**Configure Apache With TLS/SSL Certificate on Ubuntu 18**

<https://hostadvice.com/how-to/configure-apache-with-tls-ssl-certificate-on-ubuntu-18/>

STEP 1: Prepare the certs files

1. Copy the 3 cert files into one like below as a .pem file: Copy and paste the contents of the certificates into a new file with the following order:

|  |
| --- |
| -----BEGIN CERTIFICATE-----  <Your SSL Server Cert contents>  -----END CERTIFICATE-----  -----BEGIN CERTIFICATE-----  <HydrantID SSL ICA Cert contents>  -----END CERTIFICATE-----  -----BEGIN CERTIFICATE-----  <QuoVadis Root CA Cert contents>  -----END CERTIFICATE----- |

NOTE: Remove any blank lines.

1. Copy this .pem file and the .key file to somewhere on the server

 Step 2: Configuring the Firewall

1. Make sure that the TCP port 443 is open. Instead of port 80 SSL uses port 443. We will be using Uncomplicated Firewall (UFW)
2. To enable UFW use the following command

$ sudo ufw enable

1. Allow the predefined apache settings for the firewall using the following command

$ sudo ufw allow 'Apache Full'

1. You  can check the list of current rules using the following command.

$ sudo ufw status

1. To allow future connections allow OpenSSH

$ sudo ufw allow 'OpenSSH'

Step 3: Apache virtual host configuration

1. Navigate to the default Apache site config directory using the following command and make changes as below:

$ sudo nano /etc/apache2/sites-available/default-ssl.conf

* Edit this: ServerAdmin webmaster@localhost to this : ServerAdmin email@example.net
* Add this right below the ServerAdmin line: ServerName YOUR\_IP\_OR\_DOMAIN\_NAME
* Now, edit these lines with our certificate location (path where you put the pem and key files)

Text

Description automatically generated

* Add below Proxy info

<Proxy \*>  
 Order deny,allow  
 Allow from all  
 </Proxy>  
 ProxyPreserveHost On  
 <Location "/">

RedirectMatch 400 etc|passwd #for directory traversal vulnerability  
 ProxyPass "<http://server-ip:5000/>"  
 ProxyPassReverse "<http://server-ip:5000/>"  
 </Location>

* Save and close the file

Step 4: Enable the Apache SSL module

1. Enable the SSL module using following command

$ sudo a2enmod ssl

1. Now enable the site we have just edited:

$ sudo a2ensite default-ssl.conf

1. Restart Apache:

$ sudo service apache2 restart

1. The website is now secure, access it using following address in the browser [**https://YOUR\_SERVER\_IP**](https://YOUR_SERVER_IP)