UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ — INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

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

– CNO V. Seguridad Informática

Nombre: Cavazos Zaraí, Gutiérrez Hernández, Marrueco Medina, Salazar Hernández
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 regla.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de paquetes	Permitir o bloquear tráfico
NAT	Traducción de direcciones	Port Forwarding
MANGLE	medir calidad de servicio de los paquetes	Paquetes que no deban ser inspeccionados
RAW	Excepciones al seguimiento de conexiones	Monitoreo de conexiones
SECURITY	realiza una auditoria que verifica la seguridad https	verificar la seguridad de una pagina web

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*

Para entrada de datos a varios puertos de destino (80, 443)

5. *Variables y opciones communes*

a) Limitar intentos por minuto

--limit

b) Filtrar por IP de origen

-s ó --source

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

-L -v

d) Ver reglas con contadores (paquetes y bytes)

-L -n

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 eth0 hacia los puertos 20, 80, 443, siempre que sea parte de una conexión nueva o establecida

7. *Permitir tráfico HTTP entrante*

iptable -A INPUT -p tcp --dport 80 -j ACCEPT

8. *Permitir todo el tráfico saliente*

iptable -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 --sports 80,443 -m state

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

--state ESTABLISHED, RELATED -j ACCEPT

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