UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

# ACTIVIDAD:

# CÓDIGOS

Institución: Universidad Politécnica de San Luis Potosí

## Materia:

CNO V – Seguridad Informática

## Estudiante:

López Castro Diego – 182032

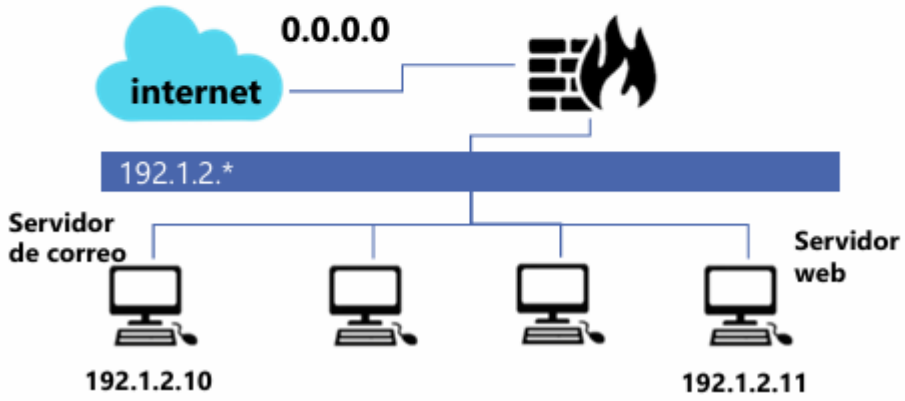
## Profesor:

Mtro. Servando López Contreras

## Fecha de entrega:

02 – Febrero – 2026

Teniendo en cuenta la topología de red mostrada completa la tabla con las reglas de iptables que deberían aplicarse en el Firewall para llevar a cabo las acciones solicitadas. Las reglas, siempre que sea posible, deben determinar protocolo, dirección IP origen y destino, puerto/s origen y destino y el estado de la conexión.




**1. Establecer una política restrictiva.**

Iptable -P DROP

**2. Permitir el tráfico de conexiones ya establecidas.**

Iptable -A FORWARD -m state ESTABLISHED -j ACCEPT

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

Iptable -A FORWARD -p TCP -d 192.1.2.10 –dport53 -j ACCEPT

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

Iptable -A POSROUTING -p TCP -s 192.1.2.11 –dport25 -j ACCEPT

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

Iptable -A PREROUTING -p TCP -d 192.1.2.10 –dport25 -j ACCEPT

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

Iptable -A FORWARD -p TCP -d 192.1.2.10 –dport80 -j ACCEPT

**7. Permitir tráfico HTTP desde la red local a Internet**

Iptable -A FORWARD -p TCP -s 192.1.2.11 –dport443 -j ACCEPT