UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Servicios de VPN comerciales: ventajas, riesgos de uso y alternativas.

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Calatayud Giner, Jorge

Tutor/a: Pons Terol, Julio

CURSO ACADÉMICO: 2022/2023

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Servicios de VPN Comerciales: Ventajas, riesgos de uso y alternativas.

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Autor: Jorge Calatayud Giner

Tutor: Julio Pons Terol

Curso 2022-2023

Resum

En els darrers anys el negoci dels serveis de VPN comercials ha patit un creixement sense precedents. En aquest treball s'estudiaran els avantatges i els inconvenients de l'ús d'aquests serveis per a l'usuari mitjà. Finalment, es compararan les diferents alternatives a aquests serveis i es mostrarà la instal·lació i la configuració d'aquestes alternatives fent una anàlisi exhaustiva del seu rendiment.

Paraules clau: VPN, ciberseguretat, connexions, xifrat, tunneling.

Resumen

En los últimos años el negocio de los servicios de redes privadas virtuales (VPN) comerciales ha sufrido un crecimiento sin precedentes. En este trabajo se estudian las ventajas e inconvenientes del uso de estos servicios para el usuario medio. Por último se comparan las diferentes alternativas a estos servicios y se muestra la instalación y configuración de estas alternativas haciendo un análisis exhaustivo de su rendimiento.

Palabras clave: Vpn, ciberseguridad, conexiones, cifrado,tunneling.

Abstract

In recent years the business of commercial virtual private networks (VPN) services has experienced unprecedented growth. This paper study the advantages and disadvantages of using these services for the average user. Finally, the different alternatives to these services are compared and the installation and configuration of these alternatives are shown, making an exhaustive analysis of its performance.

Key words: Vpn, cybersecurity, connections, encryption and tunneling.

Índice general

Índice de figuras

CAPÍTULO 1
Introducción

VPN o ***Virtual Private Network*** es una tecnología la cual permite la creación de una conexión segura y privada entre varios dispositivos a través de una red publica, como es el caso de internet. Esta conexión se basa en la creación de un túnel virtual entre el usuario de la conexión VPN y el servidor VPN complementado con protocolos de cifrado y autenticación.[1]

Beneficiándose de esta tecnología ha aparecido un servicio el cual nos referiremos como **VPN comercial**. Este servicio se basa en la utilización de una conexión VPN para aumentar la seguridad de sus clientes durante su conexión a internet, mediante una interfaz sencilla y con un proceso de configuración irrisorio.[16]

El uso de las VPNs comerciales ha aumentado exponencialmente en los últimos años debido a varios factores como la informatización repentina del mundo donde vivimos, convirtiéndose en un negocio muy lucrativo para las empresas que lo ofertan.

1.1 Motivación

Actualmente es muy difícil escapar de los anuncios de empresas anunciando su servicio VPN como si fuese la solución a todos tus problemas de seguridad informática: Anuncios en redes sociales, pago a influencers para que recomienden su productos, entradas patrocinadas en periódicos y blogs anunciando su producto, donde muchas veces no se puede identificar que es un contenido promocional.

Esto me suscita las siguientes preguntas:¿Es de verdad el negocio de las VPN comerciales tan seguro y rentable para que puedan permitirse esta inversión multimillonaria en publicidad o no es tan seguro como podría parecer a simple vista?¿Existe alguna alternativa a estos servicios la cual me permita tener seguridad sin entregarle mi información a este tipo de empresas?

Resolver estas dudas son mi principal motivación detrás de este trabajo.

1.2 Objetivos

El objetivo principal de este trabajo de investigación es indagar sobre como de conveniente es el uso de servicio de VPN comercial para el usuario medio, posibles alternativas creadas por el usuario y su viabilidad y rendimiento comparándolas con el servicio que nos ofrece el mercado.

1.3 Estructura de la memoria

Este trabajo se divide en 8 capítulos:

1. **Introducción:** En el capítulo actual se hace una presentación a los conceptos de VPN y VPN comercial y se describe la motivación y los objetivos propios de este proyecto.
2. **Estado del arte:** En el apartado actual se estudiará el estado actual del arte en cuanto a alternativas a servicios VPN comerciales y el estudio de la seguridad del uso de estos servicios. También se realizará un breve estudio del mercado para tener una mejor perspectiva del asunto en cuestión.
3. **Fundamentos de una VPN:** En este capítulo se tratará a grandes rasgos los fundamentos técnicos detrás de una conexión VPN y su utilidad en términos de ciberseguridad.
4. **Servicios de VPN comercial:** En este apartado describiremos la situación de mercado en la que se encuentran los servicios VPN comerciales y su riesgos de uso.
5. **Alternativa al uso de servicios de VPN comercial:** En este capitulo se propondrán algunas alternativas factibles al uso de servicios de VPN comerciales.
6. **Implementación de las soluciones:** En está sección se mostrará como se podría implementar alguna de las soluciones propuestas en el apartado anterior.
7. **Análisis de rendimiento:** Este capítulo se trata de un análisis del rendimiento que nos ofrece cada una de nuestras alternativas
8. **Conclusiones:** En esta sección se mostrarán las conclusiones a las que se han llegado con este proyecto.

CAPÍTULO 2
Estado del arte

Como se ha comentado con anterioridad el objetivo detrás de este proyecto es dilucidar como de conveniente es el uso de servicios de VPN comerciales frente otras alternativas vigentes, por tanto será necesario realizar este análisis diferenciando dos cuestiones, que aún al estar claramente relacionadas es necesario darle un tratamiento diferente: La conveniencia del uso de servicios de VPN comerciales y la presentación de alternativas.

También en este apartado se hará un análisis de la situación actual del mercado de los servicios de VPN comercial, ya que es vital para el correcto estudio del estado del arte de las problemáticas tratadas en este trabajo.

2.1 Conveniencia del uso de servicios de VPN comercial

En cuanto la conveniencia del uso de estos servicios, es difícil encontrar artículos académicos que traten esta problemática siendo [18] uno de los pocos que con cierta profundidad que se ha podido encontrar durante la investigación.

En lo que refiere a **RiuNet** esta temática no ha sido tratada con profundidad en ninguno de los trabajos académicos que se pueden encontrar en esta plataforma.

A pesar de esto, esta problemática ha sido abordada por diferentes portales WEB de prestigio como puede ser el medio digital **Buissnes Insider**[5] y otros de menos renombre como **vpnranks**[8] o **restoreprivacy**[12].

2.2 Alternativas al uso de servicios de VPN comercial

El estudio de alternativas a estos servicios de VPN comercial ha sido documentado en numerosas ocasiones. Actualmente en **RiuNet** al utilizar la palabra clave **"VPN"** hemos podido encontrar 233 estudios, de los cuales gran parte tratan la implementación de este tipo de soluciones.

Centrándonos en el campo de los artículos académicos, estos se pueden encontrar de manera bastante sencilla al ser un área muy estudiada a lo largo del tiempo siendo [19] y [20] ejemplos de ello. A pesar de la amplia existencia de artículos académicos que propongan alternativas a los servicios comerciales de VPN, estos conllevan una complejidad o desembolso económico que los hacen poco factibles para usuarios tecnológicos no-expertos, siendo este trabajo enfocado a ese tipo de usuario hemos decidido descartar este tipo de alternativas.

En la búsqueda de soluciones de implementaciones más sencillas hemos dado con artículos los cuales realizan implementaciones más asequibles para el usuario medio como puede ser [21] y [22], las cuales han sido las opciones elegidas en nuestro caso.

2.3 Situación de mercado

En los últimos años había un claro crecimiento del consumo de estos servicios. En 2019 se calculaba que el tamaño de mercado del negocio de las VPN era de 25,56 miles de millones de dolares y se estima que de 2019 hasta 2027 va a haber un crecimiento anual compuesto del 17,4 por ciento.[11] También ha crecido el número de personas que conocen este tipo de servicios, ya que en 2022 el 88 por ciento de los estadounidense eran conscientes de la existencia de las VPN siendo este porcentaje un 3 por ciento superior al año anterior (fig.2.1).[2]

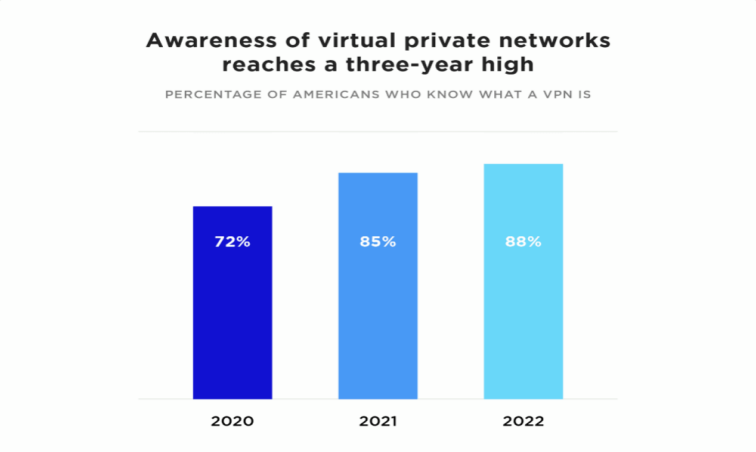

Figura 2.1: Conocimiento estadounidense sobre las VPNs.

Este aumento se puede explicar por la informatización repentina que ha sufrido por la mayoría de sectores laborales y el acercamiento a la informática que han recibido muchas personas en los últimos años.

En cuanto a la motivación de uso de estos servicios, el 55 por ciento de los usuarios en Estados Unidos una de sus motivaciones para el uso de este tipo de servicios era para aumentar su seguridad informática[2]. Esta preocupación de los usuarios de este tipo de servicios por su seguridad en la red aumenta la necesidad de realizar una análisis de la seguridad que estas proporcionan.

CAPÍTULO 3
Fundamentos de una VPN

La creación del primer protocolo de VPN data del año 1996, desde entonces este tipo de conexiones llevan siendo utilizadas en entornos empresariales para diversas labores como acceder a redes comerciales privadas. No sería hasta la década de los 2000 que no se comenzaría a ofertar servicios de VPN comercial, siendo estos una revolución en cuanto a ciberseguridad se refiere.[17]

El objetivo de estos servicios de VPN comercial es utilizar una conexión VPN como intermediario para una conexión posterior. El caso más ejemplar sería el siguiente: nos encontramos en una red insegura y queremos transmitir unos datos mediante internet, nos conectamos a una VPN y transmitimos los datos hacia nuestro objetivo final. Nuestros datos habrán ido de nuestro dispositivo origen mediante esta red insegura pero como los protocolos VPN realizan una encriptación, estos se vuelven indescifrables para un supuesto atacante, luego serán recibidos por nuestro servidor VPN y estos serán reenviados por la red a la cual está conectado nuestro servidor VPN, a priori segura, hasta nuestro destinatario final.

A pesar de la antigüedad de esta tecnología y los avances tecnológicos de los últimos años, esta sigue vigente en la actualidad siguiendo un funcionamiento similar al originario de entonces, aunque con mejoras en los protocolos utilizados.

3.1 Funcionamiento de una VPN

En cuanto a la tecnología VPN se refiere no podemos hablar de un protocolo único ya que hay diversos tipos de VPN. Según cuál sea la motivación detrás de la creación de la misma, utilizará un tipo de protocolo u otro, pero a grandes rasgos el funcionamiento de una conexión VPN lo podemos dividir en 5 procedimientos consecutivos:

- **Autenticación**: Antes de poder realizar efectiva una conexión VPN el equipo que va realizar esta conexión tendrá que autenticarse, normalmente mediante un usuario y contraseña, una vez demostrada la identidad de este equipo se determinará si es posible esta conexión y en que condiciones se realizará.

- **Establecimiento de túnel**: A continuación se deberá crear un túnel virtual entre ambas partes, este se crea mediante técnicas de **tunelización**. Entendemos como **tunelización** o *tunneling* al proceso de encapsulamiento de un tipo de tráfico de red dentro de otro protocolo, para poder transmitirlo de forma eficiente, ya que sin esta encapsulación la conexión sería imposible. Un ejemplo paradigmático del uso de este tipo de técnicas sería el siguiente: Existen dos redes las cuales son independientes la una de la otra y se busca que varios dispositivos establezcan una conexión segura, para conseguir esto bastará con que una de las redes encapsule sus mensajes como tráfico de la otra red, permitiendo así la transmisión segura por la red intermediaria. En esta parte de la conexión se logra la consolidación de este túnel para con posterioridad encapsular los paquetes necesarios. Dependiendo de las necesidades del usuario, al crear la conexión VPN se utilizará una técnica de tunelización o otra, es decir no podemos hablar de un protocolo uniforme para todas las VPN, aunque los protocolos más comúnmente usados en cuanto a tunelización para VPN se refiere serian ***L2TP*** (Protocolo de Túnel de Capa 2), ***IPSec*** (Protocolo de Seguridad de Internet) y ***PPTP*** (Protocolo de Túnel de Punto a Punto).

- **Cifrado y encapsulamiento**: El siguiente paso es el cifrado y encapsulamiento de los paquetes que se van a enviar por parte del dispositivo origen. El encapsulamiento será hecho mediante el protocolo de *tunneling* anteriormente concertado con el servidor. Una vez realizado este encapsulamiento de los paquetes dispuestos a enviar, se procederá al cifrado de estos mismos, para su transmisión segura. Este cifrado se realiza mediante algoritmos criptográficos siendo los más comunes el **AES** y **3DES** entre otros.

- **Enrutamiento y transporte de los datos**: A continuación se realizará el correspondiente enrutamiento y envío de los datos desde la maquina origen, este proceso se realiza por el protocolo de enrutamiento propio de la red por la cual se realice este envío.

- **Desencapsulación y descifrado de datos**: Una vez recibido los paquetes en la red anfitrión del servicio VPN estos son paquetes se desencapsularán y descifrarán para posteriormente ser retransmitidos a la destinación final de estos mismos.

3.2 Utilidad del uso de una conexión VPN

La utilización de una conexión es de gran utilidad en cuanto la seguridad se refiere. Debido a la naturaleza de este tipo de conexiones, estas conexiones están totalmente cifradas desde la salida de los paquetes desde la maquina cliente hasta la llegada a la red anfitriona de este servicio.

Al estar encriptada esta conexión garantiza un nivel de privacidad superior, ya que estos paquetes no pueden ser a priori descifrados por un posible atacante. Además una conexión VPN garantiza la integridad de los datos enviados ya que los protocolos utilizados en la conexiones VPN suelen tener

algún mecanismo para controlar la integridad de los mensajes. Estas dos características son muy útiles cuando pretendes hacer alguna conexión dentro de una red la cual no esté garantizada su seguridad como es el caso de una conexión WIFI pública.

Otro beneficio de la utilización de una conexión VPN es el anonimato que te otorga. Al enrutarse tu tráfico a través del servidor VPN, el servidor destino percibirá como ip origen la ip del servidor VPN, complicando así la tarea de rastreo por agentes externos, como anunciantes y otro tipo de rastreadores.

Otra ventaja que te puede otorgar la utilización de una VPN sería cambiar tu ubicación geográfica a ojos del servidor web al cual vas a realizar una conexión, adoptando la ubicación propia del servidor VPN al cual estés conectado. Esta característica te permite acceder a contenido en internet los cuales serían inaccesibles desde tu país de origen debido a alguna restricción geográfica, lo cual es una práctica que no alentamos a realizar.

Como último apunte una conexión VPN se puede utilizar para acceder a recursos propios de la red anfitriona como si estuviese el dispositivo cliente dentro de esta red. Actualmente debido al gran aumento de teletrabajos cada vez es más común el uso de este tipo de conexiones en el sector laboral e incluso académico, permitiendo acceder a escritorios virtualizados o recursos propios de la red local de la empresa mediante una conexión VPN.

CAPÍTULO 4
Riesgos de utilización de servicios de VPN comercial

Una VPN comercial es un servicio ofertado por una empresa privada que facilita el uso de una conexión VPN. La configuración de este tipo de servicios consiste en instalar un software y registrarse en él. Esta facilidad de configuración es uno de los motivos por los cuales han podido cautivar a tantos usuarios.

La utilización de una conexión VPN, como se ha indicado anteriormente, puede tener beneficios a la hora de conectarse a internet frente a no utilizar una. No obstante, el uso de servicios VPN comerciales puede poner en riesgo tu privacidad y seguridad por varios motivos.

Una de las motivaciones que puede tener un usuario para utilizar un servicio de este tipo es mantener tu anonimidad durante el transcurso de tu conexión a internet. Teniendo esto en cuenta, se conocen casos de servicios de VPN los cuales recogen tus datos de usuario para venderlos como Big Data o utilizarlos para posicionar anuncios personalizados. Esta practica es más comúnmente realizadas por parte de los servicios VPN comerciales gratuitos o de bajo costo a que es una manera de mantenerlos rentables, como ya advirtió Simon Migliano, jefe de investigación del portal prestigioso **Top10VPN** en [5] , los servicios de VPN gratuitos suelen estar repletos de anuncios específicos para cada usuario dependiendo de su comportamiento en la red, ofreciendo una protección de datos muy pobre. Proveer acceso a una serie de servidores VPN conlleva su gasto, por tanto siempre que no estés pagando por el servicio esté contendrá anuncios para su mantenimiento.

