

== Firewall IPTABLES ==

Ejecución

es necesario ser administrador: sudo iptables ...

Opciones de visualización

iptables -L (ver listado de reglas)

iptables -L -t filter (tabla filter) // -t nat

iptables -L INPUT (sólo reglas INPUT) // FORWARD, OUTPUT

iptables -n -L (visualización numérica) // -nL

iptables -L --line-numbers (numerar las reglas)

Política por defecto

iptables -P INPUT DROP

Acciones sobre iptables

service iptables start/stop/restart/save/status

Añadir regla

iptables -A OUTPUT -p tcp -j ACCEPT

-s ip (origen)

-s ip/mask

-d ip (destino)

-d ip/mask

-p protocolo (tcp,udp,icmp,all...)

--sport puerto (puerto de origen)

--dport puerto (puerto de destino)

-i interfaz (tarjeta de red de entrada)

-o interfaz (tarjeta de red de salida)

-M mac

-j acción (ACCEPT-aceptar/DROP-denegar)

iptables -A INPUT -s 224.220.0.0/16 -d 10.6.0.0/16 -p udp -i eth0 -j DROP

iptables -A INPUT -sport 21 -dport 21 -j DROP

Insertar regla

iptables -I OUTPUT posición regla

iptables -I OUTPUT 2 -s 10.13.0.0/16 -j DROP

Borrar regla

iptables -D cadena posición

iptables -D FORWARD 3

iptables -F (eliminar todas las reglas)