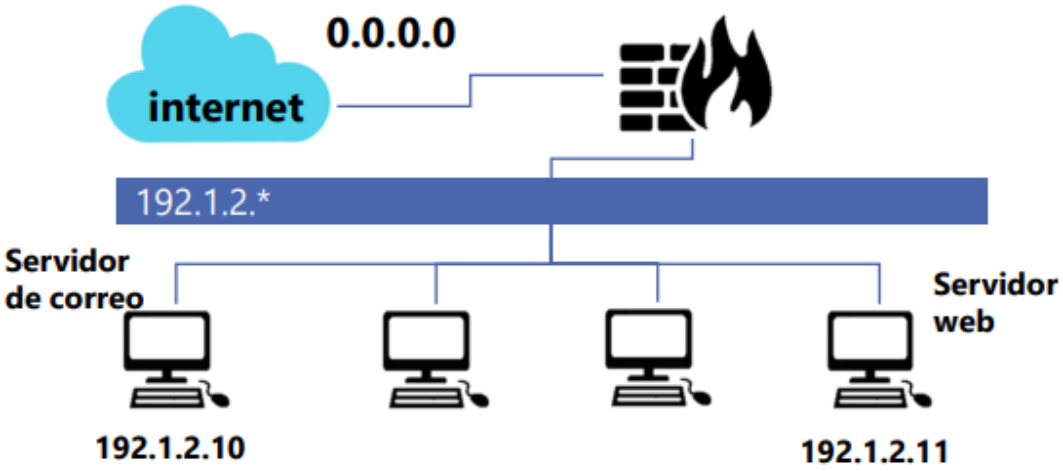
04 DE FEBRERO DE 2026

# ACT04 – MECANISMOS DE DEFENSA EN RED

178823 - RODOLFO CAVAZOS ZACARIAS
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

> 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:

Iptables -A INPUT -j ACCEPT

2.- Permitir el tráfico de conexiones ya establecidas.

Iptables – A INPUT - -state ESTABLISHED -j ACCEPT

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

Iptables -A INPUT -p tcp - - dport 22 -s 192.1.2-* -j ACCEPT

4.- Aceptar correo entrante proveniente de internet en el servidor de correo.

Iptables -A INPUT -p tcp - - dport 22 -s 0.0.0.0 -j ACCEPT

5.- Permitir correo saliente a internet desde el servidor del correo.

Iptables -A OUTPUT -p tcp - -dport 22 -s 192.1.2.10 -j ACCEPT

6.- Aceptar conexiones HTTP desde internet a nuestro servidor web.

Iptables -A OUTPUT -p tcp - -dport -s 0.0.0.0 -j ACCEPT

7.- Permitir trafico HTTP desde la red local a internet.

Iptables -A INPUT -p tcp - -sport 22 -192.1.2.11 -j ACCEPT