

Act.03 - Interpretación y traducción de políticas de filtrado en iptables

- CNO V. Seguridad Informática

Nombre: Donald Lemón Gómez Alarcón
Fecha: 4 de febrero de 2026 Calf: A

1. Completa los espacios conforme se explica el flujo del paquete.

Cuando un paquete llega al sistema, primero pasa por una cadena, después por una tabla y finalmente se ejecuta una acción.

2. Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	filtrado de paquetes	bloquear puerto
NAT	traducción de direcciones	compartir internet
MANGLE	modificar paquetes	Medir calidad de servicio
RAW	realizar seguimiento de red	Ignorar paquetes
SECURITY	Analizar el propósito / servicio	Políticas

3. Anatomía de un comando iptables:

iptables -A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT

4. Este comando permite:

Acepta el comunicado TCP en frente por los puertos 80 y 443

5. Variables y opciones comunes

- a) Limitar intentos por minuto

--limit 5/min

- b) Filtrar por IP de origen

-s 192.168.1.10

- c) Ver solo números, sin DNS (ni resolución de puertos)

iptables -L -n

- d) Ver reglas con contadores (paquetes y bytes)

-L -v -c (contadores)

6. ¿Qué hace esta regla?

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 \ -m state --state NEW,ESTABLISHED -j ACCEPT

Permite el tráfico SSH, HTTP y HTTPS que entra y mantiene

conexiones establecidas

7. Permitir tráfico HTTP entrante

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

8. Permitir todo el tráfico saliente

iptables -A OUTPUT -j ACCEPT

9. Permitir SSH solo desde la IP 192.168.1.50

iptables -A INPUT -p tcp --dport 22 -s 192.168.1.50 -j ACCEPT

10. Permitir tráfico TCP entrante a puertos 80 y 443 solo si es conexión establecida o relacionada

iptables -A INPUT -p tcp -m multiport --dports 80,443 -m state --state ESTABLISHED,RELATED -j ACCEPT

11. Permitir tráfico TCP entrante por eth0 a 22, 80 y 443, registrar intentos y permitir solo NEW y ESTABLISHED

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443

-m state NEW,ESTABLISHED -j ACCEPT

7-con puerto 56

iptables -A INPUT -p tcp -m multiport --dports 56,80 -j ACCEPT

11) iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443
-m conntrack --ctstate NEW,ESTABLISHED -j LOG --log-prefix
"conexion mala" -j ACCEPT