

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

- CNO V. Seguridad Informática

Nombre: José Emmanuel López López 187078
Fecha: 03/02/2026 Calf: _____

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

Cuando un paquete llega al sistema, primero pasa por una tabla,
después por una cadena 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	Permitir tráfico
NAT	Traducción de direcciones	Redireccionamiento
MANGLE	Modificación de paquetes	Cambiar conexiones
RAW	Excepciones de paquetes	Paquetes que no deben inspeccionarse
SECURITY	Excepciones de paquetes	Excepciones

3. Anatomía de un comando iptables:

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

4. Este comando permite:

HTTPS / HTTP

5. Variables y opciones comunes

a) Limitar intentos por minuto

--limit 5/min

b) Filtrar por IP de origen

-s / --source

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

-n

d) Ver reglas con contadores (paquetes y bytes)

-L -V

6. ¿Que hace esta regla?

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

Permite tráfico TCP entrante por la interfaz eth0
a los puertos 22, 80, 443, siempre que sea parte de
una conexión nueva o establecida.

7. Permitir tráfico HTTP entrante

`iptables -A INPUT -p tcp --port 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 -p tcp --dport 22,80,443 -m state --state NEW,ESTABLISHED -j ACCEPT`

`-s 192.168.1.50 -j ACCEPT`