

PREROUTING: ANTES DE RUTEAR.

Significa que todavía no está definido para donde va el paquete. El paquete pasa por DNAT y luego pasa por la tabla de ruteo y ahí se define el destino. Justamente DNAT cambia la IP destino del paquete, entonces es NECESARIO que esté antes de la tabla de ruteo.

POSTROUTING: DESPUES DE RUTEAR.

Significa que ya está claro el destino del paquete, ya pasó por la tabla de ruteo. Pero antes de salir a la red, SNAT cambia la IP origen del paquete por otra IP. SNAT se suele usar cuando tenés una LAN (ej: 192.168.100.0/24) y tenés que mandar un paquete a internet. Como no se puede mandar un paquete con IP PRIVADA a internet, cuando éste pasa por el router, SNAT le pone a cada paquete la IP PUBLICA del router. Por eso es necesario definir la interfaz de destino (que sería el cable por donde salís a internet) Todo lo que vaya por esa interfaz tiene que tener IP PUBLICA.

Ejemplo: `iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j MASQUERADEDNAT.`

Se suele usar para lo contrario. Por ejemplo, vos estás en China y querés entrar a un servidor web que tenés en la PC de tu casa, que está en una LAN con la IP 192.168.100.1. ¡Es imposible mandar por internet un paquete con IP destino PRIVADA! Entonces le mandás el paquete al router de tu casa (que tiene IP PUBLICA) Cuando el paquete pasa por el router, DNAT le cambia la IP destino por la IP PRIVADA de tu PC.

Ejemplo: `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.100.1:80`

En ambos casos eth0 sería la interfaz para internet.

- DNAT se puede hacer con PREROUTING
- SNAT se puede hacer con POSTROUTING