

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN MẠNG NÂNG CAO
MÃ HỌC PHẦN: INT1483**

**BÀI THỰC HÀNH
Sử dụng công cụ OpenVPN**

Sinh viên thực hiện: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

Nội dung thực hành

Khởi động bài lab:

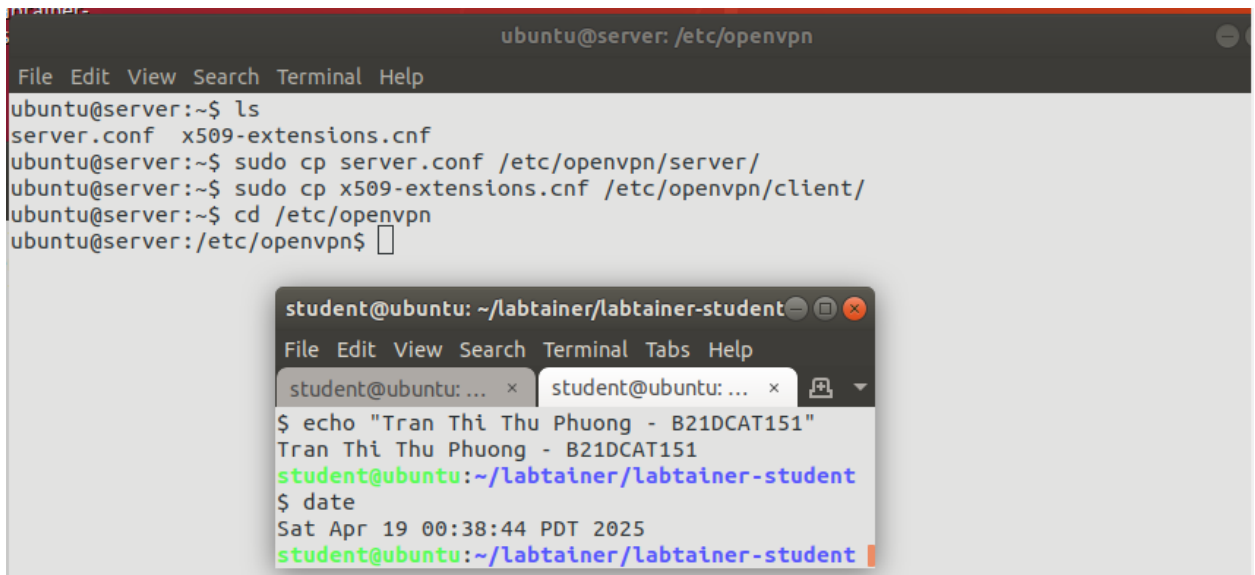
Vào terminal, gõ :

labtainer -r ptit-openvpn

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện tương ứng server và client.

