****

**Creating Key File & Implementing SSL in Cloud Armor**

**Document Information**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.No** | **Version No.** | **Prepared By** | **Approved By** | **Date & Month** | **Description** |
| **1** | **1.0** | **Shanmuga Priyan** |  | **22.07.2020** | **Initial Version** |
|  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Document Name:**  SOP For Creating a Key File & Implementing SSL in Cloud Armor | |
| **Project:** TVS & Sons | |
| **Subject**: Creating an Instance | |
| **Document No.:** TVS-GCP-0020 | **Version:** 1.0 |
| **Prepared by:** Shanmuga Priyan, 1CloudHub | **Date:** 22.07.2020 |
| **Reviewed by:** | **Date:** |
| **Reviewed by:** | **Date:** |

**Table of Contents**

[**Purpose:** 3](#_Toc34999356)

[**Responsibility:** 3](#_Toc34999357)

[**Steps to Perform the Activity.** 3](#_Toc34999358)

# **Purpose:**

The purpose of this document is to create a private key file from .PFX file and to map the same in Google Cloud Armor to enable the SSL in Network Load balancing for all the sites.

## **Responsibility:**

1CH team is responsible for implementing SSL file in Cloud Armor once the certificates are expired or newly added.

### **Steps to Perform the Activity.**

**Step 1:** If we don’t have exact CSR file, we need to follow the below steps to change the .PFX file into CSR file.

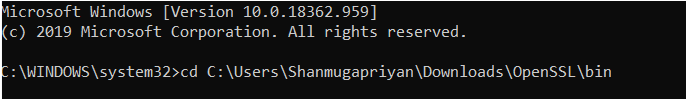
**Step 2:** Download Open SSL software to your desktop or Laptop so that we can change the .PFX file into CSR format.

