Álvaro Almellones Fernández

PRÁCTICA 9
PKI, CA. CERTIFICADOS. SERVIDORES SEGUROS SSL-TLS (HTTPS y FTPS).

Tener en cuenta para las evidencias de este ejercicio, que se debe **personalizar lo máximo** posible cada propiedad de los certificados creados, los nombres de cada uno de los ficheros, información de CA, etc.

1. **(0,5 puntos)** Instalación de servidor Ubuntu servers, denominado intranet-PKI-XXxx en la zona de intranet, mediante IP fija. (172.16.?.5). Se recomienda que se configure SSHD para que acepte la autentificación mediante cifrado asimétrico.

```
root@almellonesfernandez-firewall:~# ssh -i /root/keys/almellonesfernandez almellonesfernandez@172.16.102.5
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of mié 05 feb 2025 10:25:49 UTC

  System load:  0.01              Processes:             249
  Usage of /:   44.0% of 9.75GB   Users logged in:       0
  Memory usage: 8%                IPv4 address for ens33: 172.16.102.5
  Swap usage:   0%


El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 131 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


Last login: Wed Feb  5 10:21:27 2025 from 172.16.102.1
almellonesfernandez@almellonesfernandez-PKI-intranet ~$
```

Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-PKI-intranet:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.102.5  netmask 255.255.255.0  broadcast 172.16.102.255
        inet6 fe80::20c:29ff:febd:6fdd  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:bd:6f:dd  txqueuelen 1000  (Ethernet)
        RX packets 257  bytes 30050 (30.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 263  bytes 31578 (31.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 84  bytes 6352 (6.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84  bytes 6352 (6.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

almellonesfernandez@almellonesfernandez-PKI-intranet:~$ sudo netstat -putan |grep 22
[sudo] password for almellonesfernandez:
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
tcp6       0     36 172.16.102.5:22         172.16.102.1:37186      ESTABLISHED 1239/sshd: almellon
almellonesfernandez@almellonesfernandez-PKI-intranet:~$
```

Álvaro Almellones Fernández

2. (0,5 puntos) Creación de PKI y CA, lo más personalizados posible (fichero vars). Se debe configurar como mínimo:

• CN. Nombre Común o commonName (CA XXxx).

• CountryName, stateOrProvinceName, localityName, emailAddress.

• OU. Unidad organizativa

• Fecha de validez de la entidad certificadora.

• Fecha de validez de los certificados autofirmados.

• Algoritmo de firma de certificado (SHA-512).

• Otros dos que creáis oportuno (tamaño keys, etc.) para personalizar más vuestro CA a partir del fichero vars.

```
almellonesfernandez@almellonesfernandez-PKI-intranet:~$ openvpn --version
OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 2.10
DCO version: N/A
Originally developed by James Yonan
Copyright (C) 2002-2024 OpenVPN Inc <sales@openvpn.net>
Compile time defines: enable_async_push=no enable_comp_stub=no enable_crypto_ofb_cfb=yes enable_dco=yes enable_dco
_arg=yes enable_debug=yes enable_dependency_tracking=no enable_dlopen=unknown enable_dlopen_self=unknown enable_dl
open_self_static=unknown enable_fast_install=needless enable_fragment=yes enable_iproute2=no enable_libtool_lock=y
es enable_lz4=yes enable_lzo=yes enable_maintainer_mode=no enable_management=yes enable_option_checking=no enable_
pam_dlopen=no enable_pedantic=no enable_pkcs11=yes enable_plugin_auth_pam=yes enable_plugin_down_root=yes enable_p
lugins=yes enable_port_share=yes enable_selinux=no enable_shared=yes enable_shared_with_static_runtimes=no enable_
silent_rules=no enable_small=no enable_static=yes enable_strict=no enable_strict_options=no enable_systemd=yes ena
ble_unit_tests=no enable_werror=no enable_win32_dll=yes enable_wolfssl_options_h=yes enable_x509_alt_username=yes
with_aix_soname=aix with_crypto_library=openssl with_gnu_ld=yes with_mem_check=no with_openssl_engine=auto with_sy
sroot=no
almellonesfernandez@almellonesfernandez-PKI-intranet:~$
```

```
almellonesfernandez@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa$ ls
easyrsa  openssl-easyrsa.cnf  vars.example  x509-types
almellonesfernandez@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa$ sudo ./easyrsa init-pki

Notice
------
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* /etc/openvpn/easy-rsa/pki

Using Easy-RSA configuration:
* undefined

almellonesfernandez@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa$ ls
easyrsa  openssl-easyrsa.cnf  pki  vars.example  x509-types
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# cat vars | grep set_var
# "set_var" -- this means any set_var command that is uncommented has been
#set_var EASYRSA          "${0%/*}"
#set_var EASYRSA_OPENSSL          "openssl"
#set_var EASYRSA_OPENSSL          "C:/Program Files/OpenSSL-Win32/bin/openssl.exe"
#set_var EASYRSA_PKI              "$PWD/pki"
#set_var EASYRSA_TEMP_DIR         "$EASYRSA_PKI"
#set_var EASYRSA_DN     "cn_only"
set_var EASYRSA_REQ_COUNTRY      "ES"
set_var EASYRSA_REQ_PROVINCE     "MALAGA"
set_var EASYRSA_REQ_CITY         "SANTA ROSALIA-MAQUEDA"
set_var EASYRSA_REQ_ORG          "AlmellonesFernandez S.L."
set_var EASYRSA_REQ_EMAIL        "aalmfer2001@g.educaand.es"
set_var EASYRSA_REQ_OU           "Departamento de Seguridad AAF"
#set_var EASYRSA_PRESERVE_DN      1
#set_var EASYRSA_NO_PASS          1
set_var EASYRSA_KEY_SIZE         4096
set_var EASYRSA_ALGO             rsa
#set_var EASYRSA_CURVE            secp384r1
set_var EASYRSA_CA_EXPIRE        730
set_var EASYRSA_CERT_EXPIRE      365
#set_var EASYRSA_CRL_DAYS         180
#set_var EASYRSA_RAND_SN          "yes"
#set_var EASYRSA_PRE_EXPIRY_WINDOW      90
#set_var EASYRSA_NS_SUPPORT       "no"
#set_var EASYRSA_NS_COMMENT       "Easy-RSA Generated Certificate"
#set_var EASYRSA_EXT_DIR          "$EASYRSA/x509-types"
#set_var EASYRSA_KDC_REALM        "CHANGEME.EXAMPLE.COM"
#set_var EASYRSA_SSL_CONF         "$EASYRSA_PKI/openssl-easyrsa.cnf"
set_var EASYRSA_DIGEST           "sha512"
#set_var EASYRSA_BATCH            ""
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

Las dos variables nuevas que he añadido son la de rsa y key size para que al ser mas largo el tamaño de las keys sean más seguras

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa build-ca
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)

Enter New CA Key Passphrase:

Confirm New CA Key Passphrase:
..+.....+....+........+.......+...+............+...+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++*...+.....+...+...+.........+...+.......+..................+..+...+...+....+...+.....+......+.......+.......
..+........+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+......+....+.....+......+.+
........+.......+.....+...+......+...+.....................+.........+...+..+.+.....................+........+.+.
.+.......+.........................+...+....+..............+.....................+..........+.....................+....
...................+.......+..+......+.+......+..+...+....+......+.............+...+.+......+...+..+...+.+.......
..+.....................+.................+.......+...+.....+...+......+.............+...+...+.................+..
.+.+...........+.......+......+......+........+.+.....+....+...++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++
........+.....+..........+..+.........+....+..+...+.+...+.....+.+.........+..+....+..............+..+...+........
.+...+....+......+...+..+.............+..+.........+...+.+......+...+...++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++*.............+...+..+...+.+........+...+..........+...+.....+....+...++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++*..........+.....................+..+.....................+.......+.......
.+.....................+...+.....+....+..........+...........+...+....+...+..+.......+...+.....+.............
...+....+...+...+.........+.........+.....+..................+...+.....+............+......+.....+.............
....+.+.....+.+......+.............+...+......+.......+.............+...+.........+...+.....+....+.....+....+..
...........+.....+.....+.............+.....+....+...........+.........+.....+....+.....+....+.....+...+..+.+.
.....+............+...........+.............+......+.........+...+......+............+......+.................
...+.+......+......+..+.+.........+..+....+......+.....+.+..+.+......+......+.................+...........+....+.
.+....+..............+......+.............+.+..+...........+.............+..+.....+..+.....+...+....+.
.....+.................+..........+...........+...........+.........++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++
```

```
-----
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.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:CA-almellonesfernandez

Notice
------
CA creation complete. Your new CA certificate is at:
* /etc/openvpn/easy-rsa/pki/ca.crt

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa/pki# ls
ca.crt           index.txt       inline  openssl-easyrsa.cnf  reqs     serial
certs_by_serial  index.txt.attr  issued  private              revoked
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa/pki# ls private/
ca.key
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa/pki#
```

Álvaro Almellones Fernández

3. (2 puntos) Creación de 3 pares de llaves (.key y .crt) para servidores sin contraseña que usaremos a lo largo de todo el curso.

a) Servidor Apache (Https) (XXxx-https.key y XXxx-https.crt). (0,5 puntos)

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa gen-req almellonesfernandez-https nopass
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
...+.+.....+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*........+...++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++*.........+.....................+.............+..+.+............+.......
+.......+.....+............+.............+...+..+.........+..........+........+......+........................+..
....+.....+......+.......+.....+......+.+..............+....+...+.....+............+.+.........................+
...+.....+.+.........+..+.........+.+.....+....+...........+..........+...+..+....+.....+.........+....+..........
.+......+...............+..........+.....................+.............+..+...+.............................+..+.+..
+.......+......+...........+...+.+.....+......+................+...+..+............+..+....+.....+..............
......+...+....+......+......+......+..+.............+..+..........+..+..................+.......+...+..+.........
....+...+..+...+...+.+.........+.............+......+.....+.+..................+.....+......+..........+........
...............+......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+.....+....+..+....+...........+....+...+..+.+...+.....+....+..+.+............+...........+.+...+.....+.+..+....+
.....+.+.................++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+...+....+........
...+....+..+................+.....+....+...+.....+.................+.......+...+..+.+......+........+...+...+.+..
....+............+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+....+......+.........+.
.+.............+.....+.+..+....+.....+..............................+.....+...+....+..+.+..............+...++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----
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.
-----
Common Name (eg: your user, host, or server name) [almellonesfernandez-https]:
```



```
-----
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.
-----
Common Name (eg: your user, host, or server name) [almellonesfernandez-https]:

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /etc/openvpn/easy-rsa/pki/reqs/almellonesfernandez-https.req
* key: /etc/openvpn/easy-rsa/pki/private/almellonesfernandez-https.key

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa sign-req server almellonesfernandez-https
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
You are about to sign the following certificate:
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a server certificate
for '365' days:

subject=
    commonName                = almellonesfernandez-https

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes

Using configuration from /etc/openvpn/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'almellonesfernandez-https'
Certificate is to be certified until Feb  5 11:57:51 2026 GMT (365 days)

Write out database with 1 new entries
Database updated
```

```
Notice
------
Certificate created at:
* /etc/openvpn/easy-rsa/pki/issued/almellonesfernandez-https.crt

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls -l pki/issued/
total 8
-rw------- 1 root root 7464 feb  5 11:57 almellonesfernandez-https.crt
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls -l pki/private/
total 8
-rw------- 1 root root 3272 feb  5 11:54 almellonesfernandez-https.key
-rw------- 1 root root 3414 feb  5 11:30 ca.key
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

En los siguientes apartados te muestro es proceso con menos información para que las capturas no ocupen tanto

b) Servidor vsftpd (ftps) (XXxx-ftps.key y XXxx-ftps.crt) (0,5 puntos)

