CRISTIAN ALEJANDRO RODRIGUEZ MORENO
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

El firewall debe iniciar con una política restrictiva, bloqueando todo tráfico por defecto. Luego, se permite únicamente el tráfico de conexiones ya establecidas o relacionadas, para que las respuestas legítimas no sean bloqueadas.

1. Política restrictiva

iptables -P FORWARD DROP

2. Permitir conexiones ya establecidas o relacionadas:

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

3. Permitir tráfico DNS saliente (TCP) desde la red local:

iptables -A OUTPUT -p tcp --dport 53 -s 192.1.2.0/24 -j ACCEPT

4. Aceptar correo entrante (SMTP) desde Internet hacia servidor de correo (192.1.2.10)

iptables -A INPUT -p tcp --dport 25 -d 192.1.2.10 -j ACCEPT

5. Permitir correo saliente (SMTP) desde servidor de correo (192.1.2.10) hacia Internet:

iptables -A OUTPUT -p tcp --dport 25 -s 192.1.2.10 -j ACCEPT

6. Aceptar conexiones HTTP entrantes desde Internet hacia servidor web (192.1.2.11):

iptables -A INPUT -p tcp --dport 80 -d 192.1.2.11 -j ACCEPT

7. Permitir tráfico HTTP saliente desde la red local hacia Internet:

iptables -A OUTPUT -p tcp --dport 80 -s 192.1.2.0/24 -j ACCEPT