Guía 2

1. **Añadir una regla a la cadena INPUT para aceptar todos los paquetes que se originan desde la dirección 192.168.106.200.**
   iptables -A INPUT -s 192.168.106.200 -j ACCEPT
2. **Eliminar todos los paquetes que entren.**
   iptables -A INPUT -j DROP
3. **Permitir la salida de paquetes.**
   iptables -A OUTPUT -j ACCEPT
4. **Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.106.200.**

   iptables -A INPUT -s 192.168.106.200 -j DROP
5. **Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección de red 192.168.0.0.**

   iptables -A INPUT -s 192.168.0.0/24 -j DROP
6. **Permitir el acceso al servidor web (puerto TCP 80).**
   iptables -A INPUT -p tcp --dport 80 -j ACCEPT
7. **Permitir el acceso a nuestro servidor ftp (puerto TCP 20 y 21).**
   iptables -A INPUT -p tcp - dport 20 -j ACCEPT
   iptables -A INPUT -p tcp --dport 21 -j ACCEPT
8. **Permitimos a la máquina con IP 192.168.106.200 conectarse por medio de SSH.**
   iptables -A INPUT -s 192.168.106.200 -p tcp --dport 22 -j ACCEPT
9. **Rechazamos a la máquina con IP 192.168.106.200 conectarse por medio de Telnet.**
   iptables -A INPUT -s 192.168.106.200 -p tcp --dport 23 -j DROP
10. **Rechazamos todo el tráfico que ingrese a nuestra red LAN 192.168.0.0 /24 desde una red remota, como Internet, a través de la interfaz eth0.**
    iptables -A FORWARD -s 0.0.0.0/0 -i eth0 -d 192.168.1.0/24 -j DROP
11. **Cerramos el rango de puerto bien conocido desde cualquier origen:**
    iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 1:1024 -j DROP
    iptables -A INPUT -s 0.0.0.0/0 -p udp --dport 1:1024 -j DROP
12. **Aceptamos que vayan de nuestra red 192.168.0.0/24 a un servidor web (puerto 80)**
    iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -p tcp --dport 80 -j ACCEPT
13. **Aceptamos que nuestra LAN 192.168.0.0/24 vayan a puertos https**
    iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -p tcp --dport 443 -j ACCEPT
14. **Aceptamos que los equipos de nuestra red LAN 192.168.0.0/24 consulten los DNS, y denegamos todo el resto a nuestra red**
    iptables -A FORWARD -s 192.168.1.0/24 -t eth1 -p tcp --dport 53 -j ACCEPT
    iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -p udp --dport S3 -j ACCEPT
    iptables -A FORWARD -s 192.168.1.0/24 -j DROP
15. **Permitimos enviar y recibir e-mail a todos**
    iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 25 -j ACCEPT
    iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 110 -j ACCEPT
16. **Cerramos el acceso de una red definida 192.168.3.0/24 a nuestra red LAN 192.168.2.0/24**
    iptables -A INPUT -s 192.168.3.0/24 -d 192.168.1.0/24 -j DROP
17. **Permitimos el tráfico TCP de un equipo específico 192.168.3.5 a un servicio (puerto 5432) que ofrece un equipo específico (192.168.0.5) y su respuesta**

    iptables -A FORWARD -s 192.168.3.5 -d 192.168.0.5 -p tcp -dport 5432 -j accept

    iptables -A FORWARD -s 192.168.0.5 -d 192.168.3.5 -p tdp -sport 5432 -j accept
18. **Permitimos el paso de paquetes cuya conexión se encuentra establecida**

    iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT