Practica 09. Shorewall: Doble firewall con DMZ

Seguridad de Sistemas Informáticos

Cheuk Kelly Ng Pante (alu0101364544@ull.edu.es)

29 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:

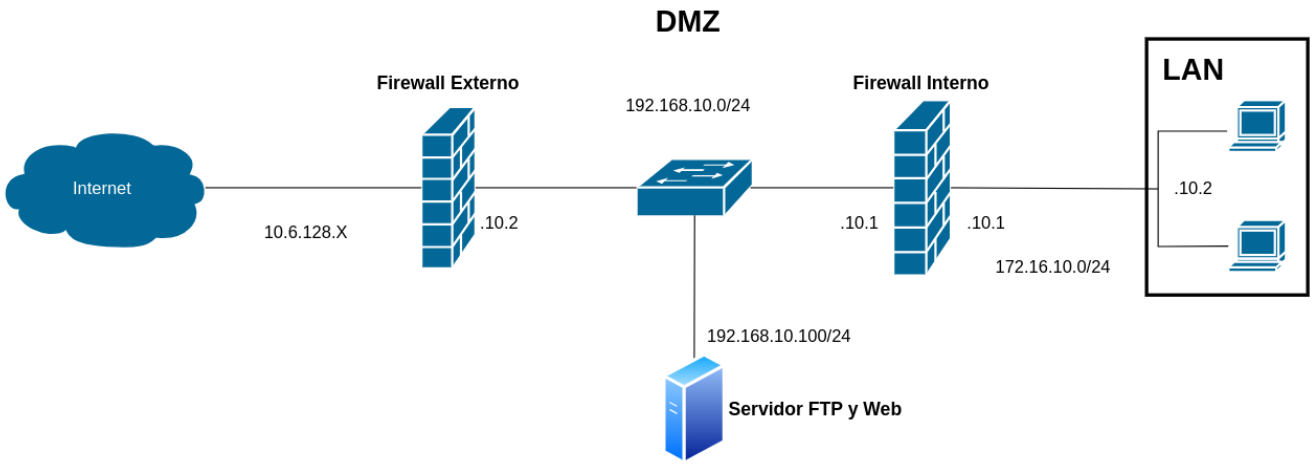

Figura 1.1: Diseño de red con dos firewalls y tres zonas

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.

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/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            PROTO   PORT    IPSEC   MARK    USER    SWITCH  ORIGDEST        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 conexion en ambos servicios

4. Configurar el firewall con unas políticas por defecto:

5. Bibliografía

1. Thomas M. Eastep. (2020). snat — Shorewall SNAT/Masquerade definition file. Shorewall. Recuperado de `https://shorewall.org/manpages/shorewall-snat.html`
2. De Luz, S. (2023). Servidor FTP ProFTPd para Linux: Instalación y configuración. Redes Zone. Recuperado de `https://www.redeszone.net/tutoriales/servidores/proftpd/`