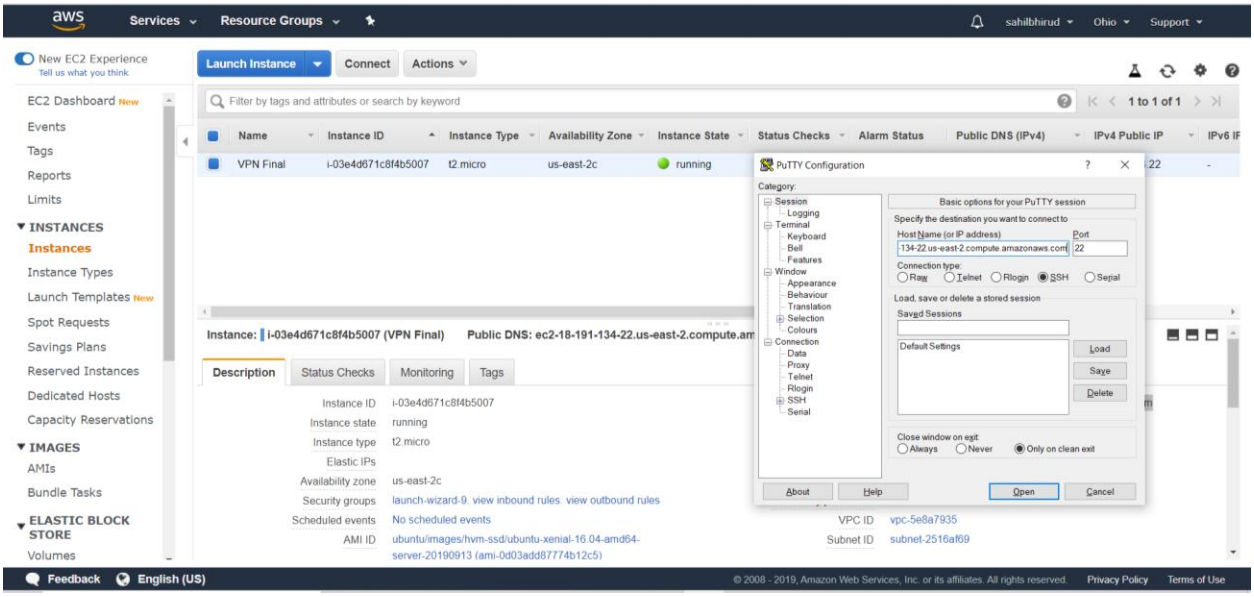
ITIS 6240 – Applied Cryptography

Project VPN

Sahil Bhirud

In this project, I have set up an IKEv2 VPN Server and generated server keys using IPSec command. Below are the steps I performed to complete the project:

1. I have used an Amazon EC2 instance as an Ubuntu 16.04 server and opened its ports for All Traffic and connected to it using Putty.



2. After launching this instance, I updated the system and installed Strongswan using the following commands:

   i. ***sudo apt-get update***

   ii. ***wget http://download.strongswan.org/strongswan-5.8.1.tar.bz2***

iii. ***tar xjvf strongswan-5.8.1.tar.bz2; cd strongswan-5.8.1***

iv. ***./configure --prefix=/usr --sysconfdir=/etc***

v. ***make***

vi. ***sudo make install***

ubuntu@ip-172-31-15-22: ~

```
ubuntu@ip-172-31-15-22:~$ wget http://download.strongswan.org/strongswan-5.8.1.tar.bz2
--2019-11-23 14:58:14--  http://download.strongswan.org/strongswan-5.8.1.tar.bz2
Resolving download.strongswan.org (download.strongswan.org)... 152.96.80.46, 2001:620:130:a080::46
Connecting to download.strongswan.org (download.strongswan.org)|152.96.80.46|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://download.strongswan.org/strongswan-5.8.1.tar.bz2 [following]
--2019-11-23 14:58:14--  https://download.strongswan.org/strongswan-5.8.1.tar.bz2
Connecting to download.strongswan.org (download.strongswan.org)|152.96.80.46|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4517921 (4.3M) [application/x-bzip2]
Saving to: 'strongswan-5.8.1.tar.bz2'

strongswan-5.8.1.tar.bz2                      100%[===================================================================================================>]   4.31M  3.37MB/s    in 1.3s

2019-11-23 14:58:16 (3.37 MB/s) - 'strongswan-5.8.1.tar.bz2' saved [4517921/4517921]

ubuntu@ip-172-31-15-22:~$
```

Type here to search

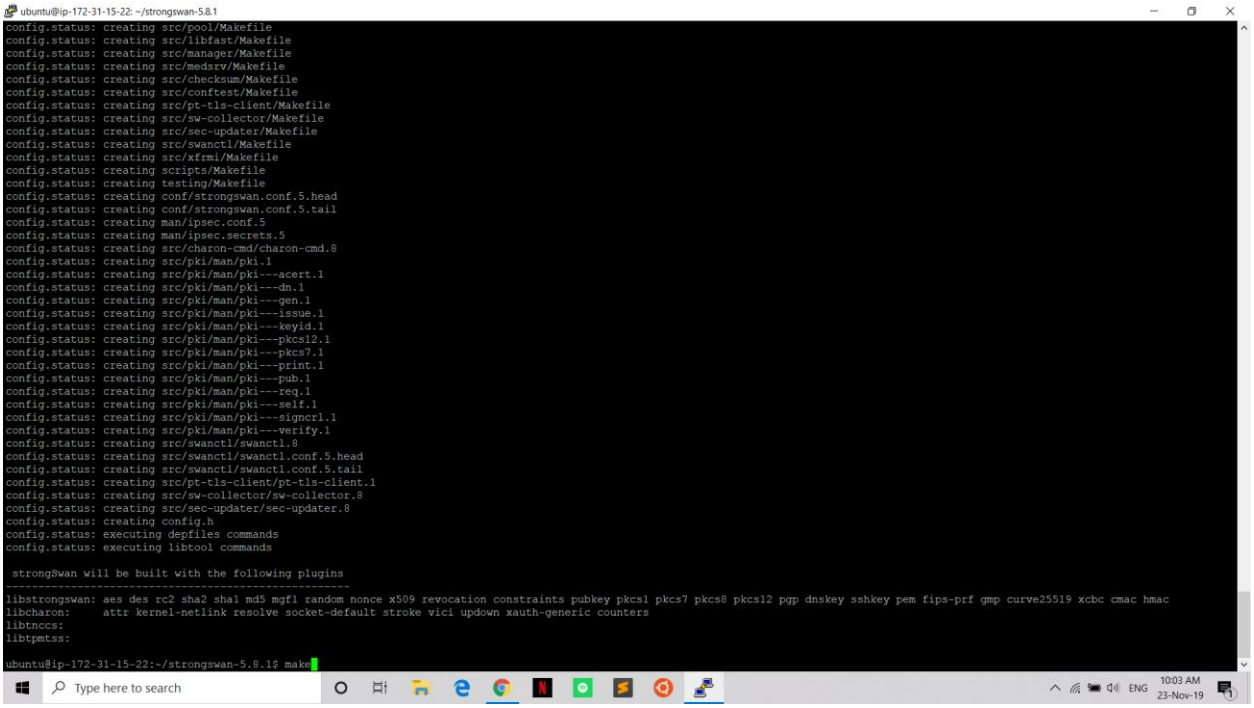
ENG 9:58 AM 23-Nov-19

ubuntu@ip-172-31-15-22: ~/strongswan-5.8.1

```
ubuntu@ip-172-31-15-22:~/strongswan-5.8.1$ clear
ubuntu@ip-172-31-15-22:~/strongswan-5.8.1$ ./configure --prefix=/usr --sysconfdir=/etc
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... no
checking whether make supports nested variables... no
checking whether UID '1000' is supported by ustar format... yes
checking whether GID '1000' is supported by ustar format... yes
checking how to create a ustar tar archive... gnutar
checking whether make supports nested variables... (cached) no
checking for pkg-config... no
checking for a sed that does not truncate output... /bin/sed
checking configured UDP ports (500, 4500)... ok
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... none
checking dependency style of gcc... none
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.h... yes
checking whether byte ordering is bigendian... no
checking how to print strings... printf
checking for a sed that does not truncate output... (cached) /bin/sed
checking for fgrep... /bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
```

Type here to search

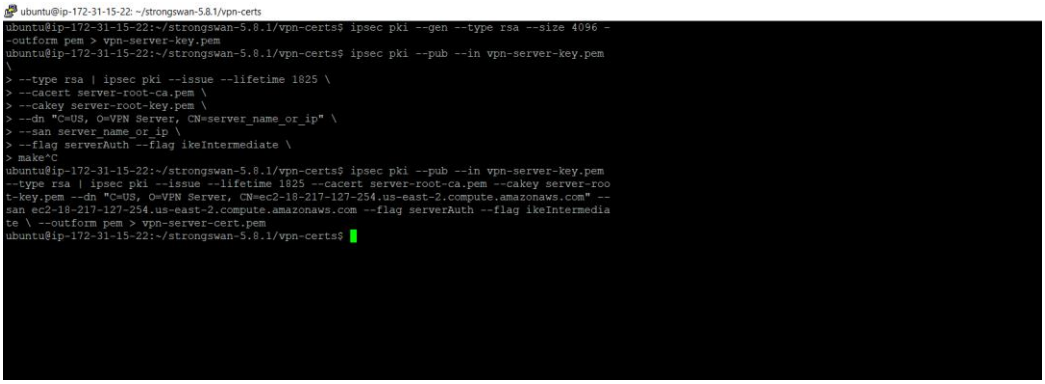
ENG 10:00 AM 23-Nov-19



3. Next, I generated the root key and the certificate for the server using the following commands:

   i. ***ipsec pki --gen --type rsa --size 4096 --outform pem > server-root-key.pem***

   ii. ***ipsec pki --self --ca --lifetime 3650 --in server-root-key.pem --type rsa --dn "C=US, O=VPN Server, CN=VPN Server" --outform pem > server-root-ca.pem***

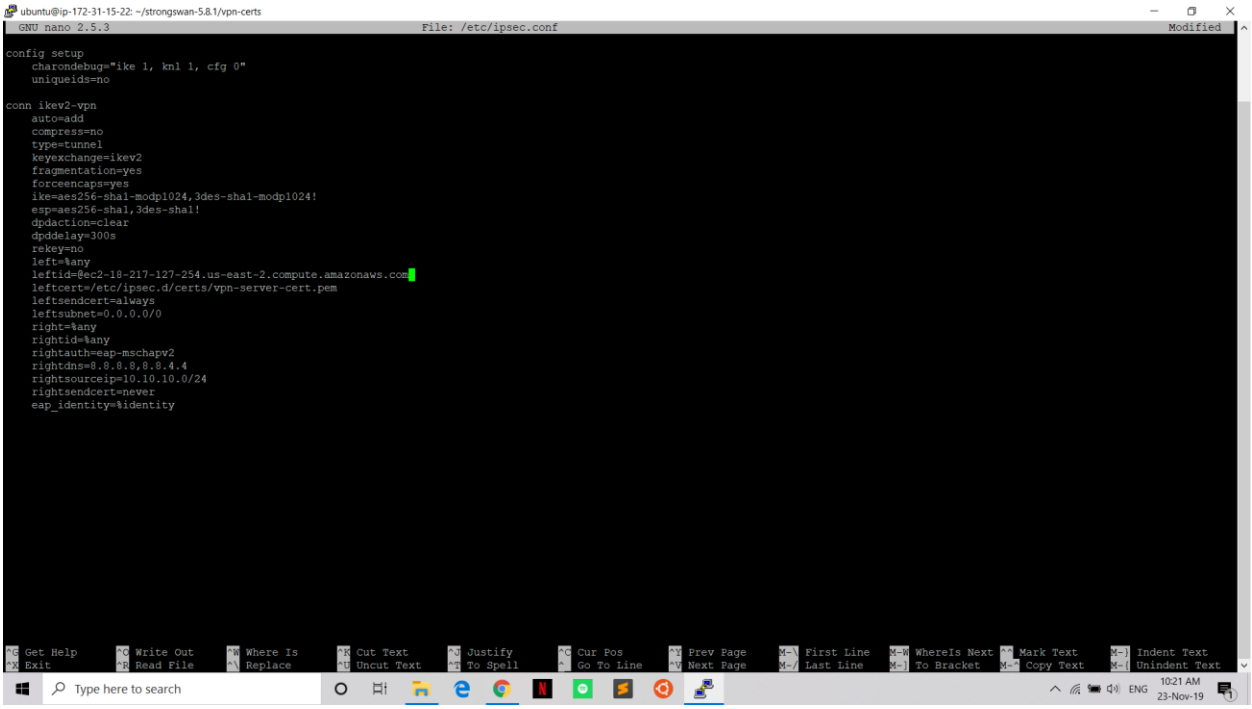


4. I generated a certificate for the VPN Server so that the client can verify the server's authenticity.

   i. ***ipsec pki --gen --type rsa --size 4096 --outform pem > vpn-server-key.pem***

   ii. ***ipsec pki --pub --in vpn-server-key.pem --type rsa | ipsec pki --issue --lifetime 1825 --cacert server-root-ca.pem --cakey server-root-key.pem --dn "C=US, O=VPN Server, CN=ec2-18-217-127-254.us-east-2.compute.amazonaws.com" --san ec2-18-217-127-254.us-east-2.compute.amazonaws.com --flag serverAuth --flag ikeIntermediate --outform pem > vpn-server-cert.pem***

