

# Practica 09. Shorewall: Doble firewall con DMZ

Seguridad de Sistemas Informáticos

Carlos Pérez Fino y Cheuk Kelly Ng Pante

6 de diciembre de 2023

## Índice general

<b>1. Configuración de red con dos firewalls y tres zonas</b>	<b>1</b>
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
<b>2. Habilitar <i>NAT</i> utilizando la configuración de <i>Shorewall</i></b>	<b>3</b>
<b>3. Configurar el cliente en la red interna y servidor en la DMZ</b>	<b>5</b>
3.1. Configuración del cliente en la red interna . . . . .	5
3.2. Configuración del servidor en la DMZ . . . . .	5
<b>4. Configurar el firewall con unas políticas por defecto:</b>	<b>7</b>
<b>5. Configurar reglas utilizando Macros para permitir el tráfico necesario</b>	<b>12</b>
<b>6. Bibliografía</b>	<b>17</b>

## 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:

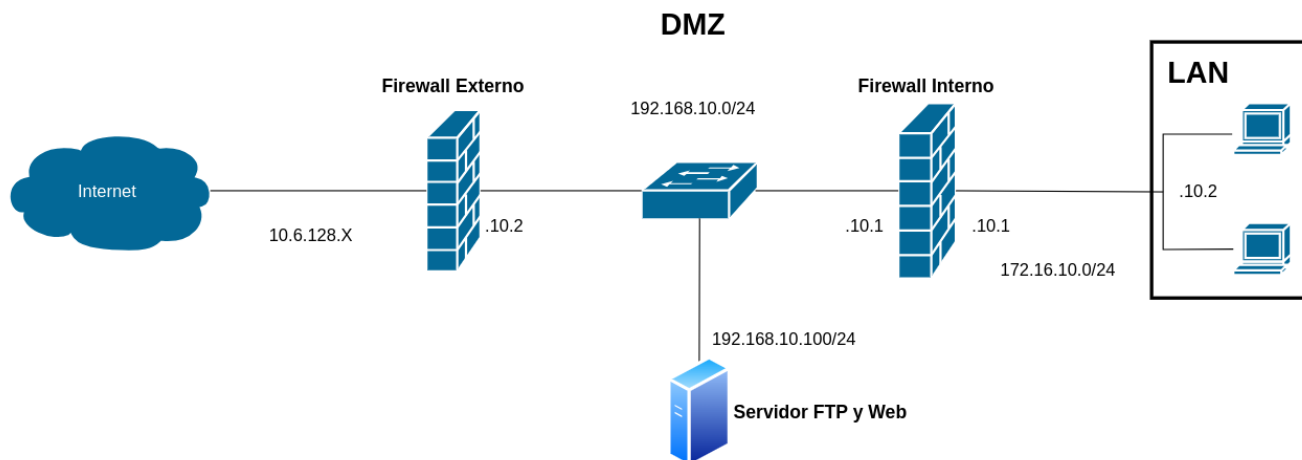


Figura 1.1: Diseño de red con dos firewalls y tres zonas

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 a 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 8*, 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:

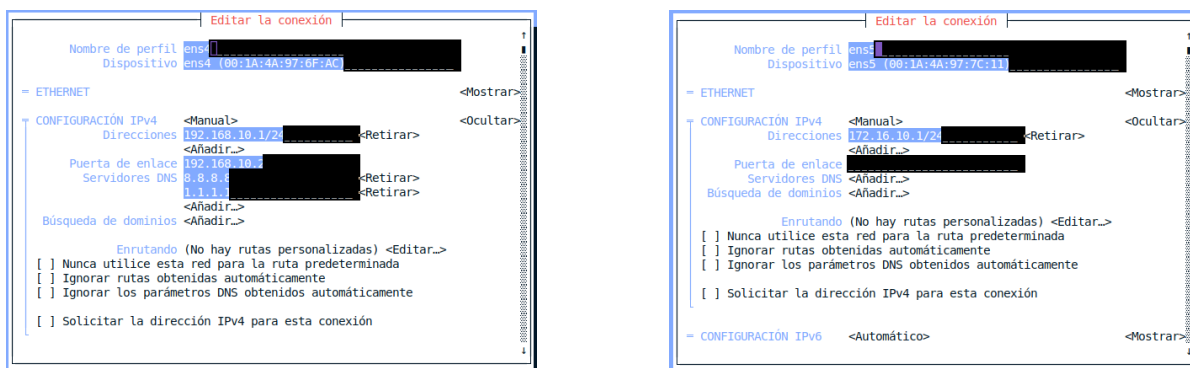


Figura 1.2: Configuración de las interfaces en el firewall interno

## 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:

```
root@fw-Externo-p09:/etc/shorewall# 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:97:6f:af brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.6.129.75/22 brd 10.6.131.255 scope global dynamic ens3
        valid_lft 2528sec preferred_lft 2528sec
    inet6 fe80::21a:4aff:fe97:6faf/64 scope link
        valid_lft forever preferred_lft forever
3: ens8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:1a:4a:97:52:12 brd ff:ff:ff:ff:ff:ff
    altname enp0s8
    inet 192.168.10.2/24 brd 192.168.10.255 scope global ens8
        valid_lft forever preferred_lft forever
    inet6 fe80::21a:4aff:fe97:5212/64 scope link
        valid_lft forever preferred_lft forever
root@fw-Externo-p09:/etc/shorewall#
```

(a) Configuración de la red en el firewall externo

```
[root@FWInterno ~]# 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: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:1a:4a:97:6f:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/24 brd 192.168.10.255 scope global noprefixroute ens4
        valid_lft forever preferred_lft forever
    inet6 fe80::ac1b:208:a715:a06b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:1a:4a:97:7c:11 brd ff:ff:ff:ff:ff:ff
    inet 172.16.10.1/24 brd 172.16.10.255 scope global noprefixroute ens5
        valid_lft forever preferred_lft forever
    inet6 fe80::87d6:730d:b305:85a2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@FWInterno ~]#
```

(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*

Antes de empezar con la configuración del *NAT*, hay que asegurarse que en los dos firewalls esté habilitado el reenvío de paquetes IP o *IP forwarding*. Para ello, se va a utilizar el siguiente comando:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

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
# ZONE  INTERFACE      BROADCAST  OPTIONS
net     NET_IF            -           tcpflags,dhcp,nosmurfs,routefilter,logmartians,sourceroute=0,physical=ens3
-       LOC_IF            -           tcpflags,nosmurfs,routefilter,logmartians,physical=ens8
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 `/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 10.6.129.75;
}
```

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:

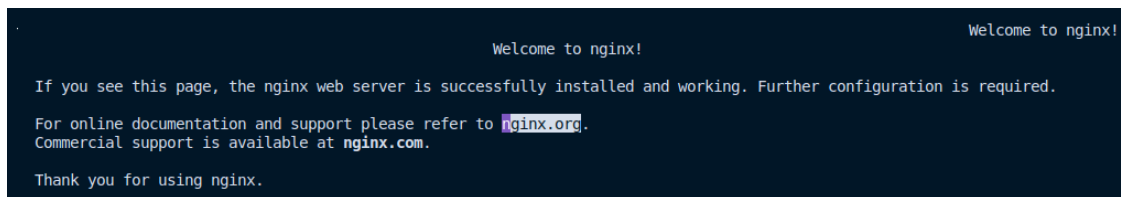


Figura 3.1: `nginx` en el firewall externo

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



## 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
firewall-cmd --zone=external --add-interface=ens4
```

