

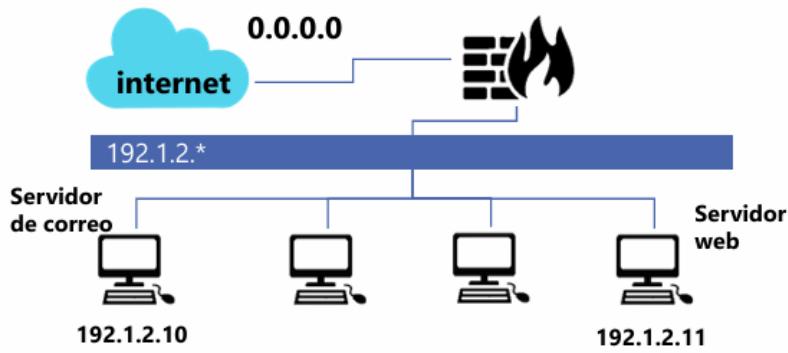
ACTIVIDAD 04

Mecanismos de defensa en red.



Zarate Domínguez David - 175842

4 DE FEBRERO DEL 2026
UPSLP
CNO V Seguridad Informática



1. Establecer una política restrictiva.

- *iptables -P INPUT DROP*
- *iptables -P FORWARD DROP*
- *iptables -P OUTPUT DROP*

2. Permitir el tráfico de conexiones ya establecidas.

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

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

- *iptables -A FORWARD -p tcp --dport 53 -j ACCEPT*

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

El puerto estándar para correo (SMTP) es el 25. El destino es la IP 192.1.2.11.

- *iptables -A FORWARD -p tcp -d 192.1.2.11 --dport 25 -j ACCEPT*

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

- *iptables -A FORWARD -p tcp -s 192.1.2.11 --dport 25 -j ACCEPT*

6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.

El destino es la IP 192.1.2.10 en el puerto 80.

- *iptables -A FORWARD -p tcp -d 192.1.2.10 --dport 80 -j ACCEPT*

7. Permitir tráfico HTTP desde la red local a Internet

- *iptables -A FORWARD -p tcp --dport 80 -j ACCEPT*