

Practica 09. Shorewall: Doble firewall con DMZ

Seguridad de Sistemas Informáticos

Carlos Pérez Fino y Cheuk Kelly Ng Pante

3 de diciembre de 2023

Índice general

1. Configuración de red con dos firewalls y tres zonas	1
1.1. Configuración de la red en el firewall externo	1
1.2. Configuración de la red en el firewall interno	2
1.3. Resultado de la configuración de la red en el firewall externo e interno	2
2. Habilitar <i>NAT</i> utilizando la configuración de <i>Shorewall</i>	3
3. Configurar el cliente en la red interna y servidor en la DMZ	5
3.1. Configuración del cliente en la red interna	5
3.2. Configuración del servidor en la DMZ	5
4. Configurar el firewall con unas políticas por defecto:	7
5. Configurar reglas utilizando Macros para permitir el tráfico necesario	10
6. Bibliografía	11

1. Configuración de red con dos firewalls y tres zonas

Esta práctica se va a realizar una configuración de un firewall con DMZ utilizando *Shorewall* y *firewalld*. Se va a implementar un diseño con doble firewall (Interno con *firewalld* y externo con *Shorewall*) con dos interfaces para gestionar las zonas de Internet, DMZ y LAN. La DMZ se localiza entre los dos firewalls configurados.

Se va a partir del siguiente diseño de red con dos firewalls y tres zonas:

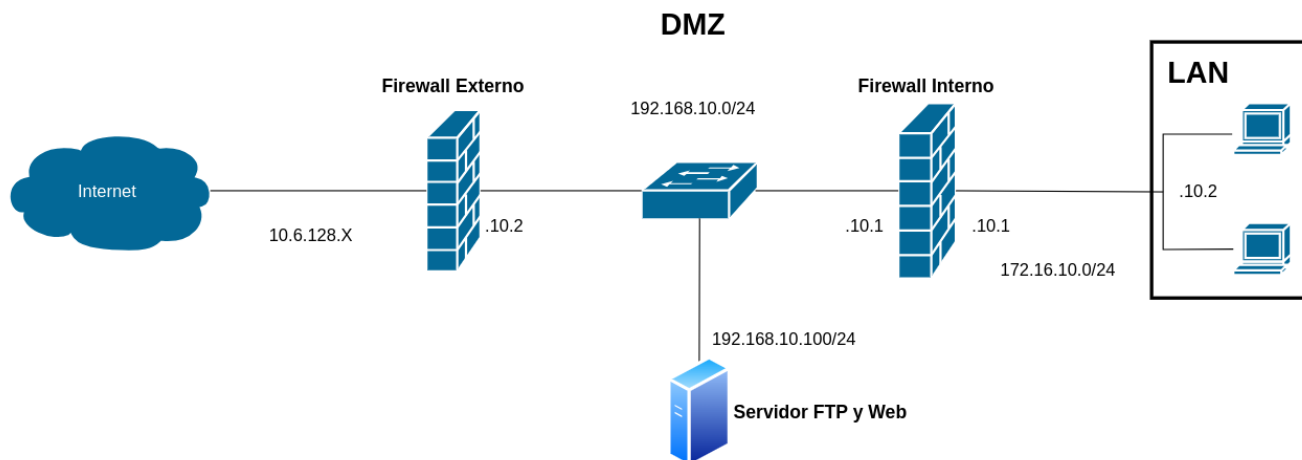


Figura 1.1: Diseño de red con dos firewalls y tres zonas

Esta red tendrá tres zonas: *priv* para la red interna, *fw* para el firewall y *dmz* para la DMZ, con el siguiente direccionamiento:

- **Internet:** la red especificada por el servidor DHCP externo.
- **Red Interna:** Clase C privada como subred de una clase B privada: 172.16.X.0/24.
- **DMZ:** Clase C privada 192.168.X.0/24.

1.1. Configuración de la red en el firewall externo

Para la configuración de la red en el firewall externo, se va a configurar la interfaz que va conectada a la DMZ, para ello se va a configurar el archivo `/etc/network/interfaces` con la siguiente configuración:

```
auto ens4
iface ens4 inet static
    address 192.168.10.2
    netmask 255.255.255.0
```

Una vez configurada la interfaz, se va reiniciar el servicio de red con el siguiente comando:

```
sudo systemctl restart networking
```

1.2. Configuración de la red en el firewall interno

Para la configuración de la red en el firewall interno, se va a configurar dos interfaces, una que va conectada a la DMZ y otra que va conectada a la red interna. Como esta máquina es un *CentOS*, la configuración de la red lo haremos con *nmtui*. Para la instalación de *nmtui*, se va a utilizar el siguiente comando: `sudo yum install NetworkManager-tui`

Ya instalado, iniciamos el servicio con el siguiente comando: `sudo systemctl start NetworkManager`

Una vez instalado *nmtui*, se va a configurar la interfaz que va conectada a la DMZ y a la red interna, queda de la siguiente manera:



Figura 1.2: Configuración de las interfaces en el firewall interno

1.3. Resultado de la configuración de la red en el firewall externo e interno

Una vez configurada la red en el firewall externo e interno, se va a comprobar que la configuración se ha realizado correctamente. Para ello, se va a utilizar el comando `ip a` en ambos firewalls, quedando de la siguiente manera:

```
usuario@FW-Externo-p09:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:1a:4a:97:7b:fd brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.6.128.84/22 brd 10.6.131.255 scope global dynamic ens3
        valid_lft 2598sec preferred_lft 2598sec
    inet6 fe80::21a:4aff:fe97:7b52/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:1a:4a:97:51:f6 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 192.168.10.2/24 brd 192.168.10.255 scope global ens4
        valid_lft forever preferred_lft forever
    inet6 fe80::21a:4aff:fe97:51f6/64 scope link
        valid_lft forever preferred_lft forever
usuario@FW-Externo-p09:~$
```

(a) Configuración de la red en el firewall externo

```
[usuario@centos ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:1a:4a:97:51:5d brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:1a:4a:97:7b:52 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/24 brd 192.168.10.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
    inet 172.16.10.1/24 brd 172.16.10.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::21a:4aff:fe97:7b52/64 scope link
        valid_lft forever preferred_lft forever
[usuario@centos ~]$
```

(b) Configuración de la red en el firewall interno

Figura 1.3: Resultado de la configuración de la red en el firewall externo e interno

Una vez hecha la configuración de la red, se va a borrar las interfaces externas por defecto en el servidor, en el cliente y en el firewall interno.

2. Habilitar *NAT* utilizando la configuración de *Shorewall*

Para habilitar *NAT*, lo haremos en el firewall externo ya que es el que está conectado a Internet. Para hacerlo usaremos *Shorewall*, que describe los requisitos de firewall utilizando entradas en un conjunto de archivos de configuración. Shorewall lee esos archivos de configuración y, con la ayuda de las utilidades *iptables*, *iptables-restore*, *ip* y *tc* configura el *Netfilter* y el tráfico de red relacionado de acuerdo con esos requisitos.

La instalación de este programa se va a utilizar el siguiente comando: `sudo apt install shorewall`

Para habilitar el *forwarding* lo haremos configurando el fichero `/etc/shorewall/shorewall.conf` con la siguiente configuración:

```
root@FW-Externo-p09:/etc/shorewall# vi /etc/shorewall/shorewall.conf
root@FW-Externo-p09:/etc/shorewall# cat /etc/shorewall/shorewall.conf | grep IF_FORWARDING=
IF_FORWARDING=Yes
root@FW-Externo-p09:/etc/shorewall#
```

Figura 2.1: Configuración de *forwarding* en *Shorewall*

Una vez habilitado el *forwarding*, se va a configurar los diferentes archivos de configuración de *Shorewall*. En este caso, al instalar *Shorewall* en el firewall externo y como es una máquina *Debian*, no crea los ficheros de configuración por defecto, por lo que hay que crearlos. Creamos dentro del directorio `/etc/shorewall/` los siguientes archivos de configuración:

- **zones:** declara las zonas de red.

```
root@FW-Externo-p09:/etc/shorewall# cat zones
#
# Shorewall -- /etc/shorewall/zones
#
# 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_OPTIONS      OUT_OPTIONS
fw             firewall
net            ipv4
loc            ipv4
dmz            ipv4
root@FW-Externo-p09:/etc/shorewall#
```

Figura 2.2: Configuración de `/etc/shorewall/zones`

- **interfaces:** define las interfaces de red del firewall.

```

root@FW-Externo-p09:/etc/shorewall# cat interfaces
#
# Shorewall -- /etc/shorewall/interfaces
#
# 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
net        WAN_IF        -              tcpflags,dhcp,nosmurfs,routefilter,logmartians,sourceroute=0,physical=ens3
-          LOC_IF        -              tcpflags,nosmurfs,routefilter,logmartians,physical=ens4
root@FW-Externo-p09:/etc/shorewall#

