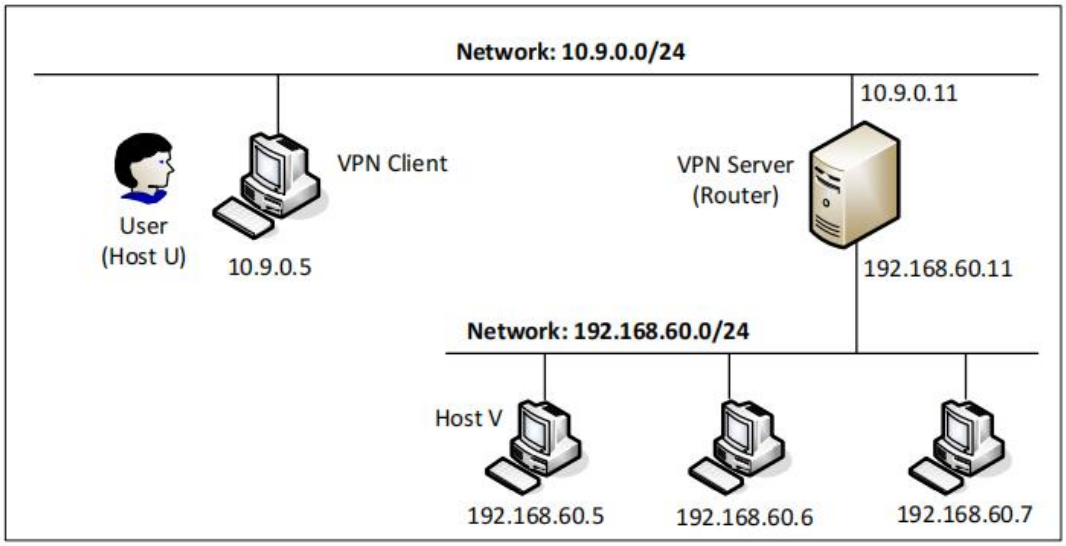
VPN Lab: The Container Version

57118214 陈佳杰

Task 1: Network Setup

实验环境如下图所示



Task 2: Create and Confifigure TUN Interface

Task 2.a: Name of the Interface

在 10.9.0.5 上运行 tun.py

```
root@52b71d779f85:/volumes#  chmod a+x tun.py
root@52b71d779f85:/volumes#  tun.py
Interface Name: tun0
```

可以看到新的接口，用姓氏 chen 作为接口名

```
3: chen0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group def
ault qlen 500
    link/none
```

Task 2.b: Set up the TUN Interface

在 tun.py 中添加两行代码

```
23 os.system("ip addr add 192.168.53.99/24 dev {}".format(ifname))
24 os.system("ip link set dev {} up".format(ifname))
```

再次运行后看到接口有了具体的网段

```
4: chen0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel stat
e UNKNOWN group default qlen 500
    link/none
    inet 192.168.53.99/24 scope global chen0
       valid_lft forever preferred_lft forever
```

Task 2.c: Read from the TUN Interface

修改 tun.py

```
26 while True:
27 # Get a packet from the tun interface
28     packet = os.read(tun, 2048)
29     if packet:
30         ip = IP(packet)
31         print(ip.summary())
```

在运行程序的同时 ping 192.168.53.1，程序输出 ICMP 报文

```
root@52b71d779f85:/volumes#  tun.py
Interface Name: chen0
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
```

但是 ping 192.168.60.5 程序没有输出

```
root@52b71d779f85:/# ping 192.168.53.1
PING 192.168.53.1 (192.168.53.1) 56(84) bytes of data.
^C
--- 192.168.53.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3058ms

root@52b71d779f85:/# 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 ---
4 packets transmitted, 0 received, 100% packet loss, time 3060ms
```

因为程序抓取的是经过 chen0 端口，即 192.168.53.99/24 网段的报文

Task 2.d: Write to the TUN Interface

修改 tun.py 构造回复包

```
while True:
# Get a packet from the tun interface
    packet = os.read(tun, 2048)
    if packet:
        ip = IP(packet)
        print(ip.summary())
        newip = IP(src=ip.dst, dst=ip.src)
        newpkt = newip/ip.payload
        os.write(tun, bytes(newpkt))
```

收到了回复，程序也有输出

```
root@52b71d779f85:/# ping 192.168.53.1
PING 192.168.53.1 (192.168.53.1) 56(84) bytes of data.
64 bytes from 192.168.53.1: icmp_seq=1 ttl=64 time=2.31 ms
64 bytes from 192.168.53.1: icmp_seq=2 ttl=64 time=3.19 ms
64 bytes from 192.168.53.1: icmp_seq=3 ttl=64 time=2.02 ms
64 bytes from 192.168.53.1: icmp_seq=4 ttl=64 time=3.03 ms
^C
--- 192.168.53.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.018/2.637/3.189/0.486 ms
```

```
root@52b71d779f85:/volumes#  tun.py
Interface Name: chen0
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-reply 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-reply 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-reply 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-reply 0 / Raw
```

