Álvaro Almellones Fernández

PRÁCTICA 11
VPN. VPN ENTRE SEDES GEOGRÁFICAMENTE SEPARADAS.

Antes de empezar con el ejercicio, debe tener en cuenta que las reglas de iptables y de configuración del servidor tienen que ir apareciendo poco a poco, no vale ponerlas y ejecutarlas al principio del ejercicio. No se corregirá la práctica si se realiza esto. Use funciones tipo (vpn-general, vpn-lan, vpn dmz, vpn-wan, según corresponda).

INSTALACIÓN DE SERVIDOR VPN

1. **(1 punto)** Realice la instalación del servidor VPN en el servidor firewall en la red 172.18.?.0, usando certificados creados en práctica de PKI, CA, y usando como nombre del dispositivo tun-XX (donde Xx, alias que queráis). Ejemplo (tun-cova), que una vez conectado será tun-cova-0. Evidencie.

a. Configuración del fichero server.conf mínima, no mostrando comentarios, para que sea más elegible su contenido.

```
root@almellonesfernandez-firewall:/etc/openvpn/server# grep -vE '^\s*[#;]' server.conf

port 1194

proto udp

dev tun2


ca /etc/openvpn/server/servervpn/ca.crt
cert /etc/openvpn/server/servervpn/almellonesfernandez-vpn.crt
key /etc/openvpn/server/servervpn/almellonesfernandez-vpn.key

dh none

data-ciphers-fallback AES-256-CBC

topology subnet

server 172.18.102.0 255.255.255.0

ifconfig-pool-persist /var/log/openvpn/ipp.txt




push "redirect-gateway local def1"
```

Álvaro Almellones Fernández

```
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 192.168.40.1"




persist-key
persist-tun

status /var/log/openvpn/openvpn-status.log


verb 3


root@almellonesfernandez-firewall:/etc/openvpn/server#
```

No me dejaba poner mis apellidos enteros a la tarjeta tun, he decidido poner mi número para así también tener esta tarjeta de red igual que las otras (wan2,lan2,etc..)

b. Servido arrancando y escuchando por tarjeta tun-XX0.

```
root@almellonesfernandez-firewall:/etc/openvpn/server# openvpn --config server.conf
2025-02-22 18:59:21 Note: --data-ciphers-fallback with cipher 'AES-256-CBC' disables data channel offload.
2025-02-22 18:59:21 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-22 18:59:21 library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 2.10
2025-02-22 18:59:21 DCO version: N/A
2025-02-22 18:59:21 WARNING: --keepalive option is missing from server config
2025-02-22 18:59:21 net_route_v4_best_gw query: dst 0.0.0.0
2025-02-22 18:59:21 net_route_v4_best_gw result: via 192.168.1.1 dev wan2
2025-02-22 18:59:21 NOTE: your local LAN uses the extremely common subnet address 192.168.0.x or 192.168.1.x.  Be aware that this might create routing conflicts if you connect to the VPN server from public locations such as internet cafes that use the same subnet.
2025-02-22 18:59:21 TUN/TAP device tun2 opened
2025-02-22 18:59:21 net_iface_mtu_set: mtu 1500 for tun2
2025-02-22 18:59:21 net_iface_up: set tun2 up
2025-02-22 18:59:21 net_addr_v4_add: 172.18.102.1/24 dev tun2
2025-02-22 18:59:21 Could not determine IPv4/IPv6 protocol. Using AF_INET
2025-02-22 18:59:21 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-02-22 18:59:21 UDPv4 link local (bound): [AF_INET][undef]:1194
2025-02-22 18:59:21 UDPv4 link remote: [AF_UNSPEC]
2025-02-22 18:59:21 MULTI: multi_init called, r=256 v=256
2025-02-22 18:59:21 IFCONFIG POOL IPv4: base=172.18.102.2 size=253
2025-02-22 18:59:21 IFCONFIG POOL LIST
2025-02-22 18:59:21 Initialization Sequence Completed
```

```
root@almellonesfernandez-firewall:/etc/netplan# netstat -putan |grep 1194
root@almellonesfernandez-firewall:/etc/netplan# ifconfig |grep tun2
root@almellonesfernandez-firewall:/etc/netplan# netstat -putan |grep 1194
udp        0      0 0.0.0.0:1194            0.0.0.0:*                           12006/openvpn
root@almellonesfernandez-firewall:/etc/netplan# ifconfig |grep tun2
tun2: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
root@almellonesfernandez-firewall:/etc/netplan#
```

Como podemos observar antes de ejecutar el comando no aparece la conexión por el puerto 1194 ni aparece la tun2 en el momento que ejecutamos el comando aparece.

c. Configuración del cortafuegos mínima para que el servidor escuche por la tarjeta wan. Muestre que los contadores de la regla iptables están inicializadas.

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:~/scripts# iptables -L -n -v --line-number
Chain INPUT (policy DROP 5 packets, 160 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
2       47  3000 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde WAN */
3        1    28 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           /* Permitir ping desde cualquier subred *
/
4        0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde LAN */
5        0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde DMZ */
6        0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3128 /* Zona LAN */
7        0     0 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3129 /* Zona WLAN */
8        0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED /* Respuestas O
UTPUT */
9        0     0 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194 /* Permitir el puerto que us
a VPN */
```

Por ahora solo he puesto la regla que permite que funcione VPN y se iran añadiendo las siguientes reglas poco a poco

d. Nmap donde se observe que el servidor firewall tiene el puerto abierto UDP.

```
alvaro@LAPTOP-BK7DSVDP:~$ sudo nmap -sU -p 1194 192.168.1.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-22 19:14 CET
Nmap scan report for 192.168.1.108
Host is up (0.00067s latency).

PORT     STATE SERVICE
1194/udp open  openvpn

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
alvaro@LAPTOP-BK7DSVDP:~$
```

Álvaro Almellones Fernández

CLIENTE VPN – TO – SERVER VPN

2. **(1,5 puntos)** Conexión **desde cliente LINUX** usando comando openvpn y del fichero .ovpn con el certificado cliente.crt sin contraseña, **del cliente número 1** creado en nuestra CA. Se debe mostrar como mínimo las siguientes capturas.

a. Fichero de configuración del fichero clienteXXxx1.ovpn, donde se demuestre que ha sido creado por vuestra entidad certificadora.

```
  GNU nano 7.2                          almellonesfernandez-cliente1.ovpn
client
dev tun2
proto udp
remote 192.168.1.108 1194
resolv-retry infinite
nobind
persist-key
persist-tun
cipher AES-256-CBC
verb 3

<ca>
-----BEGIN CERTIFICATE-----
MIIFbDCCA1SgAwIBAgIUIE3H4uTiv8zCBOdp/auximF7iiQwDQYJKoZIhvcNAQEN
BQAwITEfMB0GA1UEAwwWQ0EtYWxtZWxsb25lc2Zlcm5hbmRlejAeFw0yNTAyMDUx
MTMwNDNaFw0yNzAyMDUxMTMwNDNaMCExHzAdBgNVBAMMFkNBLWFsbWVsbG9uZXNm
ZXJuYW5kZXowggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCLlgPeB4Ww
6XIUzqdxjjKkJBfwrRdAQEcjOJrUK49Bs1K1EqRwyjiPEK1Dq6eWZso3ryh9f6ld
AeXf1J8Xq6qjQDLHVLqzev11Lf82Yfs4UXn2EVTtdxzbAOoOX5/D63RIM+aciE7z
RttUJQjzyZiqR0/VOb5EWqlirEm6U9lbVcK2rdr3+p6Kg27lQJNtnISzSaBJc7B7
fIrDuXXGExbrpPgYuUQAu5mLo7PAs3dXkizBOVfFDQy6uMRL8K6MGZDLjpgf/FDY
ft2LrBs3zUy75b0OeDEQKzB3JT3hkm4rcll1aFQPfvJHVkAlIUYfU7+ZzlHJXK7T
iK7tZmmIusTRghpCF35oTtkibi7HAOjSF/Qn1f9FNADr3z2bEz2N8USA61laVGWw
IAmaBz8BLhz0NV8T9DSYRfcJYwbMzNrnx3VUr1y0ddepJfERFBAo4mtIeVG0Ba3k
QOrqWZdlnkf2omPK/rwNldsFqknnGqCB9/yfhbzdbc1Ia8QCkck7lylzapqTpSs0
KWmH2sR5yVNouksyFawX6wlepmA879R157gDOUWjmfP4yrfFoJDSUt0im0cktvfJ
1ebuaWvA/BoVe97pgRoFLXBi7apXy2taVD2Ncmel+s/4AAy9hgFpL0/n/BzdmiaV
vaMIt3jfwckrBkyIJEK9Z50N8UwgfEoi4QIDAQABo4GbMIGYMAwGA1UdEwQFMAMB
                                                [ 229 líneas leídas ]
```

```
<ca>
-----BEGIN CERTIFICATE-----
MIIFbDCCA1SgAwIBAgIUIE3H4uTiv8zCBOdp/auximF7iiQwDQYJKoZIhvcNAQEN
BQAwITEfMB0GA1UEAwwWQ0EtYWxtZWxsb25lc2Zlcm5hbmRlejAeFw0yNTAyMDUx
MTMwNDNaFw0yNzAyMDUxMTMwNDNaMCExHzAdBgNVBAMMFkNBLWFsbWVsbG9uZXNm
ZXJuYW5kZXowggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCLlgPeB4Ww
6XIUzqdxjjKkJBfwrRdAQEcjOJrUK49Bs1K1EqRwyjiPEK1Dq6eWZso3ryh9f6ld
AeXf1J8Xq6qjQDLHVLqzev11Lf82Yfs4UXn2EVTtdxzbAOoOX5/D63RIM+aciE7z
RttUJQjzyZiqR0/VOb5EWqlirEm6U9lbVcK2rdr3+p6Kg27lQJNtnISzSaBJc7B7
fIrDuXXGExbrpPgYuUQAu5mLo7PAs3dXkizBOVfFDQy6uMRL8K6MGZDLjpgf/FDY
ft2LrBs3zUy75b0OeDEQKzB3JT3hkm4rcll1aFQPfvJHVkAlIUYfU7+ZzlHJXK7T
iK7tZmmIusTRghpCF35oTtkibi7HAOjSF/Qn1f9FNADr3z2bEz2N8USA61laVGWw
IAmaBz8BLhz0NV8T9DSYRfcJYwbMzNrnx3VUr1y0ddepJfERFBAo4mtIeVG0Ba3k
QOrqWZdlnkf2omPK/rwNldsFqknnGqCB9/yfhbzdbc1Ia8QCkck7lylzapqTpSs0
KWmH2sR5yVNouksyFawX6wlepmA879R157gDOUWjmfP4yrfFoJDSUt0im0cktvfJ
1ebuaWvA/BoVe97pgRoFLXBi7apXy2taVD2Ncmel+s/4AAy9hgFpL0/n/BzdmiaV
vaMIt3jfwckrBkyIJEK9Z50N8UwgfEoi4QIDAQABo4GbMIGYMAwGA1UdEwQFMAMB
Af8wHQYDVR0OBBYEFG4ccgJbOL6O23bW9dtZnXtGr0tEMFwGA1UdIwRVMFOAFG4c
cgJbOL6O23bW9dtZnXtGr0tEoSWkIzAhMR8wHQYDVQQDDBZDQS1hbG1lbGxvbmVz
ZmVybmFuZGV6ghQgTcfi5OK/zMIE52n9q7GKYXuKJDALBgNVHQ8EBAMCAQYwDQYJ
KoZIhvcNAQENBQADggIBAGAo9q5jSsdkJA5EXc1iY4tZoevpzcGpHPpcAGhE3xL4
paK0ivFDZNhaLppYqF6uHzOXpYXkdIbGkOtsPHFKzngB8QSqD2+poulGCgCSqgvC
gMFAYfj2QaQFQs9JxekztO2lB9H6bUsTZux4yr10GVQZ/ld+sTH0ZhSWz+5wj2h4
pPz70pVz2modLg3+WD7qyoLqQcZQOpv43W0zcxnKGVNJedPPrDVqhZFgoTL0Y++v
jmh0UVKUc5LdeeQe7IxIfPS8OCVIWNIRlhi7zErg3HDFlp6d6KmE0vxFT/hNdaB0
2AuUPISaWRENxqjB2Lux6trqJKb4slh4eBcpMS44pJ6GKfTwl1qUJoGWoSVsCSlL
Fco2ojeuPCcR5HJk+dPXCD8QgHCQF28pEGSd3W+FXVNnaYmOOdlJpTjG2Az+3hep
/K+jaglhttfo/9Lblhho3HgNBTepL4zMPBtAJqhCPZhPT9uSRpx7BrrURzAhy/ME
HilmatO8spb7QYTsQFkZufzrexjX7ZFoF8c/SWic1uB4jrHNl9ij1wEMER7xWKoG
07xrZoRXtvz2Qn6yEGj+O+Rc1YylCdyHMbM1HO7ic/41HjeaQgHVgNiedp7ZzhBn
wtMD6MZc2Dd21jAgeJhRkI60bh9ebUZ2IL1KmirzzhJfU0stCtqgBv7pC/rYFV+d
-----END CERTIFICATE-----
</ca>
```

Álvaro Almellones Fernández

```
<cert>
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:
```

```
       5C:74:46:24:A5:E4:9D:61
-----BEGIN CERTIFICATE-----
MIIFgDCCA2igAwIBAgIQV1Ho23AkVcw0bRehBDostDANBgkqhkiG9w0BAQ0FADAh
MR8wHQYDVQQDDBZDQS1hbG1lbGxvbmVzZmVybmFuZGV6MB4XDTI1MDIwNTE2Mjg1
NVoXDTI2MDIwNTE2Mjg1NVowJzElMCMGA1UEAwwcYWxtZWxsb25lc2Zlcm5hbmRl
ei1jbGllbnRlMTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALWI5tFK
ganz/50rb8zOdFRtZNAv/sdPpM8GnPCWVRAX2kAxKwSVQkNhVzFncutRdnQr0406
DURD0DEdZxaCQg02JczEhsv2wTCmSYzglmgil4TpXqqIcEUdSv0dWq6Kmd9Yw1RW
t82pHhZp3YI+Sg0HFcWnKD2sRLBPD/Dm5xf8ubPStKjdvgqbdmqtFRunW36x4cYk
f5ySfpevjkwu1U2mcyZXTZ2Z7DRNqW7OsYuPgIJRoMPdLfdquB7wzyN28Waejrsw
+ijmTAATm/C+kvNpzUl2sn0S0AxpqgD60gDF2CZ2PuM64KMXsEGf/LRLMXTS4JQo
htQV8LEbpn4yVZelJ8NwMnqpxSWb4HGfkgKwM8skiRsdPg6e7kA6zcuGo8XSUHeA
iOKtWrS1opwoK3Dka8eiAibiZuc7E3wzwkteyTOBl4fPZl2HEX/2pxknqPYCK8tc
6TXdnvW8aU6QBSicYUvNVEyZzlbozT5pC0wt4xuVvoZH+RFNJp49gh4NgCZdkCae
05HSELFdgFqDy8ZWE4wyw6ZDLjI4km5a7Sg7r5JHwF7EydDeiHZ6d/oxbwW1siye
tXfRSeQfcgqDBhrdAfgGTvORn6zuhvB5132Vt1HwBy4kwm2FG+x+mFKYPcZEErS8
MKn7uYvWXQ5RQx1s+Kpu3iMu165ukXkmFgulAgMBAAGjga0wgaowCQYDVR0TBAIw
ADAdBgNVHQ4EFgQUPYnWyogwgFyHCbYSOodPn5GdbbQwXAYDVR0jBFUwU4AUbhxy
Als4vo7bdtb121mde0avS0ShJaQjMCExHzAdBgNVBAMMFkNBLWFsbWVsbG9uZXNm
ZXJuYW5kZXqCFCBNx+Lk4r/MwgTnaf2rsYphe4okMBMGA1UdJQQMMAoGCCsGAQUF
BwMCMAsGA1UdDwQEAwIHgDANBgkqhkiG9w0BAQ0FAAOCAgEAidmXveRzXKksI2f7
YP6iSwRBpVyFfDLnio0fPVZ0LdRaMxwqCF1ePqcHWZFcp/poJUMgNUsholH810e/
frFaTBQ/D5iSw7fMkNee09PAp85ka/hcrfCW+2SHNsP6ZUZ0C8dW+84jHmHpdIjc
7rcDypswJOi4d+kJvxZFbiUpD72P4BlUC+sG4qp+hJROZsPz0jDaSXbLAPvMP+Ly
hjqdNj947wx9aqUt+sWWISpfozdyu3uzWNJmywV+CLG0Qud/GMJ/oF2dc2hlbyNi
Wvmifu4a1He4wFJRGSIcI7PXs9GJEBPG1pSO3aSWyXWNQD8cpRXjBNFBMN7jquxR
m7RI/ijJJXkJhCVTbli1Q4tzq9P7MKGXRVB6KOIrNPVlxgbo3TLholN9RhhB8f/f
ojA3BNGPh80Jxwjs1ifqhOS5P8AE/Z6a1HGZEMb8vEzKuqpryZ01kZRPbJv9pu4+
7N+D+IlMMwoq/uQDnhIAbgHTeP6/zvye4aKwvKRN/N7sKd6L1OHALSy9gObJSBSi
PivOopHWcuutHSt/AMx7AJKAb33+jeid87IAlhgmehuy5yQ2jlsl6ag4CMPLnVm0
TvMIzxEw+MjLFgSpJHpgQ3+xsiDbINQl9YztDhQzrQ9yTOgTs9CbIKEO7fEQE3UP
XnUzQexlIwskio1FXHRAJKXknQE=
-----END CERTIFICATE-----
</cert>
```

Álvaro Almellones Fernández