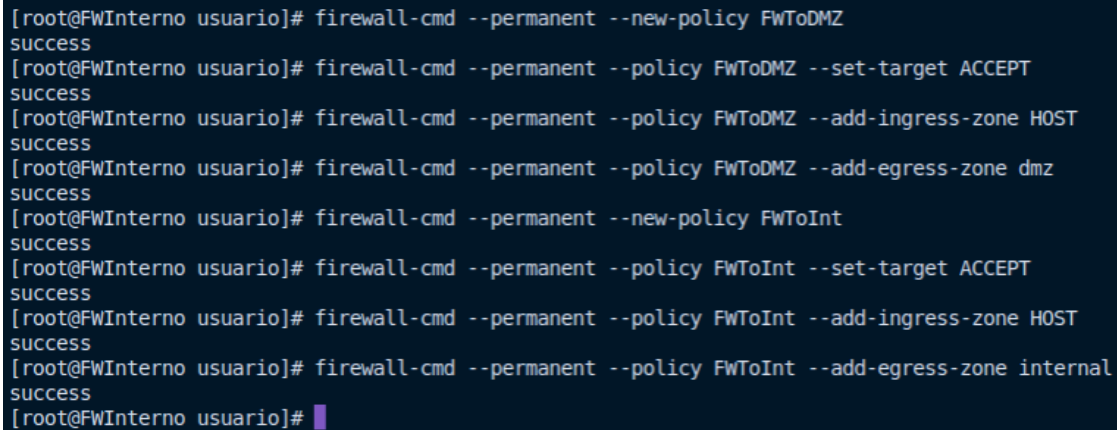
En la configuración de la zona exterior ponemos la interfaz que va hacia Internet, en este caso es *ens4*.

```
[root@FWInterno usuario]# firewall-cmd --zone=dmz --list-all
dmz
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@FWInterno usuario]# firewall-cmd --zone=internal --list-all
internal
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: cockpit dhcpv6-client dns http https mdns samba-client ssh
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@FWInterno usuario]# firewall-cmd --zone=external --list-all
external (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens4
  sources:
  services: ssh
  ports: 1-65535/tcp
  protocols:
  forward: no
  masquerade: yes
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@FWInterno usuario]#
```

Figura 4.1: Políticas por defecto

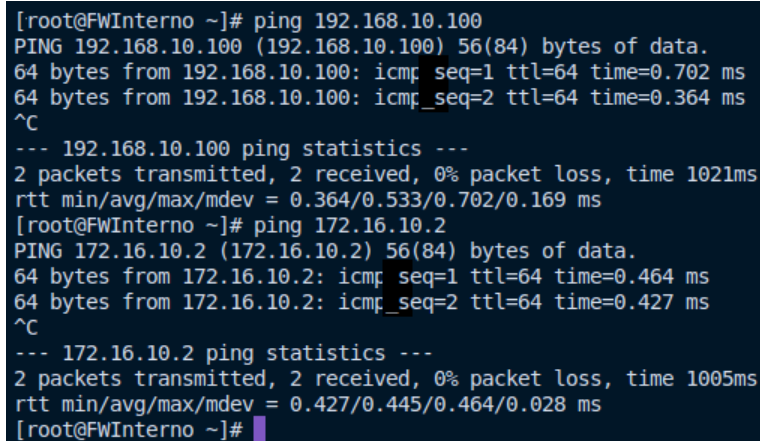
- ACCEPT para tráfico FW a DMZ y FW a Red Interna

```
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
```



```
[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

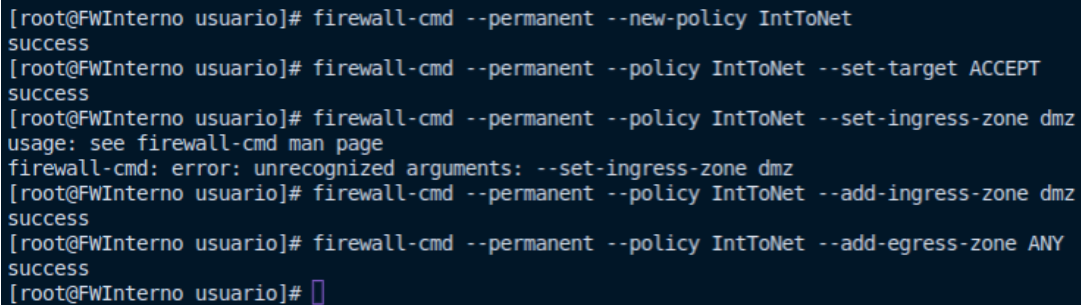


