NETFILTER/IPTABLES

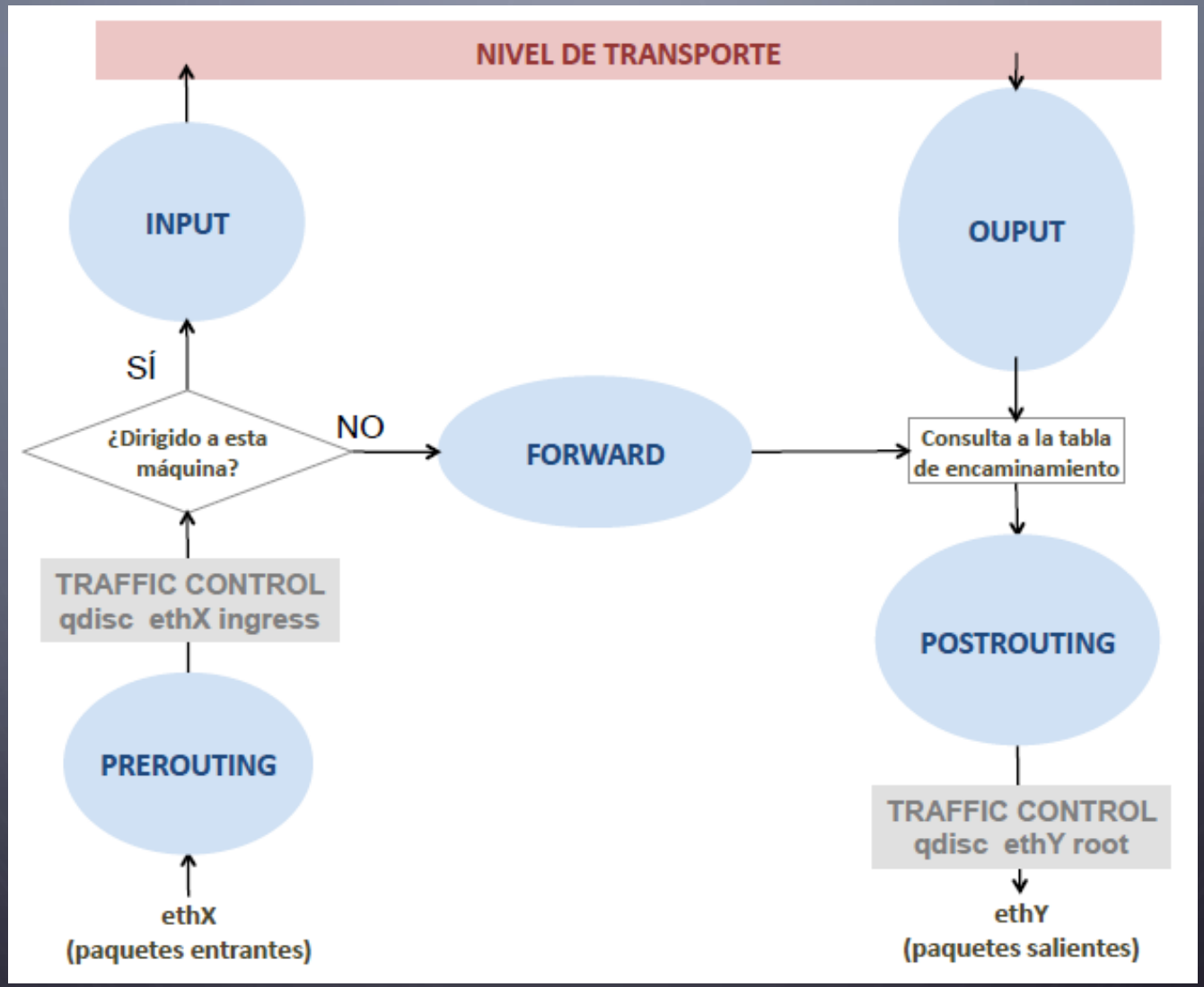
Ing. Germán Imeroni
Ing. Leonardo Dominguez
CyDAR 2018

