

# Escuela de Ingeniería en Computación

---

## Redes IC-7602

---

*Apuntes 30-10-2022*

Profesor: Nereo Campos

Estudiante: Mario Fernández Robert - 2018163975

---

## Conceptos importantes

---

Cuando se expone a internet una aplicación es importante respetar los puertos de consenso

- Puerto 80:
  - Navegación no segura (http)
  - Siempre está abierto
  - Puerto default
  - Permite hacer filtros de contenido
- Puerto 443:
  - Se fuerza una comunicación segura
  - Información viaja encriptada
  - Útil en la dark web

## Firewall (iptables)

---

### Tablas y cadenas

Útiles para tomar decisiones de ruteo ya sea antes o después de recibir un paquete, se definen como reglas en el firewall de la estación, en linux se puede utilizar iptables, cabe destacar que SO's como Alpine o Centos tienen reglas pre-configuradas que pueden interferir con nuestro desarrollo.

Estas reglas también nos ayudan a transformar paquetes de la manera que nos parezca conveniente y así tener control sobre nuestro network.

Con estas reglas podemos aceptar o rechazar paquetes de diferentes maneras, incluso bloqueando todo el tráfico entrante de un puerto o bloqueando el tráfico saliente, etc.

Estas reglas nos permiten tener seguridad en capas, lo cual es muy conveniente para evitar cualquier tipo de ataque malicioso.

### Reglas de filtrado

- INPUT: Hace referencia a los paquetes que llegan al sistema
- OUTPUT: Filtrado de los paquetes que salen de nuestra red
- FORWARD: Referencia al tráfico que el router reenvía a otros equipos

## Tabla NAT

- PREROUTING: Mediante esta cadena, indicamos que se realice una determinada acción sobre el paquete antes de que sea enrutado. Por ejemplo, para que desde el exterior se tenga acceso a un servidor.
- POSTROUTING: Permite realizar una determinada acción antes de que el paquete salga del firewall.
- OUTPUT: Permite modificar los paquetes generados en el propio firewall antes de ser enrutados.

## Parametros

- -p, --protocol: Sirve para especificar el protocolo que se utiliza (tcp, udp, icmp, etc. Además, si queremos especificar el puerto, se acompaña del parámetro -dport.
- -s, --source: Con este parámetro indicamos la dirección IP de origen.
- -d, --destination: Especificamos la dirección IP de destino.
- -i, --in-interface: Especifica la interfaz de red de entrada (eth0, eth1,...)
- -o, --out-interface: Especifica la interfaz de red de salida (eth0, eth1,...)

## Acciones

Una vez definida la regla, hay que indicar la acción que realizaremos sobre aquellos paquetes que la cumplan. Para indicar esta acción, haremos uso del parámetro -j seguido de alguno de los siguientes valores

- ACCEPT: Mediante esta acción estamos indicando que el paquete sea aceptado.
- DROP: Se elimina el paquete y no se le envía al equipo que hizo la petición ningún mensaje de respuesta.
- REJECT: Similar al caso anterior, pero en esta ocasión se manda un paquete ICMP al equipo que hizo la petición para indicarle que no está permitida.
- DNAT: Esta acción es utilizada en la cadena PREROUTING de la tabla NAT para modificar la IP de destino. Tiene que llevar asociado el parámetro -to.
- SNAT: Acción asociada en la cadena POSTROUTING para modificar la IP origen. Al igual que el caso anterior, le tiene que acompañar el parámetro -to.
- MASQUERADE: Acción equivalente a SNAT pero utilizada cuando tenemos una dirección IP dinámica en la interfaz de salida.
- REDIRECT: Se utiliza en la cadena PREROUTING para modificar la dirección IP que tenga la interfaz de red de entrada.