Introduction

The Linux kernel in Ubuntu provides a packet filtering system called netfilter, and the traditional interface for manipulating netfilter are the iptables suite of commands. iptables provide a complete firewall solution that is both highly configurable and highly flexible.

Becoming proficient in iptables takes time, and getting started with netfilter firewalling using only iptables can be a daunting task. As a result, many frontends for iptables have been created over the years, each trying to achieve a different result and targeting a different audience.

The Uncomplicated Firewall (ufw) is a frontend for iptables and is particularly well-suited for host-based firewalls. ufw provides a framework for managing netfilter, as well as a command-line interface for manipulating the firewall. ufw aims to provide an easy to use interface for people unfamiliar with firewall concepts, while at the same time simplifies complicated iptables commands to help an adminstrator who knows what he or she is doing. ufw is an upstream for other distributions and graphical frontends.

UFW in Ubuntu

Ubuntu 8.04 LTS introduced ufw, and it is available by default in all Ubuntu installations after 8.04 LTS.

**Available Versions in supported versions of Ubuntu**

* **Ubuntu 12.04 ESM**: 0.31.1-1
* **Ubuntu 14.04 ESM**: 0.34~rc-0ubuntu2
* **Ubuntu 16.04 LTS**: 0.35-0ubuntu2
* **Ubuntu 18.04 LTS**: 0.36-0ubuntu0.18.04.1
* **Ubuntu 19.04**: 0.36-1ubuntu1
* **Ubuntu 19.10**: 0.36-1ubuntu3
* **Ubuntu 20.04**: 0.36-6
* **Ubuntu Core**: 0.36pre

**Features**

ufw has the following features:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Feature** | **0.31.1-1** | **0.34~rc-0ubuntu2** | **0.34-2** | **0.35** |
| default incoming policy (allow/deny) | yes | yes | yes | yes |
| allow/deny incoming rules | yes | yes | yes | yes |
| IPv6 (by default) | yes | yes | yes | yes |
| status | yes | yes | yes | yes |
| logging (on/off) | yes | yes | yes | yes |
| extensible framework | yes | yes | yes | yes |
| python 2.5 support | yes | no | no | no |
| application integration | yes | yes | yes | yes\* |
| IPv4 rate limiting via 'limit' command | yes | yes | yes | yes |
| internationalization | yes | yes | yes | yes |
| multiport incoming rules | yes | yes | yes | yes |
| debconf/preseeding | yes | yes | yes | yes |
| default incoming policy (reject) | yes | yes | yes | yes |
| reject incoming rules | yes | yes | yes | yes |
| rule insertion | yes | yes | yes | yes |
| log levels | yes | yes | yes | yes |
| per rule logging | yes | yes | yes | yes |
| outgoing filtering (on par with incoming) | yes | yes | yes | yes |
| filtering by interface | yes | yes | yes | yes |
| bash completion | yes | yes | yes | yes |
| upstart support | yes | yes | yes | yes |
| improved reporting | yes | yes | yes | yes |
| reset command | yes | yes | yes | yes |
| rsyslog support | yes | yes | yes | yes |
| delete by rule number | yes | yes | yes | yes |
| python 2.6 support | yes | yes | yes | yes |
| 'show listening' report | yes | yes | yes | yes |
| python 2.7 support | yes | yes | yes | yes |
| increased protocol support (ah, esp) | yes | yes | yes | yes |
| IPv6 rate limiting via 'limit' command | -- | yes | yes | yes |
| python 3.2 support | -- | yes | yes | no |
| python 3.3 support | -- | yes | yes | yes |
| 'show added' report | -- | yes | yes | yes |
| python 3.4 support | -- | yes | yes | yes |
| before/after extensibility hooks | -- | yes | yes | yes |
| routed packet filtering (FORWARD) | -- | yes | yes | yes |
| systemd support | -- | -- | yes | yes |
| increased protocol support (igmp, gre) | -- | -- | yes | yes |
| python 3.5 support | -- | -- | yes | yes |
| Snappy for Ubuntu Core support | -- | -- | -- | yes |
| per rule comments | -- | -- | -- | yes |

* support for application integration is limited on Ubuntu Core at this time

Basic Usage

Getting started with ufw is easy. For example, to enable firewall, allow ssh access, enable logging, and check the status of the firewall, perform:

$ sudo ufw allow ssh/tcp

$ sudo ufw logging on

$ sudo ufw enable

$ sudo ufw status

Firewall loaded

To Action From

-- ------ ----

22:tcp ALLOW Anywhere

This sets up a default deny (DROP) firewall for incoming connections, with all outbound connections allowed with state tracking.

On Ubuntu Core, simply replace 'ufw' with 'ufw.cmd'. Eg:

$ sudo ufw.cmd enable

**Advanced Functionality**

As mentioned, the ufw application is capable of doing anything that iptables can do. This is achieved by using several sets of rules files, which are nothing more than iptables-restore compatible text files. Fine-tuning ufw and/or adding additional iptables commands not offered via the ufw command is a matter of editing various text files1:

* **/etc/default/ufw**: high level configuration, such as default policies, IPv6 support and kernel modules to use
* **/etc/ufw/before[6].rules**: rules in these files are evaluated before any rules added via the ufw command
* **/etc/ufw/after[6].rules**: rules in these files are evaluated after any rules added via the ufw command
* **/etc/ufw/sysctl.conf**: kernel network tunables
* **/var/lib/ufw/user[6].rules** or **/lib/ufw/user[6].rules** (0.28 and later): rules added via the ufw command (should not normally be edited by hand)
* **/etc/ufw/ufw.conf**: sets whether or not ufw is enabled on boot, and in 9.04 (ufw 0.27) and later, sets the LOGLEVEL
* **/etc/ufw/after.init**: initialization customization script run after ufw is initialized (ufw 0.34 and later)
* **/etc/ufw/before.init**: initialization customization script run before ufw is initialized (ufw 0.34 and later)

After modifying any of the above files, activate the new settings with:

$ sudo ufw disable

$ sudo ufw enable

1 On Ubuntu Core, these files are located under /var/lib/apps/ufw\*/current. See 'ufw.doc ufw-on-snappy' on an Ubuntu Core system for details.

More Information

* Ubuntu 16.04 LTS (Xenial Xerus)
  + [Server Guide - Firewall](https://help.ubuntu.com/16.04/serverguide/firewall.html)
  + [ufw manual](http://manpages.ubuntu.com/manpages/xenial/en/man8/ufw.8.html)
  + [ufw framework manual](http://manpages.ubuntu.com/manpages/xenial/en/man8/ufw-framework.8.html)
* Ubuntu 18.04 LTS (Bionic Beaver)
  + [Server Guide - Firewall](https://help.ubuntu.com/18.04/serverguide/firewall.html)
  + [ufw manual](http://manpages.ubuntu.com/manpages/bionic/en/man8/ufw.8.html)
  + [ufw framework manual](http://manpages.ubuntu.com/manpages/bionic/en/man8/ufw-framework.8.html)
* Ubuntu 19.10 (Eoan Ermine)
  + [ufw manual](http://manpages.ubuntu.com/manpages/eoan/en/man8/ufw.8.html)
  + [ufw framework manual](http://manpages.ubuntu.com/manpages/eoan/en/man8/ufw-framework.8.html)
* Ubuntu 20.04 (Focal Fossa)
  + [ufw manual](http://manpages.ubuntu.com/manpages/focal/en/man8/ufw.8.html)
  + [ufw framework manual](http://manpages.ubuntu.com/manpages/focal/en/man8/ufw-framework.8.html)
* Ubuntu Core
  + See 'ufw.doc' on your Ubuntu Core system, specifically 'ufw.doc ufw-on-snappy | less' to see how ufw differs on Ubuntu Core.
* [Ubuntu Community Documentation on UFW](https://help.ubuntu.com/community/UFW)
* **Specification**: [UbuntuFirewallSpec](https://wiki.ubuntu.com/UbuntuFirewallSpec)
* **Code**: <https://launchpad.net/ufw>
* Graphic User Interface for UFW: [Gufw](https://help.ubuntu.com/community/Gufw).

Uncomplicated Firewall

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#searchInput)

|  |  |
| --- | --- |
| **Uncomplicated Firewall** | |
| [**Stable release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | 0.36-6[[1]](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#cite_note-UcF-Wiki-1) / August 25, 2019; 12 months ago |
| [**Repository**](https://en.wikipedia.org/wiki/Repository_(version_control)) | * [code.launchpad.net/ufw](https://code.launchpad.net/ufw)   [Edit this at Wikidata](https://www.wikidata.org/wiki/Q2577905#P1324) |
| **Written in** | [Python](https://en.wikipedia.org/wiki/Python_(programming_language)) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Linux](https://en.wikipedia.org/wiki/Linux) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License) |
| **Website** | [launchpad.net/ufw](https://launchpad.net/ufw), [manpages.ubuntu.com/manpages/bionic/en/man8/ufw.8.html](https://manpages.ubuntu.com/manpages/bionic/en/man8/ufw.8.html) |

**Uncomplicated Firewall** (**UFW**) is a program for managing a [netfilter](https://en.wikipedia.org/wiki/Netfilter) [firewall](https://en.wikipedia.org/wiki/Firewall_(computing)) designed to be easy to use. It uses a [command-line interface](https://en.wikipedia.org/wiki/Command-line_interface) consisting of a small number of simple commands, and uses [iptables](https://en.wikipedia.org/wiki/Iptables) for configuration. UFW is available by default in all [Ubuntu](https://en.wikipedia.org/wiki/Ubuntu_(operating_system)) installations after 8.04 LTS.[[1]](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#cite_note-UcF-Wiki-1)



**Contents**

* [1GUIs for Uncomplicated Firewall](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#GUIs_for_Uncomplicated_Firewall)
* [2Features](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#Features)
* [3References](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#References)
* [4External links](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#External_links)

GUIs for Uncomplicated Firewall[[edit](https://en.wikipedia.org/w/index.php?title=Uncomplicated_Firewall&action=edit&section=1)]

|  |  |
| --- | --- |
| **Gufw (GUI for Uncomplicated Firewall)** | |
| GUI for Uncomplicated Firewall | |
| [**Original author(s)**](https://en.wikipedia.org/wiki/Software_developer) | Gufw Developers |
| [**Stable release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | [20.04.1-1](https://packages.ubuntu.com/focal/gufw) |
| [**Repository**](https://en.wikipedia.org/wiki/Repository_(version_control)) | * [code.launchpad.net/ufw](https://code.launchpad.net/ufw)   [Edit this at Wikidata](https://www.wikidata.org/wiki/Q2577905#P1324) |
| **Written in** | [Python](https://en.wikipedia.org/wiki/Python_(programming_language)), [PyGObject](https://en.wikipedia.org/wiki/PyGObject) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Linux](https://en.wikipedia.org/wiki/Linux) |
| [**Platform**](https://en.wikipedia.org/wiki/Computing_platform) | [GTK](https://en.wikipedia.org/wiki/GTK) |
| **Available in** | More languages [[1]](https://translations.launchpad.net/gui-ufw) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License) |
| **Website** | [gufw.org](https://gufw.org/) |

|  |  |
| --- | --- |
| **kmyfirewall** | |
| [**Developer(s)**](https://en.wikipedia.org/wiki/Software_developer) | KLajos et al. |
| [**Repository**](https://en.wikipedia.org/wiki/Repository_(version_control)) | * [code.launchpad.net/ufw](https://code.launchpad.net/ufw)   [Edit this at Wikidata](https://www.wikidata.org/wiki/Q2577905#P1324) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Linux](https://en.wikipedia.org/wiki/Linux) |
| [**Platform**](https://en.wikipedia.org/wiki/Computing_platform) | [Qt](https://en.wikipedia.org/wiki/Qt_(framework)) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License) |
| **Website** | [launchpad.net/ufw](https://launchpad.net/ufw) [Edit this on Wikidata](https://www.wikidata.org/wiki/Q2577905?uselang=en#P856) |

|  |  |
| --- | --- |
| **UFW KControl Module** | |
| [**Repository**](https://en.wikipedia.org/wiki/Repository_(version_control)) | * [code.launchpad.net/ufw](https://code.launchpad.net/ufw)   [Edit this at Wikidata](https://www.wikidata.org/wiki/Q2577905#P1324) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Linux](https://en.wikipedia.org/wiki/Linux) |
| [**Platform**](https://en.wikipedia.org/wiki/Computing_platform) | [Qt](https://en.wikipedia.org/wiki/Qt_(framework)) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License) |
| **Website** | [www.linux-apps.com](https://www.linux-apps.com/content/show.php/UFW+KControl+Module?content=137789) |

