Instituto Tecnológico Las Américas

(ITLA)

Sistemas Operativos 3 (SO3)

Daniel Alejandro Moreno Martínez

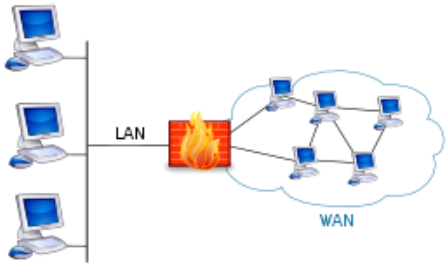
Matrícula: 2010-2946

How to

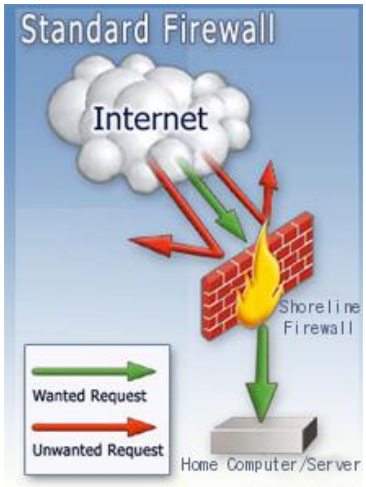
¡ ¡ ¡ How to: Firewall ! ! !

Firewall

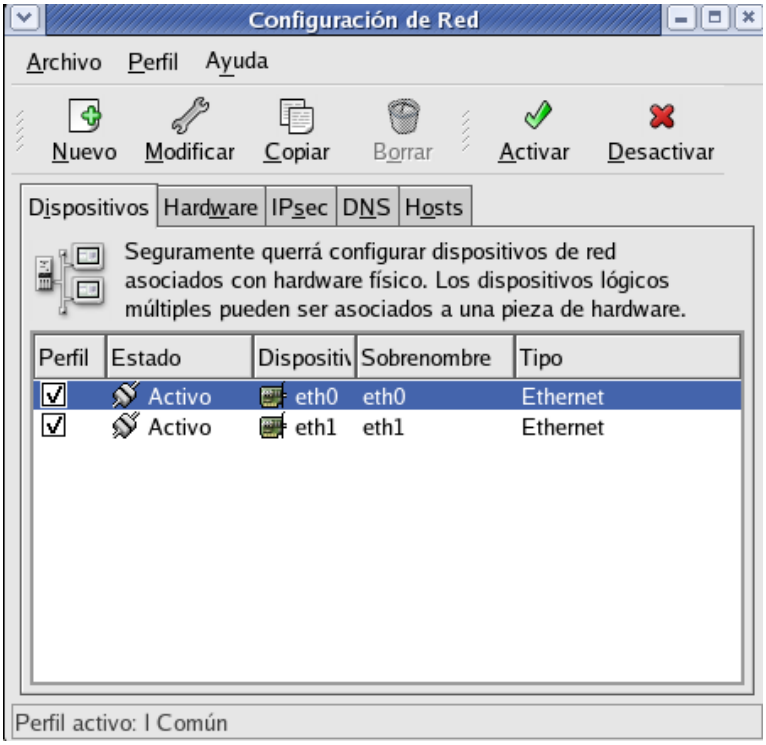
Un **cortafuego (firewall en inglés)** es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.



El **firewall** que vamos a instalar en esta práctica será shorewall. **Shorewall** es un software que permite crear más o menos fácilmente un firewall a partir del firewall interno de Linux (**IPTables**). Shorewall viene con casi todas las distribuciones de Linux.

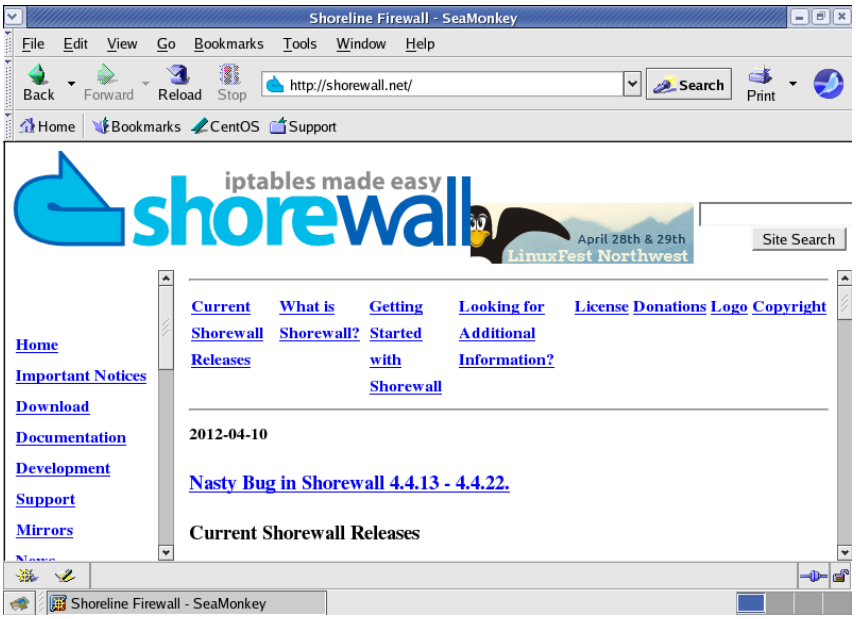


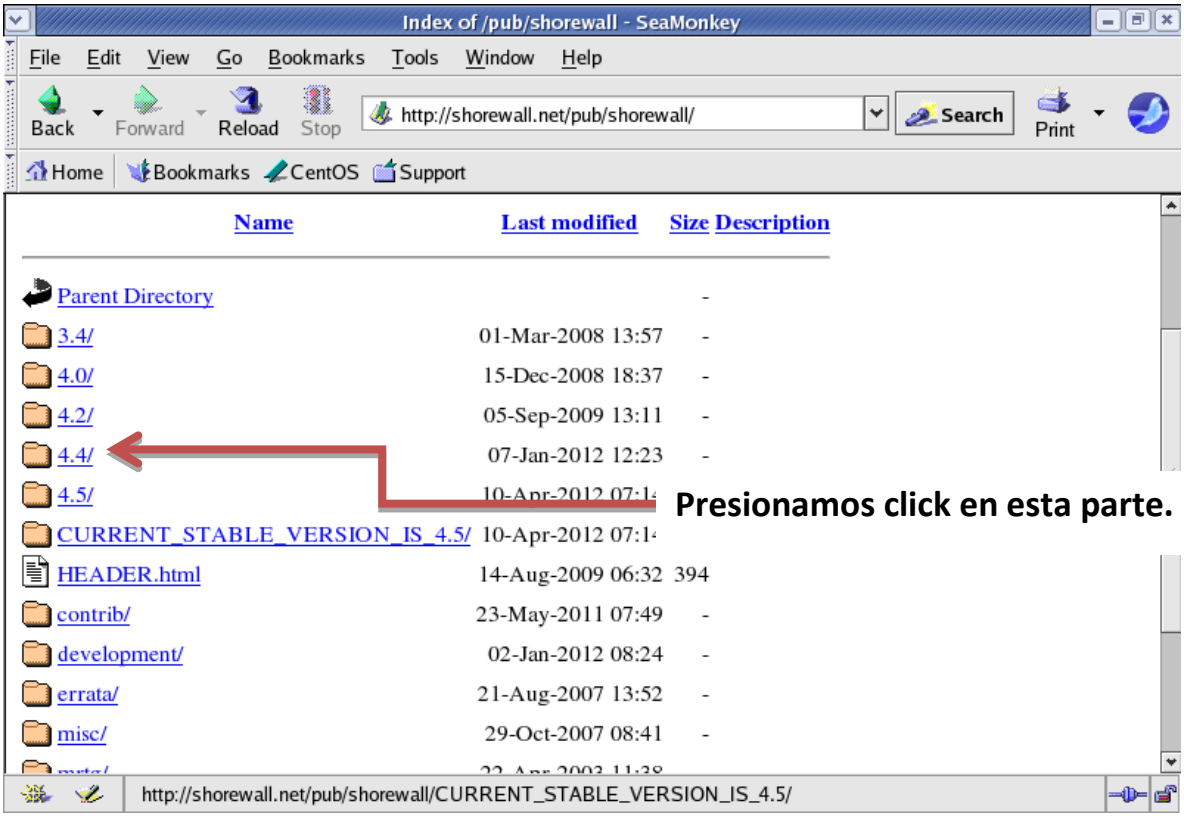
Para esta práctica es necesario que nuestra maquina **tenga dos tarjetas NIC,** en este caso lo hicimos en una máquina virtual. Una con acceso a internet y otra para la red local.



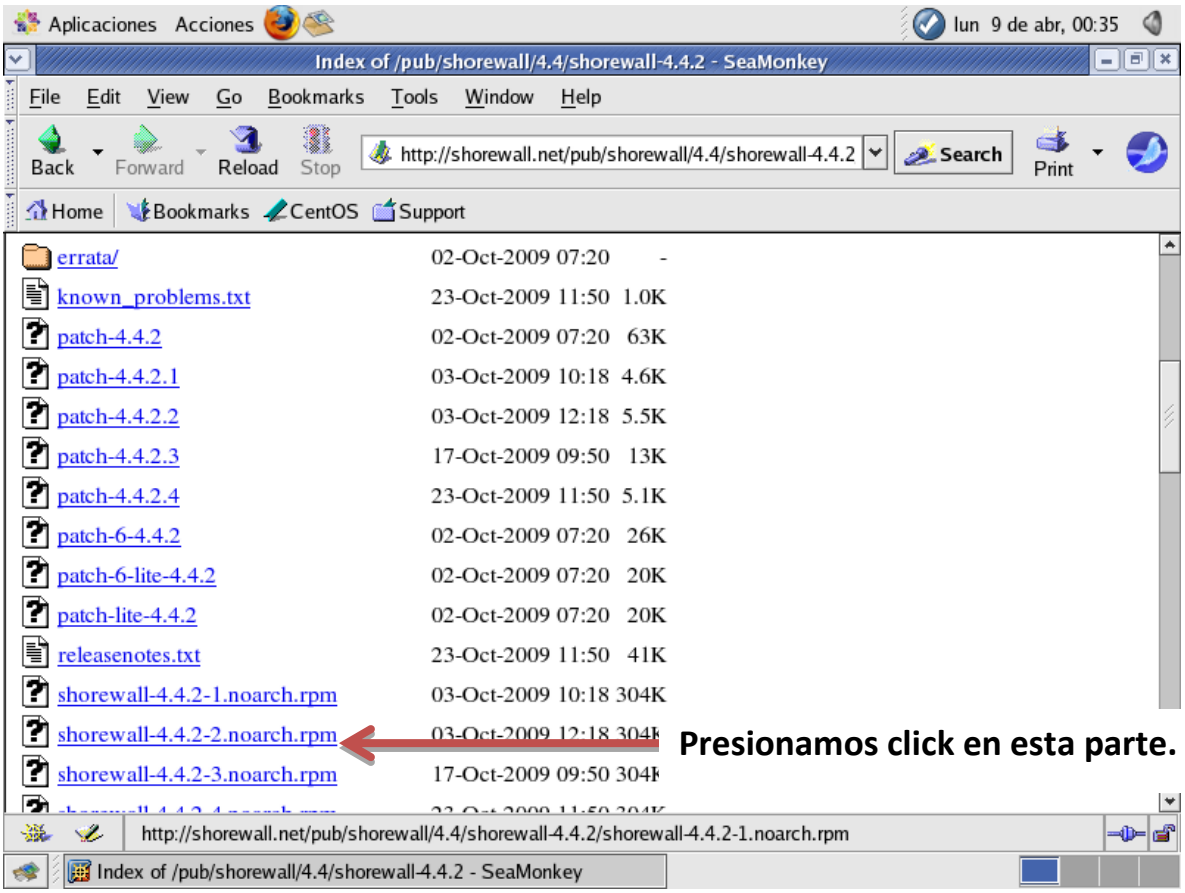
Vamos a descargar **shorewall** desde su página. Para esto podemos usar el siguiente link o seguir los pasos que muestro a continuación.

