

MANUAL DE CONFIGURACIÓN DE SERVIDOR PROXY CON FIREWALL

Administración de Servicios en Red

Integrates:

Campos Gómez Fernanda Ivette

Hernández López César Erick

Ruiz Pérez Alejandro

EQUIPO 5

# 

[**INTRODUCCIÓN**](#_vc2d9mbcfn7l) **2**

[**SQUID**](#_i5qmc4uqyj57) **2**

[**SQUIDGUARD**](#_1bvrmuou18by) **4**

[**SHOREWALL**](#_9k9zesi2eza5) **6**

[**OBSERVIUM**](#_3izoovor8ji) **10**

[**CLIENTES**](#_6t03vqxmztsi) **16**

[Cliente IOS](#_nvxozw2pd3ef) 16

[CLIENTE ANDROID](#_3fy7fitcl8l) 18

[CLIENTE FIREFOX](#_p7taeuohfx69) 18

[CLIENTE WINDOWS](#_i5ucn7v2pwj3) 19

# 

# INTRODUCCIÓN

En este manual se explica la forma de configuración del servidor proxy Squid, así como su extensión SquidGuard; la configuración sobre filtrado de direcciones URL y el redireccionamiento. Además, se explica la configuración de Shorewall como firewall de dos interfaces de red, las distintas reglas implementadas y cada uno de los archivos necesarios.

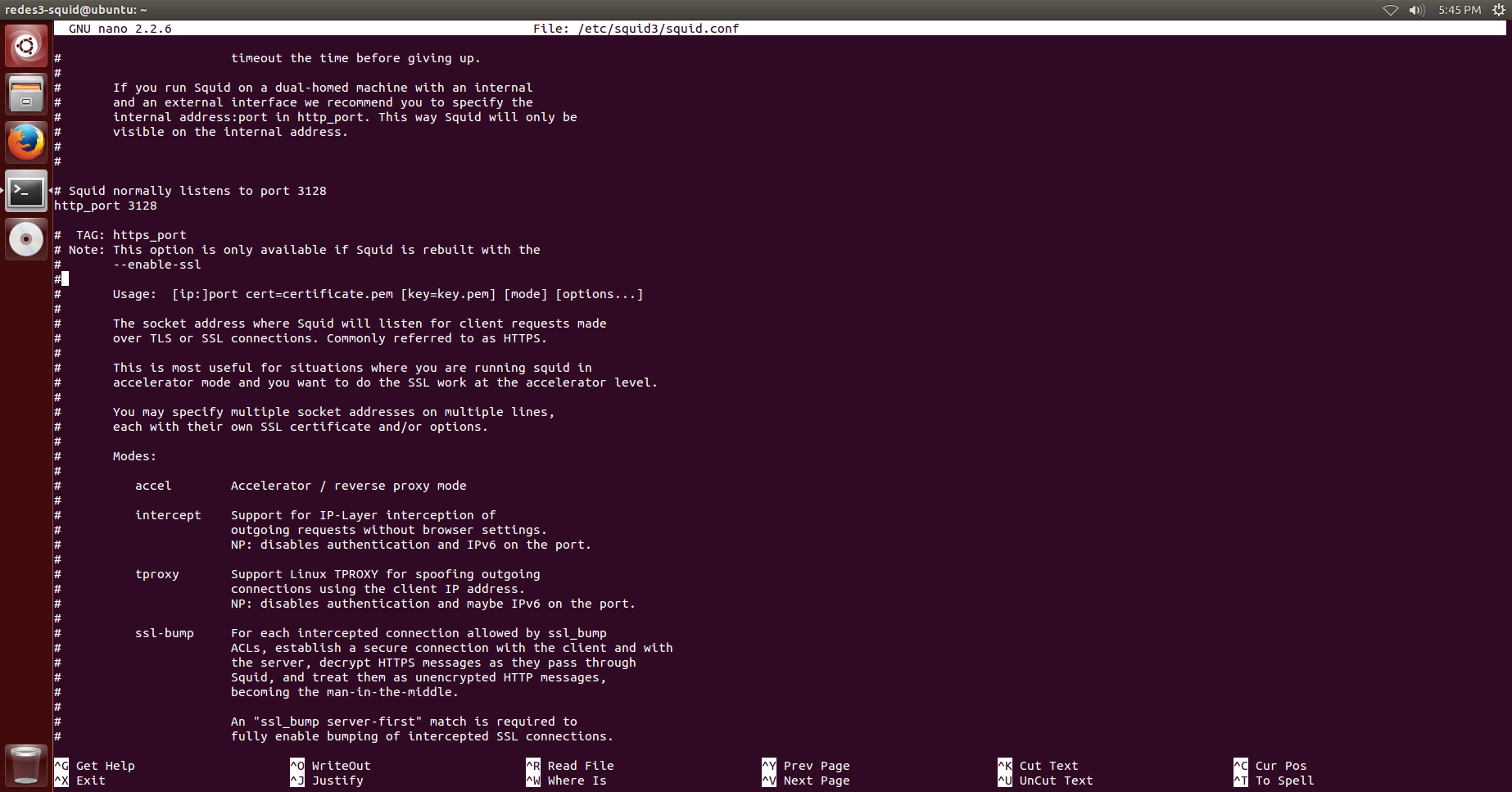
También se agrega la configuración de Observium para monitoreo de las interfaces de red, así como algunas gráficas que ejemplifican el monitoreo.

Se anexan los ajustes correspondientes en distintos clientes para el uso del Proxy antes mencionado.

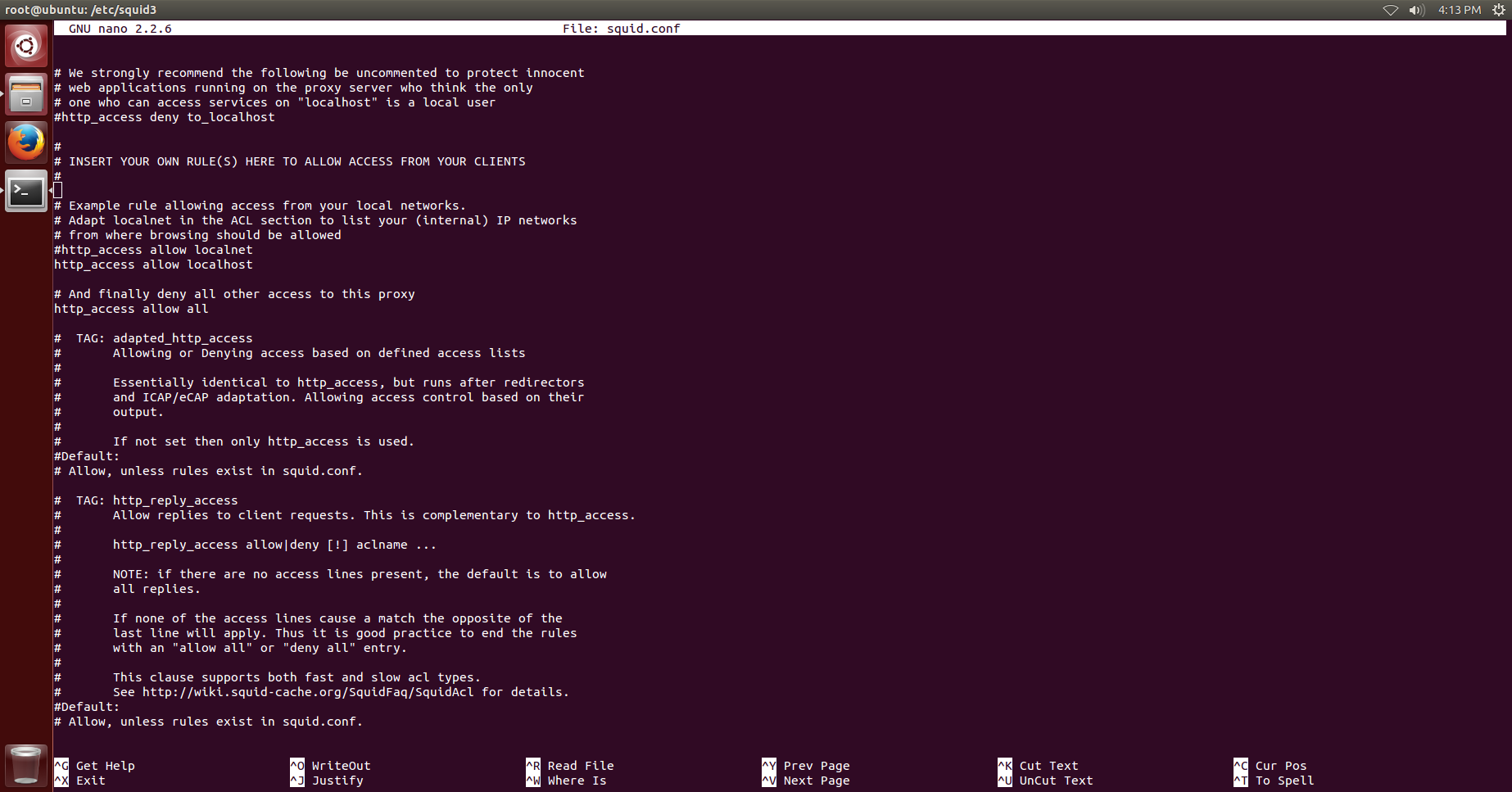
# SQUID

El archivo para la configuración de squid por defecto se encuentra en /etc/squid3/squid.conf

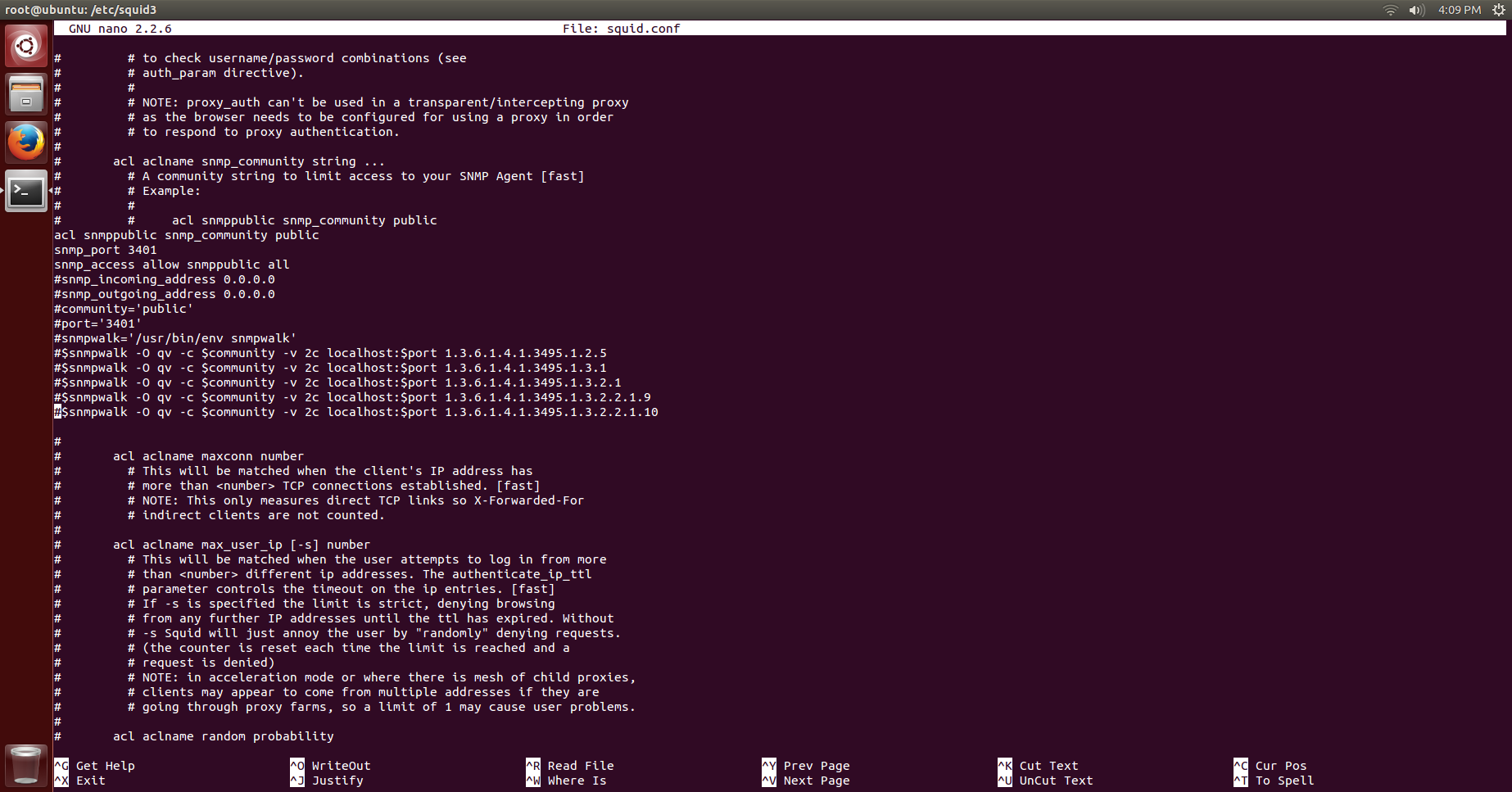
1. Configuramos el puerto en el que desamos que Squid escuche las peticiones, por defecto es el 3128.



