PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

PLAN DE DISERTACIÓN
PROPUESTA DE IMPLEMENTACIÓN DE VOIP Y VPN PARA LA EMPRESA FERROTOOLS

AUTOR
KEVIN ESTEBAN LEÓN CAMPOS

QUITO DM, 2022

DEDICATORIA

El presente trabajo lo dedico a mis padres Jeanette y Carlos quienes con su apoyo, cariño y esfuerzo me han permitido cumplir esta meta en mi vida, a mi hermana Lorena quien ha estado siempre para brindarme su apoyo y consejo, finalmente a los amigos que encontré en las aulas de clase con quienes compartí horas de estudio y esparcimiento.

AGRADECIMIENTO

Agradezco primeramente a Dios, por permitirme concluir mis estudios, a mis maestros quienes supieron impartir sus conocimientos durante la carrera y a toda mi familia por su motivación y apoyo constante.

RESUMEN

Mediante el presente trabajo se realiza la disertación y propuesta de implementación de VOIP y VPN, haciendo uso de una herramienta de software libre, para permitir que los empleados de la empresa FERROTOOLS puedan efectuar sus actividades laborales sin la necesidad de asistir de manera presencial debido a la coyuntura generada en nuestro país por motivo de la pandemia de COVID, lo cual ha imposibilitado a los empleados acceder a las instalaciones de la empresa.

Inicialmente se realizará un análisis de la situación actual de la empresa en lo que respecta a sus equipos e infraestructura, así como revisar las necesidades de la empresa y el número de empleados.

Seguido de esto, se diseñará la red VPN haciendo uso de herramientas de software libre y tomando en cuenta el análisis realizado previamente, para lo cual se realiza un estudio de la mejor opción de herramientas a utilizar tanto para VPN como para voz IP.

Así también se realizará la instalación y configuración del sistema operativo seleccionado y la configuración necesaria para el correcto funcionamiento de la VPN y VoIP.

Finalmente, se efectuará la configuración en cada equipo del usuario y las respectivas pruebas para de esta manera garantizar el funcionamiento adecuado de la red VPN y de las llamadas VoIP.

Contenido

CAPÍTULO 1

INTRODUCCIÓN

A consecuencia de la pandemia generada por el covid-19 muchas empresas en el ecuador se vieron obligas a cambiar su modalidad de trabajo de una presencial a una telemática, para lo cual hicieron uso de tecnologías que permitan a sus empleados desempeñar sus labores desde sus hogares a través del internet pero manteniendo una conexión segura a la información de la empresa, dicha tecnología es conocida como VPN o red privada virtual, la cual permite crear un túnel de comunicación dentro una red en este caso el internet y además encripta la información para mantenerla segura.

La empresa Ferrotools como otras empresas que no contaban con una infraestructura adecuada para la implementación de una VPN se vio obligada a buscar una herramientas que les permita seguir realizando sus actividades, sin embargo tenían muchos problemas de conexión, por lo que se plantea la opción de implementar una VPN y VoIP intentando no incidir en gastos exuberantes, para lo cual era necesario revisar la infraestructura actual y utilizar de una más optima los recursos actuales y hacer uso de software libre.

JUSTIFICACIÓN

La empresa Ferrotools, dedicada por más de 25 años a la comercialización de herramientas para la industria tanto para empresas de la ciudad de Quito como para las de otras ciudades, se vio afectada con la pandemia del Covid-19, ya que todas sus actividades de ventas y su personal tuvieron que ser trasladadas a teletrabajo y su consumo de llamadas telefónicas representa un costo elevado ya que actualmente se utiliza comunicación mediante planes celulares.

Los vendedores de la empresa no pueden conectarse de manera adecuada al sistema que posee la empresa para realizar sus actividades, ya que los servidores debido a que tienen algunos años de antigüedad no soportan la conexión remota además de no poseer una conexión segura, lo que implica un riesgo para la información que maneja la empresa.

PLANTEAMIENTO DEL PROBLEMA

La empresa Ferrotools dedicada a la comercialización de herramientas para la industria, debido a que no cuenta con un adecuado diseño de infraestructura de red de datos para la empresa, y equipos de computación considerados obsoletos, se vio afectado con la pandemia del covid-19 ya que se vio obligada a implementar el teletrabajo lo cual requiere de una red que le permita además de la correcta conexión y transmisión de datos de manera local, la facilidad de una conexión remota que permita además tener una mejor seguridad y una correcta comunicación de los empleados. La empresa al no contar con la red adecuada se vio afectada en sus ventas ya que las facturas no se podían realizar en el tiempo adecuado, y tampoco se podía contar con datos actualizados del stock de bodega lo que en consecuencia implica una pérdida económica y además dificulta la toma de decisiones al no contar con información real y actualizada.

ANTECEDENTES

La Voz Sobre IP (VoIP) más conocida como telefonía IP es una tecnología en la cual a diferencia de la telefonía tradicional en la que la voz se transmite de manera analógica, la VoIP digitaliza, comprime y encapsula la voz para ser transmitida a través de redes LAN (Red de Área Local) o WAN (Red de Área Amplia) lo cual representa un ahorro tanto de infraestructura como de costo de llamada. Esta tecnología tiene mucha aceptación dentro de las empresas ya que permite la integración de la transmisión de datos y de voz dentro de una misma red lo cual representa un ahorro en el costo de configuración y mantenimiento de equipos, además de permitir ubicaciones remotas. (Martin Portillo, 2015)

Una VPN (Red Privada Virtual) es una tecnología de red que permite extender una red local privada a través de una red pública como por ejemplo el Internet. Esta tecnología es útil para establecer redes sobre áreas geográficas extensas como puede ser diferentes puntos dentro de una misma ciudad, lo cual al utilizar una red ya existente como es el internet permite ahorrar costos de infraestructura y además permite una mayor seguridad en la transmisión de información entre los distintos puntos de la red VPN. (Carrillo, 2016)

Para la implementación de estas tecnologías se puede hacer uso de herramientas tanto de software como de hardware, pero lo más importante es el protocolo que se utilice, todo dependerá de la configuración que quiera realizar, en el caso de las configuraciones basadas en hardware siempre tendrán un mayor rendimiento, se puede encontrar equipos en las marcas Cisco, Linksys, D-Link, etc. Las configuraciones por software son más personalizables pero son las que menor rendimiento ofrecen, entre las herramientas que existen son los propios ajustes de los sistemas operativos como Windows, Linux o Mac además otras herramientas de código abierto como OpenVPN o FreeS/Wan. (Carrillo, 2016)

Tanto la VoIP como las VPN son ampliamente utilizados actualmente en distintas empresas, entre las más destacadas son las empresas financieras que al requerir de seguridad en los datos que se maneja en las distintas sucursales que pueda tener además de una continua comunicación entre las mismas. En el caso de las empresas financieras se requiere una red de alta disponibilidad que evite la perdida de conexión y la perdida de datos. (Barrera, 2020)

OBJETIVOS

OBJETIVO GENERAL

Proponer la implementación de VoIP y VPN que permitan a la empresa mejorar su productividad y la seguridad de la información en la empresa.

OBJETIVOS ESPECÍFICOS

- Analizar la infraestructura de red que posee actualmente la empresa.
- Diseñar la infraestructura y comunicación en los servidores.
- Realizar una propuesta de implementación de VoIP y VPN para mejorar la productividad y seguridad.

METODOLOGÍA

Para la investigación se utilizará una metodología descriptiva en donde se definirán los conceptos relacionados a las VPN y VoIP y se determinara las herramientas y hardware necesario para lograr realizar su implementación. Para realizar la implementación será necesario lo siguiente:

- **Análisis de la situación actual de la red de la empresa:** en este punto se realizará un reconocimiento del servicio de internet actual que posee la empresa, los equipos de red que posee y establecer los servicios que requiere para obtener un modelo de la red existente.

- **Planificación del servicio VPN Y VoIP:** se realizará un modelo tentativo de red en el que se especificará la arquitectura y la topología necesaria, utilizando hardware moderno y herramientas de software libre.

- **Configuración simulada de la red VPN Y VoIP:** se realizará una simulación de la red propuesta para ejecutar pruebas de rendimiento y estabilidad antes de elegir la configuración más adecuada.

CAPÍTULO 2

2.1 MARCO TEÓRICO

2.1.1 Tecnología de acceso remoto

Al hablar de tecnologías de acceso remoto básicamente se refiere a la capacidad de acceder a una conexión de red en cualquier momento y en cualquier lugar, lo que en la actualidad resulta ser representativo en el ámbito de redes, debido a que tanto en el ámbito laboral como académico, ha permitido que puedan desempeñar sus actividades desde casa o sucursales remotas, y de esta manera se permita realizar consultas de archivos, documentación o utilización de aplicaciones necesarias para el cumplimiento de actividades diarias. Así también, cabe mencionar que esta tecnología ha generado un apogeo en lo que se refiere a redes privadas virtuales - VPN.

Así también, se debe mencionar que en un inicio las empresas para poder hacer llamadas y conectarse con una red corporativa, debían realizar instalaciones a módems, requiriendo la instalación de varios de ellos lo cual resultaba ser costoso y demandaba de mayor soporte tecnológico, de la misma manera también resultaba costoso si los usuarios estaban alejados de la empresa, lo cual provocaba que se deban realizar llamadas de larga distancia considerando que el teletrabajador tenía que mantenerse conectado por largo tiempo, no obstante todo esto en la actualidad fue reemplazado por las VPN para realizar el acceso remoto (Jota Fonseca, 2018).

2.1.2 Red privada virtual

"Una red privada virtual (VPN) permite a su empresa ampliar de forma segura la intranet privada a través de la infraestructura existente de una red pública como Internet. Con VPN, su empresa puede controlar el tráfico de la red a la vez que proporciona características de seguridad importantes, como por ejemplo la autenticación y la privacidad de datos." (IBM, 2021).

En conclusión, una red privada virtual es una red pública, pero que funciona dentro de un medio privado, por lo que permite a los usuarios realizar sus actividades desde un punto remoto como

si estuviese dentro de la red local, sin embargo, una red de este tipo requiere de un adecuado ancho de banda para funcionar de forma correcta, por lo que si el número de usuarios se incrementa el ancho de banda que recibe cada uno se verá reducido.

2.1.3 Funcionamiento de una VPN

El método en el que opera una VPN consiste en proporcionar a los usuarios los respectivos permisos para que puedan comunicarse mediante una vía "virtual" de Internet y lo cual adicionalmente brinda la seguridad que ofrecen solamente las redes privadas.

Cabe indicar que, para poder usar Internet para una VPN, se puede presentar un importante problema el cual es que la información privada que maneja la empresa recorren sin ninguna seguridad por internet, la cual podría ser manipulada o robada por otras personas, no obstante, al respecto existe una solución que es el tunneling, que son paquetes que se envían y son primeramente encriptados, luego se resguardan en paquetes IP y posteriormente se transfieren mediante una vía a través de Internet.

"En conclusión, una VPN es un enlace punto a punto entre dos puntos, en donde toda la información que se transmite por esta se mantendrá asegurada por la encriptación de sus datos, de esta manera los usuarios de ambos extremos pueden estar conectados a través del túnel de manera transparente" (Pomar Pascual, 2019).

2.1.4 Tipos VPN

Una vez realizada la investigación se pudo determinar que existen tres tipos de redes VPN, a continuación, se detalla cada una de ellas para determinar se principales cualidades:

VPN basada en hardware

Este tipo de red privada virtual se encuentran fundamentadas en hardware y son únicamente

equipos diseñados para dicha función, un ejemplo son “los routers, que son seguros y sencillos de usar, brindando un rendimiento significativo, puesto que todos los procesos se encuentran diseñados al funcionamiento de la red, en comparación de un sistema operativo que usa demasiados recursos del procesador para ofrecer otros servicios” (Quezada Lozano, 2016).

Cabe indicar que “estos sistemas están fundamentados en routers que encriptan información” (Quezada Lozano, 2016), que si bien se consideran seguros y sencillos de utilizar, para su ejecución demandan una configuración bien elaborada, así como definida de manera correcta, además de ser equipos considerados como costosos.

VPN basada en firewall

“Son aquellas redes privadas virtuales que usan 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” (Quezada Lozano, 2016).

La desventaja de este tipo de VPN es la optimización de su desempeño, ya que, al no contar con un hardware dedicado, el rendimiento de la conexión se ve afectada.

VPN basada en software

Las VPN basadas en software son utilizadas principalmente cuando son implementados diferentes firewalls y enrutadores y realizar una conexión de punto a punto entre los mismos.

Este tipo de VPN ofrece una mayor flexibilidad en lo que se refiere al manejo del trafico de la red, además “Muchos productos basados en software permiten que el tráfico del túnel dependa solamente de la dirección o protocolo, a diferencia de los productos basados en hardware, que encapsulan el tráfico independientemente del protocolo” (Quezada Lozano, 2016).

2.1.5 Protocolos VPN

Para la implementación de una VPN existen distintos protocolos que pueden ser utilizados, entre los que tenemos:

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" (IZA, 2021), " (…) 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" (Castellano, 2017).

IPSec: "Protocolo de seguridad de internet el cual permite varios servicios de seguridad para el protocolo de internet (IP) tanto para IPv4 como para IPv6, fue diseñado para soportar dos modos de cifrado" (IZA, 2021).

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" (IZA, 2021).

Para poder funcionar, este protocolo "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)" (Castellano, 2017).

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" (Castillo, 2020).

"Este tipo de protocolos SSL versión 3.0 y TLS versión 1.0 son iguales, no obstante, una diferencia, son considerados sus diseñadores. SSL/TLS admite su validación del cliente y del servidor, utilizando claves públicas y certificados digitales, y suministra una comunicación

segura a través del cifrado de la información tanto del emisor como del receptor. Además, este protocolo funciona en un punto medio entre el protocolo TCP y el protocolo de aplicación" (Castillo, 2020).

Así también se debe indicar que este protocolo es muy amplio para efectuar tareas de comercio electrónico a tal punto que "entidades como Visa, MasterCard, American Express y muchas de las principales empresas de la rama financiera han aceptado SSL para realizar la actividad económica en Internet" (Castellano, 2017).

WireGuard: Consiste en "un protocolo VPN innovador ya que ofrece una solución más segura, sencilla y rápidaa sus usuarios con respecto a otros protocolos, este protocolo se ejecuta sobre UDP" (Vpnranks, 2020).

Cabe indicar que "este protocolo presenta simplicidad de código, lo que facilita la implementación, así como permite un mayor rendimiento y menos errores" (Vpnranks, 2020).

2.1.6 Software libre

El software libre comúnmente está disponible sin ningún costo o con un costo minino debido a los costos de distribución en otros medios, sin embargo, no siempre el software libre es sinónimo de software gratis, ya que se puede distribuir de manera comercial sin dejar de ser un software libre.

De igual manera, el "software gratis puede incluir en algunas ocasiones el código fuente, no obstante, este tipo de software no obligatoriamente puede ser libre a menos que se garanticen los derechos de modificación y que estas versiones modificadas puedan ser distribuidas" (ECURED, 2020).

2.1.7 Sistema Operativo Linux

El sistema operativo Linux es libre y gratuito, a diferencia de Windows o MacOS, no pertenece a ninguna compañía, en su lugar existe una comunidad de varias empresas y personas que continuamente contribuyen en su desarrollo.

"En definitiva, Linux es un sistema que nace de la combinación de varios proyectos entre los que destacan GNU y la Free Software Foundation además del propio núcleo de Linux encabezado por Linus Torvalds" (Adeva, 2021). El desarrollo de Linux el mejor ejemplo en lo que se refiere a software libre, ya que "todo su código fuente puede ser utilizado, modificado y distribuido libremente por cualquier bajo los términos de la licencia GPL o Licencia Pública General de GNU y otras licencias" (Adeva, 2021).

2.1.8 Distribuciones de Linux para Firewall

PFSENSE

Pfsense es un sistema operativo orientado a firewall muy utilizado en pequeñas y medianas empresas ya que permite segmentar su red además de otros servicios. Este sistema operativo está basado en FreeBSD, por lo que es un sistema operativo muy estable y seguro. La interfaz gráfica que ofrece es muy intuitiva y sencilla para el usuario (Luz, 2022).

Es un sistema operativo que consume muy pocos recursos, sin embargo, dependiendo del uso que se le dé, el número de usuarios y los servicios que se activen será necesario contar con un equipo con mayor potencia y memoria. "Este sistema operativo se puede instalar en prácticamente cualquier ordenador actual, pero lógicamente el rendimiento que se obtendrá dependerá del hardware, y lo mismo ocurre con la configuración que se haya realizado en el propio cortafuegos" (Luz, 2022). El punto débil de este sistema es su compatibilidad con las tarjetas de red, es recomendable utilizar la marca Intel, aunque existen otras marcas que son igualmente compatibles.

IPFIRE

“IP Fire es una distribución de Linux de código abierto endurecido que funciona principalmente como enrutador y cortafuegos; un sistema de firewall independiente con una consola de administración basada en web para su configuración” (Rosepac, 2021).

Este sistema está centrado en la flexibilidad, además de ser muy versátil ya que se puede adaptar tanto a redes de pequeñas empresas como a redes domésticas.

OPNSENSE

El sistema operativo OPNSENSE está orientado a ser utilizado como router y firewall, y se puede adaptar tanto a redes domesticas como empresariales, adicionalmente incorpora herramientas y configuraciones que solo firewalls comerciales ofrecen, pero de manera gratuita.

2.1.9 VPN con software libre

El disponer de este tipo de red permite lograr desempeñarse de una manera más dinámica y sencilla ya que independiente de la ubicación las personas en la actualidad pueden realizar sus actividades laborales, desde cualquier lugar en que se encuentren, ya que mediante herramientas servicios o programas, se puede mantener una comunicación permanente con las personas del entorno laboral.

Cabe indicar que para establecer una conexión VPN se necesita de un cliente y un servidor, en donde el cliente debe tener instalado y configurado los parámetros de conexión y en el servidor instalado y configurado el respectivo usuario que permita la conexión remota.

En este sentido y de acuerdo con el estudio ejecutado, es pertinente describir el siguiente sistema VPN:

2.1.9.1 Sistema OpenVPN

Este tipo de sistema no solo sirve como un protocolo de comunicación, sino que también funciona como una aplicación de código abierto mediante el cual se realiza conexiones VPN, maneja una licencia de software libre.

Así también, "la arquitectura de conexión y comunicación es la representativa de una VPN, basada en punto-a-punto. Para realizar esta conexión se necesita validación jerárquica entre los usuarios y el servidor a través de certificados SSL/TLS + RSA de forma remota. Además, soporta todo tipo de enlaces de red, como WiFi IEEE 802.11, Ethernet 802.3 y red de datos móviles" (IZA, 2021).

2.1.9.2 Principales características

OpenVPN es un protocolo de conexión de código abierto, enfocado principalmente en conexiones de túnel de red y "se encuentra equipado con capacidades de servidor OpenVPN, capacidades de administración empresarial, paquetes de software de OpenVPN Connect UI y OpenVPN Client" (Castellano, 2017).

Este protocolo utiliza el cifradi AES-256 bits que "esencialmente irrompible, con autenticación RSA de 2048 bits y algoritmo hash SHA1 de 160 bits" (Castellano, 2017).

Entre otras de las características que ofrece tenemos:

- Ser multiplataforma
- Multi cliente y multi usuario
- Control de acceso de usuarios
- Soporte de métodos de autenticación LDAP y Local DB
- Alta escalabilidad, ya que soporta hasta 10000 conexiones simultaneas.
- Múltiples niveles de seguridad

2.1.9.3 Seguridad en OpenVpn

Si bien OpenVPN facilita la creación de un servidor al cual acceder a través de internet, es decir permite a los usuarios remotos conectarse a la red de una empresa utilizando este servidor OpenVPN, este termina convirtiéndose en blanco de un sin número de ataques, por esta razón se deben implementar mecanismos que mejoren la seguridad del acceso a la VPN, en este aspecto OpenVPN permite hacer uso de la autenticación TLS, lo cual permite evitar los ataques denegación de servicio (Linuxito, 2018).

2.1.9.4 Clientes OpenVpn

OpenVPN cuenta con un cliente de conexión, el cual puede ser instalado en diferentes sistemas operativos de escritorio como Ubuntu, MacOS y Windows, además de plataformas móviles como Android y IOS (Stackscale, 2020).

2.1.10 Voz IP

La Voz IP es la transmisión de voz utilizando las redes de internet en lugar de las redes telefónicas tradicionales PSTN que utilizan las redes telefónicas físicas. “La telefonía IP, sin embargo, es mucho más versátil, ya que permite la transmisión de voz, datos y video a una variedad de dispositivos como teléfonos inteligentes, computadoras personales, tabletas y teléfonos IP a un costo menor” (desconocido, 2021). Las redes de internet fueron creadas originalmente para la transmisión de datos, pero debido a su éxito se adaptó para también permitir la transmisión de voz como paquetes de datos (desconocido, 2021).

2.1.10.1 Como funciona la VoIP

Para realizar llamadas a través de la tecnología VoIP, es necesario utilizar un software especial instalado en el teléfono inteligente, tableta o computadora. Cuando habla al micrófono, la voz se detecta como ondas de sonido físicas. Este programa los convierte en código binario que se agrupará en pequeños paquetes de datos. (Robine, ¿Qué es la Voz sobre IP y cuáles son sus

ventajas?, 2021)

Los paquetes de datos en código binario se transmitirán a través de Internet al dispositivo receptor, independientemente de su ubicación geográfica. Por ejemplo, se pueden realizar llamadas desde España a Japón de forma muy rápida ya un coste mucho menor que utilizando la telefonía analógica (Robine, ¿Qué es la Voz sobre IP y cuáles son sus ventajas?, 2021).

2.1.10.2 Tipos de llamadas IP

Las llamadas IP se pueden realizar de 3 maneras distintas, las cuales se detalla a continuación:

Teléfonos IP

"Estos teléfonos se parecen a los teléfonos normales con un auricular, un altavoz para hablar y botones, pero en lugar de tener los conectores telefónicos tradicionales RJ-11, los teléfonos IP tienen un conector Ethernet RJ-45" **(3cx.es, 2021)**. Los teléfonos se conectan directamente al enrutador y poseen el hardware y software necesarios para atender la llamada IP **(3cx.es, 2021)**.

