

3-2-2026

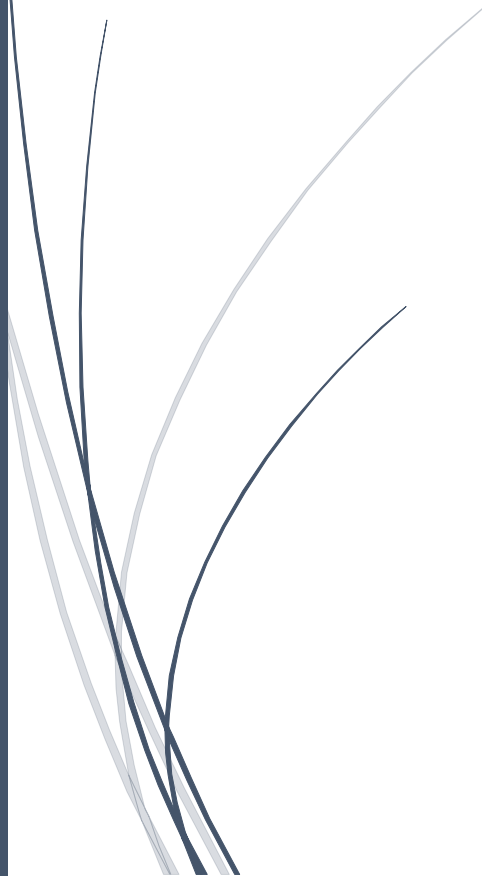
CNO V: Seguridad Informática

Hernández Fernández Diego Osvaldo
– 182217

Mtro. Servando López Contreras

ACTIVIDAD 03

Interpretación y traducción de
políticas de filtrado en iptables



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

- CNO V. Seguridad Informática

Nombre: Diego Osvaldo Hernández Hernández - 182217Fecha: 03/10/2026 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 CHAIN y finalmente se ejecuta una RULES/ACTION

2. Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta)
FILTER	Filtrado de Paquetes	Permite o bloquea el paso de tráfico.
NAT	Traducción de Direcciones	Los IP Privados se convierten por Symmetric (Público, externo)
MANGLE	Modificación de Paquetes	Cambio Cabeceras
RAW	Excepciones al sistema de firewall	Paquetes que no necesitan inspección → Mangle
SECURITY	Definición de Servicios	Servicios que no necesitan inspección para algunos puertos → Mangle

3. Anatomía de un comando iptables:
iptables -A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT

4. Este comando permite:

5. Variables y opciones comunes

- a) Limitar intentos por minuto

--limit --limit 5/minute

- b) Filtrar por IP de origen

--source --source 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)

iptables -L -v -n --line

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

-A INPUT: Añade la regla a la cadena de entrada

-i eth0: Especifica que el paquete debe entrar obligatoriamente por conexión eth0

-p tcp: Solo protocolo TCP

-m multiport --dports 22,80,443: Múltiple para agrupar varios puertos en una sola regla (http, https, etc.).

-j Accept: Adecuado acepto.

-m state --state NEW, ESTABLISHED: Solo permite paquetes que están iniciando una conexión nueva o tienen puertos de una sesión legítima previamente aceptada.

Basamente permite tráfico de red de entrada en conexiones específicas = D

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

Conexión del L2

```
iptables -A INPUT -i eth0 -p tcp
```

Conexión del 9

```
-> iptables -A INPUT -p tcp --dport 22 -s 192.168.1.50 -j Accept
```

Limpiar el orden de las tablas.

Linku -> iptables

-j -> Antes de la conexión de los puertos.