```
[root@FWInterno ~]# ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp: seq=1 ttl=64 time=0.702 ms
64 bytes from 192.168.10.100: icmp: seq=2 ttl=64 time=0.364 ms
^C
--- 192.168.10.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1021ms
rtt min/avg/max/mdev = 0.364/0.533/0.702/0.169 ms
[root@FWInterno ~]# ping 172.16.10.2
PING 172.16.10.2 (172.16.10.2) 56(84) bytes of data.
64 bytes from 172.16.10.2: icmp: seq=1 ttl=64 time=0.464 ms
64 bytes from 172.16.10.2: icmp: seq=2 ttl=64 time=0.427 ms
^C
--- 172.16.10.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.427/0.445/0.464/0.028 ms
[root@FWInterno ~]#
```

Figura 4.3: Resultado de ACCEPT para tráfico FW a DMZ y FW a Red Interna

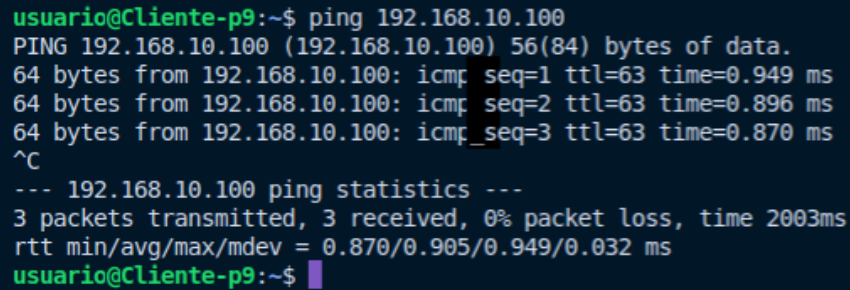
- **ACCEPT para tráfico Red Interna a DMZ**

```
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
```



```
[root@FWInterno usuario]# firewall-cmd --permanent --new-policy IntToNet
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy IntToNet --set-target ACCEPT
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy IntToNet --set-ingress-zone dmz
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: --set-ingress-zone dmz
[root@FWInterno usuario]# firewall-cmd --permanent --policy IntToNet --add-ingress-zone dmz
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy IntToNet --add-egress-zone ANY
success
[root@FWInterno usuario]#
```

Figura 4.4: ACCEPT para tráfico Red Interna a DMZ



```
usuario@Cliente-p9:~$ ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp: seq=1 ttl=63 time=0.949 ms
64 bytes from 192.168.10.100: icmp: seq=2 ttl=63 time=0.896 ms
64 bytes from 192.168.10.100: icmp: seq=3 ttl=63 time=0.870 ms
^C
--- 192.168.10.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.870/0.905/0.949/0.032 ms
usuario@Cliente-p9:~$
```

Figura 4.5: funcionamiento del ACCEPT para tráfico Red Interna a 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
```

```
[root@FWInterno usuario]# firewall-cmd --permanent --new-policy IntToNet
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy IntToNet --set-target ACCEPT
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy IntToNet --add-ingress-zone internal
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy IntToNet --add-egress-zone ANY
success
[root@FWInterno usuario]#
```

Figura 4.6: ACCEPT para tráfico Red Interna a Internet

```
usuario@Cliente-p9:~$ curl ull.es
<html>
<head><title>302 Found</title></head>
<body>
<center><h1>302 Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
usuario@Cliente-p9:~$
```

Figura 4.7: Resultado de ACCEPT para tráfico Red Interna a Internet

- **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
```

```
[root@FWInterno usuario]# firewall-cmd --permanent --new-policy DMZToInt
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy DMZToInt --set-target REJECT
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy DMZToInt --add-ingress-zone dmz
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy DMZToInt --add-egress-zone internal
success
[root@FWInterno usuario]#
```

Figura 4.8: REJECT para tráfico DMZ a Red Interna

