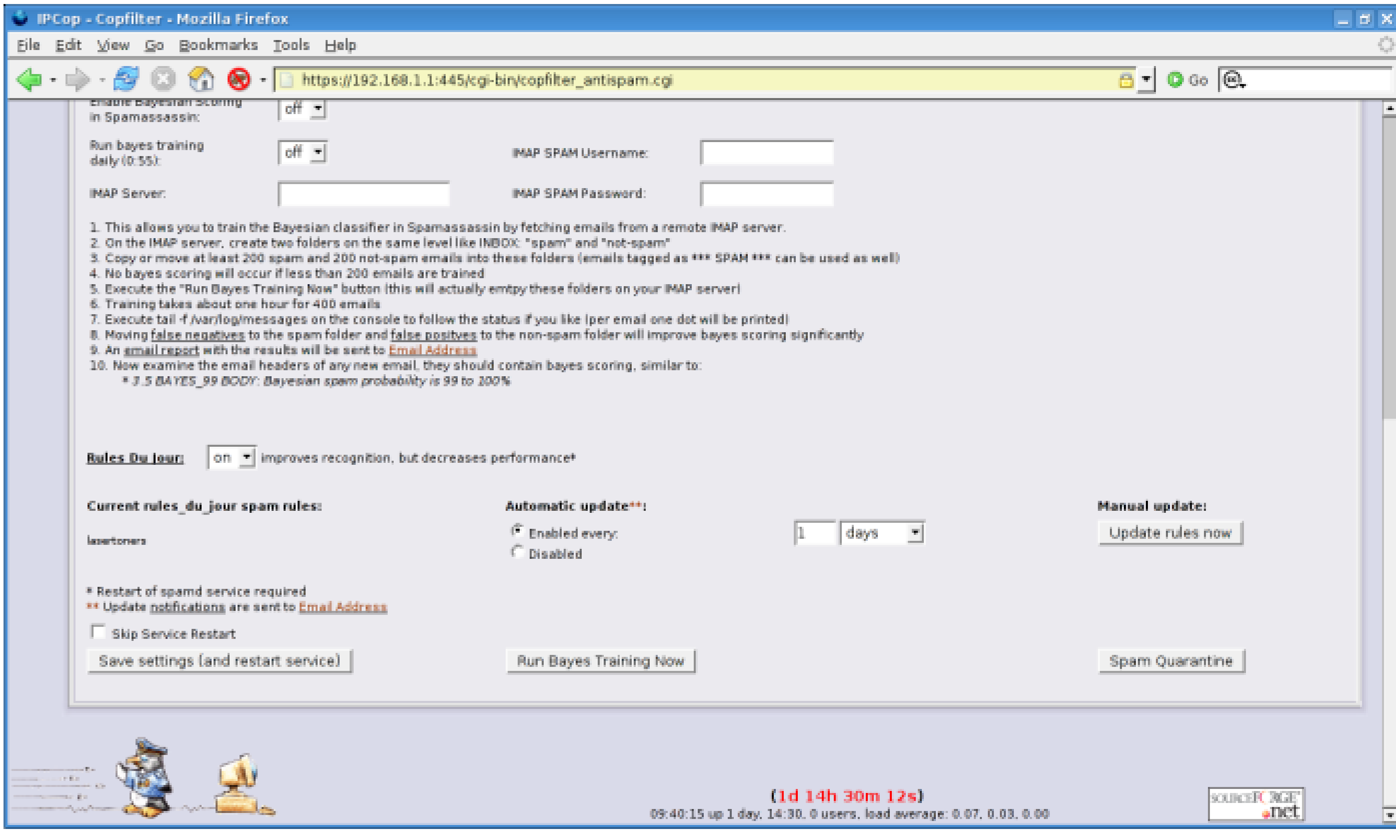
AntiSpam - SpamAssassin and Rules Du Jour

