

Practica 09. Shorewall: Doble firewall con DMZ

Seguridad de Sistemas Informáticos

Carlos Pérez Fino y Cheuk Kelly Ng Pante

30 de noviembre 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	3
3.1. Configuración del cliente en la red interna	3
3.2. Configuración del servidor en la DMZ	3
4. Configurar el firewall con unas políticas por defecto:	4
5. Bibliografía	5

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:

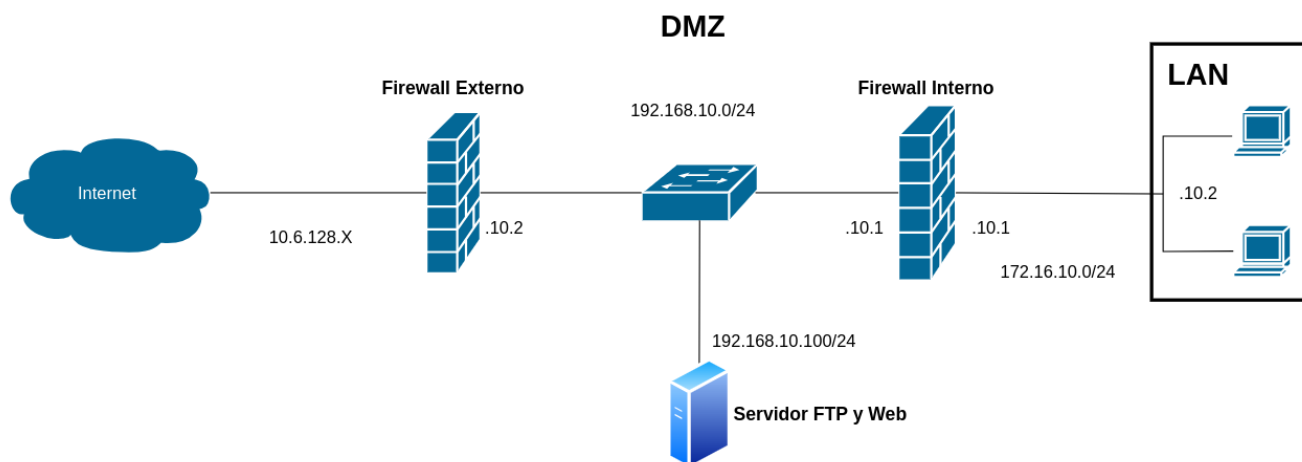


Figura 1.1: Diseño de red con dos firewalls y tres zonas

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`

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:

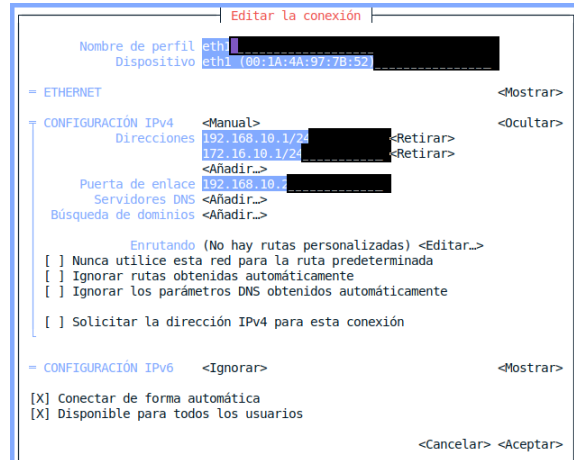


Figura 1.2: Configuración

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:fe97:7bfd/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* utilizando la configuración de *Shorewall*, se va a configurar el archivo *snat* en el directorio */etc/shorewall/* con la siguiente configuración:

```
#
# Shorewall -- /etc/shorewall/snats
#
# For information about entries in this file, type "man shorewall-snats"
#
# See http://shorewall.net/manpages/shorewall-snats.html for more information
#
#####
#ACTION          SOURCE          DEST          PROTO  PORT  IPSEC  MARK  USER  SWITCHORIGDEST  PROBABILITY
MASQUERADE       192.168.10.0/24  ens3          all    *    *      *      *      *                  *
```

Figura 2.1: Configuración de *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

3.2. Configuración del servidor en la DMZ

Para configurar el servidor en la DMZ, primero se va a instalar el servicio Web *nginx* con el siguiente comando: `sudo apt install nginx`

Luego, 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`

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`

POR TERMINAR, poner cual es la config de *proftpd* y pruebas de conexión en ambos servicios

4. Configurar el firewall con unas políticas por defecto:

5. 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. De Luz, S. (2023). Servidor FTP ProFTPD para Linux: Instalación y configuración. Redes Zone. Recuperado de <https://www.redeszone.net/tutoriales/servidores/proftpd/>