Instalar Firewall en Linux Server con Shorewall

“Descubre el procedimiento que yo personalmente utilizo para instalar un Linux Server Firewall en tu casa u oficina ! “

Por Wilmer Huamaní Córdova

Web : http://configurarlinuxserver.com

Linux Server Firewall con Shorewall

Actualmente, muchas empresas están solicitando servicios de implementación Firewall para la protección de los recursos internos de su red local. Quiero compartir contigo la forma de cómo se implementa un servidor Firewall con shorewall para tener una protección de seguridad en los datos que ingresan desde Internet a tu red local así también los que salen desde tu segmento interno de la Red local a internet ; ambos deben pasar necesariamente por el servidor Firewall. La implementación puede ser con dos o tres tarjetas de red instaladas en la computadora o ordenador que va ha cumplir la función de Firewall. En nuestro caso la implementación será con dos tarjetas de red y es llamado Bastion home. Antes de hacer la implementación del Firewall con Shorewall se debe conocer los conceptos de firewall y Shorewall respectivamente.

Qué es Firewall ? Un Firewall es un controlador de punto de acceso para todo el tráfico que ingresa a la red interna. Así también, es un controlador de punto de acceso para todo el tráfico que sale de la red interna. Un firewall sobre la red tiene un propósito de prevenir el peligro potencial de la Internet hacia tu red interna. Un servidor firewall tiene dos funciones principales y que a continuación se detalla:

- Te previene de usuarios no autorizados que quieren ganar acceso a la red de datos y recursos.
- Te da la seguridad que la interacción entre la Internet y la red interna sea conforme a las reglas de seguridad y políticas de vuestra organización.

Qué es Shorewall ? Shorewall es un software que te facilita generar las reglas de configuración del netfilter . Es un conjunto de ficheros que se utiliza para configurar y controlar los paquetes del núcleo Linux .

Procedimiento para habilitar tarjetas de Red:

Una vez instalado el sistema operativo Linux Slackware 12 ó 12.2 se debe configurar las dos tarjetas de red para que cumpla la función de Bastion home. Además, tener presente la lista de rangos de IPs de las clases A, B y C respectivamente, que tú vas ha eliges con que clase de IPs vas a trabajar, y que a continuación se detalla:

Clase	Rango inicio	Rango Final
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.0.0	223.255.255.0

Direcciones Privadas disponibles:

Clase	Rango inicio	Rango Final
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

1.- # ifconfig Al ejecutar ese comando vas a visualizar las tarjetas instaladas en tu sistema operativo Linux.
2.- Tener presente que Linux identifica a las tarjetas de la siguiente manera:

eth0 , eth1 etc.. eso está de acuerdo a las dos tarjetas de Red que vamos a configurar.

3.- # /etc/rc.d/rc.inet1.conf ir al fichero editando con
mcedit rc.inet1.conf (Presionar enter).

Tienes que adicionar la ip en el fichero rc.inet1.conf lo siguiente:

```
# config information for eth1:
  IPADDR[1]="172.16.0.1 "
  NETMASK[1]="255.255.0.0 "
  USE_DHCP[1]=""
  DHCP_HOSTNAME[1]=""
```

4.- # ip route ls vas a visualizar las dos tarjetas de red con su respectiva scope link. Además, te vas ha fijar quien tiene el default via , la cual te indica la red externa. En nuestro caso será eth0
5.- # route vas a visualizar las dos tarjetas de red lista para ser un Bastion Home
6.- # ping 172.16.0.1 tiene que responder (interface interna)
7.-# ping 192.168.1.8 tiene que responder (Esta ip es configurado cuando instalas el sistema operativo Linux según manual de instalación).
8.- Como las dos tarjetas ya están listas para ser un Firewall .Entonces se procede a instalar el shorewall.

Procedimiento Shorewall :

- Shorewall tiene el archivo principal **# /etc/shorewall/shorewall.conf**
- Shorewall usa el término de zona
  fw: Propio firewall
  net: Internet
  loc: La red local

1.- Para hacer el firewall con shorewall necesitas dos paquetes que es la siguiente:
- Shorewall-common
- Shorewal-perl (the newer and master compiler written in perl)

No obstante, la vas a encontrar en http://www.shorewall.net cuya opción es el siguiente:
- Download
- Download sites
- Buscar Seatle,Washington, USA FTP (Browse)
- Buscar dentro del ftp la carpeta 4.2
- Elegir shorewall-4.2.6
  Bajar **shorewall-common-4.2.6.tar.bz2**
  Bajar **shorewall-perl-4.2.6.2.tar.bz2**

2.- Desempaquetas los archivos con el siguiente comando:
tar –jxf shorewall-common-4.2.6.tar.bz2
tar –jxf shorewall-perl-4.2.6.2.tar.bz2

3.- Ir al directorio desempaquetado de shorewall-perl-4.2.6.2
4.- Dentro del **directorio shorewall-perl-4.2.6.2**
Escriba **./install.sh** (presionar enter para instalar)

```
root@flex:~/Desktop/shorewall-perl-4.2.6.2# ls
COPYING     Shorewall/     compiler.pl*  prog.footer   prog.functions   prog.header   rele
README.txt  changelog.txt  install.sh*   prog.footer6  prog.functions6  prog.header6  shor
root@flex:~/Desktop/shorewall-perl-4.2.6.2# ./install.sh
Installing Shorewall-perl Version 4.2.6.2

Compiler installed in /usr/share/shorewall-perl/compiler.pl
Module Shorewall/Accounting installed as /usr/share/shorewall-perl/Shorewall/Accounting.pm
Module Shorewall/Actions installed as /usr/share/shorewall-perl/Shorewall/Actions.pm
Module Shorewall/Chains installed as /usr/share/shorewall-perl/Shorewall/Chains.pm
Module Shorewall/Compiler installed as /usr/share/shorewall-perl/Shorewall/Compiler.pm
Module Shorewall/Config installed as /usr/share/shorewall-perl/Shorewall/Config.pm
Module Shorewall/IPAddrs installed as /usr/share/shorewall-perl/Shorewall/IPAddrs.pm
Module Shorewall/Nat installed as /usr/share/shorewall-perl/Shorewall/Nat.pm
Module Shorewall/Policy installed as /usr/share/shorewall-perl/Shorewall/Policy.pm
Module Shorewall/Proc installed as /usr/share/shorewall-perl/Shorewall/Proc.pm
Module Shorewall/Providers installed as /usr/share/shorewall-perl/Shorewall/Providers.pm
Module Shorewall/Proxyarp installed as /usr/share/shorewall-perl/Shorewall/Proxyarp.pm
Module Shorewall/Rules installed as /usr/share/shorewall-perl/Shorewall/Rules.pm
Module Shorewall/Tc installed as /usr/share/shorewall-perl/Shorewall/Tc.pm
Module Shorewall/Tunnels installed as /usr/share/shorewall-perl/Shorewall/Tunnels.pm
Module Shorewall/Zones installed as /usr/share/shorewall-perl/Shorewall/Zones.pm
Program skeleton file footer installed as /usr/share/shorewall-perl/prog.footer
Program skeleton file footer6 installed as /usr/share/shorewall-perl/prog.footer6
Program skeleton file functions installed as /usr/share/shorewall-perl/prog.functions
Program skeleton file functions6 installed as /usr/share/shorewall-perl/prog.functions6
Program skeleton file header installed as /usr/share/shorewall-perl/prog.header
Program skeleton file header6 installed as /usr/share/shorewall-perl/prog.header6
Shorewall-perl Version 4.2.6.2 Installed
root@flex:~/Desktop/shorewall-perl-4.2.6.2#
```

5.- Ahora entrar al directorio desempaquetado **shorewall-common-4.2.6**

6.- Dentro del directorio **shorewall-common-4.2.6**

Escriba **./install.sh** (presionar enter para instalar)

```
root@flex:~/Desktop# ls
Home.desktop    Text\ File                shorewall-common-4.2.6.tar.bz2  shutter-0.70.orig/
New\ Folder/    mozilla-firefox.desktop   shorewall-perl-4.2.6.2/         shutter_0.70~ppa11.orig.tar.gz
System.desktop  shorewall-common-4.2.6/   shorewall-perl-4.2.6.2.tar.bz2  trash.desktop
root@flex:~/Desktop# cd shorewall-common-4.2.6
root@flex:~/Desktop/shorewall-common-4.2.6# ls
COPYING             install.sb*         macro.GMhet         macro.NNTP          macro.SSH           restored
INSTALL             interfaces          macro.GRE           macro.NNTPS         macro.SVN           rfc1918
Makefile            ipsec               macro.Git           macro.NTP           macro.SixXS         route_rules
Makefile-lite       ipsecvpn            macro.Gnutella      macro.NTPbrd        macro.Submission    routestopped
README.txt          isusable            macro.HTTP          macro.OpenVPN       macro.Syslog        rules
Samples/            lib.base            macro.HTTPS         macro.PCA           macro.TFTP          shorewall*
accounting          lib.cli             macro.ICQ           macro.POP3          macro.Telnet        shorewall-common.spec
action.Drop         lib.config          macro.IMAP          macro.POP3S         macro.Telnets       shorewall.conf
action.Reject       lib.dynamiczones    macro.IMAPS         macro.PPtP          macro.Time          start
action.template     maclist             macro.IPIP          macro.Ping          macro.Trcrt         started
actions             macro.AllowICMPs    macro.IPP           macro.PostgreSQL    macro.VNC           stop
actions.std         macro.Amanda        macro.IPPserver     macro.Printer       macro.VNCL          stopped
blacklist*          macro.Auth          macro.IPsec         macro.RDP           macro.Web           strip*
changelog.txt       macro.BitTorrent    macro.IPsecah       macro.RNDC          macro.Webmin        swping
configpath          macro.BitTorrent32  macro.IPsecnat      macro.Rdate         macro.Whois         swping.init*
continue            macro.CVS           macro.IRC           macro.Reject        macro.template      tcclasses
default.debian      macro.DAAP          macro.JAP           macro.Rfc1918       manpages/           tcdevices
ecn                 macro.DCC           macro.JabberPlain   macro.Rsync         masq                tcfilters
fallback.sb*        macro.DNS           macro.JabberSecure  macro.SANE          modules             tcrules
firewall*           macro.Distcc        macro.Jabberd       macro.SMB           nat                 tos
hosts               macro.Drop          macro.Jetdirect     macro.SMBBI         netmap              tunnel*
init                macro.DropNoisy     macro.L2TP          macro.SMBswat       params              tunnels
init.archlinux.sb*  macro.DropUPnP      macro.LDAP          macro.SMTP          policy              uninstall.sb*
init.debian.sb*     macro.Edonkey       macro.LDAPS         macro.SMTPS         providers           wait4ifup*
init.sb*            macro.FTP           macro.Mail          macro.SNMP          proxyarp            zones
initdone*           macro.Finger        macro.MySQL         macro.SPAMD         releasenotes.txt
root@flex:~/Desktop/shorewall-common-4.2.6# ./install.sh_
```

7.- Hay que editar # / etc/ shorewall/shorewall.conf

mcedit shorewall.conf

```
root@flex:/# ls
bin/  boot/  dev/  etc/  home/  lib/  media/  mnt/  opt/  proc/  root/  sbin/  srv/  sys/  tmp/  usr/  var/
root@flex:/# cd etc/shorewall
root@flex:/etc/shorewall# mcedit shorewall.conf_
```

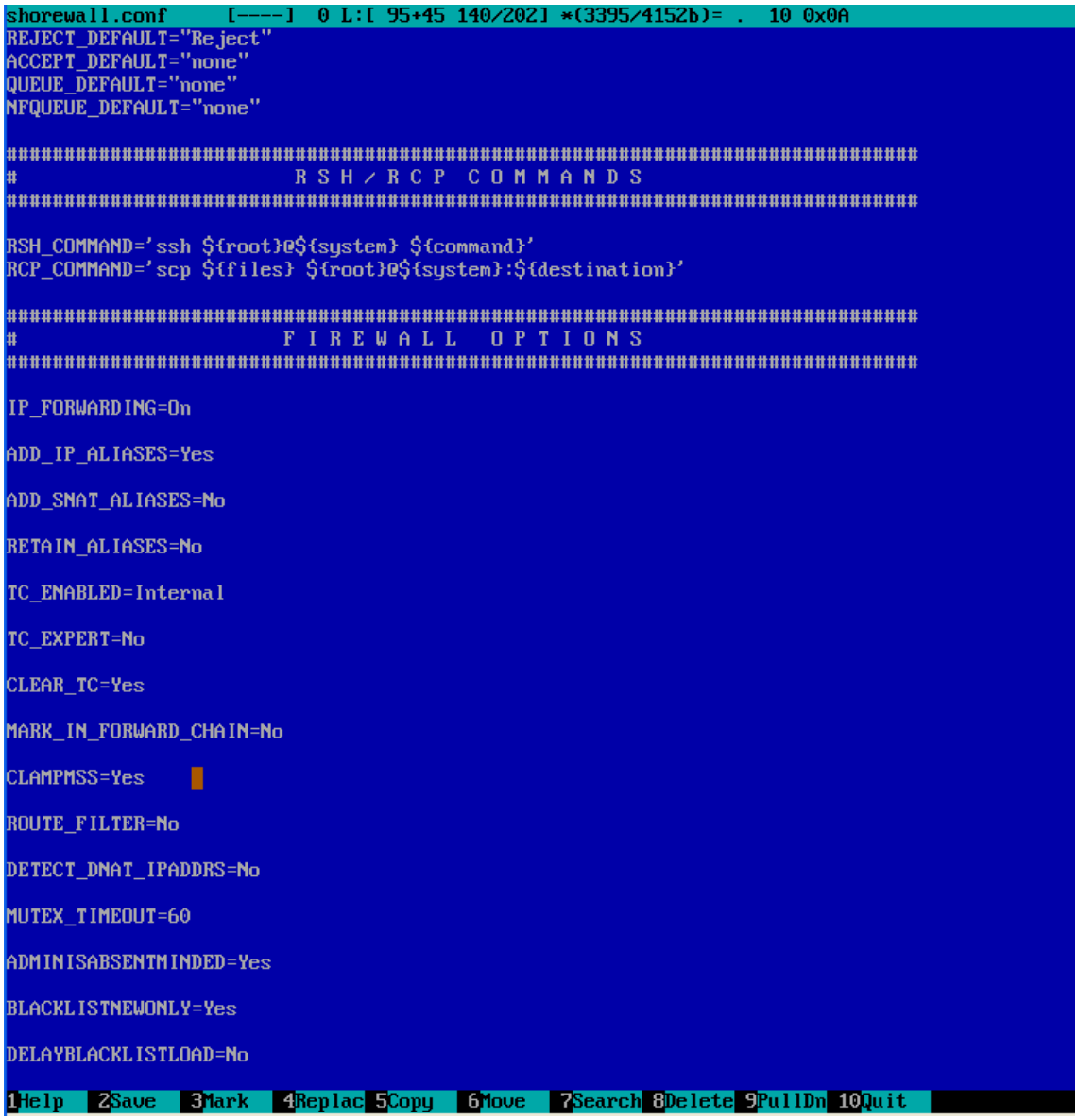
Dentro del fichero **shorewall.conf** tienes que buscar **ESTARTUP ENABLED**

- La vas a encontrar como ESTARTUP_ ENABLED=No
- La tienes que cambiar a **ESTARTUP_ ENABLED=Yes**

Así también buscar en el mismo fichero **shorewall.conf** FIREWALL OPTIONS

- La vas a encontrar como CLAMPMSS=No
- La tienes que cambiar **a** **CLAMPMSS=Yes**

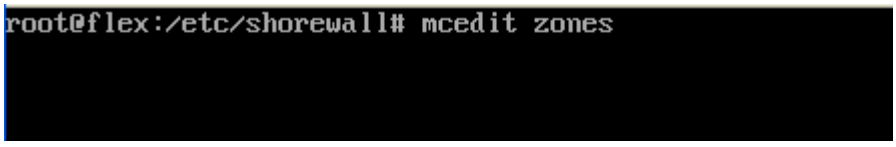
```
shorewall.conf     [----] 19 L:[  1+ 0   1/202] *(19  /4152b)= #  35 0x23
##############################################################################
#  /etc/shorewall/shorewall.conf Version 4 - Change the following variables to
#  match your setup
#
#  This program is under GPL
#  [http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt]
#
#  This file should be placed in /etc/shorewall
#
#  (c) 1999,2000,2001,2002,2003,2004,2005,
#      2006,2007,2008 - Tom Eastep (teastep@shorewall.net)
#
#  For information about the settings in this file, type "man shorewall.conf"
#
#  Additional information is available at
#  http://www.shorewall.net/Documentation.htm#Conf
##############################################################################
#                      S T A R T U P   E N A B L E D
##############################################################################

STARTUP_ENABLED=Yes

##############################################################################
#                              V E R B O S I T Y
##############################################################################

VERBOSITY=1

##############################################################################
#                              C O M P I L E R
#      (setting this to 'perl' requires installation of Shorewall-perl)
##############################################################################

SHOREWALL_COMPILER=

##############################################################################
#                              L O G G I N G
##############################################################################

LOGFILE=/var/log/messages

STARTUP_LOG=
```

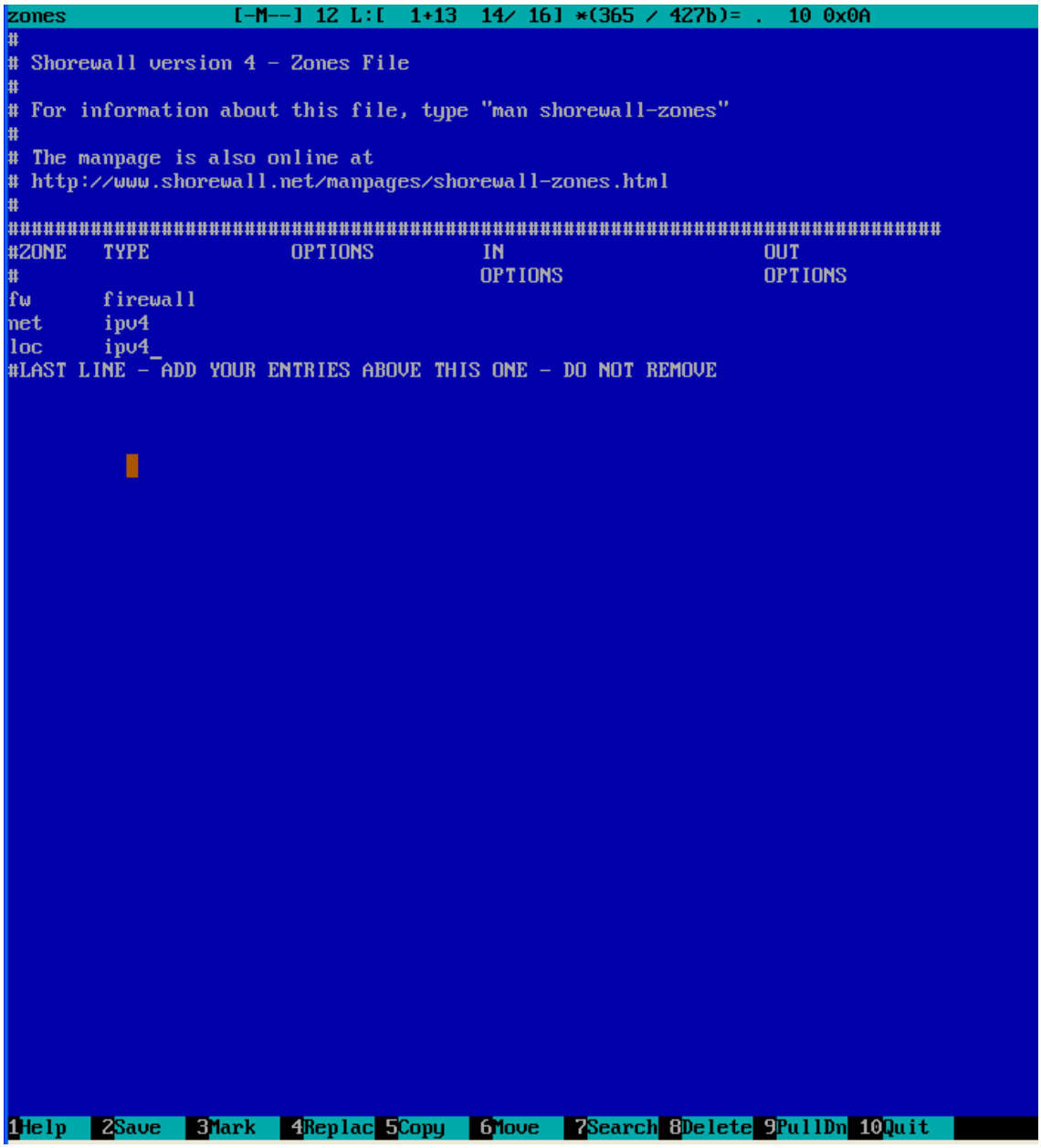


8.- Se tiene que configurar los siguientes ficheros :

/etc/shorewall/zones
#/etc/shorewall/interfaces
#/etc/shorewall/policy
#/etc/shorewall/rules
#/etc/shorewall/masq
#/etc/shorewall/routestopped

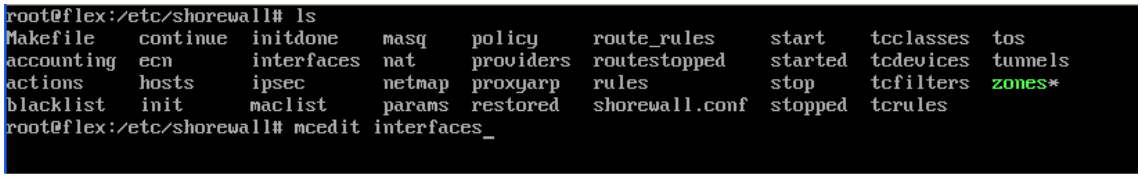
9.- editar #/etc/shorewall/zones para declarar las zonas de red.
#mcedit zones





