

- [Partners](#)
- [Support](#)
- [Community](#)
- [Ubuntu.com](#)
- [Page History](#)
- [Login to edit](#)

Gufw

[English](#)[Español](#)[Français](#)[Deutsch](#)[Italiano](#)[Россию](#)

Introduction



Gufw is a firewall powered by UFW (Uncomplicated Firewall). For an overview of firewalls, please see Firewall.

Installation

Contents

1. Introduction
2. Installation
3. Usage
 1. Enabling

In order to install Gufw, you must have the Universe repository enabled. To install, use Synaptic, or run from Terminal:

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

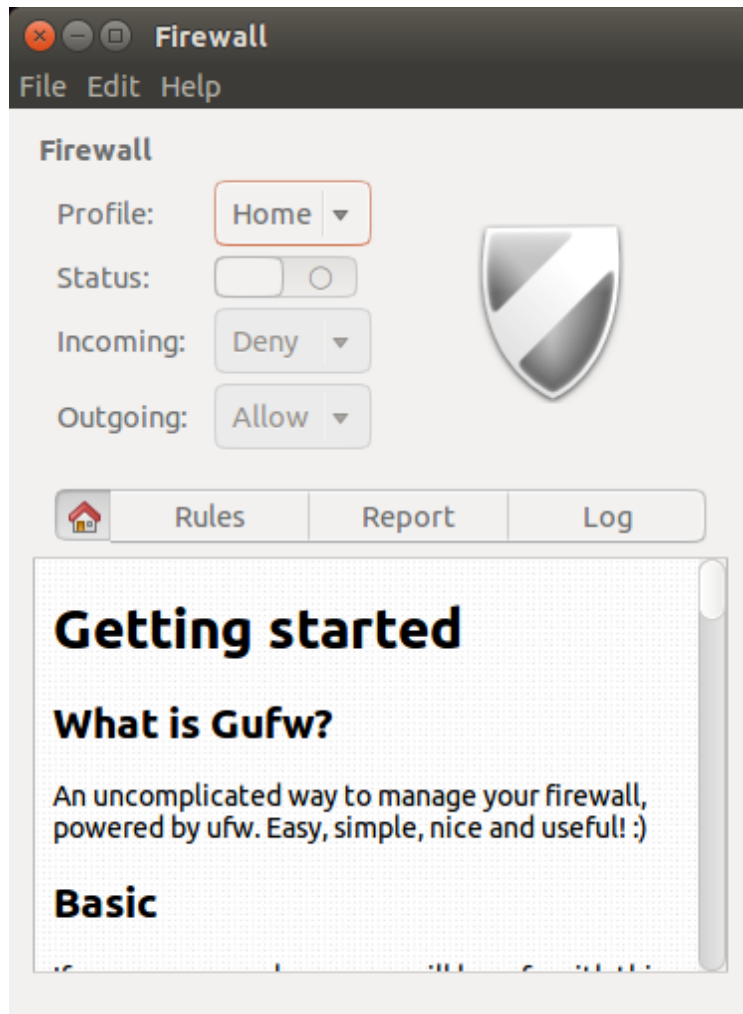
Usage



To access GUFW, go to
System->Administration->Firewall configuration.

By default, the firewall is disabled.

- 2. Adding Rules
- 4. Preferences
- 5. Use Gufw without Graphical Environment or Remote Computer
 - 1. Requirements
 - 2. How use it
- 6. Enable IP forwarding
 - 1. Requirements
 - 2. How use set it
- 7. Other Resources
 - 1. General
 - 2. Online Great (Updated) Tutorials in this language



Enabling

To enable the firewall, simply check the **Enabled** button and the default will be set to **Deny** for incoming traffic and **Allow** for outgoing traffic.