```

Figura 2.3: Configuración de */etc/shorewall/interfaces*

- **hosts:** define zonas en terminos de subredes y/o direcciones IP individuales.

```

root@FW-Externo-p09:/etc/shorewall# cat hosts
#
# Shorewall -- /etc/shorewall/hosts
#
# For information about entries in this file, type "man shorewall-hosts"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-hosts.html
#
#####
#ZONE      HOSTS              OPTIONS
loc        LOC_IF:172.16.10.0/24
dmz        LOC_IF:192.168.10.0/24
root@FW-Externo-p09:/etc/shorewall#

```

Figura 2.4: Configuración de */etc/shorewall/hosts*

- **snat:** contiene las definiciones de *SNAT*.

```

root@FW-Externo-p09:/etc/shorewall# cat snat
#
# Shorewall -- /etc/shorewall/snat
#
# For information about entries in this file, type "man shorewall-snat"
#
# See http://shorewall.net/manpages/shorewall-snat.html for more information
#
#####
#ACTION      SOURCE      DEST
MASQUERADE   192.168.10.0/24   ens3
MASQUERADE   172.16.10.0/24    ens3
root@FW-Externo-p09:/etc/shorewall#

```

Figura 2.5: Configuración de */etc/shorewall/snat*

3. Configurar el cliente en la red interna y servidor en la DMZ

3.1. Configuración del cliente en la red interna

Para configurar el cliente en la red interna, se va a configurar el archivo el archivo `/etc/network/interfaces` con la siguiente configuración:

```
auto ens4
iface ens4 inet static
    address 172.16.10.2
    netmask 255.255.255.0
    gateway 172.16.10.1
```

3.2. Configuración del servidor en la DMZ

Para configurar el servidor en la DMZ, primero vamos a configurar la interfaz que va conectada a la DMZ, para ello se va a configurar el archivo `/etc/network/interfaces` con la siguiente configuración:

```
auto ens4
iface ens4 inet static
    address 192.168.10.100
    netmask 255.255.255.0
    gateway 192.168.10.2
```

y luego se va a instalar el servicio web con el siguiente comando: `sudo apt install nginx`

Ahora, se va a configurar el archivo `/etc/nginx/sites-available/default` y añadimos el siguiente contenido:

```
server {
    listen 192.168.10.100:80;
    server_name 10.6.128.84;
}
```

Una vez configurado el archivo, se va a reiniciar el servicio `nginx` con el siguiente comando: `sudo systemctl restart nginx`

A continuación, se va a comprobar que el servicio `nginx` está funcionando correctamente, para ello se vamos a utilizar un navegador de texto en el firewall externo, aquí una captura de pantalla del resultado:

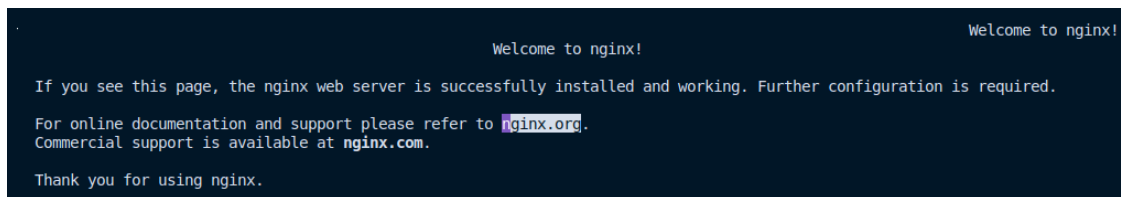


Figura 3.1: `nginx` en el firewall externo

Ya con el servicio `nginx` configurado, se va a instalar el servicio `proftpd` para tener un servidor FTP. Para su instalación se va a utilizar el siguiente comando: `sudo apt install proftpd`

Con el servicio *proftpd* instalado, se va a iniciar el servicio: `systemctl start proftpd`

Ahora se va a probar el funcionamiento del servidor FTP, para ello se va a utilizar el comando *ftp* firewall externo, aquí una captura de pantalla del resultado:

```
root@FW-Externo-p09:/etc/shorewall# ftp 192.168.10.100
Connected to 192.168.10.100.
220 Servidor ProFTPD (Debian) [::ffff:192.168.10.100]
Name (192.168.10.100:usuario): ftpuser
331 Contraseña necesaria para ftpuser
Password:
230 Usuario ftpuser conectado
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||56210|)
150 Abriendo conexión de datos en modo ASCII para file list
226 Transferencia completada
ftp> ls
229 Entering Extended Passive Mode (|||37291|)
150 Abriendo conexión de datos en modo ASCII para file list
-rw-r--r-- 1 root root 0 Nov 30 19:04 a.txt
drwxr-xr-x 2 root root 4096 Nov 30 19:04 prueba
226 Transferencia completada
ftp>
```

Figura 3.2: Resultado de la prueba del servidor FTP en el firewall externo

Finalmente, para poder acceder con la IP pública del firewall externo, hay que configurar un port forwarding a través de añadir reglas de DNAT en */etc/shorewall/rules*:

#ACTION	SOURCE	DEST	PROTO	DPORT
DNAT	net	dmz:192.168.10.100	tcp	20
DNAT	net	dmz:192.168.10.100	tcp	21
DNAT	net	fw:192.168.10.2	tcp	22
DNAT	net	dmz:192.168.10.100	tcp	80

Tras poner las reglas, ya se puede acceder al servidor web desde el exterior:

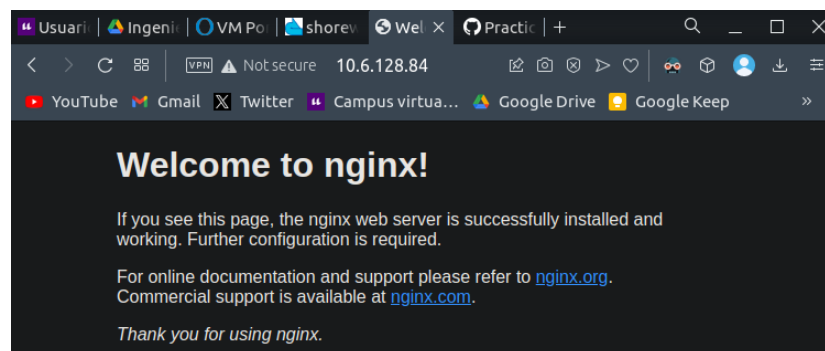


Figura 3.3: Resultado de la prueba del servidor web en el navegador

4. Configurar el firewall con unas políticas por defecto:

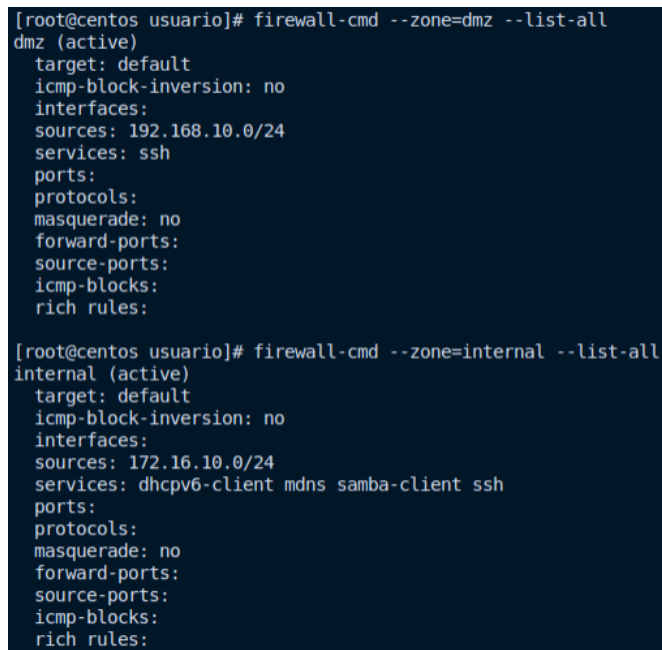
Antes de empezar a configurar el firewall instalamos en el firewall interno *firewalld* con el siguiente comando: `sudo yum install firewalld`, y lo iniciamos con el siguiente comando:

```
sudo systemctl start firewalld
```

Antes de configurar las políticas por defecto, hay que configurar las zonas. Esto lo haremos en el firewall interno. *firewalld* viene preconfigurado con las DMZ e interna, pero hay que agregar las redes que tenemos a esas zonas. Para ello, se va a utilizar los siguientes comandos:

```
firewall-cmd --zone=dmz --add-source=192.168.10.0/24
```

```
firewall-cmd --zone=internal --add-source=172.16.10.0/24
```



```
[root@centos usuario]# firewall-cmd --zone=dmz --list-all
dmz (active)
target: default
icmp-block-inversion: no
interfaces:
sources: 192.168.10.0/24
services: ssh
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:

[root@centos usuario]# firewall-cmd --zone=internal --list-all
internal (active)
target: default
icmp-block-inversion: no
interfaces:
sources: 172.16.10.0/24
services: dhcpv6-client mdns samba-client ssh
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

Figura 4.1: Políticas por defecto

■ ACCEPT para tráfico FW a DMZ y FW a Red Interna