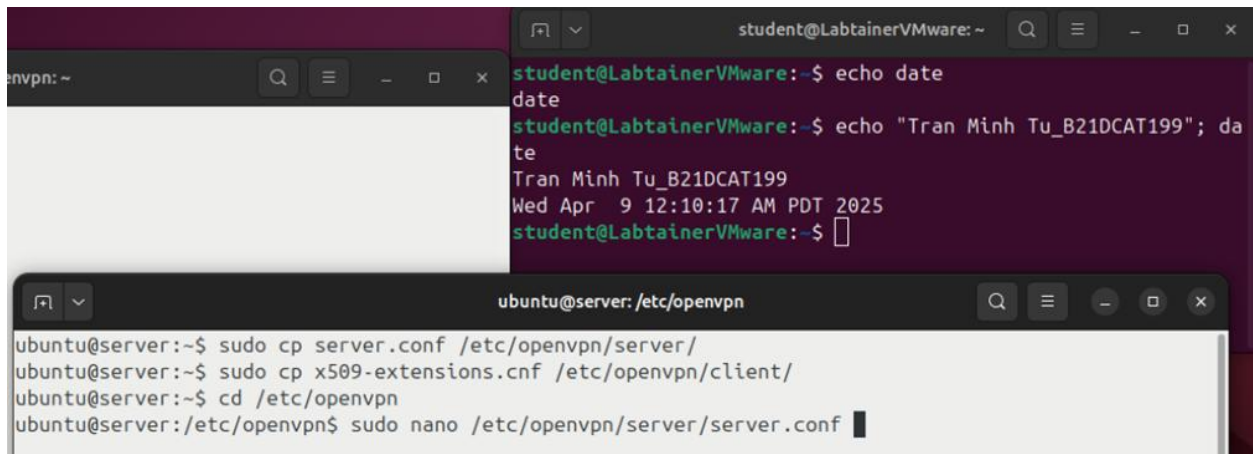
- Ta sẽ tiến hành thực hiện trong thư mục `/etc/openvpn/` nên ta tiến hành di chuyển file cấu hình `x509-extension` và `server.conf` vào thư mục client và server:

```
sudo cp server.conf /etc/openvpn/server/  
sudo cp x509-extensions.cnf /etc/openvpn/client/  
cd /etc/openvpn
```



```
ubuntu@server: /etc/openvpn  
File Edit View Search Terminal Help  
ubuntu@server:~$ ls  
server.conf x509-extensions.cnf  
ubuntu@server:~$ sudo cp server.conf /etc/openvpn/server/  
ubuntu@server:~$ sudo cp x509-extensions.cnf /etc/openvpn/client/  
ubuntu@server:~$ cd /etc/openvpn  
ubuntu@server:/etc/openvpn$  
  
student@ubuntu: ~/labtainer/labtainer-student  
File Edit View Search Terminal Tabs Help  
student@ubuntu: ... x student@ubuntu: ... x  
$ echo "Tran Thi Thu Phuong - B21DCAT151"  
Tran Thi Thu Phuong - B21DCAT151  
student@ubuntu:~/labtainer/labtainer-student  
$ date  
Sat Apr 19 00:38:44 PDT 2025  
student@ubuntu:~/labtainer/labtainer-student
```

- Đầu tiên ta sẽ tiến hành cấu hình cho VPN server



```
student@LabtainerVMware: ~  
student@LabtainerVMware:~$ echo date  
date  
student@LabtainerVMware:~$ echo "Tran Minh Tu_B21DCAT199"; da  
te  
Tran Minh Tu_B21DCAT199  
Wed Apr 9 12:10:17 AM PDT 2025  
student@LabtainerVMware:~$  
  
ubuntu@server: /etc/openvpn  
ubuntu@server:~$ sudo cp server.conf /etc/openvpn/server/  
ubuntu@server:~$ sudo cp x509-extensions.cnf /etc/openvpn/client/  
ubuntu@server:~$ cd /etc/openvpn  
ubuntu@server:/etc/openvpn$ sudo nano /etc/openvpn/server/server.conf
```

- Chỉnh sửa cấu hình các tham số cho VPNServer trong file: *server.conf*. Các tham số cần sửa bao gồm: <IP SERVER> và <PORT> (192.168.1.3 và 443)

```

ubuntu@server: /etc/openvpn
File Edit View Search Terminal Help
GNU nano 4.8 /etc/openvpn/server/server.conf Modified
local 192.168.1.3
port 442
proto udp4
dev tun
keepalive 10 120

topology subnet
server 10.8.0.0 255.255.255.0

student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Tabs Help
student@ubuntu: ... x student@ubuntu: ... x
$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/labtainer-student
$ date
Sat Apr 19 00:38:44 PDT 2025
student@ubuntu:~/labtainer/labtainer-student

