Lab6-Firewall Exploration Lab

57118205 邱沐瑶

目录

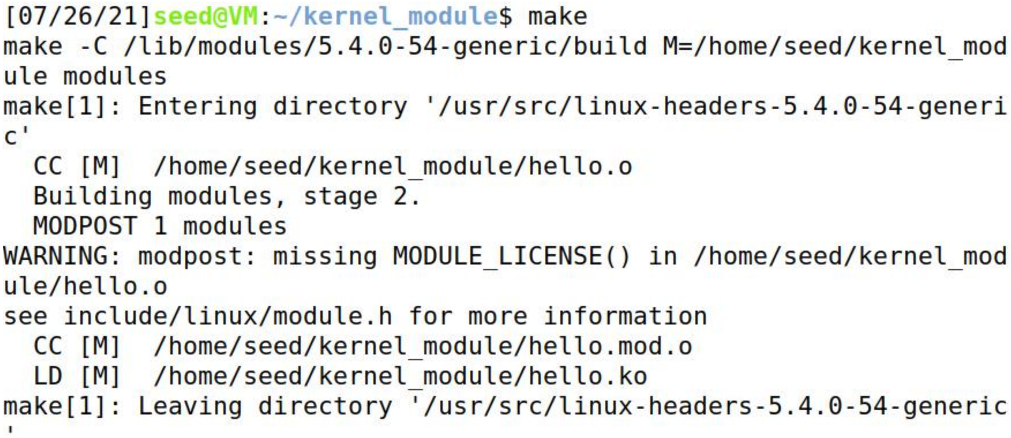
Task 1: Implementing a Simple Firewall....1
Task 1.A: Implement a Simple Kernel Module....1
Task 1.B: Implement a Simple Firewall Using Netfilter....2
Task 2: Experimenting with Stateless Firewall Rules....4
Task 2.A: Protecting the Router....4
Task 2.B: Protecting the Internal Network....5
Task 2.C: Protecting Internal Servers....6
Task 3: Connection Tracking and Stateful Firewall....7
Task 3.A: Experiment with the Connection Tracking....7
Task 3.B: Setting Up a Stateful Firewall....8
Task 4: Limiting Network Traffific....9
Task 5: Load Balancing....10

Task 1: Implementing a Simple Firewall

Task 1.A: Implement a Simple Kernel Module

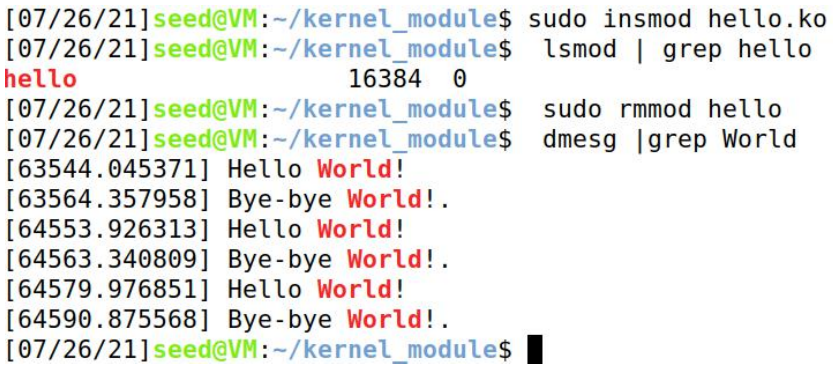
因为原始目录存在空格，目录的空格被 make 识别为编译的 target。

将 kernel_module 拷贝到 /home/seed/目录下，编译，显示编译成功。



```
[07/26/21]seed@VM:~/kernel_module$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/kernel_mod
ule modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generi
c'
  CC [M]  /home/seed/kernel_module/hello.o
  Building modules, stage 2.
  MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /home/seed/kernel_mod
ule/hello.o
see include/linux/module.h for more information
  CC [M]  /home/seed/kernel_module/hello.mod.o
  LD [M]  /home/seed/kernel_module/hello.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic
'
```

测试以下命令（测试原因加载卸载了三次，截图没有体现。故 dmesg 有三次 hello bye 信息）

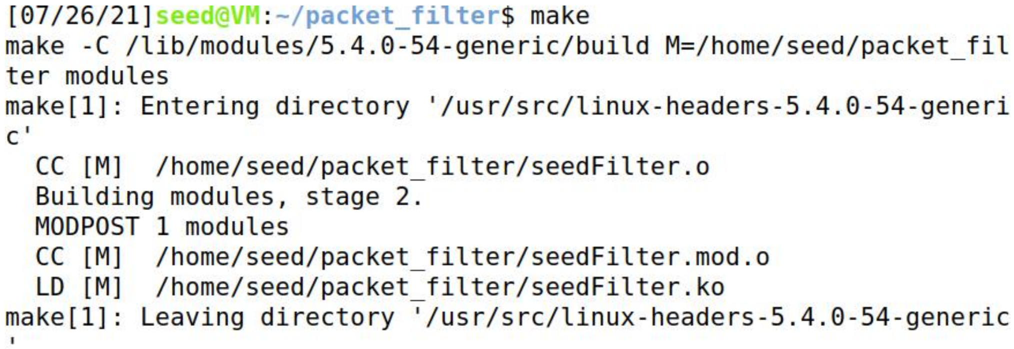


```
[07/26/21]seed@VM:~/kernel_module$ sudo insmod hello.ko
[07/26/21]seed@VM:~/kernel_module$  lsmod | grep hello
hello                  16384  0
[07/26/21]seed@VM:~/kernel_module$  sudo rmmod hello
[07/26/21]seed@VM:~/kernel_module$  dmesg |grep World
[63544.045371] Hello World!
[63564.357958] Bye-bye World!.
[64553.926313] Hello World!
[64563.340809] Bye-bye World!.
[64579.976851] Hello World!
[64590.875568] Bye-bye World!.
[07/26/21]seed@VM:~/kernel_module$ 
```

Task 1.B: Implement a Simple Firewall Using Netfilter

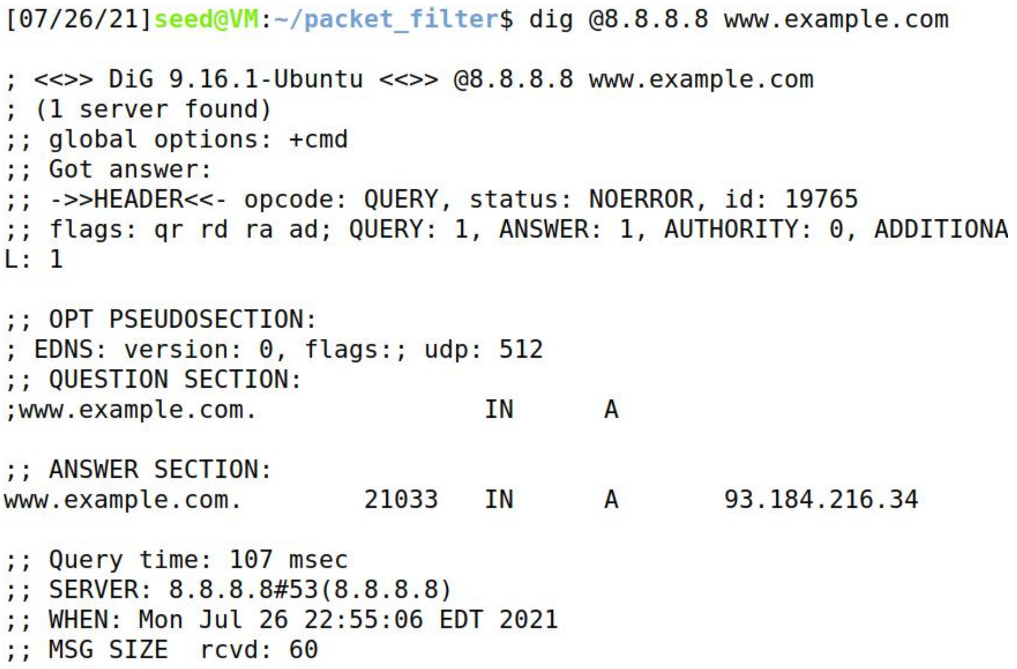
1. Compile the sample code using the provided Makefile.

将文件拷贝到 /home/seed/ 下，编译，编译成功。



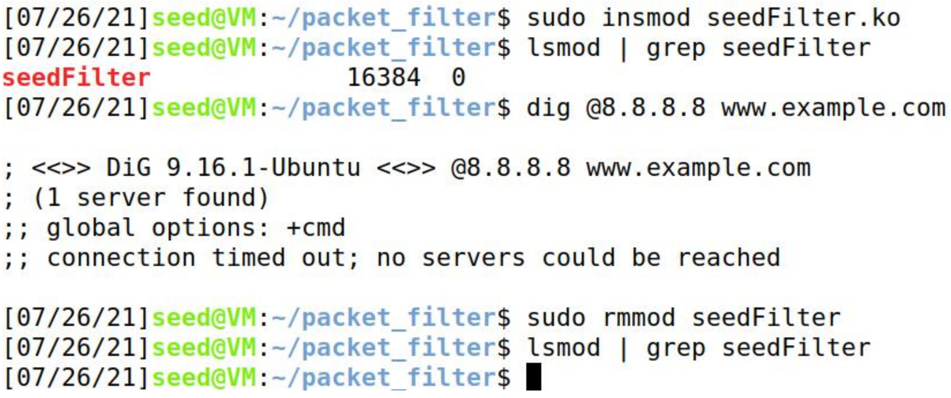
```
[07/26/21]seed@VM:~/packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/packet_fil
ter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generi
c'
  CC [M]  /home/seed/packet_filter/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/packet_filter/seedFilter.mod.o
  LD [M]  /home/seed/packet_filter/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic
'
```

加载内核前，执行 dig @8.8.8.8 www.example 命令，得到响应。



```
[07/26/21]seed@VM:~/packet_filter$ dig @8.8.8.8 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19765
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONA
L: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        21033   IN      A       93.184.216.34

;; Query time: 107 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Jul 26 22:55:06 EDT 2021
;; MSG SIZE  rcvd: 60
```

将模块加载到内核，防火墙生效，dig @8.8.8.8 www.example 命令无效。



```
[07/26/21]seed@VM:~/packet_filter$ sudo insmod seedFilter.ko
[07/26/21]seed@VM:~/packet_filter$ lsmod | grep seedFilter
seedFilter             16384  0
[07/26/21]seed@VM:~/packet_filter$ dig @8.8.8.8 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached

[07/26/21]seed@VM:~/packet_filter$ sudo rmmod seedFilter
[07/26/21]seed@VM:~/packet_filter$ lsmod | grep seedFilter
[07/26/21]seed@VM:~/packet_filter$ 
```