```
<key>
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQC1iObRSoGp8/+d
K2/MznRUbWTQL/7HT6TPBpzwllUQF9pAMSsElUJDYVcxZ3LrUXZ0K9ONOg1EQ9Ax
HWcWgkINNiXMxIbL9sEwpkmM4JZoIpeE6V6qiHBFHUr9HVquipnfWMNUVrfNqR4W
ad2CPkoNBxXFpyg9rESwTw/w5ucX/Lmz0rSo3b4Km3ZqrRUbp1t+seHGJH+ckn6X
r45MLtVNpnMmV02dmew0TaluzrGLj4CCUaDD3S33arge8M8jdvFmno67MPoo5kwA
E5vwvpLzac1JdrJ9EtAMaaoA+tIAxdgmdj7jOuCjF7BBn/y0SzF00uCUKIbUFfCx
G6Z+MlWXpSfDcDJ6qcUlm+Bxn5ICsDPLJIkbHT4Onu5AOs3LhqPF0lB3gIjirVq0
taKcKCtw5GvHogIm4mbnOxN8M8JLXskzgZeHz2ZdhxF/9qcZJ6j2AivLXOk13Z71
vGlOkAUonGFLzVRMmc5W6M0+aQtMLeMblb6GR/kRTSaePYIeDYAmXZAmntOR0hCx
XYBag8vGVhOMMsOmQy4yOJJuWu0oO6+SR8BexMnQ3oh2enf6MW8FtbIsnrV30Unk
H3IKgwYa3QH4Bk7zkZ+s7obwedd9lbdR8AcuJMJthRvsfphSmD3GRBK0vDCp+7mL
1l0OUUMdbPiqbt4jLteubpF5JhYLpQIDAQABAoICABF0/A9RzSTJCkJ0uCBXlS++
QlTT3LoRcl2XOvXW2xC8XnhQUhzzdocQwAgH9PDkqVG0GjipRbfUFpv2giCTv6LS
G3H0zyqjjMHvJ8EEouoaM3xsTbZz/unijoDHNx50RSZJfKUqXqwIEJTistKwx0G3
9fPHJpNBsuxKehO2PLBdlQUSJN3dTwZpm0pYYSCC6EVHeVjqzxvBKavQDczNLyVz
tXyRJi1a7TA9bKbzePbdAqRlkaJsLVyu1kxhZ2X3bPDrm/mr1M6kkNfsCtGsneiK
+tsO70ygR8H90kOcWyAIZogSVGtZENuWLlStPCmhVnzvv3l36TlRb880Q788e2b7
m2MwmWv7kqu4PivCX/+IQEIexVOOtlbNK97VVCloQ7Nk0XurWqeq0PU314419SXe
gjs/xM5e0L+LYpLHFg5ZzpB3/jYmI7BxfA+lCmGNZXMqw3xD+oVmVLDvmvyJ42c/
CYd8TkvrUx5M02G5KJD/pk39J7IcivTbgZ7ochNqK2C52WFfiZtb1ubrgTONvn4c
Z3hdoqj+SxkOS1ZMOm/dhC7n3jNQh8kcx9ww7MlFFbObl8AgVbiPzB1bngigjanD
bWQeLl+XTNXFQ2+fjRfzfSWM33a17uwIJ3Amlf1Z47CDEhUSu0c3KsxrjhRAO4sJ
7WM0M6ZP9quAaurh2MGRAoIBAQDanlFHRIW7aSqFXJPfymj9KsnAfb2K35HfjxPc
YlIQxYN3t8jVO/rK+fsDuLUfm8tbWpLlKcVwNqG7Rho+IOqpWYucu+k3B3fheQvm
37iXmCNBzF/HtvNdBQW16TT0qCaWemX011wec2PGN0eHymH6nn9KrQknIOQpa0XQ
m/9DZJTNrdU68cqeEjwdEwmLEOD0Oq0fUNQffFGMRxUMFSSRSL6NUU9AtXYB+2C8
HxnxiXua7+YuHmMaNkelj+rzuVIkswd6bVAbsEXT1KwQrw6FkNfrpJKcoaZzsszK
+VDE7s1IIz5NaQW87q8HUwNxuizetoqwApyVfPx8dxFfsiTRAoIBAQDUk0386asA
jQ8GoxAGcuFQLHEbHNRAvIXi/8F6cB2r45L0RLhstiRrhw86uObmoOWjYplNvGsB
2RXgZJCya6ZRP9WcI9jUozzPqv3H8MkzKBYFNT6y3jiY0+RgJx17J1fGcRE28xMg
Sv2y3LPs+JBCBW4UOSdo12NmWaWKYTx7ssrg3d8BpGza9rgtdmcaDqarIhvzl0W/
PKIH053PyKVWNsGHOjyLYICTK+Q/A2R+nZ+UrTmR3+hJK8D20NbqsbkbnnZgqWDb
QXFlxlk1fXj7NN1k6Kv8uTo5SnvRTxbKXDVtSGfEI7hVlHVF9JzpRZmuE8VSJJdX
F8txDi01vD6VAoIBAARj0XYA5j6RKg1rgnyn79vFlC+NVtUHEELQ+LEgOE2l6bHp
utqtTaftxSCaAOkVk8vN0c1QPWq3bh/4lGZS+uNTrP4Et/Ym7D1W1OpZ67b/kxWr
KPE1t0VS6H5ypGGVTtEOvCVifbMO1h4Q1hrf8X+61wuE1f43Jt2+DbTWrRWJW4OV
zgZU/KCX9SUQUMy+FgZRd1B9qwTG1kxe0QlhE07niwwDaff+rNP1XEfqx/aVsCm4
T4L1kT/hfybP8QPb4M5j2e6Xa1hi/cP3LU1Ydo4wDmXo9Bi5FkKUgJBC2WBa+zxL
mOCtDzRwBou7GwKZnnUKbVaDdul5jQhiy7KEPUECggEBAJOqI9GdLAl880Qj/5zL
LpK33HX+B79Udhjimq8HtMTTmCCQoB/8Qr5jGoQrL1Jj0EE329BxI1AsUZMHqLAY
MXddRXBqQlQrdLG5UQMT01/y56EEhKJR1bTr9EeKxGLpSILzxgaKwe17ylH2GBJz
9Bm4lef8b9DXVhgiC+lddFtlLqMX3LLSWj+chQInrqUeKk7UqeADZBLc9p1DNevB
sIB8FuFt5eLXzVjuc2YGYEfIDLOFxWj8xeoWN7v8BF8Rx8lUwVySLFMCWdhd+Vg7
6c9uwKA5NEehD73+bJZQPz+g4Agi9Nn+Ci2ArBpFOr6cd43B9B8EhhCc2diWBXe/
ZSUCggEBAMR5FVmjkxeLHRmSJtGButRS5DWuLlX5qWa9LXmZgKAYiWGZxQ8QBsZi
E/erZFBbaPGQU4UMY6hQU6c6BDnwngCaHtWZcSXCXcL/u2HWMBrcG4L3QrLzq828
K9YpnmSzFZ7FvfoVC04xPz6NROIC5+EIDZoYNopwBjoBKBhRmEBpM827zUMWAkdx
fTJZX4SdzSAcYisEofP1FTX46rH561D36/Z/kvVaxP0zqCqVHySdeKNcTexT99hS
+ei1ZopR1wNz6Sox2XE+aZxShv09BxukzGSIoy0YcP9nf8zPeDUJ1iKgPlZGSOUi
Yor09HCO9YE0POKfN9f4hGc/tRRfiwk=
```

El archivo .ovpn consta de la configuracion de vpn mas los archivos ca.cert, el certificado del cliente (en este caso cliente1) y la clave privada del cliente

b. Realice primera conexión con cliente openvpn y muestre movimiento de contadores de iptables (INPUT).

```
almellonesfernandez@almellonesfernandez-VirtualBox:~$ sudo openvpn --config almellonesfernandez-cliente1.ovpn
2025-02-23 17:41:12 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-02-23 17:41:12 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305). OpenVPN ignores --cipher for cipher negotiations.
2025-02-23 17:41:12 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2025-02-23 17:41:12 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-23 17:41:12 library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 2.10
2025-02-23 17:41:12 DCO version: N/A
2025-02-23 17:41:12 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.108:1194
2025-02-23 17:41:12 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-02-23 17:41:12 UDPv4 link local: (not bound)
2025-02-23 17:41:12 UDPv4 link remote: [AF_INET]192.168.1.108:1194
2025-02-23 17:41:12 TLS: Initial packet from [AF_INET]192.168.1.108:1194, sid=686ee730 990e182b
2025-02-23 17:41:12 VERIFY OK: depth=1, CN=CA-almellonesfernandez
2025-02-23 17:41:12 VERIFY KU OK
2025-02-23 17:41:12 Validating certificate extended key usage
2025-02-23 17:41:12 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-02-23 17:41:12 VERIFY EKU OK
2025-02-23 17:41:12 VERIFY OK: depth=0, CN=almellonesfernandez-vpn
2025-02-23 17:41:12 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 4096 bits RSA, signature: RSA-SHA512, peer temporary key: 253 bits X25519
2025-02-23 17:41:12 [almellonesfernandez-vpn] Peer Connection Initiated with [AF_INET]192.168.1.108:1194
2025-02-23 17:41:12 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-02-23 17:41:12 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-02-23 17:41:12 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway local def1,dhcp-option DNS 8.8.8.8,dhcp-option DNS 192.168.40.1,route-gateway 172.18.102.1,topology subnet,ifconfig 172
.18.102.2 255.255.255.0,peer-id 0,cipher AES-256-GCM,protocol-flags cc-exit tls-ekm dyn-tls-crypt,tun-mtu 1500'
2025-02-23 17:41:12 OPTIONS IMPORT: --ifconfig/up options modified
2025-02-23 17:41:12 OPTIONS IMPORT: route options modified
2025-02-23 17:41:12 OPTIONS IMPORT: route-related options modified
2025-02-23 17:41:12 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
2025-02-23 17:41:12 OPTIONS IMPORT: tun-mtu set to 1500
2025-02-23 17:41:12 net_route_v4_best_gw query: dst 0.0.0.0
2025-02-23 17:41:12 net_route_v4_best_gw result: via 192.168.1.1 dev enp0s3
2025-02-23 17:41:12 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=enp0s3 HWADDR=08:00:27:a7:51:33
2025-02-23 17:41:12 TUN/TAP device tun0 opened
2025-02-23 17:41:12 net_iface_mtu_set: mtu 1500 for tun0
2025-02-23 17:41:12 net_iface_up: set tun0 up
2025-02-23 17:41:12 net_addr_v4_add: 172.18.102.2/24 dev tun0
2025-02-23 17:41:12 net_route_v4_add: 0.0.0.0/1 via 172.18.102.1 dev [NULL] table 0 metric -1
2025-02-23 17:41:12 net_route_v4_add: 128.0.0.0/1 via 172.18.102.1 dev [NULL] table 0 metric -1
2025-02-23 17:41:12 Initialization Sequence Completed
2025-02-23 17:41:12 Data Channel: cipher 'AES-256-GCM', peer-id: 0, compression: 'lzo'
2025-02-23 17:41:12 Timers: ping-restart 120
2025-02-23 17:41:12 Protocol options: protocol-flags cc-exit tls-ekm dyn-tls-crypt
```

```
2025-02-23 17:29:10 almellonesfernandez-cliente1/192.168.1.111:56859 SENT CONTROL [almellonesfernandez-cliente1]: '
PUSH_REPLY,redirect-gateway local def1,dhcp-option DNS 8.8.8.8,dhcp-option DNS 192.168.40.1,route-gateway 172.18.10
2.1,topology subnet,ifconfig 172.18.102.2 255.255.255.0,peer-id 0,cipher AES-256-GCM,protocol-flags cc-exit tls-ekm
 dyn-tls-crypt,tun-mtu 1500' (status=1)
2025-02-23 17:29:10 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:11 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:11 almellonesfernandez-cliente1/192.168.1.111:56859 Data Channel: cipher 'AES-256-GCM', peer-id: 0
2025-02-23 17:29:11 almellonesfernandez-cliente1/192.168.1.111:56859 Protocol options: protocol-flags cc-exit tls-e
km dyn-tls-crypt
2025-02-23 17:29:11 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:11 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:12 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:12 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:12 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:12 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:13 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:13 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:13 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:13 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:14 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:14 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
2025-02-23 17:29:14 almellonesfernandez-cliente1/192.168.1.111:56859 IP packet with unknown IP version=15 seen
```



```
root@almellonesfernandez-firewall:~# sudo iptables -L -n -v
Chain INPUT (policy DROP 194 packets, 9200 bytes)
 pkts bytes target     prot opt in     out     source               destination
   12  1192 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
  770 56168 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH
 desde WAN */
   15   420 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           /* Permitir ping desde cua
lquier subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH
 desde LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH
 desde DMZ */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3128 /* Zona LAN *
/
    0     0 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3129 /* Zona WLAN
*/
  444 99059 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
/* Respuestas OUTPUT */
    8   336 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194 /* Permitir e
l puerto que usa VPN */
```

c. Ip asignadas a la tarjeta virtual del cliente linux y del servidor.

Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-VirtualBox: ~   almellonesfernandez@almellonesfernandez-VirtualBox: ~
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.111  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fea7:5133  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a7:51:33  txqueuelen 1000  (Ethernet)
        RX packets 3683  bytes 3254184 (3.2 MB)
        RX errors 0  dropped 28  overruns 0  frame 0
        TX packets 1305  bytes 181417 (181.4 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  (Bucle local)
        RX packets 365  bytes 32750 (32.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 365  bytes 32750 (32.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 172.18.102.2  netmask 255.255.255.0  destination 172.18.102.2
        inet6 fe80::baaa:45c4:cfd2:f971  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 100  bytes 5976 (5.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

almellonesfernandez@almellonesfernandez-VirtualBox:~$
```

```
tun2: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 172.18.102.1  netmask 255.255.255.0  destination 172.18.102.1
        inet6 fe80::2aaf:2652:2347:5dec  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9  bytes 432 (432.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wan2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.108  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fec3:dfc9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c3:df:c9  txqueuelen 1000  (Ethernet)
        RX packets 2417  bytes 268805 (268.8 KB)
        RX errors 0  dropped 32  overruns 0  frame 0
        TX packets 1315  bytes 187718 (187.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.102.1  netmask 255.255.255.0  broadcast 192.168.102.255
        inet6 fe80::20c:29ff:fec3:dfe7  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c3:df:e7  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 1076 (1.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@almellonesfernandez-firewall:~#
```


d. Captura de fichero del servidor donde aparece que está IP se ha asignado correctamente.

```
  GNU nano 7.2                                  /var/log/openvpn/ipp.txt
almellonesfernandez-cliente1,172.18.102.2
```

e. Tcpdump en servidor firewall vpn de la conexión vpn realizada.

```
root@almellonesfernandez-firewall:~# sudo tcpdump port 1194
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wan2, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:50:03.075279 IP 192.168.1.111.46079 > almellonesfernandez-firewall.openvpn: UDP, length 85
17:51:17.755413 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 14
17:51:17.755615 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 26
17:51:17.761972 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 303
17:51:17.766227 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 1222
17:51:17.766326 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 1222
17:51:17.766385 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 1222
17:51:17.766461 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 200
17:51:17.769306 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 26
17:51:17.769723 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 30
17:51:17.771096 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 34
17:51:17.790308 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 1222
17:51:17.790461 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 26
17:51:17.791874 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 1222
17:51:17.791989 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 30
17:51:17.792825 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 1222
17:51:17.793078 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 399
17:51:17.793821 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 196
17:51:17.794009 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 238
17:51:17.794720 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 34
17:51:17.795380 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 34
17:51:17.796334 IP almellonesfernandez-firewall.openvpn > 192.168.1.111.60674: UDP, length 318
17:51:17.797827 IP 192.168.1.111.60674 > almellonesfernandez-firewall.openvpn: UDP, length 34
```

f. Captura de la salida systemctl status en el cliente, explicando con sus palabras algunas de los mensajes que salen, relacionándolo con las diferentes opciones de configuración.

```
almellonesfernandez@almellonesfernandez-VirtualBox:/etc/openvpn/client$ ls
almellonesfernandez-cliente1.ovpn  client.conf
almellonesfernandez@almellonesfernandez-VirtualBox:/etc/openvpn/client$ sudo systemctl restart openvpn-client@client.ser
vice
almellonesfernandez@almellonesfernandez-VirtualBox:/etc/openvpn/client$ sudo systemctl status openvpn-client@client.serv
ice
● openvpn-client@client.service - OpenVPN tunnel for client
     Loaded: loaded (/usr/lib/systemd/system/openvpn-client@.service; disabled; preset: enabled)
     Active: active (running) since Mon 2025-02-24 14:18:44 CET; 2s ago
       Docs: man:openvpn(8)
             https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 2611 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 4388)
     Memory: 1.6M (peak: 1.8M)
        CPU: 41ms
     CGroup: /system.slice/system-openvpn\x2dclient.slice/openvpn-client@client.service
             └─2611 /usr/sbin/openvpn --suppress-timestamps --nobind --config client.conf

feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: TUN/TAP device tun0 opened
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: net_iface_mtu_set: mtu 1500 for tun0
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: net_iface_up: set tun0 up
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: net_addr_v4_add: 172.18.102.2/24 dev tun0
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: net_route_v4_add: 0.0.0.0/1 via 172.18.102.1 dev [NULL] t>
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: net_route_v4_add: 128.0.0.0/1 via 172.18.102.1 dev [NULL]>
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: Initialization Sequence Completed
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: Data Channel: cipher 'AES-256-GCM', peer-id: 1, compressi>
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: Timers: ping-restart 120
feb 24 14:18:44 almellonesfernandez-VirtualBox openvpn[2611]: Protocol options: protocol-flags cc-exit tls-ekm dyn-tls->
lines 1-24/24 (END)
```

Para poder observar los logs de status he tenido que copiar el archivo .ovpn en la ruta /etc/openvpn/client con el nombre de client.conf . Y al realizar un restart del servicio y usar un status me muestra logs como que se crea una tarjeta llamada tun, se le asigna una ip

Álvaro Almellones Fernández

(172.18.102.2), etc…

Álvaro Almellones Fernández

3. **(1 punto)** Conexión **desde cliente Windows GUI (openVPN Connect)** usando fichero .ovpn con el certificado del cliente número 3 (cree certificados pero no muestre este proceso) creado en nuestra CA. Evidencie:

a. Fichero de configuración del fichero clienteXXxx2.ovpn, donde se demuestre que ha sido creado por vuestra entidad certificadora.

```
client
dev tun2
proto udp
remote 192.168.1.108 1194
resolv-retry infinite
nobind
persist-key
persist-tun
data-ciphers AES-256-CBC
verb 3

<ca>
-----BEGIN CERTIFICATE-----
MIIFbDCCA1SgAwIBAgIUIE3H4uTiv8zCBOdp/auximF7iiQwDQYJKoZIhvcNAQEN
BQAwITEfMB0GA1UEAwwWQ0EtYWxtZWxsb25lc2Zlcm5hbmRlejAeFw0yNTAyMDUx
MTMwNDNaFw0yNzAyMDUxMTMwNDNaMCExHzAdBgNVBAMMFkNBLWFsbWVsbG9uZXNm
ZXJuYW5kZXowggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCLlgPeB4Ww
6XIUzqdxjjKkJBfwrRdAQEcjOJrUK49Bs1K1EqRwyjiPEK1Dq6eWZso3ryh9f6ld
AeXf1J8Xq6qjQDLHVLqzev11Lf82Yfs4UXn2EVTtdxzbAOoOX5/D63RIM+aciE7z
RttUJQjzyZiqR0/VOb5EWqlirEm6U9lbVcK2rdr3+p6Kg27lQJNtnISzSaBJc7B7
fIrDuXXGExbrpPgYuUQAu5mLo7PAs3dXkizBOVfFDQy6uMRL8K6MGZDLjpgf/FDY
ft2LrBs3zUy75b0OeDEQKzB3JT3hkm4rcll1aFQPfvJHVkAlIUYfU7+ZzlHJXK7T
iK7tZmmIusTRghpCF35oTtkibi7HAOjSF/Qn1f9FNADr3z2bEz2N8USA61laVGWw
IAmaBz8BLhz0NV8T9DSYRfcJYwbMzNrnx3VUr1y0ddepJfERFBAo4mtIeVG0Ba3k
QOrqWZdlnkf2omPK/rwNldsFqknnGqCB9/yfhbzdbc1Ia8QCkck7lylzapqTpSs0
KWmH2sR5yVNouksyFawX6wlepmA879R157gDOUWjmfP4yrfFoJDSUt0im0cktvfJ
1ebuaWvA/BoVe97pgRoFLXBi7apXy2taVD2Ncmel+s/4AAy9hgFpL0/n/BzdmiaV
vaMIt3jfwckrBkyIJEK9Z50N8UwgfEoi4QIDAQABo4GbMIGYMAwGA1UdEwQFMAMB
Af8wHQYDVR0OBBYEFG4ccgJbOL6O23bW9dtZnXtGr0tEMFwGA1UdIwRVMFOAFG4c
cgJbOL6O23bW9dtZnXtGr0tEoSWkIzAhMR8wHQYDVQQDDBZDQS1hbG1lbGxvbmVz
ZmVybmFuZGV6ghQgTcfi5OK/zMIE52n9q7GKYXuKJDALBgNVHQ8EBAMCAQYwDQYJ
KoZIhvcNAQENBQADggIBAGAo9q5jSsdkJA5EXc1iY4tZoevpzcGpHPpcAGhE3xL4
paK0ivFDZNhaLppYqF6uHzOXpYXkdIbGkOtsPHFKzngB8QSqD2+poulGCgCSqgvC
gMFAYfj2QaQFQs9JxekztO2lB9H6bUsTZux4yr10GVQZ/ld+sTH0ZhSWz+5wj2h4
pPz70pVz2modLg3+WD7qyoLqQcZQOpv43W0zcxnKGVNJedPPrDVqhZFgoTL0Y++v
jmh0UVKUc5LdeeQe7IxIfPS8OCVIWNIRlhi7zErg3HDFlp6d6KmE0vxFT/hNdaB0
2AuUPISaWRENxqjB2Lux6trqJKb4slh4eBcpMS44pJ6GKfTwl1qUJoGWoSVsCSlL
Fco2ojeuPCcR5HJk+dPXCD8QgHCQF28pEGSd3W+FXVNnaYmOOdlJpTjG2Az+3hep
/K+jaglhttfo/9Lblhho3HgNBTepL4zMPBtAJqhCPZhPT9uSRpx7BrrURzAhy/ME
HilmatO8spb7QYTsQFkZufzrexjX7ZFoF8c/SWic1uB4jrHNl9ij1wEMER7xWKoG
07xrZoRXtvz2Qn6yEGj+O+Rc1YylCdyHMbM1HO7ic/41HjeaQgHVgNiedp7ZzhBn
wtMD6MZc2Dd21jAgeJhRkI60bh9ebUZ2IL1KmirzzhJfU0stCtqgBv7pC/rYFV+d
-----END CERTIFICATE-----
</ca>
```

