

Cortafuegos para el día a día

No Sólo para Expertos

Los cortafuegos son cada vez más complejos. Por suerte, las herramientas para su manejo son cada vez más simples y más accesibles para los usuarios normales.

POR JOE CASAD Y ACHIM LEITNER

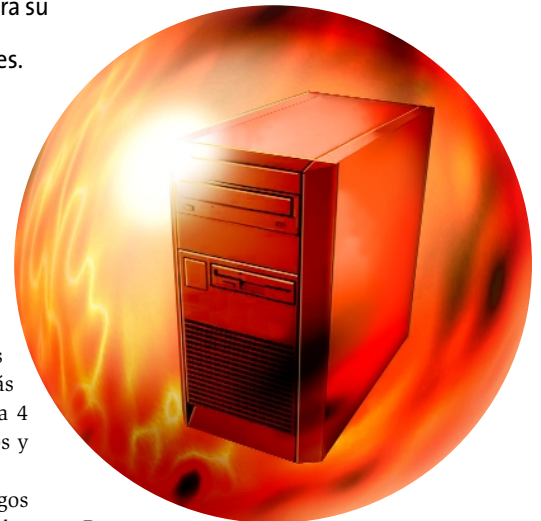
Su ordenador le permite ver el mundo, pero usted no quiere que el mundo le vea. Los intrusos son cada vez más sofisticados y cabe esperar a que alguno se de cuenta tarde o temprano de que su equipo está sin protección. Si se conecta a Internet, necesita estar detrás de algún tipo de cortafuegos.

Hay cortafuegos de muchos tamaños, formas, precios y diseños. Es bastante interesante notar que, lo que se solía llamar cortafuegos, ahora tan solo es uno más de la gran gama de productos de

seguridad. El cortafuegos tradicional es una especie de router que reside en la Capa 3 del modelo de referencia OSI. La Capa 3 es la capa de la pila que escucha al Protocolo de Internet, lee direcciones IP y toma decisiones sobre donde dirigir los datagramas IP. Un cortafuegos además inspecciona las cabeceras de la Capa 4 (TCP o UDP) para identificar servicios y evaluar flags.

Pero los productos de cortafuegos modernos pueden operar en otros niveles de la pila de protocolos (Figura 1). Esta metodología multinivel puede extenderse de modo descendente a la Capa 2, donde encontrará el llamado *bridgwall*. Mientras que un bridge (o switch) simplemente evaluará la dirección MAC, el *bridgwall* inspeccionará los paquetes de la Capa 2 hasta la Capa 4. El *bridgwall* es un filtrador de paquetes hecho y derecho, tan flexible como un switch.

Un gateway a nivel de aplicación proporciona una capa adicional de seguridad al más alto nivel. El gateway captura la conexión TCP actuando como un proxy entre el cliente y el servidor. Esto permite al cortafuegos antes de finalizar mirar el protocolo de aplicación y detectar los paquetes ilegales que incumplan las reglas del protocolo basadas en RFC.



Por supuesto que la mayoría de las variantes de cortafuegos son productos caros para grandes redes y configuraciones complejas. Nosotros estamos más interesados en lo que podemos hacer sólo con Linux y con un software de cortafuegos fácil de encontrar.

Como veremos en el tema de portada de este mes, Linux tiene una buena colección de cortafuegos, incluyendo algunas utilidades poderosas que simplifican el proceso de configuración de modo que no hace falta ser un experto para manejar uno.

En nuestro artículo sobre Guarddog vamos a mostrar como usar este programa KDE para realizar configuraciones de cortafuegos IPTables o IPChains. En nuestro siguiente artículo, sobre Bridgwall, hablamos de los instrumentos para configurar un cortafuegos a nivel de la Capa 2.

Un problema en el manejo de cortafuegos es la cantidad de datos que maneja y que se acumulan en los registros del software de protección. En nuestro tercer artículo se habla de herramientas para el manejo y análisis de los registros de los cortafuegos. Y nuestra última historia describe Shorewall, otra utilidad que no es un cortafuegos propiamente hablando, sino un instrumento para simplificar la configuración de un cortafuegos. ■

EN PORTADA

Guarddog.....11

La utilidad de KDE Guarddog proporciona una interfaz intuitivo para la configuración de cortafuegos en Linux.

Bridgwall.....14

Un cortafuegos a nivel de bridge puede proporcionar una solución simple con un mínimo de reconfiguración.

Analizadores Registros.....18

Herramientas para analizar los ficheros de log y que nos ayudan a entender el estado de la red.

Shorewall.....22

Shorewall es un conjunto de ficheros para la configuración de cortafuegos basados en filtros de red.

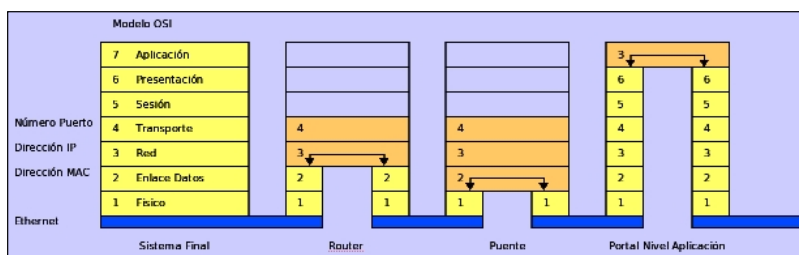


Figura 1: Los cortafuegos modernos puede actuar como bridges (izquierda), routers (centro) o gateways a nivel de aplicación (derecha).