10.- Editar #/etc/shorewall/interfaces para declarar las interfaces

#mcedit interfaces

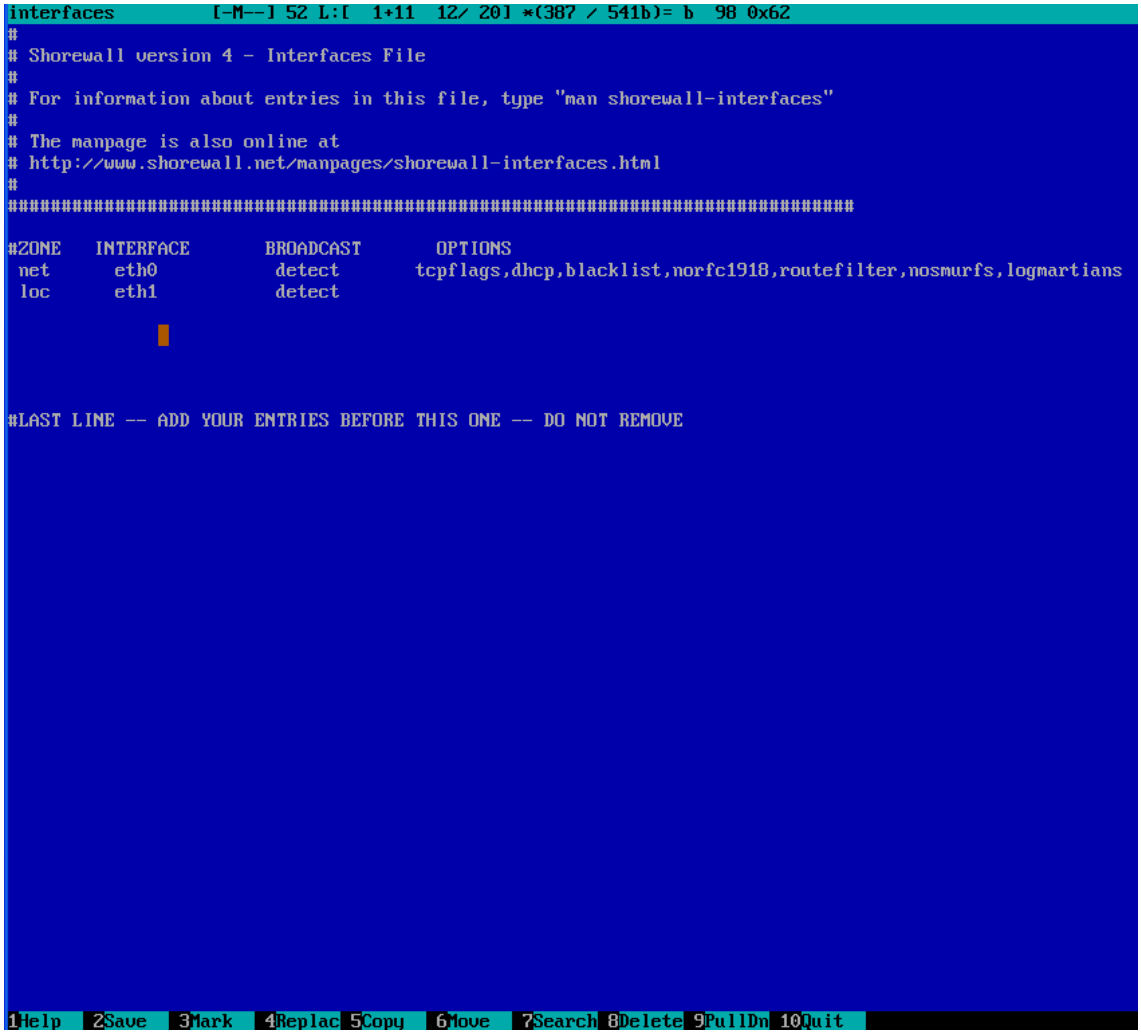


Las interfaces archivan servicios para definir el firewall. Es decir, las zonas que van a ser tomadas en cuenta por el firewall.

Web : http://configurarlinuxserver.com

Tcpflag: Paquetes o datos que ingresan a la interfaz eth0 se comprueban para saber si hay ciertas combinaciones ilegales de TCP flags.
Routefilter: Indica al núcleo que debe rechazar los paquetes de la interfaz cuya dirección de origen se haya encaminada de fuera .Es decir , con otra interfaz distinta.

Nosmurfs: Filtra paquetes que viene de un broadcast.
Blacklist: Es usado cuando en los registros log del sistema se observe alguna dirección IP del intruso que esté intentando ingresar a la red ; en ese momento tienes que ponerlo en la lista negra cuya dirección de fichero es #/etc/shorewall/blacklist .
Norfc1918: Le dice al núcleo de no enrutar direcciones especificas como las privadas.
Logmartians: Le indica al shorewall que registre paquetes y que va con la habilitación del routefilter.



Web : http://configurarlinuxserver.com

11.- Para visualizar la dirección IP de las interfaces o tarjetas de red efectuar los siguientes comandos :

ip route ls

```
root@flex:/etc/shorewall# ls
Makefile    continue  initdone    masq    policy     route_rules     start    tcclasses  tos
accounting  ecn       interfaces  nat     providers  routestopped    started  tcdevices  tunnels
actions     hosts     ipsec       netmap  proxyarp   rules           stop     tcfilters  zones*
blacklist   init      maclist     params  restored   shorewall.conf  stopped  tcrules
root@flex:/etc/shorewall# ip route ls
192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.8
172.16.0.0/16 dev eth1  proto kernel  scope link  src 172.16.0.1
127.0.0.0/8 dev lo  scope link
default via 192.168.1.1 dev eth0  metric 1
root@flex:/etc/shorewall#
```

ip addr ls dev eth0

```
root@flex:/etc/shorewall# ip addr ls dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:32:52:12 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.8/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe32:5212/64 scope link
       valid_lft forever preferred_lft forever
root@flex:/etc/shorewall#
```

ip addr ls dev eth1

```
root@flex:/etc/shorewall# ip addr ls dev eth1
3: eth1: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:dd:62:fa brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.1/16 brd 172.16.255.255 scope global eth1
    inet6 fe80::a00:27ff:fedd:62fa/64 scope link
       valid_lft forever preferred_lft forever
root@flex:/etc/shorewall# _
```

12.- Hay que verificar con el comando # shorewall check la configuración o compilación.

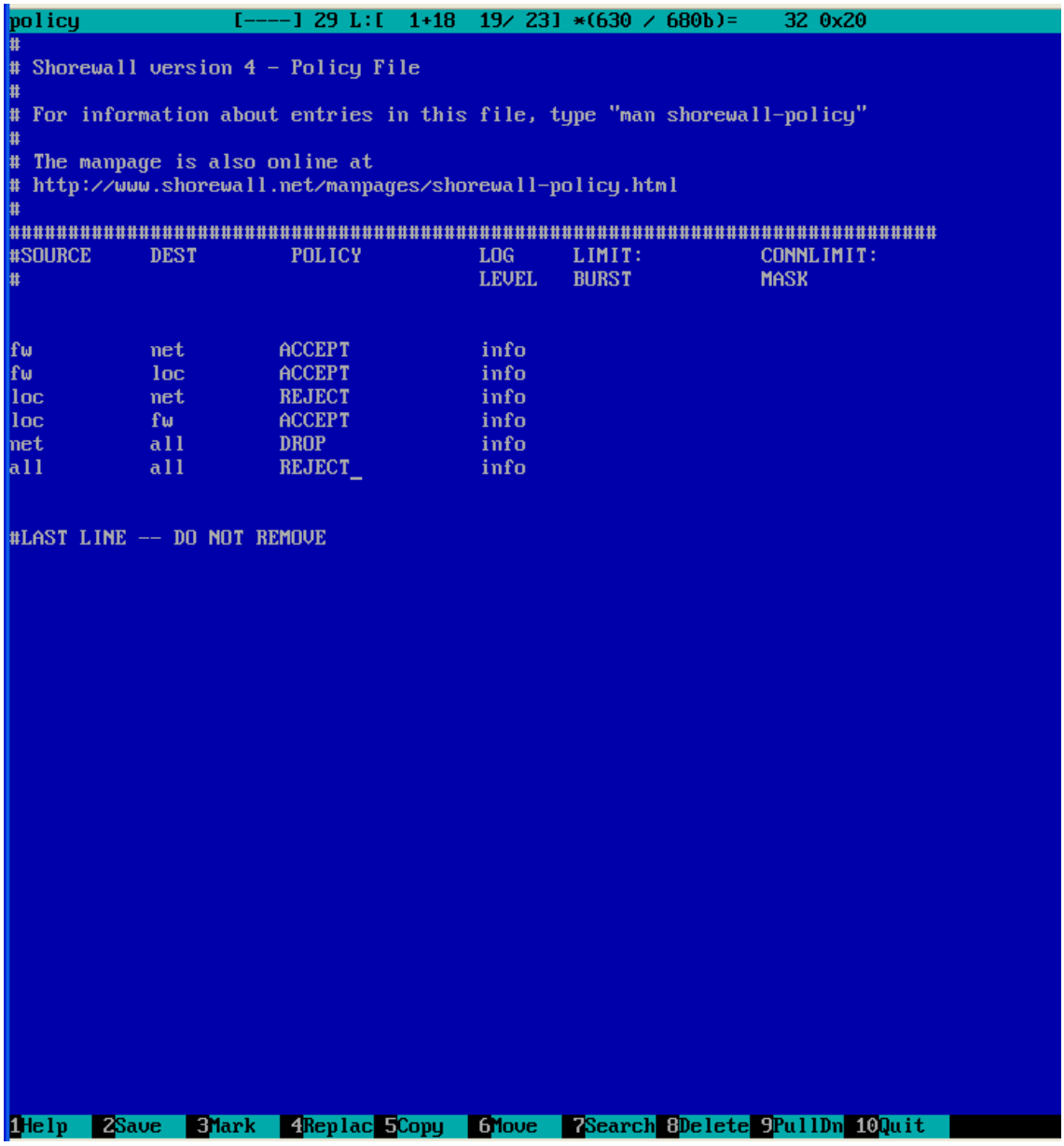
```
root@flex:/etc/shorewall# ls
Makefile    continue  initdone    masq    policy     route_rules     start    tcclasses  tos
accounting  ecn       interfaces  nat     providers  routestopped    started  tcdevices  tunnels
actions     hosts     ipsec       netmap  proxyarp   rules           stop     tcfilters  zones*
blacklist   init      maclist     params  restored   shorewall.conf  stopped  tcrules
root@flex:/etc/shorewall# shorewall check_
```

13.- Al hacer la complilación sale un error ya que falta la configuración de policy

```
root@flex:/etc/shorewall# ls
Makefile    continue  initdone    masq    policy     route_rules     start    tcclasses  tos
accounting  ecn       interfaces  nat     providers  routestopped    started  tcdevices  tunnels
actions     hosts     ipsec       netmap  proxyarp   rules           stop     tcfilters  zones*
blacklist   init      maclist     params  restored   shorewall.conf  stopped  tcrules
root@flex:/etc/shorewall# shorewall check
Checking...
Checking /etc/shorewall/zones...
Checking /etc/shorewall/interfaces...
Determining Hosts in Zones...
Preprocessing Action Files...
   Pre-processing /usr/share/shorewall/action.Drop...
   Pre-processing /usr/share/shorewall/action.Reject...
   ERROR: No policy defined from zone fw to zone net
root@flex:/etc/shorewall# _
```

14.- editar #/etc/shorewall/policy para dar políticas de acceso de una zona a otra.
#mcedit policy

```
root@flex:/etc/shorewall# ls
Makefile    continue  initdone    masq    policy     route_rules     start    tcclasses  tos
accounting  ecn       interfaces  nat     providers  routestopped    started  tcdevices  tunnels
actions     hosts     ipsec       netmap  proxyarp   rules           stop     tcfilters  zones*
blacklist   init      maclist     params  restored   shorewall.conf  stopped  tcrules
root@flex:/etc/shorewall# mcedit policy
```



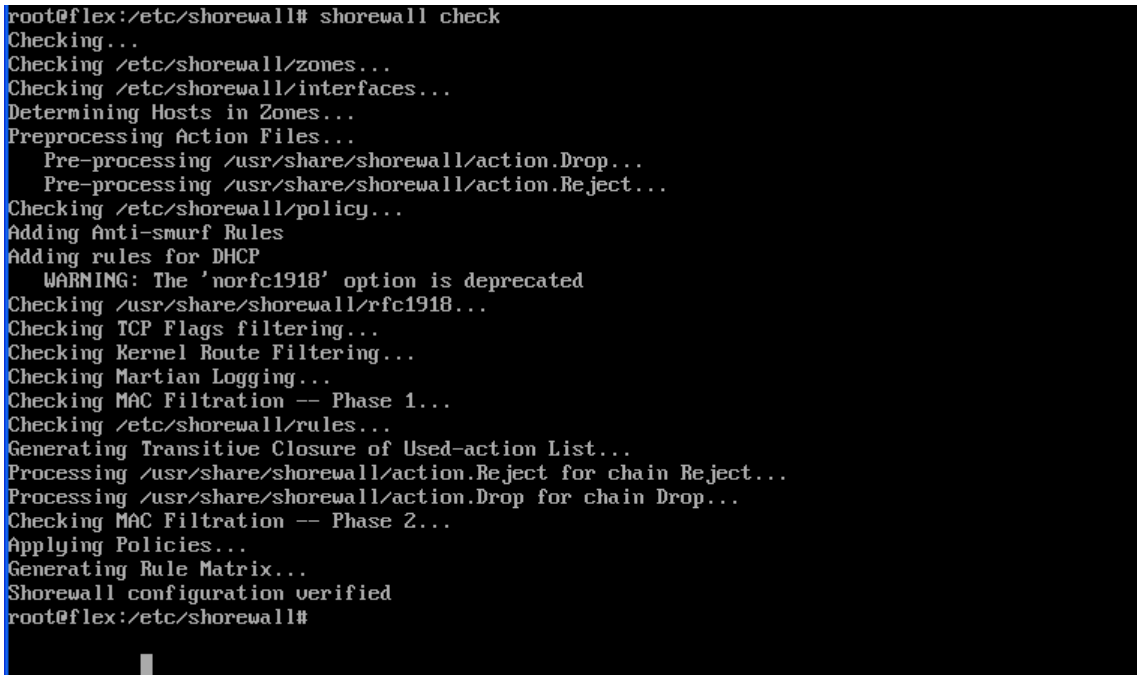
Tener presente en lo siguiente:

- **ACCEPT**: Indica aceptar la conexión.
- **DROP:** Escucha la conexión pero la ignora. Es decir, no le remite ningún mensaje al solicitante.
- **REJECT:** Rechaza la conexión pero le envía un mensaje al solicitante que ha sido rechazada.

15.- Usar para verificar los comandos siguientes:

shorewall check

shorewall show capabilities



```
root@flex:/etc/shorewall# shorewall show capabilities
Shorewall has detected the following iptables/netfilter capabilities:
   NAT: Available
   Packet Mangling: Available
   Multi-port Match: Available
   Extended Multi-port Match: Available
   Connection Tracking Match: Available
   Extended Connection Tracking Match Support: Not available
   Old Connection Tracking Match Syntax: Not available
   Packet Type Match: Available
   Policy Match: Available
   Physdev Match: Available
   Physdev-is-bridged Support: Available
   Packet length Match: Available
   IP range Match: Available
   Recent Match: Available
   Owner Match: Available
   Ipset Match: Not available
   CONNMARK Target: Available
   Extended CONNMARK Target: Available
   Connmark Match: Available
   Extended Connmark Match: Available
   Raw Table: Available
   IPP2P Match: Not available
   CLASSIFY Target: Available
   Extended REJECT: Available
   Repeat match: Available
   MARK Target: Available
   Extended MARK Target: Available
   Mangle FORWARD Chain: Available
   Comments: Available
   Address Type Match: Available
   TCPMSS Match: Available
   Hashlimit Match: Available
   NFQUEUE Target: Available
   Realm Match: Available
   Helper Match: Available
   Connlimit Match: Not available
   Time Match: Not available
   Goto Support: Available
root@flex:/etc/shorewall#
```

