

## PRÁCTICA 4

Emilio Aparicio Benítez

Instalación de un certificado SSL autofirmado 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 nuestro 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 líneas debajo de donde pone SSL Engine on:

```
GNU nano 2.2.6 File: /etc/apache2/sites-available/default-ssl

# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
LogLevel warn

CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined

Alias /doc/ "/usr/share/doc/"
<Directory "/usr/share/doc/">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride None
    Order deny,allow
    Deny from all
    Allow from 127.0.0.0/255.0.0.0 ::1/128
</Directory>

#    SSL Engine Switch:
#    Enable/Disable SSL for this virtual host.
SSLEngine on
SSLCertificateFile /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key

#    A self-signed (snakeoil) certificate can be created by installing
#    the ssl-cert package. See
#    /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
#    If both key and certificate are stored in the same file, only the

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

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:

```
GNU nano 2.2.6 File: script.sh

#!/bin/sh
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

iptables -P INPUT DROP
iptables -P OUTPUT DROP

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

iptables -A INPUT -i eth1 -p tcp -m multiport --dports 22,80,443 -m state --sta$
iptables -A OUTPUT -o eth1 -p tcp -m multiport --sports 22,80,443 -m state --st$

[ Read 16 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

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:

## MÁQUINA 1

```
ou must be root)
Perhaps iptables or your kernel needs to be upgraded.
iptables v1.4.12: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
iptables v1.4.12: can't initialize iptables table `nat': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
iptables v1.4.12: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
iptables v1.4.12: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
iptables v1.4.12: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
iptables v1.4.12: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
multiport: Could not determine whether revision 1 is supported, assuming it is.
iptables v1.4.12: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
swap1@swap1:~$ sudo ./script.sh
swap1@swap1:~$
```



## MÁQUINA 2

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2604 (2.6 KB)  TX bytes:2604 (2.6 KB)

swap1@swap1:~$ curl https://192.168.1.100
^Z
[1]+  Stopped                  curl https://192.168.1.100
swap1@swap1:~$ curl https://192.168.1.100
curl: (60) SSL certificate problem, verify that the CA cert is OK. Details:
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
More details here: http://curl.haxx.se/docs/sslcerts.html

curl performs SSL certificate verification by default, using a "bundle"
of Certificate Authority (CA) public keys (CA certs). If the default
bundle file isn't adequate, you can specify an alternate file
using the --cacert option.
If this HTTPS server uses a certificate signed by a CA represented in
the bundle, the certificate verification probably failed due to a
problem with the certificate (it might be expired, or the name might
not match the domain name in the URL).
If you'd like to turn off curl's verification of the certificate, use
the -k (or --insecure) option.
swap1@swap1:~$
```