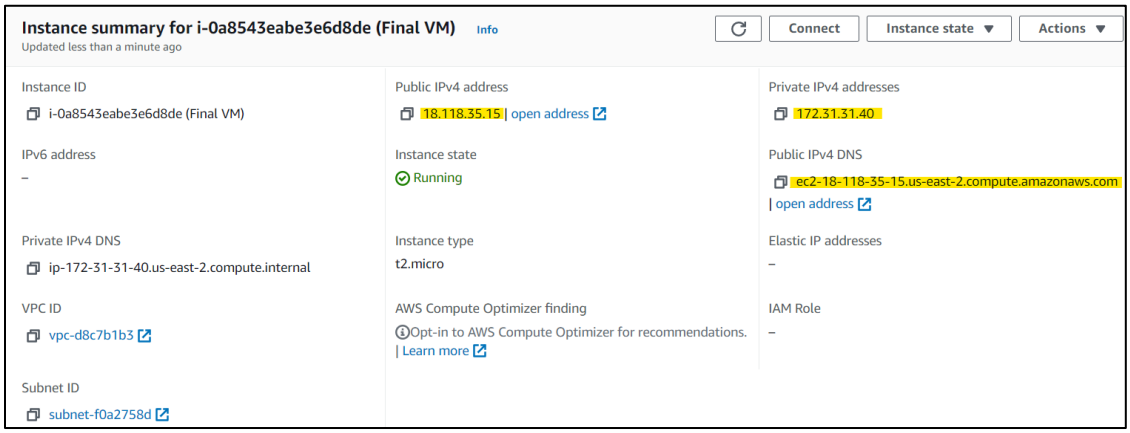
I used AWS EC2 instance and created an Ubuntu 18.04 VM. Below is the screenshot of the instance details -



1. Below are all steps and command that you used to install your StrongSwan server.

   a. Firstly, made sure ubuntu was accessed with root user using command **sudo su**
   b. Updated the instance to make sure it runs in the latest kernel version and updated repository indexes:

      apt update && sudo apt full-upgrade -y

   c. All the prerequisites were installed using below commands to install StrongSwan
      apt install libgmp-dev
      apt-get install -y m4
      apt install gcc
      apt install make

   d. Downloaded StrongSwan

      wget http://download.strongswan.org/strongswan-5.9.4.tar.bz2

```
root@ip-172-31-11-41:/home/ubuntu# wget http://download.strongswan.org/strongswan-5.9.4.tar.bz2
--2021-11-10 21:07:31--  http://download.strongswan.org/strongswan-5.9.4.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-5.9.4.tar.bz2 [following]
--2021-11-10 21:07:31--  https://download.strongswan.org/strongswan-5.9.4.tar.bz2
Connecting to download.strongswan.org (download.strongswan.org)|152.96.80.46|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4651000 (4.4M) [application/x-bzip2]
Saving to: 'strongswan-5.9.4.tar.bz2'

strongswan-5.9.4.tar.bz2              100%[=====================================================================>]   4.43M  4.15MB/s    in 1.1s

2021-11-10 21:07:33 (4.15 MB/s) - 'strongswan-5.9.4.tar.bz2' saved [4651000/4651000]
```

   e. Uncompressed the file using - **bunzip2 strongswan-5.9.4.tar.bz**
   f. Unpacked the tarball using - **tar xvf strongswan-5.9.4.tar**
   g. Navigated to directory- **cd strongswan-5.9.4**
   h. Configured StrongSwang using - **./configure --prefix=/usr --sysconfdir=/etc**

i. Built the sources using - **make**
j. Installed the binaries suing - **make install**
k. StrongSwan is installed as seen in the below screenshot.

```
ubuntu@ip-172-31-11-41:~$ ipsec version
Linux strongSwan U5.9.4/K5.11.0-1021-aws
University of Applied Sciences Rapperswil, Switzerland
See 'ipsec --copyright' for copyright information.
ubuntu@ip-172-31-11-41:~$
```

2. The process and screenshot that you generate the root keys etc.

a. Created a Certificate Authority

i. Firstly, a directory structure was created to store all the assets
mkdir -p ~/pki/{cacerts,certs,private}

ii. Locking down the permissions so that private files can't be seen by other users
chmod 700 ~/pki

