Front-ends for IPtables

Building Firewalls

Netfilter is a powerful kernel based Firewall for Linux, but handling the IPtables command line tool is definitely non-trivial. GUI programs can make life easier for admins.

BY NICO LUMMA

Friedrich Keller, visipix.com

Personal firewalls are here to stay, but for many users getting their firewall configuration right can be a genuine challenge. Modern kernels provide netfilter modules for firewalling tasks and use IPtables to configure them, and a variety of GUI-based front-ends have been implemented to simplify the IPtables configuration process.

These front-ends simplify the task of creating firewall rules, and launching them when required. Some programs support inexperienced users, by providing wizards to query the required firewall characteristics, and creating an appropriate ruleset.

This article will be looking at four tools, which are mainly distinguished by their GUIs. *Knetfilter* was written for KDE, *Firestarter*, on the other hand, is a GNOME application, whereas *Jay's Iptables Firewall* provides text based menus and the *Easy Firewall Generator for IPTables* is Web based.

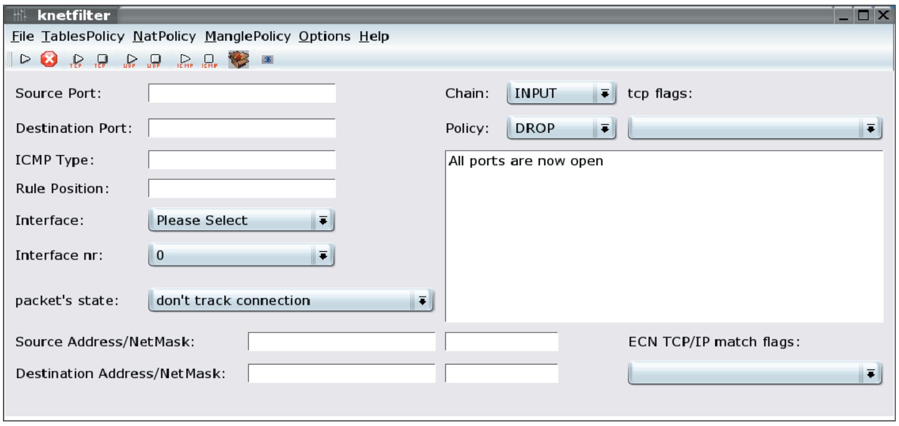
Knetfilter

Knetfilter [1] is an fully-featured tool that provides traffic analysis functionality in addition to firewall configuration. Knetfilter not only allows you to create and modify IPtables rulesets, but also provides a convenient front-end for *nmap* and *tcpdump*.

Knetfilter is quite simple to use, but it does assume some prior knowledge of *IPtables*. The main menu allows you to add rules, but you will need to know what you are doing. After defining filter rules, you can use a menu to specify how the rule will be incorporated into your existing ruleset, and to stipulate the protocols to which it will be applied. This approach allows for quick and easy rule generation, where rules can be applied to any available protocol. Knetfilter is extremely powerful and even provides so-called traffic shaping facilities, that is, it allows you to assign more or less bandwidth to specific computers.

The excellent NAT (Network Address Translation) menu is used whenever the firewall will be protecting not only its own host, but a complete network. If you need more complex NAT rules, you can additionally define port forwarding parameters to allow SSH access to a computer behind the firewall, for example. After creating rules, it is generally a good idea to use the front-end for *tcpdump* to analyze the incoming traffic and *nmap* to scan your ports, ensuring that specific services are available, or generally to check for open ports.

In addition to the fact that Knetfilter is integrated with KDE, it is the large selection of features that make this tool so valuable. Knetfilter does not offer enough in the line of help to allow for impromptu firewall configuration. Al-



knetfilter
File TablesPolicy NatPolicy ManglePolicy Options Help
TCP TCP UDP UDP ICMP ICMP

Source Port:

Destination Port:

ICMP Type:

Rule Position:

Interface: Please Select

Interface nr: 0

packet's state: don't track connection

Source Address/NetMask:

Destination Address/NetMask:

Chain: INPUT

tcp flags:

Policy: DROP

All ports are now open

ECN TCP/IP match flags:

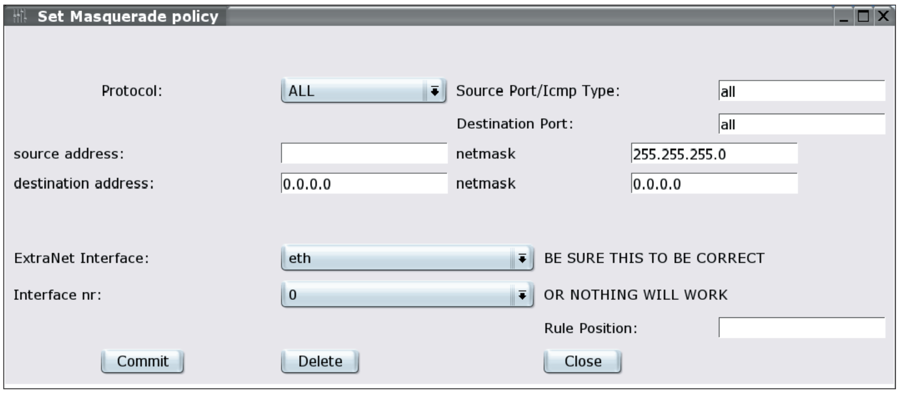
Figure 1: The Knetfilter interface allows you to create new rules

though Knetfilter can handle the whole range of *IPtables* functionality, no support is provided for creating rules.

Firestarter

There are two versions of Firestarter [2], for GNOME 1.x and GNOME 2.x, respectively. When you launch the program, the Firestarter druid appears to help set up the firewall and ask a lot of sensible questions about the firewall's intended use. Depending on the features you need, the druid may go into more detail and prompt you to specify the services where port redirection is required. After saving the configuration, you can use the new firewall straight away.

Besides the excellent druid, Firestarter's other major benefit is the monitoring function. You can check what kind of traffic is passing through your computer, and modify its configuration correspondingly. This is a useful feature for inexperienced users, as there is no need to put hours of thought into what might happen. Instead you can simply use the druid to setup the firewall and then observe the kind of traffic that is getting through. You can then modify the firewall to provide a customized firewall solution for your needs.



Set Masquerade policy

Protocol: ALL

Source Port/Icmp Type: all

Destination Port: all

source address:

netmask 255.255.255.0

destination address: 0.0.0.0

netmask 0.0.0.0

ExtraNet Interface: eth

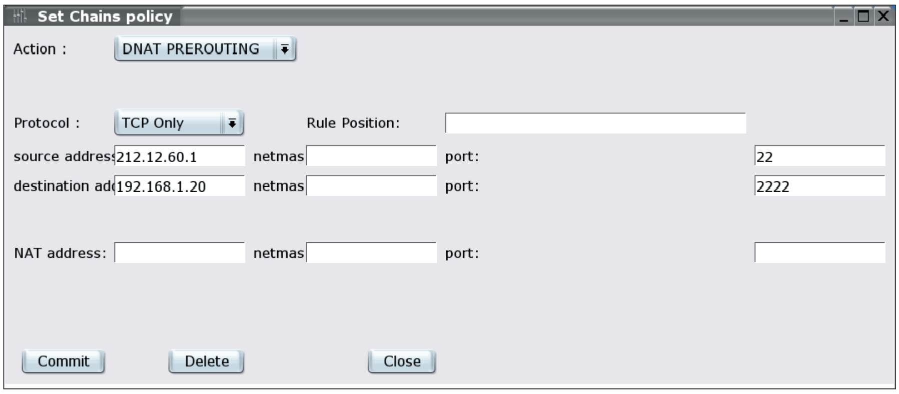
BE SURE THIS TO BE CORRECT

Interface nr: 0

OR NOTHING WILL WORK

Rule Position:

Figure 2: Masquerading settings for Knetfilter



Set Chains policy

Action : DNAT PREROUTING

Protocol : TCP Only

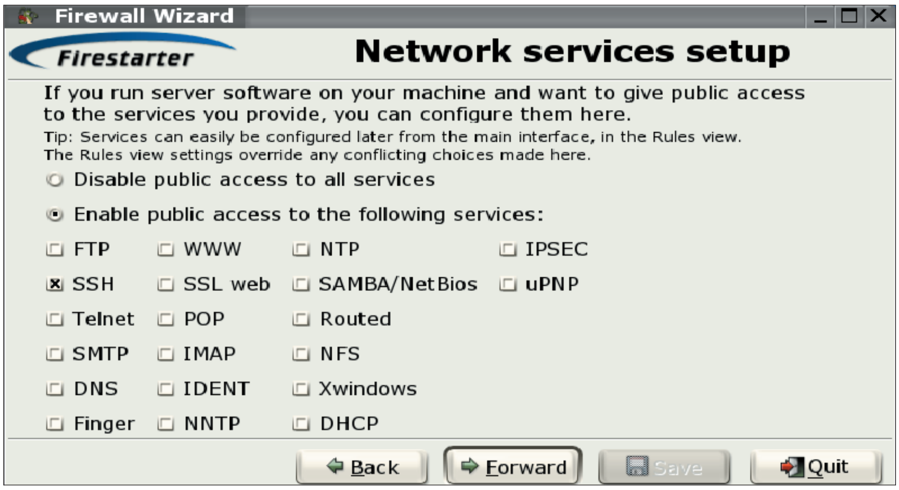
Rule Position:

source addres 212.12.60.1 netmas port: 22

destination ad 192.168.1.20 netmas port: 2222

NAT address: netmas port:

Figure 3: Port redirection with Knetfilter



Firewall Wizard

Firestarter

Network services setup

If you run server software on your machine and want to give public access to the services you provide, you can configure them here.

Tip: Services can easily be configured later from the main interface, in the Rules view. The Rules view settings override any conflicting choices made here.

○ Disable public access to all services

● Enable public access to the following services:

□ FTP	□ WWW	□ NTP	□ IPSEC
☒ SSH	□ SSL web	□ SAMBA/NetBios	□ uPNP
□ Telnet	□ POP	□ Routed	
□ SMTP	□ IMAP	□ NFS	
□ DNS	□ IDENT	□ Xwindows	
□ Finger	□ NNTP	□ DHCP	

Figure 4: Selection of open ports in the Firestarter druid

The *Hits* menu, which contains a number of selectable items for various events, is a good idea: It allows you to block a host, for example, or allow the host to access only a specified service.

Firestarter is a simple tool that will facilitate firewall configuration for beginners in particular. Realtime firewall monitoring is a welcome feature that further underlines the positive impression the tool leaves you with.

Jay's Iptables Firewall

Jay's Iptables Firewall [3] is a text based graphical front-end that lets you to add firewalling even to remote computers.

firewall-config.pl --new creates a new configuration file when you call the program. You can then select items from the menus and compile a firewall to suit your own needs. With no wizard, you will need to navigate the menu items one by one and add content to the best of your ability. After creating and saving your ruleset, you can type */etc/init.d/fw-jay start* to launch; */etc/init.d/fw-jay stop* will stop the firewall.

Jay's Iptables Firewall is not a GUI tool, but provides a hybrid tool based on the command-line and a simple front-end, although this does mean that it will run without any trouble on most systems. You can quickly configure a simple firewall and should have no difficulty adding more complex rules.

Easy Firewall Generator for IPTables

You do not need to run the Easy Firewall Generator for IPTables [4] on your own host in contrast to the other tools introduced so far. If required, you can even

