Sintaxis general:

La sintaxis para cualquier comando de IPTABLES es la siguiente:

iptables -t ***<tabla>*** *-****<comando>*** ***<cadena>*** ***{opciones}*** *-j* ***<acción>***

Tablas:

Hay 3 tablas (o cadenas), que indican qué tipo de operación puede hacer el router con los paquetes.

- **FILTER: En esta tabla hay reglas que dicen qué hacer con los paquetes, pero sin modificarlos. Esta es la tabla por defecto, si no se indica otra.**
- **NAT**: Implica a los paquetes que requieren crear nuevas conexiones. Normalmente implica algún tipo de traducción de dirección, ya sea dirección o puerto **(modifican el paquete).**
- **MANGLE: Implica modificaciones más sofisticadas del paquete, que van más allá de su dirección. Utilizada para realizar marcas de tráfico.**

Comandos: *(Los comandos son todos en mayúsculas)*

A: Agrega una regla.
D: Borra una regla de una cadena.
F: Vacía una cadena (borra todas las reglas).
L: Lista todas las reglas.
P: Permite definir la política por defecto a aplicar.

Cadena:

Cadena	**Paquetes analizados**	**Tabla donde se utiliza**
INPUT	Paquetes entrantes que están destinados a la PC donde está operando el iptables.	FILTER , MANGLE
OUTPUT	Paquetes en el momento de ser recibidos por la estación donde está operando el iptables. Esta cadena analiza paquetes propios y enrutados.	FILTER, MANGLE, NAT
FORWARD	Paquetes que son enrutados por la PC donde está operando iptables.	FILTER, MANGLE
PREROUTING	Paquetes en el momento de ser recibidos por la estación donde está operando el iptables. Esta cadena analiza paquetes propios y enrutados.	NAT, MANGLE
POSTROUTING	Paquetes en el momentos de ser enviados por la estación donde está operando el iptables. Esta cadena analiza los paquetes propios y enrutados.	NAT, MANGLE

Opciones:

Opciones	**Resultado**
-i <ethX>	Permite especificar la interface entrante. Donde ethX debe reemplazarse por la interfaz correspondiente (eth0, eth1, eth2, etc)
-o <ethX>	Permite especificar la interface saliente.
-s <X.X.X.X/Y>	Permite especificar la dirección IP origen. Donde X.X.X.X simboliza la IP y /Y simboliza la máscara de red.
-d <X.X.X.X/Y>	Permite especificar la dirección IP destino. Donde X.X.X.X simboliza la IP y /Y simboliza la máscara de red.
-p	Permite especificar el protocolo [tcp, udp, icmp, etc].
Para protocolos TCP y UDP	
-sport	Permite especificar el puerto de origen. Para especificar un rango válido de puertos, separe ambos números del rango con dos puntos (:)
-dport	Permite especificar el puerto de destino. Para especificar un rango válido de puertos, separe ambos números del rango con dos puntos (:)
Para TCP	
--syn	Se aplica a todos los paquetes TCP diseñados para iniciar una comunicación, comúnmente llamados *paquetes SYN*. Cualquier paquete que lleve datos no se toca. Use un signo de exclamación (**!**) después de **--syn** para que seleccione los paquetes no-SYN.
--tcp-flags <tested flag list> <set flag list>	Permite paquetes TCP que tengan ciertos bits (banderas) específicos puestos, para que coincidan con la regla. La opción de correspondencia **--tcp-flags** acepta dos parámetros. El primero es la máscara; una lista separada por comas de las marcas a ser examinadas en el paquete. El segundo parámetro es una lista separada por comas de las marcas que deben ser definidas en la regla con la que se pretende concordar. Por ejemplo, una regla **iptables** que contenga las siguientes especificaciones solo se corresponderá con paquetes TCP que tengan definida la marca SYN, y que no tengan definidas las marcas ACK ni FIN: **--tcp-flags ACK,FIN,SYN SYN** Use el signo de exclamación (**!**) después de **--tcp-flags** para revertir el efecto de coincidencia de la opción.
Para ICMP	
--icmp-type	Establece el nombre y número del tipo de ICMP a corresponderse con la regla. Puede obtenerse una lista de nombres ICMP válidos al ingresar el comando **iptables -p icmp -h**.

Opciones de módulos:

Utilización de modulos	
-m <*module-name*>	Donde <*module-name*> es el nombre del módulo de comparación. Algunos módulos válidos son : Módulo **limit** — Pone límites sobre cuántos paquetes se toman para una regla particular. Módulo **state** — Habilita el chequeo del estado de la conexión.
Módulo limit	
--limit	Establece la cantidad máxima posible de correspondencias en un period de tiempo determinado, especificado como un par ***<value>/<period>***. Por ejemplo, utilizar **--limit 5/hour** permite 5 correspondencias con la regla a cada hora Los períodos se pueden especificar en segundos, minutos, horas o días. Si no se utiliza un número o modificador de tiempo, se asume el valor predeterminado de **3/hora**.
--limit-burst	Pone un límite en el número de paquetes que pueden coincidir con la regla en cada momento. Esta opción se especifica como un entero y no se debe usar junto con la opción **--limit**. Si no se especifica un valor, el valor predeterminado cinco (5) es asumido.
Módulo state	
--state	Chequea a un paquete con los siguientes estados de conexión: o **ESTABLISHED** — El paquete está asociado a otros paquetes en una conexión establecida. Necesita aceptar este estado si quiere mantener una conexión entre un cliente y un servidor o **INVALID** — El paquete es chequeado no está asociado a una conexión conocida. o **NEW** — El paquete chequeado es para crear una conexión nueva o es parte de una conexión de doble vía que no fue vista previamente. Necesita aceptar este estado si quiere permitir conexiones nuevas a un servicio. o **RELATED** — El paquete coincidente está iniciando una conexión relacionada de alguna manera a otra existente. Un ejemplo de esto es FTP, que usa una conexión para el control del tráfico (puerto 21) y una conexión separada para la transferencia de datos (puerto 20). Estos estados de conexión pueden ser utilizados combinados con otros, si se los separa con comas, como por ejemplo **-m state --state INVALID,NEW**

Acciones:

Acción	Resultado	Tabla donde se utiliza	Cadena donde se utiliza
DROP	Descarta el paquete que coincide con las opciones.	FILTER	INPUT OUTPUT FORWARD
ACCEPT	Acepta el paquete que coincide con las opciones.	FILTER	INPUT OUTPUT FORWARD
REJECT	Descarta el paquete que coincide con las opciones, enviando un mensaje ICMP al origen notificando el descarte.	FILTER	INPUT OUTPUT FORWARD
SNAT --to-source x.x.x.x	Modifica la dirección de origen del paquete por la especificada en X.X.X.X	NAT	POSTROUTING
DNAT --to-destination x.x.x.x	Modifica la dirección de destino del paquete por la especificada en X.X.X.X	NAT	PREROUTING
MASQUERADE	Modifica la dirección de origen del paquete por la que tenga asignada la interfaz saliente	NAT	POSTROUTING