http://www.shorewall.net/pub/shorewall/CURRENT_STABLE_VERSION_IS_4.4/shorewall-4.4.21/

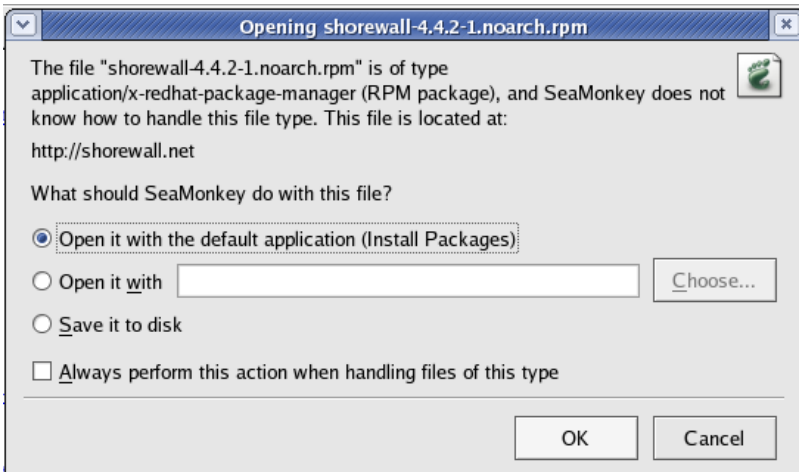




Presionamos click en esta parte.



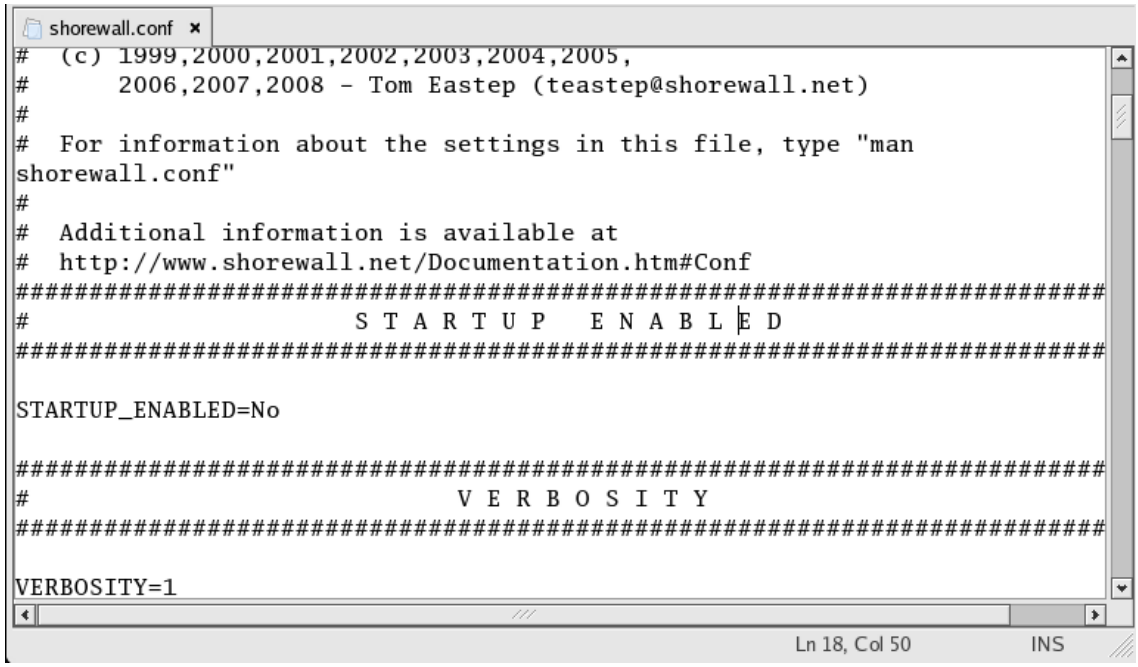
Presionamos click en esta parte.



Hacemos Clic en aceptar para procesar la instalación del paquete que acabamos de descargar.

Luego de que completemos la instalación procedemos a configurar nuestro firewall, nos dirigimos a la línea de comandos. Los archivos de configuración están en: **/etc/shorewall.**

Editamos los archivos necesarios: Para que arranque al inicio el demonio.



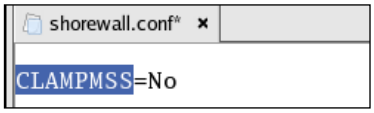
Debemos cambiar el parámetro de **STARTUP_ENABLED=NO** a **YES** para activar nuestro firewall.

