

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

- CNO V. Seguridad Informática

Nombre: José Emmanuel López López 187098
 Fecha: 03/02/2026 Calf: _____

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

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

- Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de paquetes	Rechazar tráfico
NAT	Traducción de direcciones	Redireccionamiento
MANGLE	Modificación de paquetes	Comprimir cabeceras
RAW	Excepciones al filtro principal	Paquetes que no deben inspeccionarse
SECURITY	Seguridad de conexión	Autorización

- Anatomía de un comando iptables:

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

- Este comando permite:

HTTPS / HTTP

- Variables y opciones comunes

- Limitar intentos por minuto

--limit s/mm

- Filtrar por IP de origen

-S / --source

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

-L -n

- Ver reglas con contadores (paquetes y bytes)

-L -v

- ¿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 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 --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 -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 -m multiport --dports 22,80,443 -m state --state NEW,ESTABLISHED -j LOG --log-prefix "REQUERIMIENTOS" -j ACCEPT

RELATED

-j ACCEPT