IPTABLES

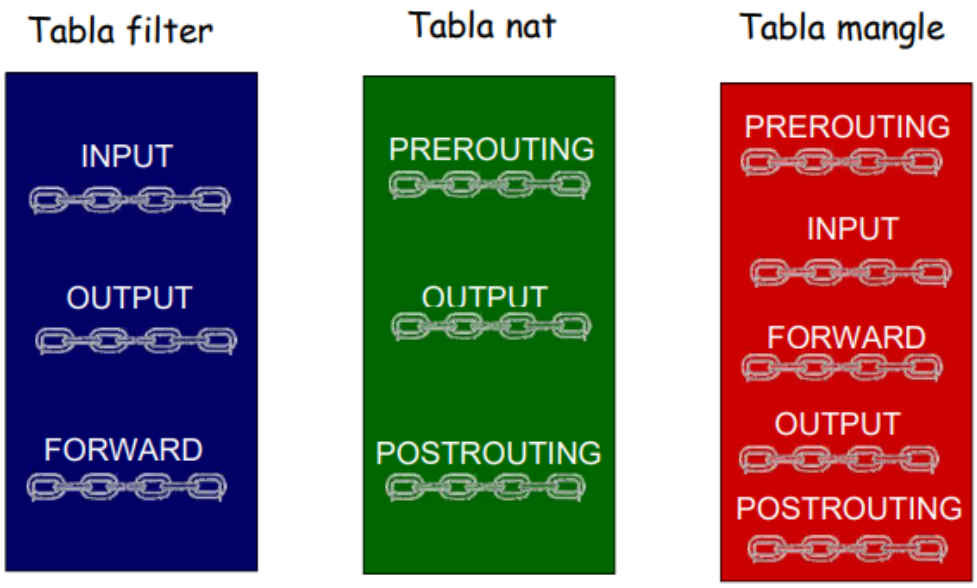
QUE SON?

- Es una herramienta avanzada de filtrado de paquetes en Linux
- Iptables gestiona, mantiene e inspecciona las reglas de filtrado de paquetes IPv4 a través de tabla

FUNCIONES DE IPTABLES

- Implementar un cortafuegos
- Configurar un dispositivo de nat
- Marca y modifica los paquetes.

TABLAS DE IPTABLES



CONSTRUCCION DE UNA REGLA

EJEMPLOS

Solo se desea que la dirección 10.10.23.17 puede

acceder a la página de la compañía

Dos formas de hacerlo

– Depende del resto de las reglas en el servidor web

• Negamos todo y solo permitimos el paso a la IP deseada

• Aceptamos todo y no permitimos el paso a la IP deseas

iptables -P INPUT DROP

iptables -A INPUT -s 10.10.10.23.17 -p tcp --dport 80 -j ACCEPT

#

iptables -P INPUT ACCEPT

iptables -A INPUT -s ! 10.10.10.23.17 -p tcp --dport 80 -j DROP

Solo se desea el acceso a Google

iptables -A OUTPUT -p tcp –dport 443 -j ACCEPT

iptables -A INPUT -p tcp --sport 443 -j ACCEPT

iptables -A OUTPUT -p udp --dport 53 -j ACCEPT

iptables -A INTPUT -p udp --sport 53 -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

ping 8.8.8.8

Ahora podemos ir metiendo las reglas para cada servidor

Como serán paquetes con destino a otras máquinas se aplica FORWARD

Servidor WEB 211.34.149.2

 # Acceso a puerto 80

iptables −A FORWARD −d 211.34.149.2 −p tcp −−dport 80 −j ACCEPT