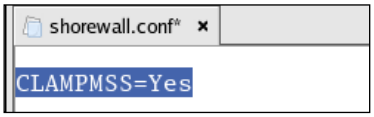
```
##############################################################################
#                       S T A R T U P   E N A B L E D
##############################################################################

STARTUP_ENABLED=Yes

##############################################################################
```

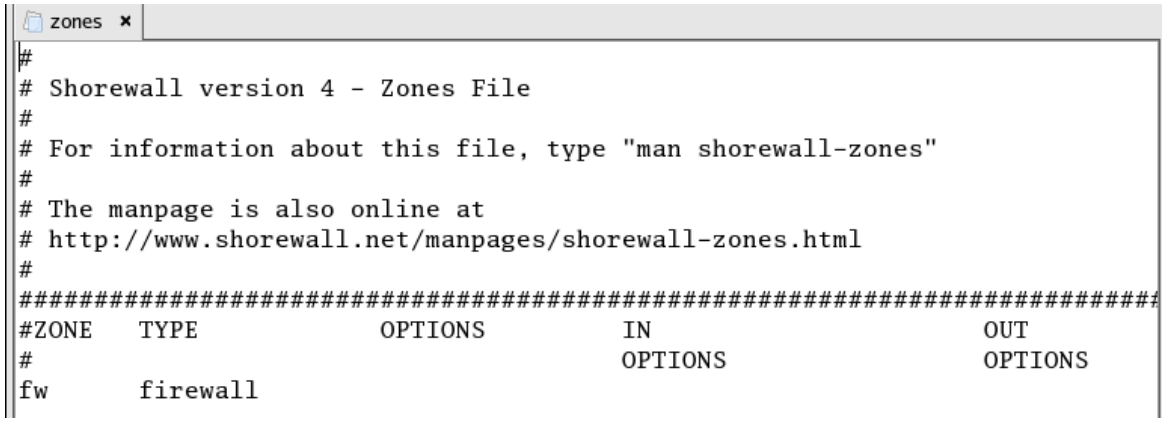
Buscamos la línea **CLAMPMSS** y cambiamos el valor predeterminado **No** a **Yes.**



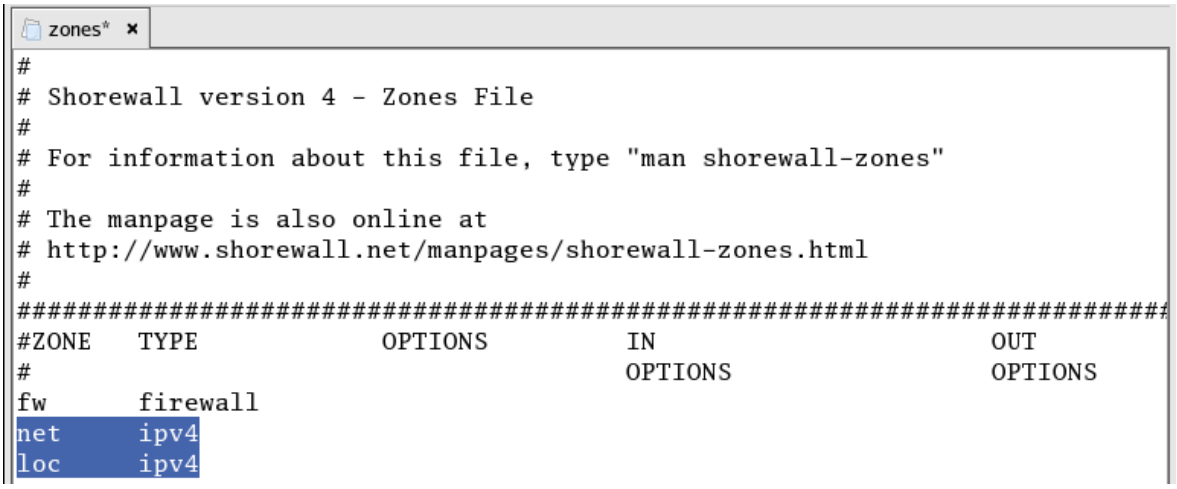


Luego de esto **guardamos los cambios** y salimos. Ahora vamos a agregar las **zonas** que vamos a administrar desde nuestro **servidor firewall.**

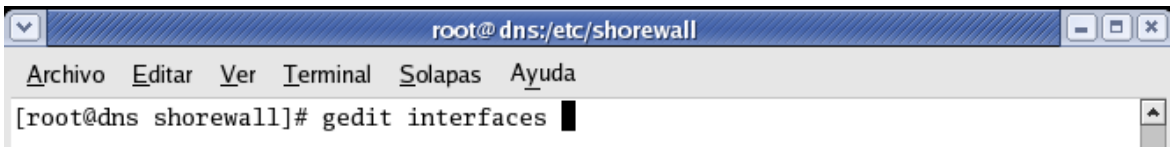
Podemos ver que nos aparecerá el archivo de configuración.



