# ACTIVIDAD 03

Interpretación y traducción de políticas de filtrado en iptable

3 DE FEBRERO DE 2026

UPSLP

CNO V Seguridad Informática

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

**– CNO V. Seguridad Informática**

Nombre: David Zárate Domínguez

Fecha: 03/02/2025 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 accion/regla

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

| Tabla | Propósito principal | Ejemplo de uso (01 palabra o frase corta). |
|---|---|---|
| **FILTER** | filtrado de paquetes (ej. Firewall) | permitir o bloquear trafico |
| **NAT** | traduccion de direcciones | hacer NAT o port forwarding |
| **MANGLE** | modificacion avanzada de paquetes | Cambiar cabeceras |
| **RAW** | excepciones al seguimiento de conexiones | paquetes que no deberian ser inspeccionados |
| **SECURITY** | aplicar etiquetas de seguridad SELinux | contextos de seguridad adicionales |

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*
Permite el trafico entrante a traves del protocolo TCP hacia los puertos de destino 80 (HTTP) y 443 (HTTPS)
5. *Variables y opciones communes*

***a) Limitar intentos por minuto***

--limit

***b) Filtrar por IP de origen***

-s o --source

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

iptables -L -n

***d) Ver reglas con contadores (paquetes y bytes)***

iptables -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 trafico TCP entrante por la interfaz eth0 a los puertos 22, 80 y 443, siempre que sea parte de una conexion nueva o establecida

7. *Permitir tráfico HTTP entrante*
   iptables -A INPUT -p tcp --dport 80 -j ACCEPT

8. *Permitir todo el tráfico saliente*
   iptables -P OUTPUT 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*
    iptable -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*
    1. iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -j LOG --log-prefix "Intento_Entrada:"
    2. iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state NEW,ESTABLISHED -j ACCEPT