Otro de los problemas que tienen este tipo de servicios es la procedencia de estos servicios, ya que según un informe del portal **Top10VPN**, las 10 VPN comerciales gratuitas más conocidas son propiedad de alguna empresa china en mayor o menor medida[5] y casi un tercio de las VPN más relevantes son propiedad de seis empresas chinas, según un estudio de **VPNpro**[9]. Este hecho es más preocupante teniendo en cuenta que en china el uso de servicios VPN no aprobados por el gobierno está prohibido, las cuales para que este apruebe este servicio la empresa propietaria tiene que darle acceso exclusivo a esta[10] y que es común la colaboración de la empresas chinas con su gobierno[7], lo cual pone en duda la seguridad de estos servicios. Otro ejemplo de esta problemática seria la empresa **Kape,** esta se trata de una empresa fundada por dos ex-militares israe-

líes. Esta empresa antes era conocida como **crossrider** y se dedicaba a implantar adware en los equipos de usuarios. Este dato es preocupante ya que **Kape** en los últimos años ha comprado 3 empresas de VPN **Cyberghost, privateinternetaccces y Zenmate**, lo cual habla muy mal de la seguridad de los servicios de VPN comercial.[12]

Otro punto controversial es la política **no-log**. Esta es una política que consiste en que la empresa se compromete a no almacenar los datos de las conexiones que el usuario ha hecho. La mayoría de empresas que ofrecen estos servicios suelen hacer gala de tener esta política de privacidad, lo cual es difícil de demostrar incluso se han encontrado varios casos en el pasado de incumplimiento de esta política. Evidentemente el incumplimiento de esta política es una violación de la privacidad del usuario. Un ejemplo de esto es el caso de PureVPN donde esta ayudó al gobierno de Estados Unidos proviniéndoles información de un cliente suyo el cual estaba siendo investigado por el FBI, lo cual significa que estaban incumpliendo la política no-log ya que si no hubiese ningún tipo de registro hubiese sido imposible otorgarle esa información al FBI.[3] Según un estudio del portal de VPNRanks en el cúal se analizó las políticas de seguridad de 101 servicios de VPN, se llegó a la conclusión que solo 3 de esas 101 se podían llegar a llamar seguras, afirmando en [8] que la política no-log solo se trata de un termino de marketing para atraer a compradores potenciales y que en la practica esta política no existía como tal.

En conclusión el uso de este tipo de servicios puede llegar a ser inseguro, aunque no se pueda demostrar que todos lo sean. Por tanto el usuario es el que debe saber, según sus necesidades y la importancia que de a su seguridad en la red, si le vale la pena optar por usar este servicio, buscar alternativas o incluso no usar ningún tipo de conexión VPN.

CAPÍTULO 5
Alternativa al uso de servicios de VPN comercial: Servidor VPN propio

Como se ha discutido con anterioridad un servicio de VPN comercial no siempre es la mejor de las opciones en cuanto a seguridad de tus datos se refiere; ante estos existe una alternativa la cual te brinda claras ventajas a nivel seguridad, crear un **servidor VPN propio**.

Este al estar gestionado única y exclusivamente por el usuario le otorga un control absoluto del tráfico garantizando una seguridad superior de los datos del usuario al no ser gestionados por ninguna empresa externa.

Existen varias alternativas para la creación de un servidor VPN propio según donde quieras alojarlo pero nosotros discutiremos las más relevantes dentro de nuestro criterio, las cuales son: Alojar nuestro servidor VPN en un router, en una maquina física (por ejemplo un ordenador personal) y en un servidor externo.

5.1 Utilización de un router como servidor VPN

El uso de tu router personal como VPN tiene varios beneficios como la fácil configuración de los clientes que estén conectados a ese router, pero este tiene algunos inconvenientes.

La configuración de un router puede llegar a ser muy tediosa para usuarios no especializados. La mayoría de routers no tienen la función de servidor VPN por defecto por lo que en gran parte de los casos esto obliga al usuario a instalar manualmente un software que lo permita, siendo esto muy peligroso para el usuario inexperto, ya que hay casos en los cuales si la instalación se hace de manera incorrecta puede llegar a dejar el router inservible.[4]

Una alternativa a instalar un software que permita la utilización de tu router como servidor VPN es comprar un router que incluya esta función, lo cual puede a llegar a ser muy costoso.

Como conclusión la utilización de un router como servidor VPN puede llegar a ser beneficiosa, siempre que dispongas de uno con la funcionalidad preinsta-

lada o que la facilidad que este otorga sea lo suficientemente importante para el usuario como para que el desembolso económico valga la pena.

5.2 Utilización de un dispositivo físico como servidor VPN

Utilizar un dispositivo físico como un servidor VPN tiene ciertas ventajas frente al resto de alternativas, el principal beneficio de este es la facilidad de instalación de este mismo. Esta sencillez se debe a que la mayoría de dispositivos modernos, como los ordenadores personales y los smartphones, utilizan sistemas operativos sofisticados que de manera nativa o con una fácil instalación permiten la utilización de estos como servidor.

A pesar de la facilidad de configuración que supone esta alternativa, esta tiene un claro inconveniente frente a la alternativa que mostraremos a continuación. Esta es la obligación de mantener encendida siempre la maquina que queremos utilizar como servidor siempre que queramos hacer uso de la conexión VPN, lo cual causa un gasto energético considerable en la mayoría de casos.

Este problema se podría a llegar a solventar adquiriendo una máquina de bajo consumo como una *raspberry pi*, la cual consume de media casi 100 veces menos que un portátil[13] [14], pero siendo la configuración de esta más compleja para usuarios no expertos que la de otro tipo de dispositivos más convencionales.

5.3 Utilización de un servidor externo como servidor VPN.

Esta solución solventa varios problemas que nos ocasionaban las dos alternativas anteriormente expuestas. Esta alternativa nos garantiza la creación de un servidor VPN propio sin la necesidad de tener ni un router con la funcionalidad VPN, reduciendo así el coste, ni tampoco tener que tener operativa 24 horas al día una maquina propia.

Otra ventaja frente a las soluciones anteriormente mencionadas es el coste de esta misma, el cual puede llegar a ser nulo ya que existen varios planes de alquiler de servidores de baja capacidad gratuitos, como por ejemplo que ofrece la empresa Oracle.

La única desventaja frente a las alternativas anteriormente mostradas es la complejidad de configuración de nuestro servidor externo, siendo esta algo más tediosa que las anteriores soluciones pero siendo aún así una posibilidad para todo tipo de usuarios ya que esta no tiene una complejidad exagerada.

CAPÍTULO 6
Implementación de las soluciones

En este apartado implementaremos las alternativas anteriormente presentadas. En este caso no se mostrará la implementación de la solución basada en la utilización de un router como servidor VPN, ya que según mi criterio es la alternativa con menos potencial de entre las anteriormente mencionadas.

6.1 Implementación de un servidor VPN en un dispositivo físico

Como ejemplo de esta implementación utilizaremos una máquina Windows 10, la cual es muy similar a otras versiones de Windows y es el caso más común entre los usuarios. Otro beneficio que nos otorga la utilización de una maquina Windows 10 frente a otras con otro sistema operativo es la facilidad de instalación ya que el propio sistema operativo permite esta opción.

El primer paso de nuestra instalación será obtener nuestra IP publica y IP privada de nuestra maquina anfitrión. Para obtener nuestra IP publica en mi caso he utilizado una página web externa llamada *https://www.cualesmiip.com/* (fig. 6.1) pero existen muchas paginas alternativas a esta web, también existiendo la opción de obtener esta IP entrando a la pagina de configuración del router al que esté conectado vuestra maquina.

Figura 6.1: Captura de la pagina web *https://www.cualesmiip.com/* (censurada).

Para obtener la IP privada de nuestra maquina bastará con acceder a la maquina de comandos de nuestro dispositivo y utilizar el comando *IpConfig* (fig.6.2). También tomaremos nota de cual es nuestra puerta de enlace predeterminada ya que nos será de utilidad en el futuro.

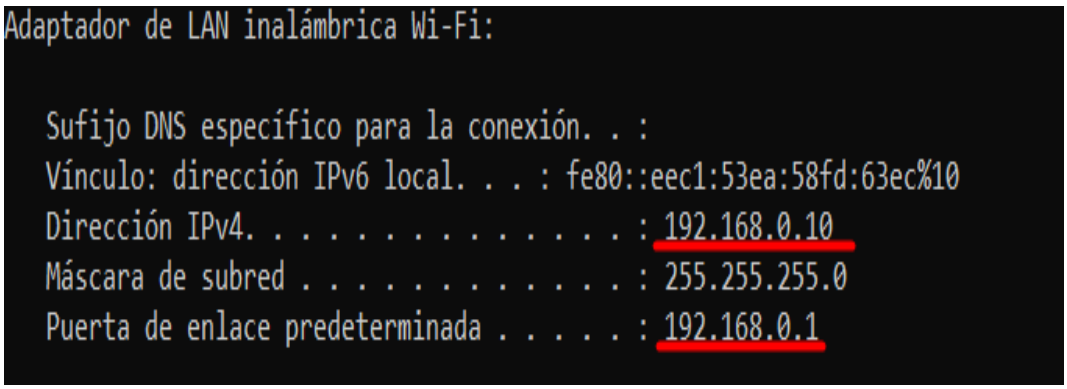

Figura 6.2: Captura de la orden ipconfig.

Una vez hecho esto entraremos al *centro de redes y recursos compartidos*, que se encuentra dentro del panel de control de nuestro ordenador y una vez ahí accederemos a la opción *cambiar configuración del adaptador* (fig.6.3).

Figura 6.3: Captura del menú cambiar configuración del adaptador.

Una vez dentro del menú tendremos que utilizar el comando *alt+a* para que aparezca un menú desplegable en el cual pulsaremos la opción *nueva conexión entrante* (fig.6.4).

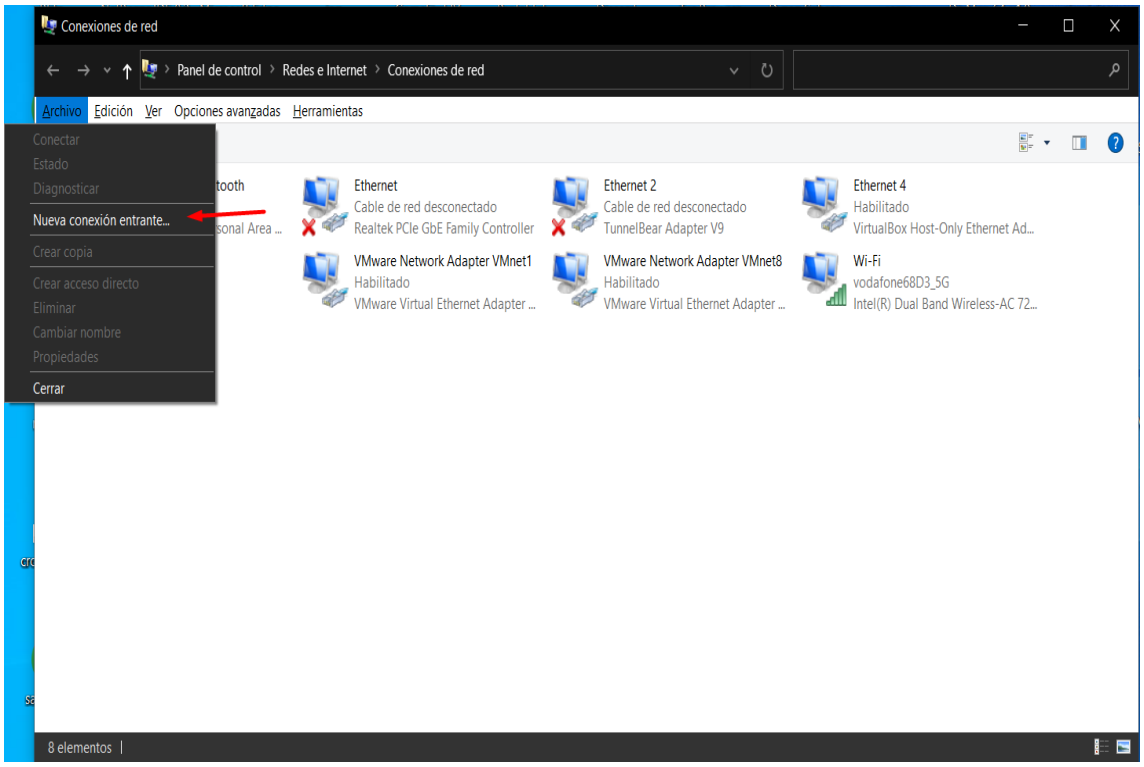

Figura 6.4: Captura de acceso al menú nueva conexión entrante.

Al clicar en esa opción se nos abrirá un menú el cual nos pedirá que indiquemos que usuarios serán capaces de conectarse a esta conexión. En nuestro caso al querer crear una conexión VPN tendremos que entrar en la opción *Agregar a alguien* (fig.6.5).

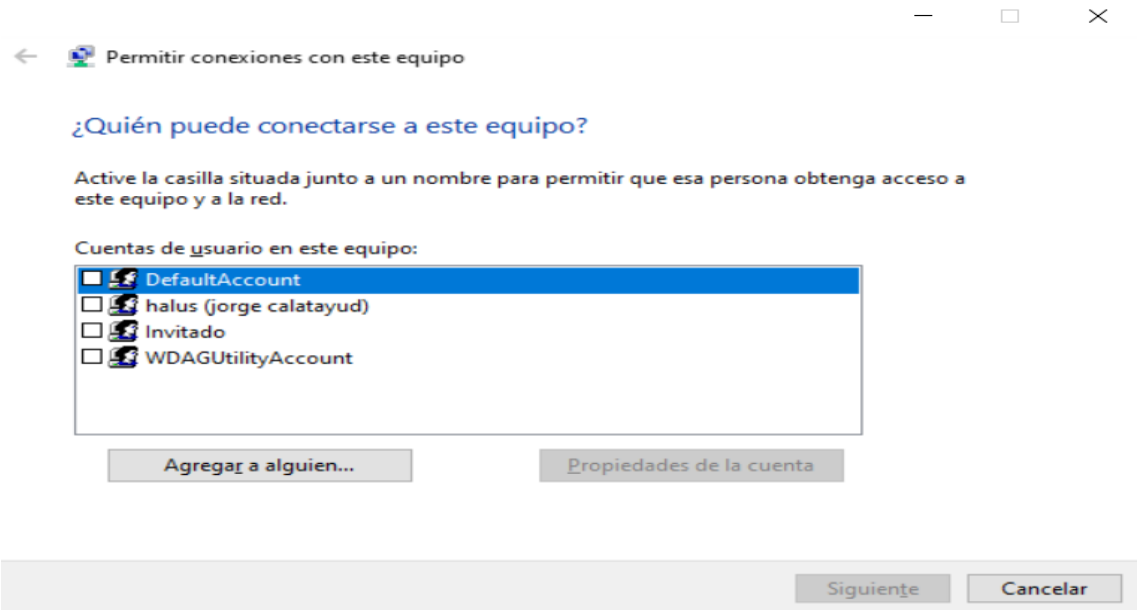

Figura 6.5: Captura del menu añadir nueva conexión entrante.

En esta ventana (fig.6.6) se nos requerirá la información del usuario cliente el cual vaya a conectarse a nuestro servidor VPN. Este paso se deberá repetir una vez para cada dispositivo que vaya a realizar una conexión a nuestro servidor. Una vez creado nuestros usuarios seleccionaremos la casilla que se encuentra a la izquierda de cada uno de estos y clicaremos el botón de siguiente.

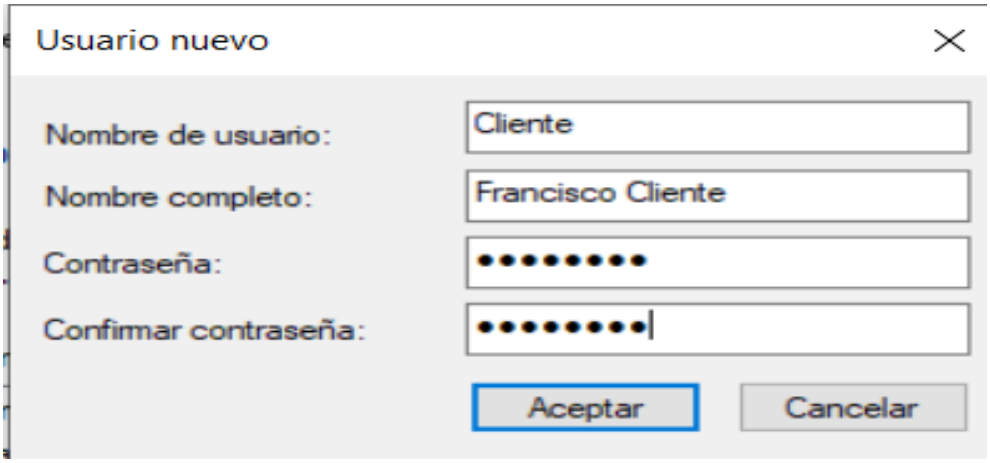

Figura 6.6: Captura del menu Agregar a alguien.

A continuación aparecerá una ventana emergente (fig.6.7), la cual te dará la opción de que nuestra conexión sea a través de internet, en nuestro caso marcaremos que sí, ya que se trata de una conexión VPN.

