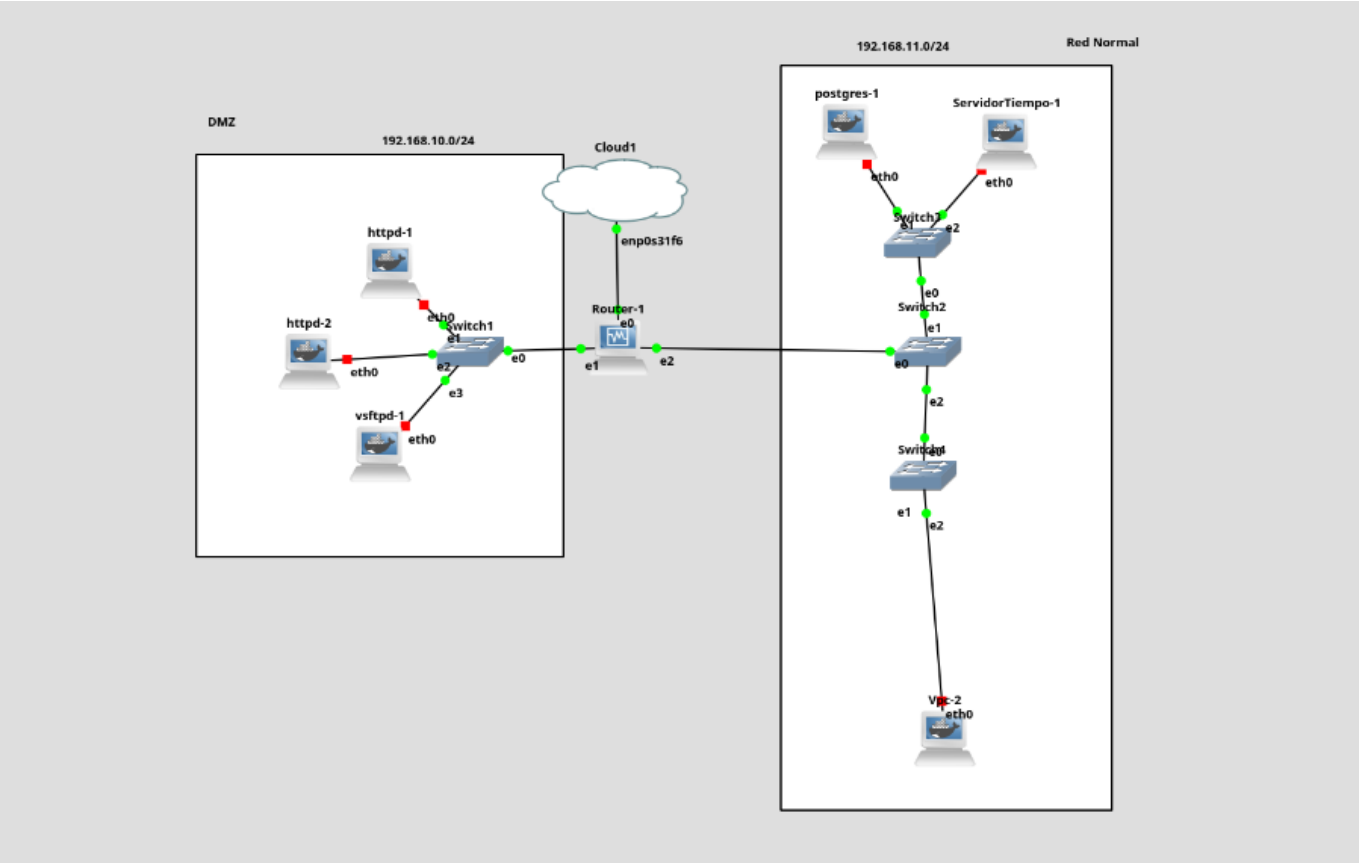
UD3 – Instalación y configuración de cortafuegos y proxies

Configuración netplan

```
    # Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: true
      nameservers:
        addresses: [10.239.3.7, 10.239.3.8]
    #DMZ
    enp0s8:
      addresses: [192.168.10.1/24]
    # LAN
    enp0s9:
      addresses: [192.168.11.1/24]
```

- Con esto tendremos la configuracion del netplan como router y la red de la **DMZ** y la **LAN**



1. Como ya solemos hacer, simularemos que Internet es la red del aula

2. La LAN de la empresa tiene una dirección privada con la máscara correspondiente para poder tener un rango para servidores y otro para equipos de los empleados dentro de la misma red (la red no debe entrar en conflicto con nuestra red del aula)

- Cambiaré la red del servidor de tiempo a 192.168.11.170 para que me sea mas cómodo.
- Así los equipos de Postgre y el servidor de tiempo trabajarán con máscara 25 (255.255.255.128) y los equipos normales y el del administrador con máscara 26 (255.255.255.192).

3. La DMZ tendrá la dirección de red que creamos conveniente (tampoco puede entrar en conflicto con la red del aula)

- La dmz tiene la red 192.168.10.1/24

4. Se debe realizar un enmascaramiento tando de la LAN como de la DMZ hacia el exterior, de manera que todos los equipos salgan con la IP pública del router

```
# Establece políticas predeterminadas (denegar todo)
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT DROP


# Permite el tráfico de retorno y las conexiones establecidas
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Configuracion básica del enroutamiento
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

5. Todos los equipos de los empleados (los servidores NO) en la LAN deben poder realizar lo siguiente (únicamente, el resto debe estar denegado):

Consultar páginas web.