2. Hook the printInfo function to all of the netfilter hooks.

① 数据报从进入系统，进行 IP 校验以后，首先经过第一个 HOOK 函数 NF_IP_PRE_ROUTING 进行处理；

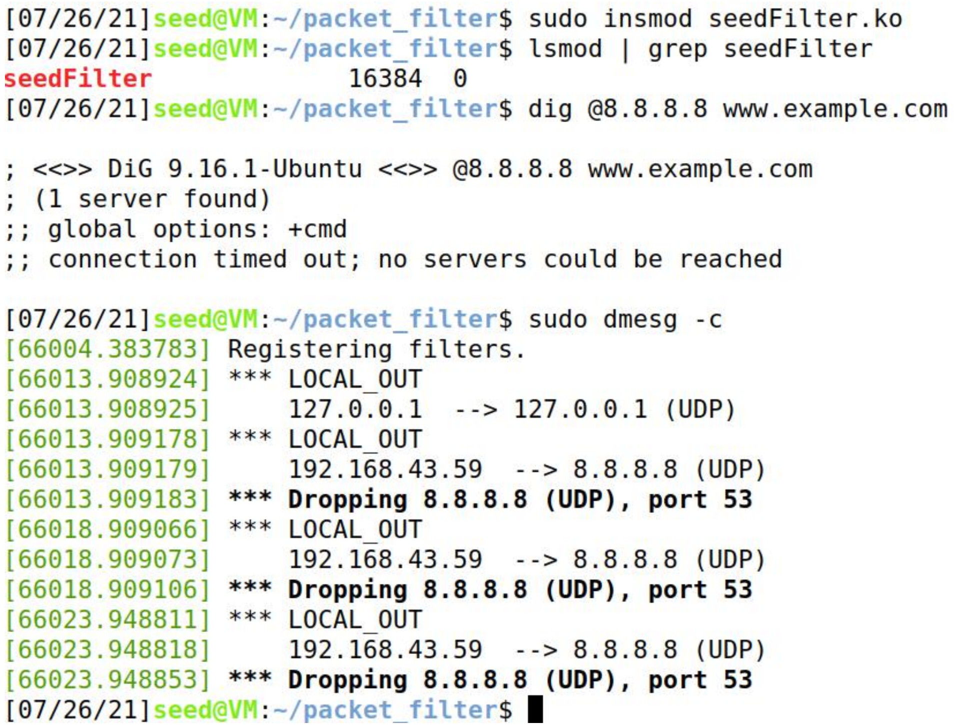
然后就进入路由代码，其决定该数据报是需要转发还是发给本机的；

② 若该数据报是发被本机的，则该数据经过 HOOK 函数 NF_IP_LOCAL_IN 处理以后然后传递给上层协议；

③ 若该数据报应该被转发则它被 NF_IP_FORWARD 处理；

④ 经过转发的数据报经过最后一个 HOOK 函数 NF_IP_POST_ROUTING 处理以后，再传输到网络上。

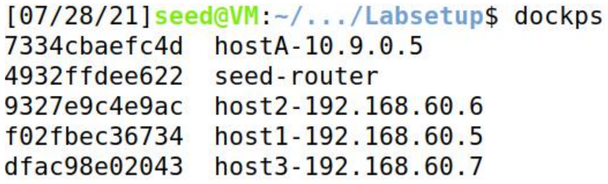
⑤ 本地产生的数据经过 HOOK 函数 NF_IP_LOCAL_OUT 处理后，进行路由选择处理，然后经过 NF_IP_POST_ROUTING 处理后发送出去。



```
[07/26/21]seed@VM:~/packet_filter$ sudo insmod seedFilter.ko
[07/26/21]seed@VM:~/packet_filter$ lsmod | grep seedFilter
seedFilter             16384  0
[07/26/21]seed@VM:~/packet_filter$ dig @8.8.8.8 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached

[07/26/21]seed@VM:~/packet_filter$ sudo dmesg -c
[66004.383783] Registering filters.
[66013.908924] *** LOCAL_OUT
[66013.908925]     127.0.0.1  --> 127.0.0.1 (UDP)
[66013.909178] *** LOCAL_OUT
[66013.909179]     192.168.43.59  --> 8.8.8.8 (UDP)
[66013.909183] *** Dropping 8.8.8.8 (UDP), port 53
[66018.909066] *** LOCAL_OUT
[66018.909073]     192.168.43.59  --> 8.8.8.8 (UDP)
[66018.909106] *** Dropping 8.8.8.8 (UDP), port 53
[66023.948811] *** LOCAL_OUT
[66023.948818]     192.168.43.59  --> 8.8.8.8 (UDP)
[66023.948853] *** Dropping 8.8.8.8 (UDP), port 53
[07/26/21]seed@VM:~/packet_filter$ 
```

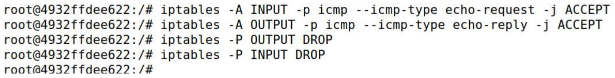
Task 2: Experimenting with Stateless Firewall Rules

Task 2.A: Protecting the Router



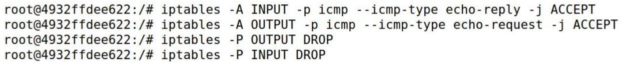
```
[07/28/21]seed@VM:~/.../Labsetup$ dockps
7334cbaefc4d  hostA-10.9.0.5
4932ffdee622  seed-router
9327e9c4e9ac  host2-192.168.60.6
f02fbec36734  host1-192.168.60.5
dfac98e02043  host3-192.168.60.7
```

输入以下命令，ping 和 telnet 都失败了。

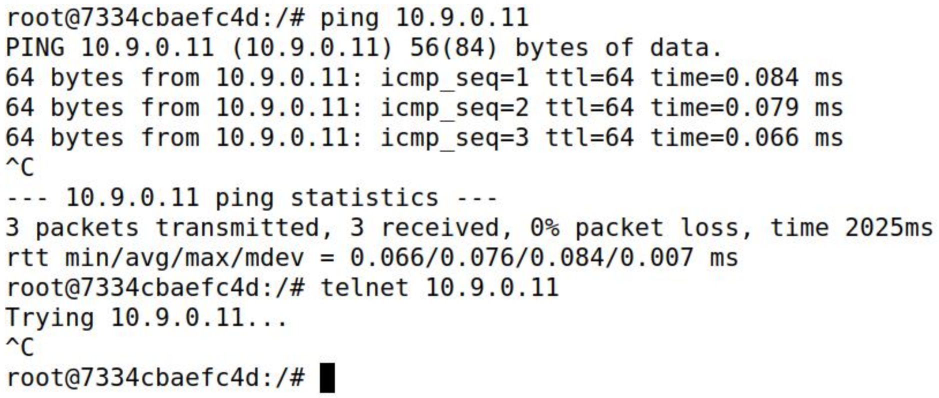


```
root@4932ffdee622:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@4932ffdee622:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@4932ffdee622:/# iptables -P OUTPUT DROP
root@4932ffdee622:/# iptables -P INPUT DROP
root@4932ffdee622:/#
```

顺序修改一下，ping 成功，telnet 失败。



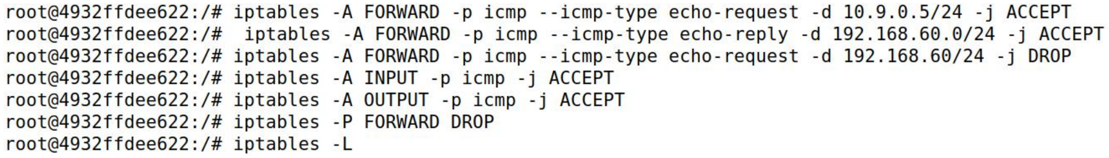
```
root@4932ffdee622:/# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@4932ffdee622:/# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
root@4932ffdee622:/# iptables -P OUTPUT DROP
root@4932ffdee622:/# iptables -P INPUT DROP
```



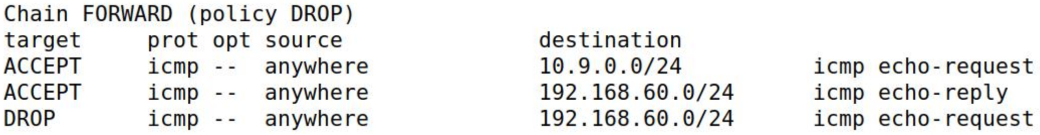
```
root@7334cbaefc4d:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.084 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.079 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.066 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.066/0.076/0.084/0.007 ms
root@7334cbaefc4d:/# telnet 10.9.0.11
Trying 10.9.0.11...
^C
root@7334cbaefc4d:/# █
```

Task 2.B: Protecting the Internal Network

输入以下命令。

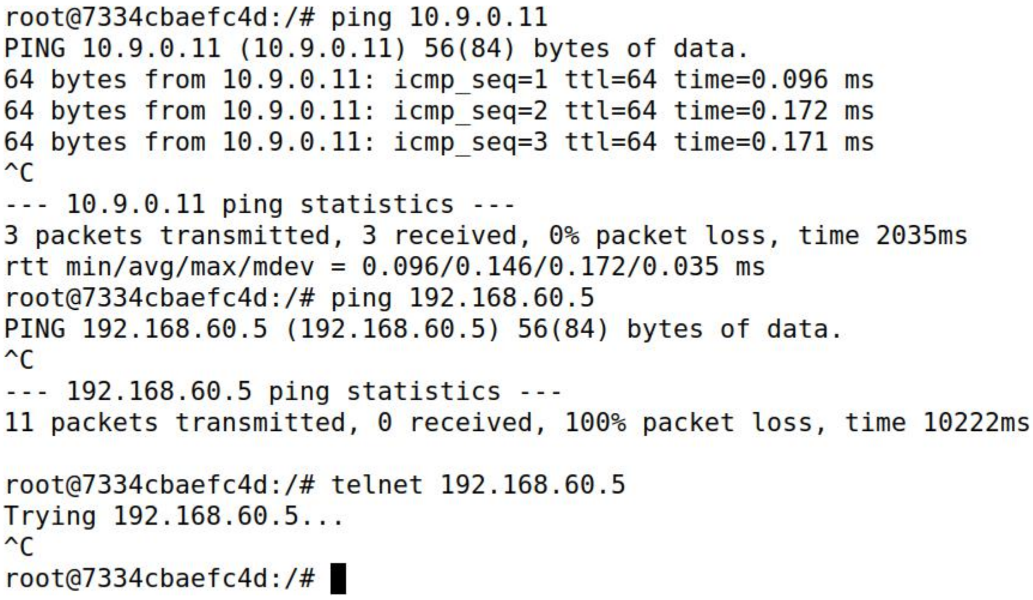


```
root@4932ffdee622:/# iptables -A FORWARD -p icmp --icmp-type echo-request -d 10.9.0.5/24 -j ACCEPT
root@4932ffdee622:/#  iptables -A FORWARD -p icmp --icmp-type echo-reply -d 192.168.60.0/24 -j ACCEPT
root@4932ffdee622:/# iptables -A FORWARD -p icmp --icmp-type echo-request -d 192.168.60/24 -j DROP
root@4932ffdee622:/# iptables -A INPUT -p icmp -j ACCEPT
root@4932ffdee622:/# iptables -A OUTPUT -p icmp -j ACCEPT
root@4932ffdee622:/# iptables -P FORWARD DROP
root@4932ffdee622:/# iptables -L
```



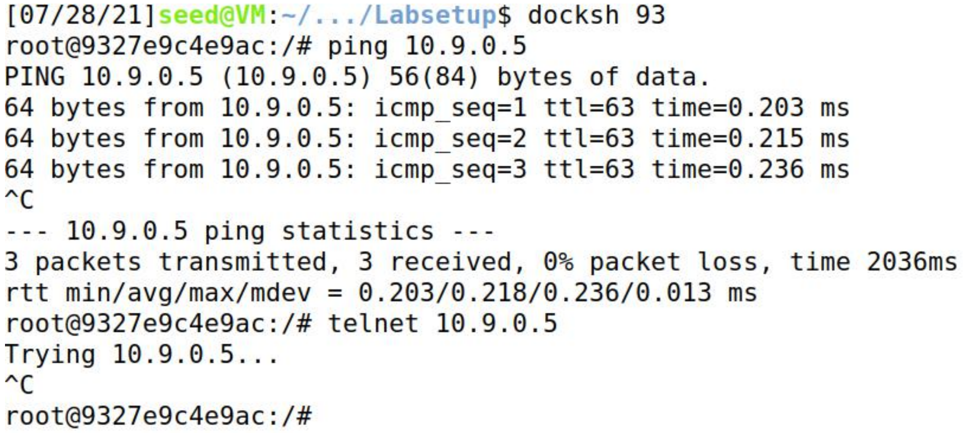
```
Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             10.9.0.0/24          icmp echo-request
ACCEPT     icmp --  anywhere             192.168.60.0/24      icmp echo-reply
DROP       icmp --  anywhere             192.168.60.0/24      icmp echo-request
```

从外部主机 ping 路由器，ping 成功。 ping 内部主机，ping 失败。telnet 内部主机，失败。



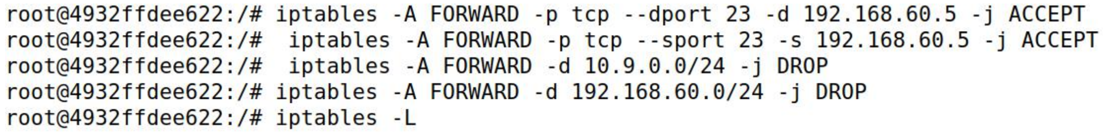
```
root@7334cbaefc4d:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.096 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.172 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.171 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.096/0.146/0.172/0.035 ms
root@7334cbaefc4d:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
^C
--- 192.168.60.5 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10222ms

root@7334cbaefc4d:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
root@7334cbaefc4d:/# █
```

内部主机 ping 外部主机，ping 成功。telnet 外部主机，失败。

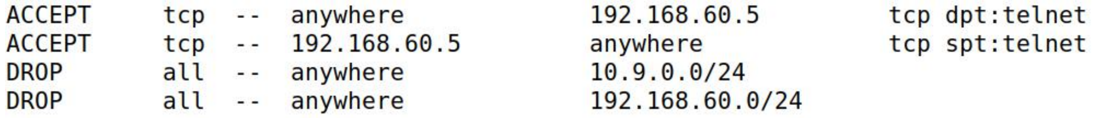


```
[07/28/21]seed@VM:~/.../Labsetup$ docksh 93
root@9327e9c4e9ac:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.203 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.215 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.236 ms
^C
--- 10.9.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2036ms
rtt min/avg/max/mdev = 0.203/0.218/0.236/0.013 ms
root@9327e9c4e9ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@9327e9c4e9ac:/#
```

Task 2.C: Protecting Internal Servers

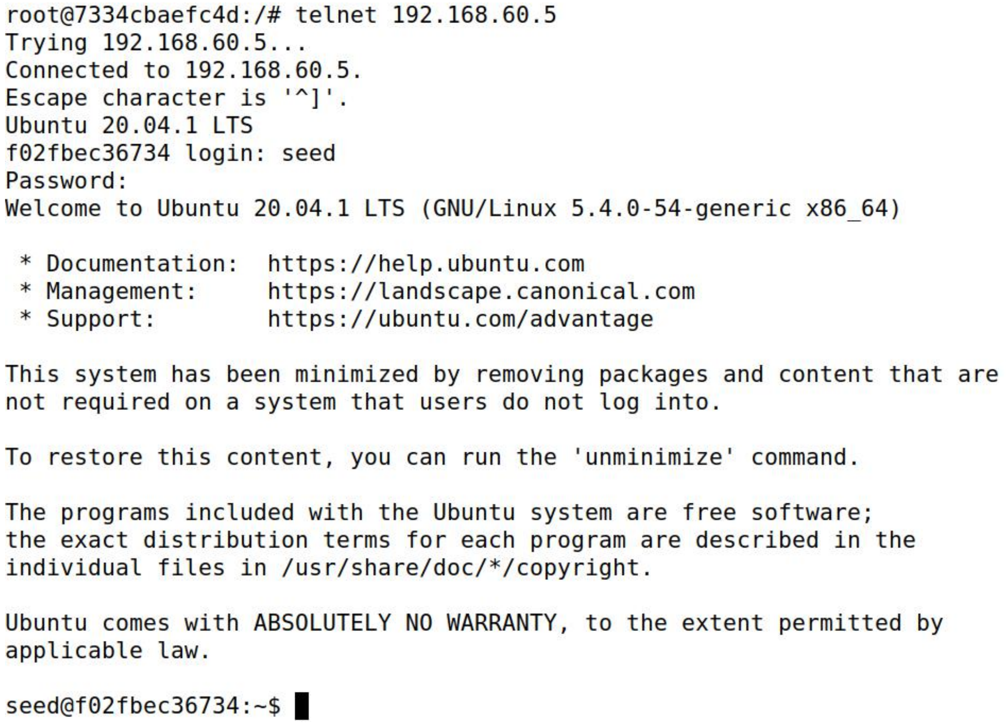


```
root@4932ffdee622:/# iptables -A FORWARD -p tcp --dport 23 -d 192.168.60.5 -j ACCEPT
root@4932ffdee622:/#  iptables -A FORWARD -p tcp --sport 23 -s 192.168.60.5 -j ACCEPT
root@4932ffdee622:/#  iptables -A FORWARD -d 10.9.0.0/24 -j DROP
root@4932ffdee622:/# iptables -A FORWARD -d 192.168.60.0/24 -j DROP
root@4932ffdee622:/# iptables -L
```



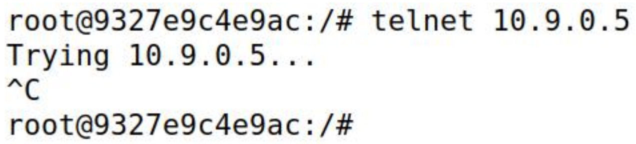
```
ACCEPT     tcp  --  anywhere             192.168.60.5         tcp dpt:telnet
ACCEPT     tcp  --  192.168.60.5         anywhere             tcp spt:telnet
DROP       all  --  anywhere             10.9.0.0/24
DROP       all  --  anywhere             192.168.60.0/24
```

从外部主机 telnet 内部主机，成功。



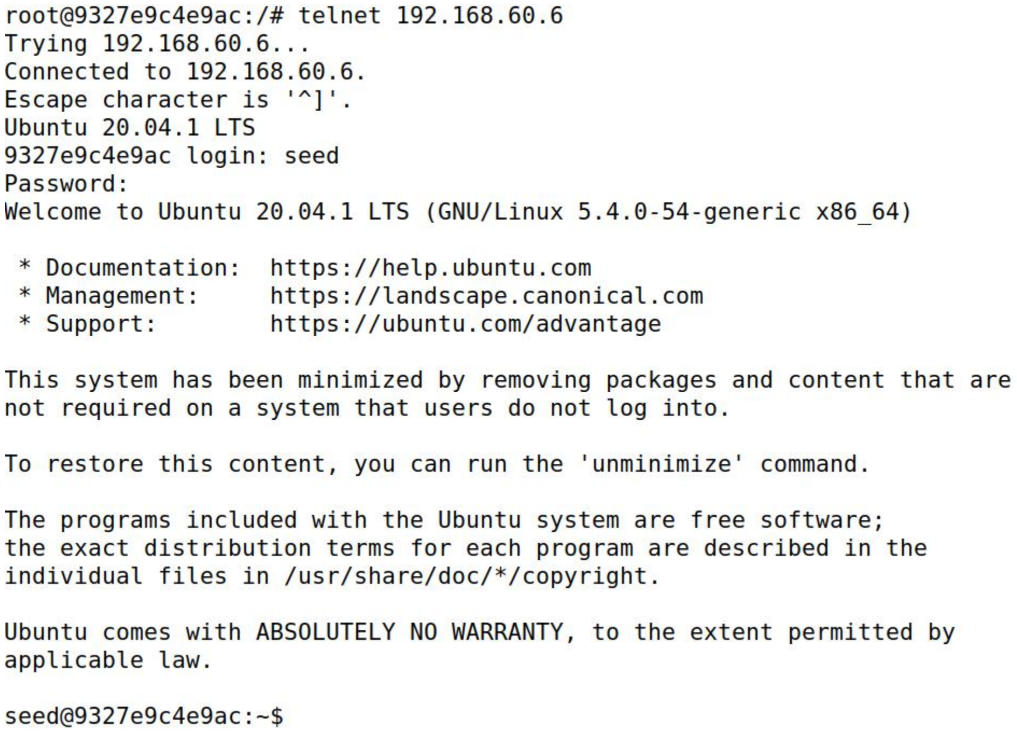
```
root@7334cbaefc4d:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f02fbec36734 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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@f02fbec36734:~$ █
```

外部主机 telnet 内部主机，失败。



```
root@9327e9c4e9ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@9327e9c4e9ac:/#
```

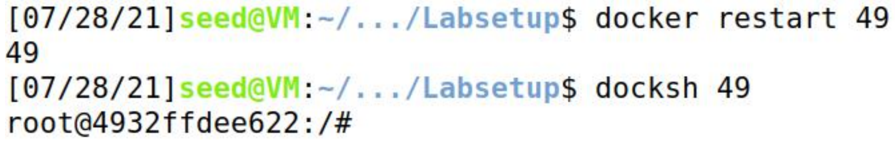
内部主机 telnet 内部主机，成功。



```
root@9327e9c4e9ac:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
9327e9c4e9ac 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@9327e9c4e9ac:~$
```

Task 3: Connection Tracking and Stateful Firewall

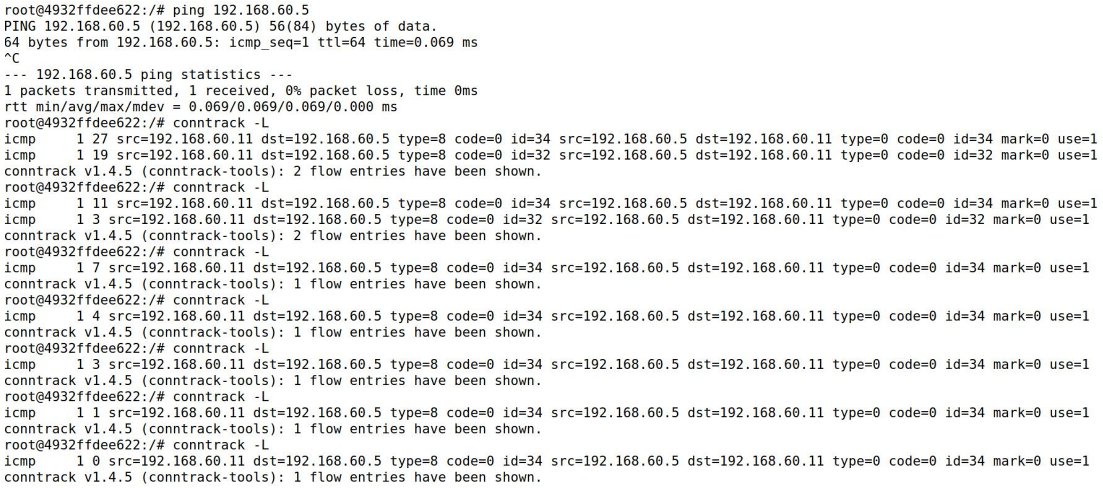
重启路由器容器。



```
[07/28/21]seed@VM:~/.../Labsetup$ docker restart 49
49
[07/28/21]seed@VM:~/.../Labsetup$ docksh 49
root@4932ffdee622:/#
```

