Lab 8 – Firewall Exploration

Container:

```
[04/14/25]seed@VM:~/.../10_FirewallExplorationLab$ dockps
4e6333443848  seed-router
2936e09737c6  host3-192.168.60.7
ec5d95dd9f6a  host1-192.168.60.5
31ed12552a93  hostA-10.9.0.5
076350c4c830  host2-192.168.60.6
[04/14/25]seed@VM:~/.../10_FirewallExplorationLab$
```

Task 2: Experimenting with Stateless Firewall Rules

Task 2.A: Protecting the Router

ทำการอนุญาตให้ ping หา router ได้เท่านั้น

```
[04/14/25]seed@VM:~/.../10_FirewallExplorationLab$ docksh 4e
root@4e6333443848:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@4e6333443848:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@4e6333443848:/# iptables -P OUTPUT DROP
root@4e6333443848:/# iptables -P INPUT DROP
root@4e6333443848:/#
```

ทดลอง ping หา router

```
[04/14/25]seed@VM:~/.../10_FirewallExplorationLab$ docksh 29
root@2936e09737c6:/# ping 10.9.0.11 -c 4
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=0.264 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.165 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.150 ms

--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.150/0.192/0.264/0.043 ms
root@2936e09737c6:/#
```

ทดลอง telnet ไปที่ router จะพบว่าไม่สามารถทำได้

```
root@2936e09737c6:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@2936e09737c6:/#
```

Task 2.B: Protecting the Internet Network

ทำการตั้งกฎให้กับวง 192.168.60.0/24

1. host ภายนอก ping host ภายในไม่ได้

2. host ภายนอก ping router ได้

3. host ภายใน ping host ภายนอกได้

4. packet อื่นๆ ระหว่างภายในและภายนอกถูกบล็อกทั้งหมด

```
root@4e6333443848:/# 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
42: eth0@if43: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group defaul
t
    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
46: eth1@if47: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group defaul
t
    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@4e6333443848:/#
```

Interface ที่เชื่อมกับ host ภายนอกคือ eth0 และ Interface ที่เชื่อมกับ host ภายในคือ eth1

```
root@4e6333443848:/# iptables -A FORWARD -i eth1 -p icmp -j ACCEPT
root@4e6333443848:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
root@4e6333443848:/# iptables -A INPUT -p icmp -j ACCEPT
root@4e6333443848:/# iptables -A OUTPUT -p icmp -j ACCEPT
root@4e6333443848:/# iptables -P OUTPUT DROP
root@4e6333443848:/# iptables -P INPUT DROP
root@4e6333443848:/# iptables -P FORWARD DROP
root@4e6333443848:/# 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@4e6333443848:/#
```

โดยรูปภาพด้านบนเป็นการตั้งกฎตามคำสั่งต่อไปนี้

ลำดับ	คำสั่ง
1	iptables -A FORWARD -i eth1 -p icmp -j ACCEPT
อนุญาตให้ packet ที่ eth1 และเป็น ICMP packet ผ่านไปได้	
2	iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
อนุญาตให้ packet ที่ eth0 เป็น ICMP packet echo-reply ผ่านไปได้	
3	iptables -A INPUT -p icmp -j ACCEPT iptables -A OUTPUT -p icmp -j ACCEPT
อนุญาตให้ packet ICMP เข้ามาและออกจากเครื่องตนเองได้	
4	iptables -P OUTPUT DROP iptables -P INPUT DROP iptables -P FORWARD DROP
Default ให้ packet ที่ INPUT, OUTPUT, FORWARD ถูกดรอปทิ้งทั้งหมด	

ทำการทดสอบว่ากฎที่ตั้งไว้ทำงานได้หรือไม่

- host ภายนอก ping หา host ภายในไม่ได้ แต่ host ภายนอก ping หา router ได้

```
[04/14/25]seed@VM:~/.../10_FirewallExplorationLab$ docksh 31
root@31ed12552a93:/# ping 192.168.60.7 -c 4
PING 192.168.60.7 (192.168.60.7) 56(84) bytes of data.

--- 192.168.60.7 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3072ms

root@31ed12552a93:/# ping 10.9.0.11 -c 4
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=0.155 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.157 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.169 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.138 ms

--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.138/0.154/0.169/0.011 ms
root@31ed12552a93:/#
```

