

## ¿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.

```

usuario@usuario-H81M-D2V: ~
colisiones:0 long.colaTX:1000
Bytes RX:22351 (22.3 KB) TX bytes:22351 (22.3 KB)

usuario@usuario-H81M-D2V:~$ ping 192.168.8.
ping: unknown host 192.168.8.
usuario@usuario-H81M-D2V:~$ ping 192.168.8.1
PING 192.168.8.1 (192.168.8.1) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 192.168.8.1 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11252ms

usuario@usuario-H81M-D2V:~$ 
root@usuario-H81M-D2V:~# ping 192.168.8.1
PING 192.168.8.1 (192.168.8.1) 56(84) bytes of data.
64 bytes from 192.168.8.1: icmp_seq=1 ttl=64 time=0.446 ms
64 bytes from 192.168.8.1: icmp_seq=2 ttl=64 time=0.481 ms
64 bytes from 192.168.8.1: icmp_seq=3 ttl=64 time=0.484 ms
64 bytes from 192.168.8.1: icmp_seq=4 ttl=64 time=0.340 ms
64 bytes from 192.168.8.1: icmp_seq=5 ttl=64 time=0.531 ms
64 bytes from 192.168.8.1: icmp_seq=6 ttl=64 time=0.390 ms
64 bytes from 192.168.8.1: icmp_seq=7 ttl=64 time=0.332 ms
^C
--- 192.168.8.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6136ms
rtt min/avg/max/mdev = 0.332/0.429/0.531/0.071 ms
root@usuario-H81M-D2V:~# sudo -l
root@usuario-H81M-D2V:~# iptables -A INPUT --proto icmp -j DROP
root@usuario-H81M-D2V:~# iptables -A OUTPUT --proto icmp -j DROP
root@usuario-H81M-D2V:~# 

```