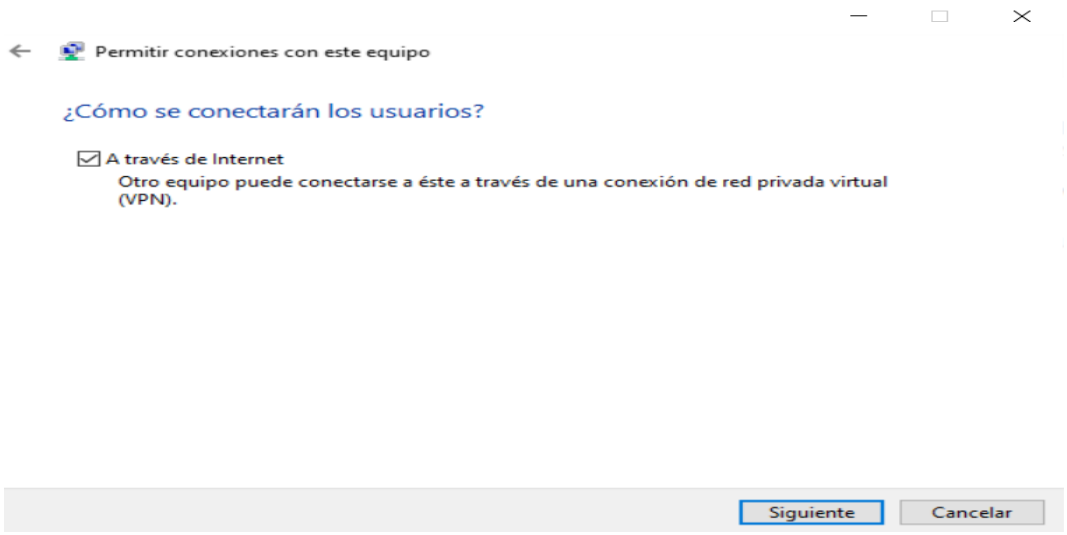

Figura 6.7: Captura de la opción A través de internet.

Por último se mostrará una ventana (fig.6.8) la cual servirá para indicar que tipo de protocolos se permiten en la conexión. En nuestro caso particular solo permitiremos conexiones **IpV4** pero las otras opciones pueden a llegar a ser interesante en otras situaciones. También desde este menú podremos acceder a otras configuraciones de la conexión para esto pulsaremos la opción *propiedades*.

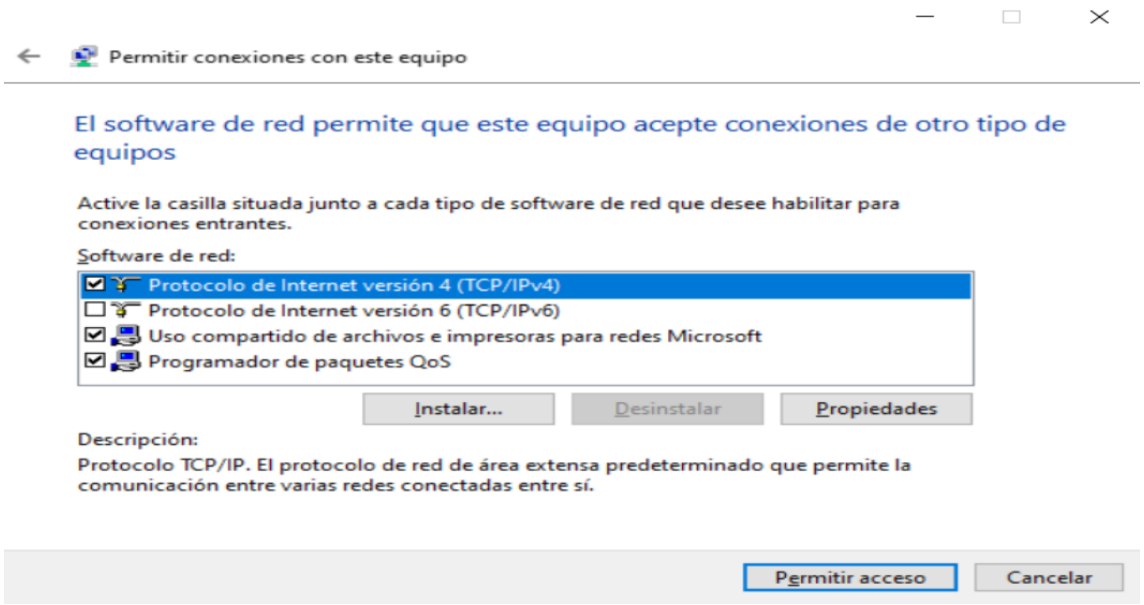

Figura 6.8: Captura del menú para especificar los protocolos permitidos.

En el menú de propiedades (fig.6.9) podremos especificar las direcciones IP de las conexiones entrantes, en nuestro caso vamos a limitarlo a 11 direcciones IP. Para eso, partiendo de mi dirección IP privada, seleccionaré 11 valores que estén en nuestro rango.

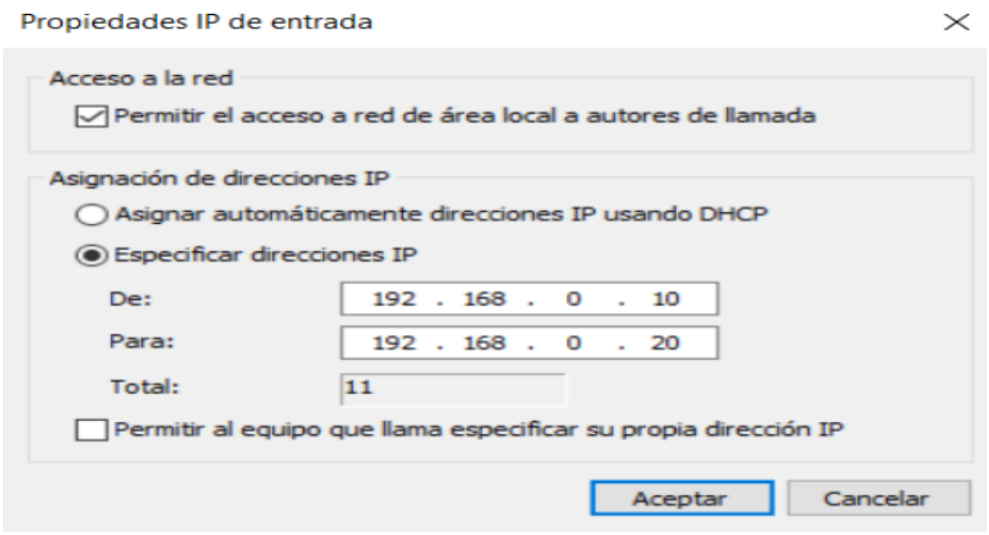

Figura 6.9: Captura del menú para especificar el rango de direcciones de los clientes.

Una vez hayamos seleccionado el rango de ip de nuestra VPN pulsaremos el botón de aceptar en ambas ventanas y nos saldrá un mensaje de confirmación con el nombre de nuestro equipo, ese es el identificador de nuestro equipo el cual nos permitirá la conexión a nuestro servidor, por lo tanto es importante guardarlo. Una vez anotado el nombre, cerramos la ventana.

El siguiente paso será acceder al apartado llamado *Firewall de Windows defender* (fig.6.10) dentro de nuestro panel de control y acceder a la opción *Permitir que una aplicación o una característica a través de Firewall de Windows Defender*.

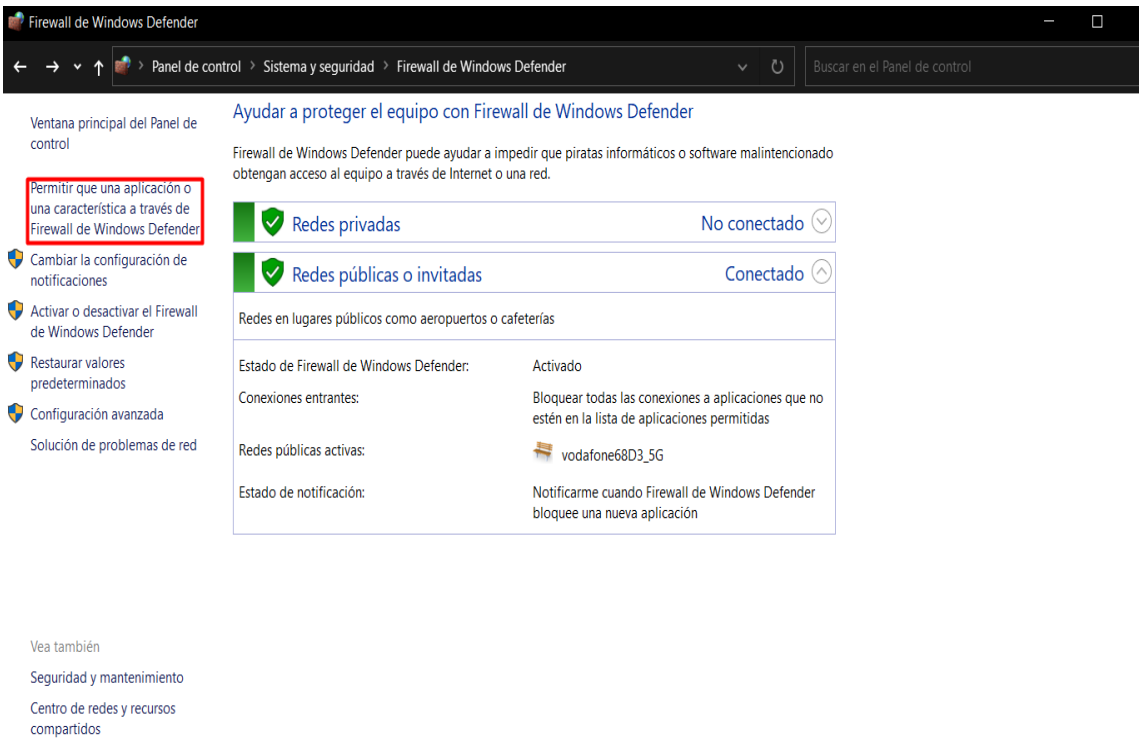

Figura 6.10: Configuración de nuestro Firewall I.

Una vez dentro de ese menú clicaremos el botón de arriba a la derecha con el nombre *cambiar configuración* y nos cercioraremos de que la característica *Enrutamiento y acceso remoto* (fig.6.11) está preseleccionada tanto para redes publicas como privadas, si no es así habrá que seleccionarlas.

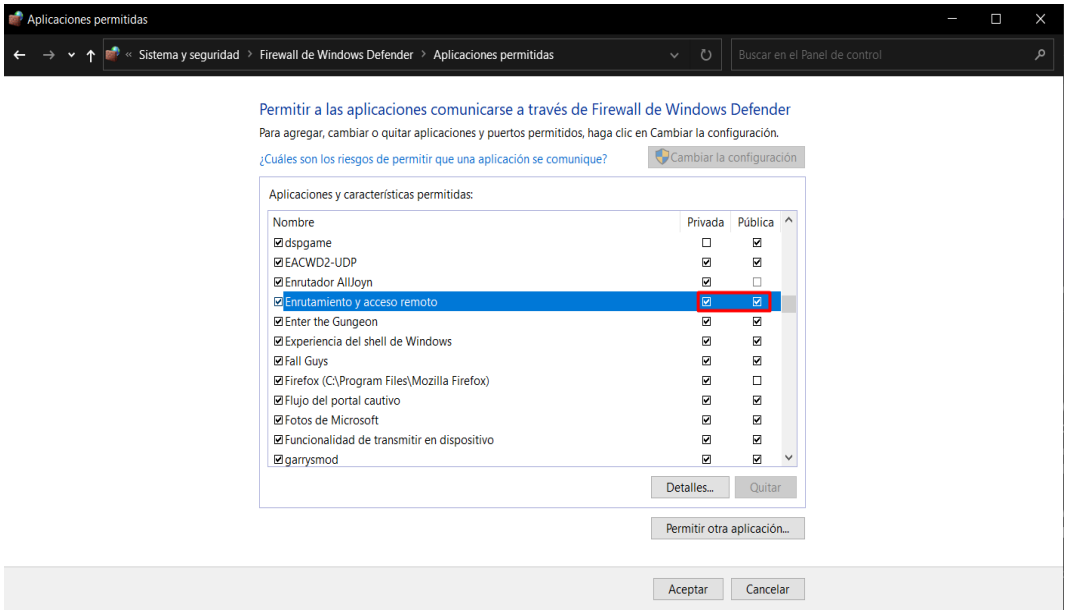

Figura 6.11: Configuración de nuestro firewall II.

Por último tendremos que acceder a la configuración de nuestro router (fig.6.12) al cual está conectado la maquina que va a servir como servidor VPN. Según el modelo de router que tengas se entrará de una forma o otra pero en nuestro caso será introduciendo la siguiente dirección ip en nuestro navegador *http://192.168.0.1/*, la cual es la dirección ip de nuestra puerta de enlace predeterminada.

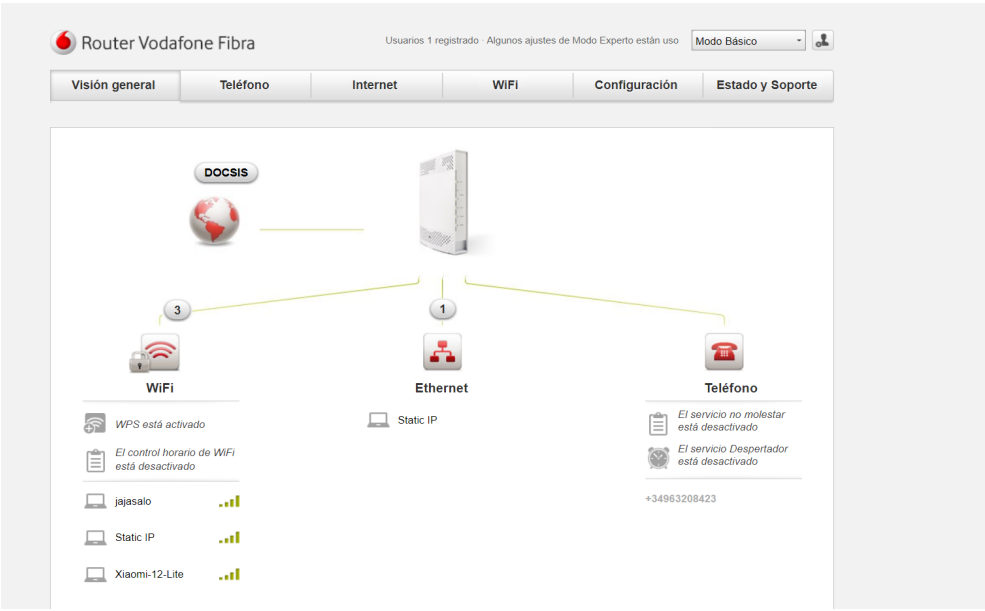

Figura 6.12: Pagina de configuración de nuestro router personal.

Al haber accedido a la configuración del router tendremos que acceder a la sección de redireccionamiento de puertos de nuestro router (fig.6.13). Una vez ahí la configuración puede cambiar según el modelo de router que tengamos. En nuestro caso solo hará falta poner la dirección IP privada de nuestro dispositivo, los puertos por los cuales activaremos nuestra redirección en nuestro caso es el *1723*, ya que se trata del puerto por el cual funciona el protocolo VPN, tanto para el puerto publico como el de nuestra LAN y seleccionar el protocolo *TCP/UDP*.

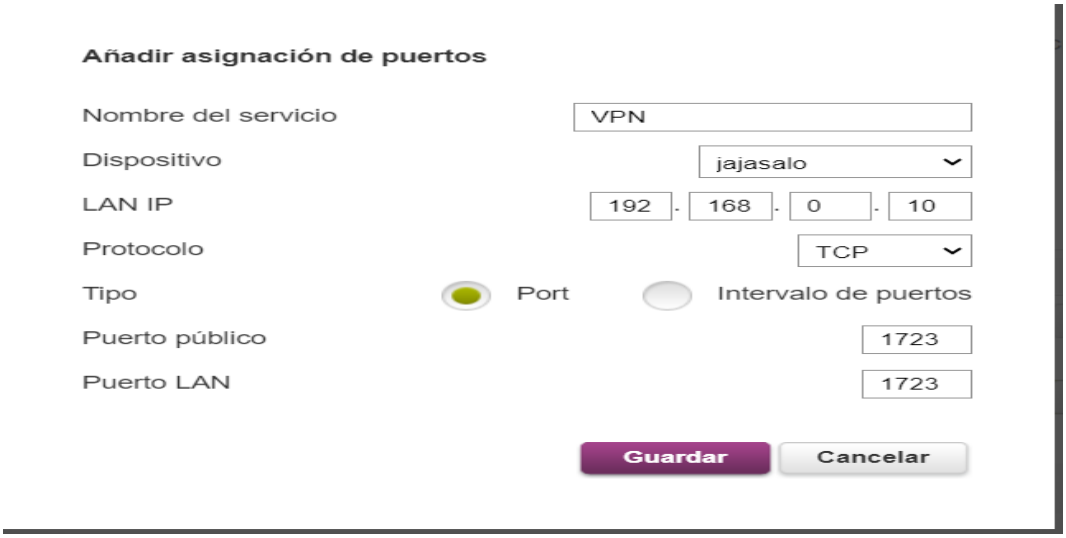

Figura 6.13: Configuración del redireccionamiento de puertos de nuestro router.

Una vez realizado la configuración de puertos nuestra configuración habrá terminado.

