

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

## - CNO V. Seguridad Informática

Nombre: ERIK De la Rosa RodriguezFecha: 03 febrero 2025 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	bloquear
<b>NAT</b>	Traducción de direcciones	Redireccionar puertos
<b>MANGLE</b>	Modificación de paquetes	Modificar paquetes cambiando TTL
<b>RAW</b>	Excluir seguimiento de conexiones	Reducir carga en un servidor
<b>SECURITY</b>	Aplicar etiquetas SELinux	Control de acceso obligatorio

3. Anatomía de un comando iptables:

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

4. Este comando permite:

Permitir tráfico TCP entrante a los puertos 80 y 443  
HTTP HTTPS

5. Variables y opciones comunes

a) Limitar intentos por minuto

--limit slurp

b) Filtrar por IP de origen

-s

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

Se crea una regla al final de la tabla filter, en la cual  
permite el tráfico TCP entrante por la interfaz eth0  
a los servicios de SSH, HTTP, HTTPS.

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 ESTABLISHED,RELATED -j ACCEPT
```

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

Registro

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

Permitir

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

Acción

Regla

HTTP entrante

```
INPUT --dport 80
```

SSH entrante

```
INPUT --dport 22
```

Tráfico solo

```
OUTPUT
```

Filtrar IP origen

```
-s IP
```

Interfaz

```
-i eth0
```

Varios puertos

```
-m multiport --dports
```

Estado conexión

```
-m state --state
```

Permitir

```
-j ACCEPT
```

Registro

```
-j LOG
```