UNIVERSIDAD POLITECNICA 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: Brian Salvador Espinoza Agustín 175031

Fecha: 04/02/2026 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/acción.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de Paquetes	bloquear conexiones SSH
NAT	traducción de direcciones IP	Port Forwarding
MANGLE	medir Calidad del Servicio	Cambiar cabeceras
RAW	Seguimiento de Paquetes	Paquetes no inspeccionados
SECURITY	marcas etiquetas de seguridad	Paquete autorizado por autoridad

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*

Define la tabla, cadena, el protocolo el parametro multiport permite analizar varios puertos estamos analizando los puertos de origen 80 y 443 y los acepta

5. *Variables y opciones commúnes*

a) Limitar intentos por minuto

--limit 5/minute

b) Filtrar por IP de origen

-s 192.168.25.0/24

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

-list -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 el trafico TCP entrante por interfaz eth0 a los puertos 22, 80 y 443, siempre que sea parte de una conexión nueva o establecida.

Puertos:
22 - SSH
80 - HTTP
443 - HTTPS

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 --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 -i eth0 -m multiport --dports 80, 22, 443 -m state --state NEW, ESTABLISHED. -j ACCEPT

11) iptables -A INPUT -p tcp -i eth0 -m multiport --dports