PRÁCTICA 4

Emilio Aparicio Benítez

Instalación de un certificado SSL autofirmdo para configurar el acceso por HTTPS:
El proceso de instalación lo voy a realizar sobre la máquina 1 porque como todos los compañeros, intentamos hacerlo con el balanceador (Máquina 3) pero no nos funciona.

a2enmod
ssl service apache2 restart
mkdir /etc/apache2/ssl openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

```
swap1@swap1:~$ sudo a2enmod ssl
[sudo] password for swap1:
Module ssl already enabled
```

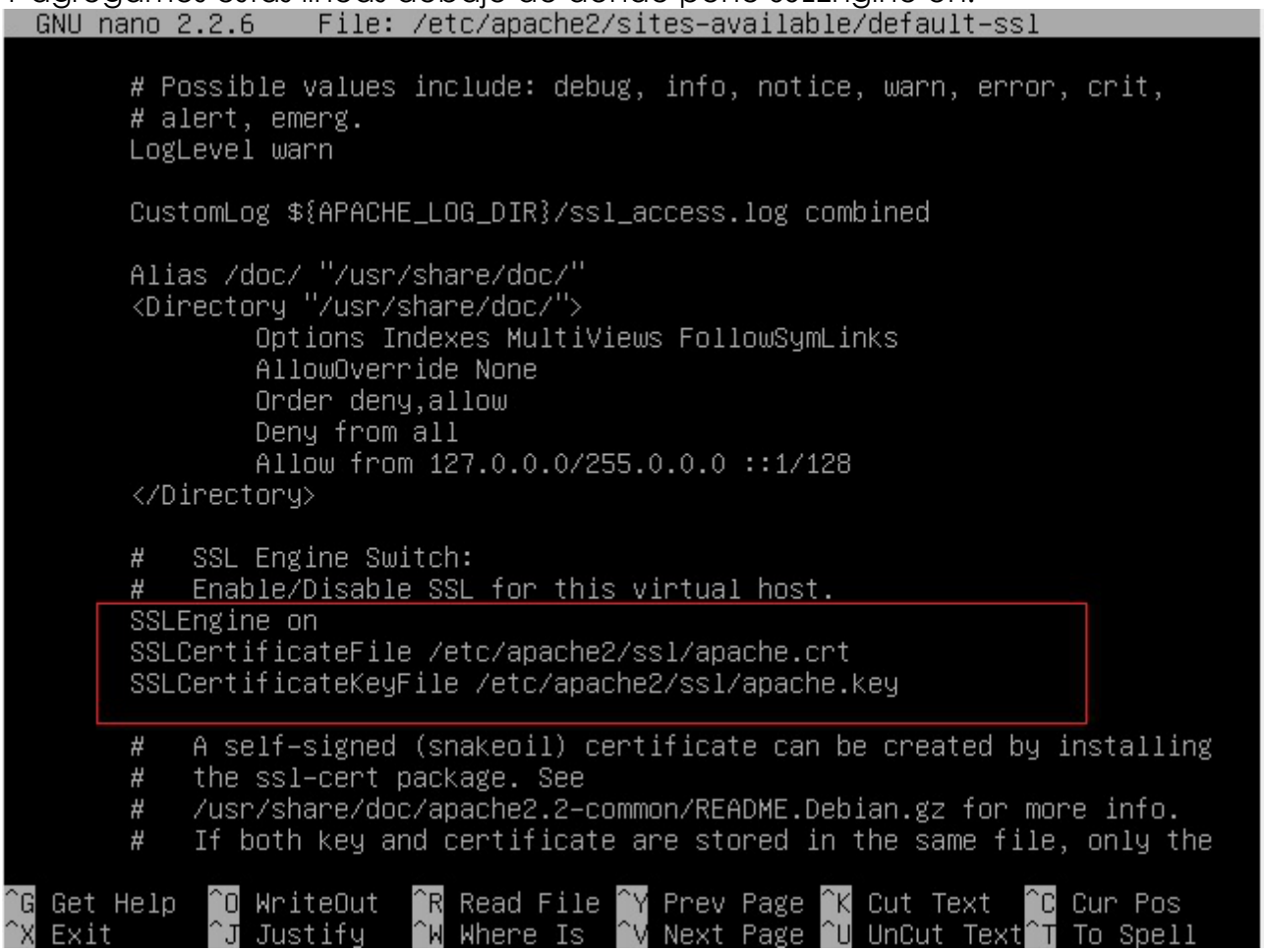
Tras ello metemos los datos de nuesto dominio:

```
swap1@swap1:~$ sudo a2enmod ssl
[sudo] password for swap1:
Module ssl already enabled
swap1@swap1:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
Generating a 2048 bit RSA private key
.....................................................................
.....................................................................
.....+++
.....+++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
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]:ES
State or Province Name (full name) [Some-State]:Granada
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:swap
Organizational Unit Name (eg, section) []:swap
Common Name (e.g. server FQDN or YOUR name) []:swap
Email Address []:swap@info.com
```

