Before we start

This guide provides information how to generate required keys and root Certificate Authority for encrypted (TLS) export of flows generated by Flowmon Probe or encrypted flow forwarding from one Flowmon Collector to another over TCP connection. Encrypted flow export functionality is available since Flowmon OS version 8.03.00 and encrypted flow forwarding is available since Flowmon OS version 8.02.00.

To generate keys and certificates it is possible to use openssl library which is already installed on Flowmon Appliances or any other Linux or Windows version.

Key generation

For TCP/TLS, the set of keys and certificates have to be generated for flow exporting device (exporter) and for collector. All certificates must be signed by the same certification authority (CA). Its certificate (CA certificate) must be provided together with key and certificate to each configuration using TCP/TLS protocol. The CA certificate is used to ensure that the exporter and collector are legitimate.

CA root certificate

If you don't have any CA in your corporation yet it is possible can generate a private key and certificate using the following steps.

1. Generate CA private key using command

```
openssl genrsa -out rootCA.key 2048
```

2. Generate self-signed certificate for CA

```
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
```

This will start a process of generating a certificate, where you will need to fill some details you would like to have on certificate. For example, you can see what could be entered.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CZ
State or Province Name (full name) [Some-State]:n/a
Locality Name (eg, city) []:Brno
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Flowmon Networks, a.s.
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:flowmon.com.
Email Address []:support@flowmon.com
```

Create a certificate for exporter/collector

Now for each exporter and collector you will need to create a certificate which will be signed by the CA certificate we created or one used in company.

1. At first, we generate a private key

```
openssl genrsa -out exporter.key 2048
```

2. Then create a certificate signing request

```
openssl req -new -key exporter.key -out exporter.csr
```

Here you will be asked again various questions like when generating a certificate for authority. The important question to answer is **Common name**, where you should fill the IP or domain name of the appliance.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CZ
State or Province Name (full name) [Some-State]:n/a
Locality Name (eg, city) []:Brno
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Flowmon Networks, a.s.
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:127.0.0.1
Email Address []:support@flowmon.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

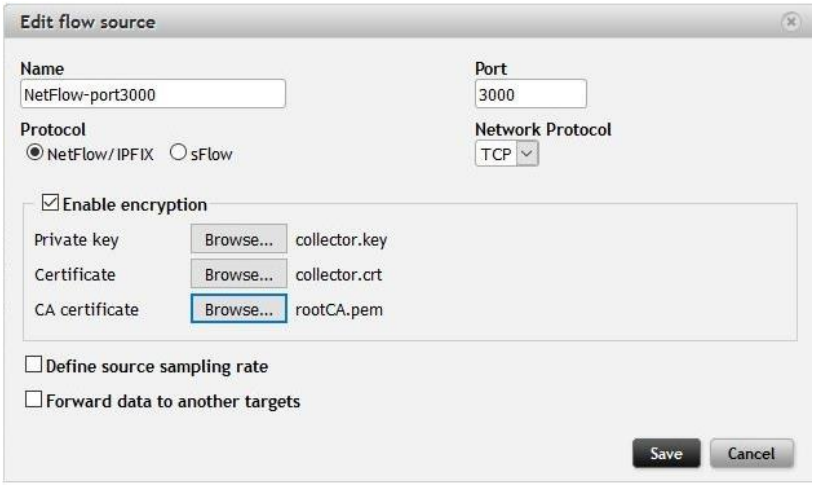
3. And we need to sign it using the CA certificate and key

```
openssl x509 -req -in exporter.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
exporter.crt -days 1024 -sha256
Signature ok
subject=/C=CZ/ST=n/a/L=Brno/O=Flowmon Networks,
a.s./OU=IT/CN=127.0.0.1/emailAddress=support@flowmon.com
Getting CA Private Key
```

Using certificates for configuration

Please repeat previous step for all the Probes and Collectors in your infrastructure where you want to use encrypted flow export or forwarding. Once you have generated a certificates for all the devices as well as root certification authority you can upload them into devices and configure encrypted flow forwarding.

First part is to configure a collector to accept TCP connection over TLS. This is done in Configuration center → FMC Config.



Then configure also exporter to use its certificate. This is done in Configuration center → Exporters.