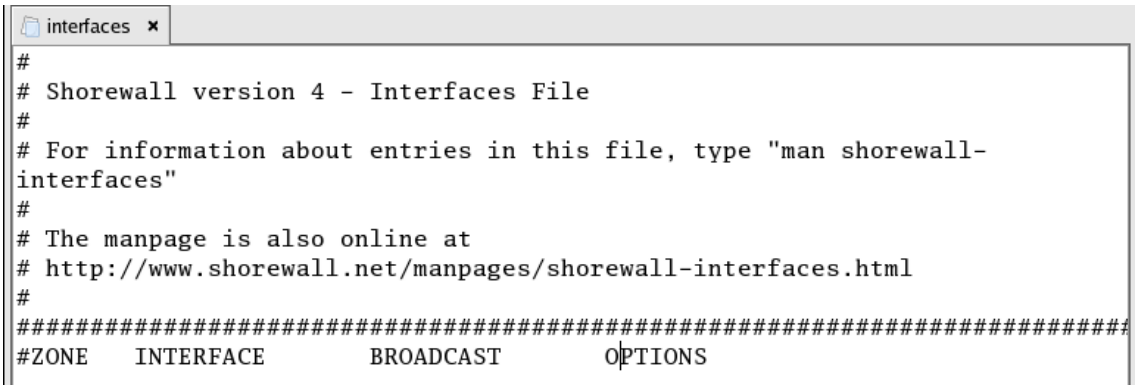
Editamos el archivo **zones** en mi caso 3 zonas van a existir: Una de estas zonas es **net** que es la conexión a internet con el tipo **Ipv4**, **loc** que será la conexión local de la red interna con el tipo **Ipv4** y **fw** que es la del **firewall.**



Guardamos y salimos. Luego editamos el archivo **interfaces** que va a definir a que interfaz pertenece cada **zonas**.

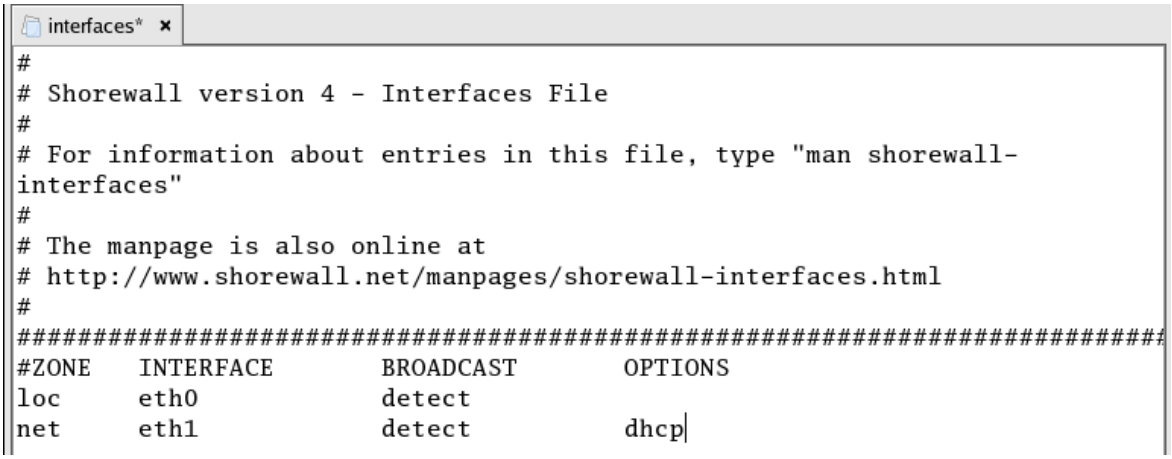


Nos aparecerá el archivo de configuración.

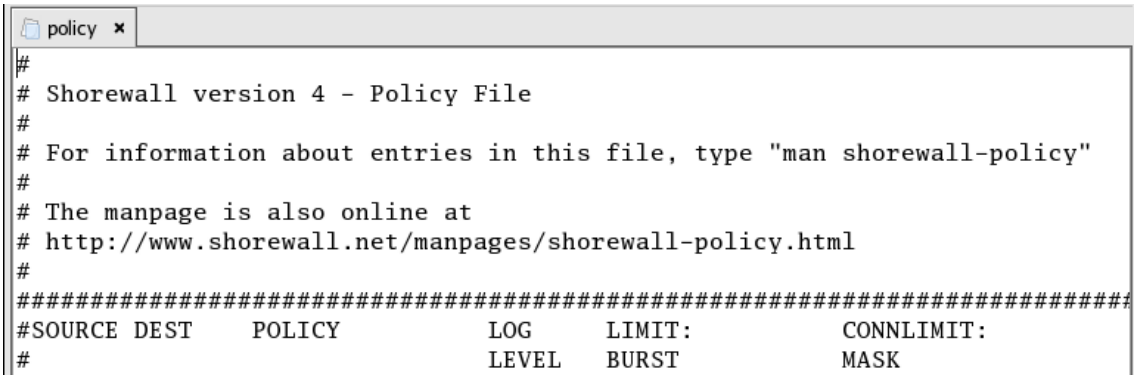


Hemos configurado 2 **zonas net y loc**, tenemos 2 interfaces Ethernet **eth0 y eth1**.

