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

– CNO V. Seguridad Informática

Nombre: Josué Emiliano Rosales Ramírez

Fecha: 13/02/2026 Calf: 9

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 regla.

2. *Relaciona cada tabla con su propósito principal.*

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	filtrar paquetes	permitir tráfico
NAT	traducción de direcciones	asignación de IP's
MANGLE	modificación de paquetes	cambia cabeceras
RAW	seguimientos de paquetes y conexiones	auditoría
SECURITY	etiquetas de seguridad	aplica reglas a niveles de paquetes

3. *Anatomía de un comando iptables:*

iptables -A Input -p tcp -m multiport --dports 80,443 -j accept

4. *Este comando permite:*
Acepta el tráfico de los puertos 80 y 443

5. *Variables y opciones communes*

a) Limitar intentos por minuto

--limit

b) Filtrar por IP de origen

-s o -source

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

-list -n

d) Ver reglas con contadores (paquetes y bytes)

-list -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

Acepta el tráfico desde la interfaz de entrada de eth0 de los puertos 22, 80, 443, donde su estado de conexión es nueva o establecida

7. *Permitir tráfico HTTP entrante*

iptables -A Input -p tcp --dports 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 --dports 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 80,443 -m state Established,Related

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; JLOG --log-prefix "Intento: =