FACULTAD DE INGENIERÍA

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

MENCIÓN REDES DE COMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES

Título: **ESTUDIO PARA LA IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL(VPN) UTILIZANDO HERRAMIENTAS DE SOFTWARE LIBRE. Caso de estudio "COMISION FULBRIGHT DEL ECUADOR"**

AUTOR: LUIS MARCELO QUISHPE IZA

DIRECTOR: GUILLERMO ALFONSO GALLEGOS ARIAS

QUITO, 2021 – MARZO

DEDICATORIA

Quiero dedicar este trabajo a mi familia, mi amada esposa Mirian por toda su ayuda y con quien he pasado un sin número de momentos y varias etapas de mi vida durante 24 años, a mis hijos Cristian y Valeria quienes son los que me dan la fuerza para levantarme cada día y son quienes han llenado toda mi vida de alegrías.

AGRADECIMIENTO

Agradezco a Dios, quien nos permite ser seres inteligentes que aprenden día con día y pueden elegir el camino a su futuro y mientras él me lo permita, seguiré intentando mejorar tanto como ser humano, así como profesional.

Agradezco también a mi madre quien no pudo ayudarme con mis primeros deberes cuando era niño y no porque no quería, sino porque sus conocimientos no le permitieron, con quien llore muchas noches por no poder terminar dichos deberes, pero me enseñó a ser una persona responsable, amable, luchadora y nunca decir no puedo, en otras palabras, me enseñó a ser una persona de bien.

A mi padre y mis hermanos que de una u otra forma hicieron de mí la persona que hoy en día soy.

INTRODUCCIÓN

Con el acelerado avance de la tecnología, la necesidad de reducir costos en: infraestructura, oficinas, recursos, tiempo las empresas en el mundo se han visto en la necesidad de contratar personal que realicen sus labores de forma remota, llamado comúnmente como teletrabajo mediante el cual un empleado puede acceder a sistemas, aplicaciones y recursos de una empresa sin necesidad de estar físicamente en las instalaciones de dicha empresa, dicha capacidad no puede brindar un servicio de red privada virtual(VPN) que no es más que crear una red dentro de otra utilizando para esto un túnel de comunicación creado por medio del servicio de internet, un servicio VPN debe contar además con los protocolos y métodos de encriptación necesarios para establecer una conexión segura, evitando que la información que viaje por dicho túnel pueda ser visibles por terceras personas.

La COMISION FULBRIGHT DEL ECUADOR como la mayoría de empresas del país no tenía contemplado el que sus empleados realicen teletrabajo, razón por lo cual todos sus sistemas y recursos funcionan de manera local, esto dio paso a la necesidad de requerir una solución de manera urgente el momento en que fue declarado por el gobierno nacional un estado emergencia y con esto la decisión de que las personas no puedan salir de sus hogares siendo la mejor opción el realizar un estudio para la implementación de una red privada virtual intentando en lo posible el evitar incurrir en gastos mayores, con lo cual se debía optar por soluciones de software libre.

JUSTIFICACIÓN

En la actualidad se hace necesario que los empleados puedan laborar de forma remota y tengan acceso a los servicios, equipos e información de una empresa de la manera más sencilla y con la seguridad necesaria, esto permitirá a los empleados ser más productivos, impidiendo que se vean limitados el momento de realizar sus labores al encontrarse por diferentes razones fuera de las oficinas de la empresa.

El avance de la tecnología puede conllevar a estar desactualizados, siendo siempre necesario revisar la mayor documentación posible en cuanto a nuevas tecnologías y estándares de seguridad para que la red privada virtual que se implemente permita a la institución y sus empleados disponer de las herramientas y servicios para el trabajo remoto con una tecnología actual y con la seguridad más adecuada.

Es importante tener la información de las condiciones actuales como son el número de usuarios que van a utilizar el servicio, la estructura de la red y los equipos que la empresa dispone para la implementación, esto permitirá implementar una red privada virtual que cubra los requerimientos, se utilice los recursos existentes de la empresa y que los usuarios tengan el acceso remoto a los servicios, equipos e información que dispone la empresa.

El realizar el diseño permitirá indicar la tecnología a utilizar, el número de usuarios, características del equipo servidor, los enlaces existentes, el tipo de seguridad, el software y los paquetes necesarios para realizar la implementación de la red privada virtual, con lo cual los usuarios podrán hacer uso de los servicios de la empresa de manera remota con las tecnologías y herramientas más actuales.

El implementar una red privada virtual permitirá a los empleados tener acceso remoto a los servicios que normalmente solo se puede utilizar desde el interior de la empresa, esto les llevaría a ser más productivos, impidiendo que se vean limitados el momento de realizar sus labores fuera de las instalaciones de la empresa.

El evaluar calidad del servicio y realizar las pruebas de funcionamiento permite verificar que la red privada virtual implementada cubra los requerimientos y brinde el servicio de forma eficiente dentro de los parámetros de calidad debidos, lo cual permitirá a los usuarios utilizar

los servicios y equipos de la red local de manera remota dentro de los parámetros de calidad de servicio adecuados.

PLANTEAMIENTO DEL PROBLEMA

La Comisión Fulbright del Ecuador no cuenta una red privada virtual implementada, impidiendo a los empleados tener acceso a los servicios y los equipos de la red local de la empresa de manera remota con herramientas tecnológicas actuales, que realice cifrado, autenticación y con la seguridad de que la información de la empresa no se encontrará en riesgo, tomando en cuenta que la información que viajara por esta red es privada y confidencial que de caer en las manos equivocadas podría resultar perjudicial para la empresa, considerando además que en ocasiones los empleados necesitarán conectarse desde servicios de internet públicos y sin protección.

Los empleados de las áreas de contabilidad y académica no pueden utilizar el sistema de facturación y el sistema académico que se encuentran instalados y funcionando en servidores locales de la empresa, lo que implica que los empleados no puedan realizar el registro de notas, matriculas, inscripciones y facturación mientras no asistan a sus puestos de trabajo físicamente, haciendo imposible que la empresa pueda cumplir con los servicios que brinda en el área académica que es parte de su razón de existir.

El personal del resto de áreas no puede realizar teletrabajo debido a la falta de una herramienta para poder acceder a la información confidencial y necesaria para el correcto desenvolvimiento de sus labores diarias de manera remota, lo que impide que los empleados puedan optar a la modalidad de trabajo aceptada por el ministerio de trabajo, debido al inconveniente producido por la pandemia que afecta al país.

ANTECEDENTES

La Comisión Fulbright del Ecuador es una organización sin fines de lucro que brinda varios servicios a personas del Ecuador en el ámbito educativo a continuación se detalla el trabajo que realizan.

> La Comisión Fulbright de Ecuador fue establecida en 1956 mediante decreto ejecutivo entre los gobiernos de Estados Unidos y Ecuador para facilitar la administración del programa educativo. La Comisión binacional tiene un directorio comprendido de ocho miembros, cuatro estadounidenses y cuatro ecuatorianos, quienes asumen la responsabilidad de supervisar los objetivos a largo plazo del Programa Fulbright. Aproximadamente 1.900 ciudadanos ecuatorianos y 845 ciudadanos estadounidenses han sido seleccionados como Fulbrighters desde 1956 a través del programa en Ecuador.
>
> Adicionalmente, la Comisión Fulbright ofrece Asesoría Académica y mantiene dos pequeñas, pero completas, bibliotecas en Quito y Guayaquil donde los estudiantes pueden buscar los programas académicos que mejor calzan con sus necesidades. Además, los interesados pueden recibir información o asesoría sobre la documentación necesaria para admisiones en universidades americanas y los exámenes estandarizados pertinentes. (Fulbright,2019)

Finalmente, "la Comisión tiene un Programa de Enseñanza de Inglés para adultos. El programa completo comprende ocho niveles con ochenta horas de clase por nivel. Los cursos se ofrecen cada trimestre en Quito únicamente" (Fulbright, 2019).

La Comisión Fulbright del Ecuador debido a la emergencia que presenta el país por la pandemia existente se ha vista en la necesidad de que sus empleados puedan acceder de forma remota a los servicios informáticos con los que cuenta la empresa y de esta forma puedan realizar teletrabajo de acuerdo a lo dispuesto por el ministerio de trabajo del Ecuador.

De acuerdo a lo que se informa en la página web del Ministerio de trabajo del Ecuador:

El teletrabajo es una iniciativa que rompe esquemas, con esto se evalúa el trabajo de acuerdo a los resultados y no por el horario, En un estudio del Ministerio del Trabajo se señala que 15.200 personas a nivel nacional teletrabajan en la empresa privada, siendo el objetivo que en dos años sean unas 76.000 personas las que realicen teletrabajo. (*Ministerio de Trabajo del Ecuador*, 2020)

Se debe añadir además que:

"El trabajo remoto es un tipo de proceso de trabajo para mantener a los trabajadores realizando sus actividades laborales a distancia o fuera del entorno de trabajo" (Mohamed et al., 2019), sin olvidar que existen diferentes tipos de trabajo remoto según los trabajadores que lo utilizan," el lugar, tipo de trabajo, el medio ambiente y el propósito del uso"(Mohamed et al., 2019).

En el mundo existen muchas empresas que han optado por el teletrabajo en gran parte de su planta laboral como es el caso de Cisco Systems y que de acuerdo a lo indicado por:

> Francois Leens representante de Cisco Systems en Ecuador, compartió la experiencia de esta compañía que a escala mundial cuenta con 70 mil empleados en 160 países bajo esta modalidad, y en el país suman 17, precisó que para el funcionamiento de esta normativa es necesario otorgar las herramientas a los empleados y entrenarles en el uso de la tecnología. El Teletrabajo permite dar equilibrio entre la vida personal y laboral. (*Ministerio de Trabajo del Ecuador*, 2020)

Casi todos se conectan a una red e internet es la red informática más grande que existe en este mundo, el Internet abarca muchas redes, pero son redes conectadas entre sí. Una de las soluciones para este problema es una red privada virtual (VPN), una VPN es un dispositivo de red o serie de dispositivos utilizados para interconectar varias redes juntas. (Nawej y Du, 2019)

La evolución del comercio electrónico mundial aumenta la demanda de comunicación confiable. Para una comunicación segura, la mayoría de las organizaciones usan el método tradicional de línea dedicada para conectarse usuarios remotos u oficinas. Pero el principal problema con la línea privada dedicada es que no es barato el planificar e implementar, además que toma bastante tiempo para instalar y activar, actualmente las organizaciones quieren usar las técnicas de comunicación que son relativamente baratos y más confiables. Estos aspectos introducen comunicación alternativa segura y privada con mecanismos como la red privada virtual (VPN). (Jahan et al., 2017)

"Las tecnologías VPN juegan un papel vital en diversas comunicaciones, entornos como empresas, organizaciones militares, institutos educativos e incluso individuos"(Jahan et al., 2017), "siendo por tanto necesario investigar y comparar varias soluciones VPN, su rendimiento en hardware con múltiples plataformas que van desde recursos muy limitados a muy poderosos. Aspectos no funcionales, relacionados alrededor seguridad, capacidad de manejo y facilidad de

uso, deben tomarse en cuenta para evaluar su idoneidad para futuros casos de uso" (Lackorzynski et al., 2019).

De acuerdo a lo indicado es importante realizar un estudio completo de las tecnologías VPN de software libre que se encuentran en el mercado, además se debe realizar la selección de la opción de la tecnología que mejor cumpla los requerimientos, recursos existentes y el crecimiento de la empresa, así como será necesario realizar la implementación y pruebas de funcionamiento, para poder dar acceso de manera remota a los empleados tanto a los equipos como a los servicios de los que se dispone localmente la empresa con la seguridad necesaria para evitar perdida de información o que personas no autorizadas puedan hacer uso del acceso remoto, como lo menciona la diferentes investigaciones indicadas anteriormente.

OBJETIVOS

OBJETIVO GENERAL

Realizar el estudio para la implementación de una Red Privada Virtual(VPN) utilizando herramientas de software libre en la Comisión Fulbright del Ecuador para permitir el acceso remoto a los servicios de la empresa.

OBJETIVOS ESPECÍFICOS

- Realizar el estudio de las diferentes tecnologías de acceso remoto en software libre para realizar el diseño e implementación de la red privada virtual más adecuado a las necesidades de la empresa recopilando información actual y de las principales bases científicas.
- Establecer los requerimientos y recursos de los que dispone la empresa, analizando las condiciones actuales, el número de usuarios, la estructura de la red, las características de los equipos con lo cual la red privada virtual funcionará dentro de los parámetros

adecuados permitiendo a los usuarios el acceso remoto a los servicios de los que dispone la empresa.

- Diseñar la red privada virtual utilizando el resultado del análisis de las tecnologías, los estándares de seguridad, recursos de la empresa en cuanto a infraestructura tecnológica, así como los requerimientos, con lo cual los usuarios podrán hacer uso de los servicios de la empresa de manera remota con las tecnologías y herramientas más actuales.
- Realizar la implementación de red privada virtual con software libre utilizando el estudio y análisis de requerimientos permitiendo a los empleados tener acceso a los servicios y los equipos de la red local de la empresa de manera remota con herramientas tecnológicas actuales y con la seguridad debida.
- Evaluar el funcionamiento de la red implementada por medio de pruebas de conectividad, encriptación y validando que los valores de latencia, tráfico, la perdida de paquetes estén dentro de valores aceptables lo cual permitirá a los usuarios utilizar los servicios y equipos de la red local de manera remota dentro de los parámetros de calidad de servicio adecuados.

CONTENIDO

INDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este trabajo de titulación realiza el estudio y la implementación de una solución de red privada virtual (VPN), utilizando para esto herramientas de software libre, logrando con esto que los empleados de la institución COMISION FULBRIGTH DEL ECUADOR puedan realizar sus labores de forma no presencial dado el hecho que se ha producido en el país debido a la pandemia de COVID que ha impedido que dichos funcionarios puedan acceder a las instalaciones.

En primera instancia se realizará un análisis del estado actual de la institución, las características de computadores y servidores, el estado y características de la red local, así como el servicio de internet con el que se dispone, es necesario de igual manera establecer el número de empleados que laboran.

Como segunda etapa se diseñará la red privada virtual, tomando en cuenta el análisis de la primera etapa, así como los requisitos a cubrirse por el servicio, teniendo en cuenta que se debe utilizar herramientas de software libre, se debe definir el equipo a utilizarse, el sistema operativo que debe instalarse, los servicios que deberá tener el servidor, la aplicación VPN seleccionada y que será configurada, de igual manera se debe definir los usuarios que harán uso del servicio.

Como tercera etapa se implementará la red privada virtual conforme al diseño realizado, se procederá con la instalación del sistema operativo, la configuración e instalación de los servicios adicionales, así como la instalación y configuración del servicio VPN.

Finalmente, se realizará la configuración de los clientes y pruebas necesarias, para confirmar la estabilidad de la red, se realizará pruebas de acceso remoto a través de la VPN, demostrando de esta forma que los funcionarios pueden laborar de manera normal desde fuera de las instalaciones de la institución.

1. FUNDAMENTOS TEÓRICOS.

1.1. Tecnologías de acceso remoto.

El realizar una conexión a una red desde un sitio distante se lo conoce como acceso remoto, esto ha sido algo muy importante en el mundo de las redes, ya que existen empresas que promueven viajes con objetivo trabajo de sus empleados o permiten que sus empleados realicen trabajo desde el hogar o desde sucursales remotas, dado que en estos casos los empleados necesitan tener acceso a la red privada de la empresa para realizar consulta de ciertos archivos o requieren utilizar los diferentes servicios tecnológicos con los que cuenta en la oficina, la necesidad del acceso remoto ha sido la causa principal del auge de las redes privadas virtuales o más conocidas como VPN. (Díaz y Vieyra, 2015)

Antes de que las VPN sean utilizadas como una opción para poder realizar el acceso remoto, una empresa debía instalar módems para que el usuario remoto pueda hacer una llamada y de esta manera realizar la conexión con la red de tipo corporativa. En el caso de organizaciones que requerían conectar muchos usuarios de forma remotos, terminaban viéndose en la necesidad de instalar muchos módems y así formaban bancos o pilas de módems, el acceso remoto de este tipo resultaba caro, además que se requería que la empresa cuente con mayor soporte sobre la tecnología, de igual manera resultaba caro si los usuarios se encontraban bastante alejados de la empresa, debiendo realizar en ocasiones llamadas de larga distancia, tomándose en cuenta además del largo tiempo que un tele-trabajador debía permanecer conectado. (Fonseca,Castañeda y Arévalo, 2018)

1.2. Red privada virtual

Las redes privadas virtuales en realidad son redes que se forman sobre una red pública compartida, logrando con esto simular una red privada, las redes VPN normalmente tienen como propietario a una empresa que permite el acceso seguro a diferentes sedes interconectados, utilizando para esto la red de un proveedor de servicios, para este caso un proveedor de internet. (Zapata, 2016)

En si la red VPN es una red de tipo pública funcionando en un entorno privado y confidencial que permite que el usuario trabaje en un sitio distante como si estuviera en una red local, se podría ver como una desventaja de este tipo de red que se depende de un ancho de banda, esto implica que cuando más usuarios se encuentren conectados al servicio, se reducirá el ancho de banda del que cada usuario pueda hacer uso. (Zapata, 2016)

1.3. Método de operación de una VPN

Una VPN proporciona a los usuarios con los permisos debidos comunicarse mediante un túnel "virtual" de Internet y además le permite contar con la seguridad que únicamente se da en las redes privadas. Para usar Internet para una VPN, es necesario saber que el principal problema que se puede presentar es que los paquetes con la información privada de la empresa viajan por Internet y esa información puede ser vista o robada por terceras personas, pero hay una solución que es el tunneling, esto no es más que los paquetes se envían son encriptados primeramente y luego se encapsulan en paquetes IP y se transmiten mediante un túnel por medio de Internet. En realidad, una VPN es un enlace punto a punto entre dos hosts, toda la información que se transmite por la VPN estará asegurada por la encriptación de sus datos, con esto los usuarios de ambos extremos pueden estar conectados a través del túnel de manera transparente. (Pomar, 2019)

1.4. Tipos de red privada virtual

De acuerdo a lo que se ha podido investigar se tienen los siguientes tipos de VPN:

- VPN basada en hardware.
- VPN basada en firewall.
- VPN basada en software.

VPN basada en hardware. Las redes privadas virtuales que se basan en hardware no son más que equipos dedicados, como ejemplo:

> Los routers, los cuales son seguros y fáciles de usar, ofreciendo un gran rendimiento, ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema

> operativo, el cual utiliza muchos recursos del procesador para brindar otros servicios (Quezada, 2016)

Este tipo de sistemas se encuentran basados en routers que encriptan la información, son seguros y fáciles de usar, pero para su funcionamiento requieren de una configuración bien realizada, así como definida correctamente, son equipos de un costo alto. Estos sistemas cuentan con la capacidad de asegurar un paquete en una parte de la red, utilizando para esto el tunneling de paquetes. (Quezada, 2016)

VPN basada en firewall. Este tipo de redes privadas virtuales utilizan:

> Los mecanismos de seguridad del servidor, incluyendo la restricción de acceso a la red interna, y realiza la traducción de direcciones, satisfaciendo los requisitos de autenticación. La mayoría de los firewalls comerciales también optimizan al núcleo del sistema operativo, al despojar a los servicios innecesarios o peligrosos, proporcionando de esta manera una seguridad adicional para el servidor VPN. La desventaja de este tipo de tecnología es poder optimizar su desempeño de manera eficiente sin mermar las aplicaciones del sistema operativo, el rendimiento en este tipo de VPN decrece, ya que no se tiene hardware especializado de encriptación. (Quezada, 2016)

VPN basada en software. Este tipo de red privad virtual es ideal donde ambos extremos de la VPN no están controlados por la empresa o cuando diferentes firewalls y enrutadores se encuentran implementados, se tratan de redes privadas virtuales independientes que ofrecen mayor flexibilidad en la manera en que se gestiona el tráfico de red. (Quezada Lozano, 2016)
"Muchos productos basados en software permiten que el tráfico de túnel dependa de la dirección o protocolo, a diferencia de los productos basados en hardware, que en general encapsulan el tráfico que manejan, independientemente del protocolo" (Quezada, 2016).

1.5. Protocolos usados en VPN

Los protocolos que mayormente se utilizan el momento de implementar una VPN son:

PPTP: "Point-to-Point Tunneling Protocol, este protocolo fue desarrollado por un grupo de ingenieros de Ascend Communcations:U.S. Robotics,3Com Corporation, Microsoft y ECI Telematics" (Zapata, 2016), permite el intercambio de datos de forma segura de un cliente a un

servidor formando de esta manera una Red Privada Virtual (VPN) , utilizando para esto TCP/IP. (Zapata, 2016)

IPSec: "Protocolo de seguridad de internet que permite varios servicios de seguridad para el protocolo de internet (IP) tanto para IPv4 como paraIPv6, este protocolo fue diseñado para soportar dos modos de cifrado" (Zapata, 2016).

L2TP: "Llamado también Layer 2 Tunneling Protocol, es un protocolo de estándar aprobado por el IETF, creado para corregir las deficiencias de los protocolos PPTP y L2F" (Zapata, 2016),

Este protocolo para realizar su trabajo "utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado, L2TP,es una variación de un protocolo de encapsulamiento IP que incluye mecanismos de autenticación PPP, PAP y CHAP(RFC 2661)" (Zapata, 2016).

Protocolo OpenVPN SSL/TLS: "Los protocolos SSL (Secure Socket Layer) y TLS (Transport Layer Security) son protocolos de la capa de transporte que proporcionan comunicaciones seguras en Internet" (Quezada, 2016).

> Los protocolos SSL versión 3.0 y TLS versión 1.0 son idénticos, una de las diferencias, son sus diseñadores. SSL/TLS permite la autenticación tanto del cliente como del servidor, usando claves públicas y certificados digitales, y proporciona comunicación segura mediante el cifrado de la información entre emisor y receptor. SSL/TLS funciona por encima del protocolo de transporte (normalmente TCP) y por debajo de los protocolos de aplicación. Este protocolo está muy extendido para realizar actividades de comercio electrónico de tal manera que Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet. (Quezada Lozano, 2016)

WireGuard

Se trata un protocolo VPN innovador ya que ofrece una solución más segura, sencilla y rápida a sus usuarios con respecto a otros protocolos, este protocolo se ejecuta sobre UDP (Vpnranks, 2020).

Este protocolo presenta simplicidad de código, lo cual facilita la implementación, así como permite un mayor rendimiento y menos errores. (Vpnranks, 2020)

1.6. Software libre

El software libre suele estar disponible gratuitamente, o muchas veces al precio de costo de la distribución a través de otros medios, no siendo obligatorio que sea así, es por esto que no se debe asociar el termino software libre como "software gratuito" (al que se le denomina comúnmente Freeware), ya que puede ser distribuido comercialmente ("software comercial") y no perder el carácter de libre. De igual manera, el "software gratis" puede incluir en algunas ocasiones el código fuente sin embargo, este tipo de software no necesariamente puede ser libre a menos que se garanticen los derechos de modificación y que estas versiones modificadas puedan ser distribuidas. (ECURED, 2020)

1.7. Sistema Operativo Linux

La historia de Linux

"Linux es un sistema operativo (SO) de open source y una plataforma de infraestructura de TI" (RedHat, 2020).

Su creador fue Linus Torvalds cuando se encontraba en la universidad, la idea de Linus fue crear una versión de open source, como una alternativa del sistema operativo MINIX, el cual estaba basado originalmente en Unix, solo que esta versión debía ser completamente gratuita. Este sistema se ha convertido en el SO con una gran cantidad de usuarios, siendo además el Sistema Operativo más usado para trabajar como servidores de Internet los cuales están disponibles públicamente, es necesario mencionar también que es el único usado en supercomputadoras. (RedHat, 2020)

"Tal vez lo mejor sobre Linux es que es open source. Linux se lanza en virtud de la Licencia de uso público GNU (GPL)" (RedHat, 2020).

La Licencia GNU(GPL) que permite que todos pueden ejecutar, estudiar, compartir y modificar el software, es importante indicar que el código modificado también puede ser distribuido o vendido, pero todo esto se debe hacer con la misma licencia, siendo esta una de las ventajas con respecto a los sistemas operativos tradicionales conocidos los cuales están bloqueados y no pueden ser modificados. (RedHat, 2020)

1.7.1. La seguridad de Linux

"La seguridad no permite implementarla para luego simplemente olvidarnos de ella. Debe ser parte integrante de cualquier empresa y de cualquier estrategia de implementación" (RedHat, 2020).

La mejor seguridad es la que se implementa en capas.

La seguridad debe ser integral y no una función, Cuando se habla de seguridad de la TI, el sistema operativo desempeña un trabajo mucho más amplio que comprende el hardware al igual que los usuarios con acceso a dicho hardware y las aplicaciones que están implementadas en este, de una forma más amplia se deben tomar en cuenta la gestión de riegos, el control y su cumplimiento, en seguridad se deben abordar todos los aspectos que la comprenden. (RedHat, 2020)

Linux es un sistema modular lo que permite la administración fácil de la seguridad, cada parte del sistema Linux puede ser auditada, supervisada y protegida, este sistema cuenta con herramientas y módulos que permiten bloquear, informar y además solucionar los problemas de seguridad que pueden darse, como una de las características importantes se tiene que Linux trata de forma separada el espacio del usuario del kernel del sistema, esto impide que los usuarios puedan acceder a los procesos que se ejecutan por parte de dicho sistema. (RedHat, 2020)

Por supuesto, no existe un sistema operativo completamente seguro, pero hay medidas que se puede implementar y ventajas que Linux ofrece para estar protegido de una mejor manera.

1.7.2. Distribuciones de Linux empresariales.

GNU/Linux es el sistema empresarial por excelencia, se trata de un sistema flexible, fiable, seguro, sin dejar pasar que se trata de un software gratuito, o al menos más barato, haciendo con esto posible que las empresas inviertan en otras áreas y se despreocupen de las licencias, es importante indicar que el código fuente puede ser modificado, creando con esto soluciones personalizadas y con esto cubrir las necesidades o ajustarlo a los requerimientos de la empresa. (LinuxAdictos, 2019)

"Linux no ha triunfado en lo que tiene que ver a equipos de escritorio, pero sin duda es más reconocido por su trabajo en servidores, supercomputadoras y a nivel empresarial" (linuxadictos, 2020).

Entre las distribuciones que se consideran las más interesantes se tienen:

SUSE Linux Enterprise Server (SLES)

SUSE está más presente en distribuciones para empresas, Suse Linux es un fuerte competidor de RedHat en este campo sorprendiendo siempre con nuevas soluciones para los clientes. Es importante indicar que SUSE cuenta con el apoyo de SAP. (linuxadictos, 2020)

Red Hat Enterprise Linux (RHEL)

Red Hat es otro de las distribuciones completas de Linux, claro que esto es a cambio de pagar una cantidad mínima, comparándolo con otros sistemas operativos que muchas veces ofrecen menos características. (linuxadictos, 2020)

Debian

Cuenta con una gran comunidad formada por desarrolladores siendo un sistema fiable, robusto, así como estable que permite la implementación de una solución de oficina como un poderoso servidor. (linuxadictos, 2020)

Además, "Debian ofrece algunas alternativas notorias en cuanto al kernel, como kFreeBSD o NetBSD, aunque otros no sean tan interesantes como Debian GNU/Hurd" (linuxadictos, 2020).

La distro Debian no tiene una versión para servidores como si lo tiene Ubuntu, siendo uno de sus fuerte la optimización de recursos y su seguridad, Debian puede ser adaptado por el administrador del sistema a las necesidades de cada empresa, pues se parte de una distribución base. (Redeszone, 2019)

"Debian, es un sistema para aquellos que quieran un sistema también fiable, seguro, robusto y sólido, pero con paquetería DEB y AppArmor como sistema de protección por defecto" (LinuxAdictos, 2019).

CentOS (Community ENTerprice Operating System):

CentOS es una distribución que nace como una compilación a partir de Red Hat Enterprice Linux, siendo gratuito, siendo la filosofía de la empresa el ofrecer un producto de tipo empresarial a valor cero, esta distro es robusta, estable y siendo además fácil de instalar y utilizar. (linuxadictos, 2020)

Al tratarse de una distro basada en RedHat es actualizado frecuentemente, se encuentra libre de bug y vulnerabilidades, además si se necesita contar con un servidor basado en paquetería RPM y con un módulo de seguridad como lo es SELinux se debe elegir CentOS. (LinuxAdictos, 2019)

Canonical Ubuntu Server/Ubuntu Cloud

Canonical Ubuntu es también de código abierto y gratuito se trata de una distribución que hereda mucho del sistema de escritorio, pero orientada a servidores así, como para la nube. (linuxadictos, 2020)

Ubuntu Server es la mejor distribución para los usuarios que quieren una experiencia instalar y empezar a utilizar, sin complejas configuraciones ni problemas. Ubuntu Server es básicamente Ubuntu Desktop, pero no cuenta con la interfaz y tampoco cuenta con muchos de los paquetes que vienen instalados por defecto, a cambio cuenta con varias herramientas de servidor como OpenStack, Mitaka, Nginx y LXD entre otros. (Redeszone, 2019)

Fedora

Fedora es una distribución de Linux de código abierto siendo de las más estables, es desarrollado por el proyecto Fedora y respaldado por la comunidad, fue creado para probar futuras actualizaciones de Red Hat. (LinuxAdictos, 2019)

"Con más de 20000 paquetes, Fedora es rápido, seguro y muy fácil de usar incluso para los recién llegados a Linux" (LinuxAdictos, 2019).

1.8. Red privada virtual con software libre

En el tiempo que se vive actualmente se ha vuelto mucho más sencillo el trabajar desde casa o cualquier ubicación distante a la empresa, debido a que las herramientas, programas y servicios sean gratuitos o no, permiten tener en otras palabras una oficina móvil, estando constantemente comunicado, sea con compañeros, usuarios, clientes o proveedores.

"Otra herramienta muy útil para el teletrabajo que añade mayor seguridad es la tecnología VPN, que cifra las comunicaciones y permite trabajar con información importante sin miedo a que los datos sean robados por otros" (Hipertextual, 2013).

Para establecer una conexión VPN es necesario un cliente y un servidor, el primero instalado y configurado en el ordenador personal y el segundo instalado y configurado en el servidor que da acceso a la red local a través de una red pública. (Hipertextual, 2013)

De acuerdo a la investigación realizada se ha optado por describir los siguientes sistemas VPN:

1.8.1. LogMeIn Hamachi

Se trata de un servicio de redes virtuales el cual puede ser instalado en minutos, permitiendo acceder de manera remotamente y con la seguridad necesarias a la red de una empresa, para lo cual es necesario contar con una conexión de internet, Hamachi es un servicio bajo demanda que se encarga de proporcionar a los usuarios las conexiones remotas necesarias, se debe indicar además que esta tecnología no se preocupa de la tecnología o infraestructura. (Logmeininc, 2020).

"Todos los usuarios de Hamachi deben contar con una suscripción de pago o gratuita para crear redes de Hamachi o unirse a ellas, es gratuita para uso personal y ofrece planes de pago para uso profesional" (LogMeIn, 2017).

1.8.2. SoftEther VPN (Software Ethernet VPN)

Es un software VPN multiprotocolo siendo fácil de usar y de los más potentes que se pueden encontrar, puede funcionar en Windows, Linux, Mac, Solaris, es además de código abierto, permite uso personal como comercial y de forma gratuita. (SoftEther, 2019)

Características

Entre las características más relevantes de SoftEther se tienen:

Alternativa a OpenVPN y VPN de Microsoft.

Es compatible con Windows, Mac, iOS y Android.

Permite configurar el servidor VPN detrás del firewall o NAT.

Tiene una gran compatibilidad con los productos VPN más populares de la actualidad, es además capas de admitir protocolos como SSL-VPN, OpenVPN, L2TP, EtherIP, L2TPv3 e IPsec, como un único software VPN. (SoftEther, 2019)

Se debe indicar que SoftEther VPN es un software gratuito es decir puede ser descargado y usado no debiendo realizarse pago alguno, fue desarrollado como investigación de tesis de la maestría de Daiyuu Nobori. (SoftEther, 2019)

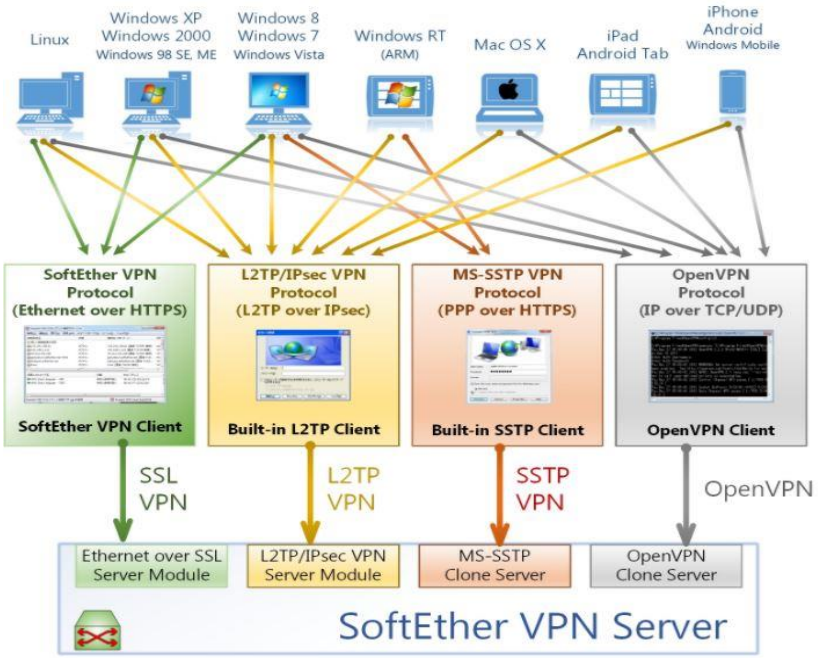

Figura 1. 1 SoftEther VPN Server. (SoftEther, 2019)

1.8.3. AnyConnect

"AnyConnect Secure Mobility Client (ver figura 1.2), puede empoderar a sus empleados para hacer esto y aún proporcionar la seguridad necesaria para ayudar a garantizar que su organización está segura y protegida" (Cisco, 2020).

Cisco AnyConnect ofrece múltiples servicios de seguridad para proteger la empresa, proporcionando además la visibilidad y el control que es necesaria para identificar quién y qué dispositivos acceden a la empresa. (Cisco, 2020)

"La amplia gama de servicios de seguridad de Cisco AnyConnect incluye funciones como la aplicación de acceso remoto, funciones de seguridad web y protección de roaming" (Cisco, 2020).

"Cisco AnyConnect ofrece su departamento de TI todas las funciones de seguridad necesarias para proporcionar un sistema robusto, fácil de usar y experiencia móvil altamente segura" (Cisco, 2020).

"Los clientes de AnyConnect están disponibles en un amplio conjunto de plataformas, incluidas Windows, macOS,Linux, iOS, Android, Windows Phone / Mobile, BlackBerry y ChromeOS" (Cisco, 2020).

Figura 1. 2 Cisco AnyConect-Way more tan VPN. (Cisco, 2020)

1.8.4. OpenVPN

OpenVPN no es solo un protocolo de comunicación sino también una aplicación de código abierto que permite realizar conexiones VPN, maneja una licencia de software libre (Castillo, 2020)

> La programación de la aplicación está realizada principalmente en C, y se basa en enlaces de tipo SSL (Secure Sockets Layer) y TLS (Transport Layer Security). OpenVPN no soporta por tanto protocolos L2TP o PPTP, ya que es un protocolo personalizado basado los dos anteriormente citados.
>
> La arquitectura de conexión y comunicación es la típica de una VPN, basada en punto-a-punto. Para efectuar esta conexión se requiere validación jerárquica entre usuarios y servidor a través de certificados SSL/TLS + RSA de forma remota. Soporta todo tipo de enlaces de red, como WiFi IEEE 802.11, Ethernet 802.3 y red de datos móviles. (Castillo, 2020)

"OpenVPN ofrece una alternativa liviana y rentable a otras tecnologías VPN que está bien adaptada para los mercados de pymes y empresas" (OpenVpn, 2015).

1.8.4.1. Principales características

Entre algunas de las características de OpenVPN se tienen que permite tener un adaptador de red Ethernet virtual utilizando un solo puerto UDP o TCP, Maneja herramientas de encriptación y autenticación así como certificación de la biblioteca SSL lo que permite proteger la red privada, en cuanto a cifrado es posible utilizar el cifrado convencional que se basa en la clave estática o el cifrado de clave pública que se basa en certificados, OpenVPN se basa en SSL que es el estándar que permite tener comunicaciones seguras cuando se está haciendo uso del internet, por último se añade que con OpenVpn se pueden tener redes de túneles a través de firewalls, además admite redes de túnel sobre NAT (OpenVpn, 2015).

OpenVPN cuenta con portabilidad multiplataforma, brinda estabilidad, escalabilidad a miles de clientes, su instalación es relativamente fácil y presenta soporte para IP dinámicas y NAT, es un sistema que admite métodos de autenticación alternativos por medio de su módulo de complemento. OpenVPN maneja seguridad de nivel industrial, el cual ha sido diseñado para

proteger tanto ataques pasivos como activos, se debe mencionar también que OpenVPN trabaja en varias plataformas como Solaris, Linux, Mac, OpenBSD y Windows. Uno de los principales objetivos de OpenVPN es la recuperación de errores, esto quiere decir que si la capa IP deja de funcionar por unos 5 minutos, el momento en que vuelva a funcionar todo el tráfico del túnel será reanudado de inmediato, permite de igual manera controlar los parámetros de seguridad del túnel VPN, sin dejar de lado la protección del mismo servidor. (OpenVpn, 2015)

1.8.4.2. Seguridad en OpenVpn

OpenVPN permite tener un servidor con acceso desde cualquier IP a través de internet, es decir los usuarios remotos podrán acceder a la red corporativa de una empresa utilizando este servidor OpenVPN. (Linuxito, 2018)

El problema en sí de tener acceso público a la VPN, es que se termina volviendo blanco de un sinnúmero de ataques, siendo esto una razón por la cual se debe mejorar la seguridad de los equipos que permiten el acceso a la VPN, para esto OpenVPN permite recurrir al mecanismo de autenticación TLS, logrando con esto bloquear ataques DoS más conocidos como ataque de negación de servicio. (Linuxito, 2018)

Clientes OpenVpn

El cliente de OpenVPN se puede instalar en diferentes plataformas como CentOS o RedHat, Ubuntu, Debían, Mac OS, de igual forma puede ser instalado en las diversas versiones de Windows de microsoft. (Stackscale, 2020)

1.9. Firewall software libre

Actualmente es necesarios tener un firewall o cortafuegos, pues los servidores que no cuentan con uno se encuentran expuestos a los ataques y violaciones de seguridad por personas malintencionadas. (Guiadev, 2014)

"El objetivo de un firewall es principalmente bloquear los accesos no autorizados a ciertas áreas y/o servicios, el firewall puede ser utilizado para proteger los accesos a servidores vía ssh, accesos a cuentas cPanel, accesos vía FTP, entre algunos" (Guiadev, 2014).

El firewall es uno de los aspectos de seguridad más importantes de en todo equipo informático, pudiendo ser este una aplicación o un dispositivo completo, el cual regulará las conexiones sean estas entrantes o salientes, utilizando para esto reglas predefinidas. (Merino, 2020)

"En Linux, no existe un firewall como se acostumbra a entenderlo en entornos Windows, sino que técnicamente sus funciones se dividen entre varios programas que trabajan en sucesivas capas o niveles" (Merino, 2020)

- **Nivel 1: Netfilter**

  "Es un framework integrado en el mismo kernel de Linux, que permite al sistema operativo llevar a cabo diversas operaciones relacionadas con las redes (traducción de direcciones y puertos, filtrado de paquetes, rastreo de conexiones, entre otros" (Merino, 2020).

  No es posible interactuar de forma directa con Netfilter, sino que se cuenta con una API la cual permite a otras aplicaciones actuar como intermediario. (Merino, 2020)

- **Nivel 2: Iptables / Nftables**

  "Iptables es una herramienta que se puede invocar desde la línea de comandos, y que desembarcó en Linux a partir del lanzamiento de la versión 2.4 del kernel como sustituto del ya obsoleto ipchains" (Merino, 2020).

  Por medio de Iptables se pueden cambiar los parámetros de funcionamiento de Netfilter a través de reglas de filtrado, debiéndose mencionar que iptables está siendo sustituido por un nuevo software conocido como Nftables, esta herramienta sustituye igualmente a ip6tables, arptables y ebtables, Nftables es más flexible y escalable que iptables usando para esto una sintaxis más compacta e intuitiva (Merino, 2020).

- **Nivel '2,5': Front-ends no-gráficos**

  Nftables ha simplificado la tarea de crear las reglas del firewall de Linux, pero con el pasar del tiempo se han ido desarrollando nuevas herramientas que trabajan sobre Nftables e Iptables (Merino, 2020), algunas de estas herramientas son:

UFW: Siglas de 'Uncomplicated Firewall', una herramienta para usuarios domésticos creada por Canonical para Ubuntu, que lo incluye por defecto desde la versión 8.04.

APF: Siglas de 'Advanced Policy Firewall'. En este caso, se está ante un software específicamente diseñado para proteger servidores.

Shorewall: Shorewall es otro cortafuegos, avanzado y polivalente, que se puede manejar desde la terminal. (Merino, 2020)

FirewallD

FirewallD permite implementar reglas de tráfico que son persistentes a través de una línea de comando e interfaces de tipo gráfica, es parte de los repositorios de la mayoría de distribuciones de Linux. (bluehosting, 2016)

El utilizar FirewallD presenta dos diferencias principales, si se compara con la forma de trabajar con iptables:

"FirewallD utiliza zonas y servicios en lugar de cadenas y reglas.

FirewallD administra los grupos de reglas dinámicamente, permitiendo actualizaciones sin tener que romper las sesiones y conexiones." (bluehosting, 2016).

FirewallD no es más que un contenedor para iptables, este permite trabajar de manera mas sencilla que las reglas que se debían generar en iptables, los comandos que se utilizaban en iptables pueden ser tambien utilizados en FirewallD. (bluehosting, 2016)

"El uso de firewall, es una de las mejores formas de proteger el sistema del tráfico no deseado procedente de redes externas. Una herramienta perfecta para tal efecto, es FirewallD, que además es open source" (G.B., 2020).

- **Nivel 3: Front-ends gráficos**

Los usuarios que están acostumbrados a usar Windows o Mac esperan contar con una herramienta de tipo gráfica con la cual pueda configurar su firewall, seguramente los usuarios de Linux agradecerían en contar con una sistema grafico para la configuración del firewall. (Genbeta, 2020)

Entre algunas de las aplicaciones graficas de firewall existentes se tienen:

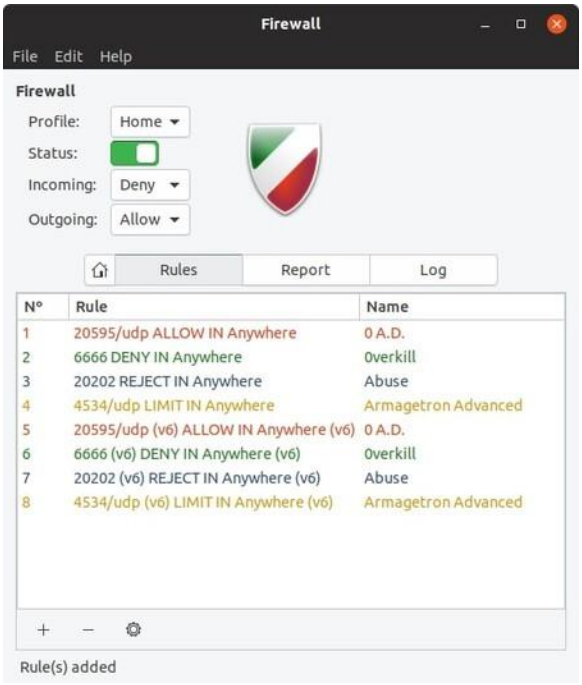

Figura 1. 3 Front End gráfico. (Genbeta, 2020)

GUFW: "Es la interfaz gráfica oficial de UFW. Centrado en la usabilidad, viene de serie con toda una serie de reglas pre configuradas para aplicaciones y servicios concretos que se pueden ir configurando" (Genbeta, 2020).

Figura 1. 4 Douane. (Genbeta, 2020)

Douane: "Douane está dotado de una interfaz sencilla, por no decir simplista, para usuarios domésticos que no quieran complicarse la vida" (Genbeta, 2020).

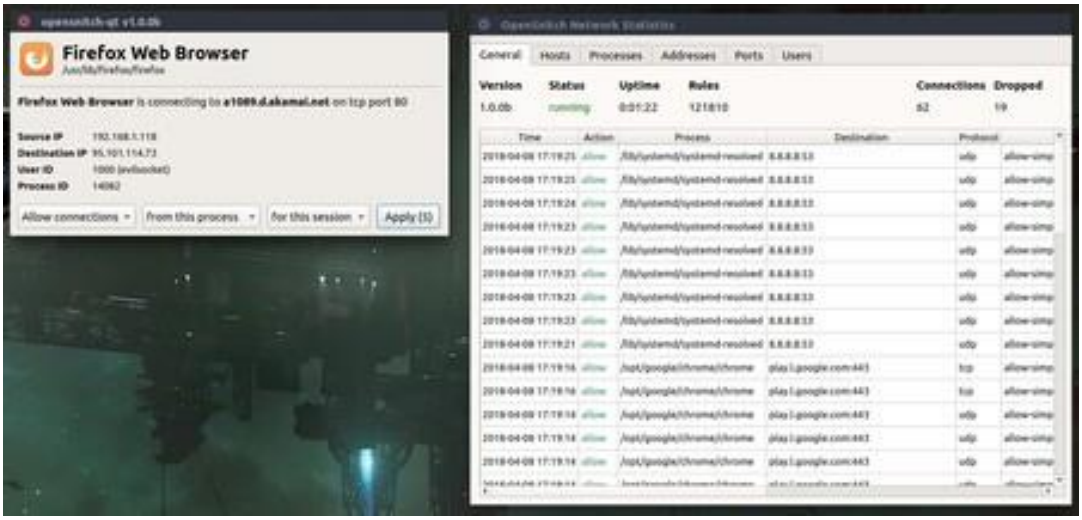

Figura 1. 5 OpenSnitch. (Genbeta, 2020)

OpenSnitch: "OpenSnitch es una aplicación para Linux creada a partir del código de un cortafuegos nativo de MacOS, Little Snitch" (Genbeta, 2020).

1.10. Servidor proxy de Linux

Un servidor proxy no es más que un sistema o equipos que se encarga de guardar las páginas que son visitadas, para que sí se intenta visitar nuevamente la misma página , dicha página será traída del proxy, con esto se consigue que la navegación web sea más rápida, con este proceso también se reduce el tráfico hacia internet. (Mokhtar, 2017)

Un servidor proxy puede reducir el tráfico externo aproximadamente un 45%, se puede configurar el proxy para el control de acceso (Mokhtar, 2017), es decir se puede controlar el acceso por usuarios, por equipos, por horario, por páginas y un sinnúmero más de opciones de control

Entre los servidores proxy Linux se tienen:

"Squid, Varnish, Polipo, TinyProxy entre otros más" (Mokhtar, 2017).

1.11. Encriptación de datos

Aunque comúnmente se utiliza la palabra encriptar indistintamente, de lo investigado la palabra no tiene significado real sino más bien es reconocido por la RAE como ocultar o sinónimo de cifrar.

Cifrar:

"Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger" (RAE, 2020).

> El cifrado es un método para evitar que alguien no pueda tener acceso a información que se desea preservar. Este método consiste en alterar un mensaje antes de transmitirlo, generalmente mediante la utilización de una clave, de modo que su contenido no sea legible para los que no posean dicha clave. De esta forma, cualquier persona que tenga acceso al mensaje no podrá entender su contenido a menos que cuente con la clave para descifrarlo. No solo es necesario cifrar, sino hacerlo de manera que la información no sea inteligible ni manipulada por terceros. Sin esta última condición, el cifrado no tendría valor. (Carvajal, 2019)

1.11.1. Sistemas de encriptación

Entre los sistemas de encriptación se tiene 3 tipos que son:

1.11.1.1. Encriptación simétrica

Figura 1. 6 Encriptación simétrica. (Nextvision, 2017)

Para que este sistema funciones de usa la misma clave para cifrar y descifrar la información que viaja entre emisor y receptor, los mismos que debieron ponerse de acuerdo sobre la clave que se va a utilizar, este tipo de sistema es en realidad el más inseguro debido a que la clave que se utilice para la comunicación es fácil de interceptar, igualmente es una clave poco práctica tomando en cuenta que la seguridad del cifrado depende de que tan fuerte sea la clave y en este sistema la misma puede resultar demasiado larga. (Nextvision, 2017)

1.11.1.2. Encriptación asimétrica

Figura 1. 7 Encriptación asimétrica. (Nextvision, 2017)

Este sistema utiliza para la encriptación una clave pública, trabaja con 2 claves diferentes entre emisor y receptor, la clave pública se transmite a todos los nodos que requieran enviar información cifrada y la otra clave es privada y secreta, las claves están vinculadas y su relación es los suficientemente complejas asegurando de esta forma imposible que se obtenga la clave privada a partir de la pública, el sistema se basa en el algoritmo RSA. (Nextvision, 2017)

Las claves que se utilizan en este sistema sirven para encriptar la información, permiten asegurar que el mensaje cifrado mantenga su integridad, además de certificar la autenticidad del emisor, el principal inconveniente de este sistema es que a pesar de ser más segura, el proceso se vuelve lento dado que el tiempo de procesamiento que se requiere, las claves deben ser más largas que en el cifrado simétrico obteniendo como resultado del cifrado un mensaje más largo que el original. (Nextvision, 2017)

1.11.1.3. Encriptación híbrida

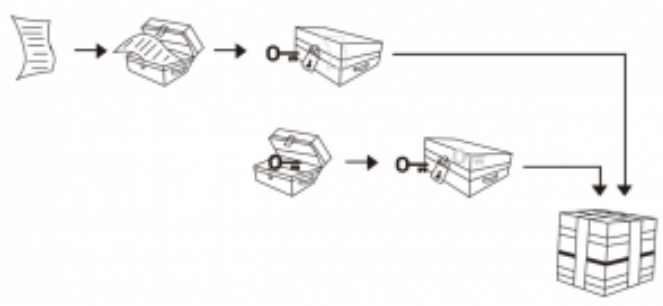

Figura 1. 8 Encriptación hibrida. (Nextvision, 2017)

Este sistema utiliza los mejor de los sistemas simétrico y asimétrico con lo cual se solventa los problemas que presentan cada uno, la encriptación de tipo hibrida sigue los siguientes pasos:

Se genera una clave privada y una pública (desde el receptor).

Se encripta el archivo al mismo tiempo en el que se generan las claves.

El receptor envía su clave pública.

Se encripta el archivo con la clave pública recibida.

Se envía el archivo cifrado de forma síncrona y la clave de forma asíncrona (Nextvision, 2017).

De esta manera el sistema hibrido es bastante útil al enviar información cifrada de manera simultánea a varios usuarios. (Nextvision, 2017)

1.11.1.4. Comparación de cifrado simétrico y asimétrico

Como se indicó cada sistema presenta sus ventajas y desventajas, las mismas son vistas desde las siguientes perspectivas:

- **Velocidad**:

"La principal ventaja del cifrado simétrico es que es mucho más rápido y ágil. De modo que, si se quiere cifrar una gran cantidad de información, se ahorrará tiempo con este tipo" (Oficina de Seguridad del Internauta, 2019).

Por el contrario, "el cifrado asimétrico es mucho más lento. Si el rendimiento es un factor clave a tener en cuenta, no es la mejor opción" (Oficina de Seguridad del Internauta, 2019).

- **Seguridad**:

El cifrado simétrico no presta tanta seguridad, ya que el hecho de enviar la clave supone una gran vulnerabilidad.

"La ventaja del cifrado asimétrico es el hecho de que puede comunicar de forma segura, claves públicas a terceros, este tipo tiene la libertad de entregar la clave pública, mientras la clave privada permanece con el usuario" (Oficina de Seguridad del Internauta, 2019).

- **Número de claves**:

"La administración de claves también es un beneficio al usar el cifrado asimétrico. Solo necesitas un par de claves, por usuario, para cada uno, para poder cifrar mensajes para todos los demás usuarios" (Oficina de Seguridad del Internauta, 2019).

2. ANÁLISIS DE CONDICIONES ACTUALES

2.1.Análisis de equipos que dispone la institución.

La Comision Fulbright del Ecuador al momento dispone de los siguientes equipos:

Cantidad	Ubicación	Tipo de equipo	Sistema Operativo	Características	Servicio	Dominio
1	Sistemas	Servidor	Windows server 2008	Dell: Intel Xeon X5560 2.8 ghz.	Active Directory local	Fulbright.local
1	Sistemas	Servidor	Windows Server 2012	Proliant ML110 G9 / Intel Xeon E5-2603v3 6-Core	Aplicaciones	Fulbright.local
1	Sistemas	Clon Servidor	Centos 5.2	Proc: Corei3, Mem: 2GB Ram, DD: 350GB	Servidor de correos(masivos)	----------
1	Sistemas	Clon Servidor	Centos 5.4	Proc: Corei3, Mem: 2GB Ram, DD: 350GB	Firewall y proxy	----------
8	Staff	Escritorio	Windows7 Pro	Core i3		Fulbright.local
4	Staff	Escritorio	Windows7 Pro	Core 2 Quad		WorkGroup
12	Staff	Escritorio	Windows7 Pro y Windows 10	Core i 5		10 Fulbright y 2 Workgroup
11	Staff	Escritorio	Windows7 Pro y Windows 10	Core i 7		WorkGroup
1	Staff	Escritorio	Windows7 Pro	Dual Core		WorkGroup
1	Staff	Escritorio	Windows7 Pro	P4		Sin red

Tabla 2. 1 Listado de equipos Comisión Fulbright

2.2. Estado actual de la red local y red pública

Al momento se cuenta con dos servicios de internet con proveedores distintos, con el primer proveedor se mantiene un servicio de tipo PYME de 75Mbps simétrico con una dirección IP pública, El otro servicio de internet es un servicio home de 2Mbps de subida por 1Mbps de bajada de igual manera con una dirección IP pública.

El internet del servicio PYME es distribuido a la red interna a través de un servidor Linux con Centos 5.4 utilizando el paquete de squid como proxy de internet e iptables como el firewall de protección y control de accesos entre el internet y red local.

En el servicio de internet home está conectado un equipo Linux con Centos 5.2 este se utiliza para realizar el envío de correo masivo con la ayuda de una aplicación(GroupMail) en el que se debe programar el envío a las listas de correo, tiene configurado un servidor de correos con Sendmail con un dominio diferente al dominio utilizado por el personal de la Comision Fulbright, con lo cual se evita que se bloquee el dominio de trabajo si se llegara a caer en listas negras la cuenta que se utiliza en el envío masivo.

En la red interna se cuenta con un servidor Dell con Windows Server 2008, el cual es el servidor de dominio local para controlar los accesos de usuarios, así como es el encargado de la administración de las carpetas compartidas con los permisos debidos.

Se ha implementado un equipo con varios discos, generando el espacio suficiente para poder realizar de esta forma los respaldos de manera automática y continua de las carpetas con información importante y bases de datos de los sistemas utilizados.

Además, se tiene un servidor de aplicaciones con el sistema de contabilidad, que es un sistema cliente servidor. Se tiene igualmente un sistema académico y de matrículas el que es utilizado por el personal de ETP

Los sistemas de contabilidad y académico funcionan únicamente en la red local, de igual manera existen carpetas compartidas a las cuales solo se tiene acceso desde el interior de la institución, lo cual es un inconveniente el momento en que el personal requiere realizar teletrabajo.

En lo que tiene que ver a infraestructura, se tiene red con categoría 6 y categoría 5e, el edificio principal consta de 2 pisos, en el primer piso se tiene un rack de pared con un patch panel y

switch no administrable de 24 puertos, se encuentra además un router inalámbrico para cubrir las principales áreas de este piso, este switch está conectado al rack del segundo piso, en el cual se tienen dos patch panel y 2 switch no administrables de 24 puertos cada uno, los mismos que están conectados en cascada, en este piso se tienen 3 routers inalámbricos para cubrir con señal inalámbrica la mayor parte del área del piso.

Existe un área de aulas(ETP) con 11 computadores de escritorio con tarjetas inalámbricas esta área se cubre con un router inalámbrico.

A continuación, en la figura 2.1 se observa la distribución de la red de la Comision Fulbright.

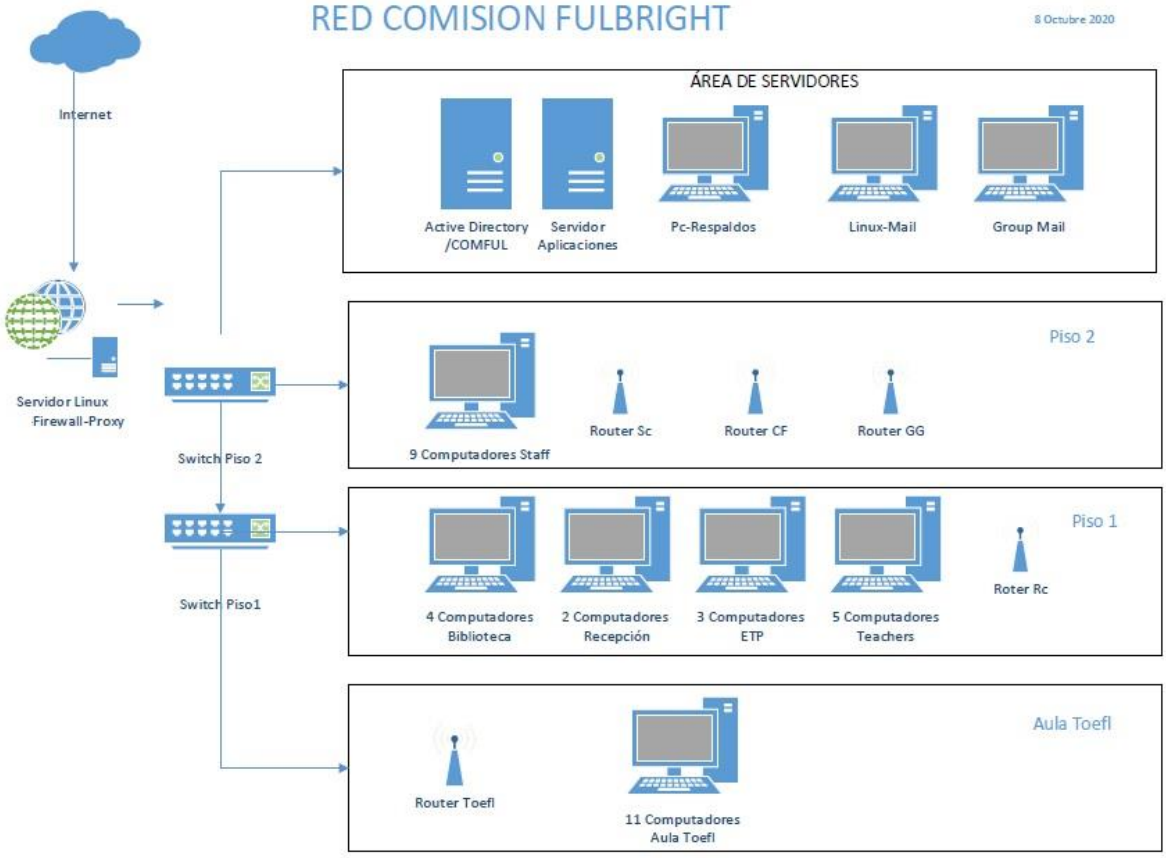

Figura 2. 1 Distribución de la red de la Comision Fulbright del Ecuador.

2.3. Levantamiento de la información

En reunión mantenida con la Dirección de la institución, se establece la necesidad que existe de que el personal pueda realizar el trabajo desde sus hogares, dada la situación que se ha

presentado debido a la emergencia y las medidas implementadas por el gobierno por el riesgo de contraer COVID, debiendo en la brevedad posible encontrarse una solución, que en lo posible se evite incurrirse en gastos mayores.

En la institución existe la necesidad de que su personal pueda trabajar desde su casa o cualquier lugar como si se encontrase en la oficina, lo cual hasta el momento no ha sido necesario, se debe tomar en cuenta que en este trabajo remoto los datos utilizados deben viajar de forma segura debido a que la información que se mantiene en la empresa tiene un uso restringido, no debiendo correrse riesgos de que personas no autorizadas puedan tener acceso a la misma.

Se debe establecer que personas de la institución podrán contar con el servicio, quienes cuentan con servicio de internet, quienes cuentan con equipos en sus hogares, así como que equipos son necesarios adquirirse para poder dotar a todo el personal de las herramientas necesarias para poder realizar trabajo no presencial.

2.4. Características de equipos a utilizarse

Luego de revisado los requerimientos de los empleados de la institución, es necesario presentar el hardware que se deben adquirir para la implementación del servidor VPN, así como las características de los equipos que deberán suministrarse a algunos de los funcionarios para que puedan conectarse al servicio y de esa manera poder realizar teletrabajo, tomando en cuenta que la empresa dispone ya de algunas laptops.

La cantidad y características de los equipos se muestran en las tablas:

Computador para servidor VPN	
Cantidad	**Características**
1	Computador Servidor Linux VPN: Core-i5 o Superior Memoria ram de 8GB o superior Disco duro 500MB o superior 2 tarjetas de red pci Express

Tabla 2. 2 Características de computador para servicio VPN

Laptops para personal	
Cantidad	**Características**
4	Laptop: Sistema Operativo Windows 10 PRO, Memoria Ram de 8 o 16 GB Disco duro de 1 Terabyte Wifi, Bluetooth, puertos: Usb 3.0, VGA, HDMI, RJ45, Salida para audífonos/estéreo, entrada de micrófono, lector de tarjetas

Tabla 2. 3 Características de laptops para el personal

2.5. Informe de requerimientos y estado actual de la institución

Luego de haber revisado el estado actual de la institución, se ha llegado a las siguientes conclusiones:

- Tomando en cuenta que la empresa cuenta con un servicio de internet al igual que la mayoría de empleados, se ha optado por la opción de instalar un servicio VPN, el cual permitirá que el personal de la institución pueda conectarse desde sus hogares o cualquier otro lugar a través del servicio de internet y con todas las seguridades que permiten implementarse a través de un servicio de este tipo.
- La institución cuenta con aproximadamente 11 funcionarios de planta y 6 docentes que laboran por horas con lo cual, para la implementación de la VPN, debe considerarse que se conectaran al servicio un mínimo de 11 usuarios pudiente llegar a un máximo de 17.
- Los usuarios deberán conectarse a la red interna pudiendo de esta forma tener acceso a sus equipos para trabajar mediante escritorio remoto para los casos en los que se requiera utilizar las aplicaciones locales, de igual manera podrán tener accesos a las carpetas compartidas y demás servicios con los que cuenta la red de la Comision Fulbright, dando a los usuarios la visión de estar trabajando dentro de las instalaciones de la institución.

- En cuanto al servicio de internet, es necesario solicitar a la institución realizar una upgrade al siguiente plan de internet PYME que dispone el proveedor, que es de 100MB simétrico lo cual permitirá mantener un servicio adecuado y garantizar en parte el servicio VPN.
- Al momento como pasarela entre la red institucional e internet se tiene un equipo Linux con la distribución de Centos versión 5.4, la cual es una versión que fue lanzada en el 2009 y por ende es necesario realizar el cambio a una nueva versión, en cuanto al hardware que se utiliza se trata de un computador Core i3 con 2 GB de memoria lo cual en su momento cumplía con los requerimientos necesarios y que de igual manera es necesario se cambie el equipo para tener un equipo estable por un buen tiempo.
- La Dirección de la institución ha analizado el caso de cada funcionario determinando que existen personas que no cuentan con equipos adecuados para poder conectarse remotamente a la oficina y ha definido que es necesario adquirir 4 laptop para que el personal pueda tenerlos en sus hogares y realizar teletrabajo, de manera adicional se analizará la posibilidad de poder contratar algún tipo de plan corporativo de internet que incluya a los funcionarios o conceder un bono adicional para que su personal pueda mantener un servicio adecuado de internet en sus hogares.

3. DISEÑO DE LA RED PRIVADA VIRTUAL

3.1. Determinar sistema operativo, distribución, versión a instalar

Luego de haber revisado la información de los sistemas operativos y de analizar la opción de contar con un sistema operativo que no implique pago de licencias ha sido necesario decidirse por una de las distribuciones de Linux, dado que Linux brinda la seguridad necesaria, flexibilidad, un sistema estable con todas las ventajas siendo en la mayoría de casos gratuito al menos de menor precio a uno de pago.

Dado la cantidad de opciones que existe en distribuciones Linux, el elegir una se volvió una tarea compleja y a momento algo confusa, para el estudio se ha tomado algunas de las distribuciones más conocidas para posteriormente analizar sus características, ventajas y desventajas.

Entre las distribuciones para empresas con sus ventajas y desventajas que se pueden observar en las tablas 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 y que sirven para el análisis están las siguientes:

- Suse Linux Enterprice Server
- Red Hat Enterprise Linux (RHEL)
- Debian
- Centos
- Ubuntu
- Fedora

SUSE LINUX ENTERPRISE SERVER	
VENTAJAS	**DESVENTAJAS**
Es 100% libre.	No es fácil de usar.
Existe una baja probabilidad de que el equipo se vea afectado por virus.	En algunos casos se carece de soporte de Hardware.
Centro de Control Avanzada Yast.	La falta de potentes programas informáticos específicos.
Facilidad en instalación de los programas.	Los lanzamientos no incluyen las últimas versiones.
Increíble colección de herramientas, en cualquier distribución posees al menos más de 2000 paquetes diferentes.	No se emiten recomendaciones de seguridad.
Alta estabilidad de trabajo.	.
Comunidad abierta de desarrolladores, permite compilar tus propios paquetes y subirlos al sitio comunitario.	

Tabla 3. 1 Ventajas y desventajas de Suse Linux

RED HAT ENTERPRICE LINUX(RHEL)	
VENTAJA	**DESVENTAJAS**
Cuenta con un ambiente grafico de uso sencillo, siendo este muy útil tanto para usuarios expertos como principiantes.	Se debe ser parte un régimen de servicios o contar con una suscripción para tener acceso a un soporte completo del sistema.
Es compatible con la mayoría de arquitecturas de hardware.	Por cuestión de copyright se deja de contar con ciertas características del sistema.
De contarse con la suscripción debida, se tiene soporte y actualizaciones durante 7 o 10 años.	El sistema no cuenta con soporte a NTFS por defecto, pero si pude ser instalado si se lo desea.
Se cuenta con una mayor estabilidad y control	Se tienen costos en mantenimiento de seguridad y actualizaciones al no tenerse la suscripción.

El sistema demuestra un alto rendimiento en cuanto al funcionamiento de aplicaciones	
Permite mantener un control adecuado en cuanto a la optimización de recursos, tomando en cuenta que este sistema está enfocado a centros de datos y virtualización.	

Tabla 3. 2 Ventajas y desventajas de Red Hat Enterprise Linux

DEBIAN	
VENTAJAS	**DESVENTAJAS**
Distribución100% libre y gratuita.	Es necesario contar con conocimientos de Linux.
Actualmente Debian es un sistema de los más estables	El tiempo de lanzamiento entre versiones estables es demasiado largo
No es susceptible a virus o malwares.	El no contar con conocimientos de Linux puede dificultar su instalación.
Debian, posee miles de paquetes pre-compilados estables.	Es necesario realizar el montaje manual de dispositivos externos como por ejemplo una flash memory.
Gran estabilidad.	Kit de distribución muy conservador.
Desarrollo intenso con un gran control de calidad.	Versión del kernel relativamente antigua.
Gigantesca biblioteca de paquetes en sus repositorios.	La gestión democrática de sus proyectos conduce a soluciones ambiguas, esto causa conflictos en su comunidad de desarrolladores y paraliza el desarrollo del proyecto.
Soporte para muchas arquitecturas de procesador.	

Tabla 3. 3 Ventajas y desventajas Debian

CENTOS	
VENTAJAS	**DESVENTAJAS**
El estar basado en RedHat es posible tener muchas actualizaciones en cuanto a seguridad.	Es necesario contar con un conocimiento avanzado en Linux para un correcto manejo y mantenimiento del sistema.
Es un sistema de código abierto y libre de pago o suscripciones.	
CentOS se considera una distribución estable ,debido en parte a sus actualizaciones menos frecuentes.	

Cuenta con paneles de control se desea ofrecer servicios de alojamiento en la web	
Es altamente recomendado para empresas.	
CentOS se puede convertir en un sistema muy liviano si se instalan los servicios y paquetes únicamente necesarios.	
Toda su estructura está configurados para sacar el máximo provecho al hardware del servidor.	
Es un sistema sumamente robusto, debido a que sus actualizaciones son menos frecuentes.	
Se cuenta con 5 años para soporte y 10 años en cuanto a actualizaciones de tipo críticas .	
Es compatible con cPanel, Plesk y con CloudLinux	
La mayoría del software de seguridad licenciado se enfoca en RHEL/CentOS	
Posee una amplia comunidad, así como documentación y es compatible con la mayoría de documentación de RedHat.	
En cuanto a seguridad CentOS está entre los mejores	

Tabla 3. 4 Ventajas y desventajas de CentOS

UBUNTU	
VENTAJAS	**DESVENTAJAS**
Sistema de Código abierto	Ubuntu no es compatible con Cpanel
Se basa en la arquitectura Debian,	Se recomienda para principiantes
Cuenta con actualizaciones frecuentes para corregir errores existentes.	Actualizado frecuentemente

El centro de software de Ubuntu tiene más de 40,000 aplicaciones disponibles	Excesiva dependencia de Debian.
Seguridad de primer nivel	Las versiones no LTS, tan solo tienen 9 meses de soporte.
Paquetes DEB usando el administrador de paquetes	
Ciclos de lanzamiento fijo con buenos periodos de soporte.	
Gran documentación.	
Distribución generalista con una comunidad muy amplia.	
Tremendos repositorios y una amplia variedad de aplicaciones listas para su instalación.	
Es la distro linux que tiene más drivers compatibles ya compilados.	

Tabla 3. 5 Ventajas y desventajas Ubuntu

FEDORA	
VENTAJAS	**DESVENTAJAS**
Desarrollo: Patrocinado y financiado por Red Hat, es desarrollado por el proyecto Fedora	Debido a las pruebas de Rhel, lanza nuevas versiones en intervalos muy cortos
Distribución linux open source	Buena para estaciones de trabajos y servidores no críticos
Innovaciones constantes.	Al estar patrocinada por RedHat, las prioridades de Fedora se centran en resolver problemas corporativos, y no en los errores de las computadoras personales.
Excelentes características de seguridad.	Algunas implementaciones demasiado prematuras (vimos el ejemplo de KDE 4 y GNOME 3), que ahuyentaron a usuarios de escritorio.

Tabla 3. 6 Ventajas y desventajas Fedora

Luego de revisar las características, ventaja y desventajas que brindan cada una de las distribuciones Linux que se ha seleccionado, se ha encontrado como mejores opciones a Red Hat Enterprise y CentOS, pues ofrecen seguridad, estabilidad y están enfocadas a empresas lo cual permite tener las herramientas necesarias para contar con un servidor con muy buenas características técnicas. Finalmente, me he decidido en utilizar CentOS dado que básicamente

este es lo mismo que Red Hat Enterprise solo que no tiene ningún tipo de pago o suscripción que al momento es lo que más se apega a los solicitado por la Comision Fulbright del Ecuador, para la instalación se utilizará la última versión estable al momento que es CentOS 8.

3.2. Determinar software de red privada virtual a instalar

Luego de haber analizado las distribuciones de Linux y seleccionar la que va a ser instalada en el equipo, el mismo que va a trabajar como servidor proxy, firewall y VPN, es necesario realizar el estudio de las diferentes opciones que existen en cuanto a el sistema VPN que se instalará en el servidor.

Entre las opciones de VPN se encuentran:

LOGMEIN HAMACHI	
Descripción: Se trata de una aplicación comercial para redes privadas virtuales que establece vínculos directos entre computadoras que están bajo firewalls.	
VENTAJAS	**DESVENTAJAS**
Hamachi ha sido una de las mejores alternativas para poder crear una LAN virtual.	Quejas de algunos usuarios ha ido aumentado sobre picos de latencia y otros problemas.
Brinda una gran seguridad de conexión y una comunicación muy eficaz	Se trata de una solución gratuita que permite la asignación de una dirección IP para crear una red virtual hasta para cinco personas.
El software cifra las conexiones con protocolos AES de 256 bits	Se utiliza con planes de pago.
Si se dispone de acceso a Internet y el usuario tiene las credenciales apropiadas, puede hacer cambios y restablecer la red.	Al momento presenta muchos problemas de conexión.
Es compatible prácticamente con todas las versions de windows.	Es compatible únicamente en versión Beta con Linux y Mac OS X.
	Se desconoce las características de su funcionamiento a detalle

Tabla 3. 7 Características, ventajas y desventajas de Logmein Hamachi

SOFTETHER VPN	
Características: GNU GPL, inicio release 2013, desarrollado: SoftetherVPN project, University of Tsukuba, Japan, inicio como un proyecto de tesis en Japón.	
Se ejecuta en varias plataformas: Windows, Mac OS , Linux,Solaris, iOS y Android	SoftEtherVPN es conocido como algo más nuevo y complejo
Puede trabajar con diferentes protocolos: OpenVpn, L2TP/Ipsec, SSTP de Microsoft, VPN over HTTPS y muchos otros.	
Es un software libre de muy fácil instalación y gestión	
Establece VPN sobre el protocolo ICMP y DNS, burlando los dispositivos de seguridad que se encuentran en la red.	
Ofrece resistencia a la alta restricción de los firewalls,	
Cuenta con opción de traspasar firewalls con múltiples restricciones por medio del protocolo SSL/TLS VPN	
• Posee diversos métodos de encriptación, tales como AES 256-bit y RSA 4096.	
• Brinda características de seguridad, tal como logging y firewall internos dentro del túnel VPN.	
• Ofrece un throughput de 1Gbps, logrando tal rendimiento con poco consumo de memoria y de CPU.	

Tabla 3. 8 Características, ventajas y desventajas de SoftEther VPN

CISCO ANYCONNECT	
Características: Cisco AnyConnect es un agente unificado que presta numerosos servicios de seguridad para proteger la empresa. Esto significa que no solo proporciona acceso **VPN** mediante capa de conexión segura (**SSL**) e IPsec IKEv2, sino que también ofrece una seguridad mejorada mediante los distintos módulos integrados.	
Permite a los empleados trabajar sin importar su ubicación física desde equipos personales o corporativos.	Cisco AnyConnect tiene planes de suscripción: licencias a plazo (1,3 y 5 años) o licencias perpetuas. El precio empresarial depende también de la cantidad de usuarios o dispositivos a proteger

Acceso VPN mediante capa de conexión segura (SSL) e IPsec IKEv2.	
AnyConnect está disponible para una amplia gama de plataformas, por ejemplo, Windows, Mac OS X, Linux, iOS, Android, Windows Phone, BlackBerry y Google Chrome.	
Los appliances de seguridad adaptativa de Cisco proporcionan conectividad SSL a través de diversos navegadores en numerosas plataformas. Los administradores pueden proporcionar acceso VPN sin cliente a los terminales no gestionados y ofrecen acceso a varias aplicaciones web y basadas en TCP/IP	
Acceso a red muy seguro, AnyConnect Network Access Manager proporciona funciones de conectividad sobresalientes. Los administradores pueden controlar a qué redes o recursos se pueden conectar los terminales. Seguridad web.-Gracias a la combinación de la seguridad web con el acceso VPN, los administradores pueden proporcionar una movilidad altamente segura e integral a todos los usuarios finales.	
Ofrece la posibilidad de supervisar el uso de la aplicación a través del módulo AnyCOnnect Network Visibility en Windows y Mac	
Acceso de usuario completo	
perspectivas del comportamiento de usuarios y terminales	
Defensa contra amenazas	

Tabla 3. 9 Características, Ventajas y desventajas de Cisco AnyConnect

OPENVPN	
Características: Inicio release 2002, GNU GPL, Desarrollado por OpenVPN technologies	
VENTAJAS	**DESVENTAJAS**
Se trata un protocolo muy seguro.	La configuración puede ser algo difícil en algunas plataformas.

Puede utilizar claves de cifrado de 256 bits.	
El protocolo OpenVPN puede evitar de manera fácil cualquier firewall.	En ocasiones se pueden tener caídas de velocidad en la conexión por el cifrado seguro que maneja.
OpenVPN puede ser configurado tanto con protocolo TCP como UDP, lo cual permite mayor control en las conexiones	OpenVPN requiere para su funcionamiento que se ejecuten aplicaciones de terceros.
OpenVPN se ejecuta prácticamente todas las plataformas.	
La autenticación se puede hacer de forma muy cómoda mediante el nombre de usuario y la contraseña, además de que se puede configurar una Clave Pública (PKI).	
Hay muchos tutoriales disponibles en los que puedes aprender a sacarle el máximo provecho a OpenVPN	

Tabla 3. 10 Características, ventajas y desventajas de OpenVPN

Analizadas las tablas de características, se ha llegado a tener como posibles alternativas a SoftEther y OpenVPN, dadas todas las características que se tienen en los dos sistemas, por lo que fue necesario analizar más a fondo estas dos opciones y encontrar un diferencial que permita elegir un sistema para poder instalar y configurar en el servidor la mejor alternativa.

"OpenVPN es tanto un protocolo VPN como un software que utiliza técnicas VPN para asegurar conexiones punto a punto y de sitio a sitio. Actualmente, es uno de los protocolos VPN más populares entre los usuarios de VPN" (Cactusvpn, 2019).

Además, se indica que también:

> Este protocolo hace uso de la seguridad de SSL/TLS para dotar de seguridad a las comunicaciones, utiliza tanto un canal de control que usa TLS, como un canal de datos con AES-256-GCM para tener la máxima seguridad.
>
> Además, la autenticación se puede realizar con el típico usuario/contraseña, o también se podrá configurar una Infraestructura de Clave Pública (PKI) con certificados digitales. (Redeszone.net, 2020)

Es decir, Openvpn es un protocolo de código abierto que además cuenta con su propia aplicación igual dicha aplicación de código abierto, y es uno de los sistemas más seguros dada la encriptación y autenticación que permite configurar.

Se tiene igualmente:

> En resumen, las redes privadas virtuales se han vuelto populares y hay toda una ciencia que las respalda. Depende de usted tratar de comprenderlos tanto como sea posible y, finalmente, encontrar la combinación que más le convenga. Cuando se trata de elegir entre SoftEther VPN y OpenVPN, recomiendo de todo corazón el primero por el hecho de que es más nuevo y más rápido, además de todas las demás ventajas que tiene. Por otro lado, OpenVPN no debe olvidarse, ya que también tiene sus propios beneficios: es prácticamente configurable y el nivel de cifrado y seguridad es muy alto. En otras palabras, si prefiere estable y tradicional, es posible que desee elegir OpenVPN (LimeVpn, 2020).

En conclusión, la razón principal para usar el sistema OpenVPN es porque es muy seguro dado su nivel de cifrado, realmente estable, siendo configurable y además una opción transparente debido a que es de código abierto y funciona en múltiples plataformas, no debiendo olvidarnos que maneja su propio protocolo y que además se cuenta con una comunidad que está a cargo del desarrollo y actualizaciones necesarias.

3.3. Determinar los servicios adicionales y herramientas de seguridad

En vista de que luego del análisis de los sistemas operativos se decidió utilizar la distribución de Linux CentOS en su versión 8 y el software de red privada virtual que se instalará y configurará es OpenVPN al ser una de los sistemas VPN más seguros, además de ser tanto una aplicación como un protocolo, es necesario establecer los servicios adicionales y las seguridades que deben implementarse.

3.3.1. Servicio de Firewall (Muro Cortafuegos)

El equipo que en el que se va a instalar y configurar OpenVPN, también dará la cara al internet, por lo que es necesario instalar un firewall que permita:

"Proteger a la red privada, de una gran cantidad de intrusiones o ataques que pueden producirse desde otras redes, este firewall también puede bloquear el acceso, se debe permitir el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red. (ID Group, 2020)

Como servicio de firewall se instalará y configurará firewallD, dado que en instalaciones que he realizado anteriormente ya he podido trabajar con iptables, lo que me ha permitido conocer de todas sus ventajas y firewallD utiliza como base a iptables.

3.3.2. Servicio de Proxy de internet

Se debe igualmente tomar en cuenta que al estar este equipo conectado al internet se debe configurar el servicio proxy para que puedan acceder a internet todos los computadores de la red local, por lo cual se ha decidido instalar y configurar squid proxy, este servicio permite tener un sistema de cache lo cual agiliza el acceso a las páginas web dado a los usuarios una experiencia de velocidad y estabilidad, igualmente permite diferentes configuraciones de acceso sea este acceso o bloqueo por páginas, navegación a grupo de equipos o grupos de red, navegación por horarios entre algunas de las facilidades, como algo importante de squid es que permitirá tener un proxy transparente lo que evitará realizar configuración alguna a cada uno de los equipos para que la navegación sea enrutada al nuevo equipo servidor de manera automática.

3.4. Diseño gráfico de la red a implementarse

En la figura 3.1 se puede observar el diseño de la red vpn a implementarse.

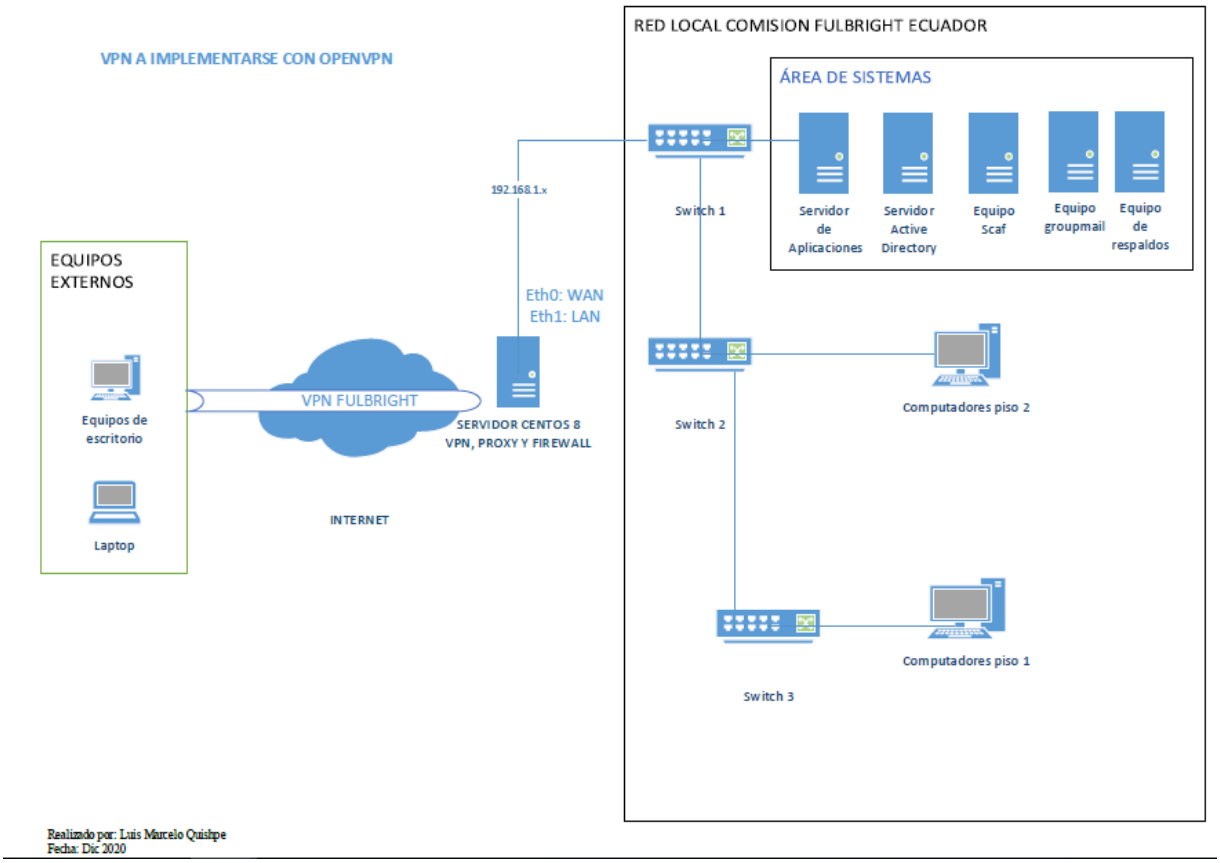

Figura 3. 1 Diseño Vpn a implementarse en la Comision Fulbright del Ecuador.

3.5. Clientes VPN a crearse

De acuerdo a los requerimientos indicados por la institución será necesario crear los siguientes usuarios, los mismos que deberán tener acceso remoto a los siguientes servicios, ver tabla 3.11

CLIENTE VPN	Usuario	área	Uso	Carpeta compartida
Client01	mlogana	sistemas	Escritorio Remoto	Comful
Client02	kaguilar	Staff	Escritorio Remoto	Comful
Client03	rracines	Staff	Escritorio Remoto	Comful
Client04	mmantilla	Staff	Escritorio Remoto	Comful
Client05	eteran	staff	Escritorio Remoto	Comful

Client06	ksoto	Etp	Escritorio Remoto	Comful
Client07	mnaranjo	Directora		Comful
Client08	llincango	contador	Escritorio Remoto	Comful
Client09	lmquishpe	sistemas	Escritorio Remoto	Comful
Client10	clara	contador externo	Escritorio Remoto	Comful
Client11	glandeta	recepción	Escritorio Remoto	Comful

Tabla 3. 11 Listado de Clientes VPN

4. IMPLEMENTACIÓN DE LA RED PRIVADA VIRTUAL

4.1. Descripción de equipos

Luego de haber seleccionado la distribución de CentOS 8, es necesario proceder con la instalación y configuración del mismo.

Al momento la Comision Fulbright del Ecuador adquirió un computador nuevo conforme los requerimientos técnicos solicitados en el informe de características de los equipos a utilizarse en el capítulo 2, dado que el computador anterior ya cumplió con su tiempo de vida útil, se debe destacar que este computador debe contar con dos tarjetas de red, la primera se conectará al ISP para enlazar el servicio de internet y la segunda deberá conectarse al switch de la red local.

De igual manera se adquirieron 4 laptop, para que parte de los funcionarios que no contaban con equipos en sus hogares puedan conectarse a la VPN y realizar teletrabajo

En la figura 4.1 se observa el equipo ensamblado con las dos tarjetas de red colocadas.

Figura 4. 1 Computador a ser utilizado como Servidor VPN, Firewall y Proxy

En la figura 4.2 se puede observar las laptops adquiridas y sobre las cuales se configurará el cliente Openvpn.

Figura 4. 2 Modelo de Laptop en la que se instalará el cliente OpenVPN

4.2. Instalación y configuración del sistema operativo Linux

Fue necesario realizar la descarga de CentOS 8 desde internet y se generó un USB de arranque para poder iniciar con la instalación.

Se enciende el computador con el USB de arranque que se generó, y se selecciona como opción de inicio el USB.

Crear USB de arranque para instalar Centos 8.1

Para crear un USB de arranque se eligió utilizar RaWrite32 y se lo instaló en un computador figura 4.3, figura 4.4 y figura 4.5

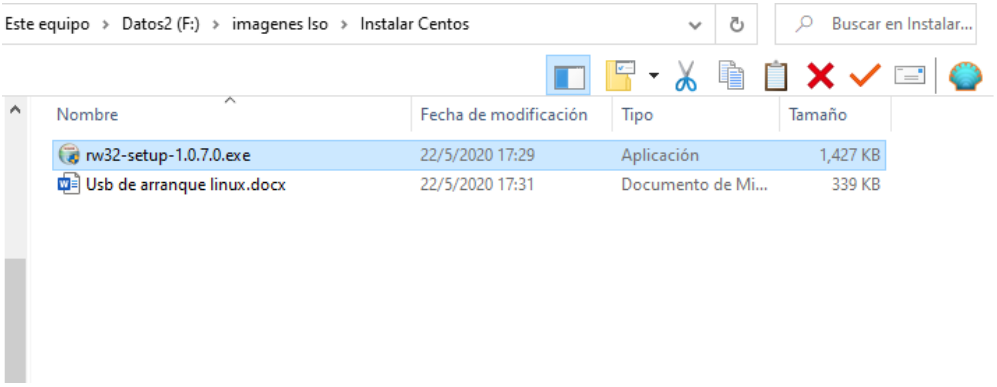

Figura 4. 3 RaWrite, Aplicación para generar USB de arranque

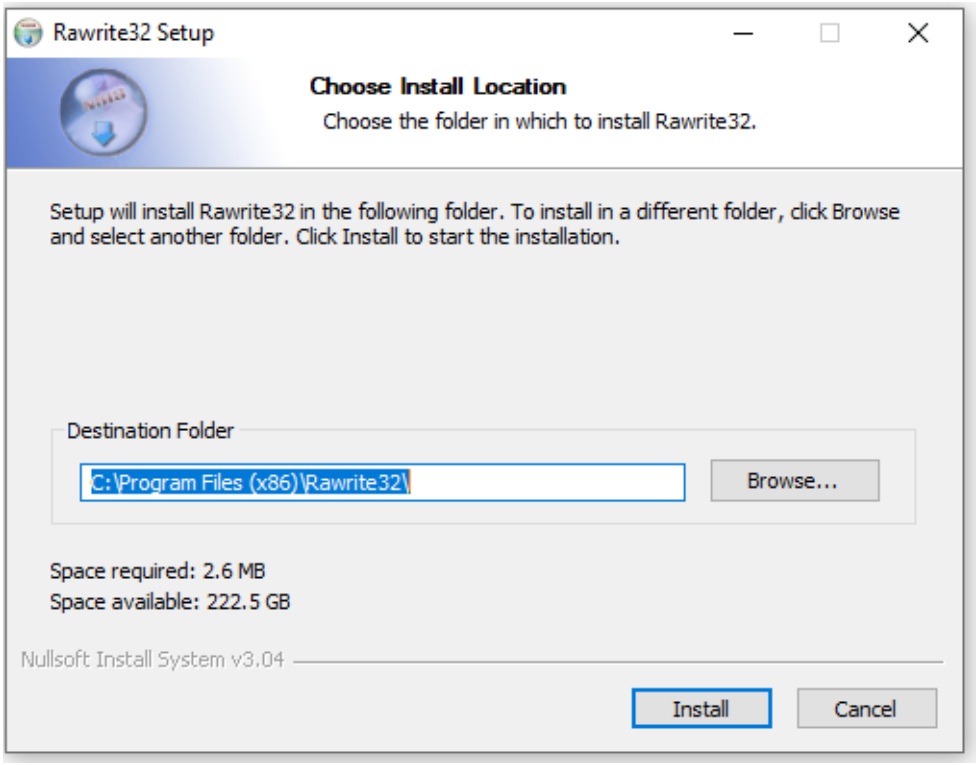

Figura 4. 4 Selección del destino de la instalación

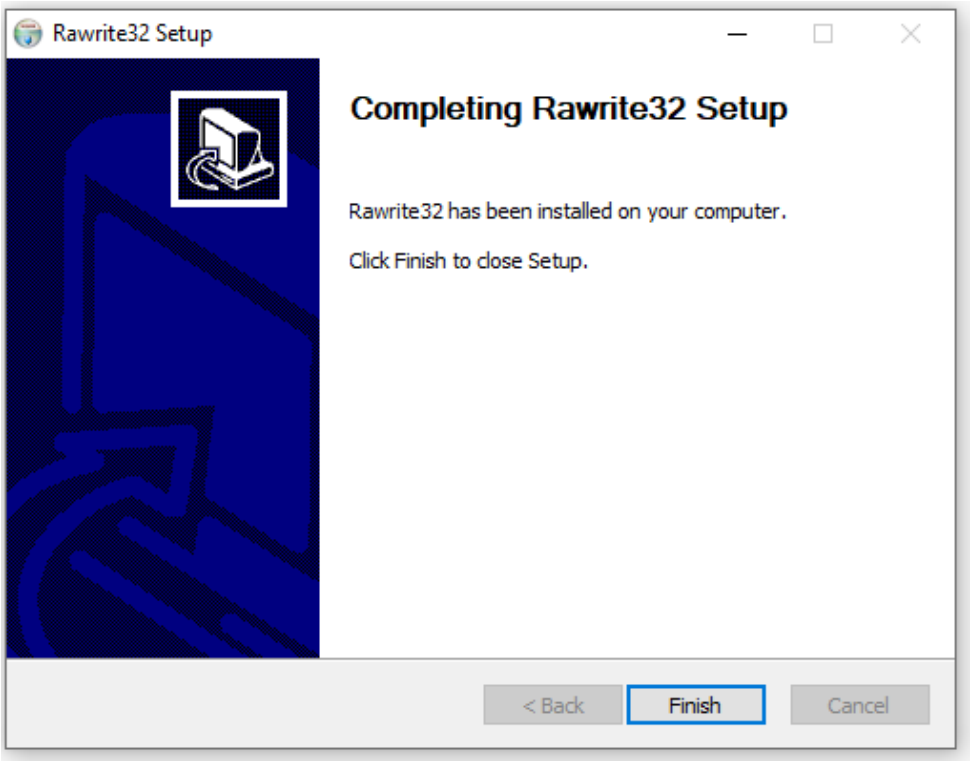

Figura 4. 5 Rawrite32 instalación finalizada

Una vez instalada, se debe ejecutar la aplicación, se selecciona la unidad USB y el archivo ISO para generar el arranque desde USB, como se observa en la figura 4.6.

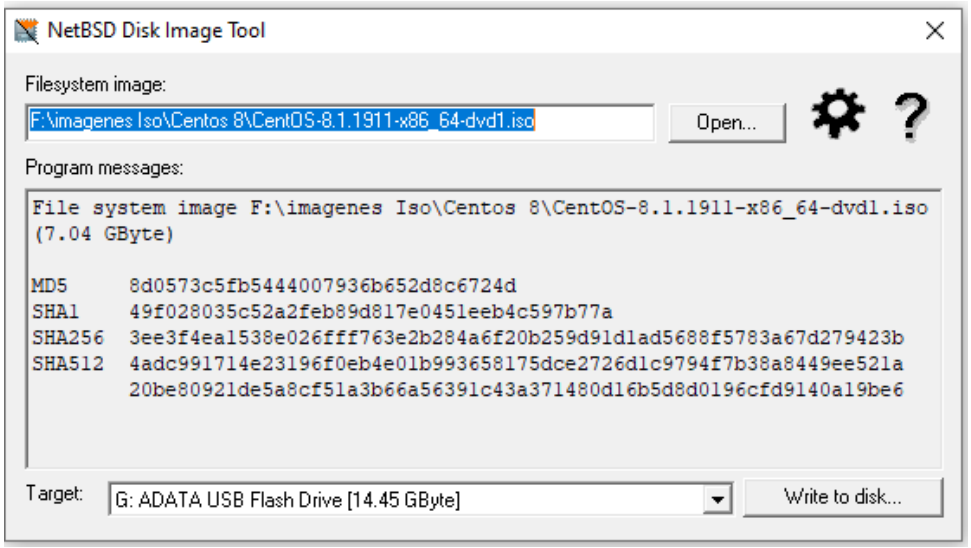

Figura 4. 6 Crear usb de arranque con la imagen de CentOS 8

Se debe dar click en write to disk y esperar a que termine el proceso.

Pasos seguidos para instalar Centos 8.

Se inicia el equipo colocando la usb de arranque y se espera a que el arranque sea reconocido, en ocasiones va a ser necesario configurar el bios del computador para que realice el inicio desde los puertos usb.

En la figura 4.7 se puede observar la pantalla con la que se inicia la instalación de Centos, se seleccionará: **Install Centos linux 8.**

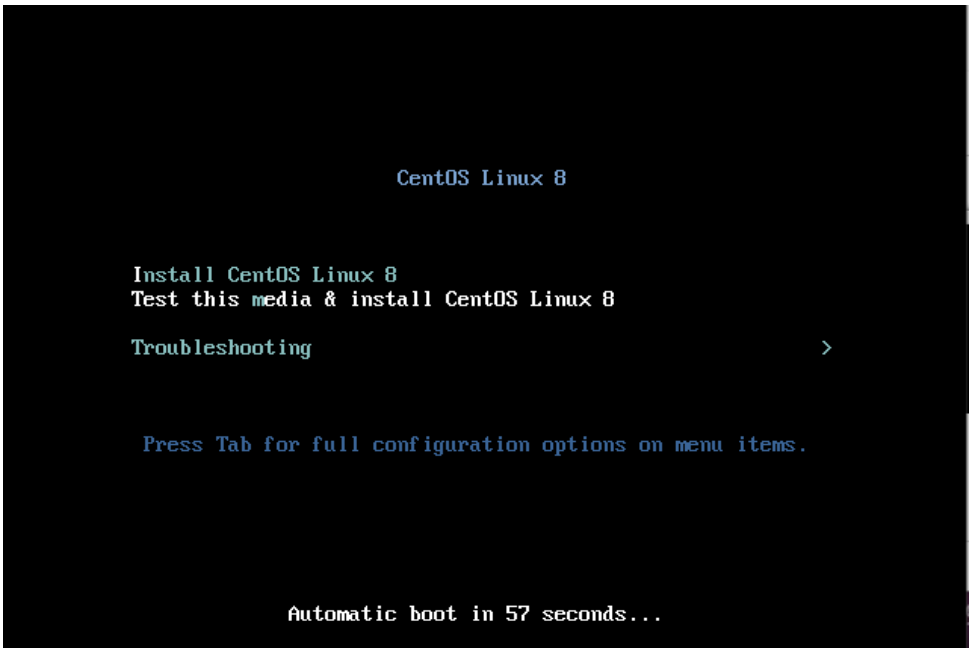

Figura 4. 7 Pantalla inicial de instalación de CentOS 8

Se selecciona el Idioma a utilizarse durante la instalación como indica la figura 4.8

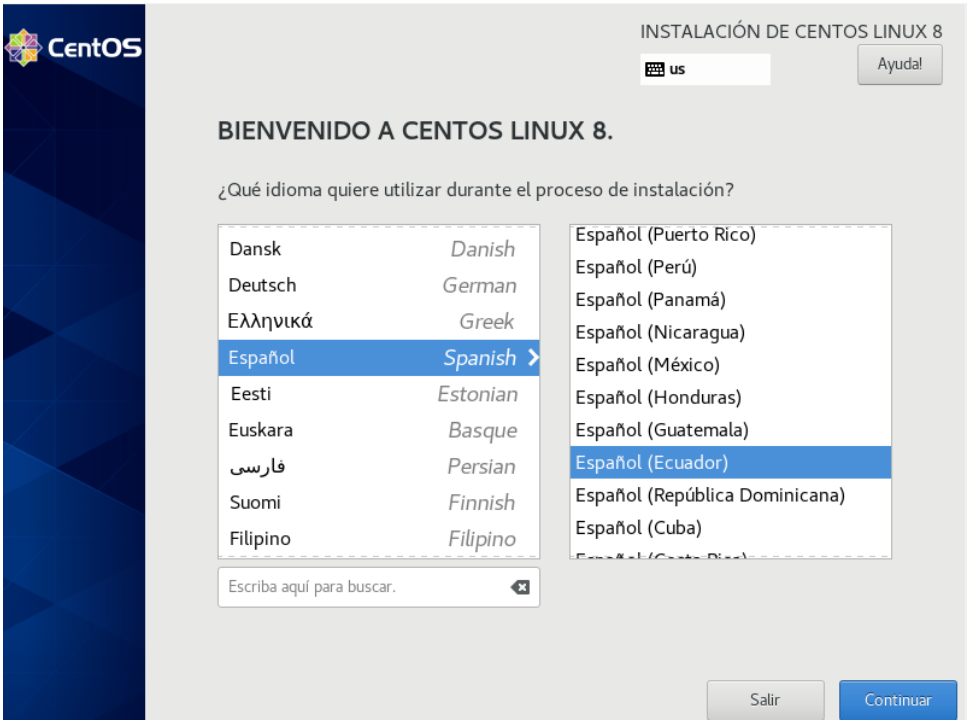

Figura 4. 8 Selección del idioma de instalación

En la siguiente ventana será posible configurar lo siguiente:

- Distribución del teclado.
- Fecha y hora.
- Fuente de la instalación.
- Seleccionar el software a instalar.
- Destino de la instalación.
- Kdump.

Se selecciona el icono con el símbolo de advertencia, en este caso se debe seleccionar el destino de la instalación ver figura 4.9.

Figura 4. 9 Resumen de instalación CentOS 8.

Es necesario configur la región, fecha y hora ver figura 4.10

Figura 4. 10 Configurar Región, fecha y hora

Se selecciona configuración de almacenamiento personalizada y se presiona "Hecho", ver figura 4.11

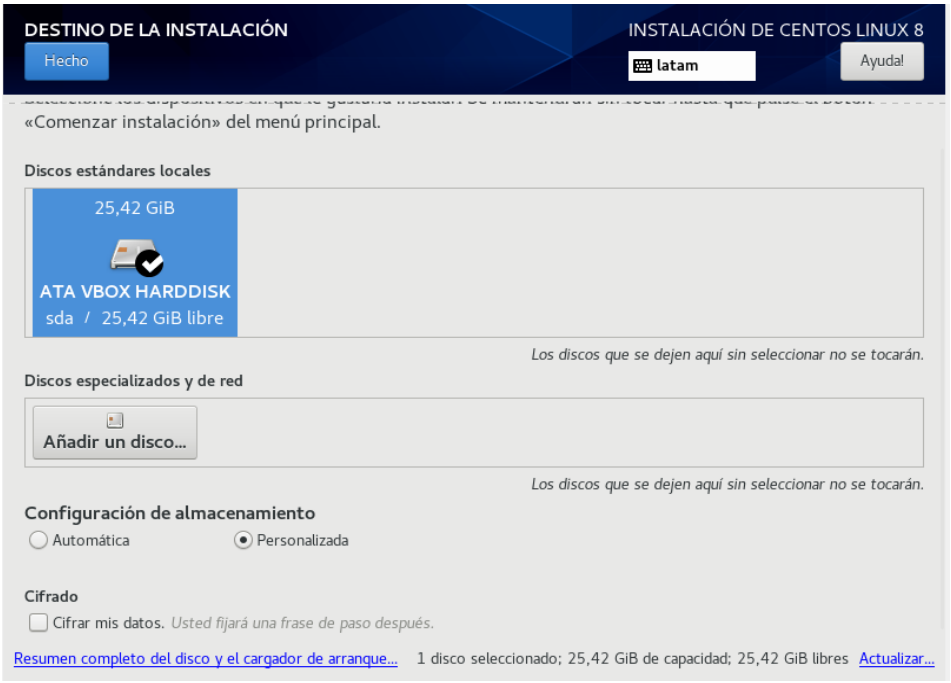

Figura 4. 11 Selección de destino de instalación

Como se observa en la figura 4.12, se realiza la creación de las particiones de forma manual, cabe indicar que también se puede realizar las particiones de forma automática.

Figura 4. 12 Particionado manual

Se agregan para este caso 3 particiones, ver figura 4.13:

- /
- /boot
- Swap

Se puede crear también si se lo considera necesario /home, /usr y otras, caso contrario estos directorios se crearán bajo /

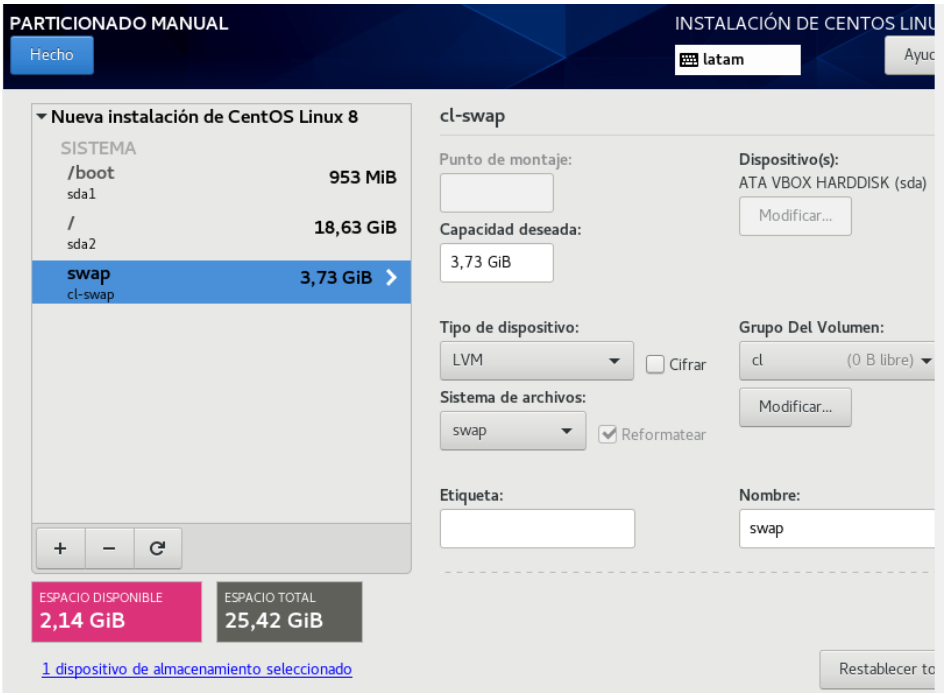

Figura 4. 13 Detalle de particiones creadas.

Como se indica en la figura 4.14, se configura los parámetros de la red wan y lan, esto se puede realizar igualmente una vez finalizada la instalación de CentOS.

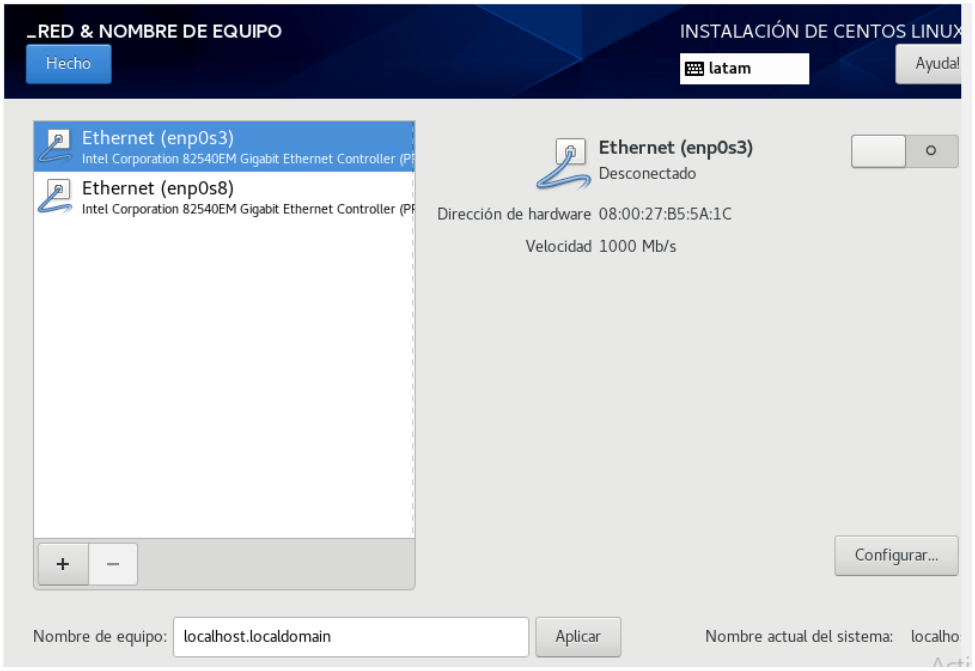

Figura 4. 14 Configuración de los dispositivos de red

Se selecciona el tipo de servidor, así como los paquetes que se van a instalar como se observa en la figura 4.15.

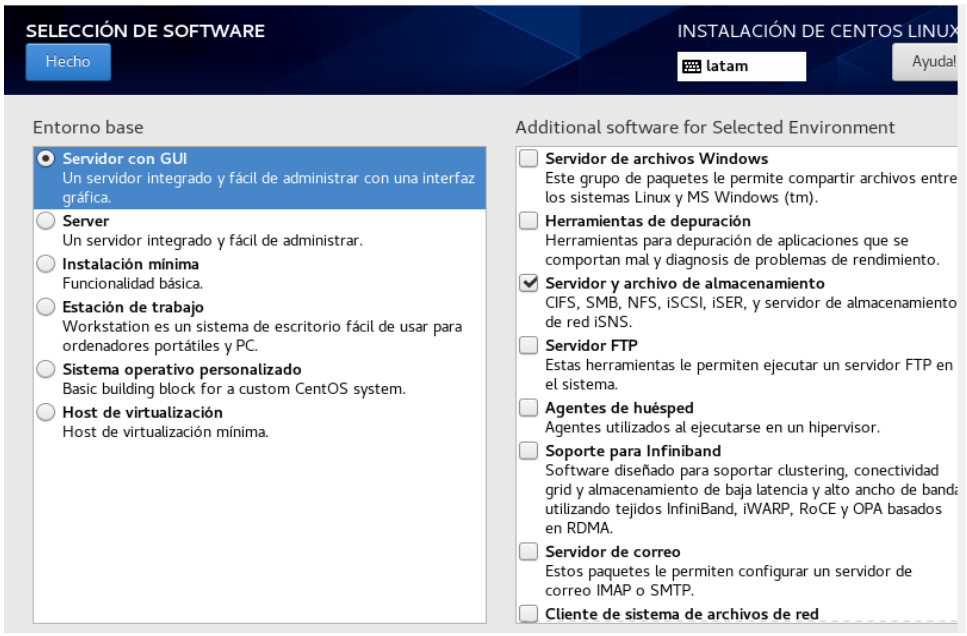

Figura 4. 15 Selección de tipo de servidor y paquetes CentOS

Luego de configurar los parámetros de instalación se presiona en empezar instalación, ver figura 4.16

Figura 4. 16 Resumen final de instalación

Como se puede ver en la figura 4.17 y figura 4.18, es necesario crear la contraseña del usuario root, que es el administrador de Linux.

Figura 4. 17 Ajustes de usuario

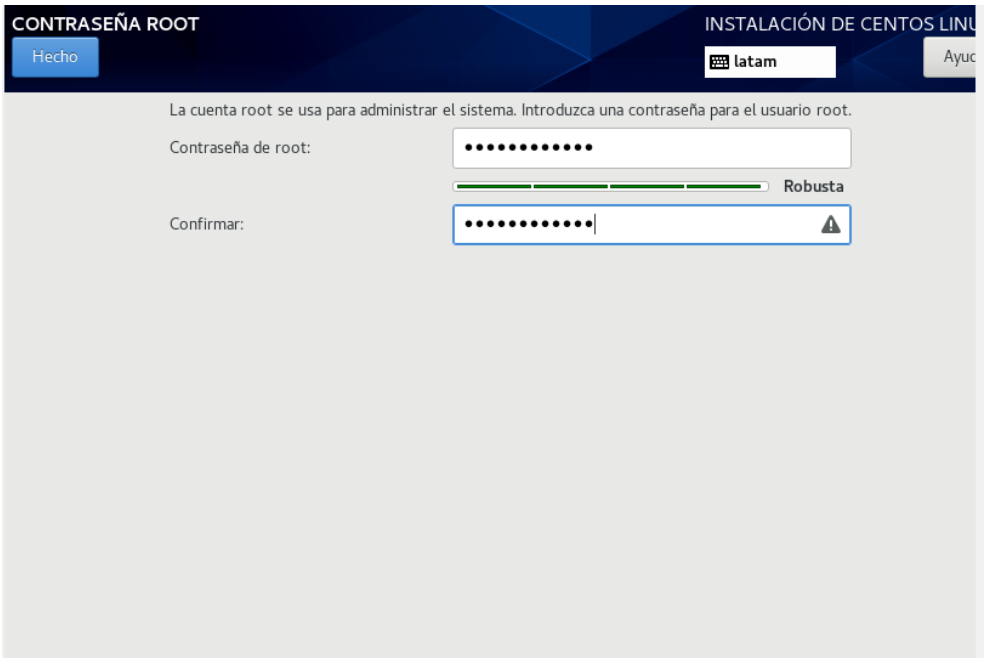

Figura 4. 18 Registro de contraseña de cuenta root

Al finalizar la instalación de paquete y reiniciar el equipo, el sistema solicitará aceptar la licencia ver figura 4.19 y figura 4.20

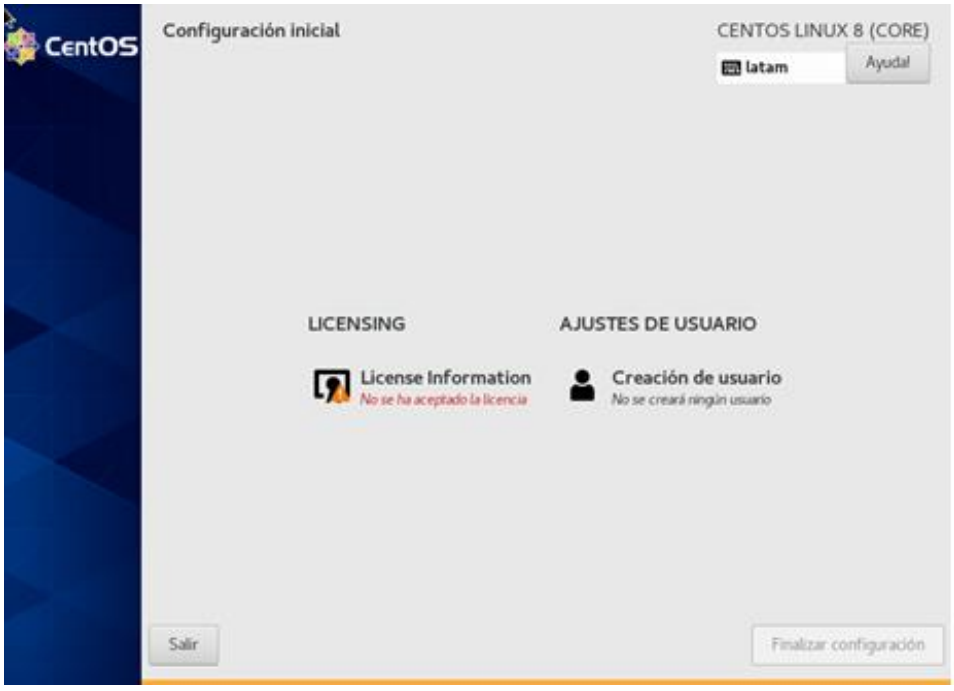

Figura 4. 19 Configuración Inicial

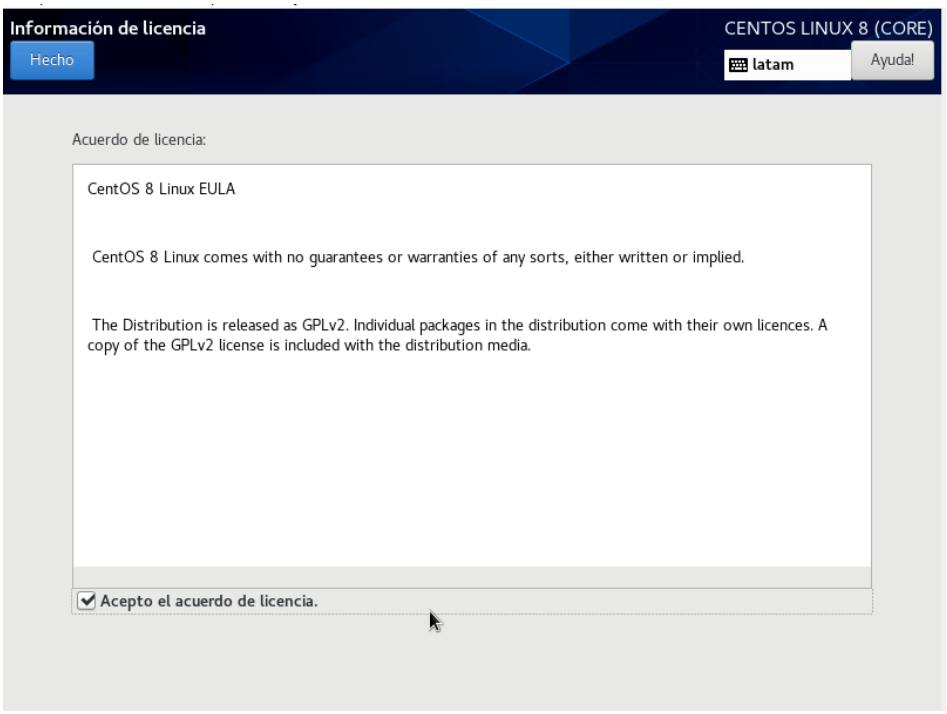

Figura 4. 20 Acuerdo de licencia CentOS Linux 8

Para finalizar es necesario continuar con unos pasos adicionales como se puede observar en los gráficos siguientes.

El sistema muestra una pantalla de bienvenida, ver figura 4.21

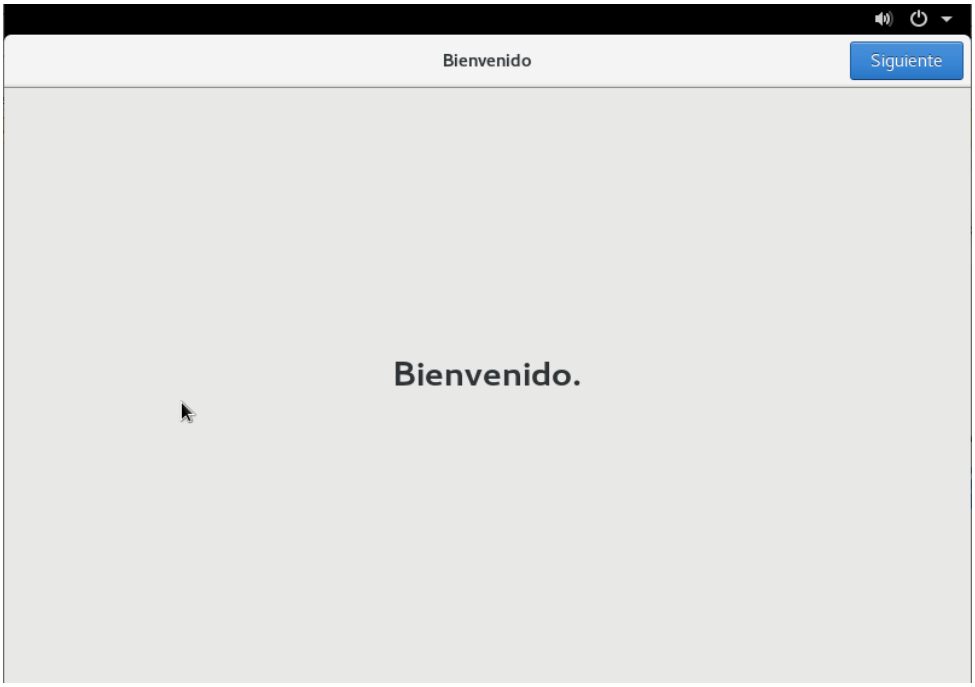

Figura 4. 21 Pantalla de bienvenida CentOS

Se presiona en siguiente en la pantalla de privacidad que permite habilitar los servicios de ubicación si son necesarios. ver figura 4.22

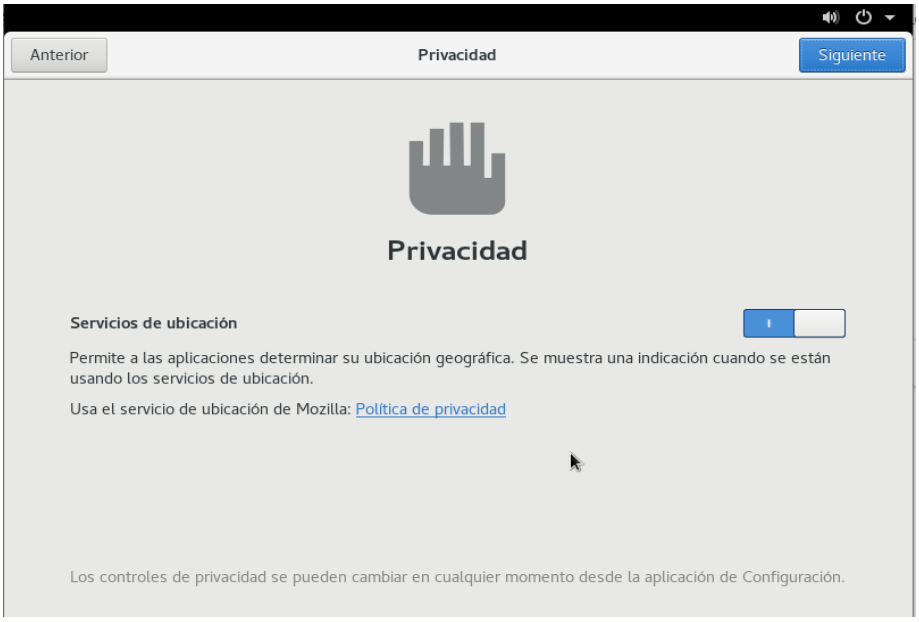

Figura 4. 22 Pantalla de privacidad, servicios de ubicación CentOS

Si se desea, se puede configurar las cuentas en línea como se puede observar en la figura 4.23

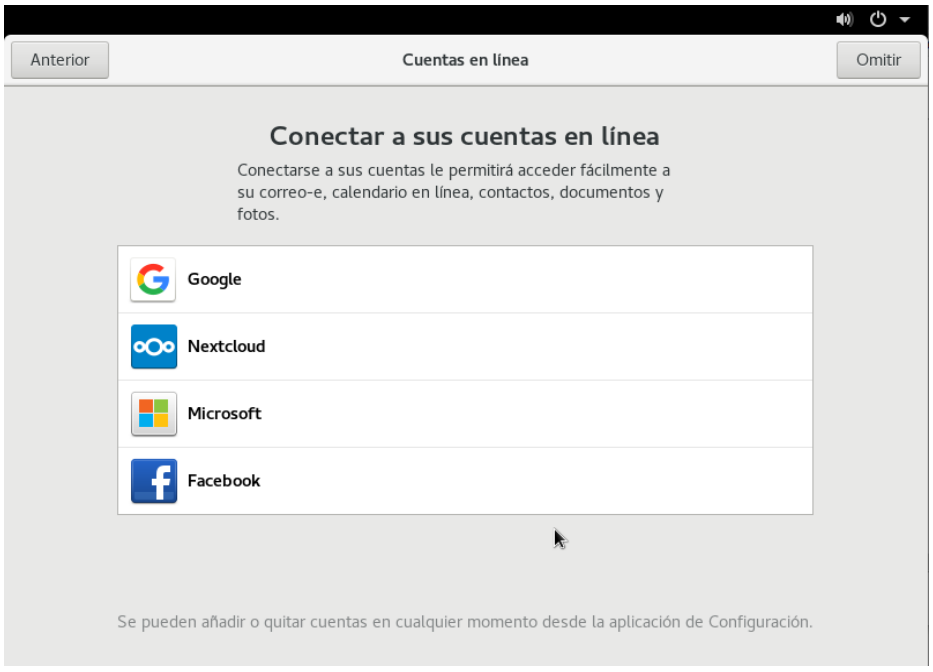

Figura 4. 23 Configurar cuentas en línea

Finalmente se puede configurar un usuario y contraseña para el usuario no root, ver figura 4.24 y figura 4.25

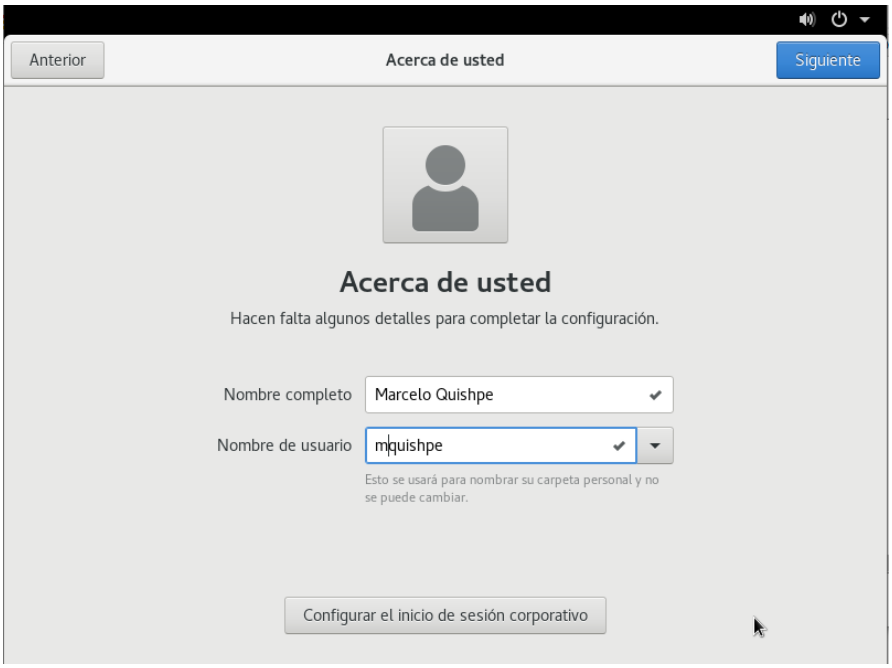

Figura 4. 24 Pantalla de creación e usuario no root

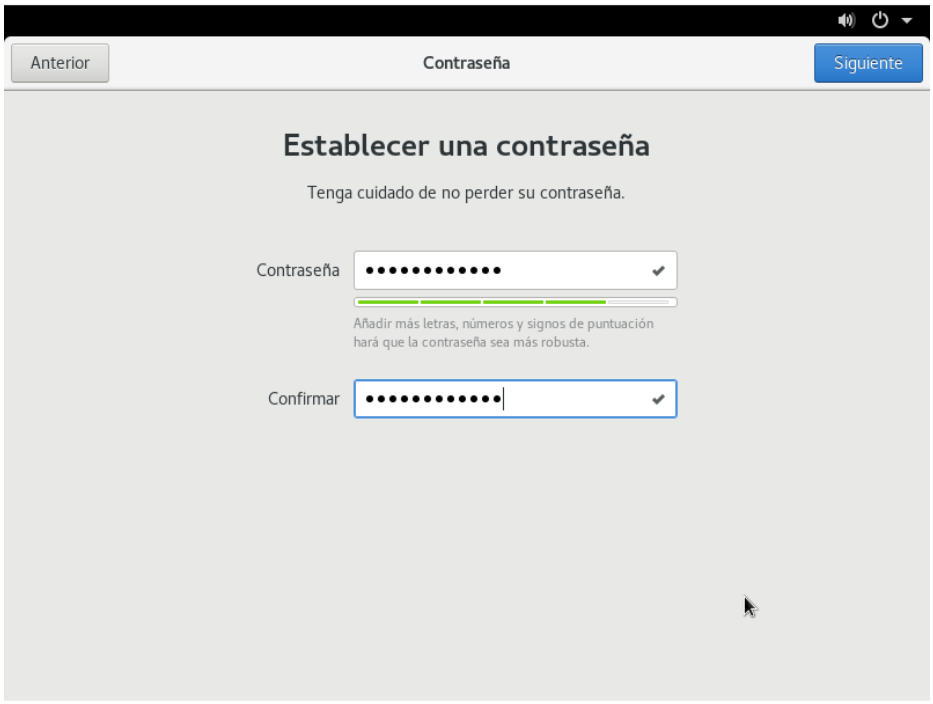

Figura 4. 25 Establecer contraseña.

Con esto se finalizó la instalación de CentOS, como se observa en las figuras 4.26 y 4.27

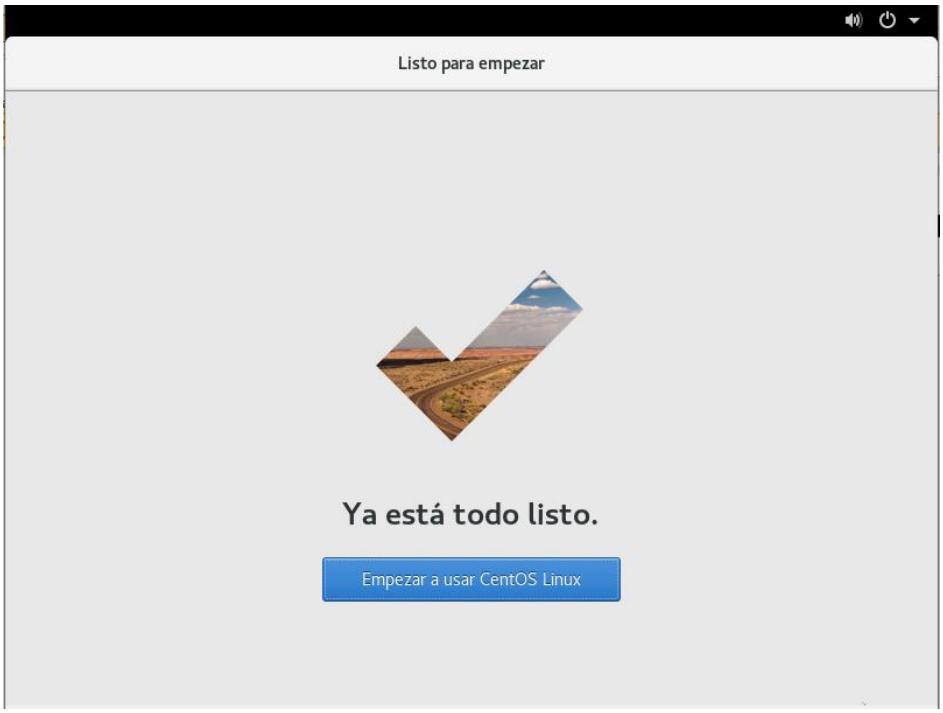

Figura 4. 26 Instalación de CentOS 8 finalizada con éxito

Figura 4. 27 Pantalla de ingreso a CentOS 8

4.3. Instalación y configuración del firewall

Como FirewallD viene preinstalado en CentOS 8, pero es necesario activarlo pues por defecto está desactivado.

Desde este momento es necesario conocer la importancia de saber utilizar el terminal de Linux.

"El **Terminal de Linux** es una consola, similar a CMD o PowerShell(pero mucho más avanzada que ambas), utilizada para permitir a los usuarios más avanzados y técnicos controlar hasta el más mínimo detalle del sistema operativo" (Softzone.es, 2020).

Por medio de esta consola se debe ejecutar los comandos para realizar las configuraciones necesarias en Linux, ver figura 4.28.

Figura 4. 28 Terminal Linux

Lo siguiente permite iniciar el servicio.

sudo systemctl start firewalld

Con este comando se activa el servicio.

sudo systemctl enable firewalld

Se puede ver si firewalld está ejecutándose o no por medio de, ver figura 4.29:

sudo firewall-cmd –state

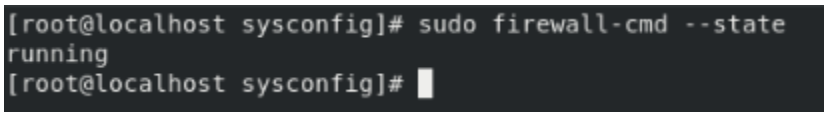

Figura 4. 29 Consultar el estado de firewalld

Con systemctl status firewalld, se puede ver el estado del demonio de firewalld, ver figura 4.30

```
[root@localhost sysconfig]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-11-30 09:37:53 -05; 1 months 6 days ago
     Docs: man:firewalld(1)
 Main PID: 1733 (firewalld)
    Tasks: 2 (limit: 26213)
   Memory: 38.4M
   CGroup: /system.slice/firewalld.service
           └─1733 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid
```

Figura 4. 30 Consultar el estado del demonio de firewalld

De acuerdo a lo investigado firewalld administra las reglas por medio de zonas y según lo mencionado por (DigitalOcean, 2020) " El demonio firewalld gestiona grupos de reglas usando entidades denominadas *zonas*. Las zonas son conjuntos de reglas que determinan el tráfico que debe permitirse según el nivel de confianza en la red. Se asignan interfaces de red a las zonas para indicar qué comportamientos debe permitir el firewall."

Con el siguiente comando se puede consultar las zonas activas.

sudo firewall-cmd --get-active-zones

Es necesario empezar configurando las zonas con las que el firewall va a trabajar, en este caso se utilizará las zonas externa e interna.

Se asignará la tarjeta de red incorporada a la tarjeta madre a la zona externa y la tarjeta de red instalada en el socket pci express se asignará a la zona interna.

sudo firewall-cmd --zone=externa --add-interface=eno1 --permanent

sudo firewall-cmd --zone=interna --add-interface=enp1s0 –permanent

En figura 4.31, consulta nuevamente las zonas activas.

```
[root@localhost ~]# sudo firewall-cmd --get-active-zones
external
  interfaces: eno1
internal
  interfaces: enp1s0
libvirt
  interfaces: virbr0
[root@localhost ~]#
```

Figura 4. 31 Consultar zonas activas

La tarjeta externa se configura en modo DHCP, para que el momento que se conecte al ISP, este se encargue de asignarle la IP pública contratada, esto se puede cambiar en: /etc/sysconfig/network-scripts/ifcfg–eno1, ver figura 4.32

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eno1
UUID=27ba8ee1-b84a-4564-ae94-7ba2819f683b
DEVICE=eno1
ONBOOT=yes
ZONE=external
HWADDR=70:85:C2:FE:91:01
~
~
```

Figura 4. 32 Configuración de la tarjeta de red eno1- conectada al ISP

En la figura 4.33 se muestra la IP asignada pública asignada vía DHCP por el proveedor ISP, se debe digitar ipconfig.

```
[root@localhost ~]# ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 181.199.73.159  netmask 255.255.255.0  broadcast 181.199.73.255
        inet6 2800:bf0:1fff:f061:7285:c2ff:fefe:9101  prefixlen 64  scopeid 0x0<
```

Figura 4. 33 Información de la IP conectada a internet.

Si se ejecuta [root@localhost ~]# vim /etc/sysconfig/network-scripts/ifcfg-enp1s0

Se debe ingresar al archivo de configuración de la tarjeta de red que se va a conectar al switch de la red local y aquí se configurar la IP interna y la máscara de red, como se ve en la figura 4.34

IP: 192.168.1.100

MASK: 255.255.255.0 o 24

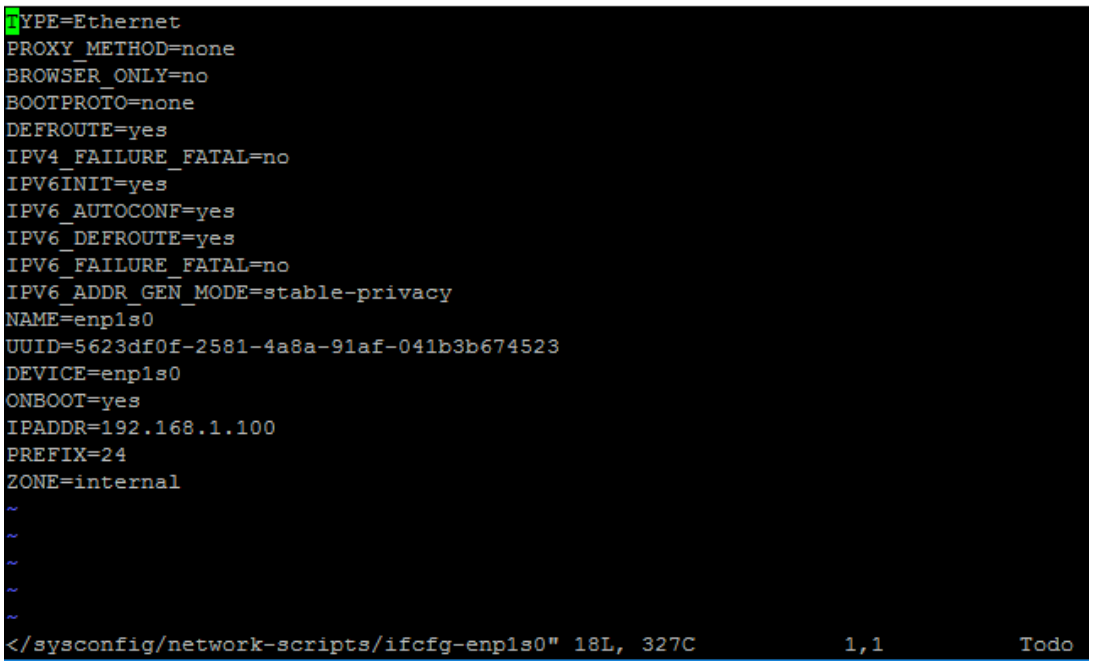

Figura 4. 34 Archivo de configuración de tarjeta de red conectada a la red local

En la figura 4.35 se muestra la IP configurada en el paso anterior, para esto se debe digitar **ipconfig** en el terminal de Linux.

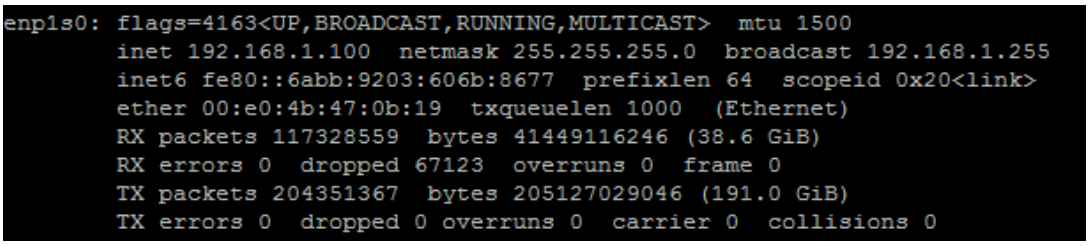

Figura 4. 35 Configuración de la tarjeta de red local

A continuación, se debe habilitar en la zona externa e interna los puertos y los servicios que se considere necesarios para los servicios que va a brindar el servidor Linux, posteriormente se habilitarán otros servicios, puertos y redireccionamientos conforme se vayan instalando los servicios de openvpn y squid proxy.

Se habilita en la zona externa el puerto 2222 para poder conectarme de forma remota al equipo centOS y se realiza el forward de dicho puerto al puerto 22(servicio ssh), ver figura 4.36 y figura 4.37

```
[root@localhost sysconfig]# sudo firewall-cmd --zone=external --add-port=2222/tcp --permanent
```

Figura 4. 36 Comando para adicionar el puerto 2222 a la zona externa

```
[root@localhost sysconfig]# sudo firewall-cmd --zone=external --add-forward-port=port=2222:proto=tcp:topor
t=22 --permanent
```

Figura 4. 37 Comando para adicionar forward del puerto 222 al puerto 22 para acceso ssh..

Se habilita en la zona externa el puerto 443 para permitir las conexiones https (puerto seguro), ver figura 4.38

```
[root@localhost ~]# sudo firewall-cmd --zone=external --add-port=443/tcp --permanent
```

Figura 4. 38 Habilitar en red externa el puerto 443, https

Es necesario volver a cargar firewalld para que los cambios tomen efecto, ver figura 4.39

```
[root@localhost ~]# firewall-cmd reload
```

Figura 4. 39 Comando para volver a cargar firewalld

Firewall-cmd reload, elimina cualquier configuración que se encuentre en ejecución y aplica la configuración que se ha almacenado como permanente, esto no interrumpe las conexiones y sesiones que se encuentren establecidas.

4.4. Instalación y configuración del proxy de internet

Se inicia con la instalación de squid, para esto se debe ejecutar en el terminal lo siguiente para asegurarnos que se encuentre actualizado el sistema de paquetes, ver figura 4.40, es necesario asegurarse primero que se tiene acceso a internet para que pueda realizar dicha actualización.

```
[root@localhost ~]# sudo dnf update
CentOS-8 - AppStream                            6.7 kB/s | 4.3 kB     00:00
CentOS-8 - Base                                 6.5 kB/s | 3.9 kB     00:00
CentOS-8 - Extras                               1.1 kB/s | 1.5 kB     00:01
Extra Packages for Enterprise Linux Modular 8 -  52 kB/s |  60 kB     00:01
Extra Packages for Enterprise Linux 8 - x86_64   71 kB/s |  60 kB     00:00
Dependencias resueltas.
================================================================================
 Paquete                        Arq.   Versión                 Repo       Tam.
================================================================================
Instalando:
 centos-linux-release           noarch 8.3-1.2011.el8          BaseOS     22 k
     se sustituye  centos-release.x86_64 8.1-1.1911.0.9.el8
     se sustituye  centos-repos.x86_64 8.1-1.1911.0.9.el8
 kernel                         x86_64 4.18.0-240.1.1.el8_3    BaseOS    4.3 M
 kernel-core                    x86_64 4.18.0-240.1.1.el8_3    BaseOS     30 M
 kernel-devel                   x86_64 4.18.0-240.1.1.el8_3    BaseOS     17 M
```

Figura 4. 40 Comando para actualizar sistema de paquetes

Como se puede observar la figura 4.41, dado que squid está por defecto en los repositorios de CentOS, solo se debes ejecutar el siguiente comando para que se instale squid y todos los paquetes necesarios para que funcione sin problemas.

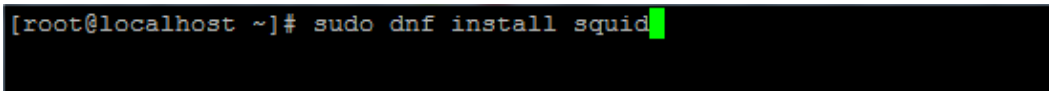

Figura 4. 41 Comando para iniciar realizar la instalación de squid

Con el comando que se muestra en la figura 4.42 se habilitas el servicio squid.

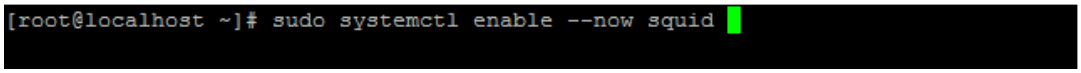

Figura 4. 42 Comando para habilitar el servicio squid

Squid cuenta con un archivo tipo texto denominado squid.conf que está ubicado en /etc/squid, el mismo que se recomienda respaldarlo antes de realizar cambios al mismo.

cp /etc/squid/squid.conf /etc/squid/squid.conf.bak

Se ingresa al archivo squid.conf para editarlo, ver figura 4.43

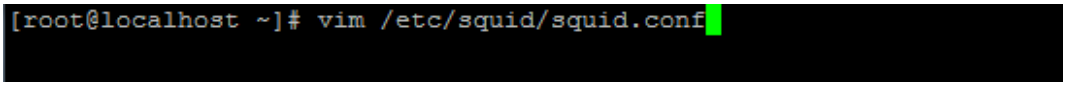

Figura 4. 43 Comando para ingresar a editar el archivo squid.conf

Se crea una lista de control de acceso para definir la red local que utilizará squid como proxy.

acl fulbright src 192.168.1.0/24 # Red local fulbright

Esto crea una" variable" acl con el nombre fulbright con esto se especifica los hosts de red que van a utilizar el servicio de proxy.

Una vez definida la ACL, se debe adicionar una línea donde se hace referencia al ACL fulbright para permitirle el acceso, para esto se debe utilizar http_access para permitir o negar el acceso a los navegadores.

http_access allow fulbright

Esta línea debe ser colocada antes de http_access deny all, pues squid lee la configuración de arriba hacia abajo por esto el orden en el que se colocan la configuración es importante.

Squid por defecto escucha las peticiones por el puerto 3128, como necesito tener un proxy transparente voy a utilizar de forma adicional el puerto 3129 intercept para esta tarea, para esto lo agrego en una línea de esta manera:

http_port 192.168.1.100:3128

http_port 3129 intercept

Es importante para este caso no quitar el puerto 3128, pues esto causa problemas y evita que squid funcione como proxy transparente, con lo cual no es necesario configurar el proxy de red en cada navegar de los equipos de la red local.

En la figura 4.44, figura 4.45 y figura 4.46, se observa el archive squid.conf con todas las líneas que fueron agregadas.

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed

#acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl fulbright src 192.168.1.0/24        # Red local fulbright
#acl localnet src 10.0.0.0/8            # RFC 1918 local private network (LAN)
#acl localnet src 100.64.0.0/10         # RFC 6598 shared address space (CGN)
#acl localnet src 169.254.0.0/16        # RFC 3927 link-local (directly plugged) machines
#acl localnet src 172.16.0.0/12         # RFC 1918 local private network (LAN)
#acl localnet src 192.168.0.0/16                # RFC 1918 local private network (LAN)
#acl localnet src fc00::/7              # RFC 4193 local private network range
#acl localnet src fe80::/10             # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports
```

Figura 4. 44 Configuración squid.conf, parte1

```
# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed

#http_access allow localnet
#http_access allow localhost
http_access allow fulbright

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128  MQ: Se añade intercept
#http_port 3128
http_port 192.168.1.100:3128

http_port 3129 intercept
# MQ: Se añade 25 may 2020
visible_hostname squid.proxy

# Uncomment and adjust the following to add a disk cache directory.
```

Figura 4. 45 Configuración squid.conf, parte2

```
# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320

# MQ: Se añadio desde aqui 24 may 2020
# Anonymize Traffic
# via off

forwarded_for on
forwarded_for truncate
#request_header_access From deny all
#request_header_access Server deny all
#request_header_access WWW-Authenticate deny all
#request_header_access Link deny all
#request_header_access Cache-Control deny all
#request_header_access Proxy-Connection deny all
#request_header_access X-Cache deny all
#request_header_access X-Cache-Lookup deny all
#request_header_access Via deny all
#request_header_access X-Forwarded-For deny all
#request_header_access Pragma deny all
#request_header_access Keep-Alive deny all
cache_dir aufs /var/spool/squid 50000 16 256
cache_swap_low 90
cache_swap_high 95
```

Figura 4. 46 Configuración squid.conf, parte3

Una vez realizada la configuración, se guardan los cambios y se reinicia squid con el siguiente comando:

systemctl restart squid

De igual manera squid puede ser iniciado con systemctl start squid, o activarlo para que inicie con el sistema con systemctl on squid

Es necesario realizar algunos cambios en el firewall, primero se agrega el puerto 3129 a la zona interna para que el servidor pueda comunicarse por dicho puerto con la red local y responder a peticiones de uso de squid, ver figura 4.47

Figura 4. 47 Comando para habilitar puerto3129 en la zona interna del firewall

Como se indica en la figura 4.48 y la figura 4.49 es necesario habilitar primero el enmascaramiento con add-masquerade en la zona deseada, para poder reenviar el tráfico de un puerto a otro o de una dirección a otra, en este caso se necesita realizar reenvíos desde la red interna y externa por lo que se va a activar mascarade en las dos zonas (interna y externa).

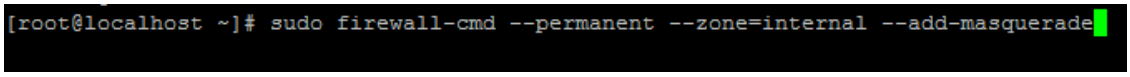

Figura 4. 48 Comando que activa enmascaramiento en zona interna

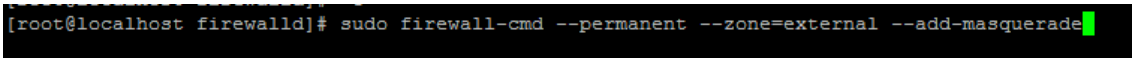

Figura 4. 49 Comando que permite enmascaramiento en zona externa

Se debe redirigir automáticamente las peticiones que se hagan desde la red local desde el puerto 80 y enviarlas al puerto 3129, antes de esto es importante tomar en cuenta habilitar el enmascaramiento en la zona.

El redireccionamiento al puerto 3129 se lo puede realizar de dos formas:

Opción1. Utilizando reglas enriquecidas

firewall-cmd –permanent –zone = internal –add-rich-rule ='rule family="ipv4" source address="192.168.1.0/24" forward-port port="80" protocol="tcp" to-port="3129"'`

Opción2. Regla convencional de firewalld:

sudo firewall-cmd --zone="internal" --add-forward-port=port=80: proto=tcp:toport =3129:toaddr=192.169.1.100 --permanent

Para este caso se optó por la opcion2.

Se recarga el firewall para que estos últimos cambios tomen efecto.

firewall-cmd –reload

Toda la configuración que debe haberse establecido en el firewall hasta el momento en la zona interna se puede ver en la figura 4.50 y en la zona externa en la figura 4.51

```
[root@localhost firewalld]# firewall-cmd --zone=internal  --list-all
internal (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp1s0
  sources:
  services: cockpit dhcpv6-client mdns samba-client ssh
  ports: 3129/tcp
  protocols:
  masquerade: yes
  forward-ports: port=80:proto=tcp:toport=3129:toaddr=192.169.1.100
  source-ports:
  icmp-blocks:
  rich rules:
```

Figura 4. 50 Configuración de la zona interna

```
[root@localhost ~]# firewall-cmd --zone=external  --list-all
external (active)
  target: default
  icmp-block-inversion: no
  interfaces: eno1
  sources:
  services: ssh
  ports: 2222/tcp 443/tcp
  protocols:
  masquerade: yes
  forward-ports: port=2222:proto=tcp:toport=22:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:

[root@localhost ~]#
```

Figura 4. 51 Configuración de la zona externa

Para que funcione el redireccionamiento es necesario habilitar esto en /etc/sysctl.conf, para esto se ejecuta lo que se muestra la figura 4.52

```
[root@localhost ~]# vim /etc/sysctl.conf
```

Figura 4. 52 Comando para abrir archivo sysctl.conf

En este archivo se agrega la línea: net.ipv4.ip_forward = 1, como se observa en la figura 4.53

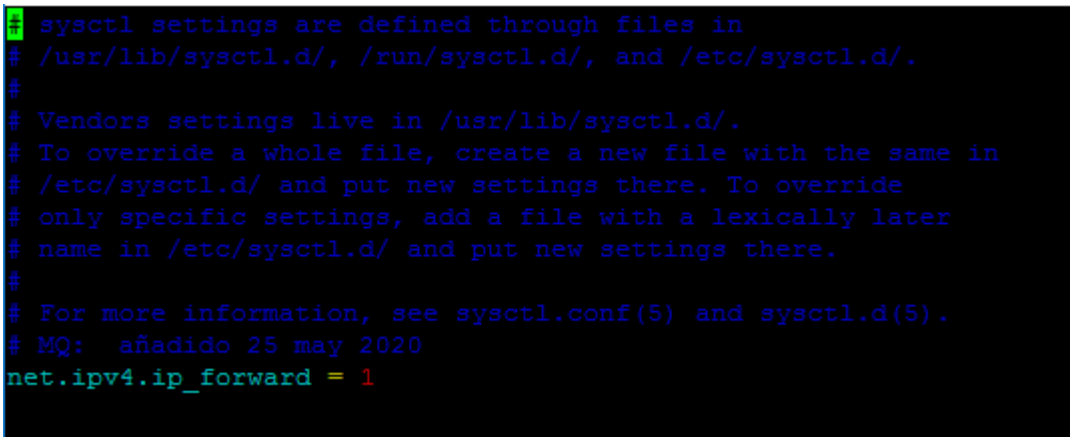

Figura 4. 53 Configuración del archivo sysctl.conf

Con esto se tiene funcionando el servicio de proxy en modo transparente con permiso de acceso desde la red local.

Aunque no es necesario se procede a cambiar el hostname del servidor a fulbright.server como se observa en la figura 4.54

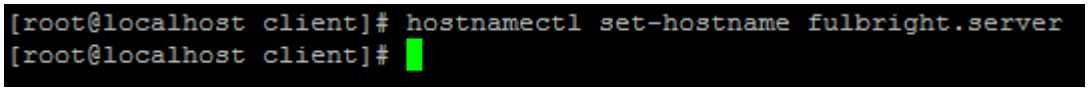

Figura 4. 54 Cambiar nombre del servidor

4.5. Instalación y configuración de OpenVPN

"OpenVPN es una aplicación de código abierto que permite crear una vpn segura a través del servicio de internet, utiliza la biblioteca OpenSSL para la encriptación, además permite utilizar varios mecanismos de autenticación, como claves basadas en certificados y usuario /contraseña" (Arul, 2019), para este proyecto se utilizará la autenticación basada en certificados.

El proceso de instalación se realiza utilizando el terminal de Linux y utilizando privilegios de root.

Se inicia instalando el paquete dnf install epel-release, para agregar el repositorio EPEL necesario para descargar los paquetes de OpenVPN, como indica la figura 4.55, se debe digitar la letra s, indicando que se está de acuerdo con la instalación el momento en que el proceso lo requiera y se espera a que finalice la instalación.

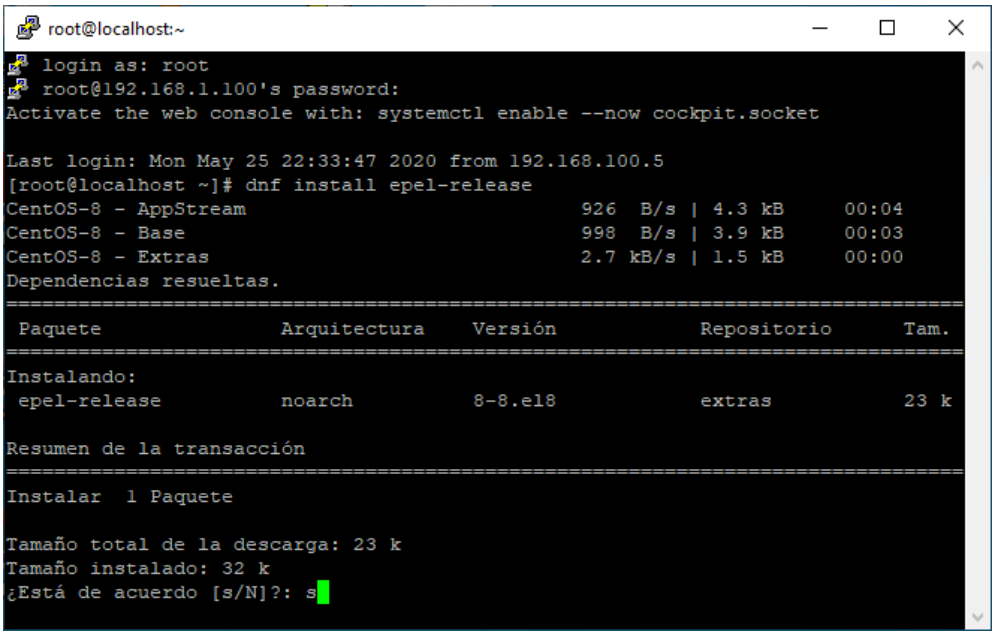

Figura 4. 55 Instalación de epel-release

4.5.1. Instalación de OpenVPN

Se instala openvnp, ejecutando dnf install openvpn como se puede observar en las figuras 4.56, 44.57 y 44.58, se debe digitar la letra s, indicando que se está de acuerdo con la descarga y con la instalación el momento en que el proceso lo requiera y se espera a que finalice la instalación.

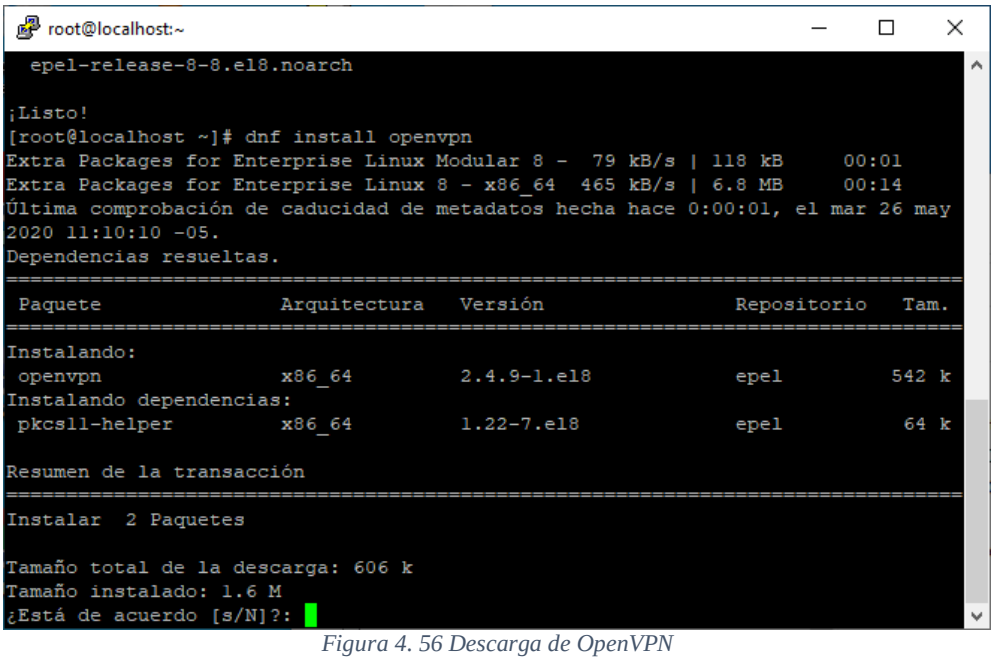

Figura 4. 56 Descarga de OpenVPN

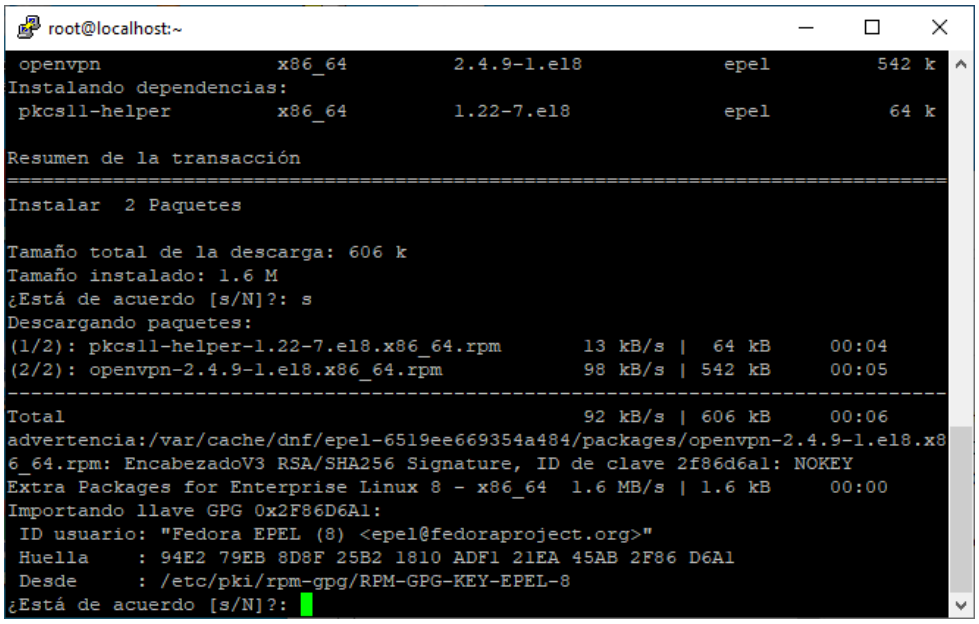

Figura 4. 57 Confirmar instalación de OpenVPN

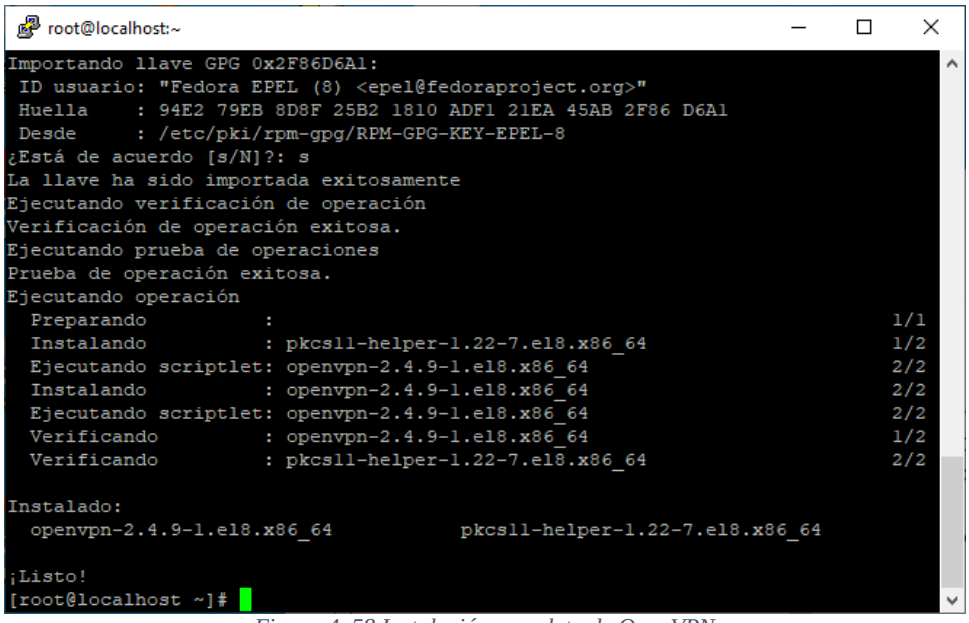

Figura 4. 58 Instalación completa de OpenVPN

4.5.2. Instalación y configuración de Easy-RSA

Como se indica en la figura 4.59, una vez instalado OpenVPN, es necesario ingresar al directorio /etc/openvpn, en este se debe descargar el script easy-rsa ejecutando el comando:

wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz

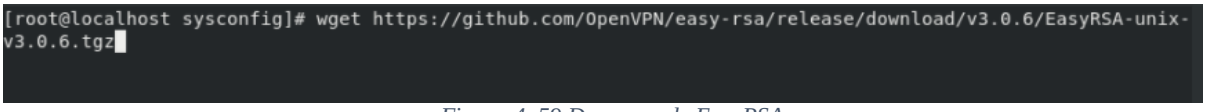

Figura 4. 59 Descarga de EasyRSA

Lo siguiente es extraer el archivo EasyRSA-unix-v3.0.6.tgz y mover todo lo extraído a una nueva carpeta con el nombre easy-rsa, para realizar esto se debe estar dentro del directorio /etc/openvpn/, ver figura 4.60

tar -xf EasyRSA-unix-v3.0.6.tgz

mv EasyRSA-v3.0.6/ easy-rsa/

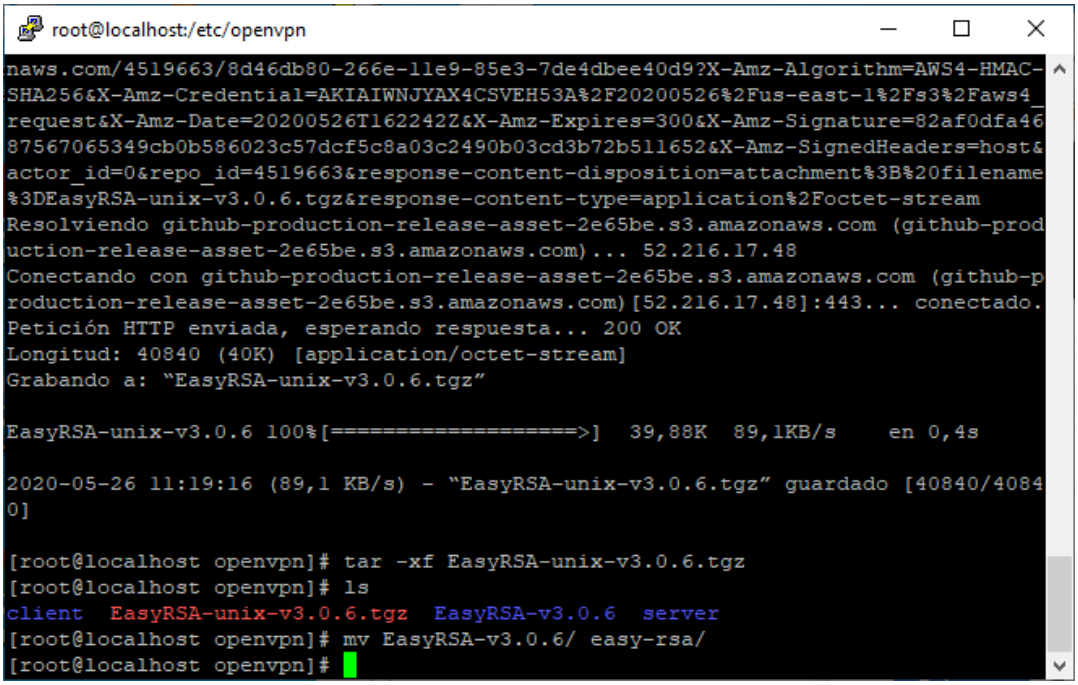

Figura 4. 60 Descomprimir EasyRSA

A continuación, como se puede ver en la figura 4.61, se crea un archivo vars dentro de /etc/openvpn/easy-rsa/

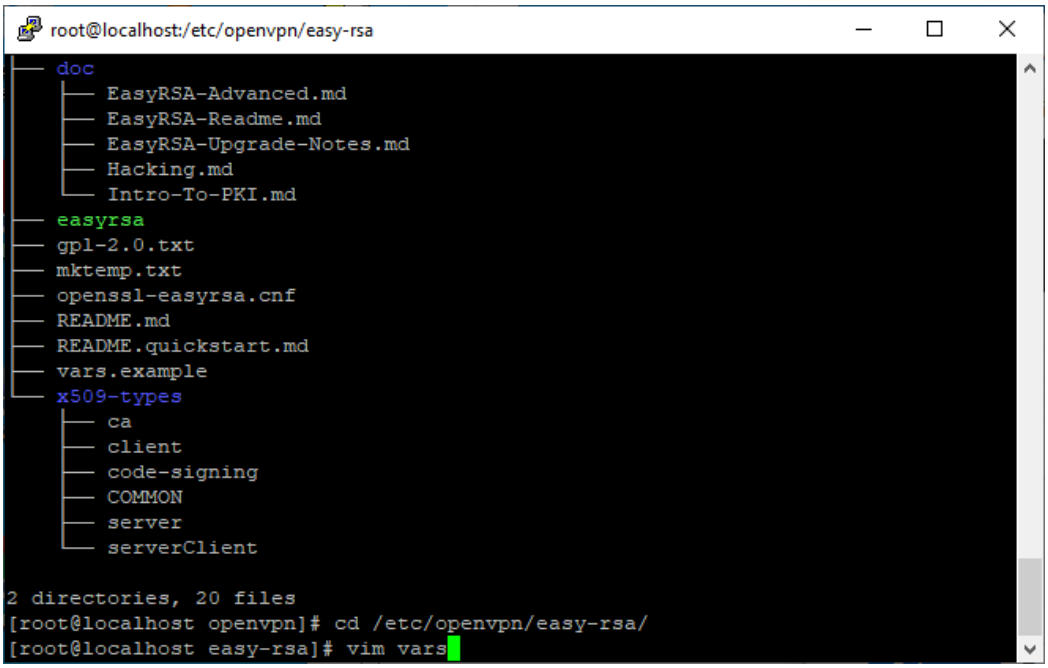

Figura 4. 61 Comando para crear el archivo vars

Es necesario ingresa en el archivo vars la información siguiente, ver figura 4.62

Figura 4. 62 Información de configuración a ingresarse en el archivo vars

Por defecto se tiene un tiempo de expiración de CA de 7500 días y para el certificado de 365 días, para este caso cambie la expiración del certificado a 3650 días.

Se graba el archivo vars y se cierra el mismo, para esto se presiona la tecla escape "ESC" con esto en la parte inferior del archivo se habilitará una zona para digitar ":wq",

es necesario dar a este archivo permisos de ejecución ejecutando los siguiente:

chmod +x vars

4.5.3. Construcción de claves Openvpn

Se procede a crear las claves OpenVpn en base al archivo vars que se creó, se creará la clave CA, las claves de servidor, del cliente, el archivo DH y CRL PEM, estas claves deben construirse con los comandos de easyrsa.

Se ingresa a la carpeta /etc/openvpn/easyrsa/

cd /etc/openvpn/easy-rsa

Se inicializa el directorio PKI (Public Key Infrastruture) y se crea la clave CA, como se ve en la figura 4.63, estando en /etc/openvpn/easy-rsa/

Se ejecuta:

./easyrsa init-pki

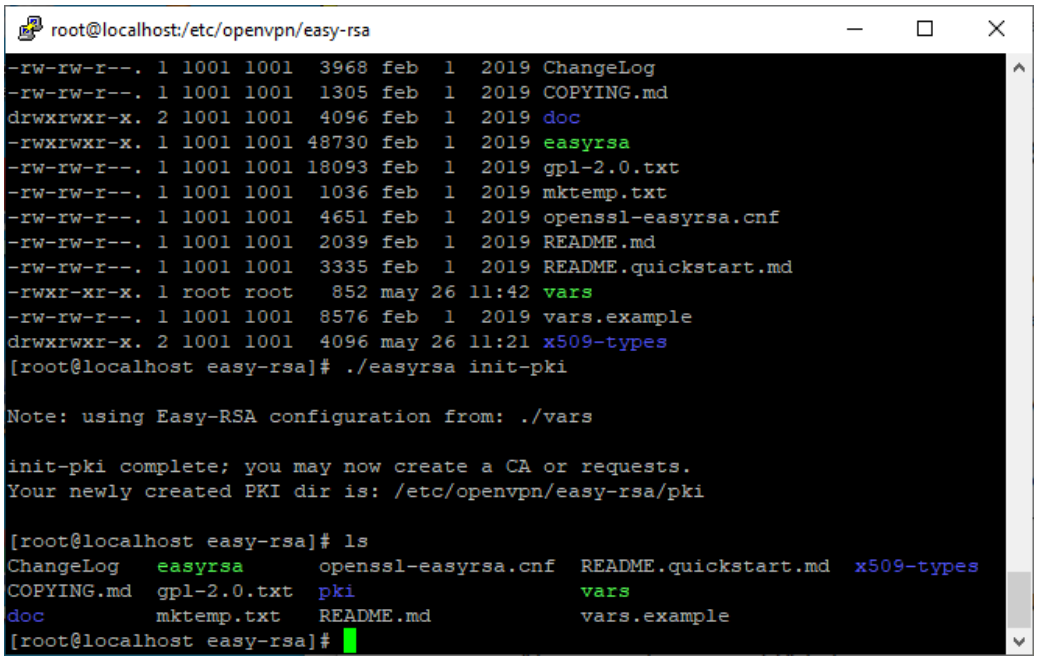

Figura 4. 63 Comandos para iniciar el directorio PKI

Esto presenta el mensaje de que se ha creado el directorio PKI y la ubicación del mismo:

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

Una vez finalizado la creación de PKI se ejecuta:

./easyrsa build-ca

Al ejecutar ./easyrsa build-ca, como se puede ver en la figura 4.64

se presenta el siguiente error:

"**Can't load /etc/openvpn/easy-rsa/pki/.rnd into RNG** ",

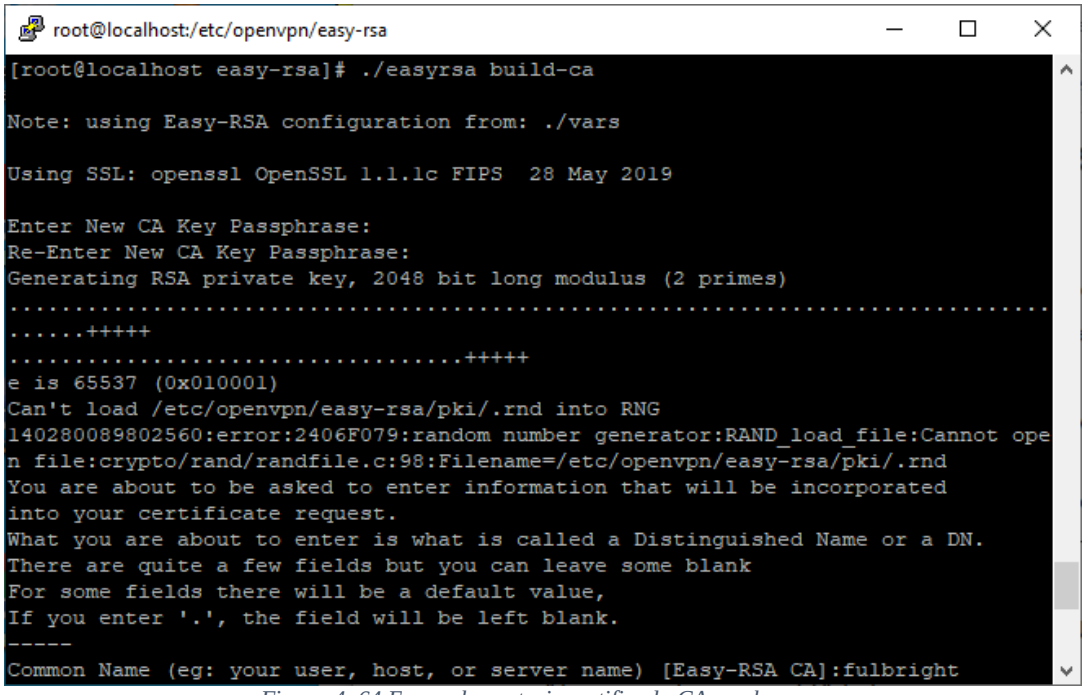

Figura 4. 64 Error al construir certificado CA en el server

Por lo que fue necesario borrar del archivo openssl-easyrsa.cnf que está ubicado en /etc/openvpn/easy-rsa/ la siguiente línea

RANDFILE = $ENV::EASYRSA_PKI/.rnd

Y se ejecuta nuevamente

./easyrsa build-ca.

En este paso se solicitará la clave para CA y de forma opcional el nombre para el servidor CA, esto permite obtener el archivo **ca.crt** y **ca.key** en el directorio **/etc/openvpn/easy-rsa/pki,** como se puede observar en la figura 4.65

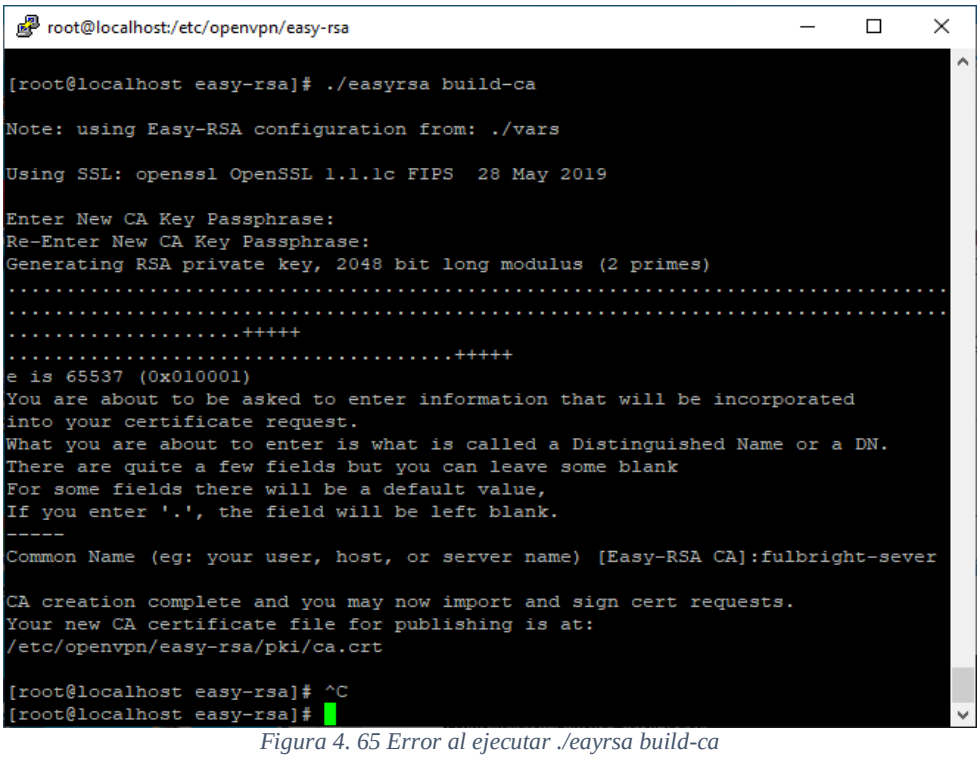

Figura 4. 65 Error al ejecutar ./eayrsa build-ca

Crear clave del servidor

Se procede como se muestra en la figura 4.66 a crear la clave del servidor que lo nombre como fulbright-server, para lo cual es necesario ejecutar el comando:

./easyrsa gen-req fulbright-server nopass

El colocar **nopass**, permite deshabilitar la contraseña para la clave **fulbright-server.**

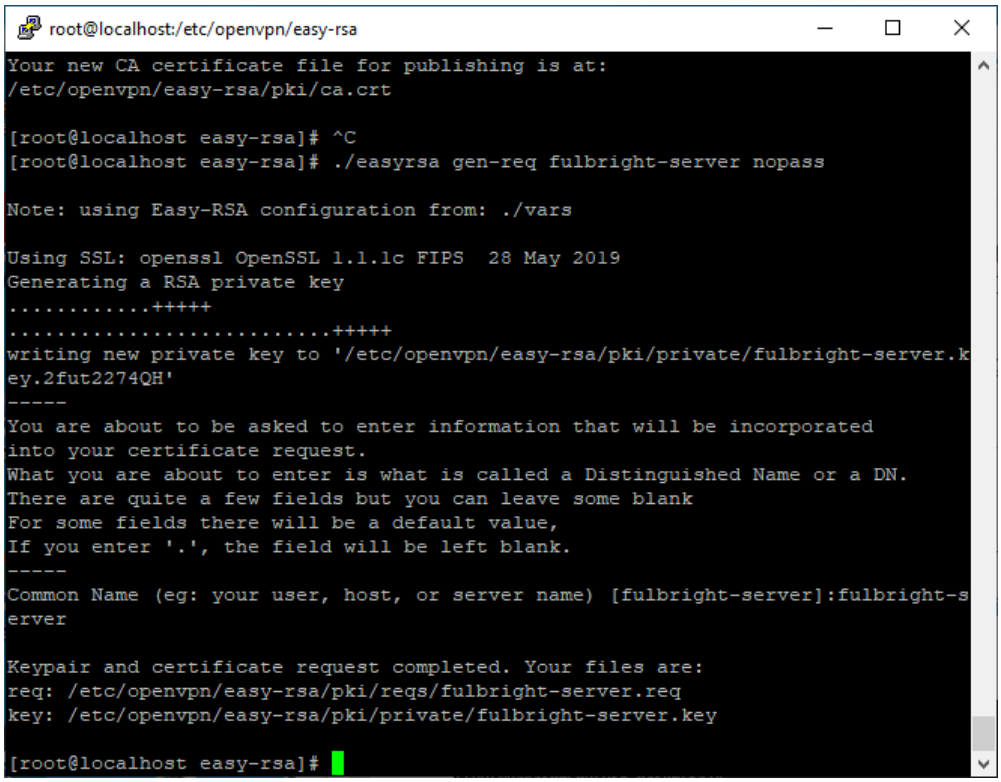

Figura 4. 66 Ejecutar comando ./easyrsa gen-req fulbright-server nopass

Se procede a firmar la clave anterior (fulbright-server)como se observa en la figura 4.67 utilizando el certificado CA, con el comando:

./easyrsa sign-req server fulbright-server

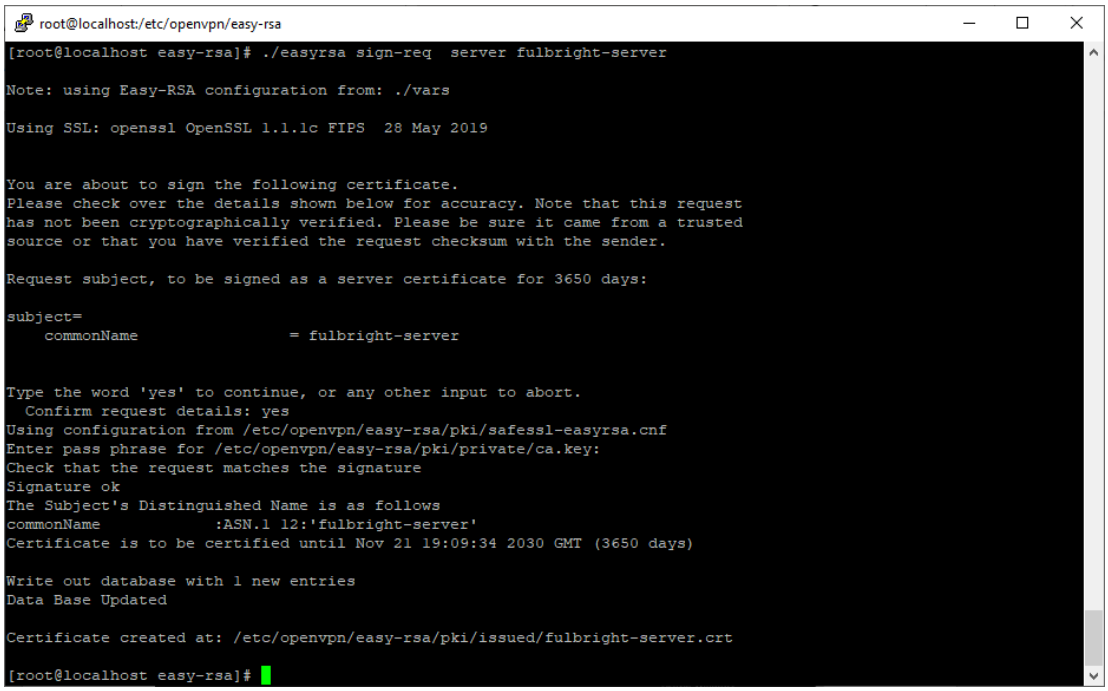

Figura 4. 67 Comando para firmar el servidor fulbright-server

En este paso se solicita el ingreso de la clave CA que se registró anteriormente, esto genera el certificado fulbright-server.crt en el directorio /etc/openvpn/easy-rsa/pki/issued/ como se puede ver en la figura 4.68

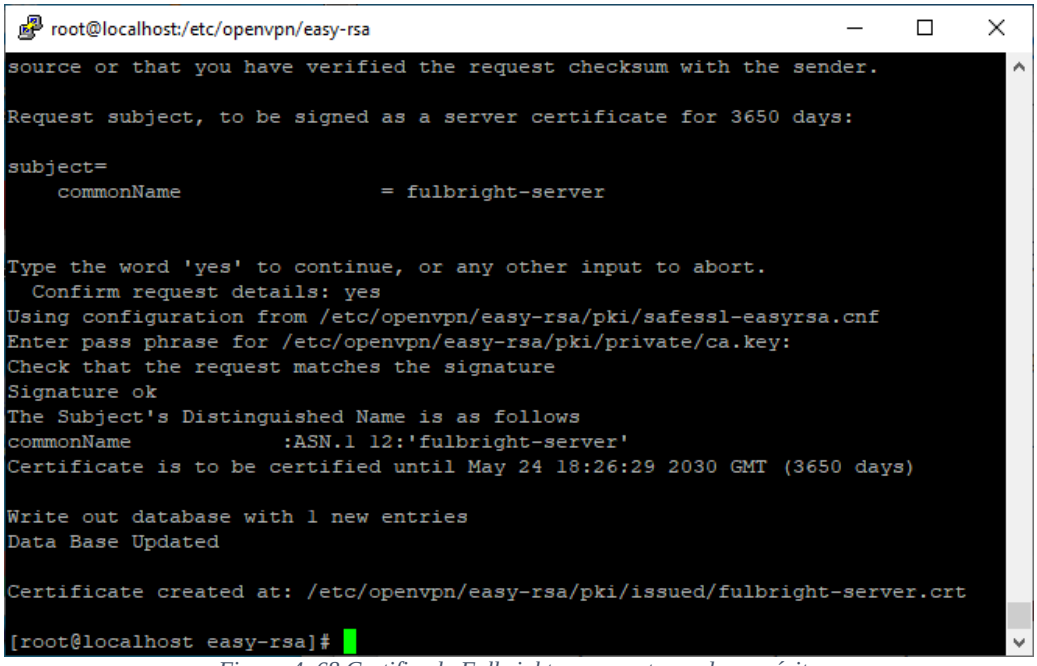

Figura 4. 68 Certificado Fulbright-server.crt creado con éxito

Una vez creado el certificado Fulbright-server.crt, se debe verificar el archivo de certificado utilizando el comando OpenSSL, esto no debe presentar errores, como se observa en la figura 4.69.

openssl verify -CAfile pki/ca.crt pki/issued/Fulbright-server-crt

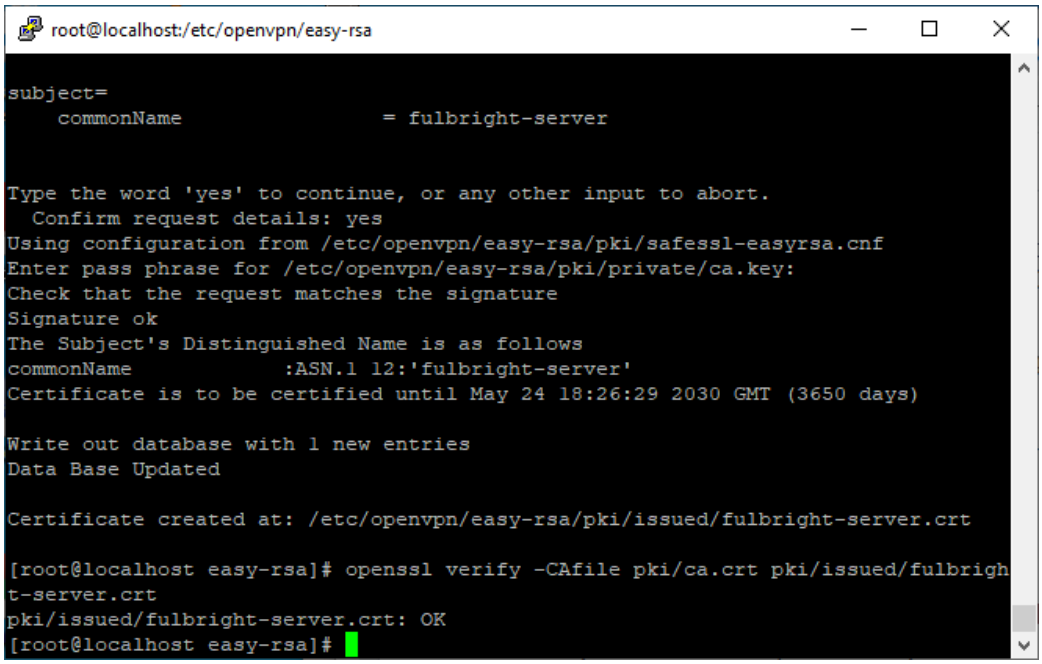

Figura 4. 69 Verificar certificar Fulbright-server.crt con comando OpenSSL

4.5.4. Generar los clientes que van a conectarse al servidor OpenVPN

Este proceso es necesario realizarlo por cada cliente que vaya a hacer uso del servidor OpenVPN, para que de ser el caso sea posible inactivar el acceso de cada uno, en este caso solo realizó la captura de la creación del cliente1**.**

Se ingresa a la carpeta /etc/openvpn/easyrsa/

cd /etc/openvpn/easy-rsa

Como se observa en la figura 4.70, se ejecuta:

./easyrsa gen-req client01 nopass

Para crear el requerimiento del cliente y la clave privada para el cliente, como resultado de esto se tendrán los archivos: client01.req archivo de requerimiento y client01.key como la clave privada.

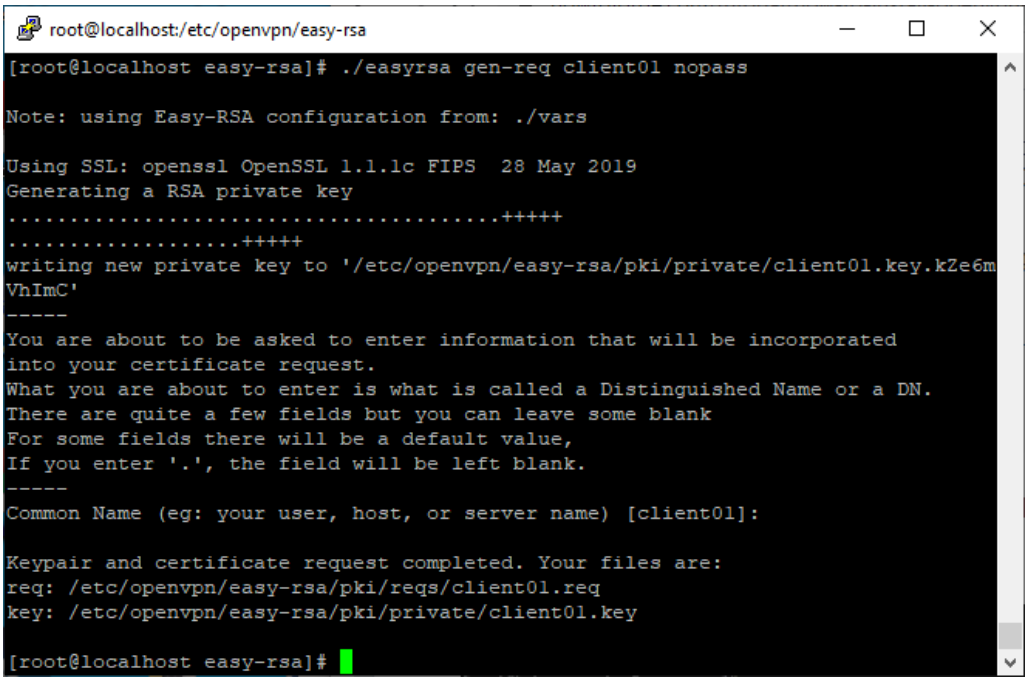

Figura 4. 70 Creación de cliente1

Se firma el requerimiento generado para el cliente utilizando el certificado CA, como se indica en la figura 4.71 se debe ejecutar:

./easyrsa sign-req client clientXX

Aquí se debe digitar "yes" y la clave de CA el momento en que se solicite, esto creará el certificado para el cliente1, con el nombre client01.crt

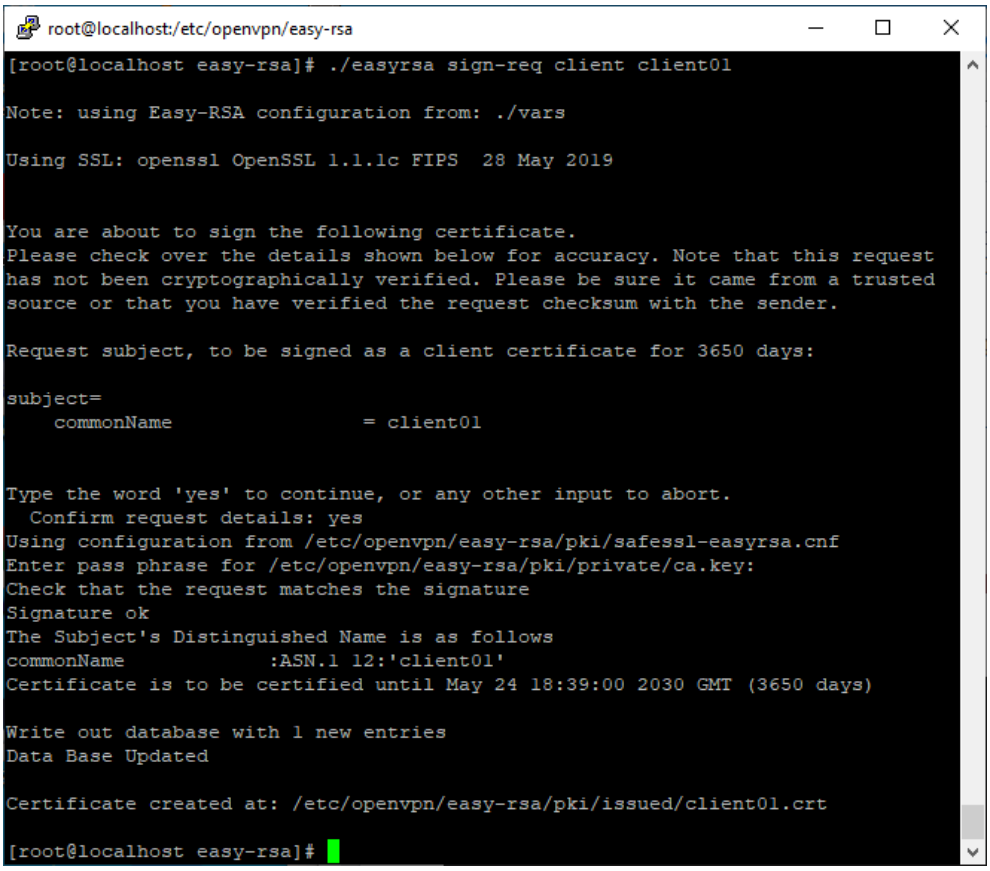

Figura 4. 71 Comando para firmar el certificado de Cliente1

Como se indica en la figura 4.72, se debe verificar el certificado client01.crt generado, para esto se debe ejecutar el comando:

openssl verify -CAfile pki/ca.crt pki/issued/client01.crt

Para ejecutar el comando anterior se debe ingresar en el directorio /etc/openvpn/easy-rsa

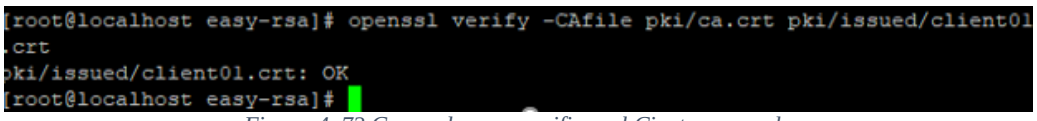

Figura 4. 72 Comando para verificar el Ciente generado

Para contar con mayor seguridad se debe utilizar la clave Diffie-Hellman, con esto se va a generar la clave DH '2048' basándome en el archivo de configuración 'vars' que se creó anteriormente como se puede observar en la figura 4.73.

./easyrsa gen-dh

Esto creará el archivo dh.pem en el directorio /ect/openvpn/easy-rsa/pki/

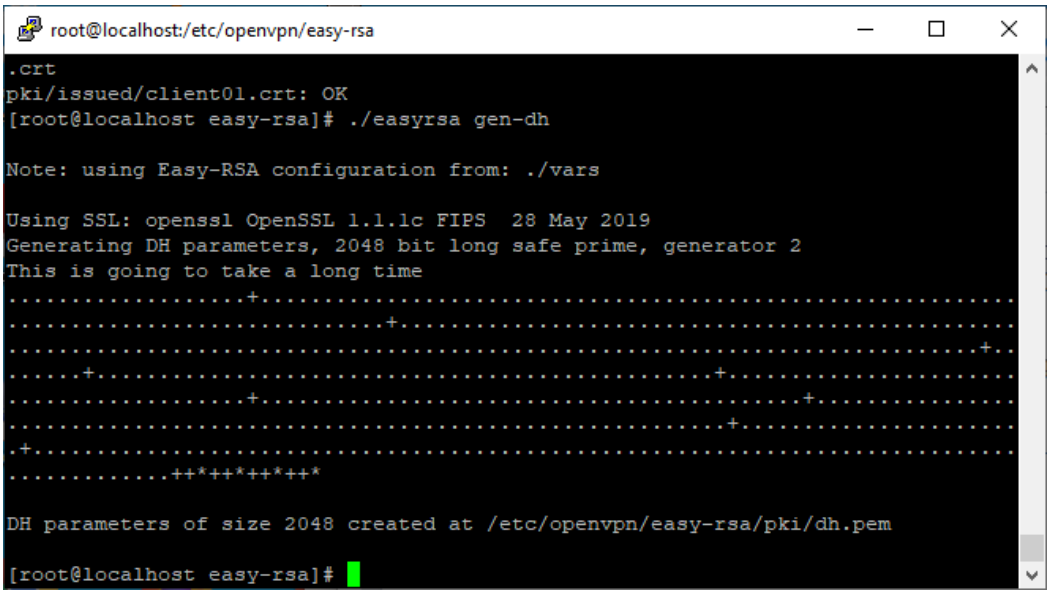

Figura 4. 73 Comando para crear dh.pem

Si en algún momento se desea dar de baja o eliminar uno de los clientes, solo es necesario ejecutar el comando easy-rsa.

./easyrsa revoke cliente

Luego se debe ejecutar: ./easyrsa gen-crl , esto generará el archivo crl.pem en /etc/openvpn/easy-rsa/pki que se copiará luego a la carpeta server

Como se observa en la figura 4.74, luego de haber creado los certificados necesarios, es necesario copiarlos a la carpeta server a los archivos:

ca.crt

fulbright-server.crt

fulbright-server.key

dh.pem.

crl.pem

De igual manera se copian a la carpeta client los archivos:

ca.crt

client01.crt

client01.key

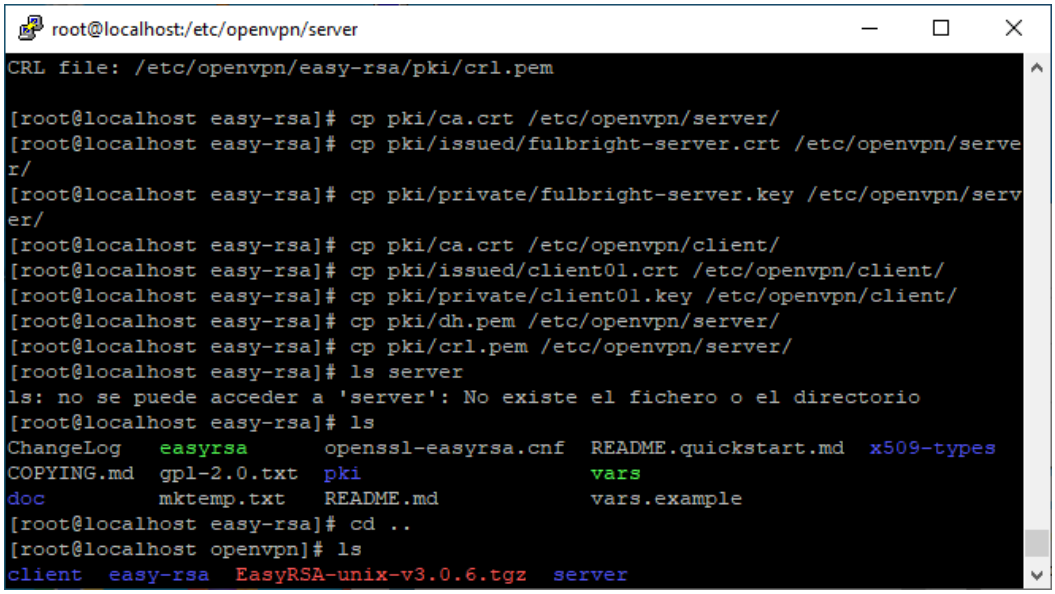

Figura 4. 74 Copia de archivos a carpeta server y client

Crear archivo de configuración de OpenVPN

Para esto se ingresa en el terminal de Linux a la carpeta

/etc/openvpn/server/

Y crea el archivo server.conf con el comando vim:

vim server.conf

En este archivo se coloca la siguiente información, como se indica en la figura 4.75:

port 1194
proto udp
dev tun

OpenVPN Server Certificate - CA, server key and certificate
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/fulbright-server.crt
key /etc/openvpn/server/fulbright-server.key

#DH and CRL key
dh /etc/openvpn/server/dh.pem
crl-verify /etc/openvpn/server/crl.pem

Network Configuration - Internal network

```
# Redirect all Connection through OpenVPN Server
server 10.5.0.0 255.255.255.0
push "redirect-gateway def1"

# Using the DNS from https://dns.watch
push "dhcp-option DNS 200.67.222.222"
push "dhcp-option DNS 200.67.220.220"

#Enable multiple clients to connect with the same certificate key
duplicate-cn

# TLS Security
cipher AES-256-CBC
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-
AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-
RSA-WITH-AES-128-CBC-SHA256
auth SHA512
auth-nocache

# Other Configuration
keepalive 20 60
persist-key
persist-tun
compress lz4
daemon
user nobody
group nobody

# OpenVPN Log
log-append /var/log/openvpn.log
verb 3
```

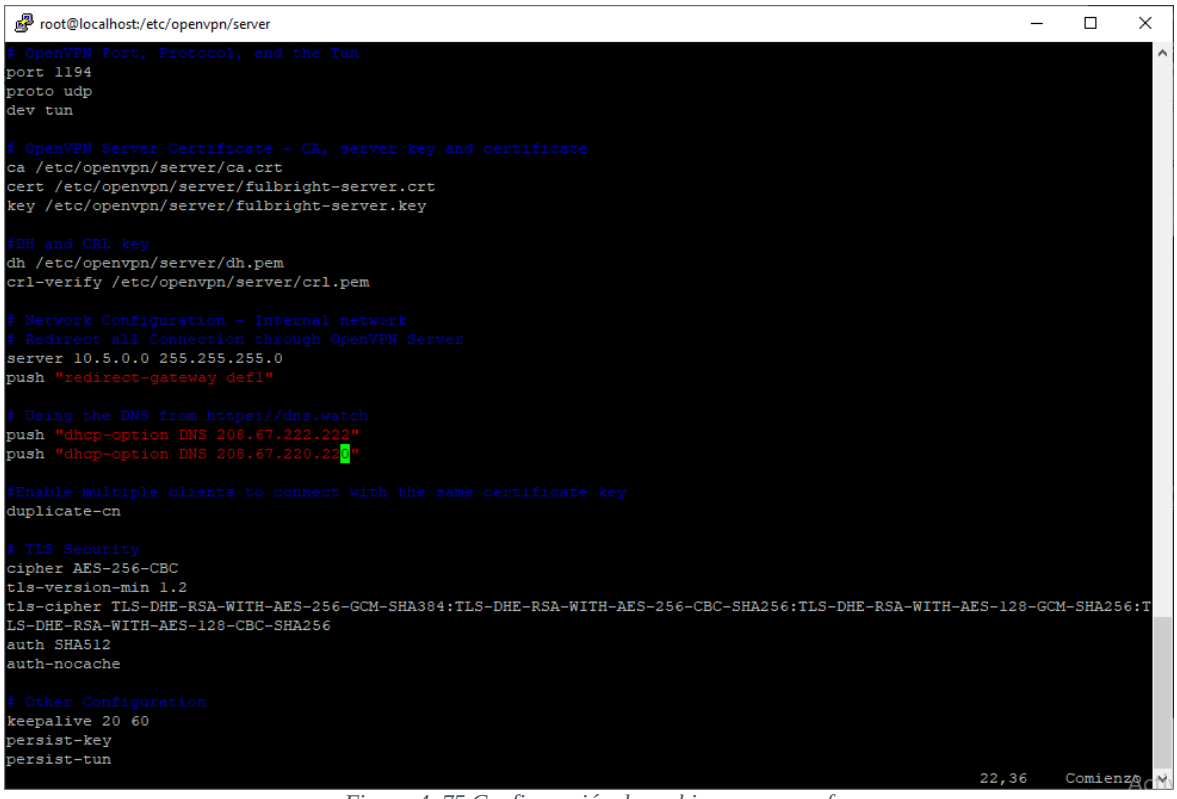

Figura 4. 75 Configuración de archivo server.conf

4.5.5. Configurar Firewall para funcionamiento de OpenVPN

Es necesario configurar el routing en firewalld

Verifico que este habilitado Port-forwarding en /etc/sysctl.conf, como se puede observar en la figura 4.76

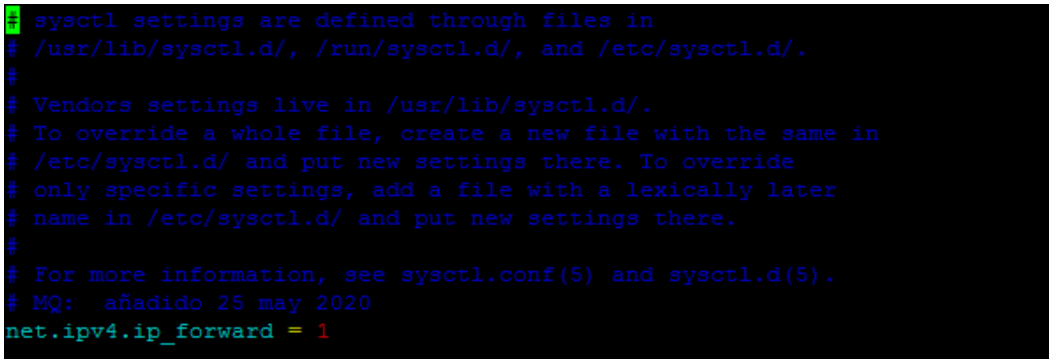

Figura 4. 76 Activación de forward

Agrego el servicio vpn a la zona externa, ejecutando:

firewall-cmd --permanent --zone=external --add-service=openvpn

Agrego la interface tun0, se crea con OpenVPN a la zona externa, ejecutando:

firewall-cmd --permanent --zone=external --add-interface=tun0

Para habilitar NAT desde la red interna 10.5.0.0/24 de OpenVPN a la IP externa, se ejecuta lo siguiente:

- SERVERIP=$(ip route get 1.1.1.1 | awk 'NR==1 {print $(NF-2)}')
- firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.5.0.0/24 -o $SERVERIP -j MASQUERADE

En la figura 4.77 se observa lo que debe generarse una vez habilitado NAT del paso anterior

```
<?xml version="1.0" encoding="utf-8"?>
<direct>
  <passthrough ipv="ipv4">-t nat -A POSTROUTING -s 10.5.0.0/24 -o 181.199.73.159 -j MASQUERADE</pas
sthrough>
</direct>
~
```

Figura 4. 77 Configuración archivo /etc/firewalld/direct.xml

Es necesario recargar el firewall:

firewall-cmd --reload

En la figura 4.78 se puede observar la configuración final del firewalld.

```
[root@localhost etc]# firewall-cmd --zone=external  --list-all
external (active)
  target: default
  icmp-block-inversion: no
  interfaces: eno1 tun0
  sources:
  services: openvpn ssh
  ports: 2222/tcp 443/tcp 1194/udp
  protocols:
  masquerade: yes
  forward-ports: port=2222:proto=tcp:toport=22:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:

[root@localhost etc]#
```

Figura 4. 78 Configuración de Firewalld

4.5.6. Iniciar el servicio OpenVPN

Se inicia el servicio ejecutando:

systemctl start openvpn-server@server

systemctl enable openvpn-server@server

Se puede verificar el estado de OpenVPN como se observa en la figura 4.79 si se ejecuta:

netstat -plntu

systemctl status openvpn-server@server

```
[root@localhost firewalld]# systemctl status openvpn-server@server
● openvpn-server@server.service - OpenVPN service for server
   Loaded: loaded (/usr/lib/systemd/system/openvpn-server@.service; enabled; vendor preset:>
   Active: active (running) since Sun 2021-01-10 18:00:25 -05; 4 days ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Main PID: 666 (openvpn)
   Status: "Initialization Sequence Completed"
    Tasks: 1 (limit: 26213)
   Memory: 3.4M
   CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
           └─666 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status->
```

Figura 4. 79 Estado del servicio OpenVPN

4.6. Configuración del cliente vpn en los equipos remotos

Se crean los certificados y clave para los clientes del client01 al client10 que se van a conectar, en la figura 4.80 se puede observar los clientes generados.

```
[root@fulbright ~]# cd /etc/openvpn/client
[root@fulbright client]# ls
ca.crt          client03.crt  client05.crt  client07.crt  client09.crt
client01.ovpn   client03.key  client05.key  client07.key  client09.key
client02.crt    client04.crt  client06.crt  client08.crt  client10.crt
client02.key    client04.key  client06.key  client08.key  client10.key
[root@fulbright client]#
```

Figura 4. 80 Clientes generados

Es necesario crear el archivo de configuración del cliente, este archivo tendrá la extensión ovpn y será colocado en el directorio de configuración del cliente openVPN instalado en el computador del usuario.

Se lo puede crear en Linux en el directorio /etc/openvpn/client/, con el comando:

Vim client01.ovpn

En este se ingresa la siguiente información, ver figura 4.81:

```
client
dev tun
proto udp

remote 181.199.73.159 1194

ca ca.crt
cert client01.crt
key client01.key

cipher AES-256-CBC
auth SHA512
auth-nocache
tls-version-min 1.2
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA2
56:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
remote-cert-tls server

resolv-retry infinite
compress lz4
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
~
```

Figura 4. 81 Archivo de configuración client.ovpn generado en linux

Es posible también generar el archivo con un editor de texto de Windows, ver figura 4.82

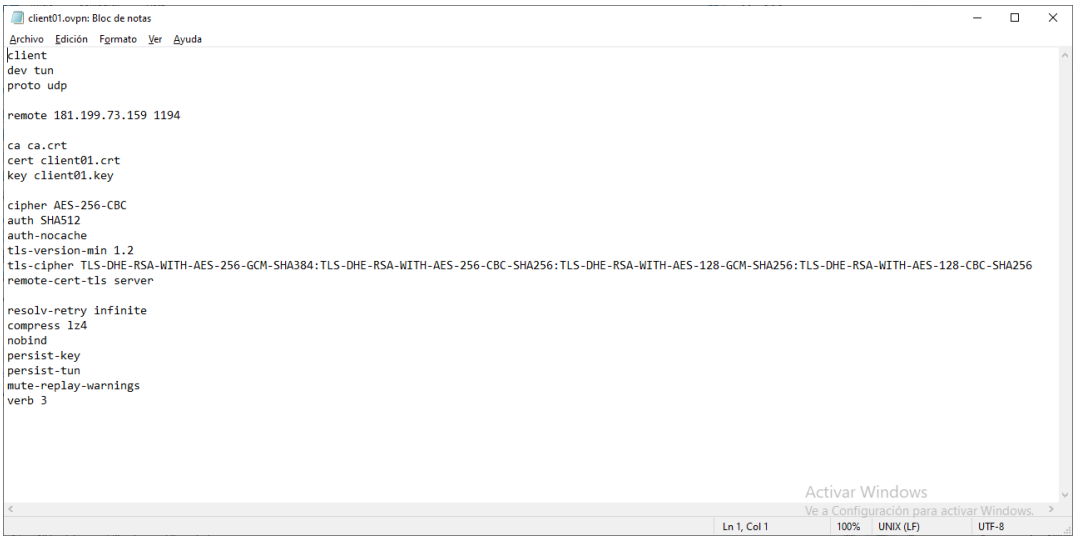

Figura 4. 82 Archivo de configuración client.ovpn generado en block de notas

Instalación del software OpenVPN Cliente en equipo.

Para instalar el cliente de openvpn es necesario descargar el paquete de instalación de la página oficial de OpenVPN, ver figura 4.83, se seleccionó la última versión existente al momento openvpn-2.4.9 desde https://openvpn.net/community-downloads/

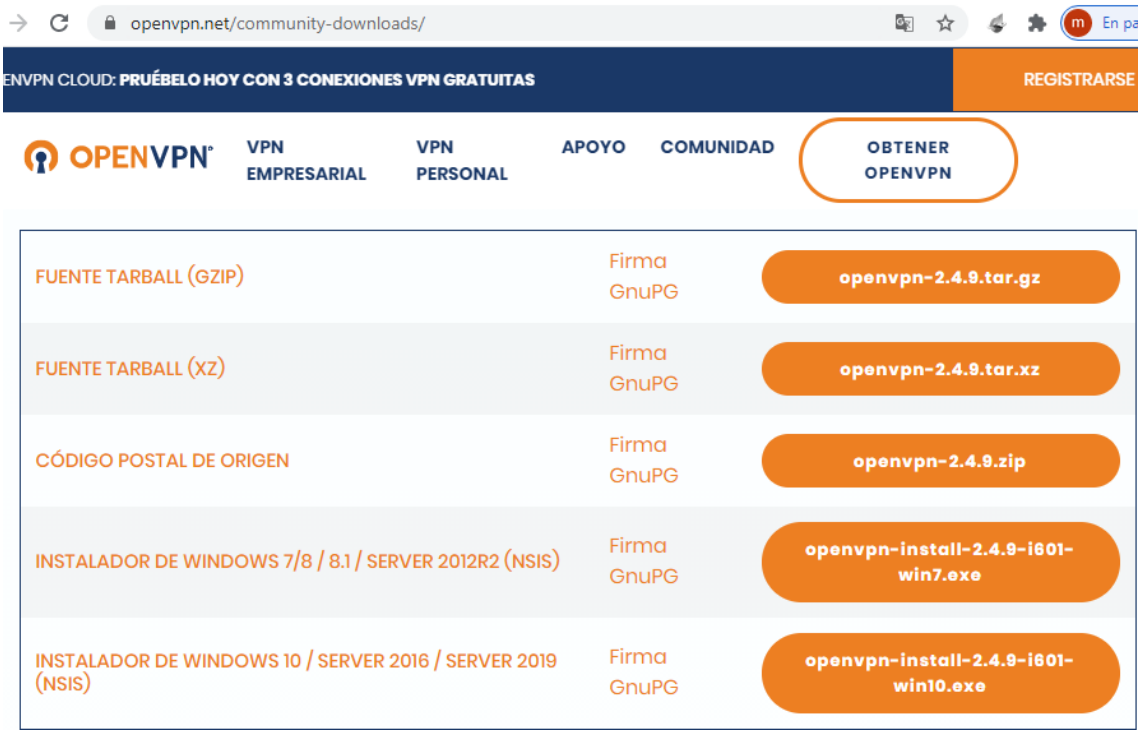

Figura 4. 83 Página de descarga de OpenVPN Client

En Windows se debe ejecutar openvpn-install-2.4.9 con permisos de administrador, ver figura 4.84, es importante descargar el instalador de acuerdo a la versión del sistema operativo que se tenga en el equipo cliente.

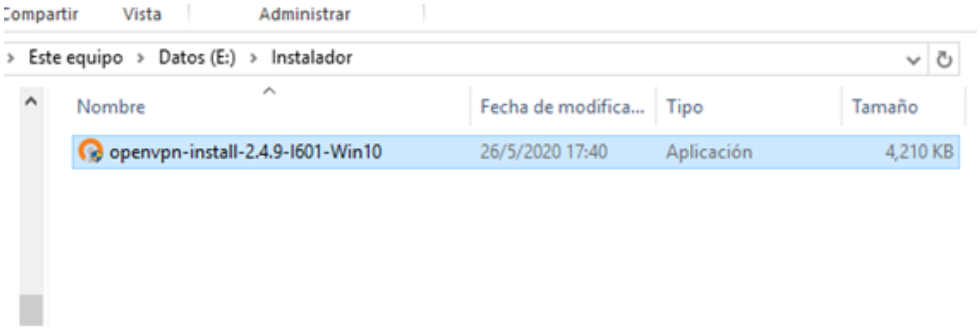

Figura 4. 84 Instalador de OpenVPN

Luego de ejecutar el instalador aparece la ventana de bienvenida a la instalación de OpenVPN, como se observa en la figura 4.85.

Se presiona siguiente para continuar.

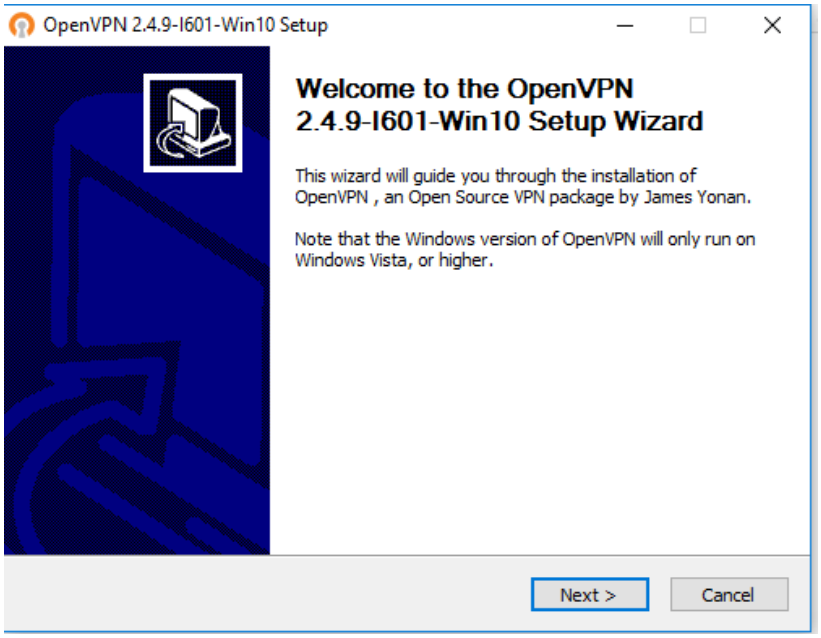

Figura 4. 85Pantalla de bienvenida de instalador de OpenVPN

La siguiente ventana es de aceptación de la licencia, se acepta la misma para continuar como se observa en la figura 4.86

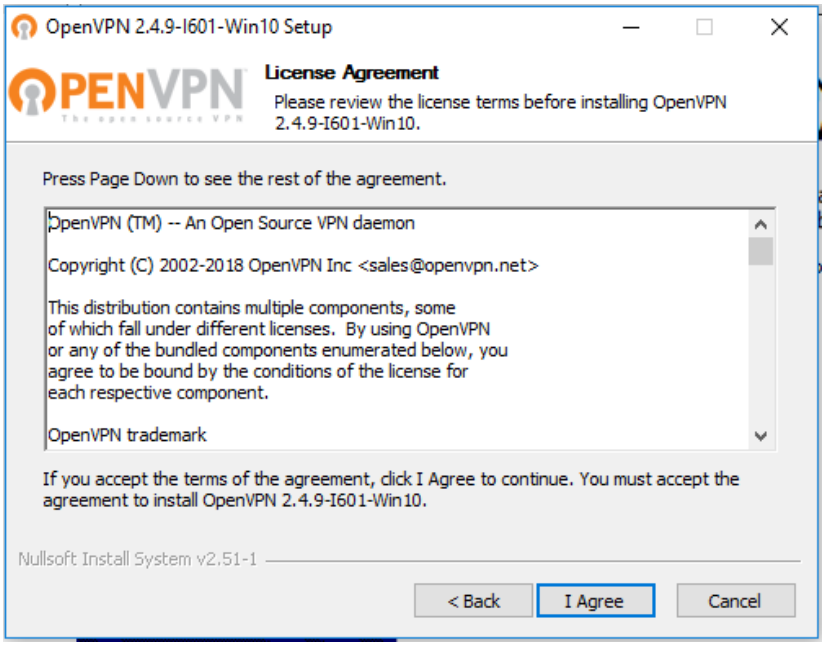

Figura 4. 86 Acuerdo de licencia de OpenVPN

Se selecciona los componentes de OpenVPN a instalarse, en este caso se selecciona todo, ver figura 4.87

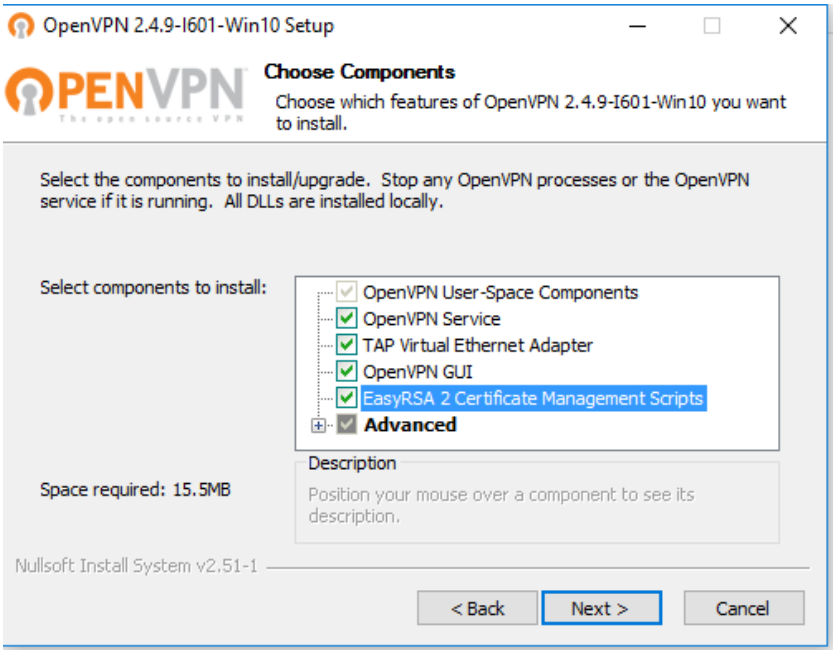

Figura 4. 87 Selección de paquetes a ser instalados

Se selecciona la ubicación de la carpeta de instalación, se deja la que está por defecto y se presiona instalar como se indica en la figura 4.88

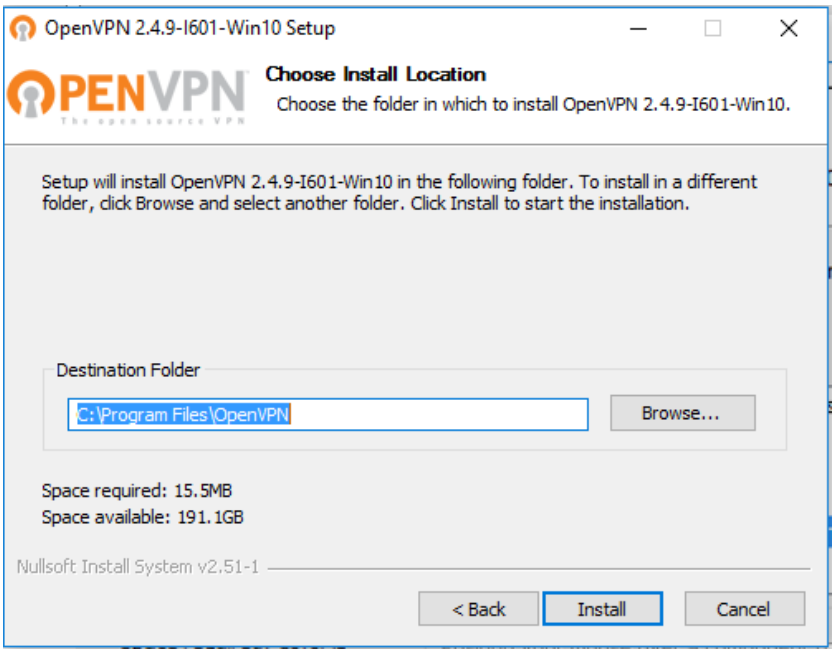

Figura 4. 88 Selección de ubicación de la carpeta de instalación

Como se observa en la figura 4.89, se espera a que finalice la instalación y se presiona siguiente.

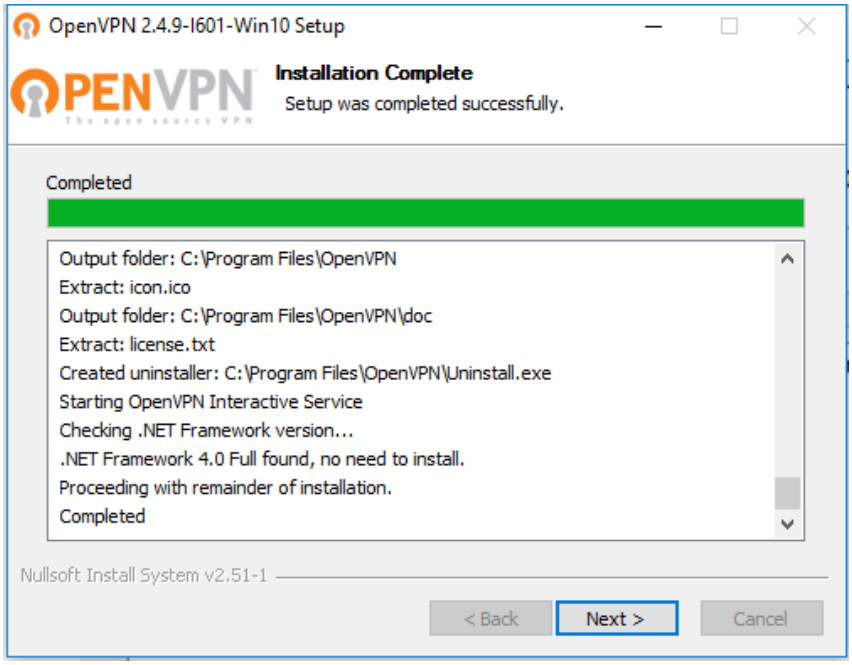

Figura 4. 89 Instalación completa de OpenVPN

Como se observa en la figura 4.90, es necesario colocar en la carpeta que se creó al instalar OpenVPN **c:/Program Files/OpenVPN/Config,** los archivos de uno de los clientes que se generaron en el servidor.

Para esta instalación se utilizó los archivos del client01 que son:

Client01.crt

Client01.key

Client01.ovpn

También se debe copiar aquí el archive ca.crt que es el certificado de seguridad del server.

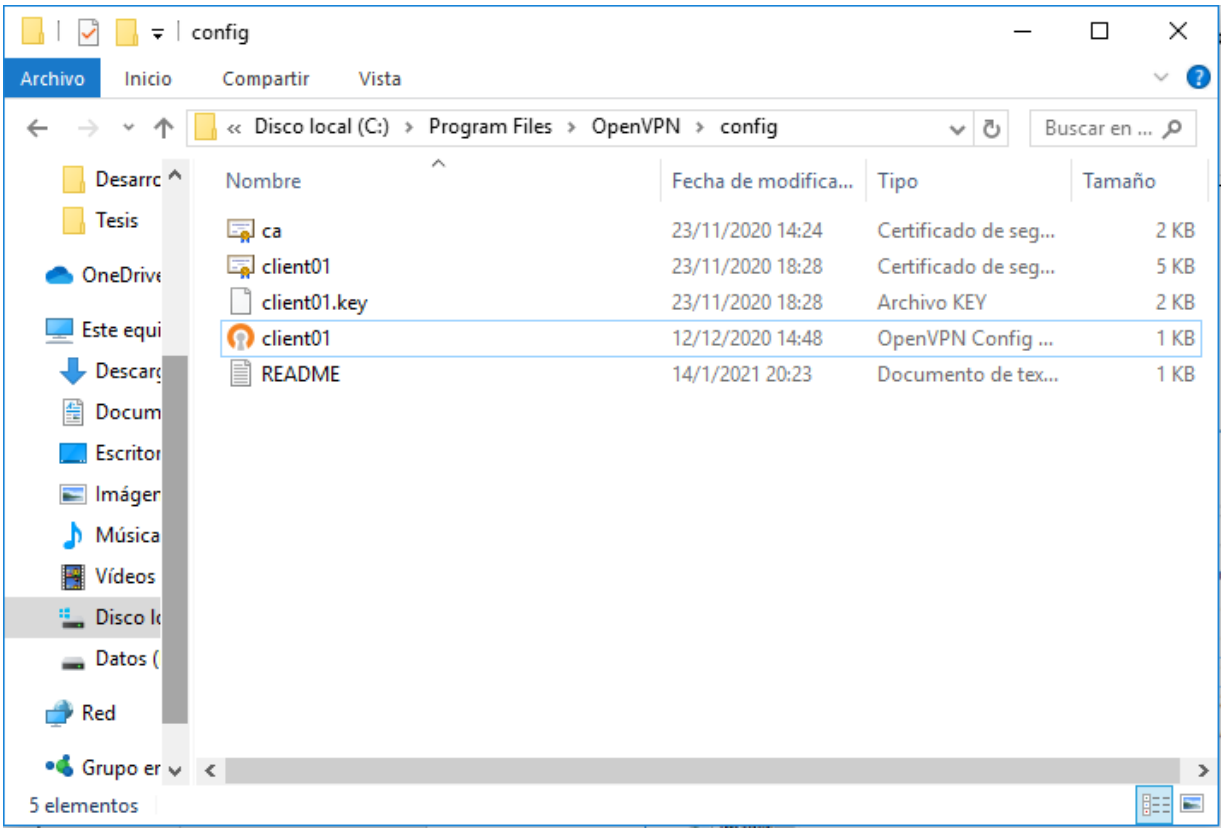

Figura 4. 90 Archivos a ser copiados en la carpeta config de OpenVPN

Dentro de cada archivo clientXX.ovpn es necesario editar y cambiar los nombres del archivo clientXX.crt y clientXX.key como se observa en la figura 4.91

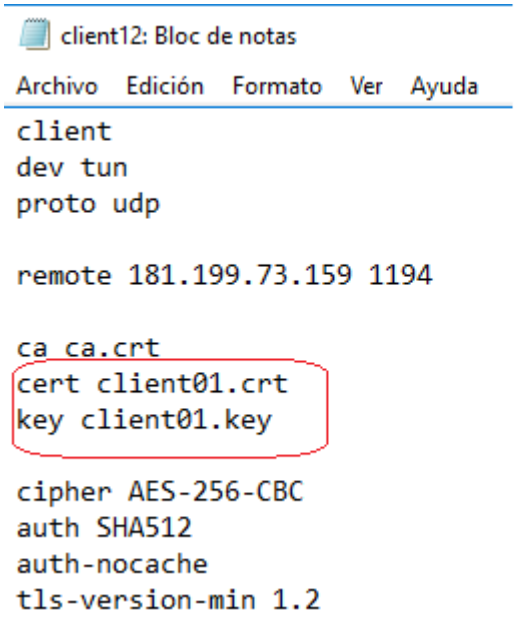

Figura 4. 91 Contenido del archivo Client09.ovpn

Se busca el programa OpenVPN instalado entre los programas de Windows y se selecciona ejecutar, la primera vez será necesario ejecutarlo como administrador, como se observa en la figura 4.92

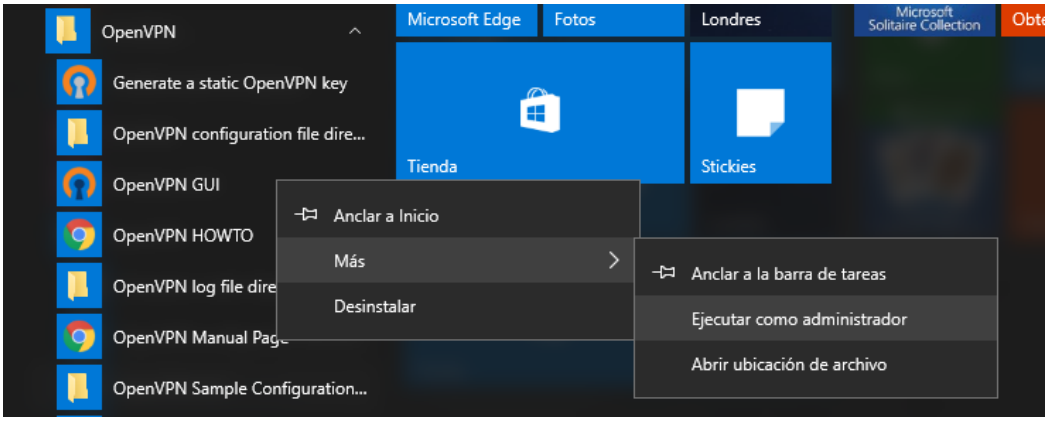

Figura 4. 92 Ejecutar OpenVPN cliente como administrador.

