ACTIVIDAD 04

Seguridad Informática

4 DE FEBRERO DE 2026

CASTILLO OLVERA CARLOS RENÉ

182033

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

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

```
iptables -A FORWARD -p tcp \
-s 192.1.2.0/24 -d 0.0.0.0/0 \
--dport 53 -m state --state NEW -j ACCEPT
```

4. Aceptar correo entrante desde Internet al servidor de correo

```
iptables -A FORWARD -p tcp \
-s 0.0.0.0/0 -d 192.1.2.10 \
--dport 25 -m state --state NEW -j ACCEPT
```

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

```
iptables -A FORWARD -p tcp \
-s 192.1.2.10 -d 0.0.0.0/0 \
--dport 25 -m state --state NEW -j ACCEPT
```

6. Aceptar conexiones HTTP desde Internet al servidor web

```
iptables -A FORWARD -p tcp \
-s 0.0.0.0/0 -d 192.1.2.11 \
--dport 80 -m state --state NEW -j ACCEPT
```

7. Permitir tráfico HTTP desde la red local a Internet

```
iptables -A FORWARD -p tcp \
-s 192.1.2.0/24 -d 0.0.0.0/0 \
--dport 80 -m state --state NEW -j ACCEPT
```