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

– CNO V. Seguridad Informática

Nombre: Juan Alejandro Pérez Ventura

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 acción.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Permite / bloquea tráfico	Bloquear conexiones SSH
NAT	Modifica IPs y/o puertos	Compartir internet
MANGLE	Modifica paquetes avanzados	Cambio de cabeceras
RAW	Excepciones del seguimiento conex.	Desactivar conntrack
SECURITY	Aplicar etiquetas de seguridad	Contextos de seguridad

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 que va entrando al equipo.

5. *Variables y opciones communes*

a) Limitar intentos por minuto

--limit

b) Filtrar por IP de origen

-S

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

-n

d) Ver reglas con contadores (paquetes y bytes)

-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 también el tráfico TCP entrante por eth0 en los ports 22, 80 y 443, sólo si ya fue establecido.

7. *Permitir tráfico HTTP entrante*

```
iptables -A INPUT -p tcp --dport 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 --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 22,80,43 \ -m conntrack
```

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 22,80,43 \
-m conntrack --ctstate NEW,ESTABLISHED \
-j LOG --log-prefix "Firewall: "
--ctstate ESTABLISHED,RELATED -j ACCEPT
```