Construye tu propio cortafuegos: SmoothWall

16 de Junio de 2006
Por José Manuel Gómez
http://www.kriptopolis.org/cortafuegos

Quién sabe. A lo mejor los Reyes Magos han sido generosos contigo y por fin puedes permitirte retirar ese viejo PC que tan buenos -o tan malos- ratos te dio. Sea como sea, es probable que dispongas de un PC viejo y no sepas qué hacer con él.

Donarlo al Tercer Mundo no es mala opción, aunque no siempre sabe uno cómo hacerlo ni a dónde dirigirse. En cualquier caso, si has decidido quedarte con tu viejo PC y buscarle alguna utilidad, te propongo seguir este artículo para convertirlo en un excelente cortafuegos...

El objetivo es disponer de un cortafuegos mediante hardware ideal para un usuario doméstico. Se trata de que la instalación sea sencilla y funcione perfectamente desde el principio, con la configuración por defecto. Si necesitas adaptarlo más a tus necesidades, lo podrás hacer después de una forma sencilla, mediante tu navegador habitual. El cortafuegos será completo, en el sentido de que además del firewall propiamente dicho, dispondrás de un proxy (Squid), un IDS o detector de intrusiones (Snort), herramientas de administración, servidor DHCP, gestión de IPs dinámicas, conexión a servidores horarios, posibilidad de VPN (red privada virtual), etc, etc.

Si añado además que todo esto lo lograrás mediante un equipo Linux, es posible que te asustes y pienses que este proyecto excede tus posibilidades. Pero lo cierto es que no, porque no necesitas saber ni una palabra de Linux para que todo funcione al 100%.

Características del proyecto

Las posibles topologías y configuraciones de una red son casi infinitas, así que te anticipo que aquí **me limitaré al caso más sencillo**: tu PC viejo (cortafuegos) se conecta a Internet y tu PC nuevo se conecta al cortafuegos mediante un cable.

Todas las variantes (inalámbricas, etc.) son posibles, pero tendrás que indagar por tu cuenta en la abundante documentación disponible.

AVISO MUY IMPORTANTE: Necesitas dedicar tu viejo equipo al completo a este proyecto. Tu disco duro será formateado y todo lo que contenga desaparecerá. No se te ocurra seguir los pasos que se indican en un equipo donde quieras conservar el sistema operativo o la información que contenga, ni si se trata del único equipo de que dispones. ¿Queda claro? Entonces sigue leyendo...

Materiales necesarios

Vas a necesitar:

1. **Tu viejo PC:** El mínimo recomendable es un Pentium (cualquier tipo de Pentium o AMD 586 o similares de Cyris o IBM, mejor con un procesador de 150 Mhz para arriba). En cuanto a RAM, cuanta más mejor, pero 32-64 MB sería el mínimo. ¿Disco duro? Ideal, más de 2GB (si es menor, menos sitio para ficheros de registro). Una unidad de CD-ROM facilita la instalación. No hace falta ratón. Teclado, tarjeta gráfica y monitor sólo hacen falta para la

instalación, y pueden ser cualesquiera. Módem, sólo si te conectas a tu proveedor mediante uno. Tarjeta de red en el resto de casos.

2. **Una segunda tarjeta de red:** Para instalarla tu viejo PC debe disponer de una ranura PCI libre. Tu nueva tarjeta ha de ser compatible con Linux, pero eso no representa ningún problema, porque sirven prácticamente todas. En mi caso compré la más barata que encontré (10 euros), Made in China y de chip, en principio, desconocido (la caja sólo exhibía un nada tranquilizador "compatible con Windows XP"). Sin embargo el cortafuegos (es decir, Linux) la reconoció de inmediato como portadora de un chip Realtek totalmente compatible. En mi caso el único problema que encontré fue con las interrupciones; mi viejo equipo estaba cargado de tarjetas y tuve que retirar algunas y reubicar otras (ensayo y error), hasta que todo funcionó.
3. **Un cable de red cruzado:** Ojo aquí, porque no te va a servir el que viene con tu nueva tarjeta. Cuando se trata de unir equipo (viejo) con equipo (nuevo) necesitas que el cable sea cruzado, es decir, que los pines que "emiten" en uno vayan conectados a los que "reciben" del otro, y viceversa. En los envases de este tipo de cables suele figurar la palabra *Crossover*. Para que te hagas una idea, a mí el cablecito en cuestión me costó 12 euros, pero sin él no hay nada que hacer. Comprobarás que has acertado cuando, tras encender y unir ambos equipos con este cable, veas que se iluminan las lucecitas de ambas tarjetas de red. Sin este requisito previo es inútil intentar nada.
4. **SmoothWall:** Es el imprescindible software que dará vida al invento. Se trata en realidad de una distribución Linux adaptada a su funcionamiento como cortafuegos. Gratis y de código libre, con licencia GPL. Debes descargar SmoothWall Express 2.0 y quemar un CD con esa imagen ISO. Baja rápido y son sólo unos 40 megas.

