If you want to check your existing rules, use the following command:

# iptables -L -n -v

You can enable logging by this command (for example for INPUT chain):

iptables -A INPUT -j LOG

Toallow incoming traffic:

iptables -A INPUT -p tcp --dport xxx -j ACCEPT

You can allow multiple ports at once, by using **multiport**, below you can find such rule for both incoming and outgoing connections:

# iptables -A INPUT -p tcp -m multiport --dports 22,80,443 -j ACCEPT

# iptables -A OUTPUT -p tcp -m multiport --sports 22,80,443 -j ACCEPT

Loopback access (access from 127.0.0.1) is important and you should always leave it active:

# iptables -A INPUT -i lo -j ACCEPT

# iptables -A OUTPUT -o lo -j ACCEPT

You can block access to your system from specific MAC address by using:

# iptables -A INPUT -m mac --mac-source 00:00:00:00:00:00 -j DROP

If you don’t want to have too many concurrent connection established from single IP address on given port you can use the command below:

# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 3 -j REJECT

If you want to flush your firewall chains, you can use:

# iptables -F

You can flush chains from specific table with:

# iptables -t nat -F

if you want to save your firewall rules, you can use the iptables-save command. You can use the following to save and store your rules in a file:

# iptables-save > ~/iptables.rules

If you want to restore a list of iptables rules, you can use iptables-restore. The command looks like this:

# iptables-restore < ~/iptables.rules

FIREWALLD

firewall-cmd –state

firewall-cmd --zone=public --add-service=http

firewall-cmd --zone=public --add-port=5000/tcp

It is also possible to specify a sequential range of ports by separating the beginning and ending port in the range with a dash. For instance, if our application uses UDP ports 4990 to 4999, we could open these up on “public” by typing:

* sudo firewall-cmd --zone=public --add-port=4990-4999/udp

Copy

After testing, we would likely want to add these to the permanent firewall. You can do that by typing:

* sudo firewall-cmd --zone=public --permanent --add-port=5000/tcp
* sudo firewall-cmd --zone=public --permanent --add-port=4990-4999/udp
* sudo firewall-cmd --zone=public --permanent --list-ports