



UNIVERSIDAD
DE GRANADA

PRÁCTICA 4: ASEGURAR LA GRANJA WEB

ANA BUENDÍA RUIZ-AZUAGA

Correo electrónico

anabuenrúa@correo.ugr.es

E.T.S. INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

Granada, a 14 de mayo de 2022

ÍNDICE GENERAL

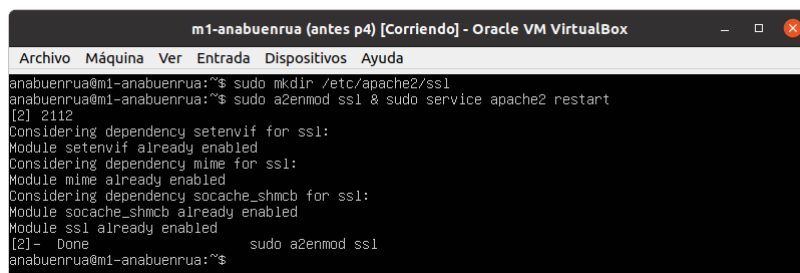
1.	CERTIFICADO AUTOFIRMADO SSL	3
1.1.	Opciones avanzadas	4
2.	APACHE CON CERTIFICADO SSL	5
2.1.	Opciones avanzadas	8
3.	NGINX COMO BALANCEADOR PARA PETICIONES HTTPS	10
3.1.	Opciones avanzadas	10
4.	IPTABLES	12
4.1.	Configuración básica	12
4.2.	Opciones avanzadas	14
5.	CONFIGURAR CORTAFUEGOS AL ARRANQUE	20
6.	CERTBOT	22
6.1.	Configuración de apache en m1	22
6.2.	Configuración de nginx en m3	22
7.	BIBLIOGRAFÍA	26

CERTIFICADO AUTOFIRMADO SSL

Vamos a comenzar trabajando en `m1`, todos los comandos y configuraciones que se van a mostrar a continuación se realizarán en esta máquina.

Primero creamos la carpeta donde vamos a guardar los certificados `/etc/apache2/ssl` y luego vamos a activar el módulo `ssl` y relanzamos `apache`, para lo que ejecutamos los comandos que se muestran en (1).

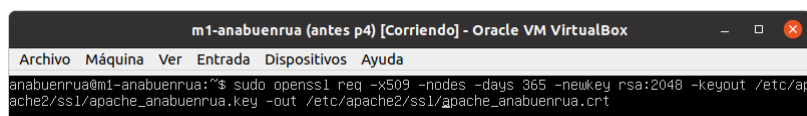
Figura 1: Creación del directorio para almacenar los certificados, instalación del módulo `ssl` y relanzar `apache`.



```
m1-anabuenrúa (antes p4) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
anabuenrúa@m1-anabuenrúa:~$ sudo mkdir /etc/apache2/ssl
anabuenrúa@m1-anabuenrúa:~$ sudo a2enmod ssl & sudo service apache2 restart
[2] 2112
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
[2]- Done          sudo a2enmod ssl
anabuenrúa@m1-anabuenrúa:~$
```

Ahora procedemos a crear los certificados con `ssl`, como se ve en (2).

Figura 2: Creación de los certificados con `ssl`.



```
m1-anabuenrúa (antes p4) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
anabuenrúa@m1-anabuenrúa:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ap
ache2/ssl/apache_anabuenrúa.key -out /etc/apache2/ssl/apache_anabuenrúa.crt
```

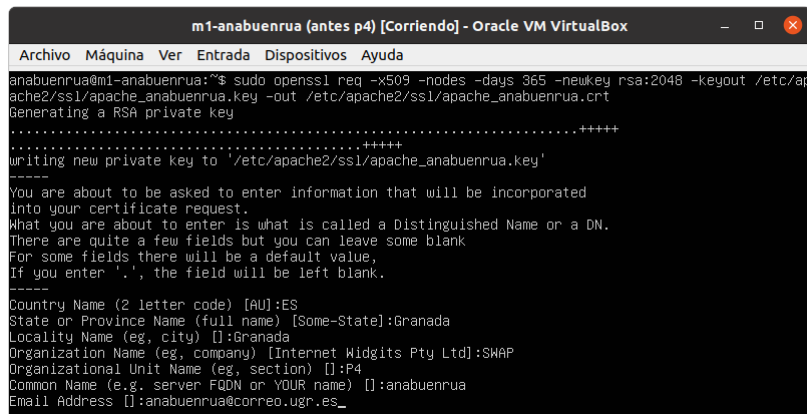
En (2) hemos usado varios argumentos que explicamos a continuación:

- `-x509`: Autofirma el certificado.
- `-days`: Indica que el certificado va a tener 365 días de validez.
- `-keyout`: Especifica el fichero donde se va a guardar la clave.
- `-out`: Especifica el fichero donde se va a guardar el certificado.

Además, le hemos indicado que la clave es de 2048 bits.

A continuación introducimos los datos que nos piden por línea de comandos, se ve en (3).

Figura 3: Introducimos los datos requeridos para la creación del certificado.



```
m1-anabuenrue (antes p4) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
anabuenrue@m1-anabuenrue:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ap
ache2/ssl/apache_anabuenrue.key -out /etc/apache2/ssl/apache_anabuenrue.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/apache2/ssl/apache_anabuenrue.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) []:P4
Common Name (e.g. server FQDN or YOUR name) []:anabuenrue
Email Address []:anabuenrue@correo.ugr.es_
```

1.1 OPCIONES AVANZADAS

Como opciones avanzadas, se van a comentar distintos argumentos para generar los certificados con `openssl req`.

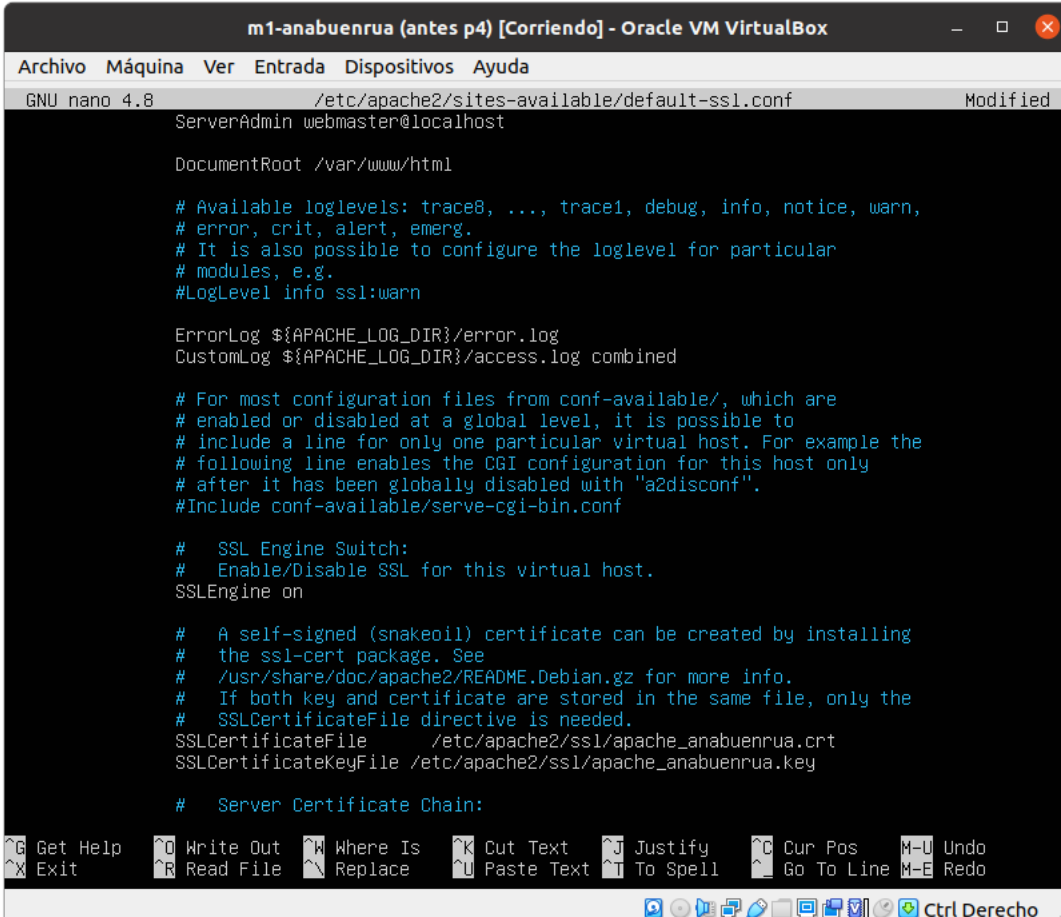
- `-inform DER/PEM` especifica el formato de entrada de los datos.
- `-outform DER/PEM` especifica el formato de salida de los datos.
- `-subj /type0=value0/type1=value1/type2=...` permite especificar los datos desde la orden. Las abreviaturas que sustituyen a `type0`, `type1` están predefinidas y pueden consultarse en el manual.
- `-text` imprime el certificado en forma de texto.

APACHE CON CERTIFICADO SSL

Para configurar apache para que use el certificado SSL que acabamos de generar, vamos a empezar configurando la ruta de los certificados en apache.

Editamos el archivo `/etc/apache2/sites-available/default-ssl` con la información de nuestros certificados, como se muestra en (4).

Figura 4: Archivo `/etc/apache2/sites-available/default-ssl`.



```
m1-anabuenrúa (antes p4) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8      /etc/apache2/sites-available/default-ssl.conf  Modified
ServerAdmin webmaster@localhost

DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

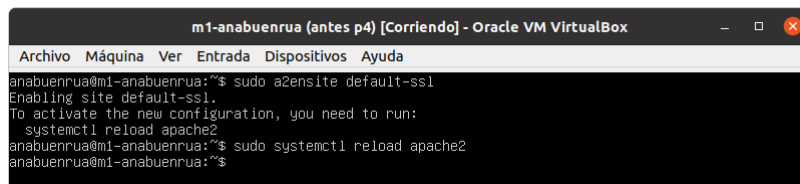
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

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

# Server Certificate Chain:
```

Ahora activamos el sitio `default-ssl`, para lo que se ejecuta (5).

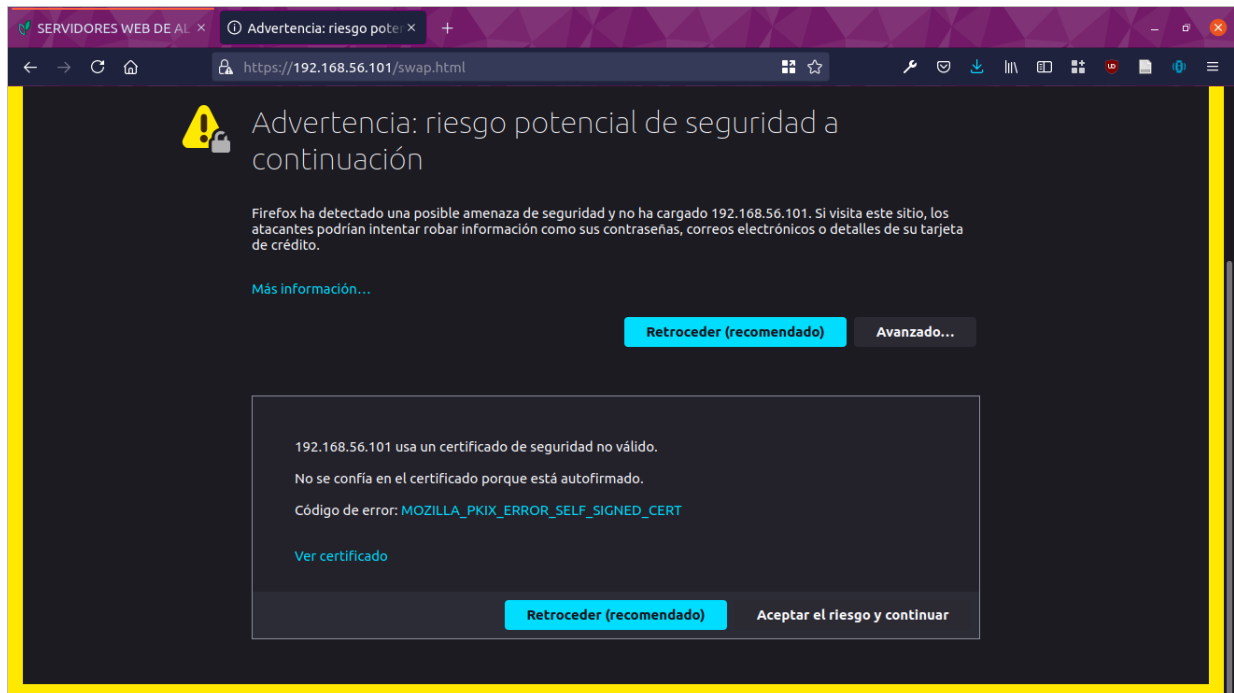
Figura 5: Activación del sitio default-ssl



Para comprobar que hemos realizado todo correctamente, ahora accedemos a m1 desde el navegador, como en las otras prácticas vamos a acceder a la página `swap.html` usando https.

Nos informa de que la conexión no es segura porque el certificado es autofirmado, pero le damos a continuar de todas formas, como se ve en (6).

Figura 6: Aviso de conexión no segura al acceder a m1 desde el navegador.



Tras el aviso, accedemos a la página, donde vemos en la parte de la url el candado a la izquierda, aunque tiene una exclamación, indicando de nuevo que el certificado es autofirmado. Esto puede verse en (7)

Si pulsamos sobre este candado y le damos a más información, nos muestra más detalles sobre el certificado, como se muestra en (8).

Finalmente, vamos a copiar los certificados de m1 en m2, para lo que vamos a usar `scp`.

Figura 7: Acceso a swap.html de m1.

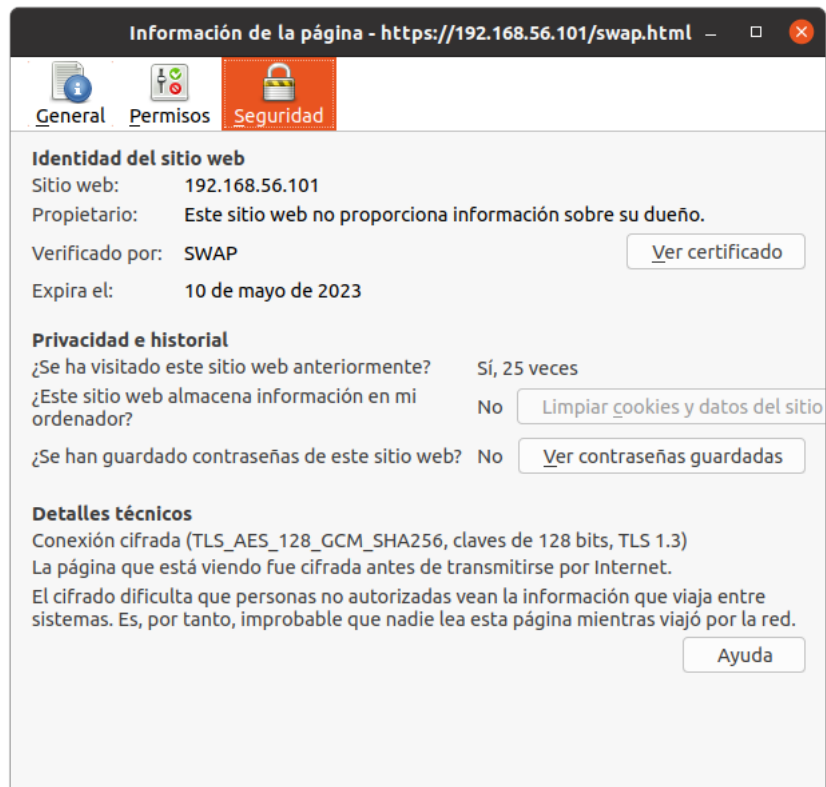
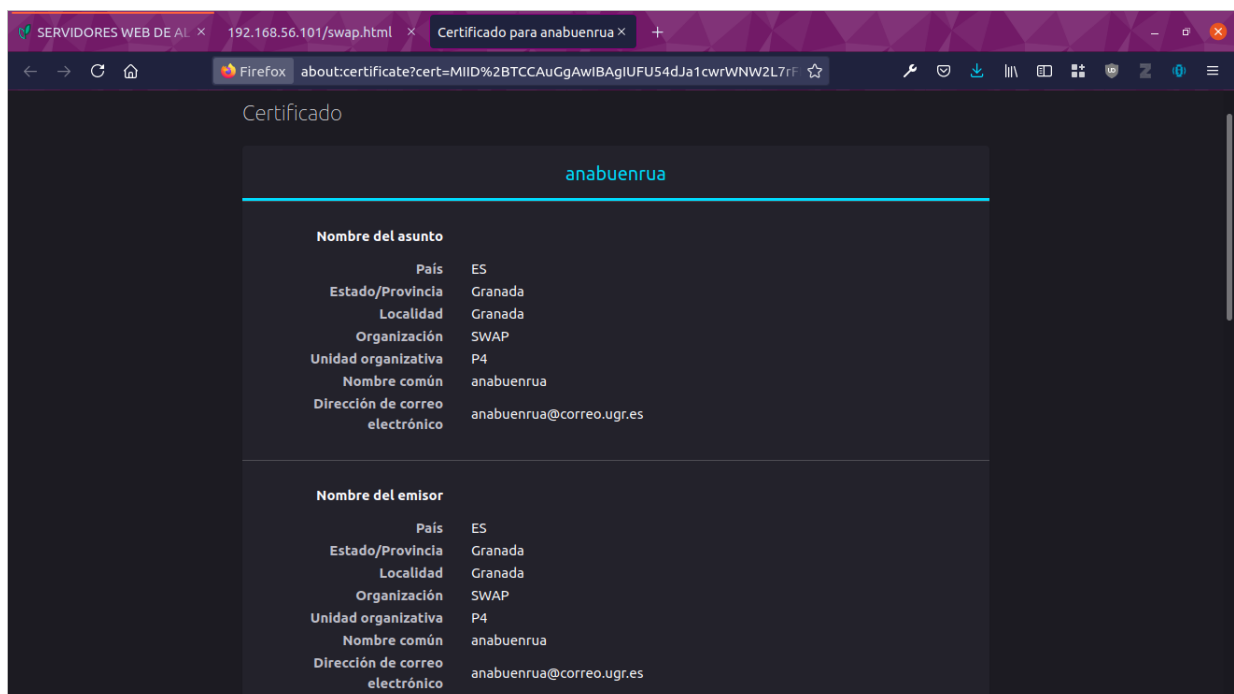
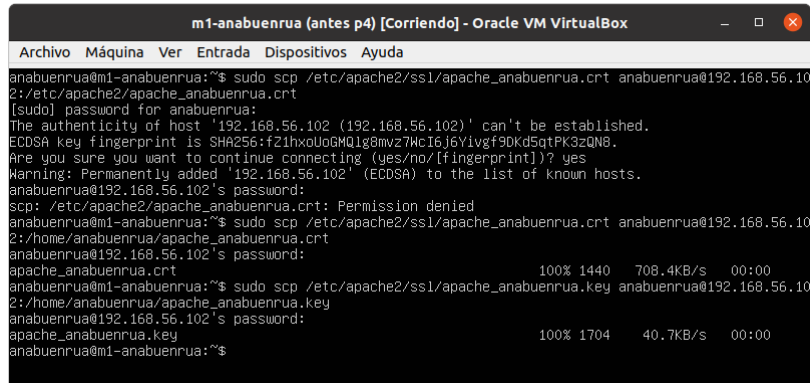


