

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

- CNO V. Seguridad Informática

Nombre: Cavazos Zagal, Guadalupe Hernández, Morquecho Medina, Salazar Hernández

Fecha: 03/02/2024 Calif: _____

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.

2. Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de paquetes	Permitir o denegar tráfico
NAT	Traducción de direcciones	Port forwarding
MANGLE	Modificar paquetes	Paquetes que no deben ser inspeccionados
RAW	Excepciones al seguimiento de conexiones	Monitoreo de conexiones
SECURITY	Realiza una auditoría que verifica la seguridad https	Verificar la seguridad de una página web

3. Anatomía de un comando iptables:

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

4. Este comando permite:

Diferencia de puertos a varios puertos de destino (80, 443)

5. Variables y opciones comunes

a) Limitar intentos por minuto

- limit

b) Filtrar por IP de origen

-s ó --source

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

-L -v

d) Ver reglas con contadores (paquetes y bytes)

-L -n

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 eth0

7. Permitir tráfico HTTP entrante
iptables -A INPUT -p tcp --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 --source 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 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 LOG --log-prefix

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