UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

3-2-2026

CNO V: Seguridad Informática

Hernández Fernández Diego Osvaldo – 182217

Mtro. Servando López Contreras

ACTIVIDAD 03

Interpretación y traducción de políticas de filtrado en iptables

UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSÍ — INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

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

– CNO V. Seguridad Informática

Nombre: Diego Osvaldo Hernández Fernández - 182217 Calif: _____

Fecha: 03/02/2026

1. *Completa los espacios conforme se explica el flujo del paquete.*

Cuando un paquete llega al sistema, primero pasa por una TABLE después por una CHAIN y finalmente se ejecuta una RULES/ACTION

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de Paquetes	Permite o bloquea el paso de los paq.
NAT	Traducción de Direcciones	Uso IP Públicas se divide por segmento (Casa, carro)
MANGLE	Modificación de Paquetes	Cambiar Cabeceras → Marcar PT
RAW	Excepciones al seguimiento de conexiones	Paquetes que no necesitan procesamiento
SECURITY	Auditorías de Seguridad	Servidor web muy importante para asegurar estos puertos

3. *Anatomía de un comando iptables:*

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

- -A: Sistema debe agregar o añadir
- INPUT: La regla se aplicara a los paquetes entrantes
- -p tcp: Paquetes que utilicen el protocolo TCP
- -m multiport: Multiples puertos en una sola linea
- --dports: Puertos destino
- -j Accept: Aceptar

4. *Este comando permite:*

Que el servidor reciba tráfico de red de forma segura y abierta

5. *Variables y opciones communes*

a) Limitar intentos por minuto

--limit → --limit 5/minute

b) Filtrar por IP de origen

-s 0' --source → -s 192.168.1.0/24

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

-L -n

d) Ver reglas con contadores (paquetes y bytes)

iptables -L -v -n --line-

- -m state --state NEW, ESTABLISHED: Solo permite paquetes que estan iniciando una conexion nueva o forma parte de una sesion legitima previamente aceptada
- -j Accept: El firewall acepta.

-A INPUT
-j
-p
-m
--dports
ACCEPT

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
```

- -A INPUT: Añade la regla a la cadena de entrada
- -i eth0: Especifica que el paquete debe entrar obligatoriamente por la interfaz eth0
- -p tcp: Solo protocolo TCP
- -m multiport --dports 22,80,443: Modulo para agrupar varios puertos en una sola regla (http, https, etc).

Básicamente permite tráfico de red de entrada en puertos específicos =D

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 -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

Conexión del LL
iptables -L INPUT -i eth0 -p tcp

Conexión del 9
-> iptables -L INPUT -p tcp --dport 22 -s 192.168.1.50 -j ACCEPT

Limpieza de reglas de las tablas.

Filter -> iptables
-j -> Acción de la cadena