Lab 8 – Firewall Exploration

Container:

```
[04/09/25]seed@VM:~/.../volumes$ dockps
df7fd34706b5  hostA-10.9.0.5
3f2efe2f273a  seed-router
797d1c134324  host2-192.168.60.6
f0f33decb2cf  host1-192.168.60.5
0e6f9a562670  host3-192.168.60.7
[04/09/25]seed@VM:~/.../volumes$
```

Task 2: Experimenting with Stateless Firewall Rules

Task 2.A: Protecting the Router

- ปกป้อง router ด้วยการอนุญาตให้ ping หา router ได้อย่างเดียวเท่านั้น

```
root@3f2efe2f273a:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@3f2efe2f273a:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@3f2efe2f273a:/# iptables -P OUTPUT DROP
root@3f2efe2f273a:/# iptables -P INPUT DROP
root@3f2efe2f273a:/#
```

- คำสั่งที่ 1 และ 2 คืออนุญาตให้ ICMP packet เข้าและออกได้ (INPUT, OUTPUT) ส่วนคำสั่งที่ 3 และ 4 เป็นการตั้ง default ของ packet ที่ INPUT, OUTPUT ถูก drop ทั้งหมด

- ทดลอง ping หา router จากเครื่องอื่น จะสามารถ ping router ได้

```
root@df7fd34706b5:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.151 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.122 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.102 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2042ms
rtt min/avg/max/mdev = 0.102/0.125/0.151/0.020 ms
root@df7fd34706b5:/#
```

- ทดลอง telnet เข้า router จากเครื่องอื่น จะไม่สามารถเชื่อมต่อได้

```
root@df7fd34706b5:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@df7fd34706b5:/#
```

- แต่ในการทำ task ในส่วนต่อไปจะต้องให้ router รับส่ง packet ทั้งหมดได้ตามเดิม โดยใช้คำสั่งต่อไปนี้

```
root@3f2efe2f273a:/# iptables -F
root@3f2efe2f273a:/# iptables -P OUTPUT ACCEPT
root@3f2efe2f273a:/# iptables -P INPUT ACCEPT
root@3f2efe2f273a:/#
```

Task 2.B: Protecting the Internet Network

- ปกป้อง host ภายในวง 192.168.60.0/24 ด้วยการตั้งค่า router ให้เป็นไปตามกฎดังต่อไปนี้

1. host ภายนอก ping host ภายในไม่ได้
2. host ภายนอก ping router ได้
3. host ภายใน ping host ภายนอกได้
4. packet อื่นๆ ระหว่างภายในและภายนอกถูกบล็อกทั้งหมด

```
root@3f2efe2f273a:/# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
65: eth0@if66: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.11/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
73: eth1@if74: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a8:3c:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.60.11/24 brd 192.168.60.255 scope global eth1
       valid_lft forever preferred_lft forever
root@3f2efe2f273a:/#
```

- จาก # ip addr จะเห็นว่า interface ที่เชื่อมกับ host ภายนอกคือ eth0 (outside) ส่วน interface ที่เชื่อมกับ host ภายในคือ eth1 (inside)

```
root@3f2efe2f273a:/# iptables -A FORWARD -i eth1 -p icmp -j ACCEPT
root@3f2efe2f273a:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
root@3f2efe2f273a:/# iptables -A INPUT -p icmp -j ACCEPT
root@3f2efe2f273a:/# iptables -A OUTPUT -p icmp -j ACCEPT
root@3f2efe2f273a:/# iptables -P OUTPUT DROP
root@3f2efe2f273a:/# iptables -P INPUT DROP
root@3f2efe2f273a:/# iptables -P FORWARD DROP
root@3f2efe2f273a:/# iptables -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 0

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
root@3f2efe2f273a:/#
```

- แต่ละคำสั่งมีความหมายดังนี้

No	Command
1	`iptables -A FORWARD -i eth1 -p icmp -j ACCEPT`
	อนุญาตให้ packet ที่ขา eth1 และเป็น ICMP packet ผ่านไปได้ (FORWARD)
2	`iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT`
	อนุญาตให้ packet ที่ขา eth0 เป็น ICMP packet echo-reply ผ่านไปได้ (FORWARD)
3	`iptables -A INPUT -p icmp -j ACCEPT` `iptables -A OUTPUT -p icmp -j ACCEPT`
	อนุญาตให้ packet ICMP เข้ามา (INPUT) และออกจาก (OUTPUT) เครื่องตนเองได้