Figura 8: Información del certificado mostrada por firefox.



Para ello, primero creamos el directorio para almacenar los certificados en cada máquina y luego los copiamos mediante scp, ejecutando los comandos de (9) en m1.

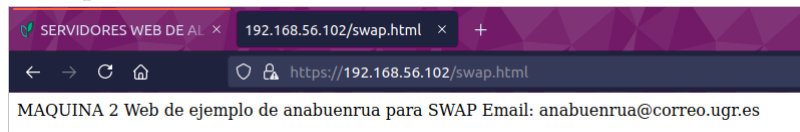
Figura 9: Copia de certificados de m1 en m2 mediante scp.



```
m1-anabuenrúa (antes p4) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
anabuenrúa@m1-anabuenrúa:~$ sudo scp /etc/apache2/ssl/apache_anabuenrúa.crt anabuenrúa@192.168.56.102:/etc/apache2/
[sudo] password for anabuenrúa:
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ECDSA key fingerprint is SHA256:f21hxoUoGMQlg8mvz7McI6j6Ylvf9DKd5qtPK3zQN8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
anabuenrúa@192.168.56.102's password:
scp: /etc/apache2/apache_anabuenrúa.crt: Permission denied
anabuenrúa@m1-anabuenrúa:~$ sudo scp /etc/apache2/ssl/apache_anabuenrúa.crt anabuenrúa@192.168.56.102:/home/anabuenrúa/
anabuenrúa@192.168.56.102's password:
apache_anabuenrúa.crt 100% 1440 708.4KB/s 00:00
anabuenrúa@m1-anabuenrúa:~$ sudo scp /etc/apache2/ssl/apache_anabuenrúa.key anabuenrúa@192.168.56.102:/home/anabuenrúa/
anabuenrúa@192.168.56.102's password:
apache_anabuenrúa.key 100% 1704 40.7KB/s 00:00
anabuenrúa@m1-anabuenrúa:~$
```

Ahora movemos los ficheros al mismo directorio que en m1 y repetimos el proceso para activar el módulo ssl, configuramos el archivo `/etc/apache2/sites-available/default-ssl`, activarlo y reiniciamos apache, de forma análoga a como lo hemos hecho en m1, y comprobamos que funciona en (10)

Figura 10: Comprobación del funcionamiento correcto de m2 con los certificados.



2.1 OPCIONES AVANZADAS

Podemos obtener el certificado mediante openssl, para ello he usado mi ordenador anfitrión como se ve en (11).

Y comprobamos que nos muestra el certificado.

Además, se pueden añadir otras opciones de apache con `SSLOptions +opcion`.

También se puede activar la redirección para que toda conexión http la redirija a ser https:

```
<VirtualHost *:80>
    // Cosas

    Redirect "/" "https://your_domain_or_IP/"

    //Más cosas
</VirtualHost>
```


Figura 11: Obtención del certificado mediante openssl.

```

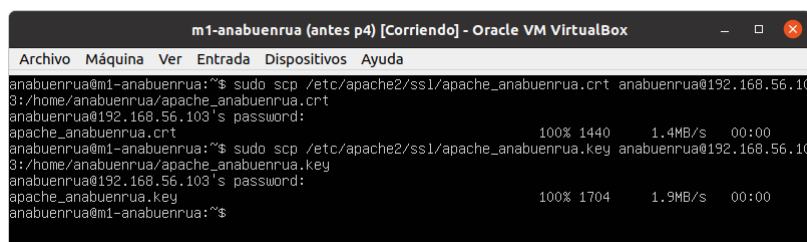
mapachana@mapachana-Aspire-E5-574G: ~
mapachana@mapachana-Aspire-E5-574G:~$ openssl s_client -connect 192.168.56.101:443 -showcerts
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 C = ES, ST = Granada, L = Granada, O = SWAP, OU = P4, CN = anabuenrúa, emailAddress = anabuenrúa@correo.ugr.es
verify error:num=18:self signed certificate
verify return:1
depth=0 C = ES, ST = Granada, L = Granada, O = SWAP, OU = P4, CN = anabuenrúa, emailAddress = anabuenrúa@correo.ugr.es
verify return:1
---
Certificate chain
 0 s:C = ES, ST = Granada, L = Granada, O = SWAP, OU = P4, CN = anabuenrúa, emailAddress = anabuenrúa@correo.ugr.es
 1 i:C = ES, ST = Granada, L = Granada, O = SWAP, OU = P4, CN = anabuenrúa, emailAddress = anabuenrúa@correo.ugr.es
-----BEGIN CERTIFICATE-----
MIID+TCCAUGgAwIBAgIU54dJa1cwrWNW2L7rFIHhYvpVkwDQYJKoZIhvcNAQEL
BQAwYsxCzAJBgNVBAYTAkVTRAwDgYDVQQIDAdHcmFuYWRhMRwDgYDVQQHDAdH
cmFuYWRhMRwDgYDVQQKDARTV0FQMswCQYDVQQLEDAJQNDETMBEGA1UEAwKYW5h
YnVlbnJ1YTenMCUGCSqGSIb3DQEQJARYYYW5hYnVlbnJ1YUbjb3JyZW8udWdyLnVz
MB4XDTIyMDUxMDA3MzIzMFOxMDA3MzIzMFOwYsxCzAJBgNVBAYTAkVTRAwDgYDVQQIDAdHcmFuYWRhMRwDgYDVQQKDARTV0FQMswCQYDVQQLEDAJQNDETMBEGA1UEAwKYW5hYnVlbnJ1YTenMCUGCSqGSIb3DQEQJARYYYW5hYnVlbnJ1YUbjb3JyZW8udWdyLnVzMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA1VLOUfZwc3UHFor259W1SaT8S+CuyK89wzTr7WSQpZr
MwJvHF4PyjOCEASphtewOXyc2MlN/R2g1K3m40jCg7WYvrHbFHAat5ktrkEIj4h
psB8OCAFLtnEOPo10bgOxHw15vvTmcQxc6by1DNGrsBYOPc62t12hPcEdqHEYXs
P0vNAUuhCbST/cYdn7+49vvD9mh/bbGu0J3/Ec/sNshc09sRHgt0EoultdUUABy
2b0V7LnS48aStPEw09e31xGEAZoh0oorfLD7+jk7++mgERep80qBTno/H9qd+HK
lskCaf93705JnLRQKEP/hY7JWunGacLndBQlICIWQIDAQABo1MwUTAdBgNVHQ4E
FgQUZel+LjQ0WxH7Dddfg04+vhTZyRYWdYDVR0jBBgwFoAUZel+LjQ0WxH7Dddfg04+vhTZyRYWdYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEANKF/
gdfZgsZsKQVRQ0jLvnY1t3NnyJyF8NbrbEPxfx5la9gnWvroyj5ln4Kd6NM5TEc8
+0syr9I0Yw6JGrMOYwuxnpdc/RcLLb6qWf1xsGwBkmOMF55NMAWpdQtEN1CLsAP
DDhsD43nT8yBFQdyvngZG8pzJTzK9Pc3dIqnNRD59LduQANYMnhQ/VNbbH44/FqF
ZH1/OwGzk0GT1IwK67crfnp89KC8ZnzMd7LH9eWwWEN0e0rewpvryo50Zhrq7Y
a5IsQqdk85vWUj7t76rdx/rj5bWgXi33y9DwZL0R2tLneFsdwudA1ancIj7EP6HL
BYWjzoIyISZbCHFSww==
-----END CERTIFICATE-----
---
Server certificate
subject=C = ES, ST = Granada, L = Granada, O = SWAP, OU = P4, CN = anabuenrúa, emailAddress = anabuenrúa@correo.ugr.es

