Iptables Cheat-Sheet Actualizado

Iptables es una herramienta de nivel kernel en Linux que permite aplicar reglas de filtrado de paquetes y otras manipulaciones para fortalecer la seguridad de red.

Ver Reglas Actuales

Vertodas las reglas con detalles:

iptables -L -v

Ver reglas de la cadena INPUT con numeración:

iptables -L INPUT -nv --line-numbers

Bloquear Direcciones IP

Bloquearuna IP específica:

sudo iptables -I INPUT -s 201.128.33.200 -j DROP

Bloquear un rango de IPs:

sudo iptables -I INPUT -s 201.128.33.0/24 -j DROP

Desbloquear una IP:

sudo iptables -D INPUT -s 201.128.33.200 -j DROP

Bloquear Puertos

Bloquear puerto 25(TCP y UDP):

sudo iptables -A INPUT -p tcp --dport 25 -j DROP

sudo iptables -A INPUT -p udp --dport 25 -j DROP

Desbloquear puerto 25:

sudo iptables -A INPUT -p tcp --dport 25 -j ACCEPT

sudo iptables -A INPUT -p udp --dport 25 -j ACCEPT

Abrir Puerto a IP Específica

Ejemplo: permitir acceso MySQLdesde 1.2.3.4: sudo iptables -I INPUT -i eth0 -s 1.2.3.4 -p tcp --

dport 3306 -j ACCEPT -m comment --comment "MySQL Access By IP"

Abrir puerto para todas las IPs:

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

Eliminar Reglas

Ver reglascon número de línea: sudo

iptables -L INPUT -n --line-numbers **Eliminar**

por número: sudo iptables -D INPUT

[numero_de_regla]

Políticas por Defecto (DEFAULT POLICY)

Políticas de denegación por defecto:

sudo iptables -P INPUT DROP sudo iptables -P OUTPUT DROP

sudo iptables -P FORWARD DROP

Permitir interfaz local (loopback):

sudo iptables -A INPUT -i lo -j ACCEPT

sudo iptables -A OUTPUT -o lo -j ACCEPT

Loguear paquetes denegados:

sudo iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables-INPUT denied: " --log-level 7

sudo iptables -A OUTPUT -m limit --limit 5/min -j LOG --log-prefix "iptables-OUTPUT denied: " --log-level 7

Permitir Ping y Traceroute

Permitir salida de ping y respuesta: sudo iptables -A OUTPUT -p icmp --icmp-type 8 -m state state

NEW,ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A INPUT -p icmp --icmp-type 0 -m state --state ESTABLISHED,RELATED -j ACCEPT

Permitir TTL excedido (traceroute):

sudo iptables -A INPUT -p icmp --icmp-type 11 -m state --state ESTABLISHED,RELATED -j ACCEPT

Permitir Tráfico Web y DNS

HTTP/HTTPS:

sudo iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p tcp -m multiport --sports 80,443 -m state --state ESTABLISHED -j ACCEPT

DNS y NTP:

sudo iptables -A OUTPUT -p udp -m multiport --dports 53,123 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p udp -m multiport --sports 53,123 -m state --state ESTABLISHED -j ACCEPT

Guardar Reglas (Persistencia)

Guardar reglas manualmente:

sudo iptables-save > /etc/iptables/rules.v4

Usar iptables-persistent (Ubuntu/Debian):

sudo apt install iptables-persistent

sudo netfilter-persistent save

Extras

Limpiar todas las reglas:

sudo iptables -F

Ver reglas NAT:

sudo iptables -t nat -L -n -v

Reiniciar iptables (si es necesario):

sudo systemctl restart netfilter-persistent

Actualizado a julio de 2025

https://www.linkedin.com/in/imane-l