The Sysadmin's Daily Grind: FireHOL

OFF THE WALL

If you don't have time to tinker with complicated firewall rules, you might want to check out the clever FireHOL approach.

BY CHARLY KÜHNAST

There's no place like home. I can hear a quiet humming sound from the broom cupboard next to the kitchen. At least it's quiet until I open the door. When I do, I'm treated to a noise like a jet with engine trouble. Between lamp fuel, shoe polish, and miscellaneous jars stands the technology that connects me to the outside world. Beside the modems provided by my telco and an asthmatic Cisco – which is to blame for most of the noise – resides a PC old-timer, my firewall.

Originally, my manual iptables rules just handled masquerading for outgoing connections from the LAN, with a couple of custom rules for individual servers. Over time, the rules have become increasingly complex, and as they did, I found myself searching even harder for a management tool.

Finally, I found FireHOL [1]. In contrast to Firewall Builder [2], the FireHOL tool does not have a graphical user interface. Instead, you just add simple directives to a configuration file and FireHOL translates them into iptables commands.

If you just need masquerading and want to restrict it to http traffic, this short configuration is all you need:

```
interface eth0 home
   client all accept
```

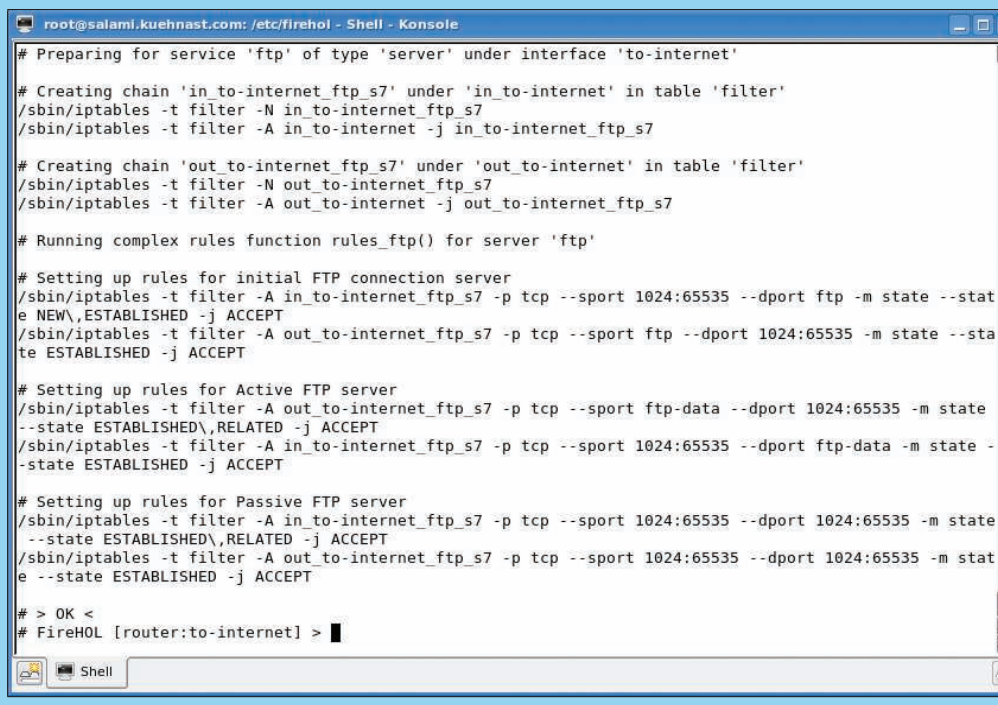

Figure 1: FireHOL reduces the administrative effort involved with configuring a firewall. This screenshot shows a control file for FTP connections.

```
interface eth1 internet
   client all accept
router to-internet
inface eth0 outface eth1
      masquerade
      route http accept
```

The *client all accept* lines let the firewall establish arbitrary connections on the LAN and the Internet.

To avoid restricting masquerading to http and open up the door for any protocol, you just need to change the last line like so:

```
route all accept
```

Based on this directive, FireHOL generates several dozen iptables commands. The reason for this is that it has special handling for complex protocols such as active FTP. Figure 1 shows part of the rule ruleset that handles FTP.

FireHOL lets you watch it work and offers the practical *explain* function to facilitate this. You can use the interactive shell to type rules in the syntax shown in the sample, and the tool responds with the corresponding iptables rules, which FireHOL will apply if you ask it to do so.

After quietly simplifying the management of my home firewall, I now have time to think about doing something about the noise coming from the broom cupboard. ■

INFO

[1] FireHOL: *http://firehol.sourceforge.net*

[2] Firewall Builder: *http://www.fwbuilder.org/*

THE AUTHOR

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, fresh water aquariums, and learning Japanese, respectively.