```
root@almellonesfernandez-PKI-intranet /etc/openvpn/easy-rsa# ./easyrsa gen-req almellonesfernandez-ftps nopass
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
```

```
Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /etc/openvpn/easy-rsa/pki/reqs/almellonesfernandez-ftps.req
* key: /etc/openvpn/easy-rsa/pki/private/almellonesfernandez-ftps.key

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa sign-req server almellonesfernandez-ftps
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars
```

```
Notice
------
Certificate created at:
* /etc/openvpn/easy-rsa/pki/issued/almellonesfernandez-ftps.crt

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls -l pki/issued/
total 16
-rw------- 1 root root 7458 feb  5 12:02 almellonesfernandez-ftps.crt
-rw------- 1 root root 7464 feb  5 11:57 almellonesfernandez-https.crt
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls -l pki/private/
total 12
-rw------- 1 root root 3268 feb  5 12:02 almellonesfernandez-ftps.key
-rw------- 1 root root 3272 feb  5 11:54 almellonesfernandez-https.key
-rw------- 1 root root 3414 feb  5 11:30 ca.key
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

c) Servidor OpenVPN (XXxx-vpn.key y XXxx-vpn.crt) (0,5 puntos)

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa gen-req almellonesfernandez-vpn nopass
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /etc/openvpn/easy-rsa/pki/reqs/almellonesfernandez-vpn.req
* key: /etc/openvpn/easy-rsa/pki/private/almellonesfernandez-vpn.key

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa sign-req server almellonesfernandez-vpn
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars
```

```
Notice
------
Certificate created at:
* /etc/openvpn/easy-rsa/pki/issued/almellonesfernandez-vpn.crt

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls -l pki/issued/
total 24
-rw------- 1 root root 7458 feb  5 12:02 almellonesfernandez-ftps.crt
-rw------- 1 root root 7464 feb  5 11:57 almellonesfernandez-https.crt
-rw------- 1 root root 7452 feb  5 12:12 almellonesfernandez-vpn.crt
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls -l pki/private/
total 16
-rw------- 1 root root 3268 feb  5 12:02 almellonesfernandez-ftps.key
-rw------- 1 root root 3272 feb  5 11:54 almellonesfernandez-https.key
-rw------- 1 root root 3272 feb  5 12:10 almellonesfernandez-vpn.key
-rw------- 1 root root 3414 feb  5 11:30 ca.key
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

d) Evidencie que las diferentes llaves públicas autofirmadas por nuestra CA contienen: (0,5 puntos)

• Cada uno de los cambios personalizados obligatorios realizados en fichero vars en apartado número dos.

• Los dos cambios realizados por vosotros.

• Números de serie que tiene cada certificado público (.crt). ¿Por qué se crean con esta numeración?

Se usa esta enumeración para asegurar que cada certificado sea único

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# cat pki/issued/almellonesfernandez-https.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            eb:81:6a:de:0d:ff:b4:ab:2c:cc:c2:95:9e:2d:4a:d1
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=CA-almellonesfernandez
        Validity
            Not Before: Feb  5 11:57:51 2025 GMT
            Not After : Feb  5 11:57:51 2026 GMT
        Subject: CN=almellonesfernandez-https
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-PKI-intranet /etc/openvpn/easy-rsa# cat pki/issued/almellonesfernandez-ftps.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            39:8c:82:6f:0b:f6:02:c0:c8:1f:7c:a3:17:30:11:06
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=CA-almellonesfernandez
        Validity
            Not Before: Feb  5 12:02:58 2025 GMT
            Not After : Feb  5 12:02:58 2026 GMT
        Subject: CN=almellonesfernandez-ftps
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# cat pki/issued/almellonesfernandez-vpn.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            22:4f:da:aa:8e:89:8f:70:87:0e:85:f7:91:70:5e:44
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=CA-almellonesfernandez
        Validity
            Not Before: Feb  5 12:12:29 2025 GMT
            Not After : Feb  5 12:12:29 2026 GMT
        Subject: CN=almellonesfernandez-vpn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

No he encontrado las variables de correo electrónico, localidad, etc en las claves aunque estuvieran sin comentar.

Álvaro Almellones Fernández

4. (1 punto) Creación de 2 pares de llaves (.key y .crt) para 2 clientes (una con contraseña y otra sin contraseña) que posteriormente usaremos para identificarnos en diferentes servidores a lo largo del todo el curso.

a) Cliente número 1 sin contraseña (XXxx-cliente1.key y XXxx-cliente.crt). (0,25 puntos)

Álvaro Almellones Fernández

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa sign-req client almellonesfernandez-cliente
1
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
You are about to sign the following certificate:
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a client certificate
for '365' days:

subject=
    commonName                = almellonesfernandez-cliente1

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes

Using configuration from /etc/openvpn/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'almellonesfernandez-cliente1'
Certificate is to be certified until Feb  5 16:28:55 2026 GMT (365 days)

Write out database with 1 new entries
Database updated
```



```
Notice
------
Certificate created at:
* /etc/openvpn/easy-rsa/pki/issued/almellonesfernandez-cliente1.crt

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa/pki# ls
ca.crt           index.txt       index.txt.attr.old  inline  openssl-easyrsa.cnf  reqs     serial
certs_by_serial  index.txt.attr  index.txt.old       issued  private              revoked  serial.old
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa/pki# ls -l private/
total 20
-rw------- 1 root root 3272 feb  5 16:25 almellonesfernandez-cliente1.key
-rw------- 1 root root 3268 feb  5 12:02 almellonesfernandez-ftps.key
-rw------- 1 root root 3272 feb  5 11:54 almellonesfernandez-https.key
-rw------- 1 root root 3272 feb  5 12:10 almellonesfernandez-vpn.key
-rw------- 1 root root 3414 feb  5 11:30 ca.key
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa/pki# ls -l issued/
total 32
-rw------- 1 root root 7308 feb  5 16:28 almellonesfernandez-cliente1.crt
-rw------- 1 root root 7458 feb  5 12:02 almellonesfernandez-ftps.crt
-rw------- 1 root root 7464 feb  5 11:57 almellonesfernandez-https.crt
-rw------- 1 root root 7452 feb  5 12:12 almellonesfernandez-vpn.crt
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa/pki#
```

b) Cliente número 2 con contraseña, (XXxx-cliente1.key y XXxx-cliente.crt). (0,25 puntos)

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa gen-req almellonesfernandez-cliente2
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
```

```
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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.
-----
Common Name (eg: your user, host, or server name) [almellonesfernandez-cliente2]:

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /etc/openvpn/easy-rsa/pki/reqs/almellonesfernandez-cliente2.req
* key: /etc/openvpn/easy-rsa/pki/private/almellonesfernandez-cliente2.key

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa sign-req client almellonesfernandez-cliente
2
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
You are about to sign the following certificate:
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a client certificate
for '365' days:

subject=
    commonName                = almellonesfernandez-cliente2

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes


Using configuration from /etc/openvpn/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'almellonesfernandez-cliente2'
Certificate is to be certified until Feb  6 11:16:13 2026 GMT (365 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* /etc/openvpn/easy-rsa/pki/issued/almellonesfernandez-cliente2.crt

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```



```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls -l pki/issued/
total 40
-rw------- 1 root root 7308 feb  5 16:28 almellonesfernandez-cliente1.crt
-rw------- 1 root root 7308 feb  6 11:16 almellonesfernandez-cliente2.crt
-rw------- 1 root root 7458 feb  5 12:02 almellonesfernandez-ftps.crt
-rw------- 1 root root 7464 feb  5 11:57 almellonesfernandez-https.crt
-rw------- 1 root root 7452 feb  5 12:12 almellonesfernandez-vpn.crt
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls -l pki/private/
total 24
-rw------- 1 root root 3272 feb  5 16:25 almellonesfernandez-cliente1.key
-rw------- 1 root root 3414 feb  6 11:13 almellonesfernandez-cliente2.key
-rw------- 1 root root 3268 feb  5 12:02 almellonesfernandez-ftps.key
-rw------- 1 root root 3272 feb  5 11:54 almellonesfernandez-https.key
-rw------- 1 root root 3272 feb  5 12:10 almellonesfernandez-vpn.key
-rw------- 1 root root 3414 feb  5 11:30 ca.key
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

Álvaro Almellones Fernández

c) Evidencie que las diferentes llaves públicas para clientes autofirmadas por nuestra CA contienen: (0,5 puntos)

• Cada uno de los cambios personalizados obligatorios realizados en fichero vars en apartado número dos.

• Los dos cambios realizados por vosotros.