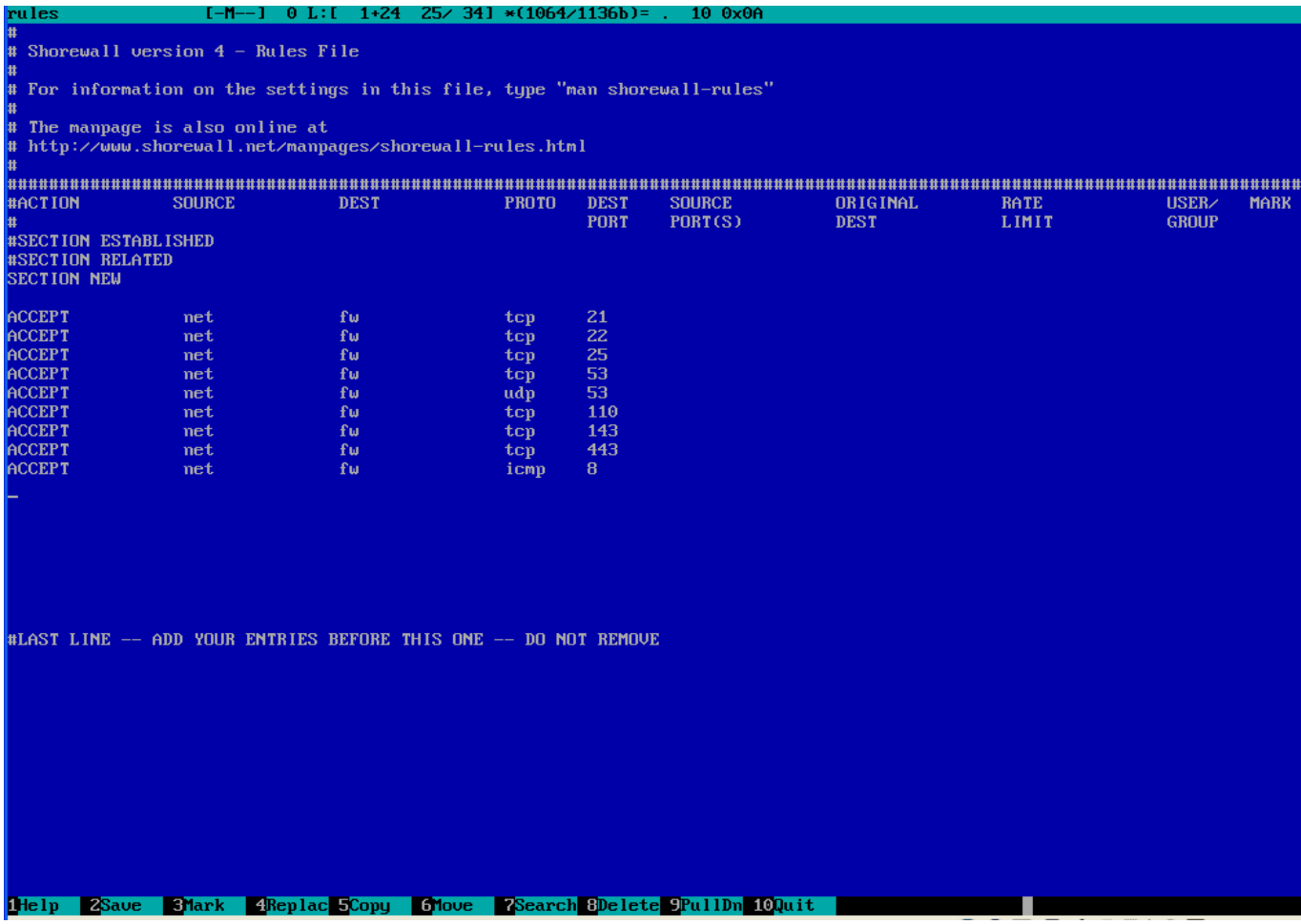
16.- editar #/etc/shorewall/rules para declarar la rules de red.

#mcedit rules

```
root@flex:/etc/shorewall# ls
Makefile    continue  initdone    masq    policy     route_rules     start    tcclasses  tos
accounting  ecn       interfaces  nat     providers  routestopped    started  tcdevices  tunnels
actions     hosts     ipsec       netmap  proxyarp   rules           stop     tcfilters  zones*
blacklist   init      maclist     params  restored   shorewall.conf  stopped  tcrules
root@flex:/etc/shorewall# mcedit rules
```

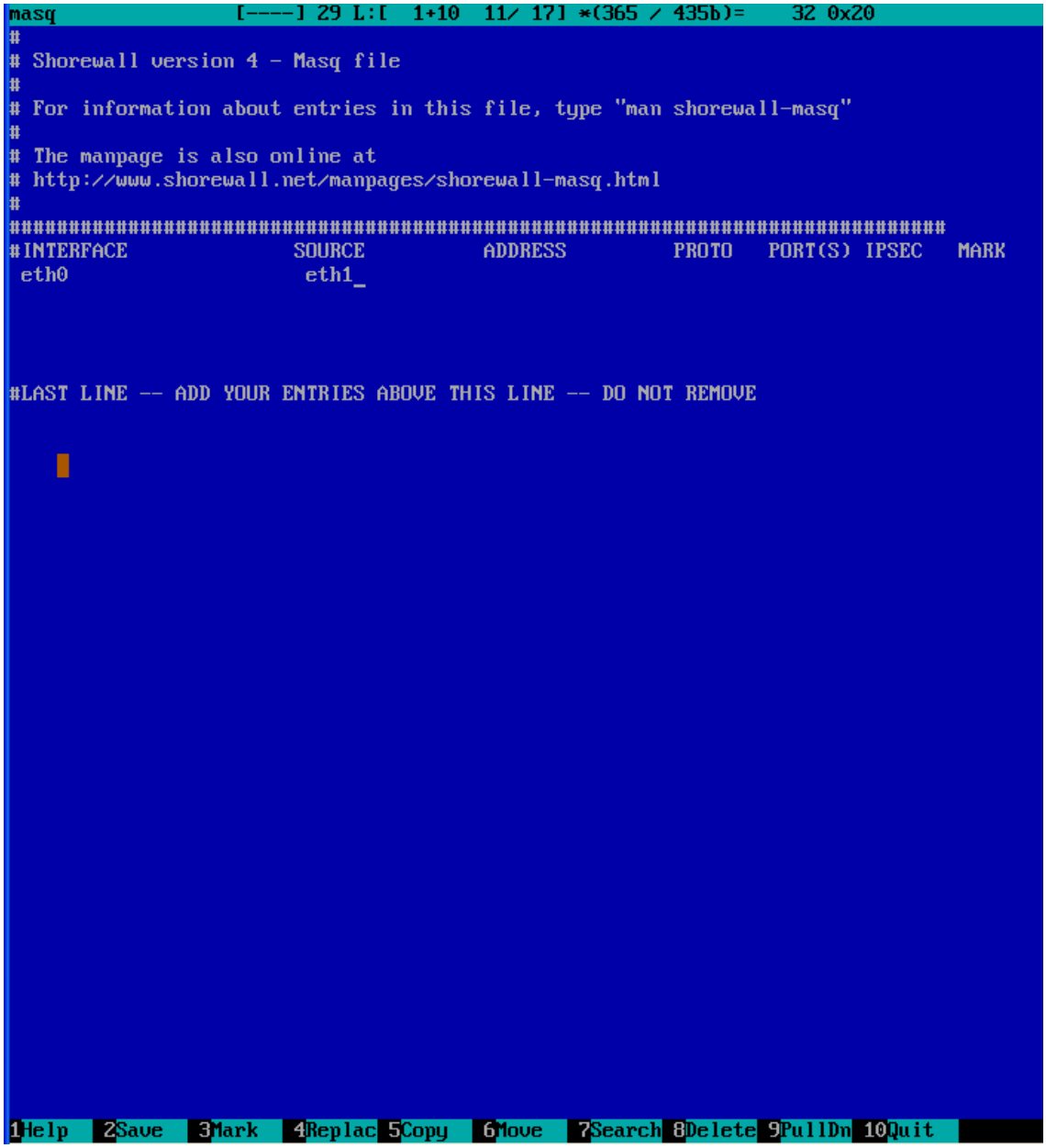
En el fichero rules se definen las reglas que permitirán o denegarán el acceso a servicios y puertos desde , y hacia zonas del firewall.
El script permite SMTP, HTTPS, NTP, POP3, ICMP(8) desde la Internet para el firewall.
Tener presente de lo siguiente:

SSH es el puerto 22
WWW es el puerto 80
HTTPS es el puerto 443

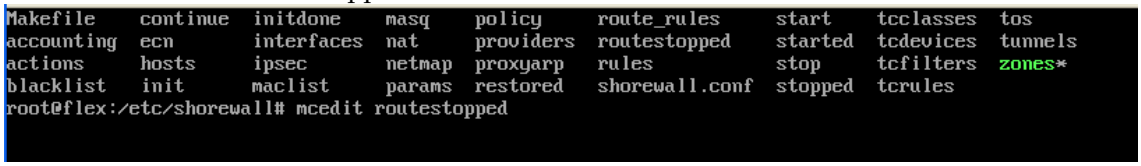


17.- editar #/etc/shorewall/masq para declarar dinámicamente los NAT y el origen NAT.
#mcedit masq

