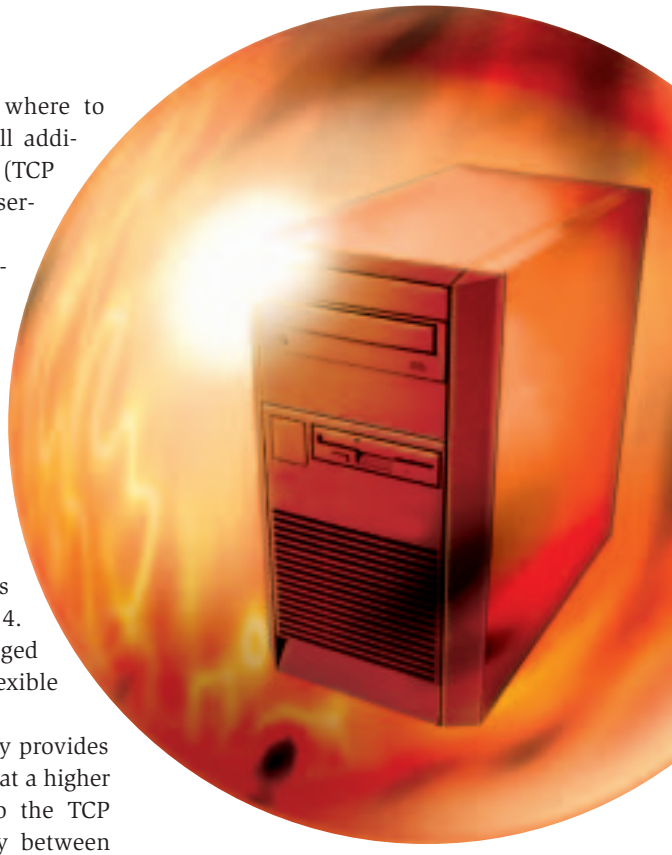
Firewalls for the everyday

Not Just for Experts

Firewalls are becoming evermore sophisticated. Luckily, the tools for managing firewalls are becoming simpler and more accessible for ordinary users. BY JOE CASAD AND ACHIM LEITNER



Your computer lets you see the world, but you don't want the world to see you. Intruders are becoming more sophisticated, and it isn't enough anymore to hope they won't notice your inconspicuous workstation. If you're connected to the Internet, you'd better be behind some kind of firewall.

Firewalls come in many sizes, shapes, prices, and designs. Interestingly enough, what used to be called a firewall is now only one of a wide range of security products. The traditional firewall is a form of router that resides in Layer 3 of the OSI reference model. Layer 3 is the layer of the stack that listens for the Internet Protocol, reads IP addresses, and makes decisions about where to route IP datagrams. A firewall additionally inspects the Layer 4 (TCP or UDP) headers to identify services and evaluate flags.

But modern firewall products can operate at other levels of the protocol stack (Figure 1). This multilevel approach can extend downward to Layer 2, where you'll find the so-called *bridgewall*. Whereas a legacy bridge (or switch) will simply evaluate MAC addresses, the bridgewall inspects packets from Layer 2 right up to Layer 4. The bridgewall is a full-fledged packet filter that is just as flexible as a switch.

An application-level gateway provides an additional layer of security at a higher level. The gateway taps into the TCP connection acting as a proxy between the client and the server. This allows the firewall to take a close look at the application protocol and detect illegal packets that break RFC-based protocol rules.

Of course, many of the more exotic firewall variants are expensive hardware products for large networks and complex configurations. We're much more interested in what you can do with only Linux and easy-to-find firewall software.

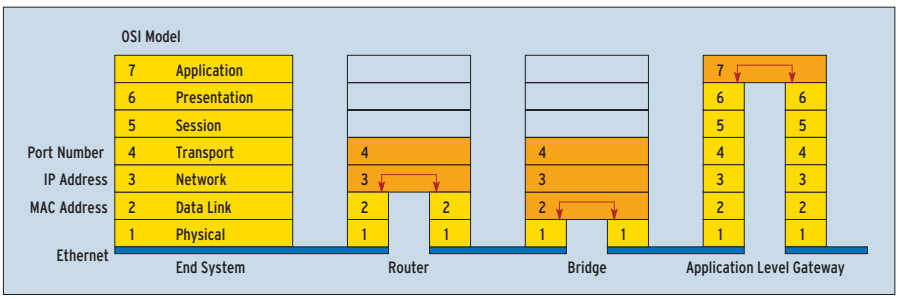


Figure 1: Modern firewalls can operate as bridges (left), routers (center), or application-level gateways (right).

As you'll learn in this month's issue, Linux has a good collection of firewall tools, including some powerful utilities that simplify the firewall configuration process so that you don't have to be an expert to manage your firewall.

In our lead article on Guarddog we'll show how to use this KDE program to set up IPtables or IPchains firewall configurations. Our next article, on Bridgewall, discusses the tools for configuring a bridging-level Layer 2 firewall.

One problem with managing firewalls is managing the abundance of data that accumulates in firewall logs. Our third article discusses tools for managing and analyzing firewall logs. And our final story describes Shorewall – another utility that is not a firewall itself but is, instead, a tool for simplifying firewall configuration. ■