```

NGINX COMO BALANCEADOR PARA PETICIONES HTTPS

Para configurar nginx con los certificados ssl, comenzamos copiando los ficheros de m1 a m3 mediante scp, se puede ver en (12).

Figura 12: Copia de certificados de m1 a m3 mediante nginx.



Creamos una carpeta ssl como anteriormente y movemos ahí los certificados copiados.

Ahora editamos el fichero de configuración de nginx `/etc/nginx/conf.d/default.conf` añadiendo un servidor nuevo como se muestra en (13).

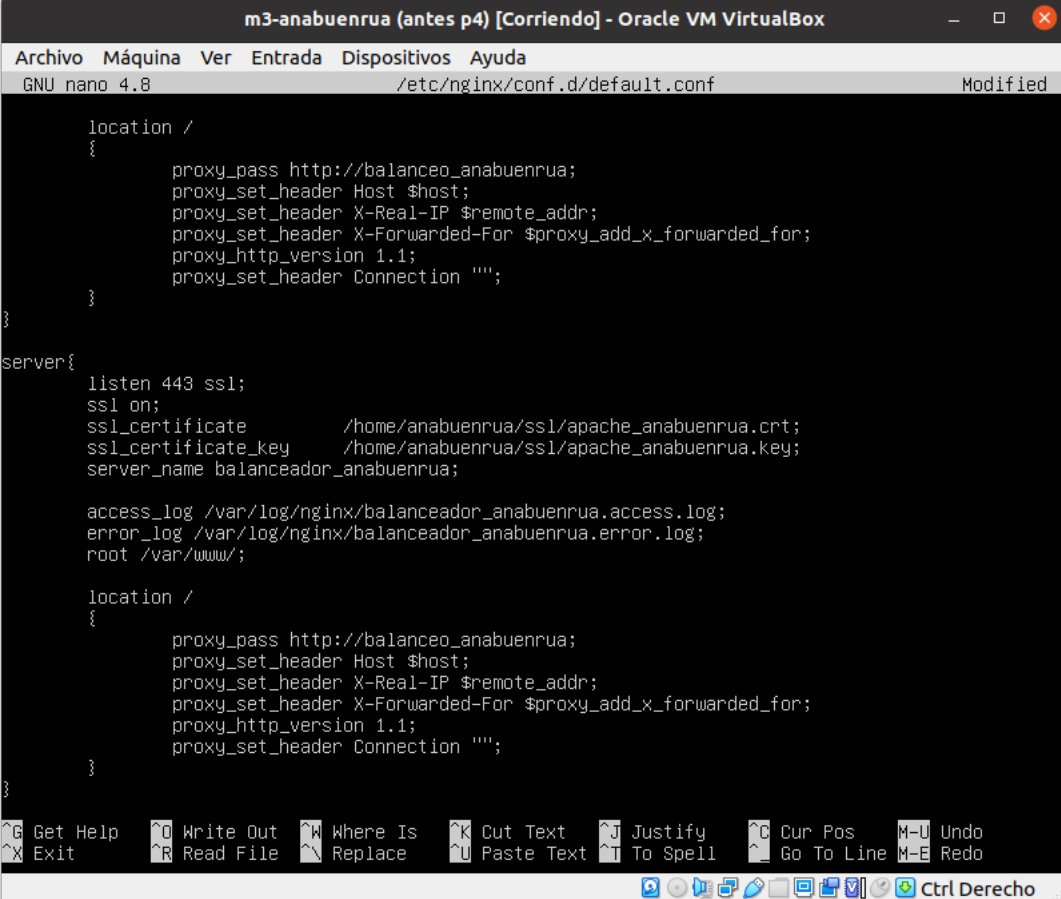
Relanzamos nginx con `sudo systemctl restart nginx` y comprobamos que podemos acceder al balanceador por https, como se ve en (14).

3.1 OPCIONES AVANZADAS

Como configuraciones adicionales para nginx se pueden usar varias directivas dentro del archivo de configuración `/etc/nginx/conf.d/default.conf`:

- `ssl_protocols <lista de protocolos>`. Su función es indicar que las conexiones por SSL y TLS que se van a establecer deben ser compatibles con las de la lista de protocolos indicada. Por ejemplo, `SSLv2`, `TLSv1` o `TLSv2`.
- `ssl_ciphers <lista de protocolos>`. Su función es, de análogamente a `ssl_protocols`, limitar las conexiones a aquellas compatibles con los sistemas cifrados listados.

Figura 13: Fichero /etc/nginx/conf.d/default.conf.



```

m3-anabuenrúa (antes p4) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8  /etc/nginx/conf.d/default.conf  Modified

    location /
    {
        proxy_pass http://balanceo_anabuenrúa;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_http_version 1.1;
        proxy_set_header Connection "";
    }
}

server{
    listen 443 ssl;
    ssl on;
    ssl_certificate /home/anabuenrúa/ssl/apache_anabuenrúa.crt;
    ssl_certificate_key /home/anabuenrúa/ssl/apache_anabuenrúa.key;
    server_name balanceador_anabuenrúa;

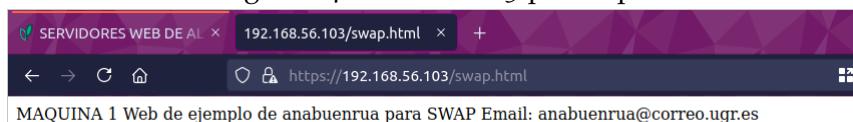
    access_log /var/log/nginx/balanceador_anabuenrúa.access.log;
    error_log /var/log/nginx/balanceador_anabuenrúa.error.log;
    root /var/www/;

    location /
    {
        proxy_pass http://balanceo_anabuenrúa;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_http_version 1.1;
        proxy_set_header Connection "";
    }
}

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
^X Exit      ^R Read File  ^N Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo

```

Figura 14: Acceso a m3 por https.



IPTABLES

Comprobamos que el cortafuegos iptables está ya instalado en todas las máquinas con `iptables --version`.

Vamos a comenzar creando un script para aceptar todo el tráfico, ya que es la restricción más amplia al no tener ninguna y aceptar cualquier petición.

Después, iremos añadiendo otras reglas más específicas para restringir el tráfico, recordando siempre que la última regla introducida tiene prioridad sobre las anteriores.

Creamos un directorio en cada máquina `/home/anabuenruea/scripts_iptable` para almacenar todos los scripts.

En primer lugar realizamos el script para permitir todo el tráfico, para ello creamos el script (15) en m1.