Editamos el archivo de configuración del sitio default-ssl:
nano /etc/apache2/sites-available/default-ssl

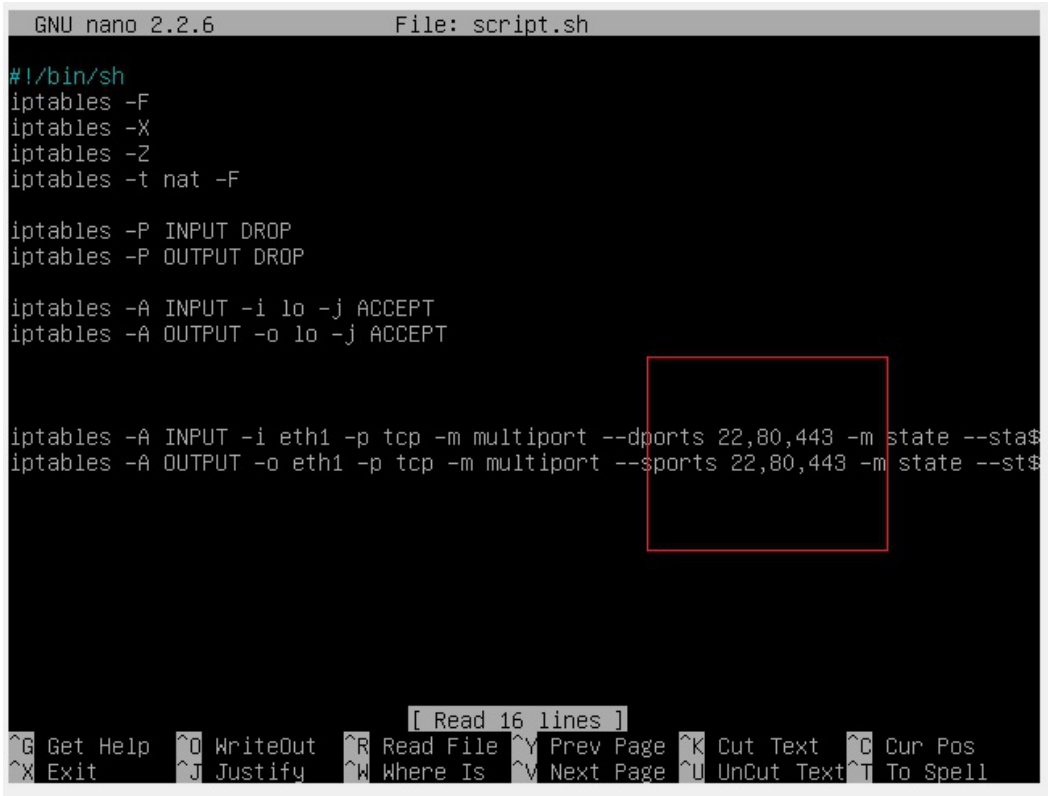
```
swap1@swap1:~$ sudo nano /etc/apache2/sites-available/default-ssl
```

Y agregamos estas lineas debajo de donde pone SSLEngine on:



Ahora procedemos a la configuración del cortafuegos iptables en Linux :

En primer lugar vamos a necesitar un script en el cuál vamos a escribir lo siguiente:



Con ello podemos usar los puertos 22,80 y 443, y ahora vamos a comprobar su funcionamiento haciendo un curl desde la máquina 2 a la máquina 1: