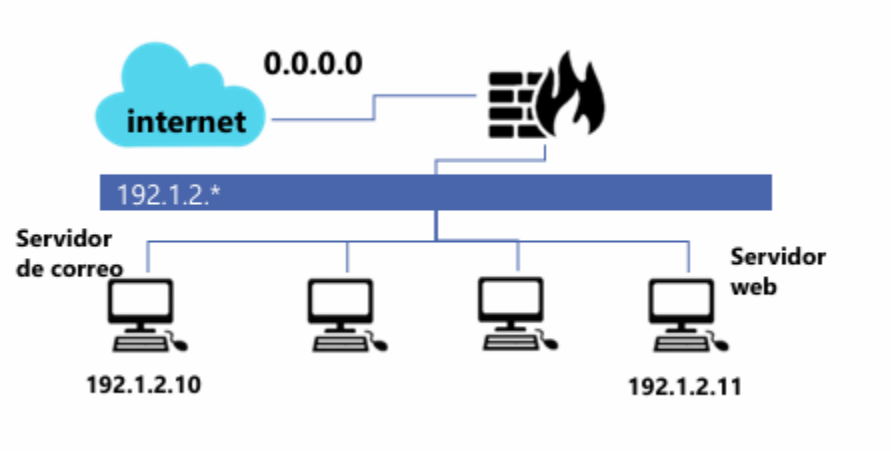
4 DE FEBRERO DE 2026

ACTIVIDAD 4

MECANISMOS DE DEFENSA DE UNA RED

BRIAN SALVADOR ESPINOZA AGUILAR
175031
Universidad Politécnica de San Luis Potosí

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 -p tcp - -dports 80 -j DROP

2. Permitir el tráfico de conexiones ya establecidas.

    Iptables -A INPUT -p tcp -m state - -state ESTABLISHED -j ACCEPT

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

    iptables -A OUTPUT -p tcp -j ACCEPT

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

    Iptables -A INPUT -p tcp -s 192.1.2.10 -ACCEPT

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

    Iptables -A OUTPUT -p tcp -s 192.1.2.10 -ACCEPT

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

    iptables -A INPUT -p tcp -s 192.1.2.10 - -dports 80 -j ACCEPT

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

    Iptables -A INPUT -p tcp - -dports 80 -j ACCEPT