

## Configuraciones de cortafuegos con Guarddog

# ¡Cuidado con el Perro!

El programa KDE Guarddog promete una configuración fácil del cortafuegos de Linux con tan solo unos cuantos clics. Guarddog ayuda a los usuarios inexpertos a proteger sus máquinas, e incluso redes completas, contra los atacantes.

POR HOLGER JUNGE



Las herramientas IPChains (Linux 2.2) e IPTables (Linux 2.4) configuran el cortafuegos de Linux, pero estas herramientas de línea de comandos pueden ser algo crípticas para los recién llegados a Linux. Simon Edwards desarrolló Guarddog [1] para simplificar la tarea de configurar el cortafuegos. Guarddog es una utilidad basada en GUI para manejar los cortafuegos. La utilidad Guarddog viene con licencia GPL y funciona tanto en KDE 2 como KDE 3.

Los usuarios se pueden descargar la versión estable 2.2.0 desde [2]. Además de los fuentes, el sitio tiene también disponible los binarios ya listos para ser ejecutados para Mandrake, Red Hat y Debian. Si desea probar las últimas características, pruebe la versión 2.3.2 desde [2]. Pero antes de hacerlo, compruebe los pros y los contras en el cuadro "Para los Valientes".

Guarddog está diseñado para usuarios domésticos o de redes privadas. Aunque distribuciones como Red Hat, Mandrake y Suse tienen herramientas simples basadas en GUI para los cortafuegos, carecen de la posibilidad de manejar sistemas distribuidos. Los usuarios más exigentes que requieran una configuración más detallada, probablemente preferirán usar Guarddog.

### Agujeros de Seguridad

Los usuarios inexpertos tienen que ser muy cuidadosos cuando configuren un

cortafuegos con Guarddog. La facilidad que supone escoger una opción y hacer clic en ella de la GUI a menudo lleva a los usuarios a abrir más puertos de los necesarios. Por otro lado, es bastante fácil "reforzar" una máquina hasta tal punto que algunos servicios dejen de funcionar.

También hay que tener en cuenta que Guarddog es una aplicación KDE y no debería ejecutarse en un servidor en el sentido tradicional de la palabra. Si tiene un servidor dedicado en su LAN, lo propio es crear una configuración con

### Para los Valientes

La versión de desarrollo actual de Guarddog es la 2.3.2. Hay varias reticencias para usar esta versión en entornos productivos. Por un lado, el usuario valiente puede encontrar algunas características nuevas. La versión 2.3.2 soporta áreas de puertos para los protocolos definidos por el usuario. Los desarrolladores han modificado también la versión para soportar Linux 2.6 y han añadido algunos protocolos nuevos a la lista, como RSync, Distcc, GKrellm, Bittorrent, PGP Key Server, Jabber sobre SSL y el protocolo Microsoft Media Server.

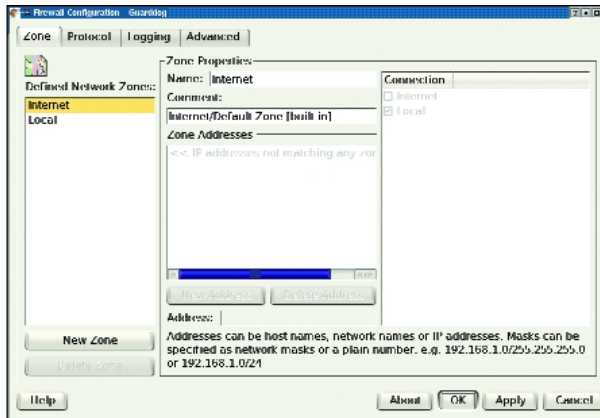


Figura 1: El GUI de Guarddog después de ser ejecutado con dos zonas de red preconfiguradas: *Internet* y *Local*.

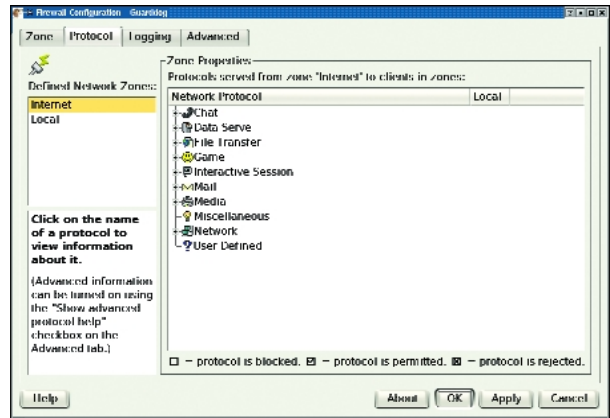


Figura 2: La solapa *Protocol* permite especificar el protocolo permitido o denegado por el cortafuegos. No hay que preocuparse por los números de puerto.

Guarddog en un ordenador distinto y luego copiar el script resultante al servidor.

Como Guarddog está basado en IPChains o en IPTables, los usuarios deben asegurarse que los módulos necesarios del kernel estén disponibles en el servidor. La mayoría de las distribuciones se hacen cargo de esto automáticamente. Si su distribución no lo hace, necesitará recompilar el kernel para que incluya IPTables o IPChains.

Guarddog usa comandos filtros orientados al protocolo. Los usuarios no necesitan especificar los números de puertos, lo que ayuda a evitar errores de configuración.

Asimismo Guarddog soporta grupos de máquinas o zonas y permite a los usuarios la opción de establecer zonas desmilitarizadas (DMZ).

## La GUI

Se debe ejecutar Guarddog con los privilegios de root para permitir al programa aplicar las reglas del cortafuegos. La Figura 1 muestra Guarddog justo después de haber sido ejecutado. Desafortunadamente, la GUI de Guarddog no es muy intuitiva. La GUI de Guarddog tiene cuatro solapas. La primera de estas solapas, la solapa *Zones*, permite a los usuarios agrupar las máquinas en zonas.

*Zone Properties* acepta direcciones IP o rangos de direcciones para la zona. Hay dos zonas preconfiguradas llamadas *Internet* y *Local* que el usuario no puede borrar. La zona *Internet* automáticamente incluye cualquier dirección IP

que no esté incluida en cualquier otra zona. *Local* incluye las direcciones de la tarjeta de red local. Una máquina individual estará bien con tan solo estas dos zonas.

Se puede usar la solapa *Protocol* (Figura 2) para permitir o denegar protocolos específicos. La estructura en árbol del lado derecho de la ventana organiza los protocolos por categorías. Normalmente el servicio DNS es el primero que se necesita habilitar. La entrada DNS está ubicada en la categoría *Network*. Haciendo clic en la caja de verificación de *DNS - Domain Name Server* se coloca una marca de verificación que indica que el servicio está permitido.

(Asegúrese que se aplican los cambios pulsando *Apply*). Si se pulsa de nuevo la caja de verificación la marca se transforma en una X para indicar que el cortafuegos denegará de forma explícita las conexiones que usen este protocolo. Una caja de verificación vacía indica que el cortafuegos ignorará cualquier petición al puerto.

Los protocolos HTTP, FTP (en la categoría *File Transfer*) y los protocolos de correo SMTP y POP3 son otros protocolos que se usan habitualmente.

## Registro de Protocolos

La solapa *Logging* (véase la Figura 3) proporciona opciones detalladas para el

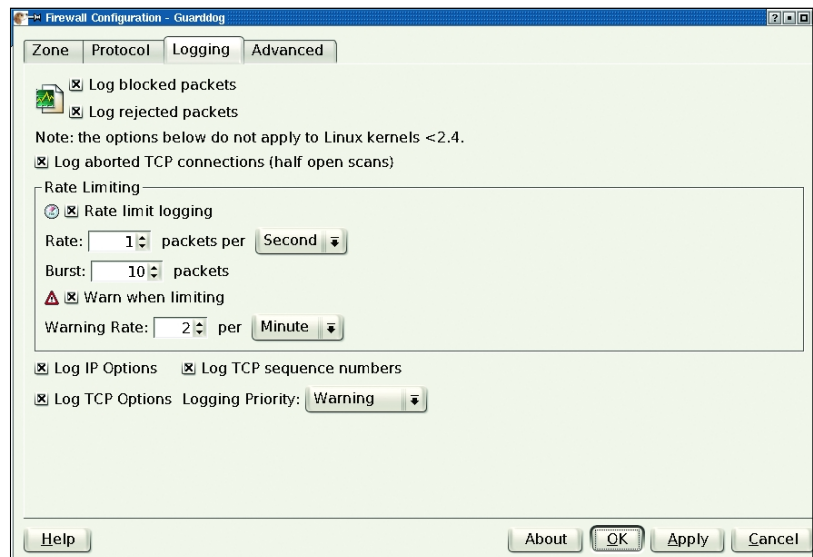


Figura 3: Los administradores pueden usar la solapa *Logging* para especificar que clase de registro debe proporcionar el cortafuegos.

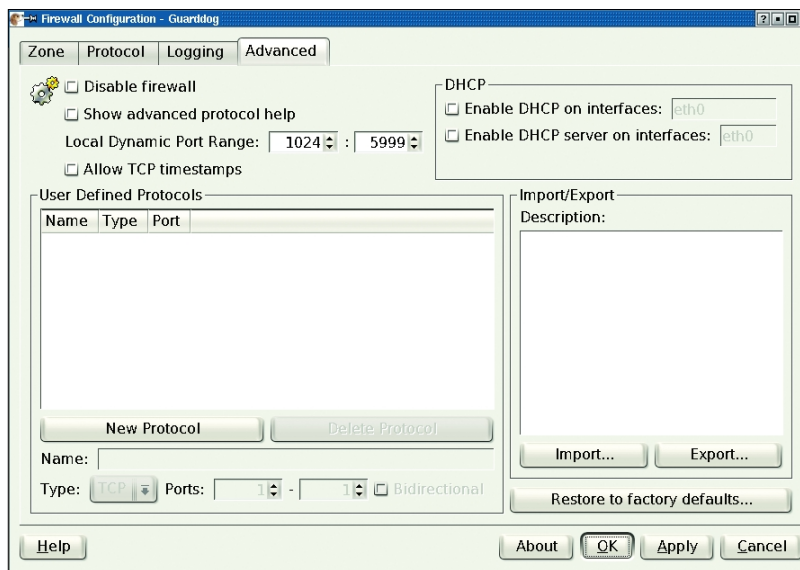


Figura 4: Guarddog soporta configuraciones del cortafuegos detalladas. Por ejemplo, los usuarios pueden definir protocolos y exportar e importar scripts.

