Actividad 4 Mecanismos de defensa de red

Mauricio Josafat Salinas Carrillo
4 de febrero de 2026

Iptables para las siguientes reglas:

1. Establecer política restrictiva:

    iptables -P INPUT DROP

    iptables -P OUTPUT DROP

    iptables -P FORWARD DROP

2. Permitir el trafico de conexiones ya establecidas

    Iptables -a INPUT

3. Aceptar trafico DNS (TCP) saliente de la red local

    iptables -a OUTPUT -p tcp -j ACCEPT

4. Aceptar correo entrante proveniente de internet en el servidor de correo

    iptables -A FORWARD -d 192.168.1.10 -p tcp --dport 25 -j ACCEPT

5. Permitir correo saliente a internet desde el servidor de correo.

    iptables -A FORWARD -s 192.168.1.10 -p tcp --dport 25 -j ACCEPT

6. Aceptar conexiones HTTP desde internet a Nuestro servidor web.

    iptables -A FORWARD -d 192.168.1.20 -p tcp --dport 80 -j ACCEPT

7. Permitir tráfico HTTP desde la red local a internet

    iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 80 -j ACCEPT