INFO

[1] Knetfilter: *http://expansa.sns.it/knetfilter/*

[2] Firestarter: *http://firestarter.sourceforge.net/*

[3] Jay's Iptables Firewall: *http://firewall-jay.sourceforge.net/*

[4] Easy Firewall Generator: *http://firewall-jay.sourceforge.net/*

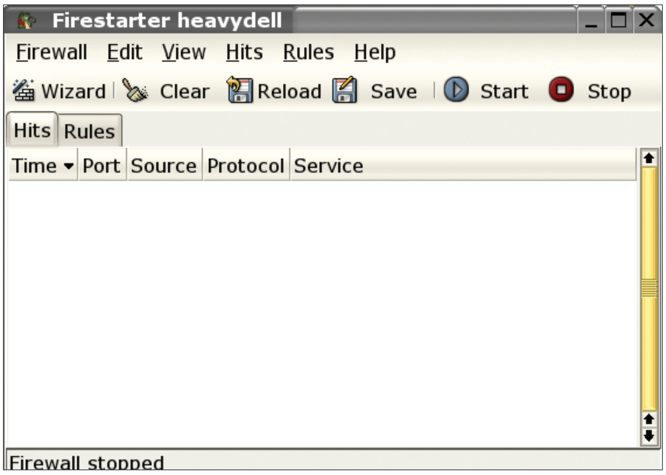
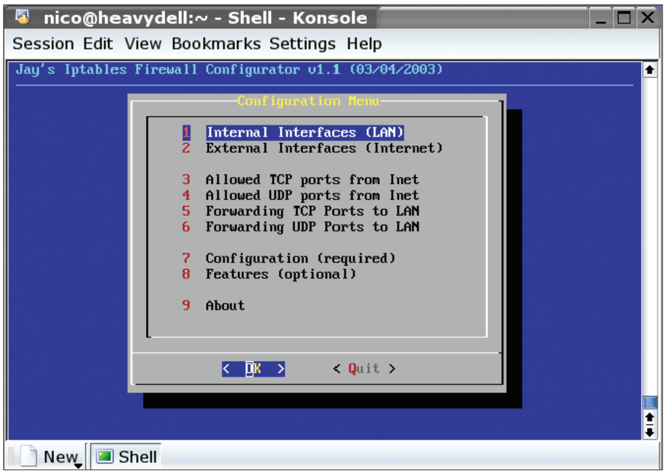

Firestarter heavydell
Firewall Edit View Hits Rules Help
Wizard Clear Reload Save Start Stop
Hits Rules
Time Port Source Protocol Service
Firewall stopped

Figure 5: Firestarter main window


nico@heavydell:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
New Shell

```
Jay's Iptables Firewall Configurator v1.1 (03/04/2003)

                Configuration Menu
   1  Internal Interfaces (LAN)
   2  External Interfaces (Internet)

   3  Allowed TCP ports from Inet
   4  Allowed UDP ports from Inet
   5  Forwarding TCP Ports to LAN
   6  Forwarding UDP Ports to LAN

   7  Configuration (required)
   8  Features (optional)

   9  About

          < OK >        < Quit >
```

Figure 6: Jay's Firewall with Ncurses look

use the tool's website to create the firewall directly. If you do not trust the website operator, or want to see what is going on, you might prefer to install the PHP script on your own Web server.

Using the Easy Firewall Generator could not be easier: You simply answer a few questions, referring to the IP address, the IP address type (static/dynamic), and specify whether you will be protecting a single system or a whole network. You will need to supply the IP addresses for the network, if you are firewalling a network. You can additionally stipulate the services that will be available on the computer to prevent the firewall configuration from blocking them.

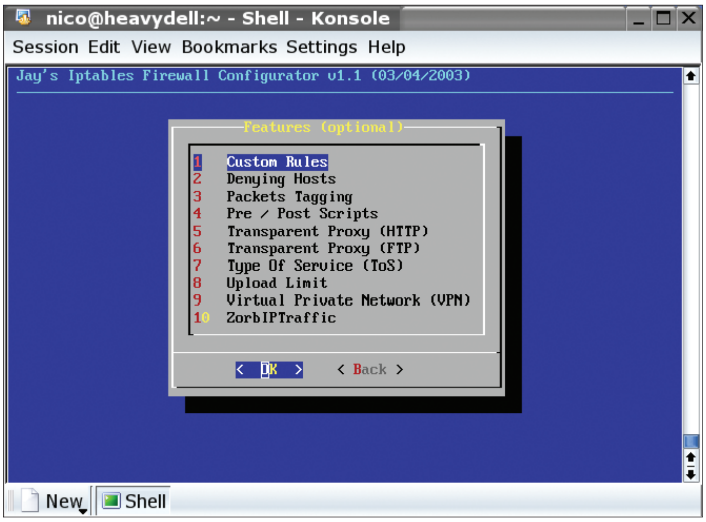
After completing all these settings, a text file containing a complete firewall script is created. You can then type *start / stop* to start or stop the firewall, allowing you to run the firewall when the system is initialized by adding it to appropriate */etc/rcX.d* directories. You may also need to modify the path to *iptables* to get things running.

The advantage that this approach provides is obvious: You can avoid installing software, but still configure a functional firewall within a few minutes. The script can easily be added to your computer's boot process to provide persistent protection for the machine.

Conclusion

If you do not fancy the idea of configuring *iptables* manually, you will probably be quite happy with one of the tools described here. Whether you prefer Knetfilter or Firestarter will largely depend on your skill level. If you are content to do without KDE or GNOME, Jay's Iptables Firewall may be the answer. And if you are looking to generate a firewall with as little effort as possible, you might opt for the Web front-end described last.

The rulesets these tools create are quite useful for production systems, and especially those created by the Web-based solution are simple enough to be understandable. Any firewall, no matter how powerful it may be, is useless, if its users do not understand it, and are thus incapable of modifying the ruleset to reflect changing demands. ■

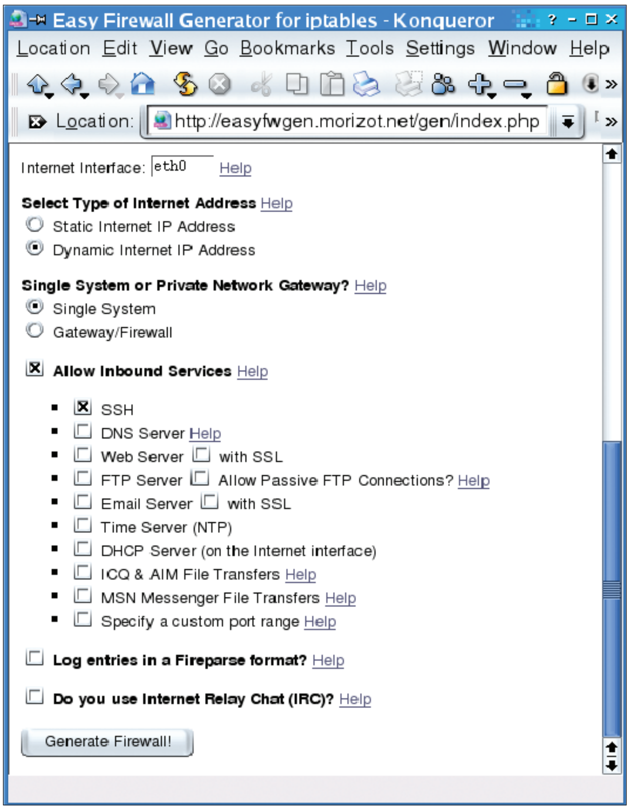

nico@heavydell:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
New Shell

```
Jay's Iptables Firewall Configurator v1.1 (03/04/2003)

              Features (optional)
   1  Custom Rules
   2  Denying Hosts
   3  Packets Tagging
   4  Pre / Post Scripts
   5  Transparent Proxy (HTTP)
   6  Transparent Proxy (FTP)
   7  Type Of Service (ToS)
   8  Upload Limit
   9  Virtual Private Network (VPN)
   10 ZorbIPTraffic

          < OK >        < Back >
```

Figure 7: Jay's Firewall Features


Easy Firewall Generator for iptables - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: http://easyfwgen.morizot.net/gen/index.php

Internet Interface: eth0 Help

Select Type of Internet Address Help
○ Static Internet IP Address
● Dynamic Internet IP Address

Single System or Private Network Gateway? Help
● Single System
○ Gateway/Firewall

☒ **Allow Inbound Services** Help

- ☒ SSH
- □ DNS Server Help
- □ Web Server □ with SSL
- □ FTP Server □ Allow Passive FTP Connections? Help
- □ Email Server □ with SSL
- □ Time Server (NTP)
- □ DHCP Server (on the Internet interface)
- □ ICQ & AIM File Transfers Help
- □ MSN Messenger File Transfers Help
- □ Specify a custom port range Help

□ **Log entries in a Fireparse format?** Help

□ **Do you use Internet Relay Chat (IRC)?** Help

Generate Firewall!

Figure 8: The Easy Firewall Generator is controlled by a PHP script