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

– CNO V. Seguridad Informática

Nombre: Juan Diego Aguilar Espinoza

Fecha: 4/02/2026 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 Rule/action.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrar trafico	Filtrar paquetes
NAT	Traducir direcciones	Cuando se conectan diferentes dispositivos a una red
MANGLE	Modificar paquetes	Poner marcas a los cabezales
RAW	Excepciones al seguimiento de paquetes	No inspecciona ciertos paquetes
SECURITY	Auditoria a los servicios	Permite o no un servicio

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*

Permitir trafico tcp a travez de los puertos de destino 80 y 443

5. *Variables y opciones communes*

Limitar intentos por minuto

-m –limit 5/min

a) Filtrar por IP de origen

-s 192.168.1.10

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

Iptables -L -n

c) Ver reglas con contadores (paquetes y bytes)

Iptables -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

Permitir trafico tcp entrante por la interfaz eth0 en los puertos 22,80,443 solo si el paquete pertenece a una conexión NEW o ESTABLISHED

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 -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 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*

REGISTRAR INTENTOS

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 \ -m state --state NEW -j LOG --log-prefix "INTENTO_TCP: "

``

PERMITIR CONEXIONES NEW Y ESTABLISHED

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