```

- Tạo chứng chỉ và khóa của cơ quan cung cấp chứng chỉ gốc:

sudo openssl req -x509 -newkey rsa:4096 -keyout ca.key -sha256 -days 3650 -set_serial 00 -out ca.crt -subj "/C=VN/ST=HN/L=HD/O=PTIT/CN=<Mã sinh viên>" -addext nsComment="ROOT CA"

```

ubuntu@server: /etc/openvpn
File Edit View Search Terminal Help
ubuntu@server:/etc/openvpn$ sudo openssl req -x509 -newkey rsa:4096 -keyout ca.key -sha256 -days
3650 -set_serial 00 -out ca.crt -subj "/C=VN/ST=HN/L=HD/O=PTIT/CN=B21DCAT151" -addext nsComment="
ROOT CA"
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
Enter PEM pass phrase:

```

- Kiểm tra thông tin chứng chỉ gốc đã tạo:

openssl x509 -in ca.crt -text -noout

```

ubuntu@server:/etc/openvpn$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = VN, ST = HN, L = HD, O = PTIT, CN = B21DCAT151
        Validity
            Not Before: Apr 19 07:46:45 2025 GMT
            Not After : Apr 17 07:46:45 2035 GMT
        Subject: C = VN, ST = HN, L = HD, O = PTIT, CN = B21DCAT151
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (4096 bit)
            Modulus:

```

```

student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Tabs Help
student@ubuntu: ... x student@ubuntu: ... x
$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/labtainer-student
$ date
Sat Apr 19 00:38:44 PDT 2025
student@ubuntu:~/labtainer/labtainer-student

```

- Chỉnh sửa cấu hình mở rộng cho chứng chỉ số x509 trong file: *x509-extensions.cnf*
`sudo nano client/x509-extensions.cnf`
 thay "extendedKeyUsage = <Type>" bằng "extendedKeyUsage = clientAuth, serverAuth"

```

ubuntu@server:/etc/openvpn
File Edit View Search Terminal Help
GNU nano 4.8 client/x509-extensions.cnf Modified
[v3_vpn_server]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
extendedKeyUsage = clientAuth, serverAuth
keyUsage = digitalSignature,keyEncipherment
nsComment= "OpenVPN Server Signed Certificate"

[v3_vpn_client]

```

```

student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Tabs Help
student@ubuntu: ... x student@ubuntu: ... x
$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/labtainer-student
$ date
Sat Apr 19 00:38:44 PDT 2025
student@ubuntu:~/labtainer/labtainer-student

```

- Tạo yêu cầu chứng chỉ (CSR) và cặp khóa cho máy chủ và kí bởi trung tâm cung cấp chứng chỉ CA :

```

sudo openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr -subj
"/C=VN/ST=HN/L=HD/O=PTIT/CN=SERVER"

```

- Tạo và kí chứng chỉ của server bằng khóa và chữ kí của CA:

```

sudo openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -sha256 -
days 730 -text -out server.crt -extensions v3_vpn_server -extfile client/x509-
extensions.cnf