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



IPCop - Copfilter - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.1:445/cgi-bin/copfilter_antispam.cgi
Go

Enable Bayesian Scoring in Spamassassin: off

Run bayes training daily (0:55): off

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 emtpy 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 positves 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%*

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

Current rules_du_jour spam rules:

lasertoners

Automatic update:**

● Enabled every: 1 days

○ Disabled

Manual update:

* Restart of spamd service required

** Update notifications are sent to Email Address

□ Skip Service Restart

(1d 14h 30m 12s)

09:40:15 up 1 day, 14:30, 0 users, load average: 0.07, 0.03, 0.00

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

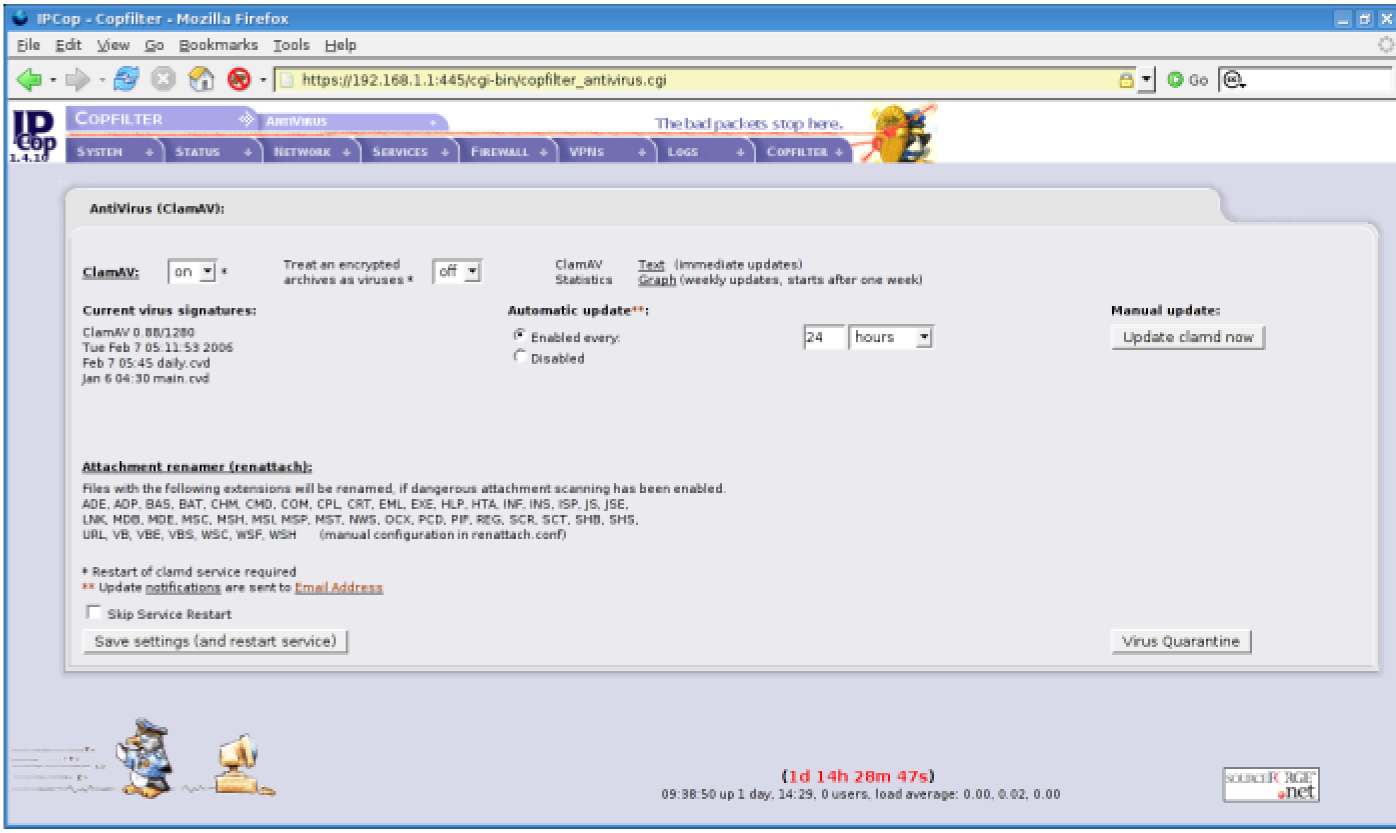
- Enable Spamassasin ON
- Score required to identify email as spam 6
- Send daily spam digest ON
- Razor, DCC, DNSBL ON
- Rules Du Jour - ON
- Automatic Update Enable every 1 days
- Then click on Save settings (and restart service)

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
Go
IPCop 1.4.10
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)
Graph (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, MSI, MSP, MST, NWS, OCX, PCD, PIF, 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

(1d 14h 28m 47s)
09:38:50 up 1 day, 14:29, 0 users, load average: 0.00, 0.02, 0.00

- 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.

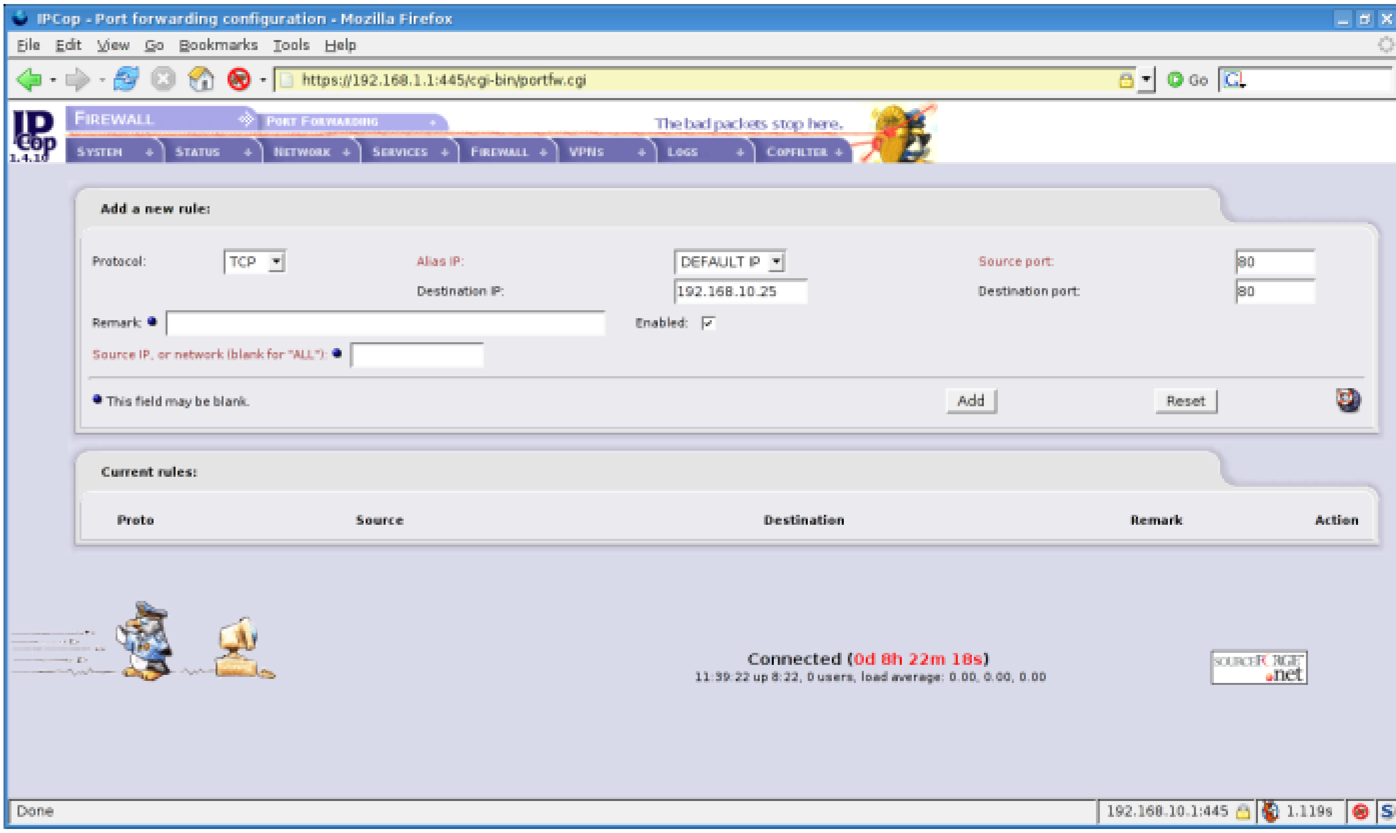
Allowing traffic between Different Networks