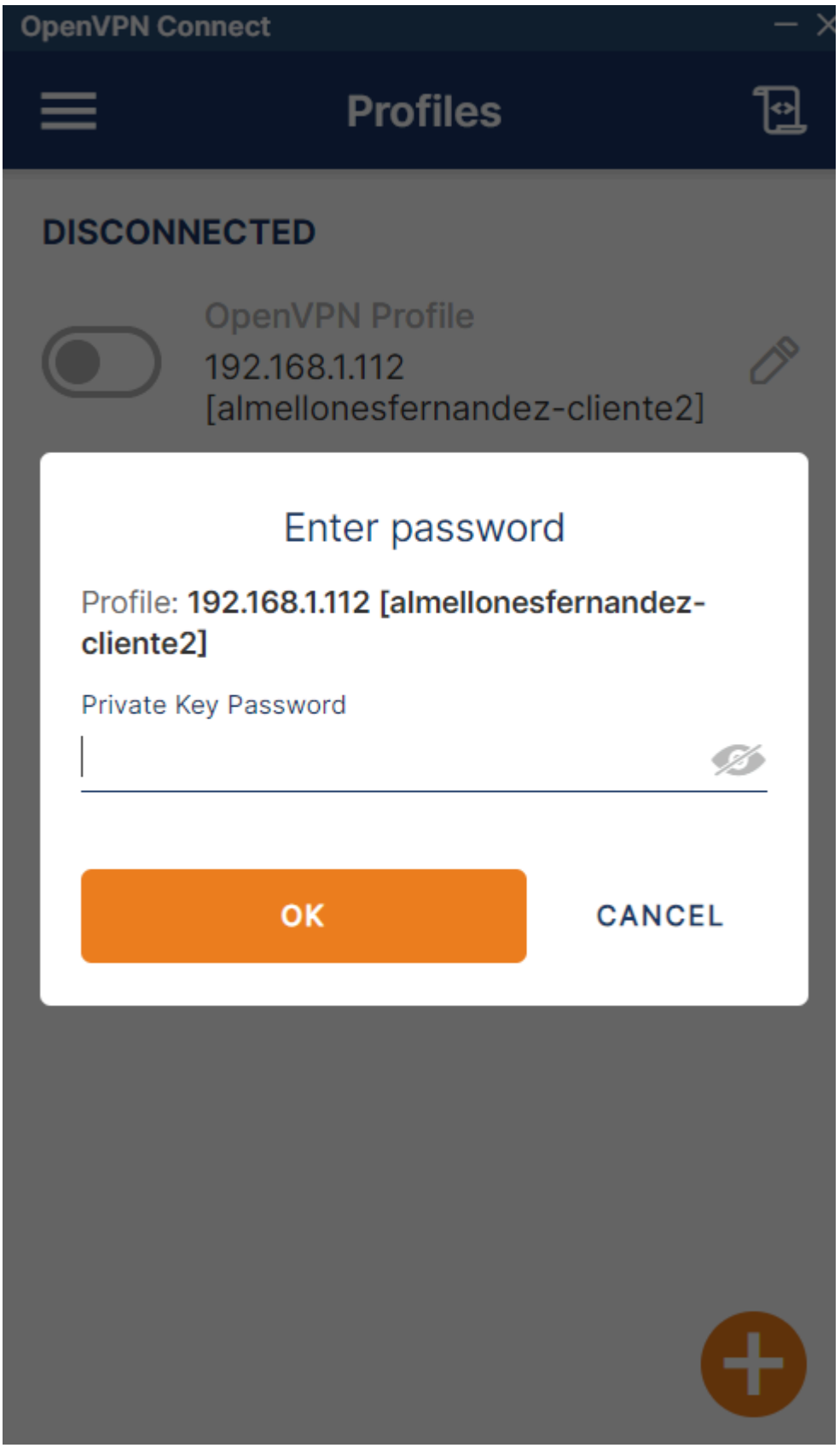
```
<cert>
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9b:e4:b5:7b:61:e9:d0:82:13:bb:27:81:ae:72:69:53
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=CA-almellonesfernandez
        Validity
            Not Before: Feb 24 19:44:51 2025 GMT
            Not After : Feb 24 19:44:51 2026 GMT
        Subject: CN=almellonesfernandez-cliente3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:ba:9b:d4:81:7c:9b:00:4d:0c:fb:f7:25:b3:83:
                    29:51:2f:a3:21:ff:37:e7:89:8e:0d:39:70:7d:08:
                    61:28:1d:50:22:04:64:a0:0b:39:4f:d2:25:8c:de:
                    a3:6e:93:f8:13:3a:f3:e0:6f:ce:3e:26:b1:3d:e1:
                    8b:ed:df:21:13:bb:3a:9f:b7:c2:23:86:d2:83:af:
                    b1:08:4c:2f:a4:c7:89:d2:7a:eb:56:89:87:f3:78:
                    9a:09:bf:5c:b6:7f:b9:11:ff:7d:ba:1a:54:84:2a:
                    79:29:c9:5e:96:ae:83:1b:e4:2d:fc:2a:21:09:bd:
                    e6:c5:97:50:81:22:60:30:b2:93:4e:26:bf:c6:93:
                    09:00:ac:77:8d:76:23:84:33:02:bb:34:81:a8:06:
                    d1:51:e4:8f:1d:67:34:99:5b:ca:c1:86:01:47:dc:
                    32:43:04:6f:a1:c0:15:39:c1:92:c7:c9:8b:60:92:
                    7a:68:70:b1:7b:88:cd:b9:8a:85:25:76:15:66:9d:
                    00:a8:f1:d7:2d:63:8a:1f:ac:00:f3:13:1a:75:cf:
                    10:52:bd:57:7c:8a:dd:2c:a7:3b:c1:51:60:4a:25:
                    d7:6f:dc:fa:b9:64:2e:22:03:6f:5c:42:12:68:20:
                    8d:cc:74:04:30:b4:59:7d:2a:1b:23:87:a4:69:87:
                    ff:ef:a3:ff:79:e9:2c:43:9b:b0:b7:71:c3:2b:7e:
                    e5:25:fe:ae:9a:25:2b:8b:ce:a7:20:67:d3:9d:e0:
                    5a:20:5c:f0:3e:b6:f5:c6:55:1d:ff:fb:dd:e9:5f:
                    49:08:85:d5:05:20:5a:54:20:39:5b:63:46:b4:8e:
                    ca:64:d9:fd:83:fa:36:a2:38:ac:99:ac:a3:49:7c:
                    e4:4b:a3:b4:40:bc:28:73:7e:1d:fb:d6:fb:0d:91:
                    91:bb:d6:16:71:03:f0:65:e8:70:76:f2:94:b3:e8:
                    d0:ef:34:e1:fa:b8:ce:ad:71:f1:da:f9:c6:88:37:
                    46:2f:75:d1:eb:e5:64:e1:00:98:08:c3:05:cf:d2:
                    32:e2:45:ba:db:4e:c9:d1:c7:49:3a:d1:5d:a3:ab:
                    c5:75:29:66:44:73:03:dc:32:23:46:7c:ba:7c:72:
                    1d:b1:ea:02:e8:5b:10:df:81:72:e4:8a:c6:53:86:
                    f7:70:88:5a:c7:15:1a:d1:13:ce:74:47:62:c0:93:
                    70:10:f4:f7:c8:73:8d:52:00:fa:a3:d9:eb:d2:82:
                    30:5a:dd:3b:11:7e:6c:43:97:7d:aa:e3:f9:f1:62:
                    08:36:02:1e:d9:56:bc:35:72:de:12:be:04:4a:be:
                    e1:0c:ed:a5:2b:4e:2c:77:2c:8f:f4:76:ca:1d:47:
                    09:5a:a7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                16:00:5F:08:CE:19:84:DF:7A:81:7B:CB:FA:6C:5E:44:14:63:5D:BD
            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
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 Key Usage:
                Digital Signature
    Signature Algorithm: sha512WithRSAEncryption
```

b. Realice primera conexión con cliente openvpn **(openVPN Connect)** y muestre movimiento de contadores de iptables (INPUT). Muestre información que aparece en el cliente GUI, y compare con lo que aparece en el servidor VPN. Demuestre que se solicita contraseña.

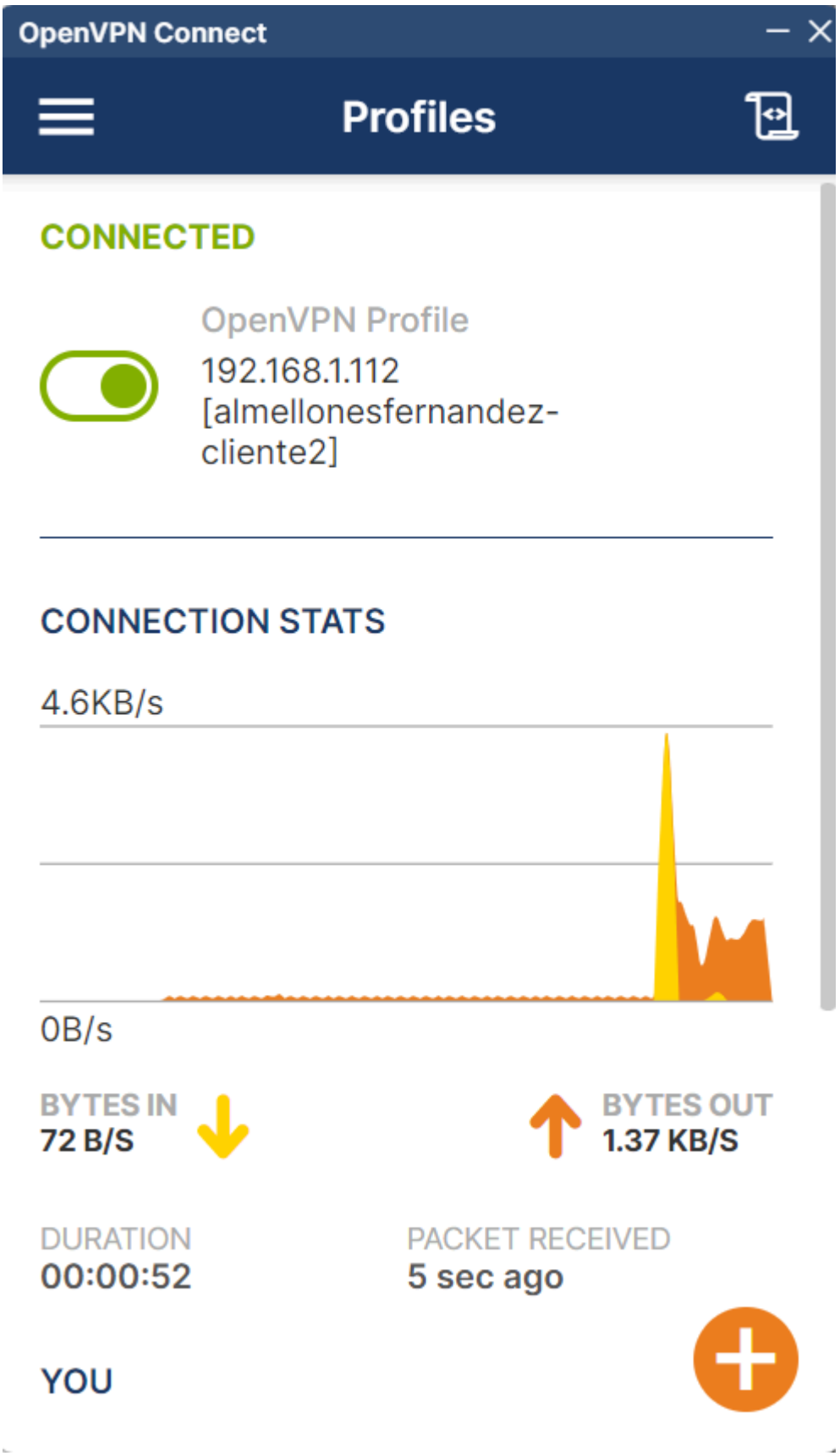
Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall ~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 4 packets, 172 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
    0     0 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194 /* Permitir el puerto que usa VPN */
  962 72572 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde WAN */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           /* Permitir ping desde cualquier subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde DMZ */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3128 /* Zona LAN */
    0     0 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3129 /* Zona WLAN */
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED /* Respuestas OUTPUT */
```

Álvaro Almellones Fernández



Álvaro Almellones Fernández



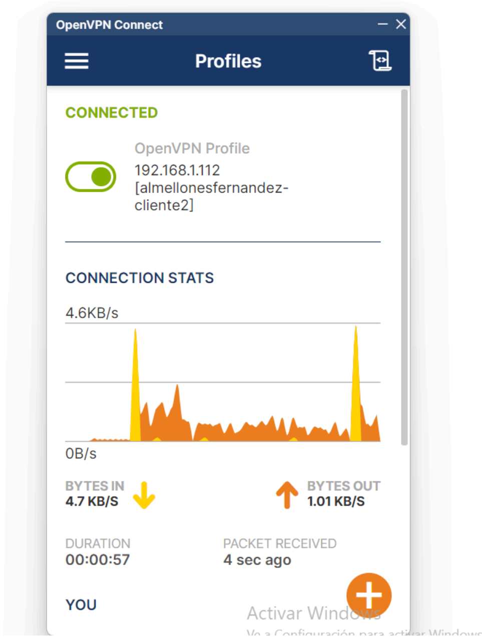
Álvaro Almellones Fernández

```
2025-02-24 20:54:29 SENT CONTROL [almellonesfernandez-cliente3]: 'PUSH_REPLY,redirect-gateway local def1,dhcp-option DNS 8.8.8.8,dhcp-option DNS 192.168.40.1,route-gateway 172.18.102.1,topology subnet,ifconfig 172.18.102.3 255.255.255.0,peer-id 1,cipher AES-256-GCM,protocol-flags cc-exit tls-ekm dyn-tls-crypt,tun-mtu 1500' (status=1)
2025-02-24 20:54:29 almellonesfernandez-cliente3/192.168.1.108:63802 PUSH: Received control message: 'PUSH_REQUEST'
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 Data Channel: cipher 'AES-256-GCM', peer-id: 0
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 Protocol options: protocol-flags cc-exit tls-ekm dyn-tls-crypt
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
2025-02-24 20:54:31 almellonesfernandez-cliente3/192.168.1.108:63802 IP packet with unknown IP version=15 seen
```

```
root@almellonesfernandez-firewall:/etc/openvpn/server# iptables -L -n -v
Chain INPUT (policy DROP 30 packets, 1694 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
   71 13248 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0            udp dpt:1194 /* Permitir el puerto que usa VPN */
 2236  166K ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desde WAN */
    1    28 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualquier subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desde LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desde DMZ */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3128 /* Zona LAN */
    0     0 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3129 /* Zona WLAN */
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Respuestas OUTPUT */
```

c. Ip asignadas a la tarjeta virtual del cliente windows y del servidor. Captura de fichero del servidor donde aparece que está IP se ha asignado correctamente. Debería aparecer como segunda.

```
C:\Users\alvar>ipconfig

Configuración IP de Windows


Adaptador desconocido Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::3af4:3c31:79a5:b635%26
   Dirección IPv4. . . . . . . . . . . . . . : 172.18.102.3
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . : politecnicomalaga.com

Adaptador de Ethernet Ethernet 2:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet vEthernet (Default Switch):

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::e5be:491d:7012:5e17%30
   Dirección IPv4. . . . . . . . . . . . . . : 172.20.208.1
   Máscara de subred . . . . . . . . . . . . : 255.255.240.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet vEthernet (WSL (Hyper-V firewall)):

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::9c9c:cc4c:7822:c2f9%106
   Dirección IPv4. . . . . . . . . . . . . . : 172.27.128.1
   Máscara de subred . . . . . . . . . . . . : 255.255.240.0
   Puerta de enlace predeterminada . . . . . :
```

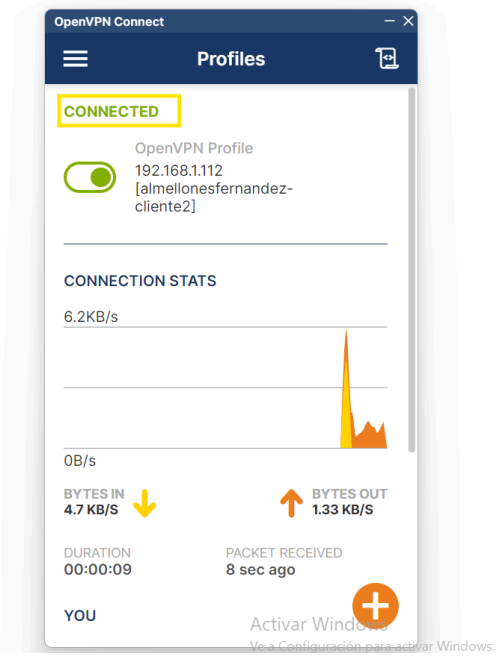


Álvaro Almellones Fernández

```
 GNU nano 7.2                                  /var/log/openvpn/ipp.txt
almellonesfernandez-cliente1,172.18.102.2,
almellonesfernandez-cliente3,172.18.102.3,
```

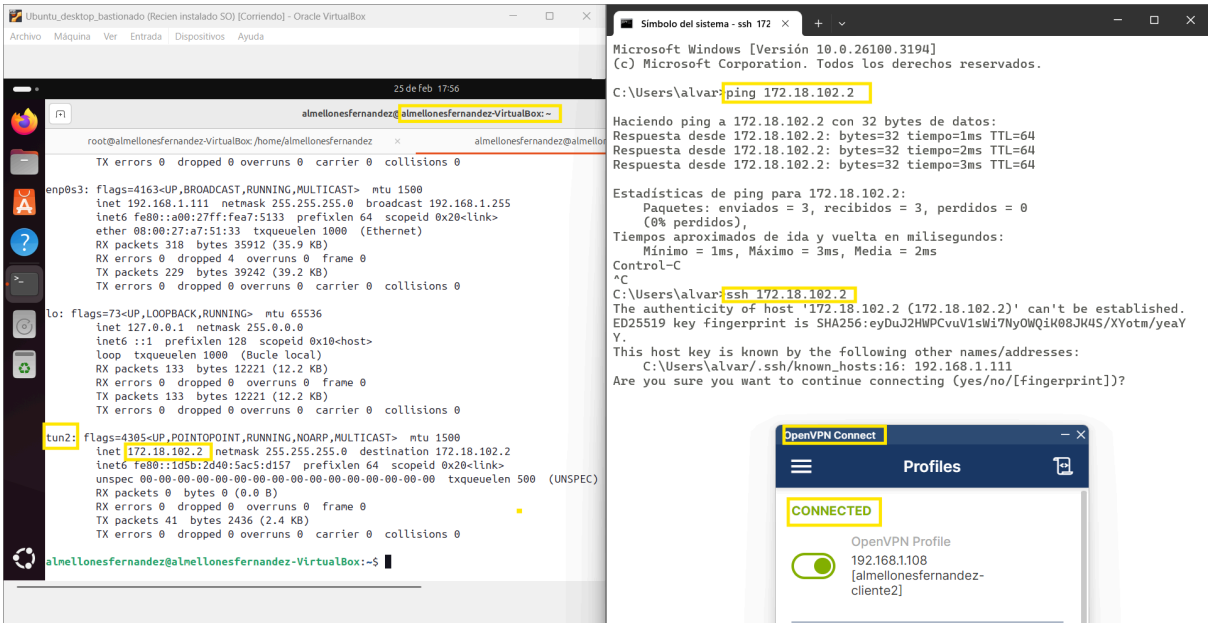
d. Tcpdump en servidor firewall vpn de la conexión vpn realizada.

```
root@almellonesfernandez-firewall /etc/openvpn/server# tcpdump port 1194
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wan2, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:20:13.897676 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 14
21:20:13.897867 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 26
21:20:13.898491 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 309
21:20:13.904722 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 1222
21:20:13.904910 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 1222
21:20:13.905024 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 1222
21:20:13.905115 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 200
21:20:13.905231 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 26
21:20:13.905344 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 30
21:20:13.905889 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 34
21:20:13.911158 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 1288
21:20:13.911158 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 1288
21:20:13.911158 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 1288
21:20:13.911158 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 285
21:20:13.911357 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 26
21:20:13.911479 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 30
21:20:13.912491 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 196
21:20:13.912848 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 238
21:20:13.912906 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 34
21:20:13.913171 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 34
21:20:13.913264 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 73
21:20:13.915003 IP almellonesfernandez-firewall.openvpn > 192.168.1.108.62933: UDP, length 318
21:20:14.827215 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 34
21:20:14.827215 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 131
21:20:14.827215 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 350
21:20:14.827215 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 286
21:20:14.827215 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 89
21:20:14.827215 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 73
21:20:14.827215 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 101
21:20:14.827215 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 101
21:20:14.827300 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 106
21:20:14.827300 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 121
21:20:14.827300 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 101
21:20:14.827300 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 101
21:20:14.827300 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 101
21:20:14.996596 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 131
21:20:15.012930 IP 192.168.1.108.62933 > almellonesfernandez-firewall.openvpn: UDP, length 106
```



e. Realice cambios en el fichero de configuración del servidor VPN, para que los diferentes clientes VPN conectados, puedan verse entre ellos. Evidencie que pueden verse con un ping y con ssh.

```
root@almellonesfernandez-firewall:/etc/openvpn/server# grep -vE '^\s*[#;]' /etc/openvpn/server/server.conf |gr
ep client
client-to-client
root@almellonesfernandez-firewall:/etc/openvpn/server#
```



Álvaro Almellones Fernández

4. (1 punto) Realice los cambios necesarios en el fichero de configuración del servidor VPN y de las reglas de iptables, para que se permita que los diferentes clientes openvpn una vez conectado, pueda alcanzar el servidor VPN con ping y ssh. Evidencie:

a. Cambios en el fichero de configuración del servidor VPN para permitir conexiones.

No he tenido que modificar nada en el fichero de configuración para que funcione, con las configuraciones por defecto que he usado siguiendo el manual ya funciona

b. Reglas de iptables **concretas** para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

```
  GNU nano 7.2                          firewall-almellonesfernandez.sh
squid() {
# Regla para configurar el squid, es bueno quitar poner a DROP de  lan/wlan a wan (80,443) para asegurarnos. No necesario.
        # No Transparente zona lan
        iptables -t filter -A INPUT -i $lan -p tcp --dport 3128 -j ACCEPT  -m comment --comment "Zona LAN"
        iptables -t nat -A PREROUTING -i $lan -s 172.16.102.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3128
        #Decomentar linea anterior para que sea no transparente.

        # Transparente zona wlan
        iptables -t filter -A INPUT -i $wlan -p tcp --dport 3129 -j ACCEPT -m comment --comment "Zona WLAN"
        iptables -t nat -A PREROUTING -i $wlan -s 192.168.102.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3129

        #No necesario hacer PREROUTING ya que se configura el navegador para ir al 3129, y va directamente
}

vpn-general() {

iptables -t filter -A INPUT -p udp --dport 1194 -i $wan -j  ACCEPT -m comment --comment "Permitir el puerto que usa VPN"
iptables -t filter -A INPUT -p icmp -i $tun -j  ACCEPT -m comment --comment "Permitir hacer ping desde la tun a firewall"
iptables -t filter -A INPUT -p tcp --dport 22 -i $tun -j  ACCEPT -m comment --comment "Permitir ssh desde tun"


}



echo "Arrancado Cortafuegos de Alvaro Almellones. Bastionado de Redes y Sistemas"

variables # Carga de variables
generales # Reglas generales
loopback # Reglas de loopback
vpn-general
```

c. Capturas de la conexión realizada (contadores) y establecidas (netstat y tcpdump) correctamente, donde se demuestre que se alcanza mediante ping al servidor VPN por la tarjeta tun-XXxx0, usando el cliente Linux vpn. Muestre que se han creado las rutas para alcanzar dicha red (ip route).

```
root@almellonesfernandez-firewall:~# sudo iptables -L -n -v
Chain INPUT (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
    0     0 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194 /* Permi
tir el puerto que usa VPN */
    0     0 ACCEPT     1    --  tun2   *       0.0.0.0/0            0.0.0.0/0           /* Permitir hacer pin
g desde la tun a firewall */
    0     0 ACCEPT     6    --  tun2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permiti
r ssh desde tun */
   19  1192 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permiti
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez   almellonesfernandez@almellonesfernandez-VirtualBox: ~
        loop  txqueuelen 1000  (Bucle local)
        RX packets 168  bytes 16688 (16.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 168  bytes 16688 (16.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun2: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 172.18.102.2  netmask 255.255.255.0  destination 172.18.102.2
        inet6 fe80::68b8:d767:e177:83a4  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 7  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 114  bytes 6916 (6.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

almellonesfernandez@almellonesfernandez-VirtualBox:~$ ping 172.18.102.1
PING 172.18.102.1 (172.18.102.1) 56(84) bytes of data.
64 bytes from 172.18.102.1: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 172.18.102.1: icmp_seq=2 ttl=64 time=0.775 ms
64 bytes from 172.18.102.1: icmp_seq=3 ttl=64 time=1.14 ms
64 bytes from 172.18.102.1: icmp_seq=4 ttl=64 time=0.721 ms
^C
--- 172.18.102.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3025ms
rtt min/avg/max/mdev = 0.721/0.961/1.207/0.215 ms
almellonesfernandez@almellonesfernandez-VirtualBox:~$ ssh 172.18.102.1
The authenticity of host '172.18.102.1 (172.18.102.1)' can't be established.
ED25519 key fingerprint is SHA256:BjipMtMZmAj4tR6Wxt0/9tJ9TR/uWQhE+knS8vD73G8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

```
root@almellonesfernandez-firewall:~# sudo iptables -L -n -v
Chain INPUT (policy DROP 7 packets, 224 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
   16  4698 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194 /* Permi
tir el puerto que usa VPN */
    3   252 ACCEPT     1    --  tun2   *       0.0.0.0/0            0.0.0.0/0           /* Permitir hacer pin
g desde la tun a firewall */
   12  3566 ACCEPT     6    --  tun2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permiti
r ssh desde tun */
```

```
root@almellonesfernandez-firewall:~# netstat -putan |grep 22
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      2267/sshd: root@pts
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
tcp6       0      0 ::1:6010                :::*                    LISTEN      2267/sshd: root@pts
tcp6       0      0 172.18.102.1:22         172.18.102.2:59248      ESTABLISHED 4192/sshd: [accepte
tcp6       0      0 192.168.1.108:22        192.168.1.112:56173     ESTABLISHED 2267/sshd: root@pts
tcp6       0      0 192.168.1.108:22        192.168.1.112:56294     ESTABLISHED 3506/sshd: root@not
tcp6       0     48 192.168.1.108:22        192.168.1.112:56293     ESTABLISHED 3504/sshd: root@pts
tcp6       0      0 192.168.1.108:22        192.168.1.112:56174     ESTABLISHED 2269/sshd: root@not
udp        0      0 0.0.0.0:54422           0.0.0.0:*                           1375/(squid-1)
root@almellonesfernandez-firewall:~#
```

```
root@almellonesfernandez-firewall:~# tcpdump -i tun2 port 22
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
18:29:32.670761 IP 172.18.102.2.39668 > almellonesfernandez-firewall.ssh: Flags [F.], seq 1070583919, ack 6600
20236, win 545, options [nop,nop,TS val 679093649 ecr 3899973276], length 0
18:29:32.671834 IP almellonesfernandez-firewall.ssh > 172.18.102.2.39668: Flags [F.], seq 1, ack 1, win 567, o
ptions [nop,nop,TS val 3900016973 ecr 679093649], length 0
18:29:32.673455 IP 172.18.102.2.39668 > almellonesfernandez-firewall.ssh: Flags [.], ack 2, win 545, options [
nop,nop,TS val 679093655 ecr 3900016973], length 0
18:29:33.957640 IP 172.18.102.2.37610 > almellonesfernandez-firewall.ssh: Flags [S], seq 801318745, win 64240,
 options [mss 1400,sackOK,TS val 679094939 ecr 0,nop,wscale 7], length 0
18:29:33.957707 IP almellonesfernandez-firewall.ssh > 172.18.102.2.37610: Flags [S.], seq 4286453547, ack 8013
18746, win 65160, options [mss 1460,sackOK,TS val 3900018259 ecr 679094939,nop,wscale 7], length 0
18:29:33.958708 IP 172.18.102.2.37610 > almellonesfernandez-firewall.ssh: Flags [.], ack 1, win 502, options [
nop,nop,TS val 679094940 ecr 3900018259], length 0
18:29:33.959415 IP almellonesfernandez-firewall.ssh > 172.18.102.2.37610: Flags [P.], seq 1:43, ack 1, win 510
, options [nop,nop,TS val 3900018261 ecr 679094940], length 42: SSH: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.8
18:29:33.960584 IP 172.18.102.2.37610 > almellonesfernandez-firewall.ssh: Flags [.], ack 43, win 502, options
[nop,nop,TS val 679094942 ecr 3900018261], length 0
18:29:33.965539 IP 172.18.102.2.37610 > almellonesfernandez-firewall.ssh: Flags [P.], seq 1:43, ack 43, win 50
```

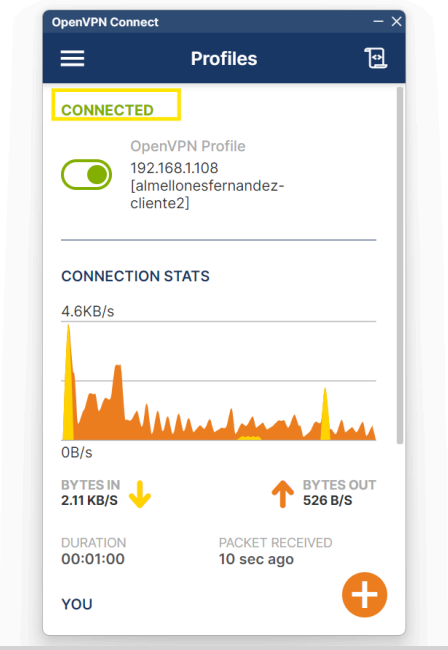
```
root@almellonesfernandez-firewall:~# tcpdump -i tun2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
18:31:54.355436 IP 172.18.102.2.38831 > prod-ntp-3.ntp1.ps5.canonical.com.ntp: NTPv4, Client, length 48
18:31:57.240328 IP 172.18.102.2.59012 > ubuntu-content-cache-1.ps5.canonical.com.http: Flags [S], seq 16300143
71, win 64240, options [mss 1400,sackOK,TS val 481791063 ecr 0,nop,wscale 7], length 0
18:32:04.032158 IP 172.18.102.2 > almellonesfernandez-firewall: ICMP echo request, id 2860, seq 1, length 64
18:32:04.032190 IP almellonesfernandez-firewall > 172.18.102.2: ICMP echo reply, id 2860, seq 1, length 64
18:32:05.033191 IP 172.18.102.2 > almellonesfernandez-firewall: ICMP echo request, id 2860, seq 2, length 64
18:32:05.033219 IP almellonesfernandez-firewall > 172.18.102.2: ICMP echo reply, id 2860, seq 2, length 64
18:32:05.368057 IP 172.18.102.2.59012 > ubuntu-content-cache-1.ps5.canonical.com.http: Flags [S], seq 16300143
71, win 64240, options [mss 1400,sackOK,TS val 481799191 ecr 0,nop,wscale 7], length 0
18:32:06.034238 IP 172.18.102.2 > almellonesfernandez-firewall: ICMP echo request, id 2860, seq 3, length 64
18:32:06.034262 IP almellonesfernandez-firewall > 172.18.102.2: ICMP echo reply, id 2860, seq 3, length 64
18:32:07.037144 IP 172.18.102.2 > almellonesfernandez-firewall: ICMP echo request, id 2860, seq 4, length 64
18:32:07.037173 IP almellonesfernandez-firewall > 172.18.102.2: ICMP echo reply, id 2860, seq 4, length 64
18:32:08.038572 IP 172.18.102.2 > almellonesfernandez-firewall: ICMP echo request, id 2860, seq 5, length 64
18:32:08.038602 IP almellonesfernandez-firewall > 172.18.102.2: ICMP echo reply, id 2860, seq 5, length 64
18:32:09.039275 IP 172.18.102.2 > almellonesfernandez-firewall: ICMP echo request, id 2860, seq 6, length 64
18:32:09.039305 IP almellonesfernandez-firewall > 172.18.102.2: ICMP echo reply, id 2860, seq 6, length 64
^C
15 packets captured
15 packets received by filter
0 packets dropped by kernel
root@almellonesfernandez-firewall:~#
```

d. Capturas de la conexión realizada (contadores) y establecidas (netstat y tcpdump) correctamente, donde se demuestre que se alcanza mediante ping al servidor VPN por la tarjeta tun-XXxx0 usando el cliente Openvpn GUI de Windows.

```
root@almellonesfernandez-firewall:~/scripts# ./firewall-almellonesfernandez.sh
Arrancado Cortafuegos de Alvaro Almellones. Bastionado de Redes y Sistemas
root@almellonesfernandez-firewall:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 32 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
    0     0 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194 /* Permitir el puerto que
usa VPN */
    0     0 ACCEPT     1    --  tun2   *       0.0.0.0/0            0.0.0.0/0           /* Permitir hacer ping desde la tun a f
irewall */
    0     0 ACCEPT     6    --  tun2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir ssh desde tun */
   28  1792 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde WAN */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           /* Permitir ping desde cualquier subred
 */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde DMZ */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3128 /* Zona LAN */
    0     0 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3129 /* Zona WLAN */
```

Álvaro Almellones Fernández

```
Microsoft Windows [Versión 10.0.26100.3194]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\alvar>ping 172.18.102.1

Haciendo ping a 172.18.102.1 con 32 bytes de datos:
Respuesta desde 172.18.102.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.18.102.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.18.102.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.18.102.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.18.102.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\alvar>ssh 172.18.102.1
The authenticity of host '172.18.102.1 (172.18.102.1)' can't be established.
ED25519 key fingerprint is SHA256:BjipMtMZmAj4tR6Wxt0/9tJ9TR/uWQhE+knS8vD73G8.
This host key is known by the following other names/addresses:
    C:\Users\alvar/.ssh/known_hosts:6: 192.168.75.130
    C:\Users\alvar/.ssh/known_hosts:19: 192.168.1.112
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```




```
root@almellonesfernandez-firewall ~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 47 packets, 3140 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
  513 71496 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194 /* Permitir el puerto que
usa VPN */
    4   240 ACCEPT     1    --  tun2   *       0.0.0.0/0            0.0.0.0/0           /* Permitir hacer ping desde la tun a f
irewall */
    7  1805 ACCEPT     6    --  tun2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir ssh desde tun */
   50  3200 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH desde WAN */
    2    56 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           /* Permitir ping desde cualquier subred
 */
```

```
root@almellonesfernandez-firewall:~# netstat -putan |grep 22
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      2267/sshd: root@pts
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
tcp6       0      0 ::1:6010                :::*                    LISTEN      2267/sshd: root@pts
tcp6       0      0 172.18.102.1:22         172.18.102.3:54638      ESTABLISHED 5444/sshd: [accepte
tcp6       0      0 192.168.1.108:22        192.168.1.112:56173     ESTABLISHED 2267/sshd: root@pts
tcp6       0      0 192.168.1.108:22        192.168.1.112:56294     ESTABLISHED 3506/sshd: root@not
tcp6       0     48 192.168.1.108:22        192.168.1.112:56293     ESTABLISHED 3504/sshd: root@pts
tcp6       0      0 192.168.1.108:22        192.168.1.112:56174     ESTABLISHED 2269/sshd: root@not
udp        0      0 0.0.0.0:54422           0.0.0.0:*                           1375/(squid-1)
root@almellonesfernandez-firewall:~#
```

```
root@almellonesfernandez-firewall:~# tcpdump -i tun2 port 22
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
18:43:15.917430 IP 172.18.102.3.64664 > almellonesfernandez-firewall.ssh: Flags [R.], seq 1656572512, ack 1132
40816, win 0, length 0
18:43:18.038474 IP 172.18.102.3.64665 > almellonesfernandez-firewall.ssh: Flags [S], seq 386584438, win 65535,
 options [mss 1400,nop,wscale 8,nop,nop,sackOK], length 0
18:43:18.038509 IP almellonesfernandez-firewall.ssh > 172.18.102.3.64665: Flags [S.], seq 454210430, ack 38658
4439, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
18:43:18.038879 IP 172.18.102.3.64665 > almellonesfernandez-firewall.ssh: Flags [.], ack 1, win 255, length 0
18:43:18.039602 IP almellonesfernandez-firewall.ssh > 172.18.102.3.64665: Flags [P.], seq 1:43, ack 1, win 502
, length 42: SSH: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.8
18:43:18.041192 IP 172.18.102.3.64665 > almellonesfernandez-firewall.ssh: Flags [P.], seq 1:34, ack 43, win 25
5, length 33: SSH: SSH-2.0-OpenSSH_for_Windows_9.5
18:43:18.041261 IP almellonesfernandez-firewall.ssh > 172.18.102.3.64665: Flags [.], ack 34, win 502, length 0
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:~# tcpdump -i tun2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
18:45:17.780114 IP 172.18.102.3.54679 > dns.google.domain: 16405+ A? kv601.prod.do.dsp.mp.microso
ft.com. (52)
18:45:17.807870 IP 172.18.102.3.60249 > dns.google.domain: 25142+ A? ssl.gstatic.com. (33)
18:45:17.807892 IP 172.18.102.3.60249 > 192.168.40.1.domain: 25142+ A? ssl.gstatic.com. (33)
18:45:18.040177 IP almellonesfernandez-firewall.ssh > 172.18.102.3.64665: Flags [F.], seq 4542120
85, ack 386585952, win 524, length 0
18:45:18.250484 IP almellonesfernandez-firewall.ssh > 172.18.102.3.64665: Flags [F.], seq 0, ack
1, win 524, length 0
18:45:18.458304 IP almellonesfernandez-firewall.ssh > 172.18.102.3.64665: Flags [F.], seq 0, ack
1, win 524, length 0
18:45:18.780889 IP 172.18.102.3.54679 > 192.168.40.1.domain: 16405+ A? kv601.prod.do.dsp.mp.micro
soft.com. (52)
18:45:18.829048 IP 172.18.102.3 > almellonesfernandez-firewall: ICMP echo request, id 1, seq 12,
length 40
18:45:18.829073 IP almellonesfernandez-firewall > 172.18.102.3: ICMP echo reply, id 1, seq 12, le
ngth 40
18:45:18.874303 IP almellonesfernandez-firewall.ssh > 172.18.102.3.64665: Flags [F.], seq 0, ack
1, win 524, length 0
```

Álvaro Almellones Fernández

CLIENTE VPN – TO – CLIENTES RED LAN

5. (1 punto) Realice los cambios necesarios en el fichero de configuración del servidor VPN y de las reglas de iptables, para que se permita que los diferentes clientes openvpn una vez conectados, pueden alcanzar el equipo 172.16.?.2 de la red lan (ping y ssh). Evidencie:

a. Cambios **exclusivos** en el fichero de configuración del servidor VPN para permitir dichas conexiones.

```
  GNU nano 7.2                                          server.conf
# and DNS server addresses.  You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.102.0 255.255.255.0"
push "route 172.16.102.0 255.255.255.0"
;push "route 10.0.102.0 255.255.255.0"


# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy
```

b. Reglas de iptables concretas para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

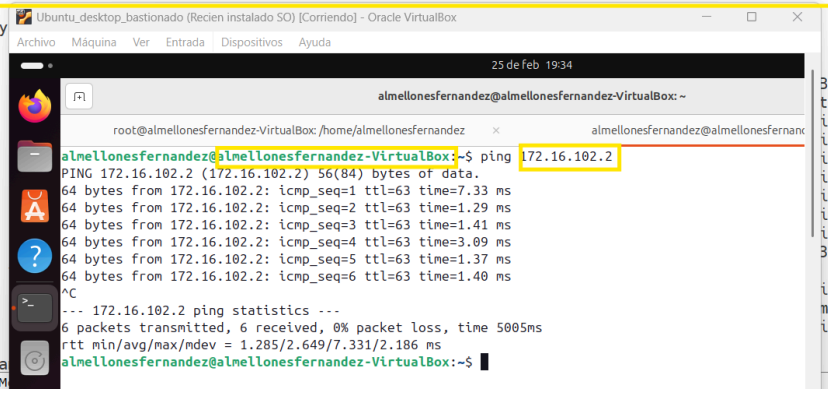
```
  GNU nano 7.2                                    firewall-almellonesfernandez.sh
iptables -t filter -A INPUT -p icmp -i $tun -j  ACCEPT -m comment --comment "Permitir hacer ping desde la tun a firewall"
iptables -t filter -A INPUT -p tcp --dport 22 -i $tun -j  ACCEPT -m comment --comment "Permitir ssh desde tun"


}
vpn-a-lan() {

iptables -t filter -A FORWARD -i $tun -o $lan -p tcp --dport 22 -d 172.16.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $tun -o $lan -p icmp  -d 172.16.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $lan -o $tun -m state --state  ESTABLISHED,RELATED -j ACCEPT
}

echo "Arrancado Cortafuegos de Alvaro Almellones. Bastionado de Redes y Sistemas"

variables # Carga de variables
generales # Reglas generales
loopback # Reglas de loopback
vpn-general
input # Reglas de input
squid
output # Reglas de output
dmz-a-wan # Reglas de dmz (zona naranja) a WAN
lan-a-wan # Reglas de intranet-lan (zona verde) a WAN
wlan-a-wan # Reglas de intranet-wlan (zona azul) a WAN
wan-a-dmz # Reglas de wan a dmz
lan-a-wlan
lan-a-dmz
vpn-a-lan

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was
```

Álvaro Almellones Fernández

c. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión al equipo 172.16.?.2, mediante un ping. Muestre que se han creado las rutas para alcanzar dicha red (ip route)

```
    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: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
    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 prefix "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 prefix "LAN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2        tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
```

```
    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: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
    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 prefix "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 prefix "LAN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2        tcp dpt:22
    6   504 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    6   504 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
```




```
Chain OUTPUT (policy
 pkts bytes target
    0     0 ACCEPT
  184 22104 ACCEPT
    0     0 ACCEPT
    0     0 DROP
    0     0 ACCEPT
    0     0 ACCEPT
    0     0 ACCEPT
    0     0 ACCEPT
    0     0 ACCEPT
    0     0 ACCEPT
    0     0 ACCEPT
    0     0 ACCEPT
HTTP y HTTPS en WAN
    0     0 ACCEPT
    0     0 ACCEPT
    0     0 ACCEPT
    0     0 ACCEPT
root@almellonesferna
ERED VERSION - Please support M
```

```
 enviar a otros procesos. Ej. DNS local */
BLISHED /* Respuestas INPUT */
terfaces ping */
itir SSH a equipos en WAN */
itir SSH a equipo en DMZ */
itir SSH a equipo en LAN */
itir SSH a equipo en LAN */
itir SSH a equipo en LAN */
itir SSH a equipo en LAN */
itir SSH a equipo en WLAN */
3,80,443 /* Permitir actualizaciones DNS,

itir DNS UDP en WAN */
mitir sincronización NTP en WAN */
itir envío de correos SMTP en WAN */
```

```
root@almellonesfernandez-firewall:/etc/openvpn/server# tcpdump -i tun2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
19:37:58.362258 IP 172.18.102.2 > 172.16.102.2: ICMP echo request, id 3214, seq 142, length 64
19:37:58.362814 IP 172.16.102.2 > 172.18.102.2: ICMP echo reply, id 3214, seq 142, length 64
19:37:59.363459 IP 172.18.102.2 > 172.16.102.2: ICMP echo request, id 3214, seq 143, length 64
19:37:59.363945 IP 172.16.102.2 > 172.18.102.2: ICMP echo reply, id 3214, seq 143, length 64
19:38:00.364117 IP 172.18.102.2 > 172.16.102.2: ICMP echo request, id 3214, seq 144, length 64
19:38:00.364565 IP 172.16.102.2 > 172.18.102.2: ICMP echo reply, id 3214, seq 144, length 64
19:38:01.365303 IP 172.18.102.2 > 172.16.102.2: ICMP echo request, id 3214, seq 145, length 64
19:38:01.365777 IP 172.16.102.2 > 172.18.102.2: ICMP echo reply, id 3214, seq 145, length 64
19:38:02.366473 IP 172.18.102.2 > 172.16.102.2: ICMP echo request, id 3214, seq 146, length 64
19:38:02.367135 IP 172.16.102.2 > 172.18.102.2: ICMP echo reply, id 3214, seq 146, length 64
19:38:03.367132 IP 172.18.102.2 > 172.16.102.2: ICMP echo request, id 3214, seq 147, length 64
19:38:03.367639 IP 172.16.102.2 > 172.18.102.2: ICMP echo reply, id 3214, seq 147, length 64
19:38:04.368298 IP 172.18.102.2 > 172.16.102.2: ICMP echo request, id 3214, seq 148, length 64
19:38:04.368811 IP 172.16.102.2 > 172.18.102.2: ICMP echo reply, id 3214, seq 148, length 64
^C
14 packets captured
14 packets received by filter
0 packets dropped by kernel
root@almellonesfernandez-firewall:/etc/openvpn/server#
```

Álvaro Almellones Fernández

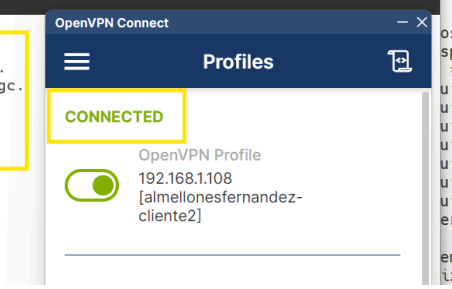
```
almellonesfernandez@almellonesfernandez-VirtualBox:~$ ip route
0.0.0.0/1 via 172.18.102.1 dev tun2
default via 192.168.1.1 dev enp0s3 proto dhcp src 192.168.1.111 metric 100
128.0.0.0/1 via 172.18.102.1 dev tun2
172.16.102.0/24 via 172.18.102.1 dev tun2
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.18.102.0/24 dev tun2 proto kernel scope link src 172.18.102.2
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.111 metric 100
almellonesfernandez@almellonesfernandez-VirtualBox:~$
```

d. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión al equipo 172.16.?.2, mediante una conexión por ssh.

```
    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: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
    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 prefix "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 prefix "LAN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
```

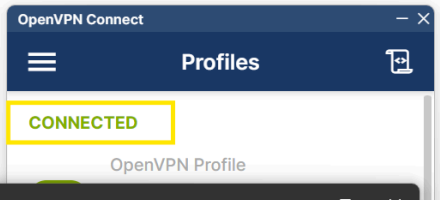
```
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    8  1845 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    7  1946 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
```

```
Símbolo del sistema

C:\Users\alvar>ssh 172.16.102.2
The authenticity of host '172.16.102.2 (172.16.102.2)' can't be established.
ED25519 key fingerprint is SHA256:H9f74icsZoYw6LTiy+KQ8iZeSGl/UUq1A9stzqMSfgc.
This host key is known by the following other names/addresses:
    C:\Users\alvar/.ssh/known_hosts:13: [localhost]:5000
Are you sure you want to continue connecting (yes/no/[fingerprint])?
C:\Users\alvar>
```




```
os procesos. Ej. DNS local */
spuestas INPUT */
 */
uipos en WAN */
uipo en DMZ */
uipo en LAN */
uipo en LAN */
uipo en LAN */
uipo en LAN */
uipo en WLAN */
ermitir actualizaciones DNS,

en WAN */
ización NTP en WAN */
```

```
root@almellonesfernandez-us-intranet:~# netstat -putan | grep 22
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
tcp6       0     52 172.16.102.2:22         172.16.102.1:35080      ESTABLISHED 1876/sshd: root@pts
tcp6       0      0 172.16.102.2:22         172.18.102.3:57532      ESTABLISHED 1966/sshd: [accepte
root@almellonesfernandez-us-intranet:~#
```




```
Símbolo del sistema - ssh 172

C:\Users\alvar>ssh 172.16.102.2
The authenticity of host '172.16.102.2 (172.16.102.2)' can't be established.
ED25519 key fingerprint is SHA256:H9f74icsZoYw6LTiy+KQ8iZeSGl/UUq1A9stzqMSfgc.
This host key is known by the following other names/addresses:
    C:\Users\alvar/.ssh/known_hosts:13: [localhost]:5000
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:/etc/openvpn/server# tcpdump -i tun2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
20:10:45.010388 IP 172.18.102.3.52321 > dns.google.domain: 45142+ A? kv601.prod.do.dsp.mp.microsoft.com. (52)
20:10:45.121038 IP 172.18.102.3.60254 > dns.google.domain: 63687+ A? www.msftconnecttest.com. (41)
20:10:45.849097 IP 172.18.102.3.63236 > 192.168.40.1.domain: 24773+ A? www.google.com. (32)
20:10:46.010780 IP 172.18.102.3.52321 > 192.168.40.1.domain: 45142+ A? kv601.prod.do.dsp.mp.microsoft.com. (52)
20:10:46.121078 IP 172.18.102.3.60254 > 192.168.40.1.domain: 63687+ A? www.msftconnecttest.com. (41)
20:10:46.849088 IP 172.18.102.3.63236 > 192.168.40.1.domain: 24773+ A? www.google.com. (32)
20:10:46.905391 IP 172.18.102.3.57589 > dns.google.domain: 9894+ A? mtalk.google.com. (34)
20:10:46.905415 IP 172.18.102.3.51572 > dns.google.domain: 52476+ A? signaler-pa.clients6.google.com. (49)
20:10:47.010979 IP 172.18.102.3.52321 > 192.168.40.1.domain: 45142+ A? kv601.prod.do.dsp.mp.microsoft.com. (52)
20:10:47.121953 IP 172.18.102.3.60254 > 192.168.40.1.domain: 63687+ A? www.msftconnecttest.com. (41)
20:10:47.812626 IP 172.18.102.3.58156 > dns.google.domain: 37065+ A? chatgpt.com. (29)
20:10:47.906386 IP 172.18.102.3.57589 > 192.168.40.1.domain: 9894+ A? mtalk.google.com. (34)
20:10:47.906409 IP 172.18.102.3.51572 > 192.168.40.1.domain: 52476+ A? signaler-pa.clients6.google.com. (49)
20:10:48.813230 IP 172.18.102.3.58156 > 192.168.40.1.domain: 37065+ A? chatgpt.com. (29)
20:10:48.849406 IP 172.18.102.3.63236 > dns.google.domain: 24773+ A? www.google.com. (32)
20:10:48.849433 IP 172.18.102.3.63236 > 192.168.40.1.domain: 24773+ A? www.google.com. (32)
20:10:48.906847 IP 172.18.102.3.51572 > 192.168.40.1.domain: 52476+ A? signaler-pa.clients6.google.com. (49)
20:10:48.906870 IP 172.18.102.3.57589 > 192.168.40.1.domain: 9894+ A? mtalk.google.com. (34)
20:10:49.011522 IP 172.18.102.3.52321 > dns.google.domain: 45142+ A? kv601.prod.do.dsp.mp.microsoft.com. (52)
20:10:49.011546 IP 172.18.102.3.52321 > 192.168.40.1.domain: 45142+ A? kv601.prod.do.dsp.mp.microsoft.com. (52)
20:10:49.122879 IP 172.18.102.3.60254 > dns.google.domain: 63687+ A? www.msftconnecttest.com. (41)
20:10:49.122917 IP 172.18.102.3.60254 > 192.168.40.1.domain: 63687+ A? www.msftconnecttest.com. (41)
20:10:49.814166 IP 172.18.102.3.58156 > 192.168.40.1.domain: 37065+ A? chatgpt.com. (29)
20:10:50.683942 IP 172.18.102.3.58194 > 172.16.102.2.ssh: Flags [S], seq 3231048317, win 65535, options [mss 1400,nop,wscale 8,n
op,nop,sackOK], length 0
20:10:50.684330 IP 172.16.102.2.ssh > 172.18.102.3.58194: Flags [S.], seq 372418034, ack 3231048318, win 64240, options [mss 146
0,nop,nop,sackOK,nop,wscale 6], length 0
20:10:50.684714 IP 172.18.102.3.58194 > 172.16.102.2.ssh: Flags [.], ack 1, win 255, length 0
20:10:50.686128 IP 172.16.102.2.ssh > 172.18.102.3.58194: Flags [P.], seq 1:43, ack 1, win 1004, length 42: SSH: SSH-2.0-OpenSSH
```

Álvaro Almellones Fernández

CLIENTE VPN – TO – CLIENTES RED DMZ

6. (1 punto) Realice los cambios necesarios en el fichero de configuración del servidor VPN y de las reglas de iptables, para que se permita que los diferentes clientes openvpn una vez conectados, pueden alcanzar el equipo 10.0.?.2 de la red lan (ssh y web (80 y 443). Evidencie:

a. Cambios **exclusivos** en el fichero de configuración del servidor VPN para permitir dichas conexiones.