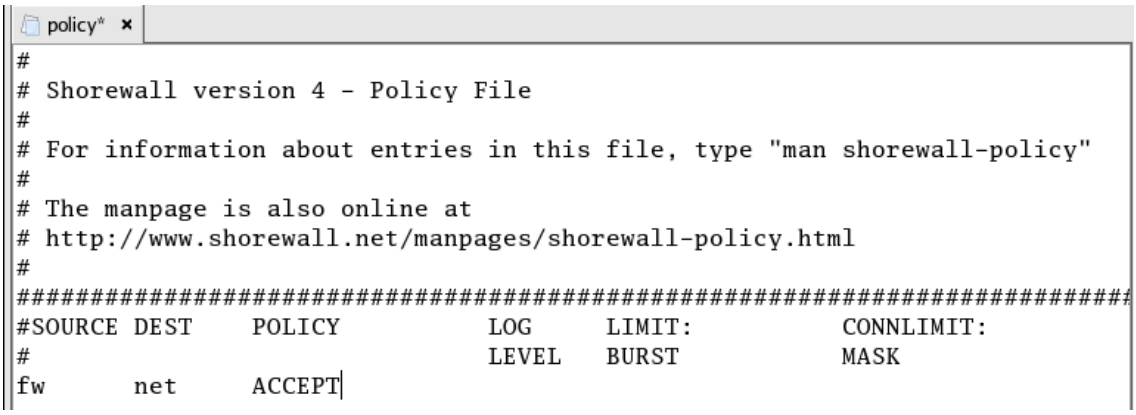
La interfaz **eth0** será para **net** que es la conexión a **internet** y **eth1** será para **loc** que es la conexión para la **red interna.** También le indicaremos que **detecte el Broadcast** de la red, en caso de alguna de las interfaces necesitara o adquiriera una dirección dinámica por **dhcp** colocamos el parámetro **dhcp en OPTIONS,** en este caso solo lo hicimos en **net** ya que **loc** tiene una **IP estática.**



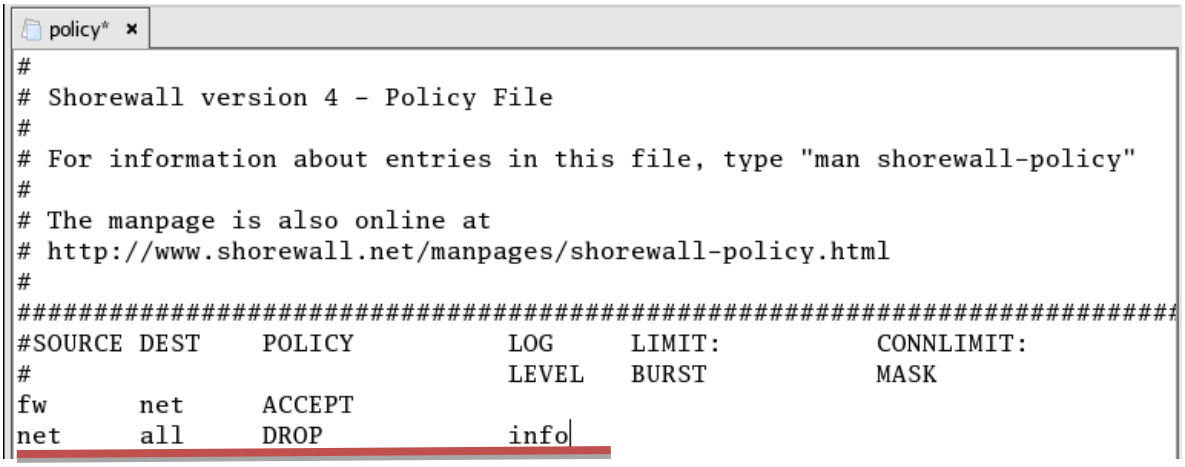
A continuación vemos el archivo de configuración.



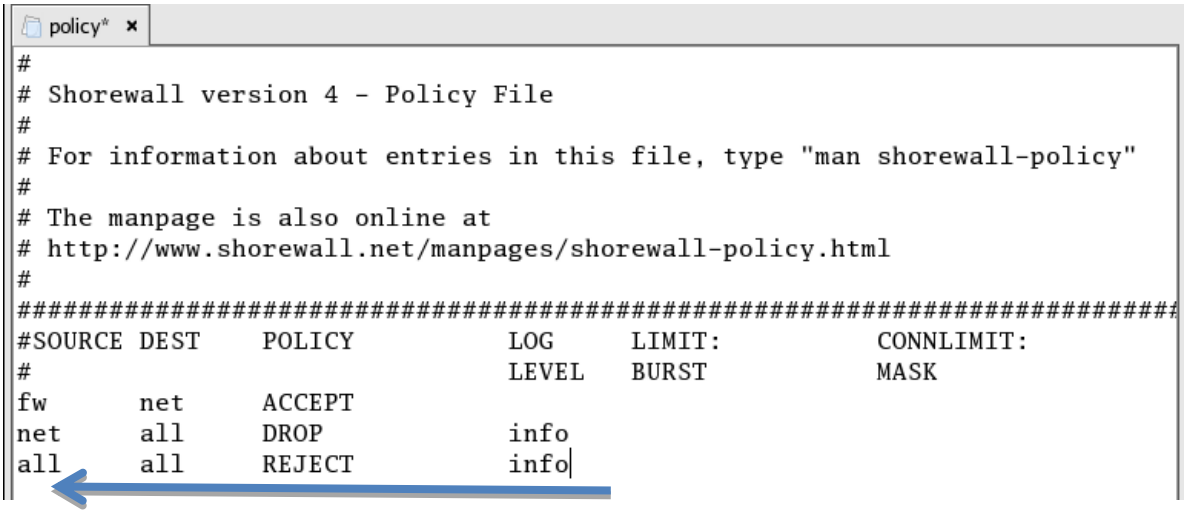
Vamos a dejar solamente 3, en **source** colocamos la **zona origen** y **dest** la zona destino y en policy debemos colocar si aceptamos, denegamos o rechazamos la conexión, en este caso aceptaremos.



Ahora todo lo que venga desde internet hacia nuestra red local lo vamos a denegar y le colocamos un **log level info.**



Ahora todo lo que no hallamos dicho u omitido lo **vamos a rechazar.**



Guardamos y salimos.