|  |  |
| --- | --- |
| **UFW Frontends** | |
| [**Original author(s)**](https://en.wikipedia.org/wiki/Software_developer) | Darwin Bautista |
| [**Stable release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | [0.3.2](https://github.com/baudm/ufw-frontends) / 2012; 8 years ago |
| [**Repository**](https://en.wikipedia.org/wiki/Repository_(version_control)) | * [code.launchpad.net/ufw](https://code.launchpad.net/ufw)   [Edit this at Wikidata](https://www.wikidata.org/wiki/Q2577905#P1324) |
| **Written in** | [Python](https://en.wikipedia.org/wiki/Python_(programming_language)), [PyGTK](https://en.wikipedia.org/wiki/PyGTK) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Linux](https://en.wikipedia.org/wiki/Linux) |
| [**Platform**](https://en.wikipedia.org/wiki/Computing_platform) | [PyGTK](https://en.wikipedia.org/wiki/PyGTK) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License) |
| **Website** | [github.com/baudm/ufw-frontends](https://github.com/baudm/ufw-frontends) |

**Gufw** is intended to be an easy, intuitive [graphical user interface](https://en.wikipedia.org/wiki/Graphical_user_interface) for managing Uncomplicated Firewall. It supports common tasks such as allowing or blocking pre-configured, common [P2P](https://en.wikipedia.org/wiki/Peer-to-peer), or individual ports. Gufw has been designed for [Ubuntu](https://en.wikipedia.org/wiki/Ubuntu_(operating_system)), but is also available in [Debian](https://en.wikipedia.org/wiki/Debian)-based distributions and in [Arch Linux](https://en.wikipedia.org/wiki/Arch_Linux); anywhere [Python](https://en.wikipedia.org/wiki/Python_(programming_language)), [GTK](https://en.wikipedia.org/wiki/GTK) and UFW are available.

Features[[edit](https://en.wikipedia.org/w/index.php?title=Uncomplicated_Firewall&action=edit&section=2)]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| [**Netfilter**](https://en.wikipedia.org/wiki/Netfilter)**feature**[[2]](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#cite_note-UB-ufw-2) | **0.16.2 (8.04 LTS)** | **0.30 (10.04 LTS)** | **0.31.1-1 (12.04 LTS)** | **0.34-0 (14.04 LTS)** | **0.35-0 (16.04 LTS)** |
| Default incoming policy (allow/deny) | Yes | Yes | Yes | Yes | Yes |
| Allow/deny incoming rules | Yes | Yes | Yes | Yes | Yes |
| IPv6 | Yes | Yes | Yes | Yes | Yes |
| Status | Yes | Yes | Yes | Yes | Yes |
| Logging (on/off) | Yes | Yes | Yes | Yes | Yes |
| Extensible framework | Yes | Yes | Yes | Yes | Yes |
| Application integration | - | Yes | Yes | Yes | Yes |
| Limit incoming rules (rate limiting) | - | Yes | Yes | Yes | Yes |
| Multiport incoming rules | - | Yes | Yes | Yes | Yes |
| debconf/preseeding | - | Yes | Yes | Yes | Yes |
| Default incoming policy (reject) | - | Yes | Yes | Yes | Yes |
| Reject incoming rules | - | Yes | Yes | Yes | Yes |
| Rule insertion | - | Yes | Yes | Yes | Yes |
| Log levels | - | Yes | Yes | Yes | Yes |
| Per rule logging | - | Yes | Yes | Yes | Yes |
| Outgoing filtering (on par with incoming) | - | Yes | Yes | Yes | Yes |
| Filtering by interface | - | Yes | Yes | Yes | Yes |
| Bash completion | - | Yes | Yes | Yes | Yes |
| Upstart support | - | Yes | Yes | Yes | Yes |
| Improved reporting | - | Yes | Yes | Yes | Yes |
| Reset command | - | Yes | Yes | Yes | Yes |
| rsyslog support | - | Yes | Yes | Yes | Yes |
| Delete by rule number | - | Yes | Yes | Yes | Yes |
| Python 2.6 support | - | - | Yes | Yes | Yes |
| 'show listening' report | - | - | Yes | Yes | Yes |
| Python 2.7 support | - | - | Yes | Yes | Yes |
| Increased protocol support (ah, esp) | - | - | Yes | Yes | Yes |
| IPv6 rate limiting via 'limit' command | - | - | - | Yes | Yes |
| Python 3.2 support | - | - | - | Yes | Yes |
| Python 3.3 support | - | - | - | Yes | Yes |
| 'show added' report | - | - | - | Yes | Yes |
| Python 3.4 support | - | - | - | Yes | Yes |
| Before/after extensibility hooks | - | - | - | Yes | Yes |
| Routed packet filtering (FORWARD) | - | - | - | Yes | Yes |
| [systemd](https://en.wikipedia.org/wiki/Systemd) support | - | - | - | - | Yes |
| Increased protocol support (igmp, gre) | - | - | - | - | Yes |
| Python 3.5 support | - | - | - | - | Yes |
| Snappy for Ubuntu Core support | - | - | - | - | Yes |
| Per rule comments | - | - | - | - | Yes |

