Universidad Politecnica de San Luis Potosi

CON V: Seguridad Informatica

Maestro: Servando Lopez Contreras

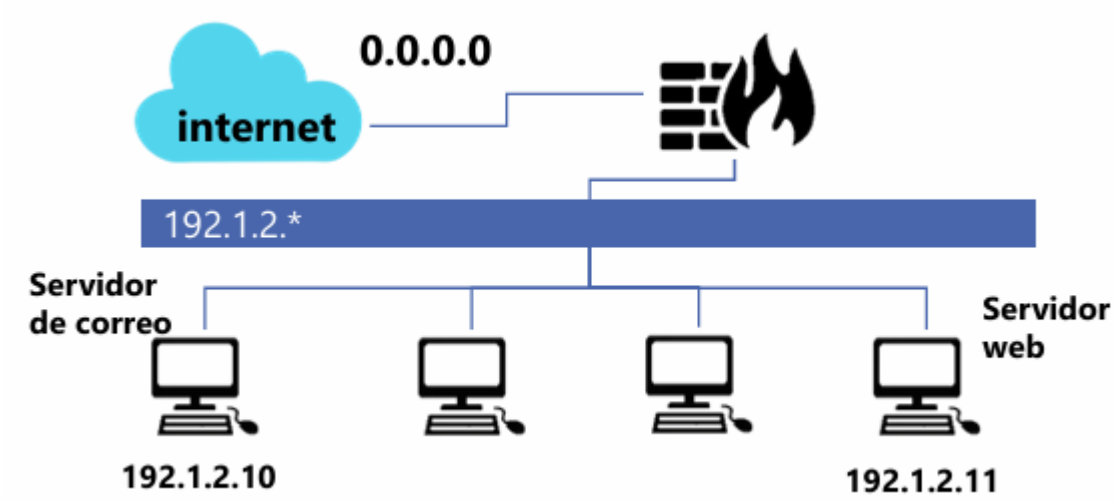
Alumno: Gómez Arreguin Donaldo Demián

Matricula: 179822

Fecha: 04 de febrero de 2026

Tarea: ACTIVIDAD 04 Mecanismos de defensa en red

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 -P INPUT DROP

Iptables -P OUTPUT DROP

2. Permitir el 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

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

Iptables -A OUTPUT -p tcp –dport 53 -s 192.1.2.0/24 -j ACCEPT

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

Iptables -A FORWARD -p tcp –dport 25-d 192.1.2.10 \ -m state –state NEW, ESTABLISHED -j ACCEPT

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

Iptables -A FORWARD -p tcp –sport 25 -s 192.1.2.10 \ -m state –state ESTABLISHED -j ACCEPT

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

Iptables -A FORWARD -p tcp –dport 80 -d 192.1.2.11 \ -m state –state NEW, ESTABLISHED -j ACCEPT

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

Iptables -A FORWARD -p tcp –dport 80 -s 192.1.2.8/24 \ -m state –state NEW, ESTABLISHED -j ACCEPT