

Memoria de la práctica 2:

Principios básicos de tunneling y VPN con OpenVPN

Laboratorio de Redes y Servicios Avanzados

Curso 2023-2024

Equipo que hace la entrega:

Apellidos	Nombre
Bermejo Lurueña	Iker
García Merlo	Angel
Galán Castro	Mario

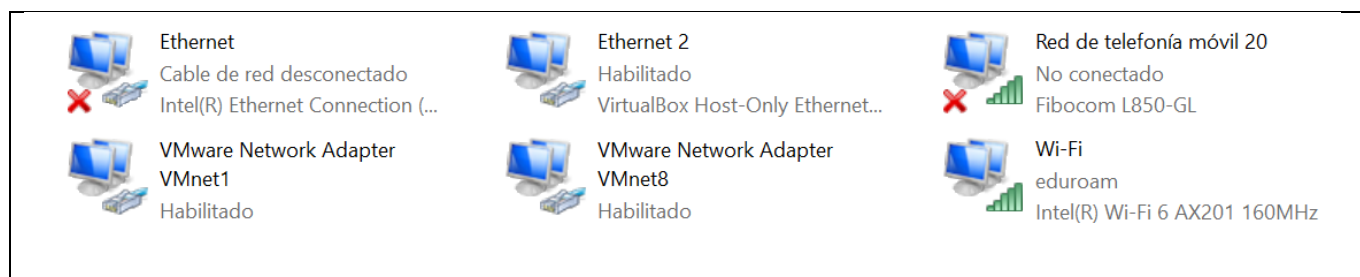
Grupo de laboratorio:

(M01M02, M10M11, X01X02, J01J02, J10J11)	J01J02
--	--------

Escenario 1

Acciones previas a la instalación del cliente (apartado 3.1)

1. Captura gráfica de las interfaces de red obtenida desde el “Panel de control\Redes e Internet\Conexiones de red”.



2. Texto con la salida del resultado de la ejecución del comando “ipconfig /all”.

```
C:\Users\ikerb>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : LAPTOP-D99MA4MC
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) Ethernet Connection (10) I219-V
Dirección física. . . . . : 00-2B-67-4F-B6-F0
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de Ethernet Ethernet 2:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : VirtualBox Host-Only Ethernet Adapter
Dirección física. . . . . : 0A-00-27-00-00-21
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::8608:e8b8:d8c8:84c6%33(Preferido)
Dirección IPv4. . . . . : 192.168.56.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
IAID DHCPv6 . . . . . : 1275723815
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de LAN inalámbrica Conexión de área local* 1:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Dirección física. . . . . : 3C-58-C2-F1-1F-CC
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de banda ancha móvil Red de telefonía móvil 20:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Generic Mobile Broadband Adapter
Dirección física. . . . . : 94-B1-99-53-55-40
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí

Adaptador de Ethernet VMware Network Adapter VMnet1:

Sufijo DNS específico para la conexión. . . :
```

```

Descripción . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Dirección física. . . . . : 00-50-56-C0-00-01
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí
Vínculo: dirección IPv6 local. . . . : fe80::9352:8216:57b1:178%10(Preferido)
Dirección IPv4. . . . . : 192.168.234.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : miércoles, 3 de abril de 2024 7:28:48
La concesión expira . . . . . : miércoles, 3 de abril de 2024 21:22:52
Puerta de enlace predeterminada . . . . :
Servidor DHCP . . . . . : 192.168.234.254
IAID DHCPv6 . . . . . : 1174425686
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
NetBIOS sobre TCP/IP. . . . . : habilitado

```

Adaptador de Ethernet VMware Network Adapter VMnet8:

```

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : VMware Virtual Ethernet Adapter for VMnet8
Dirección física. . . . . : 00-50-56-C0-00-08
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . : sí
Vínculo: dirección IPv6 local. . . . : fe80::293e:fd48:a628:c814%38(Preferido)
Dirección IPv4. . . . . : 192.168.30.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : miércoles, 3 de abril de 2024 7:28:47
La concesión expira . . . . . : miércoles, 3 de abril de 2024 21:22:52
Puerta de enlace predeterminada . . . . :
Servidor DHCP . . . . . : 192.168.30.254
IAID DHCPv6 . . . . . : 1207980118
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidor WINS principal . . . . . : 192.168.30.2
NetBIOS sobre TCP/IP. . . . . : habilitado

```

Adaptador de LAN inalámbrica Wi-Fi:

```

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Dirección física. . . . . : 3C-58-C2-F1-1F-CB
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . : sí
Vínculo: dirección IPv6 local. . . . : fe80::ea94:b587:ac7f:4a79%5(Preferido)
Dirección IPv4. . . . . : 192.168.1.108(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : martes, 2 de abril de 2024 15:14:11
La concesión expira . . . . . : jueves, 4 de abril de 2024 6:36:23
Puerta de enlace predeterminada . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 71063746
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidores DNS. . . . . : 80.58.61.250
                        80.58.61.254
NetBIOS sobre TCP/IP. . . . . : habilitado

```

3. Texto con la información de la tabla de rutas obtenida mediante la ejecución del comando "route print". Sobre dicha información identificar e indicar la dirección IP de la interfaz del PC para salir a Internet. Analizar la máscara asignada e identificar la dirección IP del Router en su red doméstica.

```

NetBIOS sobre TCP/IP. . . . . : habilitado

C:\Users\ikerb>route print

=====
Lista de interfaces
18...00 2b 67 4f b6 f0 .....Intel(R) Ethernet Connection (10) I219-V
33...0a 00 27 00 00 21 .....VirtualBox Host-Only Ethernet Adapter
20...3c 58 c2 f1 1f cc .....Microsoft Wi-Fi Direct Virtual Adapter
35...94 b1 99 53 55 40 .....Generic Mobile Broadband Adapter
10...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
38...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
5...3c 58 c2 f1 1f cb .....Intel(R) Wi-Fi 6 AX201 160MHz
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0            0.0.0.0            192.168.1.1          192.168.1.108    35
127.0.0.0          255.0.0.0          En vínculo           127.0.0.1        331
127.0.0.1          255.255.255.255    En vínculo           127.0.0.1        331
127.255.255.255    255.255.255.255    En vínculo           127.0.0.1        331
192.168.1.0        255.255.255.0      En vínculo           192.168.1.108    291
192.168.1.108      255.255.255.255    En vínculo           192.168.1.108    291
192.168.1.255      255.255.255.255    En vínculo           192.168.1.108    291
192.168.30.0       255.255.255.0      En vínculo           192.168.30.1     291
192.168.30.1       255.255.255.255    En vínculo           192.168.30.1     291
192.168.30.255     255.255.255.255    En vínculo           192.168.30.1     291
192.168.56.0       255.255.255.0      En vínculo           192.168.56.1     281
192.168.56.1       255.255.255.255    En vínculo           192.168.56.1     281
192.168.56.255     255.255.255.255    En vínculo           192.168.56.1     281
192.168.234.0      255.255.255.0      En vínculo           192.168.234.1    291
192.168.234.1      255.255.255.255    En vínculo           192.168.234.1    291
192.168.234.255    255.255.255.255    En vínculo           192.168.234.1    291
224.0.0.0          240.0.0.0          En vínculo           127.0.0.1        331
224.0.0.0          240.0.0.0          En vínculo           192.168.56.1     281
224.0.0.0          240.0.0.0          En vínculo           192.168.1.108    291
224.0.0.0          240.0.0.0          En vínculo           192.168.30.1     291
224.0.0.0          240.0.0.0          En vínculo           192.168.234.1    291
255.255.255.255    255.255.255.255    En vínculo           127.0.0.1        331
255.255.255.255    255.255.255.255    En vínculo           192.168.56.1     281
255.255.255.255    255.255.255.255    En vínculo           192.168.1.108    291
255.255.255.255    255.255.255.255    En vínculo           192.168.30.1     291
255.255.255.255    255.255.255.255    En vínculo           192.168.234.1    291
=====
Rutas persistentes:
Ninguno

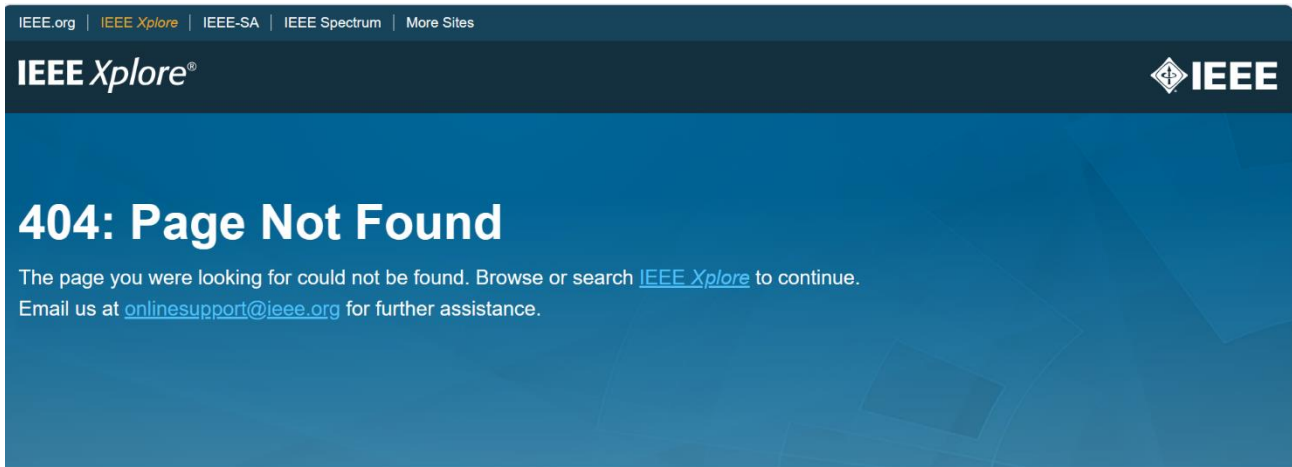
IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica      Puerta de enlace
1 331 ::1/128                        En vínculo
33 281 fe80::/64                     En vínculo
5 291 fe80::/64                     En vínculo
38 291 fe80::/64                     En vínculo
10 291 fe80::/64                     En vínculo
38 291 fe80::293e:fd48:a628:c814/128
En vínculo
33 281 fe80::8608:e8b8:d8c8:84c6/128
En vínculo
10 291 fe80::9352:8216:57b1:178/128
En vínculo
5 291 fe80::ea94:b587:ac7f:4a79/128
En vínculo
1 331 ff00::/8                       En vínculo
33 281 ff00::/8                       En vínculo
5 291 ff00::/8                       En vínculo
38 291 ff00::/8                       En vínculo
10 291 ff00::/8                       En vínculo
=====
Rutas persistentes:
Ninguno

```

- Dirección IP local: 192.168.1.108. Es una dirección IP privada perteneciente a la red local del router. Al tener la métrica más baja, es la dirección prioritaria para utilizar dentro de la red local.
- Puerta de enlace predeterminada: 192.168.1.1. Esta es la dirección IP del router al que está conectado el dispositivo. Para acceder a destinos fuera de la red local, el tráfico debe pasar por esta interfaz.
- Destino de red y máscara de red: 0.0.0.0/0. Esto indica que por esa interfaz se pueden acceder a todas las direcciones, lo que sugiere que es la puerta de enlace predeterminada para alcanzar destinos fuera de la red local.

Además, podemos analizar la máscara asignada para la dirección IP de la interfaz del PC. En este caso, si la máscara es 255.255.255.0, significa que se trata de una dirección IP de clase C, lo que indica que la red local tiene un prefijo de 24 bits (192.168.1.0/24), siendo 24 los bits asignados a la red y los restantes a los dispositivos en la red local.

4. Justificar por qué no ha podido acceder al recurso de la UPM indicado.

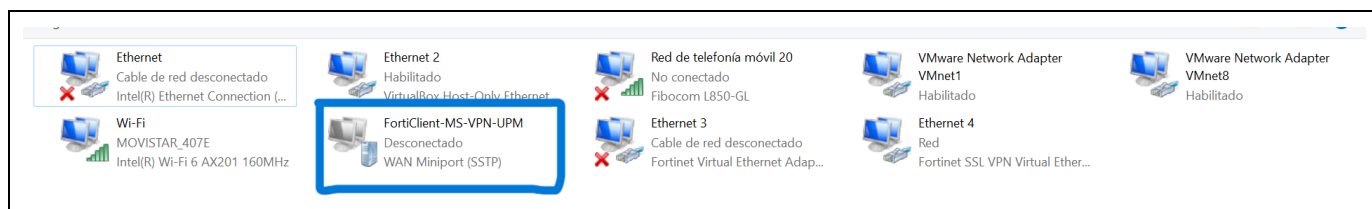


The screenshot shows the IEEE Xplore website with a dark blue header containing navigation links (IEEE.org, IEEE Xplore, IEEE-SA, IEEE Spectrum, More Sites) and the IEEE logo. The main content area has a blue background with the text '404: Page Not Found' in large white font. Below this, it says 'The page you were looking for could not be found. Browse or search IEEE Xplore to continue. Email us at onlinesupport@ieee.org for further assistance.' At the bottom, there is a small copyright notice: '© Copyright 2024 IEEE - All rights reserved.'

Esto sucede porque el acceso al recurso está limitado a la red local. Esto significa que solo quienes estén en el lugar físico donde se encuentra la red local y se conecten a su router podrán ser identificados con una dirección IP de esa red y acceder al recurso. Sin embargo, dado que no estamos físicamente en ese lugar, no podemos conectarnos al router y, como resultado, se nos niega el acceso al recurso. La única manera de acceder desde fuera de la red es a través de una conexión VPN.

Pruebas después de la conexión a la VPN SSL de la UPM (apartado 3.4)

1. Captura gráfica de las interfaces de red obtenida desde el “Panel de control\Redes e Internet\Conexiones de red”.



2. Texto con la salida del resultado de la ejecución del comando “ipconfig /all”, explicando y justificando los cambios producidos respecto de la salida del mismo comando antes de la instalación del cliente de VPN. De manera concreta, identificar la dirección IP asignada a la nueva interfaz virtual del PC una vez establecida la conexión a la VPN.



Símbolo del sistema



```
C:\Users\ikerb>ipconfig /all
```

Configuración IP de Windows

```
Nombre de host. . . . . : LAPTOP-D99MA4MC
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . : no
Proxy WINS habilitado . . . . . : no
Lista de búsqueda de sufijos DNS: upm.es
```

Adaptador de Ethernet Ethernet 4:

```
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Fortinet SSL VPN Virtual Ethernet Adapter
Dirección física. . . . . : 00-09-0F-AA-00-01
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::1829:6661:15d0:4ee0%85(Preferido)
Dirección IPv4. . . . . : 10.198.0.19(Preferido)
Máscara de subred . . . . . : 255.255.255.255
Puerta de enlace predeterminada . . . . . : 10.198.0.20
IAID DHCPv6 . . . . . : 1426065679
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidores DNS. . . . . : 138.100.4.4
                             138.100.4.8
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Adaptador de Ethernet Ethernet:

```
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) Ethernet Connection (10) I219-V
Dirección física. . . . . : 00-2B-67-4F-B6-F0
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
```

Adaptador de Ethernet Ethernet 2:

```
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : VirtualBox Host-Only Ethernet Adapter
Dirección física. . . . . : 0A-00-27-00-00-21
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::8608:e8b8:d8c8:84c6%33(Preferido)
Dirección IPv4. . . . . : 192.168.56.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
IAID DHCPv6 . . . . . : 1275723815
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidores DNS. . . . . : 138.100.4.4
                             138.100.4.8
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Adaptador de LAN inalámbrica Conexión de área local* 1:

```
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Dirección física. . . . . : 3C-58-C2-F1-1F-CC
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
```

Adaptador de banda ancha móvil Red de telefonía móvil 20:

```
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Generic Mobile Broadband Adapter
Dirección física. . . . . : 94-B1-99-53-55-40
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
```


Adaptador de Ethernet VMware Network Adapter VMnet1:

```
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Dirección física. . . . . : 00-50-56-C0-00-01
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::9352:8216:57b1:178%10(Preferido)
Dirección IPv4. . . . . : 192.168.234.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : miércoles, 3 de abril de 2024 7:28:48
La concesión expira . . . . . : miércoles, 3 de abril de 2024 21:53:12
Puerta de enlace predeterminada . . . . . :
Servidor DHCP . . . . . : 192.168.234.254
IAID DHCPv6 . . . . . : 1174425686
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidores DNS. . . . . : 138.100.4.4
                          138.100.4.8
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Adaptador de Ethernet VMware Network Adapter VMnet8:

```
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : VMware Virtual Ethernet Adapter for VMnet8
Dirección física. . . . . : 00-50-56-C0-00-08
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::293e:fd48:a628:c814%38(Preferido)
Dirección IPv4. . . . . : 192.168.30.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : miércoles, 3 de abril de 2024 7:28:47
La concesión expira . . . . . : miércoles, 3 de abril de 2024 21:53:12
Puerta de enlace predeterminada . . . . . :
Servidor DHCP . . . . . : 192.168.30.254
IAID DHCPv6 . . . . . : 1207980118
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidores DNS. . . . . : 138.100.4.4
                          138.100.4.8
Servidor WINS principal . . . . . : 192.168.30.2
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Adaptador de Ethernet Ethernet 3:

```
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Fortinet Virtual Ethernet Adapter (NDIS 6.30)
Dirección física. . . . . : 00-09-0F-FE-00-01
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
```

Adaptador de LAN inalámbrica Wi-Fi:

```
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Dirección física. . . . . : 3C-58-C2-F1-1F-CB
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::ea94:b587:ac7f:4a79%5(Preferido)
Dirección IPv4. . . . . : 192.168.1.108(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : martes, 2 de abril de 2024 15:14:11
La concesión expira . . . . . : jueves, 4 de abril de 2024 6:36:23
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 71063746
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidores DNS. . . . . : 138.100.4.4
                          138.100.4.8
                          80.58.61.250
                          80.58.61.254
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Adaptador PPP FortiClient-MS-VPN-UPM:

```
Sufijo DNS específico para la conexión. . : upm.es
Descripción . . . . . : FortiClient-MS-VPN-UPM
Dirección física. . . . . :
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Dirección IPv4. . . . . : 10.198.0.18(Preferido)
Máscara de subred . . . . . : 255.255.255.255
Puerta de enlace predeterminada . . . . . : 0.0.0.0
NetBIOS sobre TCP/IP. . . . . : habilitado
Lista de búsqueda de sufijos DNS específicos de conexión:
                                upm.es
```

C:\Users\ikerb>

Lo que ha cambiado respecto a la última salida antes de la instalación es que ahora podemos observar la inclusión de la configuración de la VPN. Podemos notar que una vez que el dispositivo se conecte a la VPN, el servidor de la VPN le asignará una dirección IP privada perteneciente a la red de la UPM. En este caso específico, la dirección IP asignada será 10.198.0.18.

3. Texto con la información de la tabla de rutas obtenida ahora mediante la ejecución del comando “route print”, identificando la dirección del servidor de VPN-SSL de la UPM. Para conocer la dirección IP del servidor de VPN-SSL usar el comando “nslookup” y traducir el nombre “vpns1.upm.es”.

En esta sección, nos centraremos en la tabla de enrutamiento IPv4. Se observan dos entradas para la dirección 0.0.0.0/0, cada una con su propia configuración.

- Primera entrada: Dirección IP: 192.168.1.108 (la misma que antes).
- Segunda entrada: Dirección IP: 10.198.0.18 (nueva dirección).

Descripción: Corresponde a la dirección IP local de la red UPM, siendo una dirección privada de la red de la UPM.

Destino de red y máscara de red: 0.0.0.0/0, indicando que todas las direcciones pueden ser accedidas a través de esta interfaz.

Además, se nota que la dirección IP de la puerta de enlace (router al que está conectado el dispositivo) aparece también como “en vínculo”. Esto se debe a que el dispositivo está conectado a través del túnel VPN.

```
=====
ILista de interfaces
18...00 2b 67 4f b6 f0 .....Intel(R) Ethernet Connection (10) I219-V
33...0a 00 27 00 00 21 .....VirtualBox Host-Only Ethernet Adapter
20...3c 58 c2 f1 1f cc .....Microsoft Wi-Fi Direct Virtual Adapter
35...94 b1 99 53 55 40 .....Generic Mobile Broadband Adapter
10...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
38...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
78...00 09 0f fe 00 01 .....Fortinet Virtual Ethernet Adapter (NDIS 6.30)
5...3c 58 c2 f1 1f cb .....Intel(R) Wi-Fi 6 AX201 160MHz
100.....FortiClient-MS-VPN-UPM
1.....Software Loopback Interface 1
=====
```

IPv4 Tabla de enrutamiento

Rutas activas:

Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.108	4260
0.0.0.0	0.0.0.0	En vínculo	10.198.0.18	4227
10.198.0.18	255.255.255.255	En vínculo	10.198.0.18	311
127.0.0.0	255.0.0.0	En vínculo	127.0.0.1	4556
127.0.0.1	255.255.255.255	En vínculo	127.0.0.1	4556
127.255.255.255	255.255.255.255	En vínculo	127.0.0.1	4556
138.100.255.9	255.255.255.255	192.168.1.1	192.168.1.108	4260
192.168.1.0	255.255.255.0	En vínculo	192.168.1.108	4516
192.168.1.108	255.255.255.255	En vínculo	192.168.1.108	4516
192.168.1.255	255.255.255.255	En vínculo	192.168.1.108	4516
192.168.30.0	255.255.255.0	En vínculo	192.168.30.1	4516
192.168.30.1	255.255.255.255	En vínculo	192.168.30.1	4516
192.168.30.255	255.255.255.255	En vínculo	192.168.30.1	4516
192.168.56.0	255.255.255.0	En vínculo	192.168.56.1	4506
192.168.56.1	255.255.255.255	En vínculo	192.168.56.1	4506
192.168.56.255	255.255.255.255	En vínculo	192.168.56.1	4506
192.168.234.0	255.255.255.0	En vínculo	192.168.234.1	4516
192.168.234.1	255.255.255.255	En vínculo	192.168.234.1	4516
192.168.234.255	255.255.255.255	En vínculo	192.168.234.1	4516
224.0.0.0	240.0.0.0	En vínculo	127.0.0.1	4556
224.0.0.0	240.0.0.0	En vínculo	192.168.56.1	4506
224.0.0.0	240.0.0.0	En vínculo	192.168.1.108	4516
224.0.0.0	240.0.0.0	En vínculo	192.168.30.1	4516
224.0.0.0	240.0.0.0	En vínculo	192.168.234.1	4516
224.0.0.0	240.0.0.0	En vínculo	10.198.0.18	56
255.255.255.255	255.255.255.255	En vínculo	127.0.0.1	4556
255.255.255.255	255.255.255.255	En vínculo	192.168.56.1	4506
255.255.255.255	255.255.255.255	En vínculo	192.168.1.108	4516
255.255.255.255	255.255.255.255	En vínculo	192.168.30.1	4516
255.255.255.255	255.255.255.255	En vínculo	192.168.234.1	4516
255.255.255.255	255.255.255.255	En vínculo	10.198.0.18	311

Rutas persistentes:

Ninguno

IPv6 Tabla de enrutamiento

Rutas activas:

Cuando destino de red	métrica	Puerta de enlace
1 331 ::1/128		En vínculo
33 281 fe80::/64		En vínculo
5 291 fe80::/64		En vínculo
38 291 fe80::/64		En vínculo
10 291 fe80::/64		En vínculo
38 291 fe80::293e:fd48:a628:c814/128		En vínculo
33 281 fe80::8608:e8b8:d8c8:84c6/128		En vínculo
10 291 fe80::9352:8216:57b1:178/128		En vínculo
5 291 fe80::ea94:b587:ac7f:4a79/128		En vínculo
1 331 ff00::/8		En vínculo
33 281 ff00::/8		En vínculo
5 291 ff00::/8		En vínculo
38 291 ff00::/8		En vínculo
10 291 ff00::/8		En vínculo

Rutas persistentes:

Ninguno

Cuando realizamos una búsqueda de DNS (nslookup) estando fuera de la red de la UPM, la dirección asociada a vpnssl.upm.es es 138.100.255.9. Esta dirección corresponde al servidor de la VPN de la UPM que se utiliza para conectarse a Internet. (Captura 1)

Sin embargo, si intentamos hacer la misma búsqueda de DNS estando conectados a la VPN, esta acción no funciona. Esto se debe a que la red a la que estamos conectados mediante la VPN ya tiene sus propios servidores de DNS y no es necesario buscar la dirección de vpnssl.upm.es externamente. (Captura 2)

```
C:\Users\ikerb>nslookup vpnssl.upm.es
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: vpnssl.upm.es
Address: 138.100.255.9

C:\Users\ikerb>nslookup vpnssl.upm.es
DNS request timed out.
    timeout was 2 seconds.
Servidor: UnKnown
Address: 80.58.61.250

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Se agotó el tiempo de espera de la solicitud a UnKnown
```

4. Identificar la dirección IP con la que sale a Internet si no está conectado a la VPN de la UPM. Utilizar algún servicio de Internet que puede localizar fácilmente haciendo, por ejemplo, la pregunta a Google: “¿Cuál es mi IP?” Justificar por qué esta dirección es distinta a la que tiene el equipo en la red doméstica.

Cuando un dispositivo se conecta a Internet desde una red doméstica, inicialmente se le asigna una dirección IP privada por el enrutador. Esta dirección es útil para la comunicación dentro de la red local, pero no es visible desde Internet.

Para que el dispositivo sea accesible desde la web, el enrutador luego asigna una dirección IP pública. Esta dirección pública actúa como una identificación en Internet, permitiendo que otros dispositivos en la red global se comuniquen con él.

Tu dirección IP es **138.100.146.137**

5. Comentar el resultado del acceso al artículo de IEEEEXPLORE e incluir una captura gráfica que contenga el "Abstract" del artículo en PDF.

AIR: Threats of Adversarial Attacks on Deep Learning-Based Information Recovery

Jinyin Chen, Jie Ge, Shilian Zheng*, Linhui Ye, Haibin Zheng,
Weiguo Shen, Keqiang Yue and Xiaoniu Yang

Abstract—A wireless communications system usually consists of a transmitter which transmits the information and a receiver which recovers the original information from the received distorted signal. Deep learning (DL) has been used to improve the performance of the receiver in complicated channel environments and state-of-the-art (SOTA) performance has been achieved. However, its robustness has not been investigated. In order to evaluate the robustness of DL-based information recovery models under adversarial circumstances, we investigate adversarial attacks on the SOTA DL-based information recovery model, i.e., DeepReceiver. We formulate the problem as an optimization problem with power and peak-to-average power ratio (PAPR) constraints. We design different adversarial attack methods according to the adversary's knowledge of DeepReceiver's model and/or testing samples. Extensive experiments show that the DeepReceiver is vulnerable to the designed attack methods in all of the considered scenarios. Even in the scenario of both model and test sample restricted, the adversary can attack the DeepReceiver and increase its bit error rate (BER) above 10%. It can also be found that the DeepReceiver is vulnerable to adversarial perturbations even with very low power and limited PAPR. These results suggest that defense measures should be taken to enhance the robustness of DeepReceiver.

WIRELESS communications plays an important role in both military and civil applications such as unmanned aerial vehicle control [1], automatic driving [2], positioning [3], Internet of Things [4], and cellular communications from the first generation (1G) to the fifth generation (5G) [5]. In a wireless communications system, information recovery plays an irreplaceable role. It refers to the process that the receiver recovers the original information bit stream sent by the transmitter from the received distorted signal which has been contaminated by noise, channel fading, and intentional/unintentional interference.

For traditional model-based information recovery methods, the receiver recovers the information from the received distorted signal through a series of processes, i.e., carrier and symbol synchronization [6], channel estimation [7], equalization [8], demodulation and channel decoding [9]. However, the recovering accuracy greatly depends on the performance of each processing module designed with theoretical assumptions which are difficult to be guaranteed in real-world scenarios. It is a challenge to precisely recover

6. Utilizando el comando "nslookup", identificar el servidor de DNS que se usa antes y después de establecer la conexión de VPN.