NETFILTER/IPTABLES

TABLAS

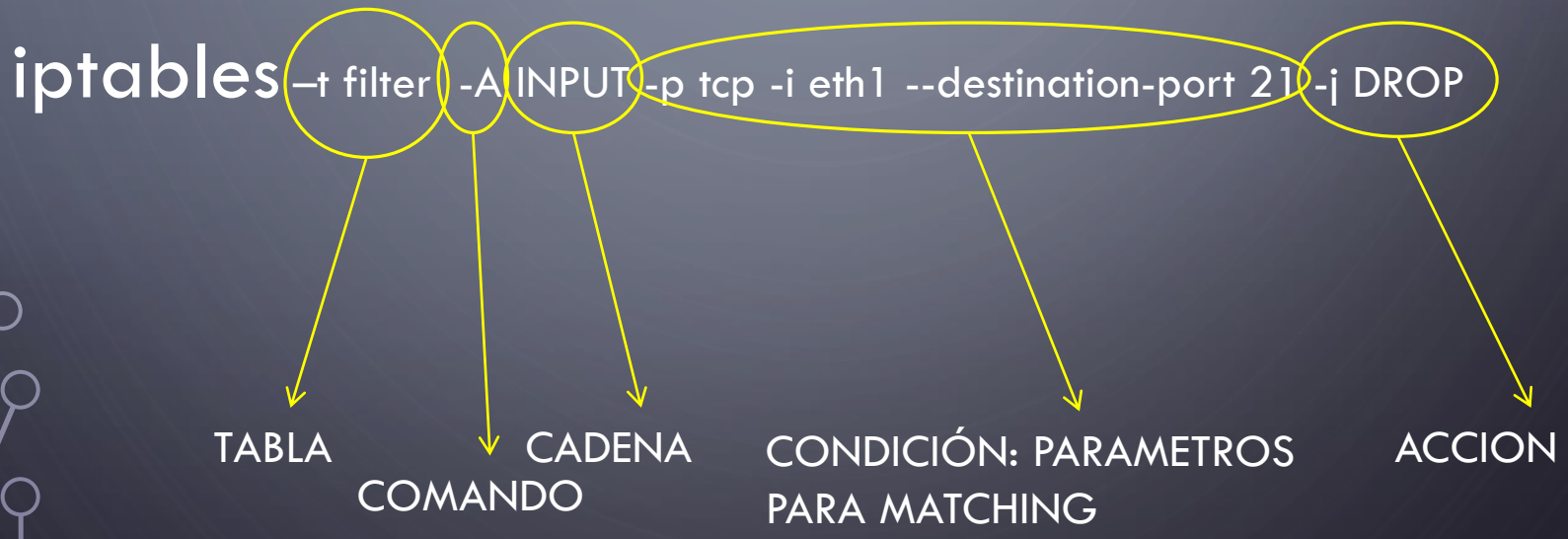
NAT	Tabla responsable de reescribir direcciones o puertos
FILTER	Tabla responsable del filtrado de paquetes
MANGLE	Tabla responsable de ajustar opciones de paquetes manejar calidad de servicio, marcado o valores de TTL

NETFILTER/IPTABLES – TIPOS DE CADENAS



NETFILTER/IPTABLES

iptables [–t <tabla>] <comando> [<cadena>] [<condición>][<acción>]
En donde […] significa "opcional"
Por ej:



NETFILTER/IPTABLES - COMANDOS

- iptables [-t <tabla>] -L [<cadena>] [-v]
  - Lista las reglas. Si se omite la cadena el comando actúa sobre todas. Con -v se mostrara también el numero de paquetes y bytes que han cumplido la condición de cada regla.
- iptables [-t <tabla>] -D <cadena> <numregla>
  - Borra una regla dado su numero de regla.
- iptables [-t <tabla>] -A <cadena> <condicion> <accion>
  - Añade una regla al final.

NETFILTER/IPTABLES - CONDICIONES

- Protocolo
  - -p <protocolo>
- Dirección IP
  - -s <dirIP[/máscara]>: dirección origen
  - -d <dirIP[/máscara]>: dirección destino
- Puerto
  - --sport <puerto|puertoInicio:puertoFin>: puerto origen
  - --dport <puerto|puertoInicio:puertoFin>: puerto destino
- Interfaz
  - -i <interfaz>: interfaz de entrada
  - -o <interfaz>: interfaz de salida

NETFILTER/IPTABLES - ACCIONES

- -j SNAT --to-source [<dirIP>][:<puerto>]
  - Realiza Source NAT sobre los paquetes salientes (es decir, se cambia dirección IP y/o puerto origen). Solo se puede realizar en la cadena POSTROUTING. Esta regla hace que también se cambie automáticamente la dirección de destino del tráfico entrante de respuesta al saliente de la misma conexión.
- -j DNAT --to-destination [<dirIP>][:<puerto>]
  - Realiza Destination NAT sobre los paquetes entrantes (es decir, se cambia dirección IP y/o puerto destino). Solo se puede realizar en la cadena PREROUTING. Esta regla solo es necesaria para abrir puertos, es decir, permitir tráfico entrante nuevo.
- -j MASQUERADE --to-source [<dirIP>][:<puerto>]
  - Permite realizar enmascaramiento IP o NAPT. Esto consiste en que el servidor identifica que uno de los equipos de la red intenta conectar a una dirección de fuera de ésta, y es el mismo servidor el que realiza la petición, en lugar de que la máquina cliente lo haga. Así, el servidor toma la dirección IP y puerto de la máquina que hace la solicitud, la "enmascara" con la dirección IP y puerto que le ha sido asignada, la envía, y cuando llega el paquete de respuesta lo "reenvía" a la máquina y puerto que realizó la petición.
- -j ACCEPT
  - Acepta el paquete
- -j DROP
  - Permite descartar el paquete sin procesarlo
- -j REJECT
  - Tiene el mismo efecto que DROP, pero retorna un paquete de error al origen

NETFILTER/IPTABLES

- Ejemplos:

ACCIONES EN TABLAS FILTER

ACCEPT, DROP , REJECT … RETURN

iptables -L -t filter //Lista las cadenas de la tabla filter

iptables –t filter -A INPUT -p tcp -i eth1 --destination-port 21 -j DROP //borra según protocolo y puerto destino

iptables –t filter -A INPUT –s 10.0.0.2 -j REJECT //rechaza los del origen especificado

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

iptables –t filter -D INPUT 1 //borra la entrada 1

iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth1 -j DNAT --to <<IP>>:8080

iptables –t filter -A FORWARD -s 10.0.0.2 -j REJECT