Adding Rules

To configure the firewall, we add rules. Simply click the **Add** button and a new window will pop up. For details about this implementation, see the UFW page. Rules can be configured for TCP and UDP ports,

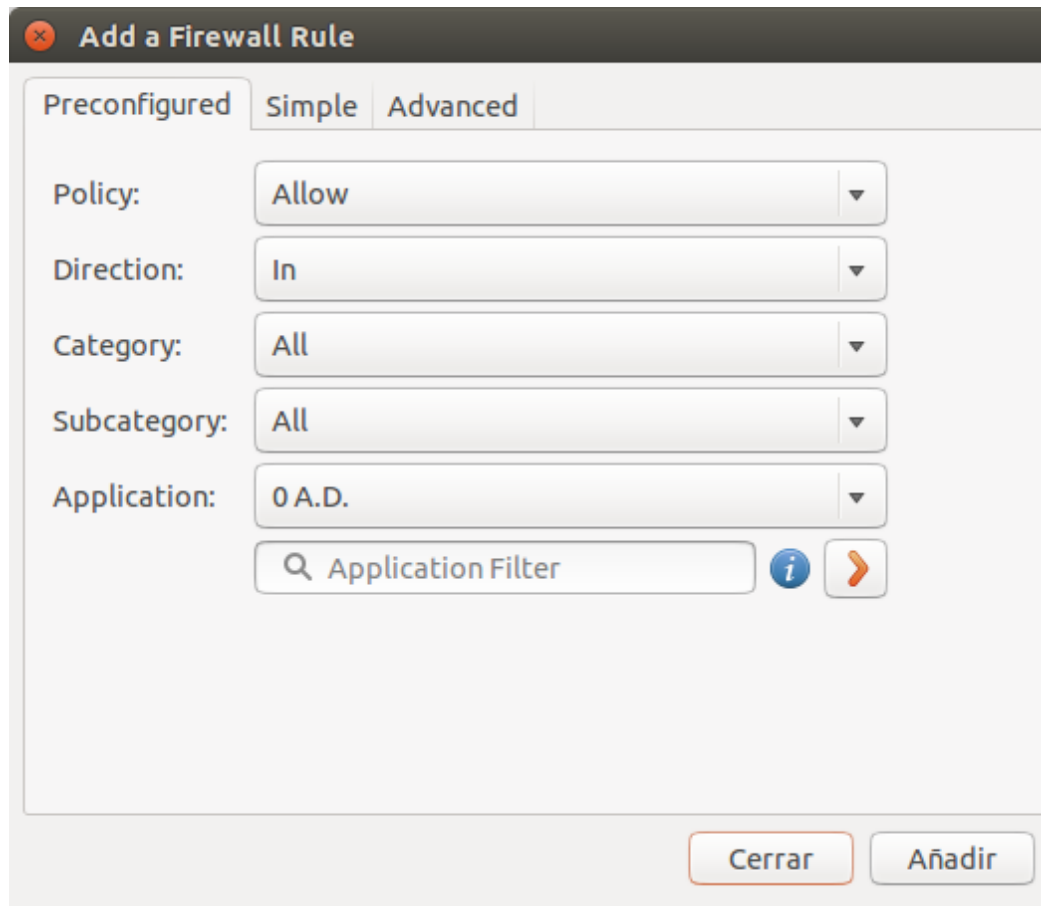
and UFW has some preconfigured programs/services to make setting up rules for them easy.

The available options for rules are *Allow*, *Deny*, *Reject*, and *Limit*:

- Allow: The system will allow entry traffic for a port.
- Deny: The system will deny entry traffic to a port.
- Reject: The system will deny entry traffic to a port and will inform the requesting for connection system that it has been rejected.
- Limit: The system will deny connections if an IP address has attempted to initiate 6 or more connections in the last 30 seconds.

