Environment Setup - two VM created

VM – 10.0.2.7

VM1 – 10.0.2.6

1. Disable all on VM

```
[07/25/21]seed@VM:~$ sudo iptables -t filter -P INPUT DROP
[07/25/21]seed@VM:~$ sudo iptables -t filter -P OUTPUT DROP
[07/25/21]seed@VM:~$ sudo iptables -t filter -P FORWARD DROP
[07/25/21]seed@VM:~$
```

Ping VM1 – failed

```
[07/25/21]seed@VM:~$ sudo ping -c 3 -W 2 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted

--- 10.0.2.6 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2046ms
```

Ping VM from VM1 – failed

```
[07/25/21]seed@VM:~$ ping -c 3 -W 3 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.

--- 10.0.2.7 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2
ms

[07/25/21]seed@VM:~$
```

Enable network by executing the same series of commands with DROP replaced by ACCEPT, then ping VM1 from VM - succeeded

```
[07/25/21]seed@VM:~$ sudo iptables -t filter -P FORWARD ACCEPT
[07/25/21]seed@VM:~$ sudo iptables -t filter -P INPUT ACCEPT
[07/25/21]seed@VM:~$ sudo iptables -t filter -P OUTPUT ACCEPT
[07/25/21]seed@VM:~$ sudo ping -c 3 -W 2 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.733 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.955 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.994 ms

--- 10.0.2.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.733/0.894/0.994/0.114 ms
[07/25/21]seed@VM:~$
```

Ping VM from VM1 – succeeded

```
[07/25/21]seed@VM:~$ ping -c 3 -W 3 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=0.798 ms
64 bytes from 10.0.2.7: icmp_seq=2 ttl=64 time=0.787 ms
64 bytes from 10.0.2.7: icmp_seq=3 ttl=64 time=0.738 ms

--- 10.0.2.7 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 202
rtt min/avg/max/mdev = 0.738/0.774/0.798/0.034 ms
[07/25/21]seed@VM:~$
```

Explanation – at the beginning all actions or packets including INPUT, OUTPUT and FORWARD were disabled/dropped, thus ping between VM and VM1 failed; then while all the packets were allowed, the ping became successful.

2. Blocking an IP

Block packets from VM1

```
[07/25/21]seed@VM:~$ sudo iptables -A INPUT -s 10.0.2.6 -j DROP
[07/25/21]seed@VM:~$
```

Ping VM from VM1 – failed

```
[07/25/21]seed@VM:~$ ping -c 3 -W 3 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.

--- 10.0.2.7 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2
ms
```

It fails because packets from IP of VM1 was blocked in VM.

Environment setup changed:

VM – 10.0.2.9

VM1 – 10.0.2.8

Block packets to VM1 and ping VM1 from VM, it failed:

```
[07/25/21]seed@VM:~$ sudo iptables -A OUTPUT -d 10.0.2.8 -j DROP
[07/25/21]seed@VM:~$ ping -c 3 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

Explanation – as packets blocked from and to IP of VM1, the pings failed.

3. List all rules

```
[07/25/21]seed@VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             10.0.2.8
[07/25/21]seed@VM:~$
```

```
[07/25/21]seed@VM:~$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  anywhere             10.0.2.8
[07/25/21]seed@VM:~$
```

4. Delete a rule – deleted OUTPUT 1 and the rule no longer exists.

```
[07/25/21]seed@VM:~$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  anywhere             10.0.2.8
[07/25/21]seed@VM:~$ sudo iptables -D INPUT 1
iptables: Index of deletion too big.
[07/25/21]seed@VM:~$ sudo iptables -D OUTPUT 1
[07/25/21]seed@VM:~$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[07/25/21]seed@VM:~$
```

5. Delete all rules in a table [filter]

```
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  anywhere             10.0.2.8
[07/25/21]seed@VM:~$ sudo iptables -f
iptables v1.6.0: no command specified
Try `iptables -h' or 'iptables --help' for more information.
[07/25/21]seed@VM:~$ sudo iptables -F
[07/25/21]seed@VM:~$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[07/25/21]seed@VM:~$
```

Before delete/flush all rules, there was one rule, afterwards no rule left.

Environment setup changed:

VM – 10.0.2.10

VM1 – 10.0.2.11

6. Drop all incoming connections except SSH (port 22)

```
[07/25/21]seed@VM:~$ sudo iptables -P INPUT DROP
[07/25/21]seed@VM:~$ sudo iptables -A INPUT -p tcp -
dport 22 -j ACCEPT
Bad argument `22'
Try `iptables -h' or 'iptables --help' for more info
rmation.
[07/25/21]seed@VM:~$ sudo iptables -A INPUT -p tcp -
-dport 22 -j ACCEPT
[07/25/21]seed@VM:~$
```

Ping failed

```
[07/25/21]seed@VM:~$ ping -c 2 10.0.2.10
PING 10.0.2.10 (10.0.2.10) 56(84) bytes of data.

--- 10.0.2.10 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1017
ms
```

But ssh to VM succeeded

```
[07/25/21]seed@VM:~$ ssh 10.0.2.10
The authenticity of host '10.0.2.10 (10.0.2.10)' can't be esta
blished.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFD
aPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.10' (ECDSA) to the list of
known hosts.
seed@10.0.2.10's password:
```

Recover by flush & set to ACCEPT for INPUT

```
[07/25/21]seed@VM:~$ sudo iptables -F
[07/25/21]seed@VM:~$ sudo iptables -P INPUT ACCEPT
[07/25/21]seed@VM:~$
```

Ping succeeded again:

```
[07/25/21]seed@VM:~$ ping -c 3 10.0.2.10
PING 10.0.2.10 (10.0.2.10) 56(84) bytes of data.
64 bytes from 10.0.2.10: icmp_seq=1 ttl=64 time=0.891 ms
64 bytes from 10.0.2.10: icmp_seq=2 ttl=64 time=0.913 ms
64 bytes from 10.0.2.10: icmp_seq=3 ttl=64 time=0.812 ms

--- 10.0.2.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.812/0.872/0.913/0.043 ms
[07/25/21]seed@VM:~$
```

7. Drop outgoing connection to DNS 8.8.8.8

```
[07/25/21]seed@VM:~$ sudo iptables -A OUTPUT -p udp --dport 53 -d 8.8.8.8 -j DROP
[07/25/21]seed@VM:~$ dig www.uwindsor.ca

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.uwindsor.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45016
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.uwindsor.ca.               IN      A

;; ANSWER SECTION:
www.uwindsor.ca.        2116    IN      A       137.207.71.197

;; Query time: 4 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sun Jul 25 16:21:21 EDT 2021
;; MSG SIZE  rcvd: 60

[07/25/21]seed@VM:~$
```

Dig www.uwindsor.ca succeeded, as default DNS server is not the outgoing connection destination denied 8.8.8.8

```
[07/25/21]seed@VM:~$ dig @8.8.8.8 www.uwindsor.ca

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @8.8.8.8 www.uwindsor.ca
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
[07/25/21]seed@VM:~$
```

But the dig with DNS server 8.8.8.8 failed, as outgoing to the DNS server was dropped.

8. Block incoming ping request

   Delete all rules by flush

```
[07/25/21]seed@VM:~$ sudo iptables -F
[07/25/21]seed@VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

BLOCKED incoming ping request

```
[07/25/21]seed@VM:~$ sudo iptables -p icmp -A INPUT --icmp-type echo-request -j DROP
[07/25/21]seed@VM:~$
```

Ping from VM1, failed

```
[07/25/21]seed@VM:~$ ping -c 3 10.0.2.10
PING 10.0.2.10 (10.0.2.10) 56(84) bytes of data.

--- 10.0.2.10 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2039
ms

[07/25/21]seed@VM:~$
```

9. Conntrack module

   Drop all incoming connections, but open conntrack from VM to VM1, telnet still succeeded to VM1.

```
[07/25/21]seed@VM:~$ sudo iptables -P INPUT DROP
[07/25/21]seed@VM:~$ sudo iptables -A INPUT -p tcp -
m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
[07/25/21]seed@VM:~$ telnet 10.0.2.11
Trying 10.0.2.11...
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login:
```

10. Save firewall rules and restore it

Environment setup changed due to connectivity issue:

