

iptables set up

```
(haras@haras)-[~]
$ sudo iptables -A -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
[sudo] password for haras:
Bad argument 'conntrack'
Try 'iptables -h' or 'iptables --help' for more information.

(haras@haras)-[~]
$ sudo iptables -A input -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables: No chain/target/match by that name.

(haras@haras)-[~]
$ sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT

(haras@haras)-[~]
$ sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT

(haras@haras)-[~]
$ sudo iptables -A INPUT -p udp --dport ssh -j ACCEPT

(haras@haras)-[~]
$ sudo iptables -A INPUT -p udp --dport 80 -j ACCEPT

(haras@haras)-[~]
$ sudo iptables -A INPUT -m conntrack -p icmp --icmp-type 11 3 --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT
Bad argument '3'
Try 'iptables -h' or 'iptables --help' for more information.

(haras@haras)-[~]
$ sudo iptables -A INPUT -m conntrack -p icmp --icmp-type 3 --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT

(haras@haras)-[~]
$ sudo iptables -A INPUT -m conntrack -p icmp --icmp-type 11 --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT

(haras@haras)-[~]
$ sudo iptables -A INPUT -m conntrack -p icmp --icmp-type 12 --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT

(haras@haras)-[~]
$ sudo iptables -A INPUT -j DROP

(haras@haras)-[~]
$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:domain
ACCEPT     tcp  --  anywhere               anywhere               udp dpt:domain
ACCEPT     udp  --  anywhere               anywhere               udp dpt:22
ACCEPT     udp  --  anywhere               anywhere               udp dpt:80
ACCEPT     icmp --  anywhere               anywhere               ctstate NEW,RELATED,ESTABLISHED icmp destination-unreachable
ACCEPT     icmp --  anywhere               anywhere               ctstate NEW,RELATED,ESTABLISHED icmp time-exceeded
ACCEPT     icmp --  anywhere               anywhere               ctstate NEW,RELATED,ESTABLISHED icmp parameter-problem
DROP       all  --  anywhere               anywhere

Chain FORWARD (policy DROP)
target     prot opt source                destination
DOCKER-USER all  --  anywhere              anywhere
DOCKER-ISOLATION-STAGE-1 all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere               ctstate RELATED,ESTABLISHED
DOCKER     all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain DOCKER (1 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source                destination
DOCKER-ISOLATION-STAGE-2 all  --  anywhere              anywhere
RETURN     all  --  anywhere              anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source                destination
DROP       all  --  anywhere              anywhere
RETURN     all  --  anywhere              anywhere

Chain DOCKER-USER (1 references)
target     prot opt source                destination
RETURN     all  --  anywhere              anywhere

(haras@haras)-[~]
$ sudo iptables -I INPUT 1 -i lo -j ACCEPT
iptables: No chain/target/match by that name.

(haras@haras)-[~]
$ sudo iptables -I INPUT 1 -i lo -j ACCEPT

(haras@haras)-[~]
$ sudo iptables -L
```

```

haras@haras:~$ sudo iptables -I INPUT 1 -i lo -j ACCEPT
haras@haras:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- lo any anywhere anywhere
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:domain
0 0 ACCEPT udp -- any any anywhere anywhere udp dpt:domain
0 0 ACCEPT udp -- any any anywhere anywhere udp dpt:22
0 0 ACCEPT udp -- any any anywhere anywhere udp dpt:80
0 0 ACCEPT icmp -- any any anywhere anywhere ctstate NEW,RELATED,ESTABLISHED icmp destination-unreachable
0 0 ACCEPT icmp -- any any anywhere anywhere ctstate NEW,RELATED,ESTABLISHED icmp time-exceeded
0 0 ACCEPT icmp -- any any anywhere anywhere ctstate NEW,RELATED,ESTABLISHED icmp parameter-problem
54 12248 DROP all -- any any anywhere anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 DOCKER-USER all -- any any anywhere anywhere
0 0 DOCKER-ISOLATION-STAGE-1 all -- any any anywhere anywhere ctstate RELATED,ESTABLISHED
0 0 ACCEPT all -- any docker0 anywhere anywhere
0 0 DOCKER all -- any docker0 !docker0 anywhere anywhere
0 0 ACCEPT all -- docker0 !docker0 anywhere anywhere
0 0 ACCEPT all -- docker0 docker0 anywhere anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain DOCKER (1 references)
pkts bytes target prot opt in out source destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
pkts bytes target prot opt in out source destination
0 0 DOCKER-ISOLATION-STAGE-2 all -- docker0 !docker0 anywhere anywhere
0 0 RETURN all -- any any anywhere anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
pkts bytes target prot opt in out source destination
0 0 DROP all -- any docker0 anywhere anywhere
0 0 RETURN all -- any any anywhere anywhere

Chain DOCKER-USER (1 references)
pkts bytes target prot opt in out source destination
0 0 RETURN all -- any any anywhere anywhere

haras@haras:~$ sudo apt install iptables-persistent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables-persistent is already the newest version (1.0.20).