```

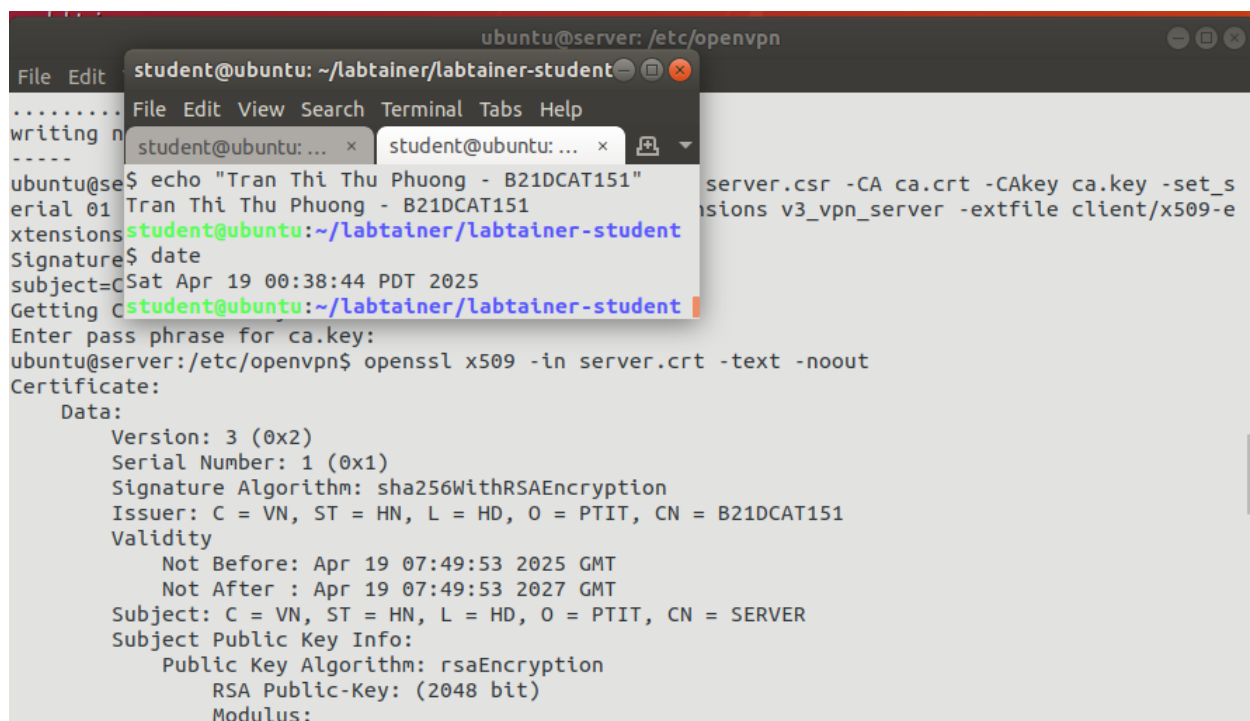
```

ubuntu@server:/etc/openvpn$ sudo nano client/x509-extensions.cnf
ubuntu@server:/etc/openvpn$ sudo openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out
server.csr -subj "/C=VN/ST=HN/L=HD/O=PTIT/CN=SERVER"
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'server.key'
-----
ubuntu@server:/etc/openvpn$ sudo openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -set_s
erial 01 -sha256 -days 730 -text -out server.crt -extensions v3_vpn_server -extfile client/x509-e
xtensions.cnf
Signature ok
subject=C = VN, ST = HN, L = HD, O = PTIT, CN = SERVER
Getting CA Private Key
Enter pass phrase for ca.key:
ubuntu@server:/etc/openvpn$

```

- Sau đó kiểm tra thông tin

openssl x509 -in server.crt -text -noout



```

File Edit View Search Terminal Tabs Help
student@ubuntu: ~/labtainer/labtainer-student
.....
writing n
-----
ubuntu@se$ echo "Tran Thi Thu Phuong - B21DCAT151"
erial 01 Tran Thi Thu Phuong - B21DCAT151
xtensions$ date
Signature$ Sat Apr 19 00:38:44 PDT 2025
subject=C$ student@ubuntu:~/labtainer/labtainer-student
Getting C$ student@ubuntu:~/labtainer/labtainer-student
Enter pass phrase for ca.key:
ubuntu@server:/etc/openvpn$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = VN, ST = HN, L = HD, O = PTIT, CN = B21DCAT151
        Validity
            Not Before: Apr 19 07:49:53 2025 GMT
            Not After : Apr 19 07:49:53 2027 GMT
        Subject: C = VN, ST = HN, L = HD, O = PTIT, CN = SERVER
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:

```

- Bước tiếp theo tạo chứng chỉ và cặp khóa cho máy khách và kí bởi trung tâm cung cấp chứng chỉ CA:

sudo openssl req -new -newkey rsa:2048 -nodes -keyout client.key -out client.csr -subj "/C=VN/ST=HN/L=HD/O=PTIT/CN=CLIENT"

- Tạo và ký chứng chỉ client với khóa và chữ kí của CA:

sudo openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -sha256 -days 365 -text -out client.crt -extensions v3_vpn_client -extfile client/x509-extensions.cnf

- Kiểm tra thông tin

openssl x509 -in client.crt -text -noout

```

ubuntu@server:/etc/openvpn$ openssl x509 -in client.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = VN, ST = HN, L = HD, O = PTIT, CN = B21DCAT151
        Validity
            Not Before: Apr 19 08:00:42 2025 GMT
            Not After : Apr 19 08:00:42 2026 GMT
        Subject: C = VN, ST = HN, L = HD, O = PTIT, CN = CLIENT
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:e6:62:54:6d:09:31:78:25:a9:34:bb:d9:5f:98:
                    1a:ff:12:66:12:94:b5:d3:2d:c3:06:22:35:cf:cc:
                    6e:cc:3f:9f:bc:a9:16:4b:00:6a:d7:c2:7d:a0:5c:
                    e2:9e:52:b2:d6:b1:2a:8a:d1:19:e3:2a:e4:a9:55:
                    2f:67:12:66:eb:29:6f:31:5e:53:4e:72:18:aa:ee:
                    b8:cc:5a:93:9a:1d:bc:2e:83:56:98:c8:9f:6d:2c:

```

```

student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Tabs Help
student@ubuntu: ... x student@ubuntu: ... x
$ date
Sat Apr 19 00:38:38 PDT 2025
student@ubuntu:~/labtainer/labtainer-student
$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/labtainer-student

```

- Tạo khóa chia sẻ giữa client và server:

sudo openvpn --genkey --secret tc.key

- Trên máy **client** (openvpn):

Copy file client.conf đến /etc/openvpn/client: *sudo cp client.conf /etc/openvpn/client/*

Chỉnh sửa file cấu hình máy khách: client.conf với các tham số cần sửa bao gồm: <IP SERVER> - là địa chỉ IP của server, <PORT> - là cổng VPN server chấp nhận kết nối:

sudo nano /etc/openvpn/client/client.conf

```

ubuntu@openvpn: ~
File Edit View Search Terminal Help
GNU nano 4.8 /etc/openvpn/client/client.conf Modified
remote 192.168.1.3 443 udp4

resolv-retry infinite

client

```

```

student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Tabs Help
student@ubuntu: ... x student@ubuntu: ... x
$ date
Sat Apr 19 00:38:38 PDT 2025
student@ubuntu:~/labtainer/labtainer-student
$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/labtainer-student

```

- Tiếp theo khởi động dịch vụ ssh trên máy client (chẳng hạn sử dụng *sudo systemctl restart ssh.service*) và trên máy **server** sử dụng scp để truyền file tới client:

sudo scp ca.crt client.crt client.key tc.key ubuntu@192.168.1.2:/home/ubuntu
(Mật khẩu tk ubuntu là ubuntu)

```

ubuntu@server: /etc/openvpn
File Edit View Search Terminal Help
ca.crt client client.csr server server.csr tc.key
ca.key client.crt client.key server.crt server.key update-resolv-conf
ubuntu@server:/etc/openvpn$ sudo scp ca.crt client.crt client.key tc.key ubuntu@192.168.1.2:/home/ubuntu
ubuntu@192.168.1.2's password:
ca.crt
100% 1964 482.6KB/s 00:00 --:-- Eca.crt
client.crt
100% 6114 1.9MB/s 00:00 --:-- Eclient.crt
client.key
100% 1784 285.7KB/s 00:00 --:-- Eclient.key
tc.key
100% 636 72.3KB/s 00:00 --:-- Etc.key
ubuntu@server:/etc/openvpn$

```

- Trên **client** chuyển file vừa nhận được vào thư mục `/etc/openvpn/client/` và chỉnh sửa lại quyền thực thi :

sudo mv -f ca.crt client.crt client.key tc.key /etc/openvpn/client/

cd /etc/openvpn/client/

*sudo chown root: **

*sudo chmod 0600 *.key*

```

ubuntu@openvpn:~$ sudo mv -f ca.crt client.crt client.key tc.key /etc/openvpn/client/
ubuntu@openvpn:~$ cd /etc/openvpn/client/
ubuntu@openvpn:/etc/openvpn/client$ sudo chown root: *
ubuntu@openvpn:/etc/openvpn/client$ sudo chmod 0600 *.key
ubuntu@openvpn:/etc/openvpn/client$

```

- Khởi động VPNserver và VPN client:
- Trên **server** :

cd /etc/openvpn

sudo openvpn --config server/server.conf

- Trên **client**:

cd /etc/openvpn/client

sudo openvpn --config client.conf &


```
ubuntu@server: /etc/openvpn
File Edit View Search Terminal Help
client.key 0% 0 0.0KB/s --:-- E
client.key 100% 1704 285.7KB/s 00:00
tc.key 0% 0 0.0KB/s --:-- E
tc.key 100% 636 72.3KB/s 00:00

ubuntu@server:/etc/openvpn$ sudo openvpn --config server/server.conf
Sat Apr 19 08:15:07 2025 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep 5 2019
Sat Apr 19 08:15:07 2025 library versions: OpenSSL 1.1.1f 31 Mar 2020, LZO 2.10
Sat Apr 19 08:15:07 2025 NOTE: your local LAN uses the extremely common subnet address 192.168.0.x or 192.168.1.x. Be aware that this might create routing conflicts if you connect to the VPN server from public locations such as internet cafes that use the same subnet.

ubuntu@openvpn: /etc/openvpn/client
File Edit View Search Terminal Help
ubuntu@openvpn:~$ sudo mv -f ca.crt client.crt client.key tc.key /etc/openvpn/client/
ubuntu@openvpn:~$ cd /etc/openvpn/client/
ubuntu@openvpn:/etc/openvpn/client$ sudo chown root: *
ubuntu@openvpn:/etc/openvpn/client$ sudo chmod 0600 *.key
ubuntu@openvpn:/etc/openvpn/client$ sudo openvpn --config client.conf &
[1] 365
ubuntu@openvpn:/etc/openvpn/client$ Sat Apr 19 08:15:33 2025 WARNING: Ignoring option 'dh' in tls-client mode, please only include this in your server configuration
Sat Apr 19 08:15:33 2025 OpenVPN 2.4.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Aug 21 2023
Sat Apr 19 08:15:33 2025 library versions: OpenSSL 1.1.1f 31 Mar 2020, LZO 2.10
Sat Apr 19 08:15:33 2025 Outgoing Control Channel Established: 1500
Sat Apr 19 08:15:33 2025 Incoming Control Channel Established: 1500
Sat Apr 19 08:15:33 2025 TCP/UDP: Preserving rate
Sat Apr 19 08:15:33 2025 Socket Buffers: R=[21Sat Apr 19 01:05:47 PDT 2025
Sat Apr 19 08:15:33 2025 UDPv4 link local: (not bound)
```

- Tiến hành kiểm tra kết nối trên client:

ifconfig tun0

ping 10.8.0.1

```
ubuntu@openvpn:/etc/openvpn/client$ ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.8.0.2 netmask 255.255.255.0 destination 0.0.0.0
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
    RX packets 8 bytes 672 (672.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 49 bytes 4116 (4.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0

ubuntu@openvpn:/etc/openvpn/client$ 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=2.81 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=1.66 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=1.97 ms
64 bytes from 10.8.0.1: icmp_seq=4 ttl=64 time=1.70 ms
```


- Kết thúc bài lab:
- Kiểm tra checkwork:

Checkwork

```

^Cstudent@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/ptit-openvpn
Labname ptit-openvpn

Student      | config_server | create_cert_key | x509_extension | sign_server | sign_client | create_tc_key | config_client | connection |
=====|=====|=====|=====|=====|=====|=====|=====|=====|
B21DCAT151   | Y             | Y               | Y               | Y           | Y           | Y           | Y           | Y           |
What is automatically assessed for this lab:

student@ubuntu:~/labtainer/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"; date
Tran Thi Thu Phuong - B21DCAT151
Sat Apr 19 01:51:23 PDT 2025
student@ubuntu:~/labtainer/labtainer-student$

```