Lo ejecutamos mediante `sudo bash aceptar_todas.sh` y comprobamos que podemos seguir accediendo normalmente a ella, como por ejemplo mediante ping, como se ve en (16).

Ahora, escribimos un script para denegar todo el tráfico, que se muestra en (17).

Y comprobamos ahora en (18) que no podemos acceder a m1 mediante ping.

4.1 CONFIGURACIÓN BÁSICA

Vamos a realizar un script con la configuración básica del cortafuegos en todas las máquinas virtuales. Esta configuración va a consistir en denegar todo el tráfico por defecto y solo permitir el tráfico en SSH, HTTP y HTTPS. Al ser un servidor, hay que tener en cuenta que se debe permitir que reciba peticiones.

Dado que la máquina m1 tenía configurado como puerto para ssh el puerto 2022, por simplicidad se ha vuelto a dejar habilitado el puerto 22 para ssh, editando el fichero `/etc/ssh/sshd_config` y cambiando el puerto del 2022 al 22. Para hacer efectiva la configuración se ha relanzado ssh con `sudo systemctl restart ssh`.

El script de configuración básica se muestra en (19)

Figura 15: Script de iptables para admitir todo el tráfico.

```

m1-anabuenrúa (antes de iptables) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8                                aceptar_todas.sh
#!/bin/sh

# Se van a eliminar todas las reglas y permitir absolutamente todo el trafico

iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
  
```

Figura 16: Ping a m1 tras configuración básica de aceptar todas las peticiones.

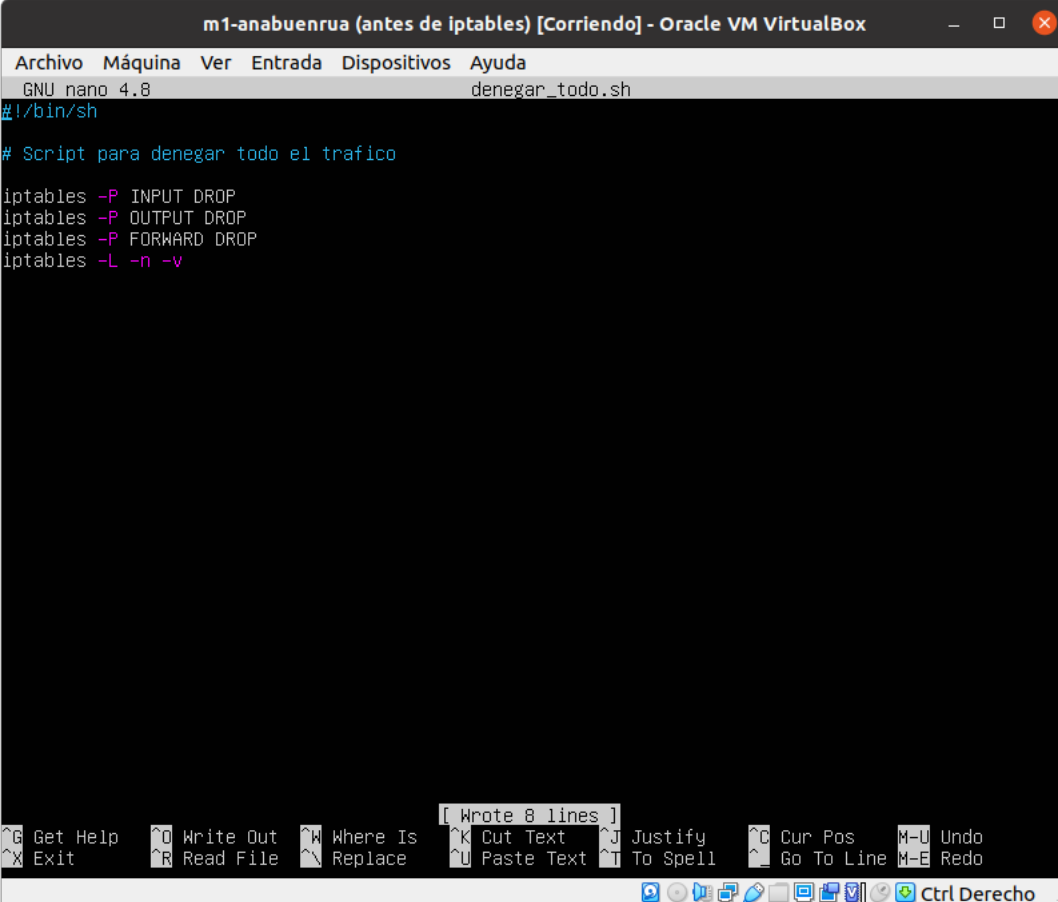
```

mapachana@mapachana-Aspire-E5-574G: ~
mapachana@mapachana-Aspire-E5-574G:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.824 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.745 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.759 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.919 ms
^C
--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.745/0.811/0.919/0.068 ms
mapachana@mapachana-Aspire-E5-574G:~$
  
```

Comprobamos que podemos acceder por http y https a m1, pero no mediante ping en (20).

Podemos comprobar que m2 y m3 funcionan de igual manera.

Figura 17: Script para denegar todo el tráfico con iptables.



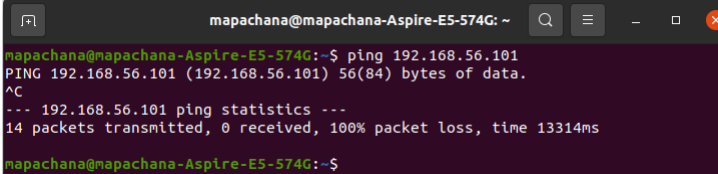
```

m1-anabuenrua (antes de iptables) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8      denegar_todo.sh
#!/bin/sh

# Script para denegar todo el trafico

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -L -n -v
  
```

Figura 18: Ping a m1 tras configuración básica de denegar todas las peticiones.



```

mapachana@mapachana-Aspire-E5-574G: ~
mapachana@mapachana-Aspire-E5-574G:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
^C
--- 192.168.56.101 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13314ms

mapachana@mapachana-Aspire-E5-574G:~$
  
```

4.2 OPCIONES AVANZADAS

La configuración anterior se puede mejorar, por ejemplo permitiendo el acceso a m1 y m2 solo a través de m3, además vamos a activar el acceso a ssh, ping y DNS en la red interna.

Para ello, modificamos el script de configuración básica anterior como se muestra en (21)

Copiamos los scripts a la máquina m2 con scp y comprobamos que la granja funciona correctamente, pues ya no deja acceder a m1 directamente, pero sí mediante m3, como se ve en (22).

Además, ya es posible hacer ping a todas las máquinas como en (23)

