SSL VPN - Certificate Based Authentication

Below are the steps to configure CA, Server and Client certificate for SSL VPN certificate based authentication.

On linux:

Create Certificate Authority(CA)

Create a working directory and openssl.cnf file specifically for this purpose.

```
# mkdir -p /opt/edoceo/etc/ssl
# cd /opt/edoceo/etc/ssl
# cp /etc/ssl/openssl.cnf ./
```

Edit openssl.cnf accordingly, adjusting paths and defaults in req_distinguished_name section.

Create a key, request and then self-sign.

```
# openssl genrsa -out labca.key 1024
# openssl req -config ./openssl.cnf -new -key labca.key -out labca.csr
# openssl x509 -req -days 3660 -in labca.csr -out labca.crt -signkey labca.key
```

Create Server Certificates

Request and sign the web-server certificate, remember the passwords when prompted!

```
# openssl genrsa -des3 -out sslserver.key 1024
# openssl req -config openssl.cnf -new -key sslserver.key -out sslserver.csr
# openssl ca -config openssl.cnf -in sslserver.csr -cert labca.crt -keyfile labca.key -out sslserver.crt
```

Create Client Certificates

Create Client Certificates in PEM (openssl), PKCS#12 (firefox) and DER (internet explorer) formats. Enter a reasonable username (eg: "first.last") and organizational unit as these will be used for the authentication.

```
# openssl genrsa -des3 -out ssluser1.key 1024
# openssl req -config openssl.cnf -new -key ssluser1.key -out ssluser1.csr
# openssl ca -config openssl.cnf -in ssluser1.csr -cert labca.crt -keyfile labca.key -out ssluser1.crt

# openssl pkcs12 -export -clcerts -in ssluser1.crt -inkey ssluser1.key -out ssluser1.p12
# openssl x509 -inform PEM -in ssluser1.crt -outform DER -out ssluser1.der
# openssl x509 -inform PEM -in labca.crt -outform DER -out labca.der
```

Import the pkcs12 to Firefox and both DER files to Internet Explorer.
How to add the Certificates on Fortigate:

To enable certificate authentication for an SSL VPN user group
1. Install a signed server certificate on the FortiGate unit and install the corresponding root certificate (and CRL) from the issuing CA on the remote peer or client.
2. Obtain a signed group certificate from a CA and load the signed group certificate into the web browser used by each user. Follow the browser documentation to load the certificates.
3. Install the root certificate and the CRL from the issuing CA on the FortiGate
4. Create a PKI user for each SSL VPN user. For each user, specify the text string that appears in the Subject field of the user’s certificate and then select the corresponding CA certificate.
5. Add the PKI users to the SSL VPN usergroup
6. Select the Server Certificate and enable Require Client Certificate on SSL VPN settings and apply the usergroup.

1. Add the SSL server Certificate on Fortigate (Under System >> Certificates >> Local Certificates).

2. To add CA certificate on Fortigate (Under System >> Certificates >> CA certificate).

4. Create PKI user using CLI

```bash
config user peer
  edit "ssluser1"
    set ca "CA_Cert_2"
    set subject "ssluser1"
  next
edit "ssluser2"
  set ca "CA_Cert_2"
  set subject "ssluser2"
  next
end
```

The subject should match the client certificate.
5. Add the PKI to SSL VPN usergroup.

6. Add Client and CA Certificate on Browser.
   To add the client certificate on Mozilla browser, goto Tools >> Options >> Advanced >> Certificates >> Add the certificates
7. Login to SSL VPN
When user enter the url/ip address of sslvpn, the user/client Certificate will be prompted.

Once you select the Certificate, Fortigate verifies the certificate and if it matches, the user will be login to SSL VPN.