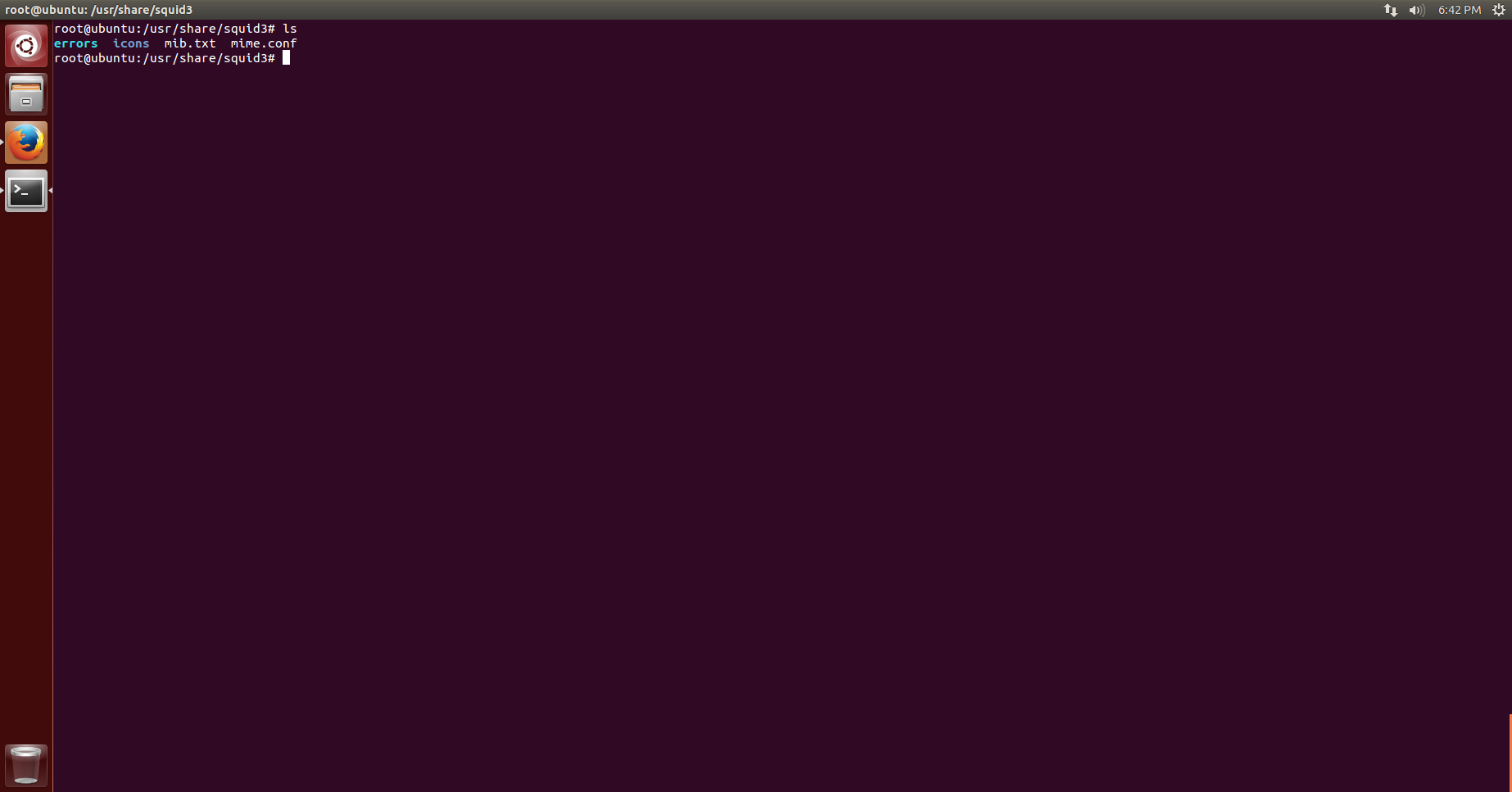
1. De las peticiones http indicamos cuáles deseamos permitir.



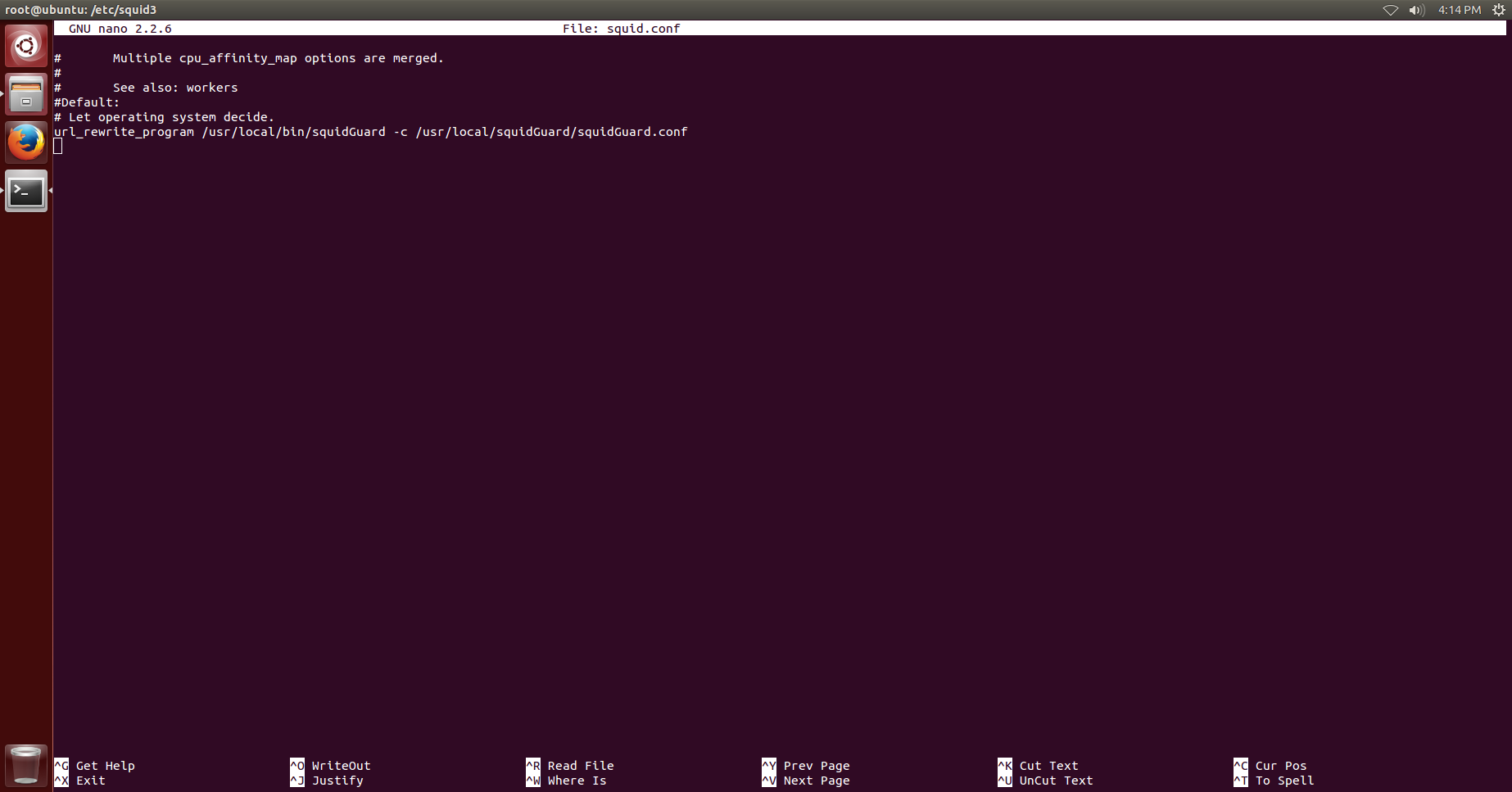
1. Indicamos la configuración para SNMP, la comunidad y el puerto.



1. En la ruta */usr/share/squid3/* podemos encontrar los OIDs dentro del archivo mib.txt



1. Al final del archivo agregamos la siguiente línea para redirigir el tráfico a SquidGuard y que siga las reglas.



# SQUIDGUARD

Instalar blacklist para filtrar contenido visitado

1. Descargamos la lista negra que deseamos usar y la descomprimimos

*sudo wget* [*http://www.shallalist.de/Downloads/shallalist.tar.gz*](http://www.shallalist.de/Downloads/shallalist.tar.gz)

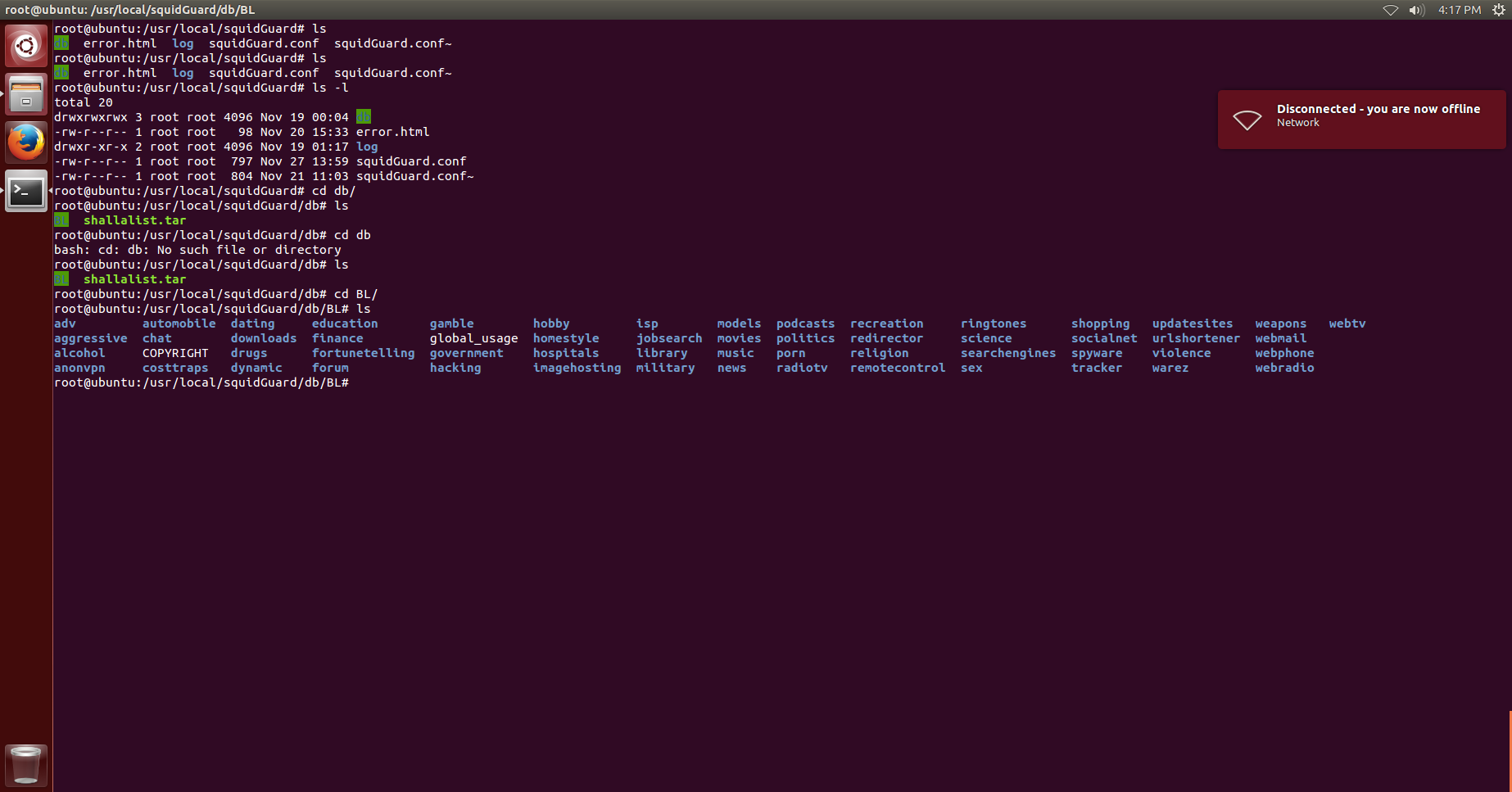
1. Dentro de la carpeta ejecutamos los siguientes comandos para que los archivos obtengan el formato deseado, que es db

*squidGuard -C all  
chown -R <squiduser> /usr/local/squidGuard/db/\**

Normalmente el squiduser es *proxy.*

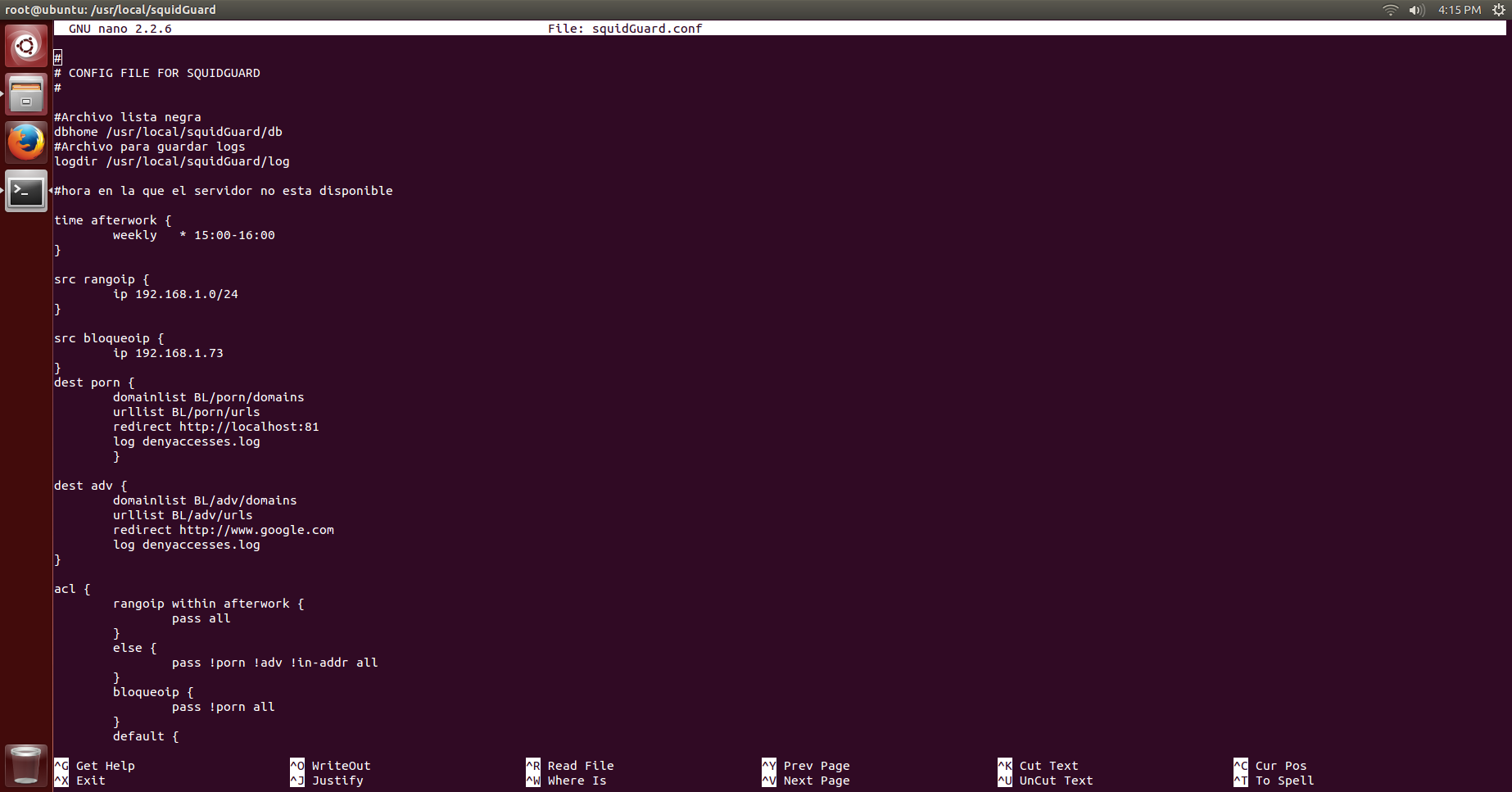


La lista que descargamos tiene algunas categorías para filtrar por defecto

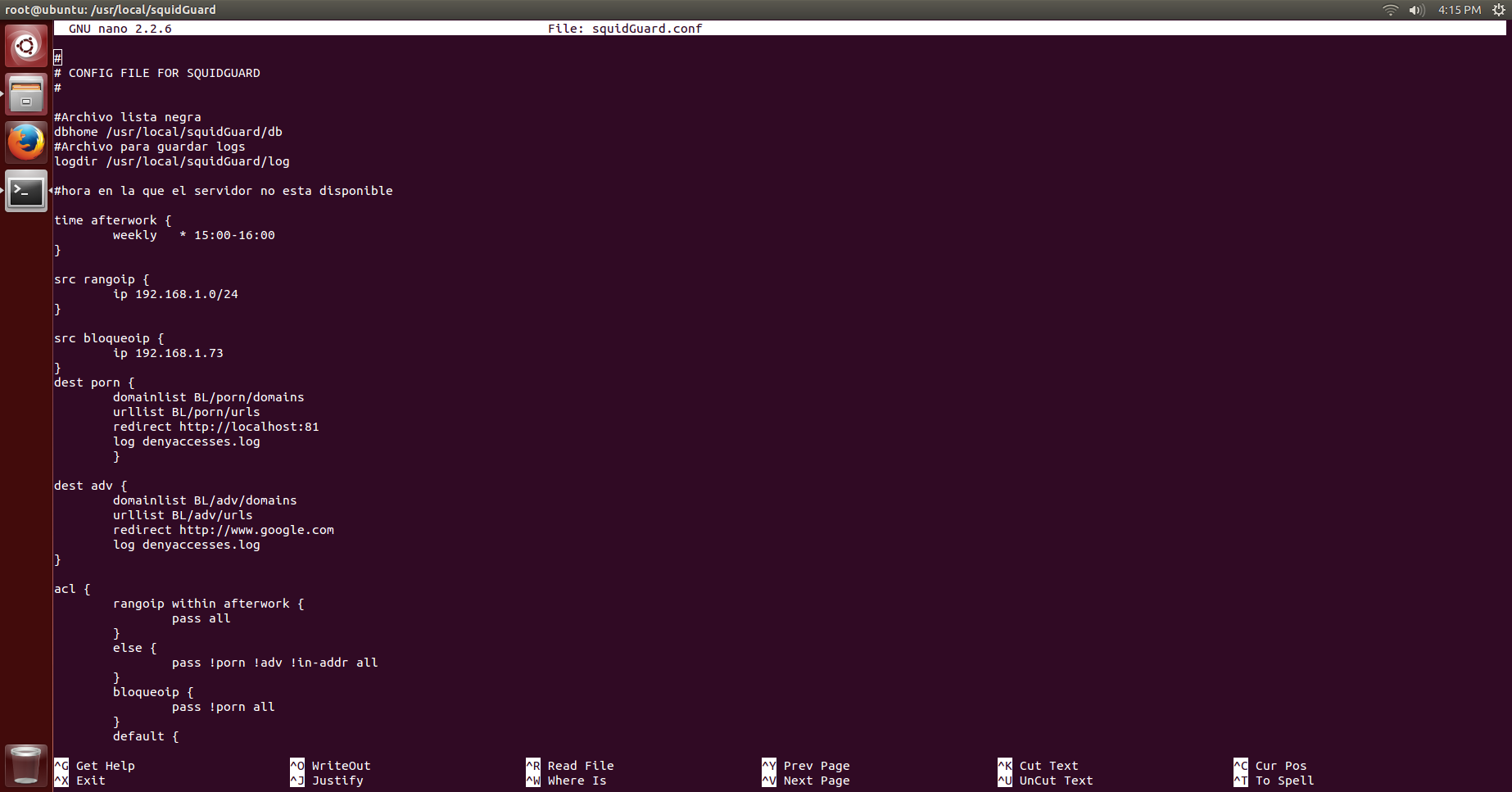


Dentro del archivo de configuración de squuidGuard, ubicado en /usr/local/squidGuard/squidGuard.conf

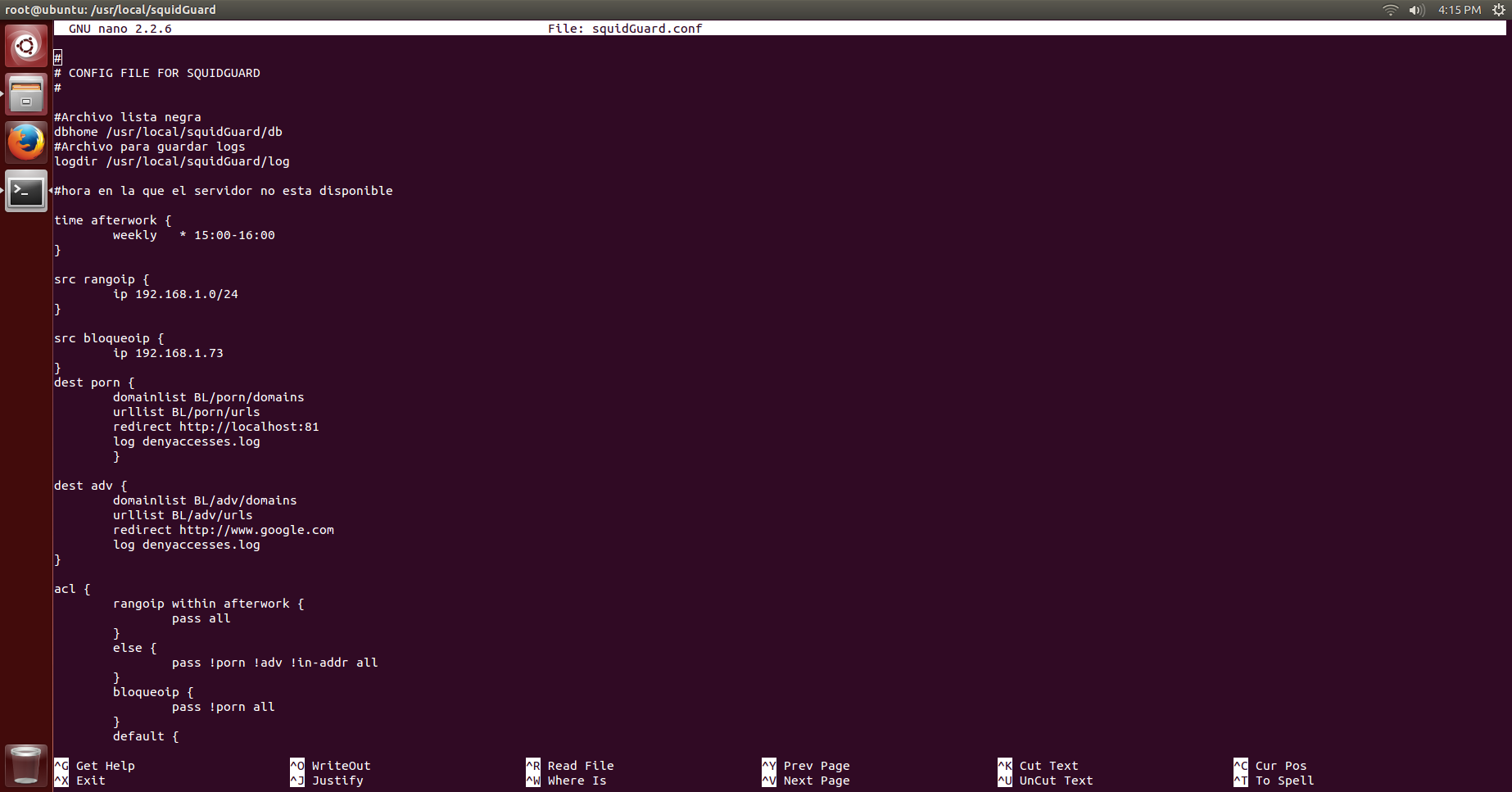
1. Indicamos la ruta de los archivos de lista negra y donde deseamos que se almacenen los logs respectivamente.



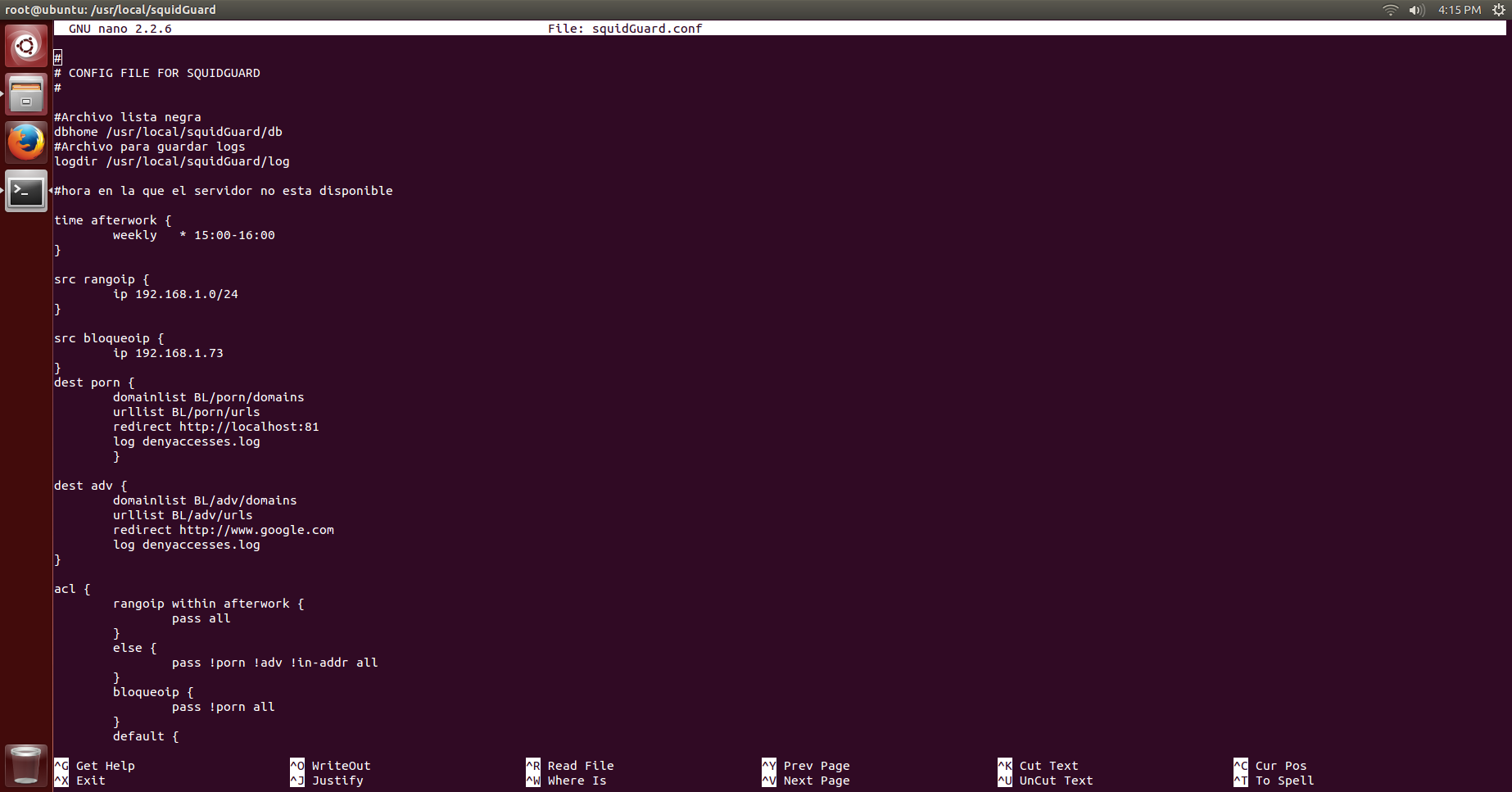
1. Podemos filtrar los accesos por tiempo con la etiqueta *time*



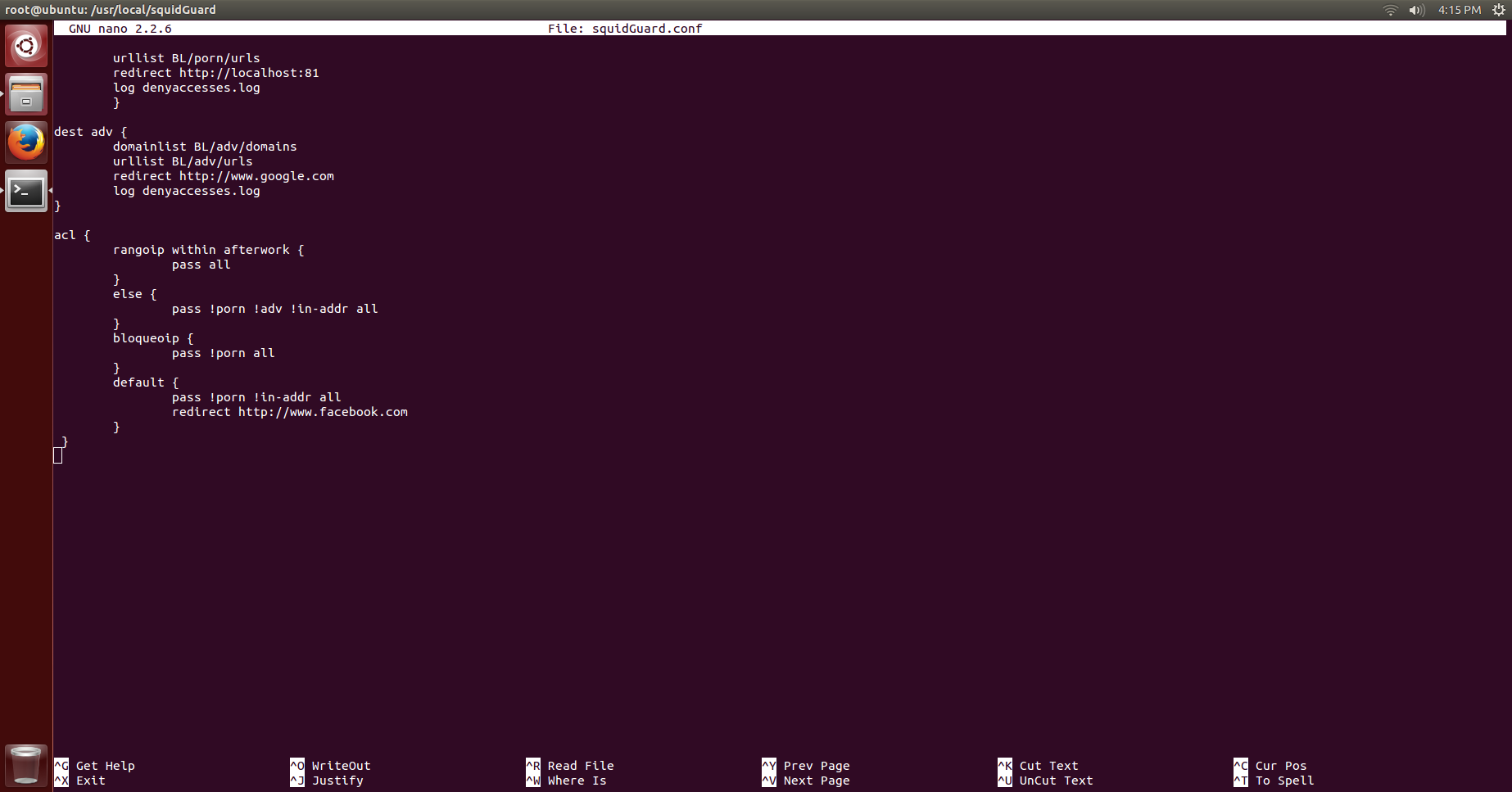
1. Podemos filtrar el acceso por rango de IP o por una IP en específico



1. Indicamos las categorías que deseamos bloquear, en éste caso serán *porn*  y *adv*, indicamos el archivo que corresponde a las URL y a los dominios, podemos indicar un archivo específico de logs para ver quién accedió a esa categoría y hacia a dónde deseamos redirigir el tráfico.

