

Universidad Politécnica de San Luis Potosí

Materia:

Seguridad Informática

Octavo Semestre

Profesor:

Servando López Contreras

Alumna:

América Fabiola Guerra Ramírez - 179884

Tarea: Actividad 4

Fecha de entrega: 4 de febrero de 2026

1. Establecer una política restrictiva.  
iptables -P INPUT DROP  
iptables -P OUTPUT DROP
2. Permitir el tráfico de conexiones ya establecidas.  
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
3. Aceptar tráfico DNS (TCP) saliente de la red local.  
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
4. Aceptar correo entrante proveniente de Internet en el servidor de correo.  
iptables -A INPUT -p tcp --dport 25 -j ACCEPT
5. Permitir correo saliente a Internet desde el servidor de correo.  
iptables -A OUTPUT -p tcp --dport 25 -j ACCEPT
6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.  
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
7. Permitir tráfico HTTP desde la red local a Internet  
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT