

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

### - CNO V. Seguridad Informática

Nombre: Jorge Emmanuel Lopez Monsivais

Fecha: 03/02/26

Calf: \_\_\_\_\_

- 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.

- Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de Paquete	Bloquear el tráfico
NAT	Traducción de direcciones	Hacer port forwarding
MANGLE	Modificación avanzada de paq	Cambiar cabeceras
RAW	Excepciones al seg de conex	Paquetes que no deben inspeccionarse
SECURITY	Aplicar etiquetas de seguridad	Contextos de seg adicionales

- Anatomía de un comando iptables:

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

- Este comando permite:

permitir protocolos HTTP/HTTPS

- Variables y opciones comunes

- Limitar intentos por minuto

--limit 5/minute

- Filtrar por IP de origen

-s ó --source 192.168.0.1/24

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

-L -n

- Ver reglas con contadores (paquetes y bytes)

-L -v

- ¿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 el tráfico entrante por la interfaz eth0 a los puertos 22, 80 y 443, mientras sea parte de una conexión nueva

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

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