Creating a Client Certificate

https://campus.barracuda.com/doc/12193120/

Before creating a client certificate you should create a CA certificate which can be used as the root CA certificate to sign the client certificates. To create a CA certificate for the server designated as SSL CA server, perform the following steps:

1. Generate a Private Key for the CA Certificate
2. Create a CA Certificate using the Private Key
3. Import the CA Certificate to the Barracuda Web Application Firewall
4. Enable Client Authentication on the Barracuda Web Application Firewall
5. Create a Client Certificate
6. Converting PEM File to PKCS #12 Format
7. Import the Client Certificate to the Browser

Step 1 - Generate a Private Key for the CA Certificate

To generate a key for a CA certificate, run the following openssl command on your server:

```
openssl genrsa 2048 > ca-key.pem
```

This generates a private key “ca-key” in PEM format.

Step 2 - Create a CA Certificate using the Private Key

Use the private key generated in **Step 1** to create the CA certificate for the server. The openssl command to generate a CA certificate is as follows:

openssl req -new -x509 -nodes -days 1000 -key ca-key.pem > ca-cert.pem

You will be prompted to provide certain information which will be entered into the certificate. See the example below:

```
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: California
Locality Name (eg, city) []: Campbell
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Barracuda
Networks
Organizational Unit Name (eg, section) []: Engineering
```

```
Common Name (eg, YOUR name) []: barracuda.yourdomain.com
Email Address []: test@myemail.com
```

This creates the CA certificate with the values above. This certificate acts as a root CA certificate for authenticating the client certificates.

Step 3 - Import the CA Certificate to the Barracuda Web Application Firewall

The created certificate needs to be uploaded in the **BASIC > Certificates > Upload Trusted (CA) Certificate** section.

Step 4 - Enable Client Authentication on the Barracuda Web Application Firewall

To be able to use the CA certificate for validating client certificates, client authentication should first be enabled.

Steps to enable client authentication:

1. Go to the **BASIC > Services** page.
2. In the **Services** section, identify the service for which you want to enable client authentication.
3. Click **Edit** next to the service. In the **Service** edit page, scroll down to the **SSL** section.
4. Set **Enable Client Authentication** and **Enforce Client Certificate** to **Yes**.
5. Select the check box(es) next to the **Trusted Certificates** parameter.
6. Specify values for other parameters as required, and click **Save Changes**.

Step 5 - Create a Client Certificate

To create a client certificate, use the following example:

```
openssl req -newkey rsa:2048 -days 1000 -nodes -keyout client-key1.pem > client-req.pem
```

```
Generating a 2048 bit RSA private key writing new private key to 'client-key1.pem'
```

```
.....+++
```

```
..+++

-----

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]: US

State or Province Name (full name) [Some-State]: California

Locality Name (eg, city) []: Campbell

Organization Name (eg, company) [Internet Widgits Pty Ltd]: Barracuda
Networks

Organizational Unit Name (eg, section) []: Tech Support

Common Name (eg, YOUR name) []: barracuda.mydomain.com

Email Address []: test@youremail.com



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

A challenge password []: Secret123

An optional company name []: -
```

This creates the private key “client-key1” in PEM format.

Now, use the following example to create a client certificate that will be signed by the CA certificate created in **Step 2**.

```
openssl x509 -req -in client-req.pem -days 1000 -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 > client-cert1.pem
```

Signature ok

subject=/C=US/ST=California/L=Campbell/O=Barracuda Networks/OU=Tech Support/CN=barracuda.mydomain.com/emailAddress=test@youremail.com

Getting CA Private Key

Step 6 - Converting PEM File to PKCS #12 Format

Use the following command to convert the “client-cert1.pem” certificate along with “client-key1.pem” to a Personal Information Exchange file (pfx token).

```
openssl pkcs12 -export -in client-cert1.pem -inkey client-key1.pem -out client-cert1.pfx
```

```
Enter Export Password:secret
```

```
Verifying - Enter Export Password: secret
```

Step 7 - Import the Client Certificate to the Browser

The client certificate created above should be sent to the client to be imported on their browser.