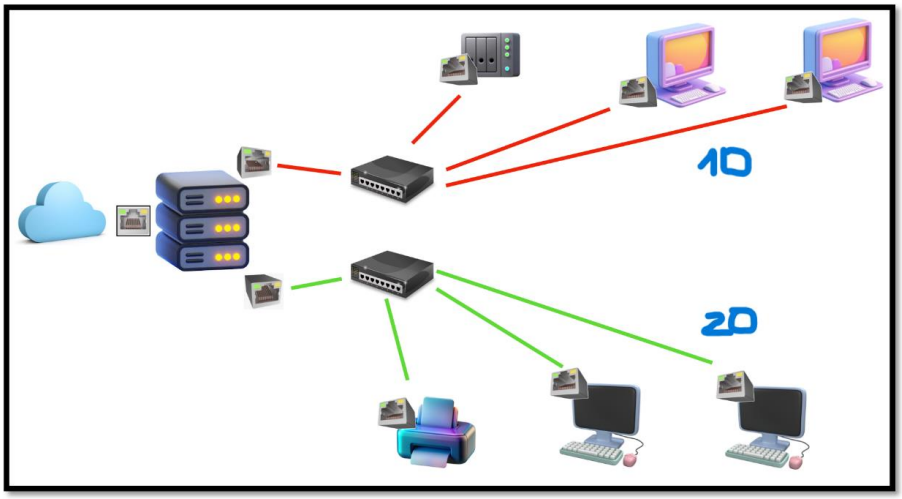
- Si no pones nada por defecto las tablas con las que se trabaja son filter
- Las reglas las lee por orden. Si cumple una ya no va a leer las siguientes
- Router no es lo mismo que internet! (de una red a internet pasas por el router, es decir, es FORWARD)

sudo iptables -L ----> Para ver lo que tenemos
sudo iptables -L -v --> Más info (interfaces p ej)



* EJERCICIO 1: Los verdes pueden hacer todo pero los rojos no pueden salir a internet.

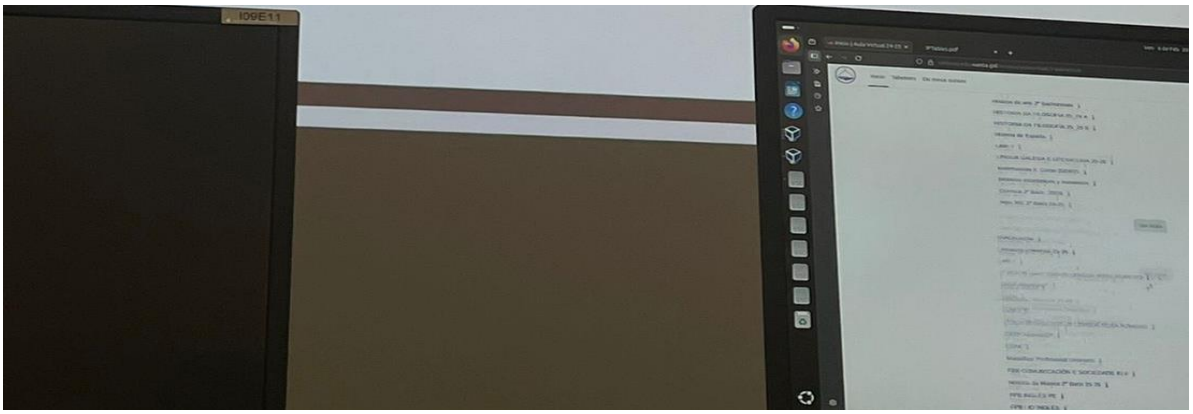
Opción 1 simple:
sudo iptables -A FORWARD -i enp0s3 -o enp0s9 -j DROP (chapar internet de una red pero no la conexión con la otra red a través del router -son las interfaces de internet y de esa red-)

Opción 2 más larga:
- Quitamos todo:
sudo iptables -P INPUT DROP
sudo iptables -P OUTPUT DROP
sudo iptables -P FORWARD DROP

-Abrir origen verde: sudo iptables -A FORWARD -s 192.168.20.101/24 -j ACCEPT (Con máscara capa toda la red, sin ella solo esa IP)
-Abrir origen rojo destino verde: sudo iptables -A FORWARD -s 192.168.10.101/24 -d 192.168.20.101/24 -j ACCEPT
-Abrir origen router destino verde: sudo iptables -A FORWARD -i enp0s3 -o enp0s8 -j ACCEPT

Opción 3 con ESTABLISHED: **REVISAR**
- Origen verde: sudo iptables -A FORWARD -s 192.168.20.101/24 -m state - -state NEW, ESTABLISHED -j ACCEPT
- Origen rojo: sudo iptables -A FORWARD -s 192.168.10.0/24 -d 192.168.20.0/24 -m state --state NEW,ESTABLISHED -j ACCEPT

* EJERCICIO 2:

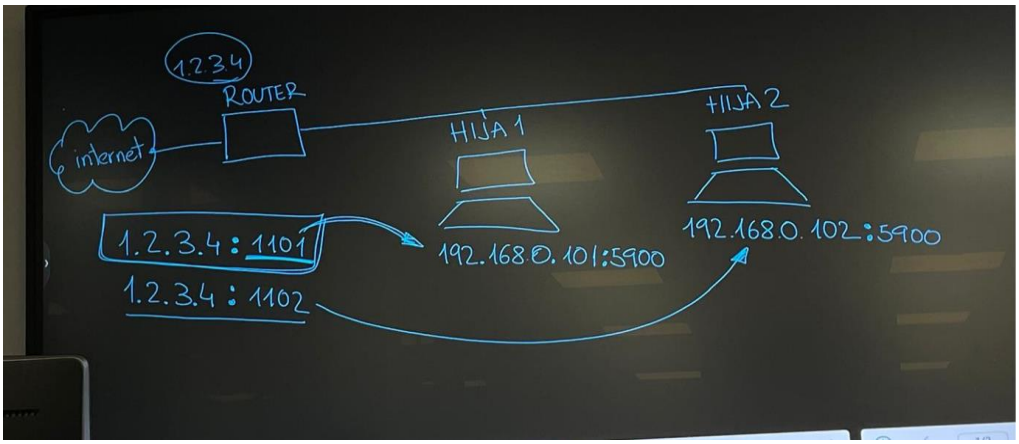


-

Puedo hacer ping a internet desde rojo? No porque tira los nuevos
- Puedo hacer ping de rojo a verde? No porque tira los nuevos
- Puedo hacer ping de un rojo a otro rojo? Sí porque están en la misma red y no pasan por el firewall

TABLAS NAT (hay que especificar con -t nat porque por defecto escribimos en filter)

* EJERCICIO: accedes a la IP pública y quieres entrar a los equipos (a través de los puertos)



sudo iptables -t nat -A PREROUTING -d 1.2.3.4 - -dport 1101 -j DNAT - -to-destination 192.168.0.101:5900