

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	2
2. Configuración de la red interna y un servidor en la DMZ	4
3. Configuración del Firewall con políticas por defecto DROP	5

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

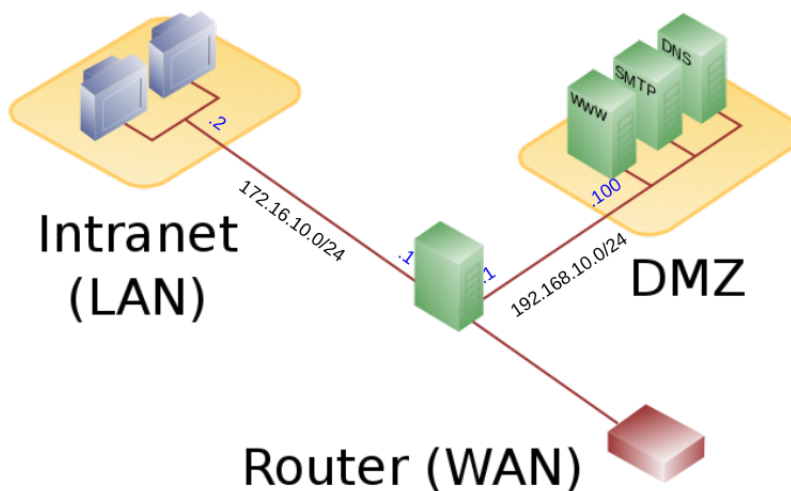


Figura 1.1: Esquema de red

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

- Máquina 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: *Cliente*

```
# 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
```

Para las diferentes máquinas, a excepción del firewall, hay que deshabilitar la interfaz de la red publica. Para ello, en el mismo fichero de configuración de las interfaces red, se borra la configuración de la interfaz que sea de la red pública y se reinicia los servicios de red.

2. Configuración 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 navegador web, en este caso se instala *links* con el comando *sudo apt-get install links*. Luego, instalamos en la maquina servidor, el servidor web *nginx* con el comando *sudo apt-get install nginx*.

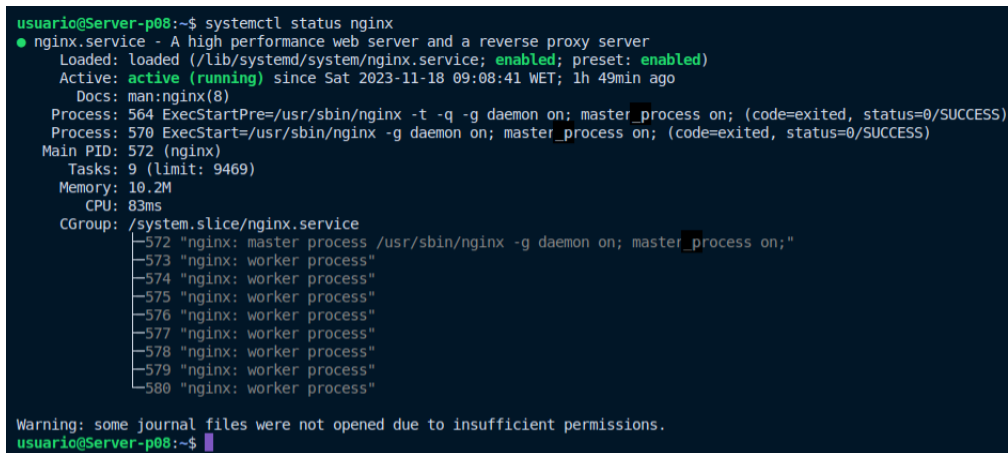
Antes de realizar la configuración de *nginx*, se debe configurar la red DMZ, del servidor web. Para ello, se accede al fichero */etc/network/interfaces* y asignamos la IP privada 192.168.10.100/24 y como gateway la IP privada del firewall, entonces el fichero de configuración de la red DMZ añadimos lo siguiente:

```
# 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
```

Ya configurado la red DMZ, 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*.



```
usuario@Server-p08:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; preset: enabled)
   Active: active (running) since Sat 2023-11-18 09:08:41 WET; 1h 49min ago
     Docs: man:nginx(8)
  Process: 564 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
  Process: 570 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 572 (nginx)
   Tasks: 9 (limit: 9469)
  Memory: 10.2M
     CPU: 83ms
  CGroup: /system.slice/nginx.service
          └─572 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
            └─573 "nginx: worker process"
              └─574 "nginx: worker process"
                └─575 "nginx: worker process"
                  └─576 "nginx: worker process"
                    └─577 "nginx: worker process"
                      └─578 "nginx: worker process"
                        └─579 "nginx: worker process"
                          └─580 "nginx: worker process"

Warning: some journal files were not opened due to insufficient permissions.
usuario@Server-p08:~$
```