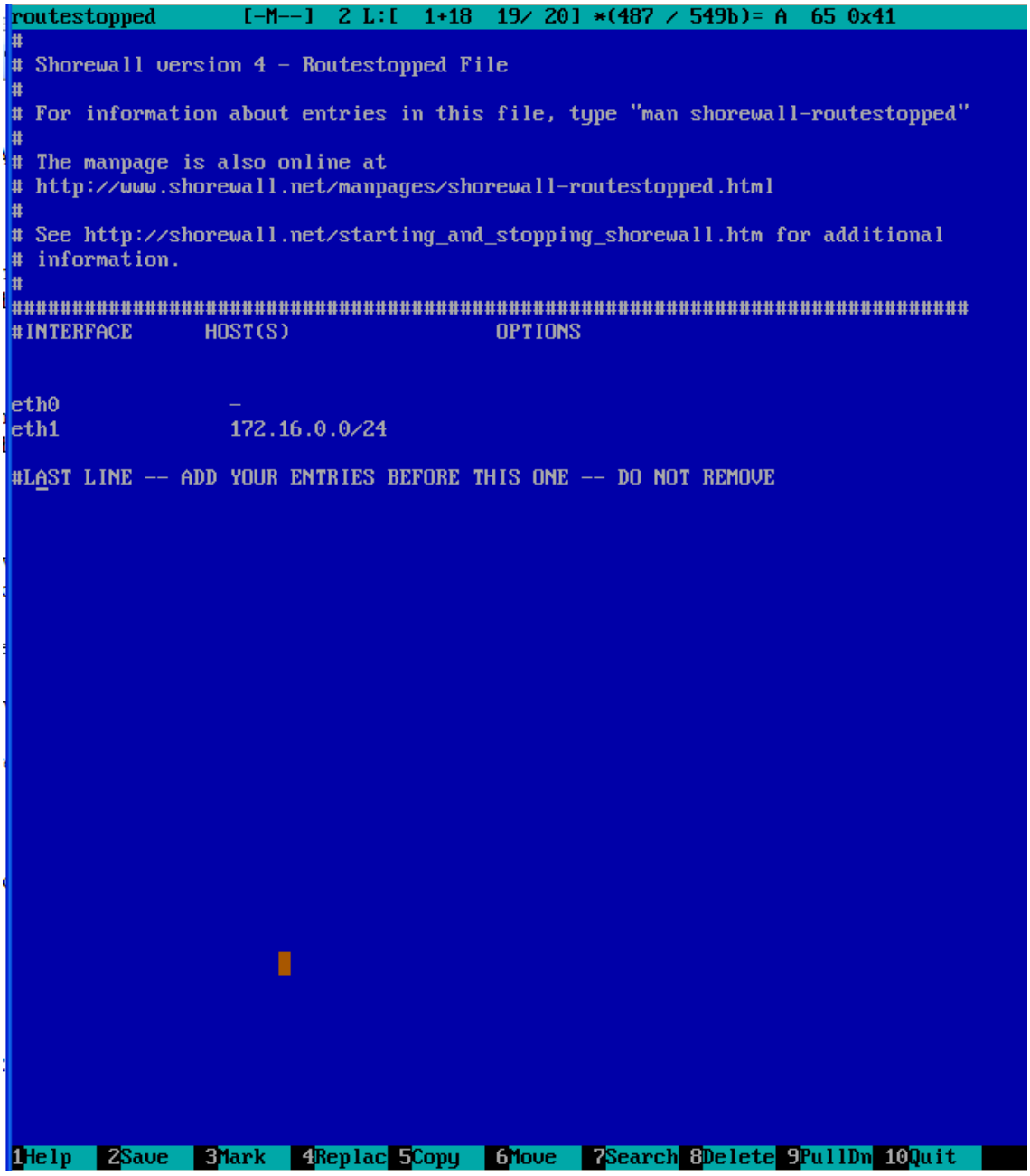
```
root@flex:/etc/shorewall# ls
Makefile    continue  initdone    masq     policy     route_rules     start    tcclasses  tos
accounting  ecn       interfaces  nat      providers  routestopped    started  tcdevices  tunnels
actions     hosts     ipsec       netmap   proxyarp   rules           stop     tcfilters  zones*
blacklist   init      maclist     params   restored   shorewall.conf  stopped  tcrules
root@flex:/etc/shorewall# mcedit masq
```



18.- editar #/etc/shorewall/routestopped para definir a los anfitriones que son accesibles cuando se detiene o se está parando el firewall.
#mcedit routestopped



Web : http://configurarlinuxserver.com



30.- Hay que iniciar el firewall escribiendo el siguiente comando:

shorewall start

Ya tienes instalado un Firewall en Linux Server y listo para utilizar la poderosa seguridad de alto nivel. Además , te sugiero que uses la herramienta **webmin** para administrar de forma gráfica y amigable el Linux Server y el Firewall.

Web : http://configurarlinuxserver.com

Procedimiento WEBMIN :

Desempaquetar el archivo webmin-1.460.tar.gz de la siguiente manera:

1.- # tar xzfv webmin-1.460.tar.gz
2.- Estar dentro del archivo desempaquetado webmin-14.60
3.- ./setup.sh

```
root@flex:~/Desktop/webmin-1.460# ./setup.sh_
```

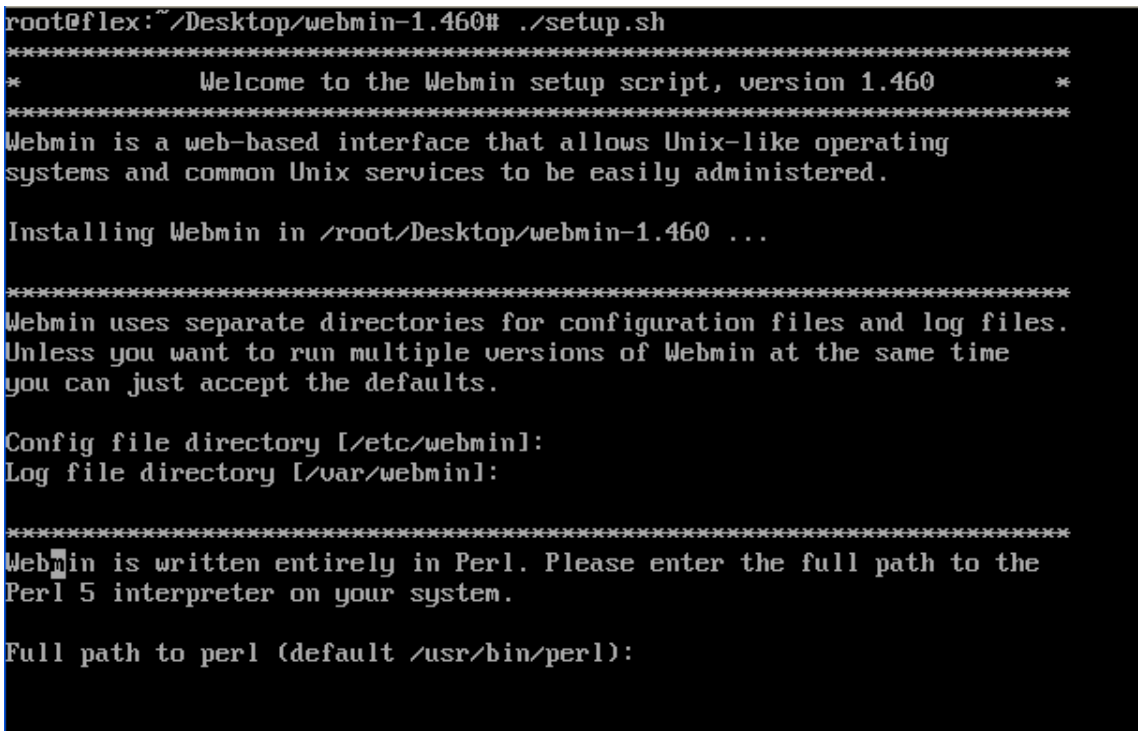
4.- Presionar enter para continuar en [/etc/webmin]:

```
root@flex:~/Desktop/webmin-1.460# ./setup.sh
*******************************************************************************
*            Welcome to the Webmin setup script, version 1.460                *
*******************************************************************************
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.

Installing Webmin in /root/Desktop/webmin-1.460 ...

*******************************************************************************
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.

Config file directory [/etc/webmin]: _
```

5.- Presionar enter para continuar en [/var/webmin]:

```
root@flex:~/Desktop/webmin-1.460# ./setup.sh
*******************************************************************************
*            Welcome to the Webmin setup script, version 1.460                *
*******************************************************************************
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.

Installing Webmin in /root/Desktop/webmin-1.460 ...

*******************************************************************************
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.

Config file directory [/etc/webmin]:
Log file directory [/var/webmin]:
```

6.- Presionar enter para continuar en [/usr/bin/perl]:



7.- Presionar enter en Web Server port (default 10000) para continuar .

