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: Elisa Alejandra Avellano Wratny

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 acción.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Firewall que filtra paquetes.	Bloquear tráfico.
NAT	Traducción de direcciones.	Conexión de diferentes dispositivos.
MANGLE	Marcar las cabeceras.	Cambiar las cabeceras.
RAW	Seguimiento a la conexión.	Realiza monitoreos.
SECURITY	Permitir el servicio de seguridad.	Permite el servicio.

3. *Anatomía de un comando iptables:*

iptables -A cadena -p tcp -m multiport --dports 80,443 -j acción

4. *Este comando permite:* Permite aplicar una acción a tráfico TCP dirigido a los puertos 80 y 443 en la cadena que se especifique.

5. *Variables y opciones communes*

a) Limitar intentos por minuto

--limit 5/minute

b) Filtrar por IP de origen

-s 192.168.1.0/24

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

-L -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 tráfico TCP entrante por la interfaz eth0 a los puertos 22, 80 y 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 -s 192.168.1.50 --dport 22 -m conntrack --ctstate NEW,
ESTABLISHED -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 conntrack --ctstate 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 -i eth0 -p tcp -m multiport --dports 22,
80,443 -m conntrack --ctstate NEW -j LOG --log-prefix
" INTENTO ENTRANTE TCP: "
```