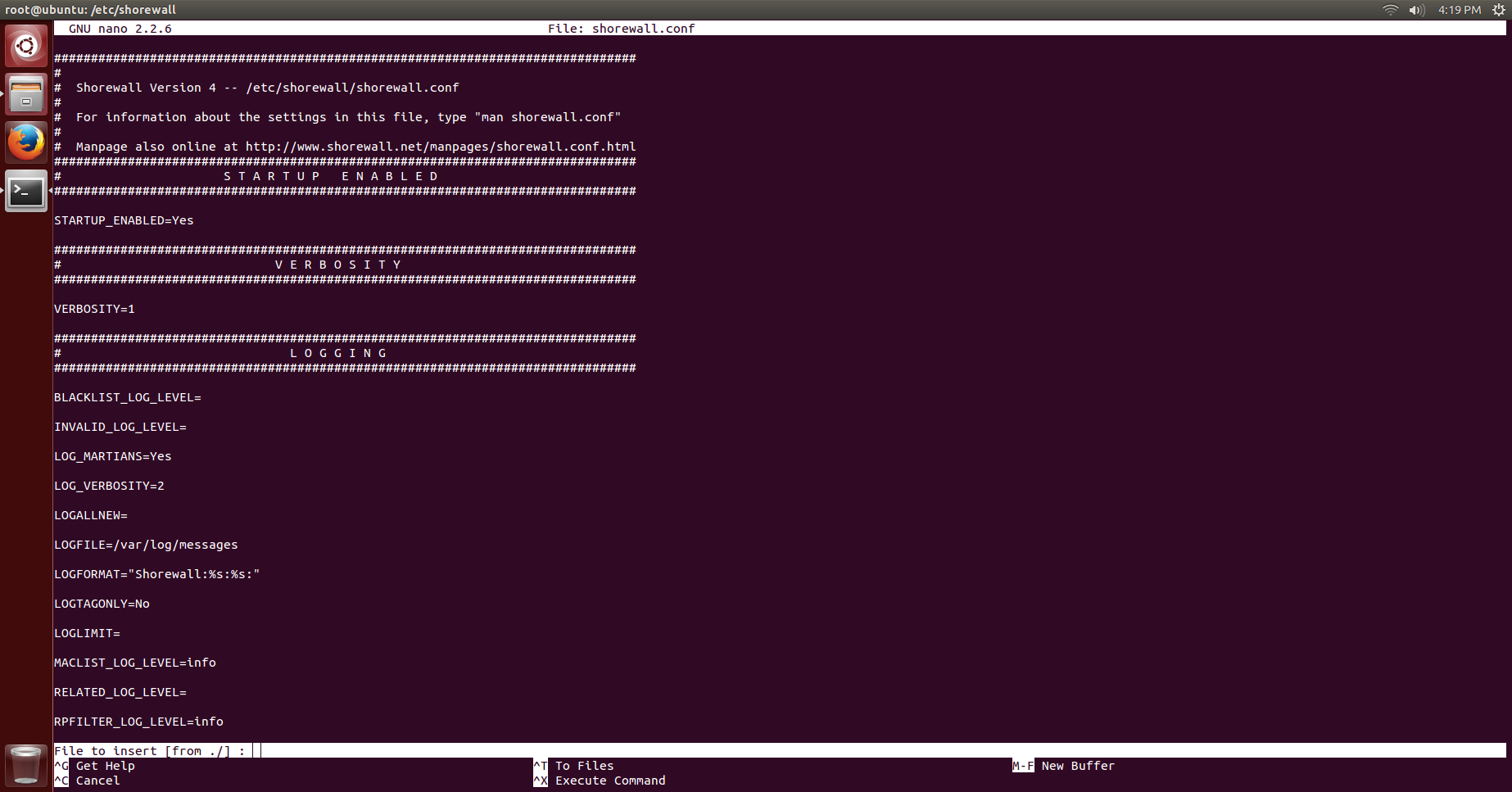


1. Al final indicamos nuestro acl, donde indicamos las reglas a seguir y las categorias que deseamos bloquear.

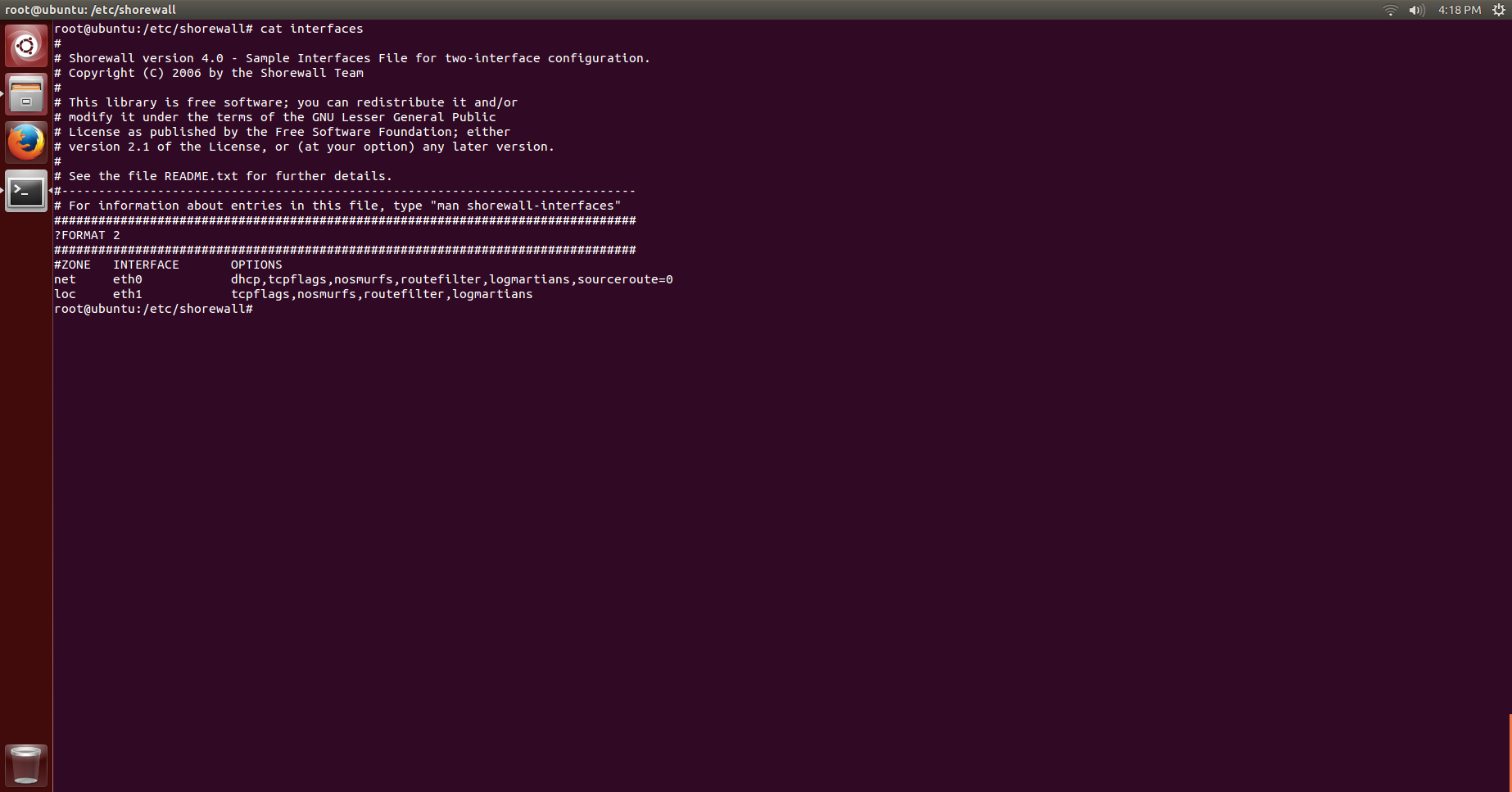


# SHOREWALL

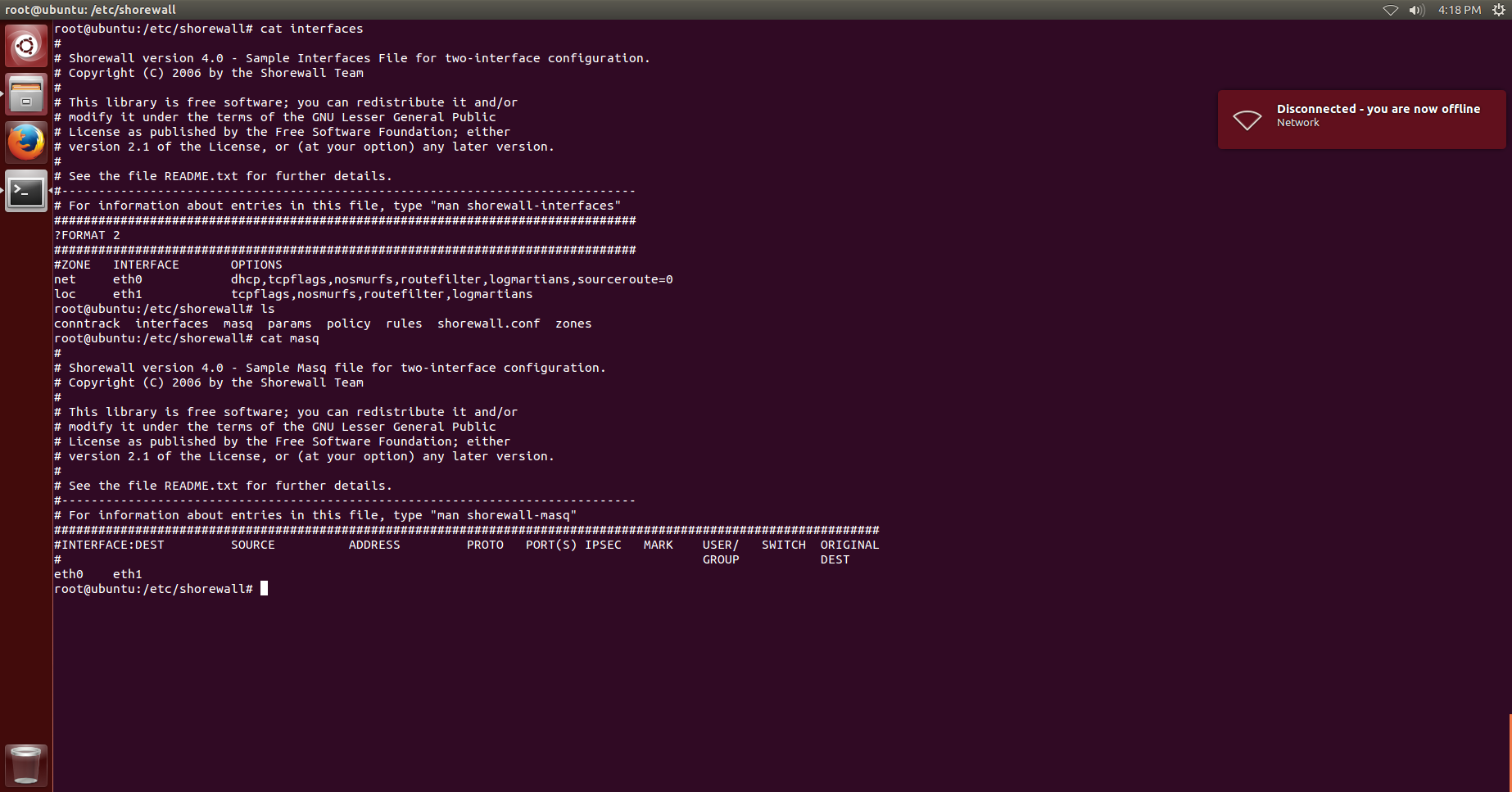
1. En el archivo de configuración de Shorewall, modificamos la opción de Startup\_enabled a yes, para poder iniciar el servicio, por defecto la opción se encuentra en no.



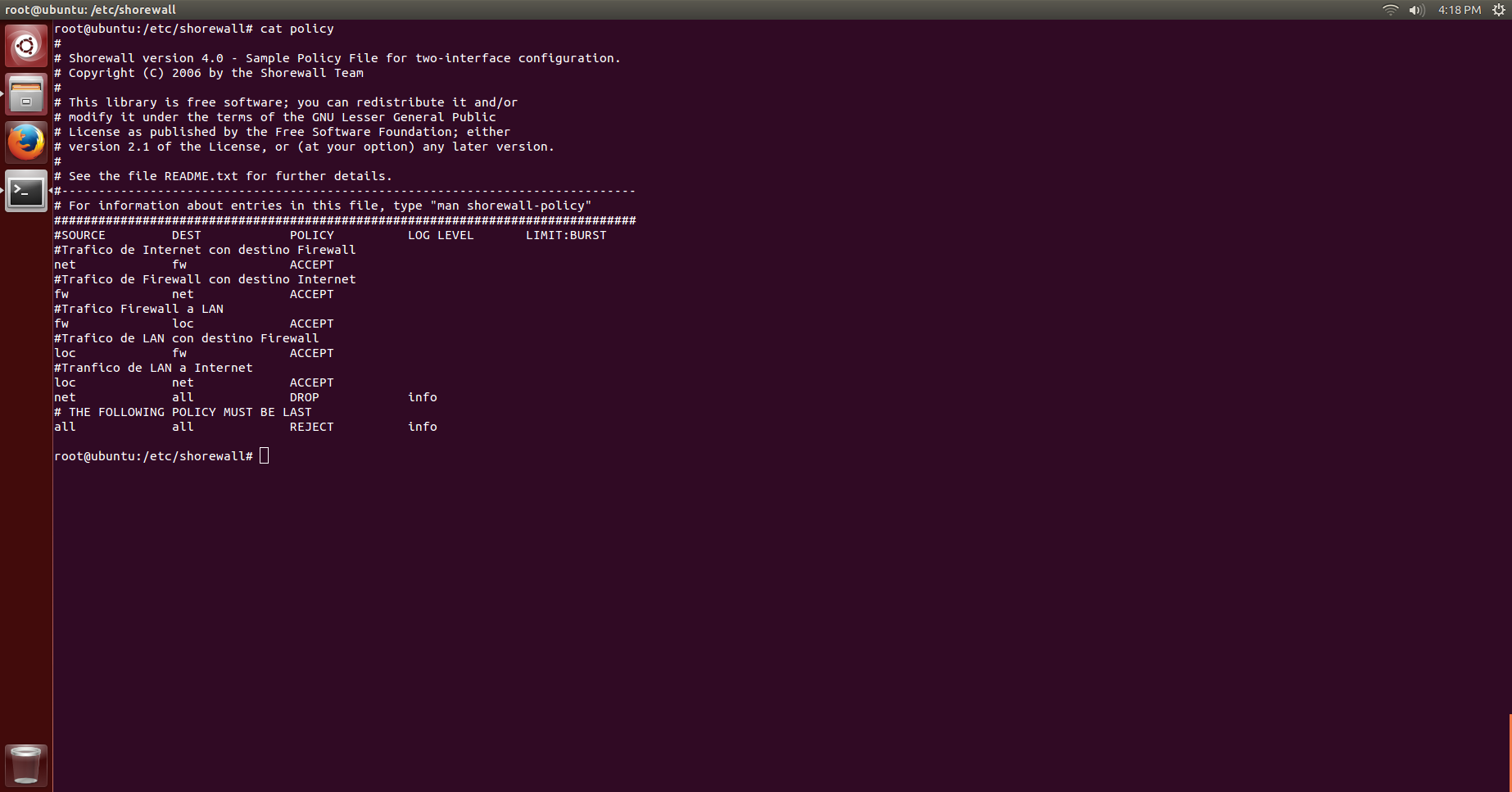
1. Modificamos el archivo *interfaces* que es donde indicamos el nombre de las interfaces de nuestro equipo y cuál corresponde a la red local y cuál a la salida a Internet



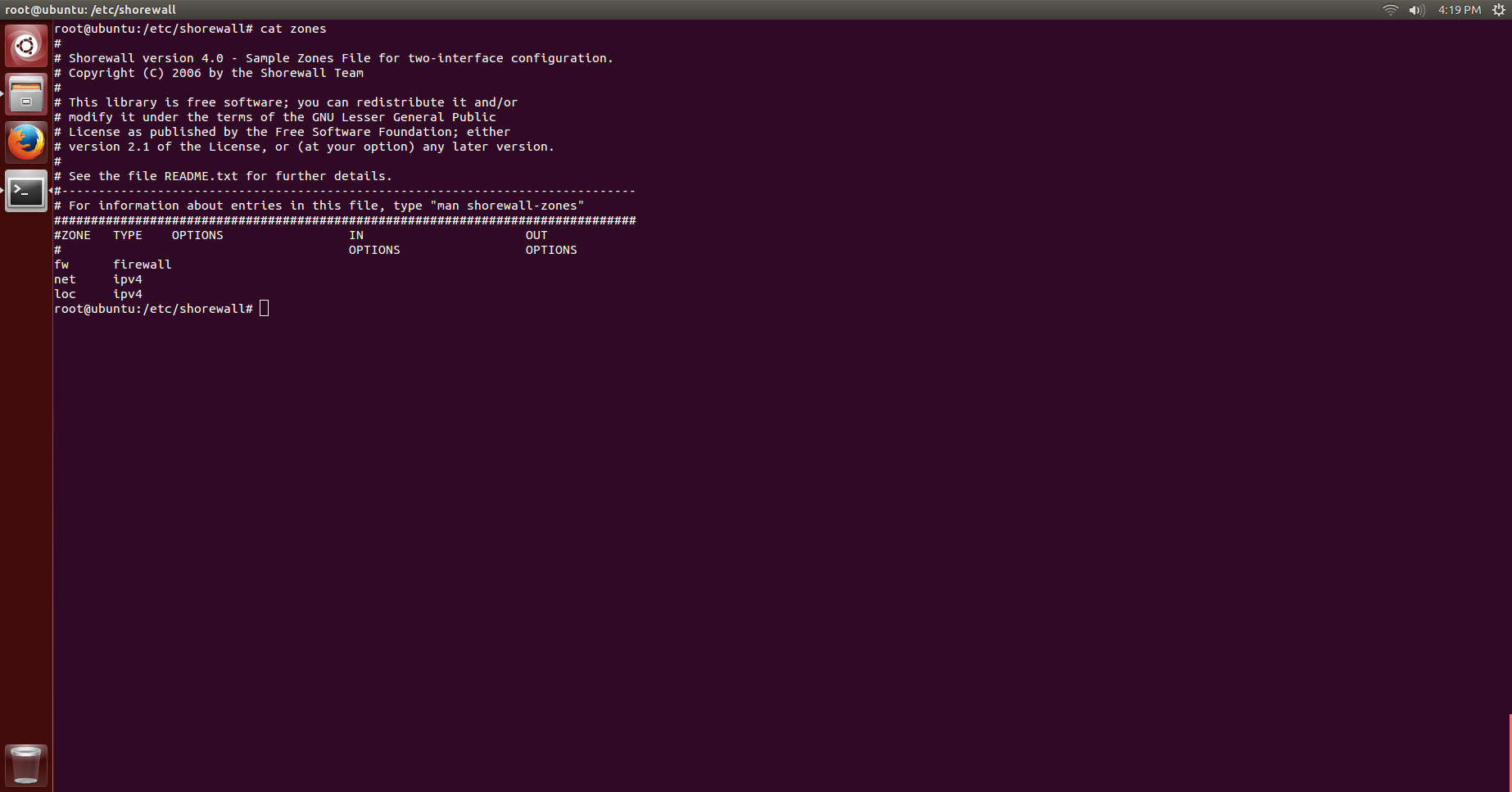
1. En el archivo *masq* indicamos cómo va a ser la comunicación, en éste caso el destino es la eth0 porque es la que corresponde a Internet