The following packages were automatically installed and are no longer required:
 libgcb-1.0-0 libglade2-0 lua-lpeg
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 491 not upgraded.

haras@haras:~$ sudo iptables -S INPUT -j DROP
iptables v1.8.9 (nf_tables): Illegal option '-j' with this command
Try 'iptables -h' or 'iptables --help' for more information.

haras@haras:~$ sudo iptables -A INPUT -j DROP

haras@haras:~$ sudo iptables -P INPUT DROP

haras@haras:~$ sudo apt install iptables-persistent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables-persistent is already the newest version (1.0.20).
The following packages were automatically installed and are no longer required:
 libgcb-1.0-0 libglade2-0 lua-lpeg
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 491 not upgraded.

haras@haras:~$ sudo iptables -t mangle -A PREROUTING -M CONNTRACK --INVALID -j DROP
iptables v1.8.9 (nf_tables): unknown option "--INVALID"
Try 'iptables -h' or 'iptables --help' for more information.

haras@haras:~$ sudo iptables -t mangle -A PREROUTING -m CONNTRACK --INVALID -j DROP
iptables v1.8.9 (nf_tables): Couldn't load match 'CONNTRACK':No such file or directory
Try 'iptables -h' or 'iptables --help' for more information.

haras@haras:~$ sudo iptables -t mangle -A PREROUTING -m conntrack --INVALID -j DROP
iptables v1.8.9 (nf_tables): unknown option "--INVALID"
Try 'iptables -h' or 'iptables --help' for more information.

```

```
(haras@haras)-[~]
$ sudo apt install iptables-persistent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables-persistent is already the newest version (1.0.20).
The following packages were automatically installed and are no longer required:
  libgcb-1.0-0 libglade2-0 lua-lpeg
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 491 not upgraded.

(haras@haras)-[~]
$ sudo iptables -S INPUT -j DROP
iptables v1.8.9 (nf_tables): Illegal option '-j' with this command
Try 'iptables -h' or 'iptables --help' for more information.

(haras@haras)-[~]
$ sudo iptables -A INPUT -j DROP

(haras@haras)-[~]
$ sudo iptables -P INPUT DROP

(haras@haras)-[~]
$ sudo apt install iptables-persistent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables-persistent is already the newest version (1.0.20).
The following packages were automatically installed and are no longer required:
  libgcb-1.0-0 libglade2-0 lua-lpeg
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 491 not upgraded.

(haras@haras)-[~]
$ sudo iptables -t mangle -A PREROUTING -M CONNTRACK --INVALID -j DROP
iptables v1.8.9 (nf_tables): unknown option "--INVALID"
Try 'iptables -h' or 'iptables --help' for more information.

(haras@haras)-[~]
$ sudo iptables -t mangle -A PREROUTING -m CONNTRACK --INVALID -j DROP
iptables v1.8.9 (nf_tables): Couldn't load match 'CONNTRACK': No such file or directory
Try 'iptables -h' or 'iptables --help' for more information.

(haras@haras)-[~]
$ sudo iptables -t mangle -A PREROUTING -m conntrack --INVALID -j DROP
iptables v1.8.9 (nf_tables): unknown option "--INVALID"
Try 'iptables -h' or 'iptables --help' for more information.

(haras@haras)-[~]
$ sudo iptables -t mangle -A PREROUTING -m conntrack --ctstate INVALID -j DROP

(haras@haras)-[~]
$ sudo iptables -t mangle -A PREROUTING -p tcp ! --syn -m conntrack --ctstate NEW -j DROP

(haras@haras)-[~]
$ sudo iptables-save > rules.v4

(haras@haras)-[~]
$ sudo cp rules.v4 /etc/iptables/

(haras@haras)-[~]
$ sudo nmap -sX 10.0.253
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-26 13:07 EST
-
```