8.- En la opción Login name (default admin) debes poner un nombre de usuario. Para el ejemplo que se llame **australia.**

9.- Tienes de poner un password para tu usuario australia

```
root@flex:~/Desktop/webmin-1.460# ./setup.sh
*******************************************************************************
*            Welcome to the Webmin setup script, version 1.460        *
*******************************************************************************
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.

Installing Webmin in /root/Desktop/webmin-1.460 ...

*******************************************************************************
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.

Config file directory [/etc/webmin]:
Log file directory [/var/webmin]:

*******************************************************************************
Webmin is written entirely in Perl. Please enter the full path to the
Perl 5 interpreter on your system.

Full path to perl (default /usr/bin/perl):

Testing Perl ...
Perl seems to be installed ok

*******************************************************************************
Operating system name:    Slackware Linux
Operating system version: 12.0.0

*******************************************************************************
Webmin uses its own password protected web server to provide access
to the administration programs. The setup script needs to know :
 - What port to run the web server on. There must not be another
   web server already using this port.
 - The login name required to access the web server.
 - The password required to access the web server.
 - If the webserver should use SSL (if your system supports it).
 - Whether to start webmin at boot time.

Web server port (default 10000):
Login name (default admin): australia
Login password:
Password again:
```

Por Wilmer Huamaní Córdova

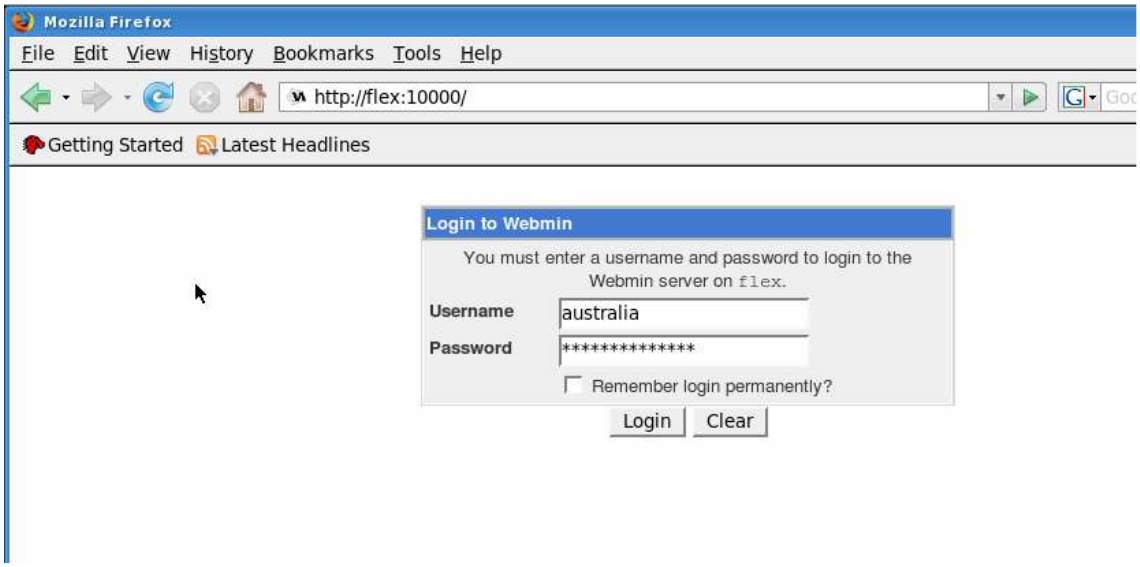
Web : http://configurarlinuxserver.com

10.- Escribir la letra **(y)** en la opción Start webmin at boot time(y/n)

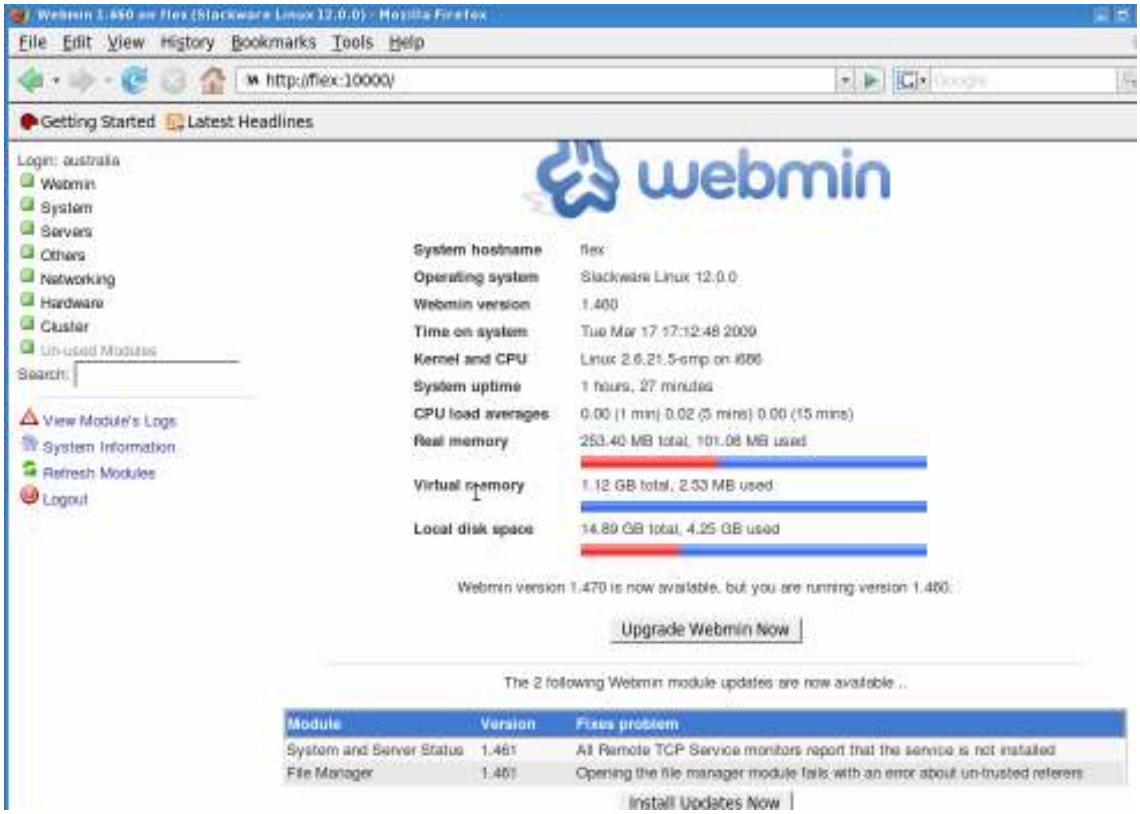
11.- Se instala el webmin con éxito.

```
******************************************************************************
Creating web server config files..
..done

Creating access control file..
..done

Inserting path to perl into scripts..
..done

Creating start and stop scripts..
..done

Copying config files..
..done

Configuring Webmin to start at boot time..
..done

Creating uninstall script /etc/webmin/uninstall.sh ..
..done

Changing ownership and permissions ..
..done

Running postinstall scripts ..
Can't load /etc/samba/smb.conf - run testparm to debug it
Can't load /etc/samba/smb.conf - run testparm to debug it
Can't load /etc/samba/smb.conf - run testparm to debug it
Can't load /etc/samba/smb.conf - run testparm to debug it
Can't load /etc/samba/smb.conf - run testparm to debug it
Can't load /etc/samba/smb.conf - run testparm to debug it
..done

Attempting to start Webmin mini web server..
Starting Webmin server in /root/Desktop/webmin-1.460
Pre-loaded WebminCore
..done

******************************************************************************
Webmin has been installed and started successfully. Use your web
browser to go to

  http://flex:10000/

and login with the name and password you entered previously.

root@flex:~/Desktop/webmin-1.460#
```

12.- En el browser de mozila escribir http://flex:10000. Además , ingresar usuario y password.



13.- El webmin está listo para que puedas administrar amigablemente Linux Server y tú Firewall que recién has instalado. Disfruta del maravilloso poder del Firewall con shorewall.



Por Wilmer Huamaní Córdova

Web : http://configurarlinuxserver.com