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.**

2. **Eliminar todos los paquetes que entren.**

3. **Permitir la salida de paquetes.**

4. **Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.106.200.**

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.**

6. **Permitir el acceso al servidor web (puerto TCP 80).**

7. **Permitir el acceso a nuestro servidor ftp (puerto TCP 20 y 21).**

8. **Permitimos a la máquina con IP 192.168.106.200 conectarse por medio de SSH.**

9. **Rechazamos a la máquina con IP 192.168.106.200 conectarse por medio de Telnet.**

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.**

11. **Cerramos el rango de puerto bien conocido desde cualquier origen**

12. **Aceptamos que vayan de nuestra red 192.168.0.0/24 a un servidor web (puerto 80)**

13. **Aceptamos que nuestra LAN 192.168.0.0/24 vayan a puertos https**

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**

15. **Permitimos enviar y recibir e-mail a todos**

16. **Cerramos el acceso de una red definida 192.168.3.0/24 a nuestra red LAN 192.168.2.0/24**

17. **Permitimos el tráfico TCP y UDP 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**

18. **Permitimos el paso de paquetes cuya conexión se encuentra establecida**