iptables

Article URL
iptables

Author
SecurityHome.eu

Published: 17 July 2025

Last updated on 25 July 2025.

Â

Iptables is a basic firewall that allows to block on ip-addresses, interface and ports.
You need to be root or have root-privilages to execute iptables (/usr/sbin/iptables)

Note that there is a sperate version for IPv4 and IPv6.
iptables -> IPv4
ip6tables -> IPv6
The option are the same for the 2 commands.

There are 3 main "tables"
Filter is the basic
nat is for Network Address Translation, if you want to forward packets from 1 network to another.
mangle allows to alter packets, change TTL or other.

Each tables has "Chains" on which you can set rules.
INPUT (filter, mangle)
OUTPUT (filter, nat, mangle)
FORWARD (filter)
PREROUTING (nat, mangle)
POSTROUTING (nat)

List current rules

```
iptables -L
iptables -L --line-numbers

iptables -L  --line-numbers
iptables -L INPUT --line-numbers
```

Flush - clear everything

With *-F*

you flush or delete all rules in the table.
Do this when you want to start from scratch.

```
iptables -F
iptables -F -t nat
```

Set default policy with *-P*

,
note: DROP will block everything, so don't do it if you have remote access.

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
```

ADD

Add a new rule with -A

```
iptables -A xxxxxxxxxx
```

for example allow SSH

```
iptables -A INPUT -p tcp --dport 23 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 23 -j ACCEPT
```

block access to samba on 1 interface : enp1s0 (on other interfaces it is still allowed)

```
iptables -A INPUT -i enp1s0 -p tcp -m tcp --dport 139 -j DROP
iptables -A INPUT -i enp1s0 -p tcp -m tcp --dport 445 -j DROP
```

with option -i you can set the interface
lo is local interface it is for the machine to talk to itself, so you should allow all traffic.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

eth0, eth1, ... is Ethernet device 0, 1 ... those are the (old) network cards
enp1s0, enp2s0 is the new name. (Ethernet interface (en), with the "p1s0" part specifying its physical location on the system using a PCI bus ID (1) and slot ID (0).)

Delete

To delete, set the same command, but replace -A with -D

```
iptables -D xxxxxxxxxx
```

Or on line-nr: (iptables -L --line-numbers)

```
iptables -D
```

Save

You can save the rules for the next restart

```
/etc/init.d/iptables save
```

saves file usually to */etc/sysconfig/iptables.save*

.
But it depends on the type of linux.
Gentoo saves it to */var/lib/iptables/rules-save*

Or you can specify your own file:

```
iptables-save -f filename
```

restore

```
iptables-restore
```

NAT

NAT or Network Address Translation allows (in IPv4) for a local IP addresses to be translated into one or more Global IP addresses.
In short words, the firewall/NAT PC becomes the face of your network to the internet. All other PC or devices are "hidden" behind this firewall.

You need to tell you system to allow it:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

And to keep it after restart/reboot

```
# nano /etc/sysctl.conf or /etc/sysctl.d/nat_forward.conf
#Add/Uncomment the following lines:
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
```

To forward the traffic from you internal network (LAN > enp2s0) to the internet (WAN > enp1s0)

This will change the source address of the packet, and with --random change the port for each session.

```
iptables -t nat -A POSTROUTING -o enp1s0 -j MASQUERADE --random
```

Allow traffic from internal (LAN > enp2s0) to external (WAN > enp1s0)

```
iptables -A FORWARD -i enp2s0 -o enp1s0 -j ACCEPT
```

Allow returning traffic from external (WAN > enp1s0) to internal (LAN > enp2s0)

```
iptables -A FORWARD -i enp1s0 -o enp2s0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

That is it for the basic routing.
You can add port forwarding, so a connection to a port on the firewall/router is forwarded to a server inside the LAN network.

```
iptables -t nat -A PREROUTING -i enp1s0 -p tcp -m tcp --dport 993 -j DNAT --to-destination 192.168.1.8:993
iptables -A FORWARD -d 192.168.1.8/32 -p tcp -m tcp --dport 993 -j ACCEPT
```

More info can always be found with

```
man iptables
```