UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Universidad Politécnica de San Luis Potosí

Ingeniería en Tecnologías de la Información

Actividad 04

Mecanismo de defensa en red

Alumno:
Erik De La Rosa Rodríguez
Matrícula: 177700

Asignatura:
CNG V: Seguridad informatica

Docente:
Mtro. Servando López Contreras

San Luis Potosí, S.L.P.
5 de febrero de 2026

Nº	Acción solicitada	Regla iptables sugerida
1	Política restrictiva	iptables -P INPUT DROP iptables -P OUTPUT DROP iptables -P FORWARD DROP
2	Permitir tráfico de conexiones ya establecidas	iptables -A INPUT -m state –state ESTABLISHED,RELATED iptables -A OUTPUT -m state –state ESTABLISHED,RELATE
3	Aceptar tráfico DNS (TCP) saliente de la red local	iptables -A OUTPUT -p tcp –dport 53 -s 192.1.2.0/24 -m state –state NEW -j ACCEPT
4	Aceptar correo entrante proveniente de Internet en el servidor de correo (192.1.2.10)	iptables -A INPUT -p tcp –dport 25 -d 192.1.2.10 -m state –state NEW -j ACCEPT
5	Permitir correo saliente a Internet desde el servidor de correo (192.1.2.10)	iptables -A OUTPUT -p tcp –dport 25 -s 192.1.2.10 -m state –state NEW -j ACCEPT
6	Aceptar conexiones HTTP desde Internet a nuestro servidor web (192.1.2.11)	iptables -A INPUT -p tcp –dport 80 -d 192.1.2.11 -m state –state NEW -j ACCEPT
7	Permitir tráfico HTTP desde la red local a Internet	iptables -A OUTPUT -p tcp –dport 80 -s 192.1.2.0/24 -m state –state NEW -j ACCEPT

Cuadro 1: Reglas de iptables para mecanismos de defensa en red