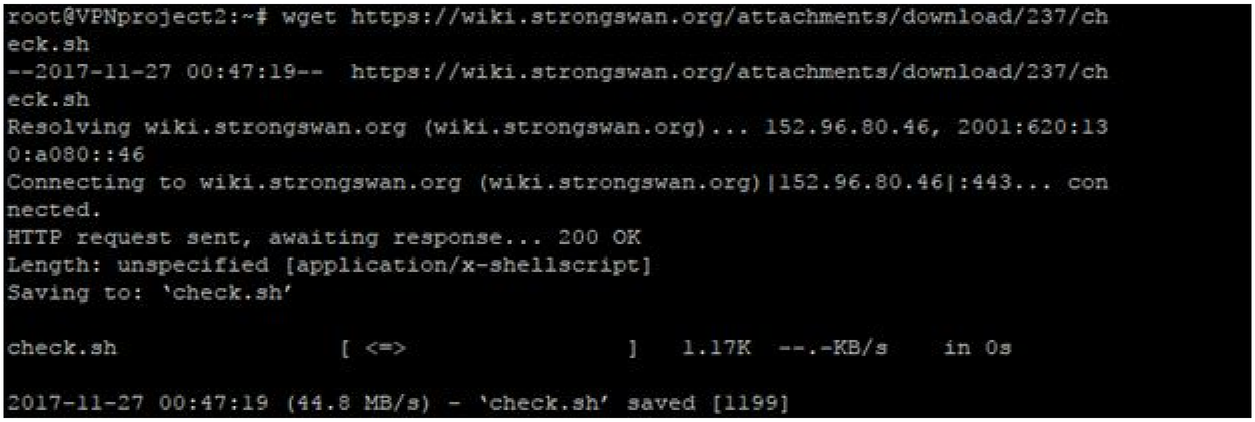
Applied Crypto - VPN Project

By Tanya Peddi

1) Installing Strongswan

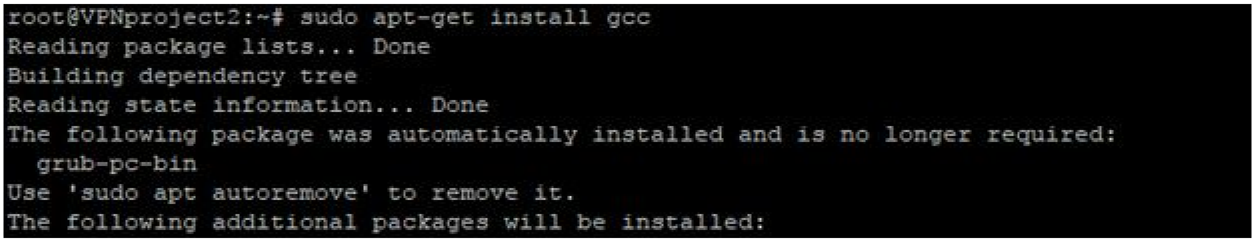
Download plugins and necessary libraries

- *wget https://wiki.strongswan.org/attachments/download/237/check.sh*
- *sudo sh check.sh*
- *sudo apt-get install gcc*
- *sudo apt-get install libgmp3-dev*
- *sudo apt-get install make*
- *sudo apt-get install build essential*
- *sudo apt-get install libssl-dev*
- *sudo apt-get update*

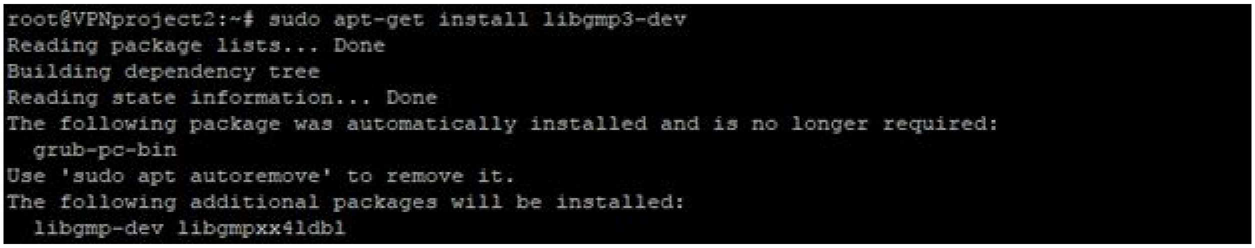


```
root@VPNproject2:~# wget https://wiki.strongswan.org/attachments/download/237/ch
eck.sh
--2017-11-27 00:47:19--  https://wiki.strongswan.org/attachments/download/237/ch
eck.sh
Resolving wiki.strongswan.org (wiki.strongswan.org)... 152.96.80.46, 2001:620:13
0:a080::46
Connecting to wiki.strongswan.org (wiki.strongswan.org)|152.96.80.46|:443... con
nected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-shellscript]
Saving to: ‘check.sh’

check.sh                [ <=>                ]   1.17K  --.-KB/s    in 0s

2017-11-27 00:47:19 (44.8 MB/s) - ‘check.sh’ saved [1199]
```

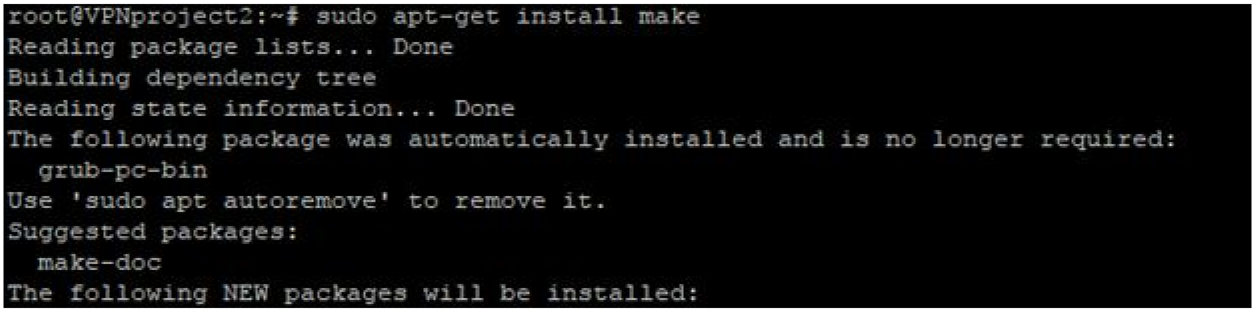
```
root@VPNproject2:~# wget https://wiki.strongswan.org/attachments/download/237/ch
eck.sh
--2017-11-27 00:47:19--  https://wiki.strongswan.org/attachments/download/237/ch
eck.sh
Resolving wiki.strongswan.org (wiki.strongswan.org)... 152.96.80.46, 2001:620:13
0:a080::46
Connecting to wiki.strongswan.org (wiki.strongswan.org)|152.96.80.46|:443... con
nected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-shellscript]
Saving to: ‘check.sh’

check.sh                [ <=>                ]   1.17K  --.-KB/s    in 0s

2017-11-27 00:47:19 (44.8 MB/s) - ‘check.sh’ saved [1199]
```



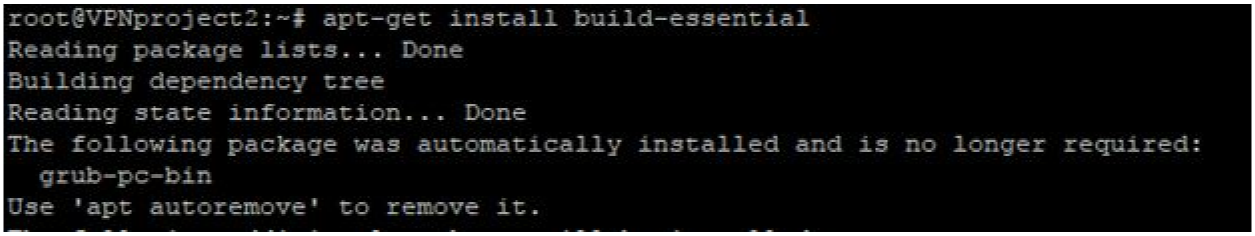
```
root@VPNproject2:~# sudo apt-get install gcc
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
```



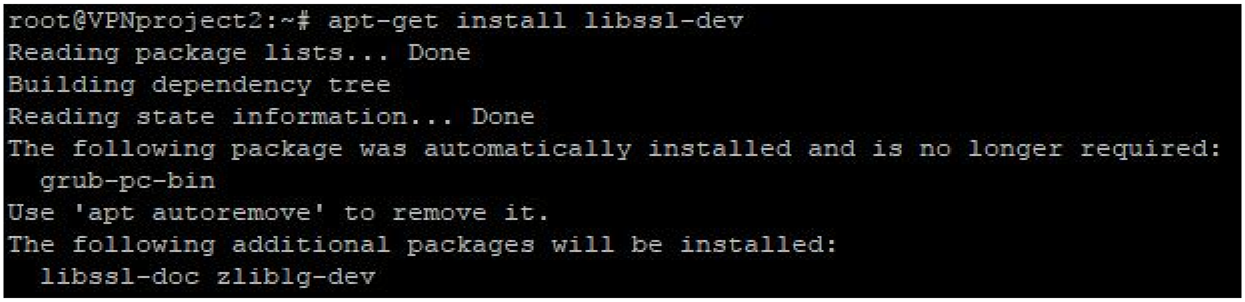
```
root@VPNproject2:~# sudo apt-get install libgmp3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libgmp-dev libgmpxx4ldbl
```



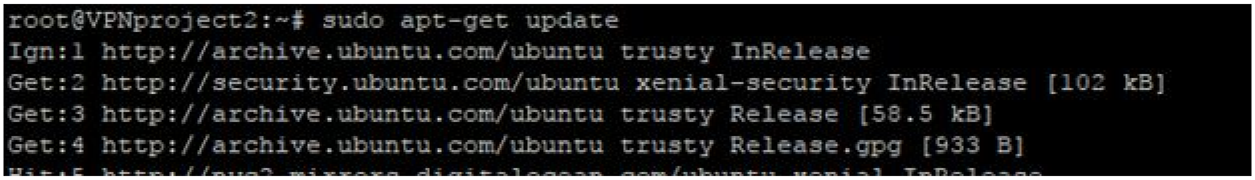
```
root@VPNproject2:~# sudo apt-get install make
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
Suggested packages:
  make-doc
The following NEW packages will be installed:
```



```
root@VPNproject2:~# apt-get install build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'apt autoremove' to remove it.
```



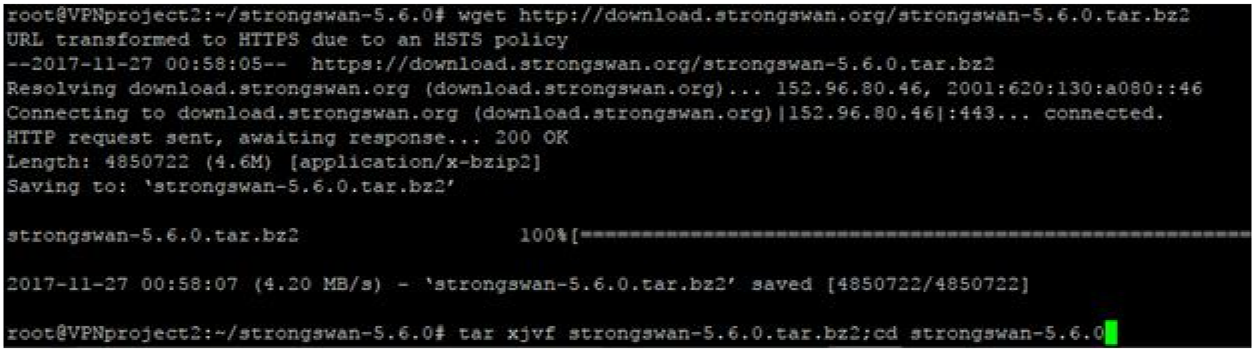
```
root@VPNproject2:~# apt-get install libssl-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'apt autoremove' to remove it.
The following additional packages will be installed:
  libssl-doc zlib1g-dev
```



```
root@VPNproject2:~# sudo apt-get update
Ign:1 http://archive.ubuntu.com/ubuntu trusty InRelease
Get:2 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Get:3 http://archive.ubuntu.com/ubuntu trusty Release [58.5 kB]
Get:4 http://archive.ubuntu.com/ubuntu trusty Release.gpg [933 B]
```

