

## Construye tu propio cortafuegos: IPCop - CopFilter

16 de Junio de 2006

Por José Manuel Gómez

<http://www.kriptopolis.org/cortafuegos>

Ya he dicho por aquí alguna vez que uno de mis defectos (que a la vez constituye probablemente una de mis virtudes) es mi afición por experimentar, y no por necesidad, sino por el propio placer de experimentar. Por pura vergüenza torera no suelo comentar los ocasionales desastres a que esa irrefrenable tendencia me lleva, aunque cualquiera puede imaginarlos. Sin embargo, esa actitud tan temeraria con lo tecnológico también produce de cuando en cuando resultados memorables (como mi abandono de Open Linux, motivado por el descubrimiento de Arch, ya comentado antes en [otra nota](#)). El caso que quiero comentar hoy es similar en su génesis, porque la verdad es que no tenía ninguna necesidad de cambiar el cortafuegos de mi máquina vieja: un satisfactorio [Smoothwall](#), que lleva meses desarrollando un excelente trabajo. Quizás precisamente por eso, porque no había ninguna necesidad, decidí lanzarme a la piscina y darle una oportunidad a [IPCop](#)...



*Actualización (domingo 18): IPCop promete dar mucho juego, así que he renovado la sección de [cortafuegos](#) para darle cabida y he creado un [foro específico](#). Muy pronto, más novedades...*

En el caso concreto de IPCop la descarga de la última versión (1.4.11, en este momento) se realiza [desde aquí](#). Se trata de una imagen ISO de 46 MB, lista para quemar un CD. Una vez realizada la descarga y la grabación, basta arrancar la máquina con el CD en su unidad. Las necesidades de hardware y el proceso de instalación son casi idénticos a los de Smoothwall, pero he puesto algunos [pantallazos aquí](#) para quien sienta curiosidad. Una vez instalado debe arrancar sin problemas, lo cual, una vez comprobado, nos permite retirar teclado, ratón y monitor del ordenador que hará de cortafuegos. A partir de ahora, conectaremos desde nuestra máquina a la dirección <https://ipcop:445>, desde la que podremos afinar al máximo el comportamiento de IPCop.



Vaya por delante que Smoothwall e IPCop tienen una concepción muy similar, algo que sin duda facilita la migración. En ambos casos se trata de descargar una imagen ISO, quemar un CD y dedicar un ordenador viejo al asunto. Y también en ambos casos la base es una distribución linux adaptada a la misión concreta de cortafuegos. Por eso, mucho de [lo que dijimos sobre Smoothwall](#) resulta también de aplicación a IPCop. De hecho, casi resultará más breve comentar aquí las **diferencias** que las similitudes:

1. Sin duda es cuestión de gustos, pero el interfaz gráfico de IPCop me resulta más moderno y agradable que el de Smoothwall. Por otro lado, todo está traducido al español (una traducción no muy elaborada, cierto, pero de gran utilidad para todos aquellos a quienes el inglés utilizado en Smoothwall pueda suponer un problema añadido). Además, los menús son desplegables en vertical, algo que quizás favorece la usabilidad frente a los menús horizontales (tipo pestaña) con varios niveles de Smoothwall.
2. La pantalla inicial de IPCop muestra la dirección IP del equipo, algo que en Smoothwall requiere un módulo adicional.
3. No se requieren actualizaciones. No sé si esto es bueno o malo, pero desde luego resulta cómodo (recordemos que tras una instalación limpia de Smoothwall necesitábamos instalar nada menos que 8 parches, con un incómodo reboot después de cada uno).
4. IPCop también permite cambiar más fácilmente las contraseñas de acceso, y también permite el acceso mediante SSH (aunque no dispone para ello de la cómoda terminal en Java que trae Smoothwall).
5. IPCop permite hacer una copia de seguridad de su configuración a un disquete (que en la traducción se llama "diskette flojo" ;).
6. La pestaña de "Estado del Sistema" muestra también los módulos cargados. En "Estado de Red" se muestran además las tablas de ruteo y de entradas ARP. El control sobre el servidor DHCP es mucho más completo. El soporte para DNS dinámico (que permite ejecutar servidores desde IPs dinámicas) es muy similar al de Smoothwall.
7. Una importante novedad respecto a Smoothwall (en que requiere un módulo específico) es que IPCop incorpora "de serie" Control de Calidad de Servicio (QoS), donde se puede configurar el caudal de tráfico asignado a diferentes puertos y servicios.
8. Excelentes gráficos de control que incluyen uso de CPU, memoria, swap y disco. Otro tanto cabe decir del Tráfico de Red para cada interfaz y las conexiones de IPTables. Pero la mayor novedad frente a Smoothwall son los gráficos de uso del proxy, que permite tenerlo todo delante con un solo vistazo.
9. En el apartado de cortafuegos todo similar: reglas de reenvío de puertos y accesos externos. También existe soporte para redes privadas virtuales (VPN).
10. Y, "last but not least", sin duda lo que más me ha gustado es la facilidad para actualizar las reglas del detector de intrusiones Snort. Si [te registras](#) en la web de Snort (2) dispondrás de una cuenta con la opción de obtener un código Oink. Cuando lo tengas lo pegas en la casilla correspondiente de IPCop y podrás descargar reglas actualizadas que se instalan automáticamente. ¡Genial!