```
  GNU nano 7.2                                    server.conf
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses.  You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.102.0 255.255.255.0"
push "route 172.16.102.0 255.255.255.0"
push "route 10.0.102.0 255.255.255.0"


# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

^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
```

b. Reglas de iptables concretas para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

```
  GNU nano 7.2                          firewall-almellonesfernandez.sh
vpn-a-dmz() {

iptables -t filter -A FORWARD -i $tun -o $dmz -p tcp --dport 22 -d 10.0.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $tun -o $dmz -p tcp --dport 80 -d 10.0.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $tun -o $dmz -p tcp --dport 443 -d 10.0.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $tun -o $dmz -p icmp  -d 10.0.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $dmz -o $tun -m state --state  ESTABLISHED,RELATED -j ACCEPT
}

echo "Arrancado Cortafuegos de Alvaro Almellones. Bastionado de Redes y Sistemas"

variables # Carga de variables
generales # Reglas generales
loopback # Reglas de loopback
vpn-general
input # Reglas de input
squid
output # Reglas de output
dmz-a-wan # Reglas de dmz (zona naranja) a WAN
lan-a-wan # Reglas de intranet-lan (zona verde) a WAN
wlan-a-wan # Reglas de intranet-wlan (zona azul) a WAN
wan-a-dmz # Reglas de wan a dmz
lan-a-wlan
lan-a-dmz
vpn-a-lan
vpn-a-dmz

^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
```

c. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión al equipo 10.0.?.2, mediante un ping,

usando el cliente vpn linux.

Supongo que aquí te refieres a que compruebe que me puedo conectar al servidor web ya que en el enunciado pides que habilite web (80 y 443) igualmente he habilitado el ping

```
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: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
    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 prefix "L
AN 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 prefix "L
AN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2   0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2   0.0.0.0/0            172.16.102.2        tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2   0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2   0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   dmz2   0.0.0.0/0            10.0.102.2          tcp dpt:22
    0     0 ACCEPT     6    --  tun2   dmz2   0.0.0.0/0            10.0.102.2          tcp dpt:80
    0     0 ACCEPT     6    --  tun2   dmz2   0.0.0.0/0            10.0.102.2          tcp dpt:443
    0     0 ACCEPT     1    --  tun2   dmz2   0.0.0.0/0            10.0.102.2
    0     0 ACCEPT     0    --  dmz2   tun2   0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

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



```
almellonesfernandez@almellonesfernandez-VirtualBox:/etc/openvpn/client$ ping 10.0.102.2
PING 10.0.102.2 (10.0.102.2) 56(84) bytes of data.
64 bytes from 10.0.102.2: icmp_seq=1 ttl=63 time=1.65 ms
64 bytes from 10.0.102.2: icmp_seq=2 ttl=63 time=2.09 ms
^C
--- 10.0.102.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.645/1.865/2.086/0.220 ms
almellonesfernandez@almellonesfernandez-VirtualBox:/etc/openvpn/client$ sudo wget http://10.0.102.2
--2025-02-26 11:49:43--  http://10.0.102.2/
Conectando con 10.0.102.2:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 188 [text/html]
Guardando como: 'index.html.3'

index.html.3                100%[=================================================>]     188  --.-KB/s    en 0s

2025-02-26 11:49:43 (39,4 MB/s) - 'index.html.3' guardado [188/188]

almellonesfernandez@almellonesfernandez-VirtualBox:/etc/openvpn/client$ sudo wget https://10.0.102.2 --no-check-certificate
--2025-02-26 11:49:47--  https://10.0.102.2/
Conectando con 10.0.102.2:443... conectado.
AVISO: no se puede verificar el certificado de 10.0.102.2, emitido por 'CN=CA-almellonesfernandez':
  Se encontró un certificado autofirmado.
    AVISO: el nombre común 'almellonesfernandez-https' del certificado no encaja con el nombre de equipo '10.0.102.2' solicitado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 185 [text/html]
Guardando como: 'index.html.4'

index.html.4                100%[=================================================>]     185  --.-KB/s    en 0s

2025-02-26 11:49:47 (53,1 MB/s) - 'index.html.4' guardado [185/185]

almellonesfernandez@almellonesfernandez-VirtualBox:/etc/openvpn/client$
```

Álvaro Almellones Fernández

```
    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: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
    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 prefix "L
AN 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 prefix "L
AN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
   23  1728 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
   44  4066 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
   14  1176 ACCEPT     1    --  tun2   dmz2    0.0.0.0/0            10.0.102.2
   67 19632 ACCEPT     0    --  dmz2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   14  1476 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a o
tros procesos. Ej. DNS local */
  486 75884 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /*
Respuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces pi
ng */
```



```
root@almellonesfernandez-firewall:~/scripts# tcpdump -i tun2 port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
11:54:51.134059 IP 172.18.102.2.42154 > 10.0.102.2.http: Flags [S], seq 4094050949, win 64240, options [mss 1400,sackO
K,TS val 1780311894 ecr 0,nop,wscale 7], length 0
11:54:51.134636 IP 10.0.102.2.http > 172.18.102.2.42154: Flags [S.], seq 1324149082, ack 4094050950, win 65160, option
s [mss 1460,sackOK,TS val 2914445175 ecr 1780311894,nop,wscale 7], length 0
11:54:51.135655 IP 172.18.102.2.42154 > 10.0.102.2.http: Flags [.], ack 1, win 502, options [nop,nop,TS val 1780311896
 ecr 2914445175], length 0
11:54:51.136460 IP 172.18.102.2.42154 > 10.0.102.2.http: Flags [P.], seq 1:126, ack 1, win 502, options [nop,nop,TS va
l 1780311897 ecr 2914445175], length 125: HTTP: GET / HTTP/1.1
11:54:51.136952 IP 10.0.102.2.http > 172.18.102.2.42154: Flags [.], ack 126, win 509, options [nop,nop,TS val 29144451
77 ecr 1780311897], length 0
11:54:51.137739 IP 10.0.102.2.http > 172.18.102.2.42154: Flags [P.], seq 1:417, ack 126, win 509, options [nop,nop,TS
val 2914445178 ecr 1780311897], length 416: HTTP: HTTP/1.1 200 OK
11:54:51.139940 IP 172.18.102.2.42154 > 10.0.102.2.http: Flags [.], ack 417, win 501, options [nop,nop,TS val 17803118
99 ecr 2914445178], length 0
11:54:51.153873 IP 172.18.102.2.42154 > 10.0.102.2.http: Flags [F.], seq 126, ack 417, win 501, options [nop,nop,TS va
l 1780311912 ecr 2914445178], length 0
11:54:51.154707 IP 10.0.102.2.http > 172.18.102.2.42154: Flags [F.], seq 417, ack 127, win 509, options [nop,nop,TS va
l 2914445195 ecr 1780311912], length 0
11:54:51.156142 IP 172.18.102.2.42154 > 10.0.102.2.http: Flags [.], ack 418, win 501, options [nop,nop,TS val 17803119
16 ecr 2914445195], length 0
```

```
root@almellonesfernandez-firewall:~/scripts# tcpdump -i tun2 port 443
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
11:56:02.270853 IP 172.18.102.2.39260 > 10.0.102.2.https: Flags [S], seq 1824772777, win 64240, options [mss 1400,sack
OK,TS val 1780383031 ecr 0,nop,wscale 7], length 0
11:56:02.271550 IP 10.0.102.2.https > 172.18.102.2.39260: Flags [S.], seq 2479940404, ack 1824772778, win 65160, optio
ns [mss 1460,sackOK,TS val 2914516311 ecr 1780383031,nop,wscale 7], length 0
11:56:02.273043 IP 172.18.102.2.39260 > 10.0.102.2.https: Flags [.], ack 1, win 502, options [nop,nop,TS val 178038303
3 ecr 2914516311], length 0
11:56:02.273900 IP 172.18.102.2.39260 > 10.0.102.2.https: Flags [P.], seq 1:386, ack 1, win 502, options [nop,nop,TS v
al 1780383034 ecr 2914516311], length 385
11:56:02.274336 IP 10.0.102.2.https > 172.18.102.2.39260: Flags [.], ack 386, win 507, options [nop,nop,TS val 2914516
314 ecr 1780383034], length 0
11:56:02.278946 IP 10.0.102.2.https > 172.18.102.2.39260: Flags [.], seq 1:1389, ack 386, win 507, options [nop,nop,TS
 val 2914516319 ecr 1780383034], length 1388
11:56:02.278953 IP 10.0.102.2.https > 172.18.102.2.39260: Flags [.], seq 1389:2777, ack 386, win 507, options [nop,nop
,TS val 2914516319 ecr 1780383034], length 1388
11:56:02.278954 IP 10.0.102.2.https > 172.18.102.2.39260: Flags [P.], seq 2777:3658, ack 386, win 507, options [nop,no
p,TS val 2914516319 ecr 1780383034], length 881
11:56:02.281783 IP 172.18.102.2.39260 > 10.0.102.2.https: Flags [.], ack 1389, win 524, options [nop,nop,TS val 178038
3040 ecr 2914516319], length 0
11:56:02.282169 IP 172.18.102.2.39260 > 10.0.102.2.https: Flags [.], ack 2777, win 546, options [nop,nop,TS val 178038
3040 ecr 2914516319], length 0
11:56:02.282752 IP 172.18.102.2.39260 > 10.0.102.2.https: Flags [.], ack 3658, win 568, options [nop,nop,TS val 178038
3040 ecr 2914516319], length 0
11:56:02.282978 IP 172.18.102.2.39260 > 10.0.102.2.https: Flags [P.], seq 386:466, ack 3658, win 568, options [nop,nop
,TS val 1780383042 ecr 2914516319], length 80
```

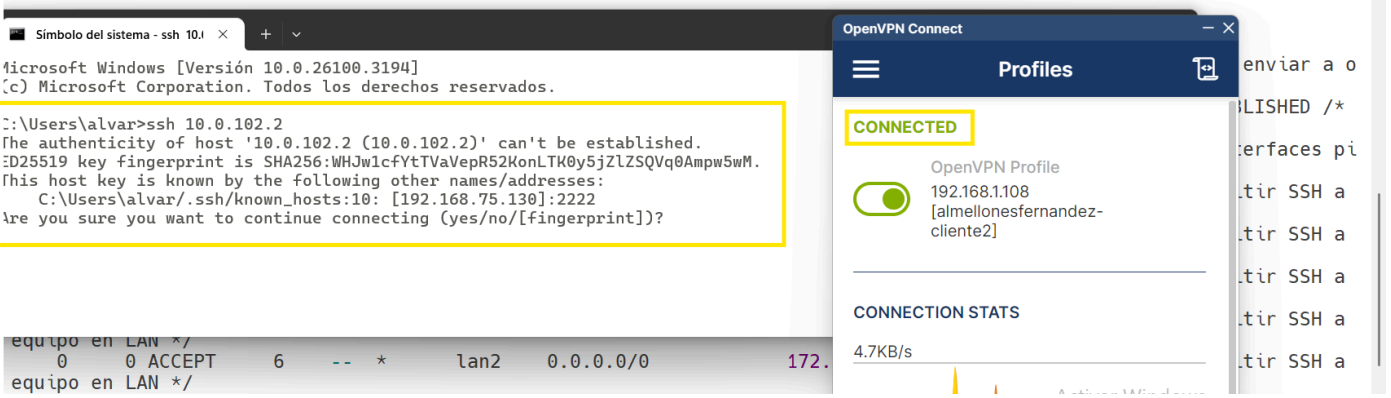
Álvaro Almellones Fernández

d. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión al equipo 10.0.?.2, mediante una conexión por ssh, usando el cliente openvpn GUI de Windows.

```
    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: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
    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 prefix "L
AN 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 prefix "L
AN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     1    --  tun2   dmz2    0.0.0.0/0            10.0.102.2
    0     0 ACCEPT     0    --  dmz2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 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 o
tros procesos. Ej. DNS local */
   10   896 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /*
```



```
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "L
 AN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    7  1805 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     1    --  tun2   dmz2    0.0.0.0/0            10.0.102.2
    6  1906 ACCEPT     0    --  dmz2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
```

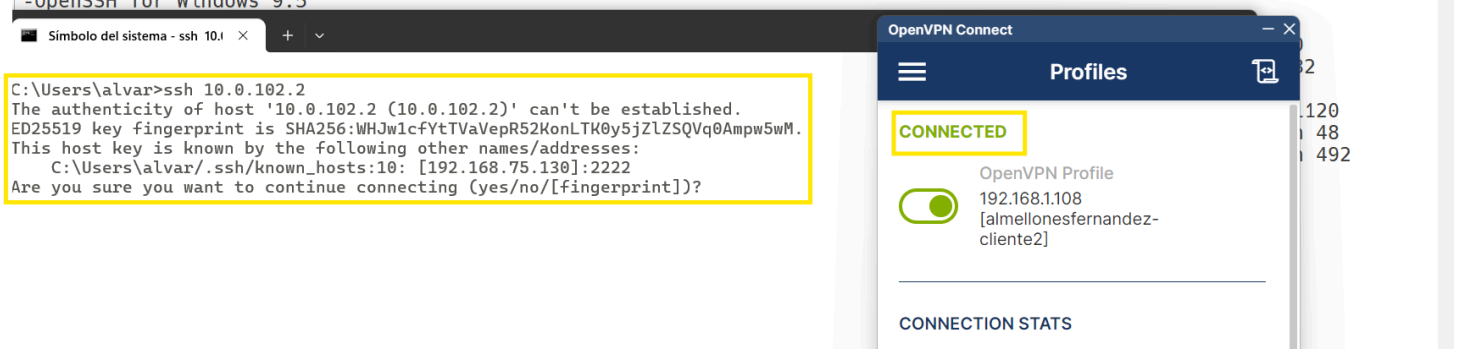



```
equipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.
equipo en LAN */
```

Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-us-dmz:/etc/apache2/sites-available$ sudo netstat -putan |grep 22
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
tcp6       0      1 10.0.102.2:22           172.18.102.3:50561      FIN_WAIT1   -
tcp6       0      0 10.0.102.2:22           172.18.102.3:51163      ESTABLISHED 2022/sshd: [accepte
tcp6       0      0 10.0.102.2:22           10.0.102.1:34616        ESTABLISHED 1723/sshd: almellon
almellonesfernandez@almellonesfernandez-us-dmz:/etc/apache2/sites-available$
```


```
root@almellonesfernandez-firewall:~/scripts# tcpdump -i tun2 port 22
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
12:06:09.701743 IP 172.18.102.3.51723 > 10.0.102.2.ssh: Flags [S], seq 2264080337, win 65535, options [mss 1400,nop,ws
cale 8,nop,nop,sackOK], length 0
12:06:09.702135 IP 10.0.102.2.ssh > 172.18.102.3.51723: Flags [S.], seq 966149143, ack 2264080338, win 64240, options
[mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
12:06:09.702640 IP 172.18.102.3.51723 > 10.0.102.2.ssh: Flags [.], ack 1, win 255, length 0
12:06:09.703879 IP 10.0.102.2.ssh > 172.18.102.3.51723: Flags [P.], seq 1:43, ack 1, win 502, length 42: SSH: SSH-2.0-
OpenSSH_9.6p1 Ubuntu-3ubuntu13.5
12:06:09.704974 IP 172.18.102.3.51723 > 10.0.102.2.ssh: Flags [P.], seq 1:34, ack 43, win 255, length 33: SSH: SSH-2.0
-OpenSSH for Windows 9.5
```



Álvaro Almellones Fernández

CLIENTE VPN – TO – CLIENTES RED WAN o INTERNET

7. (1 punto) Realice los cambios necesarios en el fichero de configuración del servidor VPN y de las reglas de iptables, para que se permita que los diferentes clientes openvpn una vez conectados, pueden alcanzar la red wan. Evidencie:

a. Cambios **exclusivos** en el fichero de configuración del servidor VPN para permitir dichas conexiones.

```
  GNU nano 7.2                                    server.conf
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"
;push "redirect-gateway def1"
push "redirect-gateway local def1"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
;push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 192.168.40.1"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.

^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
```


b. Reglas de iptables concretas para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

```
  GNU nano 7.2                          firewall-almellonesfernandez.sh
iptables -t filter -A FORWARD -i $tun -o $dmz -p tcp --dport 80 -d 10.0.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $tun -o $dmz -p tcp --dport 443 -d 10.0.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $tun -o $dmz -p icmp  -d 10.0.102.2 -j ACCEPT
iptables -t filter -A FORWARD -i $dmz -o $tun -m state --state  ESTABLISHED,RELATED -j ACCEPT
}

vpn-a-wan() {
        iptables -t nat -A POSTROUTING -s 172.18.102.0/24 -o $wan -j MASQUERADE

        iptables -t filter -A FORWARD -i $tun -o $wan -p tcp --dport 80 -j ACCEPT
        iptables -t filter -A FORWARD -i $tun -o $wan -p tcp --dport 443 -j ACCEPT
        iptables -t filter -A FORWARD -i $tun -o $wan -p udp --dport 53 -j ACCEPT
        iptables -t filter -A FORWARD -i $tun -o $wan -p icmp -j ACCEPT
        iptables -t filter -A FORWARD -i $wan -o $tun -m state --state  ESTABLISHED,RELATED -j ACCEPT
}

echo "Arrancado Cortafuegos de Alvaro Almellones. Bastionado de Redes y Sistemas"

variables # Carga de variables
generales # Reglas generales
loopback # Reglas de loopback
vpn-general
input # Reglas de input
squid
output # Reglas de output
dmz-a-wan # Reglas de dmz (zona naranja) a WAN
lan-a-wan # Reglas de intranet-lan (zona verde) a WAN
```

Álvaro Almellones Fernández

c. Capturas de éxito (contadores de iptables y traceroute) de la conexión a cualquier equipo de la zona WAN por su IP (ping). Muestre que se han creado las rutas para alcanzar dicha red (ip route)

```
    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 prefix "L
AN 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 prefix "L
AN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     1    --  tun2   dmz2    0.0.0.0/0            10.0.102.2
    0     0 ACCEPT     0    --  dmz2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     0    --  wan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED

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 o
tros procesos. Ej. DNS local */
    6   528 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /*
Respuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces pi
ng */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a
equipos en WAN */
    0     0 ACCEPT     6    --  *      dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 /* Permitir SSH a
```


A parte del ping voy a realizar un curl para comprobar la conexión a web

Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-VirtualBox ~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=19.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=18.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=17.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=17.5 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 17.504/18.239/18.965/0.613 ms
almellonesfernandez@almellonesfernandez-VirtualBox:~$ wget http://8.8.8.8
--2025-02-27 16:12:44--  http://8.8.8.8/
Conectando con 8.8.8.8:80... ^C
almellonesfernandez@almellonesfernandez-VirtualBox:~$ wget https://8.8.8.8
--2025-02-27 16:12:50--  https://8.8.8.8/
Conectando con 8.8.8.8:443... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Ubicación: https://dns.google/ [siguiente]
--2025-02-27 16:12:50--  https://dns.google/
Resolviendo dns.google (dns.google)... 8.8.4.4, 8.8.8.8, 2001:4860:4860::8888, ...
Conectando con dns.google (dns.google)[8.8.4.4]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: no especificado [text/html]
Guardando como: 'index.html.3'

index.html.3                    [ <=>                                   ]   1,35K  --.-KB/s    en 0s

2025-02-27 16:12:50 (22,1 MB/s) - 'index.html.3' guardado [1381]

almellonesfernandez@almellonesfernandez-VirtualBox:~$
```

El wget de http a google no funciona ya que todo funciona cifrado como se puede observar que por https si funciona

```
    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 prefix "L
AN 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 prefix "L
AN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     1    --  tun2   dmz2    0.0.0.0/0            10.0.102.2
    0     0 ACCEPT     0    --  dmz2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    2   120 ACCEPT     6    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:80
   26  2632 ACCEPT     6    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:53
    4   336 ACCEPT     1    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0
   23 14495 ACCEPT     0    --  wan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED

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 o
tros procesos. Ej. DNS local */
   42 17311 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /*
Respuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces pi
ng */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a
```


El único contador que no ha aumentado es el que acepta DNS ya que hemos realizado la búsqueda

Álvaro Almellones Fernández

por su ip 8.8.8.8(Google)

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# traceroute -I 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  4.337 ms  3.864 ms *
 2  192.168.144.1 (192.168.144.1)  4.582 ms * *
 3  145.red-81-41-221.staticip.rima-tde.net (81.41.221.145)  6.278 ms * *
 4  * * *
 5  * * *
 6  176.52.253.97 (176.52.253.97)  17.661 ms  15.578 ms  17.026 ms
 7  5.53.1.82 (5.53.1.82)  16.133 ms  17.869 ms  17.076 ms
 8  108.170.225.251 (108.170.225.251)  16.797 ms  17.333 ms  16.886 ms
 9  142.251.54.153 (142.251.54.153)  16.550 ms  16.137 ms  16.354 ms
10  dns.google (8.8.8.8)  15.636 ms  15.631 ms  15.386 ms
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# traceroute -I 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  172.18.102.1 (172.18.102.1)  1.425 ms  3.330 ms *
 2  _gateway (192.168.1.1)  8.275 ms  15.155 ms *
 3  192.168.144.1 (192.168.144.1)  15.167 ms  15.170 ms *
 4  145.red-81-41-221.staticip.rima-tde.net (81.41.221.145)  20.027 ms  20.033 ms *
 5  * * *
 6  * * *
 7  176.52.253.97 (176.52.253.97)  71.624 ms  50.344 ms  49.323 ms
 8  5.53.1.82 (5.53.1.82)  19.524 ms  17.883 ms  17.878 ms
 9  108.170.225.251 (108.170.225.251)  19.415 ms  17.461 ms  17.475 ms
10  142.251.54.153 (142.251.54.153)  21.205 ms  21.244 ms  21.267 ms
11  dns.google (8.8.8.8)  21.253 ms  28.508 ms  17.751 ms
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez#
```

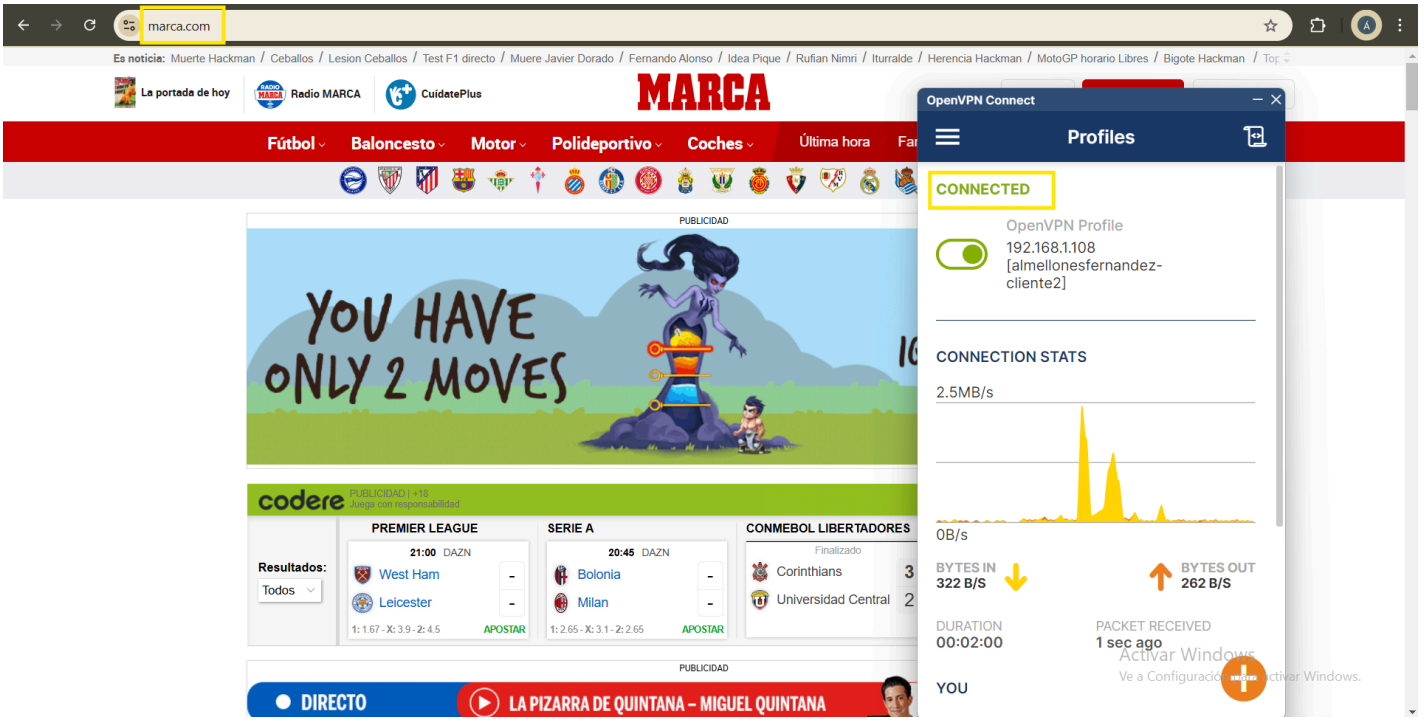
Antes de activar la vpn vemos que la ruta comienza desde la gateway de nuestra red pero al activar la vpn observamos que comienza desde la red tun

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# ip route
0.0.0.0/1 via 172.18.102.1 dev tun2
default via 192.168.1.1 dev enp0s3 proto dhcp src 192.168.1.111 metric 100
10.0.102.0/24 via 172.18.102.1 dev tun2
128.0.0.0/1 via 172.18.102.1 dev tun2
172.16.102.0/24 via 172.18.102.1 dev tun2
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.18.102.0/24 dev tun2 proto kernel scope link src 172.18.102.2
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.111 metric 100
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez#
```

d. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión a cualquier equipo de la zona WAN por su nombre dns (servidor web de internet), usando el cliente OpenVPN GUI de Windows.

Álvaro Almellones Fernández

```
    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 prefix "L
AN 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 prefix "L
AN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     1    --  tun2   dmz2    0.0.0.0/0            10.0.102.2
    0     0 ACCEPT     0    --  dmz2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  tun2   wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     0    --  wan2   tun2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED

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 o
tros procesos. Ej. DNS local */
   12  1056 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /*
Respuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces pi
```

Álvaro Almellones Fernández

```
    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 prefix "L
AN 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 prefix "L
AN to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  tun2   lan2    0.0.0.0/0            172.16.102.2        tcp dpt:22
    0     0 ACCEPT     1    --  tun2   lan2    0.0.0.0/0            172.16.102.2
    0     0 ACCEPT     0    --  lan2   tun2    0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2          tcp dpt:22
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2          tcp dpt:80
    0     0 ACCEPT     6    --  tun2   dmz2    0.0.0.0/0            10.0.102.2          tcp dpt:443
    0     0 ACCEPT     1    --  tun2   dmz2    0.0.0.0/0            10.0.102.2
    0     0 ACCEPT     0    --  dmz2   tun2    0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
   71  5148 ACCEPT     6    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0           tcp dpt:80
10004 2746K ACCEPT     6    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0           tcp dpt:443
  203 13458 ACCEPT     17   --  tun2   wan2    0.0.0.0/0            0.0.0.0/0           udp dpt:53
    0     0 ACCEPT     1    --  tun2   wan2    0.0.0.0/0            0.0.0.0/0
 8348 9657K ACCEPT     0    --  wan2   tun2    0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

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 o
tros procesos. Ej. DNS local */
12369   10M ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED /*
Respuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           /* OUTPUT todas interfaces pi
ng */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH a
equipos en WAN */
    0     0 ACCEPT     6    --  *      dmz2    0.0.0.0/0            10.0.102.2          tcp dpt:22 /* Permitir SSH a
```



```
root@almellonesfernandez-firewall:~/scripts# tcpdump -i tun2 port 443
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun2, link-type RAW (Raw IP), snapshot length 262144 bytes
16:47:01.301466 IP mad41s11-in-f10.1e100.net.https > 172.18.102.3.59663: Flags [P.], seq 4139608592:4139608665, ack 25
50821700, win 1050, length 73
16:47:01.302414 IP 172.18.102.3.59663 > mad41s11-in-f10.1e100.net.https: Flags [F.], seq 1, ack 73, win 254, length 0
16:47:01.318709 IP mad41s11-in-f10.1e100.net.https > 172.18.102.3.59663: Flags [F.], seq 73, ack 2, win 1050, length 0
16:47:01.319390 IP 172.18.102.3.59663 > mad41s11-in-f10.1e100.net.https: Flags [.], ack 74, win 254, length 0
16:47:02.729440 IP 172.18.102.3.59895 > mad41s07-in-f14.1e100.net.https: Flags [.], seq 1357267852:1357267853, ack 332
9937512, win 255, length 1
16:47:02.744112 IP mad41s07-in-f14.1e100.net.https > 172.18.102.3.59895: Flags [.], ack 1, win 1043, options [nop,nop,
sack 1 {0:1}], length 0
16:47:02.805263 IP 172.18.102.3.59950 > par21s22-in-f3.1e100.net.https: Flags [.], seq 1240133037:1240133038, ack 2223
128701, win 254, length 1
16:47:02.835873 IP par21s22-in-f3.1e100.net.https > 172.18.102.3.59950: Flags [.], ack 1, win 1044, options [nop,nop,s
ack 1 {0:1}], length 0
16:47:02.843119 IP 172.18.102.3.59898 > mad01s26-in-f163.1e100.net.https: Flags [.], seq 1524680663:1524680664, ack 41
58764362, win 253, length 1
16:47:02.873639 IP mad01s26-in-f163.1e100.net.https > 172.18.102.3.59898: Flags [.], ack 1, win 1038, options [nop,nop
,sack 1 {0:1}], length 0
16:47:03.037810 IP mad07s09-in-f10.1e100.net.https > 172.18.102.3.59628: Flags [P.], seq 1726932437:1726932623, ack 24
4436935, win 1050, length 186
16:47:03.038587 IP 172.18.102.3.59628 > mad07s09-in-f10.1e100.net.https: Flags [P.], seq 1:36, ack 186, win 252, lengt
```

Álvaro Almellones Fernández

8. (1 punto) Realice los cambios necesarios en el fichero de configuración de squid y de las reglas de iptables, para que se pueda alcanzar la red WAN desde cliente VPN haciendo uso del squid en modo transparente por el puerto 3130, cortando la página http://httpforever.com y direccionándola con deny_info personalizado para la red VPN/denegación, como por ejemplo la Web solicitada desde la red VPN con la IP ----, no puede ser descargada.

a. Cambios **exclusivos** en el fichero de configuración del servidor VPN para permitir dichas conexiones.

Aqui supongo que quieres que te muestre lo que he modificado en el archivo de configuración del squid ya que para realizar este ejercicio no he tenido que realizar ningún cambio en el archivo de configuración del servidor VPN

```
  GNU nano 7.2                              almellonesfernandez-squid.conf
http_port 172.16.102.1:3128 intercept #Zona LAN  transparente
http_port 172.18.102.1:3130 intercept #Zona VPN  transparente
http_port 192.168.102.1:3129 intercept #Zona Wlan transparente

acl RedWlan src 192.168.102.0/24 ##Zona transparente
acl Redlan src 172.16.102.0/24 ##Zona transparente
acl RedVPN src 172.18.102.0/24 ##Zona transparente


#deny_info https://www.naughtydog.com/  all

visible_hostname proxyAlmellonesfernandez.es

logformat almellonesfernandez_formato %ts %tg %>a %<a %ul %un %>rm %ru  HTTP/%rv %Sh/%<A %>Hs %<st %rm %ru %>a "%{Ref>

access_log daemon:/var/log/squid/accessAlmellonesfernandez-squid.log
access_log daemon:/var/log/squid/accessAlmellonesfernandez-combined.log combined
access_log daemon:/var/log/squid/accessAlmellonesfernandez-personalizado.log almellonesfernandez_formato
```

```
  GNU nano 7.2                              almellonesfernandez-squid.conf
acl bloqueo_vpn url_regex httpforever

http_access deny bloqueo_vpn
deny_info https://www.game.es/ bloqueo_vpn


#http_reply_access deny bloqueo_imagenes
#http_access deny bloqueo_metodo_get


#http_access allow mac_Windows

#http_access allow Hora_Allow_All Redlan

#http_access deny lista_url_prohibidas_aaf
#deny_info https://www.game.es/  lista_url_prohibidas_aaf

#http_access deny lista_Navegadores_prohibidos_aaf

#http_access deny Lista_Dominios_Prohibidos_aaf
#deny_info https://www.eroski.es/  Lista_Dominios_Prohibidos_aaf


http_access allow all
#http_access allow RedWlan
#http_access allow Redlan

^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
```

b. Reglas de iptables concretas para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

```
  GNU nano 7.2                                  firewall-almellonesfernandez.sh
        iptables -t filter -A FORWARD -i $wan -o $tun -m state --state  ESTABLISHED,RELATED -j ACCEPT
}

vpn-squid() {

        iptables -t filter -A INPUT -i $tun -p tcp --dport 3130 -j ACCEPT  -m comment --comment "Zona VPN"
        iptables -t nat -A PREROUTING -i $tun -s 172.18.102.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3130

}

echo "Arrancado Cortafuegos de Alvaro Almellones. Bastionado de Redes y Sistemas"

variables # Carga de variables
generales # Reglas generales
loopback # Reglas de loopback
vpn-general
input # Reglas de input
squid
vpn-squid
output # Reglas de output
dmz-a-wan # Reglas de dmz (zona naranja) a WAN
lan-a-wan # Reglas de intranet-lan (zona verde) a WAN
wlan-a-wan # Reglas de intranet-wlan (zona azul) a WAN
wan-a-dmz # Reglas de wan a dmz
lan-a-wlan
lan-a-dmz
vpn-a-lan
```

c. Capturas de éxito (contadores de iptables tanto en tabla filter como en tabla nat, tráfico en tcpdump, netstat) de la conexión a cualquier equipo de la zona WAN por su nombre dns (servidor web de internet), usando el cliente OpenVPN Connect de Windows o terminal (wget,curl), donde se demuestre que el tráfico está siendo interceptado, direccionado y gestionado por el squid en el puerto 3130.

```
root@almellonesfernandez-firewall:~/scripts# iptables -t filter -L -n -v
Chain INPUT (policy DROP 1 packets, 244 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
    0     0 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1194 /* Permitir el p
uerto que usa VPN */
    0     0 ACCEPT     1    --  tun2   *       0.0.0.0/0            0.0.0.0/0           /* Permitir hacer ping desde
la tun a firewall */
    0     0 ACCEPT     6    --  tun2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir ssh de
sde tun */
   21  1320 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH de
sde WAN */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           /* Permitir ping desde cualqu
ier subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH de
sde LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* Permitir SSH de
sde DMZ */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3128 /* Zona LAN */
    0     0 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3129 /* Zona WLAN */
    0     0 ACCEPT     6    --  tun2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3130 /* Zona VPN */
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED /*
Respuestas OUTPUT */
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 15 packets, 706 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 3128
    0     0 REDIRECT   6    --  wlan2  *       192.168.102.0/24     0.0.0.0/0            tcp dpt:80 redir ports 3129
    0     0 REDIRECT   6    --  tun2   *       172.18.102.0/24      0.0.0.0/0            tcp dpt:80 redir ports 3130
    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: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:10.0.102.2:80
80
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8404 to:10.0.102.2:84
04
    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 WAN */
    0     0 MASQUERADE  0    --  *      wan2    172.18.102.0/24      0.0.0.0/0
root@almellonesfernandez-firewall:~/scripts#
```

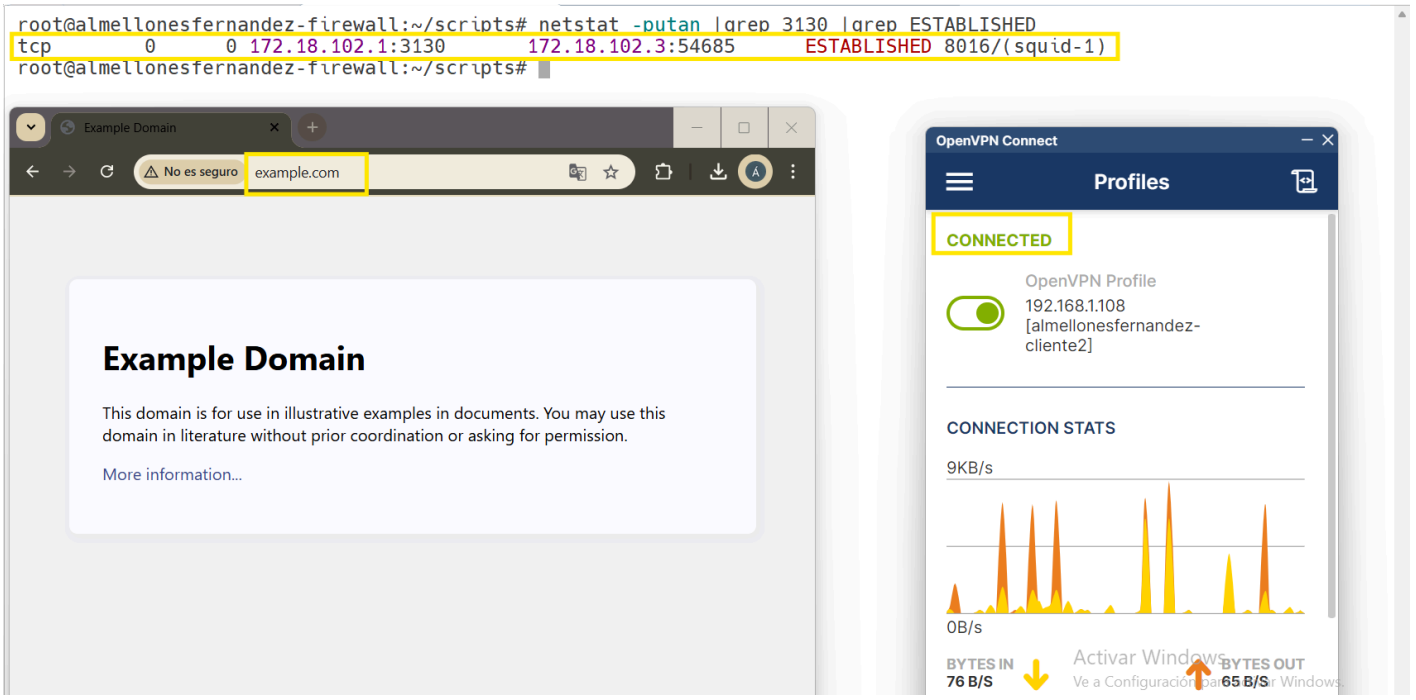
```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# wget http://example.com
--2025-02-27 17:46:02--  http://example.com/
Resolviendo example.com (example.com)... 23.192.228.80, 23.192.228.84, 23.215.0.136, ...
Conectando con example.com (example.com)[23.192.228.80]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1256 (1,2K) [text/html]
Guardando como: ‘index.html.6’

index.html.6                100%[=================================================>]   1,23K  --.-KB/s    en 0,009s

2025-02-27 17:46:02 (134 KB/s) - ‘index.html.6’ guardado [1256/1256]

root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# wget http://httpforever.com
--2025-02-27 17:46:16--  http://httpforever.com/
Resolviendo httpforever.com (httpforever.com)... 146.190.62.39, 2604:a880:4:1d0::1f1:2000
Conectando con httpforever.com (httpforever.com)[146.190.62.39]:80... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Ubicación: https://www.game.es/ [siguiente]
--2025-02-27 17:46:16--  https://www.game.es/
Resolviendo www.game.es (www.game.es)... 212.170.159.195
Conectando con www.game.es (www.game.es)[212.170.159.195]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1395630 (1,3M) [text/html]
Guardando como: ‘index.html.7’

index.html.7                100%[=================================================>]   1,33M  2,56MB/s    en 0,5s

2025-02-27 17:46:17 (2,56 MB/s) - ‘index.html.7’ guardado [1395630/1395630]

root@almellonesfernandez-VirtualBox:/home/almellonesfernandez#
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 39 packets, 1624 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 3128
    0     0 REDIRECT   6    --  wlan2  *       192.168.102.0/24     0.0.0.0/0            tcp dpt:80 redir ports 3129
    3   180 REDIRECT   6    --  tun2   *       172.18.102.0/24      0.0.0.0/0            tcp dpt:80 redir ports 3130
    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: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:10.0.102.2:80
80
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:8404 to:10.0.102.2:84
04
    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 11 packets, 759 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 WAN */
    1    60 MASQUERADE  0    --  *      wan2    172.18.102.0/24      0.0.0.0/0
root@almellonesfernandez-firewall:~/scripts#
```

```
root@almellonesfernandez-firewall:~/scripts# iptables -t filter -L -n -v
Chain INPUT (policy DROP 33 packets, 1406 bytes)
 pkts bytes target     prot opt in     out     source               destination
   12  1608 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
  736 76761 ACCEPT     17   --  wan2   *       0.0.0.0/0            0.0.0.0/0            udp dpt:1194 /* Permitir el p
uerto que usa VPN */
    0     0 ACCEPT     1    --  tun2   *       0.0.0.0/0            0.0.0.0/0            /* Permitir hacer ping desde
la tun a firewall */
    0     0 ACCEPT     6    --  tun2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir ssh de
sde tun */
  146  9392 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH de
sde WAN */
    7   270 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualqu
ier subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH de
sde LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH de
sde DMZ */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3128 /* Zona LAN */
    0     0 ACCEPT     6    --  wlan2  *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3129 /* Zona WLAN */
   20  1420 ACCEPT     6    --  tun2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3130 /* Zona VPN */
   14  3431 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /*
Respuestas OUTPUT */

Chain FORWARD (policy DROP 6 packets, 456 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:443 STRING match  "ma
rca.com" ALGO name bm /* Bloquear https de marca */ reject-with icmp-port-unreachable
```

Álvaro Almellones Fernández



d. Capturas de que se produce la denegación de la web deny_info, muestra en access.log de la denegación a la IP de la red VPN, etc.)

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# wget http://httpforever.com
--2025-02-27 17:21:11--  http://httpforever.com/
Resolviendo httpforever.com (httpforever.com)... 146.190.62.39, 2604:a880:4:1d0::1f1:2000
Conectando con httpforever.com (httpforever.com)[146.190.62.39]:80... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Ubicación: https://www.game.es/ [siguiente]
--2025-02-27 17:21:11--  https://www.game.es/
Resolviendo www.game.es (www.game.es)... 212.170.159.195
Conectando con www.game.es (www.game.es)[212.170.159.195]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1356358 (1,3M) [text/html]
Guardando como: ‘index.html.4’

index.html.4                100%[=================================================>]   1,29M  2,58MB/s    en 0,5s

2025-02-27 17:21:12 (2,58 MB/s) - ‘index.html.4’ guardado [1356358/1356358]

root@almellonesfernandez-VirtualBox:/home/almellonesfernandez#
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:/var/log/squid# tail -f  accessAlmellonesfernandez-combined.log
172.18.102.3 - - [27/Feb/2025:17:23:14 +0100] "GET http://httpforever.com/ HTTP/1.1" 302 338 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36" TCP_DENIED:HIER_NONE
172.18.102.3 - - [27/Feb/2025:17:23:27 +0100] "GET http://www.msftncsi.com/connecttest.txt HTTP/1.1" 200 296 "-" "Microsoft NCSI" TCP_MISS:ORIGINAL_DST
172.18.102.3 - - [27/Feb/2025:17:23:40 +0100] "GET http://www.msftncsi.com/connecttest.txt HTTP/1.1" 200 296 "-" "Microsoft NCSI" TCP_MISS:ORIGINAL_DST
172.18.102.3 - - [27/Feb/2025:17:23:40 +0100] "GET http://www.msftncsi.com/connecttest.txt HTTP/1.1" 200 296 "-" "Microsoft NCSI" TCP_MISS:ORIGINAL_DST
172.18.102.3 - - [27/Feb/2025:17:23:40 +0100] "GET http://www.msftncsi.com/connecttest.txt HTTP/1.1" 200 296 "-" "Microsoft NCSI" TCP_MISS:ORIGINAL_DST
172.18.102.3 - - [27/Feb/2025:17:23:40 +0100] "GET http://www.msftncsi.com/connecttest.txt HTTP/1.1" 200 296 "-" "Microsoft NCSI" TCP_MISS:ORIGINAL_DST
172.18.102.3 - - [27/Feb/2025:17:24:03 +0100] "GET http://www.msftncsi.com/connecttest.txt HTTP/1.1" 200 296 "-" "Microsoft NCSI" TCP_MISS:ORIGINAL_DST
172.18.102.2 - - [27/Feb/2025:17:26:05 +0100] "GET http://connectivity-check.ubuntu.com/ HTTP/1.1" 204 294 "-" "-" TCP_MISS:ORIGINAL_DST
172.18.102.2 - - [27/Feb/2025:17:31:05 +0100] "GET http://connectivity-check.ubuntu.com/ HTTP/1.1" 204 294 "-" "-" TCP_MISS:ORIGINAL_DST
172.18.102.3 - - [27/Feb/2025:17:32:56 +0100] "GET http://httpforever.com/ HTTP/1.1" 302 338 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36" TCP_DENIED:HIER_NONE
172.18.102.3 - - [27/Feb/2025:17:33:56 +0100] "GET http://httpforever.com/ HTTP/1.1" 302 338 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36" TCP_DENIED:HIER_NONE
172.18.102.3 - - [27/Feb/2025:17:33:56 +0100] "- error:transaction-end-before-headers NONE/0.0" 0 0 "-" "-" NONE_NONE:HIER_NONE
172.18.102.2 - - [27/Feb/2025:17:34:33 +0100] "GET http://httpforever.com/ HTTP/1.1" 302 338 "-" "Wget/1.21.4" TCP_DENIED:HIER_NONE
```

Álvaro Almellones Fernández

CONEXIÓN CLIENTE WINDOWS VPN DESDE INTERNET a SERVIDOR VPN en vuestra casa

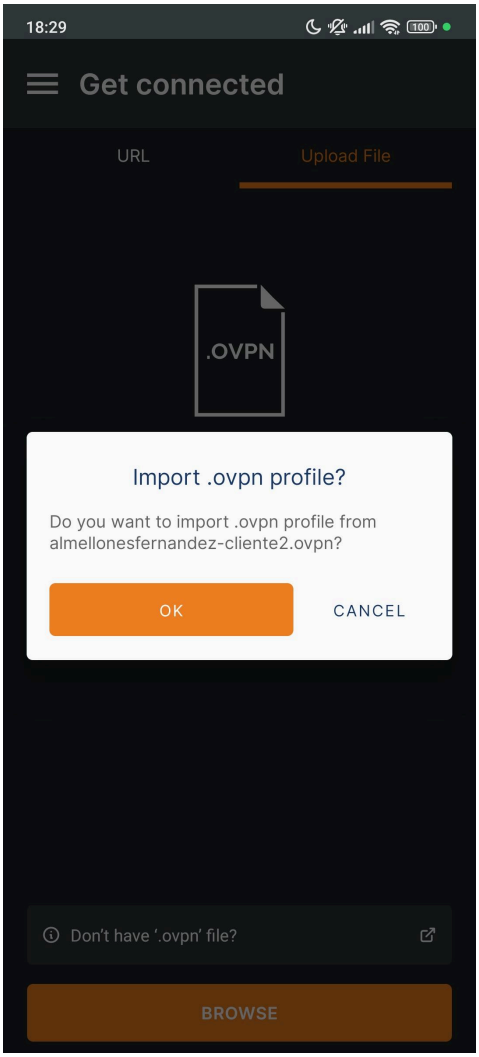
9. **(0,5 puntos) (investigación)** En este caso el cliente VPN tiene que estar en Internet (no por delante del servidor VPN), para ello podéis hacer uso de un cliente VPN de algún compañero (tendréis que proporcionales un par de llaves y los ficheros necesarios.

a. Cambios **exclusivos** en el fichero de configuración del cliente (fichero .ovpn) (cambia la opción remote IP) y del servidor para permitir dichas conexiones y configuración realizada en el router de vuestra casa para que se haga NAT desde la zona WAN a vuestro servidor VPN.

b. Se deja a elección del alumno que el tráfico viaja desde el cliente, al router y posteriormente al servidor VPN, y que se produce la conexión adecuadamente (capturas de apartados del router, netstat, tcpdump, etc.).

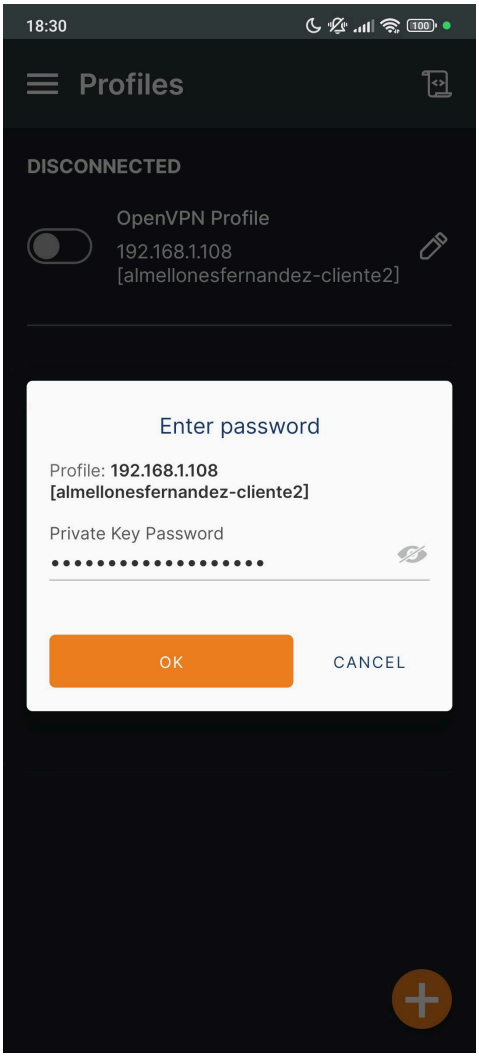
Caso de que no sea posible realizar estas configuraciones en el router de Casa, se puede cambiar este ejercicio por realizar una conexión como cliente desde un Smartphone/Tablet.

Para conectarme desde el movil solo tenemos que importar nuestro archivo .ovpn y descargarse una aplicación como OpenVPN

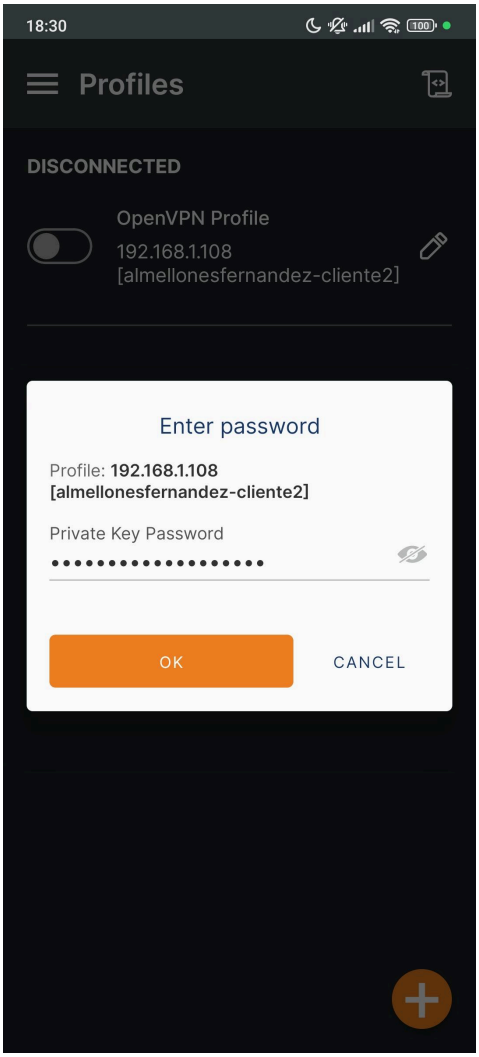


Álvaro Almellones Fernández

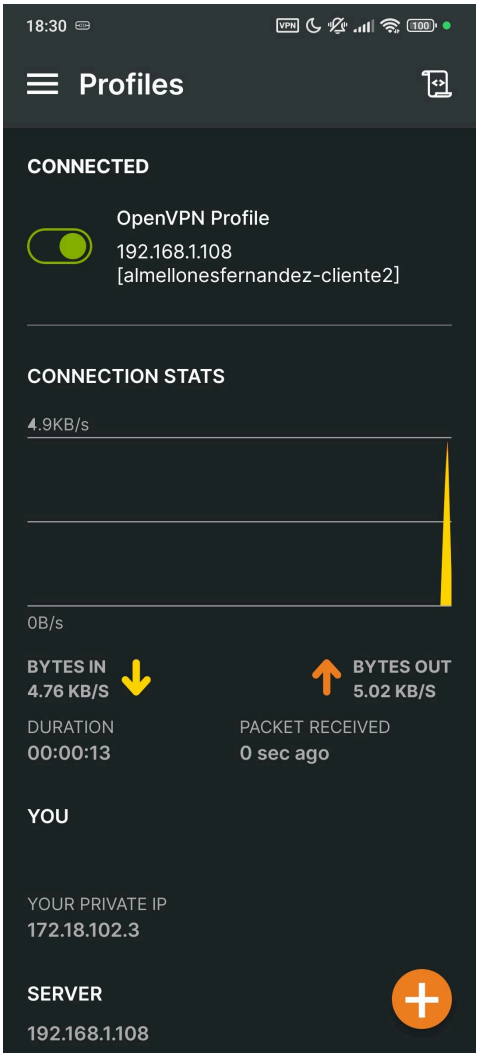
Álvaro Almellones Fernández



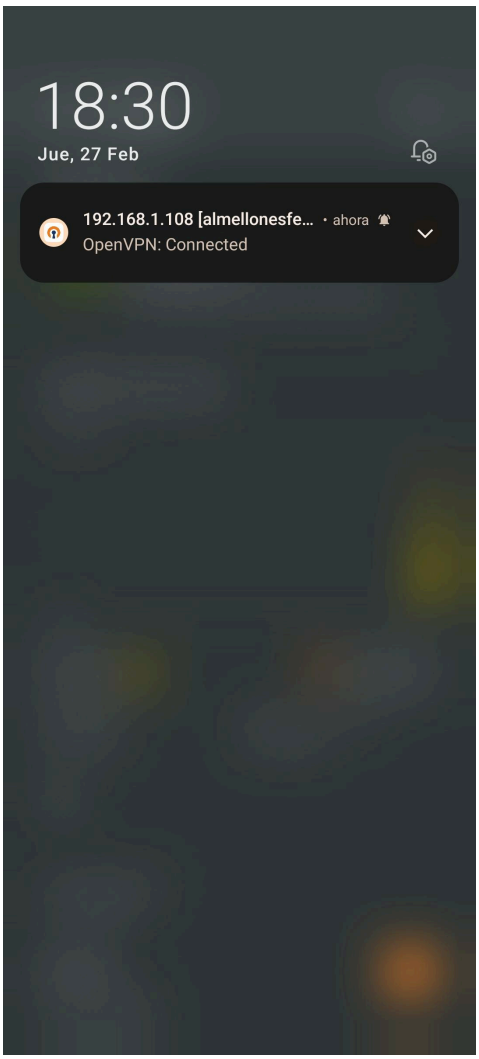
Álvaro Almellones Fernández



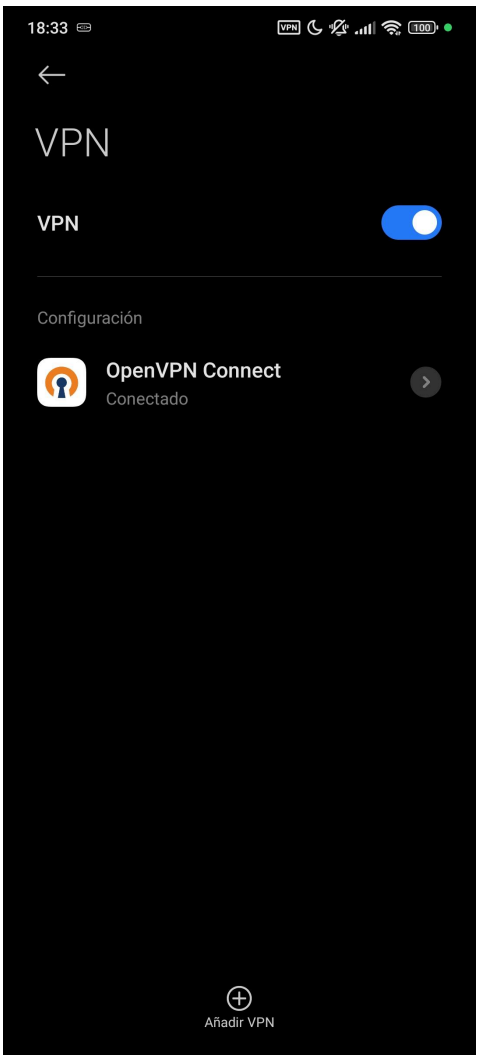
Álvaro Almellones Fernández



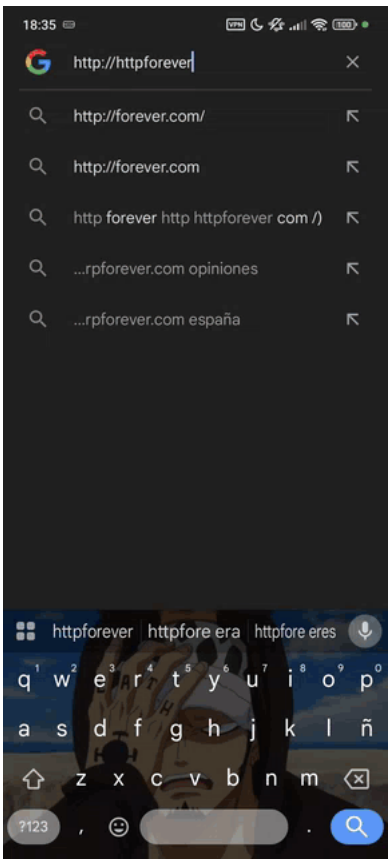
Álvaro Almellones Fernández



Álvaro Almellones Fernández



Álvaro Almellones Fernández



Para comprobar que estoy conectado desde el movil busco httpforever ya que la regla de squid del ejercicio anterior si estoy conectado a la vpn me redirecciona a la pagina deny_info (game) como se observa en la imagen

Álvaro Almellones Fernández

PARTE LAN-TO-LAN 2. CONEXIÓN DE SEDES CENTRALES Y SUCURSALES.

10. **(1 punto) (investigación)** En este caso tendréis que configurar dos firewalls (central y sucursal/franquicia de una empresa). O se monta dos infraestructuras o se hace uso de la infraestructura (sede) de un compañero de clase.

a. Captura del fichero de configuración del servidor VPN central con las opciones concretas para realizar LAN-TO LAN.
b. Pruebas de funcionamiento tal y como aparece en el manual con la sede (únicamente conexiones con redes de la sede principal, no con otras sedes ya que estas implican tener más de dos sedes).

Ejercicio no realizado por que no me iba a dar tiempo antes de la fecha limite