```
firewall-cmd --permanent --new-policy FWToDMZ
firewall-cmd --permanent --policy FWToDMZ --set-target ACCEPT
firewall-cmd --permanent --policy FWToDMZ --add-ingress-zone HOST
firewall-cmd --permanent --policy FWToDMZ --add-egress-zone dmz
firewall-cmd --permanent --new-policy FWToInt
firewall-cmd --permanent --policy FWToInt --set-target ACCEPT
firewall-cmd --permanent --policy FWToInt --add-ingress-zone HOST
firewall-cmd --permanent --policy FWToInt --add-egress-zone internal
```

```
[usuario@FWInterno ~]$ sudo su
[sudo] password for usuario:
[root@FWInterno usuario]# firewall-cmd --permanent --new-policy FWToDMZ
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy FWToDMZ --set-target ACCEPT
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy FWToDMZ --add-ingress-zone HOST
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy FWToDMZ --add-egress-zone dmz
success
[root@FWInterno usuario]# firewall-cmd --permanent --new-policy FWToInt
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy FWToInt --set-target ACCEPT
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy FWToInt --add-ingress-zone HOST
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy FWToInt --add-egress-zone internal
success
[root@FWInterno usuario]#
```

Figura 4.2: ACCEPT para tráfico FW a DMZ y FW a Red Interna

- **ACCEPT para tráfico Red Interna a DMZ**

```
firewall-cmd --zone=internal --add-service=any --permanent
firewall-cmd --zone=internal --add-source=192.168.10.100 --permanent
```

```
firewall-cmd --permanent --new-policy IntToDMZ
firewall-cmd --permanent --policy IntToDMZ --set-target ACCEPT
firewall-cmd --permanent --policy IntToDMZ --add-ingress-zone internal
firewall-cmd --permanent --policy IntToDMZ --add-egress-zone dmz
```

- **ACCEPT para tráfico Red Interna a Internet**

```
firewall-cmd --permanent --new-policy IntToNet
firewall-cmd --permanent --policy IntToNet --set-target ACCEPT
firewall-cmd --permanent --policy IntToNet --add-ingress-zone internal
firewall-cmd --permanent --policy IntToNet --add-egress-zone ANY
```

- **REJECT para tráfico DMZ a Red Interna e Internet a DMZ**

```
firewall-cmd --permanent --new-policy DMZToInt
firewall-cmd --permanent --policy DMZToInt --set-target REJECT
firewall-cmd --permanent --policy DMZToInt --add-ingress-zone dmz
firewall-cmd --permanent --policy DMZToInt --add-egress-zone internal
firewall-cmd --permanent --new-policy DMZToNet
firewall-cmd --permanent --policy DMZToNet --set-target REJECT
firewall-cmd --permanent --policy DMZToNet --add-ingress-zone dmz
firewall-cmd --permanent --policy DMZToNet --add-egress-zone ANY
```

■ **DROP para tráfico Internet a FW e Internet a Red Interna**

```
firewall-cmd --permanent --new-policy NetToFW
firewall-cmd --permanent --policy NetToFW --set-target DROP
firewall-cmd --permanent --policy NetToFW --add-ingress-zone external
firewall-cmd --permanent --policy NetToFW --add-egress-zone HOST
firewall-cmd --permanent --new-policy NetToInt
firewall-cmd --permanent --policy NetToInt --set-target DROP
firewall-cmd --permanent --policy NetToInt --add-ingress-zone external
firewall-cmd --permanent --policy NetToInt --add-egress-zone internal
```

5. Configurar reglas utilizando Macros para permitir el tráfico necesario

6. Bibliografía

1. Oliveros, D. (2013, 14 de marzo). Configurar Shorewall en Debian. Dayron Oliveros. Recuperado de <https://www.youtube.com/watch?v=20E0QxWwAlk>
2. Thomas M. Eastep. (2020). snat — Shorewall SNAT/Masquerade definition file. Shorewall. Recuperado de <https://shorewall.org/manpages/shorewall-snat.html>
3. Thomas M. Eastep. (2020). interfaces — Shorewall interfaces file. Shorewall. Recuperado de <https://shorewall.org/manpages/shorewall-interfaces.html>
4. Luz, S. (2023). Servidor FTP ProFTPD para Linux: Instalación y configuración. Redes Zone. Recuperado de <https://www.redeszone.net/tutoriales/servidores/proftpd/>
5. Alonsojpd. (2022). Solución al error Failed to download metadata for repo appstream en CentOS 8. Proyectoa. Recuperado de <https://proyectoa.com/solucion-al-error-failed-to-downloadd-metadata-for-repo-appstream-en-centos-8/>
6. firewalld. (s.f.). Concepts and Configuration. firewalld. Recuperado de <https://firewalld.org/documentation/concepts.html>