

# Configuración de shorewall

Shorewall es una herramienta de alto nivel que permite configurar netfilter de una forma más cómoda que utilizando directamente netfilter.

Esta guía describe los pasos necesarios para llevar a cabo una configuración relativamente simple en la que se dispone de un equipo (que hará las veces de firewall) con dos interfaces de red, una conectada directamente a internet y la otra a una red local. Además, la primera de ellas estará configurada en modo bridge debido a que en dicha máquina se ejecutan varias máquinas virtuales que utilizan dicha interfaz de red.

## Instalación de Shorewall

Para la instalación descrita basta con instalar el paquete shorewall.

```
emerge -av shorewall
```

## Configuración de Shorewall

Los archivos de configuración de Shorewall están en el directorio `/etc/shorewall`. Los ficheros que será necesario modificar son:

- `/etc/shorewall/zones`
- `/etc/shorewall/interfaces`
- `/etc/shorewall/masq`
- `/etc/shorewall/policy`
- `/etc/shorewall/shorewall.conf`

El fichero `zones` define las zonas sobre las que va a actuar Shorewall y su tipo. Para la configuración anterior necesitamos definir 3 zonas: la máquina en sí (`fw`), la red externa (`net`) y la red local (`loc`):

[/etc/shorewall/zones](#)

```
#####  
#####  
#ZONE TYPE          OPTIONS          IN          OUT  
#                   OPTIONS          OPTIONS  
fw  firewall  
net ipv4  
loc ipv4
```

El fichero `interfaces` define las interfaces de red utilizadas por aquellas zonas que no son del tipo `firewall`:

[/etc/shorewall/interfaces](#)

| #ZONE | INTERFACE | OPTIONS          |
|-------|-----------|------------------|
| net   | br0       | routeback,bridge |
| loc   | eno2      |                  |

El fichero `policy` define las políticas. El siguiente ejemplo permite prácticamente cualquier comunicación (la única que realmente se impide es el acceso desde la red externa a la local):

[/etc/shorewall/interfaces](#)

```
#####  
#####  
#SOURCE  DEST    POLICY      LOG    LIMIT:      CONNLIMIT:  
#        LEVEL   BURST      MASK  
loc net    ACCEPT  
fw  net    ACCEPT  
net fw     ACCEPT  
fw  loc    ACCEPT  
loc fw     ACCEPT  
net all    DROP      info  
all all    REJECT    info
```

From:

<https://lorca.act.uji.es/dokuwiki/> - Wiki de Lorca

Permanent link:

<https://lorca.act.uji.es/dokuwiki/doku.php/gentoo:shorewall?rev=1421683323>Last update: **2015/01/19 16:02**