Thiết kế & triển khai mạng IP

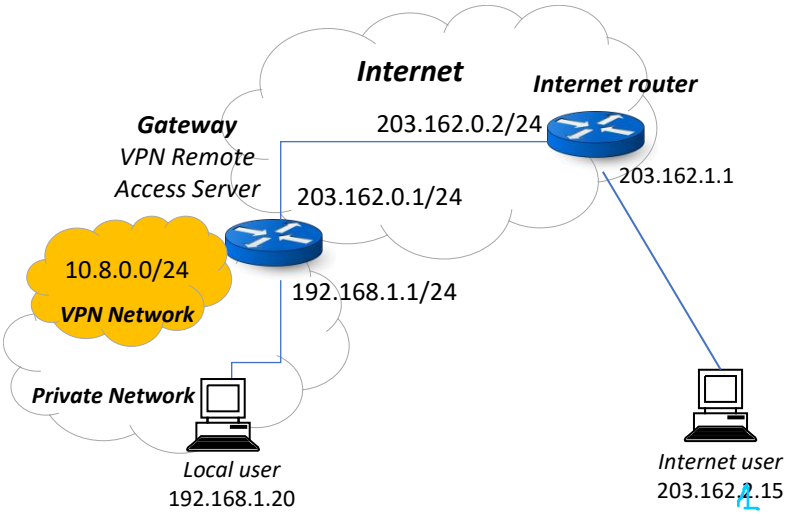
Bài thực hành: VPN

Mục lục

Contents

1 Thực hành host-to-net VPN

1.1 Sơ đồ mạng giả lập Internet



Sử dụng kiến thức bài thực hành trước, giả lập mạng Internet:

- Internet router: 203.162.0.2/24 & 203.162.1.1/24
- Internet user: 203.162.1.15/24, default gateway là 203.162.1.1
- Gateway của mạng nội bộ kết nối Internet: 203.1262.0.1/24
- Local user mạng nội bộ: 192.168.1.20/24, default gateway là 192.168.1.1
- Ping thành công từ Internet user đến Gateway của mạng nội bộ:

```
IntUser$ ping 203.162.0.1
PING 203.162.0.1 (203.162.0.1) 56(84) bytes of data.
64 bytes from 203.162.0.1: icmp_seq=1 ttl=63 time=2.56 ms
64 bytes from 203.162.0.1: icmp_seq=2 ttl=63 time=1.38 ms
64 bytes from 203.162.0.1: icmp_seq=3 ttl=63 time=1.35 ms
```

- Ping không thành công từ Internet user đến Local user của mạng nội bộ:

```
IntUser$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
From 203.162.1.1 icmp_seq=1 Destination Net Unreachable
From 203.162.1.1 icmp_seq=2 Destination Net Unreachable
From 203.162.1.1 icmp_seq=3 Destination Net Unreachable
From 203.162.1.1 icmp_seq=4 Destination Net Unreachable
```

1.2 Cài đặt & cấu hình VPN Remote Access cho Gateway

1. Thiết lập một kết nối NAT cho máy ảo Gateway để kết nối được với Internet, phục vụ cài đặt OpenVPN.
2. Download script cài đặt & cấu hình OpenVPN:

```
$ wget https://git.io/vpn -O openvpn-install.sh
HTTP request sent, awaiting response... 200 OK
Length: 23501 (23K) [text/plain]
Saving to: 'openvpn-install.sh'

openvpn-install.sh      100%[=========================>]  22.95K  --.-KB/s    in 0.003s

$ chmod +x ./openvpn-install.sh
```

3. Chạy script cài đặt OpenVPN và tạo file xác thực cho client:

```
$ sudo ./openvpn-install.sh
Which IPv4 address should be used?
     1) 203.162.0.1
     2) 192.168.1.1
IPv4 address [1]: 1

Which protocol should OpenVPN use?
   1) UDP (recommended)
   2) TCP
Protocol [1]:

What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
   1) Current system resolvers
   2) Google
   3) 1.1.1.1
   4) OpenDNS
   5) Quad9
   6) AdGuard
DNS server [1]:

Enter a name for the first client:
Name [client]:

OpenVPN installation is ready to begin.
. . . . .
Finished!

The client configuration is available in: /root/client.ovpn
New clients can be added by running this script again.
```

4. Kiểm tra trạng thái OpenVPN server sau khi cài đặt thành công:

```
$ sudo systemctl status openvpn-server@server.service
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; vendor preset:
en>
     Active: active (running) since Fri 2021-09-17 06:44:04 UTC; 3min 21s ago
```

```
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 2906 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 1071)
     Memory: 1.0M
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
             └─2906 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --
statu>

Sep 17 06:44:04 gateway openvpn[2906]: Could not determine IPv4/IPv6 protocol. Using
AF_INET
Sep 17 06:44:04 gateway openvpn[2906]: Socket Buffers: R=[212992->212992] S=[212992-
>212992]
Sep 17 06:44:04 gateway openvpn[2906]: UDPv4 link local (bound): [AF_INET]10.10.10.1:1194
Sep 17 06:44:04 gateway openvpn[2906]: UDPv4 link remote: [AF_UNSPEC]
Sep 17 06:44:04 gateway openvpn[2906]: GID set to nogroup
Sep 17 06:44:04 gateway openvpn[2906]: UID set to nobody
Sep 17 06:44:04 gateway openvpn[2906]: MULTI: multi_init called, r=256 v=256
Sep 17 06:44:04 gateway openvpn[2906]: IFCONFIG POOL: base=10.8.0.2 size=252, ipv6=0
Sep 17 06:44:04 gateway openvpn[2906]: IFCONFIG POOL LIST
Sep 17 06:44:04 gateway openvpn[2906]: Initialization Sequence Completed
```

5. Kiểm tra giao diện kết nối đường hầm VPN *tun0* được khởi tạo và thiết lập dải địa chỉ VPN (10.8.0.0/24):

```
$ ifconfig -a

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.1  netmask 255.255.255.0  destination 10.8.0.1
        inet6 fe80::f4b7:38b2:9a5a:679d  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 336 (336.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

6. Khi cần có thể stop hoặc start lại service OpenVPN, giao diện kết nối VPN *tun0* cũng được hủy bỏ khi dừng service :

```
$ sudo systemctl stop openvpn-server@server.service
$ ifconfig tun0
tun0: error fetching interface information: Device not found
$ sudo systemctl start openvpn-server@server.service
$ ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.1  netmask 255.255.255.0  destination 10.8.0.1
        inet6 fe80::3d9b:e1f2:d595:1f0e  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1  bytes 48 (48.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

7. Kiểm tra file xác thực VPN client *client.ovpn* đã được tạo ra trong thư mục */root*:

```
~$ sudo ls -l /root
-rw-r--r-- 1 root root 4990 Sep 17 07:10 client.ovpn
```

8. Để tạo thêm file xác thực VNP cho người dùng mới, chạy scrip và chọn “Add a new client”:

```
$ sudo ./openvpn-install.sh
OpenVPN is already installed.

Select an option:
   1) Add a new client
   2) Revoke an existing client
   3) Remove OpenVPN
   4) Exit
Option: 1
```

```
Provide a name for the client:
Name: NewClient
Using SSL: openssl OpenSSL 1.1.1f  31 Mar 2020
Generating a RSA private key
..............................+++++
.........................+++++
writing new private key to '/etc/openvpn/server/easy-rsa/pki/easy-rsa-
3613.IhGT9n/tmp.lCjiIP'
-----
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rsa-3613.IhGT9n/tmp.6bnJcJ
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'New_IntUser'
Certificate is to be certified until Sep 15 07:13:53 2031 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated


NewClient added. Configuration available in: /root/NewClient.ovpn
```

1.3 Gửi file xác thực VPN cho Internet user bằng dịch vụ FTP

1. Copy file xác thực *client.ovpn* từ thư mục */root* về thư mục home của user hiện tại để chuẩn bị cho Internet user download

```
$ sudo ls /root
IntUser.ovpn  New_IntUser.ovpn  client.ovpn  snap
$ sudo cp /root/client.ovpn .
$ ls -l
total 32
-rw-r--r-- 1 root root  4990 Sep 17 07:37 client.ovpn
```

2. Cài đặt FTP server trên máy Gateway để Internet user có thể download file xác thực:

```
$ sudo apt install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

3. Kiểm tra FTP service đã chạy trên Gateway:

```
$ sudo systemctl status vsftpd.service
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2021-09-17 07:26:55 UTC; 14s ago
    Process: 4125 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited,
status=0/SU>
   Main PID: 4126 (vsftpd)
      Tasks: 1 (limit: 1071)
     Memory: 608.0K
     CGroup: /system.slice/vsftpd.service
             └─4126 /usr/sbin/vsftpd /etc/vsftpd.conf
```

4. Internet user login vào FTP server của Gateway để lấy file xác thực:

```
IntUser$ ftp 203.162.0.1
Connected to 203.162.0.1.
220 (vsFTPd 3.0.3)
Name (203.162.0.1.1:hp): hp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            4990 Sep 17 07:37 IntUser.ovpn
226 Directory send OK.
ftp> get ./client.ovpn
local: ./IntUser.ovpn remote: ./IntUser.ovpn
```

```
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ./IntUser.ovpn (4990 bytes).
226 Transfer complete.
4990 bytes received in 0.00 secs (41.0244 MB/s)
ftp> bye
221 Goodbye.
$ ls -l
total 8
-rw-rw-r-- 1 hp hp 4990 Sep 17 07:40 client.ovpn
```

1.4 Cài đặt & cấu hình VNP client trên máy Internet user

1. Thiết lập một kết nối NAT cho máy ảo Internet User để kết nối được với Internet, phục vụ cài đặt OpenVPN client.
2. Cài đặt OpenVPN client cho Internet user

```
$ sudo apt install openvpn
Reading package lists... Done
Building dependency tree
Reading state information... Done
. . . . . .
```

3. Hủy kết nối NAT đến Internet và đặt default gateway của máy Internet user là Internet router. *Lưu ý:* Sau khi sử dụng xong đường truyền ra Internet để download package openvpn, cần hủy bỏ đường truyền này để máy Internet user có duy nhất một đường truyền (default gateway) đến router Internet.

```
$ ifconfig -a
enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 203.162.1.15  netmask 255.255.255.0  broadcast 203.162.1.255
        inet6 fe80::a00:27ff:fe10:1115  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:10:11:15  txqueuelen 1000  (Ethernet)
        RX packets 418  bytes 69857 (69.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 401  bytes 47976 (47.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

~$ sudo route add default gateway 203.162.1.1
$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         203.162.1.1     0.0.0.0         UG    0      0        0 enp0s10
203.162.1.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s10
```

4. Kết nối VPN đến Gateway với file xác thực *IntUser.ovpn* đã lấy về:

```
$ sudo openvpn --config ./client.ovpn
Fri Sep 17 07:51:56 2021 Unrecognized option or missing or extra parameter(s) in
/etc/openvpn/IntUser.ovpn:13: block-outside-dns (2.4.7)
Fri Sep 17 07:51:56 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4]
[EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 19 2021
Fri Sep 17 07:51:56 2021 library versions: OpenSSL 1.1.1f  31 Mar 2020, LZO 2.10
Fri Sep 17 07:51:56 2021 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR'
initialized with 256 bit key
Fri Sep 17 07:51:56 2021 Outgoing Control Channel Encryption: Using 256 bit message hash
'SHA256' for HMAC authentication
Fri Sep 17 07:51:56 2021 Incoming Control Channel Encryption: Cipher 'AES-256-CTR'
initialized with 256 bit key
Fri Sep 17 07:51:56 2021 Incoming Control Channel Encryption: Using 256 bit message hash
'SHA256' for HMAC authentication
Fri Sep 17 07:51:56 2021 TCP/UDP: Preserving recently used remote address:
[AF_INET]10.10.10.1:1194
Fri Sep 17 07:51:56 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Fri Sep 17 07:51:56 2021 UDP link local: (not bound)
Fri Sep 17 07:51:56 2021 UDP link remote: [AF_INET]203.162.0.1:1194
Fri Sep 17 07:51:56 2021 TLS: Initial packet from [AF_INET]10.10.10.1:1194, sid=ef2cf8f8
aa58749f
Fri Sep 17 07:51:56 2021 VERIFY OK: depth=1, CN=ChangeMe
Fri Sep 17 07:51:56 2021 VERIFY KU OK
Fri Sep 17 07:51:56 2021 Validating certificate extended key usage
```

```
Fri Sep 17 07:51:56 2021 ++ Certificate has EKU (str) TLS Web Server Authentication,
expects TLS Web Server Authentication
Fri Sep 17 07:51:56 2021 VERIFY EKU OK
Fri Sep 17 07:51:56 2021 VERIFY OK: depth=0, CN=server
Fri Sep 17 07:51:56 2021 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384,
2048 bit RSA
Fri Sep 17 07:51:56 2021 [server] Peer Connection Initiated with [AF_INET]10.10.10.1:1194
Fri Sep 17 07:51:57 2021 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
Fri Sep 17 07:51:57 2021 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1
bypass-dhcp,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,route-gateway
10.8.0.1,topology subnet,ping 10,ping-restart 120,ifconfig 10.8.0.2 255.255.255.0,peer-id
0,cipher AES-256-GCM'
Fri Sep 17 07:51:57 2021 OPTIONS IMPORT: timers and/or timeouts modified
Fri Sep 17 07:51:57 2021 OPTIONS IMPORT: --ifconfig/up options modified
Fri Sep 17 07:51:57 2021 OPTIONS IMPORT: route options modified
Fri Sep 17 07:51:57 2021 OPTIONS IMPORT: route-related options modified
Fri Sep 17 07:51:57 2021 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Fri Sep 17 07:51:57 2021 OPTIONS IMPORT: peer-id set
Fri Sep 17 07:51:57 2021 OPTIONS IMPORT: adjusting link_mtu to 1624
Fri Sep 17 07:51:57 2021 OPTIONS IMPORT: data channel crypto options modified
Fri Sep 17 07:51:57 2021 Data Channel: using negotiated cipher 'AES-256-GCM'
Fri Sep 17 07:51:57 2021 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256
bit key
Fri Sep 17 07:51:57 2021 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256
bit key
Fri Sep 17 07:51:57 2021 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=enp0s3
HWADDR=08:00:27:87:0c:4c
Fri Sep 17 07:51:57 2021 TUN/TAP device tun0 opened
Fri Sep 17 07:51:57 2021 TUN/TAP TX queue length set to 100
Fri Sep 17 07:51:57 2021 /sbin/ip link set dev tun0 up mtu 1500
Fri Sep 17 07:51:58 2021 /sbin/ip addr add dev tun0 10.8.0.2/24 broadcast 10.8.0.255
Tue Sep 21 05:41:57 2021 /sbin/ip route add 203.162.0.1/32 via 203.162.1.1
Tue Sep 21 05:41:57 2021 /sbin/ip route add 0.0.0.0/1 via 10.8.0.1
Tue Sep 21 05:41:57 2021 /sbin/ip route add 128.0.0.0/1 via 10.8.0.1
Fri Sep 17 07:51:58 2021 WARNING: this configuration may cache passwords in memory -- use
the auth-nocache option to prevent this
Fri Sep 17 07:51:58 2021 Initialization Sequence Completed
```

5. Mở một session mới của máy Internet user và kiểm tra kết nối VPN thành công đến Gateway và đến các máy local user:

```
$ ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=1.61 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=1.67 ms
^C
--- 10.8.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.607/1.636/1.666/0.029 ms
hp@IntUser:~$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=63 time=2.72 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=63 time=2.34 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=63 time=2.42 ms
^C
--- 192.168.1.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.341/2.493/2.716/0.160 ms
```

1.5 Tìm hiểu thêm về đường truyền VPN

1. Sau khi mở kết nối VPN thành công đến Gateway, xuất hiện giao diện kết nối đường hầm *tun0* tại máy Internet user:

```
$ ifconfig tun0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.2  netmask 255.255.255.0  destination 10.8.0.2
        inet6 fe80::92b8:8742:fc90:9f60  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 96 (96.0 B)
```

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Bảng routing cũng được thay đổi. Default gateway mới được thêm vào (10.8.0.1)

```
~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.8.0.1        128.0.0.0       UG    0      0        0 tun0
0.0.0.0         203.162.1.1     0.0.0.0         UG    0      0        0 enp0s10
10.8.0.0        0.0.0.0         255.255.255.0   U     0      0        0 tun0
128.0.0.0       10.8.0.1        128.0.0.0       UG    0      0        0 tun0
203.162.0.1     203.162.1.1     255.255.255.255 UGH   0      0        0 enp0s10
203.162.1.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s10
```

3. Kết nối từ Internet user ra Internet vẫn được duy trì nhưng đi vòng qua Gateway:

```
$ tracepath -n 203.162.0.2
 1?: [LOCALHOST]                      pmtu 1500
 1:  10.8.0.1                                              2.081ms
 1:  10.8.0.1                                              1.782ms
 2:  203.162.0.2                                           2.364ms reached
     Resume: pmtu 1500 hops 2 back 2
```

4. Tạo luật bắt gói tin trên Internet router để kiểm tra kết nối giữa Internet user và Local user. Nhận xét thấy khi ping giữa Internet user và local user, không có gói tin địa chỉ 192.168.1.20 của local user xuất hiện trên Internet router (gọi tin đã bị bọc trong đường hầm 203.162.0.1 <- -> 203.162.1.15):

```
Internet$ sudo iptables -t mangle -A FORWARD -j LOG

$ sudo iptables -L -n -t mangle
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
LOG        all  --  0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

$ tail -f /var/log/syslog | grep 192.168.1.20
```

5. Ping giữa máy Internet user và Local user và bắt các gói tin tại Internet Router thì chỉ thấy gói tin đường hầm:

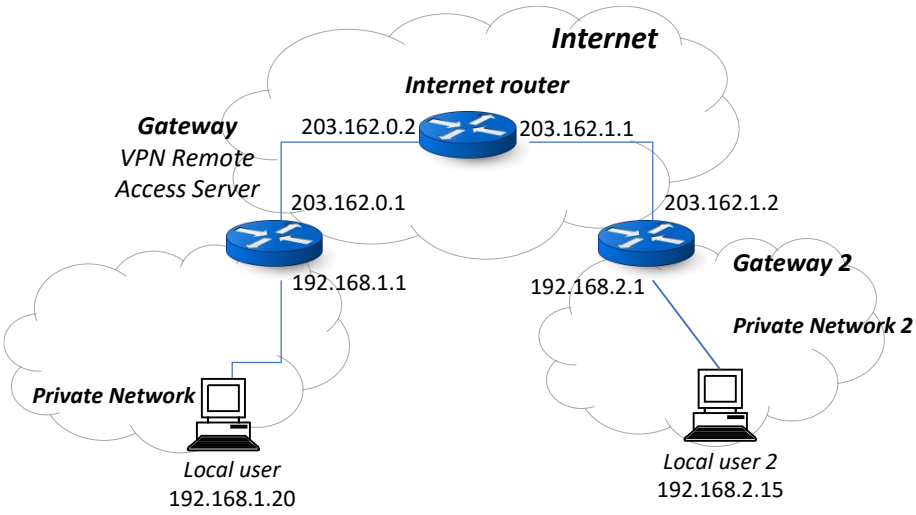
```
Internet$ Internet:~$ tail -f /var/log/syslog

Sep 21 05:54:18 Internet kernel: [344739.111305] IN=enp0s10 OUT=enp0s9
MAC=08:00:27:10:11:11:08:00:27:10:11:15:08:00 SRC=203.162.1.15 DST=203.162.0.1 LEN=68
TOS=0x00 PREC=0x00 TTL=63 ID=1491 DF PROTO=UDP SPT=42221 DPT=1194 LEN=48
Sep 21 05:54:19 Internet kernel: [344739.650394] IN=enp0s10 OUT=enp0s9
MAC=08:00:27:10:11:11:08:00:27:10:11:15:08:00 SRC=203.162.1.15 DST=203.162.0.1 LEN=136
TOS=0x00 PREC=0x00 TTL=63 ID=1624 DF PROTO=UDP SPT=42221 DPT=1194 LEN=116
Sep 21 05:54:19 Internet kernel: [344739.652167] IN=enp0s9 OUT=enp0s10
MAC=08:00:27:10:10:12:08:00:27:10:00:01:08:00 SRC=203.162.0.1 DST=203.162.1.15 LEN=136
TOS=0x00 PREC=0x00 TTL=63 ID=12392 DF PROTO=UDP SPT=1194 DPT=42221 LEN=116
Sep 21 05:54:20 Internet kernel: [344740.653419] IN=enp0s10 OUT=enp0s9
MAC=08:00:27:10:11:11:08:00:27:10:11:15:08:00 SRC=203.162.1.15 DST=203.162.0.1 LEN=136
TOS=0x00 PREC=0x00 TTL=63 ID=1849 DF PROTO=UDP SPT=42221 DPT=1194 LEN=116
Sep 21 05:54:20 Internet kernel: [344740.655027] IN=enp0s9 OUT=enp0s10
MAC=08:00:27:10:10:12:08:00:27:10:00:01:08:00 SRC=203.162.0.1 DST=203.162.1.15 LEN=136
TOS=0x00 PREC=0x00 TTL=63 ID=12396 DF PROTO=UDP SPT=1194 DPT=42221 LEN=116
Sep 21 05:54:21 Internet kernel: [344741.656333] IN=enp0s10 OUT=enp0s9
MAC=08:00:27:10:11:11:08:00:27:10:11:15:08:00 SRC=203.162.1.15 DST=203.162.0.1 LEN=136
TOS=0x00 PREC=0x00 TTL=63 ID=1931 DF PROTO=UDP SPT=42221 DPT=1194 LEN=116
```

```
Sep 21 05:54:21 Internet kernel: [344741.657821] IN=enp0s9 OUT=enp0s10
MAC=08:00:27:10:10:12:08:00:27:10:00:01:08:00 SRC=203.162.0.1 DST=203.162.1.15 LEN=136
TOS=0x00 PREC=0x00 TTL=63 ID=12623 DF PROTO=UDP SPT=1194 DPT=42221 LEN=116
Sep 21 05:54:22 Internet kernel: [344742.658738] IN=enp0s10 OUT=enp0s9
MAC=08:00:27:10:11:11:08:00:27:10:11:15:08:00 SRC=203.162.1.15 DST=203.162.0.1 LEN=136
TOS=0x00 PREC=0x00 TTL=63 ID=2112 DF PROTO=UDP SPT=42221 DPT=1194 LEN=116
Sep 21 05:54:22 Internet kernel: [344742.660272] IN=enp0s9 OUT=enp0s10
MAC=08:00:27:10:10:12:08:00:27:10:00:01:08:00 SRC=203.162.0.1 DST=203.162.1.15 LEN=136
TOS=0x00 PREC=0x00 TTL=63 ID=12677 DF PROTO=UDP SPT=1194 DPT=42221 LEN=116
```

2 Thực hành net-to-net VPN

2.1 Sơ đồ mạng giả lập Internet



Tiếp tục với sơ đồ giả lập Internet như bài trước, thay vì kết nối VPN với một Internet user, bài này kết nối VPN với một private network khác (Private Network 2). Các Gateway của Private Network cần cài đặt openvpn và openssh:

```
$ sudo apt-get install openvpn openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version (1.1.1f-1ubuntu2.8).
openvpn is already the newest version (2.4.7-1ubuntu2.20.04.3).
0 upgraded, 0 newly installed, 0 to remove and 16 not upgraded.
```

Nếu sử dụng Gateway từ bài trước (đã cài đặt openvpn và cấu hình host-to-net) thì cần kiểm tra và xóa cấu hình này đi:

```
$ sudo systemctl status openvpn-server@server
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; vendor preset:
ena>
     Active: inactive (dead) (Result: exit-code) since Tue 2021-09-21 17:32:07 +07; 23min
ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
    Process: 16794 ExecStart=/usr/sbin/openvpn --status /run/openvpn-server/status-
server.log>
   Main PID: 16794 (code=exited, status=1/FAILURE)
     Status: "Pre-connection initialization successful"

Sep 21 17:32:04 gateway2 systemd[1]: openvpn-server@server.service: Main process exited,
code>
Sep 21 17:32:04 gateway2 systemd[1]: openvpn-server@server.service: Failed with result
'exit->
Sep 21 17:32:07 gateway2 systemd[1]: Stopped OpenVPN service for server.
```

```
$ sudo systemctl disable openvpn-server@server
Removed /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service.
```

2.2 Cài đặt & cấu hình VPN server cho các gateway

1. Cài đặt openvpn & openssl:

```
$ sudo apt-get install openvpn openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version (1.1.1f-1ubuntu2.8).
openvpn is already the newest version (2.4.7-1ubuntu2.20.04.3).
0 upgraded, 0 newly installed, 0 to remove and 16 not upgraded.


tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.2  netmask 255.255.255.0  destination 10.8.0.2
        inet6 fe80::92b8:8742:fc90:9f60  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 96 (96.0 B)
```

2. Chuẩn bị file khóa kết nối lưu vào file */etc/openvpn/vpn.key* trên máy Gateway

```
$ sudo openvpn --genkey --secret /etc/openvpn/vpn.key
$ ls /etc/openvpn
client  server  server.conf  update-resolv-conf  vpn.key  vpn.log
```

3. Sử dụng FTP hoặc scp để copy file *vpn.key* vừa tạo sang Gateway 2

```
$ sudo scp /etc/openvpn/vpn.key 203.162.1.2:/etc/openvpn/vpn.ket
. . .
```

4. Cấu hình VPN trên Gateway:

```
$ sudo sudo nano /etc/openvpn/server.conf
remote 203.162.1.2      ← Remote gateway phía private network 2
float
port 8000     ← cổng TCP/UDP kết nối cho cả 2 phía local & remote
dev tun
ifconfig 10.9.0.1 10.9.0.2      ← cấu hình địa chỉ IP cho kết nối đường hầm
persist-tun
persist-local-ip
comp-lzo
ping 15
secret /etc/openvpn/vpn.key     ← file xác thực kết nối
route 192.168.2.0 255.255.255.0     ← địa chỉ private network phía remote
user nobody
group nogroup
log vpn.log
verb 1
```

5. Start VPN server trên Gateway và kiểm tra log:

```
$ sudo systemctl restart openvpn@server
$ tail -f /etc/openvpn/vpn.log
Tue Sep 21 19:27:29 2021 disabling NCP mode (--ncp-disable) because not in P2MP client or
server mode
Tue Sep 21 19:27:29 2021 WARNING: file '/etc/openvpn/vpn.key' is group or others
accessible
Tue Sep 21 19:27:29 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4]
[EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 19 2021
Tue Sep 21 19:27:29 2021 library versions: OpenSSL 1.1.1f  31 Mar 2020, LZO 2.10
Tue Sep 21 19:27:29 2021 WARNING: --ping should normally be used with --ping-restart or --
ping-exit
Tue Sep 21 19:27:29 2021 WARNING: you are using user/group/chroot/setcon without persist-
key -- this may cause restarts to fail
Tue Sep 21 19:27:29 2021 WARNING: INSECURE cipher with block size less than 128 bit (64
bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher with a larger block
size (e.g. AES-256-CBC).
```

```
Tue Sep 21 19:27:29 2021 WARNING: INSECURE cipher with block size less than 128 bit (64
bit).  This allows attacks like SWEET32.  Mitigate by using a --cipher with a larger block
size (e.g. AES-256-CBC).
Tue Sep 21 19:27:29 2021 TUN/TAP device tun0 opened
Tue Sep 21 19:27:29 2021 /sbin/ip link set dev tun0 up mtu 1500
Tue Sep 21 19:27:29 2021 /sbin/ip addr add dev tun0 local 10.9.0.1 peer 10.9.0.2
Tue Sep 21 19:27:29 2021 TCP/UDP: Preserving recently used remote address:
[AF_INET]203.162.1.2:8000
Tue Sep 21 19:27:29 2021 UDP link local (bound): [AF_INET][undef]:8000
Tue Sep 21 19:27:29 2021 UDP link remote: [AF_INET]203.162.1.2:8000
Tue Sep 21 19:27:29 2021 GID set to nogroup
Tue Sep 21 19:27:29 2021 UID set to nobody
Tue Sep 21 19:27:35 2021 Peer Connection Initiated with [AF_INET]203.162.1.2:8000
Tue Sep 21 19:27:37 2021 WARNING: this configuration may cache passwords in memory -- use
the auth-nocache option to prevent this
Tue Sep 21 19:27:37 2021 Initialization Sequence Completed
```

6. Sau khi VPN server được start thành công trên máy Gateway, giao diện mạng đường hầm *tun0* được thiết lập với địa chỉ 10.9.0.1. Bảng routing xuất hiện đường đi đến mạng remote (192.168.2.0) qua đường hầm này:

```
$ ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.9.0.1  netmask 255.255.255.255  destination 10.9.0.2
        inet6 fe80::7969:fa23:b790:ada  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 288 (288.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.9.0.2        0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s10
192.168.2.0     10.9.0.2        255.255.255.0   UG    0      0        0 tun0
203.162.0.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s9
203.162.1.0     203.162.0.2     255.255.255.0   UG    0      0        0 enp0s9
```

7. Cấu hình VPN trên Gateway 2:

```
$ sudo sudo nano /etc/openvpn/server.conf
remote 203.162.0.1      ← Remote gateway phía private network
float
port 8000    ← cổng TCP/UDP kết nối cho cả 2 phía local & remote
dev tun
ifconfig 10.9.0.2 10.9.0.1     ← cấu hình địa chỉ IP cho kết nối đường hầm
persist-tun
persist-local-ip
comp-lzo
ping 15
secret /etc/openvpn/vpn.key    ← file xác thực kết nối
route 192.168.1.0 255.255.255.0    ← địa chỉ private network phía remote
user nobody
group nogroup
log vpn.log
verb 1
```

8. Start VPN server trên Gateway 2 và kiểm tra log:

```
$ sudo systemctl restart openvpn@server
$ tail -f /etc/openvpn/vpn.log
```

9. Sau khi VPN server được start thành công trên máy Gateway 2, kiểm tra giao diện mạng đường hầm *tun0* được thiết lập với địa chỉ 10.9.0.2 và bảng routing được thêm đường đi đến mạng remote (192.168.1.0) qua đường hầm:

```
$ ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.9.0.2  netmask 255.255.255.255  destination 10.9.0.1
```

```
        inet6 fe80::429d:e7f2:565f:358d  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 21  bytes 1188 (1.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 852 (852.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.9.0.1        0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.1.0     10.9.0.1        255.255.255.0   UG    0      0        0 tun0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s10
203.162.0.0     203.162.1.1     255.255.255.0   UG    0      0        0 enp0s9
203.162.1.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s9
```

10. Trên máy trạm thuộc private network 2, kiểm tra default gateway và ping đến máy trạm thuộc private network ở xa:

```
192.168.2.15$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.1     0.0.0.0         UG    0      0        0 enp0s10
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s10
192.168.156.0   0.0.0.0         255.255.255.0   U     0      0        0 enp0s8
192.168.2.15$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=62 time=3.46 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=62 time=2.99 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=62 time=3.19 ms
```

11. Kiểm tra đường đi giữa 2 máy trạm thuộc các private network sẽ thấy xuất hiện đường hầm:

```
192.168.2.15$ tracepath -n 192.168.1.20
 1?: [LOCALHOST]                      pmtu 1500
 1:  192.168.2.1                                           0.803ms
 1:  192.168.2.1                                           0.493ms
 2:  10.9.0.1                                              2.695ms
 3:  192.168.1.20                                          3.142ms reached
     Resume: pmtu 1500 hops 3 back 3
```