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

	Default ให้ packet ที่ INPUT, OUTPUT, FORWARD ถูกดรอปทิ้งทั้งหมด

- ทดสอบว่า Firewall ตั้งค่าเป็นไปตามที่ต้องการ

1. host ภายนอก ping host ภายในไม่ได้: จะเห็นว่า host 10.9.0.5 ที่เป็น host นอกวงไม่สามารถ ping ไปหา host ภายในวงได้ (ผลจากคำสั่งที่ 4)

```
root@df7fd34706b5:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
^C
--- 192.168.60.6 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5114ms

root@df7fd34706b5:/#
```

2. host ภายนอก ping router ได้: จะเห็นว่า 10.9.0.5 สามารถ ping หา router (eth0: 10.9.0.11) ได้ (ผลจากคำสั่งที่ 3)

```
root@df7fd34706b5:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.151 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.091 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.079 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.101 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.079/0.105/0.151/0.027 ms
root@df7fd34706b5:/#
```

3. host ภายใน ping host ภายนอกได้: จะเห็นว่า host 192.168.60.6 จะสามารถ ping หา host 10.9.0.5 ได้ (ผลจากคำสั่งที่ 1 และ 2)

```
root@797d1c134324:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.309 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.102 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.134 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.147 ms
^C
--- 10.9.0.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.102/0.173/0.309/0.080 ms
root@797d1c134324:/#
```

4. packet อื่นๆ ระหว่างภายในและภายนอกถูกบล็อกทั้งหมด: ทดลอง telnet ระหว่าง host ภายนอกและภายในหรือ telnet router จะไม่สามารถทำได้

```
root@df7fd34706b5:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@df7fd34706b5:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
root@df7fd34706b5:/#
```

```
root@797d1c134324:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@797d1c134324:/# telnet 192.168.60.11
Trying 192.168.60.11...
telnet: Unable to connect to remote host: Connection timed out
root@797d1c134324:/#
```

- ทำการเคลียร์ iptables ก่อนทำ Task ต่อไป

```
root@3f2efe2f273a:/# iptables -F
root@3f2efe2f273a:/# iptables -P OUTPUT ACCEPT
root@3f2efe2f273a:/# iptables -P INPUT ACCEPT
root@3f2efe2f273a:/# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@3f2efe2f273a:/#
```

Task 2.C: Protecting Internal Servers

- ปกป้อง TCP servers ที่อยู่ภายในวง 192.168.60.0/24 ด้วยการตั้งค่า router ให้เป็นไปตามกฎดังต่อไปนี้

1. host ภายในทุกเครื่องเป็น telnet server (port 23) โดย host ภายนอกสามารถ telnet มาได้เฉพาะ 192.168.60.5 เท่านั้น
2. host ภายนอกเชื่อมต่อ telnet server ภายในไม่ได้
3. host ภายในเชื่อมต่อ telnet server ภายในได้
4. host ภายในเชื่อมต่อ telnet server ภายนอกไม่ได้
5. task นี้ห้ามใช้ connection tracking mechanism

```
root@3f2efe2f273a:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
root@3f2efe2f273a:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
root@3f2efe2f273a:/# iptables -A FORWARD -i eth1 -s 192.168.60.0/24 -d 192.168.60.0/24 -p tcp --dport 23 -j ACCEPT
root@3f2efe2f273a:/# iptables -P OUTPUT DROP
root@3f2efe2f273a:/# iptables -P INPUT DROP
root@3f2efe2f273a:/# iptables -P FORWARD DROP
root@3f2efe2f273a:/# iptables -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination

Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            192.168.60.5         tcp dpt:23
2    ACCEPT     tcp  --  192.168.60.5         0.0.0.0/0            tcp spt:23
3    ACCEPT     tcp  --  192.168.60.0/24      192.168.60.0/24      tcp dpt:23

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
root@3f2efe2f273a:/#
```

- แต่ละคำสั่งมีความหมายดังนี้

No	Command
1	`iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp \ --dport 23 -j ACCEPT`
	อนุญาตให้ packet ที่ขา eth0 (outside) ปลายทาง 192.168.60.5 เป็น TCP packet port ปลายทางเป็น 23 ผ่านไปได้ (FORWARD)
2	`iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp \ --sport 23 -j ACCEPT`
	อนุญาตให้ packet ที่ขา eth1 (inside) ต้นทาง 192.168.60.5 เป็น TCP packet port ต้นทางเป็น 23 ผ่านไปได้ (FORWARD)
3	`iptables -A FORWARD -i eth1 -s 192.168.60.0/24 -d 192.168.60.0/24 \ -p tcp --dport 23 -j ACCEPT`
	อนุญาตให้ packet ที่ขา eth1 (inside) ต้นทาง 192.168.60.0/24 ปลายทาง 192.168.60.0/24 เป็น TCP packet port ปลายทางเป็น 23 ผ่านไปได้ (FORWARD)

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

	Default ให้ packet ที่ INPUT, OUTPUT, FORWARD ถูกดรอปทิ้งทั้งหมด

- ทดสอบว่า Firewall ตั้งค่าเป็นไปตามที่ต้องการ

1. host ภายในทุกเครื่องเป็น telnet server (port 23) โดย host ภายนอกสามารถ telnet มาได้เฉพาะ 192.168.60.5 เท่านั้น: จะเห็นว่า 10.9.0.5 จะสามารถ telnet 192.168.60.5 ได้ (ผลจากคำสั่งที่ 1 และ 2)

```
root@df7fd34706b5:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f0f33decb2cf login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@f0f33decb2cf:~$ ls
seed@f0f33decb2cf:~$
```

2. host ภายนอกเชื่อมต่อ telnet server ภายในไม่ได้ (ผลจากคำสั่งที่ 4)

```
root@df7fd34706b5:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
root@df7fd34706b5:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
root@df7fd34706b5:/#
```

3. host ภายในเชื่อมต่อ telnet server ภายในได้ (ผลจากคำสั่งที่ 3)

```
root@797d1c134324:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f0f33decb2cf login: ^CConnection closed by foreign host.
root@797d1c134324:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0e6f9a562670 login: ^CConnection closed by foreign host.
root@797d1c134324:/#
```

4. host ภายในเชื่อมต่อ telnet server ภายนอกไม่ได้ (ผลจากคำสั่งที่ 4)

```
root@797d1c134324:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@797d1c134324:/#
```

- ทำการเคลียร์ iptables ก่อนทำ Task ต่อไป

```
root@3f2efe2f273a:/# iptables -F
root@3f2efe2f273a:/# iptables -P OUTPUT ACCEPT
root@3f2efe2f273a:/# iptables -P INPUT ACCEPT
root@3f2efe2f273a:/# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@3f2efe2f273a:/#
```

Task 3: Connection Tracking and Stateful Firewall

Task 3.A: Experiment with the Connection Tracking

- ใช้ conntrack ในการติดตาม packet ที่ผ่าน host router

```
root@3f2efe2f273a:/# conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
root@3f2efe2f273a:/#
```

- ICMP experiment: conntrack บอกต้นทางและปลายทาง type ของ ICMP packet และ state ถูกเก็บไว้ประมาณ 30 วินาที (จากเลข 29 ถัดจาก icmp 1 ด้านหน้าสุดของบรรทัด)

```
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.116 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.134 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.106 ms
^C
--- 192.168.60.5 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9200ms
rtt min/avg/max/mdev = 0.079/0.150/0.283/0.067 ms
root@df7fd34706b5:/#
```

```
root@3f2efe2f273a:/# conntrack -L
icmp     1 29 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=55 src=192.168.60.5
 dst=10.9.0.5 type=0 code=0 id=55 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@3f2efe2f273a:/#
```

- **UDP experiment**: state ถูกเก็บไว้ประมาณ 30 วินาที บอก IP และ port ต้นทางและปลายทาง

```
root@f0f33decb2cf:/# nc -lu 9090
hi
```

```
root@df7fd34706b5:/# nc -u 192.168.60.5 9090
hi
```

```
root@3f2efe2f273a:/# conntrack -L
udp      17 27 src=10.9.0.5 dst=192.168.60.5 sport=48427 dport=9090 [UNREPLIED]
src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=48427 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@3f2efe2f273a:/#
```