• Números de serie que tiene cada certificado público (.crt).

```
root@almellonesfernandez-PKI-intranet /etc/openvpn/easy-rsa# cat pki/issued/almellonesfernandez-cliente1.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            57:51:e8:db:70:24:55:cc:34:6d:17:a1:04:3a:2c:b4
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=CA-almellonesfernandez
        Validity
            Not Before: Feb  5 16:28:55 2025 GMT
            Not After : Feb  5 16:28:55 2026 GMT
        Subject: CN=almellonesfernandez-cliente1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b5:88:e6:d1:4a:81:a9:f3:ff:9d:2b:6f:cc:ce:
                    74:54:6d:64:d0:2f:fe:c7:4f:a4:cf:06:9c:f0:96:
                    55:10:17:da:40:31:2b:04:95:42:43:61:57:31:67:
                    72:eb:51:76:74:2b:d3:8d:3a:0d:44:43:d0:31:1d:
                    67:16:82:42:0d:36:25:cc:c4:86:cb:f6:c1:30:a6:
                    49:8c:e0:96:68:22:97:84:e9:5e:aa:88:70:45:1d:
                    4a:fd:1d:5a:ae:8a:99:df:58:c3:54:56:b7:cd:a9:
                    1e:16:69:dd:82:3e:4a:0d:07:15:c5:a7:28:3d:ac:
                    44:b0:4f:0f:f0:e6:e7:17:fc:b9:b3:d2:b4:a8:dd:
                    be:0a:9b:76:6a:ad:15:1b:a7:5b:7e:b1:e1:c6:24:
                    7f:9c:92:7e:97:af:8e:4c:2e:d5:4d:a6:73:26:57:
                    4d:9d:99:ec:34:4d:a9:6e:ce:b1:8b:8f:80:82:51:
                    a0:c3:dd:2d:f7:6a:b8:1e:f0:cf:23:76:f1:66:9e:
                    8e:bb:30:fa:28:e6:4c:00:13:9b:f0:be:92:f3:69:
                    cd:49:76:b2:7d:12:d0:0c:69:aa:00:fa:d2:00:c5:
                    d8:26:76:3e:e3:3a:e0:a3:17:b0:41:9f:fc:b4:4b:
```



```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# cat pki/issued/almellonesfernandez-cliente2.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ae:65:f0:9b:2e:38:33:60:f0:46:27:d3:08:f8:25:35
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=CA-almellonesfernandez
        Validity
            Not Before: Feb  6 11:16:13 2025 GMT
            Not After : Feb  6 11:16:13 2026 GMT
        Subject: CN=almellonesfernandez-cliente2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:bc:15:ca:14:91:de:43:40:ee:11:a3:db:64:60:
                    a2:ed:ce:63:25:6d:0c:ee:85:9a:a7:d9:3b:ea:8c:
                    2b:98:07:45:d9:23:78:be:61:3a:68:6d:8a:54:ef:
                    20:81:bd:37:c7:42:bc:64:1b:bd:70:29:d0:fc:b1:
                    52:5f:c3:14:c0:eb:bc:d0:4e:54:4b:be:ef:39:93:
                    c9:66:c0:b0:36:a6:e0:1b:c2:fa:ad:4e:e7:ab:5b:
                    e0:32:d7:cb:2f:d9:a5:32:5b:2c:17:13:4f:3e:ec:
                    f6:c4:2c:a5:a4:4b:b7:85:11:e8:f4:a7:4a:a3:1d:
```

Álvaro Almellones Fernández

5. (3 puntos) (APACHE CON HTTPS) Configuración de servidor Apache en zona DMZ (10.0.?.2), para que escuche por https (conexión cifrada). Se debe evidenciar lo siguiente:

a) Cambios en la configuración de ficheros de configuración de apache y habilitación del módulo SSL. (0,25 pt).

```
 GNU nano 7.2                  /etc/apache2/sites-available/default-ssl.conf
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost
                DocumentRoot /var/www/htmls
                # 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/ssl/certs/almellonesfernandez-https.crt
                SSLCertificateKeyFile /etc/ssl/private/almellonesfernandez-https.key
                #   Server Certificate Chain:
                                [ Read 119 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo
```



```
root@almellonesfernandez-us-dmz:~/keys/server# sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@almellonesfernandez-us-dmz:~/keys/server# sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@almellonesfernandez-us-dmz:~/keys/server#
```

b) Creación de página personalizadas (index.html) para http y otra para https. Estarán en directorios diferentes
directorios de trabajo (DocumentRoot). (0,25 pt).

Álvaro Almellones Fernández

```
root@almellonesfernandez-us-dmz /var/www/htmls# ls /var/www/
html  htmls
root@almellonesfernandez-us-dmz:/var/www/htmls# ls /var/www/html
index.php
root@almellonesfernandez-us-dmz:/var/www/htmls# cat /var/www/html/index.php
<?php
$server_ip = $_SERVER['SERVER_ADDR'];
$client_ip = $_SERVER['REMOTE_ADDR'];

echo "<h1>Esta pagina no es segura </h1>";
echo "<h1>Nombre: Alvaro </h1>";
echo "<h1>Apellidos: Almellones Fernandez</h1>";
echo "<h1>Clase: 2</h1>";
echo "<h1>IP del Servidor: $server_ip</h1>";
echo "<h1>IP del Cliente: $client_ip</h1>";
?>
root@almellonesfernandez-us-dmz:/var/www/htmls# ls /var/www/htmls
ca.crt  index.php
root@almellonesfernandez-us-dmz:/var/www/htmls# cat /var/www/htmls/index.php
<?php
$server_ip = $_SERVER['SERVER_ADDR'];
$client_ip = $_SERVER['REMOTE_ADDR'];

echo "<h1>Esta pagina es segura </h1>";
echo "<h1>Nombre: Alvaro </h1>";
echo "<h1>Apellidos: Almellones Fernandez</h1>";
echo "<h1>Clase: 2</h1>";
echo "<h1>IP del Servidor: $server_ip</h1>";
echo "<h1>IP del Cliente: $client_ip</h1>";
?>
root@almellonesfernandez-us-dmz:/var/www/htmls#
```


c) Ubicación de las diferentes llaves (XXxx-https.key, XXxx-https.crt, ca.crt). (0,25 pt).

```
root@almellonesfernandez-us-dmz:/# ls /etc/ssl/certs/ |grep almellonesfernandez
almellonesfernandez-https.crt
root@almellonesfernandez-us-dmz:/# ls /etc/ssl/private/ |grep almellonesfernandez
almellonesfernandez-https.key
root@almellonesfernandez-us-dmz:/# ls /etc/ssl/certs/ |grep ca
Actalis_Authentication_Root_CA.pem
Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.pem
ca6e4ad9.0
ca-certificates.crt
ca.crt
COMODO_Certification_Authority.pem
COMODO_ECC_Certification_Authority.pem
COMODO_RSA_Certification_Authority.pem
Entrust_Root_Certification_Authority_-_EC1.pem
Entrust_Root_Certification_Authority_-_G2.pem
Entrust_Root_Certification_Authority_-_G4.pem
Entrust_Root_Certification_Authority.pem
ePKI_Root_Certification_Authority.pem
Go_Daddy_Root_Certificate_Authority_-_G2.pem
```

d) Servicio arrancado y servicio escuchando en el 80 y 443. (0,25 pt).

```
root@almellonesfernandez-us-dmz:/# netstat -putan |grep apache
tcp6       0      0 :::80                   :::*                    LISTEN      2358/apache2
tcp6       0      0 :::443                  :::*                    LISTEN      2358/apache2
root@almellonesfernandez-us-dmz:/#
```

e) Conexión desde cliente web GUI ubicado en la zona WAN tanto en el puerto 80 como por el puerto 443, donde se demuestre.

Álvaro Almellones Fernández

Esta pagina no es segura

Nombre: Alvaro

Apellidos: Almellones Fernandez

Clase: 2

IP del Servidor: 10.0.102.2

IP del Cliente: 192.168.1.64

Esta pagina es segura

Nombre: Alvaro

Apellidos: Almellones Fernandez

Clase: 2

IP del Servidor: 10.0.102.2

IP del Cliente: 192.168.1.64

▪ Cambios de los contadores de iptables tanto de la tabla NAT como de la tabla FILTER (FORWARD) al lanzar peticiones por los dos puertos. (0,25 pt).

```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 26 packets, 1324 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REDIRECT   6    --  lan2   *       172.16.102.0/24      0.0.0.0/0            tcp dpt:80 redir ports 31
28
    0     0 REDIRECT   6    --  wlan2  *       192.168.102.0/24     0.0.0.0/0            tcp dpt:80 redir ports 31
29
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.102.2:
80
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.102.2
:443
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8080 to:10.0.102.
2:8080
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8404 to:10.0.102.
2:8404
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej NATP *
/ to:10.0.102.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de DMZ a WAN
 */
    0     0 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de LAN a WAN
 */
    0     0 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de WLAN a WA
N */
```

Álvaro Almellones Fernández

```
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.4         0.0.0.0/0
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:123
    0     0 DROP       6    --  lan2   wan2    172.16.102.5         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.5         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.5         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.5         0.0.0.0/0
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.5         0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
 /* Respuesta WAN a LAN */
    0     0 DROP       6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  wlan2  wan2    192.168.102.2        0.0.0.0/0
    0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
 /* Respuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:8080
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:8404
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     0    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefi
x "LAN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefi
x "LAN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
```


Esta pagina no es segura

Nombre: Alvaro

Apellidos: Almellones Fernandez

Clase: 2

IP del Servidor: 10.0.102.2

IP del Cliente: 192.168.1.64

Esta pagina es segura

Nombre: Alvaro

Apellidos: Almellones Fernandez

Clase: 2

IP del Servidor: 10.0.102.2

IP del Cliente: 192.168.1.64

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 64 packets, 3249 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REDIRECT   6    --  lan2   *       172.16.102.0/24      0.0.0.0/0            tcp dpt:80 redir ports 31
28
    0     0 REDIRECT   6    --  wlan2  *       192.168.102.0/24     0.0.0.0/0            tcp dpt:80 redir ports 31
29
    1    52 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.102.2:
80
    4   208 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.102.2
:443
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8080 to:10.0.102.
2:8080
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8404 to:10.0.102.
2:8404
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej NATP *
/ to:10.0.102.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 5 packets, 260 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de DMZ a WAN
 */
    0     0 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de LAN a WAN
 */
    0     0 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de WLAN a WA
N */
```



```
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.5         0.0.0.0/0
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.5         0.0.0.0/0            udp dpt:123
    2   364 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
 /* Respuesta WAN a LAN */
    0     0 DROP       6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  wlan2  wan2    192.168.102.2        0.0.0.0/0
    0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
 /* Respuesta WAN a WLAN */
    1    52 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    4   208 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:8080
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:8404
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
   28 11226 ACCEPT     0    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefi
x "LAN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefi
x "LAN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar
 a otros procesos. Ej. DNS local */
  110 10316 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
```

▪ Conexión establecida tanto en el lado del cliente como en el lado del servidor (netstat), por los dos puertos. (0,25 pt).

```
root@almellonesfernandez-us-dmz:/# netstat -putan |grep apache
tcp6       0      0 :::80                   :::*                    LISTEN      2358/apache2
tcp6       0      0 :::443                  :::*                    LISTEN      2358/apache2
tcp6       0      0 10.0.102.2:443          192.168.1.64:57834      ESTABLISHED 2362/apache2
tcp6       0      0 10.0.102.2:80           192.168.1.64:57827      ESTABLISHED 2365/apache2
root@almellonesfernandez-us-dmz:/#
```

▪ Tcpdump en el lado del servidor dmz que está escuchando conexiones tanto del 80 y 443. ¿Se observa alguna diferencia en lo que se ha reportado? (0,25 pt).

Álvaro Almellones Fernández

```
root@almellonesfernandez-us-dmz:/# sudo tcpdump port 80 -A
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:12:02.259208 IP 192.168.1.64.57842 > almellonesfernandez-us-dmz.http: Flags [F.], seq 4106075937, ack 328738036
4, win 513, length 0
E..([.@...n4...@
.f....P...!..q.P....G........
12:12:02.259250 IP almellonesfernandez-us-dmz.http > 192.168.1.64.57842: Flags [.], ack 1, win 502, length 0
E..(..@.@...
.f....@.P....q...."P....R..
12:12:02.259595 IP 192.168.1.64.57847 > almellonesfernandez-us-dmz.http: Flags [S], seq 2878284278, win 64240, opt
ions [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4[.@...n%...@
.f....P..!..........g..............
12:12:02.259595 IP 192.168.1.64.57848 > almellonesfernandez-us-dmz.http: Flags [S], seq 311118294, win 64240, opti
ons [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4[.@...n$...@
.f....P..I..........................
12:12:02.259630 IP almellonesfernandez-us-dmz.http > 192.168.1.64.57847: Flags [S.], seq 3985684905, ack 287828427
9, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
E..4..@.@...
.f....@.P........!.....2.............
12:12:02.259683 IP almellonesfernandez-us-dmz.http > 192.168.1.64.57848: Flags [S.], seq 1721752039, ack 311118295
, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
E..4..@.@...
.f....@.P..f.....I.....2.............
12:12:02.260232 IP 192.168.1.64.57847 > almellonesfernandez-us-dmz.http: Flags [.], ack 1, win 4100, length 0
E..([.@...n/...@
.f....P..!.....P.............
12:12:02.260232 IP 192.168.1.64.57848 > almellonesfernandez-us-dmz.http: Flags [.], ack 1, win 4100, length 0
E..([.@...n....@
.f....P..I.f...P.............

Host: 192.168.1.111
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safa
ri/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9


12:12:02.260428 IP almellonesfernandez-us-dmz.http > 192.168.1.64.57847: Flags [.], ack 455, win 501, length 0
E..(vb@.@...
.f....@.P........#.P...2...
12:12:02.261468 IP almellonesfernandez-us-dmz.http > 192.168.1.64.57847: Flags [P.], seq 1:405, ack 455, win 501,
length 404: HTTP: HTTP/1.1 200 OK
E...vc@.@...
.f....@.P........#.P...3...HTTP/1.1 200 OK
Date: Mon, 10 Feb 2025 12:12:02 GMT
Server: Apache/2.4.58 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 152
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

.........e.A
.0.E.2'.. EK.JQp#.'..P.iR&..O....\|............1...\........k.e.........n..b(.s..KV...).~.\.....|..    n,....5h..
..L.".Ym.wh..Zl._...*.A....
12:12:02.311430 IP 192.168.1.64.57847 > almellonesfernandez-us-dmz.http: Flags [.], ack 405, win 4098, length 0
```

Álvaro Almellones Fernández

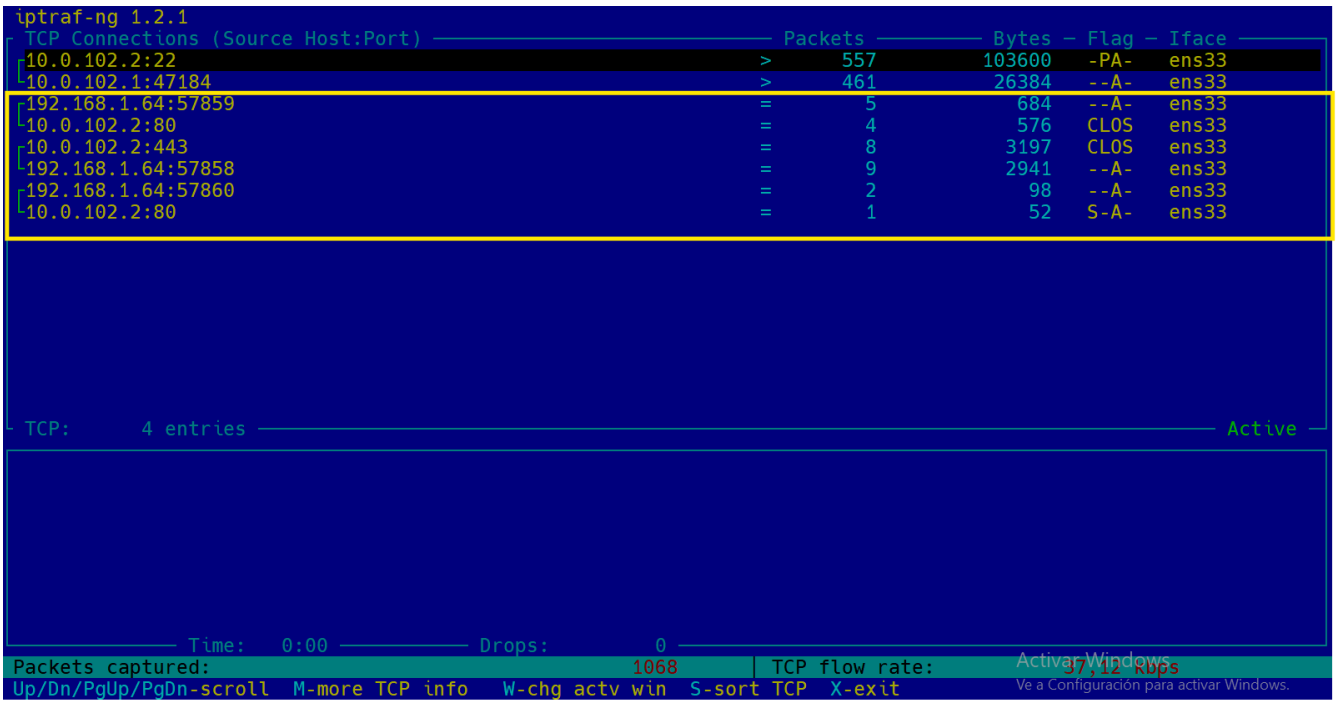
```
root@almellonesfernandez-us-dmz:/# sudo tcpdump port 443 -A
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:14:24.634150 IP 192.168.1.64.57851 > almellonesfernandez-us-dmz.https: Flags [S], seq 550814416, win 64240, opt
ions [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4[.@...m....@
.f..... ..........z.............
12:14:24.634150 IP 192.168.1.64.57852 > almellonesfernandez-us-dmz.https: Flags [S], seq 3741364972, win 64240, op
tions [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4[.@...m....@
.f.............................
12:14:24.634204 IP almellonesfernandez-us-dmz.https > 192.168.1.64.57851: Flags [S.], seq 1321336871, ack 55081441
7, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
E..4..@.@...
.f....@....N..' .......2.............
12:14:24.634246 IP almellonesfernandez-us-dmz.https > 192.168.1.64.57852: Flags [S.], seq 4048406606, ack 37413649
73, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
E..4..@.@...
.f....@.....M.N........2.............
12:14:24.635173 IP 192.168.1.64.57851 > almellonesfernandez-us-dmz.https: Flags [.], ack 1, win 4100, length 0
E..([.@...m....@
.f..... ...N..(P...W.........
12:14:24.635173 IP 192.168.1.64.57852 > almellonesfernandez-us-dmz.https: Flags [.], ack 1, win 4100, length 0
E..([.@...m....@
.f..........M.OP...>.........
12:14:24.635173 IP 192.168.1.64.57851 > almellonesfernandez-us-dmz.https: Flags [P.], seq 1:1877, ack 1, win 4100,
 length 1876
E..|[.@...f....@
.f..... ...N..(P...9Y......O...K..2.6rS...)H..]......)..>p{..Y.... ;m....).nC!...e..h@.T.Ol.Nkbi.... .........+./.
,.0............./.5.....................-.........+..........#...3.............V.o5.....3o_k.....;.*pc..1N.5...
....K..Q`.tB.3...9.i...B..p .`../8.:T...6.~..|._^....x..........          ..fve.|.0EMv..1.7v.....kH.P.U(.....7.R....
:.,.....3m...[..qf....v..).#.....&..J.)....E.hv..W...iC..|..._:.Y....o...-...P>.....3..ze       [.....T..>....2.).
```