ATA

El ATA (adaptador de teléfono analógico) es un convertidor de analógico a digital, es decir toma la señal analógica de un teléfono tradicional y la convierte en datos digitales para su transmisión a través de Internet, permite conectar un teléfono estándar convencional a la conexión a Internet para usarlo con VoIP **(3cx.es, ¿Qúe son los Teléfono SIP/teléfonos VoIP?, 2021)**.

Softphone

Un softphone es un software basado en en los sistemas de Voz sobre IP (VoIP) que permite realizar y recibir llamadas utilizando una plataforma o una aplicación web, y no con un teléfono de escritorio, cuentan con todas las funcionalidades de un teléfono fijo y, además, con algunas

características que permiten ahorrar tiempo. “El trabajo remoto y el teletrabajo son una realidad gracias a las aplicaciones de llamadas de escritorio y móvil” **(Robine, ¿Qué es un Softphone y qué ventajas tiene?, 2021)**.

2.1.10.3 PBX IP

Un sistema telefónico IP PBX o VoIP reemplaza los sistemas tradicionales PBX o telefónicos, brindando a los empleados un número de extensión, la capacidad de transferir o llamar a un colega y otras funciones, como videoconferencia. Otras llamadas se envían a través de paquetes de datos a través de redes de datos en lugar de las redes telefónicas tradicionales. Con el uso de VoIP Gateway, puede conectar las líneas telefónicas existentes a un IP PBX y realizar y recibir llamadas a través de la línea PSTN **(3cx.es, ¿Qué alternativas existen para PBX IP basadas en SIP?, 2021)**.

Un IP PBX muy utilizado es Issabel, un sistema basado en Linux, y con múltiples funcionalidades el cual se detalla a continuación.

Issabel PBX

“Es un software de código abierto (Open Source) de telefonía IP y Comunicaciones Unificadas basado en Asterisk, utilizado para montar servidores de Comunicaciones telefónicas y Unificadas, que incluye: PBX IP, correo electrónico, mensajería instantánea, fax, funciones colaborativas, etc. El objetivo de ISSABEL es el de incorporar en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial”. **(dasoft, 2021)**

Issabel integra una gran cantidad de funcionalidades de comunicación como es el módulo de call center, fax, email, entre otros, además de ser compatible con la mayoría del hardware telefónico, lo que lo convierte en un de las principales opciones de uso en el ámbito empresarial.

CAPÍTULO 3

3.1 ANÁLISIS DE CONDICIONES ACTUALES

3.1.1 Análisis de equipos que dispone la empresa

La red actual de la empresa Ferrotools muestra las siguientes características en cuanto a su estructura y configuración:

- En la empresa los equipos están organizados y administrados mediante un dominio el cual es manejado a través de un servidor de active directory
- El servicio de internet es brindado por la empresa Telconet con una conexión de fibra óptica con compartición 1:1 y un ancho de banda de 20Mbps.
- Tanto la administración de la página web como el servicio de correo electrónico es brindado por la empresa Digitalarias
- A continuación, se presenta unos cuadros de resumen de los equipos con los que cuenta la empresa (teléfonos, equipos de cómputo y servidores).

UBICACIÓN	TIPO DE EQUIPO	SISTEMA OPERATIVO	CARACTERÍSTICAS	SERVICIO
Rack de servidores	Servidor	Windows server 2008	Intel Xeon E31220 3.1ghz, 8gb RAM, 1tb HDD	Active Directory
	Servidor	Windows server 2012	Intel Xeon E31220 3.1ghz, 8gb RAM, 1tb HDD	ERP
	Central telefónica		Panasonic KX-NS500LA	Central telefónica
	Switch		DGS-10240	switch

Tabla 1: Equipos servidores

USUARIO	TIPO DE EQUIPO	SISTEMA OPERATIVO	CARACTERÍSTICAS
Recepcionista	Escritorio genérico	Windows 10	Intel Core i3, 4gb RAM, 500gb HDD
Administrador	Escritorio genérico	Windows 10	Intel Core i3, 4gb RAM, 500gb HDD
Contabilidad	Escritorio genérico	Windows 10	Intel Core i3, 4gb RAM, 500gb HDD
Bodega	Escritorio genérico	Windows 10	Intel Core i3, 4gb RAM, 500gb HDD
Vendedor 1	Escritorio genérico	Windows 10	Intel Core i3, 4gb RAM, 500gb HDD
Vendedor 2	Escritorio genérico	Windows 10	Intel Core i3, 4gb RAM, 500gb HDD
Vendedor 3	Escritorio genérico	Windows 10	Intel Core i3, 4gb RAM, 500gb HDD

Tabla 2:Equipos empleados

UBICACIÓN	Marca	Modelo
Recepcionista	Panasonic	KX-TS520LX
Administrador		
Contabilidad		
Bodega		
Vendedor 1		
Vendedor 2		
Vendedor 3		

Tabla 3: Equipos telefonía

En cuanto a la red ethernet la empresa cuenta con cableado estructurado con cable ethernet CAT.6 con una toma de red para cada estación de trabajo, de igual manera para la red de telefonía.

3.1.2 Evaluación de Equipos y Red

Al momento la empresa cuenta con un servicio de internet por fibra óptica de 100mbps simétrico y con una dirección IP publica, la empresa no cuenta con un firewall y el router del proveedor de internet se conecta directamente al switch.

En el caso de la telefonía, la empresa utiliza una central PBX de tipo analógico con 4 líneas telefónicas y 8 extensiones, por lo que si se deseara implementar telefonía IP sería necesaria la

adquisición de un equipo servidor con software PBX, un gateway que permita la conexión de las líneas telefónicas convencionales, además de los respectivos teléfonos SIP.

La empresa dispone de un servidor HP con Windows Server 2008, el cual cumple la función de active directory para controlar los accesos de usuarios, y la además de contener y administrar las carpetas compartidas con los respectivos permisos.

Adicionalmente, se dispone de un servidor de aplicaciones con el sistema de contabilidad, el cual es un sistema de tipo cliente-servidor, para el que se tiene acceso únicamente en la red local, pero la empresa está planificando el cambio de sistema de contabilidad por uno basado en la web.

La empresa cuenta actualmente con cableado estructurado simple con cable UTP categoría 6 organizado mediante canaletas, el cual provee de una conexión ethernet y una conexión telefónica en cada puesto de trabajo de la empresa.

El tráfico es manejado mediante un switch de 24 puertos de la marca D-link en el cual se conecta cada uno de los 8 computadores además de los servidores y las cámaras de seguridad y el equipo NVR.

El equipo telefónico está conformado por una central de la marca Panasonic modelo KX-NS500LA la cual tiene conexión con 4 líneas telefónicas analógicas y 10 extensiones.

En este sentido, en la ilustración 1 se detalla la distribución de la red de la empresa.

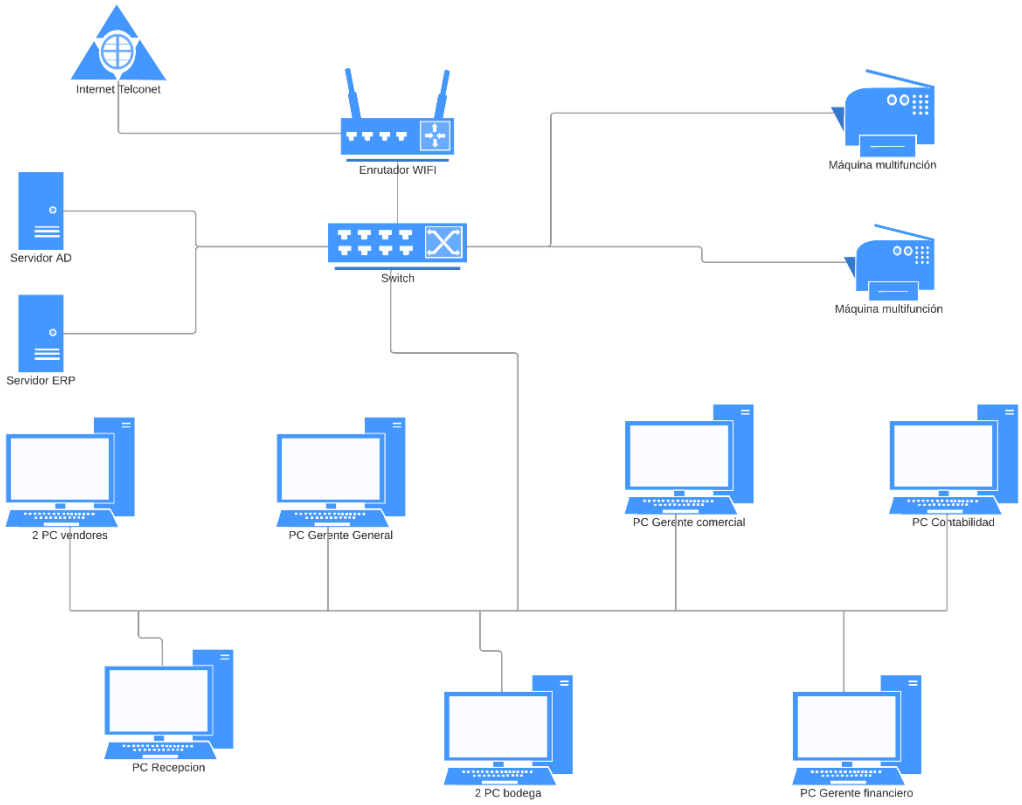

Ilustración 1: Red actual de la empresa

3.1.3 Características de equipos a utilizarse

Para la implementación de la Voz IP se creará una máquina virtual que actuara como servidor VoIP para la realización de las pruebas necesarias para este proyecto, ya que la empresa cuenta con un PBX Panasonic, y tiene planeado realizar la transición al nuevo sistema posteriormente, para la implementación de la VPN será necesario adquirir un equipo con las características que se detallan a continuación en la ilustración 2:

Computador para servidor VPN	
Cantidad	**Características**
1	Procesador Core-i3 o Superior Memoria ram de 8GB o mas Disco duro 500GB 2 tarjetas ethernet pci Express

Tabla 4: Equipo necesario para VPN

3.1.4 Reporte de situación actual de la empresa

Después de realizar una revisión del estado actual de la red de la empresa se estableció a las siguientes conclusiones:

- Considerando que la empresa cuenta con una adecuada conexión a internet, así como la mayor parte de los empleados, se implementara un servicio de VPN el cual permita a los empleados conectarse a la red de la empresa desde sus hogares o cualquier lugar que cuente con conexión a internet.

- La empresa cuenta actualmente con 3 vendedores y 1 contadoras quienes serían los principales beneficiados de la conexión remota además de las distintas gerencias.

- Durante reunión mantenida con el gerente general se informó que el actual software ERP será reemplazado por una alternativa web más moderna y que permitirá agilizar los procesos de la empresa lo cual se tomará en cuenta para la configuración de la VPN ya que ya no será necesario la conexión del servidor ERP actual.

- Se deberá adquirir un equipo, el cual será configurado para funcionar como servidor VPN.

CAPÍTULO 4

4.1 DISEÑO DE LA VPN

4.1.1 Análisis de la distribución Linux a utilizar

Después de revisar la información de las distribuciones de sistema operativo basados en Linux orientados a los firewalls se determinó que la utilización de una de estas distribuciones es lo más adecuado ya que al ser basadas en Linux son gratuitas, además de estar optimizadas para su funcionamiento como firewall y contar con funciones dedicadas a este objetivo como lo es la creación de una VPN.

