¿Qué es iptables?

IPtables es un sistema de firewall vinculado al kernel de linux. Un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación; iptables esta integrado con el kernel, es parte del sistema operativo.

¿Cómo se pone en marcha?

Realmente lo que se hace es aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall.

Para los paquetes que van a la propia maquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o maquinas se aplican simplemente reglas FORWARD.

Pero antes de aplicar esas reglas es posible aplicar reglas de NAT: estas se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino.

Incluso antes de las reglas de NAT se pueden meter reglas de tipo MANGLE, para modificar los paquetes; son reglas poco conocidas y es probable que no se usen.

Por tanto tenemos tres tipos de reglas en iptables:
− MANGLE
− NAT: reglas PREROUTING, POSTROUTING
− FILTER: reglas INPUT, OUTPUT, FORWARD

Denegar Ping con Iptables:

1.- sudo -i

2.- iptables -A OUTPUT --proto icmp -j DROP → Regla que impide que mi maquina pueda hacer ping fuera.

4.- Realizar ping a la 192.168.8.1 para ver si hace ping o no.