Ahora vamos a editar el **archivo masq,** en este archivo, se define qué interfaz hará el enmascaramiento **o nat**, en **etho** hará el enmascaramiento y **SOURCE** es el origen indicando quien realizara la petición de enmascaramiento, en este caso será **eth1**, pero también podemos colocar una subred o IP específica a la que queremos hacerle el **Nat,** colocamos la IP en source, el protocolo que puede ser **TCP** y el **puerto 25**, solo a esta dirección se le hará **Nat**. Pero en este caso se le hará Nat a todo lo que venga por **eth1 o sea la red local.**

Aquí podemos ver el archivo de configuración.

masq

```
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
###############################################################################
#INTERFACE              SOURCE          ADDRESS         PROTO   PORT(S)
IPSEC   MARK    USER/
#
GROUP
```

Editamos el archivo **masq** para que enmascare la **ip** si es que tenemos un **pool de ips** que brindan servicio externo en nuestro caso.

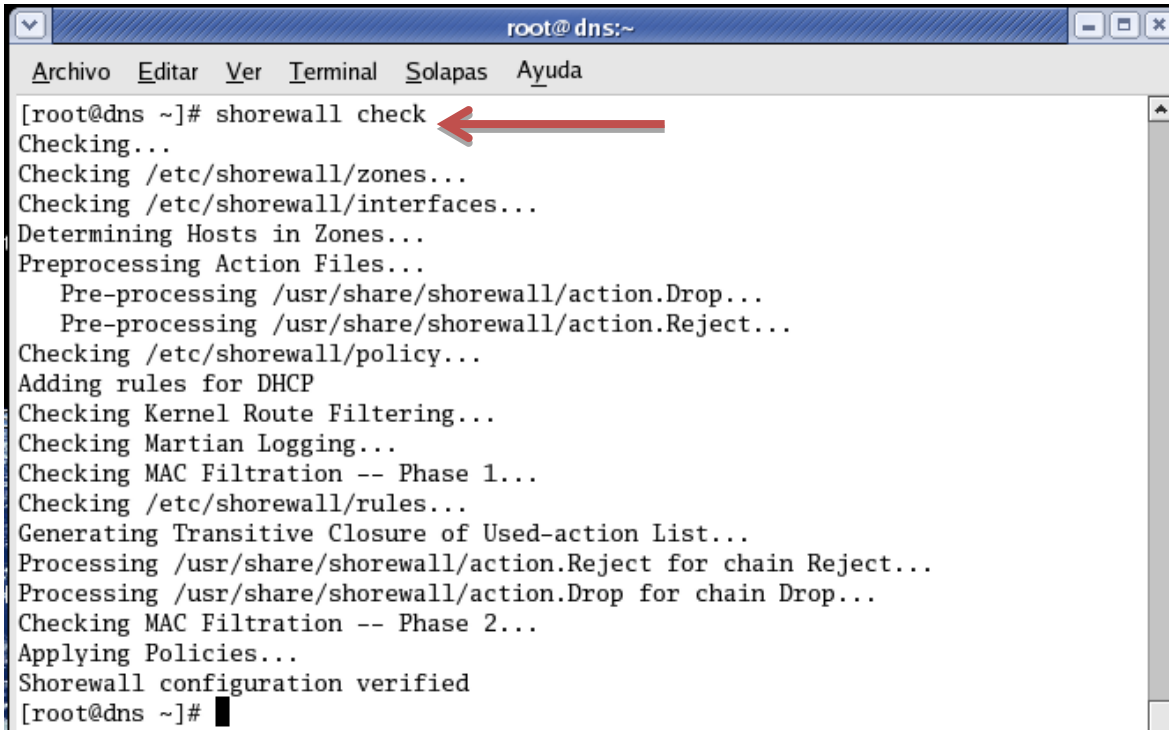
masq*

```
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
###############################################################################
#INTERFACE              SOURCE          ADDRESS         PROTO   PORT(S)
IPSEC   MARK    USER/
#
eth1                    eth0
```

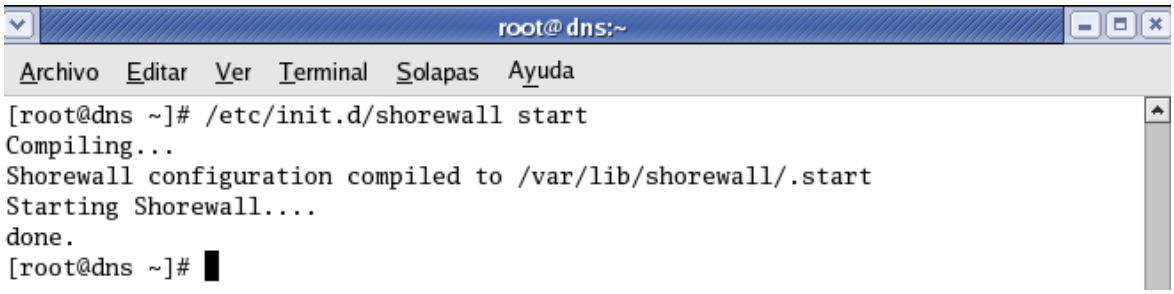
Guardamos y salimos.

Comprobar que no existe ningún error de configuración, con el comando:

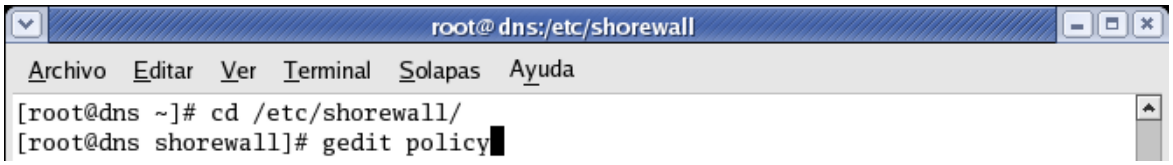
Shorewall check.