Con todo esto, ya estás preparado para empezar.

Instalación

Si tu viejo PC arranca desde el CD (revisa la BIOS a ver si puedes ajustarlo) la instalación es coser y cantar. Si no es el caso habrás de generar disquetes de arranque y el asunto se complica un poco, aunque está todo perfectamente explicado en la documentación, tres pdfs muy recomendables en caso de problemas, pero en inglés. Por cierto, toda la instalación está en inglés, aunque prácticamente sólo necesitas elegir las opciones por defecto y aceptar todo. Aunque no distingas el inglés del chino, con las explicaciones y "cutre-fotos" que incluyo en el artículo tampoco deberías tener mayor problema.

Metes el CD y arrancas el equipo viejo. Al poco tiempo pantalla de presentación y a pulsar *Enter*. Se te va a avisar, por activa y por pasiva, de que el disco duro va a ser formateado y que puedes despedirte de cualquier dato que tuvieras en él. Si a estas alturas no tienes claro esto, mejor no sigas y olvides todo el asunto. Insisto: tras la instalación el viejo PC será un cortafuegos, y no un PC al uso.

El equipo se formatea, se crea el sistema de archivo linux, se instala lilo como gestor de arranque y se instalan todos los ficheros necesarios. Se pasa a buscar (Probe) la tarjeta de red del cortafuegos que usarás para conectar a ella tu equipo (el bueno, el que contiene tu sistema operativo y tus ficheros más queridos). Una vez detectada la primera tarjeta se te presenta la opción de aceptarla (OK) o seguir buscando (Skip) para elegir la segunda tarjeta disponible (en principio esto es indiferente y puedes aceptar la primera que se detecte).

Una vez elegida la tarjeta de red se te presenta la opción de configurar su IP y su máscara de red. Esto puede sonar complicado, pero resulta tan sencillo como aceptar las opciones por defecto y pulsar OK.

Finalizada la operación el CD se expulsa y el sistema te pide ser rearrancado.

Tras el rearranque, viene la fase de configuración.

Configuración

A continuación se te pregunta si quieres restaurar una configuración previa desde un disquete (No), el teclado a usar (es), y el nombre de host (también nos vale el propuesto, *smoothwall*). Si te conectas por un proxy aquí deben ir los datos (si no, en blanco y OK). Deshabilita RDSI (ISDN, en sajón) y también ADSL en mi caso (conexión a ONO por módem cable). Puede que aquí tengas que configurar la conexión que tú utilizas.

Lo más peculiar viene ahora, al elegir la configuración de Red. SmoothWall tiene un concepto un tanto "semafórico" de los colores de los interfaces de red. Así *GREEN* es el interfaz que configuraste en la etapa anterior, al que enchufarás tu equipo real. *RED* es el interfaz (la tarjeta) donde insertarás el cable por el que tu proveedor te conecta a Internet. *YELLOW* no te importa mucho ahora; corresponde a la llamada *Zona Desmilitarizada (DMZ)*, donde se ubican los servidores (web, mail) que han de tener acceso desde la Red.

En nuestro caso, la configuración que nos interesa es *GREEN* + *RED*, así que hay que pasar a *Card Assignments* para detectar (Probe) tu segunda tarjeta, la que conectarás a Internet.

Ahora, a configurarla. *Address Setting* -> *Red* -> *OK*. En mi caso, en esta pantalla elegí DHCP, porque mi equipo recibe una IP dinámica por esa vía. Si la tuya es fija, selecciona la opción correspondiente (*Static*). El resto, queda tal cual.

Toca configurar el servidor DHCP (no el anterior, que era un cliente del de tu proveedor, sino el que dará una IP al equipo o equipos que enchufes al cortafuegos). Muchas casillas, pero basta seleccionar *Enabled* y dejar igual el resto. Observa que tu equipo (el real), o equipos, obtendrán direcciones entre 192.168.0.100 y 192.168.0.200 con esta configuración.

Se te van a pedir ahora tres nombres de login y tres contraseñas. Anótalas. *Admin* es el más importante, porque es el par login/password que te permitirá afinar la configuración a través de tu navegador web (sección siguiente). *Root* te permite acceder al cortafuegos vía consola de comandos Linux (requeriría volver a conectar monitor y teclado al cortafuegos, pero tranquilo: no lo vas a necesitar para nada). Por último, *Setup* te permite reconfigurar el cortafuegos desde consola (tampoco lo necesitarás prácticamente nunca; siempre puedes optar por reinstalar).

Se acabó lo que se daba. El sistema pide ser arrancado de nuevo. De hecho, puedes pulsar OK y desconectar teclado y monitor de tu viejo PC, reconvertido ya a cortafuegos. Salvo labores de chequeo, reinstalación o similares, no necesitarás conectarle teclado y monitor nunca más. Eso sí: asegúrate antes de que tu BIOS te permite arrancar sin teclado conectado, porque si no el sistema se puede quedar detenido y el cortafuegos no llegar a funcionar.

¿Has conectado el cable que une los dos PCs? Un extremo al equipo que vas a utilizar y el otro al interfaz que definiste como GREEN de tu nuevo cortafuegos. Al interfaz RED de éste conecta el cable de tu proveedor de Internet. Si dudas, puedes probar de nuevo cambiando los cables.

Puesta en marcha

Tu ordenador "bueno" tiene conectado en su tarjeta de red el cable de red que viene de tu flamante cortafuegos. El cortafuegos (tu caduco PC) recibe el cable del proveedor y por su segunda tarjeta conecta con el equipo bueno. Sólo el ordenador bueno necesita monitor y teclado. Enciende ambos equipos.

Lo más probable es que el equipo bueno arranque antes que el cortafuegos, por lo que es fácil que te aparezca la red como desconectada y no puedas visitar Internet hasta que el cortafuegos acabe de arrancar (se debe a que aún no dispones de dirección IP, que ahora te tiene que dar tu cortafuegos).

Pero, ¿cómo saber cuándo ha arrancado el cortafuegos, si ya no tiene monitor?. Fácil: por un lado, oirás un pitido compuesto de tres tonos; por otro, tu equipo "bueno" dispondrá de conectividad en cuanto el servidor DHCP del cortafuegos le dé una IP.

Obviamente esto debe suceder con independencia del sistema operativo de tu equipo "bueno" (en él puedes usar Windows, Linux o lo que quieras). Si no ocurre y sigues sin conexión a Internet, o bien el arranque del cortafuegos no se ha completado (necesitarás volver al principio, conectarle monitor y teclado e investigar qué ocurre) o bien la conexión entre ambos equipos no va según lo esperado (si las luces de ambas tarjetas de red -la del equipo nuevo y la del cortafuegos- funcionan prueba a intercambiar las conexiones en el cortafuegos. Si las luces de la tarjeta de red del equipo nuevo no encienden, probablemente falla el cable).

Si todo funciona según lo esperado y puedes conectarte a Internet sin problemas, acude a un servicio web de escaneo de puertos y comprueba que todos tus puertos (excepto el 8, 80 y 113 con la configuración por defecto), aparecen como *Blocked*, es decir, invisibles.

Si es así, enhorabuena: has completado el proyecto con éxito, pero aún puedes afinar más tu configuración como te explico en la siguiente sección.

Ajuste fino

Puede que no estés conforme con la configuración por defecto, que prefieras abrir o cerrar determinados puertos, poner en marcha tu proxy o tu detector de intrusiones, revisar tus ficheros de registro, ajustar la hora, instalar parches, etc, etc.