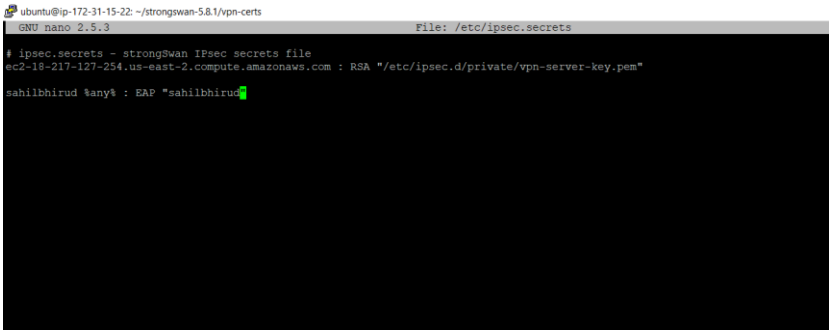
5. Next, I configured the Strongswan i.e. the ipsec.conf file



6. Configured sign in credentials in the ipsec.secrets file.

   i. ***ec2-18-217-127-254.us-east-2.compute.amazonaws.com : RSA "/etc/ipsec.d/private/vpn-server-key.pem"***

   ii. ***sahil %any% : EAP "sahil"***



7. I updated some firewall rules which I thought were creating a problem in connection of client.

   i. ***sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT***

   ii. ***sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT***

   For IPSec connections:

   iii. ***sudo iptables -A INPUT -p udp --dport 500 -j ACCEPT***

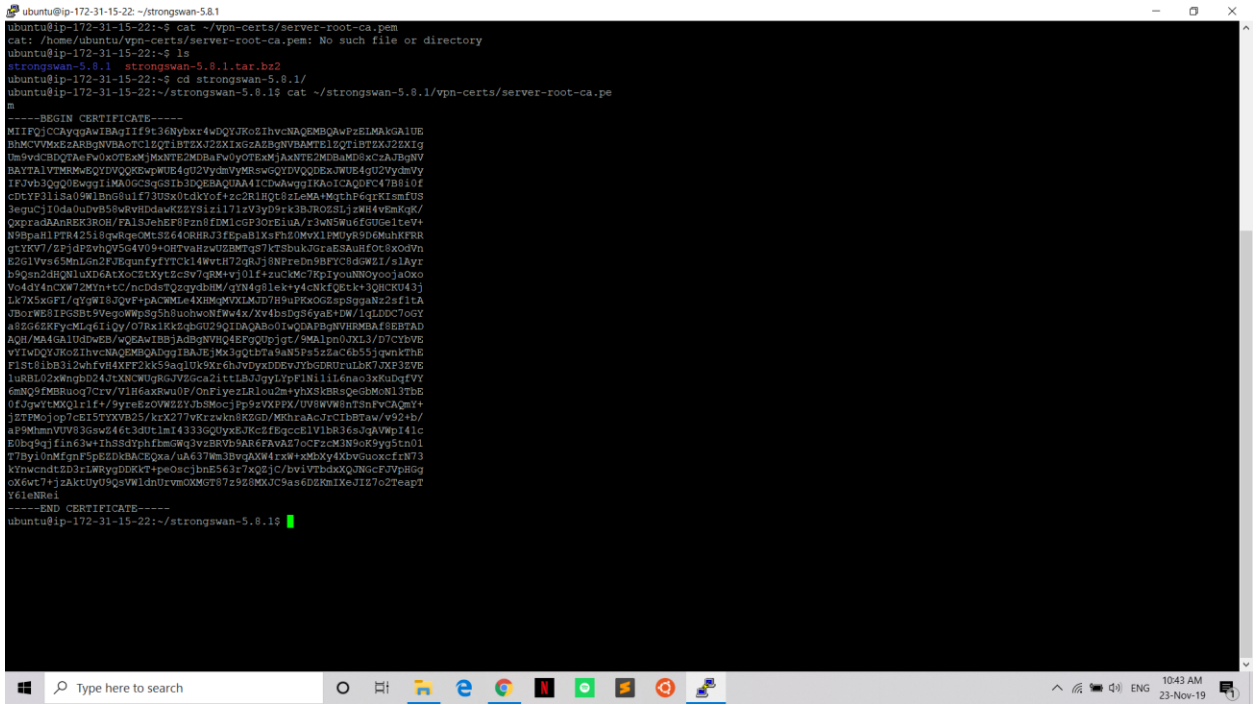
   iv. ***sudo iptables -A INPUT -p udp --dport 4500 -j ACCEPT***