Luego iniciamos nuestro **servidor firewall.**



Ya nuestro servidor está funcionando, ahora vamos a probarlo implementando una política que bloque el acceso a internet. Editamos el archivo **policy.**

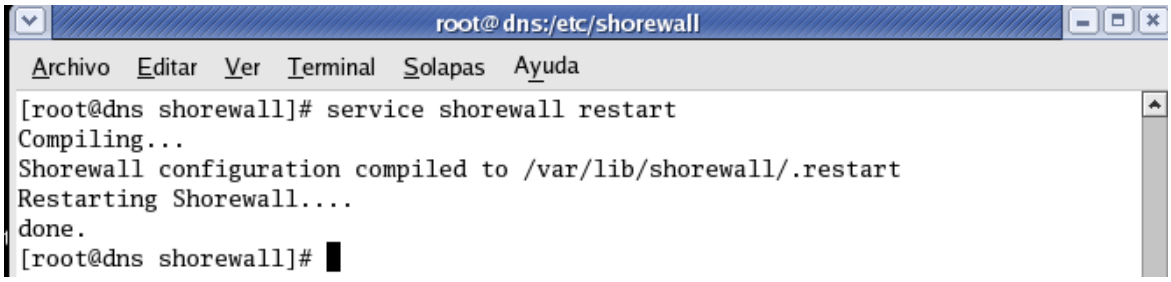


policy* ×

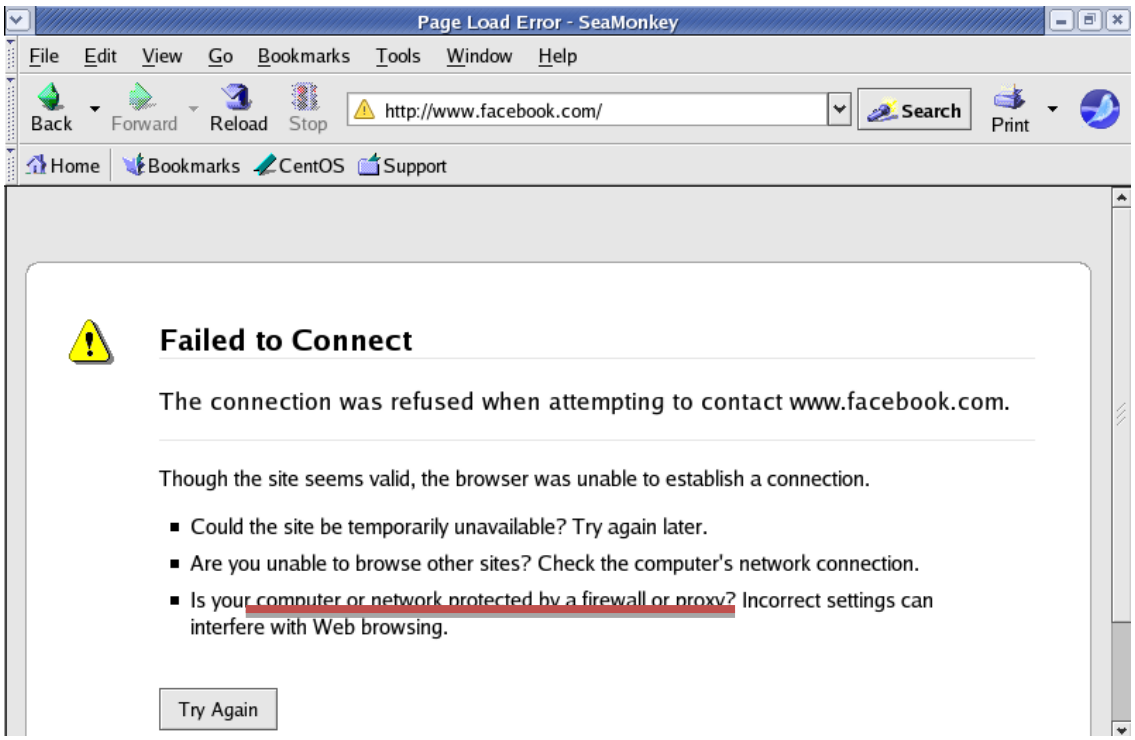
```
#
# Shorewall version 4 - Policy File
#
# For information about entries in this file, type "man shorewall-policy"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-policy.html
#
###############################################################################
#SOURCE DEST    POLICY          LOG     LIMIT:          CONNLIMIT:
#                               LEVEL   BURST           MASK
net     fw      ACCEPT
fw      net     ACCEPT
loc     fw      ACCEPT
all     loc     REJECT
loc     net     ACCEPT
```

Aquí rechazamos todo tráfico que venga de internet hacia la zona local.

Luego **reiniciamos nuestro firewall** para que aplique la política.



Luego podemos ver que nuestra política fue implementada correctamente. Vemos que no tenemos **conexión a internet.**



De esta forma hemos terminado de trabajar con lo que es **el servidor firewall**.

A continuación les dejo **unos link bastante** interesantes donde podrán encontrar mucha información sobre esta práctica y para utilizarlas en una versión más actualizada de CentOS.

http://loquitoslack.blogspot.com/2011/06/instalar-shorewall-en-centos-install.html

http://www.howtoforge.com/how-to-set-up-shorewall-firewall-on-centos-5.1

http://www.com-sl.org/como-configurar-un-firewall-con-shorewall-en-dos-interfaces-de-red-con-politicas-drop-en-centos-y-debian.html