Figura 2.1: Estado del servidor web nginx

3. Reglas de filtrado para el firewall

El script de configuración del firewall se muestra a continuación:

```
#!/bin/bash

# Reset de las reglas
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -X
iptables -t nat -Z

# Acceso ssh al firewall
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -i ens3 -p tcp --dport 22 -j ACCEPT

# Acceder desde la red interna (con la ip publica) a los servicios web
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-destination 192.168.10.100:80

# Acceder desde la red interna a servidores Web de Internet
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

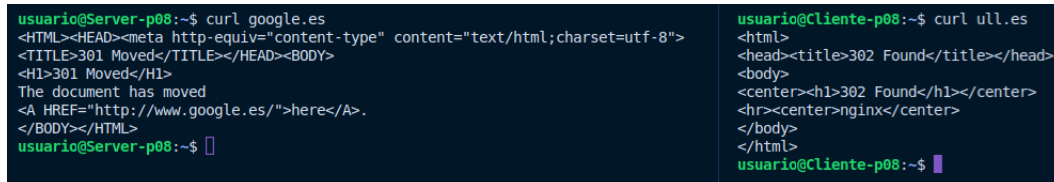
# Permite acceder a los servicios web (DMZ) desde internet
iptables -A FORWARD --match state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i ens3 -o ens7 -p tcp --match multiport --dports 80,443 -j ACCEPT

# Permitir tráfico DNS
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
```

Para permitir tráfico web desde la red interna a los servidores web de Internet, se debe añadir las siguientes reglas:

```
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
```



The image shows two terminal windows side-by-side. The left window, titled 'usuario@Server-p08:~\$', shows a 'curl google.es' command being executed. The output displays an HTTP 301 Moved response from Google, indicating the document has moved to 'http://www.google.es/'. The right window, titled 'usuario@Cliente-p08:~\$', shows a 'curl ull.es' command being executed. The output displays an HTTP 302 Found response from 'ull.es', indicating the resource is located at 'http://www.ull.es/'.

Figura 3.1: Accediendo a los servidores web de Internet desde la red interna

Para permitir el tráfico Web desde Internet al servidor web que se encuentra en la DMZ, se debe añadir las siguientes reglas:

```
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
```

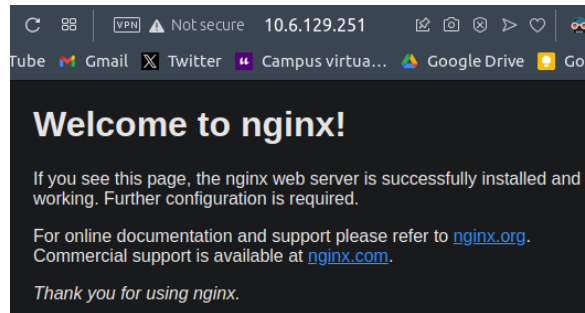


Figura 3.2: Accediendo al servidor web de la DMZ desde Internet

Y por último, para permitir el tráfico Web desde la red interna al servidor web de la DMZ, se debe añadir las siguientes reglas:

```
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-destination 192.168.10.100:80
```

En la siguiente figura se muestra el acceso al servidor web de la DMZ desde la red interna.

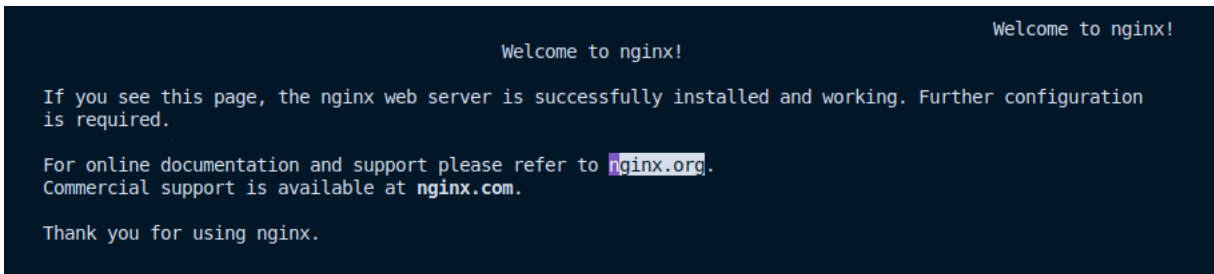


Figura 3.3: Accediendo al servidor web de la DMZ desde la red interna