   Configuring Masquerading:

   v. ***sudo iptables -t nat -A POSTROUTING -s 10.10.10.10/24 -o eth0 -m policy --pol ipsec --dir out -j ACCEPT***

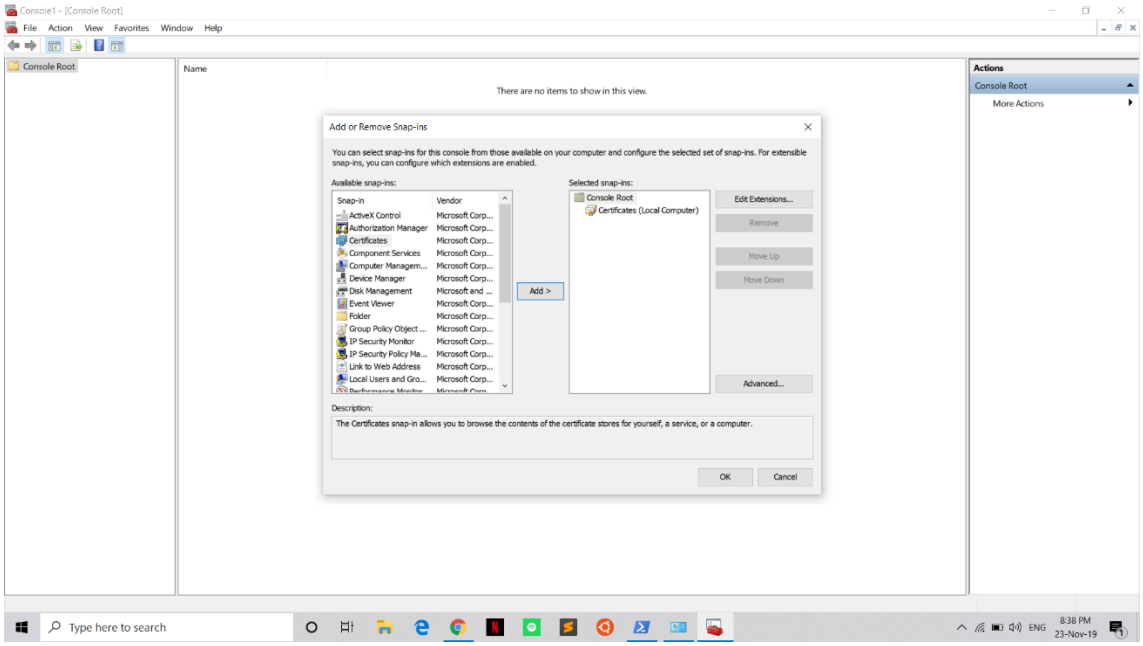
   vi. ***sudo iptables -t nat -A POSTROUTING -s 10.10.10.10/24 -o eth0 -j MASQUERADE***

8. Next, viewed the root certificate and sent it to my host (Windows) PC using the scp command.

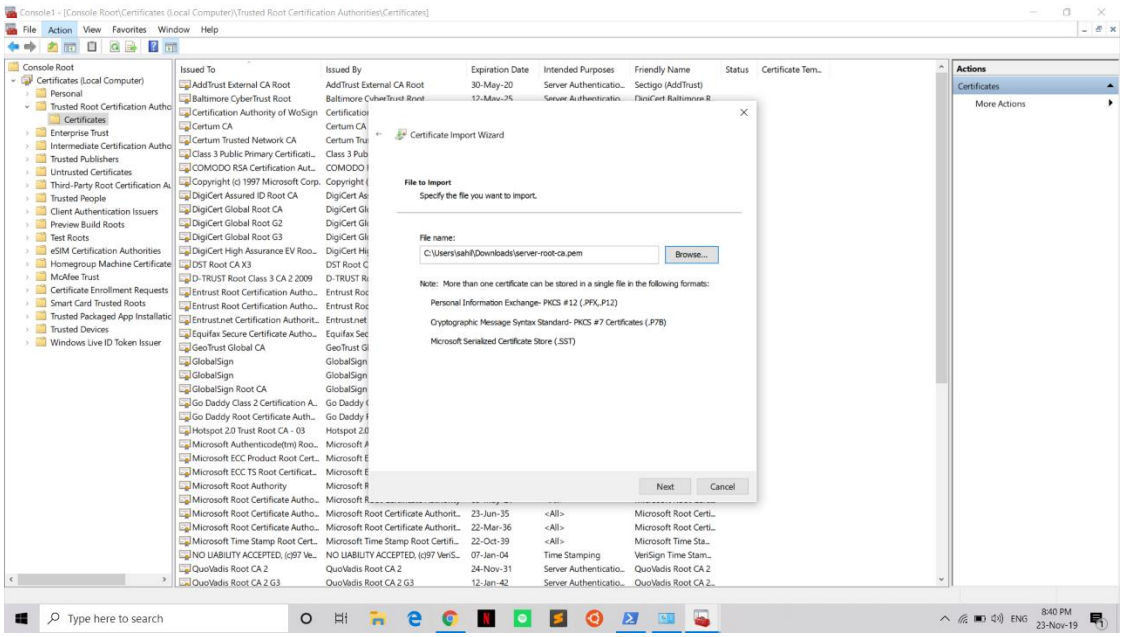


9. Following are the steps I performed on the client PC to set up a VPN connection:

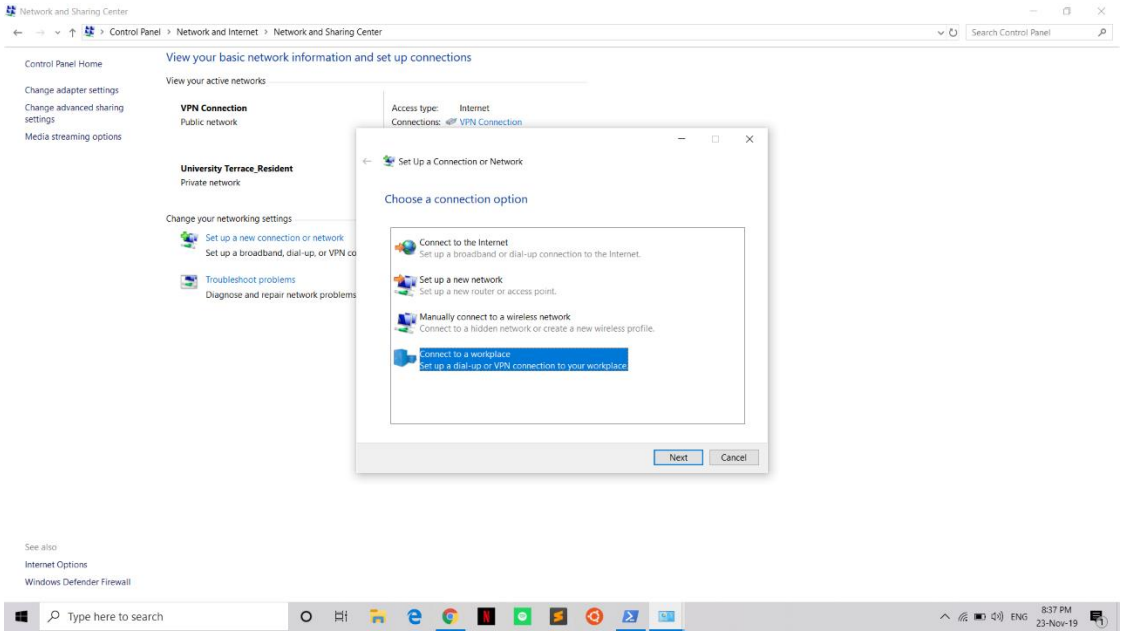
   i. I opened the Windows Management Console and added the server certificate to the trusted root certificate authority folder and saved it.



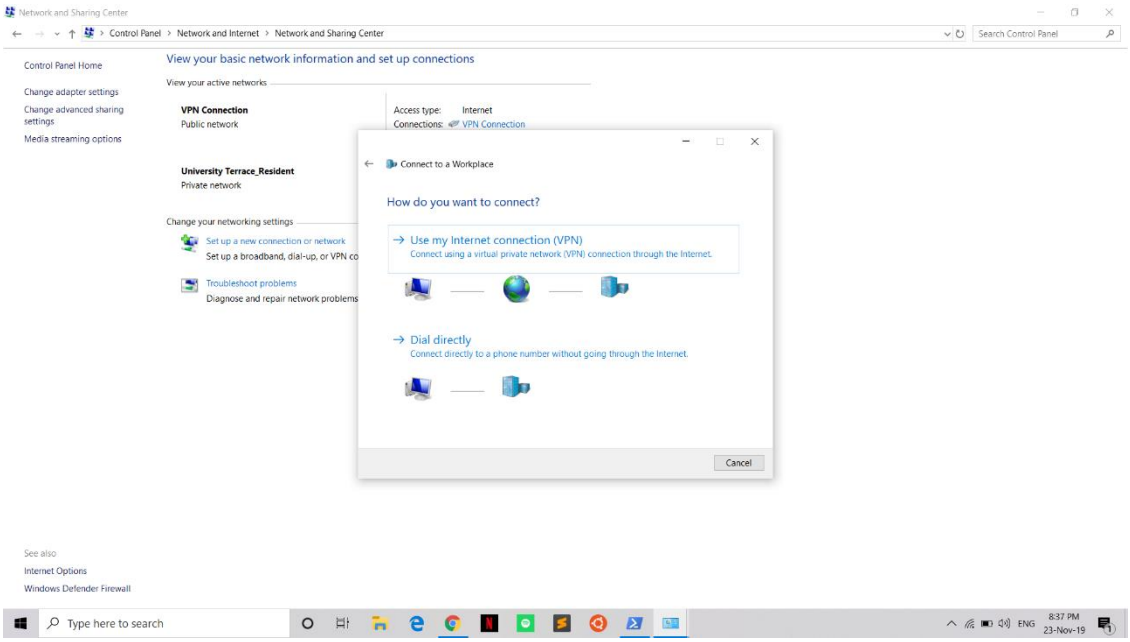
ii.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Autho
Certificates
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
eSIM Certification Authorities
Homegroup Machine Certificate
McAfee Trust
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Packaged App Installatio
Trusted Devices
Windows Live ID Token Issuer
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
Status
Certificate Tem...
Actions
Certificates
More Actions
Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
C:\Users\sahil\Downloads\server-root-ca.pem
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next
Cancel
Type here to search
ENG
8:40 PM
23-Nov-19

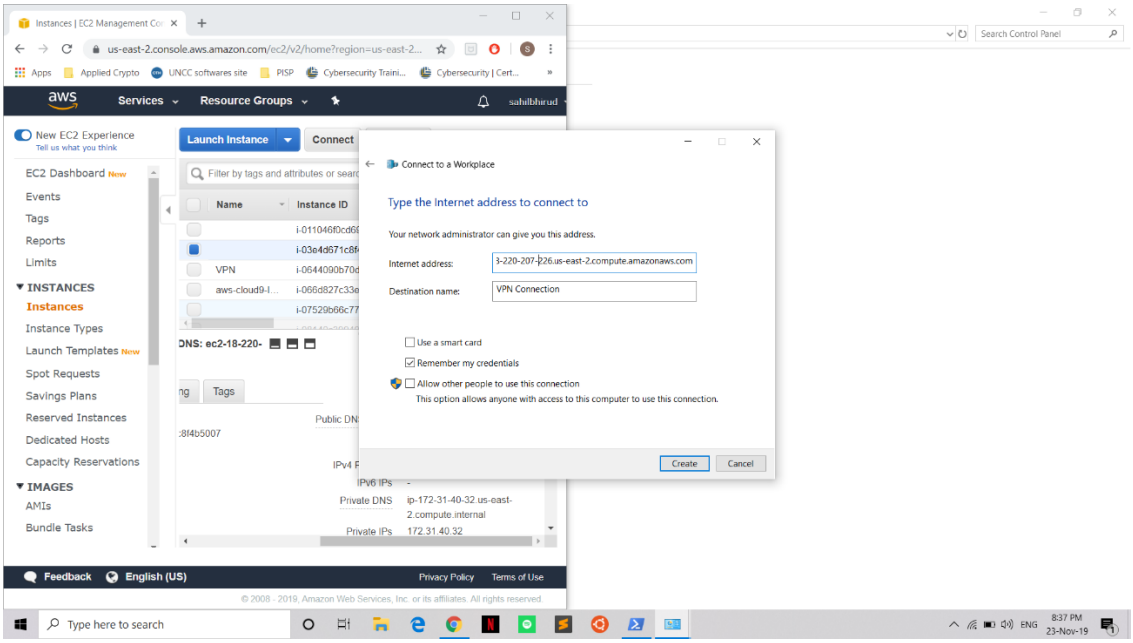
iii.


Network and Sharing Center
Control Panel > Network and Internet > Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
VPN Connection
Public network
Access type: Internet
Connections: VPN Connection
University Terrace_Resident
Private network
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN co
Troubleshoot problems
Diagnose and repair network problems
Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel
See also
Internet Options
Windows Defender Firewall
Type here to search
ENG
8:37 PM
23-Nov-19

iv.



v.



vi. Then I saved the file and connected to the new VPN Connection.

