

Instituto Tecnológico Las Américas

(ITLA)

Sistemas Operativos 3 (SO3)

Daniel Alejandro Moreno Martínez

Matrícula: 2010-2946



## How to

iii 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. **Standard Firewall** 



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/



<u> </u>	Ind	ex of /pub/shorewall - Se	aMonkey		- = ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew	r <u>G</u> o <u>B</u> ookmarks <u>T</u> ools	s <u>W</u> indow <u>H</u> elp			
Back Forward	Reload Stop	://shorewall.net/pub/shore	wall/	▼ 🙇 Search 🍏 Prin	, - 🍠
🚺 🚮 Home 🛛 🦋 Boo	kmarks 🦧 CentOS 🖆 Sup	port			
	Name	Last modified	Size Description		*
Parent Directo	<u>ory</u>		-		
<u>3.4/</u>		01-Mar-2008 13:57	-		
<u>4.0/</u>		15-Dec-2008 18:37	1 -		
<u>4.2/</u>		05-Sep-2009 13:11	-		
<u> 4.4/</u>		07-Jan-2012 12:23	5 -		
<u>4.5/</u>		10-Apr-2012 07:14	Presionan	nos click en esta	narte
	STABLE_VERSION_IS_	4.5/ 10-Apr-2012 07:14	ricsionan	ios chek en esta	parte.
HEADER.htm	<u>nl</u>	14-Aug-2009 06:32	394		
contrib/		23-May-2011 07:49	) _		
development/		02-Jan-2012 08:24	+ -		
errata/		21-Aug-2007 13:52	-		
misc/		29-Oct-2007 08:41	-		
		22 4 85 2002 11:20			
🐝 🥩 http:/	/shorewall.net/pub/shorewall/	CURRENT_STABLE_VE	RSION_IS_4.5/		- <b>)</b> - <b>6</b>

😵 Aplicaciones 🛛 Acciones 🥹 🕸		🐼 lun 9 de abr, 00:35 🔇
Index of /p	ub/shorewall/4.4/shorewall-4.4.2 - SeaMonkey	
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>B</u> ookmarks <u>T</u> o	ools <u>W</u> indow <u>H</u> elp	
Back - Forward Reload Stop	ttp://shorewall.net/pub/shorewall/4.4/shorewall 4.4.2	🧆 Search 📑 👻 🍠
🕺 🖞 Home 🛛 😻 Bookmarks 🥒 CentOS 🖆 S	upport	
errata/	02-Oct-2009 07:20 -	<b>▲</b>
known_problems.txt	23-Oct-2009 11:50 1.0K	
2 patch-4.4.2	02-Oct-2009 07:20 63K	
<b>patch-4.4.2.1</b>	03-Oct-2009 10:18 4.6K	
Patch-4.4.2.2	03-Oct-2009 12:18 5.5K	1
<b>patch-4.4.2.3</b>	17-Oct-2009 09:50 13K	
<b>patch-4.4.2.4</b>	23-Oct-2009 11:50 5.1K	
patch-6-4.4.2	02-Oct-2009 07:20 26K	
patch-6-lite-4.4.2	02-Oct-2009 07:20 20K	
patch-lite-4.4.2	02-Oct-2009 07:20 20K	
releasenotes.txt	23-Oct-2009 11:50 41K	
shorewall-4.4.2-1.noarch.rpm	03-Oct-2009 10:18 304K	
shorewall-4.4.2-2.noarch.rpm	03-Oct-2009 12:18 304k Presionamos	click on osta narto
shorewall-4.4.2-3.noarch.rpm	17-Oct-2009 09:50 304k	ener en esta parte.
	22 0-+ 2000 11-50 2041	▼
http://shorewall.net/pub/shorew	all/4.4/shorewall-4.4.2/shorewall-4.4.2-1.noarch.rpm	<b></b>
剩 月 🛗 Index of /pub/shorewall/4.4/shorewal	I-4.4.2 - SeaMonkey	

Opening shorewall-4.4.2-1.noard	ch.rpm	/////// ×
The file "shorewall-4.4.2-1.noarch.rpm" is of type application/x-redhat-package-manager (RPM package), an know how to handle this file type. This file is located at:	d SeaMonkey	does not 😰
http://shorewall.net		
What should SeaMonkey do with this file?		
Open it with the default application (Install Packages)		
O Open it with		<u>C</u> hoose
$\bigcirc$ <u>S</u> ave it to disk		
$\Box$ <u>A</u> lways perform this action when handling files of this t	ype	
Γ	ОК	Cancel

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.

roc	ot@dns:/etc/shorewall	<b>)</b> [X
<u>A</u> rchivo <u>E</u> ditar <u>V</u> er <u>T</u> erminal <u>S</u> olap	as A <u>y</u> uda	
[Daniel@dns ~]\$ su - Password: [root@dns ~]# cd /etc/shorewall/ [root@dns shorewall]# [root@dns shorewall]# gedit shor	rewall.conf	*

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

```
shorewall.conf ×
 (c) 1999,2000,2001,2002,2003,2004,2005,
                                             ٠
    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
ENABLED
              STARTUP
STARTUP_ENABLED=No
****************
                  VERBOSITY
******************
VERBOSITY=1
.
                                Ln 18, Col 50
                                         INS
```

Debemos cambiar el parámetro de **STARTUP\_ENABLED=NO** a **YES** para activar nuestro firewall.