```
usuario@Server-p9:~$ ssh usuario@172.168.10.2

```

Figura 4.9: Funcionamiento del REJECT para tráfico DMZ a Red Interna

- **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
```



```
[root@FWInterno usuario]# firewall-cmd --permanent --new-policy NetToFW
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy NetToFW --set-target DROP
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy NetToFW --add-ingress-zone external
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy NetToFW --add-egress-zone HOST
success
[root@FWInterno usuario]# firewall-cmd --permanent --new-policy NetToInt
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy NetToInt --set-target DROP
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy NetToInt --add-ingress-zone external
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy NetToInt --add-egress-zone internal
success
[root@FWInterno usuario]#
```

Figura 4.10: DROP para tráfico Internet a Red Interna e Internet a FW

## 5. Configurar reglas utilizando Macros para permitir el tráfico necesario

- Tráfico DNS para la resolución de nombres al servidor DNS externo

```
firewall-cmd --permanent --policy NetToInt --add-service=dns
firewall-cmd --permanent --policy NetToFW --add-service=dns
```

Luego en el firewall externo se añade la siguiente regla al fichero `/etc/shorewall/rules`:

#ACTION	SOURCE	DEST	PROTO	DPORT
ACCEPT	net	dmz	udp	53
ACCEPT	net	loc	udp	53

```
[root@FWInterno usuario]# firewall-cmd --permanent --policy NetToInt --add-service=dns
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy NetToFW --add-service=dns
success
```

Figura 5.1: Tráfico DNS para la resolución de nombres al servidor DNS externo

```
usuario@Cliente-p9:~$ dig ull.es

; <<> DiG 9.18.19-1-deb12u1-Debian <<> ull.es
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 26621
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5c1fb1331b50b3dc40d67f04656fe3c72537a5713d69b6ab (good)
;; QUESTION SECTION:
;ull.es.                                IN      A

;; ANSWER SECTION:
ull.es.                10800    IN      A      193.145.118.52

;; AUTHORITY SECTION:
ull.es.                10800    IN      NS      sun.rediris.es.
ull.es.                10800    IN      NS      chico.rediris.es.
ull.es.                10800    IN      NS      dns2.ull.es.
ull.es.                10800    IN      NS      dns1.ull.es.

;; ADDITIONAL SECTION:
chico.rediris.es.      1757     IN      A      162.219.54.2
sun.rediris.es.        2767     IN      A      199.184.182.1
dns1.ull.es.           10800    IN      A      193.145.120.40
dns2.ull.es.           10800    IN      A      193.145.120.80

;; Query time: 4 msec
;; SERVER: 10.4.9.30#53(10.4.9.30) (UDP)
;; WHEN: Wed Dec 06 03:00:23 WET 2023
;; MSG SIZE rcvd: 227
```

Figura 5.2: Funcionamiento del tráfico DNS para la resolución de nombres al servidor DNS externo

- Tráfico de cualquier tipo desde la red interna a servidores de Internet

```
usuario@Cliente-p9:~$ ping www.google.es
PING www.google.es (142.250.184.3) 56(84) bytes of data.
64 bytes from mad41s10-in-f3.1e100.net (142.250.184.3): icmp: seq=1 ttl=117 time=30.3 ms
64 bytes from mad41s10-in-f3.1e100.net (142.250.184.3): icmp: seq=2 ttl=117 time=30.4 ms
64 bytes from mad41s10-in-f3.1e100.net (142.250.184.3): icmp: seq=3 ttl=117 time=30.5 ms
^C
--- www.google.es ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 30.251/30.381/30.479/0.095 ms
usuario@Cliente-p9:~$
```

Figura 5.3: *PING* a google.es desde el cliente



Figura 5.4: Acceso a google.es desde el cliente mediante el navegador *links*

- **Tráfico Web y FTP desde Internet al servidor web**

En el firewall externo, en el fichero `/etc/shorewall/rules` se añade la siguiente regla:

#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	dmz:192.168.10.100	tcp	80
ACCEPT	net	dmz:192.168.10.100	tcp	http,ftp

