howtogeek.com

How to Configure Ubuntu's Built-In Firewall

By Chris Hoffman on May 29th, 2012

https://www.howtogeek.com/115116/how-to-configure-ubuntus-built-in-firewall/

Ubuntu includes its own firewall, known as ufw – short for "uncomplicated firewall." Ufw is an easier-to-use frontend for the standard Linux iptables commands. You can even control ufw from a graphical interface.

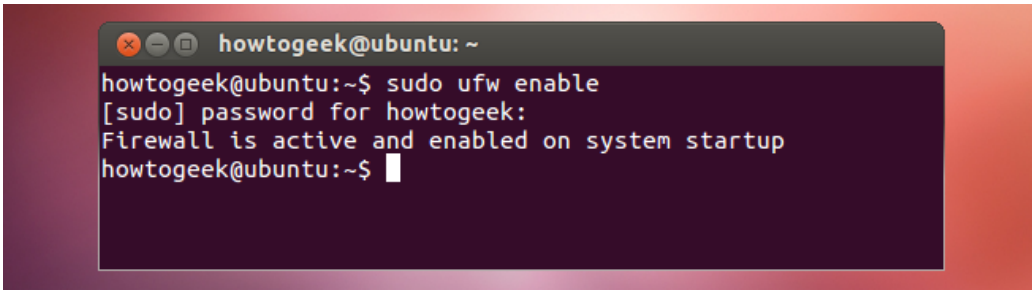
Ubuntu's firewall is designed as an easy way to perform basic firewall tasks without learning iptables. It doesn't offer all the power of the standard iptables commands, but it's less complex.

Terminal Usage

The firewall is disabled by default. To enable the firewall, run the following command from a terminal:

```
sudo ufw enable
```

You don't necessarily have to enable the firewall first. You can add rules while the firewall is offline, and then enable it after you're done configuring it.



Working With Rules

Let’s say you want to allow SSH traffic on port 22. To do so, you can run one of several commands:

sudo ufw allow 22 (Allows both TCP and UDP traffic – not ideal if UDP isn’t necessary.)

sudo ufw allow 22/tcp (Allows only TCP traffic on this port.)

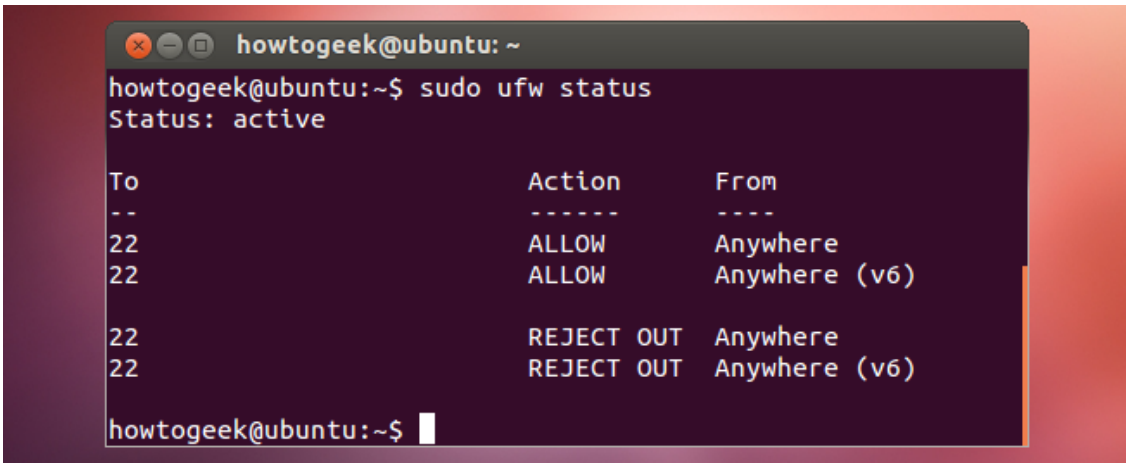
sudo ufw allow ssh (Checks the /etc/services file on your system for the port that SSH requires and allows it. Many common services are listed in this file.)

