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

Esta práctica se va a realizar una configuracion 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:

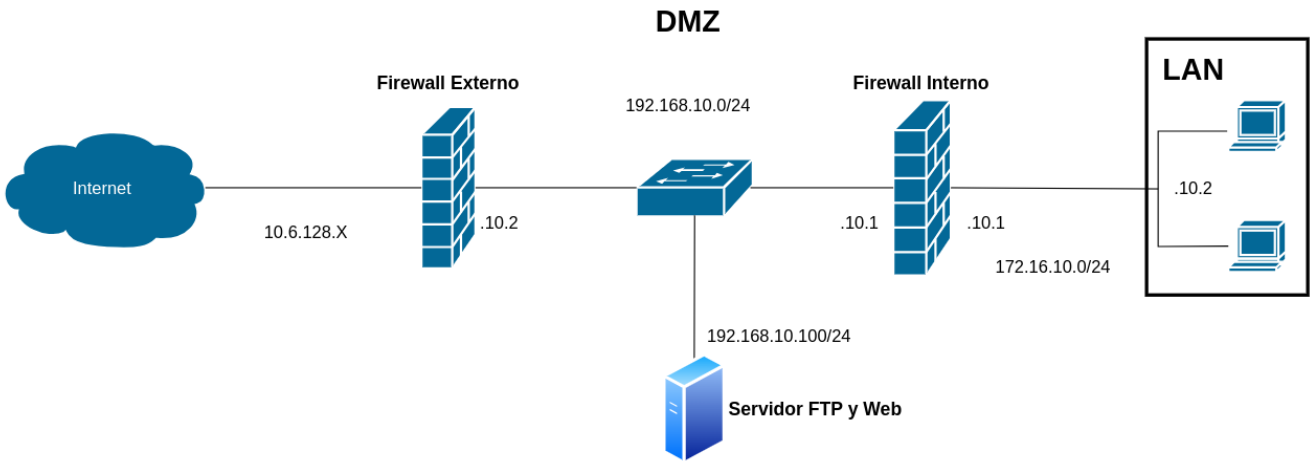


Figura 1.1: Diseño de red con dos firewalls y tres zonas

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:

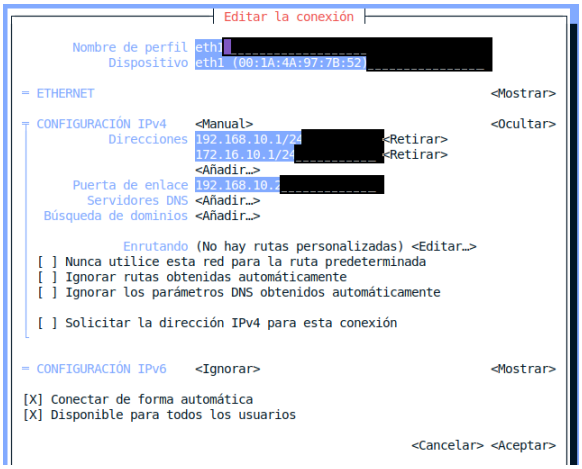
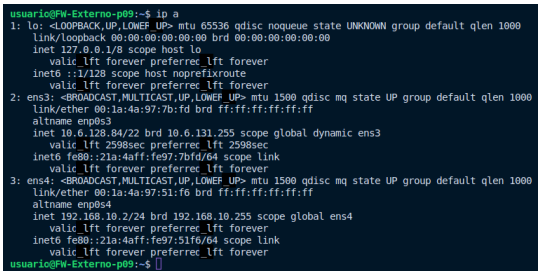


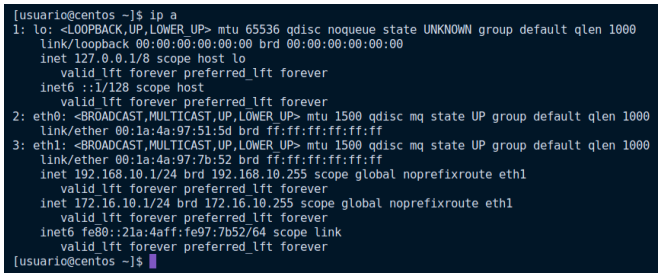
Figura 1.2: Configuración

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:



(a) Configuracion de la red en el firewall externo



(b) Configuracion 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 ello, primero habilitaremos el *forwarding* y 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 IP_FORWARDING=
IP_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 configuracion de *Shorewall*. *Shorewall* 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.

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:** contiene las definiciones de 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
wan             ipv4
lan             ipv4
dmz             ipv4
```

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

- **interfaces:** contiene las definiciones de las interfaces de red.

img/interfaces.png

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

- **hosts:** contiene las definiciones de los hosts de red.
- **snat:** contiene las definiciones 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 conexion 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/