





Translation(s): [Deutsch](#) - [Italiano](#)

---

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

**Note that some of the information in this page can be out of date.**

## More information

- [Firewalls-dnat-redirect](#) is one sticky point where hosts are in the same subnet as the DNATed service they are trying to use, and need special attention to make connections work.
- [Firewalls-local-port-redirection](#) tells you how to redirect traffic from one port to another within single machine.
- I also found this to be invaluable, along the lines of ECN:  <http://www.tldp.org/HOWTO/Adv-Routing-HOWTO/lartc.cookbook.ultimate-tc.html>
- Another very good reading on iptables, including both - new or advanced iptables users can be found here:  <http://www.frozentux.net/documents/iptables-tutorial/>
- On this wiki there's the [iptables](#) page.
- [DebianPkg: iptables-persistent](#)

## Choosing an IPtables frontend




### Introduction







There are *lots* of iptables frontends. So you have lots of choice. This section is devoted to help you making a choice among this truckload of options by comparing the tools. NB: you should install just *one* of these packages. Installing more than one will *not* make your system more secure; it will likely make your system unmanageable.

BTW: There's also a [!\[\]\(3dfb8d66e81160ad61421a3452093d1b\_img.jpg\) securityfocus article](#) (from April 2001) comparing some of these tools. Some of these are described in the [!\[\]\(21ece2018b00c7267b3324c50bbed633\_img.jpg\) Securing Debian Manual](#).

## Overview

Here's an overview of the different tools (selection inspired upon what's available in Debian unstable as of 2014-07):

Package and Upstream URL	Interface	Programming Language	Size of Source (as of 2005-10)	Releases (as of 2014-07)
<a href="#"> <u>arno-iptables-firewall</u></a>	edit (debconf)	sh	60K	< 2003-08 - 2014-04
<a href="#"> <u>ferm</u> (wiki page)</a>	edit	perl	80K	2000-12 - 2013-07
<a href="#"> <u>fiaif</u></a>	edit	bash	320K	< 2003-01 - 2013-01
<a href="#"> <u>filtergen</u></a>	edit	C	150K	< 2002-10 - 2005-05
<a href="#"> <u>firehol</u></a>	edit	bash	210K	< 2003-05 - 2014-02
<a href="#"> <u>firestarter</u></a>	gui (gnome)	C	1170K	< 2003-01 - 2005-01
<a href="#"> <u>fwbuilder</u></a>	gui (kde)	C++	1190K	< 2003-12 - 2013-04
<a href="#"> <u>guidedog</u></a>	gui (kde)	C++	590K	2001-11 - 2008-08
<a href="#"> <u>ipkungfu</u></a>	edit	sh	40K	2002-09 - 2007-01
<a href="#"> <u>mason</u></a>	shell (autolearning)	bash	500K	< 1999-03 - 2002-05
	edit, iptables	sh	70K	< 2000-

					11 -
<a href="#">netscript-2.4</a>					2004-10
	edit, webmin	sh	130K	< 2001-	12 -
<a href="#">shorewall</a>					2014-07
	edit (debconf)	perl	34K	2002-02 -	2014-07
	edit	sh	80K	2003-03 -	2014-06
	curses	C	1877K	2004-07 -	2009-04
<a href="#">Vuurmuur</a>					
	edit	python	247K	2009-05 -	2012-08

**ferm** uses a text-based configuration with keywords closely resembling iptables rules. Variables and combined rules simplify rule definitions and enhance readability.

The **fiatf** configuration file is very similar to raw iptables rules.

**Filtergen** has support for non-iptables packet filters too. The configuration file is application-specific.

**firestarter** is an application oriented towards end-users that includes a wizard useful to quickly setup firewall rules. The application includes a GUI to be able to monitor when a firewall rule blocks traffic.

**fwbuilder** is an object oriented GUI which includes policy compilers for various firewall platforms including Linux' netfilter, BSD's pf (used in OpenBSD, NetBSD, FreeBSD and MacOS X) as well as router's access-lists. It is similar to enterprise firewall management software. Complete fwbuilder's functionality is also available from the command line.



**mason** is an application which can propose firewall rules based on the network traffic your system sees.

The **netscript-2.4** Debian package description says: "DON'T use this on a server - it is designed for dedicated routers and firewalls with hardly any configured services."

**shorewall** is a firewall configuration tool which provides support for IPsec as well as limited support for traffic shaping as well as the definition of the


firewall rules. Configuration is done through a simple set of files that are used to generate the iptables rules.

**ufw**: Canonical's ufw is from Ubuntu. (New for squeeze)

**vuurmuur**: Victor Julien's  [vuurmuur](#) is not (yet?) included in Debian, but Debian packages are available in an  [apt-able archive](#).


