1) Apache changes:

a) Install httpd:

```
sudo yum update httpd

sudo yum install httpd

sudo systemctl start httpd
```

b) Install firewalld:

```
sudo yum install firewalld

sudo systemctl start firewalld

sudo systemctl enable firewalld
```

c) Install mod_ssl:

```
sudo yum install mod_ssl
```

d) Configure SSL:

a. I added to /etc/httpd/conf/httpd.conf , the following:

i. Listen 443

ii.

```
<VirtualHost *:80>
    ServerName http://83.212.98.149
    Redirect permanent / https://83.212.98.149
</VirtualHost>
```

Which is used to for the redirection from http to https.

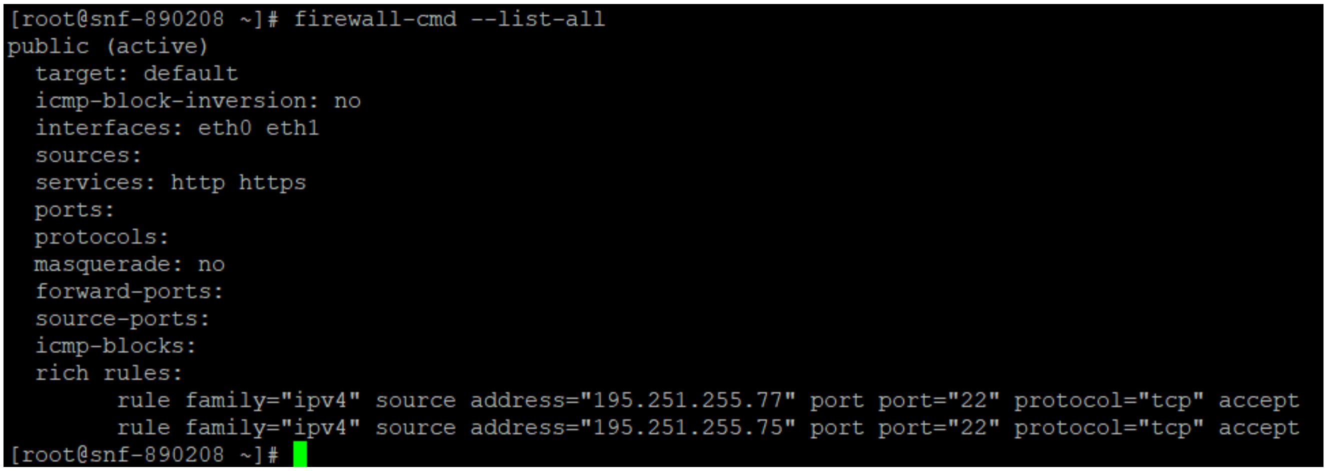
iii.

```
<VirtualHost *:443>
    ServerName 83.212.98.149
    DocumentRoot /var/www/html
    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/server.crt
    SSLCertificateKeyFile /etc/pki/tls/private/server.key
    SSLCertificateChainFile /etc/pki/tls/certs/ca.crt
</VirtualHost>
```

Where the last 3 lines are for the certificate of the server , the private key of the server and the certificate of the Certificate Authority respectively.

1. I copied server.crt and ca.crt to the folder /etc/pki/tls/certs.
2. Copied the server.key to the folder /etc/pki/tls/private

2) Screenshot of firewalld rules.



```
[root@snf-890208 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0 eth1
  sources:
  services: http https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" source address="195.251.255.77" port port="22" protocol="tcp" accept
        rule family="ipv4" source address="195.251.255.75" port port="22" protocol="tcp" accept
[root@snf-890208 ~]#
```

3) Creation of Certificate Authority (CA), CSR και SSL Certificate.

1) Certificate Authority:

   a) Creation of private key for the Certificate Authority (CA) with RSA-2048 bit:

      openssl genrsa -out ca.key 2048

   b) Creation of the certificate of CA , signing with its own key (ca.key) of previous step (valid for 365 days):

      openssl req -x509 -new -nodes -key ca.key -sha256 -days 365 -out ca.crt

2) CSR Certificate:

   a) Create private key for the SSL Certificate:

      openssl genrsa -out server.key 2048

   b) Create the CSR.

      openssl req -new -key server.key -out server.csr

3) SSL Certificate της σελίδας (*using CSR Certificate of the server and the CA certificate)*:

   openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 365 -sha256

server.crt -> SSL Certificate **, server.key** -> SSL certificate's private key

4) For the implementation of the page, I used HTML and a JavaScript script , where I test the name field , if it is the same with my University ID. If it is, we get a success message, else a false one. We must click the submit as pressing the ENTER key does not work.