

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

## - CNO V. Seguridad Informática

Nombre: América Fabiola Guerra Ramírez - 179884  
Fecha: 3 de febrero de 2020 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 regla.

2. Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrar paquetes	Bloquear puertos <del>tráfico</del>
NAT	Traducción de direcciones	Compartir internet
MANGLE	Modificar paquetes	Cambiar cabeceras
RAW	Excepción al seguimiento	Paquetes no inspeccionados
SECURITY	Aplicar políticas de seguridad	Seguridad adicional

3. Anatomía de un comando iptables:

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

4. Este comando permite:

El tráfico TCP hacia los puertos 80 y 443

5. Variables y opciones comunes

a) Limitar intentos por minuto

-- limit 5/minute

b) Filtrar por IP de origen

-s 192.168.1.0/32

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 el tráfico TCP entrante por la interfaz eth0 hacia los puertos 22, 80, 443, siempre y cuando sea nueva y este establecida

7. Permitir tráfico HTTP entrante

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

↓            ↓  
FILTER      CADENA

↓  
REGLA

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 --dport 22 -s 192.168.1.50 -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 LOG  
--log-prefix "Conexion Nueva:" -j ACCEPT