Practicaa 08. Configurando un Firewall con DMZ

Seguridad de Sistemas Informáticos

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

18 de noviembre de 2023

Índice general

1. Configuración de red con un sólo firewall, zona privada y DMZ

Para esta primera parte se crean primero las tres máquina en el IAAS y se configuran las diferentes interfaces de red de cada una de ellas. Para ello, se accede al fichero */etc/network/interfaces* y se configuran las siguientes redes siguiendo el siguiente direccionamiento:

- **Internet:** red especificada por el servidor DHCP externo
- **Red Interna:** red de clase C privada como subred de una clase B privada: 172.16.10.0/24
- **DMZ:** red de clase C privada 192.168.10.0/24

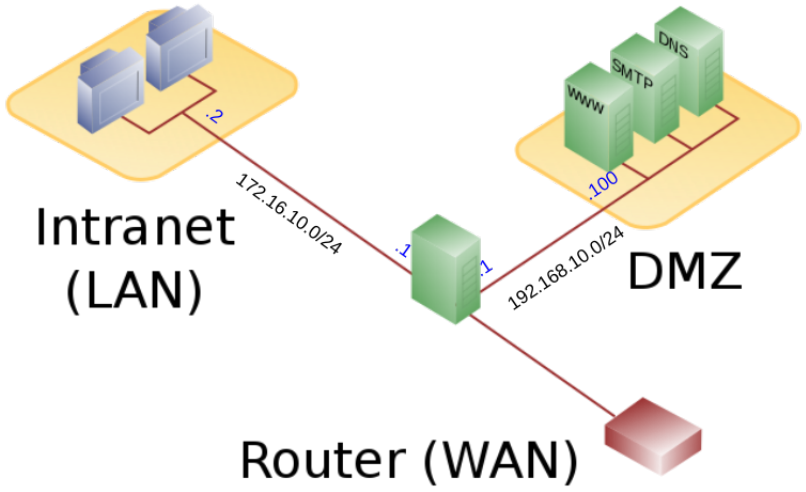

Figura 1.1: Esquema de red

La configuración de red de cada máquina se muestra a continuación:

- Maquina 1: *Firewall*

```
# The primary network interface
allow-hotplug ens3
iface ens3 inet dhcp

# The second network interace -> Server
auto ens4
iface ens4 inet static
        address 192.168.10.1
        netmask 255.255.255.0

# The third network interface -> Client
auto ens7
iface ens7 inet static
        address 172.16.10.1
        netmask 255.255.255.0
```

- Maquina 2: *Servidor*

```
# The primary network interface
allow-hotplug ens3
iface ens3 inet dhcp

# The second network interface
auto ens4
iface ens4 inet static
        address 192.168.10.100
        netmask 255.255.255.0
        gateway 192.168.10.1
```

- Maquina 2: *Cliente*

```
# The primary network interface
allow-hotplug ens3
iface ens3 inet dhcp

# The second network interface
auto ens4
iface ens4 inet static
    address 172.16.10.2
    netmask 255.255.255.255
    gateway 172.16.10.1
```

2. Configuracion de la red interna y un servidor en la DMZ

Para este apartado se configura la red interna y se instala un servidor web en la DMZ. Primero debemos instalar en el cliente un navegor web, en este caso se instala *links* con el comando *sudo apt-get install links*. Luego, instalamos el servidor web *nginx* con el comando *sudo apt-get install nginx*.

Una vez instalado *nginx* se procede a configurar el servidor web. Para ello, se accede al fichero */etc/nginx/sites-available/default* y se modifica el fichero de la siguiente manera:

```
server {
  listen 192.168.10.100:80;
  server_name 10.6.129.251;
}
```

Una vez modificado el fichero, se reinicia el servidor web con el comando *sudo systemctl restart nginx*. Ya con el servidor web configurado, configuramos las reglas firewall para permitir la redirección de tráfico del puerto 80 al servidor web. Para ello, ejecutamos las siguientes reglas *iptable* en el firewall:

```
iptables -t nat -A PREROUTING -i ens3 -p tcp --match multiport --dports 80,443 -j DNAT
--to 192.168.10.100:80

iptables -t nat -A PREROUTING -i ens4 -d 10.6.129.251 -p tcp --match multiport
--dports 80,443 -j DNAT --to 192.168.10.100:80
```

Ya con el servidor web configurado y las reglas iptables configuradas, se procede a comprobar que el servidor web funciona correctamente.

3. Configuración del Firewall con políticas por defecto DROP

El script de configuración del firewall se muestra a continuación:

```
#!/bin/bash

# Reset all tables
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -X
iptables -t nat -Z

iptables -A FORWARD -i ens4 -p tcp --match multiport --dports 80,443 -j ACCEPT
iptables -A FORWARD -i ens7 -p tcp --match multiport --dports 80,443 -j ACCEPT

iptables -A FORWARD --match state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i ens3 -o ens7 -p tcp --match multiport --dports 80,443 -j ACCEPT

iptables -A FORWARD -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -j ACCEPT

iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
```

En el punto de permitir tráfico web desde Internet al servidor web de la DMZ, aqui una captura de pantalla de la página web de *nginx* desde un navegador:

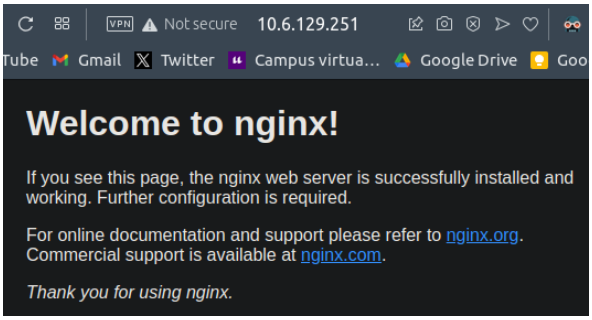

Figura 3.1: Página web de nginx desde un navegador

Luego, para el punto de permitir tráfico web desde red interna a al servidor web que está en la DMZ, una captura de pantalla accediendo al servidor web con la IP privada, 192.168.10.100, desde el cliente: q

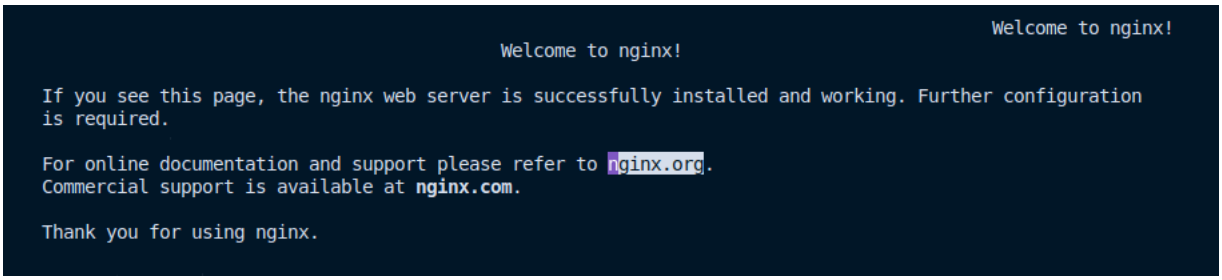

Figura 3.2: Página web de nginx desde el cliente con la IP privada