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).



IPCop - Port forwarding configuration - Mozilla Firefox

https://192.168.1.1:445/cgi-bin/portfw.cgi

Add a new rule:

Protocol:	TCP	Alias IP:	DEFAULT IP	Source port:	80
		Destination IP:	192.168.10.25	Destination port:	80

Remark: ●

Enabled: ☑

Source IP, or network (blank for "ALL"): ●

● This field may be blank.

Current rules:

Proto	Source	Destination	Remark	Action

Connected (0d 8h 22m 18s)
11:39:22 up 8:22, 0 users, load average: 0.00, 0.00, 0.00

Done

192.168.10.1:445

1.119s

Copfilter Test & Log

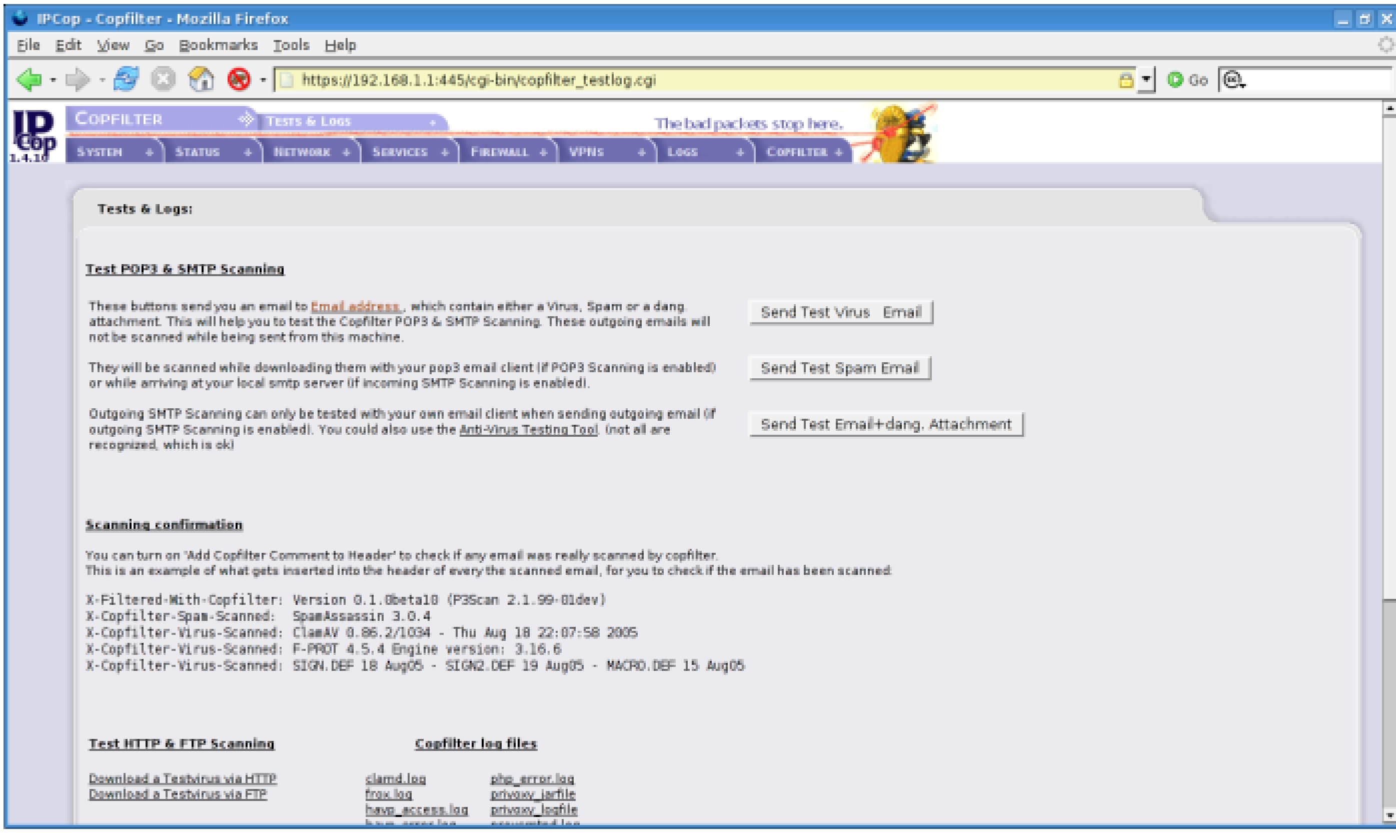
The most obvious way is via surf the web. Send and receive a test email. The Copfilter Test & Log page can help you ascertain if your configuration is proper. The tests listed are very self-explanatory in that you can examine your Email/Spam defense by clicking on the buttons in the Test POP3 & SMTP 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


