Taking the Cost Out of Firewalls

It pays to know your Linux

BY RAM SAMUDRALA

With about $1,000 and knowledge of Linux and networking principles, you can have a firewall that provides freedom, flexibility, and optimal security. In this article, Ram Samudrala shares his experience in creating a cost-effective firewall.

The Motivation

For almost two years, I dealt with a situation where I had access to a gigabit ethernet connection to the Internet, but I couldn't harness it since I was behind a commercial firewall that only supported 100Mbps. Upgrading would have required thousands of dollars, which, especially in this economy, seemed wasteful. My solution was to create a Linux-based gigabit ethernet firewall that will do the same thing. The beauty of this setup was not only that I could put together the hardware for less than $1,000, but since the software is freely copiable, there are no restrictions on the numbers of users and licenses.

It's clear that gigabit ethernet over copper is going to be the next step in networking. Even if you don't have a gigabit ethernet connection to the Internet, it's not too expensive to acquire one. It's also clear that one of the most logical ways to protect yourself from unwanted attack is through the use of a firewall. However, commercial firewall products utilizing gigabit ethernet are prohibitively expensive.

ABOUT THE AUTHOR

Ram Samudrala is a principal investigator (assistant professor) at the University of Washington. His work has led to several publications in peer-reviewed journals and freely copiable software for molecular and systems modeling (which are being used on high-performance Linux-based computing clusters that he manges). He released an album with the pseudonym Twisted Helices, with the complete album being published online free of any intellectual property restrictions. He is also the author of the Free Music Philosophy *and other texts on (and against!) intellectual property, which have been referenced in* Forbes, HotWired, *and* The New York Times.

ram@compbio.washington.edu

The Setup

Hardware Configuration

The machine I purchased for a firewall is a nice 4U rackmount with an AMD Palamino 1700+ CPU, a MSI KT3 Ultra2 KT333 MS-6380E motherboard, a small hard disk, some memory, and three Intel Pro/1000T Gigabit Server ethernet cards. All the hardware cost less than $1,000. The main thing to note here is that any computer with gigabit ethernet cards should do, assuming that its components work well with Linux (in most cases, they should).

Software Configuration

The operating system running on the firewall is Linux, and we use the KRUD distribution, version 8.0. The system is installed like any other Linux system, but all Internet-based services are turned off.

Linux supports firewalling through its netfilter/iptables subsystem. It will basically let you do anything a commercial firewall can do, and then some, including the functionality of packet filtering (stateless or stateful), all different kinds of NAT (Network Address Translation), and packet mangling. It is extremely powerful, but cumbersome to use.

There are packages that provide a cleaner interface to the iptables. One such package that we use is Shorewall, which lets you manipulate the firewall rules using simple configuration files. Our setup is such that each of the gigabit ethernet cards is assigned to three zones: the zone that compromises the external Internet ("net"), the demilitarized zone ("DMZ"), and the local network ("loc"). Using Shorewall, we can specify how traffic is to be routed across the different zones (see Figure 1).

Specifically, we allow all connections from machines in the local zone to the net zone. We allow Web and mail access to our Web/mail server(s) located in the demilitarized zone (DMZ); for this reason, all machines in the DMZ are completely mirrored since Web and mail servers, even the most up-to-date versions, could have potential security holes. Depending on your level of paranoia, you can set up the firewall such that you allow access to the firewall only from a console, or from a single host in the local zone.

We allow only secure logins, using OpenSSH, from a selected list of trusted hosts in the net zone to a dedicated gateway machine (located in the local zone). The secure logins have to pass a one-time password screen based on OPIE, as well as a permanent password screen, to be able to log in to the gateway machine. The combination of OpenSSH and OPIE for authentication is handled using Linux-PAM.

The two-password system is to address the issue of keyloggers who may record a user's permanent password (which is possible even over a secure connection). One-time passwords get around this problem, but they are not enough since users have a tendency to store their list of one-time passwords on their computers, and a computer could be stolen/compromised.

Thus the only way to gain access to our local network from the Internet is by knowing the list of one-time passwords, and the permanent password for an authorized user, and making the connection from a list of trusted hosts. The passphrase for the one-time passwords is randomly generated for each user (i.e., the users don't have a choice as to the passphrase), which is then used to generate a list of one-time passwords that a user keeps. The list can be reset at the whim of the user, with a new random passphrase being used to create a new list. A script to do this is available at (www.ram.org/computing/linux/firewall/otpgen.tgz).

The Bottom Line

The Minuses...

The downside of such a firewall is that you do need to know your Linux, and be extremely familiar with networking principles. Even though the Shorewall packages simplify management, for optimal security it helps to be familiar with the netfilter subsystem. If your system administrator is familiar with Linux, then this shouldn't be a problem.