References[[edit](https://en.wikipedia.org/w/index.php?title=Uncomplicated_Firewall&action=edit&section=3)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#cite_ref-UcF-Wiki_1-0) [***b***](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#cite_ref-UcF-Wiki_1-1) [*"UncomplicatedFirewall"*](https://wiki.ubuntu.com/UncomplicatedFirewall?action=show&redirect=UbuntuFirewall)*. Ubuntu. Retrieved 26 December 2019.*
  2. [**^**](https://en.wikipedia.org/wiki/Uncomplicated_Firewall#cite_ref-UB-ufw_2-0) [*"UFW in Ubuntu"*](https://wiki.ubuntu.com/UncomplicatedFirewall?action=show&redirect=UbuntuFirewall)*. Ubuntu. Retrieved 21 November 2016.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=Uncomplicated_Firewall&action=edit&section=4)]

* ******[***Free and open-source software portal***](https://en.wikipedia.org/wiki/Portal:Free_and_open-source_software)
* [Ubuntu Firewall – Information about *Uncomplicated Firewall* on Ubuntu](https://wiki.ubuntu.com/UbuntuFirewall)
* [Gufw – Official Gufw website](https://gufw.org/)
* [Gufw – Community Documentation](https://help.ubuntu.com/community/Gufw)

One of the many heralded aspects of Linux is its security. From the desktop to the server, you’ll find every tool you need to keep those machines locked down as tightly as possible. For the longest time, the security of Linux was in the hands of iptables (which works with the underlying *netfilter* system). Although incredibly powerful, iptables is complicated—especially for newer users. To truly make the most out of that system, it may take weeks or months to get up to speed. Thankfully, a much simpler front end for iptables is ready to help get your system as secure as you need.

That front end is Uncomplicated Firewall (UFW). UFW provides a much more user-friendly framework for managing netfilter and a command-line interface for working with the firewall. On top of that, if you’d rather not deal with the command line, UFW has a few GUI tools that make working with the system incredibly simple.

But, before we find out what GUI tools are available, it’s best to understand how the UFW command-line system works.

Working with the Command

The fundamental UFW command structure looks like this:

ufw [--dry-run] [options] [rule syntax]

Notice the *–dry-run* section. UFW includes the ability to include this argument which informs the command to not make any changes. Instead, you will see the results of your changes in the output.

As for working with the command, UFW can be used in two ways:

* Simple syntax: Specifies a port and (optionally) the protocol
* Full syntax: Specifies source, destination, port, and (optionally) the protocol

Let’s look at the simple syntax first. Say, for example, you want to allow traffic on port 22 (SSH). To do this with UFW, you’d run a command like:

sudo ufw allow 22

NOTE: I added sudo to the command because you must have admin privileges to run *ufw*. If you’re using a distribution that doesn’t take advantage of sudo, you’d first have to *su* to root and then run the same command (minus *sudo*).