```
.f..... ...N..(P...W.........
12:14:24.635173 IP 192.168.1.64.57852 > almellonesfernandez-us-dmz.https: Flags [.], ack 1, win 4100, length 0
E..([.@...m....@
.f..........M.OP...>.........
12:14:24.635173 IP 192.168.1.64.57851 > almellonesfernandez-us-dmz.https: Flags [P.], seq 1:1877, ack 1, win 4100,
 length 1876
E..|[.@...f....@
.f..... ...N..(P...9Y......O...K..2.6rS...)H..]......)..>p{..Y.... ;m....).nC!...e..h@.T.Ol.Nkbi.... .........+./.
,.0............./.5.....................-.........+..........#...3.............V.o5.....3o_k.....;.*pc..1N.5...
....K..Q`.tB.3...9.i...B..p .`../8.:T...6.~..|._^....x..........          ..fve.|.0EMv..1.7v.....kH.P.U(.....7.R....
:.,.....3m...[..qf....v..).#.....&..J.)....E.hv..W...iC..|..._:.Y....o...-...P>.....3..ze       [.....T..>....2.).
..fF..4A.y#....\..........wT..3.......G)a......+\...^B*v..../..... ...w:..A.v7M.J/...#..M...l.pL;.8t~c...|+..5../+
?T.....B%.. .&..V.Ro...rb....q..zP...zA.......4.s.6s...y.=..N.Dq. ...-$.Ih."b;....b..OR........)...'.F`....."..+..
LP.k..jKR.       .u..4..i........m.#|JQIY..(.#.t0.S..idb.f.....F...3..m..Z...LNk.8.....u..8.....zece.LSb.Z...&.q..3
..j|+>m.:.....Cc.C...#.m]+w..8.'.S...Pin......A...$..e......'s...V.y.G7.-.=Re."...p.p...x.
c.d.b{...'...\.vT.VTT....N.t...|Ce.....W...F..D|..,b...KI..w......t.R...l.."..yI..~.....................I.fc.&&...
P$..F..+..-...mf7.       ....H0Wt9......$u
qA..a,r2...I..%ff..5..p..."...v._N....{..q..I..G'8...2.....{....._M.o.j.w.#8..;v2\.}<..d...|.RXH.5v4...a.EChXYv-J
.";.|.7......#...6....O\.|.E.`o.:0.....=..... ...SR.&..<...K..J..&.{.H.Ij......y=...|...S.....94.u......\. .U..r.
F...sE.'.4.....Y.@.YR.....A&.....>A.H0...L..`iD.{.+.S(...1..h..p;.MS|..#......Y.......J.|6n?# .2dd'[.[p......"....
..O..!qG..j.!.l"....(.0|.2.j(.L.?.)M.
.......a*... ..$.l.....*..H...w.on%...#]..<.#.....................................
...
..............D......h2.......... :...hN8....R.f..s(....d.J..Q...m..E..E.#.V..H....Pi..AnG....F.}Y}F...
E6..*[..}...     ..5&..I..;._9Z N..............|L.|O`....6........=eU..`..D..h..y.       .....T"..j.......Q.......G.
K31.5v.O..%....P...      ?...
.......x...^..z....j.....;..T.In...D....l..i...y.8+S6.9.6{..G.6.......?=&.......h2.http/1.1**....).K.&. ..Q.....j.
b..V.2^....V.Z.............! .6..V@..2...]....
.4...._).V...D
12:14:24.635238 IP almellonesfernandez-us-dmz.https > 192.168.1.64.57851: Flags [.], ack 1877, win 488, length 0
E..(..@.@.%.
.f....@....N..( ..%P...2...
```


Se observa que por http se puede obtener información del servidor mientras que con https toda la información se encuentra cifrada

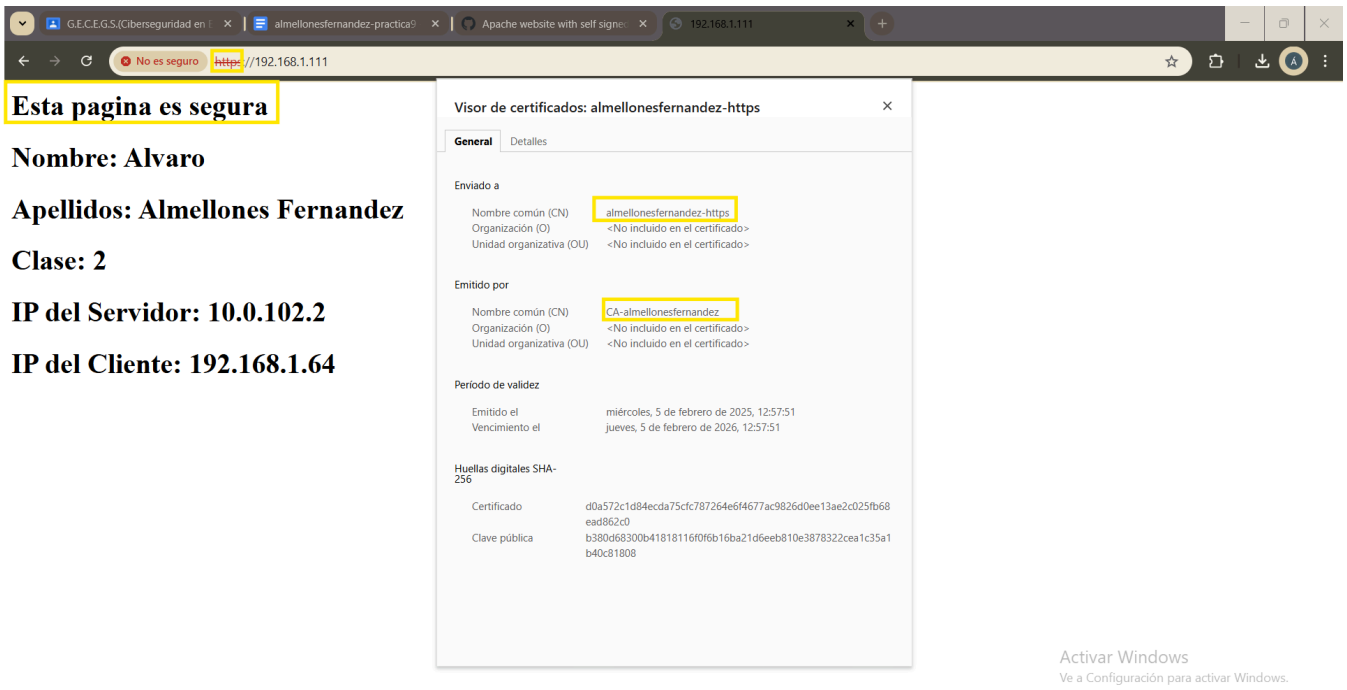
- Iptraf-ng en el lado del servidor. (0,25 pt).

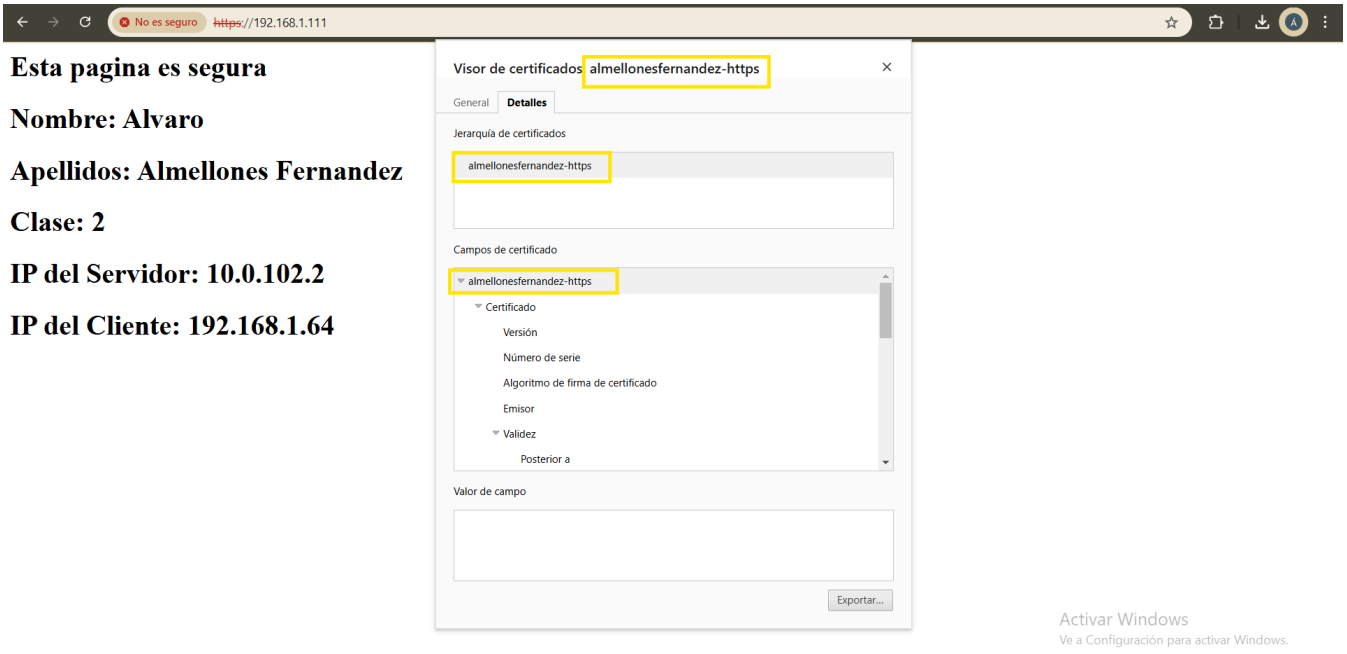
Álvaro Almellones Fernández



▪ Relacionado con https en el lado del cliente web GUI (navegador web). Evidencie que cambios ha ocurrido en su navegador. ¿Por qué dice que no es seguro, si hemos tenido que aceptar una llave pública? (0,25 pt).

Álvaro Almellones Fernández





Te sigue indicando que no es seguro porque la CA que hemos creado propia , el navegador no la reconoce como una CA segura ya que no se encuentra en las predeterminadas del navegador, pero la conexión es segura ya que está cifrada

f) Conexión desde terminal del servidor DMZ (wget,curl) en modo comando de la descarga tanto del 80 y 443 por localhost. ¿Qué ha ocurrido con el certificado público ahora? (0,25 pt).

Álvaro Almellones Fernández

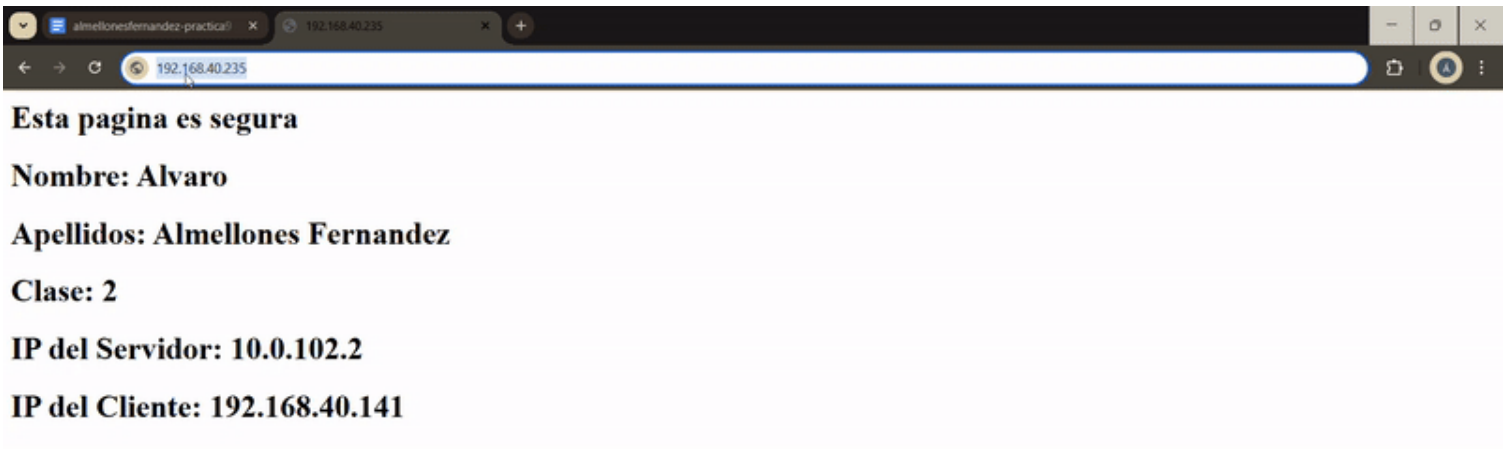
```
root@almellonesfernandez-us-dmz:/# echo "resultado http: " && echo "" && curl localhost:80 &&echo ""&& echo "resul
tado https:" && echo "" && curl localhost:443
resultado http:

<h1>Esta pagina no es segura </h1><h1>Nombre: Alvaro </h1><h1>Apellidos: Almellones Fernandez</h1><h1>Clase: 2</h1
><h1>IP del Servidor: ::1</h1><h1>IP del Cliente: ::1</h1>
resultado https:

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Reason: You're speaking plain HTTP to an SSL-enabled server port.<br />
 Instead use the HTTPS scheme to access this URL, please.<br />
</p>
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 127.0.1.1 Port 443</address>
</body></html>
root@almellonesfernandez-us-dmz:/#
```

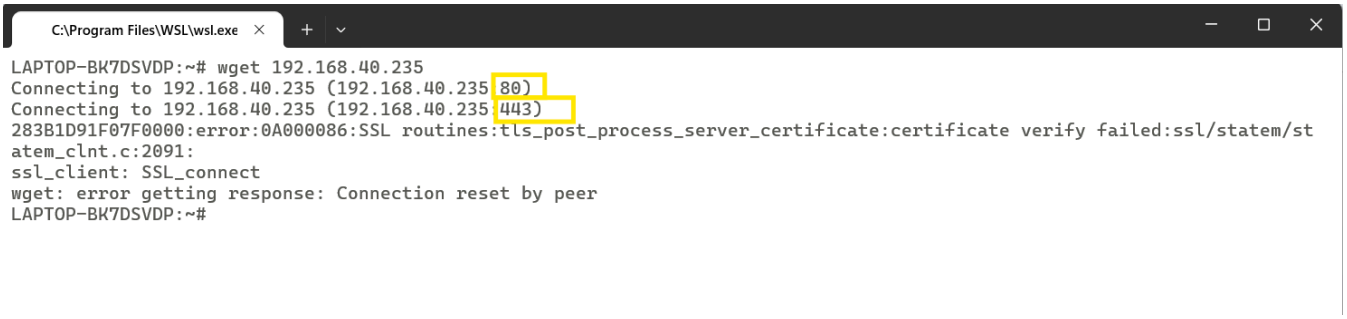
g) Realice cambios en el fichero de configuración del servidor apache para qué lo que llegue por el puerto 80, sea redireccionado automáticamente al puerto 443. Demuestre que funciona correctamente y demuestre que funciona correctamente. (0,50 pt).

He cambiado de ip porque he realizado este apartado en clase

```
  GNU nano 7.2                                 000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        Redirect permanent / https://192.168.40.235/
        # 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

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

Álvaro Almellones Fernández





Álvaro Almellones Fernández

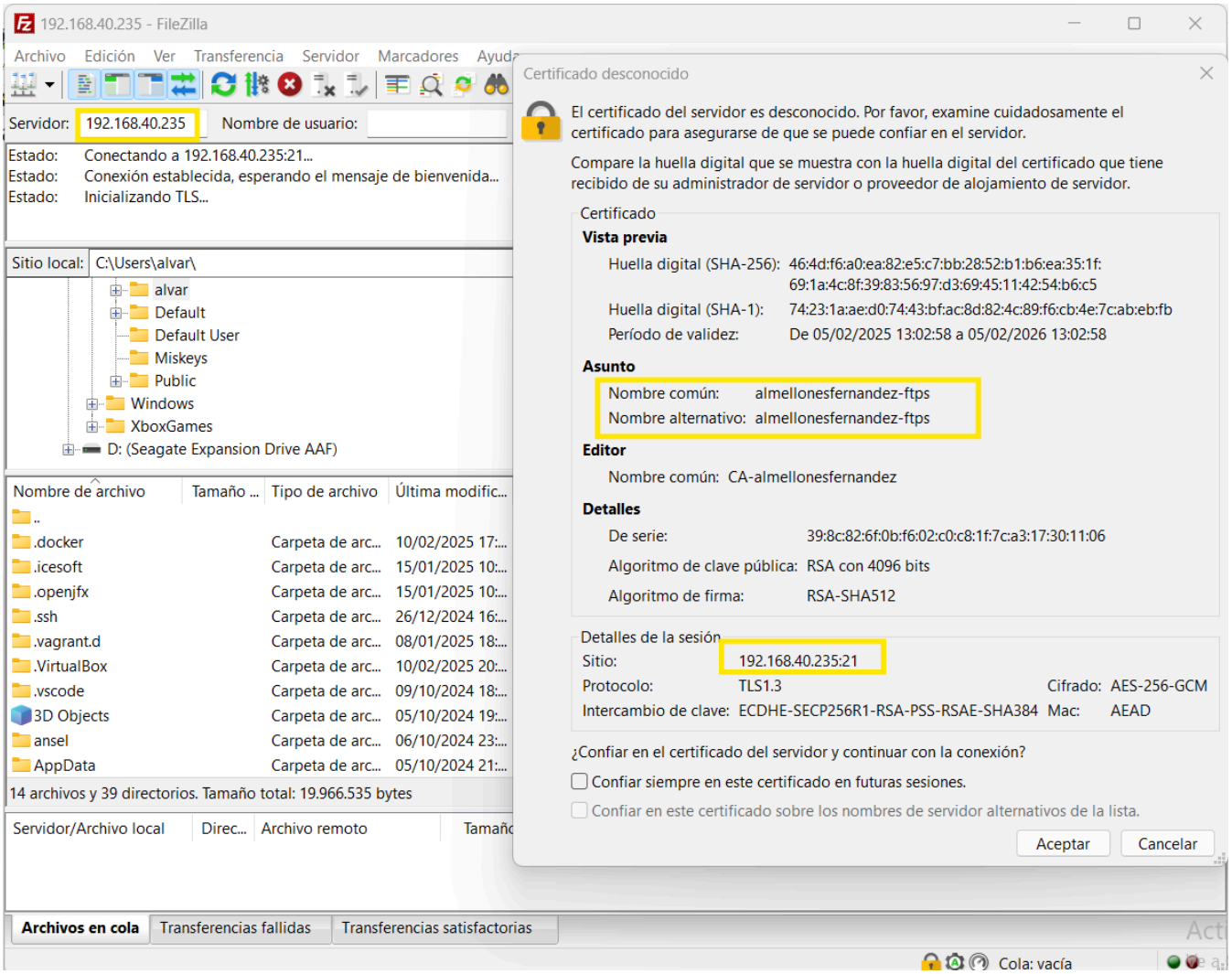
6. (1 punto) (FTPS) Configuración del servidor FTP ubicado en la zona DMZ (10.0.?.2) para que las conexiones establecidas se hagan de forma segura (ftps). Se deja al alumno que evidencie con las capturas que desee, pero deben parecerse mucho a las usadas en el ejercicio número 5 para https.

```
root@almellonesfernandez-us-dmz:/home/almellonesfernandez# netstat -putan |grep ftp
tcp6       0      0 :::21                   :::*                    LISTEN      810/vsftpd
root@almellonesfernandez-us-dmz:/home/almellonesfernandez#
```

```
root@almellonesfernandez-us-dmz:/home/almellonesfernandez# ls /etc/ssl/certs/ | grep ftps
almellonesfernandez-ftps.crt
root@almellonesfernandez-us-dmz:/home/almellonesfernandez# ls /etc/ssl/private/ | grep ftps
almellonesfernandez-ftps.key
root@almellonesfernandez-us-dmz:/home/almellonesfernandez# ls /etc/ssl/certs/ | grep ca
Actalis_Authentication_Root_CA.pem
Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.pem
ca6e4ad9.0
ca-certificates.crt
ca.crt
COMODO_Certification_Authority.pem
COMODO_ECC_Certification_Authority.pem
COMODO_RSA_Certification_Authority.pem
```

```
  GNU nano 7.2                                /etc/vsftpd.conf
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty.  Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
#ssl_enable=NO

rsa_cert_file=/etc/ssl/certs/almellonesfernandez-ftps.crt
rsa_private_key_file=/etc/ssl/private/almellonesfernandez-ftps.key
ssl_enable=YES
force_local_logins_ssl=YES
force_local_data_ssl=YES

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

Álvaro Almellones Fernández




```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 27 packets, 3864 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REDIRECT   6    --  lan2   *       172.16.102.0/24      0.0.0.0/0            tcp dpt:80 redir ports 31
28
    0     0 REDIRECT   6    --  wlan2  *       192.168.102.0/24     0.0.0.0/0            tcp dpt:80 redir ports 31
29
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.102.2:
80
   72  3744 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21 to:10.0.102.2:
21
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.102.2
:443
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8080 to:10.0.102.
2:8080
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8404 to:10.0.102.
2:8404
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej NATP *
/ to:10.0.102.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 72 packets, 3744 bytes)
```

Álvaro Almellones Fernández