Si la instalación fue correcta, puedes hacer eso y más mediante tu navegador habitual, sin más que teclear la siguiente dirección:

https://192.168.0.1:441

Se trata de una conexión segura con tu cortafuegos. Acepta el certificado y teclea la contraseña que elegiste para *admin* durante la instalación. Te aparecerá la pantalla de bienvenida de tu nuevo cortafuegos.

Si observas bien, verás que se te indica que existen actualizaciones sin instalar. Para instalarlas pulsa la pestaña *Maintenance*. En el momento de escribir este artículo existen 8 actualizaciones disponibles. Pulsa sobre *info* en la primera de ellas y descárgala a tu PC. Puedes instalarla desde el mismo interfaz (Examinar -> Upload). Tras instalar la primera has de volver a arrancar el cortafuegos (no, no toques el botón de encendido del viejo PC; mejor usa la pestaña *Shutdown* y luego *Reboot*). Repite el proceso (incluido el rearranque) con las actualizaciones siguientes (siempre en orden consecutivo, de la 2 a la 8). Al finalizar, tu cortafuegos estará totalmente al día.

Conclusión

Si has llegado hasta aquí con éxito, es más que probable que a partir de este punto no necesites mi ayuda. Las posibilidades de configuración de tu nuevo cortafuegos son muchas y no me toca a mí tratarlas todas. Dispones de las herramientas y los documentos necesarios. Además, SmoothWall dispone de un animado foro de usuarios donde puedes aprender mucho más de lo que yo podría enseñarte.

Por si todo eso fuera poco, mi idea es que los lectores de Kriptópolis que se animen a afrontar el proyecto se decidan a comentar aquí mismo sus experiencias, de modo que los más avanzados puedan ayudar a los rezagados.

Estáis todos invitados a participar. La posibilidad de contar en nuestra casa con un cortafuegos como SmoothWall, con sus innumerables posibilidades, y la satisfación de aprovechar para nuestra defensa un equipo que creíamos inservible, merecen sin duda el esfuerzo.

ClamAV en Smoothwall

Por José Manuel Gómez

Ahora que ya estás disfrutando de tu flamante cortafuegos, es probable que quieras perfeccionarlo aún más. ¿Qué tal añadirle un antivirus?

En nuestra línea habitual, optaremos por un antivirus de código libre: ClamAV.

Comienza por descargarte su última versión (0.88.2 en el momento de escribir este artículo).

Una vez obtenido el fichero, deberás transferirlo a tu cortafuegos. No, no es necesario que vuelvas a acoplar monitor y teclado a la máquina vieja que ejecuta SmoothWall. Puedes transferirlo *al directorio temporal (/tmp)* del cortafuegos desde tu PC, utilizando un cliente SSH o un cliente FTP que soporte SSH2 (por ejemplo, gFTP en Linux ó WinSCP en Windows, ambos de código libre) y conectando al servidor 192.168.0.1, en el puerto 222...

Para ello es necesario que previamente, a través del interfaz gráfico de control de tu cortafuegos, hayas habilitado el soporte SSH (*Services -> Remote Access*), con la opción *Allow admin access only from valid referral URLs* también activada, como te indico en la figura.

Ahora véte a *Tools -> shell* y suministra *root* como login y tu contraseña correspondiente.

A continuación necesitarás teclear -exactamente- los siguientes comandos:

```
cd /tmp
tar xzvf clamav-0.88.2.tgz -C /
./install-clamav.sh
```

Si estás conectado a Internet (deberías) verás cómo se descargan las últimas definiciones de virus automáticamente. Si quieres confirmar que todo está al día teclea *freshclam*.

Tu antivirus está instalado. Para confirmar que funciona teclea lo siguiente:

```
/usr/local/sbin/clamd
```

Tras unos segundos debería devolverte automáticamente a la línea de comandos. Si es así, todo está perfecto. Si no, revisa el fichero de registro */var/log/clamav/clamd.log* para localizar el error.

Ahora ya podrías escanear ficheros y directorios del cortafuegos y localizar y eliminar los posibles ficheros infectados, pero ése no es nuestro objetivo, sino facilitar el manejo del antivirus e integrarlo en un contexto de protección más amplio, algo que veremos en el siguiente capítulo.

- Manual de ClamAV (pdf)
- Más información sobre la integración de ClamAV en SmoothWall

DansGuardian AV en Smoothwall

Por José Manuel Gómez

Como dije en mi último artículo, no tiene ningún sentido ponernos a escanear el propio cortafuegos desde la línea de comandos. Los virus para Linux son francamente escasos, y las posibilidades de que nuestra reciente instalación tenga alguno son absolutamente remotas. Además, quien más quien menos está acostumbrado a entornos gráficos, y no resulta nada atractivo realizar escaneos desde la línea de comandos. Tampoco es nuestra propia máquina cortafuegos lo que nos interesa escanear, sino lo que nos llega desde Internet. En fin; muchos motivos nos inclinan a instalar nuestro tercer componente: DansGuardian, un sistema de filtrado de contenido que nos proveerá de un objetivo adecuado sobre el que disparar nuestro antivirus...

Ten en cuenta que, de todos los extras de que estamos dotando a nuestro cortafuegos, éste puede ser el más voraz en recursos, por lo que si no tienes 128 Mb de RAM es probable que no funcione como es debido. Desde luego DansGuardian no es imprescindible para que funcione tu cortafuegos, pero sí para integrar el antivirus en el conjunto y que todo funcione coordinadamente. También es imprescindible que hayas aplicado las 8 actualizaciones de que hablábamos en nuestro primer artículo, y que tengas instalado ClamAV tal y como explicábamos en el segundo.

Si te has decidido, el primer paso es obtener DansGuardian [1], en una versión un tanto especial, porque va parcheada con un plugin para antivirus [2]. Descarga el fichero y llévalo al *directorio temporal (/tmp)* de tu cortafuegos de la forma que indicábamos en el segundo artículo de esta serie. A continuación, procede a abrir tu sesión de acceso remoto desde el interfaz del cortafuegos, como allí también explicábamos.

Como casi siempre, para realizar la instalación no nos queda más remedio que teclear algunos comandos:

```
cd /tmp
tar xzvf dansguardian-2.8.0.6-antivirus-6.4.3.tgz -C /
./install-dgav.sh
```

Este script intentará por ti todo lo que haga falta, incluyendo la activación y configuración de tu proxy web, necesario para que todo funcione correctamente. No obstante, **y sólo si obtienes dos mensajes de fallo (FAILED) en este script**, es posible que hayas de activar tu web proxy "a mano". Para ello, desde el interfaz de tu cortafuegos (no la sesión de shell) véte a la pestaña *Services* y luego a *Web Proxy*. Marca *Transparent* y *Enabled* (si no logras salir a Internet, es posible que tengas que poner 192.168.0.1 y puerto 8080 como proxy en la configuración de conexión de tu navegador).

Para arrancar DansGuardian teclea:

```
 cd /var/smoothwall/mods/dansguardianav
./startdg
```

Si obtienes algún error, para concretarlo puedes teclear:

```
dansguardian -N
```

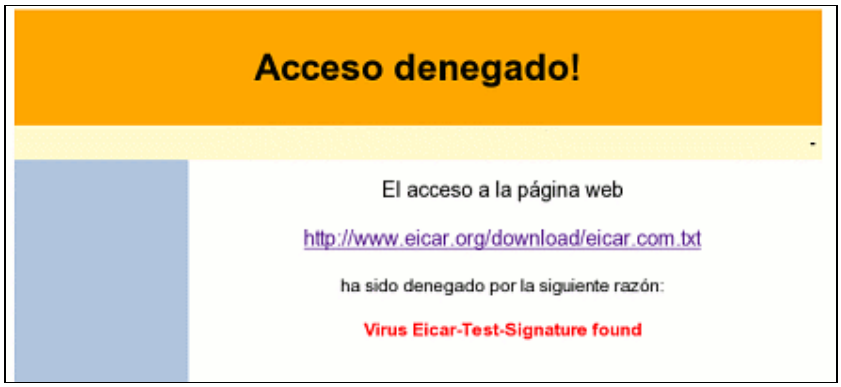
Para tratar de resolverlo, pregunta aquí o consulta el foro de Smoothwall relativo a DansGuardian.

Excelente. Tenemos un cortafuegos que funciona y un antivirus que aún no hemos utilizado, junto a un filtro de contenido al que tampoco encontramos sentido. ¿A dónde nos estás llevando, José Manuel?

Tranquilo, que en la próxima entrega ya me encargaré de que todas las piezas encajen.

1. DansGuardian
2. DansGuardian Antivirus Plugin

Un interfaz de usuario para Smoothwall



Por José Manuel Gómez

Tras instalar el cortafuegos básico, añadirle un antivirus y un filtro de contenidos, nos queda un último paso: instalar un interfaz, es decir, un panel de control desde el que poder coordinar todo el funcionamiento del conjunto y adaptarlo a nuestras necesidades. A ello dedicaremos el presente capítulo.

Os anticipo que esta entrega será la última de esta primera fase. Quiero decir con esto que nuestro cortafuegos nos puede dar sin duda mucho juego durante los meses venideros (en los que iremos ampliando paulatinamente sus posibilidades), pero antes creo necesario disponer de cierta masa crítica de lectores de Kriptópolis dispuestos a implementarlo. Este cuarto capítulo cierra, por tanto, la fase de creación de un cortafuegos-antivirus plenamente operativo, y parece conveniente esperar ahora a que al menos varias decenas de lectores puedan comprobar su efectividad y comenzar un fructífero intercambio de ideas en torno al mismo. A tal fin, y para evitar dispersiones, procedo a crear un nuevo foro específico sobre este cortafuegos y a cerrar los comentarios en los propios artículos que componen el cursillo...

Pasamos por tanto, sin más dilación, al desarrollo de este capítulo final de la fase de implementación básica. A tal fin, hemos de suponer completados los pasos previos -y en el mismo orden- indicados en los tres artículos anteriores.

Como en anteriores entregas vamos a necesitar descargar un nuevo fichero, transportarlo al *directorio temporal (/tmp)* del cortafuegos (ver capítulo segundo) y proceder a su instalación mediante los siguientes comandos:

```
cd /tmp
tar xzvf dgguiv3.04.tgz -C /
./install-dggui.sh
```

Lamento decepcionar a los amantes de las complicaciones, pero no se necesita nada más. Si vas a la página web de tu cortafuegos verás que hay una importante novedad: la aparición de la nueva pestaña *filtering*, que da paso a otras opciones que te permitirán afinar al máximo todo el conjunto:

- En concreto, desde *Status* puedes arrancar, parar y reiniciar tu filtro de contenidos. También arrancar y parar tu antivirus, y actualizar su fichero de definiciones de virus.
- Desde *Dansguardian Content Filter* accedes a 8 nuevas pestañas. Por ejemplo, en la pestaña *Misc* puedes cambiar el idioma de la página que saltará cuando intentes acceder a un contenido bloqueado o infectado por un

virus, además de marcar la opción que permitirá que tu filtro arranque automáticamente cada vez que inicies el cortafuegos (imprescindible).

- En *Groups* vas a poder gestionar qué tipo de ficheros, extensiones, dominios, URLs, etc. quieres bloquear. Se trata de una pestaña que vas a tener que visitar con muchísima frecuencia, porque tu filtro de contenidos parte de la configuración que se necesitaría en una escuela primaria (no es broma; así se dice en la web de DansGuardian). La buena noticia es que las posibilidades de configuración son tan completas que puedes hacer a tu filtro tan restrictivo o permisivo como tú quieras. Un usuario doméstico se inclinará quizás más hacia la permisividad, mientras que una pequeña oficina quizás quiera restringir la descarga de mp3 o avi, por poner un par de ejemplos.
- La pestaña *Antivirus* te permite indicar las opciones de escaneo de ficheros y demás, incluyendo incluso la posibilidad de que tu cortafuegos te envíe un correo cada vez que detecta un virus.

Si algo no va bien, es muy posible que se solucione tras arrancar de nuevo el cortafuegos (*Services -> Shutdown -> Reboot*). En todo caso hay una prueba infalible de que todo ha ido perfecto: tratar de acceder a una página infectada con un virus y comprobar si el sistema efectivamente te bloquea el acceso. Para ello, puedes servirte de los tests Eicar (accesible desde la pestaña *Antivirus -> Click Here to Test Virus Notification*. Como una imagen vale más que mil palabras, te muestro aquí lo que deberías obtener. ¡¡Guauuu!! ¿No llamarías a esto navegación segura?