Dado que existen varias opciones en distribuciones Linux para firewall, se decidió revisar las características que tiene cada una de ellas, así como su ventaja y desventajas, con el fin de determinar la mejor opción a utilizar.

Entre las distribuciones para firewall que se analizó están las siguientes:

- IPFire
- pfSense
- OPNSense

A continuación, en la tabla 4 se presenta las características deseadas en cada distribución y además se da una valoración en el rango de 1 a 10 de acuerdo con el cumplimiento de estas.

Características Deseadas	OPNsense	IPFire	PFSense
Fácil instalación	9	8	9
Incorpora Ipsec y OpenVPN	9	7	9
Permite visualizar graficas de tráfico en tiempo real	10	2	9
Actualizaciones frecuentes	8	4	8
Documentación clara	9	4	6
Consume pocos recursos	8	8	8
Permite instalación de características adicionales	9	1	7
Comunidad de soporte	8	5	7
Alta compatibilidad de hardware	9	7	8
Interfaz de configuración intuitiva	9	5	7
Configuración de cifrado VPN	8	6	7
TOTAL	96	57	85

Tabla 5: Comparativa distribuciones Linux

Una vez realizado el análisis y valoración de las opciones de sistema operativo para firewall seleccionadas, se encontró que la mejor puntuada fue OPNSense, ya que ofrece estabilidad y seguridad y está enfocado su utilización en empresas por lo que ofrece las caracteristicas necesarias para tener un servicio de VPN con excelentes características técnicas. En conclusión, se decidió la utilización del sistema operativo OPNSense ya que este ofrece las mismas características que PFsense que es una de las mejores opciones, pero con una interfaz más sencilla y fácil de configurar además de ser gratis y su documentación explica de manera clara como realizar su configuración y corregir errores.

4.1.2 Establecer software VPN a utilizar

Es necesario también determinar que protocolo de VPN se utilizará, ya que OPNSense permite la configuración de OpenVPN y de Ipsec, a continuación, en la tabla 5 se analizará las ventajas y desventajas de cada uno y se le dará una valoración en el rango de 1 a 10 de acuerdo con su cumplimiento de las características requeridas:

Características Deseadas	OpenVPN	IPsec
Configuración sencilla	7	8
funciona con protocolo UDP y TCP	10	9
Se ejecuta en todas las plataformas	9	9
Ofrece una Conexión Cifrada Y segura	8	9
La autenticación se puede realizar de manera sencilla	9	9
Comunidad de soporte	9	7
es capaz de evitar de manera fácil cualquier firewall	9	7
Ofrece una Velocidad de conexión estable y cifrada	8	7
TOTAL	69	65

Tabla 6: Comparativa protocolos VPN

Luego de analizar las tablas de características, se llegó a la decisión de utilizar OpenVPN ya que es más sencillo de configurar y es compatible con la gran mayoría de sistemas operativos, así mismo, dispone de su propia aplicación, la cual es de código abierto, además de permitir configurar encriptación, por lo que es uno de los sistemas más seguros.

Finalmente, el motivo para elegir usar el sistema OpenVPN es por su seguridad dado su nivel de cifrado estable, además dado que es open Source y se puede configurar en distintas plataformas, sin dejar de lado que maneja su propio protocolo y que tiene una comunidad que se encuentra en constante actualización de este.

4.1.3 Topología de la red a implementarse

En la ilustración 3 se puede apreciar la topología que será implementada para el funcionamiento de la VPN y la VoIP.

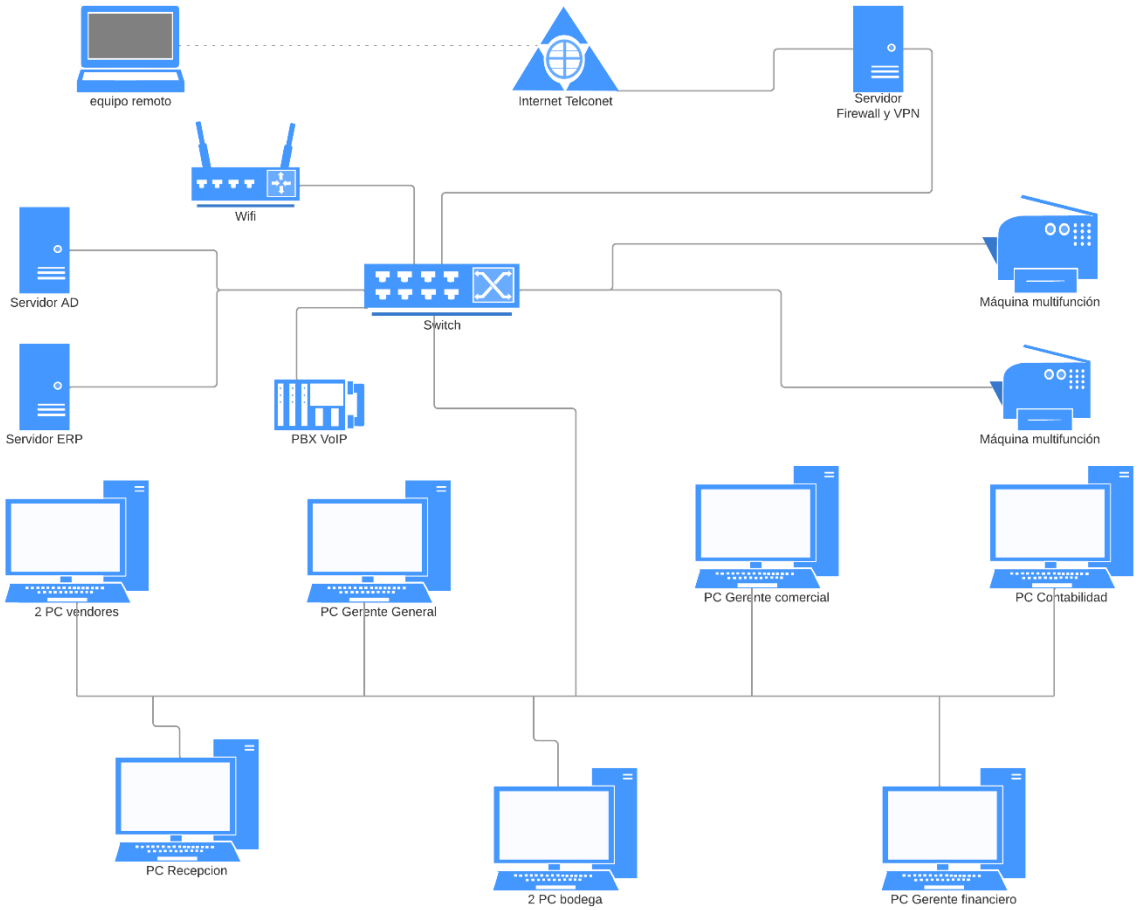

Ilustración 2: Topología de la red VPN

4.1.4 Clientes VPN a crearse

Una vez determinado el número de empleados de la empresa que harán uso de la conexión VPN, los cuales se detallan a continuación en la tabla 6 con los servicios a los que tendrá acceso cada usuario.

CLIENTE VPN	Usuario	área	Uso	Servicios
Cliente1	Ftapia	Gerente General	Escritorio Remoto	Carpetas compartidas, VoIP, Impresora
Cliente2	Grengifo	Gerente Financiera	Escritorio Remoto	Carpetas compartidas, VoIP, Impresora
Cliente3	Mcoyago	Contabilidad	Escritorio Remoto	Carpetas compartidas, VoIP, Impresora
Cliente4	FMtapia	Gerente Comercial	Escritorio Remoto	Carpetas compartidas, VoIP, Impresora
Cliente5	JCaguilar	Vendedor	Escritorio Remoto	Carpetas compartidas, VoIP, Impresora
Cliente6	Ecueva	vendedora	Escritorio Remoto	Carpetas compartidas, VoIP, Impresora
Cliente7	Barcentales	Bodega	Escritorio Remoto	Carpetas compartidas, VoIP, Impresora

Tabla 7: Usuarios de VPN

CAPÍTULO 5

5.1 IMPLEMENTACIÓN DE LA VPN Y VOIP

5.1.1 Descripción de equipos

Posteriormente y una vez determinado que se hará uso de OPNSense, es indispensable realizar la instalación y respectiva configuración del mismo.

Para la Instalación del servidor VPN se hará uso de un equipo en desuso de la empresa el cual cuenta con un procesador Core i3 y se le realizo una actualización de sus componentes como es la RAM la cual se actualizo a 8gb y el disco duro el cual se actualizo a un SSD de 128gb además de añadir una tarjeta de red adicional, ya que en la tarjeta de red integrada se conectará directamente a el equipo de conexión del ISP y en la tarjeta adicional se conectará al switch de la empresa.

Ilustración 3: CPU a configurar

5.1.2 Instalación y configuración del sistema OPNSense

Para la instalación de OPNSense se debe realizar la descarga de la imagen ISO desde su página oficial y generar un USB Booteable para empezar la instalación.

Posteriormente, se procede a prender el equipo con el USB booteable creado que fue generado, y se elige opciónde inicio el USB.

5.1.2.1 Creación de USB de instalación de OPNSense

Para la creación del USB de arranque se optó por la utilización de la herramienta Rufus y se lo instaló en un computador como se muestra a continuación:

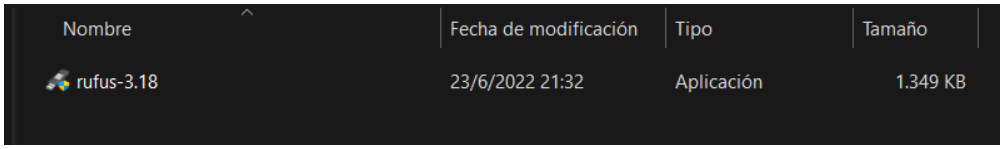

Ilustración 3: Herramienta Rufus

Luego de ser instalada, debe ser ejecutado el programa y se elige la unidad USB y el archivo ISO, descargado previamente, para crear el USB Booteable, como puede ser visualizado a continuación:

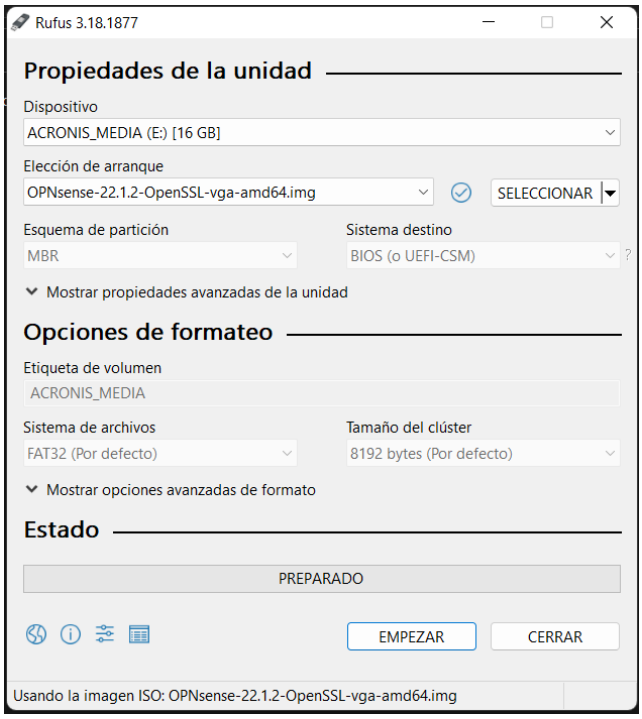

Ilustración 4: creación de USB instalador

Se debe dar clic en Empezar y esperar a que termine el proceso.

