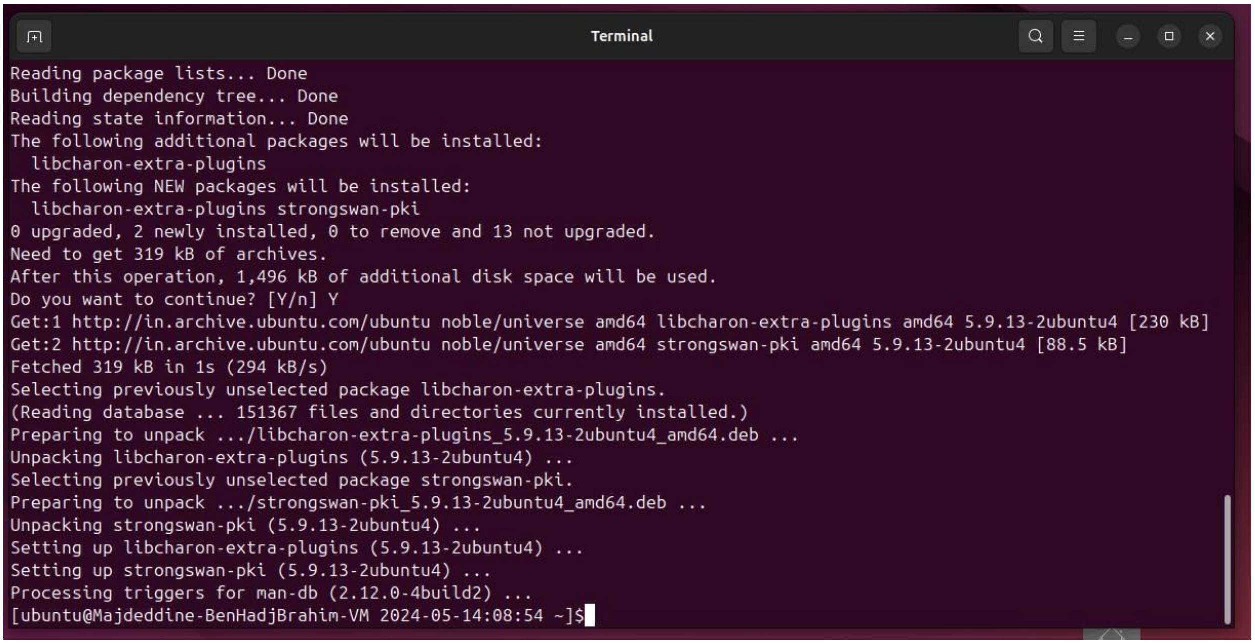
Réalisé par : Majdeddine Ben Hadj Brahim / SSIR 2B

Compte rendu « Configuration d'un VPN virtuel à l'aide de StrongSwan »

Partie 1 : Tâche préliminaire

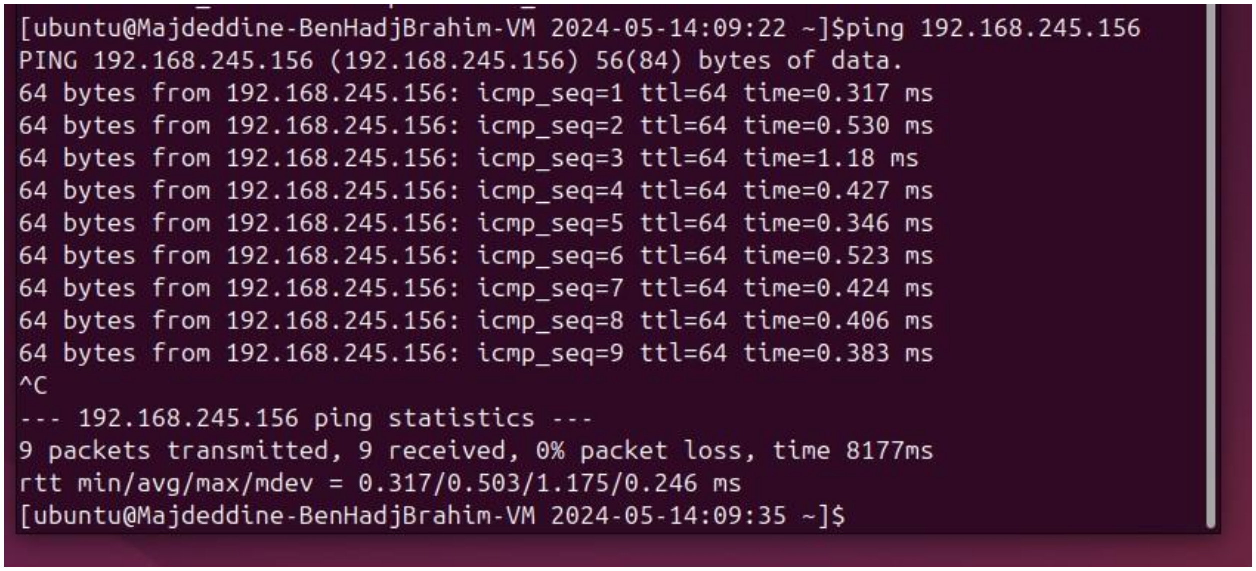
1,2,3)



```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcharon-extra-plugins
The following NEW packages will be installed:
  libcharon-extra-plugins strongswan-pki
0 upgraded, 2 newly installed, 0 to remove and 13 not upgraded.
Need to get 319 kB of archives.
After this operation, 1,496 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libcharon-extra-plugins amd64 5.9.13-2ubuntu4 [230 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 strongswan-pki amd64 5.9.13-2ubuntu4 [88.5 kB]
Fetched 319 kB in 1s (294 kB/s)
Selecting previously unselected package libcharon-extra-plugins.
(Reading database ... 151367 files and directories currently installed.)
Preparing to unpack .../libcharon-extra-plugins_5.9.13-2ubuntu4_amd64.deb ...
Unpacking libcharon-extra-plugins (5.9.13-2ubuntu4) ...
Selecting previously unselected package strongswan-pki.
Preparing to unpack .../strongswan-pki_5.9.13-2ubuntu4_amd64.deb ...
Unpacking strongswan-pki (5.9.13-2ubuntu4) ...
Setting up libcharon-extra-plugins (5.9.13-2ubuntu4) ...
Setting up strongswan-pki (5.9.13-2ubuntu4) ...
Processing triggers for man-db (2.12.0-4build2) ...
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:08:54 ~]$
```

Partie 2 : Configuration VPN utilisant l'authentification PSK

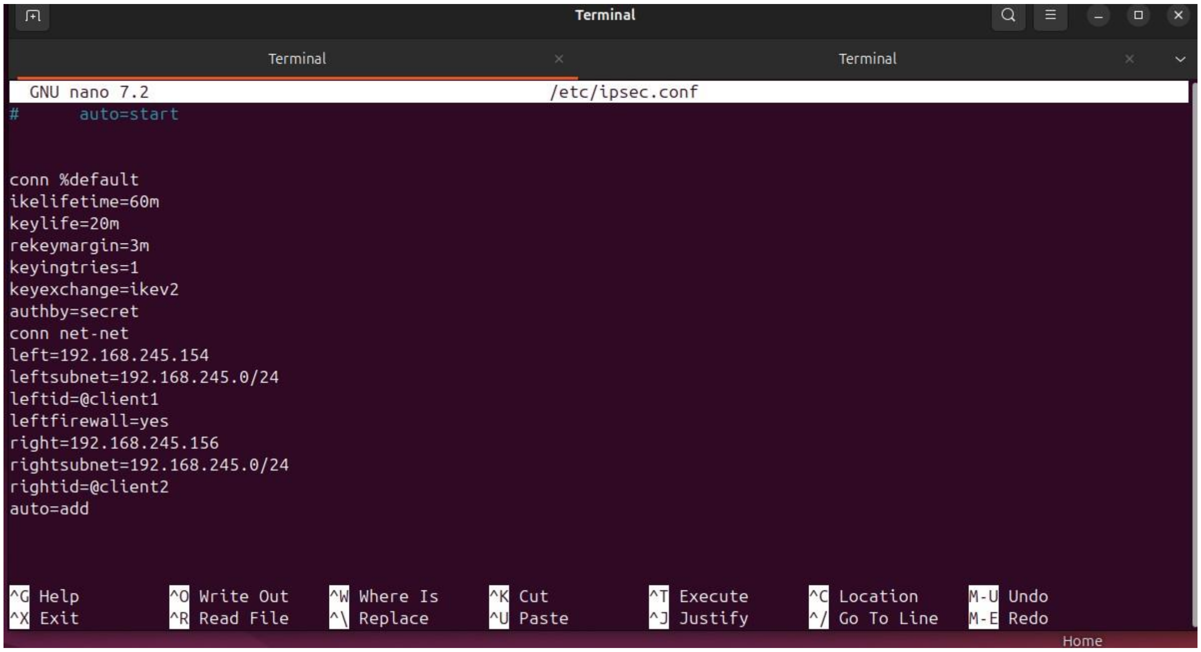
1)



```
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:09:22 ~]$ping 192.168.245.156
PING 192.168.245.156 (192.168.245.156) 56(84) bytes of data.
64 bytes from 192.168.245.156: icmp_seq=1 ttl=64 time=0.317 ms
64 bytes from 192.168.245.156: icmp_seq=2 ttl=64 time=0.530 ms
64 bytes from 192.168.245.156: icmp_seq=3 ttl=64 time=1.18 ms
64 bytes from 192.168.245.156: icmp_seq=4 ttl=64 time=0.427 ms
64 bytes from 192.168.245.156: icmp_seq=5 ttl=64 time=0.346 ms
64 bytes from 192.168.245.156: icmp_seq=6 ttl=64 time=0.523 ms
64 bytes from 192.168.245.156: icmp_seq=7 ttl=64 time=0.424 ms
64 bytes from 192.168.245.156: icmp_seq=8 ttl=64 time=0.406 ms
64 bytes from 192.168.245.156: icmp_seq=9 ttl=64 time=0.383 ms
^C
--- 192.168.245.156 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8177ms
rtt min/avg/max/mdev = 0.317/0.503/1.175/0.246 ms
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:09:35 ~]$
```

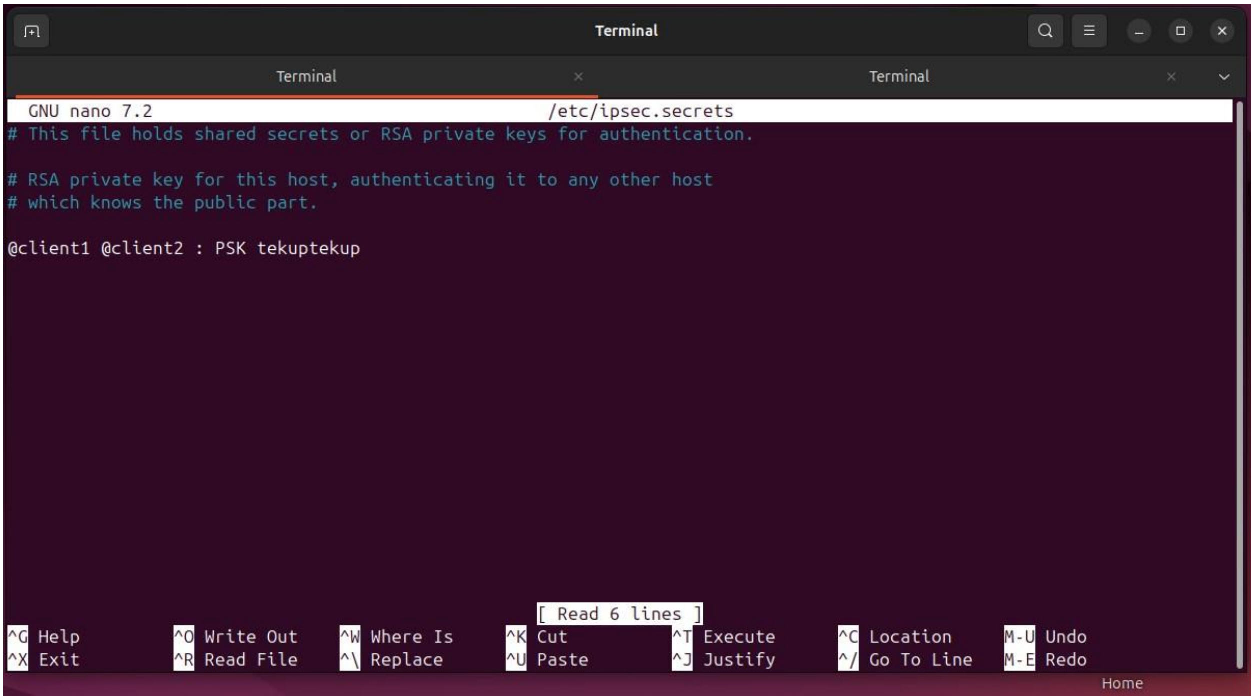
2)

2.a)



```
  GNU nano 7.2                                    /etc/ipsec.conf
#       auto=start


conn %default
ikelifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=1
keyexchange=ikev2
authby=secret
conn net-net
left=192.168.245.154
leftsubnet=192.168.245.0/24
leftid=@client1
leftfirewall=yes
right=192.168.245.156
rightsubnet=192.168.245.0/24
rightid=@client2
auto=add
```

2.b)

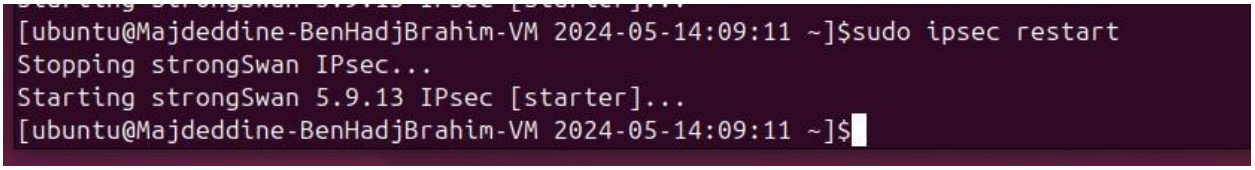


```
  GNU nano 7.2                                    /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

@client1 @client2 : PSK tekuptekup

                                                   [ Read 6 lines ]
```

2.c) J'ai fait la même configuration dans Client2, sauf que j'ai inversé la configuration dans le fichier /etc/ipsec.conf.

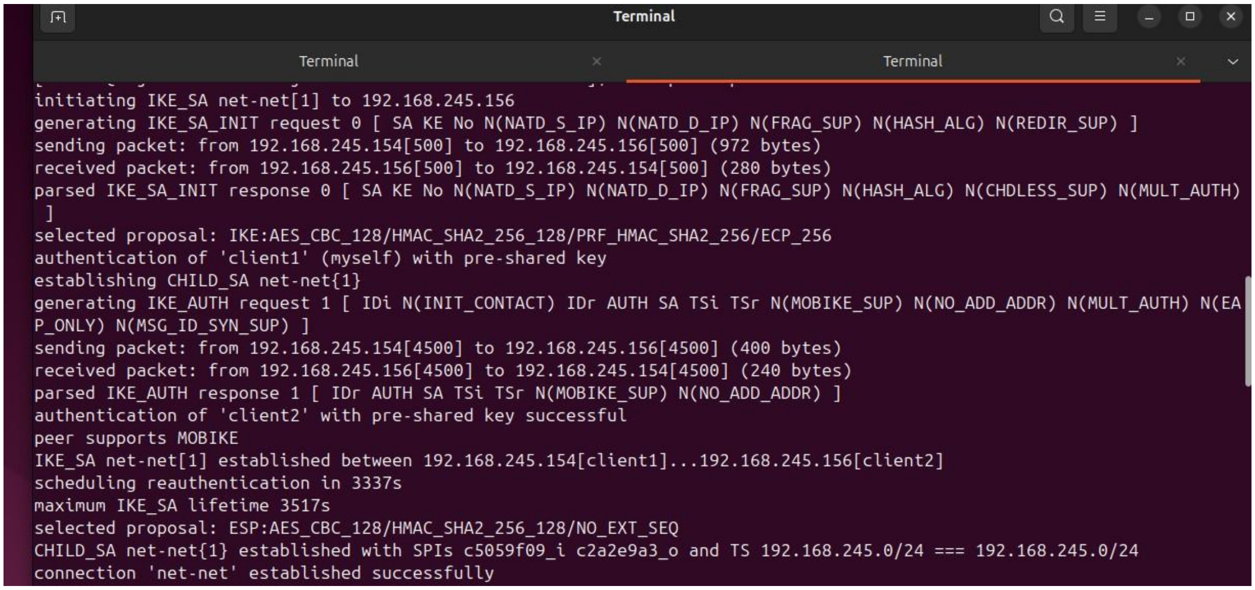
3)

3.a)



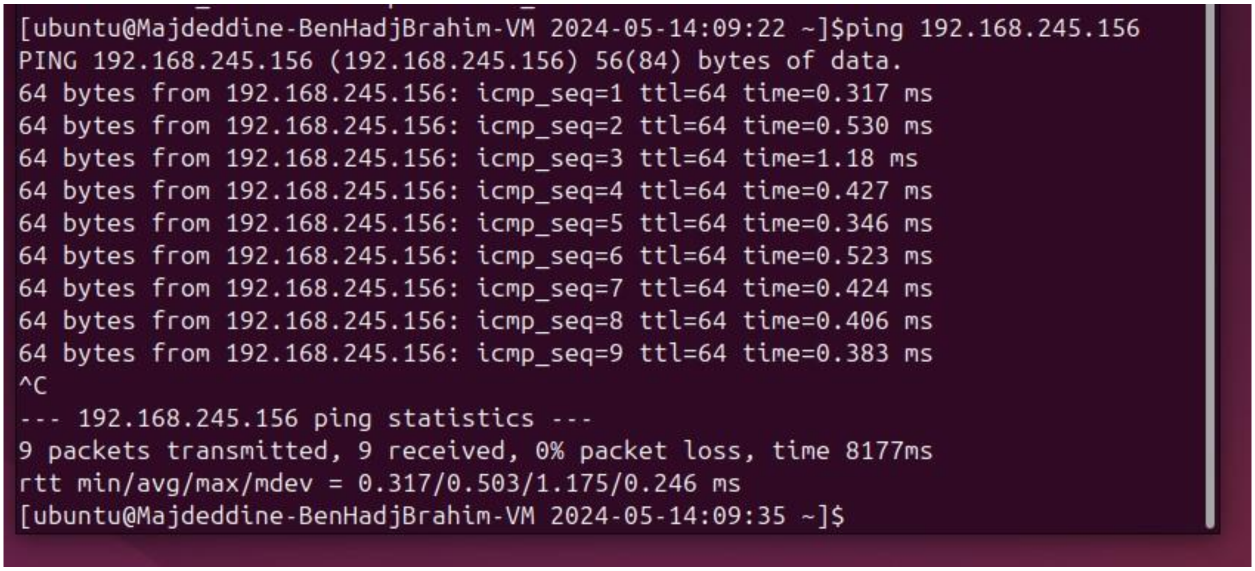
```
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:09:11 ~]$sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.9.13 IPsec [starter]...
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:09:11 ~]$
```

3.b)

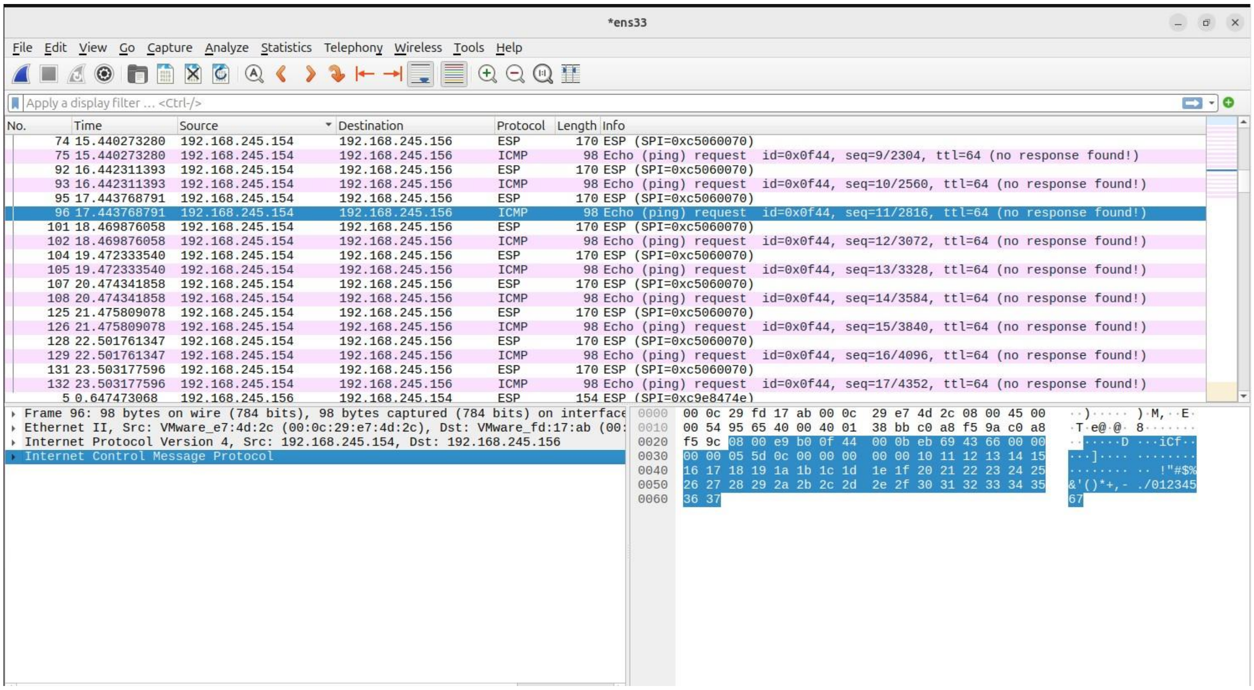


```
initiating IKE_SA net-net[1] to 192.168.245.156
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
sending packet: from 192.168.245.154[500] to 192.168.245.156[500] (972 bytes)
received packet: from 192.168.245.156[500] to 192.168.245.154[500] (280 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH)
 ]
selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256
authentication of 'client1' (myself) with pre-shared key
establishing CHILD_SA net-net{1}
generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EA
P_ONLY) N(MSG_ID_SYN_SUP) ]
sending packet: from 192.168.245.154[4500] to 192.168.245.156[4500] (400 bytes)
received packet: from 192.168.245.156[4500] to 192.168.245.154[4500] (240 bytes)
parsed IKE_AUTH response 1 [ IDr AUTH SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
authentication of 'client2' with pre-shared key successful
peer supports MOBIKE
IKE_SA net-net[1] established between 192.168.245.154[client1]...192.168.245.156[client2]
scheduling reauthentication in 3337s
maximum IKE_SA lifetime 3517s
selected proposal: ESP:AES_CBC_128/HMAC_SHA2_256_128/NO_EXT_SEQ
CHILD_SA net-net{1} established with SPIs c5059f09_i c2a2e9a3_o and TS 192.168.245.0/24 === 192.168.245.0/24
connection 'net-net' established successfully
```

3.c)



```
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:09:22 ~]$ping 192.168.245.156
PING 192.168.245.156 (192.168.245.156) 56(84) bytes of data.
64 bytes from 192.168.245.156: icmp_seq=1 ttl=64 time=0.317 ms
64 bytes from 192.168.245.156: icmp_seq=2 ttl=64 time=0.530 ms
64 bytes from 192.168.245.156: icmp_seq=3 ttl=64 time=1.18 ms
64 bytes from 192.168.245.156: icmp_seq=4 ttl=64 time=0.427 ms
64 bytes from 192.168.245.156: icmp_seq=5 ttl=64 time=0.346 ms
64 bytes from 192.168.245.156: icmp_seq=6 ttl=64 time=0.523 ms
64 bytes from 192.168.245.156: icmp_seq=7 ttl=64 time=0.424 ms
64 bytes from 192.168.245.156: icmp_seq=8 ttl=64 time=0.406 ms
64 bytes from 192.168.245.156: icmp_seq=9 ttl=64 time=0.383 ms
^C
--- 192.168.245.156 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8177ms
rtt min/avg/max/mdev = 0.317/0.503/1.175/0.246 ms
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:09:35 ~]$
```

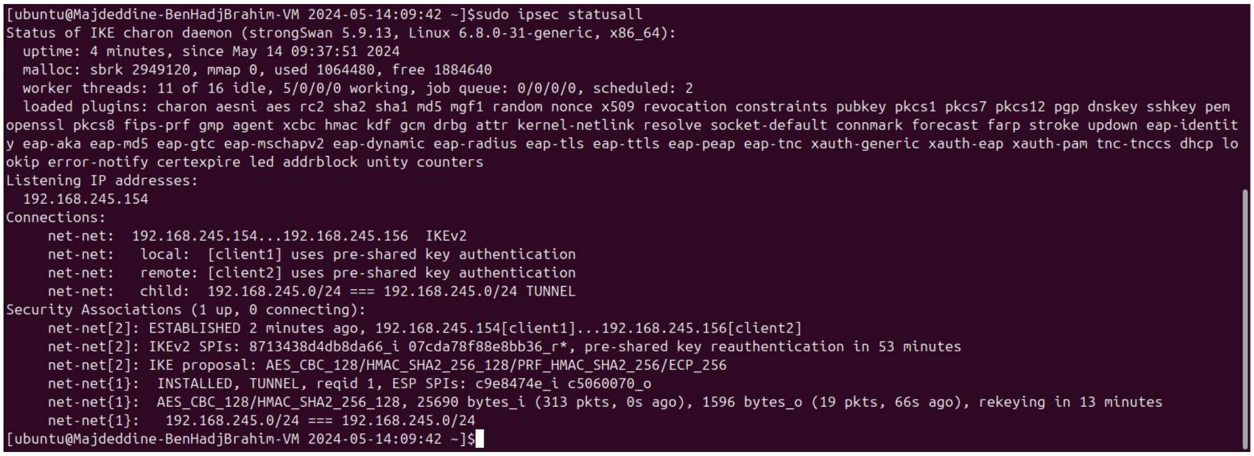

*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time          Source            Destination       Protocol Length Info
     74 15.440273280  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
     75 15.440273280  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=9/2304, ttl=64 (no response found!)
     92 16.442311393  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
     93 16.442311393  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=10/2560, ttl=64 (no response found!)
     95 17.443768791  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
     96 17.443768791  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=11/2816, ttl=64 (no response found!)
    101 18.469876058  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
    102 18.469876058  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=12/3072, ttl=64 (no response found!)
    104 19.472333540  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
    105 19.472333540  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=13/3328, ttl=64 (no response found!)
    107 20.474341858  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
    108 20.474341858  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=14/3584, ttl=64 (no response found!)
    125 21.475809078  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
    126 21.475809078  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=15/3840, ttl=64 (no response found!)
    128 22.501761347  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
    129 22.501761347  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=16/4096, ttl=64 (no response found!)
    131 23.503177596  192.168.245.154   192.168.245.156   ESP       170 ESP (SPI=0xc5060070)
    132 23.503177596  192.168.245.154   192.168.245.156   ICMP       98 Echo (ping) request  id=0x0f44, seq=17/4352, ttl=64 (no response found!)
      5 0.647473068   192.168.245.156   192.168.245.154   ESP       154 ESP (SPI=0xc9e8474e)
```

```
› Frame 96: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
› Ethernet II, Src: VMware_e7:4d:2c (00:0c:29:e7:4d:2c), Dst: VMware_fd:17:ab (00:
› Internet Protocol Version 4, Src: 192.168.245.154, Dst: 192.168.245.156
› Internet Control Message Protocol
```

```
0000  00 0c 29 fd 17 ab 00 0c  29 e7 4d 2c 08 00 45 00   ··)·····  )·M,··E·
0010  00 54 95 65 40 00 40 01  38 bb c0 a8 f5 9a c0 a8   ·T·e@·@·  8·······
0020  f5 9c 08 00 e9 b0 0f 44  00 0b eb 69 43 66 00 00   ·······D  ···iCf··
0030  00 00 05 5d 0c 00 00 00  00 00 10 11 12 13 14 15   ···]····  ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········  ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-  ./012345
0060  36 37                                              67
```

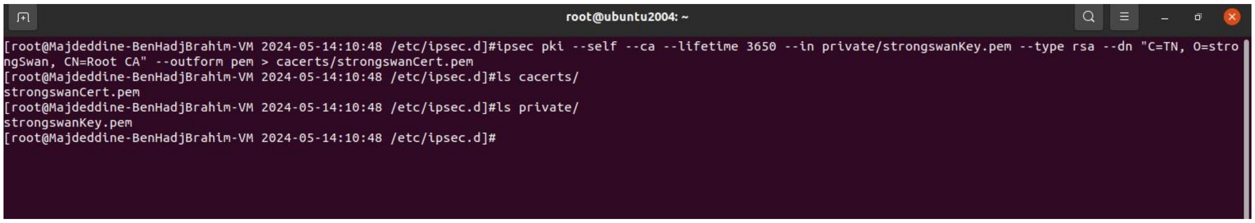
3.d)



```
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:09:42 ~]$sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.9.13, Linux 6.8.0-31-generic, x86_64):
  uptime: 4 minutes, since May 14 09:37:51 2024
  malloc: sbrk 2949120, mmap 0, used 1064480, free 1884640
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon aesni aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs12 pgp dnskey sshkey pem
openssl pkcs8 fips-prf gmp agent xcbc hmac kdf gcm drbg attr kernel-netlink resolve socket-default connmark forecast farp stroke updown eap-identit
y eap-aka eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-tls eap-ttls eap-peap eap-tnc xauth-generic xauth-eap xauth-pam tnc-tnccs dhcp lo
okip error-notify certexpire led addrblock unity counters
Listening IP addresses:
  192.168.245.154
Connections:
     net-net:  192.168.245.154...192.168.245.156  IKEv2
     net-net:   local:  [client1] uses pre-shared key authentication
     net-net:   remote: [client2] uses pre-shared key authentication
     net-net:   child:  192.168.245.0/24 === 192.168.245.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
     net-net[2]: ESTABLISHED 2 minutes ago, 192.168.245.154[client1]...192.168.245.156[client2]
     net-net[2]: IKEv2 SPIs: 8713438d4db8da66_i 07cda78f88e8bb36_r*, pre-shared key reauthentication in 53 minutes
     net-net[2]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256
     net-net{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c9e8474e_i c5060070_o
     net-net{1}:  AES_CBC_128/HMAC_SHA2_256_128, 25690 bytes_i (313 pkts, 0s ago), 1596 bytes_o (19 pkts, 66s ago), rekeying in 13 minutes
     net-net{1}:   192.168.245.0/24 === 192.168.245.0/24
[ubuntu@Majdeddine-BenHadjBrahim-VM 2024-05-14:09:42 ~]$
```

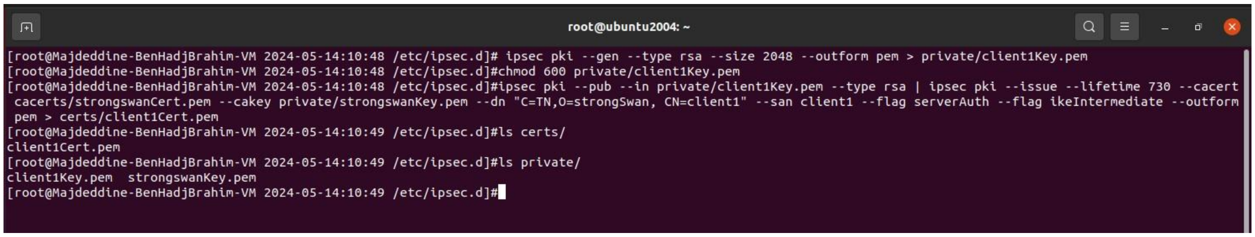
Partie 3 : Configuration VPN par authentification avec certificat X509

1,2)



```
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:48 /etc/ipsec.d]#ipsec pki --self --ca --lifetime 3650 --in private/strongswanKey.pem --type rsa --dn "C=TN, O=stro
ngSwan, CN=Root CA" --outform pem > cacerts/strongswanCert.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:48 /etc/ipsec.d]#ls cacerts/
strongswanCert.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:48 /etc/ipsec.d]#ls private/
strongswanKey.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:48 /etc/ipsec.d]#
```

3,4)

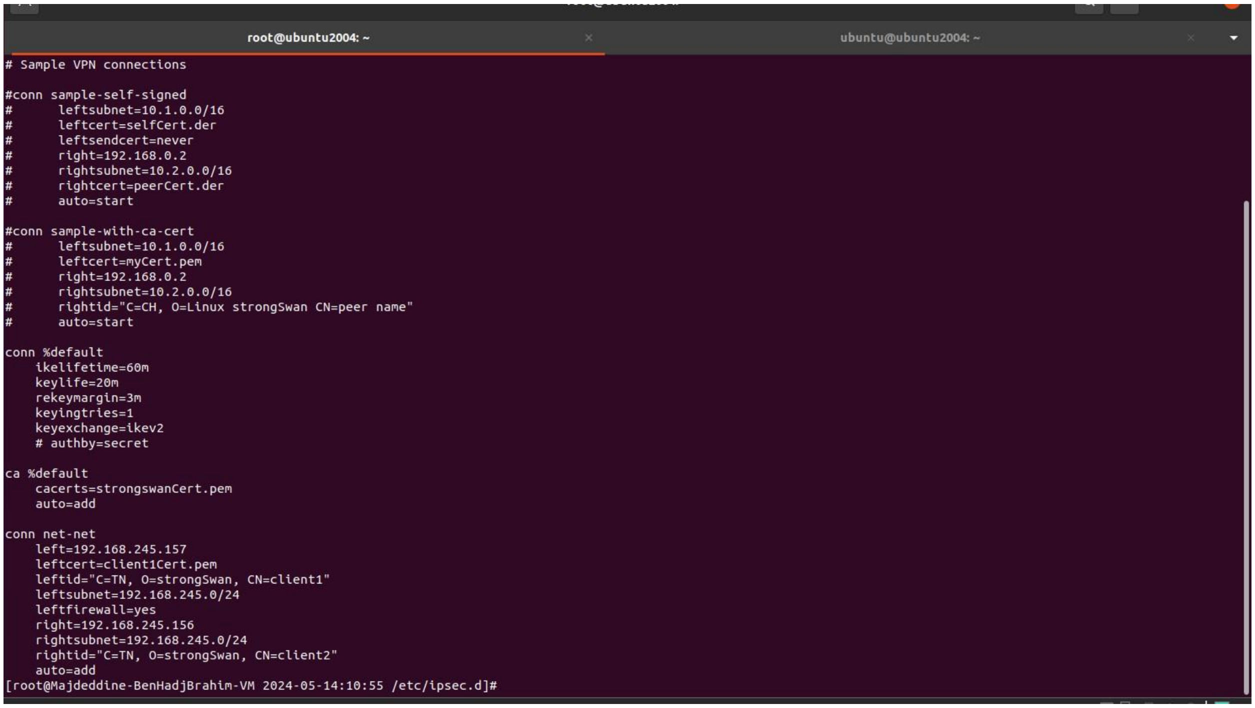


```
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:48 /etc/ipsec.d]# ipsec pki --gen --type rsa --size 2048 --outform pem > private/client1Key.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:48 /etc/ipsec.d]#chmod 600 private/client1Key.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:48 /etc/ipsec.d]#ipsec pki --pub --in private/client1Key.pem --type rsa | ipsec pki --issue --lifetime 730 --cacert
 cacerts/strongswanCert.pem --cakey private/strongswanKey.pem --dn "C=TN,O=strongSwan, CN=client1" --san client1 --flag serverAuth --flag ikeIntermediate --outform
 pem > certs/client1Cert.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:49 /etc/ipsec.d]#ls certs/
client1Cert.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:49 /etc/ipsec.d]#ls private/
client1Key.pem  strongswanKey.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:49 /etc/ipsec.d]#
```

5) J'ai utilisé les mêmes commandes que dans la question 3 pour générer le certificat pour Client2.

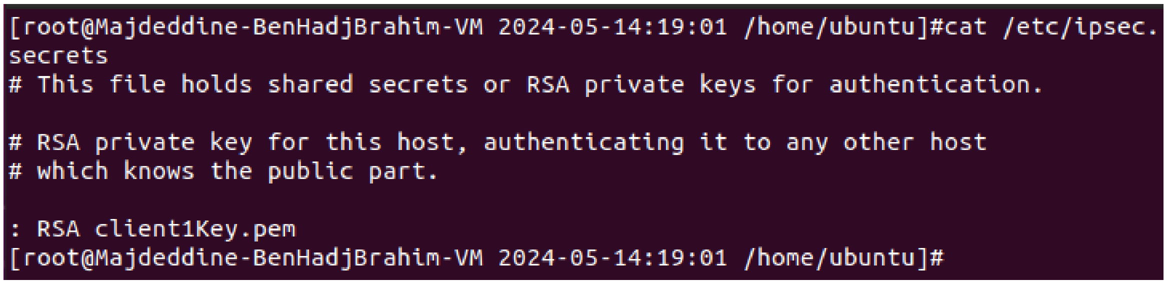
6)

6.a)



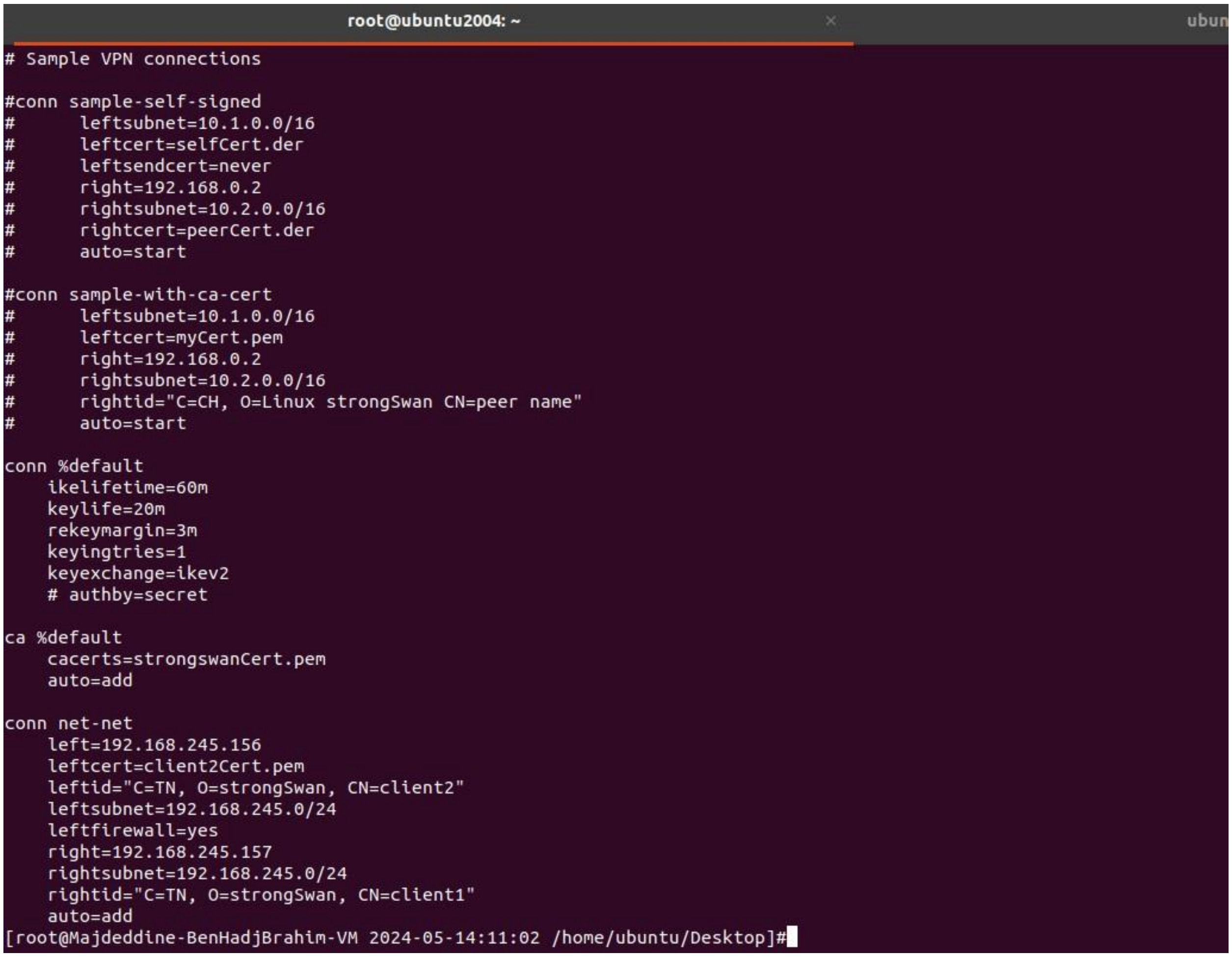
```
# Sample VPN connections

#conn sample-self-signed
#      leftsubnet=10.1.0.0/16
#      leftcert=selfCert.der
#      leftsendcert=never
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightcert=peerCert.der
#      auto=start

#conn sample-with-ca-cert
#      leftsubnet=10.1.0.0/16
#      leftcert=myCert.pem
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightid="C=CH, O=Linux strongSwan CN=peer name"
#      auto=start

conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev2
    # authby=secret

ca %default
    cacerts=strongswanCert.pem
    auto=add

conn net-net
    left=192.168.245.157
    leftcert=client1Cert.pem
    leftid="C=TN, O=strongSwan, CN=client1"
    leftsubnet=192.168.245.0/24
    leftfirewall=yes
    right=192.168.245.156
    rightsubnet=192.168.245.0/24
    rightid="C=TN, O=strongSwan, CN=client2"
    auto=add
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:10:55 /etc/ipsec.d]#
```

6.b)

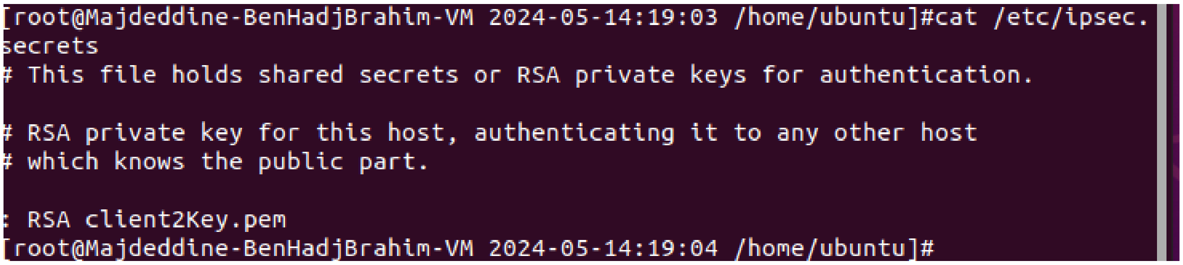


```
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:19:01 /home/ubuntu]#cat /etc/ipsec.
secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

: RSA client1Key.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:19:01 /home/ubuntu]#
```

6.c)



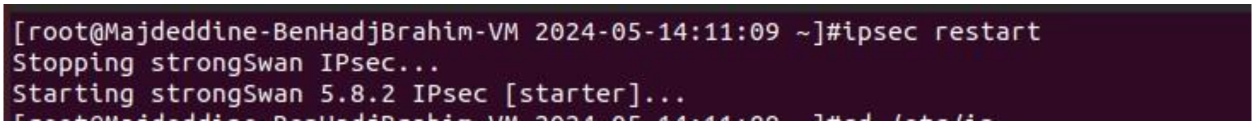
```
# Sample VPN connections

#conn sample-self-signed
#      leftsubnet=10.1.0.0/16
#      leftcert=selfCert.der
#      leftsendcert=never
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightcert=peerCert.der
#      auto=start

#conn sample-with-ca-cert
#      leftsubnet=10.1.0.0/16
#      leftcert=myCert.pem
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightid="C=CH, O=Linux strongSwan CN=peer name"
#      auto=start

conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev2
    # authby=secret

ca %default
    cacerts=strongswanCert.pem
    auto=add

conn net-net
    left=192.168.245.156
    leftcert=client2Cert.pem
    leftid="C=TN, O=strongSwan, CN=client2"
    leftsubnet=192.168.245.0/24
    leftfirewall=yes
    right=192.168.245.157
    rightsubnet=192.168.245.0/24
    rightid="C=TN, O=strongSwan, CN=client1"
    auto=add
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:11:02 /home/ubuntu/Desktop]#
```



```
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:19:03 /home/ubuntu]#cat /etc/ipsec.
secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

: RSA client2Key.pem
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:19:04 /home/ubuntu]#
```

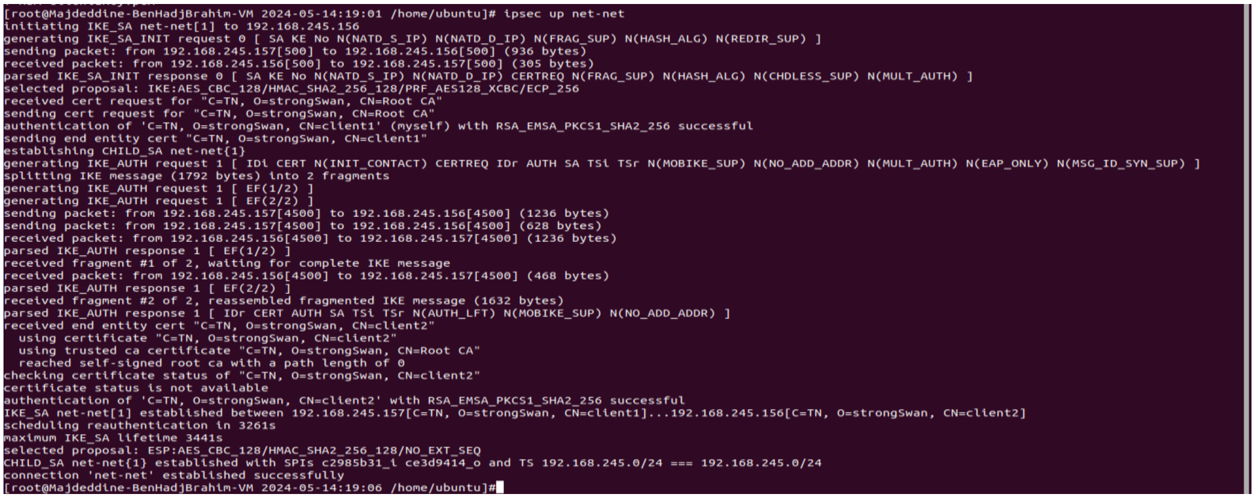
7)

7.a)



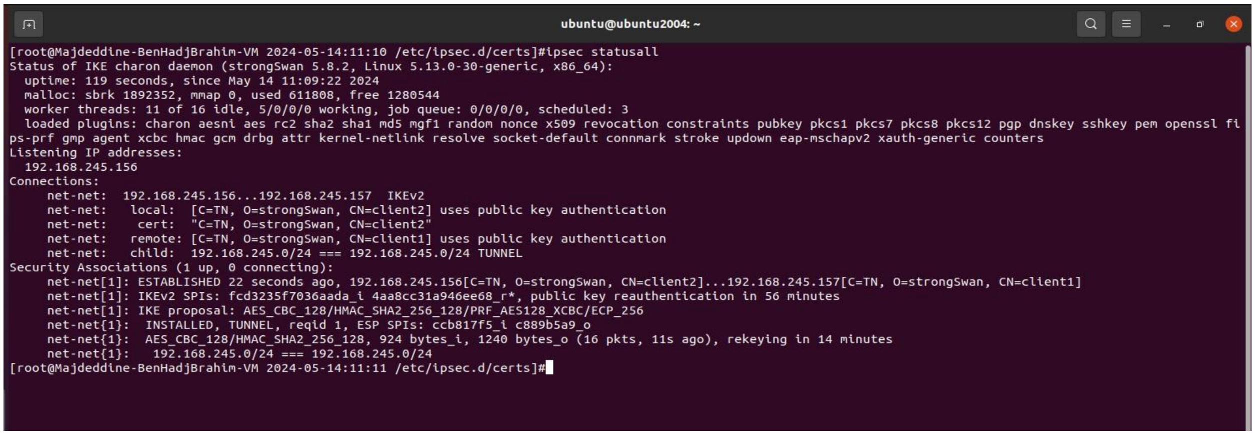
```
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:11:09 ~]#ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.8.2 IPsec [starter]...
```

7.b)



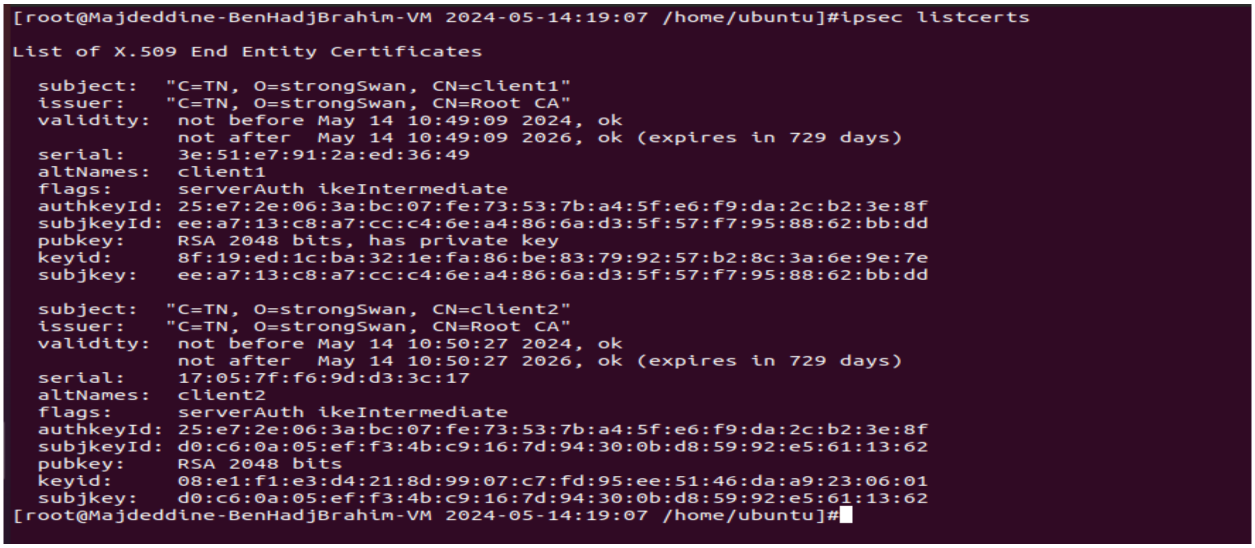
```
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:19:01 /home/ubuntu]# ipsec up net-net
initiating IKE_SA net-net[1] to 192.168.245.156
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
sending packet: from 192.168.245.157[500] to 192.168.245.156[500] (936 bytes)
received packet: from 192.168.245.156[500] to 192.168.245.157[500] (305 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_AES128_XCBC/ECP_256
received cert request for "C=TN, O=strongSwan, CN=Root CA"
sending cert request for "C=TN, O=strongSwan, CN=Root CA"
authentication of 'C=TN, O=strongSwan, CN=client1' (myself) with RSA_EMSA_PKCS1_SHA2_256 successful
sending end entity cert "C=TN, O=strongSwan, CN=client1"
establishing CHILD_SA net-net{1}
generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr AUTH SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
splitting IKE message (1792 bytes) into 2 fragments
generating IKE_AUTH request 1 [ EF(1/2) ]
generating IKE_AUTH request 1 [ EF(2/2) ]
sending packet: from 192.168.245.157[4500] to 192.168.245.156[4500] (1236 bytes)
sending packet: from 192.168.245.157[4500] to 192.168.245.156[4500] (628 bytes)
received packet: from 192.168.245.156[4500] to 192.168.245.157[4500] (1236 bytes)
parsed IKE_AUTH response 1 [ EF(1/2) ]
received fragment #1 of 2, waiting for complete IKE message
received packet: from 192.168.245.156[4500] to 192.168.245.157[4500] (468 bytes)
parsed IKE_AUTH response 1 [ EF(2/2) ]
received fragment #2 of 2, reassembled fragmented IKE message (1632 bytes)
parsed IKE_AUTH response 1 [ IDr CERT AUTH SA TSi TSr N(AUTH_LFT) N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
received end entity cert "C=TN, O=strongSwan, CN=client2"
  using certificate "C=TN, O=strongSwan, CN=client2"
  using trusted ca certificate "C=TN, O=strongSwan, CN=Root CA"
  reached self-signed root ca with a path length of 0
checking certificate status of "C=TN, O=strongSwan, CN=client2"
certificate status is not available
authentication of 'C=TN, O=strongSwan, CN=client2' with RSA_EMSA_PKCS1_SHA2_256 successful
IKE_SA net-net[1] established between 192.168.245.157[C=TN, O=strongSwan, CN=client1]...192.168.245.156[C=TN, O=strongSwan, CN=client2]
scheduling reauthentication in 3261s
maximum IKE_SA lifetime 3441s
selected proposal: ESP:AES_CBC_128/HMAC_SHA2_256_128/NO_EXT_SEQ
CHILD_SA net-net{1} established with SPIs c2985b31_i ce3d9414_o and TS 192.168.245.0/24 === 192.168.245.0/24
connection 'net-net' established successfully
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:19:06 /home/ubuntu]#
```

7.c)



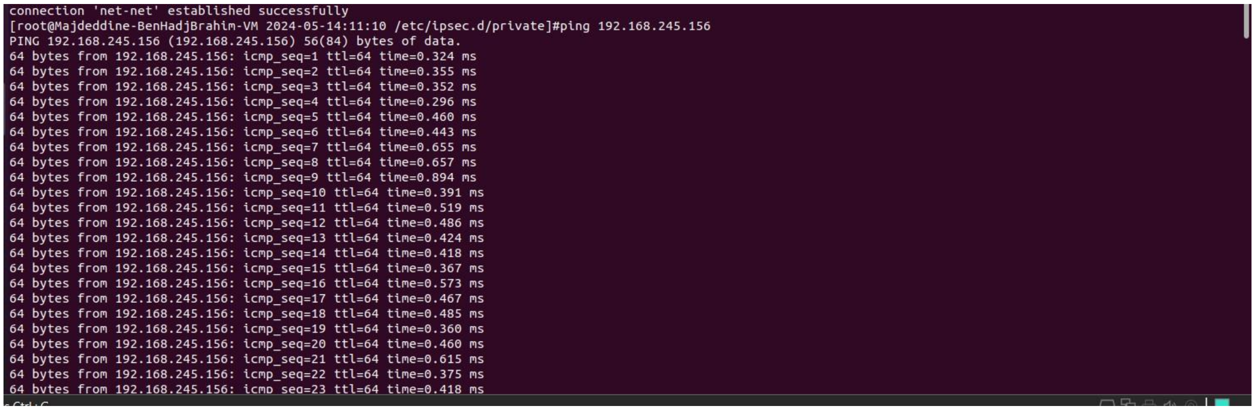
```
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:11:10 /etc/ipsec.d/certs]#ipsec statusall
Status of IKE charon daemon (strongSwan 5.8.2, Linux 5.13.0-30-generic, x86_64):
  uptime: 119 seconds, since May 14 11:09:22 2024
  malloc: sbrk 1892352, mmap 0, used 611808, free 1280544
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon aesni aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fi
ps-prf gmp agent xcbc hmac gcm drbg attr kernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters
Listening IP addresses:
  192.168.245.156
Connections:
     net-net:  192.168.245.156...192.168.245.157  IKEv2
     net-net:   local:  [C=TN, O=strongSwan, CN=client2] uses public key authentication
     net-net:    cert:  "C=TN, O=strongSwan, CN=client2"
     net-net:   remote: [C=TN, O=strongSwan, CN=client1] uses public key authentication
     net-net:   child:  192.168.245.0/24 === 192.168.245.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
     net-net[1]: ESTABLISHED 22 seconds ago, 192.168.245.156[C=TN, O=strongSwan, CN=client2]...192.168.245.157[C=TN, O=strongSwan, CN=client1]
     net-net[1]: IKEv2 SPIs: fcd3235f7036aada_i 4aa8cc31a946ee68_r*, public key reauthentication in 56 minutes
     net-net[1]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_AES128_XCBC/ECP_256
     net-net{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ccb817f5_i c889b5a9_o
     net-net{1}:  AES_CBC_128/HMAC_SHA2_256_128, 924 bytes_i, 1240 bytes_o (16 pkts, 11s ago), rekeying in 14 minutes
     net-net{1}:   192.168.245.0/24 === 192.168.245.0/24
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:11:11 /etc/ipsec.d/certs]#
```

7.d)

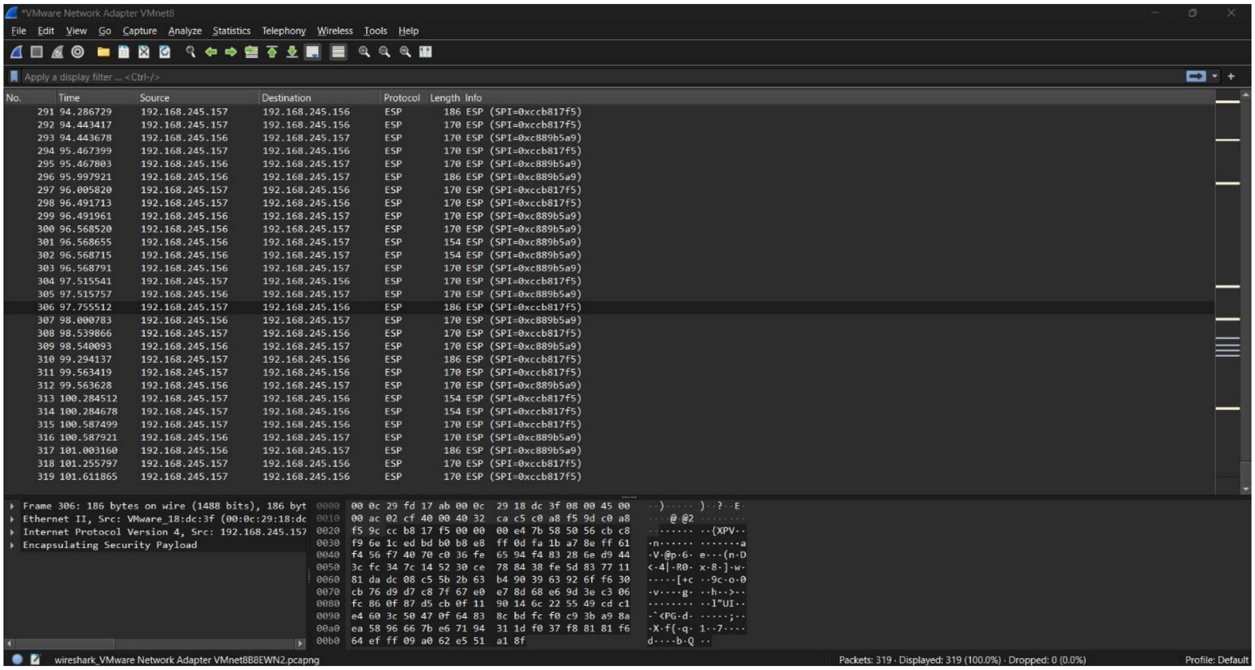


```
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:19:07 /home/ubuntu]#ipsec listcerts

List of X.509 End Entity Certificates

  subject:   "C=TN, O=strongSwan, CN=client1"
  issuer:    "C=TN, O=strongSwan, CN=Root CA"
  validity:   not before May 14 10:49:09 2024, ok
              not after  May 14 10:49:09 2026, ok (expires in 729 days)
  serial:     3e:51:e7:91:2a:ed:36:49
  altNames:   client1
  flags:      serverAuth ikeIntermediate
  authkeyId:  25:e7:2e:06:3a:bc:07:fe:73:53:7b:a4:5f:e6:f9:da:2c:b2:3e:8f
  subjkeyId:  ee:a7:13:c8:a7:cc:c4:6e:a4:86:6a:d3:5f:57:f7:95:88:62:bb:dd
  pubkey:     RSA 2048 bits, has private key
  keyid:      8f:19:ed:1c:ba:32:1e:fa:86:be:83:79:92:57:b2:8c:3a:6e:9e:7e
  subjkey:    ee:a7:13:c8:a7:cc:c4:6e:a4:86:6a:d3:5f:57:f7:95:88:62:bb:dd

  subject:   "C=TN, O=strongSwan, CN=client2"
  issuer:    "C=TN, O=strongSwan, CN=Root CA"
  validity:   not before May 14 10:50:27 2024, ok
              not after  May 14 10:50:27 2026, ok (expires in 729 days)
  serial:     17:05:7f:f6:9d:d3:3c:17
  altNames:   client2
  flags:      serverAuth ikeIntermediate
  authkeyId:  25:e7:2e:06:3a:bc:07:fe:73:53:7b:a4:5f:e6:f9:da:2c:b2:3e:8f
  subjkeyId:  d0:c6:0a:05:ef:f3:4b:c9:16:7d:94:30:0b:d8:59:92:e5:61:13:62
  pubkey:     RSA 2048 bits
  keyid:      08:e1:f1:e3:d4:21:8d:99:07:c7:fd:95:ee:51:46:da:a9:23:06:01
  subjkey:    d0:c6:0a:05:ef:f3:4b:c9:16:7d:94:30:0b:d8:59:92:e5:61:13:62
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:19:07 /home/ubuntu]#
```

7.e)



```
connection 'net-net' established successfully
[root@Majdeddine-BenHadjBrahim-VM 2024-05-14:11:10 /etc/ipsec.d/private]#ping 192.168.245.156
PING 192.168.245.156 (192.168.245.156) 56(84) bytes of data.
64 bytes from 192.168.245.156: icmp_seq=1 ttl=64 time=0.324 ms
64 bytes from 192.168.245.156: icmp_seq=2 ttl=64 time=0.355 ms
64 bytes from 192.168.245.156: icmp_seq=3 ttl=64 time=0.352 ms
64 bytes from 192.168.245.156: icmp_seq=4 ttl=64 time=0.296 ms
64 bytes from 192.168.245.156: icmp_seq=5 ttl=64 time=0.460 ms
64 bytes from 192.168.245.156: icmp_seq=6 ttl=64 time=0.443 ms
64 bytes from 192.168.245.156: icmp_seq=7 ttl=64 time=0.655 ms
64 bytes from 192.168.245.156: icmp_seq=8 ttl=64 time=0.657 ms
64 bytes from 192.168.245.156: icmp_seq=9 ttl=64 time=0.894 ms
64 bytes from 192.168.245.156: icmp_seq=10 ttl=64 time=0.391 ms
64 bytes from 192.168.245.156: icmp_seq=11 ttl=64 time=0.519 ms
64 bytes from 192.168.245.156: icmp_seq=12 ttl=64 time=0.486 ms
64 bytes from 192.168.245.156: icmp_seq=13 ttl=64 time=0.424 ms
64 bytes from 192.168.245.156: icmp_seq=14 ttl=64 time=0.418 ms
64 bytes from 192.168.245.156: icmp_seq=15 ttl=64 time=0.367 ms
64 bytes from 192.168.245.156: icmp_seq=16 ttl=64 time=0.573 ms
64 bytes from 192.168.245.156: icmp_seq=17 ttl=64 time=0.467 ms
64 bytes from 192.168.245.156: icmp_seq=18 ttl=64 time=0.485 ms
64 bytes from 192.168.245.156: icmp_seq=19 ttl=64 time=0.360 ms
64 bytes from 192.168.245.156: icmp_seq=20 ttl=64 time=0.460 ms
64 bytes from 192.168.245.156: icmp_seq=21 ttl=64 time=0.615 ms
64 bytes from 192.168.245.156: icmp_seq=22 ttl=64 time=0.375 ms
64 bytes from 192.168.245.156: icmp_seq=23 ttl=64 time=0.418 ms
```



*VMware Network Adapter VMnet8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source           Destination      Protocol Length Info
  291 94.286729   192.168.245.157  192.168.245.156  ESP      186 ESP (SPI=0xccb817f5)
  292 94.443417   192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  293 94.443678   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  294 95.467399   192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  295 95.467803   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  296 95.997921   192.168.245.156  192.168.245.157  ESP      186 ESP (SPI=0xc889b5a9)
  297 96.005820   192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  298 96.491713   192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  299 96.491961   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  300 96.568520   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  301 96.568655   192.168.245.156  192.168.245.157  ESP      154 ESP (SPI=0xc889b5a9)
  302 96.568715   192.168.245.156  192.168.245.157  ESP      154 ESP (SPI=0xc889b5a9)
  303 96.568791   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  304 97.515541   192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  305 97.515757   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  306 97.755512   192.168.245.157  192.168.245.156  ESP      186 ESP (SPI=0xccb817f5)
  307 98.000783   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  308 98.539866   192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  309 98.540093   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  310 99.294137   192.168.245.157  192.168.245.156  ESP      186 ESP (SPI=0xccb817f5)
  311 99.563419   192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  312 99.563628   192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  313 100.284512  192.168.245.157  192.168.245.156  ESP      154 ESP (SPI=0xccb817f5)
  314 100.284678  192.168.245.157  192.168.245.156  ESP      154 ESP (SPI=0xccb817f5)
  315 100.587499  192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  316 100.587921  192.168.245.156  192.168.245.157  ESP      170 ESP (SPI=0xc889b5a9)
  317 101.003160  192.168.245.156  192.168.245.157  ESP      186 ESP (SPI=0xc889b5a9)
  318 101.255797  192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
  319 101.611865  192.168.245.157  192.168.245.156  ESP      170 ESP (SPI=0xccb817f5)
```

```
> Frame 306: 186 bytes on wire (1488 bits), 186 byt
> Ethernet II, Src: VMware_18:dc:3f (00:0c:29:18:dc
> Internet Protocol Version 4, Src: 192.168.245.157
> Encapsulating Security Payload
```

```
0000  00 0c 29 fd 17 ab 00 0c  29 18 dc 3f 08 00 45 00   ··)····· )··?··E·
0010  00 ac 02 cf 40 00 40 32  ca c5 c0 a8 f5 9d c0 a8   ····@·@2 ········
0020  f5 9c cc b8 17 f5 00 00  00 e4 7b 58 50 56 cb c8   ········ ··{XPV··
0030  f9 6e 1c ed bd b0 b8 e8  ff 0d fa 1b a7 8e ff 61   ·n······ ·······a
0040  f4 56 f7 40 70 c0 36 fe  65 94 f4 83 28 6e d9 44   ·V·@p·6· e···(n·D
0050  3c fc 34 7c 14 52 30 ce  78 84 38 fe 5d 83 77 11   <·4|·R0· x·8·]·w·
0060  81 da dc 08 c5 5b 2b 63  b4 90 39 63 92 6f f6 30   ·····[+c ··9c·o·0
0070  cb 76 d9 d7 c8 7f 67 e0  e7 8d 68 e6 9d 3e c3 06   ·v····g· ··h··>··
0080  fc 86 0f 87 d5 cb 0f 11  90 14 6c 22 55 49 cd c1   ········ ··l"UI··
0090  e4 60 3c 50 47 0f 64 83  8c bd fc f0 c9 3b a9 8a   ·`<PG·d· ·····;··
00a0  ea 58 96 66 7b e6 71 94  31 1d f0 37 f8 81 81 f6   ·X·f{·q· 1··7····
00b0  64 ef ff 09 a0 62 e5 51  a1 8f                     d····b·Q ··
```

wireshark_VMware Network Adapter VMnet8B8EWN2.pcapng
Packets: 319 · Displayed: 319 (100.0%) · Dropped: 0 (0.0%)
Profile: Default