6.2 Implementación de un servidor VPN en un servidor externo

Para implementación de nuestro servicio lo primero que necesitaremos será acceso a un servidor externo. En nuestro caso estaremos utilizando un servidor de **Oracle cloud**, ya que incluye un plan gratuito que nos permite el uso de una maquina con bajas prestaciones, la cual es más que suficiente para alojar un servidor VPN funcional. Para configurar nuestro servidor primero de todo habrá que entrar en la siguiente url: *https://www.oracle.com/es/cloud/free/* y clicar en comenzar gratis lo cual nos llevará a la siguiente interfaz (fig.6.14).

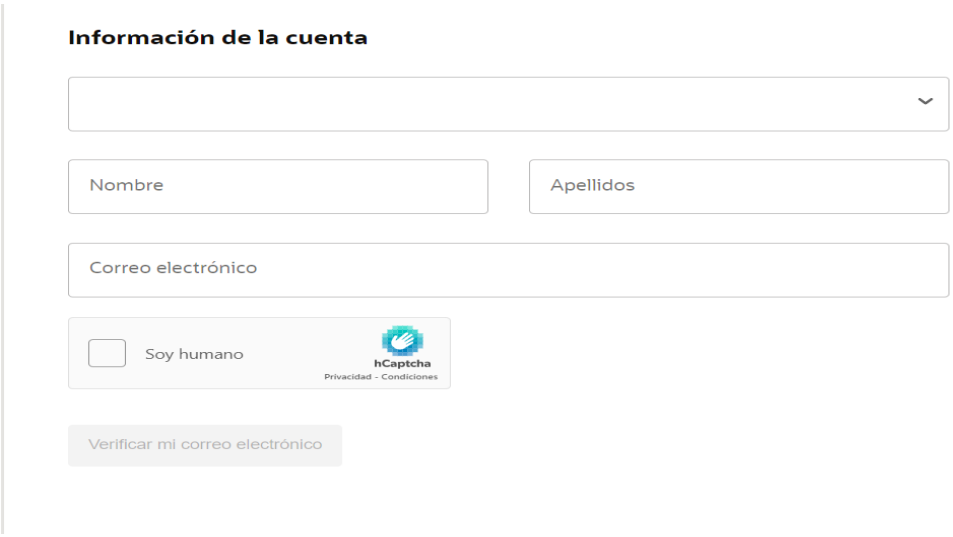

Figura 6.14: Menú de creación de cuenta.

Una vez seguido los pasos que se indican en la página web, iniciaremos sesión y accederemos a nuestro panel de control (fig.6.15). Una vez ahí clicaremos en la opción *Instances compute*.

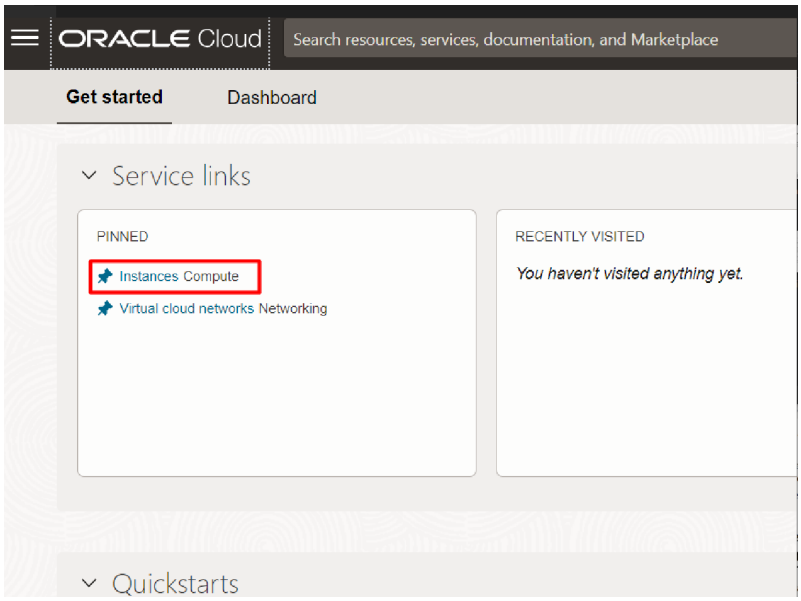

Figura 6.15: Captura del panel de control del portal de oracle.

A continuación accederemos al menu *create instance* (fig.6.16) y crearemos una instancia con los valores predefinidos (fig.6.17), ya que estos són más que suficientes para un servidor VPN con un tráfico reducido (0.48Gbps), en caso de necesitar más ancho de banda deberás cambiar la configuración a tu gusto.

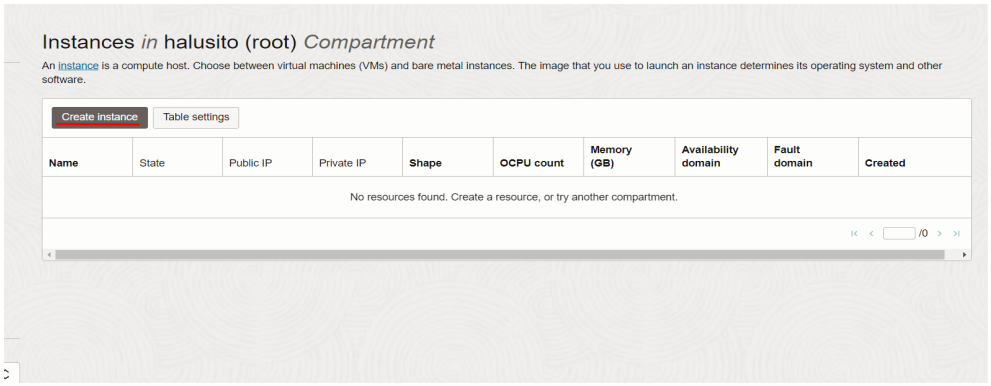

Figura 6.16: Captura del menu de instación de ordenadores.

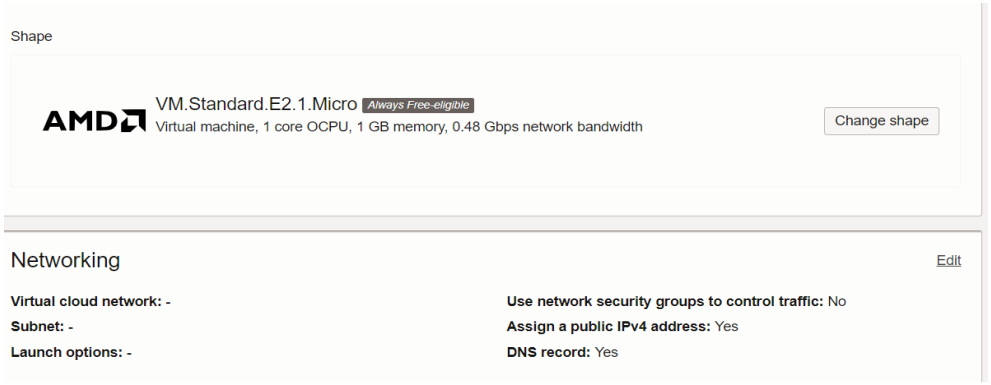

Figura 6.17: Valores predefinidos de nuestra instancia.

El único cambio mayor que haremos a la configuración inicial será cambiar la imagen de instalación para eso solo tendremos que seleccionar el botón *change image* y nos abrirá el desplegable mostrado en la figura 6.18. La imagen que en nuestro caso hemos seleccionado ha sido un *ubuntu 20.04*, ya que se trata de una distribución de linux que no genera muchas complicaciones a la hora de operar con ella.

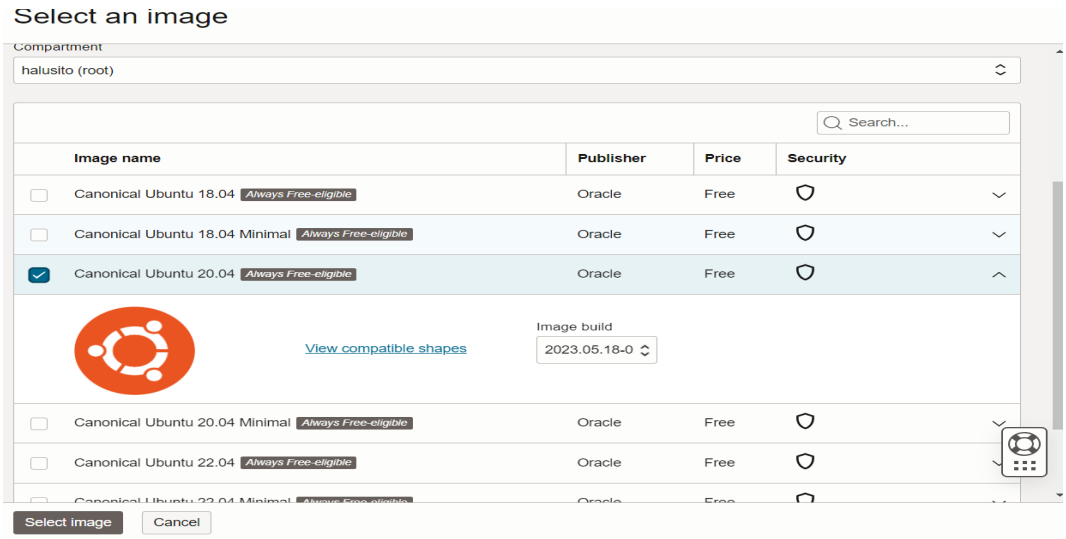

Figura 6.18: Menu de cambio de imagen de instalación.

A esta maquina nos conectaremos por ssh, en mi caso mediante el software **PuTTYgen**, para poder hacer esto deberemos crear una clave publica en el programa PuTTYgen Key generator (fig.6.19) el cual se te incluye con la instalación *PuTTYgen*. Generaremos una clave publica, añadiremos esta a la maquina en el apartado *Paste public keys* (fig.6.20) y guardaremos nuestra clave privada clicando en la opción correspondiente dentro del programa *PuTTYgen* (fig. 6.19)

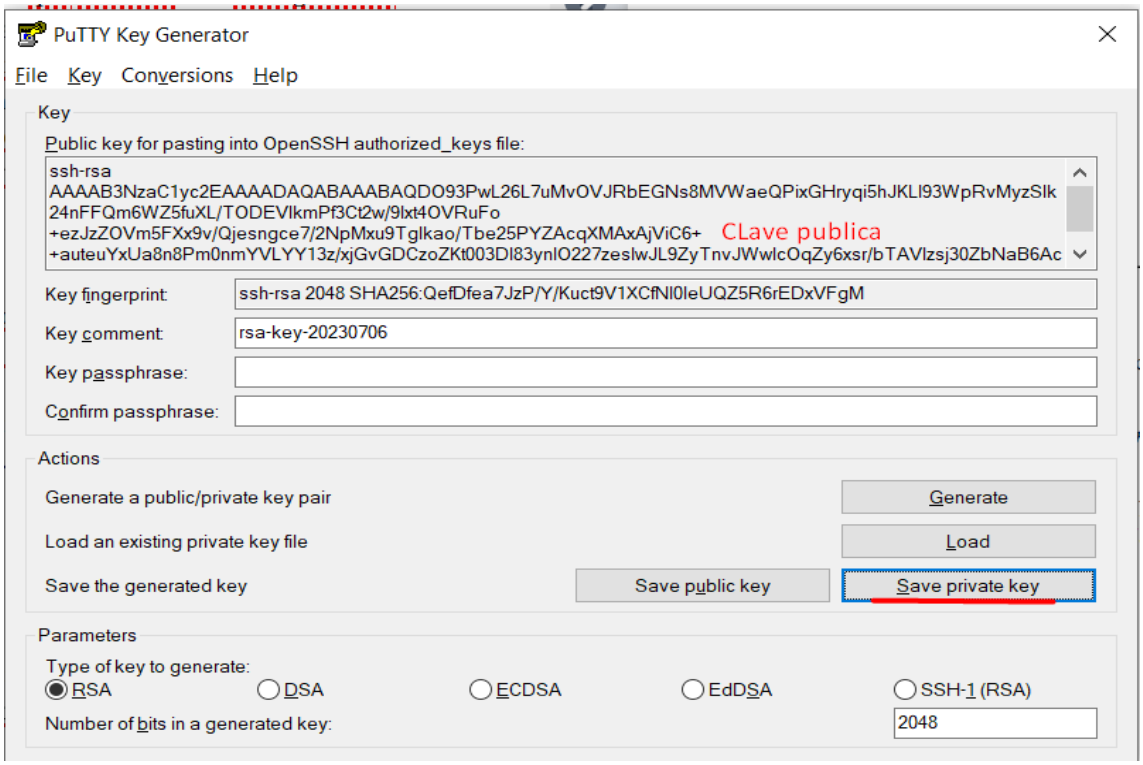

Figura 6.19: Generación de clave ssh.

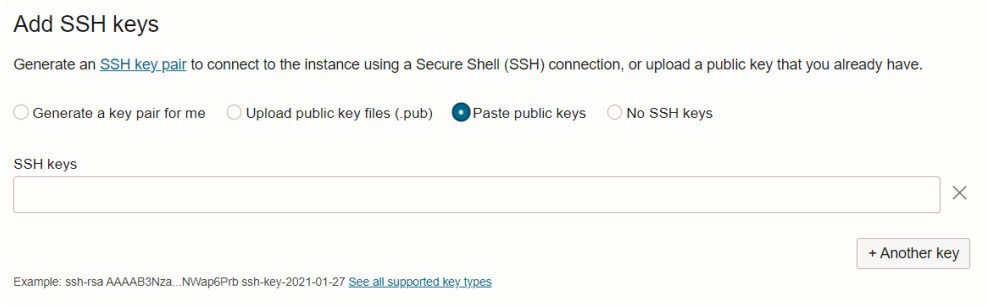

Figura 6.20: Añadido de clave ssh a nuestro programa oracle.

Una vez seleccionado la imagen tendremos que crear una nueva subred y una *virtual cloud network* (fig. 6.21) para que la máquina pueda conectarse a internet y ya podremos crear nuestra instancia.

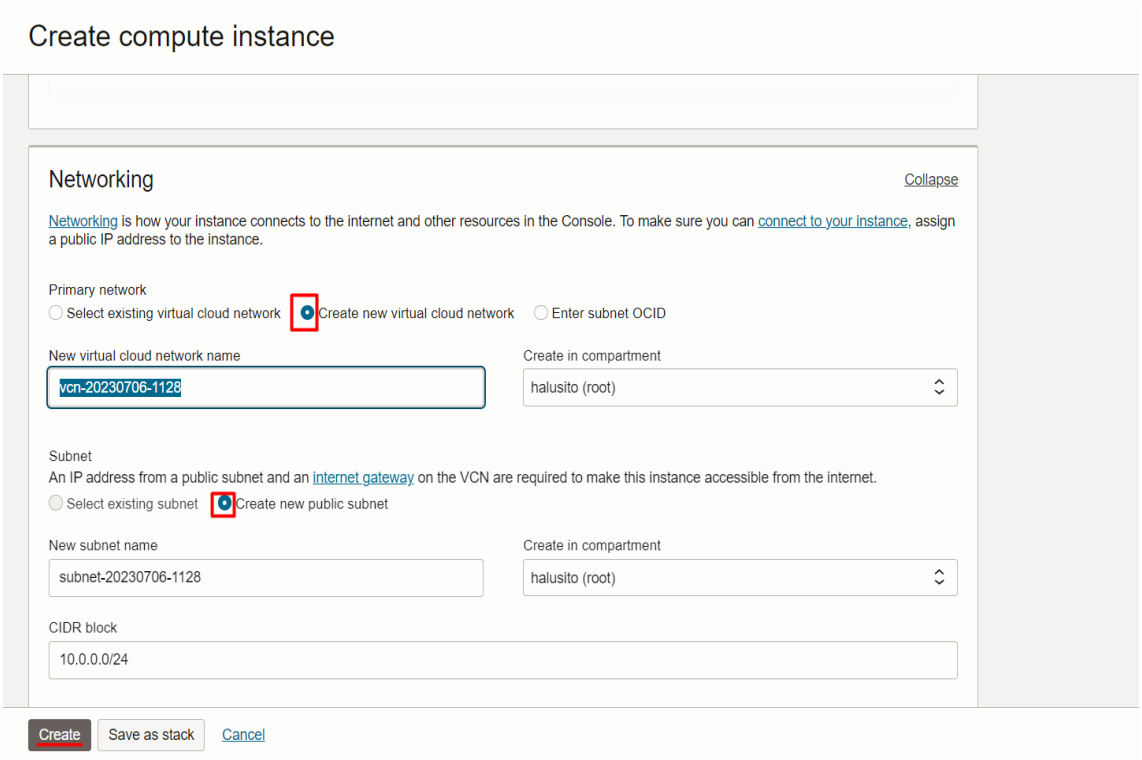

Figura 6.21: Creación de nuestra subnet.

Para encender nuestro servidor y acceder a este lo primero que tendremos que hacer es ir a nuestra pestaña de instancias clicar en la que acabamos de crear y darle al botón de encendido (fig.6.22).

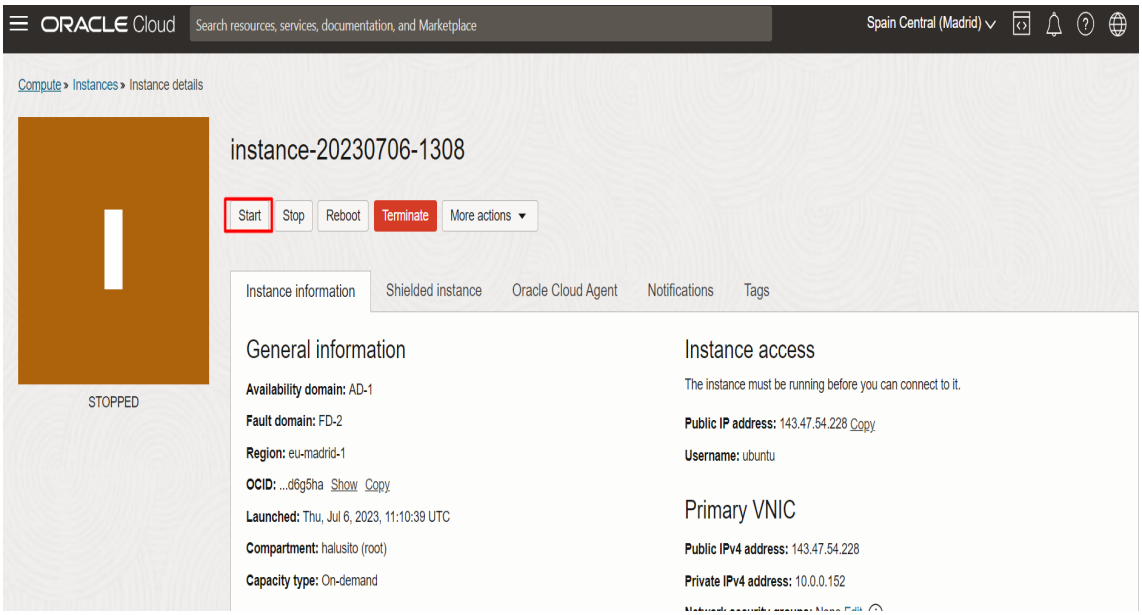

Figura 6.22: Arranque de nuestra maquina.

Para conectarnos a nuestro servidor entraremos en *PuTTY*. Como nombre de host pondremos ubuntu@"la ip de tu instancia", un ejemplo sería el siguiente: *ubuntu@143.47.54.228*. Y en el apartado auth, insertaremos nuestra llave ssh (fig.6.23) y le daremos a iniciar.

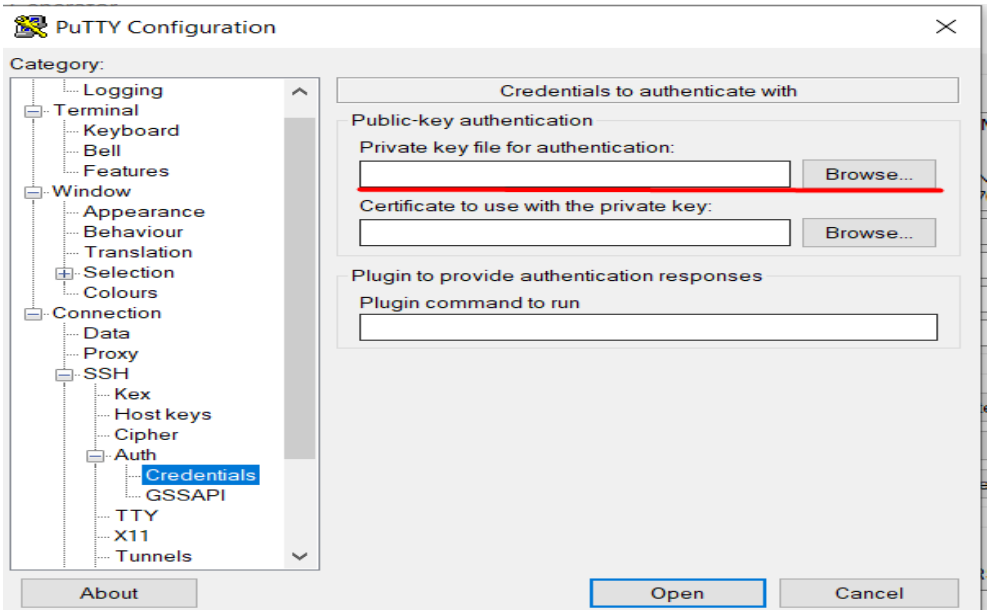

Figura 6.23: Introducción de nuestra clave ssh.

Una vez conectados por ssh al servidor procederemos a actualizar e instalar un entorno gráfico y lo necesario para poder acceder a nuestra maquina sin la necesidad de utilizar una conexión ssh. En este caso nuestro objetivo es poder conectarnos por escritorio remoto de Windows, ya que es más conveniente en nuestro caso y para realizar esto, los comando a ejecutar son los siguientes:

```
1 sudo apt update && sudo apt upgrade
2 sudo apt-get install ubuntu-desktop xrdp stacer -y
3 sudo cp /etc/iptables/rules.v4 /etc/iptables/rules.v4.bak && sudo
    truncate -s 0 /etc/iptables/rules.v4
4 sudo rm /usr/share/polkit-1/actions/org.freedesktop.color.policy
5 sudo passwd ubuntu
```

Como habréis observado el último comando sirve para cambiar la contraseña del usuario ubuntu, esto nos facilitará la entrada a nuestra maquina. Una vez acabada la instalación reiniciaremos la maquina y procederemos a habilitar el acceso a la maquina mediante escritorio remoto.

Para que nuestra maquina sea accesible mediante escritorio remoto tendremos que configurar el firewall de la misma. Para configurarlo tendremos que acceder a la configuración de nuestra maquina, entrar en la configuración de nuestra subred y una vez ahí modificar nuestra lista de seguridad, siguiendo los pasos de las figuras 6.24 y 6.25.

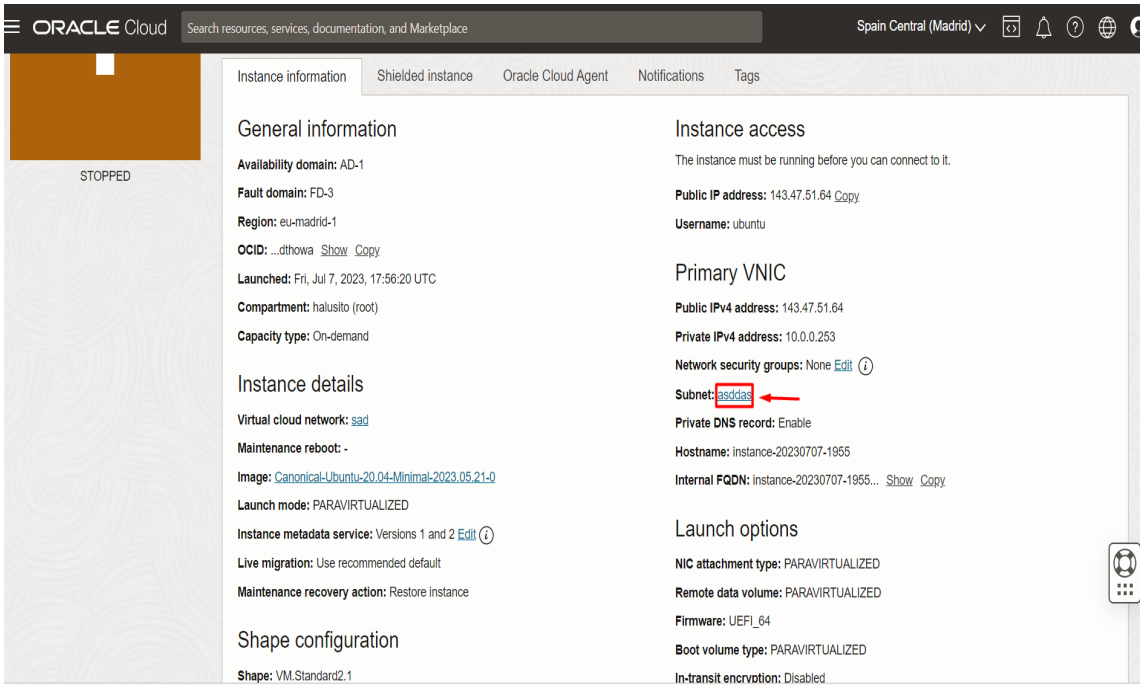

Figura 6.24: Menú de modificación de nuestra subred I.

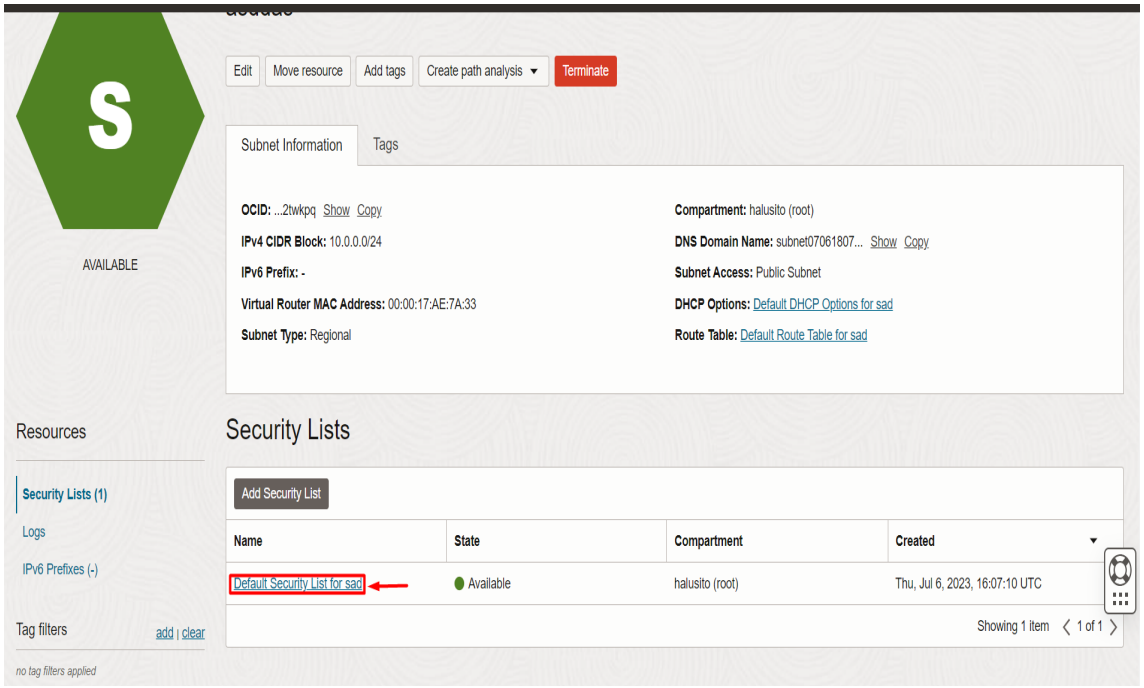

Figura 6.25: Menú de modificación de nuestra subred II.

Dentro de nuestra lista de seguridad añadiremos una nueva regla de acceso en la que abriremos el puerto 3389,ya que este se trata del puerto que utiliza el protocolo de escritorio remoto, tal y como se muestra en la figura 6.26.

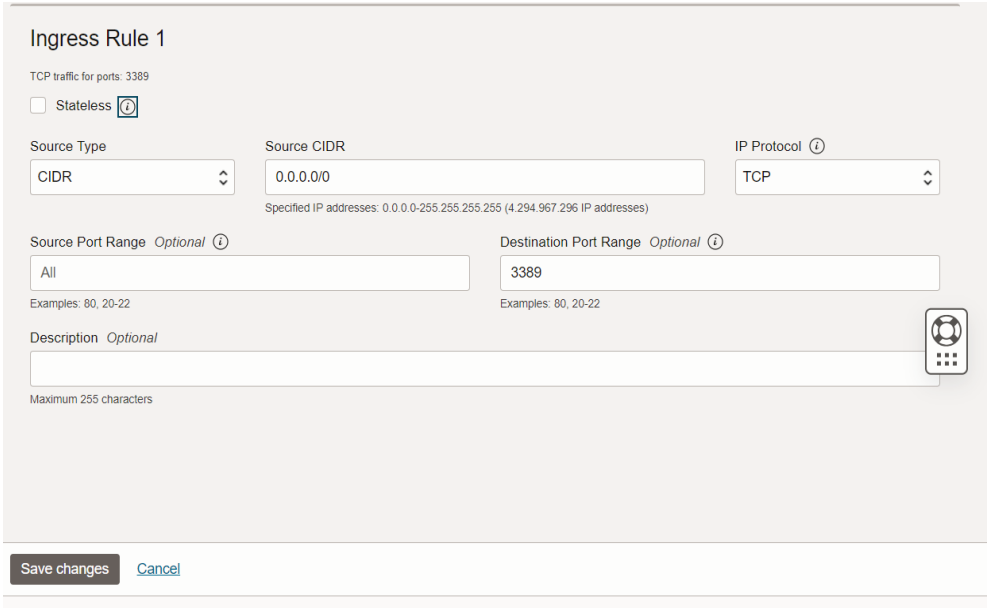

Figura 6.26: Configuración de nuestro firewall.

Llegados a este punto ya podremos acceder a nuestra maquina mediante escritorio remoto (fig.6.27). Abriremos el programa de escritorio remoto de Windows y iniciaremos sesión mediante la IP de nuestra maquina y el usuario ubuntu.

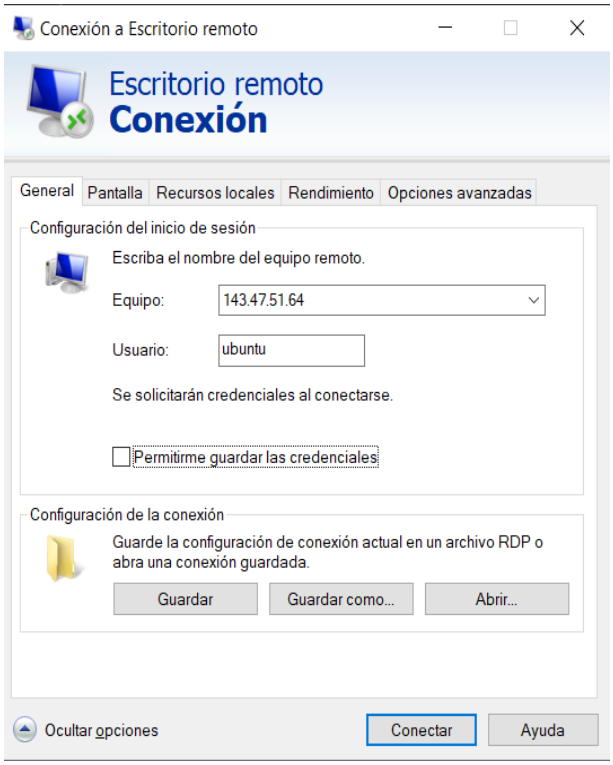

Figura 6.27: Acceso a nuestro escritorio remoto.

Una vez ya configurada nuestro dispositivo habrá que instalarle el software para convertirlo en un servidor VPN. En este caso estaremos utilizando el software *Openvpn*, el cual es una de las opciones más populares para alojar un servidor

VPN en ubuntu. Para completar su instalación solo tendremos que ejecutar los siguientes comandos:

```
apt install ca-certificates wget net-tools gnupg

wget -qO - https://as-repository.openvpn.net/as-repo-public.gpg | apt-key add -
echo "deb http://as-repository.openvpn.net/as/debian focal main">/etc/apt/sources.list.d/openvpn-as-repo.list

apt update

apt install openvpn-as
```

Por último tendremos que cambiarle la contraseña al usuario de ubuntu *Openvpn* para poder acceder al panel de control de nuestro servidor:

```
passwd openvpn
```

El último paso de nuestra configuración será acceder al panel de control (fig.6.28) que gestiona nuestro servidor VPN. Para ello tendremos que acceder a la siguiente url desde nuestro servidor: *https://nuestraip:943/admin*. Las credenciales para acceder a nuestro panel de control serán como usuario ***openvpn*** y como contraseña la contraseña elegida en el paso anterior.

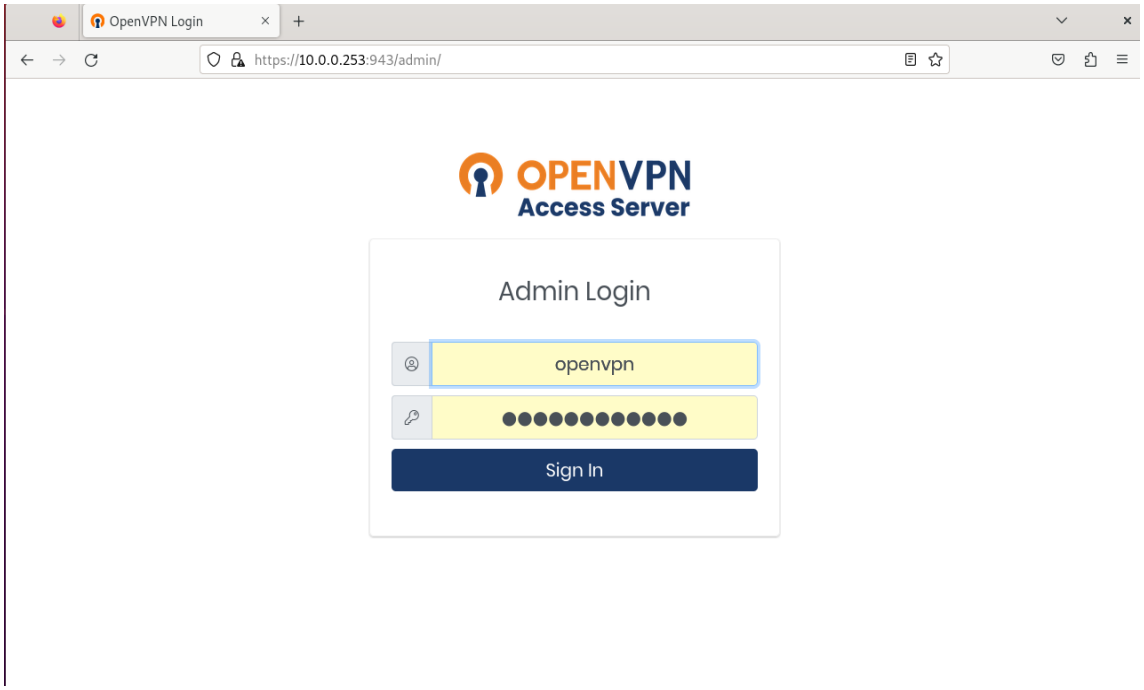

Figura 6.28: Acceso al panel de control de openvpn.