Entre los dispositivos de red se habrá creado una tarjeta de red virtual denominada TAP, como se observa en la figura 4.93, esta tarjeta se activará cuando se establezca la conexión VPN y se desactivará cuando se desconecte la conexión VPN.

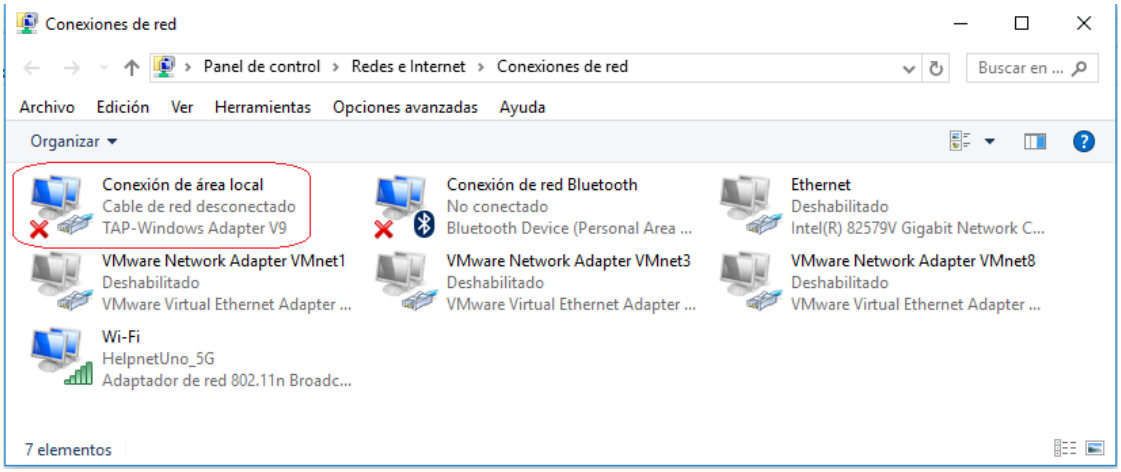

Figura 4. 93 Tarjeta virtual creada por OpenVPN en el computador cliente.

Al lado inferior derecho se observa un nuevo icono con forma de un monitor que representa la conexión de Openvpn. Como se observa en la figura 4.94

Figura 4. 94 Icono de OpenVPN

Con este último paso se habrá instalado y configurado el cliente de OpenVPN.

En el siguiente capítulo se realizaron las pruebas de conexión y funcionamiento

5. EVALUACION DE LA RED IMPLEMENTADA

5.1. Pruebas de funcionamiento

5.1.1. Verificación de conectividad

Luego de haber instalado OpenVPN client, en el equipo cliente se puede observar que se ha agregado una conexión de red con un controlador TAP que antes de establecer la conexión VPN deberá verse en estado de desconectado como se observa en la figura 5.1

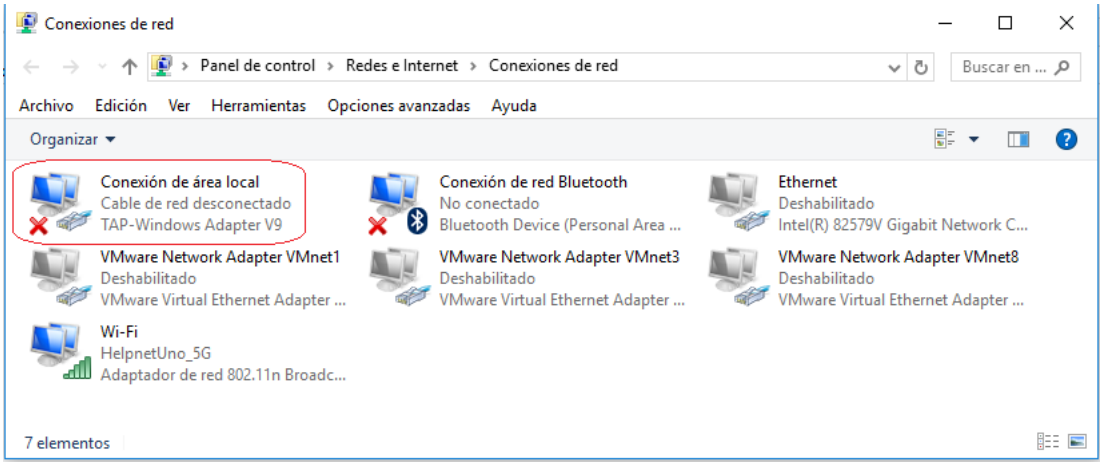

Figura 5. 1 Controlador de red de OpenVPN en estado de desconexión.

Para activar la conexión VPN se debe dar doble click sobre el icono de OpenVPN que se indica en la figura 5.2 para que se realice la conexión desde el cliente al servidor.

Figura 5. 2 Ícono de ejecución de OpenVPN

Se abre una ventana que indica el log proceso de conexión como se puede ver en la figura 5.3

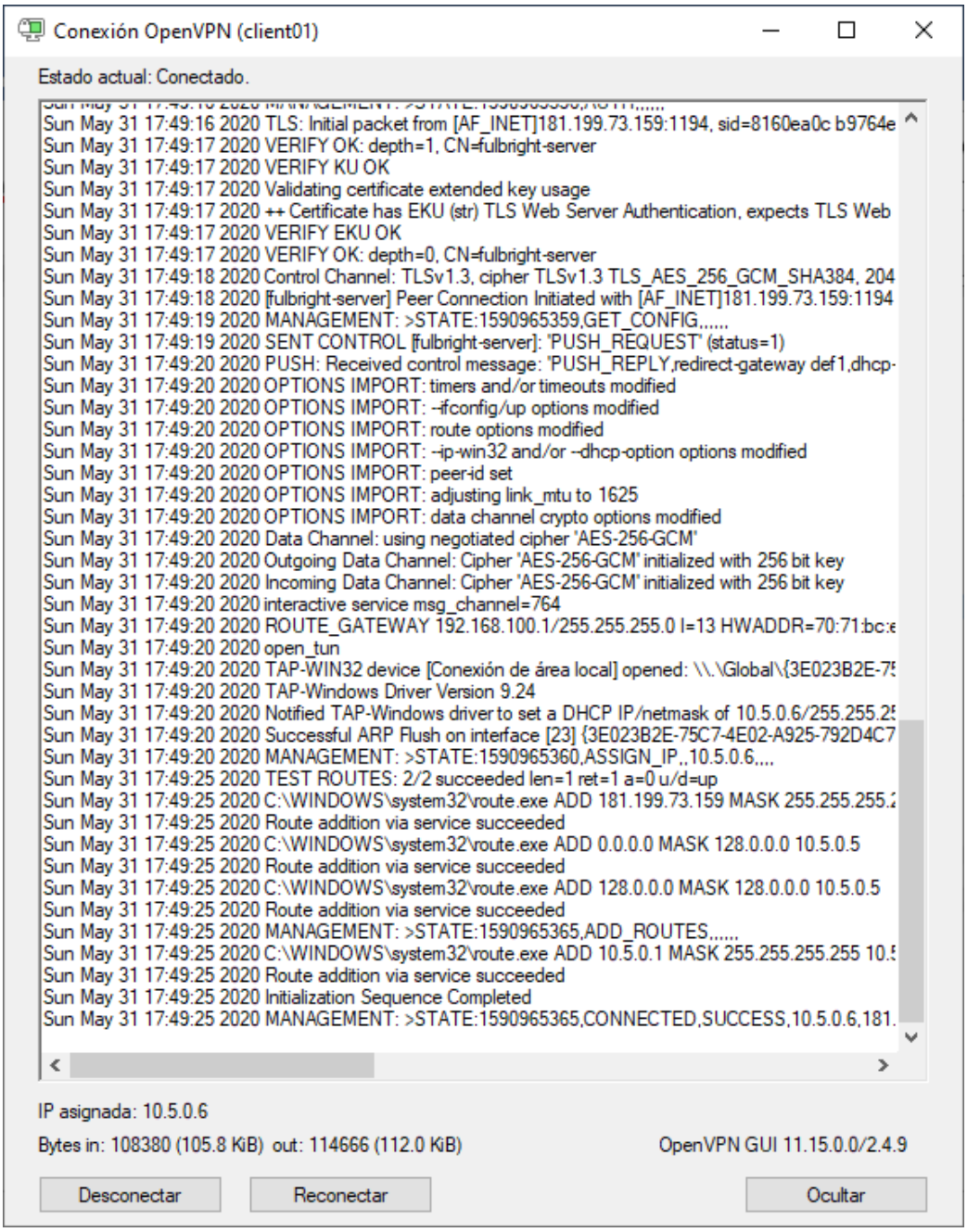

Figura 5. 3 Log de conexión del cliente al servidor de OpenVPN

Es importante detallar algunas de las partes del log de conexión, que presenta lo siguiente:

En la figura 5.4:

- La versión de OpenVPN, la versión de sistema operativo cliente y la versión de librerías OpenSSL y Lzo.
- La IP del servidor, el puerto a utilizarse (1194) y el protocolo de conexión (UDP o TCP).

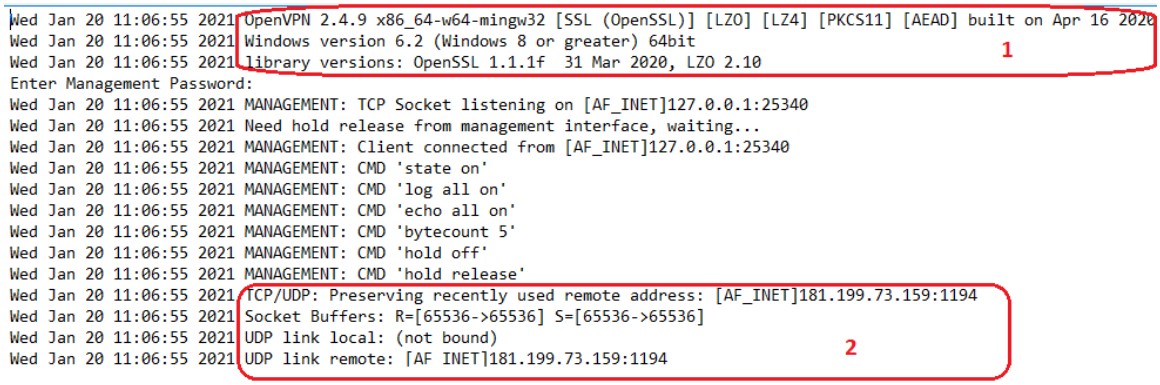

Figura 5. 4 Log de conexión, IP del servidor, puerto y protocolo TCP/UDP

En la figura 5.5:

Se observan la verificación de los métodos de autenticación.

Figura 5. 5 Log con verificación de los métodos de autenticación

En la figura 5.6, se observan el método de encriptación a utilizar

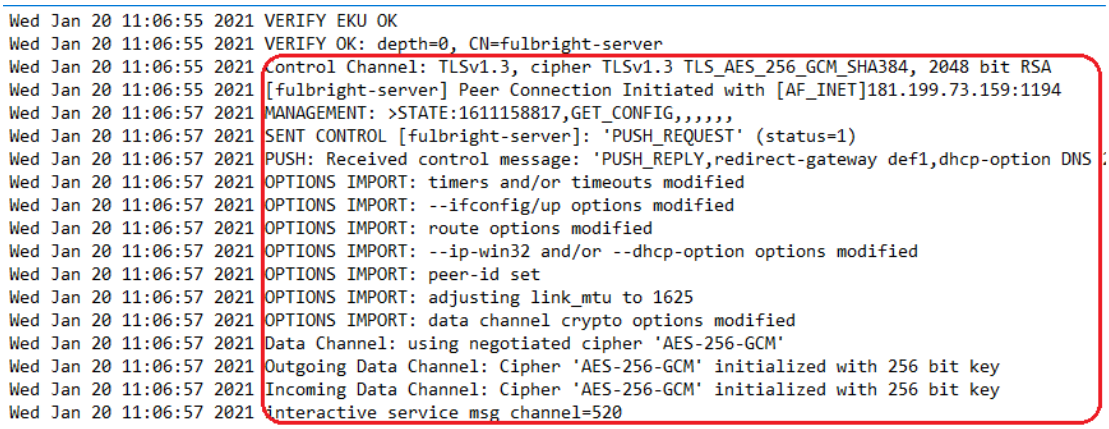

Figura 5. 6 Log con método de encriptación usado por OpenVPN

En la figura 5.7, se tiene:

- El ruteo desde las diferentes redes que se tienen: la red local, la vpn y la IP del servidor.
- Finalmente, se tiene la conexión establecida completamente.

```
Wed Jan 20 11:06:57 2021 ROUTE_GATEWAY 192.168.20.1/255.255.255.0 I=17 HWADDR=f4:b7:e2:b1:2d:c1
Wed Jan 20 11:06:57 2021 open_tun
Wed Jan 20 11:06:57 2021 TAP-WIN32 device [Conexión de área local] opened: \\.\Global\{FE335804-5BC2-4C06-B9BC-CB5555765DE5}.t
Wed Jan 20 11:06:57 2021 TAP-Windows Driver Version 9.24
Wed Jan 20 11:06:57 2021 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.5.0.10/255.255.255.252 on interface {FE335
Wed Jan 20 11:06:57 2021 Successful ARP Flush on interface [24] {FE335804-5BC2-4C06-B9BC-CB5555765DE5}
Wed Jan 20 11:06:57 2021 MANAGEMENT: >STATE:1611158817,ASSIGN_IP,,10.5.0.10,,,,
Wed Jan 20 11:07:02 2021 TEST ROUTES: 2/2 succeeded len=1 ret=1 a=0 u/d=up
Wed Jan 20 11:07:02 2021 C:\Windows\system32\route.exe ADD 181.199.73.159 MASK 255.255.255.255 192.168.20.1
Wed Jan 20 11:07:02 2021 Route addition via service succeeded
Wed Jan 20 11:07:02 2021 C:\Windows\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 10.5.0.9
Wed Jan 20 11:07:02 2021 Route addition via service succeeded
Wed Jan 20 11:07:02 2021 C:\Windows\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 10.5.0.9
Wed Jan 20 11:07:02 2021 Route addition via service succeeded
Wed Jan 20 11:07:02 2021 MANAGEMENT: >STATE:1611158822,ADD_ROUTES,,,,,,
Wed Jan 20 11:07:02 2021 C:\Windows\system32\route.exe ADD 10.5.0.1 MASK 255.255.255.255 10.5.0.9
Wed Jan 20 11:07:02 2021 Route addition via service succeeded
Wed Jan 20 11:07:02 2021 Initialization Sequence Completed
Wed Jan 20 11:07:02 2021 MANAGEMENT: >STATE:1611158822,CONNECTED,SUCCESS,10.5.0.10,181.199.73.159,1194,,
```

1

2

Figura 5. 7 Ruteo de la conexión VPN

Luego de establecerse de manera correcta la conexión de OpenVPN, el icono debe verse de color verde como se presenta en la figura 5.8

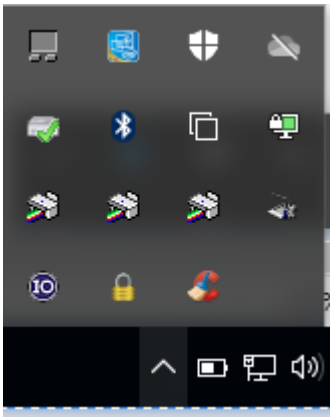

Figura 5. 8 Icono de OpenVPN conectado

Así se tendrá conectado el equipo remoto a la red de la comisión Fulbright, para poder utilizar los servicios de la red local.

5.1.2. Pruebas de conexión

Desde el equipo local se pude probar con ping a la red de la Comision Fulbright para esto primero se tiene OpenVpn sin conectar ver figura 5.9, se puede ver que no existe respuesta desde el equipo de la red local.

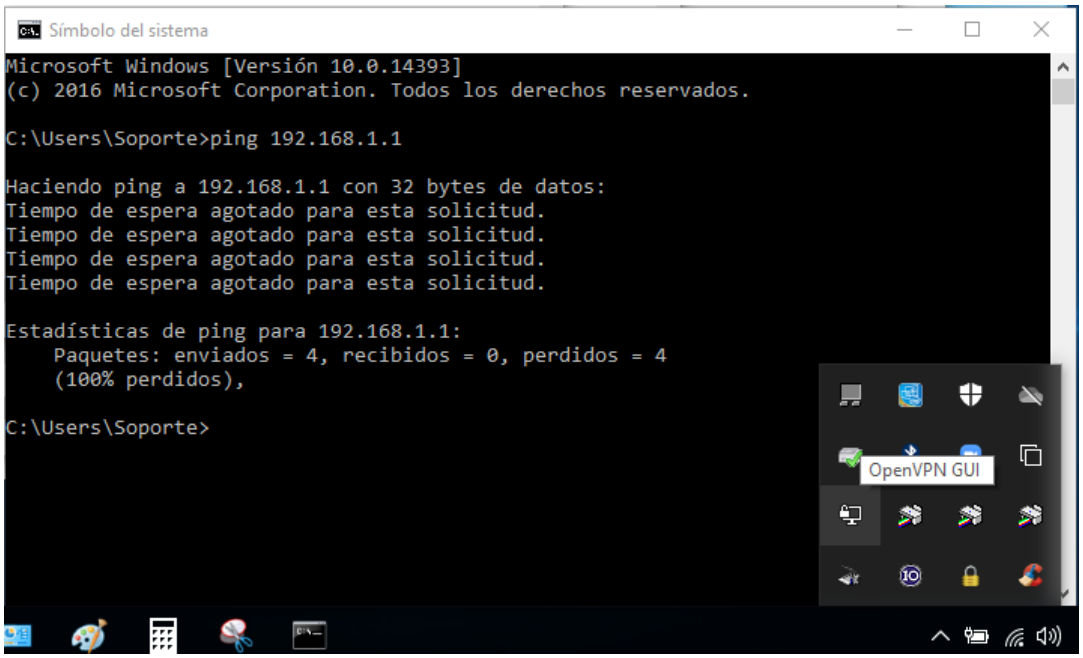

Figura 5. 9 Ping a equipo de la red local con OpenVPN desconectada

Como se puede verificar en la figura 5.10, al estar conectada la VPN existe respuesta desde la red local de las oficinas de la Comisión Fulbright, desde un computador externo a dichas oficinas

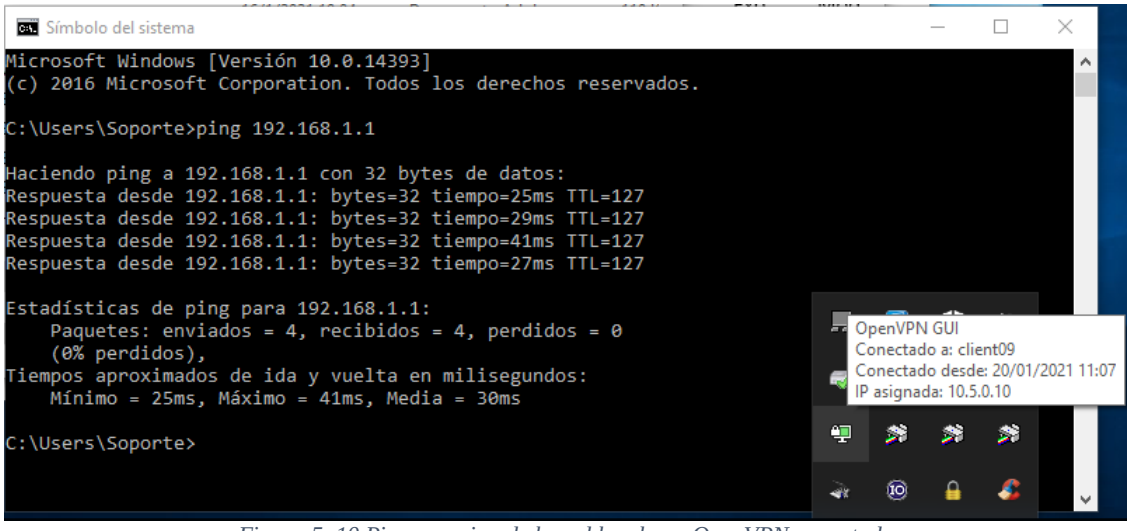

Figura 5. 10 Ping a equipo de la red local con OpenVPN conectada

En la figura 5.11, se realiza un tracert para ver la ruta que se sigue para llegar al equipo en la red de la Comision Fulbright desde el equipo externo, como se puede ver pasa por el Gateway de la VPN y por el Gateway de la oficina.

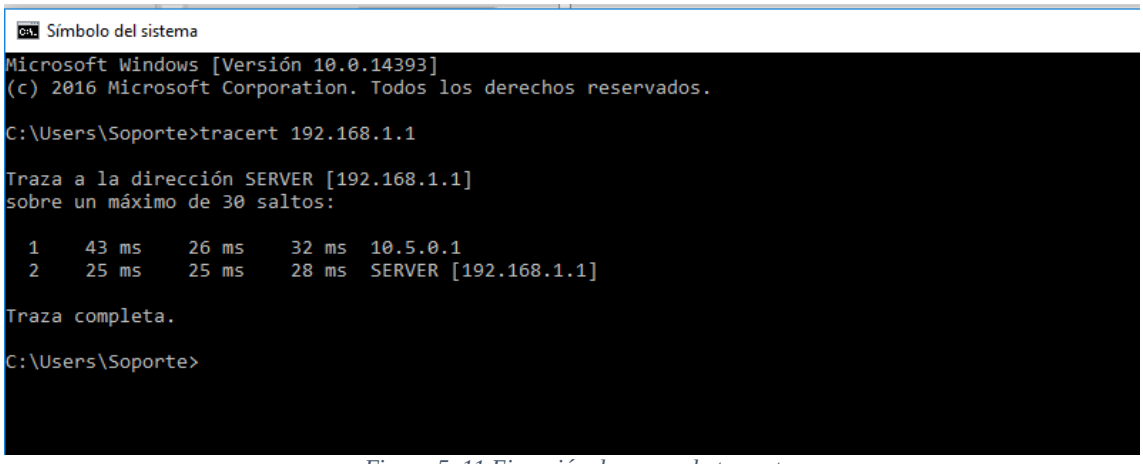

Figura 5. 11 Ejecución de comando tracert

5.1.3. Pruebas de acceso a red local y uso de servicios

Se comprueba que el firewall redireccione el puerto 2222 al 22 para tener acceso externo al servidor CentOS.

En la figura 5.12 y 5.13, se comprueba que a través del puerto 22 que es el que por defecto se utiliza para conexión ssh no es posible realizar la comunicación debido a que el proveedor de internet mantiene cerrado el puerto.

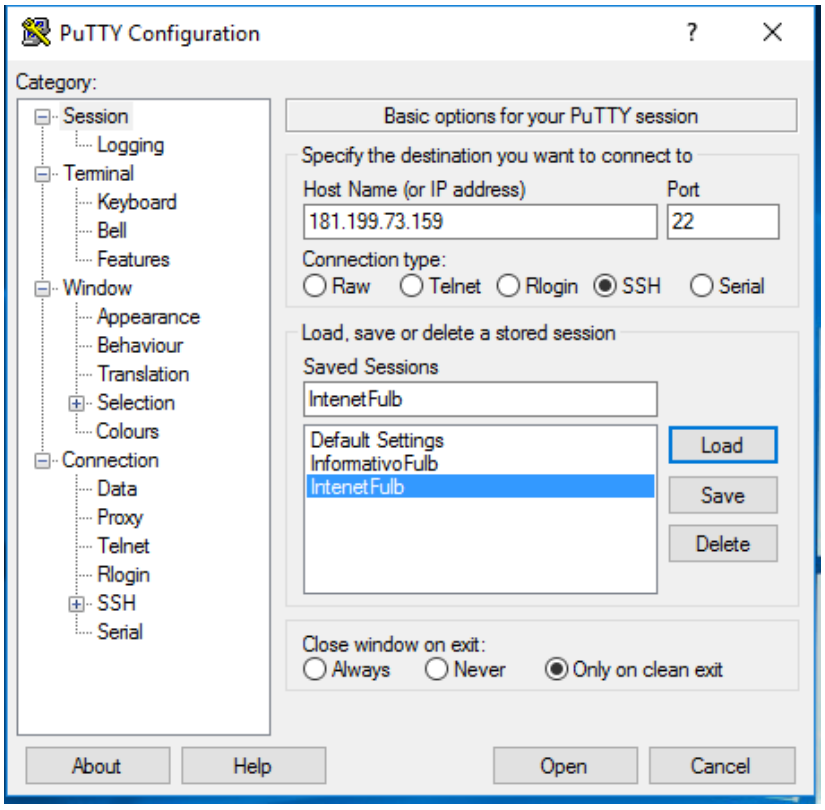

Figura 5. 12 Cliente ssh con licencia libre, conectado por puerto 22

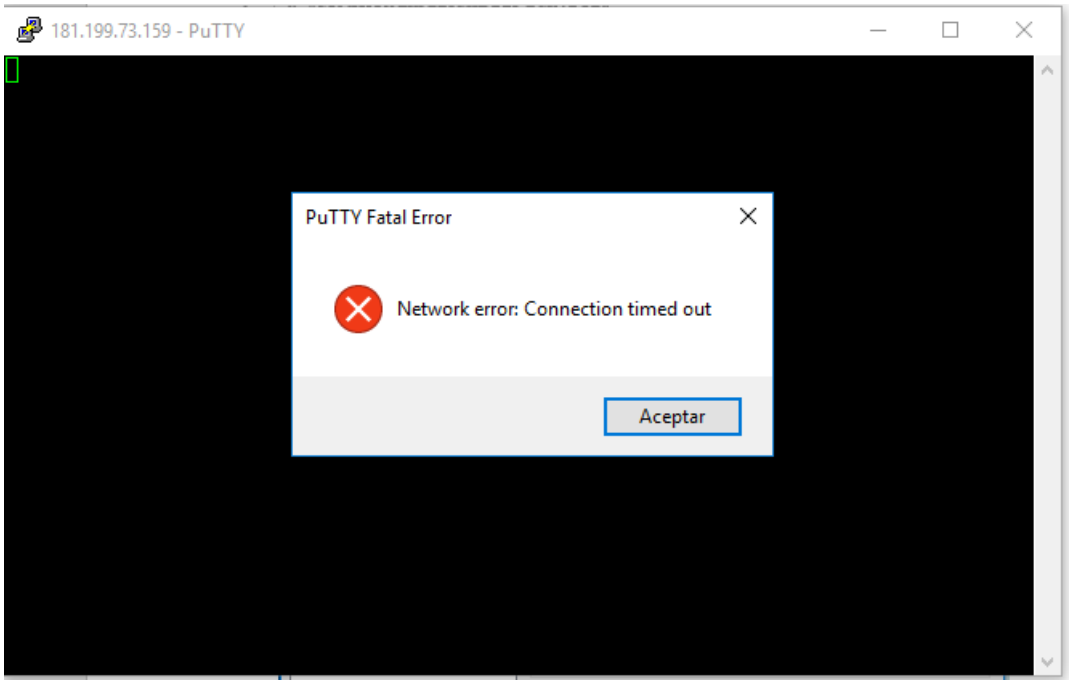

Figura 5. 13 Error de conexión a servidor CentOS por ssh. al puerto 22

En la figura 5.14 y 5.15, una vez habilitado el redireccionamiento de puerto en el firewall, se observa que es posible acceder al servidor linux a través del puerto 2222.

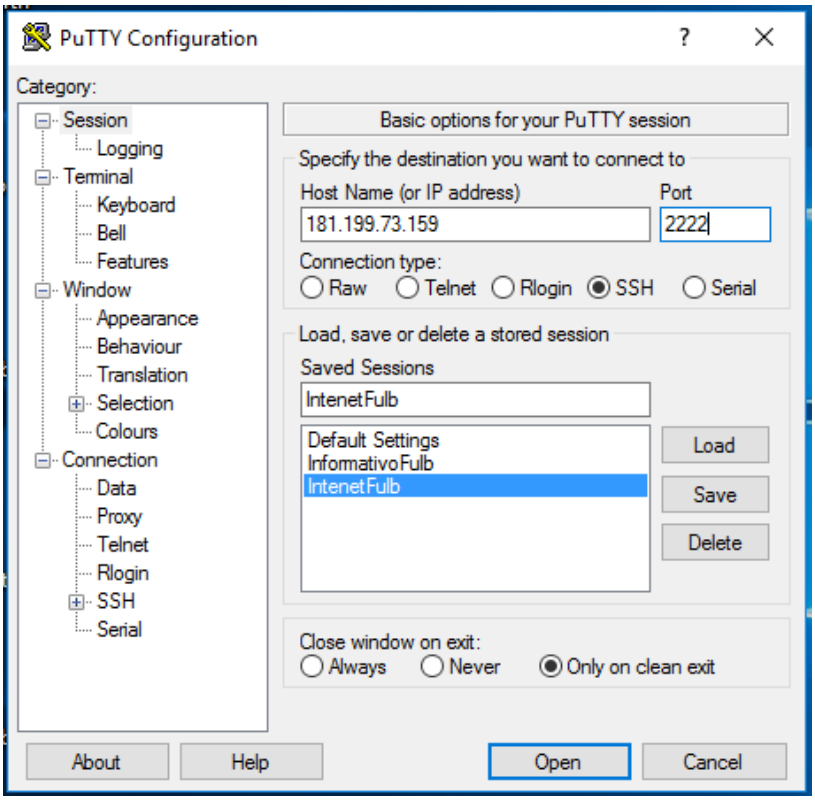

Figura 5. 14 Putty cliente ssh, conectado por puerto 2222

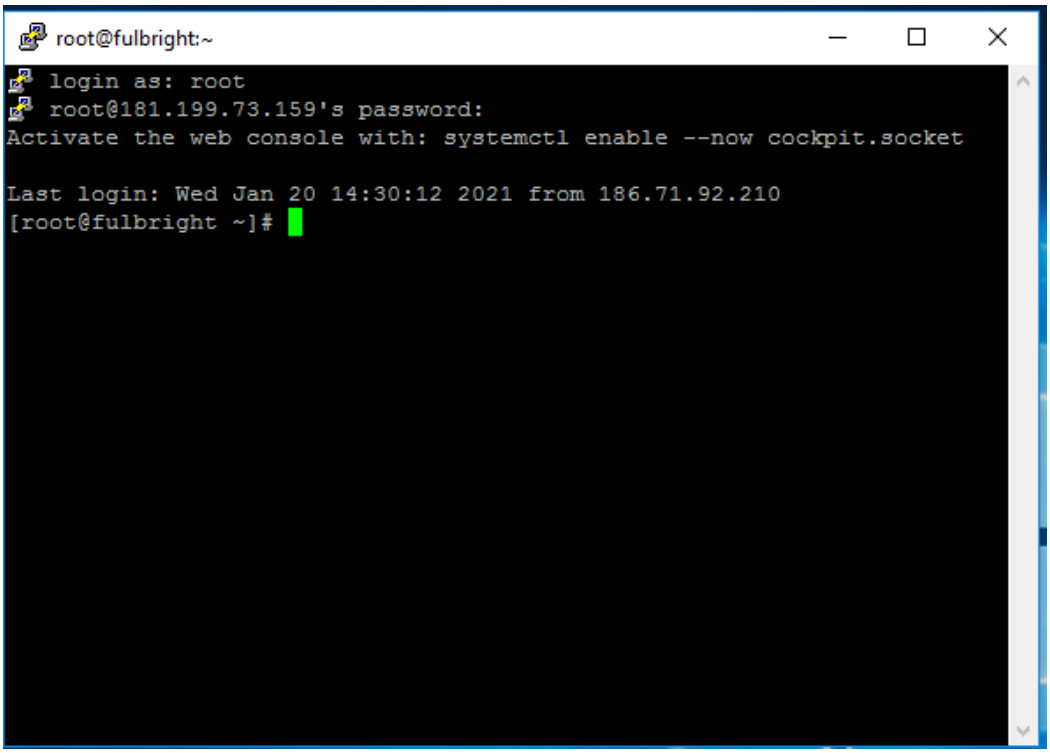

Figura 5. 15 Putty conectado exitosamente con el servidor CentOS por el puerto 2222

Se comprueba que se tiene acceso a las carpetas compartidas del equipo 192.168.1.1, para esto se debe abrir el explorador de archivos y digitar la dirección IP del equipo al que se desea acceder, ver figura 5.17, es importante indicar que esto se lo puede hacer si se cuenta con usuario y clave del usuario del dominio con los permisos respectivos como se observa en la figura 5.16.

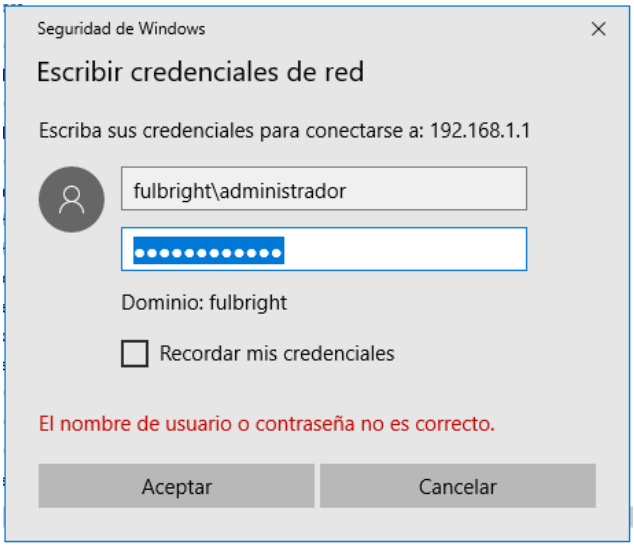

Figura 5. 16 Ingreso de credenciales a carpeta compartida

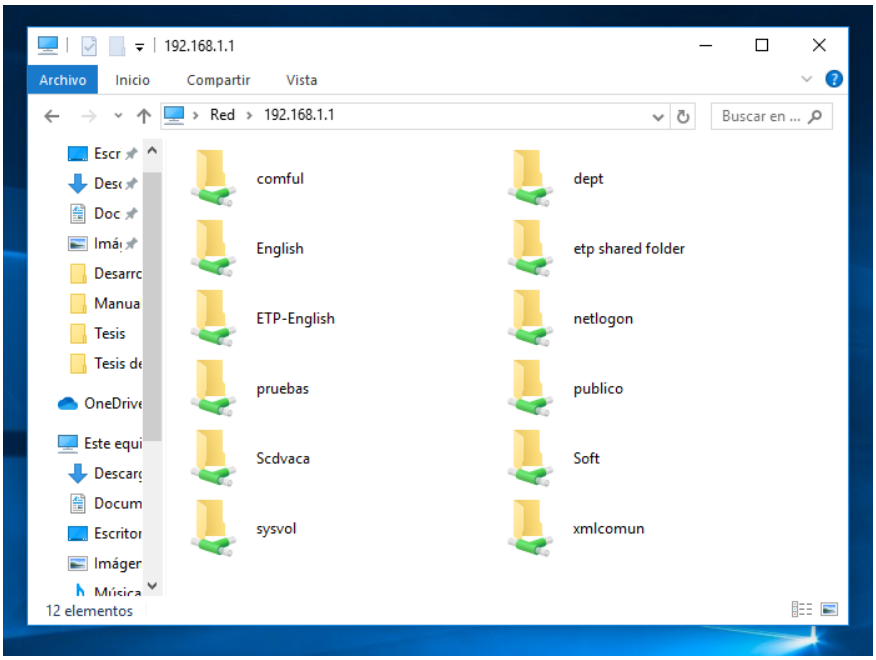

Figura 5. 17 Explorador de archivos con acceso a las carpetas compartidas.

5.1.4. Pruebas de acceso remoto a los computadores.

Se comprueba que se puede ingresar a un equipo de la red local de la Comision Fulbright por escritorio remoto.

Se presiona el icono buscar en Windows, y se digita "escritorio remoto", ver figura 5.18

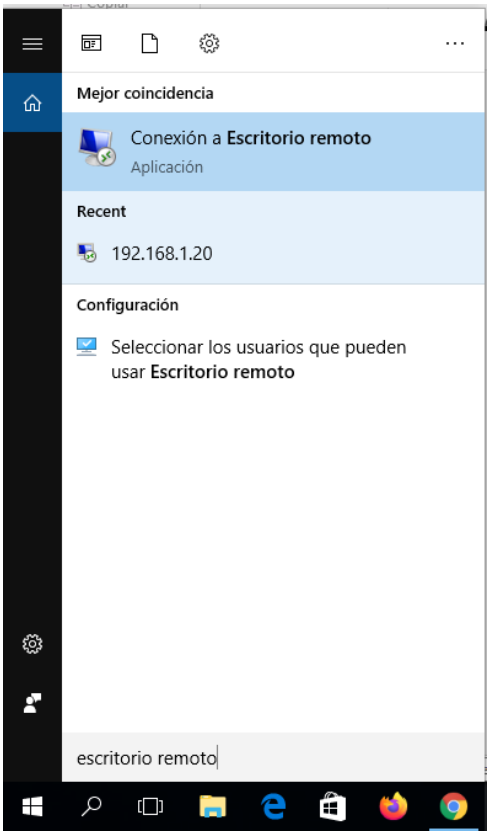

Figura 5. 18 Acceso a escritorio remoto de S.O. Windows

Se debe dar doble click sobre conexión a Escritorio remoto, esto abrirá una ventana donde se debe digitar la IP del equipo al que se desea acceder por escritorio remoto, ver figura 5.19.

Ejemplo: Equipo 192.168.1.20

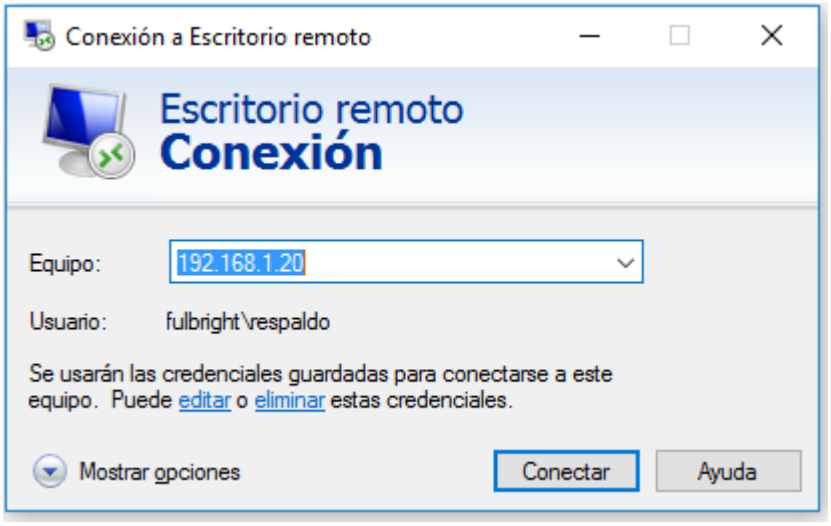

Figura 5. 19 Ventana de Conexión de Escritorio remoto

Se presiona conectar, se solicitará ingresar Usuario de dominio fulbright y la contraseña, se digitan las credenciales y se presiona aceptar, ver figura 5.20

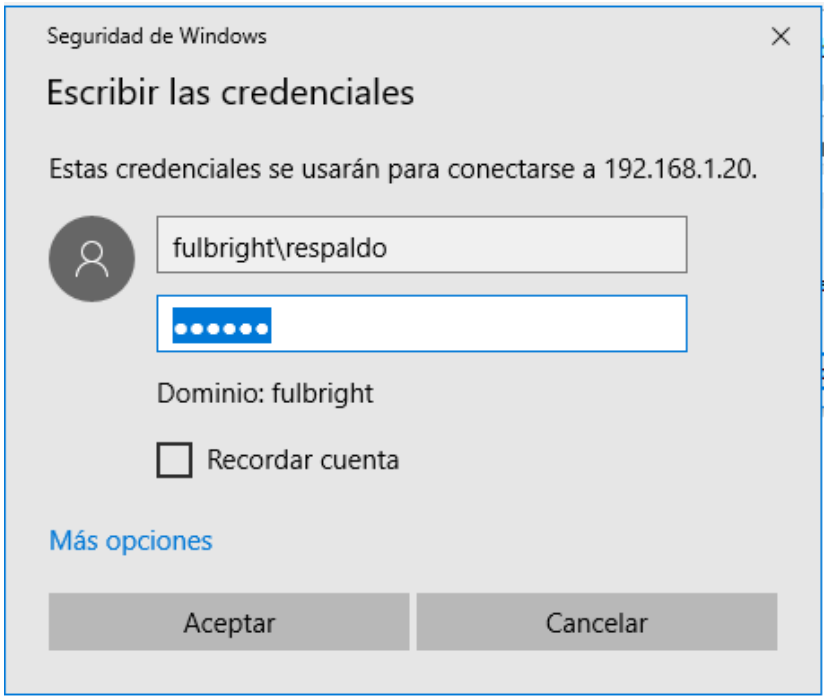

Figura 5. 20 Ingreso de credenciales de acceso remoto

En la figura 5.21 se puede ver que se accede al equipo 192.168.1.20 sin inconvenientes.

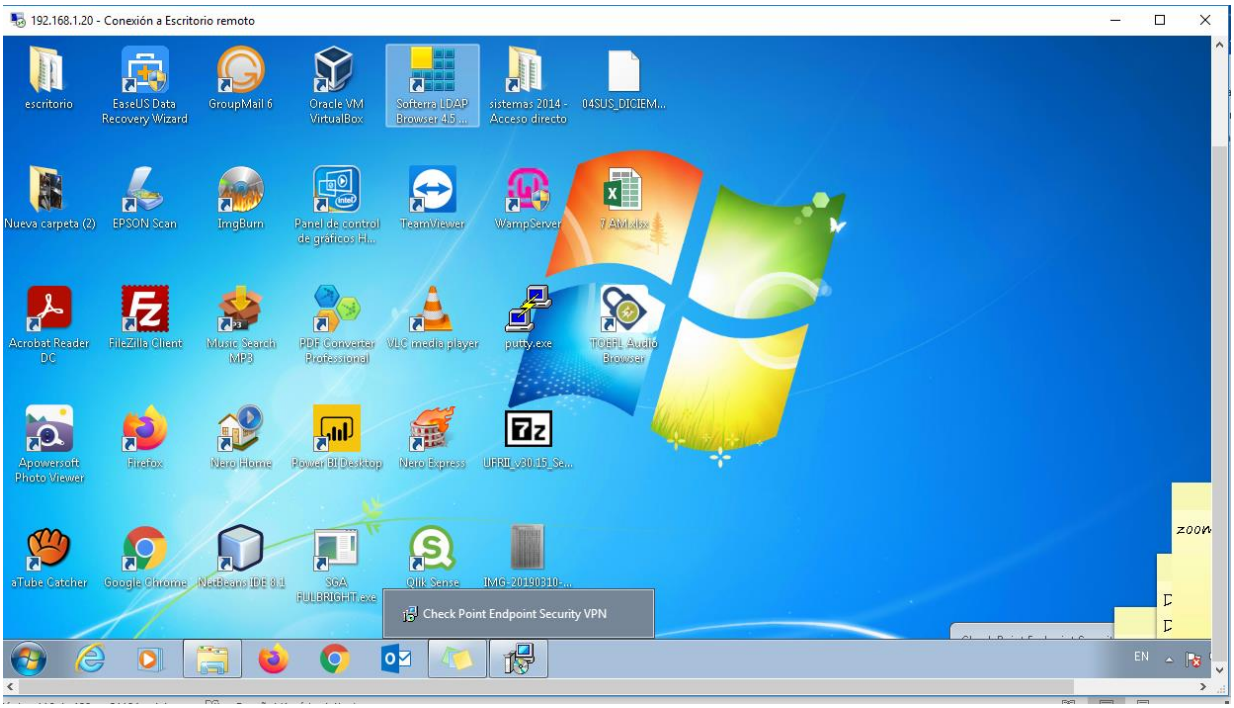

Figura 5. 21 Acceso remoto de manera exitosa a 192.168.1.20

De igual manera como se observa en la figura 5.23, es posible verificar que se puede utilizar la aplicación Scaf (sistema académico) que es una de las aplicaciones que se utiliza por parte de los funcionarios de la Comision Fulbright.

