Iptables Cheatsheet

By Dejan Panovski • Updated on Feb 9, 2026 • Download PDF

Quick reference for common iptables firewall commands

Iptables is the classic Linux firewall tool for filtering, NAT, and packet mangling. This cheatsheet covers the most common commands for inspecting rules, allowing or blocking traffic, port forwarding, and managing persistence.

View Rules

Inspect current firewall rules.

`sudo iptables -L`	List rules
`sudo iptables -L -n`	List without resolving names
`sudo iptables -L -v`	Verbose output
`sudo iptables -L -n --line-numbers`	Show rule numbers
`sudo iptables -S`	Show rules as commands
`sudo iptables -t nat -L -n -v`	View NAT rules

Default Policies

Set default policies for chains.

`sudo iptables -P INPUT DROP`	Default drop inbound
`sudo iptables -P FORWARD DROP`	Default drop forwarding
`sudo iptables -P OUTPUT ACCEPT`	Default allow outbound

Allow Traffic

Allow common inbound traffic.

`sudo iptables -A INPUT -i lo -j ACCEPT`	Allow loopback
`sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`	Allow established
`sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT`	Allow SSH
`sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT`	Allow HTTP
`sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT`	Allow HTTPS
`sudo iptables -A INPUT -p icmp -j ACCEPT`	Allow ping
`sudo iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT`	Allow subnet

Block Traffic

Drop or reject traffic.

`sudo iptables -A INPUT -s 203.0.113.10 -j DROP`	Drop IP address
`sudo iptables -A INPUT -s 203.0.113.0/24 -j DROP`	Drop subnet
`sudo iptables -A INPUT -p tcp --dport 23 -j DROP`	Block Telnet
`sudo iptables -A INPUT -p tcp --dport 25 -j REJECT`	Reject SMTP
`sudo iptables -A INPUT -m mac --mac-source XX:XX:XX:XX:XX:XX -j DROP`	Block MAC address

Port Forwarding (DNAT)

Redirect traffic to a different host or port.

`sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.1.10:80`	Forward port to host
`sudo iptables -t nat -A PREROUTING -p tcp --dport 8080 -j REDIRECT --to-port 80`	Redirect local port
`sudo iptables -A FORWARD -p tcp -d 192.168.1.10 --dport 80 -j ACCEPT`	Allow forwarded traffic

NAT (Masquerade)

Enable NAT for outbound traffic.

`sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`	NAT for interface
`sudo iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j SNAT --to-source 203.0.113.1`	Static NAT
`sudo sysctl -w net.ipv4.ip_forward=1`	Enable IP forwarding

Rate Limiting

Limit connection rates to prevent abuse.

`sudo iptables -A INPUT -p tcp --dport 22 -m limit --limit 3/min --limit-burst 3 -j ACCEPT`	Limit SSH attempts
`sudo iptables -A INPUT -p tcp --dport 80 -m connlimit --connlimit-above 50 -j DROP`	Limit connections per IP
`sudo iptables -A INPUT -p icmp -m limit --limit 1/sec -j ACCEPT`	Limit ping rate

Logging

Log matched packets for debugging.

`sudo iptables -A INPUT -j LOG --log-prefix "IPT-DROP: "`	Log dropped packets
`sudo iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "SSH: " --log-level 4`	Log SSH access
`sudo iptables -A INPUT -m limit --limit 5/min -j LOG`	Log with rate limit

Delete and Insert Rules

Manage rule order and removal.

`sudo iptables -D INPUT 3`	Delete rule number 3
`sudo iptables -D INPUT -p tcp --dport 80 -j ACCEPT`	Delete by specification
`sudo iptables -I INPUT 1 -p tcp --dport 22 -j ACCEPT`	Insert rule at top
`sudo iptables -R INPUT 3 -p tcp --dport 443 -j ACCEPT`	Replace rule number 3
`sudo iptables -F`	Flush all rules
`sudo iptables -F INPUT`	Flush INPUT chain only

Save and Restore

Persist rules between reboots.

`sudo iptables-save > /etc/iptables/rules.v4`	Save rules
`sudo iptables-restore < /etc/iptables/rules.v4`	Restore rules
`sudo apt install iptables-persistent`	Auto-persist on Debian/Ubuntu
`sudo service iptables save`	Save on RHEL and Derivatives