```
ninguno

C:\Users\ikerb>nslookup ieeexplore.ieee.org
DNS request timed out.
    timeout was 2 seconds.
Servidor: UnKnown
Address: 80.58.61.250

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Se agotó el tiempo de espera de la solicitud a UnKnown

C:\Users\ikerb>nslookup ieeexplore.ieee.org
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: d34ow7epij5zhk.cloudfront.net
Addresses: 2600:9000:24dc:3400:1e:d873:7a00:93a1
           2600:9000:24dc:9400:1e:d873:7a00:93a1
           2600:9000:24dc:1e00:1e:d873:7a00:93a1
           2600:9000:24dc:c000:1e:d873:7a00:93a1
           2600:9000:24dc:8c00:1e:d873:7a00:93a1
           2600:9000:24dc:4a00:1e:d873:7a00:93a1
           2600:9000:24dc:5200:1e:d873:7a00:93a1
           2600:9000:24dc:d800:1e:d873:7a00:93a1
           18.154.41.96
           18.154.41.83
           18.154.41.107
           18.154.41.23
Alias: ieeexplore.ieee.org
```

Después (primera) y antes (segunda).

Cuando intentamos realizar una búsqueda DNS (nslookup) mientras estamos conectados a la VPN, tenemos un problema en la resolución de DNS que lleva a cabo que la solicitud de nslookup excede el tiempo de espera. Este inconveniente puede tener diversas causas:

- Algunos programas de VPN incluyen cortafuegos o software de seguridad que pueden bloquear o interferir con las solicitudes de DNS, lo que ocasiona el tiempo de espera.
- Si el servidor no está configurado para manejar las solicitudes de DNS, no se podrá completar el nslookup.
- Problemas de conectividad o congestión en la red debido al uso del túnel VPN (aunque este último no parece ser el problema en este caso).

7. Comentar los aspectos más relevantes del análisis de tráfico capturado antes y después de la conexión de VPN con el servidor de la VPN-SSL de la UPM. Para ello, filtrar adecuadamente los datos de la captura, visualizando, por ejemplo, únicamente el tráfico intercambiado con la dirección IP del servidor de VPN-SSL de la UPM.

Antes:

No.	Time	Source	Destination	Protocol	Length	Info
2752	137.791540	52.108.8.12	192.168.1.36	TLSv1.2	313	Application Data
2755	137.840381	192.168.1.36	52.108.8.12	TCP	54	37092 → 443 [ACK] Seq=28931 Ack=4478 Win=131328 L
2767	139.146977	192.168.1.36	104.208.16.89	TCP	54	37143 → 443 [RST, ACK] Seq=3845 Ack=7584 Win=0 Le
2769	140.581686	192.168.1.36	52.108.8.12	TCP	1494	37092 → 443 [ACK] Seq=28931 Ack=4478 Win=131328 L
2770	140.581686	192.168.1.36	52.108.8.12	TCP	1494	37092 → 443 [ACK] Seq=30371 Ack=4478 Win=131328 L
2771	140.581686	192.168.1.36	52.108.8.12	TLSv1.2	499	Application Data
2772	140.581865	192.168.1.36	52.108.8.12	TCP	1494	37092 → 443 [ACK] Seq=32256 Ack=4478 Win=131328 L
2773	140.581865	192.168.1.36	52.108.8.12	TLSv1.2	1004	Application Data
2774	140.638629	52.108.8.12	192.168.1.36	TCP	60	443 → 37092 [ACK] Seq=4478 Ack=30371 Win=4194816
2775	140.638629	52.108.8.12	192.168.1.36	TCP	60	443 → 37092 [ACK] Seq=4478 Ack=31811 Win=4193280
2776	140.638629	52.108.8.12	192.168.1.36	TCP	60	443 → 37092 [ACK] Seq=4478 Ack=32256 Win=4194816
2777	140.638629	52.108.8.12	192.168.1.36	TCP	60	443 → 37092 [ACK] Seq=4478 Ack=33696 Win=4193280
2778	140.638629	52.108.8.12	192.168.1.36	TCP	60	443 → 37092 [ACK] Seq=4478 Ack=34646 Win=4194816
2779	140.663073	52.108.8.12	192.168.1.36	TLSv1.2	569	Application Data
2780	140.663073	52.108.8.12	192.168.1.36	TLSv1.2	92	Application Data

Antes de configurar la VPN, nuestro PC (192.168.1.36) y el servidor de internet se comunican directamente.

Después:

No.	Time	Source	Destination	Protocol	Length	Info
2163	58.728648	138.100.255.9	192.168.1.36	TLSv1.2	1506	Application Data
2164	58.728648	138.100.255.9	192.168.1.36	TLSv1.2	1506	Application Data
2165	58.728648	138.100.255.9	192.168.1.36	TLSv1.2	1506	Application Data
2166	58.728648	138.100.255.9	192.168.1.36	TLSv1.2	1250	Application Data, Application Data
2167	58.728733	192.168.1.36	138.100.255.9	TCP	54	27773 → 443 [ACK] Seq=380798 Ack=245593 Win=516 L
2168	58.729029	192.168.1.36	138.100.255.9	TLSv1.2	126	Application Data
2169	58.729134	192.168.1.36	138.100.255.9	TLSv1.2	126	Application Data
2170	58.729205	192.168.1.36	138.100.255.9	TLSv1.2	126	Application Data
2171	58.732437	192.168.1.36	138.100.255.9	TLSv1.2	284	Application Data
2172	58.732658	192.168.1.36	138.100.255.9	TLSv1.2	225	Application Data
2173	58.732913	192.168.1.36	138.100.255.9	TLSv1.2	620	Application Data
2174	58.733023	192.168.1.36	138.100.255.9	TLSv1.2	921	Application Data
2175	58.738248	138.100.255.9	192.168.1.36	TCP	60	443 → 27773 [ACK] Seq=245593 Ack=381244 Win=20664
2176	58.738248	138.100.255.9	192.168.1.36	TCP	60	443 → 27773 [ACK] Seq=245593 Ack=381981 Win=20664
2177	58.738248	138.100.255.9	192.168.1.36	TLSv1.2	198	Application Data, Application Data

En este segundo caso, la comunicación entre nuestra computadora y el servidor de Internet no es directa. En cambio, está intermediada por el servidor VPN de la UPM (138.100.255.9), que recibe y encripta todo el tráfico destinado a la red pública. De manera similar, el tráfico proveniente de la red pública también pasa a través del servidor VPN, que lo descifra y nos lo transmite.

Escenario 2

Configuración de la “Appliance OAS” (apartado 4.2)

1. Captura gráfica de la pantalla que demuestre que se ha instalado el servidor de OpenVPN, por ejemplo, una captura gráfica de la salida del comando “ifconfig | more” en la “Appliance OAS”. Este resultado se utilizará más adelante.

```
as0t0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 172.23.0.65 netmask 255.255.255.224 destination 172.23.0.65
    inet6 fe80::29f8:3f2c:2436:a309 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 200
    (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 288 (288.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

as0t1: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 172.23.0.97 netmask 255.255.255.224 destination 172.23.0.97
    inet6 fe80::25e4:f98c:2d34:7614 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 200
    (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 288 (288.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:fec9:d8ab prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c9:d8:ab txqueuelen 1000 (Ethernet)

--More--
```

```

inet6 fe80::20c:29ff:fec9:d8ab prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:c9:d8:ab txqueuelen 1000 (Ethernet)
RX packets 8352 bytes 1739333 (1.7 MB)
RX errors 0 dropped 14 overruns 0 frame 0
TX packets 13555 bytes 22932594 (22.9 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 58 bytes 6074 (6.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 58 bytes 6074 (6.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

pr0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::dc33:50ff:fefe:bab9 prefixlen 64 scopeid 0x20<link>
ether de:33:50:fe:ba:b9 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 13 bytes 1006 (1.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Configuración VPN Settings del servidor de OpenVPN (apartado 4.4)

1. Tabla con las direcciones usadas para las subredes e interfaces indicadas en cada caso antes de establecer una conexión de VPN. Se debería ser capaz de identificar estas direcciones en la tabla de rutas, interfaces y capturas realizadas en apartados posteriores.

Subred/Interfaz	Dirección	Subred/Interfaz	Dirección
LAN C	192.168.1.0/24	C	213.99.222.85
HAN	192.168.1.0/24	D	192.168.1.1
LAN A	172.23.0.64/26	E	192.168.1.100
A	192.168.1.1	F	192.168.1.44
B	192.168.1.36	G	172.23.0.97
		H	88.1.194.177

2. Observar el resultado de la ejecución del comando “ifconfig | more” en la consola de la “Appliance OAS”. ¿Aparece por algún lado la dirección equivalente, en su caso, a la subred “172.23.220.64/26”? Se debe utilizar esta información para completar la dirección de la interfaz “G”. Además, se debe comparar la información en este punto con la obtenida ejecutando el mismo comando en el apartado 4.2. Intentar averiguar por qué no existe una única subred. Escoger cualquiera de las direcciones IP asignadas a las interfaces “as0tx” existentes como dirección G.

Existen dos subredes, cada una con un número de direcciones equivalente a $/27$. Una de estas redes se destina para conexiones TCP, abarcando las direcciones del 64 al 95, mientras que la otra se asigna para conexiones UDP, que van desde el 96 al 127. Además, al revisar el resultado del comando "route print" en el cliente, observamos que la dirección G se identifica como la puerta de enlace para la ruta predeterminada a través de la VPN.

```
as0t0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 172.23.0.65 netmask 255.255.255.224 destination 172.23.0.65
    inet6 fe80::29f8:3f2c:2436:a309 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 200
    (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 288 (288.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

as0t1: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 172.23.0.97 netmask 255.255.255.224 destination 172.23.0.97
    inet6 fe80::25e4:f98c:2d34:7614 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 200
    (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 288 (288.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:fec9:d8ab prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c9:d8:ab txqueuelen 1000 (Ethernet)

--More--
```

Configuración del router del lado servidor (apartado 4.5)

1. ¿Sería conveniente dejar también abierto en el router el puerto 943? ¿Sería necesario para que se puedan abrir conexiones de VPN? ¿Compromete la seguridad de la VPN dejar abierto este puerto?

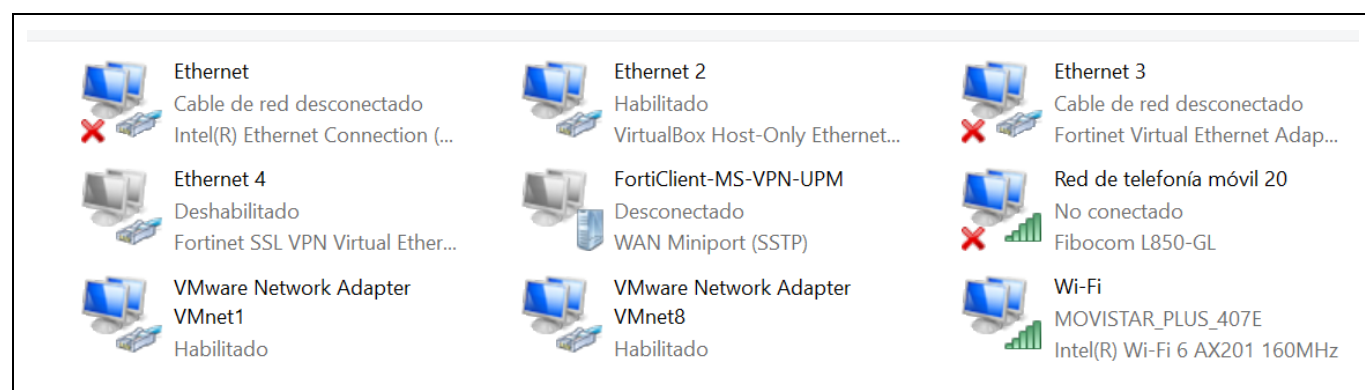
No sería recomendable dejar abierto el puerto 943 en el router, ya que esto podría permitir intentos de conexión como administrador desde máquinas que no son el host del servidor, lo que comprometería la seguridad de la VPN. Además, no es necesario abrir este puerto para establecer conexiones VPN. El puerto 443 garantiza la conectividad vía HTTPS (TCP) y el puerto 1194 proporciona el servicio de OpenVPN (UDP). Sin embargo, abrir el puerto 943 podría permitir a usuarios externos acceder al portal de configuración del servidor OpenVPN, lo que representa un riesgo para la seguridad de la red doméstica. En resumen, es preferible no dejar abierto el puerto 943 para evitar posibles brechas de seguridad en la VPN.

2. Comprobar que es posible acceder a la administración web de la "Appliance OAS" de forma remota: usar un navegador Web desde fuera de la red de su casa con la URL "https://Su_IP_pública/admin". ¿Cómo se puede evitar este problema de seguridad?

Al desactivar la función de reenvío del servidor web administrativo en la configuración de la Appliance OAS. (Admin Web Server Forwarding).

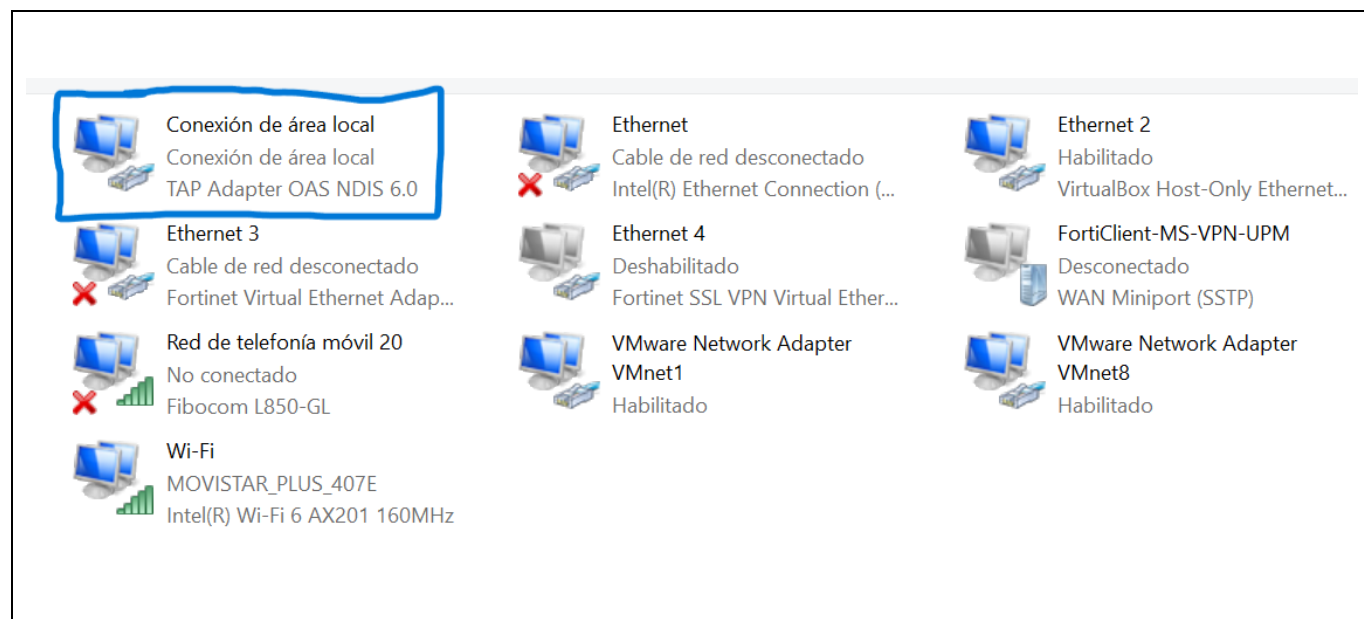
Instalación del Cliente de OpenVPN (apartado 4.6)

1. Captura gráfica de las interfaces de red existentes en el equipo antes de instalar el cliente de VPN, por ejemplo con “Panel de control → Centro de redes y recursos compartidos → Cambiar la configuración del adaptador”



Pruebas de conexión del Cliente y Servidor de OpenVPN (apartado 4.7)

1. ¿Ha aparecido alguna interfaz de red nueva en el SO del lado del cliente? Incluir una captura gráfica de las interfaces de red existentes después de instalar el cliente de VPN. Obtener la tabla de rutas del PC cliente (comando "route print") antes de iniciar la conexión de OpenVPN. Será de utilidad para comparar con la obtenida tras realizar la conexión.



```
C:\Users\ikerb>route print
=====
Lista de interfaces
94...00 ff d8 3e 2f 10 .....TAP Adapter OAS NDIS 6.0
20...00 2b 67 4f b6 f0 .....Intel(R) Ethernet Connection (10) I219-V
34...0a 20 27 00 00 22 .....VirtualBox Host-Only Ethernet Adapter
22...3c 58 c2 f1 1f cc .....Microsoft Wi-Fi Direct Virtual Adapter
37...94 b1 99 53 55 40 .....Generic Mobile Broadband Adapter
10...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
17...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
35...00 09 0f fe 00 01 .....Fortinet Virtual Ethernet Adapter (NDIS 6.30)
5...3c 58 c2 f1 1f cb .....Intel(R) Wi-Fi 6 AX201 160MHz
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0             0.0.0.0             192.168.1.1           192.168.1.36  45
127.0.0.0           128.0.0.0           172.23.0.97           172.23.0.99  257
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1    331
127.0.0.1           255.255.255.255    En vínculo            127.0.0.1    331
127.255.255.255     255.255.255.255    En vínculo            127.0.0.1    331
128.0.0.0           128.0.0.0           172.23.0.97           172.23.0.99  257
172.23.0.96         255.255.255.224    En vínculo            172.23.0.99  257
172.23.0.99         255.255.255.255    En vínculo            172.23.0.99  257
172.23.0.127        255.255.255.255    En vínculo            172.23.0.99  257
192.168.1.0         255.255.255.0      En vínculo            192.168.1.36  301
192.168.1.36        255.255.255.255    En vínculo            192.168.1.36  301
192.168.1.255       255.255.255.255    En vínculo            192.168.1.36  301
192.168.30.0        255.255.255.0      En vínculo            192.168.30.1  291
192.168.30.1        255.255.255.255    En vínculo            192.168.30.1  291
192.168.30.255      255.255.255.255    En vínculo            192.168.30.1  291
192.168.56.0        255.255.255.0      En vínculo            192.168.56.1  281
192.168.56.1        255.255.255.255    En vínculo            192.168.56.1  281
192.168.56.255      255.255.255.255    En vínculo            192.168.56.1  281
192.168.234.0       255.255.255.0      En vínculo            192.168.234.1 291
192.168.234.1       255.255.255.255    En vínculo            192.168.234.1 291
192.168.234.255     255.255.255.255    En vínculo            192.168.234.1 291
213.99.222.85       255.255.255.255    192.168.1.1           192.168.1.36  301
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1    331
224.0.0.0           240.0.0.0           En vínculo            192.168.56.1  281
224.0.0.0           240.0.0.0           En vínculo            192.168.1.36  301
224.0.0.0           240.0.0.0           En vínculo            192.168.234.1 291
224.0.0.0           240.0.0.0           En vínculo            192.168.30.1  291
224.0.0.0           240.0.0.0           En vínculo            172.23.0.99  257
255.255.255.255     255.255.255.255    En vínculo            127.0.0.1    331
255.255.255.255     255.255.255.255    En vínculo            192.168.56.1  281
255.255.255.255     255.255.255.255    En vínculo            192.168.1.36  301
255.255.255.255     255.255.255.255    En vínculo            192.168.234.1 291
255.255.255.255     255.255.255.255    En vínculo            192.168.30.1  291
255.255.255.255     255.255.255.255    En vínculo            172.23.0.99  257

Rutas persistentes:
Ninguna

IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica      Puerta de enlace
1 331 ::1/128                        En vínculo
1 331 2000::/4                       En vínculo
1 331 3000::/4                       En vínculo
1 331 fc00::/7                       En vínculo
34 281 fe80::/64                     En vínculo
5 301 fe80::/64                     En vínculo
10 291 fe80::/64                     En vínculo
17 291 fe80::/64                     En vínculo
94 281 fe80::/64                     En vínculo
34 281 fe80::6038:b146:601e:624c/128 En vínculo
94 281 fe80::60a0:5a03:7909:fc/128   En vínculo
17 291 fe80::d3eb:ce3c:c64d:5d95/128 En vínculo
10 291 fe80::e6f9:c030:14d6:1270/128 En vínculo
5 301 fe80::ea94:b587:ac7f:4a79/128 En vínculo
1 331 ff00::/8                       En vínculo
34 281 ff00::/8                       En vínculo
5 301 ff00::/8                       En vínculo
10 291 ff00::/8                       En vínculo
17 291 ff00::/8                       En vínculo
94 281 ff00::/8                       En vínculo

Rutas persistentes:
Ninguna

C:\Users\ikerb>|
```

- Después de completar la conexión a la VPN, realizar una captura en modo texto del resultado de la ejecución del comando "ipconfig /all" en el PC Cliente, incluyéndola en la memoria y comentado los resultados obtenidos.

Después de establecer la conexión, se nota la adición de un nuevo adaptador, que corresponde a la conexión establecida con OpenVPN. Hay tres aspectos a destacar:

- La interfaz se identifica como "TAP Adapter OAS NDIS 6.0":
 - TAP Adapter: Facilita la conexión de varios dispositivos a una única toma de corriente.
 - OAS: OpenVPN Access Server.

- NDIS (Network Driver Interface Specification): Especificación de interfaz de programación para controladores de red en Windows, que permite el uso de diversos protocolos de red con una variedad de adaptadores de red.
- La dirección asignada a este PC por el servidor es 172.23.0.99


```
C:\Users\ikerb>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : LAPTOP-D99MA4MC
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . . : no

Adaptador desconocido Conexión de área local:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : TAP Adapter OAS NDIS 6.0
Dirección física. . . . . : 00-FF-D8-3E-2F-10
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::60a0:5a03:7909:f0c%94(Preferido)
Dirección IPv4. . . . . : 172.23.0.99(Preferido)
Máscara de subred . . . . . : 255.255.255.224
Puerta de enlace predeterminada . . . . . :
IAID DHCPv6 . . . . . : 1577123800
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidores DNS. . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Ethernet:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Intel(R) Ethernet Connection (10) I219-V
Dirección física. . . . . : 00-2B-67-4F-B6-F0
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de Ethernet Ethernet 2:


Sufijo DNS específico para la conexión. . :
Descripción . . . . . : VirtualBox Host-Only Ethernet Adapter
Dirección física. . . . . : 0A-00-27-00-00-22
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::6038:b146:601e:624c%34(Preferido)
Dirección IPv4. . . . . : 192.168.56.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
IAID DHCPv6 . . . . . : 1275723815
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de LAN inalámbrica Conexión de área local* 1:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Dirección física. . . . . : 3C-58-C2-F1-1F-CC
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de banda ancha móvil Red de telefonía móvil 20:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Generic Mobile Broadband Adapter
Dirección física. . . . . : 94-B1-99-53-55-40
```



Símbolo del sistema

×

+

▼

```

Adaptador de banda ancha móvil Red de telefonía móvil 20:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Generic Mobile Broadband Adapter
Dirección física. . . . . : 94-B1-99-53-55-40
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí

Adaptador de Ethernet VMware Network Adapter VMnet1:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Dirección física. . . . . : 00-50-56-C0-00-01
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::e6f9:c030:14d6:1270%10(Preferido)
Dirección IPv4. . . . . : 192.168.234.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . :
IAID DHCPv6 . . . . . : 167792726
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet VMware Network Adapter VMnet8:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : VMware Virtual Ethernet Adapter for VMnet8
Dirección física. . . . . : 00-50-56-C0-00-08
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::d3eb:ce3c:c64d:5d95%17(Preferido)
Dirección IPv4. . . . . : 192.168.30.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . :
IAID DHCPv6 . . . . . : 637554774
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Ethernet 3:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Fortinet Virtual Ethernet Adapter (NDIS 6.30)
Dirección física. . . . . : 00-09-0F-FE-00-01
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Dirección física. . . . . : 3C-58-C2-F1-1F-CB
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::ea94:b587:ac7f:4a79%5(Preferido)
Dirección IPv4. . . . . : 192.168.1.36(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : jueves, 18 de abril de 2024 20:37:07
La concesión expira . . . . . : viernes, 19 de abril de 2024 19:27:50
Puerta de enlace predeterminada . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 71063746
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-58-C0-E1-00-2B-67-4F-B6-F0
Servidores DNS. . . . . : 80.58.61.250
                        80.58.61.254

