UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

4-2-2026

MECANISMOS DEDEFENSA EN RED

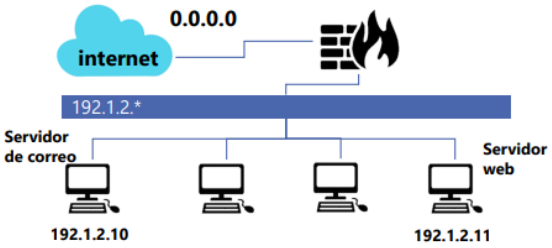
Hernández Fernández Diego Osvaldo – 182217

Mtro. Servando López Contreras

Diego Osvaldo Hernández Fernández
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

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.
2. Permitir el tráfico de conexiones ya establecidas.
3. Aceptar tráfico DNS (TCP) saliente de la red local.
4. Aceptar correo entrante proveniente de Internet en el servidor de correo.
5. Permitir correo saliente a Internet desde el servidor de correo.
6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.
7. Permitir tráfico HTTP desde la red local a Internet.

Requisición.	Comandos.
Política restrictiva	iptables -P INPUT DROP iptables -P FORWARD DROP iptables -P OUTPUT DROP
Trafico de conexiones ya establecidas	iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
Trafico DNS (TCP) saliente de la red local	iptables -A INPUT -p tcp -s 192.1.2.0/24 -d 0.0.0.0/0 --dport 22 -m state --state NEW -j ACCEPT
Correo entrante proveniente de internet	iptables -A INPUT -p tcp -s 0.0.0.0/0 -d 192.1.2.10 --dport 25 -m state --state NEW -j ACCEPT
Correo entrante saliente de internet	iptables -A INPUT -p tcp -s 192.1.2.10 -d 0.0.0.0/0 --dport 25 -m state --state NEW -j ACCEPT
Conexiones HTTP	iptables -A INPUT -p tcp -s 0.0.0.0/0 -d 192.1.2.11 --dport 80 -m state --state NEW -j ACCEPT
Red local	iptables -A INPUT -p tcp -s 192.1.2.0/24 -d 0.0.0.0/0 --dport 80 -m state --state NEW -j ACCEPT