Download Strongswan and unzip the Tar file

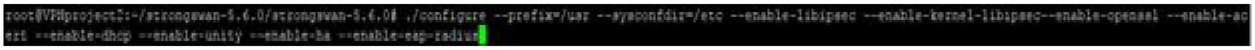
- *wget http://download.strongswan.org/strongswan-5.6.0.tar.bz2*
- *tar xjvf strongswan-5.6.0.tar.bz2;cd strongswan-5.6.0*



```
root@VPNproject2:~/strongswan-5.6.0# wget http://download.strongswan.org/strongswan-5.6.0.tar.bz2
URL transformed to HTTPS due to an HSTS policy
--2017-11-27 00:58:05--  https://download.strongswan.org/strongswan-5.6.0.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|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4850722 (4.6M) [application/x-bzip2]
Saving to: ‘strongswan-5.6.0.tar.bz2’

strongswan-5.6.0.tar.bz2               100%[=====================================================

2017-11-27 00:58:07 (4.20 MB/s) - ‘strongswan-5.6.0.tar.bz2’ saved [4850722/4850722]

root@VPNproject2:~/strongswan-5.6.0# tar xjvf strongswan-5.6.0.tar.bz2;cd strongswan-5.6.0
```

Configuring Strongswan

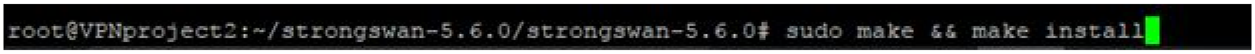
- *./configure --prefix=/usr --sysconfdir=/etc --enable-libipsec --enable-kernel-libipsec --enable-openssl --enable-acert --enable-dhcp --enable-unity --enable-ha --enable-eap-radius*



```
root@VPNproject2:~/strongswan-5.6.0/strongswan-5.6.0# ./configure --prefix=/usr --sysconfdir=/etc --enable-libipsec --enable-kernel-libipsec--enable-openssl --enable-ac
ert --enable-dhcp --enable-unity --enable-ha --enable-eap-radius
```

Installing the server

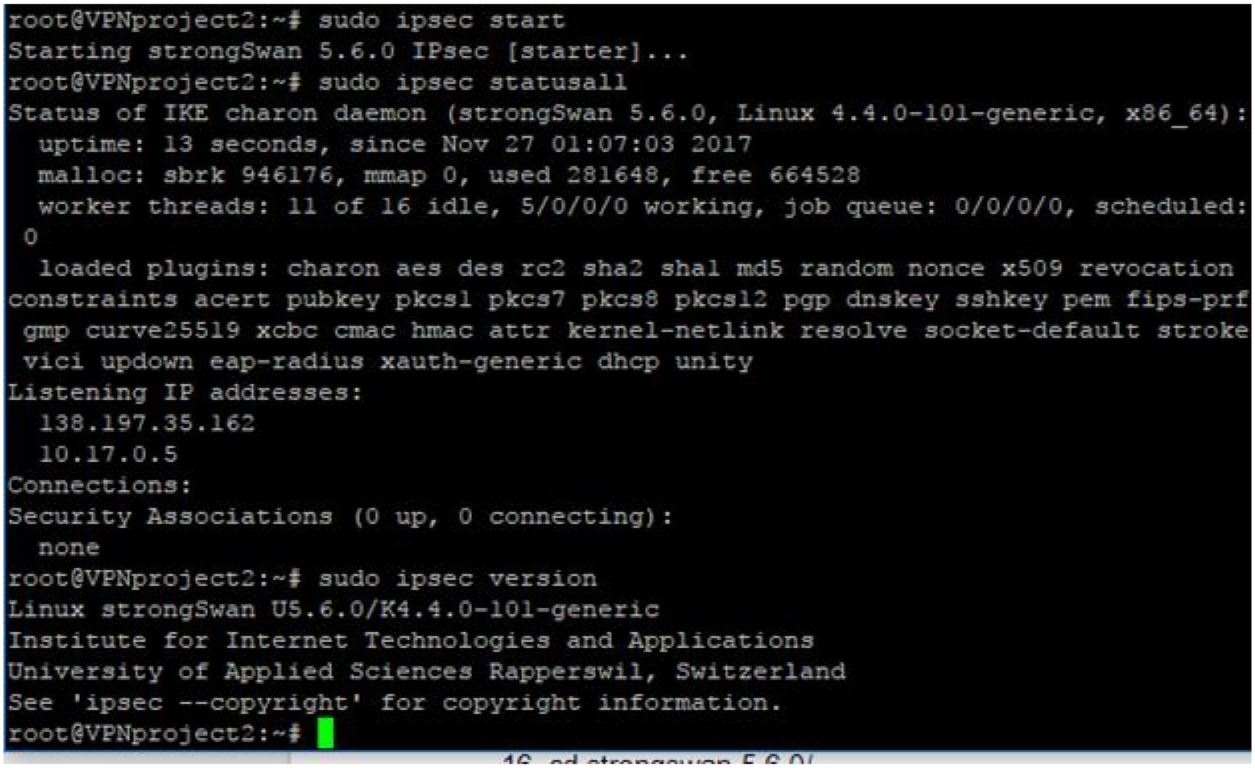
- *sudo make && make install*



```
root@VPNproject2:~/strongswan-5.6.0/strongswan-5.6.0# sudo make && make install
```

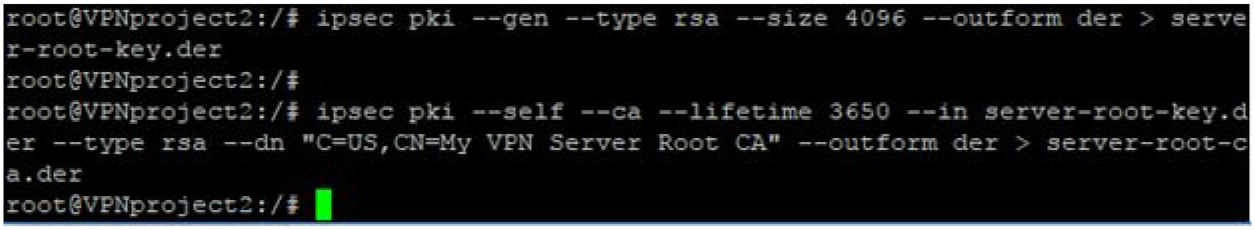
2) **Certificate Authority**

- *sudo reboot*
- *sudo ipsec start*
- *sudo ipsec statusall*
- *sudo ipsec version*



```
root@VPNproject2:~# sudo ipsec start
Starting strongSwan 5.6.0 IPsec [starter]...
root@VPNproject2:~# sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.0, Linux 4.4.0-101-generic, x86_64):
  uptime: 13 seconds, since Nov 27 01:07:03 2017
  malloc: sbrk 946176, mmap 0, used 281648, free 664528
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled:
 0
  loaded plugins: charon aes des rc2 sha2 sha1 md5 random nonce x509 revocation
constraints acert pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem fips-prf
 gmp curve25519 xcbc cmac hmac attr kernel-netlink resolve socket-default stroke
 vici updown eap-radius xauth-generic dhcp unity
Listening IP addresses:
  138.197.35.162
  10.17.0.5
Connections:
Security Associations (0 up, 0 connecting):
  none
root@VPNproject2:~# sudo ipsec version
Linux strongSwan U5.6.0/K4.4.0-101-generic
Institute for Internet Technologies and Applications
University of Applied Sciences Rapperswil, Switzerland
See 'ipsec --copyright' for copyright information.
root@VPNproject2:~#
```

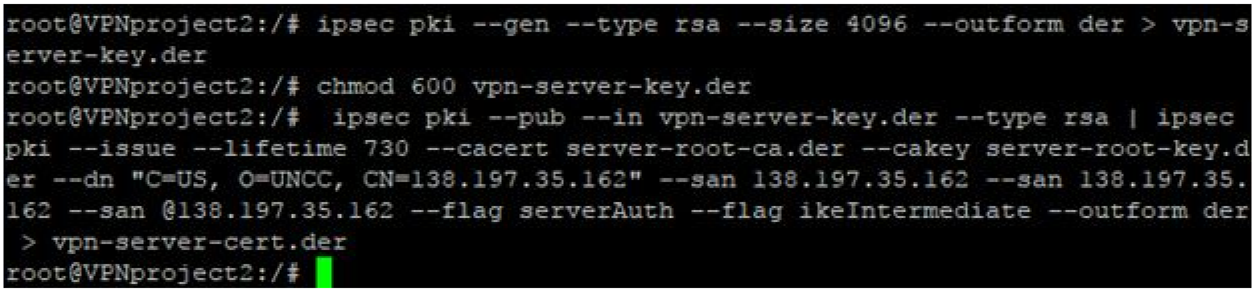
- *ipsec pki --gen --type rsa --size 4096 --outform der > server-root-key.der*
- *ipsec pki --self --ca --lifetime 3650 --in server-root-key.der --type rsa --dn "C=US,CN=My VPN Server Root CA" --outform der > server-root-ca.der*



```
root@VPNproject2:/# ipsec pki --gen --type rsa --size 4096 --outform der > serve
r-root-key.der
root@VPNproject2:/#
root@VPNproject2:/# ipsec pki --self --ca --lifetime 3650 --in server-root-key.d
er --type rsa --dn "C=US,CN=My VPN Server Root CA" --outform der > server-root-c
a.der
root@VPNproject2:/#
```

3) VPN Host Certificate

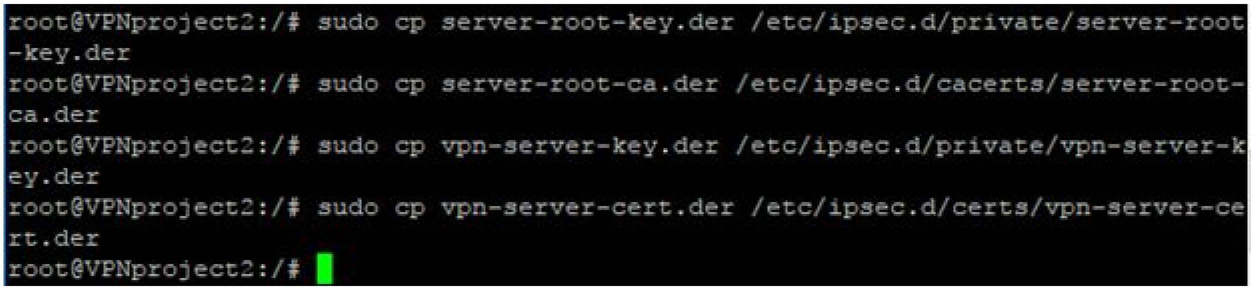
- *ipsec pki --gen --type rsa --size 4096 --outform der > vpn-server-key.der*
- *chmod 600 vpn-server-key.der*
- *ipsec pki --pub --in vpn-server-key.der --type rsa | ipsec pki --issue --lifetime 730 --cacert server-root-ca.der --cakey server-root-key.der --dn "C=US, O=UNCC, CN=138.197.35.162" --san 138.197.35.162 --san 138.197.35.162 --san @138.197.35.162 --flag serverAuth --flag ikeIntermediate --outform der > vpn-server-cert.der*



```
root@VPNproject2:/# ipsec pki --gen --type rsa --size 4096 --outform der > vpn-s
erver-key.der
root@VPNproject2:/# chmod 600 vpn-server-key.der
root@VPNproject2:/#  ipsec pki --pub --in vpn-server-key.der --type rsa | ipsec
pki --issue --lifetime 730 --cacert server-root-ca.der --cakey server-root-key.d
er --dn "C=US, O=UNCC, CN=138.197.35.162" --san 138.197.35.162 --san 138.197.35.
162 --san @138.197.35.162 --flag serverAuth --flag ikeIntermediate --outform der
 > vpn-server-cert.der
root@VPNproject2:/# 
```

4) Moving files to specific folders

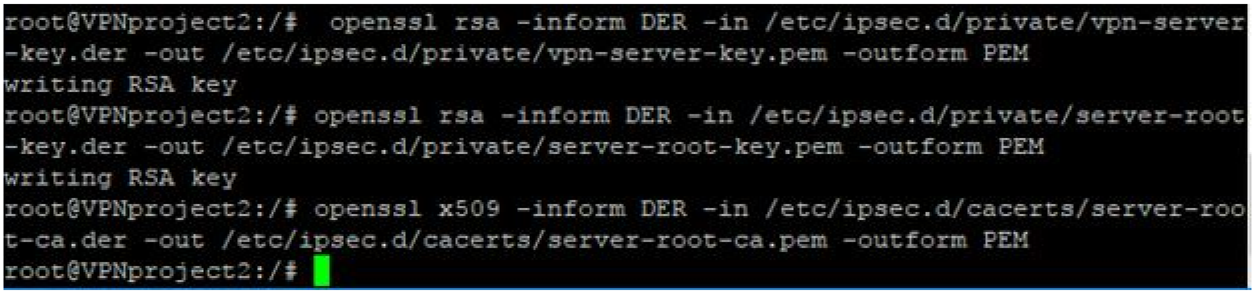
- *sudo cp server-root-key.der /etc/ipsec.d/private/server-root-key.der*
- *sudo cp server-root-ca.der /etc/ipsec.d/cacerts/server-root-ca.der*
- *sudo cp vpn-server-key.der /etc/ipsec.d/private/vpn-server-key.der*
- *sudo cp vpn-server-cert.der /etc/ipsec.d/certs/vpn-server-cert.der*



```
root@VPNproject2:/# sudo cp server-root-key.der /etc/ipsec.d/private/server-root
-key.der
root@VPNproject2:/# sudo cp server-root-ca.der /etc/ipsec.d/cacerts/server-root-
ca.der
root@VPNproject2:/# sudo cp vpn-server-key.der /etc/ipsec.d/private/vpn-server-k
ey.der
root@VPNproject2:/# sudo cp vpn-server-cert.der /etc/ipsec.d/certs/vpn-server-ce
rt.der
root@VPNproject2:/# 
```

5) Converting der files to PEM files

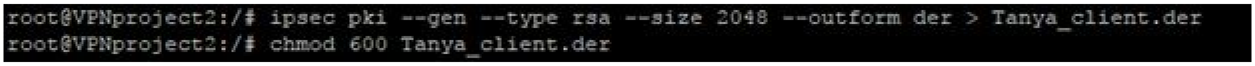
- *openssl rsa -inform DER -in /etc/ipsec.d/private/vpn-server-key.der -out /etc/ipsec.d/private/vpn-server-key.pem -outform PEM*
- *openssl rsa -inform DER -in /etc/ipsec.d/private/server-root-key.der -out /etc/ipsec.d/private/server-root-key.pem -outform PEM*
- *openssl x509 -inform DER -in /etc/ipsec.d/cacerts/server-root-ca.der -out /etc/ipsec.d/cacerts/server-root-ca.pem -outform PEM*



```
root@VPNproject2:/#  openssl rsa -inform DER -in /etc/ipsec.d/private/vpn-server
-key.der -out /etc/ipsec.d/private/vpn-server-key.pem -outform PEM
writing RSA key
root@VPNproject2:/# openssl rsa -inform DER -in /etc/ipsec.d/private/server-root
-key.der -out /etc/ipsec.d/private/server-root-key.pem -outform PEM
writing RSA key
root@VPNproject2:/# openssl x509 -inform DER -in /etc/ipsec.d/cacerts/server-roo
t-ca.der -out /etc/ipsec.d/cacerts/server-root-ca.pem -outform PEM
root@VPNproject2:/# 
```

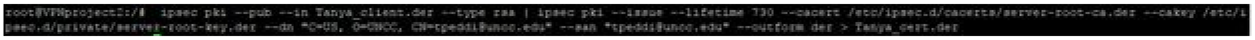
6) Client Certificate

- *ipsec pki --gen --type rsa --size 2048 --outform der > Tanya_client.der*
- *chmod 600 Manasi_client.der*



```
root@VPNproject2:/# ipsec pki --gen --type rsa --size 2048 --outform der > Tanya_client.der
root@VPNproject2:/# chmod 600 Tanya_client.der
```

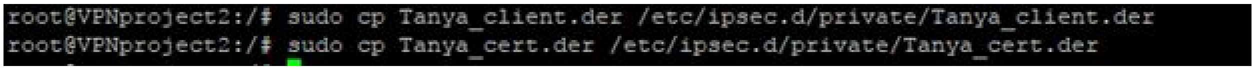
- *ipsec pki --pub --in Tanya_client.der --type rsa | ipsec pki --issue --lifetime 730 --cacert /etc/ipsec.d/cacerts/server-root-ca.der --cakey /etc/ipsec.d/private/server-root-key.der --dn "C=US, O=UNCC, CN=tpeddi@uncc.edu" --san "tpeddi@uncc.edu" --outform der > Tanya_cert.der*



```
root@VPNproject2:/#  ipsec pki --pub --in Tanya_client.der --type rsa | ipsec pki --issue --lifetime 730 --cacert /etc/ipsec.d/cacerts/server-root-ca.der --cakey /etc/i
psec.d/private/server-root-key.der --dn "C=US, O=UNCC, CN=tpeddi@uncc.edu" --san "tpeddi@uncc.edu" --outform der > Tanya_cert.der
```

We move them to require folders

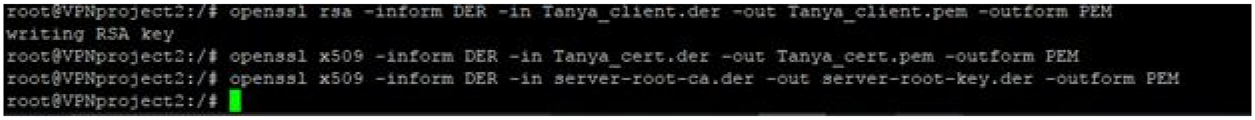
- *sudo cp Tanya_client.der /etc/ipsec.d/private/Tanya_client.der*
- *sudo cp Tanya_cert.der /etc/ipsec.d/private/Tanya_cert.der*



```
root@VPNproject2:/# sudo cp Tanya_client.der /etc/ipsec.d/private/Tanya_client.der
root@VPNproject2:/# sudo cp Tanya_cert.der /etc/ipsec.d/private/Tanya_cert.der
```

7) Convert from der to PEM files

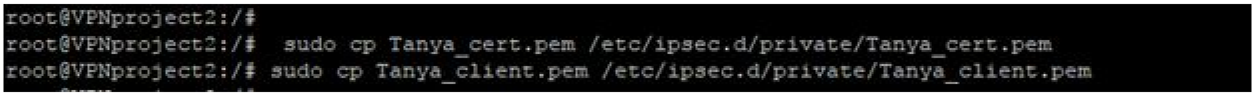
- *openssl rsa -inform DER -in Tanya_client.der -out Tanya_client.pem -outform PEM*
- *openssl x509 -inform DER -in Tanya_cert.der -out Tanya_cert.pem -outform PEM*
- *openssl x509 -inform DER -in server-root-ca.der -out server-root-key.der -outform PEM*



```
root@VPNproject2:/# openssl rsa -inform DER -in Tanya_client.der -out Tanya_client.pem -outform PEM
writing RSA key
root@VPNproject2:/# openssl x509 -inform DER -in Tanya_cert.der -out Tanya_cert.pem -outform PEM
root@VPNproject2:/# openssl x509 -inform DER -in server-root-ca.der -out server-root-key.der -outform PEM
root@VPNproject2:/#
```

We move these to required folders

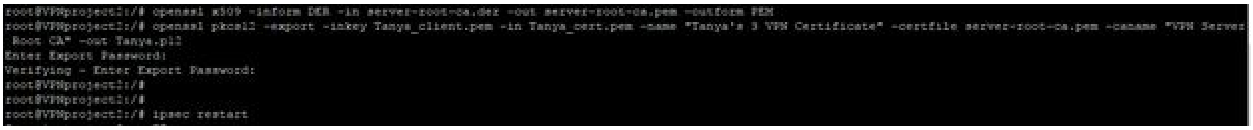
- *sudo cp Tanya_cert.pem /etc/ipsec.d/private/Tanya_cert.pem*
- *sudo cp Tanya_client.pem /etc/ipsec.d/private/Tanya_client.pem*



```
root@VPNproject2:/#
root@VPNproject2:/#  sudo cp Tanya_cert.pem /etc/ipsec.d/private/Tanya_cert.pem
root@VPNproject2:/# sudo cp Tanya_client.pem /etc/ipsec.d/private/Tanya_client.pem
```

8) Export to p12 format

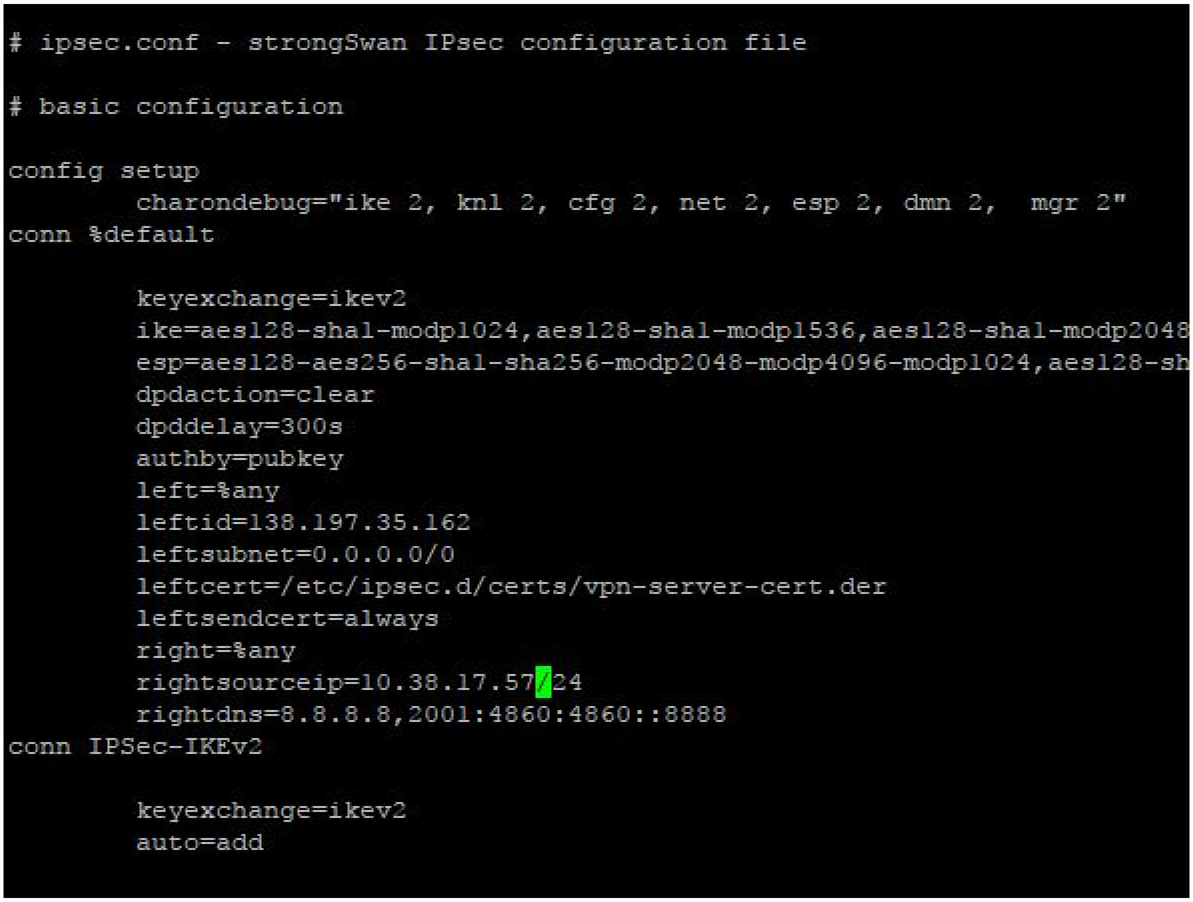
- *openssl x509 -inform DER -in server-root-ca.der -out server-root-ca.pem -outform PEM*
- *openssl pkcs12 -export -inkey Tanya_client.pem -in Tanya_cert.pem -name "My VPN Certificate" -certfile server-root-ca.pem -caname "VPN Server Root CA" -out Tanya_iphone.p12*



```
root@VPNproject2:/# openssl x509 -inform DER -in server-root-ca.der -out server-root-ca.pem -outform PEM
root@VPNproject2:/# openssl pkcs12 -export -inkey Tanya_client.pem -in Tanya_cert.pem -name "Tanya's 3 VPN Certificate" -certfile server-root-ca.pem -caname "VPN Server
 Root CA" -out Tanya.p12
Enter Export Password:
Verifying - Enter Export Password:
root@VPNproject2:/#
root@VPNproject2:/#
root@VPNproject2:/# ipsec restart
```

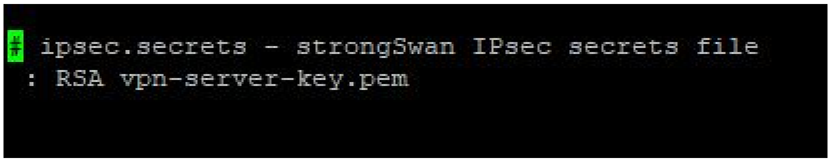
- *ipsec restart*

9) IPSEC Configuration file



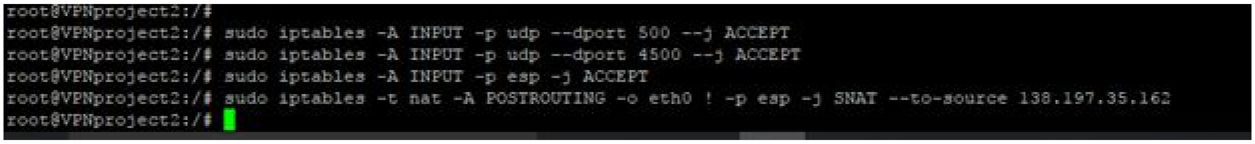
```
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        charondebug="ike 2, knl 2, cfg 2, net 2, esp 2, dmn 2,  mgr 2"
conn %default

        keyexchange=ikev2
        ike=aes128-sha1-modp1024,aes128-sha1-modp1536,aes128-sha1-modp2048
        esp=aes128-aes256-sha1-sha256-modp2048-modp4096-modp1024,aes128-sh
        dpdaction=clear
        dpddelay=300s
        authby=pubkey
        left=%any
        leftid=138.197.35.162
        leftsubnet=0.0.0.0/0
        leftcert=/etc/ipsec.d/certs/vpn-server-cert.der
        leftsendcert=always
        right=%any
        rightsourceip=10.38.17.57/24
        rightdns=8.8.8.8,2001:4860:4860::8888
conn IPSec-IKEv2

        keyexchange=ikev2
        auto=add
```

10) IPSEC Secrets file



```
# ipsec.secrets - strongSwan IPsec secrets file
 : RSA vpn-server-key.pem
```

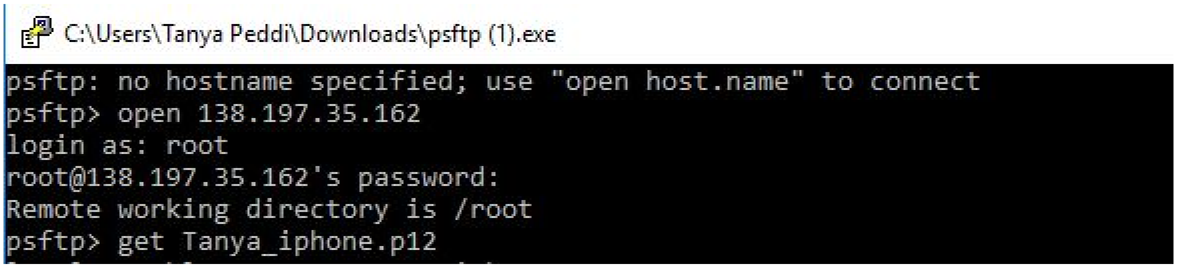
11) IPTABLES changes



```
root@VPNproject2:/#
root@VPNproject2:/# sudo iptables -A INPUT -p udp --dport 500 --j ACCEPT
root@VPNproject2:/# sudo iptables -A INPUT -p udp --dport 4500 --j ACCEPT
root@VPNproject2:/# sudo iptables -A INPUT -p esp -j ACCEPT
root@VPNproject2:/# sudo iptables -t nat -A POSTROUTING -o eth0 ! -p esp -j SNAT --to-source 138.197.35.162
root@VPNproject2:/#
```

12) Configuration of Client Machine

Using psftp.exe , we downloaded the p12 file as shown below

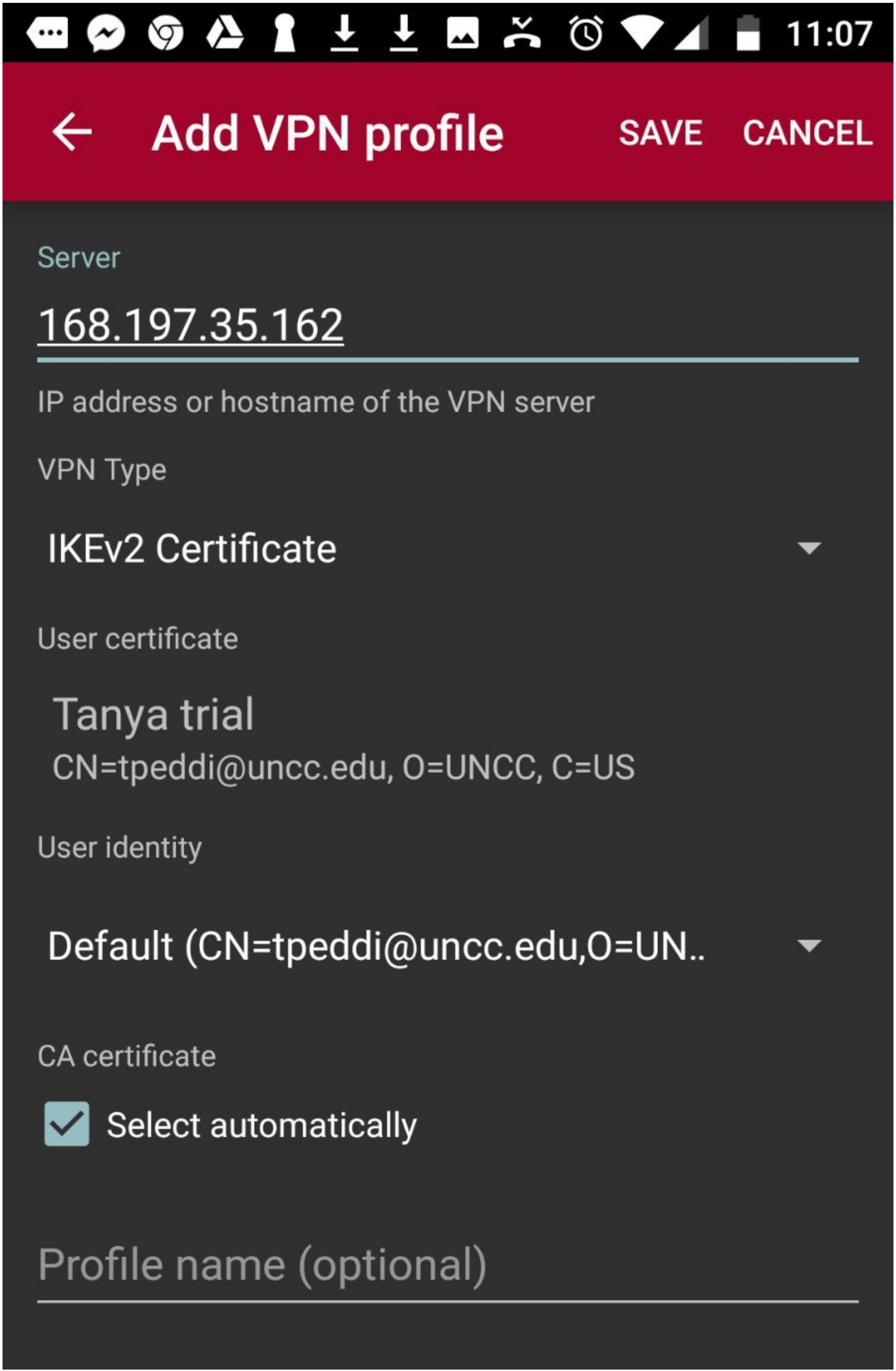


```
psftp: no hostname specified; use "open host.name" to connect
psftp> open 138.197.35.162
login as: root
root@138.197.35.162's password:
Remote working directory is /root
psftp> get Tanya_iphone.p12
```

The file was downloaded in the local machine Downloads folder from where I sent the certificate through an email to the phone.

On an android phone, I downloaded the certificate from the email and extracted it using the given password. I also installed the strongswanVPN Client app on the phone.

There I selected
-> Add VPN Profile
-> server : 138.197.35.162
-> VPN Type - IKEv2 Certificate
-> User Certificate -> selected the installed one (Tanya Trial)



Add VPN profile

Server

168.197.35.162

IP address or hostname of the VPN server

VPN Type

IKEv2 Certificate

User certificate

Tanya trial
CN=tpeddi@uncc.edu, O=UNCC, C=US

User identity

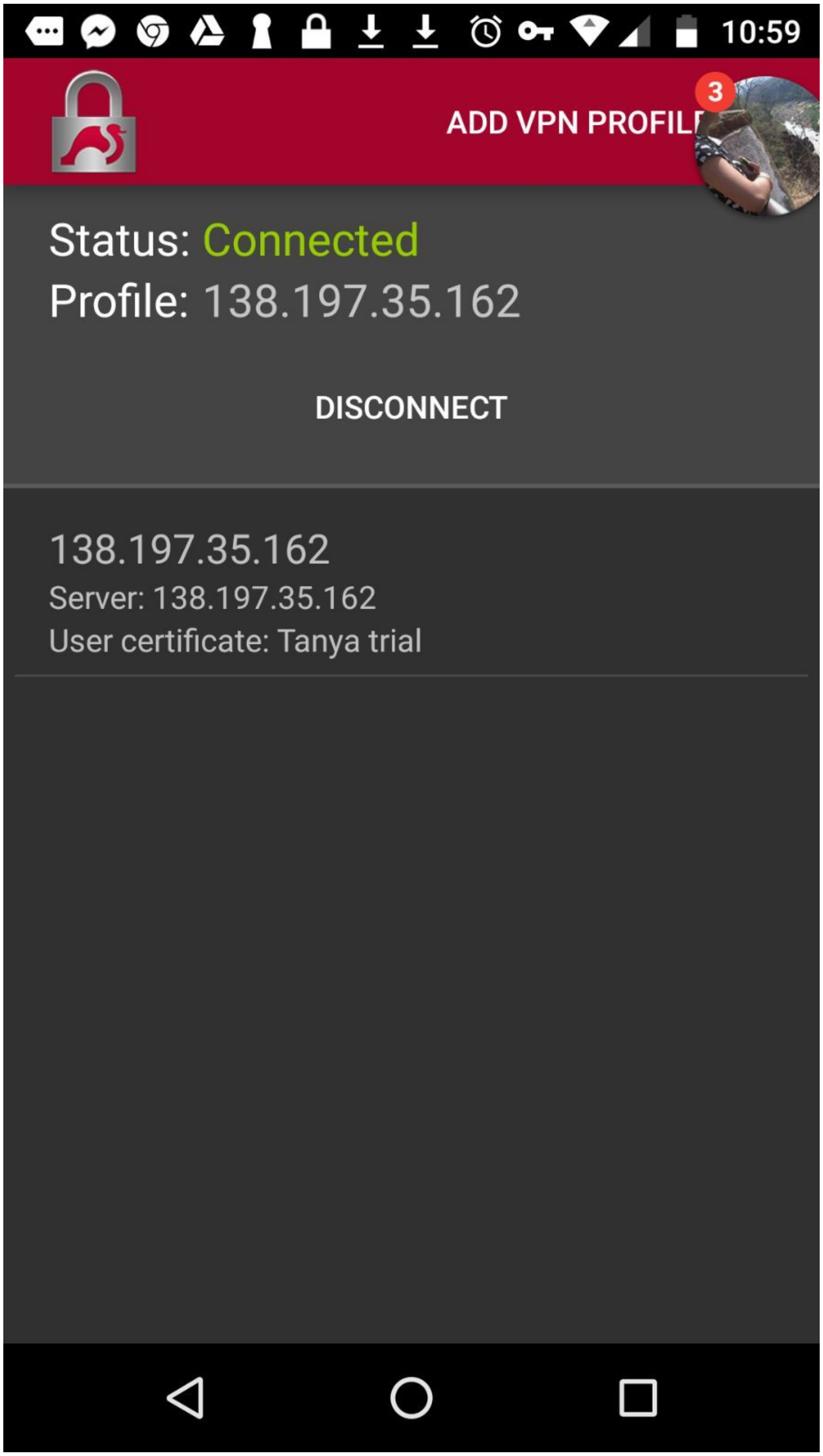
Default (CN=tpeddi@uncc.edu,O=UN..

CA certificate

☑ Select automatically

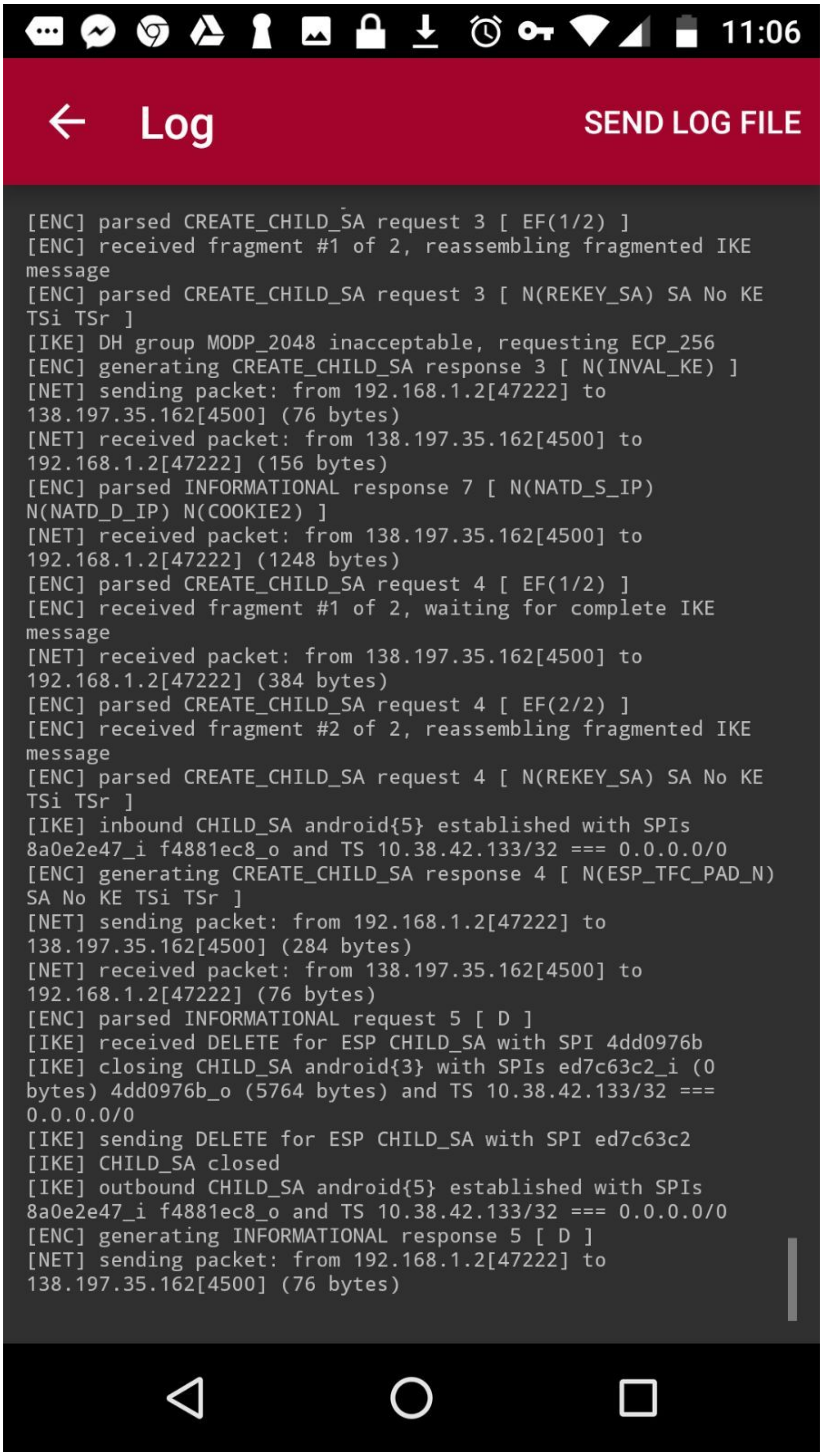
Profile name (optional)

13) Connection to Client Machine



Status: Connected
Profile: 138.197.35.162

138.197.35.162
Server: 138.197.35.162
User certificate: Tanya trial



```
[ENC] parsed CREATE_CHILD_SA request 3 [ EF(1/2) ]
[ENC] received fragment #1 of 2, reassembling fragmented IKE
message
[ENC] parsed CREATE_CHILD_SA request 3 [ N(REKEY_SA) SA No KE
TSi TSr ]
[IKE] DH group MODP_2048 inacceptable, requesting ECP_256
[ENC] generating CREATE_CHILD_SA response 3 [ N(INVAL_KE) ]
[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (76 bytes)
[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (156 bytes)
[ENC] parsed INFORMATIONAL response 7 [ N(NATD_S_IP)
N(NATD_D_IP) N(COOKIE2) ]
[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (1248 bytes)
[ENC] parsed CREATE_CHILD_SA request 4 [ EF(1/2) ]
[ENC] received fragment #1 of 2, waiting for complete IKE
message
[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (384 bytes)
[ENC] parsed CREATE_CHILD_SA request 4 [ EF(2/2) ]
[ENC] received fragment #2 of 2, reassembling fragmented IKE
message
[ENC] parsed CREATE_CHILD_SA request 4 [ N(REKEY_SA) SA No KE
TSi TSr ]
[IKE] inbound CHILD_SA android{5} established with SPIs
8a0e2e47_i f4881ec8_o and TS 10.38.42.133/32 === 0.0.0.0/0
[ENC] generating CREATE_CHILD_SA response 4 [ N(ESP_TFC_PAD_N)
SA No KE TSi TSr ]
[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (284 bytes)
[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (76 bytes)
[ENC] parsed INFORMATIONAL request 5 [ D ]
[IKE] received DELETE for ESP CHILD_SA with SPI 4dd0976b
[IKE] closing CHILD_SA android{3} with SPIs ed7c63c2_i (0
bytes) 4dd0976b_o (5764 bytes) and TS 10.38.42.133/32 ===
0.0.0.0/0
[IKE] sending DELETE for ESP CHILD_SA with SPI ed7c63c2
[IKE] CHILD_SA closed
[IKE] outbound CHILD_SA android{5} established with SPIs
8a0e2e47_i f4881ec8_o and TS 10.38.42.133/32 === 0.0.0.0/0
[ENC] generating INFORMATIONAL response 5 [ D ]
[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (76 bytes)
```

14) Log File

```
Nov 26 22:59:13 00[DMN] Starting IKE charon daemon (strongSwan 5.6.1dr3, Android
7.0 - NPJ25.93-14/2016-12-01, Moto G (4) - motorola/athene_f/motorola, Linux
3.10.84-g478d03a, armv7l)
Nov 26 22:59:13 00[LIB] loaded plugins: androidbridge charon android-log openssl
fips-prf random nonce pubkey chapoly curve25519 pkcs1 pkcs8 pem xcbc hmac
socket-default revocation eap-identity eap-mschapv2 eap-md5 eap-gtc eap-tls x509
Nov 26 22:59:13 00[JOB] spawning 16 worker threads
Nov 26 22:59:13 08[CFG] loaded user certificate 'C=US, O=UNCC,
CN=tpeddi@uncc.edu' and private key
Nov 26 22:59:13 08[CFG] loaded CA certificate 'C=US, CN=My VPN Server Root CA'
Nov 26 22:59:14 08[IKE] initiating IKE_SA android[3] to 138.197.35.162
Nov 26 22:59:14 08[ENC] 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) ]
Nov 26 22:59:14 08[NET] sending packet: from 192.168.1.28[45532] to
138.197.35.162[500] (704 bytes)
Nov 26 22:59:14 11[NET] received packet: from 138.197.35.162[500] to
192.168.1.28[45532] (38 bytes)
Nov 26 22:59:14 11[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Nov 26 22:59:14 11[IKE] peer didn't accept DH group ECP_256, it requested
MODP_2048
Nov 26 22:59:14 11[IKE] initiating IKE_SA android[3] to 138.197.35.162
Nov 26 22:59:14 11[ENC] 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) ]
Nov 26 22:59:14 11[NET] sending packet: from 192.168.1.28[45532] to
138.197.35.162[500] (896 bytes)
Nov 26 22:59:16 12[IKE] retransmit 1 of request with message ID 0
Nov 26 22:59:16 12[NET] sending packet: from 192.168.1.28[45532] to
138.197.35.162[500] (896 bytes)
Nov 26 22:59:16 13[NET] received packet: from 138.197.35.162[500] to
192.168.1.28[45532] (491 bytes)
Nov 26 22:59:16 13[ENC] 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(MULT_AUTH) ]
Nov 26 22:59:16 13[IKE] local host is behind NAT, sending keep alives
Nov 26 22:59:16 13[IKE] remote host is behind NAT
Nov 26 22:59:16 13[IKE] received cert request for "C=US, CN=My VPN Server Root
CA"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "C=CN, O=WoSign CA Limited,
CN=CA WoSign ECC Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=FR, O=Certinomis, OU=0002
433998903, CN=Certinomis - Autorit?? Racine"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=IdenTrust, CN=IdenTrust
Public Sector Root CA 1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=NL, O=Staat der Nederlanden,
CN=Staat der Nederlanden EV Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=DigiCert Inc,
OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "OU=GlobalSign Root CA - R3,
O=GlobalSign, CN=GlobalSign"
Nov 26 22:59:16 13[IKE] sending cert request for "C=IT, L=Milan, O=Actalis
S.p.A./03358520967, CN=Actalis Authentication Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=JP, O=SECOM Trust.net,
OU=Security Communication RootCA1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=IdenTrust, CN=IdenTrust
Commercial Root CA 1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=JP, O=Japanese Government,
OU=ApplicationCA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=DigiCert Inc,
OU=www.digicert.com, CN=DigiCert Assured ID Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=Starfield Technologies,
Inc., OU=Starfield Class 2 Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=TW, O=Chunghwa Telecom Co.,
Ltd., OU=ePKI Root Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=RO, O=certSIGN, OU=certSIGN
ROOT CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=FR, O=Dhimyotis, CN=Certigna"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=GeoTrust Inc.,
CN=GeoTrust Universal CA 2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=CN, O=WoSign CA Limited,
CN=Certification Authority of WoSign G2"
Nov 26 22:59:16 13[IKE] sending cert request for "O=RSA Security Inc, OU=RSA
Security 2048 V3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=NO, O=Buypass AS-983163327,
CN=Buypass Class 2 Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=SK, L=Bratislava, O=Disig a.s.,
CN=CA Disig Root R2"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "C=TR, L=Ankara, O=E-Tu??ra EBG
Bili??im Teknolojileri ve Hizmetleri A.??., OU=E-Tugra Sertifikasyon Merkezi,
CN=E-Tugra Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=DigiCert Inc,
OU=www.digicert.com, CN=DigiCert Trusted Root G4"
Nov 26 22:59:16 13[IKE] sending cert request for "C=TR, L=Gebze - Kocaeli,
O=T??rkiye Bilimsel ve Teknolojik Ara??t??rma Kurumu - T??B??TAK, OU=Ulusal
Elektronik ve Kriptoloji Ara??t??rma Enstit??s?? - UEKAE, OU=Kamu Sertifikasyon
Merkezi, CN=T??B??TAK UEKAE K??k Sertifika Hizmet Sa??lay??c??s?? - S??r??m
3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=GeoTrust Inc.,
CN=GeoTrust Primary Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=SK, L=Bratislava, O=Disig a.s.,
CN=CA Disig Root R1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, ST=New Jersey, L=Jersey
City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=DigiCert Inc,
OU=www.digicert.com, CN=DigiCert Global Root G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=FR, ST=France, L=Paris,
O=PM/SGDN, OU=DCSSI, CN=IGC/A, E=igca@sgdn.pm.gouv.fr"
Nov 26 22:59:16 13[IKE] sending cert request for "C=CH, O=SwissSign AG,
CN=SwissSign Gold CA - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=SecureTrust Corporation,
CN=SecureTrust CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=GB, ST=Greater Manchester,
L=Salford, O=Comodo CA Limited, CN=Trusted Certificate Services"
Nov 26 22:59:16 13[IKE] sending cert request for "C=SE, O=AddTrust AB,
OU=AddTrust TTP Network, CN=AddTrust Qualified CA Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=BE, O=GlobalSign nv-sa,
OU=Root CA, CN=GlobalSign Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=BM, O=QuoVadis Limited,
CN=QuoVadis Root CA 3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=GR, O=Hellenic Academic and
Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions
RootCA 2011"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=DigiCert Inc,
OU=www.digicert.com, CN=DigiCert Global Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "CN=ACCVRAIZ1, OU=PKIACCV,
O=ACCV, C=ES"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "C=BM, O=QuoVadis Limited,
CN=QuoVadis Root CA 2 G3"
Nov 26 22:59:16 13[IKE] sending cert request for "O=Cybertrust, Inc, CN=Cybertrust
Global Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=BM, O=QuoVadis Limited,
CN=QuoVadis Root CA 2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=TW, O=TAIWAN-CA, OU=Root
CA, CN=TWCA Global Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=ch, O=Swisscom, OU=Digital
Certificate Services, CN=Swisscom Root CA 2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=GB, ST=Greater Manchester,
L=Salford, O=COMODO CA Limited, CN=COMODO ECC Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=ch, O=Swisscom, OU=Digital
Certificate Services, CN=Swisscom Root CA 1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=HK, O=Hongkong Post,
CN=Hongkong Post Root CA 1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=IL, O=StartCom Ltd.,
CN=StartCom Certification Authority G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=GeoTrust Inc.,
CN=GeoTrust Global CA 2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=NL, O=Staat der Nederlanden,
CN=Staat der Nederlanden Root CA - G3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=HU, L=Budapest, O=Microsec
Ltd., CN=Microsec e-Szigno Root CA 2009, E=info@e-szigno.hu"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=AffirmTrust,
CN=AffirmTrust Commercial"
Nov 26 22:59:16 13[IKE] sending cert request for "C=ES, O=Agencia Catalana de
Certificacio (NIF Q-0801176-I), OU=Serveis Publics de Certificacio, OU=Vegeu
https://www.catcert.net/verarrel (c)03, OU=Jerarquia Entitats de Certificacio Catalanes,
CN=EC-ACC"
Nov 26 22:59:16 13[IKE] sending cert request for "C=FR, O=Certinomis, OU=0002
433998903, CN=Certinomis - Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, ST=Arizona, L=Scottsdale,
O=Starfield Technologies, Inc., CN=Starfield Services Root Certificate Authority - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=DE, O=D-Trust GmbH,
CN=D-TRUST Root Class 3 CA 2 EV 2009"
Nov 26 22:59:16 13[IKE] sending cert request for "C=ES, CN=Autoridad de Certificacion
Firmaprofesional CIF A62634068"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "E=pki@sk.ee, C=EE, O=AS
Sertifitseerimiskeskus, CN=Juur-SK"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=thawte, Inc.,
OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only,
CN=thawte Primary Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=ch, O=Swisscom, OU=Digital
Certificate Services, CN=Swisscom Root EV CA 2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=Entrust, Inc.,
OU=www.entrust.net/CPS is incorporated by reference, OU=(c) 2006 Entrust, Inc.,
CN=Entrust Root Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, ST=UT, L=Salt Lake City,
O=The USERTRUST Network, OU=http://www.usertrust.com,
CN=UTN-USERFirst-Hardware"
Nov 26 22:59:16 13[IKE] sending cert request for "C=ES, O=Generalitat Valenciana,
OU=PKIGVA, CN=Root CA Generalitat Valenciana"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=thawte, Inc., OU=(c) 2007
thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, ST=Arizona, L=Scottsdale,
O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=Digital Signature Trust,
OU=DST ACES, CN=DST ACES CA X6"
Nov 26 22:59:16 13[IKE] sending cert request for "C=CH, O=WISeKey, OU=OISTE
Foundation Endorsed, CN=OISTE WISeKey Global Root GB CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=ES, O=IZENPE S.A.,
CN=Izenpe.com"
Nov 26 22:59:16 13[IKE] sending cert request for "CN=Atos TrustedRoot 2011, O=Atos,
C=DE"
Nov 26 22:59:16 13[IKE] sending cert request for "C=EU, L=Madrid (see current
address at www.camerfirma.com/address), SN=A82743287, O=AC Camerfirma S.A.,
CN=Chambers of Commerce Root - 2008"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=Network Solutions L.L.C.,
CN=Network Solutions Certificate Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=TR, L=Ankara, O=T??RKTRUST
Bilgi ??leti??im ve Bili??im G??venli??i Hizmetleri A.??., CN=T??RKTRUST Elektronik
Sertifika Hizmet Sa??lay??c??s?? H6"
Nov 26 22:59:16 13[IKE] sending cert request for "C=FR, O=Certplus, CN=Class 2
Primary CA"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=GeoTrust Inc., OU=(c)
2008 GeoTrust Inc. - For authorized use only, CN=GeoTrust Primary Certification
Authority - G3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=GeoTrust Inc., OU=(c)
2007 GeoTrust Inc. - For authorized use only, CN=GeoTrust Primary Certification
Authority - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=VeriSign, Inc.,
OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only,
CN=VeriSign Universal Root Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=BM, O=QuoVadis Limited,
OU=Root Certification Authority, CN=QuoVadis Root Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=DE, O=T-Systems Enterprise
Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=DigiCert Inc,
OU=www.digicert.com, CN=DigiCert Assured ID Root G3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=DigiCert Inc,
OU=www.digicert.com, CN=DigiCert Assured ID Root G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, ST=Arizona, L=Scottsdale,
O=Starfield Technologies, Inc., CN=Starfield Root Certificate Authority - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=GB, ST=Greater Manchester,
L=Salford, O=Comodo CA Limited, CN=AAA Certificate Services"
Nov 26 22:59:16 13[IKE] sending cert request for "C=GB, ST=Greater Manchester,
L=Salford, O=Comodo CA Limited, CN=Secure Certificate Services"
Nov 26 22:59:16 13[IKE] sending cert request for "C=TW, O=TAIWAN-CA, OU=Root
CA, CN=TWCA Root Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=JP, O=SECOM Trust Systems
CO.,LTD., OU=Security Communication EV RootCA1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=TR, L=Ankara, O=T??RKTRUST
Bilgi ??leti??im ve Bili??im G??venli??i Hizmetleri A.??., CN=T??RKTRUST Elektronik
Sertifika Hizmet Sa??lay??c??s?? H5"
Nov 26 22:59:16 13[IKE] sending cert request for "C=NO, O=Buypass AS-983163327,
CN=Buypass Class 2 CA 1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=VISA, OU=Visa
International Service Association, CN=Visa eCommerce Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=HU, L=Budapest, O=NetLock Kft.,
OU=Tan??s??tv??nykiad??k (Certification Services), CN=NetLock Arany (Class Gold)
F??tan??s??tv??ny"
Nov 26 22:59:16 13[IKE] sending cert request for "C=FI, O=Sonera, CN=Sonera Class2
CA"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "C=BM, O=QuoVadis Limited,
CN=QuoVadis Root CA 1 G3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=VeriSign, Inc.,
OU=VeriSign Trust Network, OU=(c) 2007 VeriSign, Inc. - For authorized use only,
CN=VeriSign Class 3 Public Primary Certification Authority - G4"
Nov 26 22:59:16 13[IKE] sending cert request for "OU=GlobalSign ECC Root CA - R4,
O=GlobalSign, CN=GlobalSign"
Nov 26 22:59:16 13[IKE] sending cert request for "C=GB, O=Trustis Limited,
OU=Trustis FPS Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=DigiCert Inc,
OU=www.digicert.com, CN=DigiCert Global Root G3"
Nov 26 22:59:16 13[IKE] sending cert request for "CN=ACEDICOM Root, OU=PKI,
O=EDICOM, C=ES"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=The Go Daddy Group, Inc.,
OU=Go Daddy Class 2 Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=CN, O=WoSign CA Limited,
CN=Certification Authority of WoSign"
Nov 26 22:59:16 13[IKE] sending cert request for "C=PL, O=Unizeto Technologies S.A.,
OU=Certum Certification Authority, CN=Certum Trusted Network CA 2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=IL, O=StartCom Ltd., OU=Secure
Digital Certificate Signing, CN=StartCom Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=IL, O=StartCom Ltd., OU=Secure
Digital Certificate Signing, CN=StartCom Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "O=Digital Signature Trust Co.,
CN=DST Root CA X3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=thawte, Inc.,
OU=Certification Services Division, OU=(c) 2008 thawte, Inc. - For authorized use only,
CN=thawte Primary Root CA - G3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=BM, O=QuoVadis Limited,
CN=QuoVadis Root CA 3 G3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=SE, O=AddTrust AB,
OU=AddTrust TTP Network, CN=AddTrust Public CA Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=JP, O=Japan Certification
Services, Inc., CN=SecureSign RootCA11"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=SecureTrust Corporation,
CN=Secure Global CA"
Nov 26 22:59:16 13[IKE] sending cert request for "CN=EBG Elektronik Sertifika Hizmet
Sa??lay??c??s??, O=EBG Bili??im Teknolojileri ve Hizmetleri A.??., C=TR"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "O=Entrust.net,
OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.), OU=(c) 1999 Entrust.net
Limited, CN=Entrust.net Certification Authority (2048)"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=GeoTrust Inc.,
CN=GeoTrust Global CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=SE, O=AddTrust AB,
OU=AddTrust External TTP Network, CN=AddTrust External CA Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=GB, ST=Greater Manchester,
L=Salford, O=COMODO CA Limited, CN=COMODO RSA Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=Entrust, Inc., OU=See
www.entrust.net/legal-terms, OU=(c) 2009 Entrust, Inc. - for authorized use only,
CN=Entrust Root Certification Authority - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=VeriSign, Inc.,
OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only,
CN=VeriSign Class 3 Public Primary Certification Authority - G5"
Nov 26 22:59:16 13[IKE] sending cert request for "C=DE, O=T-Systems Enterprise
Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 3"
Nov 26 22:59:16 13[IKE] sending cert request for "C=CH, O=WISeKey, OU=Copyright
(c) 2005, OU=OISTE Foundation Endorsed, CN=OISTE WISeKey Global Root GA CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=EE, O=AS Sertifitseerimiskeskus,
CN=EE Certification Centre Root CA, E=pki@sk.ee"
Nov 26 22:59:16 13[IKE] sending cert request for "C=JP, O=SECOM Trust Systems
CO.,LTD., OU=Security Communication RootCA2"
Nov 26 22:59:16 13[IKE] sending cert request for "OU=GlobalSign Root CA - R2,
O=GlobalSign, CN=GlobalSign"
Nov 26 22:59:16 13[IKE] sending cert request for "C=PL, O=Krajowa Izba
Rozliczeniowa S.A., CN=SZAFIR ROOT CA2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=AffirmTrust,
CN=AffirmTrust Premium ECC"
Nov 26 22:59:16 13[IKE] sending cert request for "C=GB, ST=Greater Manchester,
L=Salford, O=COMODO CA Limited, CN=COMODO Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=SE, O=AddTrust AB,
OU=AddTrust TTP Network, CN=AddTrust Class 1 CA Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=NO, O=Buypass AS-983163327,
CN=Buypass Class 3 Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=AffirmTrust,
CN=AffirmTrust Premium"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, OU=www.xrampsecurity.com,
O=XRamp Security Services Inc, CN=XRamp Global Certification Authority"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "C=CN, O=China Internet Network
Information Center, CN=China Internet Network Information Center EV Certificates
Root"
Nov 26 22:59:16 13[IKE] sending cert request for "O=TeliaSonera, CN=TeliaSonera
Root CA v1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=IE, O=Baltimore, OU=CyberTrust,
CN=Baltimore CyberTrust Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=GeoTrust Inc.,
CN=GeoTrust Universal CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=Wells Fargo WellsSecure,
OU=Wells Fargo Bank NA, CN=WellsSecure Public Root Certificate Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=HU, L=Budapest, O=Microsec
Ltd., OU=e-Szigno CA, CN=Microsec e-Szigno Root CA"
Nov 26 22:59:16 13[IKE] sending cert request for "OU=GlobalSign ECC Root CA - R5,
O=GlobalSign, CN=GlobalSign"
Nov 26 22:59:16 13[IKE] sending cert request for "C=DE, O=Deutsche Telekom AG,
OU=T-TeleSec Trust Center, CN=Deutsche Telekom Root CA 2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=EU, O=AC Camerfirma SA CIF
A82743287, OU=http://www.chambersign.org, CN=Global Chambersign Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=Entrust, Inc., OU=See
www.entrust.net/legal-terms, OU=(c) 2012 Entrust, Inc. - for authorized use only,
CN=Entrust Root Certification Authority - EC1"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, ST=New Jersey, L=Jersey
City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=CH, O=SwissSign AG,
CN=SwissSign Silver CA - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=DE, O=D-Trust GmbH,
CN=D-TRUST Root Class 3 CA 2 2009"
Nov 26 22:59:16 13[IKE] sending cert request for "C=PL, O=Unizeto Sp. z o.o.,
CN=Certum CA"
Nov 26 22:59:16 13[IKE] sending cert request for "C=TW, O=Government Root
Certification Authority"
Nov 26 22:59:16 13[IKE] sending cert request for "C=EU, L=Madrid (see current
address at www.camerfirma.com/address), SN=A82743287, O=AC Camerfirma S.A.,
CN=Global Chambersign Root - 2008"
Nov 26 22:59:16 13[IKE] sending cert request for "C=NL, O=Staat der Nederlanden,
CN=Staat der Nederlanden Root CA - G2"
Nov 26 22:59:16 13[IKE] sending cert request for "C=CN, O=China Financial
Certification Authority, CN=CFCA EV ROOT"
```

```
Nov 26 22:59:16 13[IKE] sending cert request for "C=PL, O=Unizeto Technologies S.A.,
OU=Certum Certification Authority, CN=Certum Trusted Network CA"
Nov 26 22:59:16 13[IKE] sending cert request for "CN=T??RKTRUST Elektronik
Sertifika Hizmet Sa??lay??c??s??, C=TR, L=Ankara, O=T??RKTRUST Bilgi ??leti??im
ve Bili??im G??venli??i Hizmetleri A.??. (c) Aral??k 2007"
Nov 26 22:59:16 13[IKE] sending cert request for "C=EU, O=AC Camerfirma SA CIF
A82743287, OU=http://www.chambersign.org, CN=Chambers of Commerce Root"
Nov 26 22:59:16 13[IKE] sending cert request for "C=CN, O=WoSign CA Limited,
CN=CA ???????????????"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, O=AffirmTrust,
CN=AffirmTrust Networking"
Nov 26 22:59:16 13[IKE] sending cert request for "C=US, CN=My VPN Server Root CA"
Nov 26 22:59:17 13[IKE] authentication of 'C=US, O=UNCC, CN=tpeddi@uncc.edu'
(myself) with RSA_EMSA_PKCS1_SHA2_256 successful
Nov 26 22:59:17 13[IKE] sending end entity cert "C=US, O=UNCC,
CN=tpeddi@uncc.edu"
Nov 26 22:59:17 13[IKE] establishing CHILD_SA android{1}
Nov 26 22:59:17 13[ENC] generating IKE_AUTH request 1 [ IDi CERT
N(INIT_CONTACT) CERTREQ AUTH CPRQ(ADDR ADDR6 DNS DNS6)
N(ESP_TFC_PAD_N) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR)
N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Nov 26 22:59:17 13[ENC] splitting IKE message with length of 4876 bytes into 4
fragments
Nov 26 22:59:17 13[ENC] generating IKE_AUTH request 1 [ EF(1/4) ]
Nov 26 22:59:17 13[ENC] generating IKE_AUTH request 1 [ EF(2/4) ]
Nov 26 22:59:17 13[ENC] generating IKE_AUTH request 1 [ EF(3/4) ]
Nov 26 22:59:17 13[ENC] generating IKE_AUTH request 1 [ EF(4/4) ]
Nov 26 22:59:17 13[NET] sending packet: from 192.168.1.28[47222] to
138.197.35.162[4500] (1360 bytes)
Nov 26 22:59:17 13[NET] sending packet: from 192.168.1.28[47222] to
138.197.35.162[4500] (1360 bytes)
Nov 26 22:59:17 13[NET] sending packet: from 192.168.1.28[47222] to
138.197.35.162[4500] (1360 bytes)
Nov 26 22:59:17 13[NET] sending packet: from 192.168.1.28[47222] to
138.197.35.162[4500] (1008 bytes)
Nov 26 22:59:17 07[NET] received packet: from 138.197.35.162[4500] to
192.168.1.28[47222] (1248 bytes)
Nov 26 22:59:17 07[ENC] parsed IKE_AUTH response 1 [ EF(1/2) ]
Nov 26 22:59:17 07[ENC] received fragment #1 of 2, waiting for complete IKE message
Nov 26 22:59:17 15[NET] received packet: from 138.197.35.162[4500] to
192.168.1.28[47222] (1024 bytes)
Nov 26 22:59:17 15[ENC] parsed IKE_AUTH response 1 [ EF(2/2) ]
Nov 26 22:59:17 15[ENC] received fragment #2 of 2, reassembling fragmented IKE
message
Nov 26 22:59:17 15[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH
CPRP(ADDR DNS DNS6) SA TSi TSr N(AUTH_LFT) N(MOBIKE_SUP)
N(ADD_4_ADDR) ]
Nov 26 22:59:17 15[IKE] received end entity cert "C=US, O=UNCC,
CN=138.197.35.162"
Nov 26 22:59:17 15[CFG]   using certificate "C=US, O=UNCC, CN=138.197.35.162"
Nov 26 22:59:17 15[CFG]   using trusted ca certificate "C=US, CN=My VPN Server
Root CA"
Nov 26 22:59:17 15[CFG] checking certificate status of "C=US, O=UNCC,
CN=138.197.35.162"
Nov 26 22:59:17 15[CFG] certificate status is not available
Nov 26 22:59:17 15[CFG]   reached self-signed root ca with a path length of 0
Nov 26 22:59:17 15[IKE] authentication of 'C=US, O=UNCC, CN=138.197.35.162' with
RSA_EMSA_PKCS1_SHA2_384 successful
Nov 26 22:59:17 15[IKE] IKE_SA android[3] established between 192.168.1.28[C=US,
O=UNCC, CN=tpeddi@uncc.edu]...138.197.35.162[C=US, O=UNCC,
CN=138.197.35.162]
Nov 26 22:59:17 15[IKE] scheduling rekeying in 35426s
Nov 26 22:59:17 15[IKE] maximum IKE_SA lifetime 36026s
Nov 26 22:59:17 15[IKE] installing DNS server 8.8.8.8
Nov 26 22:59:17 15[IKE] installing DNS server 2001:4860:4860::8888
Nov 26 22:59:17 15[IKE] installing new virtual IP 10.38.42.133
Nov 26 22:59:17 15[IKE] CHILD_SA android{1} established with SPIs 7ee56261_i
87bbdc9b_o and TS 10.38.42.133/32 === 0.0.0.0/0
Nov 26 22:59:17 15[DMN] setting up TUN device for CHILD_SA android{1}
Nov 26 22:59:17 15[DMN] successfully created TUN device
Nov 26 22:59:17 15[IKE] received AUTH_LIFETIME of 10123s, scheduling
reauthentication in 9523s
Nov 26 22:59:17 15[IKE] peer supports MOBIKE
Nov 26 22:59:17 09[IKE] sending address list update using MOBIKE
Nov 26 22:59:17 09[ENC] generating INFORMATIONAL request 2 [
N(NO_ADD_ADDR) ]
Nov 26 22:59:17 09[NET] sending packet: from 192.168.1.28[47222] to
138.197.35.162[4500] (76 bytes)
```

```
Nov 26 22:59:17 08[NET] received packet: from 138.197.35.162[4500] to
192.168.1.28[47222] (76 bytes)
Nov 26 22:59:17 08[ENC] parsed INFORMATIONAL response 2 [ ]
Nov 26 23:02:34 09[IKE] old path is not available anymore, try to find another
Nov 26 23:02:34 09[IKE] looking for a route to 138.197.35.162 ...
Nov 26 23:02:34 09[IKE] looking for a route to 10.17.0.5 ...
Nov 26 23:02:34 09[IKE] no route found to reach 138.197.35.162, MOBIKE update
deferred
Nov 26 23:02:35 03[NET] error writing to socket: Network is unreachable
Nov 26 23:02:35 11[IKE] old path is not available anymore, try to find another
Nov 26 23:02:35 11[IKE] looking for a route to 138.197.35.162 ...
Nov 26 23:02:35 11[IKE] looking for a route to 10.17.0.5 ...
Nov 26 23:02:35 11[IKE] no route found to reach 138.197.35.162, MOBIKE update
deferred
Nov 26 23:02:35 03[NET] error writing to socket: Network is unreachable
Nov 26 23:02:36 14[IKE] old path is not available anymore, try to find another
Nov 26 23:02:36 14[IKE] looking for a route to 138.197.35.162 ...
Nov 26 23:02:36 14[IKE] requesting address change using MOBIKE
Nov 26 23:02:36 14[ENC] generating INFORMATIONAL request 3 [ ]
Nov 26 23:02:36 14[IKE] checking path 192.0.0.4[47222] - 138.197.35.162[4500]
Nov 26 23:02:36 14[NET] sending packet: from 192.0.0.4[47222] to
138.197.35.162[4500] (76 bytes)
Nov 26 23:02:36 14[IKE] checking path 192.0.0.4[47222] - 10.17.0.5[4500]
Nov 26 23:02:36 14[NET] sending packet: from 192.0.0.4[47222] to 10.17.0.5[4500] (76
bytes)
Nov 26 23:02:36 07[NET] received packet: from 138.197.35.162[4500] to
192.0.0.4[47222] (76 bytes)
Nov 26 23:02:36 07[ENC] parsed INFORMATIONAL response 3 [ ]
Nov 26 23:02:36 07[ENC] generating INFORMATIONAL request 4 [ N(UPD_SA_ADDR)
N(NATD_S_IP) N(NATD_D_IP) N(COOKIE2) N(NO_ADD_ADDR) ]
Nov 26 23:02:36 07[NET] sending packet: from 192.0.0.4[47222] to
138.197.35.162[4500] (172 bytes)
Nov 26 23:02:36 15[NET] received packet: from 138.197.35.162[4500] to
192.0.0.4[47222] (1248 bytes)
Nov 26 23:02:36 15[ENC] parsed CREATE_CHILD_SA request 0 [ EF(1/2) ]
Nov 26 23:02:36 15[ENC] received fragment #1 of 2, waiting for complete IKE message
Nov 26 23:02:36 10[NET] received packet: from 138.197.35.162[4500] to
192.0.0.4[47222] (156 bytes)
```

```
Nov 26 23:02:36 10[ENC] parsed INFORMATIONAL response 4 [ N(NATD_S_IP)
N(NATD_D_IP) N(COOKIE2) ]
Nov 26 23:02:36 08[NET] received packet: from 138.197.35.162[4500] to
192.0.0.4[47222] (576 bytes)
Nov 26 23:02:36 08[ENC] parsed CREATE_CHILD_SA request 0 [ EF(2/2) ]
Nov 26 23:02:36 08[ENC] received fragment #2 of 2, reassembling fragmented IKE
message
Nov 26 23:02:36 08[ENC] parsed CREATE_CHILD_SA request 0 [ N(REKEY_SA) SA
No KE TSi TSr ]
Nov 26 23:02:37 08[IKE] DH group MODP_2048 inacceptable, requesting ECP_256
Nov 26 23:02:37 08[ENC] generating CREATE_CHILD_SA response 0 [ N(INVAL_KE) ]
Nov 26 23:02:37 08[NET] sending packet: from 192.0.0.4[47222] to
138.197.35.162[4500] (76 bytes)
Nov 26 23:02:37 09[NET] received packet: from 138.197.35.162[4500] to
192.0.0.4[47222] (1248 bytes)
Nov 26 23:02:37 09[ENC] parsed CREATE_CHILD_SA request 1 [ EF(1/2) ]
Nov 26 23:02:37 09[ENC] received fragment #1 of 2, waiting for complete IKE message
Nov 26 23:02:37 09[NET] received packet: from 138.197.35.162[4500] to
192.0.0.4[47222] (384 bytes)
Nov 26 23:02:37 09[ENC] parsed CREATE_CHILD_SA request 1 [ EF(2/2) ]
Nov 26 23:02:37 09[ENC] received fragment #2 of 2, reassembling fragmented IKE
message
Nov 26 23:02:37 09[ENC] parsed CREATE_CHILD_SA request 1 [ N(REKEY_SA) SA
No KE TSi TSr ]
Nov 26 23:02:37 09[IKE] inbound CHILD_SA android{3} established with SPIs
ed7c63c2_i 4dd0976b_o and TS 10.38.42.133/32 === 0.0.0.0/0
Nov 26 23:02:37 09[ENC] generating CREATE_CHILD_SA response 1 [
N(ESP_TFC_PAD_N) SA No KE TSi TSr ]
Nov 26 23:02:37 09[NET] sending packet: from 192.0.0.4[47222] to
138.197.35.162[4500] (284 bytes)
Nov 26 23:02:37 11[NET] received packet: from 138.197.35.162[4500] to
192.0.0.4[47222] (76 bytes)
Nov 26 23:02:37 11[ENC] parsed INFORMATIONAL request 2 [ D ]
Nov 26 23:02:37 11[IKE] received DELETE for ESP CHILD_SA with SPI 87bbdc9b
Nov 26 23:02:37 11[IKE] closing CHILD_SA android{1} with SPIs 7ee56261_i (0 bytes)
87bbdc9b_o (4464 bytes) and TS 10.38.42.133/32 === 0.0.0.0/0
Nov 26 23:02:37 11[IKE] sending DELETE for ESP CHILD_SA with SPI 7ee56261
Nov 26 23:02:37 11[IKE] CHILD_SA closed
Nov 26 23:02:37 11[IKE] outbound CHILD_SA android{3} established with SPIs
ed7c63c2_i 4dd0976b_o and TS 10.38.42.133/32 === 0.0.0.0/0
Nov 26 23:02:37 11[ENC] generating INFORMATIONAL response 2 [ D ]
Nov 26 23:02:37 11[NET] sending packet: from 192.0.0.4[47222] to
138.197.35.162[4500] (76 bytes)
Nov 26 23:03:57 08[IKE] old path is not available anymore, try to find another
Nov 26 23:03:57 08[IKE] looking for a route to 138.197.35.162 ...
Nov 26 23:03:57 08[IKE] requesting address change using MOBIKE
Nov 26 23:03:57 08[ENC] generating INFORMATIONAL request 5 [ ]
Nov 26 23:03:57 08[IKE] checking path 192.168.1.2[47222] - 138.197.35.162[4500]
Nov 26 23:03:57 08[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (76 bytes)
Nov 26 23:03:57 08[IKE] checking path 192.168.1.2[47222] - 10.17.0.5[4500]
Nov 26 23:03:57 08[NET] sending packet: from 192.168.1.2[47222] to 10.17.0.5[4500]
(76 bytes)
Nov 26 23:03:57 09[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (76 bytes)
Nov 26 23:03:57 09[ENC] parsed INFORMATIONAL response 5 [ ]
Nov 26 23:03:57 09[ENC] generating INFORMATIONAL request 6 [ N(UPD_SA_ADDR)
N(NATD_S_IP) N(NATD_D_IP) N(COOKIE2) N(NO_ADD_ADDR) ]
Nov 26 23:03:57 09[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (172 bytes)
Nov 26 23:03:57 14[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (156 bytes)
Nov 26 23:03:57 14[ENC] parsed INFORMATIONAL response 6 [ N(NATD_S_IP)
N(NATD_D_IP) N(COOKIE2) ]
Nov 26 23:03:57 14[IKE] detected changes in NAT mappings, initiating MOBIKE update
Nov 26 23:03:57 14[ENC] generating INFORMATIONAL request 7 [ N(UPD_SA_ADDR)
N(NATD_S_IP) N(NATD_D_IP) N(COOKIE2) N(NO_ADD_ADDR) ]
Nov 26 23:03:57 14[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (172 bytes)
Nov 26 23:03:57 13[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (576 bytes)
Nov 26 23:03:57 13[ENC] parsed CREATE_CHILD_SA request 3 [ EF(2/2) ]
Nov 26 23:03:57 13[ENC] received fragment #2 of 2, waiting for complete IKE message
Nov 26 23:03:57 11[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (1248 bytes)
Nov 26 23:03:57 11[ENC] parsed CREATE_CHILD_SA request 3 [ EF(1/2) ]
Nov 26 23:03:57 11[ENC] received fragment #1 of 2, reassembling fragmented IKE
message
Nov 26 23:03:57 11[ENC] parsed CREATE_CHILD_SA request 3 [ N(REKEY_SA) SA
No KE TSi TSr ]
Nov 26 23:03:57 11[IKE] DH group MODP_2048 inacceptable, requesting ECP_256
Nov 26 23:03:57 11[ENC] generating CREATE_CHILD_SA response 3 [ N(INVAL_KE) ]
Nov 26 23:03:57 11[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (76 bytes)
Nov 26 23:03:57 07[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (156 bytes)
Nov 26 23:03:57 07[ENC] parsed INFORMATIONAL response 7 [ N(NATD_S_IP)
N(NATD_D_IP) N(COOKIE2) ]
Nov 26 23:03:57 15[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (1248 bytes)
Nov 26 23:03:57 15[ENC] parsed CREATE_CHILD_SA request 4 [ EF(1/2) ]
Nov 26 23:03:57 15[ENC] received fragment #1 of 2, waiting for complete IKE message
Nov 26 23:03:57 15[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (384 bytes)
Nov 26 23:03:57 15[ENC] parsed CREATE_CHILD_SA request 4 [ EF(2/2) ]
Nov 26 23:03:57 15[ENC] received fragment #2 of 2, reassembling fragmented IKE
message
Nov 26 23:03:57 15[ENC] parsed CREATE_CHILD_SA request 4 [ N(REKEY_SA) SA
No KE TSi TSr ]
Nov 26 23:03:57 15[IKE] inbound CHILD_SA android{5} established with SPIs
8a0e2e47_i f4881ec8_o and TS 10.38.42.133/32 === 0.0.0.0/0
Nov 26 23:03:57 15[ENC] generating CREATE_CHILD_SA response 4 [
N(ESP_TFC_PAD_N) SA No KE TSi TSr ]
Nov 26 23:03:57 15[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (284 bytes)
Nov 26 23:03:58 12[NET] received packet: from 138.197.35.162[4500] to
192.168.1.2[47222] (76 bytes)
Nov 26 23:03:58 12[ENC] parsed INFORMATIONAL request 5 [ D ]
Nov 26 23:03:58 12[IKE] received DELETE for ESP CHILD_SA with SPI 4dd0976b
Nov 26 23:03:58 12[IKE] closing CHILD_SA android{3} with SPIs ed7c63c2_i (0 bytes)
4dd0976b_o (5764 bytes) and TS 10.38.42.133/32 === 0.0.0.0/0
Nov 26 23:03:58 12[IKE] sending DELETE for ESP CHILD_SA with SPI ed7c63c2
Nov 26 23:03:58 12[IKE] CHILD_SA closed
Nov 26 23:03:58 12[IKE] outbound CHILD_SA android{5} established with SPIs
8a0e2e47_i f4881ec8_o and TS 10.38.42.133/32 === 0.0.0.0/0
```

```
Nov 26 23:03:58 12[ENC] generating INFORMATIONAL response 5 [ D ]
Nov 26 23:03:58 12[NET] sending packet: from 192.168.1.2[47222] to
138.197.35.162[4500] (76 bytes)
```