How to Create Certificates for the SIP Proxy

https://campus.barracuda.com/doc/29819546/

To secure SIP traffic by TLS, you need a certificate for each hop. There is no end-to-end security. If all SIP clients connect to a local Asterisk server that uses the SIP proxy to traverse the firewall, you must create certificates for the following:

- SIP client
- Asterisk server
- SIP Proxy service on the Barracuda CloudGen Firewall

Before You Begin

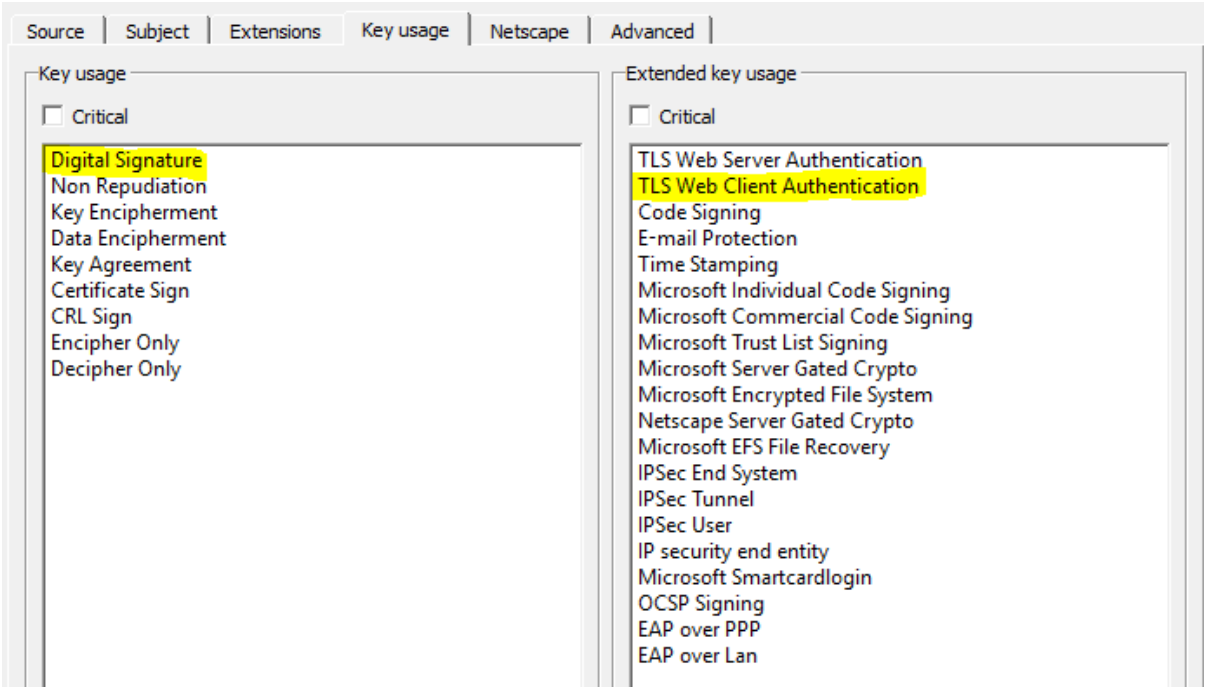
Create and export a root certificate in PEM format. For instructions, see How to Create Certificates with XCA.

Create a Client Certificate

Step 1. Create the Client Certificate

To create the client certificate:

1. In XCA, click the **Certificate signing requests** tab and then click **New Request**. The **Create Certificate Signing Request** window opens.
2. Configure the identifying information.
    1. Click the **Subject** tab.
    2. Configure the settings in the **Distinguished name** section.
    3. In the **New Key** window, enter a name for the certificate, select a key size, then click **Create**.
3. Configure the X.509 extensions.
    1. Click the **Key usage** tab.
    2. From the **Key usage** pane, select **Digital Signature**.
    3. From the **Extended key usage** pane, select **TLS Web Client Authentication**.

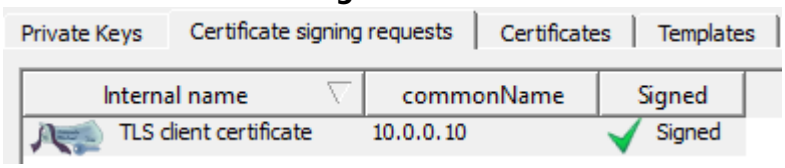


4. Click **OK** to create the certificate. It then appears under the **Certificate signing requests** tab with a **Signed** status of **Unhandled**.

Step 2. Sign the Client Certificate

To sign the client certificate:

1. Click the **Certificate signing requests** tab.
2. Right-click the client certificate and then click **Sign**. The **Create Certificate Signing Request** window opens.
3. In the **Signing** section under the **Source** tab, select **Use this Certificate for signing** and then select the root certificate from the drop-down menu.
4. Click **OK** to sign the certificate. It then appears under the **Certificate signing requests** tab with with the status of **Signed**.



Step 3. Export the Client Certificate

To export the client certificate:

1. Click the **Certificates** tab.
2. Select the client certificate and then click **Export**.
3. In the **Certifikate Export** window, select **PEM Cert + key** from the **Export Format** list and then click **OK**.

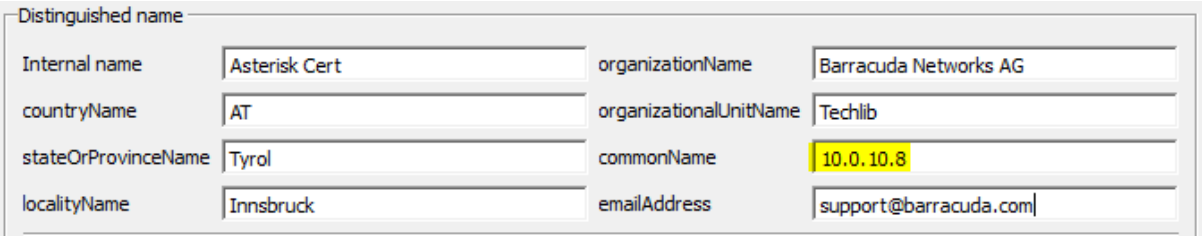
Create an Asterisk Server Certificate

If an Asterisk server is used to connect to the SIP proxy, create a certificate for the Asterisk server.

Step 1. Create a Certificate

To create a certificate for the Asterisk server:

1. Click the **Certificate signing requests** tab and then click **New Request**.
2. Configure the identifying information.
    1. Click the **Subject** tab.
    2. Configure the settings in the **Distinguished name** section.
    3. In the **commonName** field, enter the IP address of the SIP proxy (e.g., `10.0.10.8`).



    4. In the **New Key** window, enter a name for the certificate, select a key size, and then click **Create**.
3. Configure the X.509 extensions.
    1. Click the **Key usage** tab.
    2. From the **Key usage** pane, select **Digital Signature** and **Key Encipherment**.
    3. From the **Extended key usage** pane, select **TLS Web Client Authentication** and **TLS Web Server Authentication**.
4. Click **OK** to create the certificate. It then appears under the **Certificate signing requests** tab with a **Signed** status of **Unhandled**.

Step 2. Sign the Certificate

To sign the certificate:

1. Click the **Certificate signing requests** tab.
2. Right-click the client certificate and then click **Sign**. The **Create x509 Certificate** window opens.
3. In the **Signing** section under the **Source** tab, select **Use this Certificate for signing** and then select the root certificate from the drop-down menu.
4. Click **OK** to sign the certificate. It then appears under the **Certificate signing requests** tab with with the status of **Signed**.

Step 3. Export the Certificate

To export the certificate:

1. Click the **Certificates** tab.
2. Select the client certificate and then click **Export**.
3. In the **Certifikate Export** window, select **PEM Cert + key** from the **Export Format** list and then click **OK**.

Create a SIP Proxy Certificate

Step 1. Create the Certificate

To create the certificate:

1. Click the **Certificate signing requests** tab and then click **New Request**.
2. Configure the identifying information.
    1. Click the **Subject** tab.
    2. Configure the settings in the **Distinguished name** section.
    3. In the **New Key** window, enter a name for the certificate, select a key size, and then click **Create**.
3. Configure the X.509 extensions.
    1. Click the **Key usage** tab.
    2. From the **Key usage** pane, select **Digital Signature** and **Key Encipherment**.
    3. From the **Extended key usage** pane, select **TLS Web Client Authentication** and **TLS Web Server Authentication**.
4. Click **OK** to create the certificate.

Step 2. Sign the Certificate

To sign the certificate:

1. Click the **Certificate signing requests** tab.
2. Right-click the client certificate and then click **Sign**. The **Create x509 Certificate** window opens.
3. In the **Signing** section under the **Source** tab, select **Use this Certificate for signing** and then select the root certificate from the drop-down menu.
4. Click **OK** to sign the certificate. It then appears under the **Certificate signing requests** tab with with the status of **Signed**.

Step 3. Export the Certificate

To export the certificate:

1. Click the **Certificates** tab.
2. Select the client certificate and then click **Export**.
3. In the **Certifikate Export** window, select **PEM Cert + key** from the **Export Format** list and then click **OK**.

Figures

1. Client_key_usage.PNG
2. client_certificate_signed.PNG
3. asterisk_cert_common_name.PNG