Download Link -🡪 <https://sourceforge.net/projects/openssl/>

**Step 3:** Then copy the .PFX file to your local PC, where you have installed open SSL.

**Step 4:** Open command prompt in Elevated mode and navigate to the path where you have installed the Open SSL. For Ex:

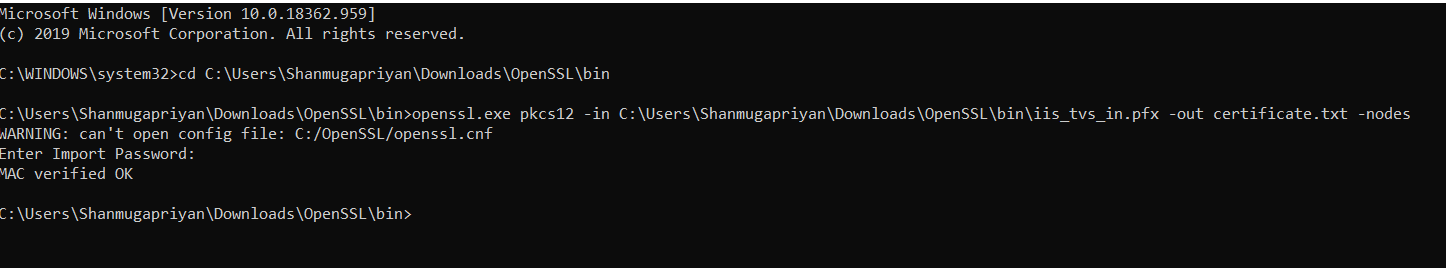
**C:\Users\Downloads\OpenSSL\Bin**



**Step 5:** Once the directory is changed to the required path, Execute the below command.

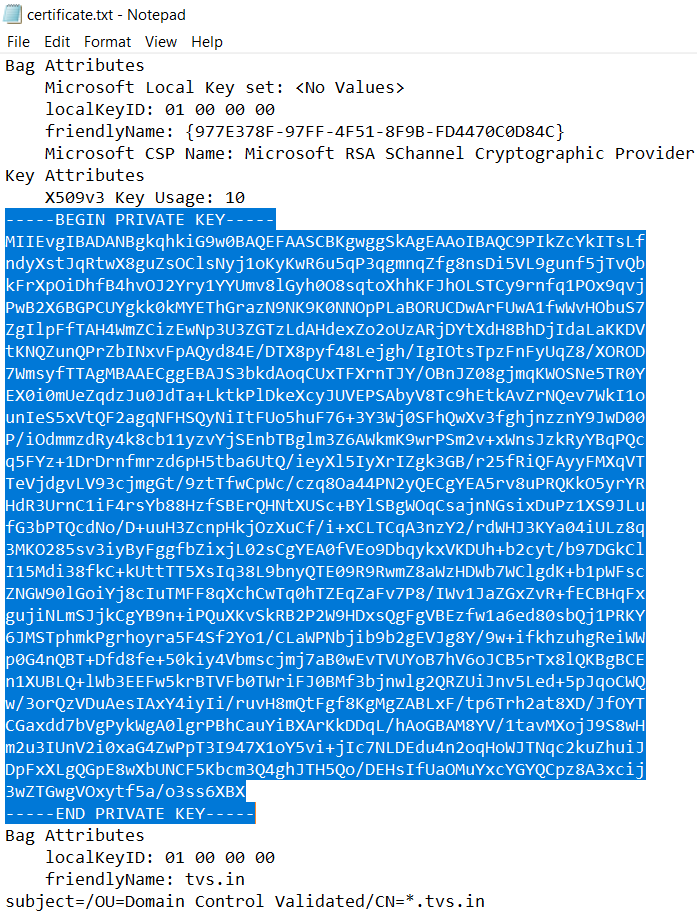
**Openssl.exe pkcs12 -in C:\PathToThePFXfile\myPFXfileName.pfx -out certificate.txt -nodes**

**Openssl.exe pkcs12 -in C:\Users\Downloads\OpenSSL\Bin\iis\_tvs\_in.pfx -out certificate.txt -nodes**

****

**Step 6:** Once entered it will prompt for the password, enter the required password, which will be generated while creating .PFX file.

**Step 7:** Once done, the output .txt file will be saved in default path, navigate to that notepad file and Copy from Begin Private Key to End Private Key as mentioned in the below screenshot.

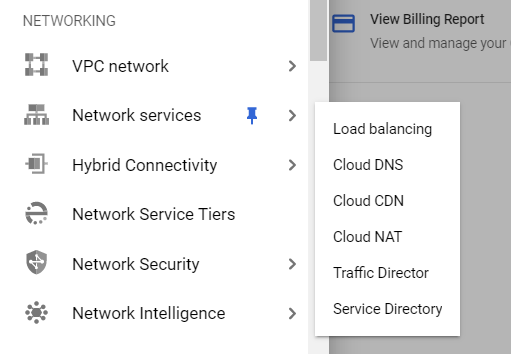


**Step 8:** Save the copied file in new notepad as .crt format.

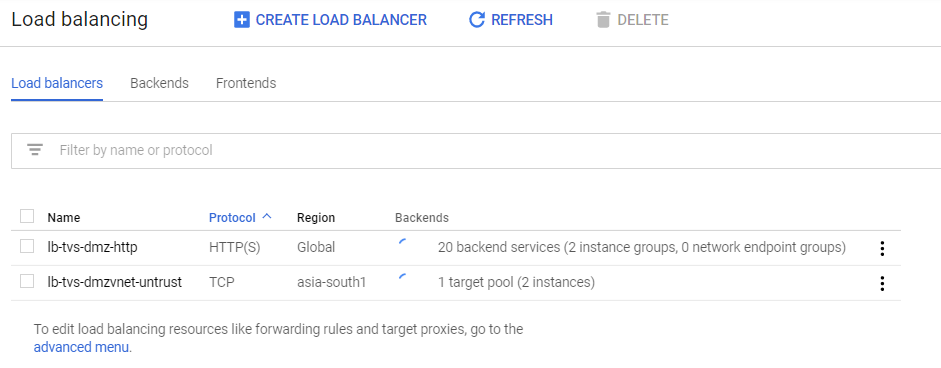
**Step 9:** Once done the above step open the saved .crt file in a notepad and copy the private key and save it in a separate notepad in .key format.

**Step 10:** Once done all the above steps, now need to upload the .key and pem files in Google Cloud Armor to enable the SSL.