```
#WEB
sudo iptables -A FORWARD -p tcp --dport 80 -m iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p tcp --dport 443 iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p tcp --sport 80 iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p tcp --sport 443 iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
```

```
#DNS
sudo iptables -A FORWARD -p udp --dport 53  iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p tcp --dport 53 iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p udp --sport 53 iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p tcp --sport 53 iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
```

Utilizar el correo electrónico (tanto POP3 como IMAP).

```
sudo iptables -A OUTPUT -p tcp --dport 110 iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 995  iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT

sudo iptables -A FORWARD -p tcp --dport 110 -d [IP_DEL_SERVIDOR_DE_CORREO]
iprange --src-range 192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p tcp --dport 995 -d [IP_DEL_SERVIDOR_DE_CORREO]
iprange --src-range 192.168.11.50-192.168.11.100 -j ACCEPT

sudo iptables -A OUTPUT -p tcp --dport 143 iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 993  iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT

sudo iptables -A FORWARD -p tcp --dport 143 -d [IP_DEL_SERVIDOR_DE_CORREO]
iprange --src-range 192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p tcp --dport 993 -d [IP_DEL_SERVIDOR_DE_CORREO]
iprange --src-range 192.168.11.50-192.168.11.100 -j ACCEPT
```

Realizar pings

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A OUTPUT -p icmp --icmp-type echo-reply iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT

sudo iptables -A FORWARD -p icmp --icmp-type echo-request iprange --src-
range 192.168.11.50-192.168.11.100 -j ACCEPT
sudo iptables -A FORWARD -p icmp --icmp-type echo-reply iprange --src-range
192.168.11.50-192.168.11.100 -j ACCEPT
```

6. Todos los equipos de la LAN deben poder acceder a los servicios ofrecidos en la DMZ.

```
iptables -A FORWARD -i enp0s8 -o enp0s9 -j ACCEPT
```

7. Los servidores de dentro de la LAN también podrán consultar páginas web (ya que esos puertos también se utilizan para actualizaciones).

```
sudo iptables -A FORWARD -p tcp --dport 80 -m iprange --src-range
192.168.11.128-192.168.11.255 -j ACCEPT
sudo iptables -A FORWARD -p tcp --dport 443 iprange --src-range
192.168.11.128-192.168.11.255 -j ACCEPT
sudo iptables -A FORWARD -p tcp --sport 80 iprange --src-range
192.168.11.128-192.168.11.255 -j ACCEPT
sudo iptables -A FORWARD -p tcp --sport 443 iprange --src-range
192.168.11.128-192.168.11.255 -j ACCEPT
#DNS
sudo iptables -A FORWARD -p udp --dport 53  iprange --src-range
192.168.11.128-192.168.11.255 -j ACCEPT
sudo iptables -A FORWARD -p tcp --dport 53 iprange --src-range
192.168.11.128-192.168.11.255 -j ACCEPT
sudo iptables -A FORWARD -p udp --sport 53 iprange --src-range
192.168.11.128-192.168.11.255 -j ACCEPT
sudo iptables -A FORWARD -p tcp --sport 53 iprange --src-range
192.168.11.128-192.168.11.255 -j ACCEPT
```

8. El servidor de tiempo será el único equipo de la LAN que pueda hacer consultas NTP al exterior.

```
sudo iptables -A OUTPUT -p udp --dport 123 -s 192.168.11.123 -j ACCEPT
# Te he puesto la ip de cuco.rediris.es, puedes poner más
sudo iptables -A FORWARD -p udp --dport 123 -d 130.206.0.1 -s
192.168.11.123 -j ACCEPT
```

9. El equipo interno del administrador debe ser el único que pueda conectarse al equipo que contiene el firewall. Se conectará por SSH.

```
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.11.99 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -d 192.168.11.99 -j ACCEPT
```

10. El administrador de la red tiene una IP pública fija en Internet (su dirección de casa) que es la 192.168.2.254. El administrador de la red debe poder acceder desde su casa por SSH al router, a su equipo dentro de la LAN, a los 2 servidores de la LAN y a los 3 servidores de la DMZ.

- Para conectarse al router

```
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.2.254 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -s 192.168.2.254 -j ACCEPT
```

- Para la red interna
- Equipo del administrador

```
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.111.99 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -d 192.168.111.99 -j ACCEPT
sudo iptables -t nat -A PREROUTING -p tcp --dport 2222 -j DNAT --to-
destination 192.168.111.99:22
```

- Servidor mariadb

```
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.111.200 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -d 192.168.111.200 -j ACCEPT
sudo iptables -t nat -A PREROUTING -p tcp --dport 2223 -j DNAT --to-
destination 192.168.111.200:22
```

- Servidor Web

```
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.111.88 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -d 192.168.111.88 -j ACCEPT
sudo iptables -t nat -A PREROUTING -p tcp --dport 2224 -j DNAT --to-
destination 192.168.111.88:22
```

- FTP

```
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.111.254 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -d 192.168.111.254 -j ACCEPT
sudo iptables -t nat -A PREROUTING -p tcp --dport 2225 -j DNAT --to-
destination 192.168.111.254:22
```

11. 12. El servidor web y el de la Intranet deben estar accesibles desde cualquier equipo del exterior (aunque sólo podemos probar las conexiones http, crearemos también la regla para permitir https). El servidor FTP debe estar accesible desde cualquier equipo del exterior.

```
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp --dport 443 -j ACCEPT
```

```
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp --dport 53 -j ACCEPT
```

13. El servidor web debe poder realizar consultas al servidor que tiene la base de datos.

```
iptables -A FORWARD -i 192.168.10.100 -o 192.168.11.0 -p tcp --dport 2323 -
j ACCEPT
```

14. No podrá consultarse nada más desde la DMZ hacia la LAN.

```
iptables -A FORWARD -i enp0s8 -o enp0s9 -j DROP
```