ubuntu@ip-172-31-42-88: /var/log

```
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[NET] received packet: from 173.95.57.197[4500] to 172.31.42.88[4500] (144 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] parsed IKE_AUTH request 1 [ EF(4/4) ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] received fragment #4 of 4, reassembling fragmented IKE message
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] parsed IKE_AUTH request 1 [ IDi CERTREQ N(MOBIKE_SUP) CPRQ(ADDR DNS NBNS SRV ADDR6 DNS6 SRV6) SA TSi TSr ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[IKE] received 59 cert requests for an unknown ca
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[IKE] initiating EAP_IDENTITY method (id 0x00)
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[IKE] peer supports MOBIKE
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[IKE] authentication of 'ec2-3-134-106-117.us-east-2.compute.amazonaws.com' (myself) with RSA signature successful
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[IKE] sending end entity cert "C=US, O=VPN Server, CN=ec2-3-134-106-117.us-east-2.compute.amazonaws.com"
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] splitting IKE message with length of 2108 bytes into 5 fragments
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] generating IKE_AUTH response 1 [ EF(1/5) ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] generating IKE_AUTH response 1 [ EF(2/5) ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] generating IKE_AUTH response 1 [ EF(3/5) ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] generating IKE_AUTH response 1 [ EF(4/5) ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[ENC] generating IKE_AUTH response 1 [ EF(5/5) ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[NET] sending packet: from 172.31.42.88[4500] to 173.95.57.197[4500] (544 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: message repeated 3 times: [ 11[NET] sending packet: from 172.31.42.88[4500] to 173.95.57.197[4500] (544 bytes)]
Nov 26 05:58:18 ip-172-31-42-88 charon: 11[NET] sending packet: from 172.31.42.88[4500] to 173.95.57.197[4500] (192 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 13[NET] received packet: from 173.95.57.197[4500] to 172.31.42.88[4500] (76 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 13[ENC] parsed IKE_AUTH request 2 [ EAP/RES/ID ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 13[IKE] received EAP identity 'sahil'
Nov 26 05:58:18 ip-172-31-42-88 charon: 13[IKE] initiating EAP_MSCHAPV2 method (id 0x77)
Nov 26 05:58:18 ip-172-31-42-88 charon: 13[ENC] generating IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 13[NET] sending packet: from 172.31.42.88[4500] to 173.95.57.197[4500] (108 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 14[NET] received packet: from 173.95.57.197[4500] to 172.31.42.88[4500] (140 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 14[ENC] parsed IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 14[ENC] generating IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 14[NET] sending packet: from 172.31.42.88[4500] to 173.95.57.197[4500] (140 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 15[NET] received packet: from 173.95.57.197[4500] to 172.31.42.88[4500] (76 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 15[ENC] parsed IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 15[IKE] EAP method EAP_MSCHAPV2 succeeded, MSK established
Nov 26 05:58:18 ip-172-31-42-88 charon: 15[ENC] generating IKE_AUTH response 4 [ EAP/SUCC ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 15[NET] sending packet: from 172.31.42.88[4500] to 173.95.57.197[4500] (76 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[NET] received packet: from 173.95.57.197[4500] to 172.31.42.88[4500] (92 bytes)
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[ENC] parsed IKE_AUTH request 5 [ AUTH ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[IKE] authentication of '172.20.5.238' with EAP successful
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[IKE] authentication of 'ec2-3-134-106-117.us-east-2.compute.amazonaws.com' (myself) with EAP
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[IKE] IKE_SA ikev2-vpn[1] established between 172.31.42.88[ec2-3-134-106-117.us-east-2.compute.amazonaws.com]...173.95.57
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[IKE] peer requested virtual IP %any
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[IKE] assigning virtual IP 10.10.10.1 to peer 'sahil'
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[IKE] peer requested virtual IP %any6
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[IKE] no virtual IP found for %any6 requested by 'sahil'
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[IKE] CHILD_SA ikev2-vpn{1} established with SPIs c199a93c_i f2a4cd74_o and TS 0.0.0.0/0 === 10.10.10.1/32
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[ENC] generating IKE_AUTH response 5 [ AUTH CPRP(ADDR DNS DNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
Nov 26 05:58:18 ip-172-31-42-88 charon: 16[NET] sending packet: from 172.31.42.88[4500] to 173.95.57.197[4500] (236 bytes)
Nov 26 05:58:46 ip-172-31-42-88 systemd[1]: Started Session 3 of user ubuntu.
ubuntu@ip-172-31-42-88:/var/log$
```

VPN Connection
Connected

University Terrace_Resident
Connected, secured

Properties

Disconnect

University Terrace _Guest
Open

BeerRaja
Secured

URCIUOLI
Secured

Network & Internet settings
Change settings, such as making a connection metered.

Wi-Fi | Airplane mode | Mobile hotspot

Type here to search

ENG 12:59 AM 26-Nov-19