- **TCP experiment: state** ถูกเก็บไว้ประมาณ 432,000 วินาที หรือประมาณ 120 ชม. บอก IP และ port ต้นทางและปลายทาง

```
root@f0f33decb2cf:/# nc -l 9090
hihi
```

```
root@df7fd34706b5:/# nc 192.168.60.5 9090
hihi
```

```
root@3f2efe2f273a:/# conntrack -L
tcp      6 431997 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=40946 dport=90
90 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=40946 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@3f2efe2f273a:/#
```

Task 3.B: Setting Up a Stateful Firewall

- ตั้ง Firewall สำหรับการเชื่อมต่อแบบ stateful โดยให้การเชื่อมต่อเหมือนกับ Task 2.C แต่เปลี่ยนให้ host ภายในสามารถ telnet host ภายนอกได้แล้ว

```
root@3f2efe2f273a:/# iptables -A FORWARD -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@3f2efe2f273a:/# iptables -A FORWARD -p tcp -i eth0 --dport 8080 --syn -m conntrack --ctstate NEW -j ACCEPT
root@3f2efe2f273a:/# iptables -A FORWARD -p tcp -i eth1 --dport 23 --syn -m conntrack --ctstate NEW -j ACCEPT
root@3f2efe2f273a:/# iptables -A FORWARD -d 192.168.60.5 -p tcp -i eth0 --dport 23 --syn -m conntrack --ctstate NE
W -j ACCEPT
root@3f2efe2f273a:/# iptables -P OUTPUT DROP
root@3f2efe2f273a:/# iptables -P INPUT DROP
root@3f2efe2f273a:/# iptables -P FORWARD DROP
root@3f2efe2f273a:/# iptables -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination

Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED
2    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:8080 flags:0x17/0x02 ctstate NEW
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:23 flags:0x17/0x02 ctstate NEW
4    ACCEPT     tcp  --  0.0.0.0/0            192.168.60.5         tcp dpt:23 flags:0x17/0x02 ctstate NEW

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
root@3f2efe2f273a:/#
```

- แต่ละคำสั่งมีความหมายดังนี้

No	Command
1	`iptables -A FORWARD -p tcp -m conntrack \` `  --ctstate ESTABLISHED,RELATED -j ACCEPT`
	อนุญาตให้ TCP packet ที่มี state เป็น ESTABLISHED, RELATED ผ่านไปได้ (FORWARD)
2	`iptables -A FORWARD -p tcp -i eth0 --dport 8080 --syn \` `  -m conntrack --ctstate NEW -j ACCEPT`
	อนุญาตให้ TCP packet ที่มี state เป็น NEW ที่ขา eth0 (outside) port ปลายทางเป็น 8080 ผ่านไปได้ (FORWARD)
3	`iptables -A FORWARD -p tcp -i eth1 --dport 23 --syn \` `  -m conntrack --ctstate NEW -j ACCEPT`
	อนุญาตให้ TCP packet ที่มี state เป็น NEW ที่ขา eth1 (inside) port ปลายทางเป็น 23 ผ่านไปได้ (FORWARD)
4	`iptables -A FORWARD -d 192.168.60.5 -p tcp -i eth0 --dport 23 \` `  --syn -m conntrack --ctstate NEW -j ACCEPT`
	อนุญาตให้ TCP packet flags SYN ที่มี state เป็น NEW ที่ขา eth0 (outside) ปลายทาง 192.168.60.5 port ปลายทางเป็น 23 ผ่านไปได้ (FORWARD)

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

	Default ให้ packet ที่ INPUT, OUTPUT, FORWARD ถูกดรอปทิ้งทั้งหมด

- ทดสอบว่า Firewall ตั้งค่าเป็นไปตามที่ต้องการ

1. host ภายในทุกเครื่องเป็น telnet server (port 23) โดย host ภายนอกสามารถ telnet มาได้เฉพาะ 192.168.60.5 เท่านั้น (ผลจากคำสั่งที่ 1, 2 และ 4)

```
root@df7fd34706b5:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f0f33decb2cf login: ^CConnection closed by foreign host.
root@df7fd34706b5:/#
```