Ufw assumes you want to set the rule for incoming traffic, but you can also specify a direction. For example, to block outgoing SSH traffic, run the following command:

sudo ufw reject out ssh

You can view the rules you’ve created with the following command:

sudo ufw status



To delete a rule, add the word delete before the rule. For example, to stop rejecting outgoing ssh traffic, run the following command:

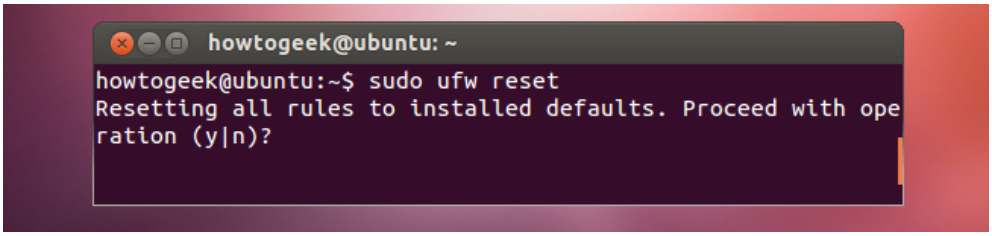
sudo ufw delete reject out ssh

Ufw’s syntax allows for fairly complex rules. For example, this rule denies TCP traffic from the IP 12.34.56.78 to port 22 on the local system:

sudo ufw deny proto tcp from 12.34.56.78 to any port 22

To reset the firewall to its default state, run the following command:

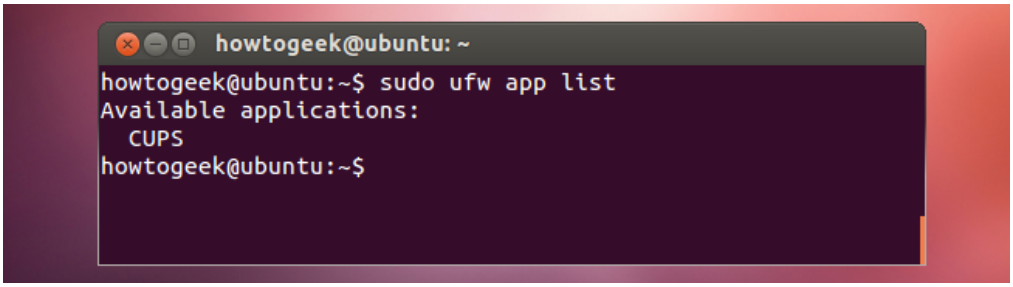
sudo ufw reset



Application Profiles

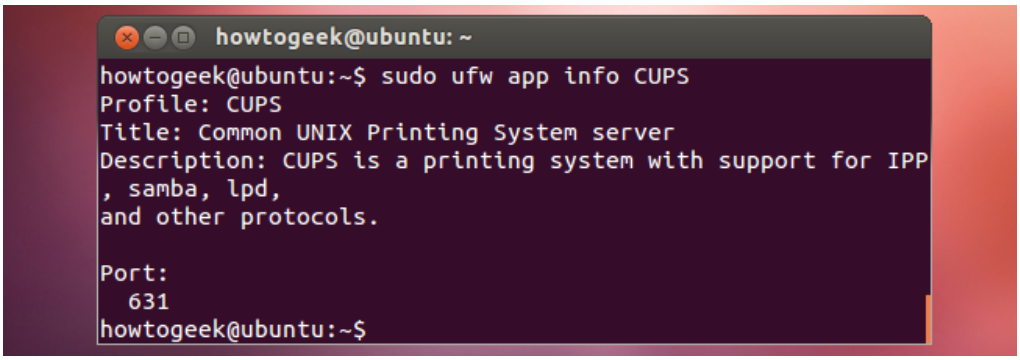
Some applications requiring open ports come with ufw profiles to make this even easier. To see the application profiles available on your local system, run the following command:

sudo ufw app list



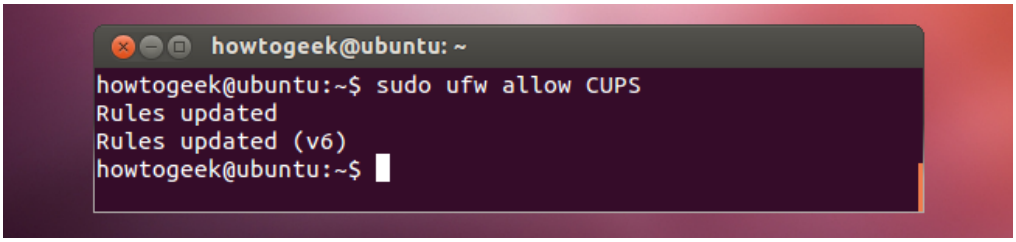
View information about a profile and its included rules with the following command:

sudo ufw app info Name



Allow an application profile with the allow command:

sudo ufw allow Name



More Information

Logging is disabled by default, but you can also enable logging to print firewall messages to the system log:

```
sudo ufw logging on
```

For more information, run the **man ufw** command to read ufw's manual page.

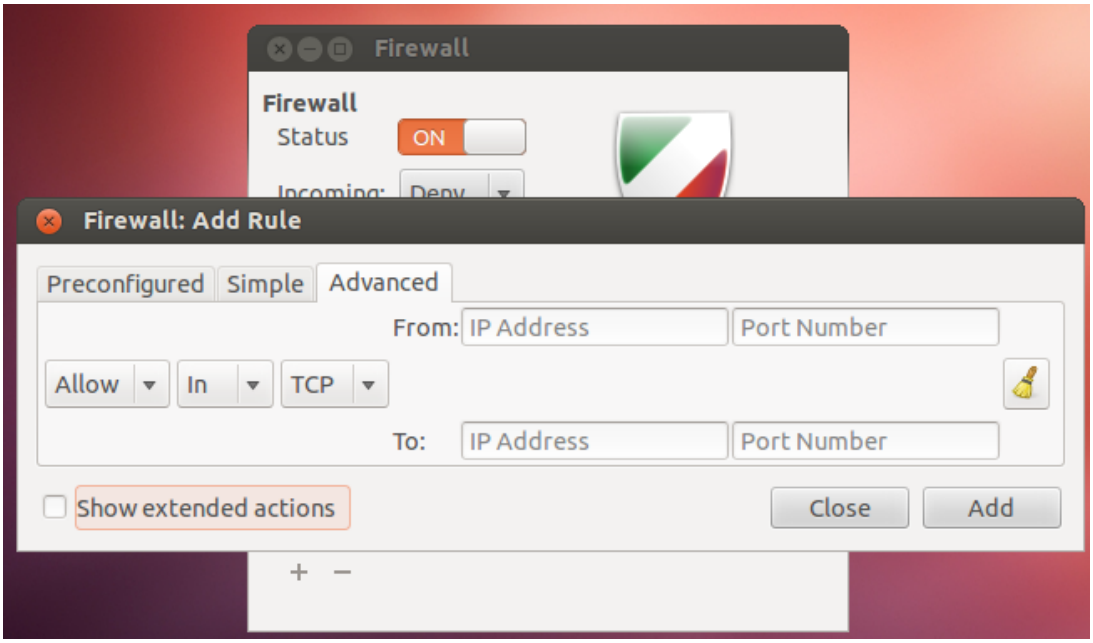
GUFW Graphical Interface

GUFW is a graphical interface for ufw. Ubuntu doesn't come with a graphical interface, but gufw is included in Ubuntu's software repositories. You can install it with the following command:

```
sudo apt-get install gufw
```

GUFW appears in the Dash as an application named Firewall Configuration. Like ufw itself, GUFW provides a simple, easy-to-use interface. You can easily enable or disable the firewall, control the default policy for inbound or outbound traffic, and add rules.

The rules editor can be used to add simple rules or more complicated ones.



Remember, you can’t do everything with ufw – for more complicated firewall tasks, you’ll have to get your hands dirty with iptables.