IPCop - Copfilter - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.1:445/cgi-bin/copfilter_testlog.cgi
Go
IP Cop 1.4.10
COPFILTER
TESTS & LOGS
The bad packets stop here.
SYSTEM
STATUS
NETWORK
SERVICES
FIREWALL
VPNS
LOGS
COPFILTER

Tests & Logs:

Test POP3 & SMTP Scanning

These buttons send you an email to Email address , which contain either a Virus, Spam or a dang. attachment. This will help you to test the Copfilter POP3 & SMTP Scanning. These outgoing emails will not be scanned while being sent from this machine.

They will be scanned while downloading them with your pop3 email client (if POP3 Scanning is enabled) or while arriving at your local smtp server (if incoming SMTP Scanning is enabled).

Outgoing SMTP Scanning can only be tested with your own email client when sending outgoing email (if outgoing SMTP Scanning is enabled). You could also use the Anti-Virus Testing Tool. (not all are recognized, which is ok)

Scanning confirmation

You can turn on 'Add Copfilter Comment to Header' to check if any email was really scanned by copfilter.
This is an example of what gets inserted into the header of every the scanned email, for you to check if the email has been scanned:

```
X-Filtered-With-Copfilter:  Version 0.1.0beta10 (P3Scan 2.1.99-01dev)
X-Copfilter-Spam-Scanned:   SpamAssassin 3.0.4
X-Copfilter-Virus-Scanned:  ClamAV 0.86.2/1034 - Thu Aug 18 22:07:58 2005
X-Copfilter-Virus-Scanned:  F-PROT 4.5.4 Engine version: 3.16.6
X-Copfilter-Virus-Scanned:  SIGN.DEF 18 Aug05 - SIGN2.DEF 19 Aug05 - MACRO.DEF 15 Aug05
```

Test HTTP & FTP Scanning

Download a Testvirus via HTTP
Download a Testvirus via FTP

Copfilter log files

clamd.log
frox.log
havp_access.log

php_error.log
privoxy_jarfile
privoxy_logfile

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_dyndns

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.