MECANISMOS DE DEFENSA DE RED

CNO V: Seguridad Informática

Alonso Castillo Omar Karim 179033
Mtro. Servando López Contreras

04/02/2026

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.

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD 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 -j ACCEPT

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

iptables -A OUTPUT -p tcp -s 192.1.2.10 -d 0.0.0.0/0 --dport 25 -j ACCEPT

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

iptables -A INPUT -p tcp -s 0.0.0.0/0 -d 192.1.2.11 --dport 80 -j ACCEPT

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

iptables -A INPUT -p tcp -s 192.1.2.0/24 -d 0.0.0.0/0 --dport 80 -j ACCEPT