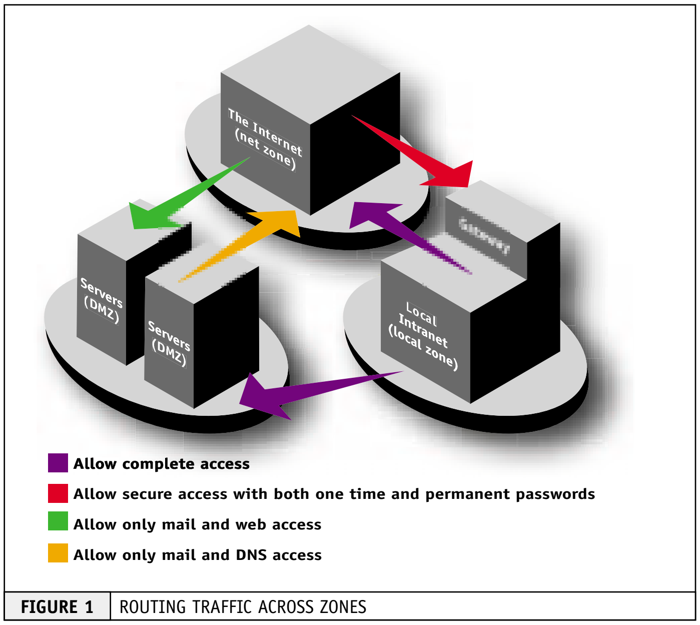

The Internet (net zone)
Gateway
Servers (DMZ)
Servers (DMZ)
Local Intranet (local zone)
🟪 Allow complete access
🟥 Allow secure access with both one time and permanent passwords
🟩 Allow only mail and web access
🟧 Allow only mail and DNS access

FIGURE 1 ROUTING TRAFFIC ACROSS ZONES

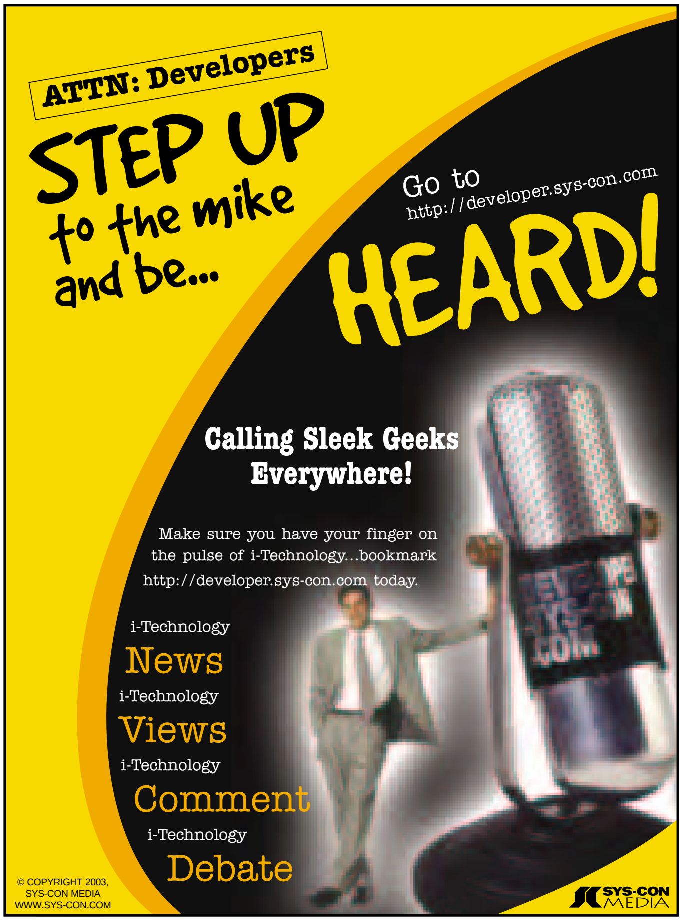
And the Pluses...

The amount of flexibility greatly outweighs the Shorewall learning curve, not to mention the cost of creation and maintenance. Another singular advantage over a commercial product is that it's easy to upgrade the hardware and software at whim.

The bottom line is that security is best achieved by a thorough understanding of networking principles and exploits. A Linux-based firewall gives you the freedom, flexibility, and the opportunity to achieve security in an optimal and economical manner.

Resources

- *KRUD:* http://tummy.com/krud
- *netfilter:* www.netfilter.org
- *Shorewall:* www.shorewall.net
- *OpenSSH:* www.openssh.com
- *OPIE:* www.inner.net/opie
- *Linux-PAM:* www.kernel.org/pub/linux/libs/pam


ATTN: Developers
STEP UP to the mike and be...
Go to http://developer.sys-con.com
HEARD!
Calling Sleek Geeks Everywhere!
Make sure you have your finger on the pulse of i-Technology...bookmark http://developer.sys-con.com today.
i-Technology News
i-Technology Views
i-Technology Comment
i-Technology Debate
SYS-CON MEDIA

LWM Advertiser Index

Advertising Partner	Web Site URL	Phone #	Page #
BASIS INTERNATIONAL / OPEN SYSTEMS	WWW.BASIS.COM / WWW.OSMCORP.COM		6
BLACKHAT	WWW.BLACKHAT.COM	916 853 8555	65
COMDEX	WWW.COMDEX.COM	650 578 6900	89
FREE SOFTWARE FOUNDATION	WWW.GNUPRESS.ORG	617 542 5942	27
HP	WWW.HP.COM/LINUX	888 HPLINUX	C4
ISAVIX	WWW.ISAVIX.COM	866 472 8849	33
LINUXWORLD CONF. & EXPO	WWW.LINUXWORLDEXPO.COM		43
LINUXWORLD MAGAZINE	WWW.LINUXWORLD.COM	888 303 5282	77
ORACLE	WWW.ORACLE.COM/LINUX		C2
PERVASIVE SOFTWARE	WWW.PERVASIVE.COM/LINUX8	800 287 4383	3
PROMICRO SYSTEMS	WWW.PROMICRO.COM	866 646 4276	8
RACKSAVER	HTTP://OPTERON.RACKSAVER.COM	888 942 3800	21
VERITAS	WWW.VERITAS.COM		15
XIMIAN	WWW.XIMIAN.COM/INFORMATION/MGMT3		C3