```
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:123
    0     0 DROP       6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.3         0.0.0.0/0
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:123
    0     0 DROP       6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.4         0.0.0.0/0
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:123
    0     0 DROP       6    --  lan2   wan2    172.16.102.5         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.5         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.5         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.5         0.0.0.0/0
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.5         0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
 /* Respuesta WAN a LAN */
    0     0 DROP       6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  wlan2  wan2    192.168.102.2        0.0.0.0/0
    0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
 /* Respuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
   72  3744 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:21
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:8080
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:8404
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
   51  5165 ACCEPT     0    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
```



```
root@almellonesfernandez-us-dmz:/# netstat -putan |grep ESTABLISHED |grep ftp
tcp6       0      0 10.0.102.2:21           192.168.1.64:58717      ESTABLISHED 1775/vsftpd
root@almellonesfernandez-us-dmz:/#
```

```
root@almellonesfernandez-us-dmz:/# tcpdump port 21 -A
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:44:38.103673 IP 192.168.1.64.58730 > almellonesfernandez-us-dmz.ftp: Flags [S], seq 2307408771, win 64240, opti
ons [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4.V@.......@
.f..j....C.......................
22:44:38.103713 IP almellonesfernandez-us-dmz.ftp > 192.168.1.64.58730: Flags [S.], seq 1133972389, ack 2307408772
, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
E..4..@.@...
.f....@...jC.....C.....2.............
22:44:38.104290 IP 192.168.1.64.58730 > almellonesfernandez-us-dmz.ftp: Flags [.], ack 1, win 513, length 0
E..(.W@.......@
.f..j....C.C...P...z........
22:44:38.106420 IP almellonesfernandez-us-dmz.ftp > 192.168.1.64.58730: Flags [P.], seq 1:21, ack 1, win 502, leng
th 20: FTP: 220 (vsFTPd 3.0.5)
E..<.o@.@..b
.f....@...jC.....C.P...2...220 (vsFTPd 3.0.5)

22:44:38.107137 IP 192.168.1.64.58730 > almellonesfernandez-us-dmz.ftp: Flags [P.], seq 1:11, ack 21, win 513, len
gth 10: FTP: AUTH TLS
E..2.X@.......@
.f..j....C.C...P...j...AUTH TLS

22:44:38.107158 IP almellonesfernandez-us-dmz.ftp > 192.168.1.64.58730: Flags [.], ack 11, win 502, length 0
E..(.p@.@..u
.f....@...jC.....C.P...2...
22:44:38.107257 IP almellonesfernandez-us-dmz.ftp > 192.168.1.64.58730: Flags [P.], seq 21:52, ack 11, win 502, le
ngth 31: FTP: 234 Proceed with negotiation.
```

Álvaro Almellones Fernández

Álvaro Almellones Fernández

7. (1 punto) (APACHE CON AUTENTIFICACIÓN DE LOS CLIENTES MEDIANTE CERTIFICADOS) Configuración adicional en el servidor Apache en zona DMZ, para que los diferentes clientes que quieran ver contenidos del servidor web, les obligue el servidor a tener que autentificarse con el certificado de clientes generados en el apartado número 4. Se deja al alumno que evidencie con las capturas que necesite tanto en el lado del cliente como en el lado del servidor.

```
root@almellonesfernandez-us-dmz:/etc/apache2/sites-available# cat default-ssl.conf
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost
                DocumentRoot /var/www/htmls
                # 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/ssl/certs/almellonesfernandez-https.crt
                SSLCertificateKeyFile /etc/ssl/private/almellonesfernandez-https.key
                #SSLCACertificateFile /etc/ssl/certs/ca.cert
                SSLCACertificateFile /etc/ssl/certs/ca.crt
                #   Server Certificate Chain:
                #   Point SSLCertificateChainFile at a file containing the
```



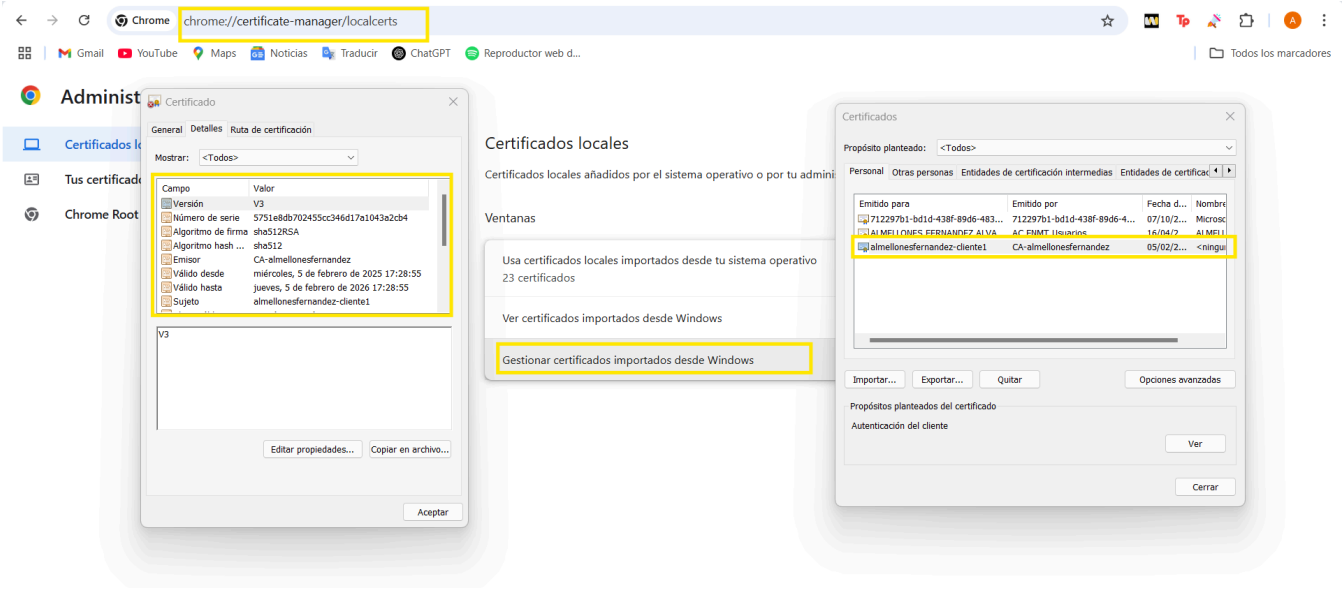
```
                #   certificate chain for the server certificate. Alternatively
                #   the referenced file can be the same as SSLCertificateFile
                #   when the CA certificates are directly appended to the server
                #   certificate for convinience.
                #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
                #   Certificate Authority (CA):
                #   Set the CA certificate verification path where to find CA
                #   certificates for client authentication or alternatively one
                #   huge file containing all of them (file must be PEM encoded)
                #   Note: Inside SSLCACertificatePath you need hash symlinks
                #               to point to the certificate files. Use the provided
                #               Makefile to update the hash symlinks after changes.
#               SSLCACertificatePath /etc/ssl/certs/
                #   Certificate Revocation Lists (CRL):
                #   Set the CA revocation path where to find CA CRLs for client
                #   authentication or alternatively one huge file containing all
                #   of them (file must be PEM encoded)
                #   Note: Inside SSLCARevocationPath you need hash symlinks
                #               to point to the certificate files. Use the provided
                #               Makefile to update the hash symlinks after changes.
                #SSLCARevocationPath /etc/apache2/ssl.crl/
                #SSLCARevocationFile /etc/apache2/ssl.crl/ca-bundle.crl
                #   Client Authentication (Type):
                #   Client certificate verification type and depth.  Types are
                #   none, optional, require and optional_no_ca.  Depth is a
                #   number which specifies how deeply to verify the certificate
                #   issuer chain before deciding the certificate is not valid.
                SSLVerifyClient require
                SSLVerifyDepth  2
                #   SSL Engine Options:
                #   Set various options for the SSL engine.
                #   o FakeBasicAuth:
```

Álvaro Almellones Fernández

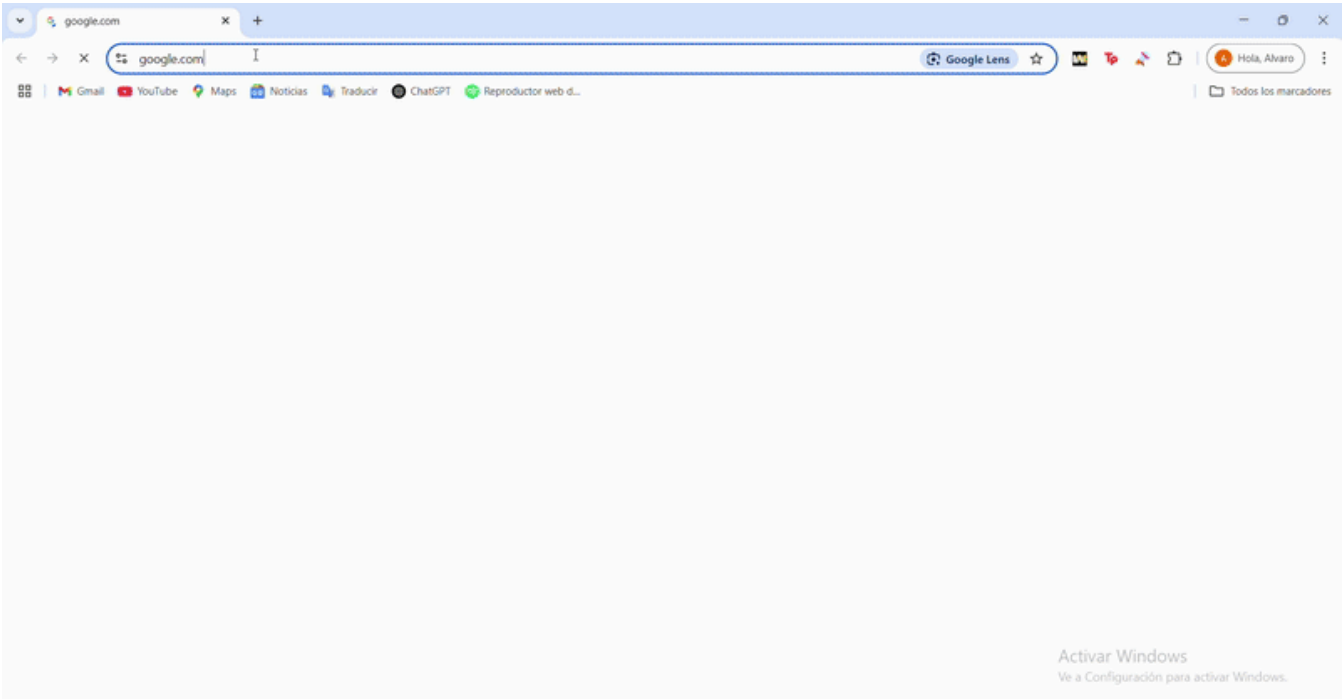
```
root@almellonesfernandez-firewall:~/keys/client/keys# openssl pkcs12 -export -out cliente.p12 -inkey almellonesfer
nandez-cliente1.key -in almellonesfernandez-cliente1.crt -certfile ca.crt
```