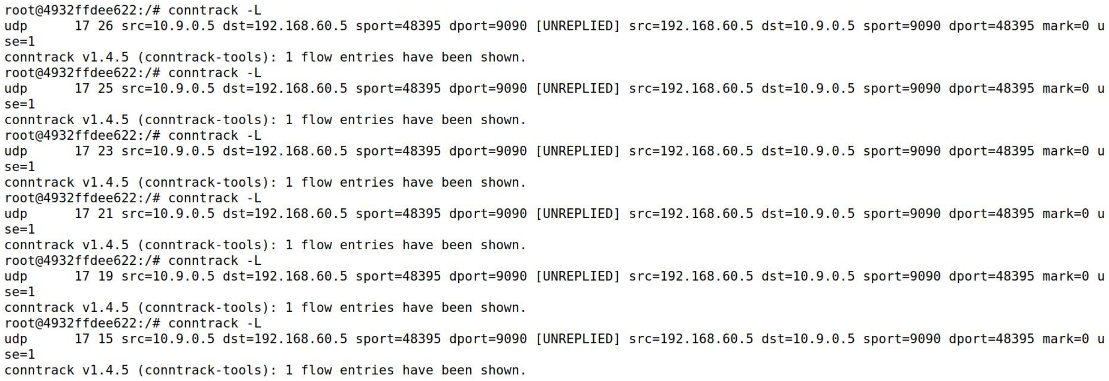
Task 3.A: Experiment with the Connection Tracking

ICMP 的连接状态保持在 25-30 秒。



```
root@4932ffdee622:/# 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=64 time=0.069 ms
^C
--- 192.168.60.5 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.069/0.069/0.069/0.000 ms
root@4932ffdee622:/# conntrack -L
icmp     1 27 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 mark=0 use=1
icmp     1 19 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=32 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=32 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
icmp     1 11 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 mark=0 use=1
icmp     1 3 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=32 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=32 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
icmp     1 7 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
icmp     1 4 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
icmp     1 3 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
icmp     1 1 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
icmp     1 0 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

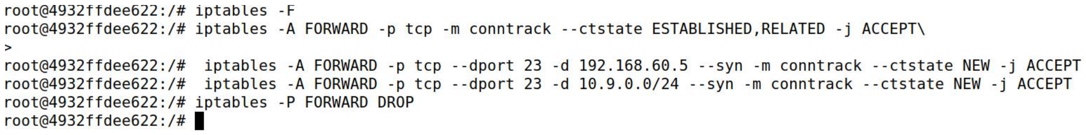
udp 连接状态保持在 25-30 秒。



```
root@4932ffdee622:/# conntrack -L
udp      17 26 src=10.9.0.5 dst=192.168.60.5 sport=48395 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=48395 mark=0 u
se=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
udp      17 25 src=10.9.0.5 dst=192.168.60.5 sport=48395 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=48395 mark=0 u
se=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
udp      17 23 src=10.9.0.5 dst=192.168.60.5 sport=48395 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=48395 mark=0 u
se=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
udp      17 21 src=10.9.0.5 dst=192.168.60.5 sport=48395 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=48395 mark=0 u
se=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
udp      17 19 src=10.9.0.5 dst=192.168.60.5 sport=48395 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=48395 mark=0 u
se=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@4932ffdee622:/# conntrack -L
udp      17 15 src=10.9.0.5 dst=192.168.60.5 sport=48395 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=48395 mark=0 u
se=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

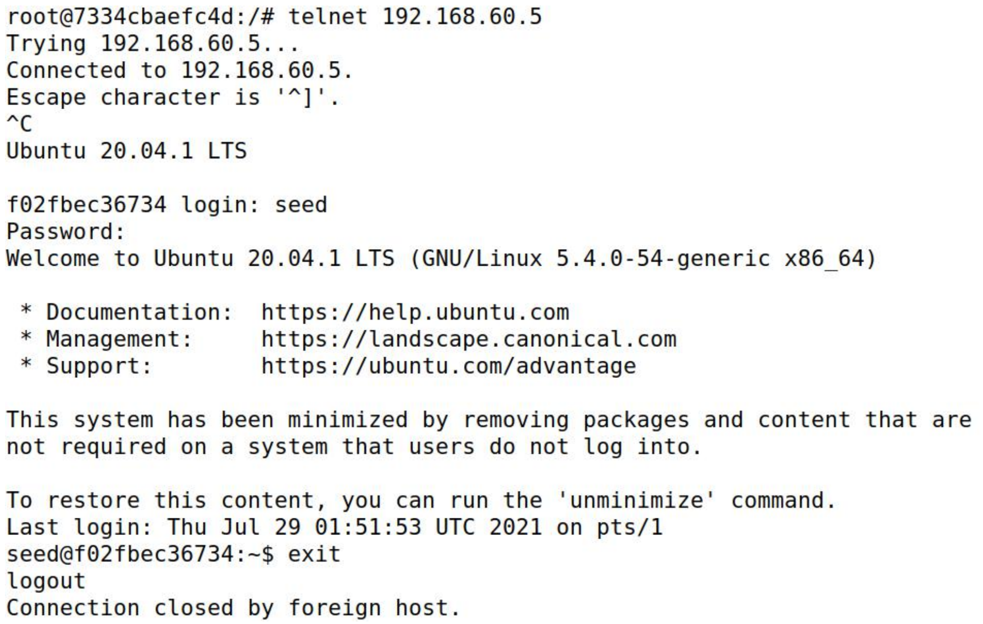
TCP 的连接状态保持时间大约为 430000 秒。

Task 3.B: Setting Up a Stateful Firewall

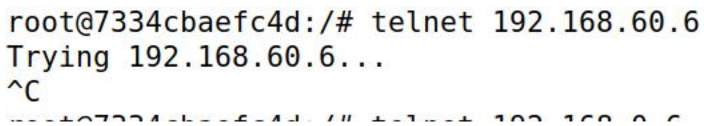


```
root@4932ffdee622:/# iptables -F
root@4932ffdee622:/# iptables -A FORWARD -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT\
>
root@4932ffdee622:/#  iptables -A FORWARD -p tcp --dport 23 -d 192.168.60.5 --syn -m conntrack --ctstate NEW -j ACCEPT
root@4932ffdee622:/#  iptables -A FORWARD -p tcp --dport 23 -d 10.9.0.0/24 --syn -m conntrack --ctstate NEW -j ACCEPT
root@4932ffdee622:/# iptables -P FORWARD DROP
root@4932ffdee622:/# █
```

外部主机 telnet 内部主机 192.168.60.5 成功，telnet 192.168.60.6 失败。

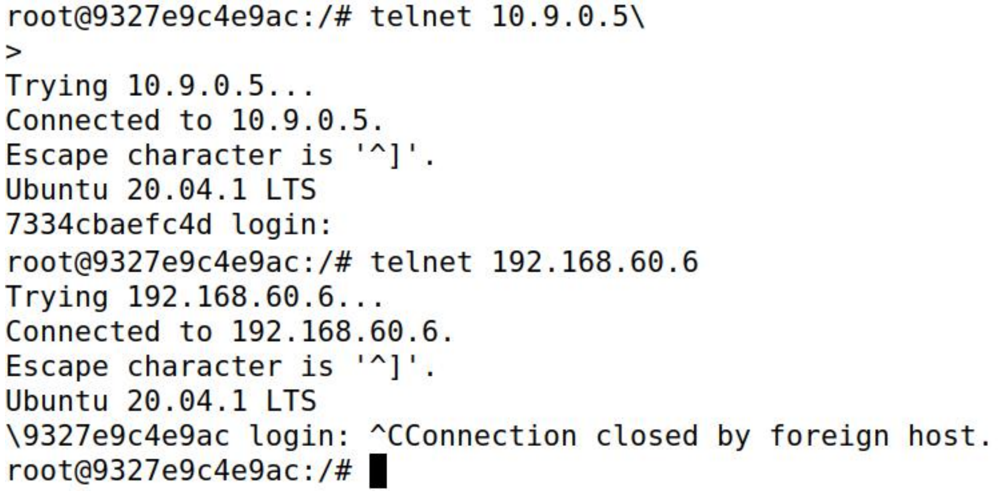


```
root@7334cbaefc4d:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
^C
Ubuntu 20.04.1 LTS

f02fbec36734 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.
Last login: Thu Jul 29 01:51:53 UTC 2021 on pts/1
seed@f02fbec36734:~$ exit
logout
Connection closed by foreign host.
```



```
root@7334cbaefc4d:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
```

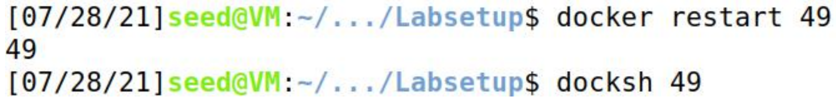
内部主机 192.168.60.5 telnet 外部主机 10.9.0.5 和内部主机 192.168.60.6 都成功。



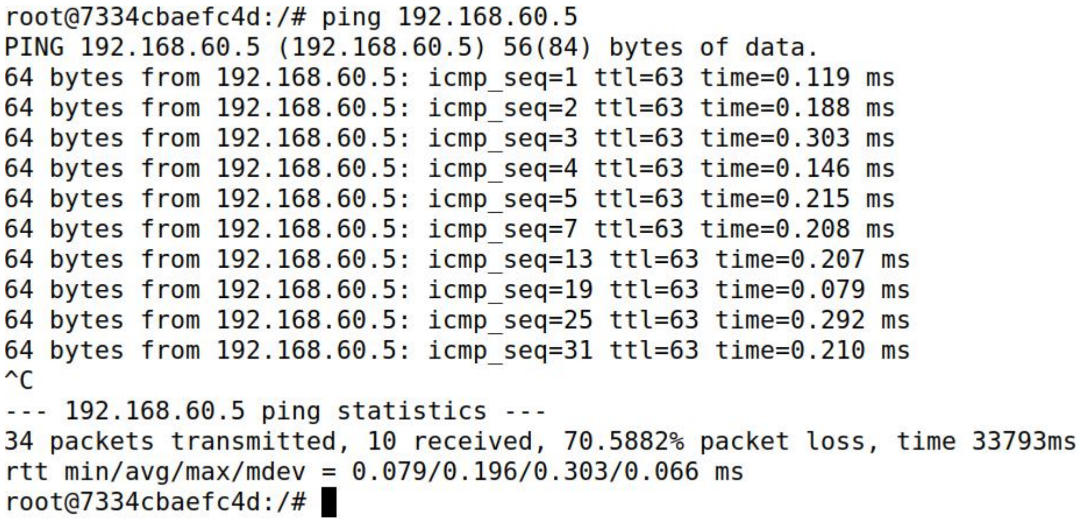
```
root@9327e9c4e9ac:/# telnet 10.9.0.5\
>
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7334cbaefc4d login:
root@9327e9c4e9ac:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
\9327e9c4e9ac login: ^CConnection closed by foreign host.
root@9327e9c4e9ac:/# 
```

Task 4: Limiting Network Traffific

重启路由器容器。



```
[07/28/21]seed@VM:~/.../Labsetup$ docker restart 49
49
[07/28/21]seed@VM:~/.../Labsetup$ docksh 49
```

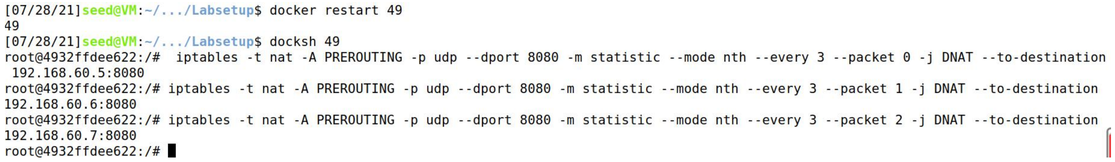


```
root@7334cbaefc4d:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.119 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.188 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.303 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.146 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.215 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.208 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.207 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.079 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.292 ms
64 bytes from 192.168.60.5: icmp_seq=31 ttl=63 time=0.210 ms
^C
--- 192.168.60.5 ping statistics ---
34 packets transmitted, 10 received, 70.5882% packet loss, time 33793ms
rtt min/avg/max/mdev = 0.079/0.196/0.303/0.066 ms
root@7334cbaefc4d:/# 
```

可以体会到前六个包发送很快。

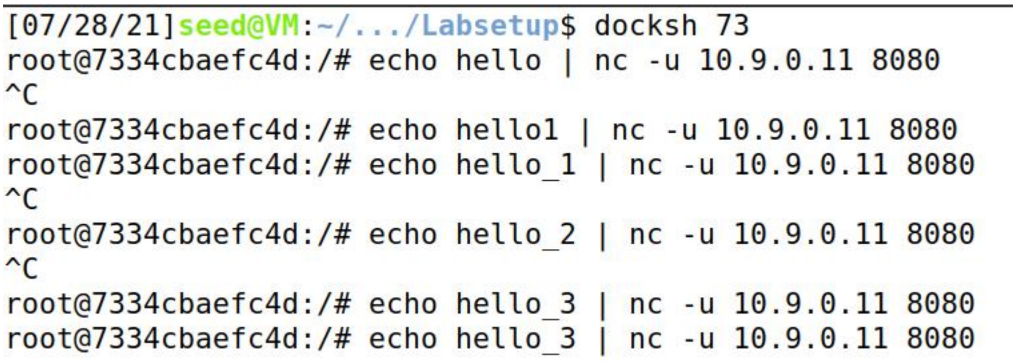
若只执行第一条命令，从外部 (10.9.0.5)ping 192.168.60.5 ， 和平时的发包速度一样。因为 iptables 默认的 FORWARD 表是接受所有包，所以如果不写第二条命令，发包会正常进行。

Task 5: Load Balancing

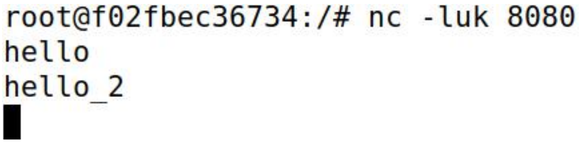


```
[07/28/21]seed@VM:~/.../Labsetup$ docker restart 49
49
[07/28/21]seed@VM:~/.../Labsetup$ docksh 49
root@4932ffdee622:/#  iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-destination
 192.168.60.5:8080
root@4932ffdee622:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 1 -j DNAT --to-destination
192.168.60.6:8080
root@4932ffdee622:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 2 -j DNAT --to-destination
192.168.60.7:8080
root@4932ffdee622:/# 
```