5.1.2.2 Instalación de OPNSense

Se arranca el equipo colocando la USB booteable y a continuación se debe esperar a que el USB sea reconocido, en ocasiones es necesario ingresar a la BIOS del equipo y configurarlo para que sea capaz de iniciar desde el dispositivo USB.

A continuación, se muestra la pantalla del inicio de instalación de OPNSense:

Ilustración 5: Pantalla de inicio de instalación

Se iniciará automáticamente el procedo de carga del sistema, una vez terminado se tiene esta pantalla:

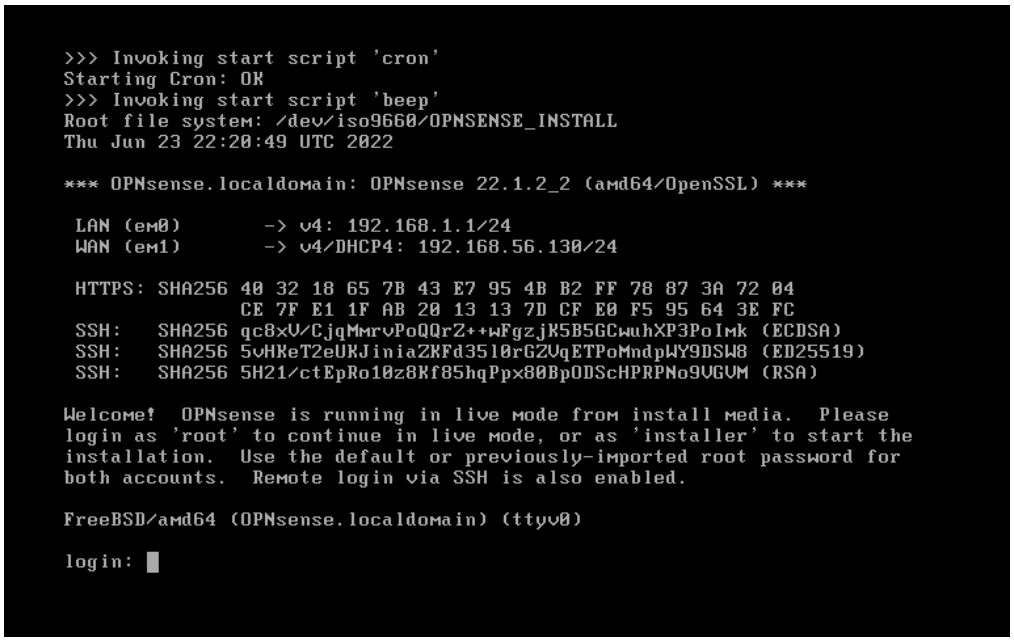

Ilustración 6: pantalla de fin de carga

El siguiente paso es iniciar la instalación del sistema en el disco duro del equipo, para esto se debe iniciar sesión con el usuario installer y la contraseña opnsense:

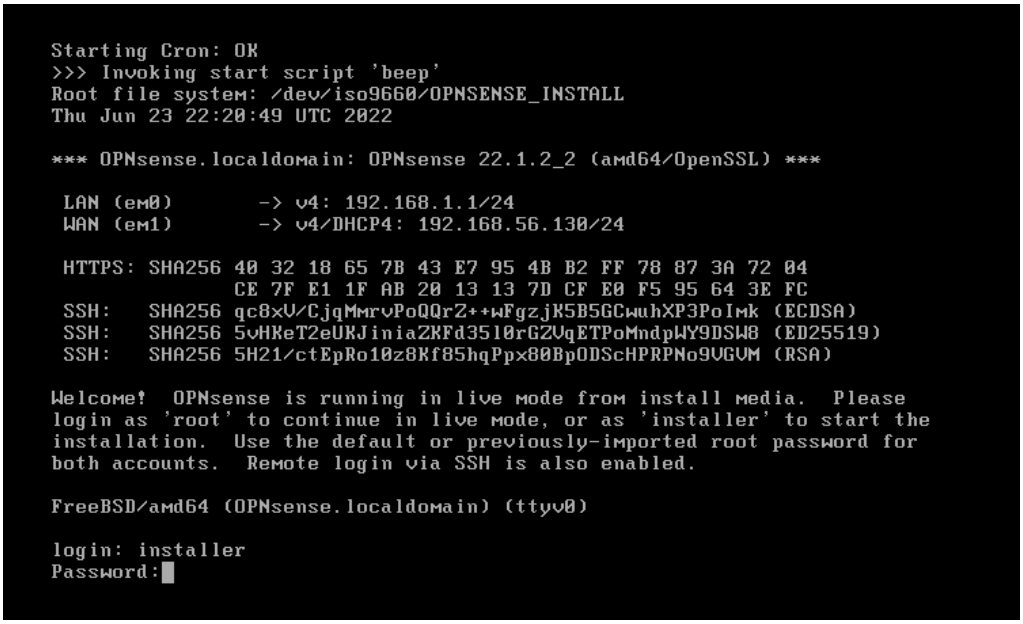

Ilustración 7: Inicio del proceso de instalación

Una vez iniciada sesión con el usuario installer se tendrá la siguiente pantalla:

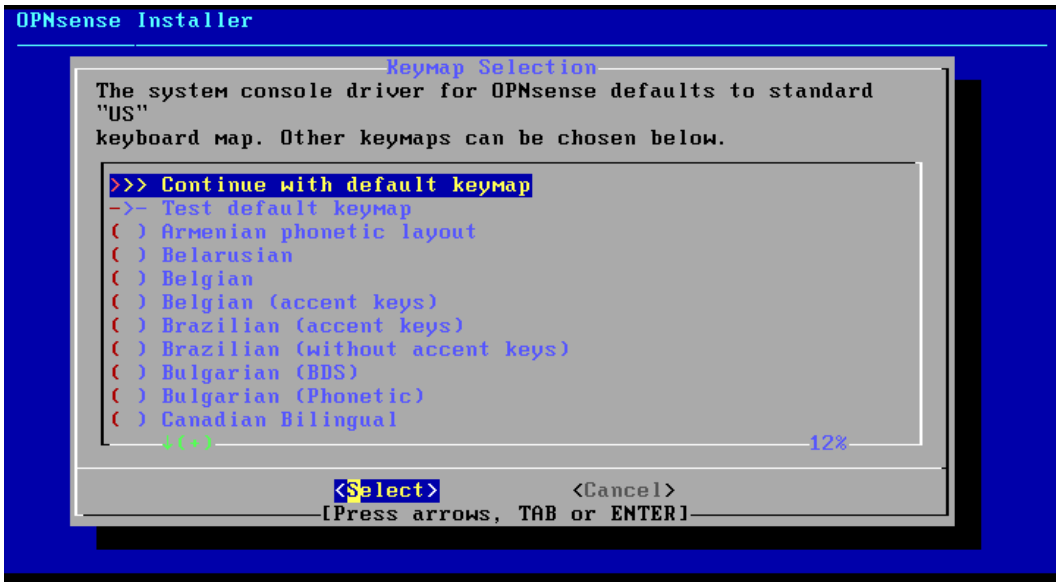

Ilustración 8: Pantalla de selección de idioma del teclado

Se selecciona el idioma con el que se usará el teclado y a continuación se presentará las siguientes opciones:

Ilustración 9: Selección de formato de instalación

Se elige la primera opción para utilizar el sistema de archivos UFS y a continuación se debe seleccionar la unidad de disco donde se instalará el sistema:

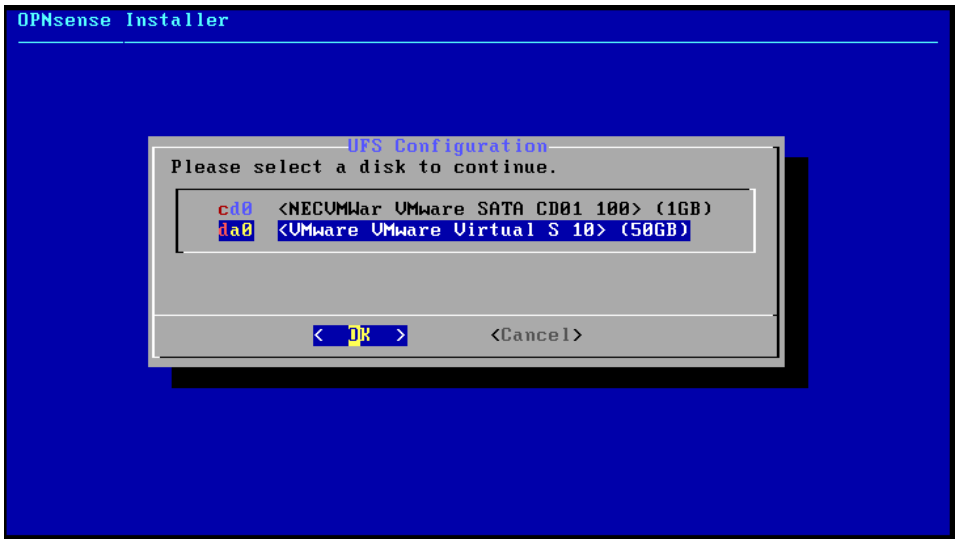

Ilustración 10: Selección de unidad de disco

Aparecerá la pregunta de si se desea continuar con la configuración predeterminada de la partición swap de 8gb, a la cual se seleccionará la opción ok.

Ilustración 11: Confirmación partición swap

Saldrá la pregunta por última vez de si se está seguro de formatear la unidad de disco seleccionada, a lo que se deberá escoger la opción YES.

Ilustración 12: Confirmación de formateo de disco

A continuación, iniciará el proceso de instalación y se deberá esperar a que este termine.

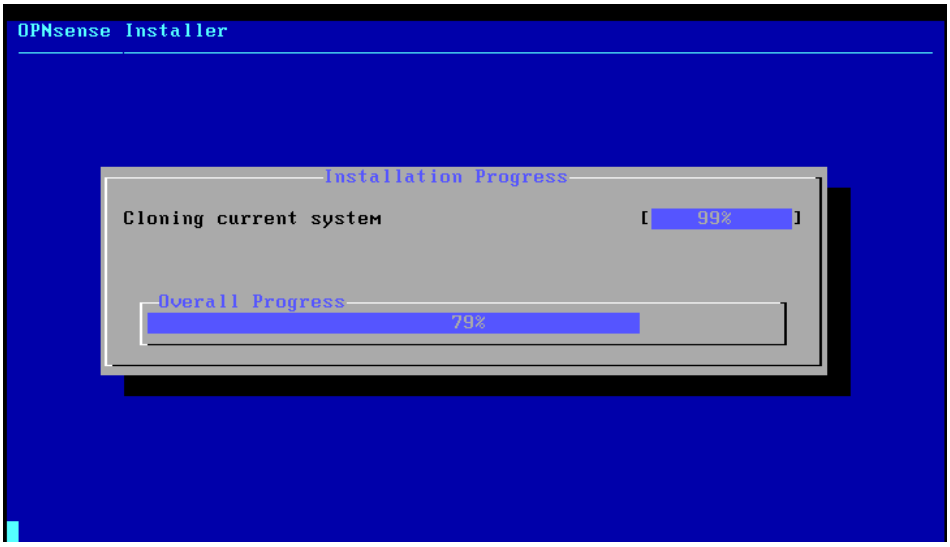

Ilustración 13: Progreso de instalación

Una vez concluido el proceso se dará la opción de cambiar la contraseña del usuario Root, lo cual es importante de realizarlo.

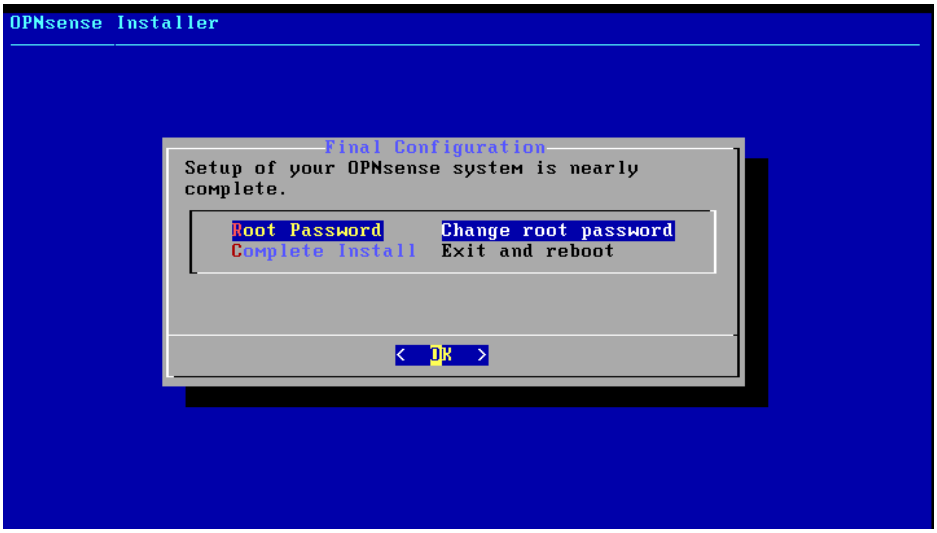

Ilustración 14: Cambio de contraseña Root

Una vez cambiada la contraseña se seleccionará la opción Complete Install y el equipo se reiniciará.

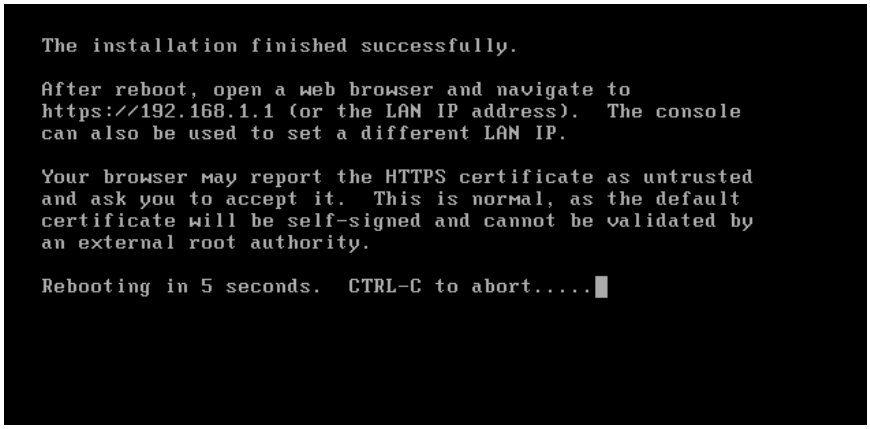

Ilustración 15: reinicio del equipo

Posteriormente y luego de que el equipo se reinicie ya se tendrá el sistema completamente instalado y se podrá empezar a configurarlo.

Ilustración 16: Login después de Reinicio

Para empezar a configurar el sistema se deberá iniciar sesión con el usuario Root y la contraseña que se acaba de cambiar, una vez iniciada la sesión se presentará las siguientes opciones:

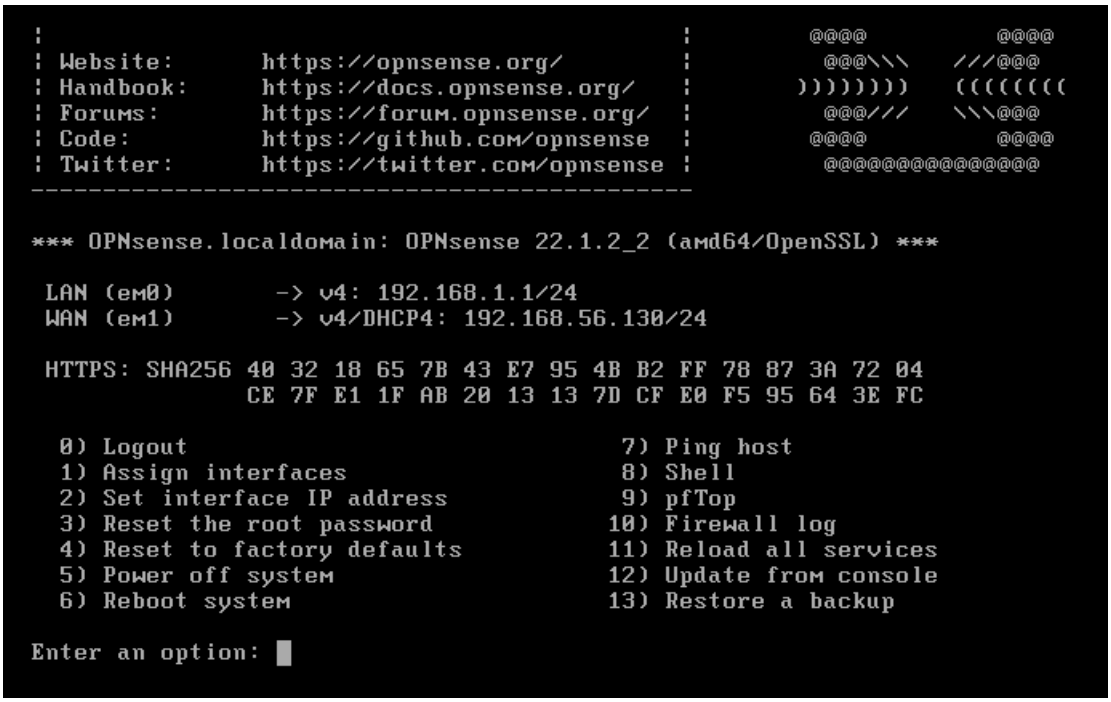

Ilustración 17: Menú de configuración

Ahora se deberá configurar las interfaces de red, es decir indicarle al sistema cual tarjeta de red se utilizará para la red WAN o la conexión a internet y cual será utilizada para la red LAN o la conexión interna, para esto se debe seleccionar la opción 1 Assign Interfaces.

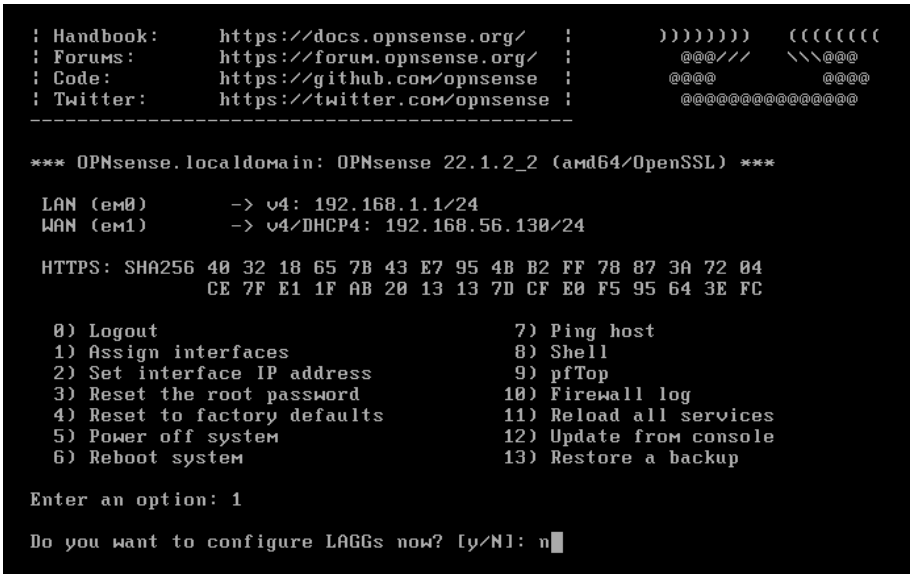

Ilustración 18: Configuración de interfaces

Aparecerá la pregunta de si se desea configurar LAGGs y VLANS, a ambas opciones se debe

seleccionar que no.

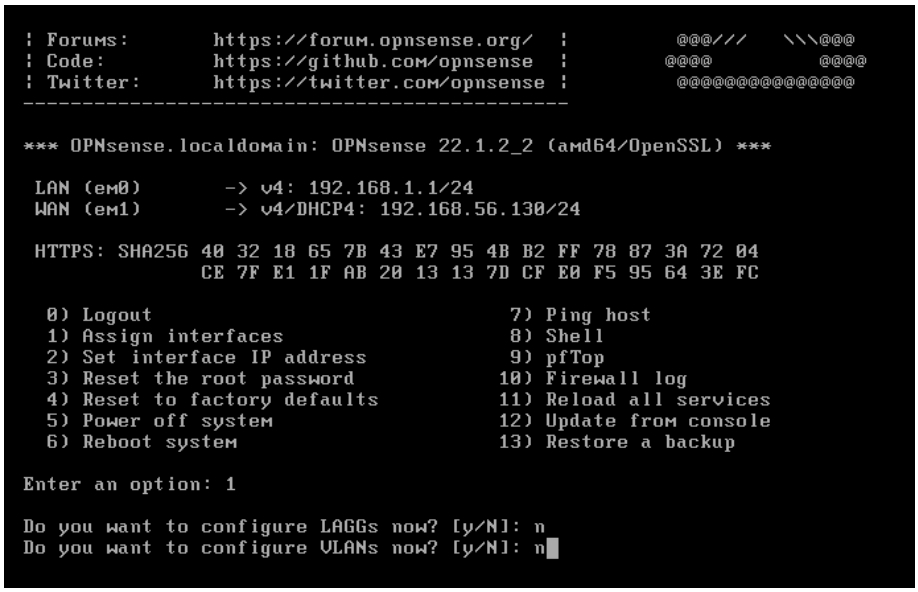

Ilustración 19: Configuración de interfaces 2

A continuación, se pedirá que se asigne el adaptador de red que será usado para la red WAN.

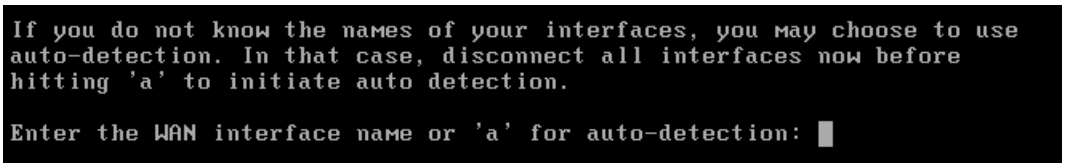

Ilustración 20: Configuración adaptador WAN

Se seleccionará el adaptador re0 que corresponde al adaptador de red integrado, a continuación se debe indicar cual será el adaptador de red para la conexión LAN, a lo que se debe seleccionar el adaptador ue0 correspondiente a la tarjeta de red secundaria.

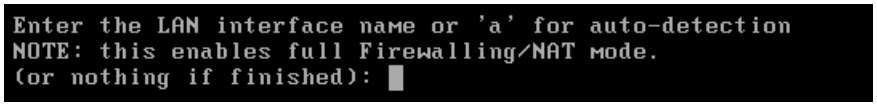

Ilustración 21: Configuración adaptador LAN

Una vez configuradas las interfaces de red, el sistema los configurará y se debe volver al menú de inicio he indicará las IP de cada interfaz de red.

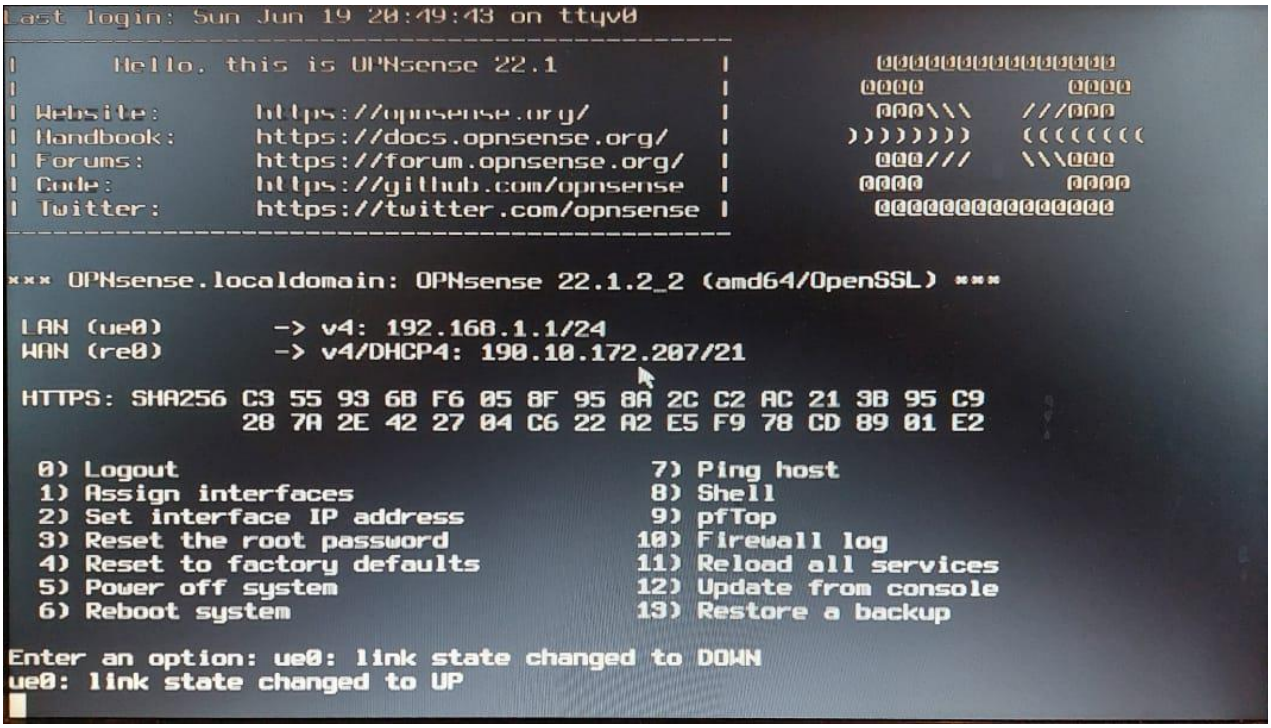

Ilustración 22: IPs Interfaces de red

Ahora que se encuentra configuradas las interfaces de red y cada una con su respectiva IP, en el caso de la interfaz WAN obtendrá la IP publica que da el proveedor de internet, es decir 190.10.172.207/21, y en el caso de la interfaz LAN se configurara una IP fija, es decir 192.168.1.1/24 la cual permitirá acceder a la interfaz de configuración grafica.

5.1.3 Configuración del firewall

Para acceder a las configuraciones del sistema OPNSense se debe acceder a través de un navegador web a la IP fija que se asignó a la interfaz LAN.

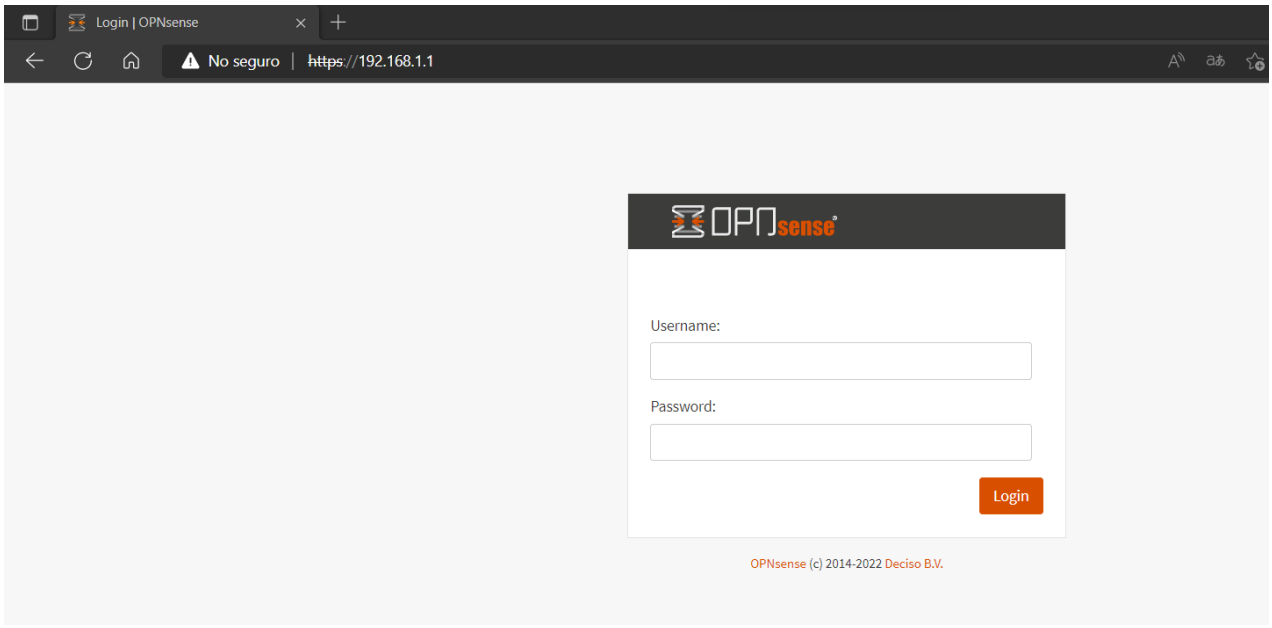

Ilustración 23: Login Interfaz Grafica

Para poder ingresar se deberá colocar el usuario y contraseña ROOT que se configuró previamente durante la instalación.

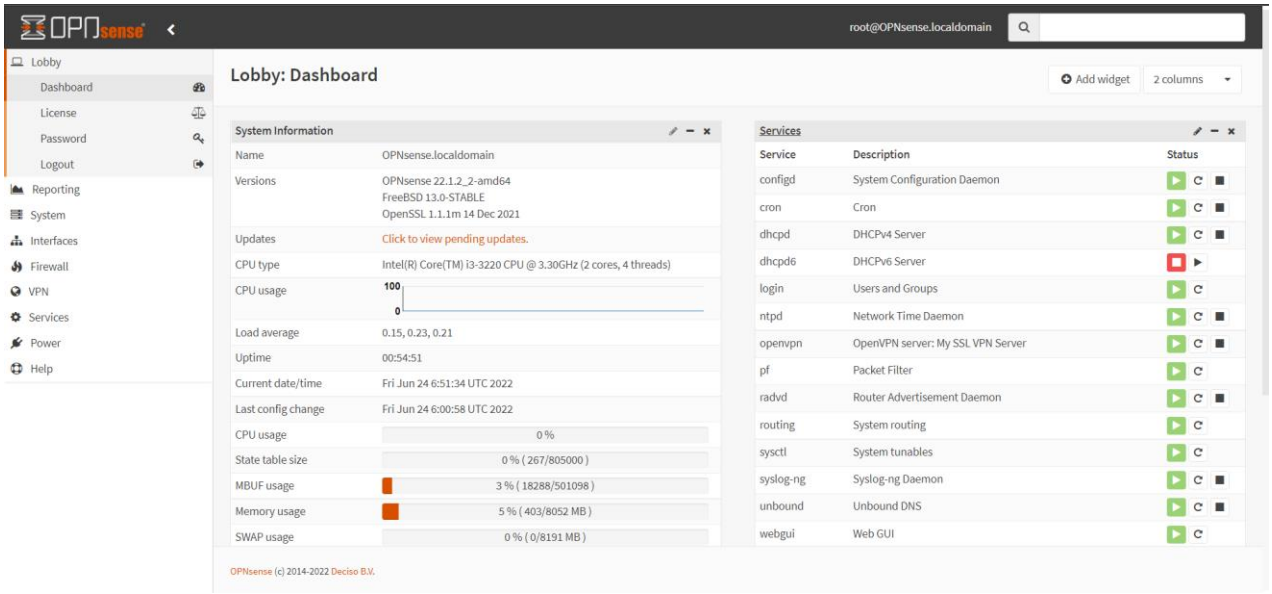

Ilustración 24: Interfaz Gráfica de configuración

El sistema OPNSense configura de manera automáticamente el servicio de firewall, por lo que

la configuración de este es necesario solamente si se quiere agregar restricciones o alguna configuración especial.

