

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

- CNO V. Seguridad Informática

Nombre: EVAN De la Rosa Rodriguez
 Fecha: 03 febrero 2025 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	Filtrado de paquetes	bloquear
NAT	Traducción de direcciones	Redireccionamiento
MANGLE	Modificación de paquetes	Paquetes scramblist TTL
RAW	Excluir seguimiento de conexiones	Verificar virus en un servidor
SECURITY	API para el firewall SELinux	Control de acceso obligatorio

3. Anatomía de un comando iptables:

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

4. Este comando permite:

Permitir tráfico TCP entrante a los puertos 80 y 443
 WWW HTTPS

5. Variables y opciones comunes

- a) Limitar intentos por minuto

--limit s/min

- b) Filtrar por IP de origen

-S

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

-L -n

- d) Ver reglas con contadores (paquetes y bytes)

-L -v

6. ¿Qué hace esta regla?

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 \ -m state --state NEW,ESTABLISHED -j ACCEPT

S Crea una regla al final de la tabla Filter en la cual Permite el tráfico TCP entrante por la interfaz eth0 a los servicios de SSH, HTTPS, HTTPS

a los servicios de SSH, HTTPS, HTTPS,

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 ESTABLISHED RELATED -j ACCEPT

11. Permitir tráfico TCP entrante por eth0 a 22, 80 y 443, registrar intentos y permitir solo NEW y ESTABLISHED

Regristro

IPtables -A INPUT -i eth0 -P tcp -m multiport --dports 22, 80, 443 -m state --state NEW -j LOG

Permitir

IPtables -A INPUT -i eth0 -P tcp -m multiport --dports 22, 80, 443 -m state --state NEW, ESTABLISHED -j ACCEPT

Acción

Regla

HTTP entrante

INPUT --dport 80

SSH entrante

INPUT --dport 22

Trafico solo

OUTPUT

Fijar IP origen

-s IP

Interface

-i eth0

Varios Puertos

-m multiport --dports

Estado conexión

-m state --state

Permitir

-j ACCEPT

Regristro

-j LOG