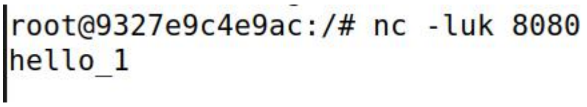
虽然是等概率发送数据，但每个主机收到的数量各不相同，甚至有的差异较大，当样本数量足够多时， 应该是趋于平均的。



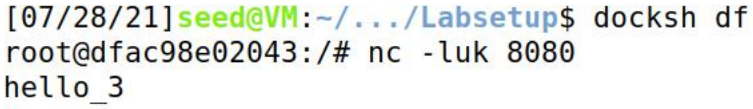
```
[07/28/21]seed@VM:~/.../Labsetup$ docksh 73
root@7334cbaefc4d:/# echo hello | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello1 | nc -u 10.9.0.11 8080
root@7334cbaefc4d:/# echo hello_1 | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_2 | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_3 | nc -u 10.9.0.11 8080
root@7334cbaefc4d:/# echo hello_3 | nc -u 10.9.0.11 8080
```



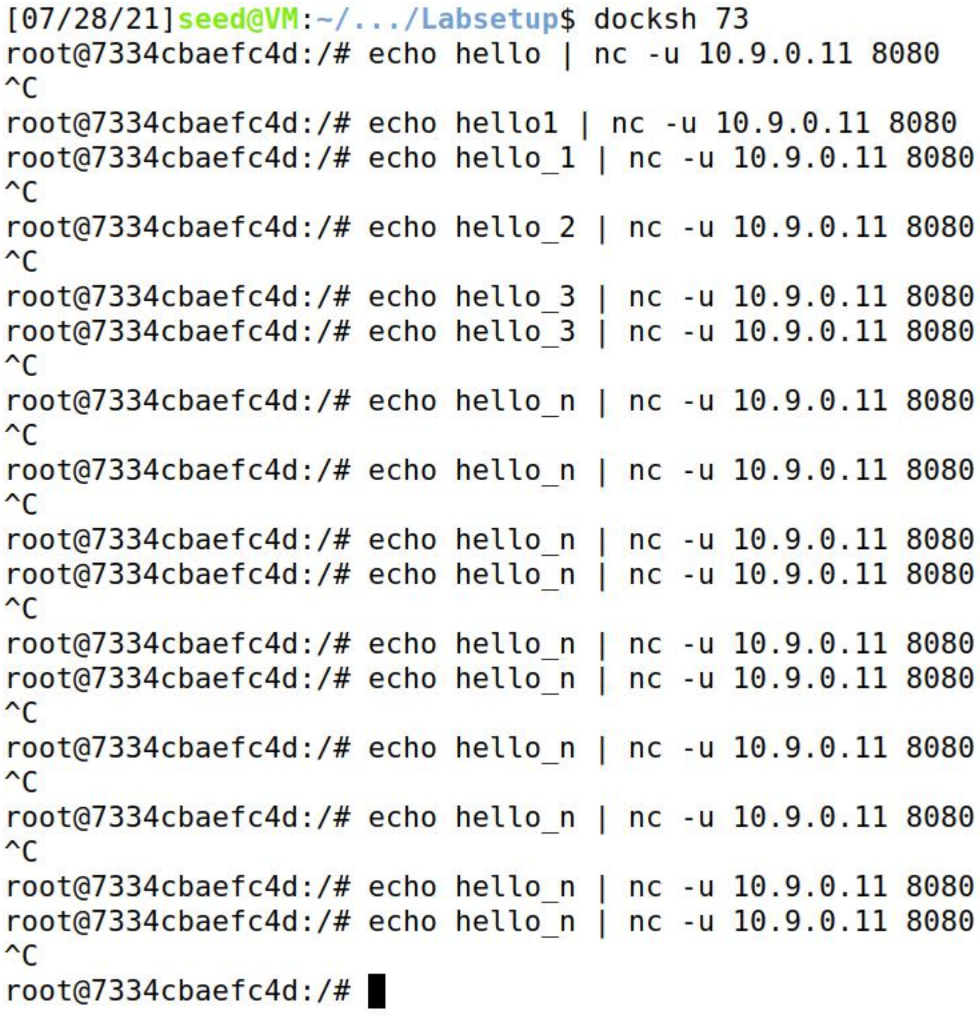
```
root@f02fbec36734:/# nc -luk 8080
hello
hello_2
```



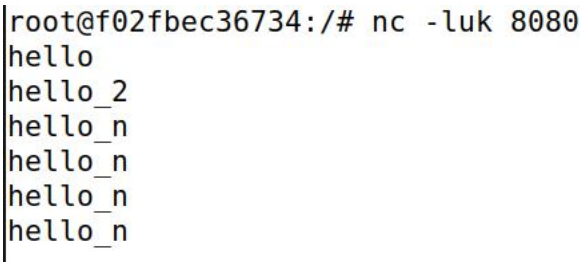
```
root@9327e9c4e9ac:/# nc -luk 8080
hello_1
```



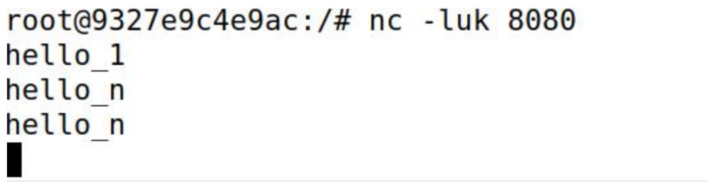
```
[07/28/21]seed@VM:~/.../Labsetup$ docksh df
root@dfac98e02043:/# nc -luk 8080
hello_3
```



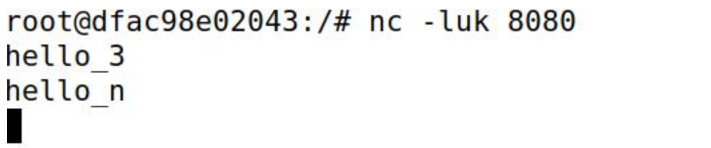
```
[07/28/21]seed@VM:~/.../Labsetup$ docksh 73
root@7334cbaefc4d:/# echo hello | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello1 | nc -u 10.9.0.11 8080
root@7334cbaefc4d:/# echo hello_1 | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_2 | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_3 | nc -u 10.9.0.11 8080
root@7334cbaefc4d:/# echo hello_3 | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
root@7334cbaefc4d:/# echo hello_n | nc -u 10.9.0.11 8080
^C
root@7334cbaefc4d:/# 
```



```
root@f02fbec36734:/# nc -luk 8080
hello
hello_2
hello_n
hello_n
hello_n
hello_n
```



```
root@9327e9c4e9ac:/# nc -luk 8080
hello_1
hello_n
hello_n
```



```
root@dfac98e02043:/# nc -luk 8080
hello_3
hello_n
```