registro de Guarddog en syslog. El registro proporciona a los usuarios una herramienta para detectar escaneos de puertos. Los usuarios de Guarddog pueden establecer la tasa de registro para restringir el número de entradas en los registros del cortafuegos. Un límite para el número máximo de entradas ayudará a evitar un ataque potencial por denegación de servicios, que a veces es causado por una tormenta de paquetes IP que llenan el syslog y sobrecarga el disco duro.

Si necesita detalles de todos los paquetes IP y TCP entrantes, puede seleccionarse la opción para registrar todos los paquetes y los números de secuencia TCP en la base de la ventana.

La solapa *Advanced* (véase la Figura 4) permite a los administradores experimentados ajustar con precisión las

opciones del cortafuegos para reflejar sus necesidades. Si algo va mal, no se preocupe: siempre se puede pulsar en *Restore to factory defaults...* para restaurar las opciones por defecto de Guarddog. Las opciones por defecto para *Local Dynamic Port Range* están bien en la mayoría de los casos. Especifica que rango de puertos puede usar Linux para las conexiones salientes.

Si echa en falta algún protocolo en la solapa *Protocol*, puede pulsar *New Protocol* e introducir el nombre del protocolo, establecer si el protocolo es TCP o UDP y especificar los números de puertos que usa.

Guarddog tiene una opción útil para importar y exportar los scripts de cortafuegos creados con la herramienta. Guarddog puede exportar la configuración actual a un script de la shell

sencillo y almacenarlo en */etc/rc.firewall*. Como los servidores normalmente no ejecutan KDE, los administradores pueden simplemente pulsar el botón *Export* para exportar un script, copiar este script al servidor y ejecutarlo en él.

## Puerta de Enlace al Mundo

Desde luego, los cortafuegos de Linux no se usan típicamente para los sistemas aislados, sino que se usan como parte de la estructura de seguridad de una red completa. En este caso, la máquina Linux actúa como una puerta de enlace y tiene dos tarjetas de red, una de cara a Internet y otra de cara a la red interna (véase la Figura 5). Es bastante simple configurar Guarddog para este escenario, sin embargo se necesita un sistema con la versión 2.4 del kernel. Además de configurar *IP masquerading* antes de instalar el cortafuegos. Guarddog no puede ayudarle en este paso, pero sí la herramienta Guidedog en [4].

El primer paso es crear una zona Guarddog nueva para la red local. Para hacerlo, pulse *New Zone* en la solapa *Zone*. Se puede llamar a la zona "LAN", por ejemplo. Después púlsese *New Address* para establecer la dirección IP, tal como *192.168.1.0/24*. Ahora púlsese en *Internet* y *Local* en *Connection* para asegurar que la LAN está conectada a Internet y al ordenador local.

Seleccione *Internet* en la solapa *Protocol* y marque las cajas para los protocolos requeridos en la columna de la LAN. Finalmente, pulse *Apply* para almacenar la configuración en */etc/rc.firewall* y lance el cortafuegos. ■

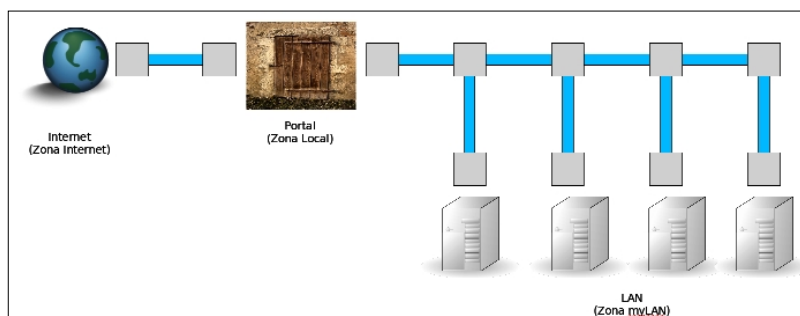


Figura 5: El ordenador cortafuegos de Linux actúa como puerta de enlace para la red interna.

### INFO

- [1] Guarddog: <http://www.simonzone.com/software/guarddog>
- [2] Descarga: <http://www.simonzone.com/software/guarddog/#download>
- [3] Manual online: <http://www.simonzone.com/software/guarddog/#manual>
- [4] Guidedog: <http://www.simonzone.com/software/guidedog/>

### EL AUTOR

Holger Junge trabaja para Lifemedien, donde se encarga de los servidores de dominio, de los servidores Web, el servidor de base de datos MySQL y el servidor de base de datos Oracle.