Task 3: Send the IP Packet to VPN Server Through a Tunnel

tun_client.py

```
os.system("ip addr add 192.168.53.99/24 dev {}".format(ifname))
os.system("ip link set dev {} up".format(ifname))
os.system("ip route add 192.168.60.0/24 dev {}".format(ifname))

sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
SERVER_IP="10.9.0.11"
SERVER_PORT=9090

while True:
  packet = os.read(tun, 2048)
  if packet:
    pkt = IP(packet)
    print(pkt.summary())
    sock.sendto(packet,(SERVER_IP, SERVER_PORT))
```

tun_sever.py

```
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock.bind((IP_A, PORT))

while True:
   data, (ip, port) = sock.recvfrom(2048)
   print("{}:{} --> {}:{}".format(ip, port, IP_A, PORT))
   pkt = IP(data)
   print(" Inside: {} --> {}".format(pkt.src, pkt.dst))
```

Ping 192.168.60.5 和 192.168.53.1 的输出如下

```
root@52b71d779f85:/volumes# python3 tun_client.py
Interface Name: chen0
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.53.1 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.60.5 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.60.5 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.60.5 echo-request 0 / Raw
IP / ICMP 192.168.53.99 > 192.168.60.5 echo-request 0 / Raw
```

```
root@cec5ca57d021:/volumes# python3 tun_server.py
10.9.0.5:57206 --> 0.0.0.0:9090
 Inside: 192.168.53.99 --> 192.168.53.1
10.9.0.5:57206 --> 0.0.0.0:9090
 Inside: 192.168.53.99 --> 192.168.53.1
10.9.0.5:57206 --> 0.0.0.0:9090
 Inside: 192.168.53.99 --> 192.168.53.1
10.9.0.5:57206 --> 0.0.0.0:9090
 Inside: 192.168.53.99 --> 192.168.53.1
10.9.0.5:57206 --> 0.0.0.0:9090
 Inside: 192.168.53.99 --> 192.168.60.5
10.9.0.5:57206 --> 0.0.0.0:9090
 Inside: 192.168.53.99 --> 192.168.60.5
10.9.0.5:57206 --> 0.0.0.0:9090
 Inside: 192.168.53.99 --> 192.168.60.5
10.9.0.5:57206 --> 0.0.0.0:9090
 Inside: 192.168.53.99 --> 192.168.60.5
```

Task 4: Set Up the VPN Server

修改 tun_server.py

```
15 ifname = ifname_bytes.decode('UTF-8')[:16].strip("\x00")
16 print("Interface Name: {}".format(ifname))
17
18 os.system("ip addr add 192.168.11.99/24 dev {}".format(ifname))
19 os.system("ip link set dev {} up".format(ifname))
20
21 server = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
22 SERVER_IP = "0.0.0.0"
23 SERVER_PORT = 9090
24 server.bind((SERVER_IP,SERVER_PORT))
25
26 while True:
27     data, (ip, port) = server.recvfrom(2048)
28     print("{}:{} --> {}:{}".format(ip, port, SERVER_IP, SERVER_PORT))
29     pkt = IP(data)
30     print(" Inside: {} --> {}".format(pkt.src, pkt.dst))
31     os.write(tun,data)
32
```

运行 tcpdump 进行抓包

```
root@cec5ca57d021:/# tcpdump -nni eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
14:02:06.919559 IP 192.168.53.99 > 192.168.60.5: ICMP echo request, id 114, seq
1, length 64
14:02:06.919589 IP 192.168.60.5 > 192.168.53.99: ICMP echo reply, id 114, seq 1,
 length 64
14:02:07.932786 IP 192.168.53.99 > 192.168.60.5: ICMP echo request, id 114, seq
2, length 64
14:02:07.932837 IP 192.168.60.5 > 192.168.53.99: ICMP echo reply, id 114, seq 2,
 length 64
14:02:08.956930 IP 192.168.53.99 > 192.168.60.5: ICMP echo request, id 114, seq
3, length 64
14:02:08.956981 IP 192.168.60.5 > 192.168.53.99: ICMP echo reply, id 114, seq 3,
 length 64
14:02:09.982655 IP 192.168.53.99 > 192.168.60.5: ICMP echo request, id 114, seq
4, length 64
14:02:09.982734 IP 192.168.60.5 > 192.168.53.99: ICMP echo reply, id 114, seq 4,
 length 64
```

可以看到 VPN 服务器在接收到 ICMP 报文后会将其转发给 Host V

Task 5: Handling Traffific in Both Directions

Client

```
while True:
  ready, _, _ = select.select([sock, tun], [], [])
  for fd in ready:
     if fd is sock:
        data, (ip, port) = sock.recvfrom(2048)
        pkt = IP(data)
        print("From socket <==: {} --> {}".format(pkt.src, pkt.dst))

        os.write(tun, bytes(pkt))
     if fd is tun:
        packet = os.read(tun, 2048)
        pkt = IP(packet)
        print("From tun ==>: {} --> {}".format(pkt.src, pkt.dst))
        sock.sendto(packet, ('10.9.0.11', 9090))
```

Server

```
while True:
   ready, _, _ = select.select([sock, tun], [], [])
   for fd in ready:
      if fd is sock:
         data, (ip, port) = sock.recvfrom(2048) a
         pkt = IP(data)
         print("From socket <==: {} --> {}".format(pkt.src, pkt.dst))
         os.write(tun, bytes(pkt))

      if fd is tun:
         packet = os.read(tun, 2048)
         pkt = IP(packet)
         print("From tun ==>: {} --> {}".format(pkt.src, pkt.dst))
         sock.sendto(packet, ('10.9.0.5', 9090))
```

运行之后可以 ping 通

```
root@52b71d779f85:/# 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=3.31 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=1.84 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=2.71 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=2.11 ms
^C
--- 192.168.60.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
```

```
root@52b71d779f85:/volumes# python3 tun_client.py
Interface Name: chen0
From tun ==>: 192.168.53.99 --> 192.168.60.5
From socket <==: 192.168.60.5 --> 192.168.53.99
From tun ==>: 192.168.53.99 --> 192.168.60.5
From socket <==: 192.168.60.5 --> 192.168.53.99
From tun ==>: 192.168.53.99 --> 192.168.60.5
From socket <==: 192.168.60.5 --> 192.168.53.99
From tun ==>: 192.168.53.99 --> 192.168.60.5
From socket <==: 192.168.60.5 --> 192.168.53.99
```

```
root@cec5ca57d021:/volumes# python3 tun_server.py
Interface Name: chen0
From socket <==: 192.168.53.99 --> 192.168.60.5
From tun ==>: 192.168.60.5 --> 192.168.53.99
From socket <==: 192.168.53.99 --> 192.168.60.5
From tun ==>: 192.168.60.5 --> 192.168.53.99
From socket <==: 192.168.53.99 --> 192.168.60.5
From tun ==>: 192.168.60.5 --> 192.168.53.99
From socket <==: 192.168.53.99 --> 192.168.60.5
From tun ==>: 192.168.60.5 --> 192.168.53.99
```

Task 6: Tunnel-Breaking Experiment

建立 telnet 连接

```
seed@45991e963406:~$ ls
seed@45991e963406:~$ cd ..
seed@45991e963406:/home$ cd ..
seed@45991e963406:/$ ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr
seed@45991e963406:/$
```

然后停止运行程序，断开 telnet 连接后发现输入无法显示
再次运行程序后，之前输入的内容会显示出来

```
seed@45991e963406:~$ ls
seed@45991e963406:~$ cd ..
seed@45991e963406:/home$ cd ..
seed@45991e963406:/$ ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr
seed@45991e963406:/$ ls -al
total 68
drwxr-xr-x   1 root root 4096 Jul 27 12:51 .
drwxr-xr-x   1 root root 4096 Jul 27 12:51 ..
-rwxr-xr-x   1 root root    0 Jul 27 12:51 .dockerenv
lrwxrwxrwx   1 root root    7 Nov  6  2020 bin -> usr/bin
drwxr-xr-x   2 root root 4096 Apr 15  2020 boot
drwxr-xr-x   5 root root  360 Jul 27 12:51 dev
drwxr-xr-x   1 root root 4096 Jul 27 12:51 etc
drwxr-xr-x   1 root root 4096 Nov 26  2020 home
lrwxrwxrwx   1 root root    7 Nov  6  2020 lib -> usr/lib
```

```
From tun ==>: 192.168.60.5 --> 192.168.53.99
From socket <==: 192.168.53.99 --> 192.168.60.5
^CTraceback (most recent call last):
  File "tun_server.py", line 27, in <module>
    ready,  ,   = select.select([sock, tun], [], [])
KeyboardInterrupt

root@cec5ca57d021:/volumes# python3 tun_server.py
Interface Name: chen0
From socket <==: 192.168.53.99 --> 192.168.60.5
From tun ==>: 192.168.60.5 --> 192.168.53.99
```