### *Debian specific information*

Some Debian-specific data about these packages:

Package and Debian package URL	Debian package description	 <a href="#">Popularity</a> (2017-01-09)
<a href="#">DebianPkg: arno-iptables-firewall</a>	Single- and multi-homed firewall script with DSL/ADSL support	491
<a href="#">DebianPkg: ferm</a>	maintain and setup complicated firewall rules	1661
<a href="#">DebianPkg: fiaif</a>	An easy to use, yet complex firewall	X
<a href="#">DebianPkg: filtergen</a>	packet filter generator for various firewall systems	11
<a href="#">DebianPkg: firehol</a>	An easy to use but powerful iptables stateful firewall	537
<a href="#">DebianPkg: firestarter</a>	gtk program for managing and observing your firewall	X
<a href="#">DebianPkg: firewallld</a>	dynamically managed firewall with support for network zones	565
<a href="#">DebianPkg: fwbuilder</a>	Firewall administration tool GUI	2323
<a href="#">DebianPkg: guidedog</a>	NAT/masquerading/port-forwarding configuration tool in Qt5	14
<a href="#">DebianPkg: ipkungfu</a>	iptables-based Linux firewall	15
<a href="#">DebianPkg: mason</a>	Interactively creates a Linux packet filtering firewall	19
<a href="#">DebianPkg: netscript-2.4</a>	Linux 2.4.x (and 2.6.x) router/firewall network configuration system	63



<a href="#">DebianPkg: shorewall</a>	Shoreline Firewall (Shorewall)	3232
<a href="#">DebianPkg: uif</a>	Advanced iptables-firewall script	29
<a href="#">DebianPkg: uruk</a>	Wrapper for Linux iptables, for filtering rules management	71
<a href="#">DebianPkg: ufw</a>	program for managing a Netfilter firewall	5377
<a href="#">DebianPkg: vuurmuur</a>	curses-based firewall	-


The number in the popularity is the number of installations. The higher the number the more installations it has. "-" and "X" denote packages not in Debian; "X" marks former packages that have been removed as of stretch.

As of 2005-11-02, for all packages (ferm, fiaif, filtergen, firehol, firestarter, fwbuilder, guidedog, hflf, ipkungfu, ipmenu, mason, netscript-2.4, shorewall, uif) the  [BTS](#) looks quite OK: no serious bugs, the packages look well-maintained.

Notes on size of package: if there are lots of sources, the package might be too bloated for your taste. However, if the size of the sources is small, there are likely less nice features. OTOH, small packages are more easy to check for errors, and might offer a nice "mean 'n' lean" feeling.

#### *Yet other ones*

There's also  [webmin-firewall](#). webmin-firewall is a webmin plugin, shipped in  [firewall.wbm.gz](#): "Configure a Linux firewall using iptables".

 [ipmenu](#), a small perl script with curses interface, wasn't shipped with the Debian etch release.







#### *Conclusion*

Now for the conclusion: we'll give a possible way to decide, using the data gathered above.

If you want a gui tool choosing firestarter or fwbuilder is probably wise: these are all popular tools. fwbuilder (for KDE) is by far the most popular. However, it is said it's definately *not* a tool for newbies. Guarddog (KDE) and firestarter (GNOME) are both equally popular. The codesize for all three is about the same.

Now suppose you don't want a gui tool, for instance since you're working on servers and don't have X libraries installed. You also might like a plain-text editable configuration file, since you manage your configuration files with a version control system. You also want a tool which is actively maintained: since 2004-09 there should have been at least one release.

Let's take a closer look at 6 of the qualifying non-gui tools:


Package and Online Documentation	Configuration file format	Size of main script
 <a href="#">arno-iptables-firewall</a>	shell	135K
 <a href="#">ferm</a>	app specific	62K
 <a href="#">firehol</a>	shell	24K + 131K = 155K
 <a href="#">shorewall</a>	app specific	203K
 <a href="#">uruk</a>	shell	9K
 <a href="#">ufw</a>	python	848 k

The **arno-iptables-firewall** Debian package comes with a debconf frontend: it is possible to configure this tool interactively.

To use **ferm**, one has to write a configuration file using keywords that are used by iptables. Ferm basically adds nesting syntax and variables to iptables rules. It seems it has the best support for IPv6 among these packages. This tool offers a quick and maintainable approach to writing firewall rules if you are used to iptables commands.



"**FireHOL** is a language to express firewalling rules, not just a script that produces some kind of a firewall." FireHOL configuration files are shell scripts (but actually don't really look like that; it seems they're about as simple as one can get). FireHOL comes with firehol-wizard(8), which creates a configuration file you'll *have* to edit manually afterwards. Support for IPv6 was added recently (it was previously available in FireHOL fork called Sanewall). This is a pretty popular tool.

"**Shorewall** is not the easiest to use of the available iptables configuration tools but I believe that it is the most flexible and powerful." It "can handle complex and fast changing network environments." It needs multiple configuration files, even for simple setups. Seems only suitable for powerusers. (Likely there are a lot of these among Debian users: shorewall is very popular!)

For **uruk**, there is an  [example uruk configuration file](#). Uruk is extremely small: this is nice if you want to adapt the tool to your own needs, or want to be very sure it does what you want: it doesn't take long to check all the code manually. Of course, the small size comes with less functionality. However, if you have very specific needs, you can easily hook your own crafted iptables rules in the uruk framework. This is documented in the uruk manpages. However, beware: the major part of this section of this wiki-page was written by the uruk-author. If you feel this page could be more objective, please edit it!

Making the final decision between the 5 short-list ones is left as an exercise to the reader: it depends on your specific situation and needs. You could install them one after the other, and try them for yourself.

*Thanks*

Thanks to  [Michael Hanke](#) for making the first start of the IPtables frontends comparison. Thanks to Victor Julien for contributing some notes on the Vuurmuur package. Provided in part by the  [debian-firewall list](#).

---

[CategorySystemAdministration](#) | [CategorySystemSecurity](#) |  
[CategoryRedundant](#): merge with [DebianFirewall](#)