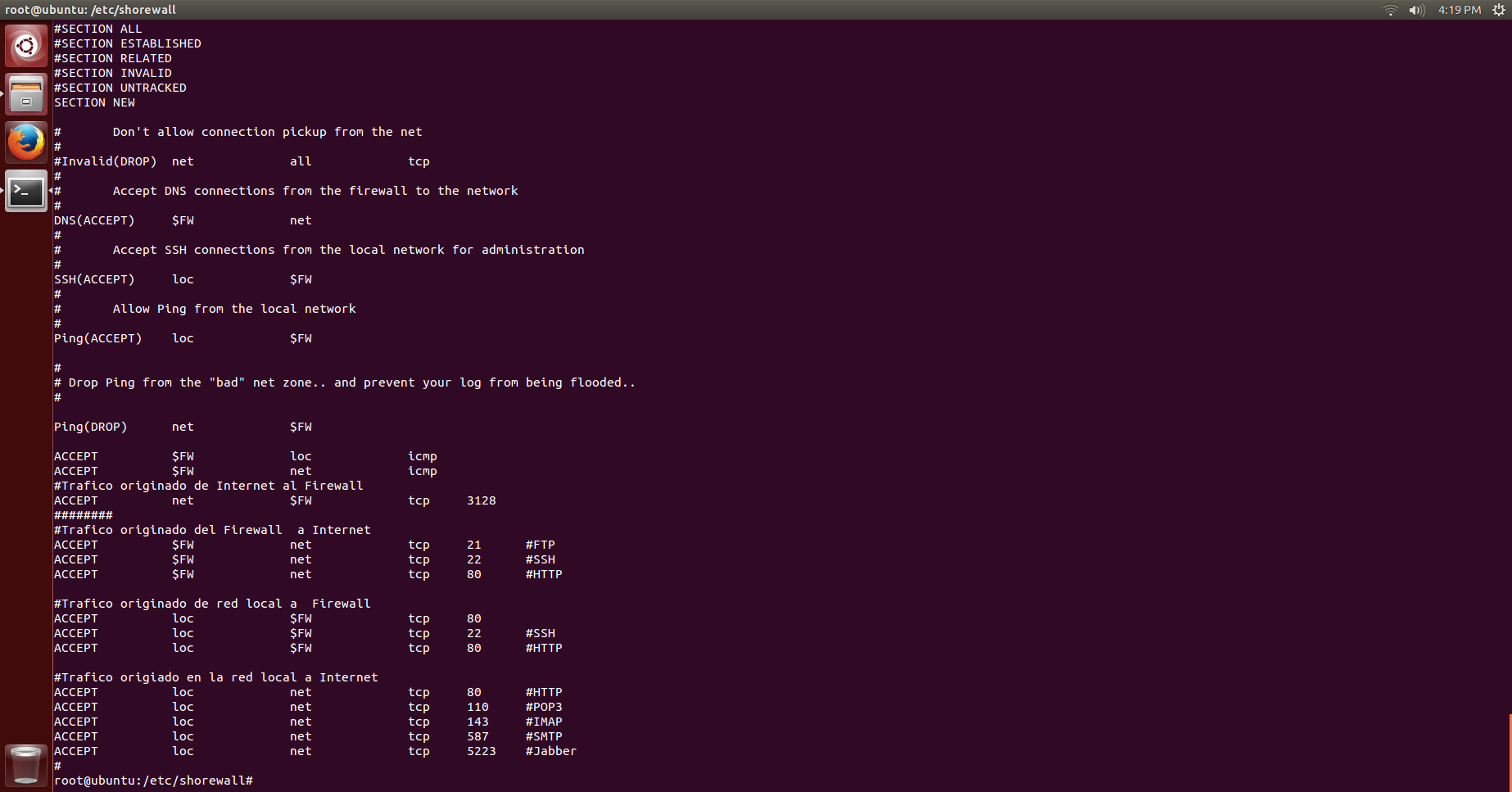
1. Indicamos en *policy* las conexiones permitidas en nuestra red, o el tráfico que deseamos que pase, en éste caso permitimos todas las conexiones.



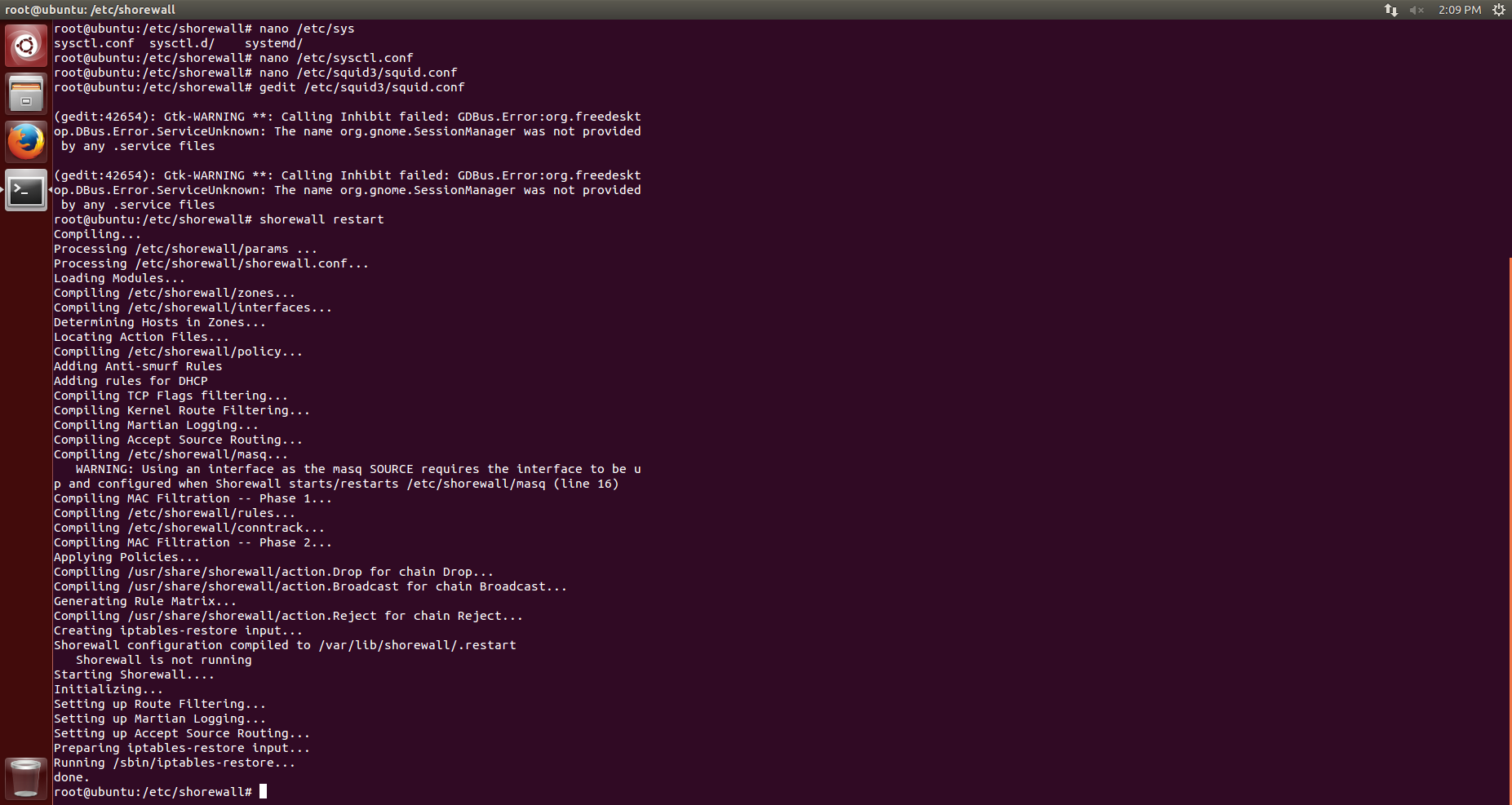
1. En el archivo zones indicamos qué tipo de IP tienen las redes conectadas a nuestro firewall.



1. En el archivo *rules* indicamos las conexiones que podemos recibir, indicando el puerto de éstas.



1. Reiniciamos el servicio de shorewall para que los cambios se apliquen al firewall, podemos ver que verifica la configuración de cada uno de los archivos.



# OBSERVIUM

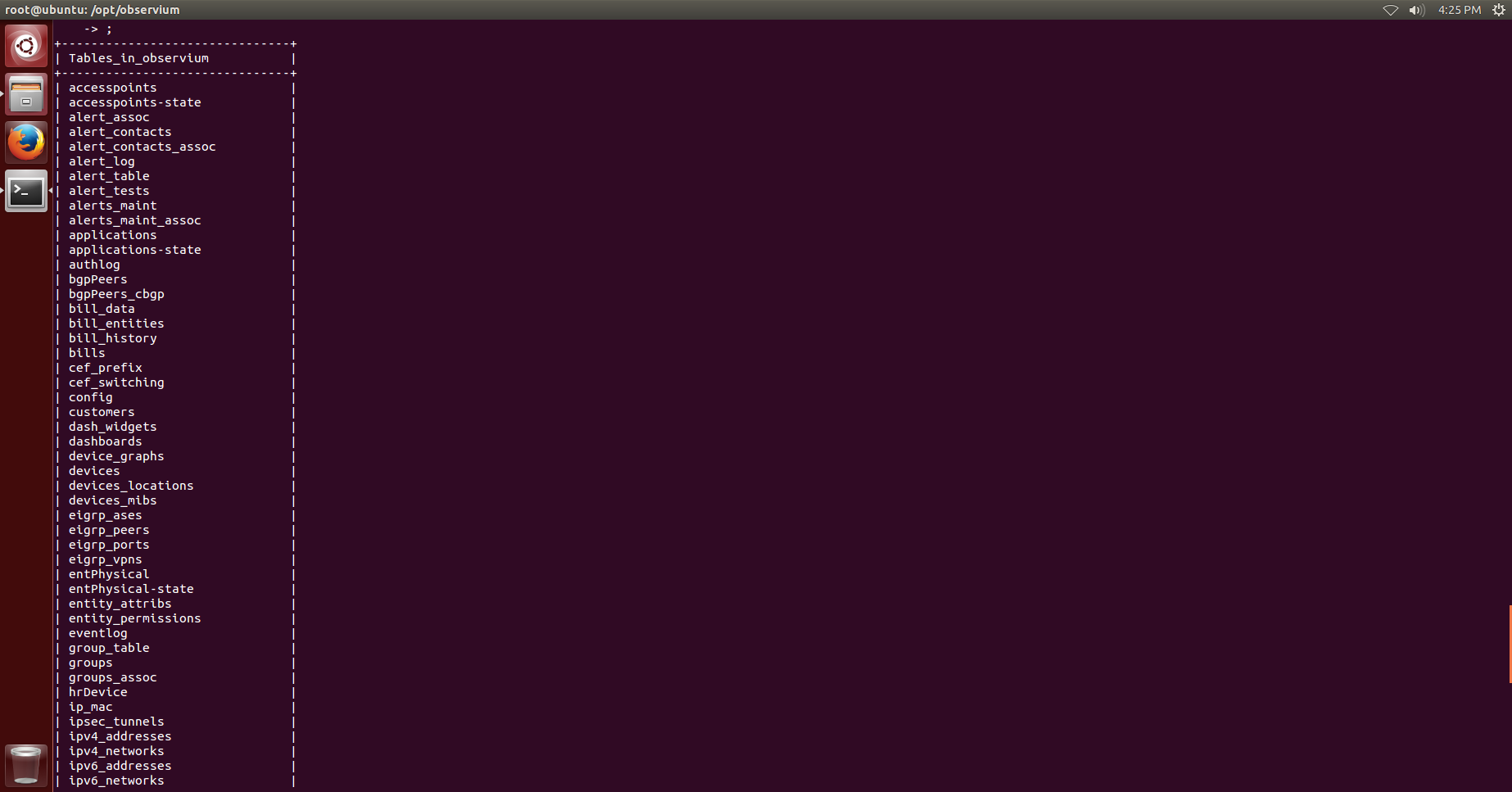
1. Creamos la base de datos correspondiente para el almacenamiento con los siguientes comandos:

*mysql -u root -p  
<mysql root password>  
mysql> CREATE DATABASE observium DEFAULT CHARACTER SET utf8 COLLATE utf8\_general\_ci;  
mysql> GRANT ALL PRIVILEGES ON observium.\* TO 'observium'@'localhost'  
 -> IDENTIFIED BY '<observium db password>';*