```
root@almellonesfernandez-firewall:~/keys/client/keys# ls
almellonesfernandez-cliente1.crt  almellonesfernandez-cliente2.crt  ca.crt       ta.key
almellonesfernandez-cliente1.key  almellonesfernandez-cliente2.key  cliente.p12
root@almellonesfernandez-firewall:~/keys/client/keys#
```

Para poder usar un certificado para autenticación con las keys que he creado en los buscadores he tenido que usar el siguiente comando para "fusionar" los tres archivos en uno con formato que permite navegadores como Chrome



Importamos la key formato.p12 a nuestro windows y dentro de la ruta de chrome de arriba podemos importarla



Álvaro Almellones Fernández

Y al intentar acceder te pide añadir un certificado, usamos el que hemos importado y ya podremos acceder al servidor

Álvaro Almellones Fernández

8. (1 punto) (REVOCACIÓN DE CERTIFICADOS). Revoque el certificado de cliente número dos con contraseña, realice todos los cambios oportunos que deba realizar y evidencie que este cliente ya no puede hacer autentificarse en el servidor apache.

```
root@almellonesfernandez-PKI-intranet /etc/openvpn/easy-rsa# ./easyrsa revoke almellonesfernandez-cliente2
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)

WARNING
=======
This process is destructive!

These files will be MOVED to the 'revoked' sub-directory:
* /etc/openvpn/easy-rsa/pki/issued/almellonesfernandez-cliente2.crt
* /etc/openvpn/easy-rsa/pki/private/almellonesfernandez-cliente2.key
* /etc/openvpn/easy-rsa/pki/reqs/almellonesfernandez-cliente2.req

These files will be DELETED:
All PKCS files for commonName : almellonesfernandez-cliente2

The inline credentials files:
* /etc/openvpn/easy-rsa/pki/almellonesfernandez-cliente2.creds
* /etc/openvpn/easy-rsa/pki/inline/almellonesfernandez-cliente2.inline

The duplicate certificate:
* /etc/openvpn/easy-rsa/pki/certs_by_serial/AE65F09B2E383360F04627D308F82535.pem

Please confirm that you wish to revoke the certificate
with the following subject:

  subject=
    commonName                = almellonesfernandez-cliente2
```



```
  serial-number: AE65F09B2E383360F04627D308F82535

  Reason: None given

Type the word 'yes' to continue, or any other input to abort.
    Continue with revocation: yes

Using configuration from /etc/openvpn/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Revoking Certificate AE65F09B2E383360F04627D308F82535.
Database updated

Notice
------
                    * IMPORTANT *

Revocation was successful. You must run 'gen-crl' and upload
a new CRL to your infrastructure in order to prevent the revoked
certificate from being accepted.

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ./easyrsa gen-crl
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/easy-rsa/vars

Using SSL:
* openssl OpenSSL 3.0.13 30 Jan 2024 (Library: OpenSSL 3.0.13 30 Jan 2024)
Using configuration from /etc/openvpn/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:

Notice
------
An updated CRL has been created:
* /etc/openvpn/easy-rsa/pki/crl.pem

root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa#
```

```
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# ls pki/ | grep crl.pem
crl.pem
root@almellonesfernandez-PKI-intranet:/etc/openvpn/easy-rsa# openssl crl -in pki/crl.pem -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN = CA-almellonesfernandez
        Last Update: Feb 11 00:35:23 2025 GMT
        Next Update: Aug 10 00:35:23 2025 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:6E:1C:72:02:5B:38:BE:8E:DB:76:D6:F5:DB:59:9D:7B:46:AF:4B:44
                DirName:/CN=CA-almellonesfernandez
                serial:20:4D:C7:E2:E4:E2:BF:CC:C2:04:E7:69:FD:AB:B1:8A:61:7B:8A:24
Revoked Certificates:
    Serial Number: AE65F09B2E383360F04627D308F82535
        Revocation Date: Feb 11 00:32:12 2025 GMT
    Signature Algorithm: sha512WithRSAEncryption
    Signature Value:
        5c:cf:d5:55:7c:15:93:74:ec:77:0c:90:49:76:31:c9:2c:48:
        ed:4a:a2:0d:10:fb:77:e4:81:e3:ed:24:e4:14:82:a6:93:ae:
        e6:83:a2:97:55:c6:a2:86:c5:55:26:30:68:42:71:c7:b7:0e:
        40:8a:a5:7e:ab:37:5f:b8:28:32:73:7a:e1:4f:89:e6:4f:05:
        94:19:14:f7:0c:b2:b5:02:5d:71:5c:a2:1f:ce:d3:ea:3b:82:
        e0:0b:23:a3:cc:02:b3:96:bf:80:a5:cd:80:2f:ba:b0:d9:ed:
        25:72:a4:cf:9f:4a:27:8b:78:6e:23:c0:25:44:71:49:01:ca:
        0f:0e:1d:c2:3b:80:5b:b5:cf:3a:a1:37:d3:d6:16:b4:a2:73:
        c4:59:23:8e:b5:b3:d0:1e:d9:e5:b8:0d:ac:59:51:ef:1b:c0:
        1a:3c:e9:71:60:e1:33:fa:66:3d:94:3b:b3:9f:84:97:87:9a:
        36:2e:69:d4:4e:8b:3e:26:ed:f7:fb:86:b0:19:05:5e:63:1d:
        66:2c:29:8c:aa:0f:3b:c7:65:cd:f5:37:eb:4f:70:c8:9b:94:
        18:5b:45:66:2d:ab:bf:f9:6a:31:7a:95:5b:92:fe:c4:5c:da:
```



```
root@almellonesfernandez-us-dmz:/etc/apache2/sites-available# cat default-ssl.conf | grep crl.pem
                SSLCARevocationFile /etc/ssl/crl.pem
                #SSLCARevocationFile /etc/ssl/crl/crl.pem
root@almellonesfernandez-us-dmz:/etc/apache2/sites-available# ls /etc/ssl |grep crl
crl
crl.pem
root@almellonesfernandez-us-dmz:/etc/apache2/sites-available#
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-us-dmz:/home/almellonesfernandez/client/keys# wget --no-check-certificate --certificate=a
lmellonesfernandez-cliente2.crt --private-key=almellonesfernandez-cliente2.key https://localhost
--2025-02-11 11:29:01--  https://localhost/
Enter PEM pass phrase:
Resolving localhost (localhost)... 127.0.0.1
Connecting to localhost (localhost)|127.0.0.1|:443... connected.
WARNING: cannot verify localhost's certificate, issued by ‘CN=CA-almellonesfernandez’:
  Self-signed certificate encountered.
WARNING: no certificate subject alternative name matches
        requested host name ‘localhost’.
HTTP request sent, awaiting response... No data received.
Retrying.

--2025-02-11 11:29:06--  (try: 2)  https://localhost/
Connecting to localhost (localhost)|127.0.0.1|:443... connected.
WARNING: cannot verify localhost's certificate, issued by ‘CN=CA-almellonesfernandez’:
  Self-signed certificate encountered.
WARNING: no certificate subject alternative name matches
        requested host name ‘localhost’.
HTTP request sent, awaiting response... No data received.
Retrying.

^X^C
root@almellonesfernandez-us-dmz:/home/almellonesfernandez/client/keys#
```

```
root@almellonesfernandez-us-dmz:/home/almellonesfernandez/client/keys# tail -f /var/log/apache2/error.log
[Tue Feb 11 11:11:13.370586 2025] [ssl:warn] [pid 4314] AH01909: 127.0.1.1:443:0 server certificate does NOT inclu
de an ID which matches the server name
[Tue Feb 11 11:11:13.378394 2025] [mpm_prefork:notice] [pid 4314] AH00163: Apache/2.4.58 (Ubuntu) OpenSSL/3.0.13 c
onfigured -- resuming normal operations
[Tue Feb 11 11:11:13.378420 2025] [core:notice] [pid 4314] AH00094: Command line: '/usr/sbin/apache2'
[Tue Feb 11 11:26:51.145588 2025] [ssl:error] [pid 4317] [client 127.0.0.1:41936] AH02039: Certificate Verificatio
n: Error (23): certificate revoked
[Tue Feb 11 11:27:38.897406 2025] [ssl:error] [pid 4319] [client 127.0.0.1:49648] AH02039: Certificate Verificatio
n: Error (23): certificate revoked
[Tue Feb 11 11:27:39.914007 2025] [ssl:error] [pid 4320] [client 127.0.0.1:49656] AH02039: Certificate Verificatio
n: Error (23): certificate revoked
[Tue Feb 11 11:27:41.931664 2025] [ssl:error] [pid 4316] [client 127.0.0.1:49664] AH02039: Certificate Verificatio
n: Error (23): certificate revoked
[Tue Feb 11 11:29:05.233373 2025] [ssl:error] [pid 4318] [client 127.0.0.1:53374] AH02039: Certificate Verificatio
n: Error (23): certificate revoked
[Tue Feb 11 11:29:06.247961 2025] [ssl:error] [pid 4317] [client 127.0.0.1:53378] AH02039: Certificate Verificatio
n: Error (23): certificate revoked
[Tue Feb 11 11:30:15.673172 2025] [ssl:error] [pid 4316] [client 192.168.1.64:50323] AH02039: Certificate Verifica
tion: Error (23): certificate revoked
```