iii. Generated a root key which is a 4096-bit RSA key that will be used to sign root certificate authority
ipsec pki --gen --type rsa --size 4096 --outform pem > ~/pki/private/ca-key.pem

```
root@ip-172-31-31-40:/etc/ipsec.d/private# cat ca-key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAulzasDH54k9kLrUQZGHbgz67ZLCP+h2lvIw9ijyDsrWFfzzi
zyhj+/+Y7Wpy6MfPSosAiUJNHJd3b4jVcJg5MTejozo7WBs5WR8tHYPp37mZvZUf
LNDm8ypoFN2E55jWcGhZaVQTiGfQCMy2656zyY/3EBVaIA6KlAqxx0HDU66iYB/d
ZriXK6+oU0pLaHbhgtdkspDxRG6E+jJ2aCVfYt7BEUAuMM9TYmSSIvrN7l0+hotj
3PRnPeqd2+m7eS1BgNPGzVE4B+SVG2sZOF3lMihdmTMNDZFE5C2MKObSzoKu37oB
d3AHAPj900fox7hNQSDf5wLqJox0PiigKmvvNtRinvkSW5uSNWF0qUg/sGFSmuew
cEpT84SNq34wxcgwn8sc9b7p2ccm9/aaQ4rfeflzOCYA70LhDV6CWjA2ur/2D079
HGHL/JGQW6X/7XXmxFHCFEtEZ2J7lF/VCtXrM3ZpGZg1LS7qEH3F8R8EhSDcy9QZ
09tPto9AUICGaWE0OurNsRv6qk1MwF41xUCYBphzpkpLozCFvc12rXQyM37kRopL
uamA4S+5DCQyJeFnIaZLsfFnvrjHxvNnPdTKuY7gv7YxHlXgueJ54DhtZ+oTgrUo
4/v0FoE3IQyBvFlSmdLIjGblCaxWnDhDK5KY0TJ46d0npCqDpbVanF9K3y8CAwEA
AQKCAgBgz623TC7wdqenb931F7TN6D+23dXda5tWaE/ryOXtZ0jTQVDdprDSDwRl
iR/qdynjInSD2VJvoOuloCKo3BsRy0KRn8WGTpYrCvwH0igjVapdBuNsB5WCCqyI
8k6BdS8os7yG7+s5uBwlBhucKRRiiAwjacQo1QT+RNP3m90ZUqX9Y3BDVW8KfbTm
l7i2qtMZgkVIUe1TzEn+I0rJbWiw1uDa0klsh7dcbLxRuZJS2lOJ101oUfpz+rZI
sJH4MB9QCjPDIwcFaqRe2vL+CiDvPnLpC9EjFC0Cj/q4oLgwGUk45cqvPh4VTkOl
hzyQy9guFiLaQfRbVClqxPX3M5zPLkZyeGgXOKELzESkh6tfvUl16IcXuX6VaI1+
um84B5+onDSRiGqNHJAO+V9ixWXE/HFZ5YQO4Qm2sVub8UVl1yWbaBQZ6r/XrsKS
7BtuhKhfXY9p+8iHEd4GNiJrGNGrTj61UCQva28tKx8DV7G249/KSL53eBm+Jbzq
VRvAobiuUSO432MfBjFB9vMoC4Ohmcn6z1Nyc/QvNEncl2qOVR+tKvjmlquSL9Hn
hF8riBOZGt8UcPubyUJ8n9LSKZqQ3bOWWedhYJus/r6d/aNgQVj+CRmwsZqQphlQ
JAfKE4sEXq8IBAotcyYtSE0fzEmmvhIEpWjo0jWzp3XAqRc8wQKCAQEA6/kU9NHv
MIdjDpIoLNuBELcchSjmzLCecckExyLzP5f38ybzQL5kmzIzkv2Ivxmp/3kjn/J0
aUmLfZeE8BrznDcwQ10fkj4x5zscHH7AZ69Az8MpcFP3NlU2/RX0qUpNNcebdw0o
/fyNNpD+6PnW6XE5LVMTFzemAdpUSladza/Strqlx8Fg5e/uGtUCit5UN3aRrF04
QSgIFmco8DIWaxE/baZllu7ePqOfimMZwMg4EX59Cq0eUIuWvRJAMJiV2z/OWwCR
Jx+WOzrUHO52LhY9zt3wNyuuf3JHV6fSNewb/W1lfESWRGdxugtpG40RmUBLF54j
hZEj4NjFQLzHIQKCAQEAyi3neiFH3FInzXihwQ+QtZ9P5lDDcFdfGIGZHOXgIzDz
+LypKWrT5qfPF/TL54XhC0bQTuENRpMM4f2GLTtrP2veCFuRaVQhEw/mCvytrNsP
0FuTW3kXJYqzK5gPEv0piYgpt5oXAfba3r7AdQBxMQ+nXv9bnhLzFmUaPnDuRHhl
7xNWYUFKt6F1MXsSOwpRz5C+QO3ACYlYFEdjXDitReOJz22PVEBrPcBcj0qZr9m2
lpjr5uL0h0IjGJEOa+/zG+Hwy8urFm24q7koZMkIyJcPz751ztl1YQiEJ6yE0Y7P
wK6a8PTpyEqZcGbJG+/OTwVct6yxHSZB0NO9yZfsTwKCAQEA0RkZictRUUZW731x
3jXvyzkHK7PPuIe1Dwzaj/8XXz2xeCQGn1NW4PL+In1JJFWAfyIAAGae4wFJetO9
9+lZ/w4kVTz6keNM4yJMya9DnVz9aFz+pkuxHtMp89/1ueFeQ46J41elAFM/ap/X
Uei5mIg86z3XB9bG4pNuceFE2hO3+zWvWy+vRnFyIxKnuxhBthf6A6tjAtGPQRLO
gvFPTjatZuNw1+r4wrbIO573Hg4NKOtVsBUxbJwUyZuXh7hd6jdDCv6YoPtraza4
6J4h2LrasCmYB7tMWCCSuUi7jA6ZytqaeCBqq1iivQIJdGFvu8XuBJKb1WqESWSs
fa4KIQKCAQA9ozkK1tKdrL5NuhU2UpR/io5FXSH4QerQAdK4KKzojagTkRDRe6wW
idptJ0hy0TIGyhP/uETf2zz2OOCLMa5Eq5IJYkE2p1teAF7VwqsAI9jyYLjQDl6s
JpXTGIyf8WaUc1qkiumww51+gxERmoztCoGoDtCOey6SyBxIOTDIyGQfYi8Jbet
vB+KckbgkQjYCvy1tsXxIloj9I+qMe1BfVkqT/B+cxU+wkJ1vPyVy/4Kc5yXy2FZ
SyR//Nk0tvaa7YsH1pPWRqUiVVSnRVLUNJmxcBNieJF8f6gqoEHt0WgtCg5an5AW
bAfTaMKvLbDsDmpx5MgqZttx2tvlddepAoIBAG4ahySTnCnmd60pn8pGe1mBt2z2
aaejYRVW+T2GyHN2r0HLK1Qg8bRMTy0iRXR1gmwun5R5oqEkoqRBRj2xYe+Lsjwl
s3XHEEJw9sxo1NOALZtEx192tNYbNXTzXbd0tbqZBYBa1dWxgdAT9mhmsf1pZYY6
EgrBAqDBsG+RY+u+xP6jXtWaBMhG4GBwPfg2KeLYhoXAudsP4dZPrQRBR/2qE4Kd
x9PmmaOOKEd+JgemYb35uDZjhxbZwgkvQWTuIk/rkGVthzCOFU9enFlkvLKow+hJ
OlKUe84Ibg81CwbHrnFIiomhvVYxVz2prFuSZY3iMSBjXFVdK0Tty42sBcw=
-----END RSA PRIVATE KEY-----
root@ip-172-31-31-40:/etc/ipsec.d/private#
```

iv. Created root certificate authority, using the above key to sign the root certificate
**ipsec pki --self --ca --lifetime 3650 --in ~/pki/private/ca-key.pem **
--type rsa --dn "CN=VPN root CA" --outform pem > ~/pki/cacerts/ca-cert.pem

```
root@ip-172-31-31-40:/etc/ipsec.d/cacerts# cat ca-cert.pem
-----BEGIN CERTIFICATE-----
MIIE8DCCAtigAwIBAgIIfbjKP5YNnjgwDQYJKoZIhvcNAQEMBQAwFjEUMBIGA1UE
AxMLVlBOIHJvb3QgQ0EwHhcNMjExMTEzMjExNTE4WhcNMzExMTExMjExNTE4WjAW
MRQwEgYDVQQDEwtWUE4gcm9vdCBDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCC
AgoCggIBALpc2rAx+eJPZC61EGRh24M+u2Swj/odpbyMPYo8g7K1hX884s8oY/v/
mO1qcujHz0qLAIlCTRyXd2+I1XCYOTE3o6M6O1gbOVkfLR2D6d+5mb2VHyzQ5vMq
aBTdhOeY1nBoWWlUE4hn0AjMtuues8mP9xAVWiAOipQKscdBw1OuomAf3Wa4lyuv
qFNKS2h24YLXZLKQ8URuhPoydmglX2LewRFALjDPU2JkkiL6ze5dPoaLY9z0Zz3q
ndvpu3ktQYDTxs1ROAfklRtrGThd5TIoXZkzDQ2RROQtjCjm0s6Crt+6AXdwBwD4
/dNH6Me4TUEg3+cC6iaMdD4ooCpr7zbUYp75ElubkjVhdKlIP7BhUprnsHBKU/OE
jat+MMXIMJ/LHPW+6dnHJvf2mkOK33n5czgmAO9C4Q1eglowNrq/9g9O/Rxhy/yR
kFul/+115sRRwhRLRGdie5Rf1QrV6zN2aRmYNS0u6hB9xfEfBIUg3MvUGdPbT7aP
QFCAhmlhNDrqzbEb+qpNTMBeNcVAmAaYc6ZKS6Mwhb3Ndq10MjN+5EaKS7mpgOEv
uQwkMiXhZyGmS7HxZ764x8bzZz3UyrmO4L+2MR5V4LnieeA4bWfqE4K1KOP79BaB
NyEMgbxZUpnSyIxm5QmsVpw4QyuSmNEyeOndJ6Qqg6W1WpxfSt8vAgMBAAGjQjBA
MA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBT/pS6u
MXAXdGyZYQSQ2LEOXjCCczANBgkqhkiG9w0BAQwFAAOCAgEAaSJuMZrZxBUsZx0U
DxTcZYUb3xvLMHgKsPIOkfUMLQ6jZlY0+CplPeFNBBcVz2db+K+O/xkdq+0dIL7g
NA/1AK9qe3rtlfvmqiqGIeoWffrCzMg+nAJpC0Bhd36Sms162zXpPBtr6qPuDXqo
cBwQZJv7qEoAYYqw4J4e8EYSKKClLlwWdn269VUpONRUnN5XDDNwrrJ0cd+Crxar
f3i9bvkRPZPDb9Ffr5QUtiiK6AMCb44N9pfKLKRRKyduzp4zIeqgf5I/0lqASNmC
ucBShfFfHcxWeCzh+3Sj9nWJKK5y+AEg56QK1vQ32jPPZZO5PwxD2TTSD3grOJ01
wLVQhihYUrP6B+4hxnMgUh36ZAqZddwXrvN4bqwsiTpcHIKuRBo9KgcUlr619/I/
37nY/rFPmwKd0vc+2npdEOxCRVcXbU7gcwl8QRYVjZluWvMk/899Kpv2jzurbOTC
mHqrWAHoFmjIiOiE4z8L/9HlhiioEuSXh3Cv8bxtA0j0YwLFAYY68zo8/l63PV2L
UjNSZRV2qldhJFM9bZzPplUEMvQ3N7tq4JSL2x6IRCrdrZ9eg+8/vzPvv58JUwuU
b7ogCgku1J8kjOKa0jATwxbqsFT9acnBZTvjYA1gqvY+KiwzmK+kbx675xddhVz2
+b1ml3aIPqccZk5KNyRQgggmmM8=
-----END CERTIFICATE-----
root@ip-172-31-31-40:/etc/ipsec.d/cacerts#
```

b. Generated a Certificate for the VPN Server

This certificate will allow the client to verify the server's authenticity using the CA certificate created in above step.

i. Firstly, private key for the VPN server is created
ipsec pki --gen --type rsa --size 4096 --outform pem > ~/pki/private/server-key.pem

```
root@ip-172-31-31-40:/etc/ipsec.d/private# cat server-key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIJKwIBAAKCAgEA7gcCR+N+/t46KTDMO5GVI7UTTJ/uY+2kwkQvkwnRYBxDQ3hA
k4jxQGxZBrH0DO3WI+HWjI9qFF7QEbOB+wOikdwMgLrANtjYSNtXd9rHAyCYI4NK
Ke+5bfGFtTtL6VrsVqAkQmsUAkd1ciMQp7J3Xit6A0RmfMQu6iHnTIBcwZuuWIYe
wytz+G/EWXCj3aux9DLRUwCPjyrI4Lp0XhbGpzNyn6pqv6+8TVSHiEQxkI6eTLz/
BUcksVPLKawChM+oHok5pDfAJQqzLlt9tXi5MBb9ewMCYIr7LWtYUmgARkIr1oE1
qZNI7zRvEnAf6jw6fX4ljH2c+OBHYL1gnA58a2EFzb05RbI6qGgLLXqNjfgTphXe
zwQguaRdfpj4uPBaa9zBKDPbeWN2T7jv3daxCXa4/YhuvZ8ysi/MEz5c2ePZEJKh
j9kBwQFsyRlJLgsEYIthZv3cpCfeW/nnNqbAFQ4LaKOi3RYueFFG1EeH0IHRU54D
FpkZi1fAgxlyXdT+L+WJeDKGeLoptQ3o5q4sxoZo5xEeAFGCFBcW4WW7LXbar732
3Hqo9VDbwwJxSB3RXXwv3T8cQDC6dylRNNWQyu6mphH47EgikFpxSn4aua1rVHhJ
0v3xjG/ffW4MxftZGC5Qtzrvx3/YVf8fO0MBMR+E890tFnJHFURFxORMLqcCAwEA
AQKCAgEArWhbyAW74nABzTpov8kK7w2fNsaZBSH/UywbwLJ5X9yXQFMeMJ2mrLmC
jjccxkKLLG7+QD7HGHoOeabePgHi8QJv9WSYXhzSTRnG+mFfdS7Mx6qBYFXuMGOx
dlvxrNr5rQ5T/DNIS3TF4lYbbyC8h9WCuVielazTRO1YNcqaSM5jUMi9JpDElyzN
zh8asobASViwWRjifXm9CMOtvVI4fV0k159uz6F2vJuldafAuEC+oMdbvvuahrm2
G/DdkOY746szXCjlidbmvRIYXhnKSHenSXPiynTWErvOh5KPCKBykX5mmtjbXLFF
bhhTl/Ey53P8ZQKqVkIGnjq5ZFfFWYl8NO2x5vXLVMWUsosOrso6RuQ+C4r9vo1i
m7T0wGb7SrZ1n4deJF0RCcVN4ptZsFQPZZOBuGqxEkeQ4Et0tfrlZ0g9dguxaf9s
X3bjNxt8SCsGlpEIzfe8+siQDJwVy/q5bSpah8l4PWgA6CWg/9Ye3e0tPnCgxj3m
QrfNlJuW2cgYq5x8l4hJZ+i1CQWfVYwIhqB1/HdlhjV86k8A9UY8CmFXU+bWQmda
EKUC0byvOOOUu4Vag4bJQjyFohmG23xlO9w+a0cMCvZs0e/Tfk35W89D+w4Omrqf
x6fl/Gc6tcqH3+8coigHuGRdZq/PNJ+s1eA6zcQj7yxbyL8J3LECggEBAPx3+d9o
J/sata79reHYvZJQpfqAvmz9B3AU7j8yaPseFjJ/ixvAJgKFLMH/aKsW6P+WGSYA
7qhwjcr0SvtGFjetNM3WBhEPaktOYXDRNJP6ONXX3/WHDEJ+sagvQE8mOY0fPQoJ
GBe1Iwdb4oS3Cb7H2+1FtC9+WKThptFM/nV6yThHNl3HiERVXQqTO4tQO+H4wO+5
zEabPRzbHMI2GELLfVnjfFmMHd6+jbtO8ARYybg8TA9WEbTJ17wpNW+zIIDVKX2+
PmuDg3Kp+2/FGuyMhL9l1K7uLLAuF8dSp6B6ZDBME1Ktlc3tmmUNrgi6nes8GUWt
+VSQ1R6OABJToQ8CggEBAPFbUoo6Hk/nIvrNXBTFruL51GkhVoedjR2n3USvJblu
fZ9m9XI9nFB6oAxyh8/ltW8h8I5ryvY21kCys2B1/9mvjJObbNIvbBWgePWSxHsq
iteWCI3949v8RT78PR4SZseGWDjkJHzuqp7qvsRpni7X4ZYIGnlEV7fsjn4CW5C3
WuhrL3tn+dKZl+NEEo0oWfXeHGYYLw81Eh+lxxhLIB0Wb/bILhjrP7P55SwBmHMH
mGNstiUptVJP2phg6PaU4mTvbldAzK80eTeKyF0Y5ZdbCQEp5iioFFmFUkk+4uQo
nvpeV0rVIiBGRzp9akMYsQ3angeaZ8j4UTUCjg436OkCggEBAJvdRfpSxzwTBU9/
dbYUpRSLjazVhrqqi8j6YwvJB17g+Ds82pjLS6wKo9Mw52GYx0fjVqtLsAt1UVSW
9SOj5VuCJzNcimpF5g2P2kBYJ+mjdSswFyfxs/PpW6zFXyJ+KtGhE4H6k1EvluyY
IYRlrDKIGJKnkdIwYnGIjgBxVDcbEtcXv8ytvsbRHJvGweAELLQZaqOVRTPh6xzB
eUO9OcUi88Rm2QI/qsE1SzL0TOGiHwcK0ro1HMFMS0/y8PaA0/Q1pWPn64lcq+5C
WuRp/3FCX0H6kA9fI1+xVSTNNoewh+H5VYSZff6gTc1NYMAq1gvAEqod+evnbmtq
p0ipMKkCggEBAO7+/zzhUCLPPlQcBpKLLiKUQUHZQVYJLTOwher9hN2aC8tMqL/3
QlJvGw04XEQBsyfY89wT4Wbt5jsquXVLY46rxwhjX97CFsVTonOKYgWUmufgKZhx
ULEFnYxBOkQM9Lmezr2HLJqJu2qiCUV1UK4SF8/5Nj3e7v2xwWgF7aXf6qU7fkk1
LKzeawkg3z3oNyzARF7Uk8T7SHcOMZhcy/ABx90XXI5QZURSsBxjeBJv8vaBL9yc
8HARouRBEm8Z/xT0As9j20ujKmVViBKoFLFL9B6y3rZjucLrwg/Ftec4UjSaNtZj
Nue+r8m7Zv4J9UlCsjnVK/BV9BQJ86EgvAECggEBAJJ7SBLN7+GiNyS5OG4QdY9Q
QcAOr0Tn9iitzt8z9VdKxe8ZNGBMtgZ+nNMH5IxogE8fm3IuWsqS6jpaEs3duyRO
aUkMm1yQ5oYQpYQe41pmVtI/9EJDNdzI0EMPQm3cZ16sMTc8W4qid+J6SJY3A0TU
ss76mmzCcEvQXYPnNbmaFHkWT7oxeZsPdlkdXx6DuQ+/v0O9gwbfE/QIdTtXYBni
aAMtc0eZUW6K77U69LFLO78sFT8g1Zzyk3f4vHD+tzaec0ZjbAnK9JJgunxw+f5H
jk1jTWxPSzQSFfobrmbVth2jARZUvWrVlj4gRxsCksU/c0XEq5PQkz3BKaJb3B8=
-----END RSA PRIVATE KEY-----
root@ip-172-31-31-40:/etc/ipsec.d/private#
```

ii. Created and signed the VPN server certificate with the certificate authority's key created in the step a- iii

**ipsec pki --pub --in ~/pki/private/server-key.pem --type rsa **
| ipsec pki --issue --lifetime 1825 \ --cacert ~/pki/cacerts/ca-cert.pem \ --cakey ~/pki/private/ca-key.pem \ --dn "CN= 18.118.35.15" --san " 18.118.35.15" \ --flag serverAuth --flag ikeIntermediate --outform pem \ ~/pki/certs/server-cert.pem

```
root@ip-172-31-31-40:/etc/ipsec.d/certs# cat server-cert.pem
-----BEGIN CERTIFICATE-----
MIIFAjCCAuqgAwIBAgIIM2rixluN25swDQYJKoZIhvcNAQEMBQAwFjEUMBIGA1UE
AxMLVlBOIHJvb3QgQ0EwHhcNMjExMTEzMjExNzEyWhcNMjYxMTEyMjExNzEyWjAX
MRUwEwYDVQQDEwwxOC4xMTguMzUuMTUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAw
ggIKAoICAQDuBwJH437+3jopMMw7kZUjtRNMn+5j7aTCRC+TCdFgHENDeECTiPFA
bFkGsfQM7dYj4daMj2oUXtARs4H7A6KR3AyAusA22NhI21d32scDIJgjg0op77lt
8YW1O0vpWuxWoCRCaxQCR3VyIxCnsndeK3oDRGZ8xC7qIedMgFzBm65Yhh7DK3P4
b8RZcKPdq7H0MtFTAI+PKsjgunReFsanM3Kfqmq/r7xNVIeIRDGQjp5MvP8FRySx
U8sprAKEz6geiTmkN8AlCrMuW321eLkwFv17AwJgivsta1hSaABGQivWgTWpk0jv
NG8ScB/qPDp9fiWMfZz44EdgvWCcDnxrYQXNvTlFsjqoaAsteo2N+BOmFd7PBCC5
pF1+mPi48Fpr3MEoM9t5Y3ZPuO/d1rEJdrj9iG69nzKyL8wTPlzZ49kQkqGP2QHB
AWzJGUkuCwRgi2Fm/dykJ95b+ec2psAVDgtoo6LdFi54UUbUR4fQgdFTngMWmRmL
V8CDGXJd1P4v5Yl4MoZ4uim1DejmrizGhmjnER4AUYIUFxbhZbstdtqvvfbceqj1
UNvDAnFIHdFdfC/dPxxAMLp3KVE01ZDK7qamEfjsSCKQWnFKfhq5rWtUeEnS/fGM
b999bgzF+1kYLlC3Ou/Hf9hV/x87QwExH4Tz3S0WckcVREXE5EwupwIDAQABo1Mw
UTAfBgNVHSMEGDAWgBT/pS6uMXAXdGyZYQSQ2LEOXjCCczAPBgNVHREECDAGhwQS
diMPMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQgCAjANBgkqhkiG9w0BAQwF
AAOCAgEAsF0JGpAbnaLYPwK1IEpsqkPQ33Wv+tLLC6rMU5EFyNyBVjuWKhV8yrj0
75fSHu8ATeuqJBYqyUqA2E1c9jqnJpL2ZRKVRukLjYdNlzYN/WTxM02JXIIJdrfl
HREVcLRYmZVCQSpUJE+TOOn2iwC/+Bkcog3ZXfY904TlD1aEjiMUnIXRG15ohvH9
2ZLxFmWvR79+7Il5NDOmbOvjxL0Z3je++Fw0sVG1DXhSR0cWSA0cC+9CyYmnk4Bn
+xg40vPlqoBniOuRSjq+mpTWOYeBBbmeIE+9aDCL04DWReZQ98pZDpbVYUcmVszn
LLhM1waPskJbU1TDTcyPfCHM14IooLgs9Ss7Q9x+NduEVRCvR+K3UJmGN9kzcE5Z
nCKp/PGb9vmnKl1xBv3mU+NP5TghmJq3fw67LpkYcD4HJgBLUDJV5MmQ20AGaRXO
pNx0wSAh7RoGrBREF+I5KjlLXQAhB0Q3BQyaL2nDYQLwFhDpn8F2sKQ2kRgE0kgX
03dtu1cP0QeAaN1qiIS1I71vSs4nVCOvXqplBrP0Ocz+XmMnDsE5Sq9yELICJA1h
9yh6njlz3ano9VHWQnEzgWRp7ZklvJkw+aN+LdDP+WZoPwicAX5HNTXFVtHGWwTj
rTSg6OWl3qOU5qHjRKP53l/XxwvGuAnAe+BAE9YBcx68EAvW4k4=
-----END CERTIFICATE-----
root@ip-172-31-31-40:/etc/ipsec.d/certs#
```

iii. Move the files into the place in the /etc/ipsec.d

cp -r ~/pki/* /etc/ipsec.d/

```
root@ip-172-31-31-40:/etc/ipsec.d# tree -f
.
├── ./aacerts
├── ./acerts
├── ./cacerts
│   └── ./cacerts/ca-cert.pem
├── ./certs
│   └── ./certs/server-cert.pem
├── ./crls
├── ./ocspcerts
├── ./policies
│   ├── ./policies/block
│   ├── ./policies/clear
│   ├── ./policies/clear-or-private
│   ├── ./policies/private
│   └── ./policies/private-or-clear
├── ./private
│   ├── ./private/ca-key.pem
│   └── ./private/server-key.pem
└── ./reqs

9 directories, 9 files
root@ip-172-31-31-40:/etc/ipsec.d#
```

3. Screenshot to show your StrongSwan configuration. That is, /etc/ipsec.conf

```
root@ip-172-31-31-40:/etc# cat ipsec.conf
config setup
    charondebug="ike 1, knl 1, cfg 0"
    uniqueids=no

conn ikev2-vpn
    auto=add
    compress=no
    type=tunnel
    keyexchange=ikev2
    fragmentation=yes
    forceencaps=yes
    dpdaction=clear
    dpddelay=300s
    rekey=no
    left=%any
    leftid=18.118.35.15
    leftcert=server-cert.pem
    leftsendcert=always
    leftsubnet=0.0.0.0/0
    right=%any
    rightid=%any
    rightauth=eap-mschapv2
    rightsourceip=10.10.10.0/24
    rightdns=8.8.8.8,8.8.4.4
    rightsendcert=never
    eap_identity=%identity
root@ip-172-31-31-40:/etc#
```

4. Steps on how you configure your client machine to be able to connect to the server (I need sufficient details to see how you make it work)

   a. In order for StrongSwan server to be able to authenticate clients, firstly we need to mention where to find the private key for the server certificate that is created. To do this, below line was added in file **/etc/ipsec.secrets**

   : RSA "server-key.pem"

   To define user credentials, below line was added

   shivani : EAP "test123"

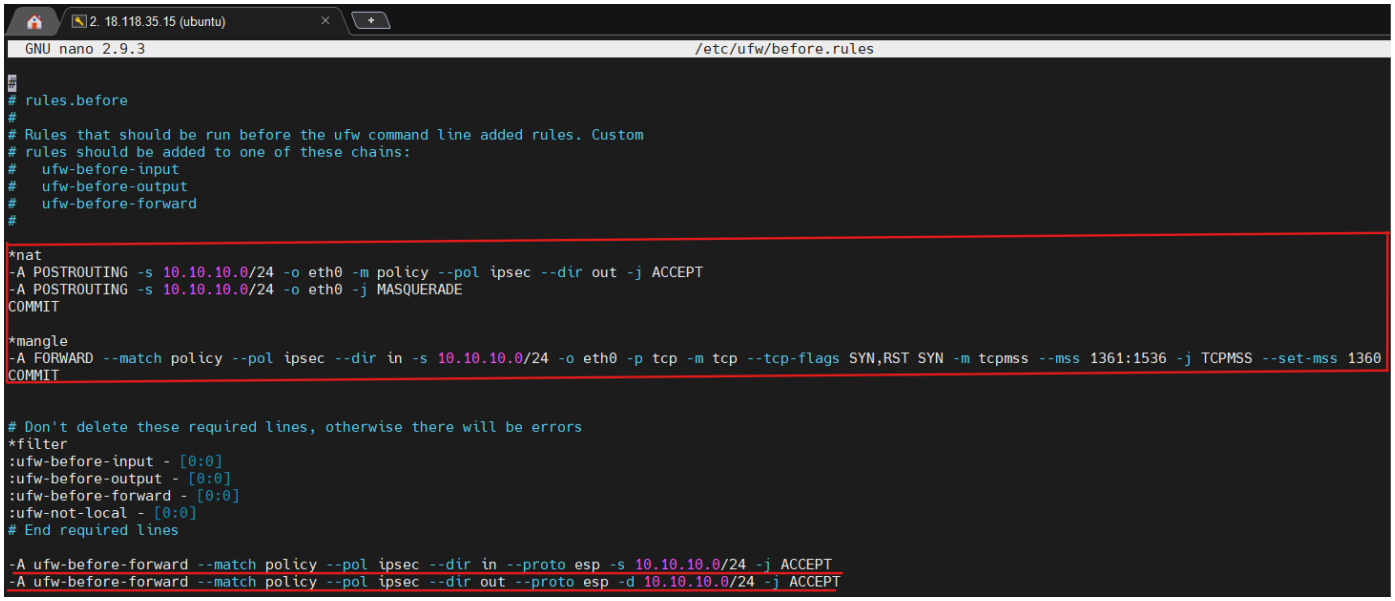
   b. Also**,** the firewall was configured to forward and allow VPN traffic through using below commands.

   ufw allow OpenSSH
   ufw enable

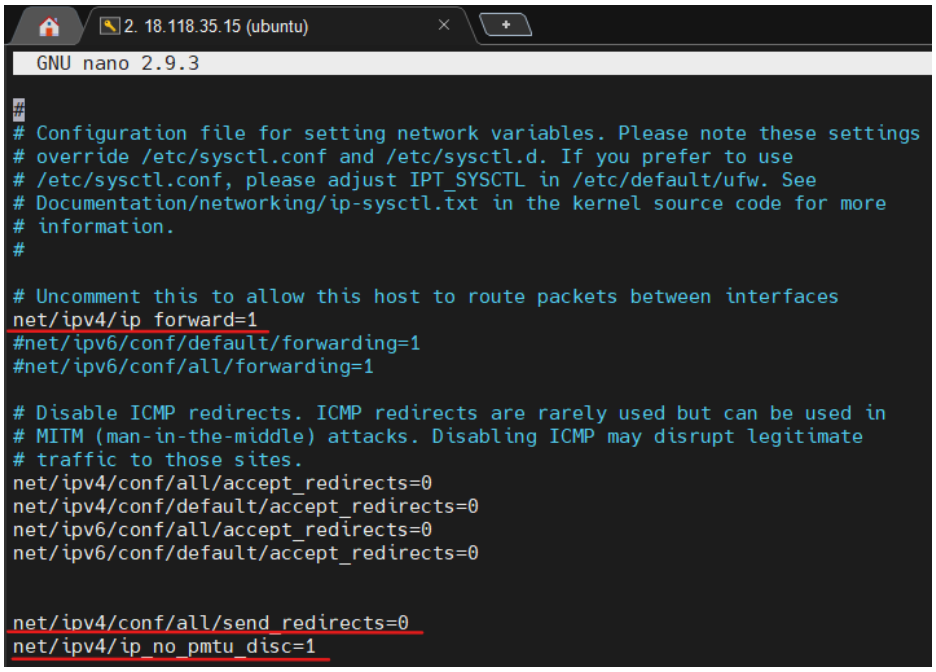
Below rule was added to allow UDP traffic to the standard IPSec ports, 500 and 4500:

ufw allow 500,4500/udp

Highlighted lines were added in file **/etc/ufw/before.rules** to correctly route and manipulate traffic between the VPN clients and the internet.

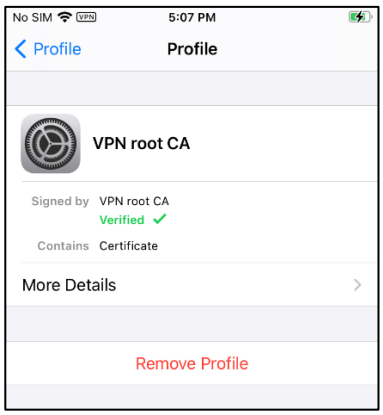


Below highlighted lines were added in **/etc/ufw/sysctl.conf** to change some network kernel parameters to allow routing from one interface to another.

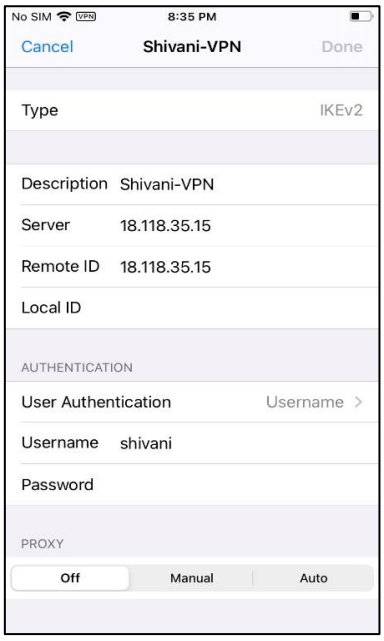


The client machine I chose to test the VPN connection was an iOS device. Below mentioned are the steps taken for configuration.

a. CA certificate at path /etc/ipsec.d/cacerts/ca-cert.pem was copied from the server and saved on my local computer with .pem extension. This saved file was mailed so as to open on the iOS device.
b. The email with the certificate as an attachment was opened on the iOS device and downloaded. From the Settings-> Profile Download, the certificated was installed using the device's password.