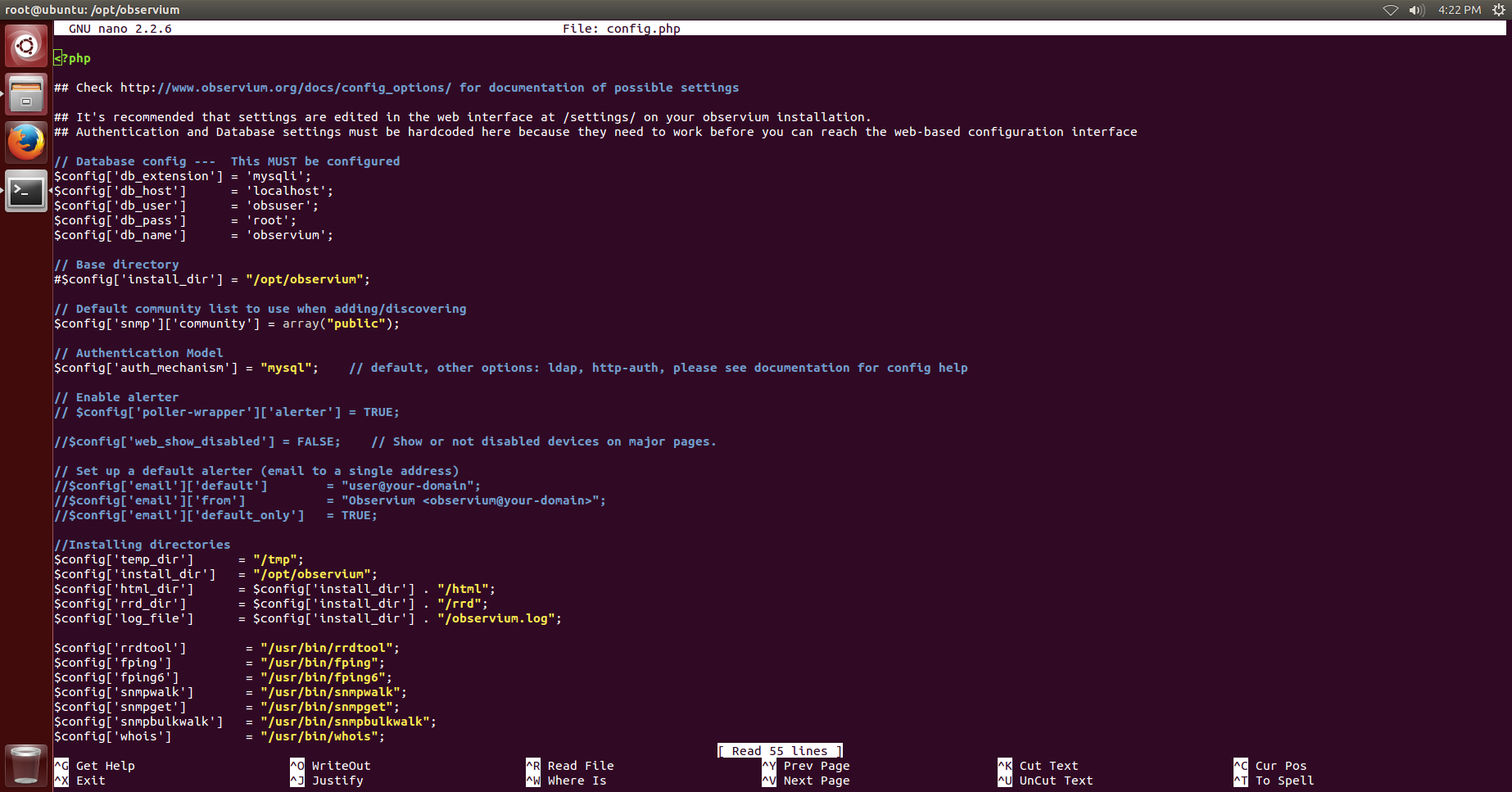
1. Corremos el script *discovery.php* que creará el esquema por default para la base de datos.

*./discovery.php -u*

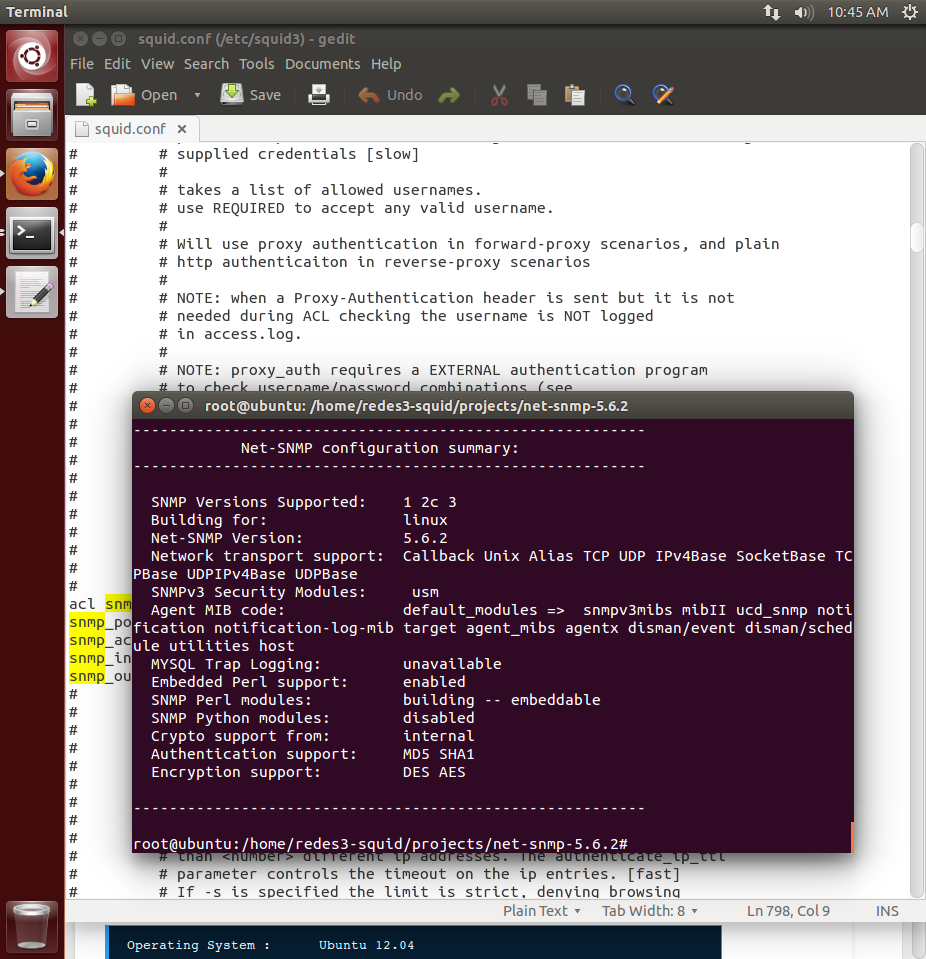
Podemos ver que se crean varias tablas después de correr el script



1. En el archivo de configuración de Observium, indicamos la base de datos que creamos para el almacenamiento de información.

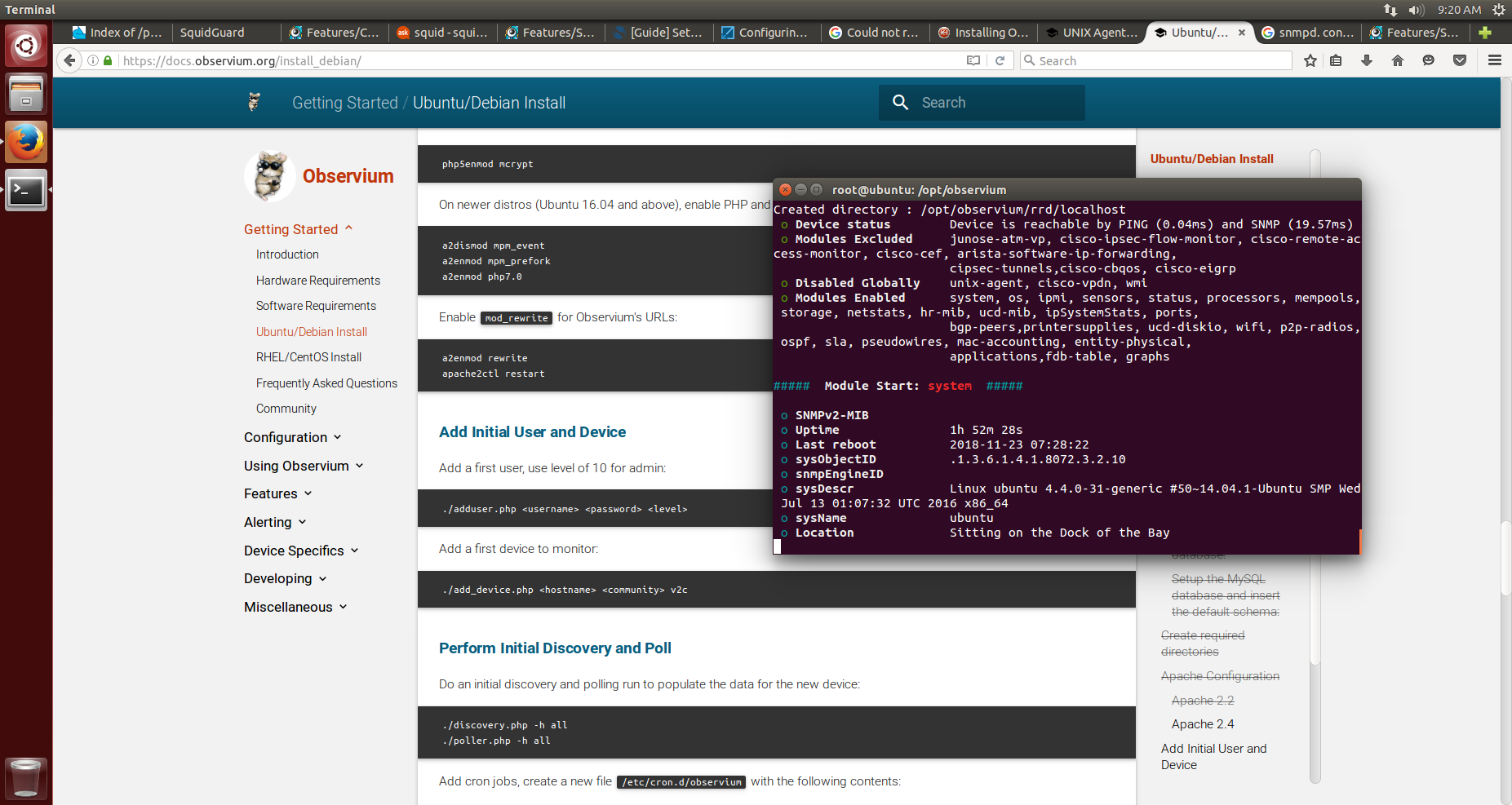


1. Configuramos Net-SNMP tanto en el cliente como en el servidor donde estará Observium, con los siguientes parámetros

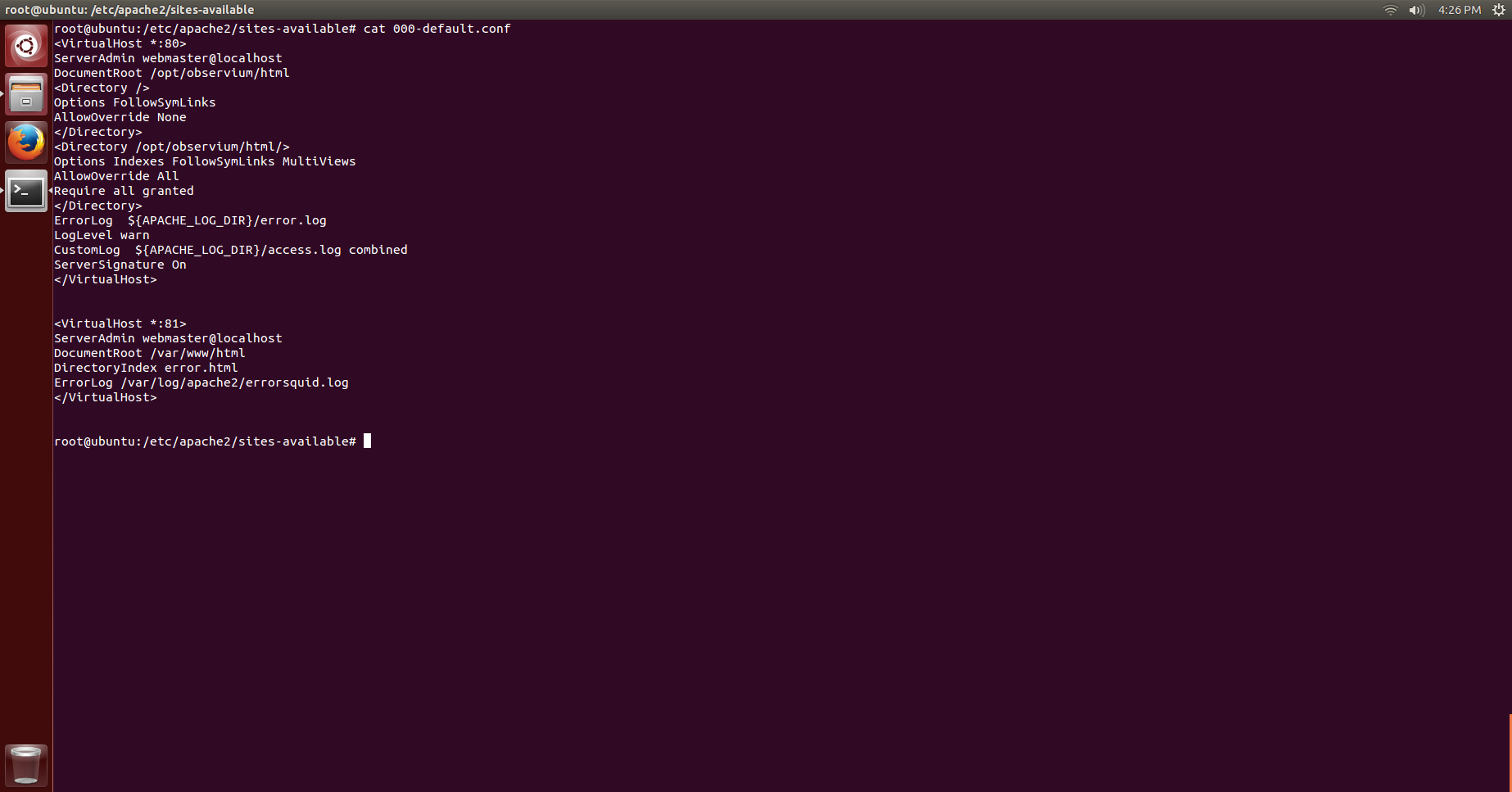


1. Agregamos el dispositivo con el script *add\_device.php*, donde podemos ver que detecta algunas características de nuestra computadora.