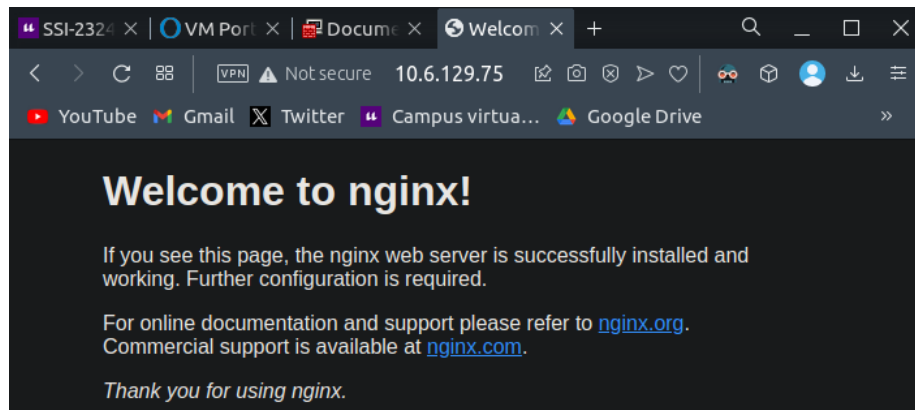


Figura 5.5: Acceso al servidor web de la DMZ desde un navegador

- **Tráfico Web desde la red Interna al servidor web de la DMZ**

```
firewall-cmd --permanent --policy IntToDMZ --add-service=http
```

Y en el firewall externo, en el fichero `/etc/shorewall/rules` se añade la siguiente regla:

#ACTION	SOURCE	DEST	PROTO	DPORT	SPORT	ORIGDEST
DNAT	loc	dmz:192.168.10.100	tcp	80	-	&NET_IF

```
[root@FWInterno usuario]# firewall-cmd --permanent --new-policy IntToDMZ
success
[root@FWInterno usuario]# firewall-cmd --permanent --policy IntToDMZ --add-service=http
success
[root@FWInterno usuario]#
```

Figura 5.6: Tráfico Web desde la red Interna al servidor web de la DMZ



```
usuario@Cliente-p9:~$ wget 192.168.10.100
--2023-12-06 03:04:52-- http://192.168.10.100/
Conectando con 192.168.10.100:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 615 [text/html]
Grabando a: «index.html.2»

index.html.2          100%[=====>]          615  --.-KB/s   en 0s
2023-12-06 03:04:52 (51,4 MB/s) - «index.html.2» guardado [615/615]

usuario@Cliente-p9:~$ wget 10.6.129.75
--2023-12-06 03:05:00-- http://10.6.129.75/
Conectando con 10.6.129.75:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 615 [text/html]
Grabando a: «index.html.3»

index.html.3          100%[=====>]          615  --.-KB/s   en 0s
2023-12-06 03:05:00 (52,8 MB/s) - «index.html.3» guardado [615/615]
```

Figura 5.7: Acceso al servidor web de la DMZ desde el cliente con dirección pública y privada

■ Configuración final del *Shorewall* en los ficheros *rules* y *policy*

• Fichero *rules*

#ACTION	SOURCE	DEST	PROTO	DPORT	SPORT	ORIGDEST
ACCEPT	net	fw	tcp	ssh		
ACCEPT	fw	dmz	tcp	ssh		
ACCEPT	fw	loc	tcp	ssh		
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		
DNAT	loc	dmz:192.168.10.100	tcp	80	-	&NET_IF
ACCEPT	net	dmz	udp	53		
ACCEPT	net	loc	udp	53		
ACCEPT	loc	net				
ACCEPT	net	dmz:192.168.10.100	tcp	http,ftp		
ACCEPT	loc	dmz:192.168.10.100	tcp	http		

• Fichero *policy*

#SOURCE	DEST	POLICY	LOG LEVEL
fw	dmz	ACCEPT	info
fw	loc	ACCEPT	info
fw	net	ACCEPT	
loc	net	ACCEPT	info
loc	fw	ACCEPT	info
loc	dmz	ACCEPT	info
net	dmz	REJECT	info
net	fw	DROP	info
net	loc	REJECT	info
dmz	fw	ACCEPT	info
dmz	loc	ACCEPT	info
dmz	net	ACCEPT	info

## 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>