4 DE FEBRERO DE 2026

ACTIVIDAD 4

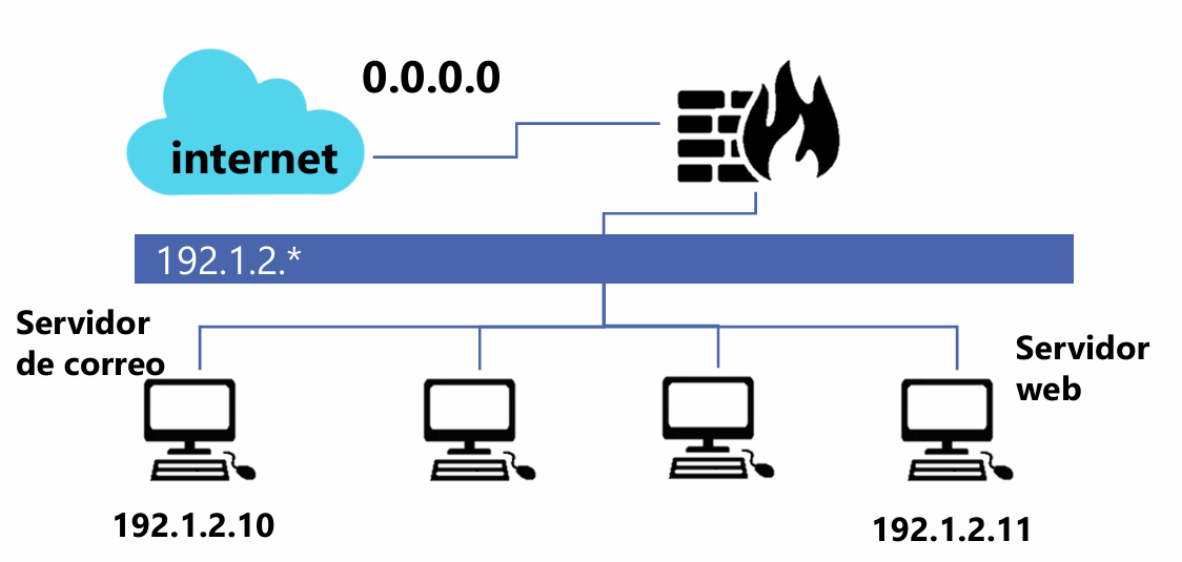
MECANISMOS DE DEFENSA EN RED

BRUNO AXEL PUENTE LUNA
177876

Contenido

Descripción

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 7 -J DROP

(Desecha las solicitudes del protocolo ECHO)

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 INPUT -p TCP - - dports 53 -o wlan0 -J ACCEPT

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

Iptables -A INPUT -p TCP -m multiport - - sports 109,110,174,143,209,465,993,995,

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

iptables -A OUTPUT -p tcp --dport 25 -j ACCEPT

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

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

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

iptables -A FORWARD -p tcp --dport 80 -s 192.168.0.0/24 -j ACCEPT iptables -A FORWARD -p tcp --dport 80 -s 192.168.0.0/24 -j ACCEPT