Figura 19: Script de configuración básica para iptables.

```

#!/bin/sh

# Configuración básica

# Elimino configuración ya existente
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Deniego todo el tráfico por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Permiso conexiones
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# Permiso acceso desde red local
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

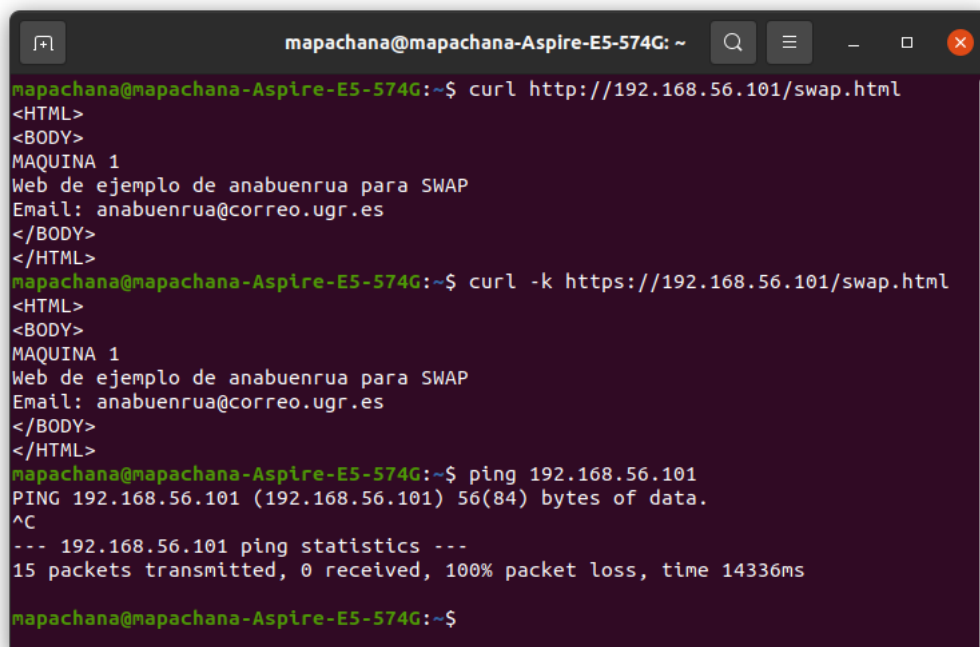
# Permiso ssh
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

# Permiso http
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

# Permiso https
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 443 -j ACCEPT

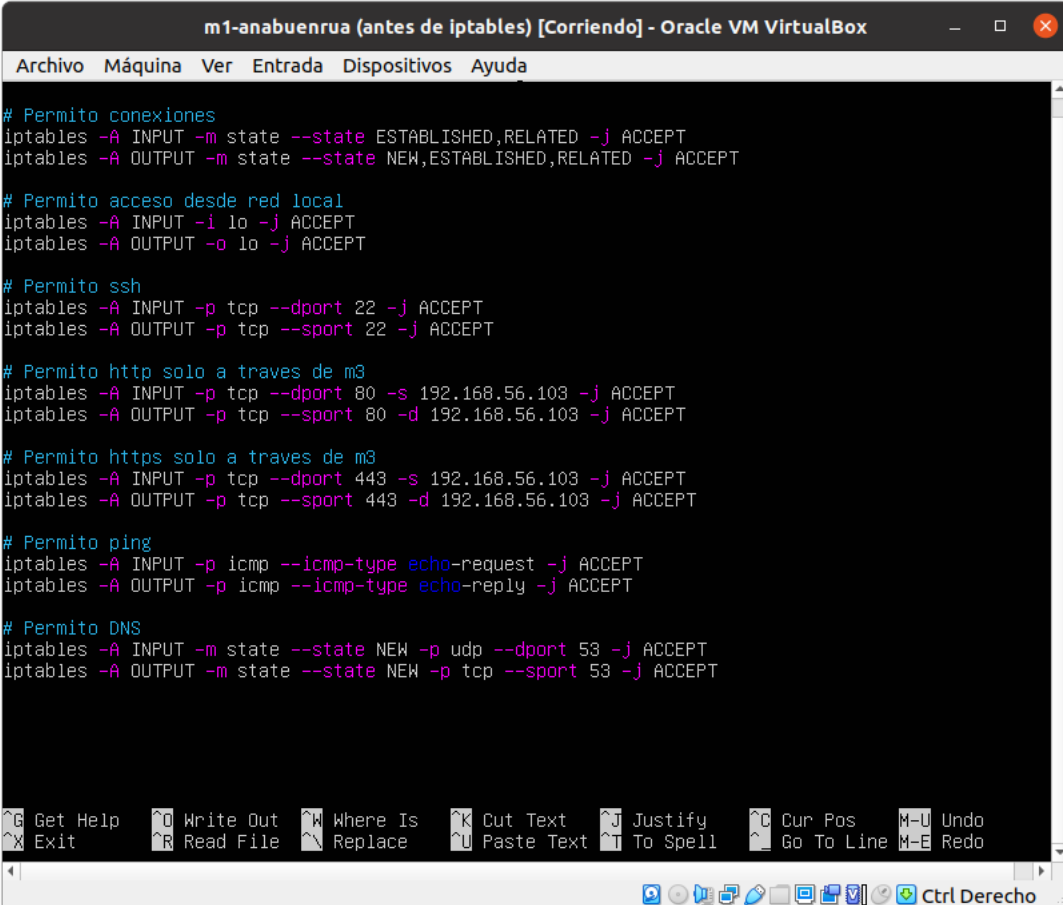
```


Figura 20: Comprobación de acceso por http y ping a m1 tras configuración básica.

A terminal window titled 'mapachana@mapachana-Aspire-E5-574G: ~' with standard window controls. It shows three commands and their outputs: 1) 'curl http://192.168.56.101/swap.html' returns an HTML body with 'MAQUINA 1' and a description of a swap example. 2) 'curl -k https://192.168.56.101/swap.html' returns the same HTML body. 3) 'ping 192.168.56.101' shows a failed ping with 100% packet loss and a time of 14336ms.

```
mapachana@mapachana-Aspire-E5-574G: ~  
mapachana@mapachana-Aspire-E5-574G:~$ curl http://192.168.56.101/swap.html  
<HTML>  
<BODY>  
MAQUINA 1  
Web de ejemplo de anabuenrúa para SWAP  
Email: anabuenrúa@correo.ugr.es  
</BODY>  
</HTML>  
mapachana@mapachana-Aspire-E5-574G:~$ curl -k https://192.168.56.101/swap.html  
<HTML>  
<BODY>  
MAQUINA 1  
Web de ejemplo de anabuenrúa para SWAP  
Email: anabuenrúa@correo.ugr.es  
</BODY>  
</HTML>  
mapachana@mapachana-Aspire-E5-574G:~$ ping 192.168.56.101  
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.  
^C  
--- 192.168.56.101 ping statistics ---  
15 packets transmitted, 0 received, 100% packet loss, time 14336ms  
mapachana@mapachana-Aspire-E5-574G:~$
```

Figura 21: Script de configuración avanzada de iptables.



The screenshot shows a terminal window titled "m1-anabuenrúa (antes de iptables) [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The terminal displays a series of iptables commands for configuring network rules. The commands are grouped by comments starting with "#". The rules allow established connections, local network access, SSH, HTTP (port 80) from 192.168.56.103, HTTPS (port 443) from 192.168.56.103, ping, and DNS (port 53). The terminal output shows the commands being executed successfully. At the bottom of the terminal window, there is a status bar with various keyboard shortcuts like ^G Get Help, ^Q Write Out, ^W Where Is, ^K Cut Text, ^J Justify, ^C Cur Pos, M-U Undo, ^X Exit, ^R Read File, ^N Replace, ^U Paste Text, ^T To Spell, ^L Go To Line, M-E Redo, and a "Ctrl Derecho" button.

```

# Permiso conexiones
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# Permiso acceso desde red local
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Permiso ssh
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

# Permiso http solo a traves de m3
iptables -A INPUT -p tcp --dport 80 -s 192.168.56.103 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -d 192.168.56.103 -j ACCEPT

# Permiso https solo a traves de m3
iptables -A INPUT -p tcp --dport 443 -s 192.168.56.103 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 443 -d 192.168.56.103 -j ACCEPT

# Permiso ping
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

# Permiso DNS
iptables -A INPUT -m state --state NEW -p udp --dport 53 -j ACCEPT
iptables -A OUTPUT -m state --state NEW -p tcp --sport 53 -j ACCEPT
  
```

Figura 22: Prueba de acceso a m1 y m3 mediante http.