- host ภายใน ping host ภายนอกได้

```
root@2936e09737c6:/# ping 10.9.0.5 -c 4
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=0.199 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.196 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.226 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.230 ms

--- 10.9.0.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.196/0.212/0.230/0.015 ms
root@2936e09737c6:/#
```

- packet อื่นๆ ระหว่างภายในและภายนอกถูกบล็อกทั้งหมด โดยทดลอง telnet

```
root@2936e09737c6:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@2936e09737c6:/# telnet 192.168.60.11
Trying 192.168.60.11...
telnet: Unable to connect to remote host: Connection timed out
root@2936e09737c6:/#
```

```
root@31ed12552a93:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
root@31ed12552a93:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@31ed12552a93:/#
```

Task 2.C: Protecting Internal Servers

ทำการป้องกัน TCP Server ในวง 192.168.60.0/24 ด้วยกฎต่อไปนี้

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@4e6333443848:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
root@4e6333443848:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
root@4e6333443848:/# iptables -A FORWARD -i eth1 -s 192.168.60.0/24 -d 192.168.60.0/24 -p tcp
 --dport 23 -j ACCEPT
root@4e6333443848:/# iptables -P OUTPUT DROP
root@4e6333443848:/# iptables -P INPUT DROP
root@4e6333443848:/# iptables -P FORWARD DROP
root@4e6333443848:/# 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@4e6333443848:/#
```

โดยรูปภาพด้านบนเป็นการตั้งกฎตามคำสั่งต่อไปนี้

ลำดับ	คำสั่ง
1	iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
อนุญาตให้ packet ที่ eth0 ปลายทาง 192.168.60.5 เป็น TCP packet port ปลายทางเป็น 23 ผ่านไปได้	
2	iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
อนุญาตให้ packet ที่ eth1 ต้นทาง 192.168.60.5 เป็น TCP packet port ต้นทางเป็น 23 ผ่านไปได้	
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 ที่ eth1 ต้นทาง 192.168.60.0/24 ปลายทาง 192.168.60.0/24 เป็น TCP packet port ปลายทางเป็น 23 ผ่านไปได้	
4	iptables -P OUTPUT DROP iptables -P INPUT DROP iptables -P FORWARD DROP
Default ให้ packet ที่ INPUT, OUTPUT, FORWARD ถูกดรอปทิ้งทั้งหมด	

ทดสอบว่ากฎที่ตั้งไว้ทำงานได้หรือไม่

- host ภายนอกสามารถ telnet มาได้เฉพาะ 192.168.60.5 เท่านั้น

```
root@31ed12552a93:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ec5d95dd9f6a 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@ec5d95dd9f6a:~$
```

- host ภายนอกเชื่อมต่อ telnet server ภายในไม่ได้

```
root@31ed12552a93:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
root@31ed12552a93:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
root@31ed12552a93:/#
```

- host ภายในเชื่อมต่อ telnet server ภายในได้

```
root@2936e09737c6:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ec5d95dd9f6a login: ^CConnection closed by foreign host.
root@2936e09737c6:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
076350c4c830 login: ^CConnection closed by foreign host.
root@2936e09737c6:/#
```

- host ภายในเชื่อมต่อ telnet server ภายนอกไม่ได้

```
root@2936e09737c6:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@2936e09737c6:/#
```

Task 3: Connection Tracking and Stateful Firewall

Task 3.A: Experiment with the Connection Tracking

ICMP experiment: conntrack บอกต้นทางและปลายทางของ ICMP packet state ถูกเก็บไว้ 30 วินาที

```
root@31ed12552a93:/# ping 192.168.60.7 -c 4
PING 192.168.60.7 (192.168.60.7) 56(84) bytes of data.
64 bytes from 192.168.60.7: icmp_seq=1 ttl=63 time=0.319 ms
64 bytes from 192.168.60.7: icmp_seq=2 ttl=63 time=0.188 ms
64 bytes from 192.168.60.7: icmp_seq=3 ttl=63 time=0.237 ms
64 bytes from 192.168.60.7: icmp_seq=4 ttl=63 time=0.224 ms

--- 192.168.60.7 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.188/0.242/0.319/0.047 ms
root@31ed12552a93:/#
```

```
root@4e6333443848:/# conntrack -L
icmp     1 25 src=10.9.0.5 dst=192.168.60.7 type=8 code=0 id=39 src=192.168.60.7 dst=10.9.0.5
 type=0 code=0 id=39 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4e6333443848:/#
```

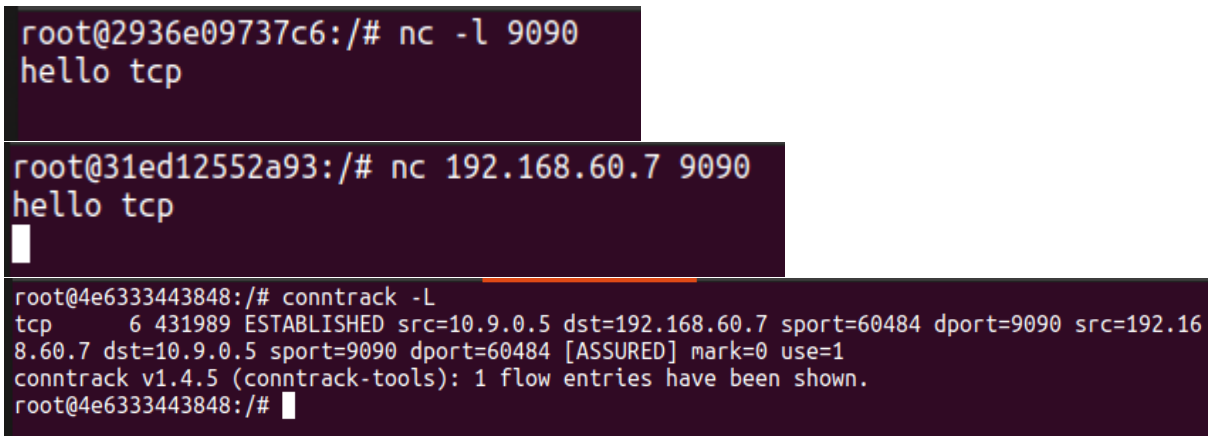
UDP experiment:บอก IP และ port ต้นทางและปลายทาง state ถูกเก็บไว้ 30 วินาที

```
root@2936e09737c6:/# nc -lu 9090
hi
```

```
root@31ed12552a93:/# nc -u 192.168.60.7 9090
hi
```

```
root@4e6333443848:/# conntrack -L
udp      17 17 src=10.9.0.5 dst=192.168.60.7 sport=48895 dport=9090 [UNREPLIED] src=192.168.6
0.7 dst=10.9.0.5 sport=9090 dport=48895 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4e6333443848:/#
```

TCP experiment บอก IP และ port ต้นทางและปลายทาง state ถูกเก็บไว้ 432,000 วินาที



Task 3.B: Setting Up a Stateful Firewall

ตั้ง Firewall สำหรับการเชื่อมต่อแบบ stateful และให้ host ภายในสามารถ telnet host ภายนอกได้

```
root@4e6333443848:/# iptables -A FORWARD -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@4e6333443848:/# iptables -A FORWARD -p tcp -i eth0 --dport 8080 --syn -m conntrack --ctstate NE
W -j ACCEPT
root@4e6333443848:/# iptables -A FORWARD -p tcp -i eth1 --dport 23 --syn -m conntrack --ctstate NEW
-j ACCEPT
root@4e6333443848:/# iptables -A FORWARD -d 192.168.60.5 -p tcp -i eth0 --dport 23 --syn -m conntrac
k --ctstate NEW -j ACCEPT
root@4e6333443848:/# iptables -P OUTPUT DROP
root@4e6333443848:/# iptables -P INPUT DROP
root@4e6333443848:/# iptables -P FORWARD DROP
root@4e6333443848:/# 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 ctst
ate NEW
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:23 flags:0x17/0x02 ctstat
e NEW
4    ACCEPT     tcp  --  0.0.0.0/0            192.168.60.5         tcp dpt:23 flags:0x17/0x02 ctstat
e NEW

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
root@4e6333443848:/#
```

โดยรูปภาพด้านบนเป็นการตั้งกฎตามคำสั่งต่อไปนี้

ลำดับ	คำสั่ง
1	iptables -A FORWARD -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
อนุญาตให้ TCP packet ที่มี state เป็น ESTABLISHED, RELATED ผ่านไปได้	
2	iptables -A FORWARD -p tcp -i eth0 --dport 8080 –syn -m conntrack --ctstate NEW -j ACCEPT
อนุญาตให้ TCP packet ที่มี state เป็น NEW ที่ eth0 port ปลายทางเป็น 8080 ผ่านไปได้	
3	iptables -A FORWARD -p tcp -i eth1 --dport 23 --syn -m conntrack --ctstate NEW -j ACCEPT
อนุญาตให้ TCP packet ที่มี state เป็น NEW ที่ eth1 port ปลายทางเป็น 23 ผ่านไปได้	
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 ที่ eth0 ปลายทาง 192.168.60.5 port ปลายทางเป็น 23 ผ่านไปได้	
5	iptables -P OUTPUT DROP iptables -P INPUT DROP iptables -P FORWARD DROP
Default ให้ packet ที่ INPUT, OUTPUT, FORWARD ถูกดรอปทิ้งทั้งหมด	

ทดสอบกฎที่ตั้งไว้ว่าทำงานได้หรือไม่

- host ภายนอกสามารถ telnet มาได้เฉพาะ 192.168.60.5 เท่านั้น
  แต่ host ภายนอกเชื่อมต่อ telnet server ภายในไม่ได้

```
root@31ed12552a93:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ec5d95dd9f6a login: ^CConnection closed by foreign host.
root@31ed12552a93:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
root@31ed12552a93:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
root@31ed12552a93:/#
```

- host ภายในเชื่อมต่อ telnet server ภายในได้
  และ host ภายในเชื่อมต่อ telnet server ภายนอกได้

Task 4: Limiting Network Traffic

จัดการจานวน packet ที่สามารถผ่าน Firewall ได้ ด้วยการใช้ limit บน iptables

จัดการจานวน packet จาก 10.9.0.5 ที่สามารถผ่านได้

```
root@4e6333443848:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j A
CCEPT
root@4e6333443848:/# 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@4e6333443848:/#
```

รูปภาพด้านบนเป็นการตั้งกฎตามคำสั่งต่อไปนี้

ลำดับ	คำสั่ง
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 10 packet/นาที และผ่านเป็นกลุ่มได้มากที่สุด 5 packet	

```
root@31ed12552a93:/# ping 192.168.60.5 -c 15
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=0.415 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.272 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.208 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.211 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.204 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.247 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.206 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.213 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.247 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.207 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.203 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.208 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.206 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.208 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.237 ms

--- 192.168.60.5 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14341ms
rtt min/avg/max/mdev = 0.203/0.232/0.415/0.052 ms
root@31ed12552a93:/#
```

```
root@4e6333443848:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
root@4e6333443848:/# 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@4e6333443848:/#
```

รูปภาพด้านบนเป็นการตั้งกฎตามคำสั่งต่อไปนี้

ลำดับ	คำสั่ง
2	iptables -A FORWARD -s 10.9.0.5 -j DROP
ตั้งค่าให้ packet จาก 10.9.0.5 ที่จะต้อง forward ถูกดรอปทิ้งทั้งหมด	

```
root@31ed12552a93:/# ping 192.168.60.5 -c 38
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=0.171 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.431 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.213 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.209 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.233 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.331 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.224 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.203 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.225 ms
64 bytes from 192.168.60.5: icmp_seq=31 ttl=63 time=0.228 ms
64 bytes from 192.168.60.5: icmp_seq=37 ttl=63 time=0.195 ms

--- 192.168.60.5 ping statistics ---
38 packets transmitted, 11 received, 71.0526% packet loss, time 37878ms
rtt min/avg/max/mdev = 0.171/0.242/0.431/0.070 ms
root@31ed12552a93:/#
```

สรุป คำสั่งที่ 1 เพียงคำสั่งเดียว packet ICMP ping-pong ยังสามารถได้รับตามปกติ เพราะ default ของ Chain FORWARD เป็น ACCEPT ในขณะที่เมื่อเพิ่มคาสั่งที่ 2 จะทาให้ได้ผลตามที่ต้องการตามที่สั่งในคาสั่งที่ 1 คือให้ผ่านได้เพียง 10 packet/นาที แล้วรับเป็นชุดได้สูงสุดเพียง 5 packet

Task 5: Load Balancing

ทำ load balance บน 3 UDP server

ใช้ nth mode (round-robin)

```
root@4e6333443848:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --eve
ry 3 --packet 0 -j DNAT --to-destination 192.168.60.5:8080
root@4e6333443848:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --eve
ry 2 --packet 0 -j DNAT --to-destination 192.168.60.6:8080
root@4e6333443848:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --eve
ry 1 --packet 0 -j DNAT --to-destination 192.168.60.7:8080
```

รูปภาพด้านบนเป็นการตั้งกฎตามคำสั่งต่อไปนี้

ลำดับ	คำสั่ง
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@4e6333443848:/# 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 e
very 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 e
very 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 e
very 1 to:192.168.60.7:8080
root@4e6333443848:/#
```

ให้ host ภายในทั้ง 3 ตัวใช้คำสั่ง nc -luk 8080 รอรับข้อความ

ให้ host ภายนอก echo ไปที่ router

```
root@31ed12552a93:/# echo round_robin_1 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo round_robin_2 | nc -u 10.9.0.11 8080
^C
^C
root@31ed12552a93:/# echo round_robin_3 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo round_robin_4 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo round_robin_5 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo round_robin_6 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/#
```

ผลที่ได้ ทั้งสามเครื่องจะได้รับข้อความวนกันไปตามลำดับ

```
root@2936e09737c6:/# nc -luk 8080
round_robin_3
round_robin_6
```

```
seed@VM: ~/.../10_FirewallExp
[04/14/25]seed@VM:~/.../10_FirewallExplo
root@076350c4c830:/# nc -luk 8080
round_robin_2
round_robin_5
```

```
seed@VM: ~/.../10_FirewallExplo.
[04/14/25]seed@VM:~/.../10_Firewall
c
root@ec5d95dd9f6a:/# nc -luk 8080
round_robin_1
round_robin_4
```

ทาการลบ nat rules ก่อนไปทาขั้นตอนถัดไป

```
root@4e6333443848:/# iptables -t nat -D PREROUTING -p udp --dport 8080 -m statistic --mode nth --eve
ry 3 --packet 0 -j DNAT --to-destination 192.168.60.5:8080
root@4e6333443848:/# iptables -t nat -D PREROUTING -p udp --dport 8080 -m statistic --mode nth --eve
ry 2 --packet 0 -j DNAT --to-destination 192.168.60.6:8080
root@4e6333443848:/# iptables -t nat -D PREROUTING -p udp --dport 8080 -m statistic --mode nth --eve
ry 1 --packet 0 -j DNAT --to-destination 192.168.60.7:8080
root@4e6333443848:/#
root@4e6333443848:/# iptables -t nat -L PREROUTING --line-numbers -n
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
root@4e6333443848:/# 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@4e6333443848:/#
```

ใช้ random mode

```
root@4e6333443848:/# 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
root@4e6333443848:/# 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
root@4e6333443848:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --
probability 1 -j DNAT --to-destination 192.168.60.7:8080
root@4e6333443848:/# 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@4e6333443848:/# 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 rando
m probability 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 rando
m probability 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 rando
m probability 1.00000000000 to:192.168.60.7:8080
root@4e6333443848:/#
```

รูปภาพด้านบนเป็นการตั้งกฎตามคำสั่งต่อไปนี้

ลำดับ	คำสั่ง
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	

ให้ host ภายในทั้ง 3 ตัวใช้คำสั่ง nc -luk 8080 รอรับข้อความ

ให้ host ภายนอก echo ไปที่ router

```
root@31ed12552a93:/# echo random_mode_1 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo random_mode_2 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo random_mode_3 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo random_mode_4 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo random_mode_5 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo random_mode_6 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo random_mode_7 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo random_mode_8 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/# echo random_mode_9 | nc -u 10.9.0.11 8080
^C
root@31ed12552a93:/#
```

```
root@2936e09737c6:/# nc -luk 8080
random_mode_4
random_mode_6
random_mode_8
```

```
seed@VM: ~/.../10_FirewallExp
root@076350c4c830:/# nc -luk 8080
random_mode_3
random_mode_9
```

```
seed@VM: ~/.../10_FirewallExplo..
root@ec5d95dd9f6a:/# nc -luk 8080
random_mode_1
random_mode_2
random_mode_5
random_mode_7
```

ผลที่ได้จะเห็นว่าทั้ง 3 เครื่องจะถูกสุ่มเพื่อรับ UDP packet