Una vez accedemos al portal de administración de nuestra VPN tendremos que añadir un nuevo usuario para nuestro ordenador cliente en la pestaña *user permisions* (fig.6.29), elegiremos un nombre y habilitaremos la opción *Allow Autologin*.

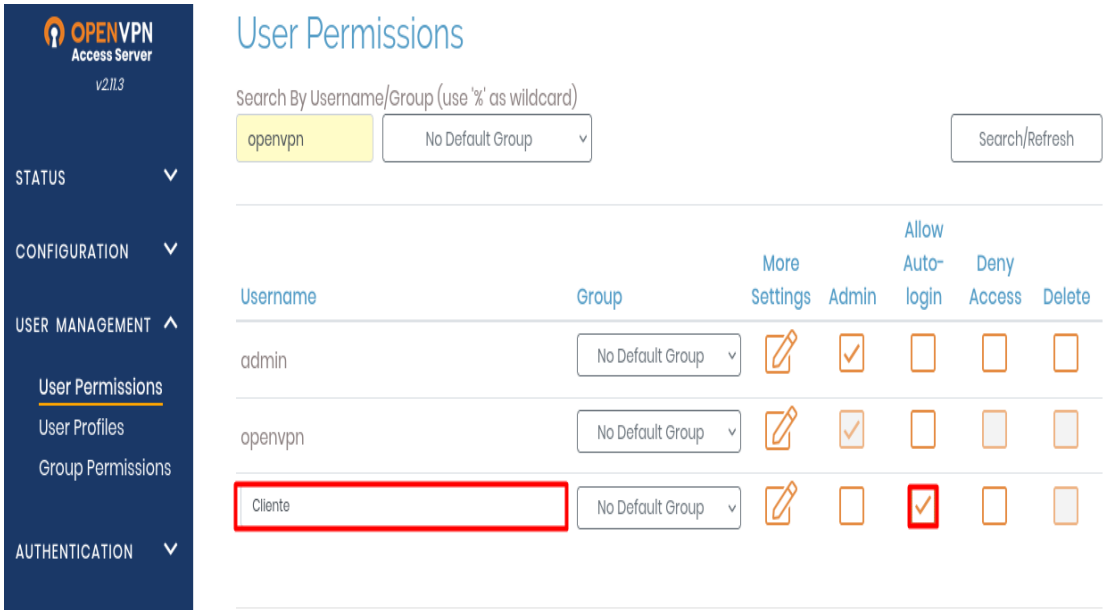

Figura 6.29: Creación del usuario cliente.

Para finalizar la creación de nuestro cliente tendremos que entrar en la pestaña de configuración de nuestro cliente (fig.6.30) y asignarle la contraseña que más nos guste.

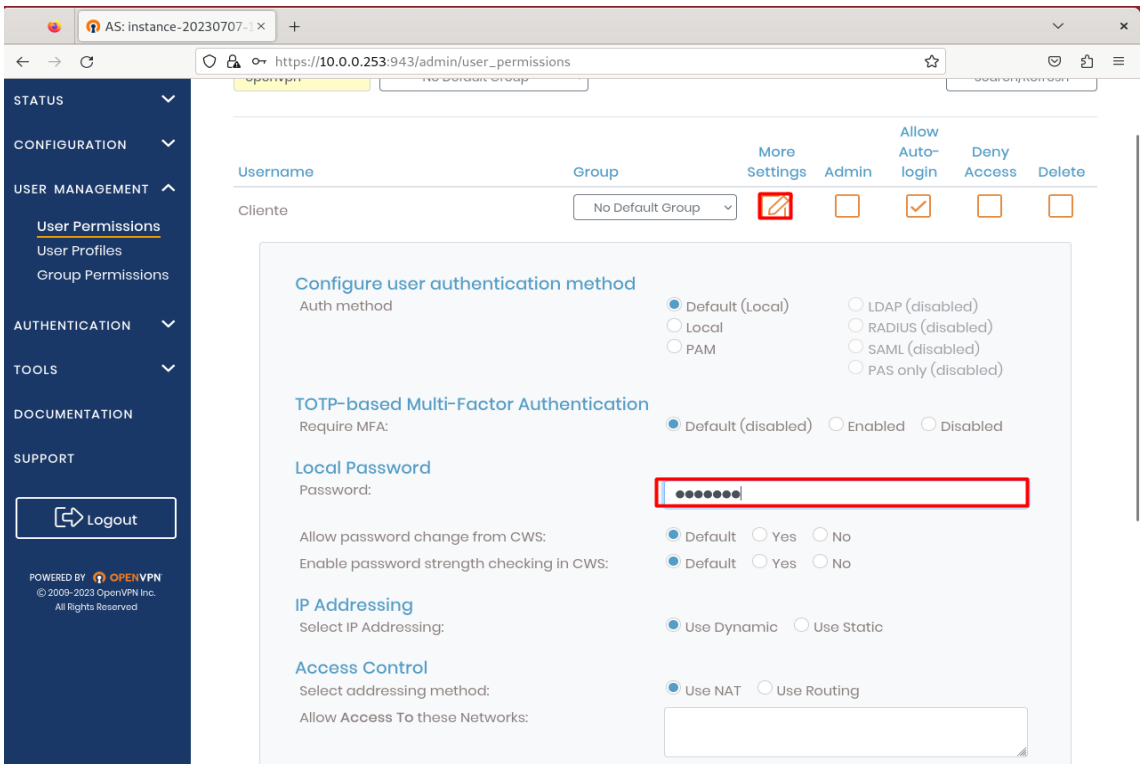

Figura 6.30: Configuración de la contraseña de nuestro cliente.

Llegados a este punto ya habremos configurado todo lo necesario para utilizar nuestro servidor externo como un servidor VPN.

6.3 Configuración de los clientes VPN

En esta sección se detallará la configuración de un cliente valido para cada una de las configuraciones anteriormente mencionadas.

En ambos casos mostraremos la configuración para un cliente con un sistema operativo Windows 10, ya que usaremos el mismo dispositivo como cliente en ambas configuraciones para facilitar las pruebas de rendimiento que realizaremos en siguientes apartados.

6.3.1. Maquina física windows.

Para configurar nuestro cliente será necesario entrar en la configuración de VPN dentro del apartado de red del *panel de control* de Windows y accederemos a la opción *agregar una conexión vpn* (fig.6.31).

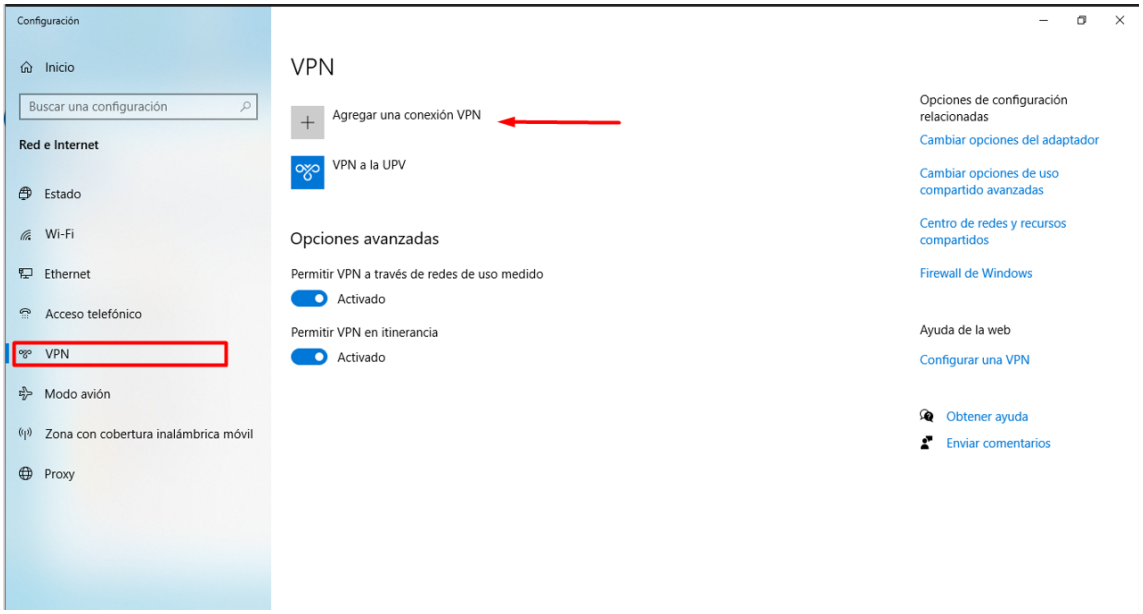

Figura 6.31: Opción *agregar una conexión vpn.*

Una vez ahí deberemos introducir los datos necesarios para establecer la conexión los cuales son los siguientes:

- Proveedor de VPN: "Windows (integrado)"
- Nombre de conexión: El nombre que más gustes para identificar la conexión
- Nombre de servidor o dirección: En este apartado tendremos que poner ip publica de nuestro dispositivo que funciona como servidor, en nuestro caso al estar conectado al mismo router que el cliente también valdría la ip privada.
- Tipo de VPN: .Automático"
- Tipo de información de inicio de sesión: "Nombre de usuario y contraseña"

- Nombre de usuario: En este apartado se deberá introducir el nombre de usuario de nuestro cliente anteriormente definido durante la configuración del servidor

- Contraseña: La contraseña del cliente definido con anterioridad.

En la figura 6.32 se muestra como ejemplo los valores empleados en nuestro caso:

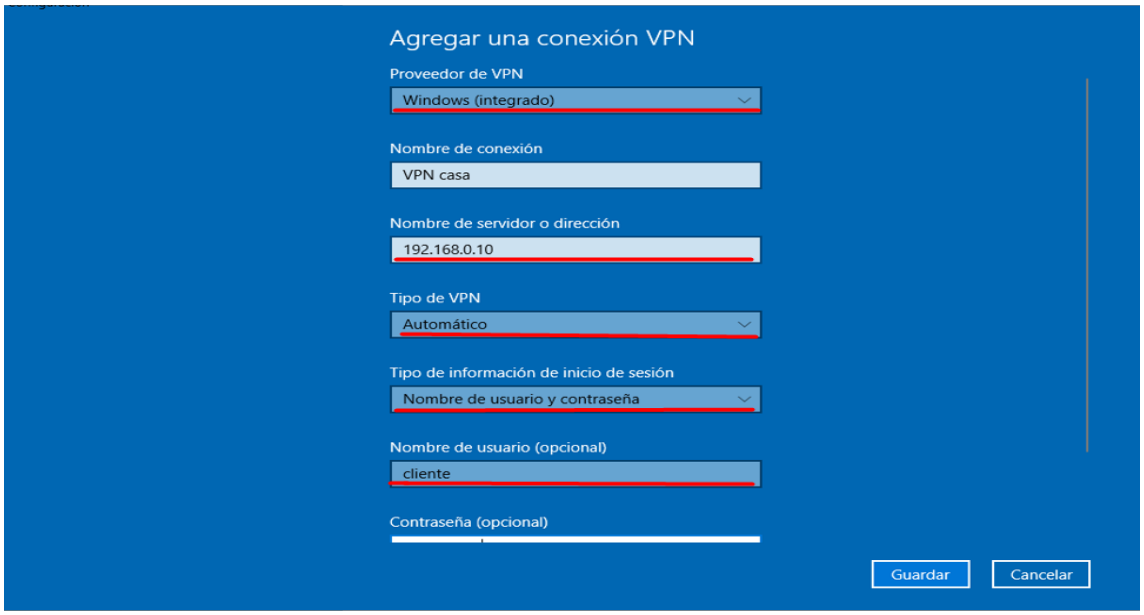

Figura 6.32: Menú *agregar una conexión vpn*.

Una vez agregada la conexión, solo hará faltar pulsar el botón de conectar para que esta sea efectiva.

6.3.2. Servidor externo ubuntu.

Para la configuración del cliente de nuestra solución basada en ubuntu será necesario acceder a la siguiente url: *https://laipdenuestroservidor*:943 (fig.6.33), en nuestro caso será la siguiente url: https://143.47.51.64:943. Una vez hayamos entrado en esta url nos pedirá las credenciales del cliente, las cuales fueron definidas por nosotros durante el proceso de instalación.

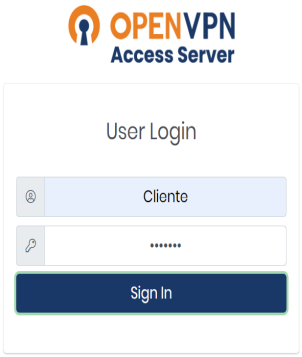

Figura 6.33: Acceso de cliente.

Y descargaremos e instalaremos el software controlador de nuestra VPN, tal como se muestra en las figuras 6.34, 6.35, 6.36 y 6.37.

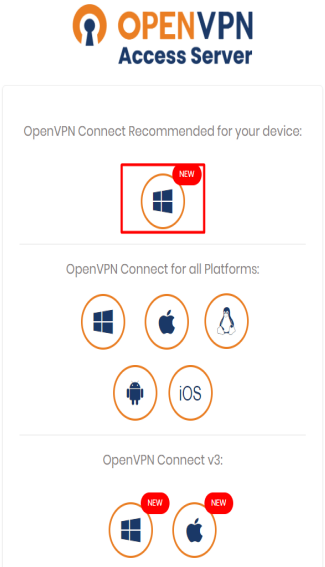

Figura 6.34: Instalación del software cliente I.

Figura 6.35: Instalación del software cliente II.

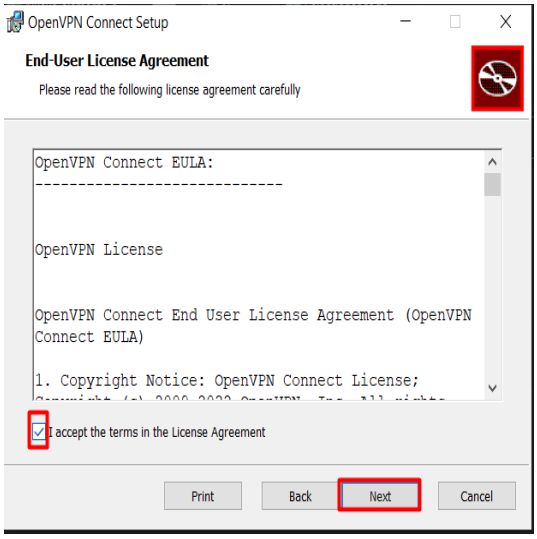

Figura 6.36: Instalación del software cliente III.

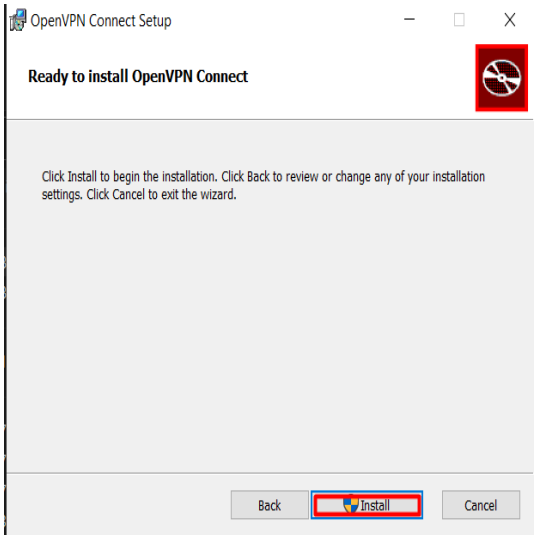

Figura 6.37: Instalación del software cliente IV.

Una vez instalado configuremos nuestro perfil introduciendo la url anteriormente accedida (fig 6.38).

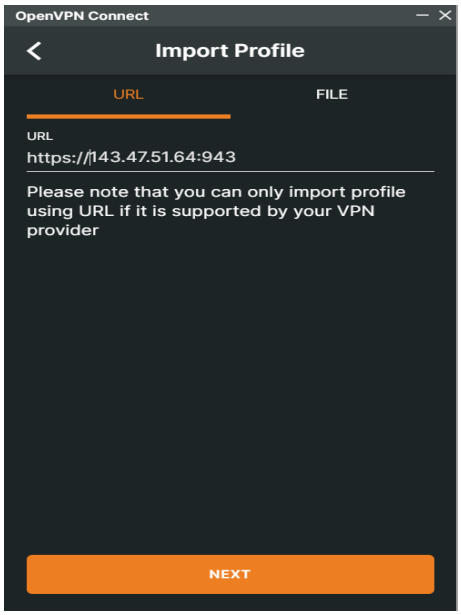

Figura 6.38: Introducción de url.

E introduciremos las credenciales de nuestro usuario cliente (fig 6.39).

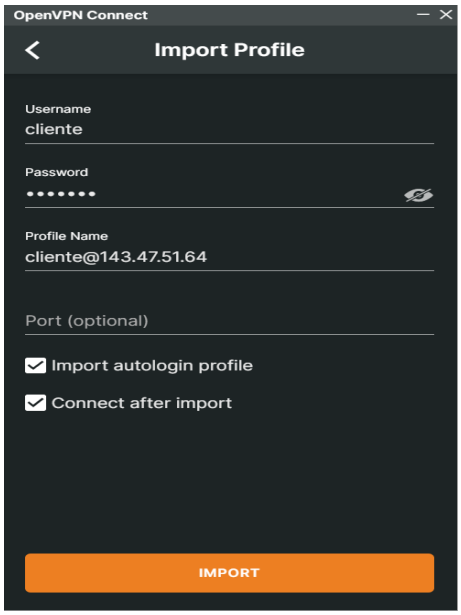

Figura 6.39: Introducción de credenciales de usuario.

Una vez realizado todos los pasos anteriores, nuestro cliente ya estará conectado a nuestro servidor VPN.

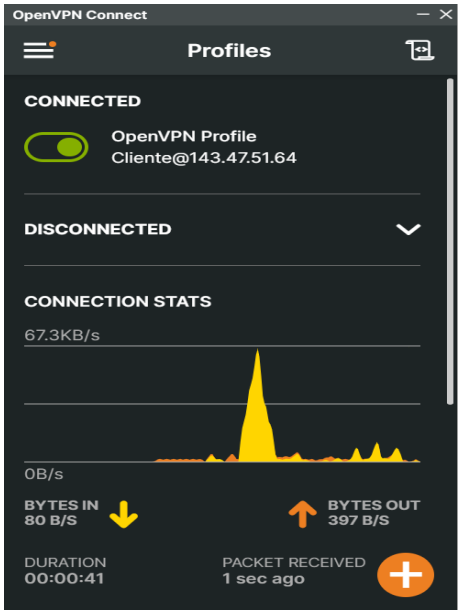

Figura 6.40: Conexión exitosa del cliente.

CAPÍTULO 7
Análisis de rendimiento

En este apartado estaremos realizando un análisis de rendimiento de nuestras dos soluciones, de un servicio VPN comercial y de mi ordenador personal sin estar conectado a una VPN. En este caso utilizaremos *Protonvpn* como VPN de pruebas ya que se trata de la VPN gratuita mejor calificada en el prestigioso portal *top10vpn*[7].

Figura 7.1: Logo de Protonvpn.

Para realizar este análisis de rendimiento utilizaremos varias metodologías: La primera de ellas será lanzar la orden **ping** desde el ordenador cliente hasta los servidores de Google y sacando el promedio del tiempo necesario para que se efectué correctamente. La siguiente prueba se trata del test de velocidad proporcionado por la empresa *Cloudfare*, este test consiste en varias pruebas exhaustivas que nos permitirán verificar la calidad de cada una de nuestras alternativas. La última prueba de rendimiento será realizada por la web: *https://www.speedtest.net/*, el cual fue catalogado por el prestigioso portal **CNET** como el mejor test velocidad en linea de 2023[15]. En nuestro caso utilizaremos la aplicación de escritorio que dispone *speedtest.net* para garantizar la mayor precisión.

Para las pruebas de rendimientos utilizaremos dos unidades: **milisegundos**, la cual nos será útil para la medición del tiempo necesario en efectuarse una orden ping, a la cual nos referiremos como **ms** y la unidad megabits por segundo, la cual representa la velocidad en la que se transfieren los datos y a la que nos referiremos como **Mbps**.

7.1 Pruebas sin conexión a una VPN

La primera conexión la cual le haremos pruebas de rendimiento será a nuestra red sin ningún tipo de conexión VPN.

```
C:\Users\halus>ping -t google.es

Haciendo ping a google.es [142.250.178.163] con 32 bytes de datos:
Respuesta desde 142.250.178.163: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=18ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=13ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=16ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=13ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=15ms TTL=119
Respuesta desde 142.250.178.163: bytes=32 tiempo=14ms TTL=119

Estadísticas de ping para 142.250.178.163:
    Paquetes: enviados = 10, recibidos = 10, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 13ms, Máximo = 18ms, Media = 14ms
```

Figura 7.2: Prueba de ping sin conexión a una vpn.

En nuestra primera prueba (fig.7.2) la cuál consistía realizar la orden ping a la dirección de *google.es* hemos obtenido que de media esta orden se realiza en unos 14 ms con un tiempo máximo y mínimo de 18 y 13 ms, respectivamente.

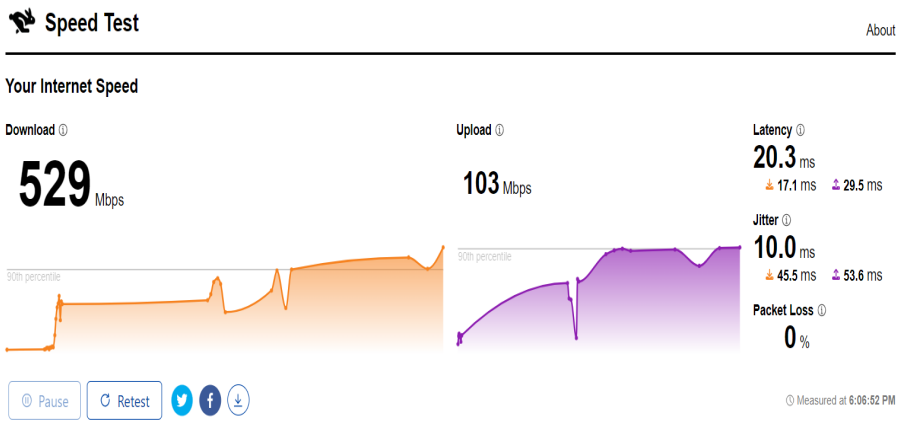

Figura 7.3: Test de Cloudfare sin conexión a una VPN.

En cuanto el test de rendimiento que nos ofrece la empresa *Cloudfare* (fig.7.3), este nos ha dado como resultado una velocidad media de descarga de 529 Mbps y una de subida de 103 Mbps.

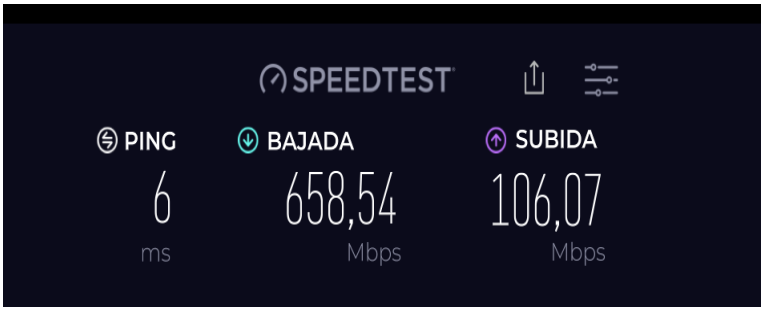

Figura 7.4: Test de Speedtest sin conexión a una VPN.

Por último,la prueba realiza mediante Speedtest(fig.7.4) tiene como resultado: 658.54 Mbps de bajada y 106.07 Mbps de subida.

7.2 Pruebas con conexión a una VPN comercial

En esta sección del proyecto se mostrarán las pruebas de rendimiento realizadas a nuestra conexión mediante el servicio de VPN comercial escogido.

```
C:\Users\halus>ping -t google.es

Haciendo ping a google.es [74.125.143.94] con 32 bytes de datos:
Respuesta desde 74.125.143.94: bytes=32 tiempo=47ms TTL=108
Respuesta desde 74.125.143.94: bytes=32 tiempo=47ms TTL=111
Respuesta desde 74.125.143.94: bytes=32 tiempo=48ms TTL=111
Respuesta desde 74.125.143.94: bytes=32 tiempo=48ms TTL=111
Respuesta desde 74.125.143.94: bytes=32 tiempo=47ms TTL=111
Respuesta desde 74.125.143.94: bytes=32 tiempo=47ms TTL=111
Respuesta desde 74.125.143.94: bytes=32 tiempo=47ms TTL=111
Respuesta desde 74.125.143.94: bytes=32 tiempo=47ms TTL=111
Respuesta desde 74.125.143.94: bytes=32 tiempo=48ms TTL=111
Respuesta desde 74.125.143.94: bytes=32 tiempo=46ms TTL=111

Estadísticas de ping para 74.125.143.94:
    Paquetes: enviados = 10, recibidos = 10, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 46ms, Máximo = 48ms, Media = 47ms
```

Figura 7.5: Prueba de ping mediante Protonvpn.

La prueba desarrollada mediante el uso de la orden ping (fig.7.5) ha dado como resultado un tiempo medio de 47 ms, durando cada llamada a la orden ping un intervalo de 46 y 48 ms.

Figura 7.6: Test de Cloudfare mediante Protonvpn.

Los resultados del test de Cloudfare (fig.7.6) serán los siguientes: 325 Mbps de descarga y 51 Mbps de subida.

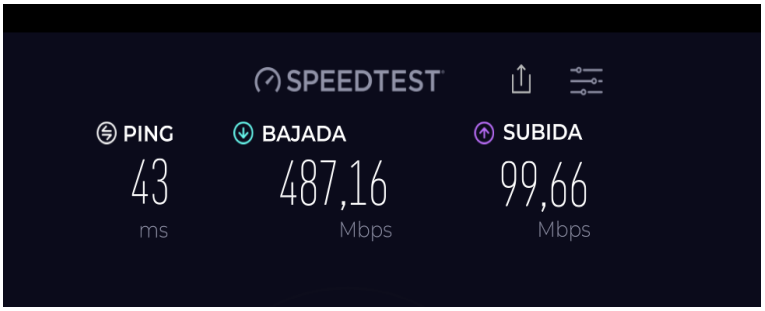

Figura 7.7: Test de Speedtest mediante Protonvpn

Finalmente, la prueba de rendimiento realizada por la aplicación de Speedtest (fig.7.7) nos ofrece como resultado 487.16 Mbps de velocidad de descarga y 99.6 Mbps de velocidad de subida.

7.3 Pruebas de la solución implementada en un dispositivo físico

En este apartado se mostrará las pruebas de rendimientos realizadas a nuestra solución implementada en una maquina física.

```
Haciendo ping a google.es [142.250.184.3] con 32 bytes de datos:
Respuesta desde 142.250.184.3: bytes=32 tiempo=15ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=15ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=16ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=25ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=15ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=18ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.184.3: bytes=32 tiempo=15ms TTL=119

Estadísticas de ping para 142.250.184.3:
    Paquetes: enviados = 10, recibidos = 10, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 14ms, Máximo = 25ms, Media = 16ms
```

Figura 7.8: Prueba de ping conectado a nuestro servidor VPN físico.

La prueba realizada mediante ordenes ping (fig.7.8) ha tenido como resultado un tiempo medio de 16 ms, estando cada una de ellas entre 14 y 25 ms.

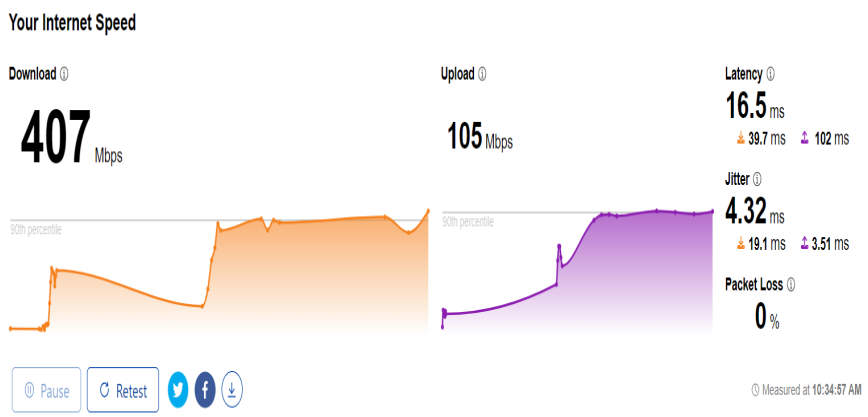

Figura 7.9: Test de Cloudfare mediante nuestro servidor VPN físico.

La segunda prueba realizada mediante la web de Cloudfare (fig.7.9) nos ha ofrecido un resultado de 407 Mbps de bajada y 105 Mbps.

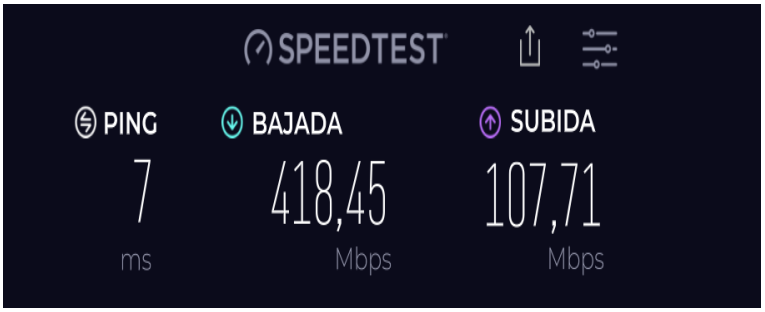

Figura 7.10: Test de Speedtest mediante nuestro servidor VPN físico.

Por último, la prueba realizada mediante la aplicación de Speedtest (fig.7.10) hemos recibido como resultado una velocidad de bajada de 418.45 Mbps y una de subida 107.71 Mbps.

7.4 Pruebas de la solución basada en un servidor de Oracle

En este apartado se mostrarán las pruebas de rendimiento hechas a nuestra implementación basada en un servidor Oracle.

```
C:\Users\halus>ping -t google.es

Haciendo ping a google.es [172.217.168.163] con 32 bytes de datos:
Respuesta desde 172.217.168.163: bytes=32 tiempo=17ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=17ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=14ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=15ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=15ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=17ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=16ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=15ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=17ms TTL=120
Respuesta desde 172.217.168.163: bytes=32 tiempo=16ms TTL=120

Estadísticas de ping para 172.217.168.163:
    Paquetes: enviados = 10, recibidos = 10, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 14ms, Máximo = 17ms, Media = 15ms
```

Figura 7.11: Prueba de ping conectado a nuestro servidor VPN externo.

La primera prueba de rendimiento basada en la utilización de ordenes ping (fig.7.11) ha tenido como tiempo de ejecución medio de 15 ms, estando cada una de en ellas en el intervalo de los 14 a 17 ms.

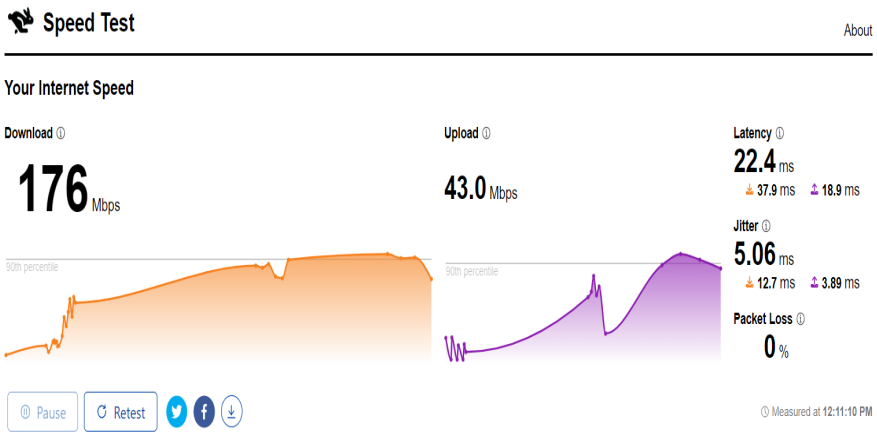

Figura 7.12: Test de Cloudfare mediante nuestro servidor VPN externo.

En cuanto a la prueba realizada por el portal web que nos ofrece Cloudfare (fig.7.12), el resultado recibido ha sido de 176 Mbps de descarga de media y 43 Mbps de subida de datos

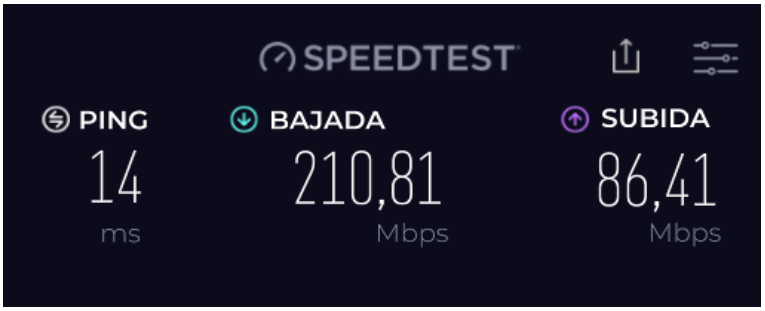

Figura 7.13: Test de Speedtest mediante nuestro servidor VPN externo.

Por último la prueba realizada mediante la aplicación de Speedtest (fig.7.13) nos ha dado como resultado 210 Mbps de bajada y 86.41 Mbps de subida.