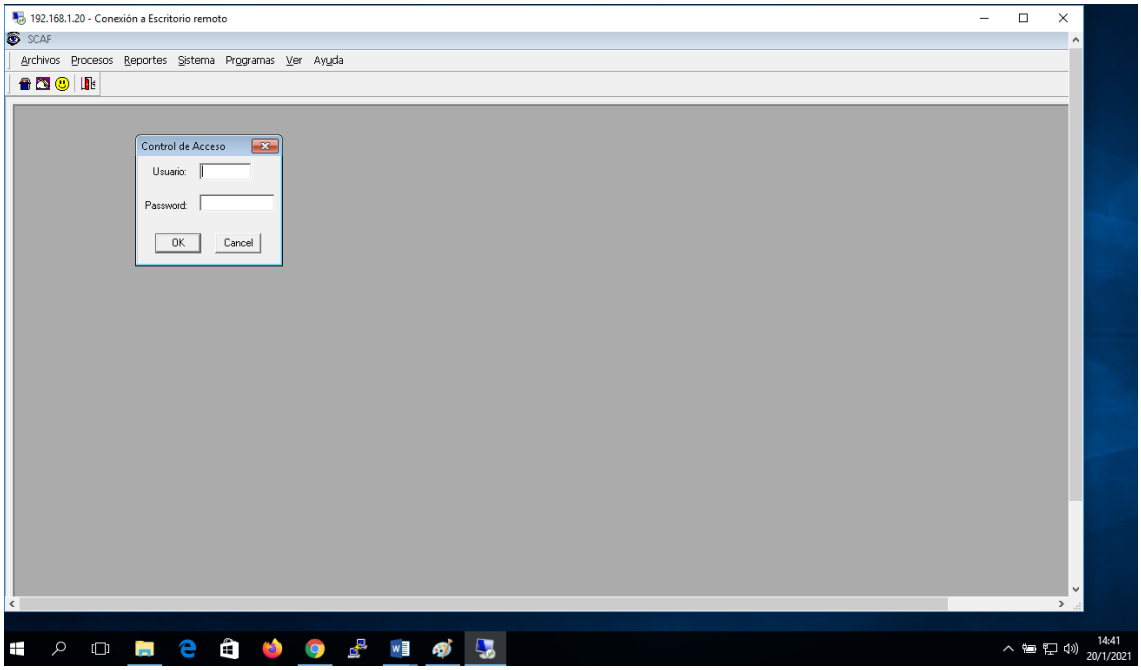

Figura 5. 22 Acceso remoto a Scaf, aplicación de uso local

De igual manera se puede acceder al sistema de contabilidad como se observa en la figura 5.24

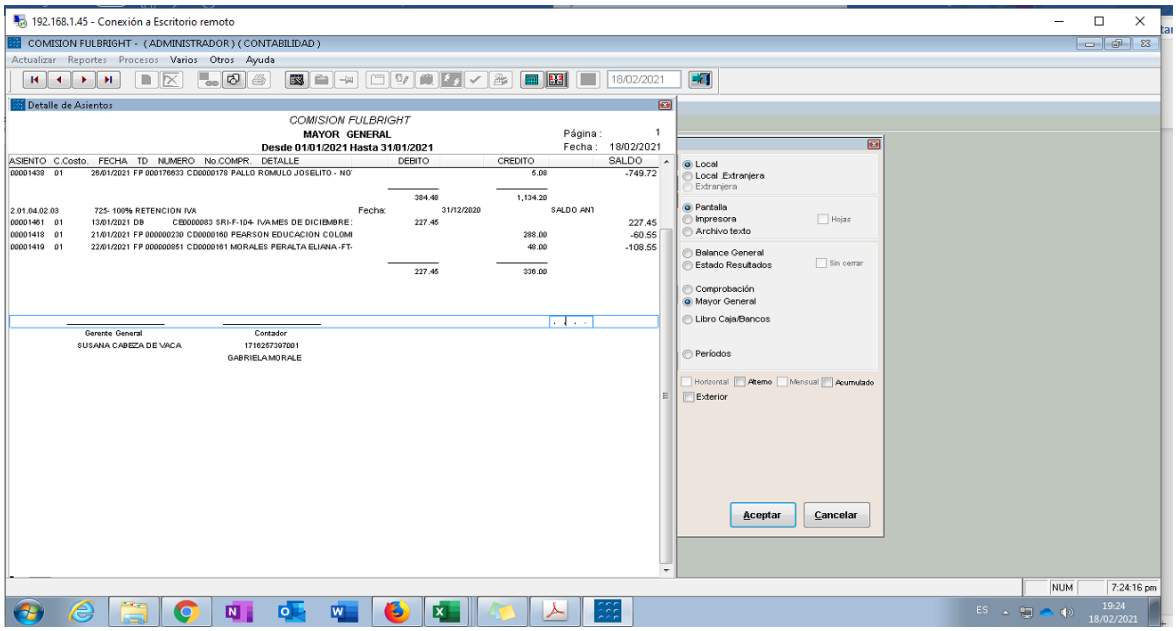

Figura 5. 23 Acceso remoto al sistema de contabilidad conectado con OpenVPN

5.2. Evaluar funcionamiento del servicio

5.2.1. Análisis de tráfico

Para realizar el análisis de tráfico, como se observa en la figura 5.25 se debe tener establecida la conexión del cliente openVPN.

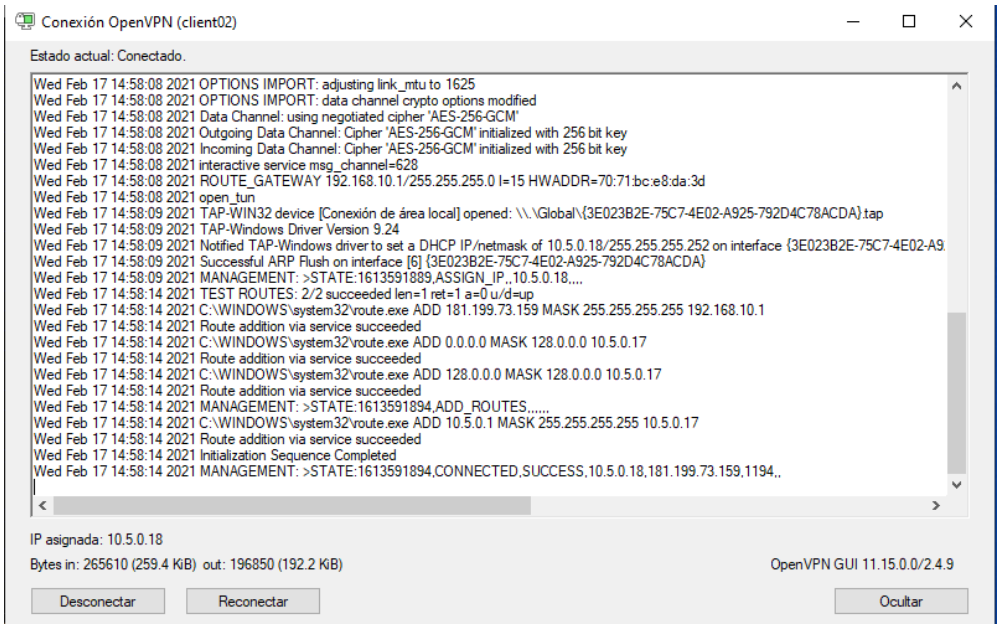

Figura 5. 24 Conexión OpenVPN establecida

Se realiza ping a 10.5.0.1, que es la IP del servidor OpenVPN de la tarjeta de red virtual creada por la herramienta VPN

En la figura 5.26, se puede ver que, de 21075 paquetes enviados, se reciben 21075 es decir existe 0 perdida de paquetes en la conexión OpenVPN establecida.

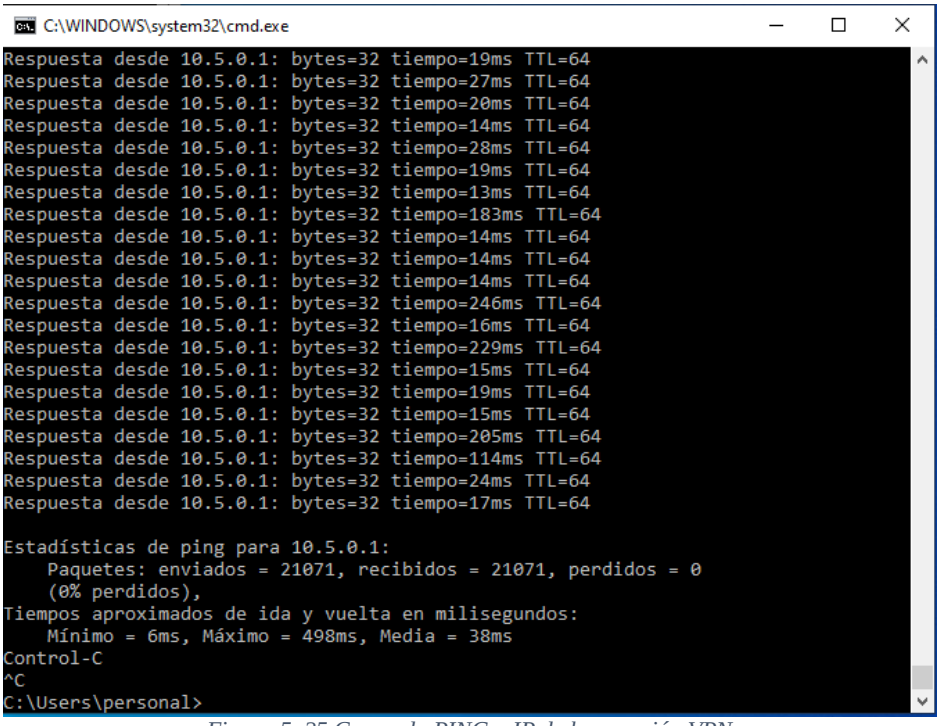

Figura 5. 25 Comando PING a IP de la conexión VPN

A manera de prueba adicional se ejecuta ping a una IP de la red local en este caso al 192.168.1.1como se observa en la figura 5.27, en dicha prueba se encuentra que, de 21096 paquetes enviados, se reciben 21096 con 0 paquetes perdidos.

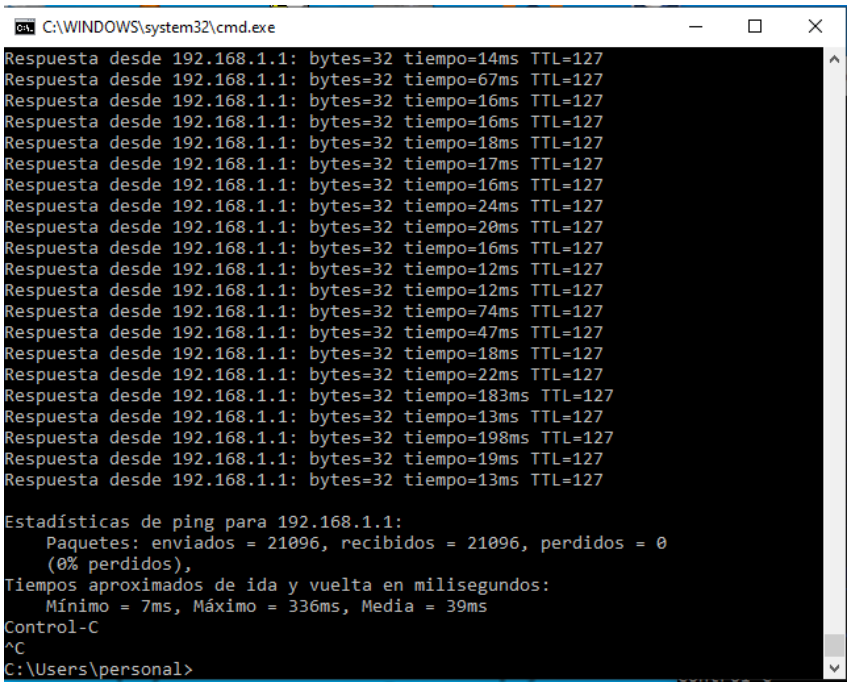

Figura 5. 26 Comando PING al servidor de la red local COMISION FULBRIGHT

De las pruebas realizadas se puede evidenciar que se tiene una conexión estable.

5.2.2. Prueba de encriptación

Durante el proceso de conexión del cliente al servidor OpenVPN, se realizan varios pasos entre estos estan la autenticación donde se establece las características del cifrado a utilizar como se puede observar en la figura 5.28

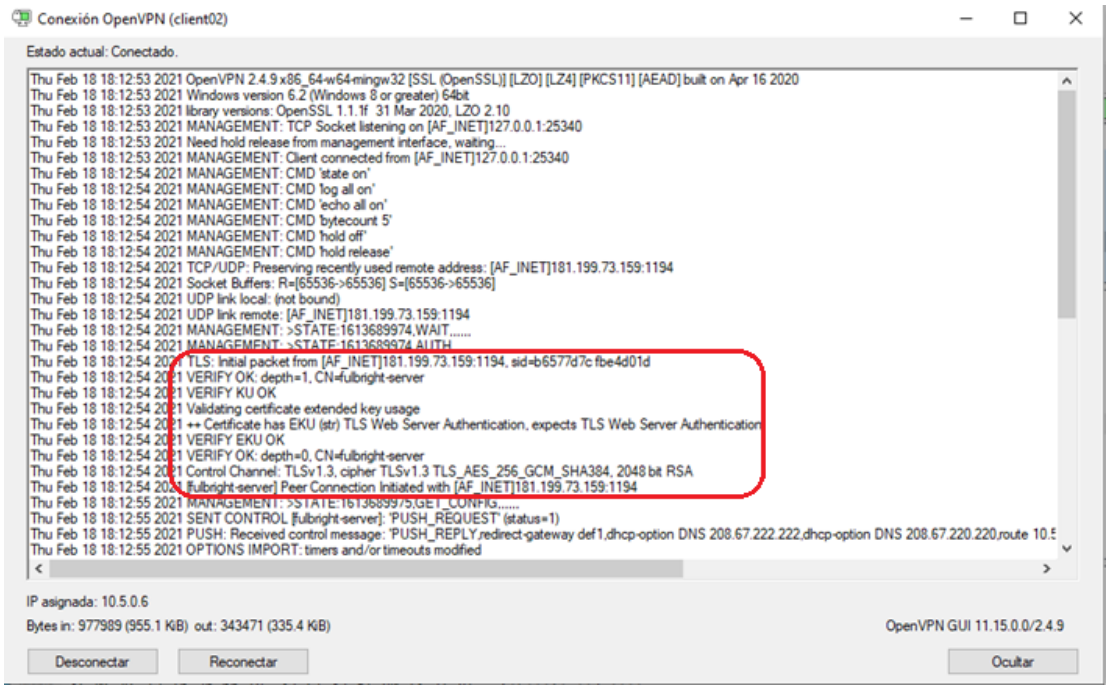

Figura 5. 27 Métodos de autenticación parte1

En la figura 5.29 se observa que el cifrado a utilizarse es AES-256 con 256 bits, lo que garantiza un alto grado de cifrado.

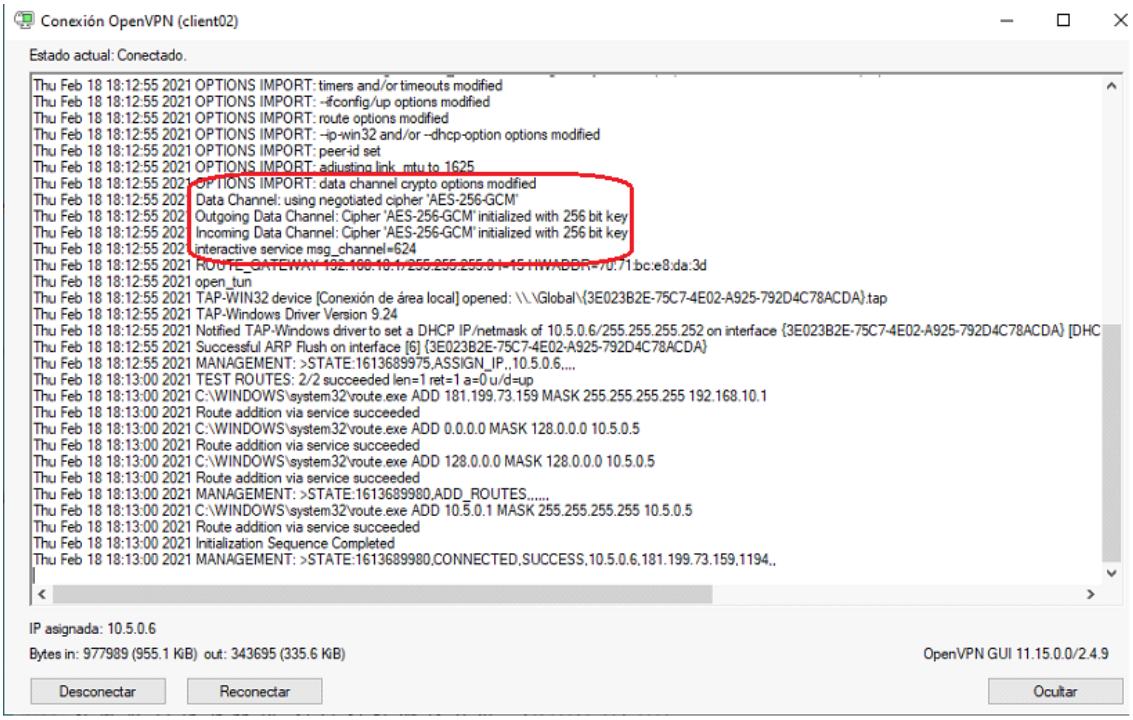

Figura 5. 28 Métodos de autenticación parte2

Para validar que se realiza la encriptación en el momento de establecer la conexión VPN se procede a utilizar WireShark Network Analizer.

Como se observa en la figura 5.30 se debe instalar y abrir la aplicación WireShark en el equipo que tiene instalado y en ejecución el cliente de OpenVPN, se selecciona la red de área local de la cual se va a capturar el tráfico.

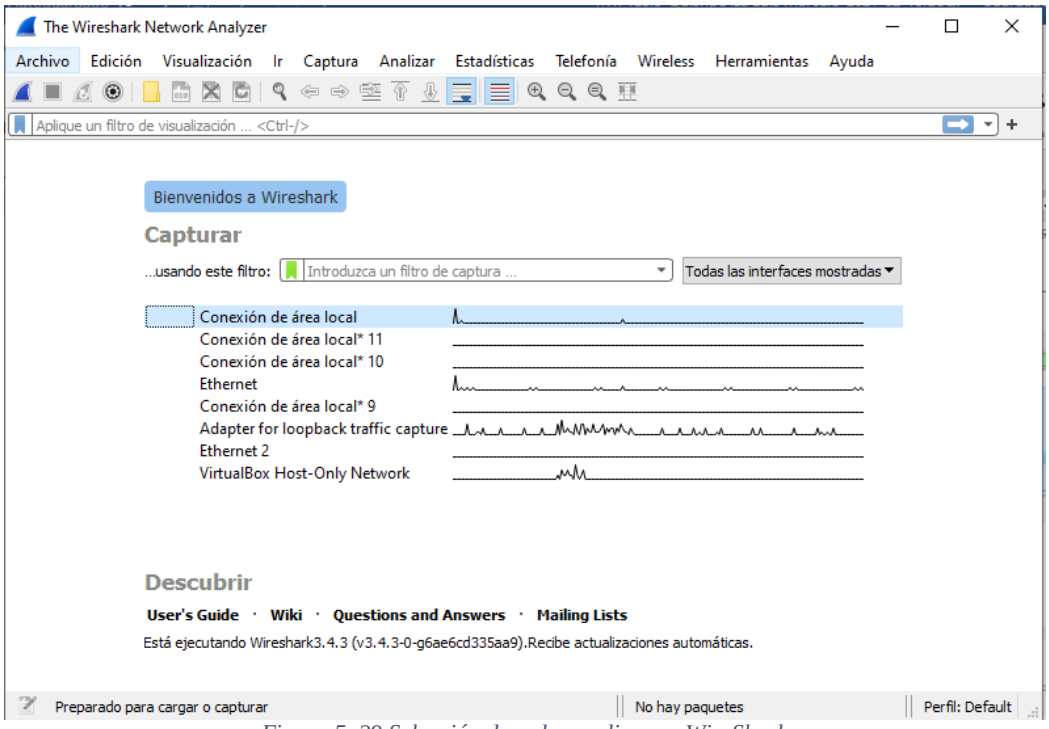

Figura 5. 29 Selección de red a analizar en WireShark

Como se observa en la figura 5.31, en el filtro de búsqueda se digita OpenVPN, esto seleccionará los paquetes con el protocolo OpenVPN, luego de lo cual se escoge cualquier paquete de la lista para que muestre la información del mismo, en el área de datos se observa que la transmisión se muestre como un galimatías, eso significa que el cifrado de VPN está funcionando de manera correcta.

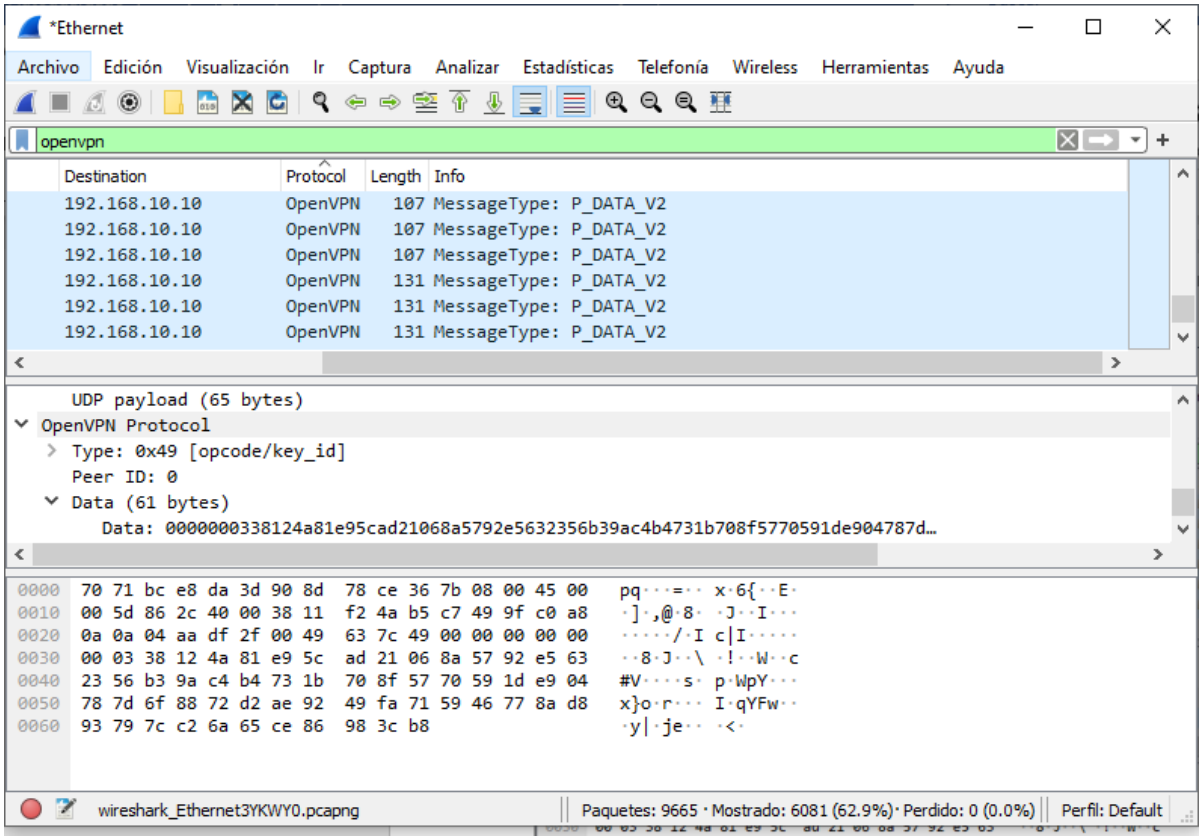

Figura 5. 30 Información de paquetes OpenVNP

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

Una vez establecidos los requerimientos y recursos de los que dispone la empresa, se utilizará el servicio de internet PYME de 75 Mbps con una dirección IP pública como medio para la conexión VPN, se realizará la compra de un computador clon mejorado para ser utilizado como servidor VPN, de igual manera la infraestructura de red local es aceptable para el funcionamiento adecuado de red privada virtual.

Luego de revisados los conceptos teóricos y analizadas las diferentes tecnologías existentes para realizar el diseño de la VPN, se ha llegado a la conclusión que se debe utilizar el sistema operativo Linux CentOS, con la versión 8, como software de red privada virtual OpenVPN, para servicio de firewall se utilizará firewalld y como servidor proxy a Squid proxy.

Una vez realizada la instalación y configuración de Linux CentOS, Firewalld, Squid Proxy y OpenVPN, se concluye que se cumple con la implementación de la red privada virtual y se establece el manual técnico de configuración de nuevos usuarios como anexo 1, con lo cual el administrador del servicio podrá agregar o eliminar cuentas de manera sencilla.

Una vez evaluado la red privada virtual, realizando la verificación de conectividad, pruebas de conexión, pruebas de pérdidas de paquetes, pruebas de acceso a la red local, pruebas de acceso remoto y prueba de encriptación se verifica que se cuenta con una red privada virtual con un adecuado funcionamiento y con la seguridad necesaria.

Realizada la implementación de la red privada virtual ha sido posible que los empleados de la COMISION FULBRIGHT DEL ECUADOR que requerían acceso de manera remota lo puedan realizar de manera sencilla, siendo para esto necesario únicamente el contar con el servicio de internet, los empleados podrán conectarse a la red local y por ende a los sistemas y servicios con los que se cuentan en la empresa desde cualquier sitio, para lo cual se estructuró una guía de usuario como anexo 2.

La implementación de la red privada virtual se ha realizado con un costo mínimo comparado con otras soluciones en las cuales se requieren adquirir equipos y licencias de uso, dado que en

este caso ha sido necesario únicamente el adquirir un equipo clon mejorado y no ha sido necesario adquirir licencias de ningún tipo al utilizar herramientas y sistemas de software libre.

6.2. RECOMENDACIONES

Se recomienda a la institución actualizar el plan de internet al siguiente ofertado que es de 100MB simétrico, para evitar tener inconvenientes si en algún momento es necesario que todos los empleados se encuentren laborando de manera simultánea.

Se recomienda utilizar equipos con sistema operativo Windows8 o superior, dado que existen problemas de compatibilidad con Windows7 al utilizar Outlook de escritorio de office365 con la VPN activa.

Se recomienda el crear un cliente de conexión a OpenVPN por cada usuario del servicio para poder realizar la eliminación de dicho cliente, sin afectar a otros usuarios el momento en que un usuario deje de laborar en la institución o se necesite retirar el acceso por alguna disposición.

Se recomienda el realizar el proceso de eliminación de cuentas cliente el momento de que un usuario de OpenVPN deje de laborar para la institución, así como el establecer políticas de manejo de credenciales de acceso para de esta manera mantener un ámbito de seguridad adecuado.

Se recomienda solicitar al proveedor de internet el cambio del tipo de fibra óptica de la última milla a una fibra con protección anti roedores, dado que los últimos meses se han presentado roturas por esta causa, presentando como inconveniente que los funcionarios no puedan conectarse a la VPN al quedarse las oficinas sin el servicio de internet.

El poder contar con un enlace VPN para que los empleados puedan realizar sus labores desde el exterior de las instalaciones, es decir sin necesidad de asistir de forma física a una oficina debe ser tomado en cuenta por las empresas e instituciones del Ecuador como una opción más de trabajo, estando conscientes de que esto no solo implica beneficios para los empleados sino también ahorro en los gastos que se producen al tener el personal de manera presencial en la empresa.

7. BIBLIOGRAFÍA

Arul, M. (13 de Diciembre de 2019). *Cómo instalar el servidor y el cliente OpenVPN con Easy-RSA 3 en CentOS 8*. Obtenido de https://www.howtoforge.com/tutorial/how-to-install-openvpn-server-and-client-with-easy-rsa-3-on-centos-8/

bluehosting. (Agosto de 2016). *Introducción a FirewallD en CentOS*. Obtenido de https://docs.bluehosting.cl/tutoriales/servidores/introduccion-a-firewalld-en-centos.html

Cactusvpn. (2019). *Que es OpenVPN y como funciona*. Obtenido de https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/que-es-openvpn/#:~:text=Desventajas%20de%20OpenVPN-,Ventajas,m%C3%A1s%20control%20sobre%20sus%20conexiones.

Carvajal Chávez, C. A. (2019). La encriptación de datos empresariales: ventajas y desventajas. Obtenido de https://recimundo.com/index.php/es/article/view/487

Castillo, J. A. (5 de abril de 2020). *Qué es OpenVPN y qué características nos da en las Redes Privadas Virtuales*. Obtenido de https://www.profesionalreview.com/2020/04/05/openvpn-que-es/

Cisco. (2020). *Cisco AnyConnect Secure Mobility Client.* Obtenido de https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45-578609.pdf

Díaz Llatance, M. A., & Vieyra Dioses, G. L. (2015). *DISEÑO DE UNA RED PRIVADA VIRTUAL PARA INTERCONECTAR LAS SUCURSALES DE LA EMPRESA TERRACARGO SAC.* Lambayeque, Perú. Obtenido de http://repositorio.unprg.edu.pe/handle/UNPRG/462

DigitalOcean. (7 de Mayo de 2020). *Cómo instalar un firewall con firewalld en CentOS 8*. Obtenido de https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-8-es#:~:text=El%20demonio%20firewalld%20gestiona%20grupos,comportamientos%20debe%20permitir%20el%20firewall.

ECURED. (2020). *Software libre*. Obtenido de https://www.ecured.cu/Software_libre

G.B., S. (Dic de 2020). *Como configurar firewalld en CentOS 8*. Obtenido de https://www.sololinux.es/como-configurar-firewalld-en-centos-8/

Genbeta. (25 de Octubre de 2020). *Los mejores cortafuegos para proteger tu equipo Linux*. Obtenido de https://www.genbeta.com/linux/mejores-cortafuegos-para-proteger-tu-equipo-linux

GNU. (Octubre de 2020). *El Sistema Operativo GNU*. Obtenido de https://www.gnu.org/philosophy/free-sw.es.html

Guiadev. (2014). *Mejores firewalls para Linux*. Obtenido de https://guiadev.com/mejores-firewalls-para-linux/

Hipertextual. (2013). *Las mejores herramientas para trabajar desde casa con VPN*. Obtenido de https://hipertextual.com/archivo/2013/10/trabajar-casa-con-vpn/

ID Group. (Agosto de 2020). *Qué es un Firewall y cómo funciona*. Obtenido de https://idgrup.com/firewall-que-es-y-como-funciona/#:~:text=Un%20firewall%2C%20tambi%C3%A9n%20llamado%20cortafuegos,ordenadores%20de%20una%20misma%20red.

Jota Fonseca, Y. M., Ramirez Castañeda, D. S., & Penagos Arévalo, A. R. (2018). *DISEÑO DE UNA RED PRIVADA VIRTUAL (VPN) CON SEGURIDAD L2PT PARA LA EMPRESA LABORATORIOS EXPOFARMA S.A.* Bogotá, Colombia. Obtenido de https://repository.ucc.edu.co/handle/20.500.12494/6193

LimeVpn. (2020). *Softether VPN vs OpenVPN*. Obtenido de https://www.limevpn.com/softether-vpn-vs-openvpn-which-one-is-better-for-you-and-why/

LinuxAdictos. (2019). *Las mejores distribuciones GNU/Linux de 2019*. Obtenido de https://www.linuxadictos.com/mejores-distribuciones-gnu-linux-2019.html

linuxadictos. (2020). *Linux Distros for Business: entornos abiertos para empresas*. Obtenido de https://www.linuxadictos.com/linux-distros-for-business.html

Linuxito. (Junio de 2018). *Mejorando la seguridad de un servidor OpenVPN con autenticación TLS*. Obtenido de https://www.linuxito.com/seguridad/1070-mejorando-la-seguridad-de-un-servidor-openvpn-con-autenticacion-tls

LogMeIn, I. (2017). *LogMeIn, Inc Guia de Usuario.* Obtenido de https://documentation.logmein.com/documentation/ES/pdf/Hamachi/LogMeIn_Hamachi_UserGuide.pdf

Logmeininc. (2020). *support.logmeininc.com*. Obtenido de https://support.logmeininc.com/es/central/help/que-es-logmein-hamachi-central-c-hamachi-abouthamachi

Merino, M. (20 de Octubre de 2020). *Los mejores cortafuegos para proteger tu equipo Linux*. Obtenido de https://www.genbeta.com/linux/mejores-cortafuegos-para-proteger-tu-equipo-linux

Mokhtar, E. (29 de marzo de 2017). *Servidor proxy de Linux*. Obtenido de https://likegeeks.com/es/servidor-proxy-de-linux-squid/

Nextvision. (Agosto de 2017). *Todo sobre encriptación de datos para empresas*. Obtenido de https://nextvision.com/todo-sobre-encriptacion-de-datos-para-empresas/

Oficina de Seguridad del Internauta. (1 de Julio de 2019). *¿Sabías que existen distintos tipos de cifrado para proteger la privacidad de nuestra información en Internet?* Obtenido de https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad#:~:text=Los%20dos%20tipos%20principales%20de,el%20uso%20de%20dos%20claves

OpenVpn. (2015). *OpenVpn Community*. Obtenido de https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn

Pomar Pascual, R. (2019). *Implementación de una red privada virtual de software libre en una empresa.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/94606/8/rpomarpTFG0619memoria.pdf

Quezada Lozano, H. D. (2016). *Diseño de una VPN para el acceso a las.* Loja, Ecuador. Obtenido de https://dspace.unl.edu.ec/jspui/bitstream/123456789/17159/1/Quezada%20Lozano%2C%20Henry%20Daniel.pdf

RAE. (2020). *Real Academia Española*. Obtenido de https://dle.rae.es/cifrar#3l3H2eG

Redeszone. (03 de marzo de 2019). *Las mejores distribuciones Linux para un servidor grande*. Obtenido de https://www.redeszone.net/2019/03/03/mejor-distro-linux-servidores/

Redeszone.net. (21 de Julio de 2020). *Alternativas a Hamachi: gratuitas, seguras y funcionales*. Obtenido de https://www.redeszone.net/tutoriales/vpn/alternativas-hamachi-gratuitas-seguras-funcionales/

RedHat. (2020). *¿Que es linux?* Obtenido de https://www.redhat.com/es/topics/linux

SoftEther. (2019). *Proyecto VPN SoftEther*. Obtenido de https://www.softether.org/

Softzone.es. (17 de Agosto de 2020). *Aprende a dominar la Terminal de Linux como un profesional*. Obtenido de https://www.softzone.es/programas/linux/terminal-linux/

Sololinux. (08 de 09 de 2020). *Fedora vs CentOS*. Obtenido de https://www.sololinux.es/fedora-vs-centos/

Stackscale. (Junio de 2020). *Clientes OpenVPN: cuáles utilizar y cómo instalarlos*. Obtenido de https://www.stackscale.com/es/blog/clientes-openvpn/

Vpnranks. (septiembre de 2020). *WireGuard vs OpenVPN*. Obtenido de https://es.vpnranks.com/blog/wiregu%C3%A1rd-vs-openvpn/

Zapata, M. A. (2016). *EVALUACIÓN DE PARÁMETROS DE CALIDAD DE SERVICIO (QoS) PARA EL DISEÑO DE UNA RED VPN CON MPLS.* Quito, Ecuador. Obtenido de http://repositorio.puce.edu.ec/handle/22000/12327

8. ANEXOS

8.1. ANEXO 1 MANUAL TÉCNICO DE CONFIGURACIÓN DE NUEVOS USUARIOS

Generar los clientes que van a conectarse al servidor OpenVPN

Este proceso es necesario realizarlo por cada cliente que vaya a hacer uso del servidor OpenVPN, para que de ser el caso sea posible inactivar el acceso de cada uno.

Se ingresa a la carpeta /etc/openvpn/easyrsa/

cd /etc/openvpn/easy-rsa

Como se observa en la figura 8.1 se ejecuta:

./easyrsa gen-req clientXX nopass

Siendo **XX= 12** el número de cliente que corresponda ejemplo client**12**.

Con esto se crea el requerimiento y la clave privada para el cliente, como resultado de esto se tendrán los archivos: client12.req (archivo de requerimiento) y client12.key (la clave privada)

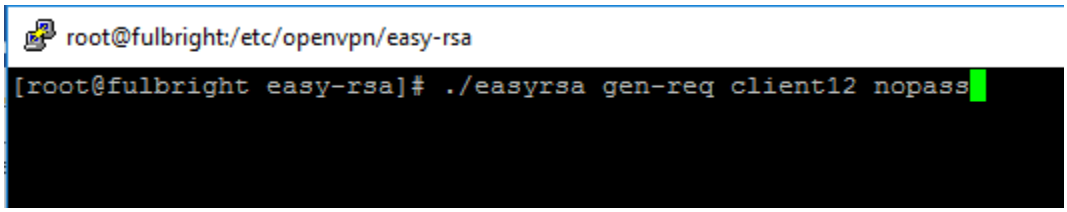

Figura 8. 1 Generar el requerimiento del nuevo usuario parte1

Se presiona ENTER cuando se solicite el Common Name, con esto se mantendrá clientXX como nombre de los archivos generados, ver figura 8.2.

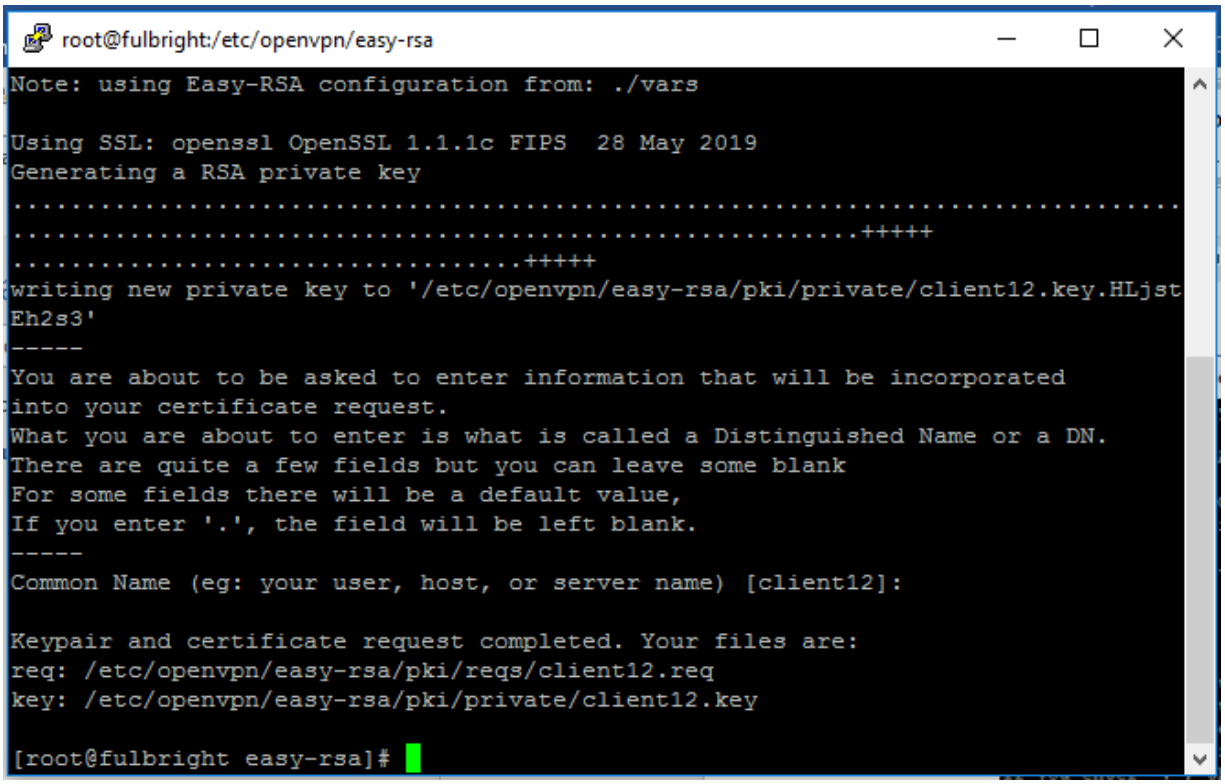

Figura 8. 2 Generar el requerimiento del nuevo usuario parte2.

Firma del cliente generado

Se firma el requerimiento generado para el cliente utilizando el certificado CA (Autoridad Certificadora), como se observa en la figura 8.3 se debe ejecutar:

./easyrsa sign-req client clientXX

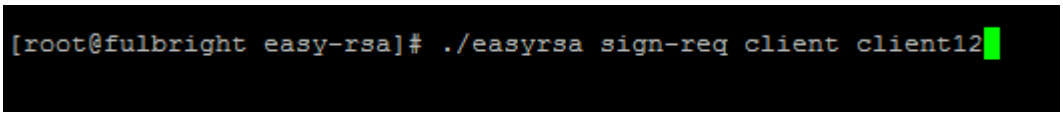

Figura 8. 3 Firma del requerimiento.parte1

En este paso se solicita verificar el requerimiento se digita "yes", ver figura 8.4

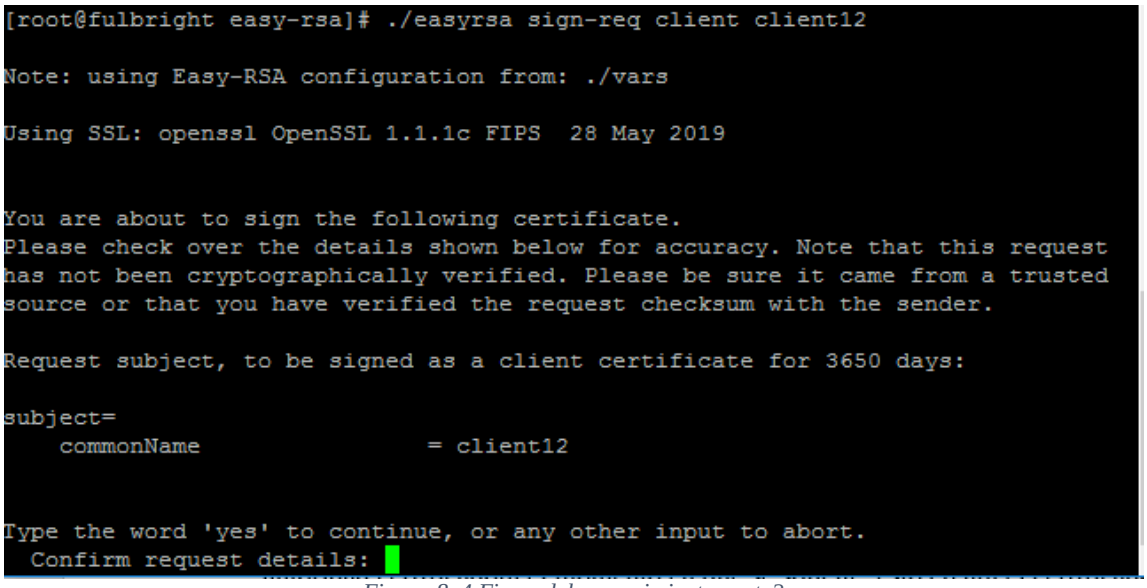

Figura 8. 4 Firma del requerimiento parte2

Se digita la clave de CA(Autoridad Certificadora) que se colocó al configurar el servidor CA en el momento en que se solicite, como se indica en la figura 8.5.

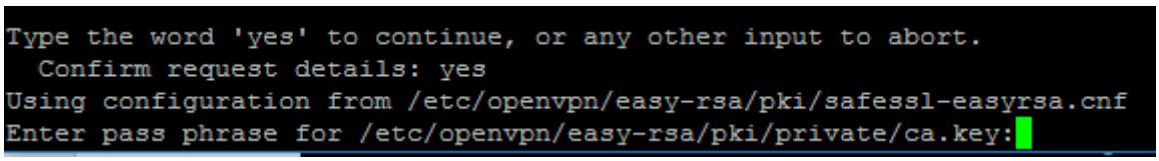

Figura 8. 5 Firma del requerimiento parte3

Esto creará el certificado para el cliente12 con el nombre client12.crt, como se observa en la figura 8.6

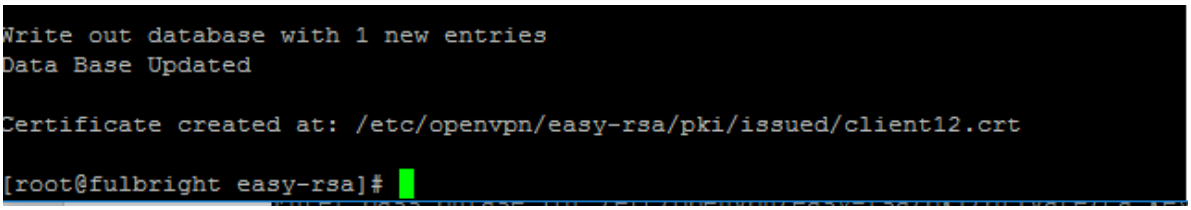

Figura 8. 6 Certificado generado

Como siguiente paso se debe verificar el certificado clientXX.crt generado, se debe ingresar en el directorio /etc/openvpn/easy-rsa y como se observa en la figura 8.7 ejecutar el comando:

openssl verify -CAfile pki/ca.crt pki/issued/clientXX.crt

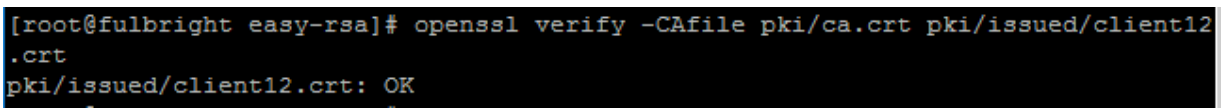

Figura 8. 7 Validación del certificado

Como se puede observar en la figura 8.8, para mantener una organización en los clientes se copia a la carpeta /etc/openvpn/client los archivos generados:

clientXX.crt

clientXX.key

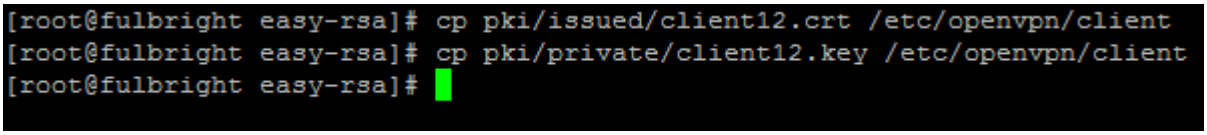

Figura 8. 8 Copia de clave privada y certificado verificado

IMPORTANTE: Estos dos archivos junto a ca.crt y clientXX.ovpn, deberán ser colocados en el equipo cliente en el momento que se realice la configuración del mismo, por lo que deberán ser copiados a una medio externo.

