



Nombre:

**Felipe Reyes**

Profesor:

**Mtro. Servando**

Tema:

**Interpretación y traducción de Políticas de  
filtrado en iptables**

**miércoles, 04 de Febrero de 2026**

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

## - CNO V. Seguridad Informática

Nombre: \_\_\_\_\_

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).
<b>FILTER</b>	Filtrado de paquetes	Administrar el tráfico de datos
<b>NAT</b>	Traducción de direcciones IP	Port forwarding
<b>MANGLE</b>	Modificación avanzada de paquete	Cambiar cabeceras
<b>RAW</b>	Excepciones al seguimiento de conexiones	Paquetes no inspeccionables
<b>SECURITY</b>	Aplicar etiquetas de seguridad	Seguridad adicional

3. Anatomía de un comando iptables:

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

4. Este comando permite:

Trafico TCP entrante por la interfaz eth0 a los puertos 22, 80

5. Variables y opciones comunes

a) Limitar intentos por minuto

--limit 5/minute

b) Filtrar por IP de origen

-s 0 --source -s 192.168.1.0/24

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

-t nat

d) Ver reglas con contadores (paquetes y bytes)

-i -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

Crea una nueva regla por la interfaz eth0, con el protocolo TCP. Donde  
pasarán los paquetes hacia los puertos 22 (SSH), 80 (HTTP) y 443 (HTTPS).  
Verifica si existe la conexión, sino la crea.

7. Permitir tráfico HTTP entrante

iptables -A input -p tcp --dport 80 -j Accept  
Filter cadena

8. Permitir todo el tráfico saliente

iptables -A out -p tcp -m multiports --dports 56,80 -j Accept

9. Permitir SSH solo desde la IP 192.168.1.50

iptables -A input -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 -i eth0 -p tcp -m multiports --dports 80,443 -m state --state New, established -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 multiports --dports 22,80,443 -m state --state New, established -j Accept