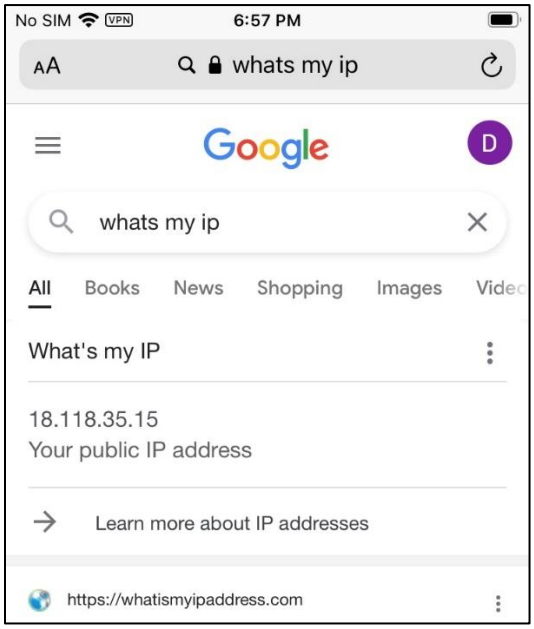
c. In Settings -> General -> VPN -> Add VPN Configuration, the VPN profile was added as per following steps-
   i. Type -- IKEv2.
   ii. Description – Shivani-VPN (Name of the VPN)
   iii. Server and Remote ID field -- 18.118.35.15
   iv. In Authentication section, the username 'Shivani' and password 'test123' was entered



5. Screenshot that you have connected to the strongswan. These screenshot should include the following: the client machine screenshot and the log file at the server to show that your client is connected.

Client Machine:

After connecting the VPN, when checked the IP address it detects as 18.118.35.15 which belongs to the public IP of the AWS instance on which the server is hosted



Log File at Server

```
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[IKE] initiating EAP_MSCHAPV2 method (id 0xC6)
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[IKE] peer supports MOBIKE
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[IKE] authentication of '18.118.35.15' (myself) with RSA signature successful
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[IKE] sending end entity cert "CN=18.118.35.15"
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/MSCHAPV2 ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[ENC] splitting IKE message with length of 1936 bytes into 2 fragments
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[ENC] generating IKE_AUTH response 1 [ EF(1/2) ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[ENC] generating IKE_AUTH response 1 [ EF(2/2) ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[NET] sending packet: from 172.31.31.40[4500] to 172.58.157.92[47500] (1236 bytes)
Nov 14 01:17:28 ip-172-31-31-40 charon: 05[NET] sending packet: from 172.31.31.40[4500] to 172.58.157.92[47500] (772 bytes)
Nov 14 01:17:28 ip-172-31-31-40 charon: 06[NET] received packet: from 172.58.157.92[47500] to 172.31.31.40[4500] (144 bytes)
Nov 14 01:17:28 ip-172-31-31-40 charon: 06[ENC] parsed IKE_AUTH request 2 [ EAP/RES/MSCHAPV2 ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 06[IKE] EAP-MS-CHAPv2 username: 'shivani'
Nov 14 01:17:28 ip-172-31-31-40 charon: 06[ENC] generating IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 06[NET] sending packet: from 172.31.31.40[4500] to 172.58.157.92[47500] (144 bytes)
Nov 14 01:17:28 ip-172-31-31-40 charon: 07[NET] received packet: from 172.58.157.92[47500] to 172.31.31.40[4500] (80 bytes)
Nov 14 01:17:28 ip-172-31-31-40 charon: 07[ENC] parsed IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 07[IKE] EAP method EAP_MSCHAPV2 succeeded, MSK established
Nov 14 01:17:28 ip-172-31-31-40 charon: 07[ENC] generating IKE_AUTH response 3 [ EAP/SUCC ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 07[NET] sending packet: from 172.31.31.40[4500] to 172.58.157.92[47500] (80 bytes)
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[NET] received packet: from 172.58.157.92[47500] to 172.31.31.40[4500] (112 bytes)
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[ENC] parsed IKE_AUTH request 4 [ AUTH ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[IKE] authentication of '172.20.10.12' with EAP successful
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[IKE] authentication of '18.118.35.15' (myself) with EAP
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[IKE] IKE_SA ikev2-vpn[6] established between 172.31.31.40[18.118.35.15]...172.58.157.92[172.20.10.12]
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[IKE] peer requested virtual IP %any
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[IKE] assigning virtual IP 10.10.10.1 to peer 'shivani'
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[IKE] peer requested virtual IP %any6
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[IKE] no virtual IP found for %any6 requested by 'shivani'
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[IKE] CHILD_SA ikev2-vpn{13} established with SPIs c4c2fec0_i 00dbaf08_o and TS 0.0.0.0/0 === 10.10.10.1/32
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[ENC] generating IKE_AUTH response 4 [ AUTH CPRP(ADDR DNS DNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
Nov 14 01:17:28 ip-172-31-31-40 charon: 10[NET] sending packet: from 172.31.31.40[4500] to 172.58.157.92[47500] (256 bytes)
root@ip-172-31-31-40:/home/ubuntu#
```