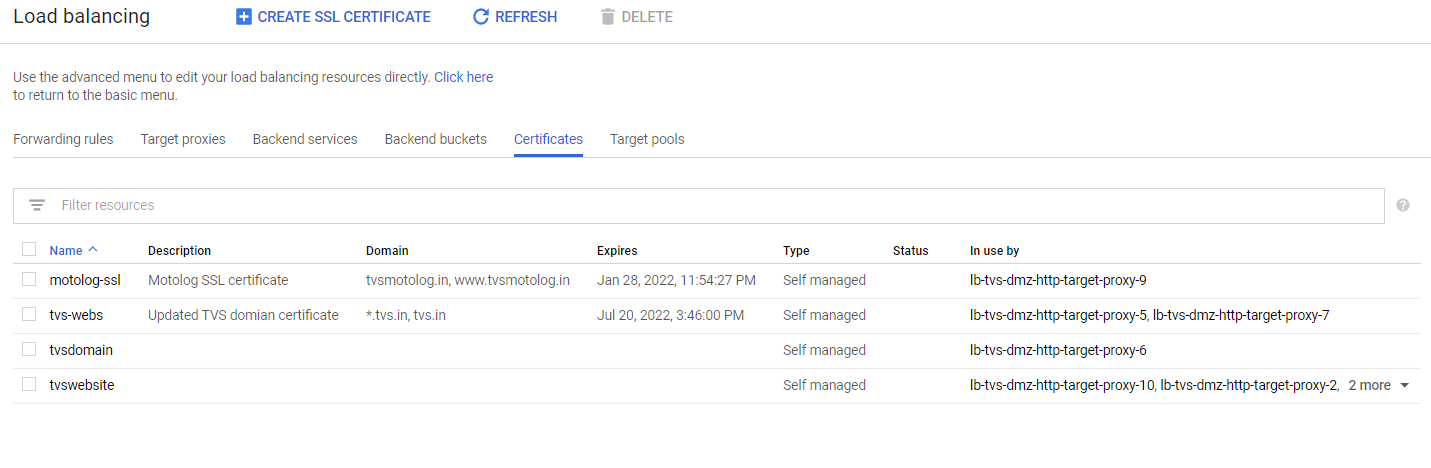
**Step 11:** Open the console, navigate to Network Load balancing in shared-NW project.



**Step 12:** There you can able to view the option called advanced menu in the bottom.

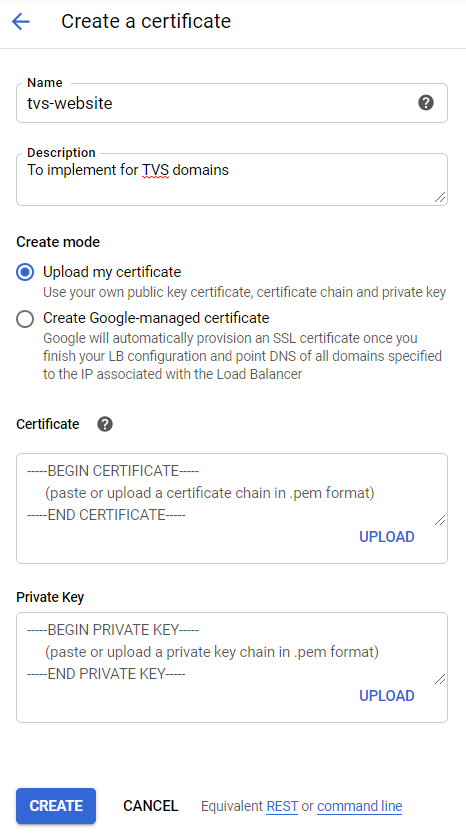


**Step 13:** Click on the Advanced menu and navigate to certificates and click on the Create SSL certificate to create a new SSL certificate for the required Domain



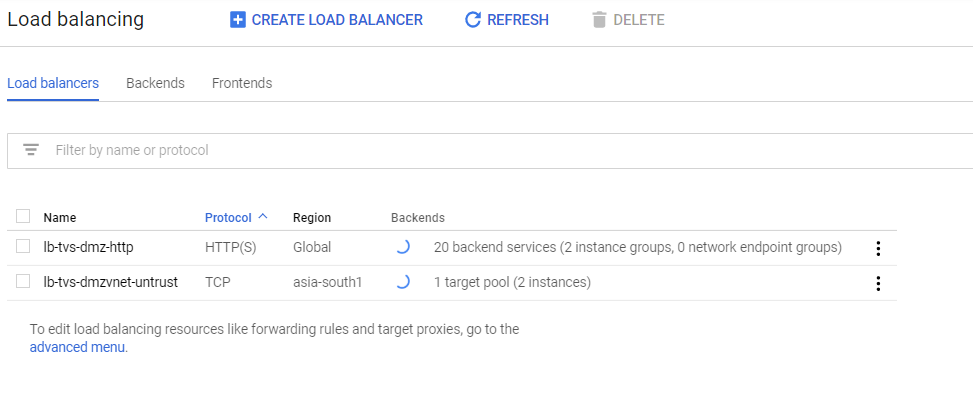
**Step 14:** Once clicked, Give the desired name for the certificate and upload the Certificate pem file which has been created while purchasing the certificate and the private key file, which has been created by following the above steps.

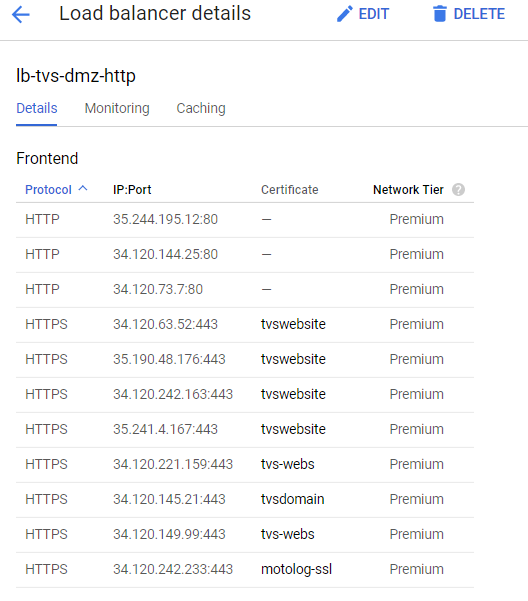
**Note:** You can either copy paste or upload the certificate directly.



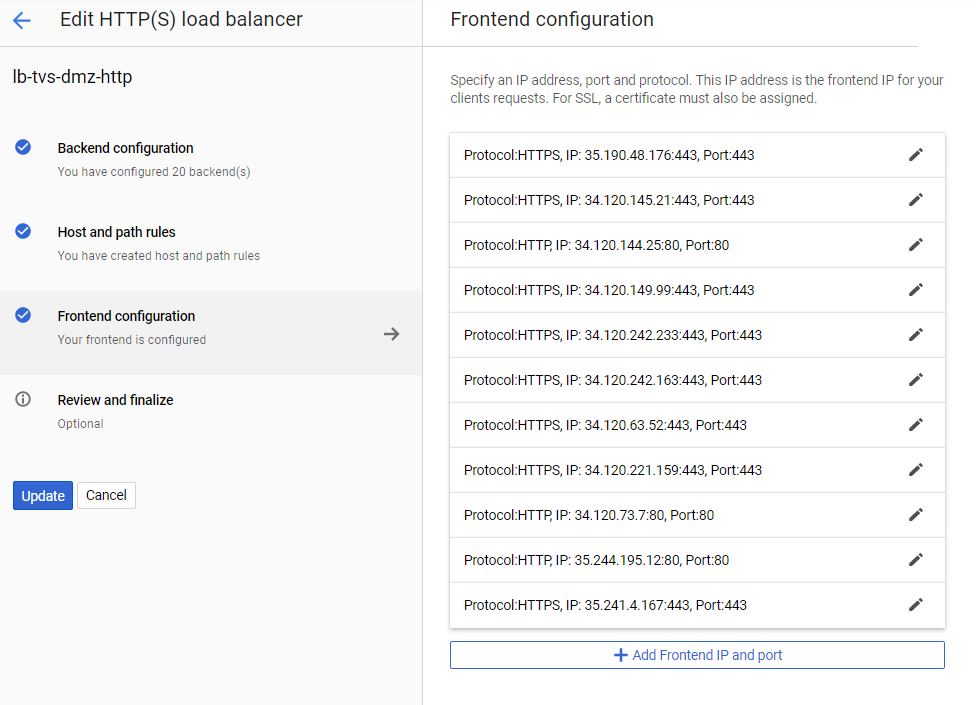
**Step 15:** Once created, we need to map the certificates to the desired sites, which has been created in the load balancer.

For that, again navigate back to the load balancer, and click on the desired load balancer where the sites have been mapped and click on edit which is in the top.





**Step 16:** The load balancing configurations will be changed to editable format, there navigate to front end configurations. And click on edit icon of the public IP which we need to change or map the certificate.



**Step 17:** Then select the desired certificate to that domain, and then click on done and update to save the changes.

Note: It will take 20 – 30 Mins to reflect in the website.

