ACTIVIDAD 03 – INTERPRETACIÓN Y TRADUCCIÓN DE POLÍTICAS DE FILTRADO EN IPTABLES

CNO V: Seguridad Informática

Alonso Castillo Omar Karim 179033
Mtro. Servando López Contreras

Primer Parcial
Universidad Politécnica de San Luis Potosí

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

– CNO V. Seguridad Informática

Nombre: Alonso Castillo Omar Kevin 179033

Fecha: 04/02/26 Calf: 8

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/Acción

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Permitir o bloquear tráfico	Firewall
NAT	Traducción de direcciones IP	Port forwarding
MANGLE	Modificación de paquetes	Cambiar cabeceras
RAW	Excepciones al seguimiento de conexiones	Paquetes que no deben ser inspeccionados
SECURITY	Aplicar etiquetas de seguridad SELinux	Contexto de seguridad adicionales

3. *Anatomía de un comando iptables:*

iptables -A CADENA -p tcp -m match module --dports 80,443 -j ACCION

4. *Este comando permite:* Tráfico web seguro hacia un servidor HTTP, HTTPS

5. *Variables y opciones communes*

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

Permite tráfico TCP entrante por la interfaz eth0 a los puertos 22, 80 y 443, siempre que sean parte de una conexión nueva o establecida

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 conntrack --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 conntrack --ctstate NEW, ESTABLISHED -j ACCEPT