7.5 Conclusiones del análisis de rendimiento

Para realizar la comparativa entre el rendimiento de las distintas soluciones hemos utilizado como base el escenario en el que nuestra conexión nuestra conectado a ninguna VPN, hemos comparado cada uno del resto de nuestros escenarios con este y sacado el porcentaje de decremento de rendimiento de cada uno de los escenarios restantes. En las tablas de cada uno de los escenarios se muestra este porcentaje de decremento de cada uno de los test realizados, diferenciando la velocidad de subida y bajada de los test de Cloudfare y Speedtest, y el porcentaje medio de empeoramiento de rendimiento.

El primer escenario a comentar se trata de el cual está conectado a una VPN comercial siendo estos los resultados (fig 7.14):

	TIEMPO IDEAL	TIEMPO SOLUCIÓN	% VARIACIÓN	% VARIACIÓN MEDIA:	38,2771022
PING	14	47	70,212766		
CLOUDFARE B	529	325	38,563327		
CLOUDFARE S	103	51	50,4854369		
SPEEDTEST B	658,54	487,16	26,0242354		
SPEEDTEST S	106,07	99,6	6,09974545		

Figura 7.14: Resultados test realizados a la VPN comercial.

De media la VPN comercial ha reducido de nuestra conexión un 38.3 por ciento, siendo en la prueba basada en ordenes ping en más de un 70 por ciento. Este aumento sin precedentes de tiempo de ejecución en la orden ping puede estar basado en que esta prueba se a realizado mediante una orden ping a la url: *google.es*, tratándose de una conexión a un servidor que se encuentra en España y teniendo en cuenta que el servidor VPN al que estamos alojados se encuentra en holanda, este retraso es en parte producto de la diferencia geográfica y no representa un problema de rendimiento en el acceso de servicios web que dispongas de servidores en zonas más cercanas a nuestro servidor VPN, aunque en cualquier caso siendo un usuario que reside en España puede causar problemas de

rendimiento, ya que será más común el acceso a sitios web con sede española y que solo tenga servidores dentro de la península. Algo más que cabe destacar es la variedad de resultados de los test de Cloudfare y Speedtest siendo el caso más destacable la velocidad de subida, siendo en el test de Cloudfare un 50.5 por ciento más lenta que el caso base y en el test de Speedtest solo un 6.1 por ciento más lenta, este suceso se puede deber a las metodologías empleadas, ya que es un suceso encontrado varias de nuestras pruebas realizadas, por lo tanto no le daremos demasiada importancia.

A continuación discutiremos los resultados de nuestra conexión VPN a nuestro servidor instalado en una maquina física (fig 7.15):

	TIEMPO IDEAL	TIEMPO SOLUCIÓN	% VARIACIÓN	% VARIACIÓN MEDIA:	13,7064815
PING	14	16	12,5		
CLOUDFARE B	529	407	23,0623819		
CLOUDFARE S	103	105	-1,9417476		
SPEEDTEST B	658,54	418,45	36,4579221		
SPEEDTEST S	106,07	107,71	-1,5461488		

Figura 7.15: Resultados test realizados a la VPN basado en un dispositivo físico.

Nuestro servidor VPN en una maquina física ha reducido el rendimiento de nuestra red un 13.7 por ciento de media, siendo el más pronunciado en la velocidad de bajada del test proporcionado por Speedtest con un 36.5 por ciento. Cabe destacar un dato que podría parecer erróneo pero tiene su debida explicación, este se trata de las velocidades de subida de ambos test. Estos han sido superiores que los del caso base, esto se puede explicar ya que el dispositivo físico que estoy utilizando como servidor VPN se encuentra conectado por Ethernet al mismo router que el ordenador cliente por lo tanto el servidor en esta materia no causa una deceleración y este ligero aumento de rendimiento se puede deber al estado de mi red en ese momento, ya que este es menor del 2 por ciento. Otra duda que nos surge con estos resultados es la siguiente: ¿Porque no se ha reducido el rendimiento de subida pero no el de bajada? Esto se debe a que nuestra velocidad de bajada es mucho superior a nuestra velocidad de subida. Esta velocidad está causando una sobrecarga en la tarjeta de red del dispositivo que aloja nuestro servidor VPN, ya que el ordenador que se está utilizando se trata de un modelo con una tarjeta de red pobre, pero esta limitación no debería existir con dispositivos con un tarjeta de red de mayor calidad.

Por último valoraremos el rendimiento de la última configuración, nuestro servidor VPN externo basado en Oracle (fig 7.16):

	TIEMPO IDEAL	TIEMPO SOLUCIÓN	% VARIACIÓN	% VARIACIÓN MEDIA:	43,6343959
PING	14	15	6,66666667		
CLOUDFARE B	529	176	66,7296786		
CLOUDFARE S	103	43	58,2524272		
SPEEDTEST B	658,54	210,81	67,9882771		
SPEEDTEST S	106,07	86,41	18,5349298		

Figura 7.16: Resultados test realizados a la VPN basado en un servidor externo.

Este ha sufrido la mayor perdida de rendimiento de todas la soluciones, un 43.6 por ciento de media, siendo de alrededor de un 67 por ciento de media cuando hablamos de velocidad de bajada. Por último comentar que estos resultados sufren de la misma anomalía que los relacionados con la VPN comercial, es decir, el porcentaje de decrecimiento de rendimiento de velocidad de subida del test de Cloudfare y Speedtest no son similares, pero este suceso ya ha sido discutido con anterioridad.

VPN COMERCIAL	VPN FÍSICA	VPN ORACLE
38,28%	13,71%	43,63%

Figura 7.17: Comparativa de todos los resultados.

En conclusión, la configuración que nos ha dado mejor rendimiento ha sido nuestro servidor físico. A pesar de este resultado, no podemos afirmar que este rendimiento se pueda garantizar en todas la situaciones ya que el buen o mal rendimiento de una red depende de muchos factores, como la localización tanto del servidor VPN como el servidor que accederemos mediante este, y al fin y al cabo estas pruebas no dejan de ser pruebas generalistas y en un entorno muy concreto, por ejemplo si no hubiese hecho estas pruebas en la misma casa, conectado al mismo router en el cual está conectado nuestro servidor basado en un dispositivo físico, las pruebas referentes a este hubiesen mostrado un decremento del rendimiento mayor, lo cual es algo que hay que tener en cuenta.

CAPÍTULO 8
Conclusiones

Este trabajo académico tenia como objetivo la indagación sobre la conveniencia de el uso de un servicio de VPN comercial y la existencia de alternativas asequibles para los usuarios convencionales.

Si hablamos de mera seguridad, podemos ratificar que sería conveniente que los usuarios clientes de este tipo de servicios se replantease el uso de estos mismos, ya que la seguridad que estos te ofrecen estos es debatible. La facilidad de configuración de nuestras alternativas sumado al rendimiento obtenido, el cual es similar al que te puede otorgar un servicio comercial, los convierte en serios competidores de los servicios comerciales equivalentes.

Este capítulo me gustaría concluirlo con una reflexión: Durante el uso de cualquier dispositivo conectado a internet, siempre sea está realizando un balance entre seguridad y comodidad, y es el propio usuario el que debe decidir la proporción que es más conveniente para este. Es cierto que las alternativas propuestas hacen más seguras tus conexiones a internet que un servicio comercial pero también es cierto que las soluciones comerciales requieren un tiempo de instalación de unos pocos minutos en cambio nuestras alternativas pueden llegar a ser horas, es cierto que nuestras soluciones no son las configuraciones más seguras para navegar por internet pero también es cierto que si aumentásemos la complejidad de estas soluciones se convertirían impracticables para la mayoría de usuarios. Por ello los usuarios, en mi humilde opinión, deberían replantearse si es necesario en su situación actual la utilización de medidas de seguridad adicionales a las que lleva integrado un sistema operativo moderno.

Bibliografía

[1] Ferguson, P., and Huston, G. What is a VPN?. *Technology and Culture*,(1998): 01-22.

[2] Security.org. (2023, 18 agosto),3rd Annual VPN Market Report: 2022. Consultado en https://www.security.org/resources/vpn-consumer-report-annual/.

[3] Josh, and Summers, J. (2022). Your VPN is lying about its "Zero-Log VPN" (here's the proof). All Things Secured. Consultado en https://www.allthingssecured.com/vpn/truth-about-vpn-logging-policies/.

[4] JCarrillo, F. (2023, 21 febrero). Router VPN: qué es y cómo configurar. Roams. Consultado en https://roams.es/companias-telefonicas/blog/internet/router-vpn/.

[5] Hamilton, I. A. (2020, 13 diciembre). You should never use a free VPN. Here's why. Business Insider. Consultado en https://www.businessinsider.com/explainer-here-is-why-you-should-never-use-free-vpn-2020-12?IR=T.

[6] Wakabayashi, D., Che, C., and Fu, C. (2022, 18 octubre). In Xi's China, the business of business is State-Controlled. The New York Times. Consultado en https://www.nytimes.com/2022/10/17/business/china-xi-jinping-business-economy.html.

[7] Migliano, S. (2023b, agosto 7). Best Free VPNs of 2023 | Fast, Private, safe and 100 percent Free. Consultado en https://www.top10vpn.com/best-vpn/free/.

[8] VPNRanks. (s. f.). Revelaciones de registros VPN - ¡Solo 3 de cada 101 proveedores están SEGUROS! VPNRanks. Consultado en https://www.vpnranks.com/es-es/recursos/vpn-logging-policies/.

[9] Ashford, W. (2019, 3 julio). Top VPNs secretly owned by Chinese firms. ComputerWeekly.com. Consultado en https://www.computerweekly.com/news/252466203/Top-VPNs-secretly-owned-by-Chinese-firms?amp=1.

[10] Markuson, D., and Markuson, D. (2023). How to use a VPN for China? Is it legal? | NordVPN. NordVPN. Consultado en https://nordvpn.com/es/blog/vpn-for-china/.

[11] Virtual Private Network Market Size, Share and Trends Analysis Report by component, by type (Site-To-Site, Remote Access, Extranet), by deployment mode, by end use, by region, and segment Forecast, 2020 - 2027. (s. f.). Consultado en https://www.grandviewresearch.com/industry-analysis/virtual-private-network-market.

[12] Taylor, S. (2021). Kape Technologies (Formerly CrossRider) now owns ExpressVPN, CyberGhost, Private Internet Access, Zenmate, and a collection of VPN "Review" websites. RestorePrivacy. Consultado en https://restoreprivacy.com/kape-technologies-owns-expressvpn-cyberghost-pia-zenmate-vpn-review-sites/.

[13] Sole, R. (2022, 27 septiembre). Ahorra en tu factura de la luz gracias a la Raspberry Pi y su bajísimo consumo. HardZone. Consultado en https://hardzone.es/noticias/componentes/consumo-raspberry-pi/.

[14] Moreno, S. (2023, 14 junio). ¿Cuánto consumo el ordenador? Sal de dudas. Gana Energía. Consultado en https://ganaenergia.com/blog/cuanto-consume-un-ordenador/.

[15] Bolden, K., and Crist, R. (2023, 12 agosto). Best Internet speed tests for 2023. CNET. . Consultado en https://www.cnet.com/home/internet/best-speed-tests/.

[16] Sánchez, L. O., and Sánchez, L. O. (2023). La historia de la ciberseguridad | NordVPN. NordVPN. Consultado en https://nordvpn.com/es/blog/historia-ciberseguridad/.

[17] Gillis, A. S. (2021). Red privada virtual o VPN. ComputerWeekly.es. Consultado en https://www.computerweekly.com/es/definicion/Red-privada-virtual-o-VPN.

[18] Khan, M. T., DeBlasio, J., Voelker, G. M., Snoeren, A. C., Kanich, C., and Vallina-Rodriguez, N. (2018, October). An empirical analysis of the commercial vpn ecosystem. In Proceedings of the Internet Measurement Conference 2018 (pp. 443-456).

[19] Santoso, B., Sani, A., Husain, T., and Hendri, N. (2021). VPN Site To Site Implementation Using Protocol L2TP And IPSec. TEKNOKOM, 4(1), 30-36.

[20] Srivatsan, S., Johnson, M. L., and Bellovin, S. M. (2010). Simple-vpn: Simple ipsec configuration.

[21] Huc, M. (2023). How to set up VPN server on Windows 10. Pureinfotech • Windows 10 and Windows 11 Help for Humans. Consultado en https://pureinfotech.com/setup-vpn-server-windows-10/.

[22] Camisso, J. (2020b). How To Set Up and Configure an OpenVPN Server on Ubuntu 20.04. DigitalOcean. Consultado en https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-ubuntu-20-04.

ANEXO

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				X
ODS 2. **Hambre cero.**				X
ODS 3. **Salud y bienestar.**				X
ODS 4. **Educación de calidad.**				X
ODS 5. **Igualdad de género.**				X
ODS 6. **Agua limpia y saneamiento.**				X
ODS 7. **Energía asequible y no contaminante.**		X		
ODS 8. **Trabajo decente y crecimiento económico.** a				X
ODS 9. **Industria, innovación e infraestructuras.**			X	
ODS 10. **Reducción de las desigualdades**.				X
ODS 11. **Ciudades y comunidades sostenibles**.				X
ODS 12. **Producción y consumo responsables.**		X		
ODS 13. **Acción por el clima.**				X
ODS 14. **Vida submarina.**				X
ODS 15. **Vida de ecosistemas terrestres.**				X
ODS 16. **Paz, justicia e instituciones sólidas.**			X	
ODS 17. **Alianzas para lograr objetivos.**				X

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

Este trabajo tiene una relación casi nula con los objetivos y metas de desarrollo sostenible (ODS) de la AG-ONU (Asamblea General de las Naciones Unidas), ya que por la naturaleza de nuestro trabajo este no cubre ninguna de las áreas a las que hace mención cada una de los ODS, con excepción del ODS 9 (Industria, innovación e infraestructuras) y el ODS 16 (Paz, justicia e instituciones sólidas) que se podría a llegar a entender que existe una pequeña relación entre nuestro proyecto y ambos objetivos.

En cuanto a los objetivos de fin de la pobreza (ODS 1), hambre cero (ODS 2), salud y bienestar (ODS 3), educación de calidad (ODS 4), igualdad de género (ODS 5), trabajo decente y crecimiento económico (ODS 8) y reducción de las desigualdades (ODS 10), es evidente que no existe ningún tipo de relación con nuestro trabajo ya que este no trata ni soluciona de ninguna forma ninguno de estos problemas globales que plantean estos ODS.

Hablando de los ODS relacionados con la acción climática y el mantenimiento del medio ambiente como son los ODS de agua limpia y saneamiento (ODS 6), ciudades y comunidades sostenibles (ODS 11), acción por el clima (ODS 13), vida submarina (ODS 14) y vida de ecosistemas terrestres (ODS 15), tampoco existe una relación notoria con el trabajo realizado ya que no son temas tratados de ningún modo. Los únicos objetivos relacionados con la acción climática y el mantenimiento del medio el cual podemos encontrar relación sería el ODS número 7 (energía asequible y no contaminante) y el número 12 (producción y consumo responsables), los cuales trataremos con profundidad más adelante.

En cuanto al objetivo 17 (alianzas para lograr objetivos), el cual habla formar alianzas entre gobiernos, sector privado y sociedad civil consideró que no se puede encontrar ningún tipo de relación con mi trabajo.

Los únicos objetivos los cuales podrían a llegar a tener una relación clara con nuestro proyecto son energía asequible y no contaminante (ODS 7), industria, innovación e infraestructuras (ODS 9), producción y consumo responsables (ODS 12) y paz, justicia e instituciones sólidas (ODS 16).

Tanto el ODS 7 como el ODS 12 se relacionan de forma parcial con nuestro trabajo ya que este proporciona soluciones las cuales están comprometidas con la necesidad de otorgar alternativas al usuario con el menor consumo de energía posible y buscando el aprovechamiento de los recursos disponibles por el usuario garantizando el consumo responsable, un ejemplo de esto sería que nuestra solución basada en un dispositivo físico permite la reutilización de dispositivos pertenecientes al usuario para la creación

de un servidor VPN como es el caso de nuestra implementación la cual está realizada en nuestro ordenador personal. La otra solución propuesta garantiza el menor consumo de energía posible ya que está basada en un servidor externo obteniendo una optimización de la energía superior a las implementaciones basadas en la creación de una infraestructura propia al compartir esta infraestructura con una variedad importante de usuarios. Por último, este proyecto también discute la necesidad de utilización de conexiones VPN según las necesidades del usuario, instando a un consumo responsable por parte de este.

El objetivo número 9 se relaciona con nuestro trabajo ya que este busca la construcción de infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación, lo cual casa perfectamente con el contenido del trabajo ya que este en el contexto de la privacidad en línea explora diferentes alternativas ante el uso de los servicios VPN comerciales las cuales pueden llegar a ser mas seguras que estos, permitiendo a los usuarios que construyan infraestructuras más resilientes y sostenibles para proteger su privacidad en línea.

El objetivo número 16 trata de promover sociedades pacíficas e inclusivas para desarrollo sostenible, proporcionando justicia para todos. Este objetivo tiene cierta relación con el proyecto ya que este explora la importancia de la privacidad y la seguridad en línea para la protección de los derechos humanos y dando alternativas a los servicios comerciales de VPN que garantizan que estos derechos sean respetados.

En conclusión, la mayoría de los objetivos propuestos por la AG-ONU tienen una relación casi nula con este proyecto, con excepción de los objetivos 9 y 16 los cuales podrían tener relación con nuestro trabajo y los objetivos 7 y 12, los cuales si tienen una relación parcial con este.