### **Más información:**

- [Galería de imágenes](#) de la instalación.

## Copfilter (I): Introducción

Por José Manuel Gómez

Mi idilio con [IPCop](#) continúa por buen camino, así que me he decidido a hacerle un buen regalo que nos ayude a consolidar nuestra felicidad. Y he encontrado el regalo ideal para IPCop. Se llama [Copfilter](#), y para IPCop viene a ser como llevarte a tu chica a El Corte Inglés y decirle que compre todo lo que quiera, sabiendo que además no te van a cargar ni un céntimo en tu VISA. En pocas palabras, Copfilter es una solución dirigida a escanear y filtrar todo tu tráfico de Internet en busca de virus y spam. Nada más y menos. Para ello, combina un montón de herramientas de código abierto, ajustadas para funcionar en buena armonía. Una vez instalado y configurado, todo el tráfico (es decir, correo -POP y SMTP- FTP y Web) es filtrado de modo transparente, impidiendo el acceso a cualquier contenido contaminado. ¿Hay quién dé más?... Con un poco más de detalle, esto es lo que hará por ti Copfilter:



### Correo electrónico

- Escaneado contra virus y spam de todos los mensajes entrantes (POP3)
- Escaneado contra virus y spam de todos los mensajes entrantes y salientes (SMTP)
- Saneado de los mensajes HTML eliminando etiquetas peligrosas.
- Escaneado de adjuntos al correo, renombrando los peligrosos.
- Añade una nota a las cabeceras de cada mensaje indicando que el correo ha sido escaneado.
- El correo se descarta o se pone en cuarentena si tiene virus o parece spam

### Tráfico Web

- Escaneado del tráfico HTTP, continuo, transparente, sin retrasos y sin bloquear descargas.
- Bloqueo de la mayoría de sitios de phishing o explotando debilidades en navegadores.
- Escaneado del tráfico FTP con cierto retraso (el fichero es descargado y escaneado en segundo plano).
- Elimina anuncios, banners, ventanas emergentes, etc.

### Red

- Todos los servicios funcionan de forma transparente, sin tener que reconfigurar ningún cliente.
- Puede utilizarse cualquier cliente de correo (Outlook, Thunderbird, Evolution...) en cualquier sistema operativo (Windows, Linux, MacOS...).
- Soporte de alias de IP para entradas MX en servidores de correo diferentes a la IP asignada.

### Monitorización

- Información detallada de cada servicio instalado.
- Monitorización de los servicios. Si alguno cayese, es reiniciado automáticamente, con notificación por e-mail.

- Los servicios pueden arrancarse o detenerse por separado desde un interfaz gráfico.

### **Administración y Manejo**

- Manejo de toda la configuración antivirus y antispam mediante interfaz gráfico, pudiendo configurarse diferentes niveles de alarma y notificación.
- Tests antivirus (en correo, web y ftp) y antispam desde el propio interfaz para verificar el sistema.

### **Estadísticas**

- Antivirus (texto): total de virus, por fecha, hora, mes, año, listado de los 200 últimos.
- Antivirus (gráfico): muestra semanal de los tipos de virus detectados.
- Antispam (texto): total de e-mails con spam por mes, día, año, listado de los últimos 200. Totales y medias por día/mes, tamaño, tiempo de escaneado, puntuación media.
- Web/FTP (texto): estadísticas mostrando los virus y las IP de origen.

### **Actualizaciones**

- Automática de actualizaciones de firmas antivirus.
- Automática de actualizaciones de juegos de reglas antispam.
- La última versión disponible de Copfilter se muestra automáticamente en el interfaz.

### **Notificaciones por correo al usuario**

- En vez de un correo infectado con virus, el usuario recibe una notificación de que se le enviado un virus, incluyendo detalles como remitente, tema y cabeceras del mensaje original. Opcionalmente, con copia al administrador.
- Resumen diario de todas las direcciones que enviaron spam en 24 horas.

### **Notificaciones por correo al administrador**

- Actualizaciones de firmas de antivirus y reglas antispam.
- Resultados del entrenamiento bayesiano.
- Servicios que fallaron y si funcionó el reinicio automático.

### **Características del software utilizado**

- Sólo Open Source (excepto para el escaner antivirus f-prot, opcional)
- Capacidades antispam mejoradas: filtro bayesiano, reglas SURBL, DNSBL, Razor, DCC y SARE.
- Capaz de utilizar dos antivirus: ClamAV (para correo, FTP y web) y/o F-Prot (para correo y ftp).
- Todos los proxies corren con usuario no root.
- Ficheros de registro de todos los servicios en el mismo directorio y accesibles desde interfaz.

