

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

#### - CNO V. Seguridad Informática

Nombre: Castillo Olvera Carlos René

Fecha: 03 de Febrero del 2026

Calf: A

- 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 Regla/Action

- Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de paquetes	Permitir o bloquear tráfico
NAT	Traducción de direcciones	Hacer NAT o port forwarding
MANGLE	Modificación avanzada de paquetes	Cambiar cabeceras
RAW	Excepciones al seguimiento de conexiones	Paquetes que no deben ser inspeccionados
SECURITY	Aplica etiquetas de seguridad	Contextos de seguridad adicionales SELinux

- Anatomía de un comando iptables:

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

- Este comando permite:

Permite protocolos: HTTP / HTTPS

- Variables y opciones comunes

a) Limitar intentos por minuto

--limit 5/m

b) Filtrar por IP de origen

-s ó --source

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

-n ó --numeric

d) 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 TCP entrante al sistema por eth0 con dirección al puerto 22 (SSH), 80 (HTTP) y 443 (HTTPS) sólo si el paquete pertenece a una conexión nueva o ya establecida.

7. Permitir tráfico HTTP entrante

ip tables -A INPUT -p tcp -d port 80 -m state --state NEW, ESTABLISHED -j ACCEPT

8. Permitir todo el tráfico saliente

ip tables -A OUTPUT -j ACCEPT

9. Permitir SSH solo desde la IP 192.168.1.50

ip tables -A INPUT -p tcp -s 192.168.1.50 -d port 22 -m state --state NEW, ESTABLISHED -j ACCEPT

10. Permitir tráfico TCP entrante a puertos 80 y 443 solo si es conexión establecida o relacionada

ip tables -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

ip tables -A INPUT -i eth0 -p tcp -m multiport --dports 22, 80, 443 -m state --state NEW -j LOG --log-prefix