

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

- CNO V. Seguridad Informática

Nombre: Karina Mendoza Aguado

Fecha: 03/02/2026

Calf: X

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

Cuando un paquete llega al sistema, primero pasa por una interfaz de red después por una regla de filtro finalmente se ejecuta una rutina.

2. Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de paquetes	Bloquear
NAT	Traducción de direcciones	Traducir
MANGLE	Modificación avanzada de Paquetes	Modificar
RAW	Excepciones al seguimiento de conexiones	Excepción
SECURITY	Aplicar etiquetas de seguridad	Aplicación

SELinux.

3. Anatomía de un comando iptables:

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

4. Este comando permite:

- Permite el tráfico TCP entrante hacia los puertos 80 y 443 para habilitar acceso web.

5. Variables y opciones comunes

- a) Limitar intentos por minuto

-- limit 5/min

- b) Filtrar por IP de origen

-s 192.168.1.0/24

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

-L -n

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

-L -v

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

- Creamos una regla para la tabla Filter, esta regla la añadimos al final.

- Definimos el paquete que pasará por la interfaz eth0

- Definimos el tipo de protocolo para TCP

- Definimos el servicio ssh y http / https

- Definimos que el estado de la conexión debe ser nueva y debe estar estable

- Aceptamos los paquetes en la interfaz.

7. Permitir tráfico HTTP entrante

iptables -A INPUT -p tcp -d 192.168.1.50 --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 -s 192.168.1.50 --dport 22 -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 conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

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

① iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m conntrack --ctstate NEW -j ACCEPT
LOG --log-prefix "Conexión nueva".

② iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT