Setting up VPN between CounterSnipe TMC and APDs

Install and Configure OpenVPN Server Environment on the TMC

```
1 apt-get install openvpn easy-rsa
```

```
2 cd /etc/openvpn
```

3 Create a new file /etc/openvpn/server.conf (vi /etc/openvpn/server.conf)
and cut and paste following lines with your company specifics highlighted in yellow.

```
proto udp
dev tun
ca ca.crt
cert yourservername.crt
key yourservername.key
dh dh1024.pem
server 10.9.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
client-to-client
client-config-dir /etc/openvpn/clients
keepalive 55 130
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Creating a Certificate Authority and Server-Side Certificate & Key

```
1 cp -r /usr/share/easy-rsa/ /etc/openvpn
```

```
2 mkdir /etc/openvpn/easy-rsa/keys
```

```
3 vi /etc/openvpn/easy-rsa/vars (choose any editor)
```

The variables below marked in yellow should be changed according to your preference.

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="MA"

export KEY_CITY="Boston"

export KEY_ORG="Your Company Name"

export KEY_EMAIL="someone@example.com"

export KEY_OU="Department/unit"

export KEY_NAME="yourservername"
```

Once done save the file.

```
4 openssl dhparam -out /etc/openvpn/dh2048.pem 2048

5 cd /etc/openvpn/easy-rsa

6 . ./vars (dot space dot/vars)

7 ./clean-all

8 ./build-ca
```

Simply press `ENTER` to pass through each prompt. If something must be changed, you can do that from within the prompt.

```
9 ./build-key-server yourservername
```

Similar output is generated as when we ran `./build-ca`, and you can again press `ENTER` to confirm each line of the Distinguished Name. However, this time there are two additional prompts:

```
Please enter the following 'extra' attributes
to be sent with your certificate request

A challenge password []:
An optional company name []:
```

Both should be left blank, so just press `ENTER` to pass through each one.

The following two require a yes so select (y)

```
Sign the certificate? [y/n]
1 out of 1 certificate requests certified, commit? [y/n]

cp /etc/openvpn/easy-rsa/keys/{yourservername.crt,
yourservername.key,ca.crt} /etc/openvpn
```

The OpenVPN server for CounterSnipe TMC is ready to go.
Please start it and check the status.

```
service openvpn start
service openvpn status (this command will return VPN server is
running)
```

Generate Certificates and Keys for CounterSnipe APDs

```
Working on the TMC/OpenVPN server in /etc/openvpn/easy-rsa.

./build-key yourapdname
```

Hit return through all of the options apart from the following two that require a yes (y)

```
Sign the certificate? [y/n]
1 out of 1 certificate requests certified, commit? [y/n]
```

Create a file named yourapdname   in /etc/openvpn/clients and add 1 line only.

ifconfig-push 10.9.0.53 10.9.0.52 (you may wish to use different IPs here, eg to match the physical IP on a particular APD, but these will work just fine as your first APD)

Transferring Certificates and Keys to Client Devices and work on client devices:

install openvpn on the APD (apt-get install openvpn)

remove all the files in /etc/openvpn (on the APD not the Server/TMC)

copy from TMC/Server yourapdname.key, yourapdname.crt, and ca.crt, to the APD's /etc/openvpn directory.

Create a file /etc/openvpn/client.conf with the following lines:

```
client
dev tun
proto udp
remote yourserver'sphysicalIPaddress 1194
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
ca ca.crt
cert yourapdname.crt
key yourapdname.key
ns-cert-type server
comp-lzo
verb 3

Restart openvpn by service openvpn restart

You are done. You can go on to create extra clients for the
remaining APDs.
```