Eliminar una cuenta cliente

Si en algún momento se desea dar de baja o eliminar uno de los clientes, solo es necesario ejecutar el comando easy-rsa.

./easyrsa revoke clientXX

Luego se debe ejecutar: ./easyrsa gen-crl , esto generará el archivo crl.pem en /etc/openvpn/easy-rsa/pki que se copiará luego a la carpeta server

Configuración del cliente vpn en los equipos remotos

Es necesario crear el archivo de configuración del cliente, este archivo tendrá la extensión "**.ovpn**" y será colocado en el directorio de configuración del cliente openVPN instalado en el computador del usuario.

Se crea en block de notas un archivo con el nombre ClientXX.ovpn, en este se ingresa la siguiente información, ver figura 8.9:

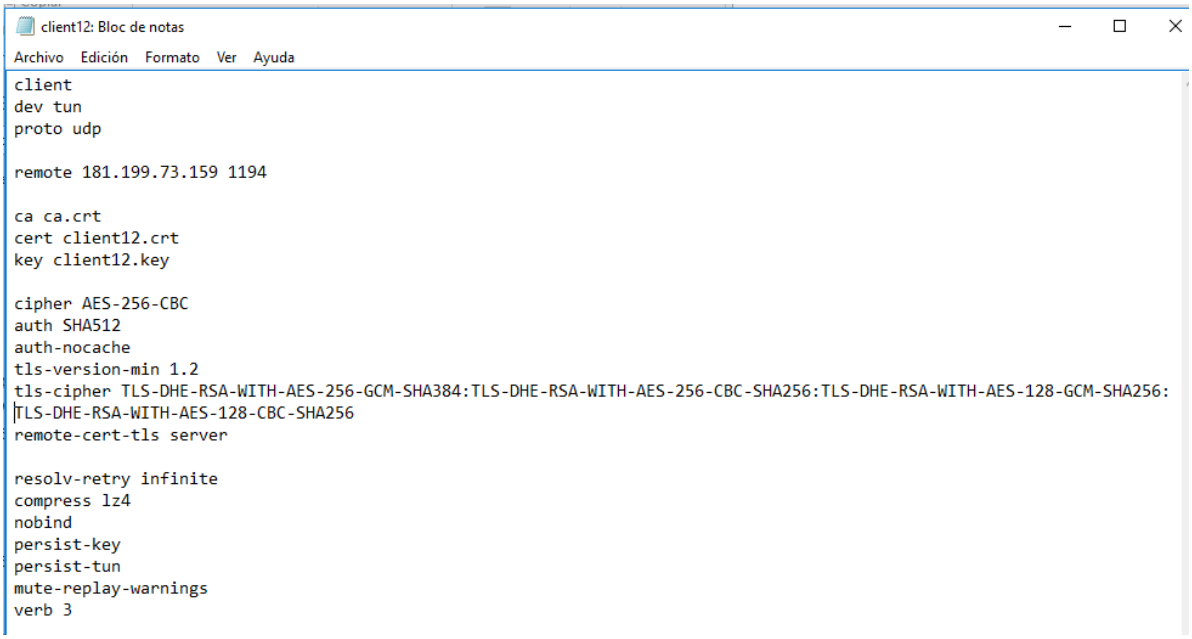

Figura 8. 9 Contenido del archivo cliente12.ovpn

Instalación del software OpenVPN Cliente en equipo.

Para instalar el cliente de openvpn es necesario descargar el paquete de instalación de la página oficial de OpenVPN, se selecciona la versión openvpn-2.4.9 desde https://openvpn.net/community-downloads/, como se puede ver en la figura 8.10

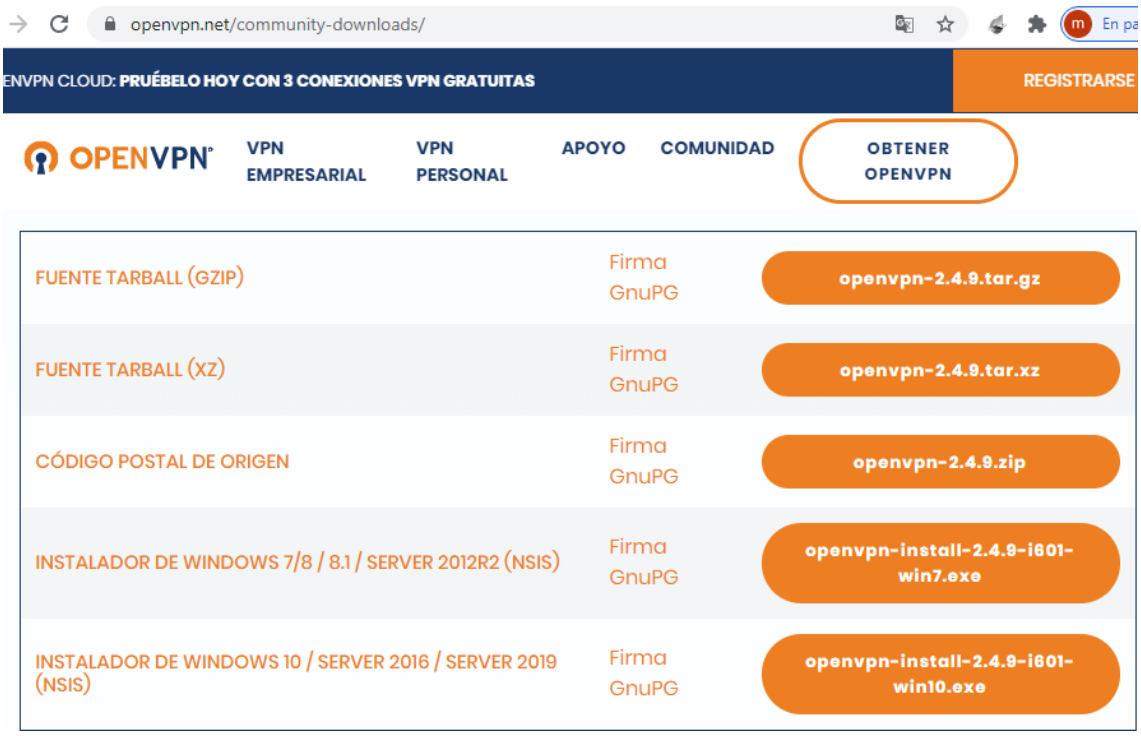

Figura 8. 10 Descarga del cliente OpenVPN

En Windows se debe ejecutar openvpn-install-2.4.9 con permisos de administrador, es importante descargar el instalador de acuerdo a la versión del sistema operativo que se tenga en el equipo cliente, ver figura 8.11

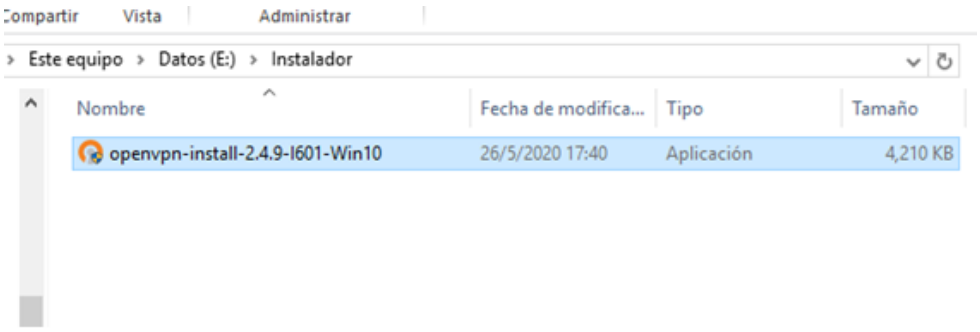

Figura 8. 11 Instalador de OpenVPN

Luego de ejecutar el instalador aparece la ventana de bienvenida a la instalación de OpenVPN, ver figura 8.12

Se presiona siguiente para continuar.

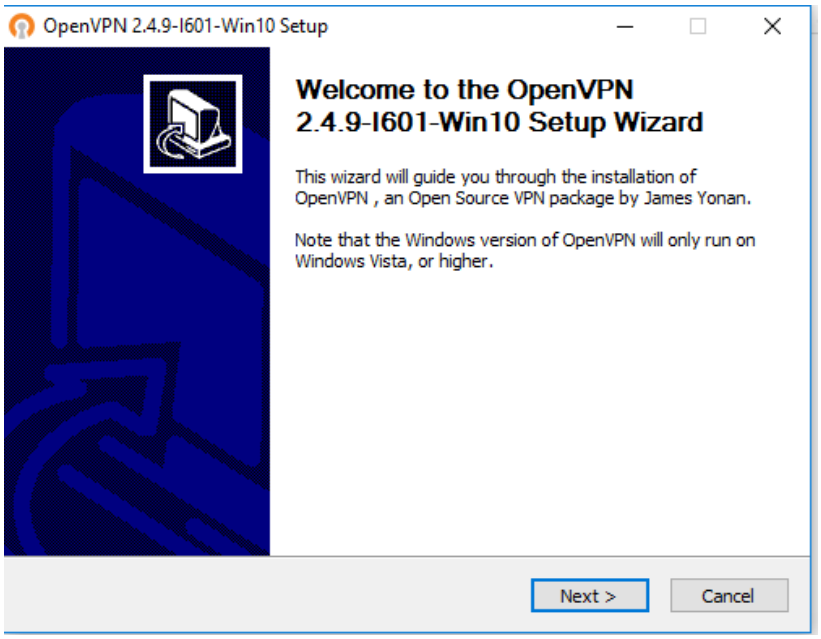

Figura 8. 12 Pantalla de bienvenida de OpenVPN Cliente

La siguiente ventana es de aceptación de la licencia como se puede ver en la figura 8.13, se acepta la misma para continuar

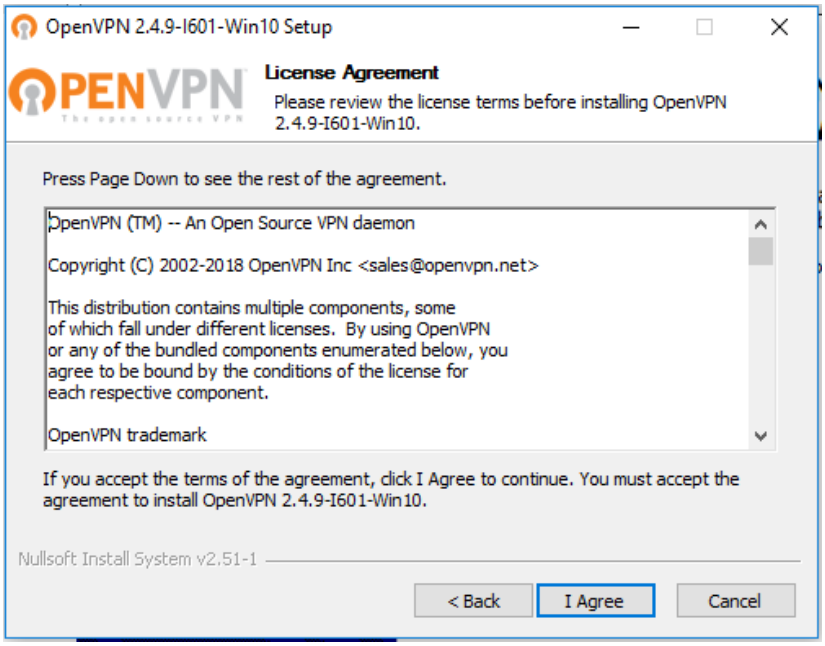

Figura 8. 13 Acuerdo de licencia de OpenVPN cliente

Se selecciona los componentes de OpenVPN a instalarse, en este caso se selecciona todo, ver figura 8.14.

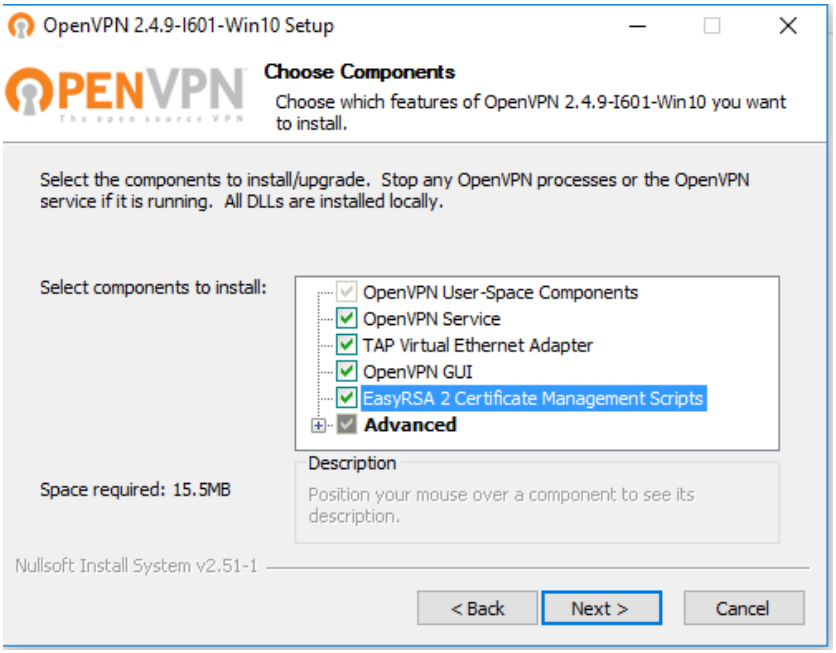

Figura 8. 14 Selección de componentes

Como se observa en la figura 8.15, se selecciona la ubicación de la carpeta de instalación, se deja la que está por defecto y se presiona instalar.

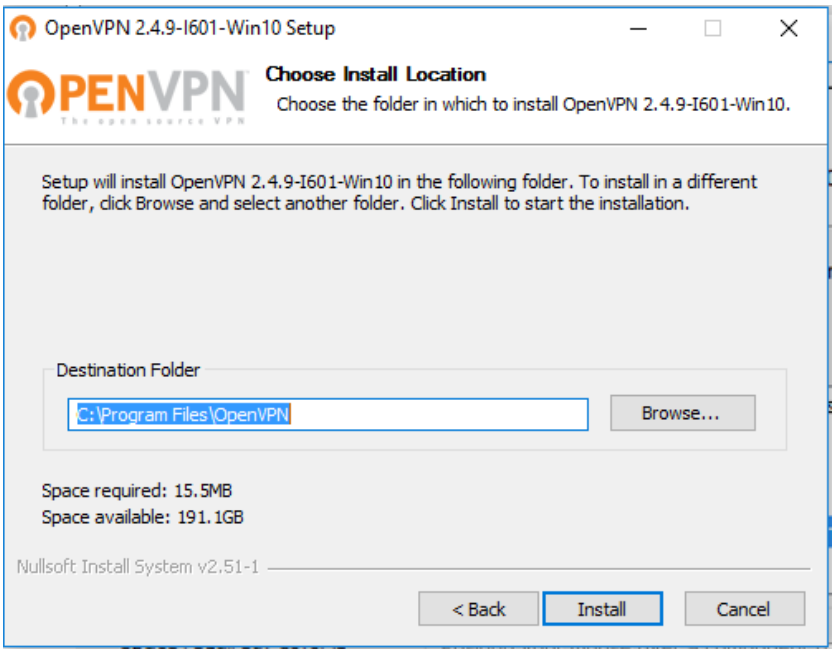

Figura 8. 15 Seleccionar la ubicación de la instalación

Se espera a que finalice la instalación y se presione siguiente, ver figura 8.16.

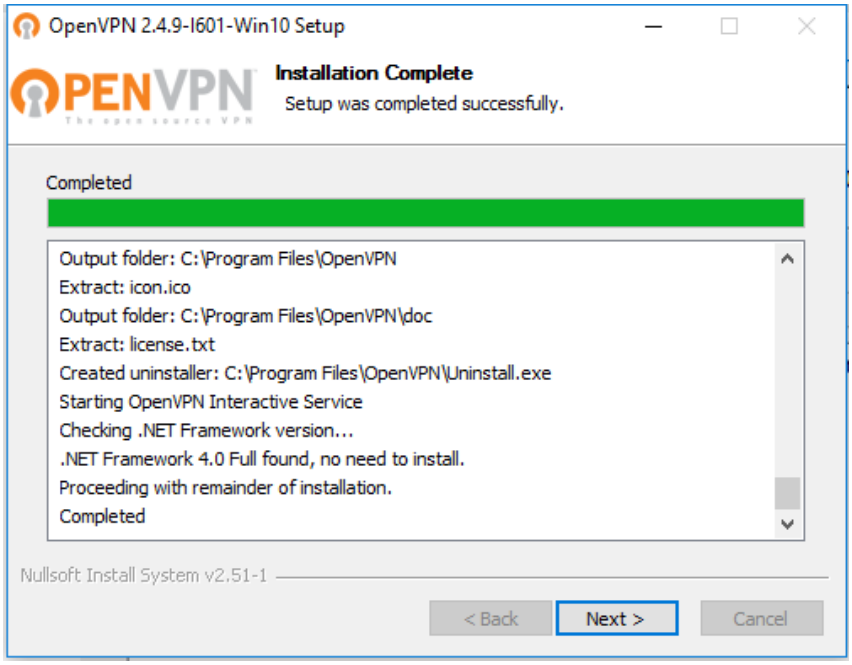

Figura 8. 16 Instalación completa

Como se observa en la figura 8.17, es necesario colocar en la carpeta que se creó al instalar OpenVPN **c:/Program Files/OpenVPN/Config,** los archivos del cliente que se generaron en el servidor.

Por ejemplo: Para el caso del client12 son:

Client12.crt

Client12.key

Client12.ovpn

Adicionalmente, se debe colocar aquí Ca.crt que es el certificado del servidor.

Ca.crt

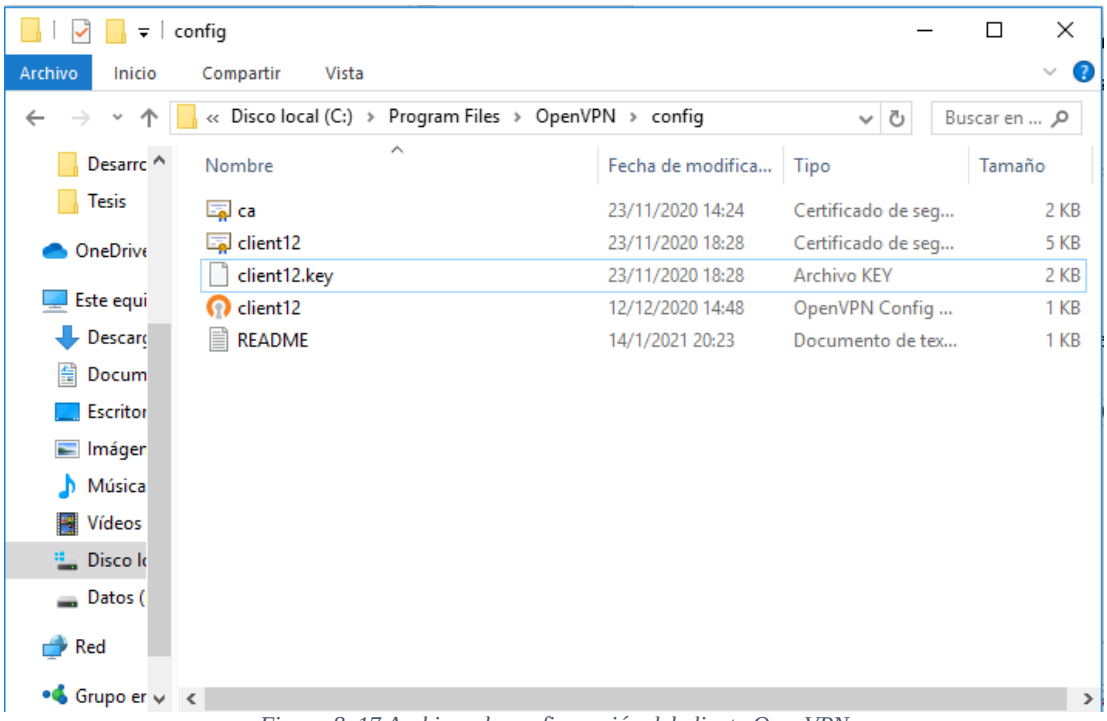

Figura 8. 17 Archivos de configuración del cliente OpenVPN

Se debe editar el archivo clientXX.ovpn y cambiar los nombres del archivo clientXX.crt y clientXX.key, en este caso debe colocarse en lugar de XX el 12, ver figura 8.18

Figura 8. 18 Cambio de número de cliente.

De acuerdo a la figura 8.19, se busca el programa OpenVPN instalado entre los programas de Windows y se lo ejecuta, la primera vez será necesario ejecutarlo como administrador.

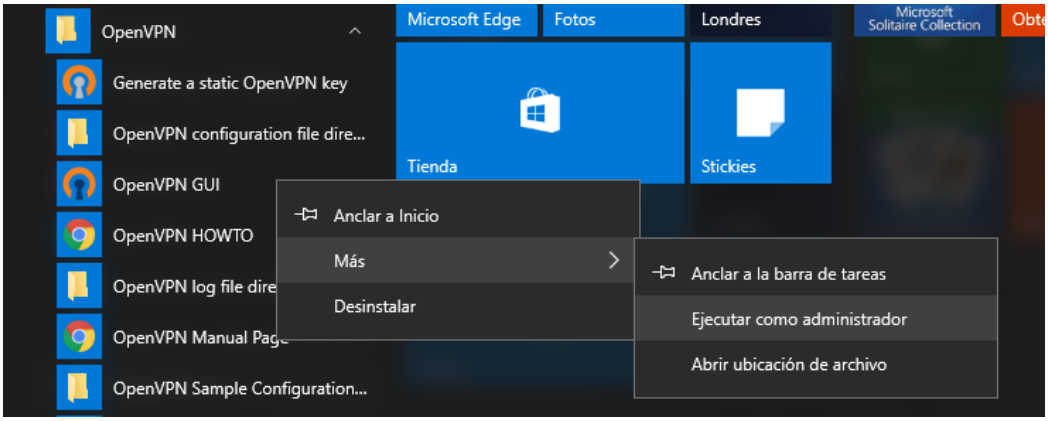

Figura 8. 19 Ejecución de OpenVPN GUI

.

Entre los dispositivos de red luego de instalar OpenVPN se habrá creado una tarjeta de red virtual denominada TAP, esta tarjeta se activará cuando se establezca la conexión VPN y se desactivará cuando se desconecte la conexión VPN, ver figura 8.20.

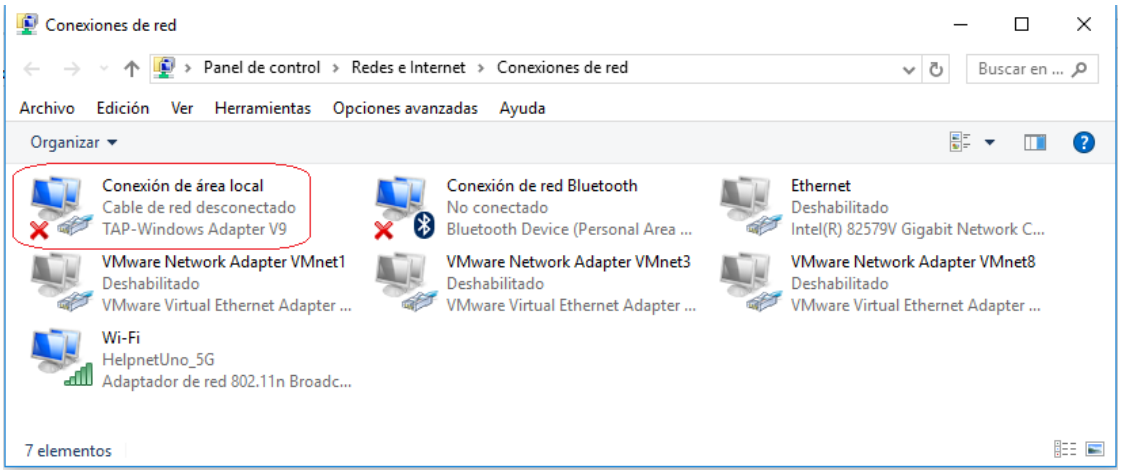

Figura 8. 20 Tarjeta de red virtual TAP

Al lado inferior derecho de la pantalla se observará un nuevo icono con forma de un monitor que representa la conexión de Openvpn, ver figura 8.21.

Figura 8. 21 Icono de OpenVPN en windows

Con este último paso se habrá instalado y configurado el cliente de OpenVPN.

8.2. ANEXO 2 GUIA DE USUARIO FINAL

Para activar la conexión VPN se debe dar doble click sobre el icono de OpenVPN ubicado en la pantalla de Windows al lado derecho inferior, para que se realice la conexión desde el cliente al servidor, ver figura 8.22 y figura 8.23.

Figura 8. 22 Icono de OpenVPN

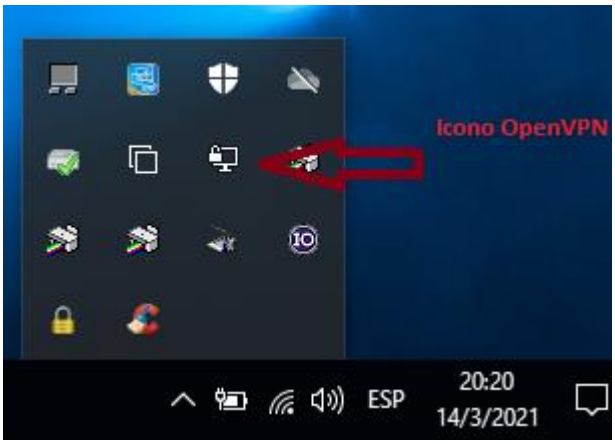

Figura 8. 23Acercamiento a icono de OpenVPN

Dar doble click sobre el ícono, esto abrirá una ventana que indica el log del proceso de conexión, ver figura 8.24.

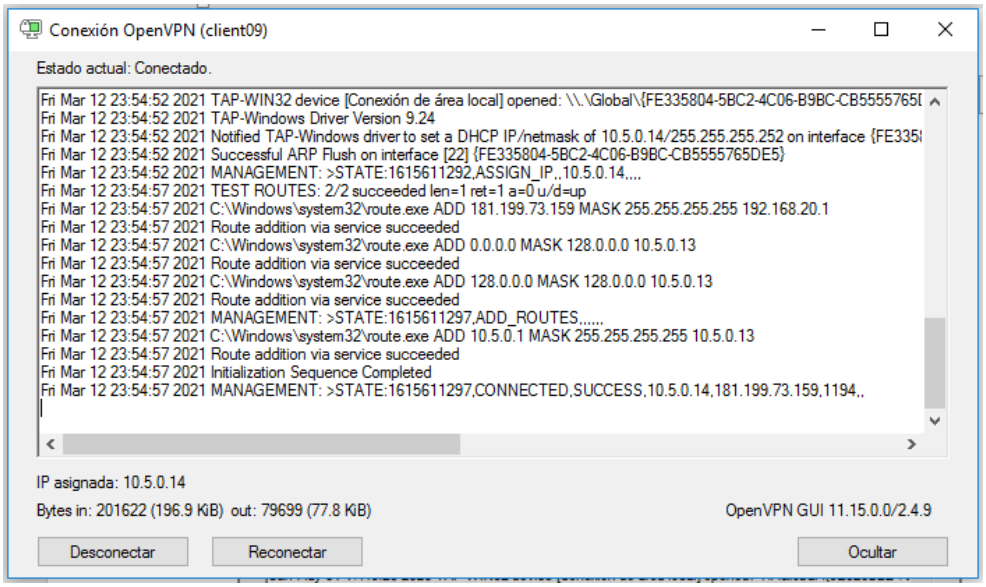

Figura 8. 24 Log de conexión de OpenVPN

Luego de establecerse de manera correcta la conexión de OpenVPN, el icono debe verse de color verde, observar figura 8.25, además pude aparecer un aviso de la IP asignada, ver figura 8.26.

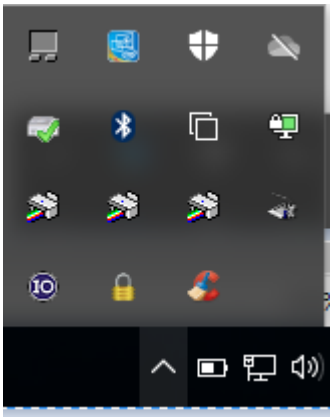

Figura 8. 25 Icono de OpenVPN, estado conectado

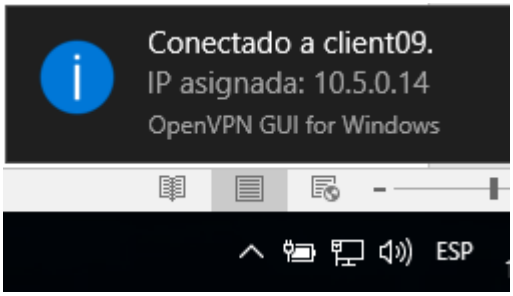

Figura 8. 26 Mensaje e conexión de OpenVPN

Así se tendrá conectado el equipo remoto a la red de la comisión Fulbright, para poder utilizar los servicios de la red local.

Configurar acceso a las carpetas compartidas

Para los usuarios que necesitan acceso a la carpeta compartida de un equipo dela red local, se debe abrir el explorador de archivos de windows y digitar la dirección IP del equipo al que se desea acceder, es importante indicar que esto se lo puede hacer únicamente si se cuenta con usuario y clave del usuario del dominio con los permisos respectivos, ver figura 8.27. luego de esto se podrán ver las carpetas compartidas en dicho equipo, ver figura 8.28

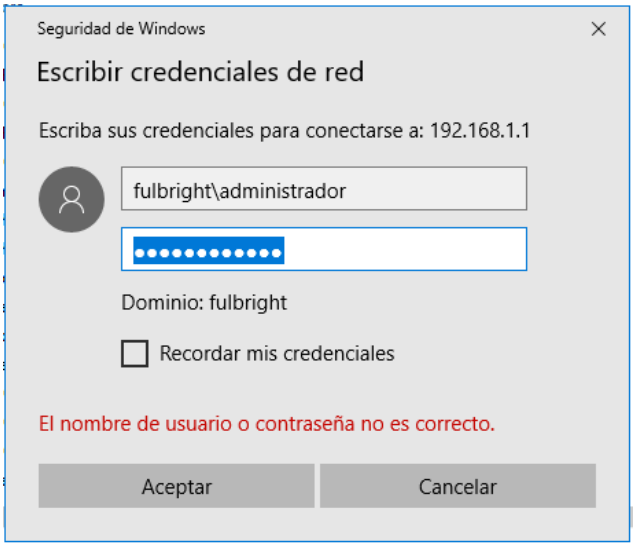

Figura 8. 27 Ingreso de credenciales de red.

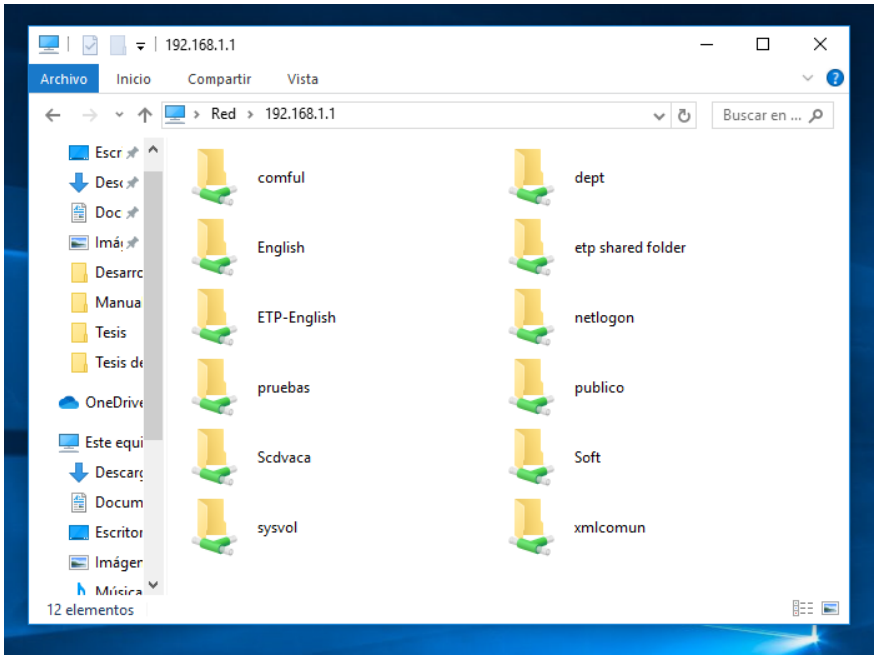

Figura 8. 28 Carpetas compartidas de equipo 192.168.1.1

Acceso remoto a los computadores.

Se presiona el icono buscar en Windows, y se digita "escritorio remoto", ver figura 8.29.

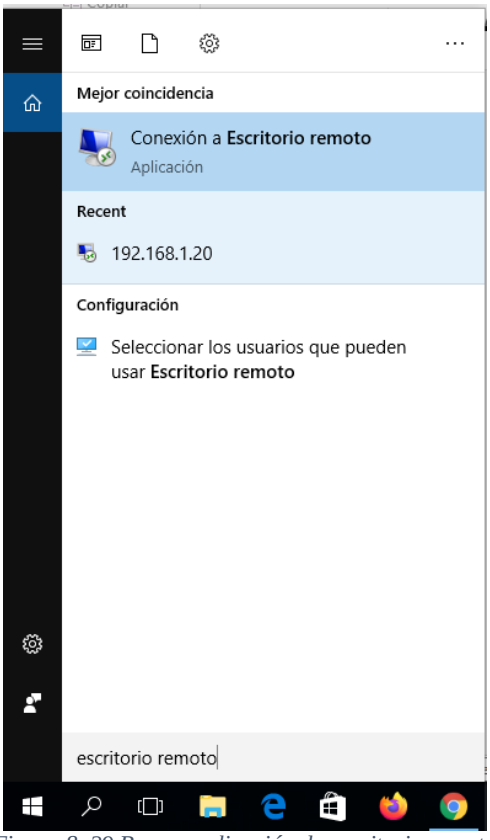

Figura 8. 29 Buscar aplicación de escritorio remoto

Se debe dar doble click sobre conexión a Escritorio remoto, esto abrirá una ventana donde se debe digitar la IP del equipo al que se desea acceder por escritorio remoto, ver figura 8.30.

Ejemplo: Equipo 192.168.1.20

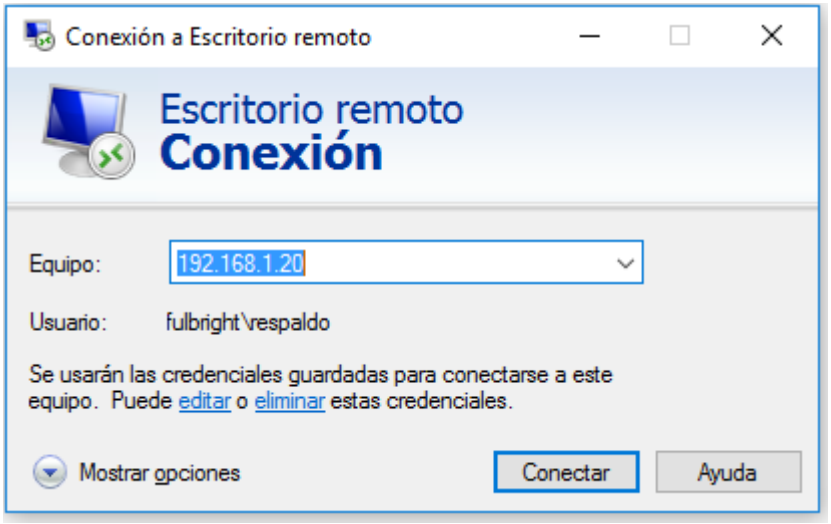

Figura 8. 30 Ventana de conexión a escritorio remoto

Se presiona conectar, se solicitará ingresar usuario de dominio fulbright y la contraseña, se digitan las credenciales y se presiona aceptar, ver figura 8.31.

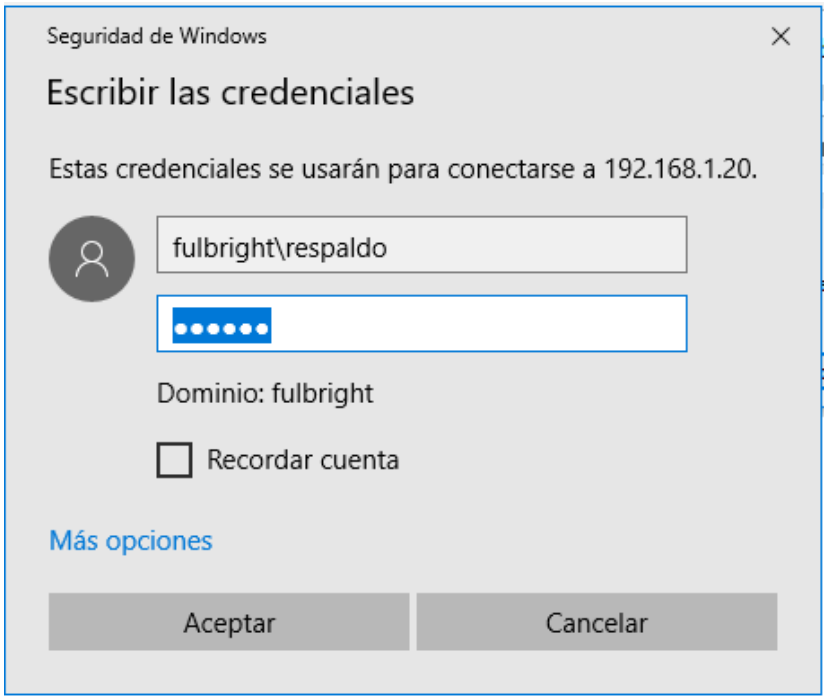

Figura 8. 31 Ingreso de credenciales para acceso a escritorio remoto

Como se puede ver en la figura 8.32, se accede al equipo 192.168.1.20 sin inconvenientes.

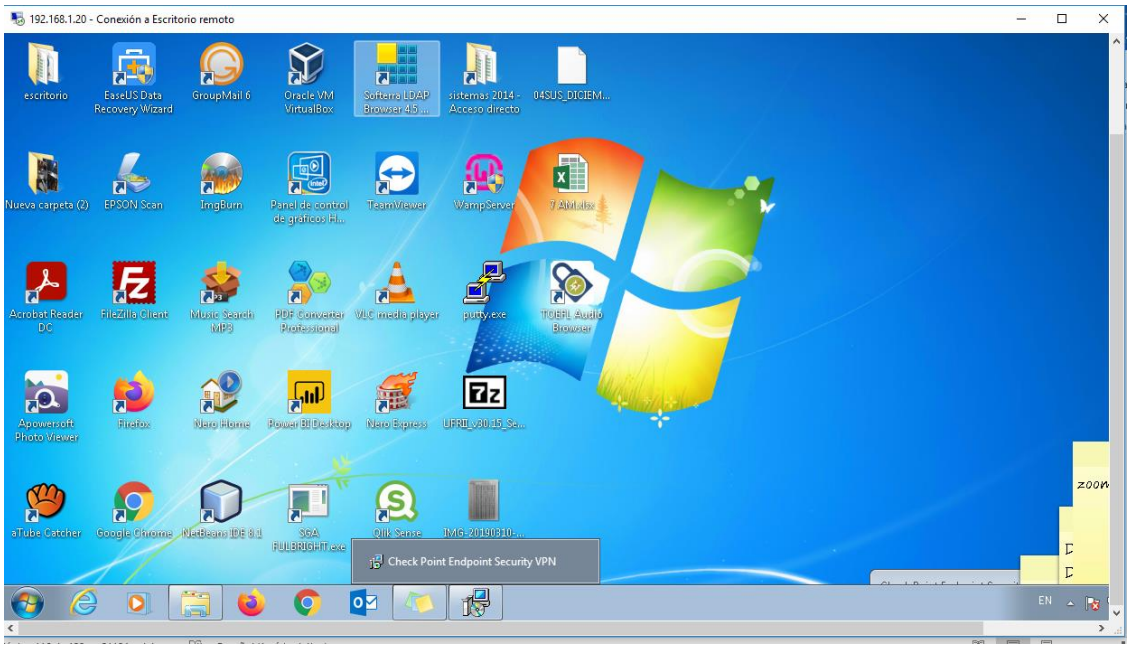

Figura 8. 32 Conexión a escritorio remoto de equipo 192.168.1.20

Desconectar OpenVPN

Para realizar la desconexión es necesario dar doble click sobre el icono de OpenVPN que debe estar de color verde, como se observa en la figura 8.33.

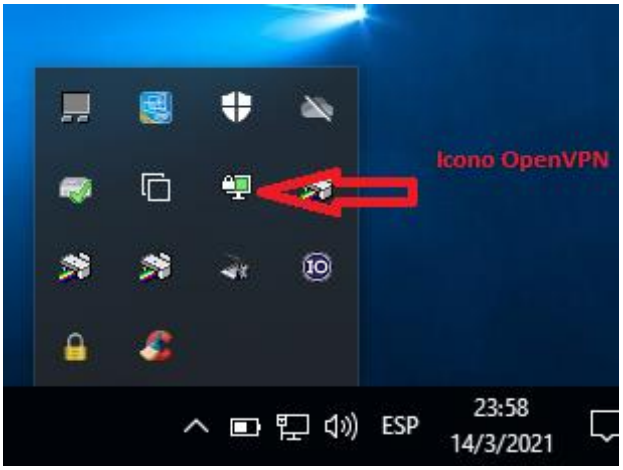

Figura 8. 33 Icono de OpenVPN en estado conectado

Se abrirá la ventana del log de conexión, en donde se debe presionar en desconectar, ver figura 8.34.

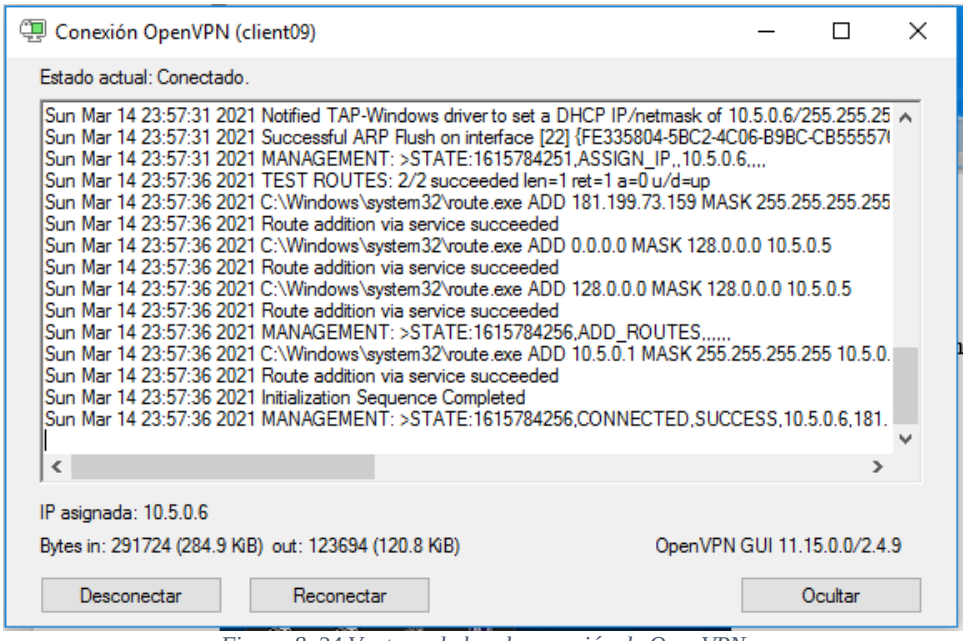

Figura 8. 34 Ventana de log de conexión de OpenVPN

Finalmente, como se observa en la figura 8.35, se habrá desconectado el servicio de OpenVPN.

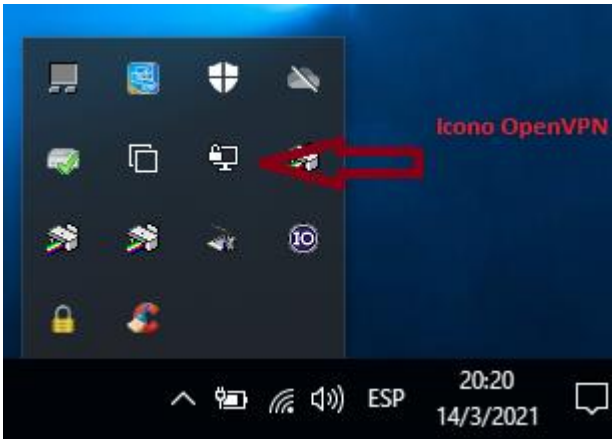

Figura 8. 35 Icono de OpenVPN en estado desconectado