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

🛅 shorewall.conf* 🗙	🗇 shorewall.conf* 🗙
CLAMPMSS=No	CLAMPMSS=Yes

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

				root@	odns:/etc/shorewall	
<u>A</u> rchivo	<u>E</u> ditar	<u>V</u> er	<u>T</u> erminal	<u>S</u> olapas	A <u>y</u> uda	
[root@dr	ns shor	ewal	l]# gedit	zones		*

Podemos ver que nos aparecerá el archivo de configuración.

```
zones ×
# Shorewall version 4 - Zones File
#
# For information about this file, type "man shorewall-zones"
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-zones.html
#ZONE
      TYPE
                  OPTIONS
                               IN
                                                  OUT
#
                               OPTIONS
                                                  OPTIONS
fw
      firewall
```

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**.

```
zones* ×
#
 Shorewall version 4 - Zones File
#
#
#
 For information about this file, type "man shorewall-zones"
#
# The manpage is also online at
 http://www.shorewall.net/manpages/shorewall-zones.html
#
#ZONE
      TYPE
                   OPTIONS
                                ΤN
                                                    OUT
#
                                OPTIONS
                                                    OPTIONS
fw
      firewall
net
      ipv4
loc
      ipv4
```

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

	root@dns:/etc/shorewall	
<u>A</u> rchivo <u>E</u> ditar <u>V</u> er <u>T</u> ermir	al <u>S</u> olapas A <u>y</u> uda	
[root@dns shorewall]# ge	dit interfaces	<u>^</u>

Nos aparecerá el archivo de configuración.

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

La interfaz **etho** 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**.

🛅 interfaces\* 🗙

```
#
# Shorewall version 4 - Interfaces File
# For information about entries in this file, type "man shorewall-
interfaces"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-interfaces.html
#ZONE
      INTERFACE
                   BROADCAST
                                OPTIONS
                   detect
loc
      eth0
                   detect
                                dhcp
net
      eth1
```

♥ /////				root@	dns:/etc/shorewall	
<u>A</u> rchivo	<u>E</u> ditar	<u>V</u> er	<u>T</u> erminal	<u>S</u> olapas	A <u>y</u> uda	
[root@dr	ns shor	rewal	l]# gedit	t policy		*

A continuación vemos el archivo de configuración.

```
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
```

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.

```
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
            ACCEPT
|fw
      net
```

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

```
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
fw
             ACCEPT
      net
                          info
      all
             DROP
net
```

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

Dicy*	×				
#					
# Shore	wall ver	sion 4 - Pol	licy File		
#					
# For in	nformati	on about ent	tries in this	file, type	e "man shorewall-policy"
#					
# The ma	anpage i	s also onlir	ne at		
# http:/	//www.sh	orewall.net/	/manpages/sho	rewall-pol:	.cy.html
#					
#######	########	############	#######################################	##########	*######################################
#SOURCE	DEST	POLICY	LOG	LIMIT:	CONNLIMIT:
#			LEVEL	BURST	MASK
fw	net	ACCEPT			
net	all	DROP	info		
all	all	REJECT	info		

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**.

$\mathbf{\nabla}$					root@	dns:/etc/shorewall	- • ×
A	rchivo	<u>E</u> ditar	<u>V</u> er	<u>T</u> erminal	<u>S</u> olapas	A <u>y</u> uda	
[r	oot@dr	ns shoi	rewal	l]# gedit	t masq		*

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/
#
                   eth0
eth1
```

Guardamos y salimos.

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

Shorewall check.

root@dns:~ Archivo Editar Ver Terminal Solapas Ayuda [root@dns ~]# 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... Checking /etc/shorewall/policy... Adding rules for DHCP Checking Kernel Route Filtering... Checking Martian Logging... Checking MAC Filtration -- Phase 1... Checking /etc/shorewall/rules... Generating Transitive Closure of Used-action List... Processing /usr/share/shorewall/action.Reject for chain Reject... Processing /usr/share/shorewall/action.Drop for chain Drop... Checking MAC Filtration -- Phase 2... Applying Policies... Shorewall configuration verified [root@dns ~]#

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.** 

				root@	@dns:/etc/shorewall	
<u>A</u> rchivo	<u>E</u> ditar	<u>V</u> er	<u>T</u> erminal	<u>S</u> olapas	A <u>y</u> uda	
[root@dn [root@dn	ıs ~]# ıs shor	cd /e ewal:	etc/shore 1]# gedi1	ewall/ t policy	y l	*

```
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
                                                 CONNLIMIT:
                                   LIMIT:
                            LEVEL
                                   BURST
                                                 MASK
#
       fw
              ACCEPT
net
fw
       net
              ACCEPT
                              Aquí rechazamos todo tráfico que
loc
       fw
              ACCEPT
all
       loc
              REJECT
                              venga de internet hacia la zona local.
              ACCEPT
loc
       net
```

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.

 $\underline{http://loquitoslack.blogspot.com/2011/06/instalar-shorewall-en-centos-install.html}$ 

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-dosinterfaces-de-red-con-politicas-drop-en-centos-y-debian.html