2. host ภายนอกเชื่อมต่อ telnet server ภายในไม่ได้ (ผลจากคำสั่งที่ 5)

```
root@df7fd34706b5:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
root@df7fd34706b5:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
root@df7fd34706b5:/#
```

3. host ภายในเชื่อมต่อ telnet server ภายในได้ (ผลจากคำสั่งที่ 1 และ 3)

```
root@797d1c134324:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0e6f9a562670 login: Connection closed by foreign host.
root@797d1c134324:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f0f33decb2cf login: ^CConnection closed by foreign host.
root@797d1c134324:/#
```

4. host ภายในเชื่อมต่อ telnet server ภายนอกได้ (ผลจากคำสั่งที่ 1 และ 3)

```
root@797d1c134324:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
df7fd34706b5 login: ^CConnection closed by foreign host.
root@797d1c134324:/#
```

- ทำการเคลียร์ iptables ก่อนทำ Task ต่อไป

```
root@3f2efe2f273a:/# iptables -F
root@3f2efe2f273a:/# iptables -P OUTPUT ACCEPT
root@3f2efe2f273a:/# iptables -P INPUT ACCEPT
root@3f2efe2f273a:/# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@3f2efe2f273a:/#
```

Task 4: Limiting Network Traffic

- จัดการจำนวน packet ที่สามารถผ่าน Firewall ได้ ด้วยการใช้ limit บน iptables

- จัดการจำนวน packet จาก 10.9.0.5 ที่สามารถผ่านได้

No	Command
1	`iptables -A FORWARD -s 10.9.0.5 -m limit \` `  --limit 10/minute --limit-burst 5 -j ACCEPT`
	อนุญาตให้ packet จาก 10.9.0.5 ผ่านไปได้ (FORWARD) 10 packet/นาที และผ่านเป็นกลุ่มได้มากที่สุด 5 packet

```
root@3f2efe2f273a:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
root@3f2efe2f273a:/# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  10.9.0.5             0.0.0.0/0            limit: avg 10/min burst 5

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@3f2efe2f273a:/#
```

```
root@df7fd34706b5:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.121 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.147 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.106 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.126 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.105 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.133 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.122 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.106 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.157 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.126 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.124 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.126 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.126 ms
^C
--- 192.168.60.5 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14318ms
rtt min/avg/max/mdev = 0.094/0.123/0.157/0.015 ms
root@df7fd34706b5:/#
```

No	Command
2	`iptables -A FORWARD -s 10.9.0.5 -j DROP`
	ตั้งค่าให้ packet จาก 10.9.0.5 ที่จะต้อง forward ถูกดรอปทิ้งทั้งหมด

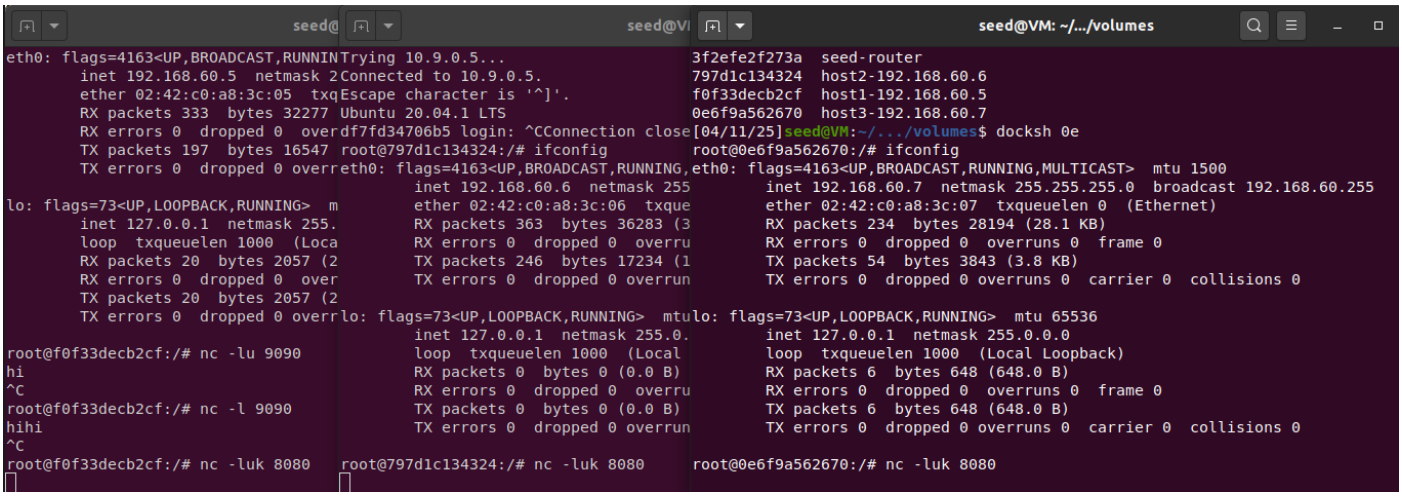
```
root@3f2efe2f273a:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
root@3f2efe2f273a:/# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  10.9.0.5            0.0.0.0/0            limit: avg 10/min burst 5
2    DROP       all  --  10.9.0.5            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@3f2efe2f273a:/#
```

```
root@df7fd34706b5:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.118 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.118 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.155 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.106 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.194 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.127 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.125 ms
64 bytes from 192.168.60.5: icmp_seq=31 ttl=63 time=0.131 ms
64 bytes from 192.168.60.5: icmp_seq=37 ttl=63 time=0.109 ms
^C
--- 192.168.60.5 ping statistics ---
38 packets transmitted, 11 received, 71.0526% packet loss, time 37883ms
rtt min/avg/max/mdev = 0.106/0.130/0.194/0.023 ms
root@df7fd34706b5:/#
```

- จะเห็นว่าด้วยคำสั่งที่ 1 เพียงอย่างเดียว packet ICMP ping-pong ยังสามารถได้รับตามปกติ เพราะ default ของ Chain FORWARD เป็น ACCEPT ในขณะที่เมื่อเพิ่มคำสั่งที่ 2 จะทำให้ได้ผลตามที่ต้องการตามที่สั่งในคำสั่งที่ 1 คือให้ผ่านได้เพียง 10 packet/นาที แล้วรับเป็นชุดได้สูงสุดเพียง 5 packet สังเกตจาก icmp_seq เลขจะถูกข้ามเป็น 7, 13, 19, ... นั่นคือ icmp_seq 8-12, 14-18, ... ถูก router ดรอปทิ้ง

Task 5: Load Balancing

- ทดลองทำ load balance บน 3 UDP servers



- ใช้ nth mode (round-robin)

No	Command
1	iptables -t nat -A PREROUTING -p udp --dport 8080 \ -m statistic --mode nth --every 3 --packet 0 \ -j DNAT --to-destination 192.168.60.5:8080 iptables -t nat -A PREROUTING -p udp --dport 8080 \ -m statistic --mode nth --every 2 --packet 0 \ -j DNAT --to-destination 192.168.60.6:8080 iptables -t nat -A PREROUTING -p udp --dport 8080 \ -m statistic --mode nth --every 1 --packet 0 \ -j DNAT --to-destination 192.168.60.7:8080
	ตั้งค่าให้ทุกๆ UPD packet ที่ 3 ปลายทาง port 8080 ส่งไปยัง 192.168.60.5:8080, ทุกๆ UPD packet ที่ 2 ปลายทาง port 8080 ส่งไปยัง 192.168.60.6:8080, ทุกๆ UPD packet ที่ 1 ปลายทาง port 8080 ส่งไปยัง 192.168.60.7:8080

```
root@3f2efe2f273a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --
packet 0 -j DNAT --to-destination 192.168.60.5:8080
root@3f2efe2f273a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 2 --
packet 0 -j DNAT --to-destination 192.168.60.6:8080
root@3f2efe2f273a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 1 --
packet 0 -j DNAT --to-destination 192.168.60.7:8080
```

```
root@3f2efe2f273a:/# iptables -t nat -L PREROUTING --line-numbers -n
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 3
to:192.168.60.5:8080
2    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 2
to:192.168.60.6:8080
3    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 1
to:192.168.60.7:8080
root@3f2efe2f273a:/#
```

```
root@df7fd34706b5:/# echo hello1 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hello2 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hello3 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hello4 | nc -u 10.9.0.11 8080
echo hello5 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hello5 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hello6 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hello7 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hello8 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hello9 | nc -u 10.9.0.11 8080
hello10
^C
root@df7fd34706b5:/#
```

```
root@f0f33decb2cf:/# nc -luk 8080
hello3
hello6
hello9
```

```
root@797d1c134324:/# nc -luk 8080
hello1
hello4
hello7
```

```
root@0e6f9a562670:/# nc -luk 8080
hello2
hello5
hello8
```

จะเห็นว่าทั้ง 3 server ผลัดกันรับ UDP packet ไล่ลำดับกันไป

- ทำการลบ nat rules ก่อนไปทำขั้นตอนถัดไป ด้วยการใช้คำสั่งเดิม แต่เปลี่ยนจาก iptables -A เป็น iptables -D

```
root@3f2efe2f273a:/# iptables -t nat -L PREROUTING --line-numbers -n
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 3
to:192.168.60.5:8080
2    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 2
to:192.168.60.6:8080
3    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 1
to:192.168.60.7:8080
root@3f2efe2f273a:/# iptables -t nat -D PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --
packet 0 -j DNAT --to-destination 192.168.60.5:8080
root@3f2efe2f273a:/# iptables -t nat -D PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 2 --
packet 0 -j DNAT --to-destination 192.168.60.6:8080
root@3f2efe2f273a:/# iptables -t nat -D PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 1 --
packet 0 -j DNAT --to-destination 192.168.60.7:8080
root@3f2efe2f273a:/# iptables -t nat -L PREROUTING --line-numbers -n
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
root@3f2efe2f273a:/# iptables -L -n --line-numbers
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
root@3f2efe2f273a:/#
```

- ใช้ random mode

No	Command
2	iptables -t nat -A PREROUTING -p udp --dport 8080 \ -m statistic --mode random --probability 0.33 \ -j DNAT --to-destination 192.168.60.5:8080 iptables -t nat -A PREROUTING -p udp --dport 8080 \ -m statistic --mode random --probability 0.5 \ -j DNAT --to-destination 192.168.60.6:8080 iptables -t nat -A PREROUTING -p udp --dport 8080 \ -m statistic --mode random --probability 1 \ -j DNAT --to-destination 192.168.60.7:8080
	ตั้งค่าให้ UPD packet ปลายทาง port 8080 มีโอกาส 33% ส่งไปยัง 192.168.60.5:8080, UPD packet ปลายทาง port 8080 มีโอกาส 50% ส่งไปยัง 192.168.60.6:8080, UPD packet ปลายทาง port 8080 มีโอกาส 100% ส่งไปยัง 192.168.60.7:8080

```
root@3f2efe2f273a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probabi
lity 0.33 -j DNAT --to-destination 192.168.60.5:8080
root@3f2efe2f273a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probabi
lity 0.5 -j DNAT --to-destination 192.168.60.6:8080
root@3f2efe2f273a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probabi
lity 1 -j DNAT --to-destination 192.168.60.7:8080
root@3f2efe2f273a:/# iptables -L -n --line-numbers
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
root@3f2efe2f273a:/# iptables -t nat -L PREROUTING --line-numbers -n
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode random proba
bility 0.33000000007 to:192.168.60.5:8080
2    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode random proba
bility 0.50000000000 to:192.168.60.6:8080
3    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode random proba
bility 1.00000000000 to:192.168.60.7:8080
root@3f2efe2f273a:/#
```

```
root@df7fd34706b5:/# echo hi1 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi2 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi3 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi4 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi5 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi6 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi7 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi8 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi9 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/# echo hi10 | nc -u 10.9.0.11 8080
^C
root@df7fd34706b5:/#
```

```
root@f0f33decb2cf:/# nc -luk 8080
hi1
hi2
hi4
hi5
hi7
hi9
```

```
hello1
hello4
hello7
^C
root@797d1c134324:/# nc -luk 8080
hi3
hi10
```

```
hello2
hello5
hello8
^C
root@0e6f9a562670:/# nc -luk 8080
hi6
hi8
```

จะเห็นว่าทั้ง 3 server ผลัดกันรับ UDP packet แบบสุ่ม โดยที่เครื่อง 192.168.60.5 ได้รับมากที่สุด แล้วจึงถูกส่งไปยังเครื่อง 192.168.60.6 หรือ 192.168.60.7 ตามลำดับ