VM – 10.0.2.12

VM1 – 10.0.2.13

1. Set firewall rules and save to file

```
[07/25/21]seed@VM:~$ sudo iptables -A OUTPUT -p tcp -d 1
0.0.2.16 -j DROP
[07/25/21]seed@VM:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination


Chain FORWARD (policy ACCEPT)
target     prot opt source               destination


Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
           tcp  --  anywhere             10.0.2.16
DROP       tcp  --  anywhere             10.0.2.16
[07/25/21]seed@VM:~$ sudo iptables-save >iptables2.rules
```

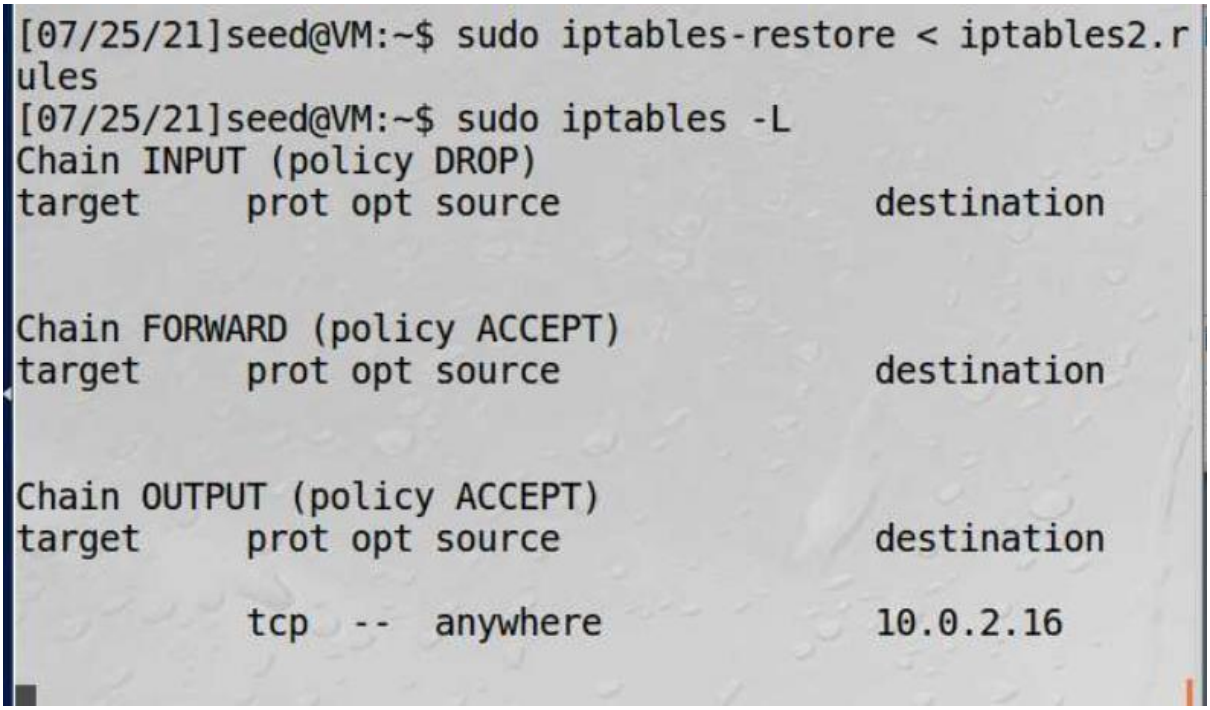
2. Flush all rules

```
[07/25/21]seed@VM:~$ sudo iptables -F
[07/25/21]seed@VM:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination


Chain FORWARD (policy ACCEPT)
target     prot opt source               destination


Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

and recover from the rules file, then the iptables rules was restored.


[07/25/21]seed@VM:~$ sudo iptables-restore < iptables2.r
ules
[07/25/21]seed@VM:~$ sudo iptables -L
Chain INPUT (policy DROP)
target   prot opt source   destination

Chain FORWARD (policy ACCEPT)
target   prot opt source   destination

Chain OUTPUT (policy ACCEPT)
target   prot opt source   destination
           tcp -- anywhere   10.0.2.16