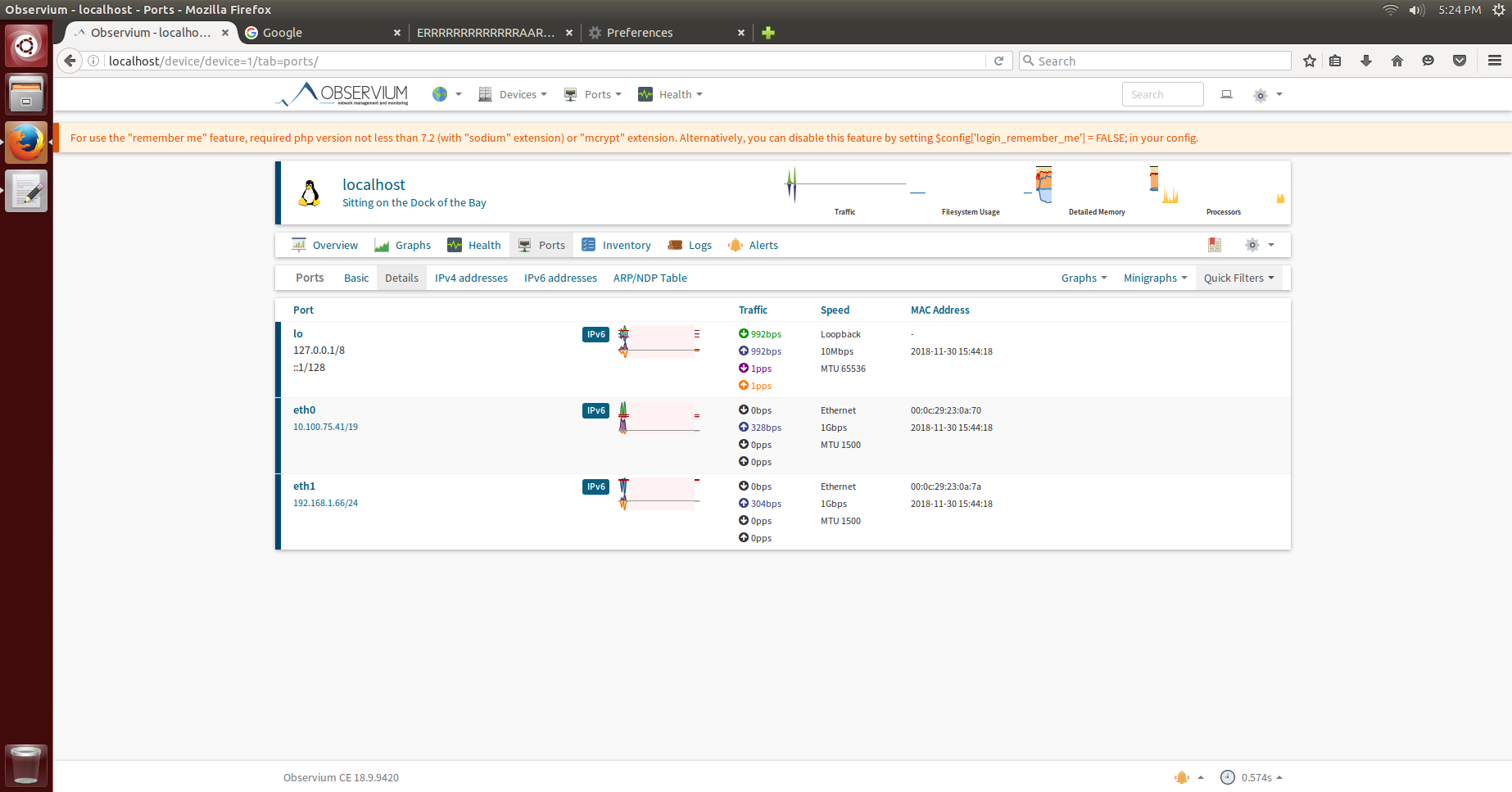
*./add\_device.php <hostname> [community] [v1|v2c] [port] [udp|udp6|tcp|tcp6]*



1. Agregamos un Host Virtual a la configuración de apache para poder acceder al servidor desde http://<ip>:80

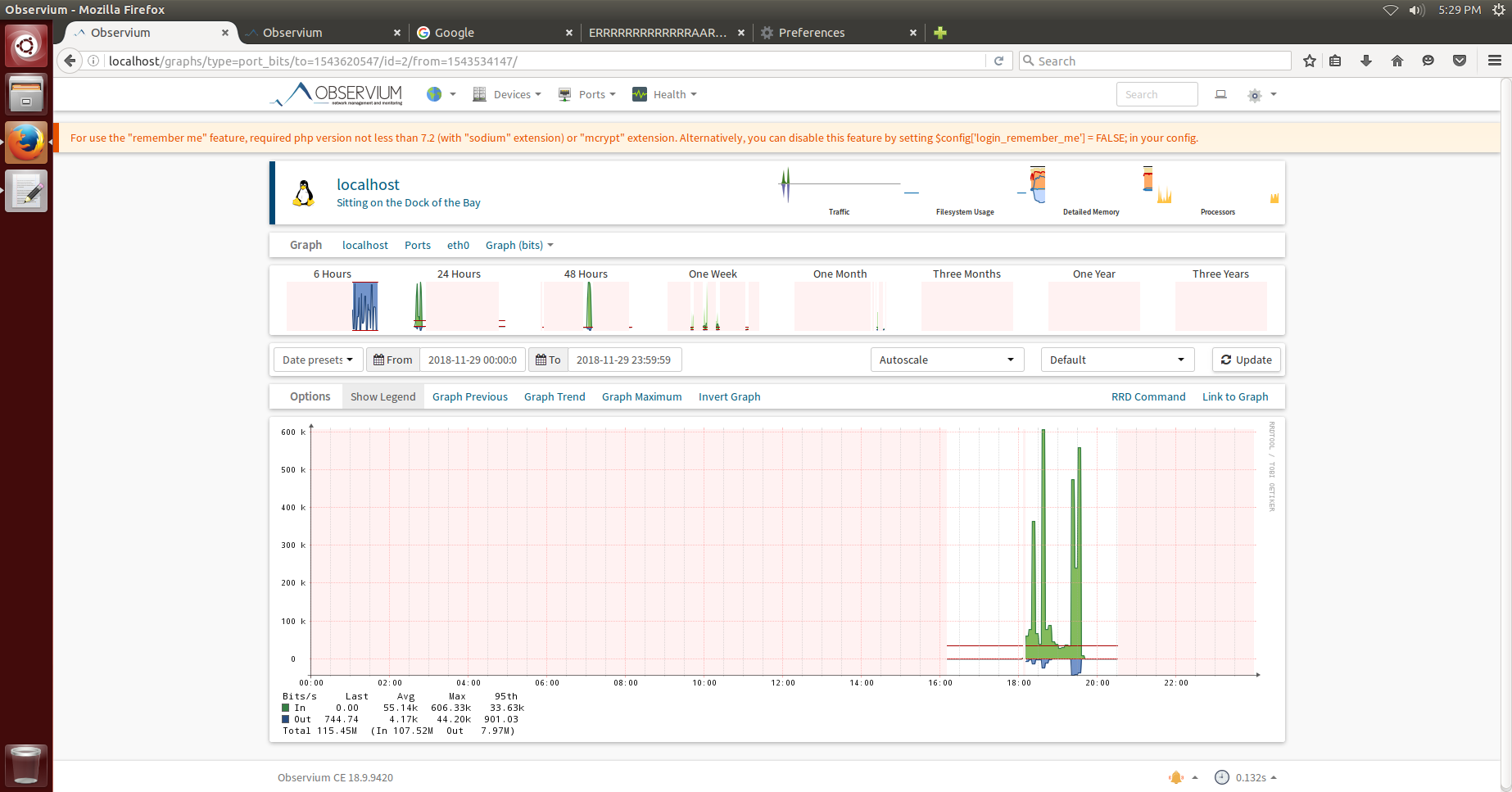


1. Podemos ver que se agregan las dos interfaces de red que tenemos en nuetro equipo.

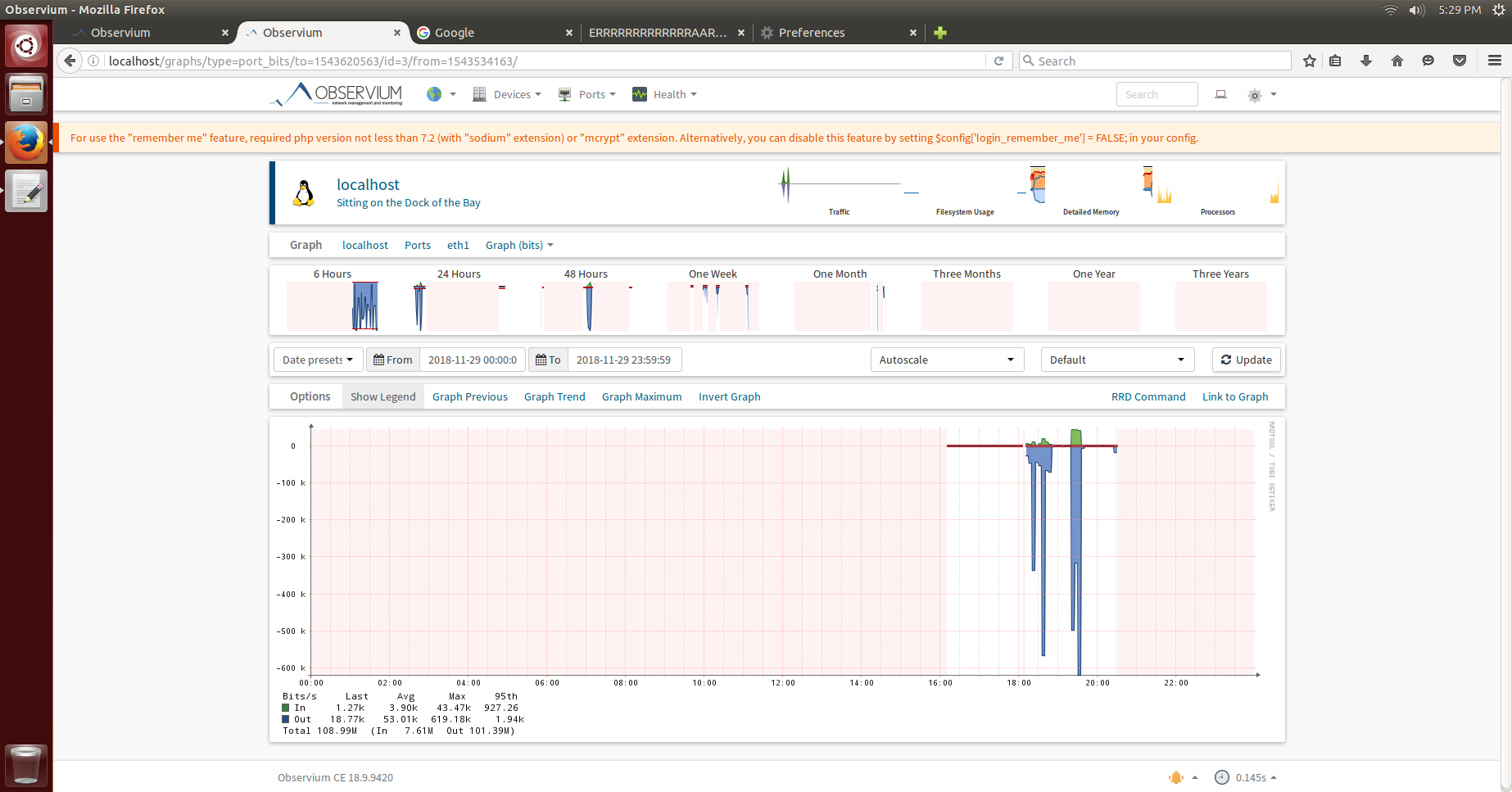


1. Podemos monitorear ambas interfaces desde gráficas distintas

*ETH0*

**

*ETH1*

**

# 

# CLIENTES

## CLIENTE IOS







## CLIENTE ANDROID

## 

## CLIENTE FIREFOX

## 

## CLIENTE WINDOWS