```

- Obtener una captura gráfica de la tabla de rutas del PC Cliente e incluirla también en la memoria.

```
C:\Users\ikerb>route print
=====
Lista de interfaces
94...00 ff d8 3e 2f 10 .....TAP Adapter OAS NDIS 6.0
20...00 2b 67 4f b6 f0 .....Intel(R) Ethernet Connection (10) I219-V
34...0a 00 27 00 00 22 .....VirtualBox Host-Only Ethernet Adapter
22...3c 58 c2 f1 1f cc .....Microsoft Wi-Fi Direct Virtual Adapter
37...94 b1 99 53 55 40 .....Generic Mobile Broadband Adapter
10...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
17...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
35...00 09 0f fe 00 01 .....Fortinet Virtual Ethernet Adapter (NDIS 6.30)
5...3c 58 c2 f1 1f cb .....Intel(R) Wi-Fi 6 AX201 160MHz
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz Métrica
0.0.0.0             0.0.0.0             192.168.1.1           192.168.1.36      45
127.0.0.0           127.0.0.0           172.23.0.97           172.23.0.99      257
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1        331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1        331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1        331
128.0.0.0           128.0.0.0           172.23.0.97           172.23.0.99      257
172.23.0.96         255.255.255.224     En vínculo            172.23.0.99      257
172.23.0.99         255.255.255.255     En vínculo            172.23.0.99      257
172.23.0.127        255.255.255.255     En vínculo            172.23.0.99      257
192.168.1.0          255.255.255.0       En vínculo            192.168.1.36      301
192.168.1.36         255.255.255.255     En vínculo            192.168.1.36      301
192.168.1.255       255.255.255.255     En vínculo            192.168.1.36      301
192.168.30.0         255.255.255.0       En vínculo            192.168.30.1      291
192.168.30.1         255.255.255.255     En vínculo            192.168.30.1      291
192.168.30.255       255.255.255.255     En vínculo            192.168.30.1      291
192.168.56.0         255.255.255.0       En vínculo            192.168.56.1      281
192.168.56.1         255.255.255.255     En vínculo            192.168.56.1      281
192.168.56.255       255.255.255.255     En vínculo            192.168.56.1      281
192.168.234.0        255.255.255.0       En vínculo            192.168.234.1     291
192.168.234.1        255.255.255.255     En vínculo            192.168.234.1     291
192.168.234.255      255.255.255.255     En vínculo            192.168.234.1     291
213.99.222.85        255.255.255.255     192.168.1.1           192.168.1.36      301
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1        331
224.0.0.0           240.0.0.0           En vínculo            192.168.56.1      281
224.0.0.0           240.0.0.0           En vínculo            192.168.1.36      301
224.0.0.0           240.0.0.0           En vínculo            192.168.234.1     291
224.0.0.0           240.0.0.0           En vínculo            192.168.30.1      291
224.0.0.0           240.0.0.0           En vínculo            172.23.0.99      257
255.255.255.255     255.255.255.255     En vínculo            127.0.0.1        331
255.255.255.0       255.255.255.255     En vínculo            192.168.56.1      281
255.255.255.255     255.255.255.255     En vínculo            192.168.1.36      301
255.255.255.255     255.255.255.255     En vínculo            192.168.234.1     291
255.255.255.255     255.255.255.255     En vínculo            192.168.30.1      291
255.255.255.255     255.255.255.255     En vínculo            172.23.0.99      257
=====
Rutas persistentes:
Ninguno

IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica      Puerta de enlace
1 331 ::1/128                        En vínculo
1 331 2000::/4                       En vínculo
1 331 3000::/4                       En vínculo
1 331 fc00::/7                       En vínculo
34 281 fe80::/64                     En vínculo
5 301 fe80::/64                     En vínculo
10 291 fe80::/64                     En vínculo
17 291 fe80::/64                     En vínculo
94 281 fe80::/64                     En vínculo
34 281 fe80::6038:b146:601e:624c/128 En vínculo
94 281 fe80::60a0:5a03:7909:f0c/128 En vínculo
17 291 fe80::d3eb:ce3c:c64d:5d95/128 En vínculo
10 291 fe80::e6f9:c030:14d6:1270/128 En vínculo
5 301 fe80::ea94:b587:ac7f:4a79/128 En vínculo
1 331 ff00::/8                       En vínculo
34 281 ff00::/8                       En vínculo
5 301 ff00::/8                       En vínculo
10 291 ff00::/8                       En vínculo
17 291 ff00::/8                       En vínculo
94 281 ff00::/8                       En vínculo
=====
Rutas persistentes:
Ninguno

C:\Users\ikerb>
```

Analizando la información de la tabla de rutas anterior, responder de forma razonada a las siguientes preguntas, suponiendo que está en el PC Cliente:

1. ¿Cuál es la dirección asignada en el cliente al adaptador de red “TAP Adapter OAS NDIS 6.0” tras establecerse la conexión de VPN?

Se observa que para la puerta de enlace 172.23.0.97, que es la dirección IP privada asignada al servidor dentro de OpenVPN, la interfaz es 172.23.0.99. Esto indica que 172.23.0.99 es la dirección asignada al cliente en ese adaptador de red.

2. ¿Cuál es el camino que sigue un paquete que sale a Internet, desde el PC Cliente, tras crear la conexión de VPN? Para responder a la pregunta anterior puede ser útil responder previamente a las siguientes preguntas: ¿Cuál es la dirección IP pública desde la que accede el cliente a los recursos de Internet? Usar alguna web externa del tipo “¿Cuál es mi IP?” para conocerlo.

NOTA: Considerar igualmente cuál era la dirección IP pública desde la que se accedía a los recursos de Internet desde el PC cliente antes de establecer la conexión de OpenVPN, recordando las pruebas realizadas en el escenario 1

El paquete virtualmente viajará a través del túnel de OpenVPN desde la interfaz 172.23.0.99 hasta el servidor OpenVPN (172.23.0.97). Luego, el servidor enviará el paquete fuera de la red de OpenVPN hacia la red del destinatario. En este proceso, el paquete tendrá como dirección de origen la dirección privada del PC que aloja el servidor. Finalmente, el router de esa red dirigirá el paquete hacia internet utilizando su dirección pública (213.99.222.85).

Tu dirección IP es **213.99.222.85**

3. Identificar la/s ruta/s por defecto existentes en la tabla de rutas. ¿Se llegan a usar la ruta o rutas por defecto? Buscar todas las entradas que tengan como interfaz la creada por OpenVPN. A continuación, identificar dos de ellas que “tapan” la ruta por defecto.

La ruta predeterminada es como la dirección principal que se utiliza cuando no sabemos cómo llegar a una red específica. En este caso, la primera entrada en la tabla de rutas se usa para cualquier red no especificada en la tabla. Se representa con una dirección de destino y una máscara de red de "0.0.0.0".

La puerta de enlace predeterminada está configurada en "192.168.1.1".

La segunda entrada también tiene una dirección de destino y una máscara de red de "0.0.0.0", lo que significa que también se aplica a cualquier red. Pero esta entrada se usa para enviar datos a través de una conexión VPN.

4. ¿Tiene sentido que aparezca la dirección del router tras el que se ha instalado el Servidor de OpenVPN en esta tabla de rutas? Razonar la respuesta.

La presencia del router en la tabla de rutas tiene sentido porque actúa como la puerta de enlace predeterminada para cualquier tráfico que no se dirija a redes específicas. Sin embargo, las rutas asociadas a la VPN tienen prioridad sobre esta puerta de enlace predeterminada, asegurando que todo el tráfico se enrute a través de la conexión VPN.

5. Comprobar si la máscara de la subred denominada “LAN A” en la **Figura 21** del enunciado es la misma en la tabla de rutas y en el Servidor de OpenVPN. No debería ser la misma. Observar que la subred /26 se ha dividido en más subredes. Para encontrar la explicación teclear el comando “ifconfig | more” en la consola del

servidor de OpenVPN y analizar las interfaces “as0tx” que aparezcan. Ver qué relación tienen con el valor de “Number of TCP y UDP daemons” que se fijen en la opción “Network Settings” del menú “CONFIGURATION” en la interfaz web del servidor.

Los valores “Number of TCP y UDP daemons”, determinan el número de procesos OpenVPN que se ejecutan en el servidor. Estos procesos son los responsables de gestionar una conexión de cliente VPN (cada proceso gestiona una conexión diferente).

Por tanto, como se han configurado dos instancias de la interfaz TAP en el servidor y cada una se asocia con una subred diferente. Entonces, la subred con máscara /26 se divide en dos subredes con máscara /27 y cada una de estas subredes son asignadas a las instancias antes mencionadas. De esta forma, cada instancia de OpenVPN será responsable de gestionar las conexiones de clientes que se conecten a través de esa subred.

6. Ejecutar en el cliente el comando “tracert” sobre una máquina de la HAN. Incluir y comentar el resultado obtenido. Repetir el experimento ejecutando el comando sobre un host externo, que responda a “ping”, de Internet.

```
C:\Users\ikerb>tracert 192.168.1.100

Traza a 192.168.1.100 sobre caminos de 30 saltos como máximo.

  1    13 ms    <1 ms    <1 ms    192.168.1.100

Traza completa.
```

“No se apreciaba el salto del paquete desde la subred de VPN”

```
C:\Users\angel>tracert www.google.es

Traza a la dirección www.google.es [172.217.168.163]
sobre un máximo de 30 saltos:

  1    11 ms    11 ms    11 ms    172.23.0.97
  2    13 ms    13 ms    11 ms    192.168.1.1
  3    14 ms    13 ms    13 ms    192.168.144.1
  4    16 ms    14 ms    14 ms    153.red-5-205-78.dynamicip.rima-tde.net [5.205.78.153]
  5     *        *        *        Tiempo de espera agotado para esta solicitud.
  6     *        *        *        Tiempo de espera agotado para esta solicitud.
  7     *        *        *        Tiempo de espera agotado para esta solicitud.
  8    16 ms    15 ms    15 ms    5.53.1.82
  9    16 ms    18 ms    14 ms    142.251.231.147
 10    29 ms    44 ms    31 ms    74.125.253.201
 11    15 ms    15 ms    19 ms    mad07s10-in-f3.1e100.net [172.217.168.163]

Traza completa.
```

Realizar un “ping” a un host externo de Internet desde el PC cliente y responder a las siguientes preguntas:

1. Explicar qué tipo de paquete o paquetes se enviará/n al equipo sobre el que se hace el ping. Si no se recuerda se puede hacer el experimento real y combinarlo con una captura de Wireshark.

Son paquetes ICMP Echo Request

```
C:\Users\angel>ping www.google.es

Haciendo ping a www.google.es [142.250.200.99] con 32 bytes de datos:
Respuesta desde 142.250.200.99: bytes=32 tiempo=14ms TTL=117
Respuesta desde 142.250.200.99: bytes=32 tiempo=15ms TTL=117
Respuesta desde 142.250.200.99: bytes=32 tiempo=37ms TTL=117
Respuesta desde 142.250.200.99: bytes=32 tiempo=15ms TTL=117

Estadísticas de ping para 142.250.200.99:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 14ms, Máximo = 37ms, Media = 20ms
```

2. Indicar qué entrada de la tabla de rutas se utilizará en primer lugar para determinar la dirección de la “Puerta de enlace” por la que el/los paquete/s saldrá/n hacia el destino. Indicar qué interfaz del PC cliente se va a utilizar en primer lugar y qué dirección IP tiene. ¿Se usa más de una entrada de la tabla de rutas del PC cliente hasta conseguir que un paquete se envíe al servidor de VPN?

La primera entrada, resaltada, utiliza la interfaz asociada con la dirección IP mostrada en la imagen. En segundo lugar, se emplea otra entrada de la tabla de rutas, específicamente la primera entrada, la cual corresponde a la ruta por defecto. El paquete se cifra y encapsula en otro paquete que se enviará a través de esta ruta hacia la red pública.

```
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0             0.0.0.0             192.168.1.1           192.168.1.36   50
0.0.0.0             128.0.0.0           172.23.0.97           172.23.0.99   257
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1     331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1     331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
128.0.0.0           128.0.0.0           172.23.0.97           172.23.0.99   257
172.23.0.97         255.255.255.224     En vínculo            172.23.0.99   257
172.23.0.99         255.255.255.255     En vínculo            172.23.0.99   257
172.23.0.127        255.255.255.255     En vínculo            172.23.0.99   257
192.168.1.0          255.255.255.0       En vínculo            192.168.1.36   306
192.168.1.36         255.255.255.255     En vínculo            192.168.1.36   306
192.168.1.255        255.255.255.255     En vínculo            192.168.1.36   306
192.168.30.0          255.255.255.0       En vínculo            192.168.30.1   291
192.168.30.1         255.255.255.255     En vínculo            192.168.30.1   291
192.168.30.255       255.255.255.255     En vínculo            192.168.30.1   291
192.168.56.0          255.255.255.0       En vínculo            192.168.56.1   281
192.168.56.1         255.255.255.255     En vínculo            192.168.56.1   281
192.168.56.255       255.255.255.255     En vínculo            192.168.56.1   281
192.168.234.0         255.255.255.0       En vínculo            192.168.234.1   291
192.168.234.1        255.255.255.255     En vínculo            192.168.234.1   291
192.168.234.255      255.255.255.255     En vínculo            192.168.234.1   291
213.99.222.85        255.255.255.255     192.168.1.1           192.168.1.36   306
224.0.0.0            240.0.0.0           En vínculo            127.0.0.1     331
224.0.0.0            240.0.0.0           En vínculo            192.168.56.1   281
224.0.0.0            240.0.0.0           En vínculo            192.168.1.36   306
224.0.0.0            240.0.0.0           En vínculo            192.168.234.1   291
224.0.0.0            240.0.0.0           En vínculo            192.168.30.1   291
224.0.0.0            240.0.0.0           En vínculo            172.23.0.99   257
255.255.255.255      255.255.255.255     En vínculo            127.0.0.1     331
255.255.255.255      255.255.255.255     En vínculo            192.168.56.1   281
255.255.255.255      255.255.255.255     En vínculo            192.168.1.36   306
255.255.255.255      255.255.255.255     En vínculo            192.168.234.1   291
255.255.255.255      255.255.255.255     En vínculo            192.168.30.1   291
255.255.255.255      255.255.255.255     En vínculo            172.23.0.99   257
=====
```

3. Dibujar un esquema de uno de los paquetes IP generados por el cliente de OpenVPN que contiene, a su vez, el paquete generado por el ping, al llegar al Router de la casa en la que está instalado el cliente. Indicar las direcciones IP contenidas en las cabeceras de ambos paquetes (del que viaja encapsulado y cifrado y del que le llega al router).

