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

– CNO V. Seguridad Informática

Nombre: Estefano Alessandro Rodríguez Morin - 178584

Fecha: 03/02/2026 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 cadena y finalmente se ejecuta una regla o acción

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	permite o bloquea tráfico	Bloquear conexiones
NAT	Port forwarding	hosting web
MANGLE	Manejo de paquetes	Calidad de Servicio
RAW	Seguimiento de paquetes	Verificación de ruta
SECURITY	Marcado de etiquetas de Segu	Proceso/Servicio autorizado

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*

Crear una regla para la tabla FILTER al final de la cadena que llega por protocolo tcp con puertos de destino 80 y 443, y los acepta

5. *Variables y opciones comunes*

a) Limitar intentos por minuto

--limit 5/minute

b) Filtrar por IP de origen

-s 192.168.25.0/24

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

-L -n

d) Ver reglas con contadores (paquetes y bytes)

-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

Se crea una regla para la tabla FILTER al final de la cadena, Se define que el paquete debe pasar por la interfaz eth0, que lleguen por el protocolo tcp, después se definen los puertos SSH, http y https, se define que debe ser parte de una conexión nueva o establecida y se deben aceptar los paquetes

7. *Permitir tráfico HTTP entrante*

```
iptables -A INPUT --dports 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 --dports 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 80,443 -s \
--State NEW,ESTABLISHED -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 -m multiport 22,80,443 \
-j LOG --log-prefix "Intento"
iptables -A INPUT -i eth0 -p tcp -m multiport --dports \
22,80,443 -s --state NEW,ESTABLISHED -j ACCEPT
```