### **En concreto, para realizar todas estas funciones CopFilter incluye:**

- P3Scan: proxy transparente para pop3.
- ProxSMTP: proxy transparente para smtp.

- HAVP (HTTP Antivirus Proxy): proxy transparente para WEB.
- frox: proxy transparente para ftp.
- Privoxy: proxy http con capacidades de filtrado para proteger privacidad, manejar cookies, controlar accesos, eliminar anuncios, pop-ups, etc.
- Clam AntiVirus: antivirus GPL.
- F-Prot Antivirus: antivirus gratuito para usuarios domésticos (no incluido, pero explicaremos cómo agregarlo). También soporta la versión corporativa para servidores de correo.
- SpamAssassin: filtro de correo para detectar spam.
- Vipul's Razor: red distribuida antispam utilizada por SpamAssassin.
- DCC: sistema distribuido para detectar correo basura.
- renattach: filtro que identifica y renombra adjuntos potencialmente peligrosos.
- RulesDuJour: para la descarga automática de nuevas versiones de reglas de SpamAssassin.
- monit: utilidad que permite manejar, monitorizar y reiniciar servicios.
- P3PMail: elimina del correo etiquetas HTML peligrosas.

Buf, la enumeración ha sido tan larga que dejaremos para otra entrega la instalación y puesta en marcha del invento. Así que id buscando un equipo viejo, instalando [IPCop](#) y preparándoos para la próxima entrega. Ningún seguidor de Kriptópolis tiene excusa para no disfrutar de este invento. Para que vayáis afilando los dientes, os dejo con un [pantallazo](#) de mi propio Copfilter en marcha.

## Copfilter (II): Instalación

*Por José Manuel Gómez*

Con [IPCop](#) funcionando, la instalación de [Copfilter](#) no representa ningún problema, puesto que todas las utilidades necesarias están empaquetadas en un solo fichero de 16 MB, que habremos de descargar [aquí y ahora](#).

El siguiente paso es subir el fichero a la máquina donde instalamos IPCop. Podemos utilizar para ello cualquiera de las [herramientas](#) (tanto para Windows como para Linux) que ya empleamos en la instalación de Smoothwall. Mostraré a continuación el proceso en linux, desde consola y con algunas utilidades diferentes para variar...

Empezamos pues subiendo el fichero de Copfilter al firewall:

```
scp -P 222 copfilter-0.82.1.tgz root@192.168.0.1:/root
```

Se te solicitará la contraseña de root para IPCop:  
root password: xxxxxxxxx

El siguiente paso es conectar con el firewall (ojo: previamente hay que activar el acceso mediante SSH en IPCop).

```
ssh 192.168.0.1 -p 222 -l root
```

Se te solicitará (otra vez) la contraseña de root para IPCop:  
root password: xxxxxxxxx

Procedemos por fin a instalar Copfilter:

```
tar xzvf copfilter-0.82.1.tgz
cd copfilter-0.82.1
./install
```

Contestamos "Y" y tras una serie de mensajes se nos dice que la instalación ha sido correcta.

Con esto sería suficiente para tener a nuestra disposición todas las utilidades de Copfilter, incluyendo ClamAV como antivirus. Pero ya puestos, ¿por qué no aprovechar para añadir otro antivirus más, de la categoría de F-Prot?

Procedemos por tanto a instalar F-Prot (gratuito sólo para uso personal), aunque este paso -insisto- es opcional.

Vamos a la [web de F-Prot](#), cumplimos las formalidades del registro y nos descargamos el fichero denominado fp-linux-ws.tar.gz (4 MB).

Seguimos el mismo proceso de antes para subirlo al cortafuegos e instalarlo:

```
scp -P 222 fp-linux-ws.tar.gz root@192.168.0.1:/root/copfilter
root password:
ssh 192.168.0.1 -p 222 -l root
root password:
cd copfilter
./setup_util -f fp-linux-ws.tar.gz
```

```
Contestar Y
Instalación correcta
exit
```

El proceso está completo. Debes disponer de una nueva opción de menú (denominada "Copfilter") donde dispones de todas las opciones. Si seleccionas la opción "Status" verás que no todas están activas, por lo que has de proceder a configurarlas.

La configuración de Copfilter depende -obviamente- de tus propias necesidades y es difícil dar directrices generales. Mejor que eso será que consultes tus dudas y dificultades en [nuestro foro](#). En mi caso fui solventando las dificultades según iban surgiendo, y mis pasos son difíciles de explicar y sistematizar aquí. Eso sí: lo que más me costó fue poner en marcha monit (la utilidad de monitorización), hasta que descubrí que no arranca mientras no configures perfectamente tu sección de e-mail.

Un recurso recomendable para aclarar posibles dudas sobre esta instalación es el documento ["The Perfect Linux Firewall Part II- IPCop & Copfilter"](#).

Ánimo, buena suerte y [comparte tu experiencia](#).