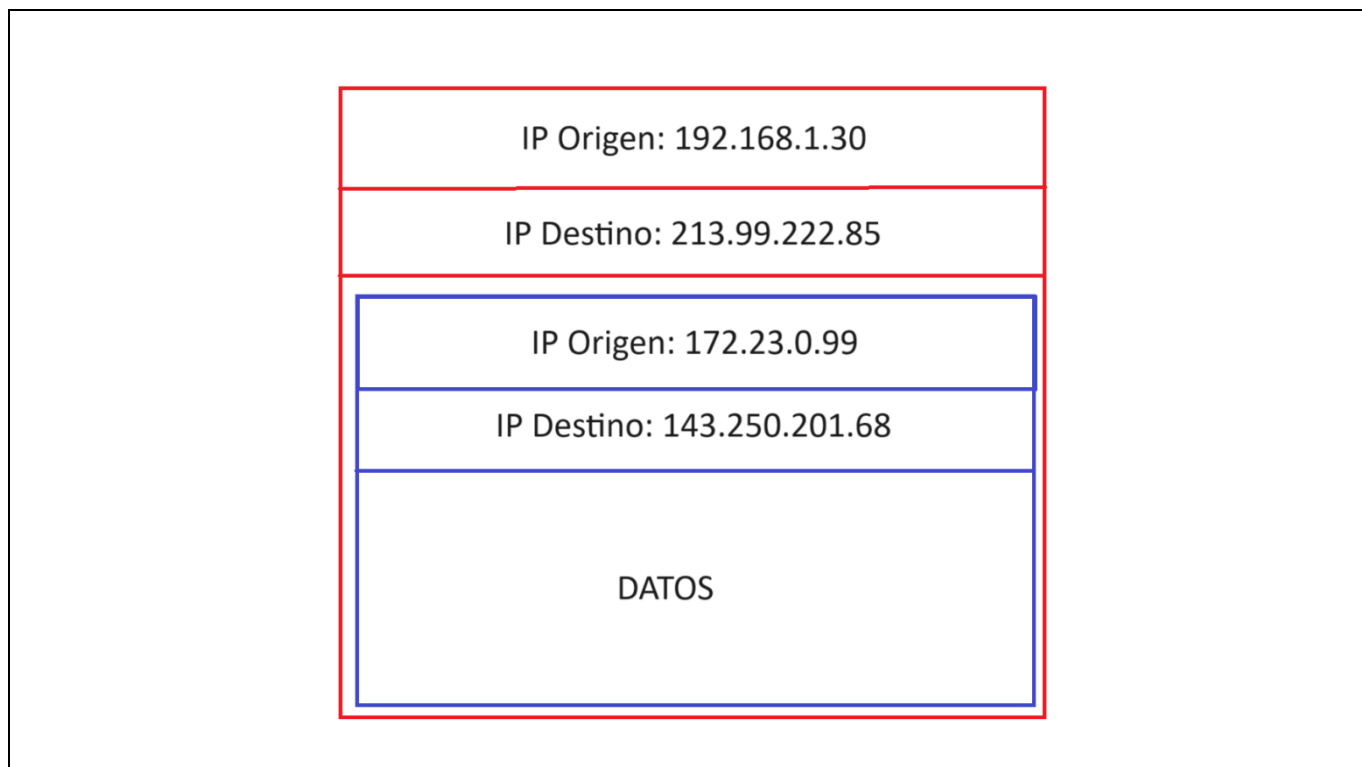
Para dibujar el esquema de los paquetes IP generados por el cliente de OpenVPN, primero identificamos las direcciones IP contenidas en las cabeceras de ambos paquetes:

Paquete azul (generado por el ping):

- IP origen: 172.23.0.99 (asignada por el servidor OpenVPN).
- IP destino: 142.250.201.68 (www.google.com).

Paquete rojo (azul encapsulado y cifrado, llega al router):

- IP origen: 192.168.1.36 (dirección de mi PC en la red privada de casa).
- IP destino: 213.99.222.85 (dirección pública del router de la red doméstica servidor).



Captura 1 Wireshark

1. Aplicando en Wireshark el filtro "ip.addr== <Dir. IP pública servidor VPN>" al tráfico capturado, analizar los primeros mensajes de la captura.



No.	Time	Source	Destination	Protocol	Length	Info
6654	10.471572	185.43.181.41	192.168.1.36	TCP	60	80 → 61858 [ACK] Seq=189 Ack=156 Win=64128 Len=0
6650	10.465976	192.168.1.36	185.43.181.41	TCP	54	[TCP Retransmission] 61858 → 80 [FIN, ACK] Seq=155 Ack=189 Win=131840 Len=0
6649	10.465922	192.168.1.36	185.43.181.41	TCP	54	[TCP Retransmission] 61858 → 80 [FIN, ACK] Seq=155 Ack=189 Win=131840 Len=0
6554	10.169613	185.43.181.41	192.168.1.36	TCP	60	80 → 61857 [ACK] Seq=189 Ack=156 Win=64128 Len=0
6551	10.164181	192.168.1.36	185.43.181.41	TCP	54	[TCP Out-Of-Order] 61858 → 80 [FIN, ACK] Seq=155 Ack=189 Win=131840 Len=0
6550	10.164177	192.168.1.36	185.43.181.41	TCP	54	[TCP Out-Of-Order] 61857 → 80 [FIN, ACK] Seq=155 Ack=189 Win=131840 Len=0
6549	10.164110	192.168.1.36	185.43.181.41	TCP	54	61858 → 80 [FIN, ACK] Seq=155 Ack=189 Win=131840 Len=0
6548	10.164110	192.168.1.36	185.43.181.41	TCP	54	61857 → 80 [FIN, ACK] Seq=155 Ack=189 Win=131840 Len=0
6547	10.164065	192.168.1.36	185.43.181.41	TCP	54	[TCP Dup ACK 6546#1] 61858 → 80 [ACK] Seq=155 Ack=189 Win=131840 Len=0
6546	10.164036	192.168.1.36	185.43.181.41	TCP	54	61858 → 80 [ACK] Seq=155 Ack=189 Win=131840 Len=0
6545	10.163902	185.43.181.41	192.168.1.36	TCP	60	80 → 61857 [FIN, ACK] Seq=188 Ack=155 Win=64128 Len=0
6544	10.163902	185.43.181.41	192.168.1.36	TCP	60	80 → 61858 [FIN, ACK] Seq=188 Ack=155 Win=64128 Len=0
6543	10.163902	185.43.181.41	192.168.1.36	HTTP	241	HTTP/1.1 200 OK (text/plain)
6542	10.163902	185.43.181.41	192.168.1.36	HTTP	241	HTTP/1.1 200 OK (text/plain)
6541	10.163902	185.43.181.41	192.168.1.36	TCP	60	80 → 61858 [ACK] Seq=1 Ack=155 Win=64128 Len=0
6540	10.163902	185.43.181.41	192.168.1.36	TCP	60	80 → 61857 [ACK] Seq=1 Ack=155 Win=64128 Len=0
6534	10.156236	192.168.1.36	185.43.181.41	TCP	208	[TCP Retransmission] 61858 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132096 Len=154
6533	10.156208	192.168.1.36	185.43.181.41	HTTP	208	GET /connecttest.txt HTTP/1.1
6531	10.156134	192.168.1.36	185.43.181.41	TCP	208	[TCP Retransmission] 61857 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132096 Len=154
6529	10.156088	192.168.1.36	185.43.181.41	HTTP	208	GET /connecttest.txt HTTP/1.1
6528	10.156064	192.168.1.36	185.43.181.41	TCP	54	[TCP Dup ACK 6527#1] 61858 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
6527	10.156042	192.168.1.36	185.43.181.41	TCP	54	61858 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
6526	10.156003	192.168.1.36	185.43.181.41	TCP	54	[TCP Dup ACK 6524#1] 61857 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
6524	10.155960	192.168.1.36	185.43.181.41	TCP	54	61857 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
6522	10.155769	185.43.181.41	192.168.1.36	TCP	66	80 → 61858 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM=1 WS=128
6521	10.155769	185.43.181.41	192.168.1.36	TCP	66	80 → 61857 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM=1 WS=128
6499	10.146912	192.168.1.36	185.43.181.41	TCP	66	[TCP Out-Of-Order] 61857 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6498	10.146912	192.168.1.36	185.43.181.41	TCP	66	[TCP Out-Of-Order] 61858 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6497	10.146726	192.168.1.36	185.43.181.41	TCP	66	61858 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6496	10.146726	192.168.1.36	185.43.181.41	TCP	66	61857 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

En esta captura podemos ver el inicio de varias conexiones TCP, con sus mensajes de aceptación de conexión como pueden ser los 200 OK, y posteriormente mensajes de cierre de conexión como los FIN ACK.

- Utilizar después el filtro “icmp|openvpn” y ordenar los mensajes temporalmente. Analizar los distintos paquetes hasta donde sea posible y comentar los resultados.

No.	Time	Source	Destination	Protocol	Length	Info
39969	40.172603	35.214.168.80	172.23.0.104	ICMP	70	Destination unreachable (Port unreachable)
39970	40.172698	35.214.168.80	172.23.0.104	ICMP	70	Destination unreachable (Port unreachable)
40331	40.470314	35.214.168.80	172.23.0.104	ICMP	70	Destination unreachable (Port unreachable)
40752	41.076993	35.214.168.80	172.23.0.104	ICMP	70	Destination unreachable (Port unreachable)
41466	42.280612	35.214.168.80	172.23.0.104	ICMP	70	Destination unreachable (Port unreachable)
42772	44.185597	35.214.168.80	172.23.0.104	ICMP	70	Destination unreachable (Port unreachable)
48283	61.743711	172.23.0.104	142.250.201.68	ICMP	74	Echo (ping) request id=0x0001, seq=186/47616, ttl=128 (reply in 48287)
48287	61.755612	142.250.201.68	172.23.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=186/47616, ttl=117 (request in 48283)
48465	62.759266	172.23.0.104	142.250.201.68	ICMP	74	Echo (ping) request id=0x0001, seq=187/47872, ttl=128 (reply in 48469)
48469	62.771459	142.250.201.68	172.23.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=187/47872, ttl=117 (request in 48465)
48623	63.779787	172.23.0.104	142.250.201.68	ICMP	74	Echo (ping) request id=0x0001, seq=188/48128, ttl=128 (reply in 48624)
48624	63.791938	142.250.201.68	172.23.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=188/48128, ttl=117 (request in 48623)
48828	64.784923	172.23.0.104	142.250.201.68	ICMP	74	Echo (ping) request id=0x0001, seq=189/48384, ttl=128 (reply in 48831)
48831	64.796956	142.250.201.68	172.23.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=189/48384, ttl=117 (request in 48828)

En esta captura podemos ver primero una serie de mensajes icmp a la dirección 172.23.0.104 que tienen como resultado “puerto inalcanzable”. A continuación vemos la segunda parte del ping, concretamente los mensajes echo request y echo reply intercambiados entre las direcciones 172.23.0.104 y 142.250.201.68.

icmp openvpn						
No.	Time	Source	Destination	Protocol	Length	Info
111078	118.287553	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111077	118.287141	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111076	118.287066	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111075	118.283019	213.99.222.85	192.168.1.36	OpenVPN	305	MessageType: P_DATA_V2
111074	118.281082	192.168.1.36	213.99.222.85	OpenVPN	261	MessageType: P_DATA_V2
111073	118.281068	192.168.1.36	213.99.222.85	OpenVPN	261	MessageType: P_DATA_V2
111072	118.281031	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111071	118.281011	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111070	118.280951	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111069	118.280926	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111068	118.280792	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111067	118.280731	192.168.1.36	213.99.222.85	OpenVPN	1223	MessageType: P_DATA_V2
111066	118.279425	213.99.222.85	192.168.1.36	OpenVPN	612	MessageType: P_DATA_V2
111065	118.279269	192.168.1.36	213.99.222.85	OpenVPN	133	MessageType: P_DATA_V2
111064	118.278947	192.168.1.36	213.99.222.85	OpenVPN	133	MessageType: P_DATA_V2
111063	118.277215	213.99.222.85	192.168.1.36	OpenVPN	1344	MessageType: P_DATA_V2
111062	118.277215	213.99.222.85	192.168.1.36	OpenVPN	1344	MessageType: P_DATA_V2
111061	118.277215	213.99.222.85	192.168.1.36	OpenVPN	1344	MessageType: P_DATA_V2
111060	118.275955	192.168.1.36	213.99.222.85	OpenVPN	146	MessageType: P_DATA_V2
111059	118.275899	192.168.1.36	213.99.222.85	OpenVPN	146	MessageType: P_DATA_V2

Visualizacion del tráfico generado una vez que se navega por internet.

Captura 2 Wireshark

1. Filtrar adecuadamente las tramas de la captura, por ejemplo, analizando únicamente el tráfico intercambiado con la dirección IP del servidor de OpenVPN y comentar los resultados.

ip.addr==213.99.222.85						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.003432	192.168.1.36	213.99.222.85	OpenVPN	948	MessageType: P_DATA_V2
4	0.003469	192.168.1.36	213.99.222.85	OpenVPN	948	MessageType: P_DATA_V2
5	0.004420	192.168.1.36	213.99.222.85	OpenVPN	235	MessageType: P_DATA_V2
6	0.004438	192.168.1.36	213.99.222.85	OpenVPN	235	MessageType: P_DATA_V2
7	0.016698	192.168.1.36	213.99.222.85	OpenVPN	948	MessageType: P_DATA_V2
8	0.016746	192.168.1.36	213.99.222.85	OpenVPN	948	MessageType: P_DATA_V2
9	0.017631	213.99.222.85	192.168.1.36	OpenVPN	146	MessageType: P_DATA_V2
10	0.024158	192.168.1.36	213.99.222.85	OpenVPN	234	MessageType: P_DATA_V2
11	0.024196	192.168.1.36	213.99.222.85	OpenVPN	234	MessageType: P_DATA_V2
12	0.030599	192.168.1.36	213.99.222.85	OpenVPN	397	MessageType: P_DATA_V2
13	0.030669	192.168.1.36	213.99.222.85	OpenVPN	397	MessageType: P_DATA_V2
14	0.030889	192.168.1.36	213.99.222.85	OpenVPN	397	MessageType: P_DATA_V2
15	0.030953	192.168.1.36	213.99.222.85	OpenVPN	397	MessageType: P_DATA_V2
16	0.035378	192.168.1.36	213.99.222.85	OpenVPN	146	MessageType: P_DATA_V2
17	0.035426	192.168.1.36	213.99.222.85	OpenVPN	146	MessageType: P_DATA_V2
18	0.039463	192.168.1.36	213.99.222.85	OpenVPN	1175	MessageType: P_DATA_V2
19	0.039502	192.168.1.36	213.99.222.85	OpenVPN	1175	MessageType: P_DATA_V2
20	0.039620	192.168.1.36	213.99.222.85	OpenVPN	1175	MessageType: P_DATA_V2

Se muestra intercambio de informacion directamente puesto que la sesion vpn esta previamente establecida.

Captura 3 Wireshark

1. Analizar el tráfico capturado centrándose en el que tiene como destino u origen la dirección del servidor de OpenVPN en la HAN y localizar los mensajes ICMP. Elegir el filtro adecuado y ordenar los mensajes temporalmente. Comentar los resultados obtenidos.

No.	Time	Source	Destination	Protocol	Length	Info
30909	25.597858	192.168.1.1	192.168.1.44	ICMP	98	Echo (ping) request id=0x695d, seq=0/0, ttl=64 (no response found!)
30973	25.623255	192.168.1.1	192.168.1.100	ICMP	98	Echo (ping) request id=0x695f, seq=0/0, ttl=64 (reply in 30974)
30974	25.623329	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x695f, seq=0/0, ttl=64 (request in 30973)
30975	25.623336	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x695f, seq=0/0, ttl=64
31220	25.728902	192.168.1.1	192.168.1.100	ICMP	98	Echo (ping) request id=0x6966, seq=0/0, ttl=64 (reply in 31221)
31221	25.728987	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x6966, seq=0/0, ttl=64 (request in 31220)
31222	25.728994	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x6966, seq=0/0, ttl=64
158948	55.063242	192.168.1.1	192.168.1.44	ICMP	98	Echo (ping) request id=0x69b8, seq=0/0, ttl=64 (no response found!)
159288	55.094493	192.168.1.1	192.168.1.100	ICMP	98	Echo (ping) request id=0x69ba, seq=0/0, ttl=64 (reply in 159323)
159323	55.094855	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x69ba, seq=0/0, ttl=64 (request in 159288)
159324	55.094864	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x69ba, seq=0/0, ttl=64
575557	85.229740	192.168.1.1	192.168.1.44	ICMP	98	Echo (ping) request id=0x6a0d, seq=0/0, ttl=64 (no response found!)
575589	85.261239	192.168.1.1	192.168.1.100	ICMP	98	Echo (ping) request id=0x6a0f, seq=0/0, ttl=64 (reply in 575590)
575590	85.261304	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x6a0f, seq=0/0, ttl=64 (request in 575589)
575591	85.261312	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x6a0f, seq=0/0, ttl=64
575704	85.364427	192.168.1.1	192.168.1.100	ICMP	98	Echo (ping) request id=0x6a16, seq=0/0, ttl=64 (reply in 575705)
575705	85.364498	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x6a16, seq=0/0, ttl=64 (request in 575704)
575706	85.364507	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x6a16, seq=0/0, ttl=64
622413	115.693968	192.168.1.1	192.168.1.44	ICMP	98	Echo (ping) request id=0x6a7e, seq=0/0, ttl=64 (no response found!)
622486	115.726185	192.168.1.1	192.168.1.100	ICMP	98	Echo (ping) request id=0x6a80, seq=0/0, ttl=64 (reply in 622487)
622487	115.726259	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x6a80, seq=0/0, ttl=64 (request in 622486)
622488	115.726269	192.168.1.100	192.168.1.1	ICMP	98	Echo (ping) reply id=0x6a80, seq=0/0, ttl=64

Al analizar el tráfico capturado, nos enfocamos en los mensajes que tienen como origen o destino la dirección del servidor de OpenVPN en la red doméstica. Utilizando un filtro ICMP, podemos aislar estos mensajes y ordenarlos cronológicamente para comprender mejor las interacciones del servidor OpenVPN.

Encontramos que hay un intercambio de mensajes ICMP entre el servidor OpenVPN y el router de la red doméstica. Esto es notable porque el comando ping fue ejecutado desde el cliente, lo que significa que los mensajes atravesaron la red pública y el router de la red doméstica (el túnel) para alcanzar el servidor OpenVPN. Una vez que los paquetes ICMP llegan al servidor, se inicia un intercambio de información capturada. Posteriormente, el servidor OpenVPN enviará mensajes de respuesta (Echo reply) al cliente a través del mismo túnel.

Análisis de perfil de cliente de “Appliance OAS” (apartado 4.8)

1. Análisis de los distintos certificados y claves que incluye el fichero “profile-7.ovpn”. Tener en cuenta que OpenVPN instala una Autoridad de Certificación (CA) y que se deben soportar las distintas necesidades de autenticación y cifrado.




profile-10.ovpn


Compartir

Detalles

Tipo	Archivo OVPN
Tamaño	9,63 KB
Ubicación del...	C:\Usuarios\ikerb\Descargas
Fecha de mod...	19/04/2024 14:29

1.

```
# OVPN_ACCESS_SERVER_WEB_CA_BUNDLE_START
# -----BEGIN CERTIFICATE-----
# MIIDFjCCAf6gAwIBAgIEZEeqNRzANBgkqhkiG9w0BAQsFADA8MTowOAYDVQQDDDFP
# cGVuVlBOIFdlYiBDQSAyMDIzLjA0LjI3IDA3OjM4OjEzIFBEVCBvcGVudnBuYXMy
# MB4XDTIzMDQyNjA3NTcxMlloXDTMzMDQyNDA3NTcxMlowPDE6MDgGA1UEAwxt3B1
# blZQTiBXZWlgaQ0EGmJyMy4wNC4yNyAwNzozODoxMyBQRFRQgb3B1bnZwbmFzMjCC
# ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1qaBn39SMLvpcwRvKSmm8P
# 3C1dlcbjeqQpj2B15C07h26XPP+yd3bclWQ0v2eHc12IY8IO2TEyZEC4g6q2UEDE
# ZXHzd4MRtZgH0irJAMVJIfY9JdElLvyNepXurEBEpo79+czzhKRbiw3rZ5bBRKZk
# FTWIsIoHeaFEzLqnCypYHDxVciD3Vrv0BrJT+cmU7xqxxTAOGaJcJ+MgmsxvbPVM
# Pl1Wh+6HXpKigRP0gbxzIC++qd78sqjaKo78igyuLoZM28zdedRx1UZE97q7E/jw
# XhYezd/ecej/1GZ0lBclH47/esDQWtkmHk3obyixeGsIEceBzcdcDEc5Zc93MLsC
# AwEAAAMgMB4wDwYDVROTAQH/BAUwAwEB/zALBgNVHQ8EBAMCAQYwDQYJKoZIhvcN
# AQELBQADggEBAC1r0NshwIHjIk0DOTihk1+MHG8aXNmHydj6Rr4VHPno5fEFbkLu
# wsfPq1NaKVfKByMCiQJLU1rgtgHc00tvYDBlou1091n0bqKhCIEagAu/NbRM1/oP
# 2W8a0HvUONhuB0VkmfHfMarBQ2uuUbGcc6qbTf3IdletIKoc07lHN+Q/pQAiws
# gTT2I700tKDaYH1Ui57uCrD6/p2zqMxq9wrGopQAja5Rt12TUNT3Xr/YxZljrNVI
# 2vUaCs+TP4Bbi9DPCsLuft2MSF5ZpyCuPnCApcEkiqjMjd7lKMrupZgyXrn0/Kdn
# +UY9JaC8KGG83a0287rhunCrLtACaCJ2fNI=
# -----END CERTIFICATE-----
# OVPN_ACCESS_SERVER_WEB_CA_BUNDLE_STOP
```

1. El certificado CA (Certificate Authority)

Proporciona la clave pública de una autoridad de certificación que emite certificados para otras entidades. Este certificado se utiliza para verificar la autenticidad del servidor al que el cliente se está conectando en una configuración de OpenVPN, garantizando así la confianza en la conexión.

2.

```
<ca>
-----BEGIN CERTIFICATE-----
MIICxTCCAa2gAwIBAgIBAjANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDDApPcGVu
VlBOIENBMB4XDTIzMDQyNjA3NTcxMFoXDTMzMDQyNDA3NTcxMFowFTETMBEGA1UE
AwwKT3BlblZQTiBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALf7
LW6jvJFYcXJ8zDtrød/6DS2PEHjuuQtjaDmeQjUtnNdZB9ZNjivlZDTy5Ey/R4G
Gl2h1N12m1dcd7Pw7uagODSUE03PowS2QON6tjZCureFEE7kOz4fb2ZG7kBAfpUJ
yt/MxdAgdTCFG++UqrxbfLLCHZe5Sqa7fmWXAHiPe6vuirIb0ylh1BB4/hn28lZZ
a8J2A+qbcGHsZ65i/oKSv79v/t+8aCasxgxBPNicBxR0redAwvKDSuVtchzMWThk
9wd98TkDydl/B+jatXPD2hP/IQ7Xqlfg/Nm30bKC9MFLssysVOEEhjKgxylF2G1H
whafjESqPzvUMXkRyCkCAwEAAAMgMB4wDwYDVR0TAQH/BAUwAwEB/zALBgNVHQ8E
BAMCAQYwDQYJKoZIhvcNAQELBQADggEBAAKkugC1lIdlWZobtBSbE/agCMTZw2AX
h/F0FV68AZA2+jQPAYjMjDYabeN1/19kK7CWjYWYvks6eK9ZMqI2ntn52Xdmpe0j
yoKoIogSXI+qun10YVFAvpjjZtoN8rh1M4dDP+iOmNfgz1Ny51ezhnD2emYBt65j
Ik0P4RgmvoFz1aa+E+mOwldUB5sngOFsmvRs17rgIU7eVnHtzpMQ5dAyK4dD6v
2gIHxfp33Kv6UPTuShWOrM7Nj+P2FEoQHzi9Bxe+TW7Jaa9Qgji5E9wnqHwcxjuw
cNdtVJf9kNnP6ufCrPz7lBYt+B/SHOUCFZNQvNdpd82oZHRwaBYNHE=
-----END CERTIFICATE-----
</ca>
```

2. Certificado del servidor OpenVPN (CA):

El certificado de la Autoridad de Certificación se encuentra dentro de las etiquetas <ca>. Este certificado contiene la clave pública de la CA que emitió el certificado del servidor OpenVPN. Es necesario para que el cliente pueda verificar la autenticidad del certificado del servidor durante el proceso de handshake TLS.

3.


```
<cert>
-----BEGIN CERTIFICATE-----
MIIC5zCCAC+gAwIBAgIBCjANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDDApPcGVu
VlBOIENBMB4XDTI0MDQxODAxMjkxMDQxODAxMjkxMDQxODAxMjkxMDQxODAxMjkx
AwwHb3BlbnZwbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALmJhQSu
V1TN4neaRe0FMQcqtWblN9dEtmFGr1BiMDTrmIdaUIPJsrHj4W1P6CTObh18whPY
EE mnCjpbjbrY0n5DcPFx9nkDhqXh8gyrVn15vgJi/WKE+yck1lZLwtUA51+S6wdn
W3N70NdxckGjIl1s9+Xy78Z8qZJcyVAmNEl38H4ClwSx3qfNUxYJW6oFRLhBjbBI
plEJr8SyZlr7qzv9ZaoYFzZ0h78nCHiFfOEwv2ZsBLVm+PRsjjPoq5I0tDlurY5
yWITl7L7NBWGS5uCjGViGVgq26xcqJbJpeZs9XU0l8tVJZSBBMr9cIPUrOJeGFwZ
Zs01T/BfFTF8QmUCAwEAAaNFMEMwDAYDVR0TAQH/BAIwADALBgNVHQ8EBAMCB4Aw
EwYDVR0lBAwwCgYIKwYBBQUHAWIwEQYJYIZIAAYb4QgEBBAQDAgeAMA0GCSqGSIb3
DQEBCwUAA4IBAQA/8Q1G/kKv7/mPU3xeeSL1i8qK2mb4aaZrMPKBA3vBqRBy2dG
VT2YK/309v/ETIId6z6Suk6Z+7VNI9trmL5PRBHWkoJl7DwonBGDo7F2ndK+mf5q
zuhz69zt1rD+JWPUkFYbfkxkz7DVfVw7/i/opUJXKiL7WfaBMHR4Cw002wgBSAn
qoWULzRfgx6CITRQnAbB4MWjKV3dlZt76YhAYDFG0484xtCMEhwdaW04WrT/k6LD
Sym1b+UIxWQhQL/5hLwbmZwALIUl4Fpg+YCXQXzloMWXDWU7qfIHA6G/S6S00CKf
+F0EB5BhCQzg1lUCwnc5I8C5MG1xYzMZbz0G
-----END CERTIFICATE-----
</cert>
```

3. Certificado del Cliente (Cert)

Este certificado, emitido para "openvpn" por la misma autoridad que el certificado de autoridad y válido hasta el 17 de abril de 2034, se emplea para autenticar al cliente VPN ante el servidor, sirviendo como identificación reconocida por la autoridad emisora.

4.

```

<key>
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQC5iYUerldUzeJ3
mkXtBTEHKrVm5TfXRLZhRq5QYjA065iHWlCDybKx4+FtT+gkzm4dfMIT2BBJpwo6
Y262NJ+Q3DxcfZ5A4a1x4fIMq1Z9eb4CYv1ihPsnJJZWS8LVA0dfkushZ1tze9DX
cXJBoyJdbPf18u/GfKmsXm1QJjRjd/B+ApcEsd6nzVMWCvuqBUS4QY2wSKZRCa/E
smZa+6s74fWwqGBC2dIe/Jwh4hXzhFr9mbAS1Zvj0bI4z6KuSNLQ5bq20cliE5ey
+zQVhkubgoxlyhlyKtusXKiwyaxmbPV1NJfLVSWUgQTK/XCD1KziXhcgWbDtU/w
XxUxfEJlAgMBAAECggEAHfavnMnrIK7/XAF20YkVGesz0KJEGmfmbF9V13WEA4fo
4jMb vazdRw1eYqD9BLSx4+E6FqpWNw7bAAL+5j4pZuOqe+VtoVzQWKv8wz8IgMg
fJIwCbEgPnoSLW2e0XeL5kt72X4/rq7YU3Lm20LXse7f0iu5vXx0hka13GPPHe4S
P//jEciHcC517oZ70ppvMLYWBP4pow4uwTAVf+LISpV2ygQ5kNkmnbvdLPA7AgXK
z9Rn8Aqr180zje5CayMcPU3SdrcoNscxWTBx4tH7LZEMK12EX4Ybbegd5Fo70fAo
ycbesBYFQDFF5XSNA7kxBtXQ0Dqwg2Z7gtw2+FwAQKBgQDpsmLk/eP3DBC55wxn
jUxOvDIEBCf8Ww7KS9ks+q/qk9koaGdanCVn6fZ/pWRtmKkCZRBtaKg/TAN+c1gj
bgvizxp8zjoaFnLirs07sAGzrweOlW4pQzvV58kMs07dD9AYpuGelcYKxsE6nt
kY5lVrihZMweKiC3r0TdvbeugQKBgQDLPoLKLHMftL/KcN1b0KDsBVLoBpWSIYWX
gccRIQPEM/0ohmq7U4FYC44SNh6mjxUV5V/bbAAurLbm6pt6xE05n6PGBN7DnQ3F
9LxXsgAsbh01lw60wAV4H6tDIqEgD7ujdWoaboy+y/T1C9OLgMkfayLFXgu8PaJQ
3IvT0Pqp5QKBgQDoFcwK/u2vgibpX4f9KuE2bEYLoQkI4HF+y/bBabDc+Lm4HH9Q
CDRjZ5uCxwFGqk5mV3IKBd7ZBaeOowYPIZHITKVuf1SN4lws/RLQDa9c01qg6fQJ
rLh90oak1LNkfx+GtEoC7+7GVCfIKXsfu0c+kvJHLjBcYKAfa4ur32aUgQKBgQCj
v0ReoLtMAZM2ZgJhmVlFwrq2B4AAERPxfRhX4kKTZycRte8/wVJq12WXJYLOWIS
lw/I19W5xRtDJieIHJI3/l9Tjd7wGRvcrlyEDXxIT5N/i9p6s+50Hoe7+i14iFRz
2IhYrVKl8er0dsfEMElad9Yez6uCy0a3B8l8KXwa5QKBGE1DrNeJ1GGVpk+TzL/z
3qtz3Su/0ZACavmN2ieZfz/M2VdK89zhu1+hNXUBKSFJBu/x8rjbexk5eo4quexi
fP+pUkoKxMcfxEeNPCFDJW1c8VZvGiurIKdIU/8POg3FFAdZHq1ZXF3o7IQJHsVf
v3c7LVj8joz60rwYyM7Oxfzo
-----END PRIVATE KEY-----
</key>

```

4. Clave privada del cliente (Key)

Esta sección del archivo contiene la clave privada utilizada por el cliente OpenVPN para autenticarse ante el servidor. La clave privada se utiliza en el proceso de establecimiento de la conexión VPN para garantizar la autenticidad y confidencialidad de la comunicación.

5. Y 6.

```

-----BEGIN OpenVPN Static key V1-----
ac8b87a37c51adf80574cda9c01aa266
cee97d50fc5319a0f4931fef7de1946a
4c850715885c4e242fde7f3528862771
3cd48c0bb3900525365ced5c1fba05b2
c3818f8b81b9fe881facf3d434a3c441
ea69cdc5b1c475269d7f0d4dcdbdccc03
1f9a21352fd3460d9d55b0f920818b0f
88fe56384649672ea6bce67c2aa1cde6
0441341994422c39bffb6d61feae8b61
dc1bca1a51d89898dbf5a268e871189c
e49cfc162bf3142750e4126b751a4365
a3b1abed1d1a9d22f889e06d6b632250
58afaa29af2cf316ad072f771c1ac4
a2c17ae80893759f9adb0457cfc49f35
35b493ebd2cf2ff4f10b6e57f628e2b5
44900dec296722af2afcf04ebaf60a0e
-----END OpenVPN Static key V1-----
</tls-auth>
## -----BEGIN RSA SIGNATURE-----
## DIGEST:sha256
## rPEYGcb+G/P2LBAT4PWIXpaGAKLJaKyh/5oiz1gBDuznDsFZ7z
## SSShuGphtcGk1n+eXWqYcREYr8NOJnVvijvzQkj9ZD6Vhso2If
## T6SWv/kZyvBw10ybZTcl7KLnwBUpc1tKmZEnTwe3Cy2tY7wM6T
## Bbl0nUuerivbGvv3i4WAnQOGLZnvqvKzYIz7po430+ZD+c1KNz
## LhpQ4AV1cnrmdv1sTr5SHFQSPSuwLlneAs6TEYeVDWyI3p6CB9
## 7dRxkh2kNMNiKwwqpkwWtv++5AZL3rxOK+iBgr8wHvyBz4+N/
## asbECA4FU+MMwqABYwxt2Tr22mqH9tWdNi4RYNwa1A==
## -----END RSA SIGNATURE-----

```

5. Esta parte del documento contiene una clave estática de OpenVPN de 2048 bits, también conocida como "tls-auth" (autenticación de capa de transporte). Esta clave se utiliza para agregar una capa adicional de seguridad a la conexión OpenVPN al autenticar los paquetes de datos intercambiados entre el cliente y el servidor.
6. Esta sección del documento contiene una firma RSA (Rivest-Shamir-Adleman) generada utilizando el algoritmo de resumen SHA-256. La firma se utiliza para verificar la autenticidad e integridad de las partes anteriores del documento.

7. y 8.


```

## -----BEGIN CERTIFICATE-----
## MIIDHzCCAgegAwIBAgIFAMpyx9gwDQYJKoZIhvcNAQELBQAwPDE6MDgGA1UEAwWx
## T3B1blZQTiBXZWlgaQ0EgMjAyMy4wNC4yNyAwNzozODoxMyBQRfQgb3B1bnZwbmFz
## MjAeFw0yNDA0MTgwMzA4MjRaFw0yNTA0MTkwMzA4MjRaMBGxGjAUBGNVBAMMDTIx
## My45OS4yMjIuODUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXqiAf
## sTXE3TgFadwtwRPvYY7dxjt83cFqfEbwT1qFbx3/5+RBFInVd3kjncU8w4zD+gbp
## 7WCB9n9jFV6MDpc/8pyqI/Ik/Mi7BvVp6LMG1dtGJ1IgOPpdchBDX/tYiOQh9o6+
## 4SvAo3+PL9PeMTZCpYX7VIuas8tMTmicykO0dA2IGBWECqIKPu7CC83vVexfniBs
## bGbN8MlK5yxWS4DKX0nLdwJspD6iZ+tNIocq3ZRtAFBg6bEFfhZz2ocBT4JdWboq
## X5ZGSyV8+X0U51xwwH3fL2W12FH0Pd9EI55IcHwwxQI+XTeFpaXYFW+qSrA1mgW
## namZ/+pIg/2CBeaPAgMBAAGjTDBKMAWGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgWg
## MBMGA1UdJQQMMAoGCCSGAQUFBwMBMBGGA1UdEQQRMA+CDTIxMy45OS4yMjIuODUw
## DQYJKoZIhvcNAQELBQADggEBADHfE7OE0Y0CVD9ZP+5ORKzXugnkvVIDOMv1Vixh
## ZX6D/6b65ewMRZl30HDhkhVvXhvBqfULmkVyHO+IeOk+U/6SPdydIdsgCvai8Ock
## qKVPRfTInlpV3roVDKq/Xp+uV4Wvgp1X8EzzsnNkKhN+0GAH6UT4sKCNIvD1Siek
## 2DlqNQ1fHroTKBILAgPZGISQR5rLDzRyhVeBKpXzzYKRTfm6WnoyWhkMp57qddyQ
## qFm7Xyp7sCms/ISz/pVLHrBA/lmVYszonAfpCKHYo590a770arH1uEq0bwBFhWT
## Rz9GOkQ0Atremco/N+Fh219PEydv/0AchmyF2d+0IBW+QeE=
## -----END CERTIFICATE-----
## -----BEGIN CERTIFICATE-----
## MIIDFjCCAF6gAwIBAgIEZEeqNRZANBgkqhkiG9w0BAQsFADA8MTowOAYDVQQDDDFP
## cGVuVlBOIFdlYiBDQSAYMDIzLjA0LjI3IDA3OjM0OjEzIFBEVCBvcGVudnBuYXMy
## MB4XDTIzMDQyNjA3NTcxMl0XDTMzMDQyNDA3NTcxMl0wPDE6MDgGA1UEAwWxT3B1
## blZQTiBXZWlgaQ0EgMjAyMy4wNC4yNyAwNzozODoxMyBQRfQgb3B1bnZwbmFzMjAe
## ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1qaBn39SMLvpcwRvKSmm8P
## 3C1dlcbjeqQpj2B15C07h26XPP+yd3bc1WQ0v2eHc12IY8IO2TEyZEC4g6q2UEDE
## ZXHzd4MRtZgH0irJAMVJIfy9JdElLvyNepXurEBEpo79+czHkRbiw3rZ5bBRKZk
## FTWIsIoHeaFEzLqnCypYHDxVciD3Vrv0BrJT+cmU7xqxxTAOGaJcJ+MgmsxvBPVm
## Pl1Wh+6HXpKigRP0gbxzIC++qd78sqjaKo78igyuloZM28zdedRx1UZE97q7E/jw
## XhYezd/ecej/1GZ01BclH47/esDQWtkmHk3obyixeGsIEceBzcdcDEc5Zc93MLSc
## AwEAAAMgMB4wDwYDVR0TAQH/BAUwAwEB/zALBgNVHQ8EBAMCAQYwDQYJKoZIhvcN
## AQELBQADggEBAC1r0NshwIHjIk0DOTihk1+MHG8aXNmHydj6Rr4VHPno5fEFbkLu
## wsfPq1NaKVfKByMCIqJLU1rgtgHc00tvYDBlou1091n0bqKhCIEagAu/NbRM1/oP
## 2W8a0HvUONhuB0VkmnfHfMarBQ2uuUbGcc6qbTf3IdletIKoc07lHN+Q/pQAiws
## gTT2I700tKDaYH1Ui57uCrD6/p2zqMxq9wrGopQAja5Rt12TUNT3Xr/YxZ1jrNVI
## 2vUaCs+TP4Bbi9DPCsLuft2MSF5ZpyCuPnCApcEkiqjMjd7lKMrupZgyXrnO/Kdn
## +UY9JaC8KGG83a0287rhunCrLtAcACJ2fNI=
## -----END CERTIFICATE-----

```