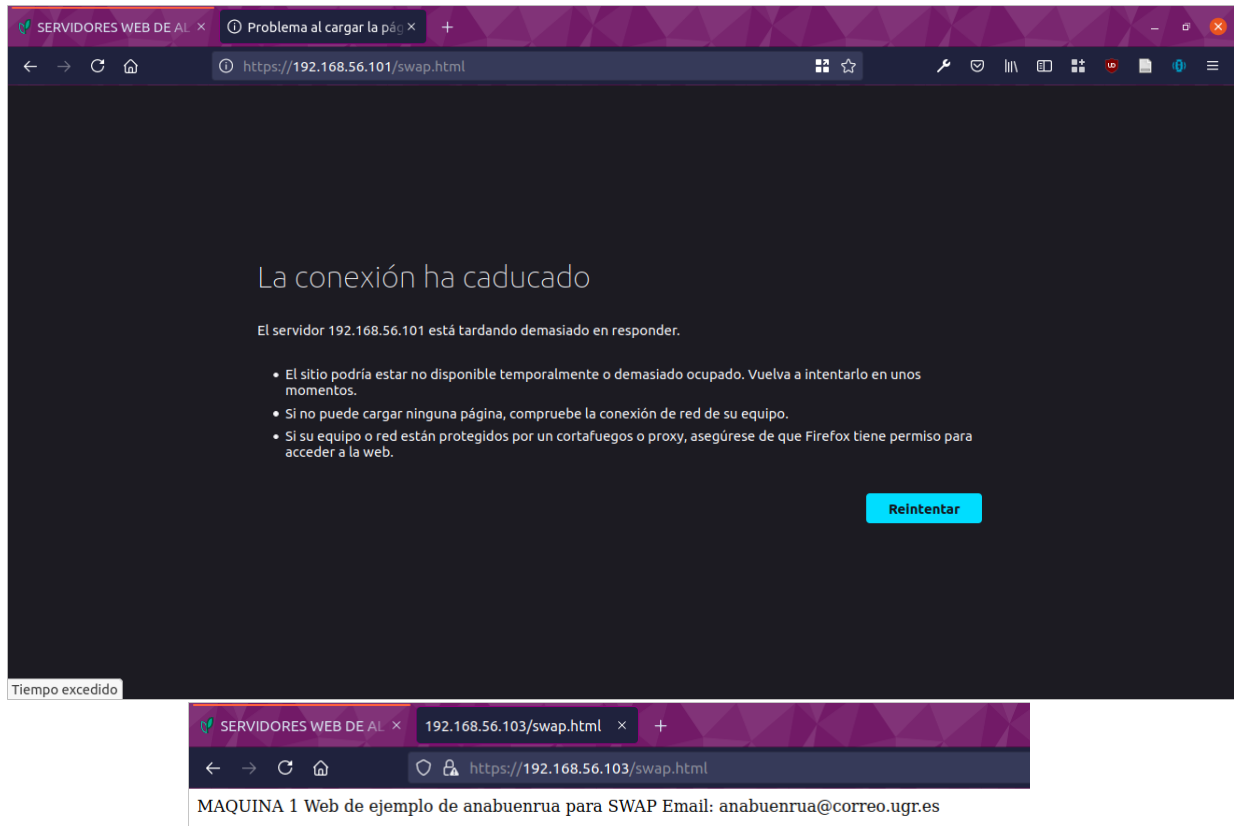
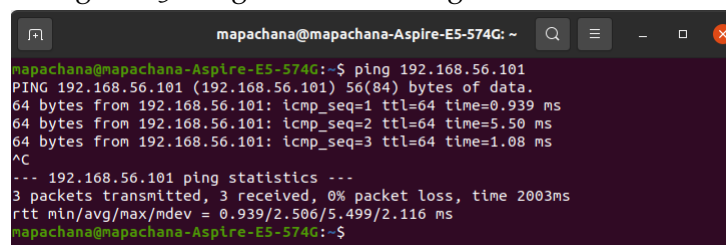


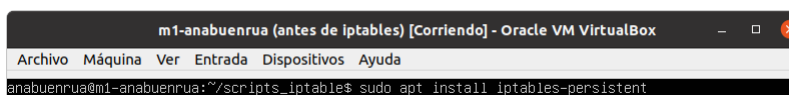
Figura 23: Ping a m1 tras configuración avanzada.



CONFIGURAR CORTAFUEGOS AL ARRANQUE

Para hacer persistentes las reglas y que se mantengan tras reiniciar las máquinas vamos a instalar `iptables-persistent`. Para ello ejecutamos (24)

Figura 24: Instalación de `iptables-persistent`.



Al instalar el paquete, seleccionamos que sí queremos guardar las reglas actuales en los ficheros correspondientes tanto en `ip4` como en `ip6`, como se ve en (25).

El paquete solo guarda las reglas al instalarse, para modificar qué reglas se van a aplicar al reiniciar el sistema, hay que guardarlas ejecutando:

```
iptables-save > /etc/iptables/rules.v4  
ip6tables-save > /etc/iptables/rules.v6
```

Probamos a ejecutarlos y comprobamos que hay que loggearse como `root` para hacerlo, como vemos en (26)

Para eliminar la configuración al inicio simplemente borramos los ficheros generados.

Figura 25: Copia de reglas tras la instalación de iptables-persistent.

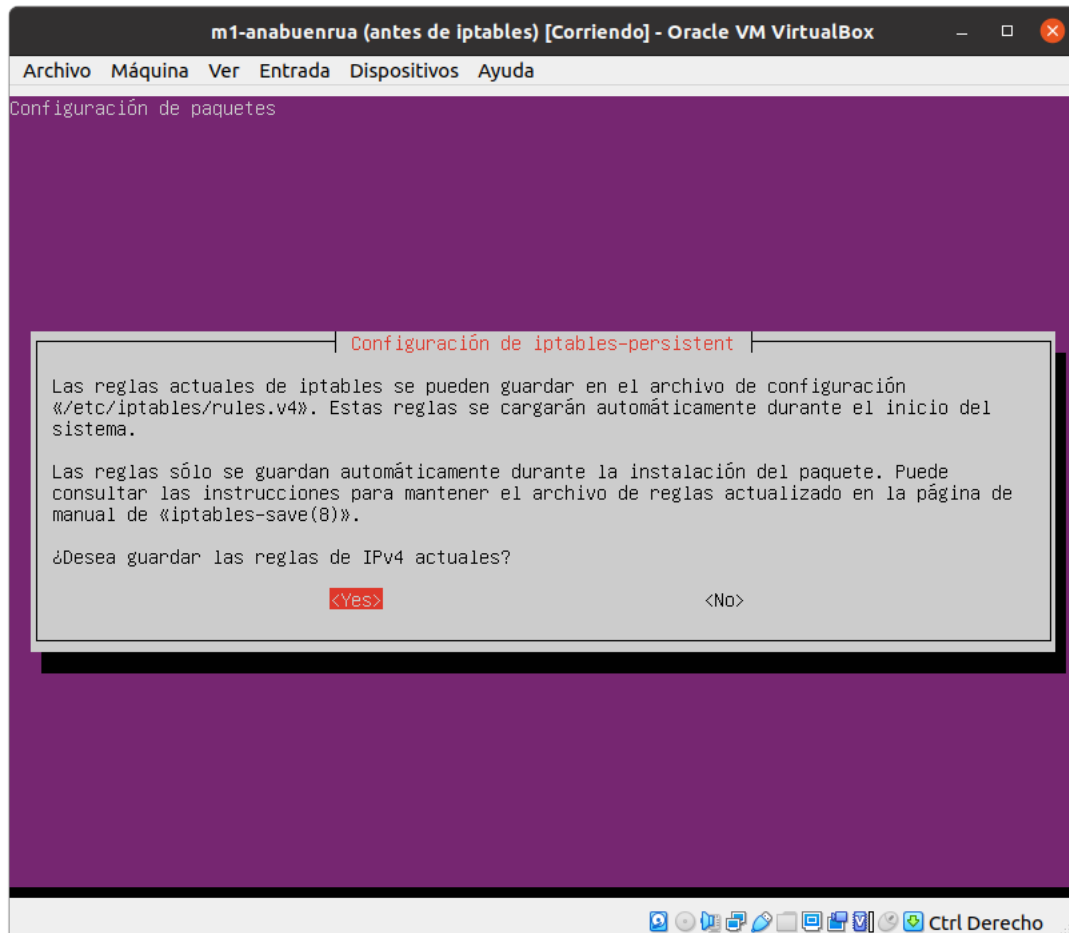
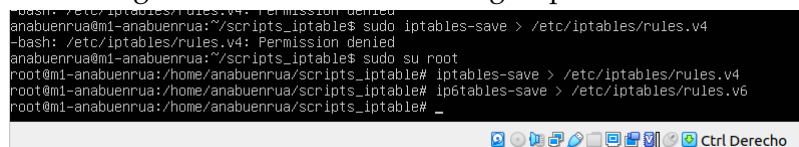


Figura 26: Modificación de reglas persistentes.



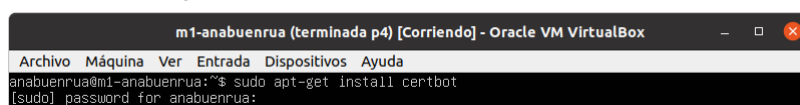
CERTBOT

Vamos a realizar la configuración en m1 y m3, para apache y nginx respectivamente.

6.1 CONFIGURACIÓN DE APACHE EN M1

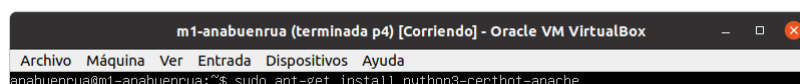
Comenzamos instalando en cada una de las máquinas virtuales certbot como se muestra en (27).

Figura 27: Instalación de certbot en m1.



En m1 comenzamos instalando el plugin para apache como en (28)

Figura 28: Instalación del plugin de certbot para apache.



Ahora, para instalar un certificado ejecutamos el comando de (29) y rellenamos los datos que nos piden.

Como no tenemos un dominio, el comando anterior nos da el error que se muestra en (30).

Por ello, para solo generar el certificado se ejecuta el comando de (31). Este comando crea el archivo `/etc/cron.d/certbot` de (32).

6.2 CONFIGURACIÓN DE NGINX EN M3

Para realizar la configuración de nginx análogamente se instala el plugin como se ve en (33).

Figura 29: Instalación de certificado en m1.

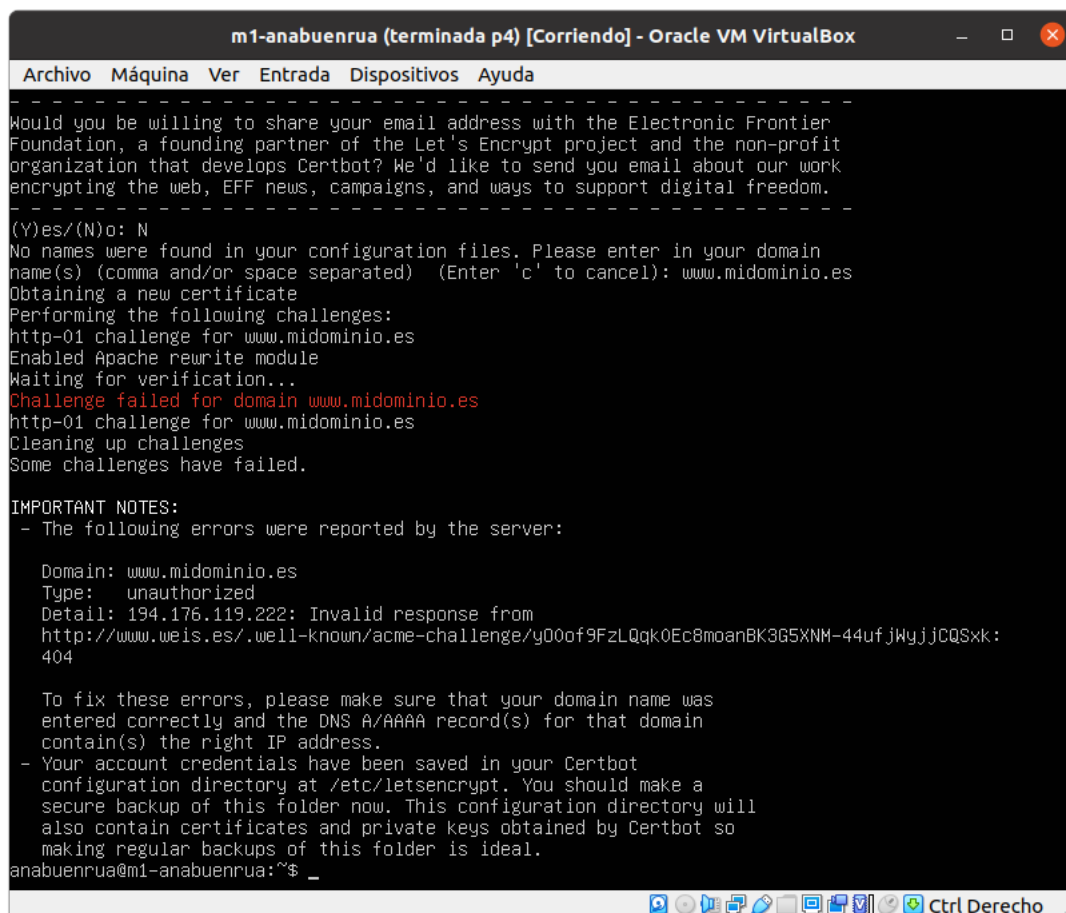


```
m1-anabuenrúa (terminada p4) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
anabuenrúa@m1-anabuenrúa:~$ sudo certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): anabuenrúa@correo.ugr.es

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
-----
(A)gree/(C)ancel: A

-----
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: N
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated) (Enter 'c' to cancel): www.midominio.es
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for www.midominio.es
Enabled Apache rewrite module
Waiting for verification...
```

Figura 30: Error de la instalación de certificado en m1.



```
m1-anabuenrúa (terminada p4) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
-----
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: N
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated) (Enter 'c' to cancel): www.midominio.es
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for www.midominio.es
Enabled Apache rewrite module
Waiting for verification...
Challenge failed for domain www.midominio.es
http-01 challenge for www.midominio.es
Cleaning up challenges
Some challenges have failed.

IMPORTANT NOTES:
- The following errors were reported by the server:

Domain: www.midominio.es
Type: unauthorized
Detail: 194.176.119.222: Invalid response from
http://www.weis.es/.well-known/acme-challenge/y00of9FzLQqk0Ec8moanBK3G5XNM-44ufjWYjjCQsXk:
404

To fix these errors, please make sure that your domain name was
entered correctly and the DNS A/AAAA record(s) for that domain
contain(s) the right IP address.
- Your account credentials have been saved in your Certbot
configuration directory at /etc/letsencrypt. You should make a
secure backup of this folder now. This configuration directory will
also contain certificates and private keys obtained by Certbot so
making regular backups of this folder is ideal.
anabuenrúa@m1-anabuenrúa:~$
```

De la misma forma ejecutamos el comando de (34) rellenando los datos, que nos devuelve el mismo error de antes al no tener dominio.

Figura 31: Generación de certificado en m1.

```
m1-anabuenrue (terminada p4) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
anabuenrue@m1-anabuenrue:~$ sudo certbot certonly --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated) (Enter 'c' to cancel):
```

Figura 32: Archivo /etc/cron.d/certbot

```
m1-anabuenrue (terminada p4) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
anabuenrue@m1-anabuenrue:~$ cat /etc/cron.d/certbot
# /etc/cron.d/certbot: crontab entries for the certbot package
#
# Upstream recommends attempting renewal twice a day
#
# Eventually, this will be an opportunity to validate certificates
# haven't been revoked, etc. Renewal will only occur if expiration
# is within 30 days.
#
# Important Note! This cronjob will NOT be executed if you are
# running systemd as your init system. If you are running systemd,
# the cronjob.timer function takes precedence over this cronjob. For
# more details, see the systemd.timer manpage, or use systemctl show
# certbot.timer.
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
0 */12 * * * root test -x /usr/bin/certbot -a \! -d /run/systemd/system && perl -e 'sleep int(rand(43200))' && certbot -q renew
anabuenrue@m1-anabuenrue:~$
```

Figura 33: Instalación del plugin de certbot para nginx en m3.

```
m3-anabuenrue (terminada p4) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
anabuenrue@m3-anabuenrue:~$ sudo apt-get install python3-certbot-nginx
```

Figura 34: Instalación de certificado en m3.

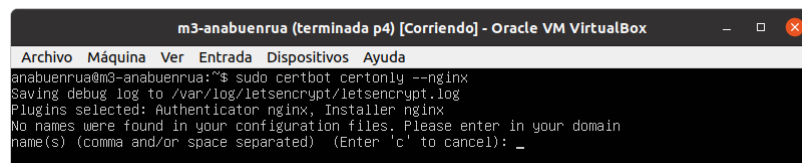
```
m3-anabuenrue (terminada p4) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
anabuenrue@m3-anabuenrue:~$ sudo certbot --nginx
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): anabuenrue@correo.ugr.es

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
-----
(A)gree/(C)ancel: A

-----
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: N
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated) (Enter 'c' to cancel): www.midominio.es
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for www.midominio.es
Using default address 80 for authentication.
nginx: [warn] the 'ssl' directive is deprecated, use the 'listen ... ssl' directive instead in /etc/
nginx/conf.d/default.conf:27
nginx: [error] invalid PID number "" in "/run/nginx.pid"
Waiting for verification...
```

Para solamente generar el certificado ejecutamos el comando y rellenamos los datos como en (35).

Figura 35: Generación de certificado en m3.



```
m3-anabuenrwa (terminada p4) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
anabuenrwa@m3-anabuenrwa:~$ sudo certbot certonly --nginx
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated) (Enter 'c' to cancel): _
```

BIBLIOGRAFÍA

- Diapositivas y gui3n de la pr3ctica.
- <http://nginx.org/en/docs/>
- <https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-18-04-es>
- <https://linuxconfig.org/how-to-make-iptables-rules-persistent-after-reboot-on-linux>
- <https://www.hostinger.com/tutorials/iptables-tutorial>
- <https://www.codegrepper.com/code-examples/shell/install+certbot+ubuntu+20.04>
- <https://www.cyberciti.biz/faq/unix-linux-check-if-port-is-in-use-command/>
- <https://easyengine.io/tutorials/nginx/troubleshooting/emerg-bind-failed-98-address-already-in-use/>