Preconfigured

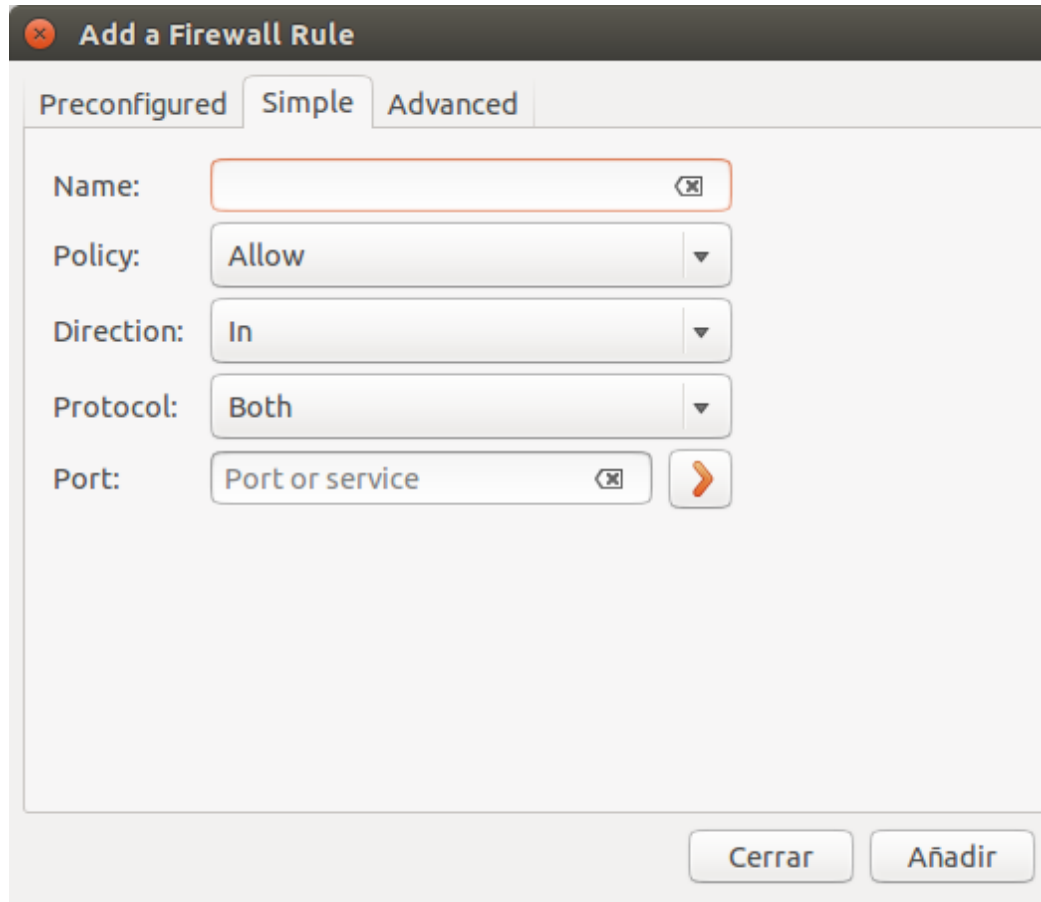
The **Preconfigured** tab gives us some options for controlling firewall options for common programs and services.



You have several categories and subcategories. You can filter by name/description/ports too.

Simple

Not all program configurations are available in Gufw, but we can still add rules for them using the **Simple** tab.



Add a Firewall Rule

Preconfigured Simple Advanced

Name:

Policy: Allow

Direction: In

Protocol: Both

Port: Port or service

Cerrar Añadir

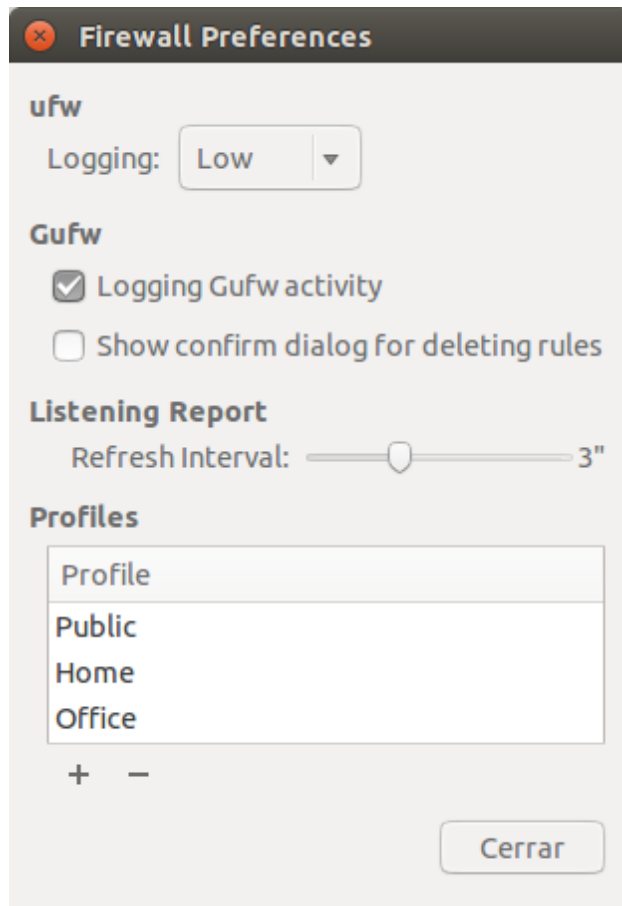
Again, we'll use the SSH example - let's just pretend for a moment that there isn't a preconfigured option for it. To enable it in the **Simple** tab, select "Allow", "TCP", "22" and click **Add**.

Advanced

Sometimes we want to configure access based on a specific IP, so we use the **Advanced** tab.

Preferences

There are a few preferences available to set in Gufw, and can be controlled from **Edit->Preferences**



Here you can control logging for ufw and for Gufw, create profiles and set general interface preferences. The default is to enable logging for ufw, and disable logging for Gufw.

Use Gufw without Graphical Environment or Remote Computer

Requirements

You can use Gufw in a Linux without Graphical Environment (for example an Ubuntu Server) or from a remote computer. You will need **Gufw 13.10.2 or higher**. Just export your X Display. All the operations in Gufw will be apply in the remote computer.

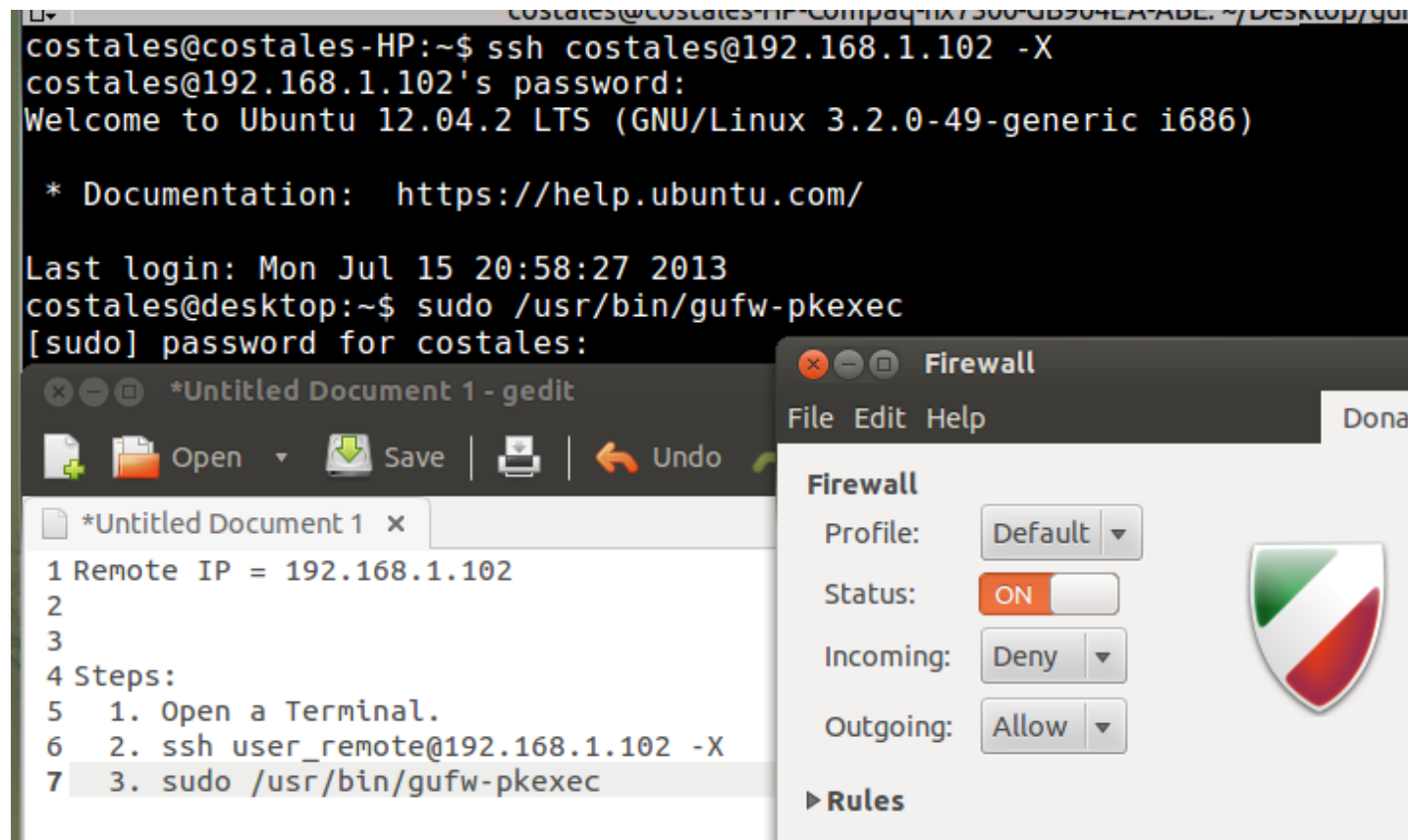
How use it

Important: If you enable the firewall under ssh without the ssh rule, you'll close the ssh connection, then before to enable Gufw under a ssh connection, append the ssh rule using ufw with this command:

```
sudo ufw enable ssh
```

- From a local computer with Linux:
 - Remote computer without graphic environment (IP = 192.168.1.102, Gufw installed and ssh server).
 - Local Linux. In the local computer, open a Terminal and run this command:

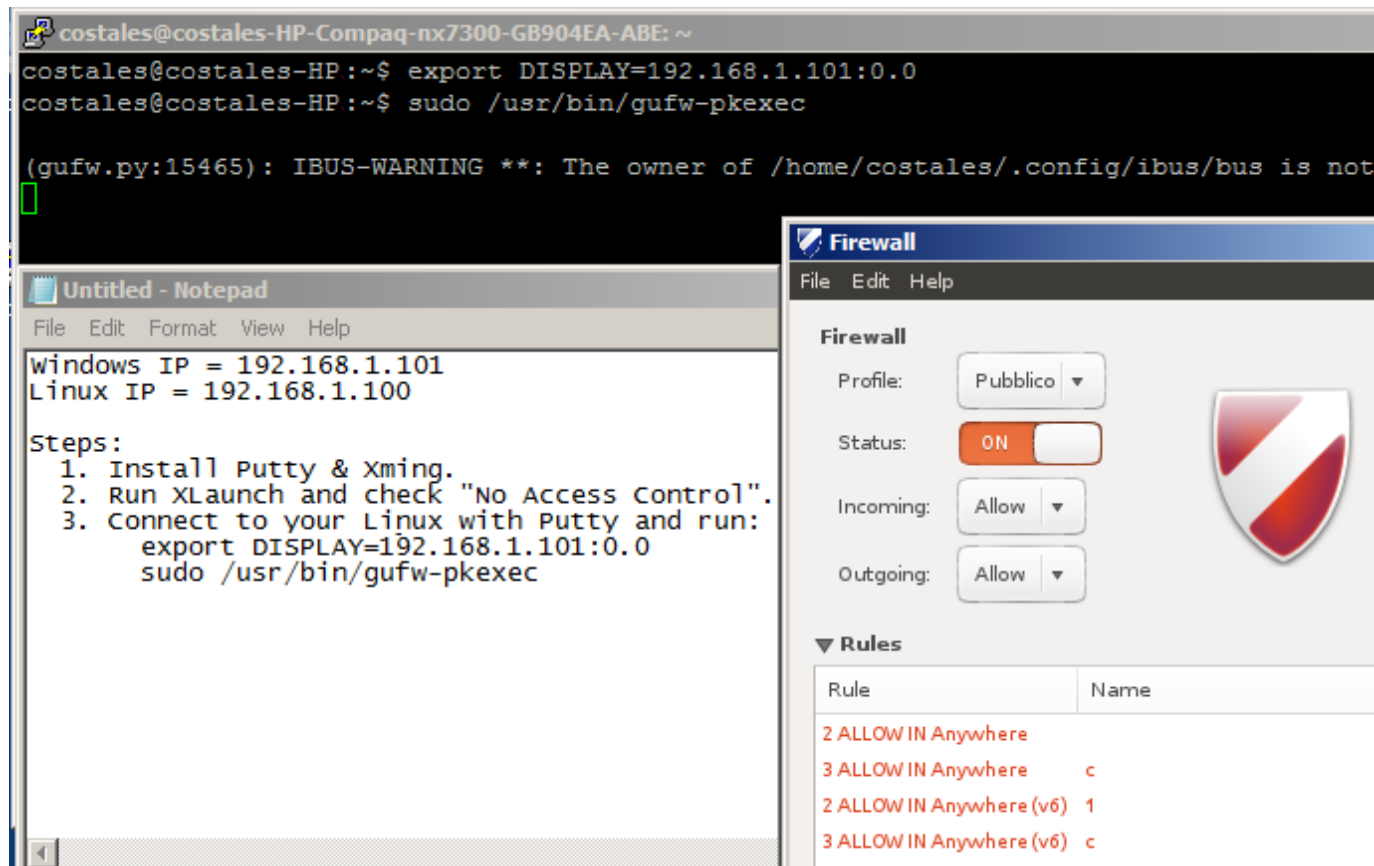
```
ssh user_remote@192.168.1.102 -X  
sudo /usr/bin/gufw-pkexec -ssh
```



- From a local computer with Windows:
 - Windows IP = 192.168.1.101; Linux IP = 192.168.1.100
 - Install Putty & Xming.
 - In Windows: Run XLaunch from the Start Menu and check "No Access Control" in the last step.
 - Connect to your Linux with Putty and run:

```
export DISPLAY=192.168.1.101:0.0
```

```
sudo /usr/bin/gufw-pkexec -ssh
```



Enable IP forwarding

Requirements

Gufw 14.10 or higher.

How use set it

To routing policy and rules, you must setup IP forwarding in the system:

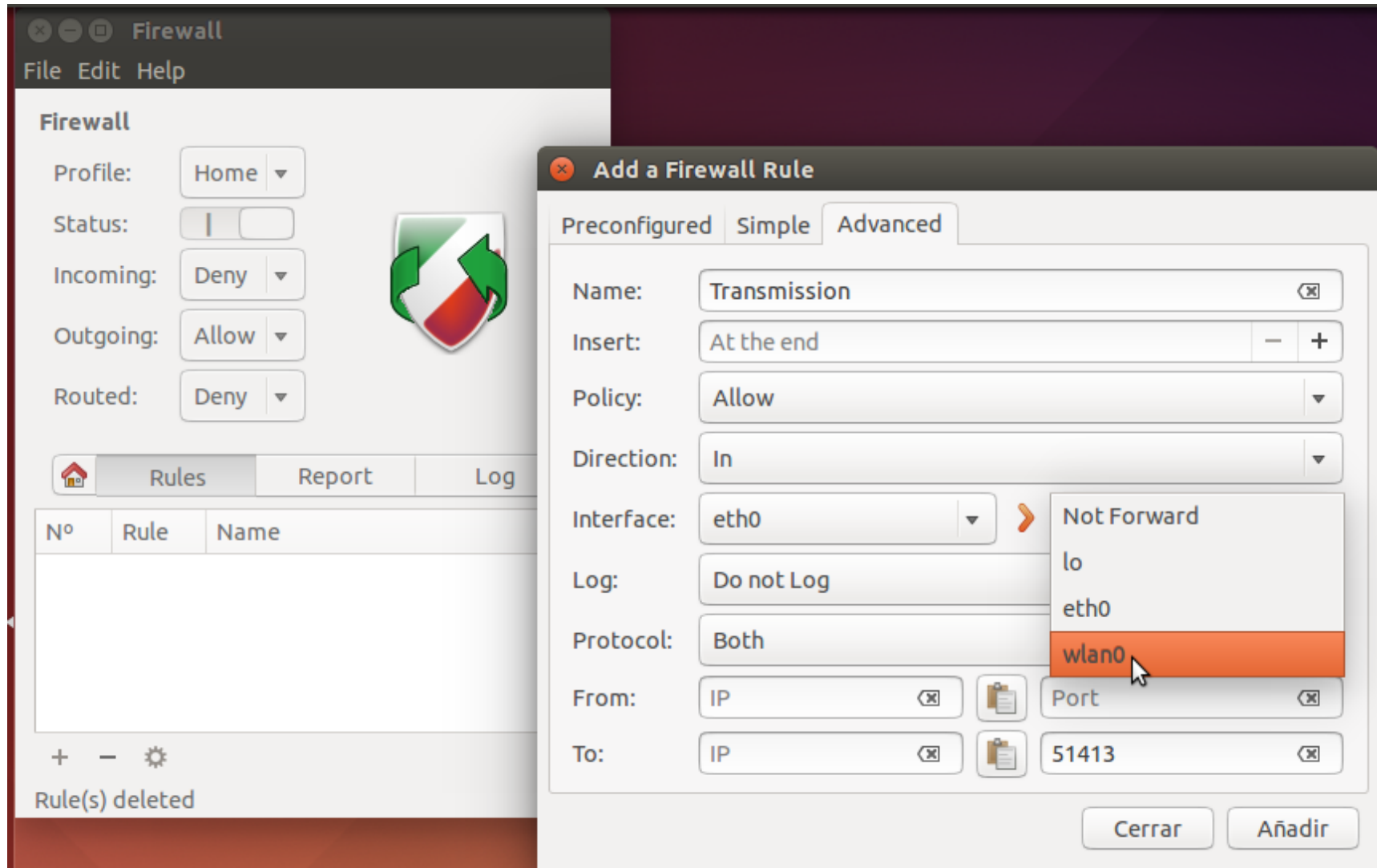
- Close Gufw
- Uncomment these 3 lines in the file `/etc/ufw/sysctl.conf`:

```
#net/ipv4/ip_forward=1
#net/ipv6/conf/default/forwarding=1
#net/ipv6/conf/all/forwarding=1
```

- Reload the firewall:

```
sudo ufw reload
```

Open Gufw, you'll see a new "Routed" option (with an arrow around the shield) and you can forward any rule from the Update window or Advanced Tab in Add window.



Other Resources

General

- Basic security
- Why is the firewall disabled by default?
- Do I need a Firewall for Ubuntu?
- Firewall
- UFW
- Ubuntu:UbuntuFirewall - UFW homepage
- <http://gufw.org> - Gufw homepage

Online Great (Updated) Tutorials in this language

- Gufw 11.04:
 - Using gufw to Configure an Ubuntu Firewall
 - Linux.com.
- Gufw 10.04:
 - Shadows of epiphany.

CategoryNetworking CategorySecurity

Gufw (last edited 2014-07-27 16:33:38 by costales @

din-184-171-231-77.ipcom.comunitel.net[77.231.171.184]:costales)