Una vez más, insisto en que no pretendo que esta guía cubra todas las posibles opciones de configuración, lo que la volvería compleja e interminable. Para eso están los foros de SmoothWall, los documentos y el nuevo foro creado en Kriptópolis, y en el que te invito desde ahora mismo a participar.

Por último me gustaría completar los cuatro capítulos de esta guía con una serie de pantallazos del cortafuegos en funcionamiento, que sin duda animarán a los más indecisos. También preveo dar al conjunto una forma más apropiada que facilite su accesibilidad desde Kriptópolis.

Gracias por haberme seguido hasta aquí y no os perdáis la oportunidad de disfrutar de la protección de primera categoría que todo buen lector de Kriptópolis merece.

Smoothwall: Configuraciones de red

Dicen que una imagen vale más que mil palabras, así que someto a vuestra atención algunos esquemas de posibles configuraciones de red con Smoothwall, que quizás podrían aclarar más de una duda:

1. Configuración básica 1: RED-GREEN, un switch y tres ordenadores.
2. Configuración básica 2: Añade a la anterior un servidor en la zona desmilitarizada (ORANGE).
3. Configuración básica 3: Añade a la anterior un acceso inalámbrico (BLUE).
4. Configuración básica 4: RED-GREEN con router y switch.
5. Configuración básica 5: RED-GREEN con tres switches.
6. Configuración compleja: Prepárate para desplazarte por la pantalla ;)
7. RED-GREEN-ORANGE (I): módem y dos hubs.
8. RED-GREEN-ORANGE-BLUE: módem, dos hubs y wireless.
9. RED-GREEN-ORANGE (II): módem, un hub y wireless en DMZ.
10. RED-GREEN-ORANGE (III): módem, dos hubs y wireless en GREEN.
11. RED-GREN: módem y un hub.

Las posibles dudas y comentarios, por favor enviadlas a nuestro foro Smoothwall. Gracias.

[Autor de los diagramas: awphuch2000]

Filtro de correo SMTP (antispam y antivirus) para nuestro cortafuegos

Por José Manuel Gómez

Este complemento es sin duda uno de los más demandados por los lectores de Kriptópolis. Y es que, si nuestro excelente cortafuegos analiza además el correo que nos llega en busca de virus y correo basura, contaremos con una ayuda inestimable para nuestra protección en la Red. Y lo mejor de todo es lo sencillo que resulta incorporar este fabuloso complemento.

Eso sí: debes tener claro desde el principio que sólo el correo que te llegue vía tu propio servidor SMTP será escaneado en el cortafuegos, pero no el procedente de las cuentas de correo (POP y similares) albergadas en servidores externos. Indudablemente esto limita la utilidad de este filtro a quienes tienen un puerto 25 a la escucha (si bien en un futuro cercano se espera contar también con soporte para POP)...

Si instalaste Smoothwall (con todas sus actualizaciones), el antivirus, el filtro y el panel, tan sólo necesitas descargar este nuevo fichero.

El proceso de instalación es idéntico al que vimos en la segunda entrega de esta serie: movemos el fichero a /tmp (como entonces indicábamos) y tecleamos exactamente lo siguiente:

```
cd /tmp
tar xzvf mfilterv015.tgz -C /
```

Ahora vamos a la pestaña Filtering -> SMTP Email Filtering del interfaz de manejo del cortafuegos, donde configuraremos nuestros propios filtros. Podemos dejar casi todos los valores por defecto, excepto el correspondiente a la dirección IP de tu servidor de correo y *Domains Allowed to Relay*, donde deberemos escribir el dominio de nuestra máquina (en máquinas aisladas suele ser *localdomain*, o el que tú le hayas dado).

En esa misma ventana que no te pase desapercibido el enlace que dice *Dspam GUI Link*, ya que desde él podrás acceder a la ventana que te permite configurar, con todo lujo de detalles, tu nuevo y sofisticado filtro antispam.

Por último, no olvides arrancar el filtro de correo desde *Filtering -> Status*, así como activar la casilla que permite habilitarlo en cada arranque.

Si tenéis comentarios, por favor enviadlos a nuestro foro sobre este cortafuegos.

Más información:

- Foro sobre este mod en Smoothwall
- Dspam (la casa madre de tu nuevo filtro antispam)
- Nota sobre DSPAM, en Kriptópolis