Conversely, say you want to prevent traffic on port 22. To do this, the command would look like:

sudo ufw deny 22

Should you want to add a protocol to this, the command would look like:

sudo ufw deny 22/tcp

What happens if you don’t happen to know the port number for a service? The developers have taken that into consideration. UFW will run against /etc/services in such a way that you can define a rule using a service instead of a port. To allow SSH traffic, that command would look like:

sudo ufw allow ssh

Pretty simple, right? You can also add protocols to the above command, in the same way you did when defining a rule via port number.

sudo ufw allow ssh/tcp

Of the available arguments, the ones you’ll use the most with the *ufw* command are:

* allow
* deny
* reject
* limit
* status: displays if the firewall is active or inactive
* show: displays the current running rules on your firewall
* reset: disables and resets the firewall to default
* reload: reloads the current running firewall
* disable: disables the firewall

If you want to use a fuller syntax, you can then begin to define a source and a destination for a rule. Say, for example, you have an IP address you’ve discovered has been attempting to get into your machine (for whatever reason) through port 25 (SMTP). Let’s say that address is 192.168.2.100 (even though it’s an internal address) and your machine address is 192.168.2.101. To block that address from gaining access (through any port), you could create the rule like so:

sudo ufw deny from 192.168.2.100/8 to 192.168.2.101 port 25

Let’s look at the*limit* option. If you have any reason for concern that someone might be attempting a denial of service attack on your machine, via port 80. You can limit connections to that port with UFW, like so:

sudo ufw limit 80/tcp

By default, the connection will be blocked after six attempts in a 30-second period.

You might also have a need to allow outgoing traffic on a certain port but deny incoming traffic on the same port. To do this, you would use the directional argument like so. To allow outgoing traffic on port 25 (SMTP), issue the command:

sudo ufw allow out on eth0 to any port 25 proto tcp

You could then add the next rule to block incoming traffic on the same interface and port:

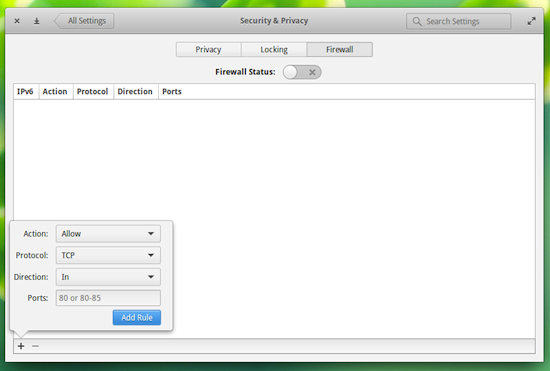
sudo ufw deny in on eth0 from any 25 proto tcp

GUI Tools

Now that you understand the basics of UFW, it’s time to find out what GUI tools are available to make using this handy firewall even easier. There aren’t many which are actively maintained, and many distributions default to one in particular. That GUI is…

[Gufw](http://gufw.org/) is one of the most popular GUI front ends for UFW. It’s available for Ubuntu, Linux Mint, openSUSE, Arch Linux, and Salix OS. With Gufw, you can easily create profiles to match different uses for a machine (home, public, office, etc.). As you might expect from such a tool, Gufw offers an interface that would make any level of user feel right at home (see Figure 1 above).

Some distributions, such as Ubuntu, don’t install Gufw by default. You will, however, find it in the Ubuntu Software Center. Search for gufw and install with a single click.

If your distribution happens to be [Elementary OS Freya](https://elementary.io/), there’s a new front end for UFW built into the settings tool that allows you to very easily add rules to UFW (Figure 2). You can learn more about the Elementary OS Freya UFW front end from my post “[Get to Know the Elementary OS Freya Firewall Tool](https://www.linux.com/learn/tutorials/853923-get-to-know-the-elementary-os-freya-firewall-tool).”

You might also come across another front end called ufw-frontends. That particular GUI hasn’t been in developed for some time now, so it’s best to avoid that particular app.

For most users, there is no need to spend the time learning iptables—not when there’s a much more user-friendly front end (that also happens to include solid GUI tools) that’ll get the job done. Of course, if you’re looking for business- or enterprise-class firewalling, you should certainly spend the time and effort to gain a full understanding of iptables.

Which is right for your needs, UFW or iptables?