5.1.4 Configuración de OpenVPN

OPNSense incorpora la opción de configuración de una red VPN mediante el uso de OpenVPN de una manera sencilla, el primer paso es configurar una autoridad de certificación. Para esto se debe ir siguiente menú System ‣ Trust ‣ Authorities y dar clic en add, y completar las opciones como se muestra a continuación:

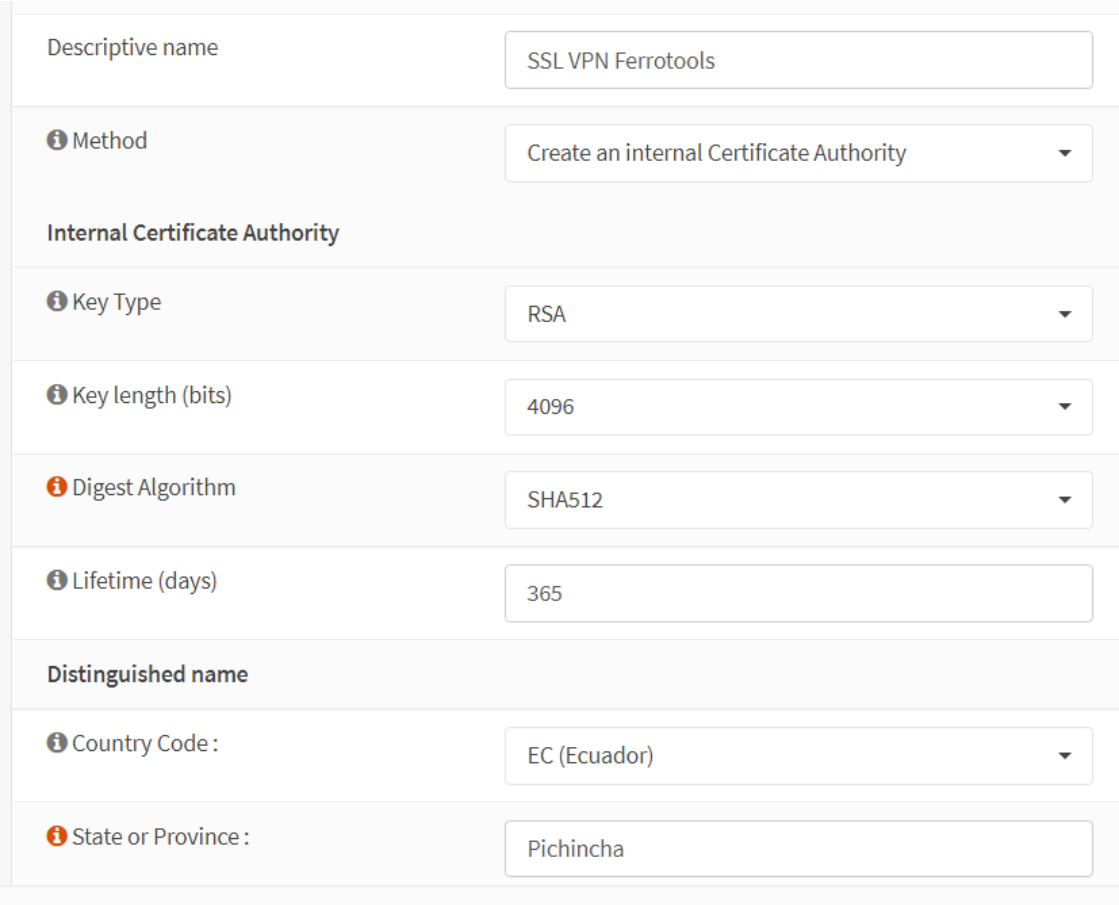

Ilustración 25:Configuración autoridad de certificado 1

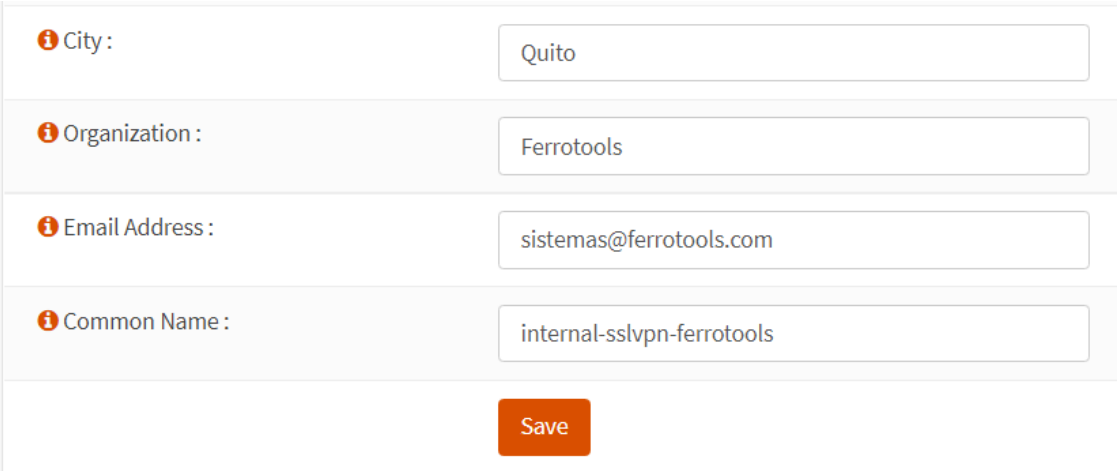

Ilustración 26: configuración autoridad de certificado 2

A continuación, se debe configurar un certificado del servidor accediendo al menú System ▸ Trust ▸ Certificates y se da clic en Add, y se aplica la siguiente configuración:

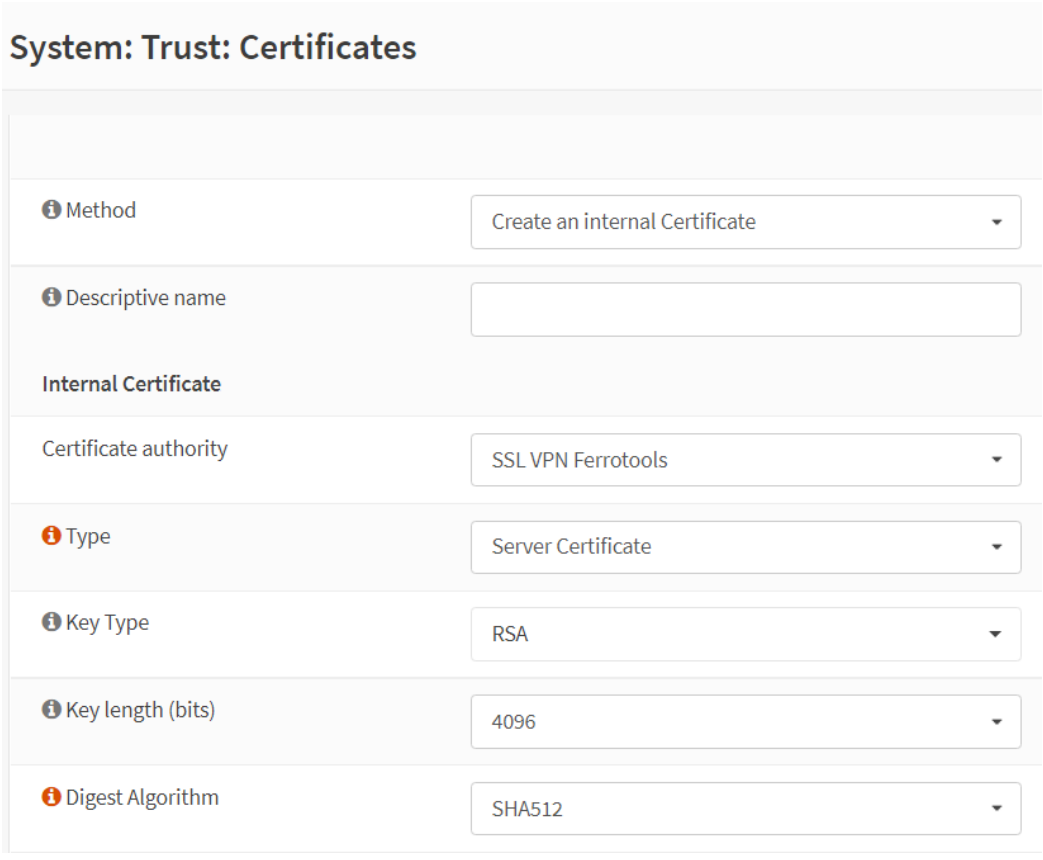

Ilustración 27: Configuración certificado servidor 1

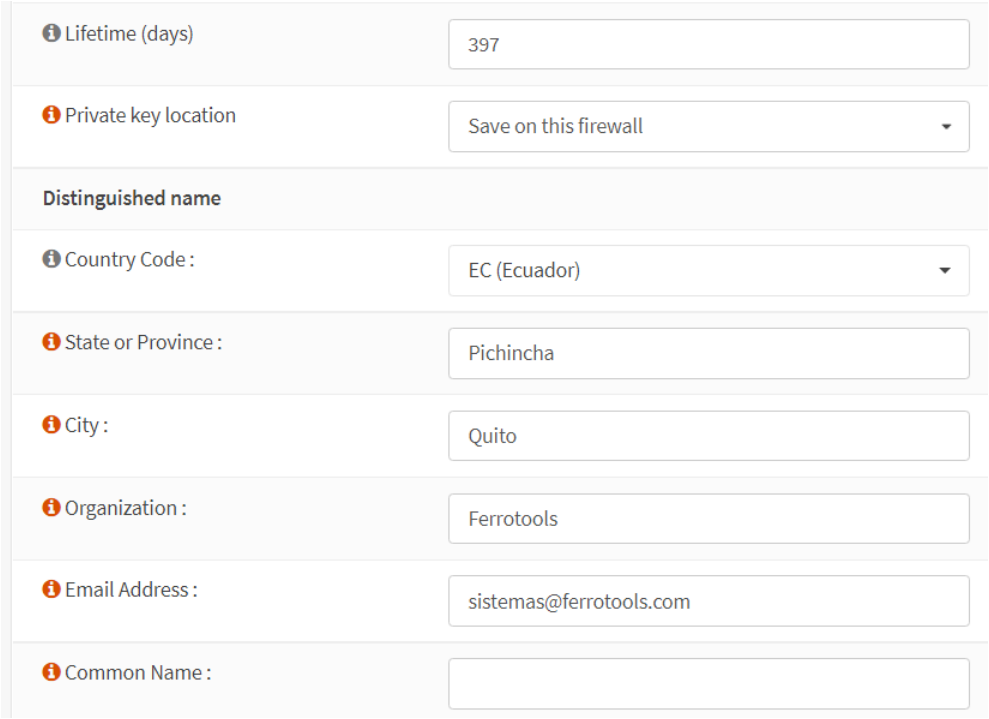

Ilustración 28: Configuración certificado servidor 2

A continuación, se podrá crear los distintos usuarios que harán uso de la conexión VPN así como sus respectivos certificados, como se muestra a continuación:

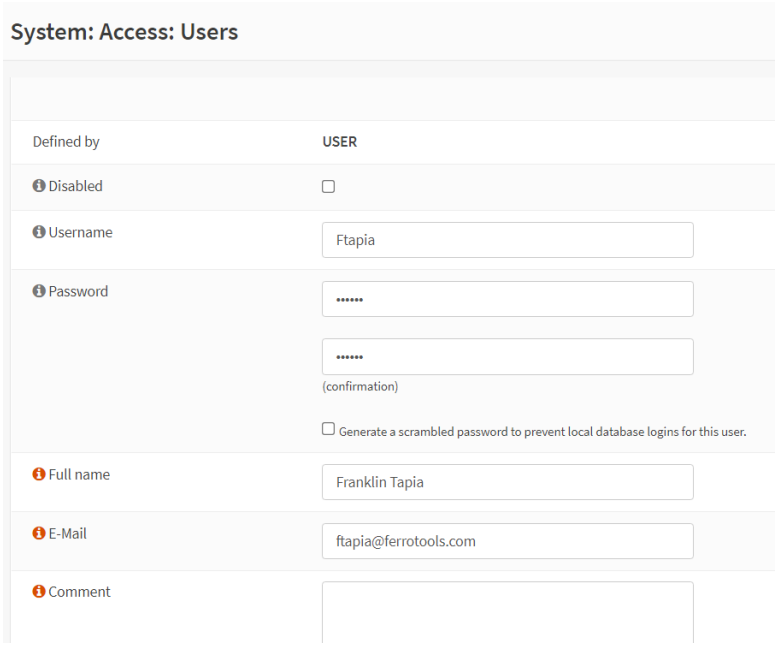

Ilustración 29: Creación de usuario 1

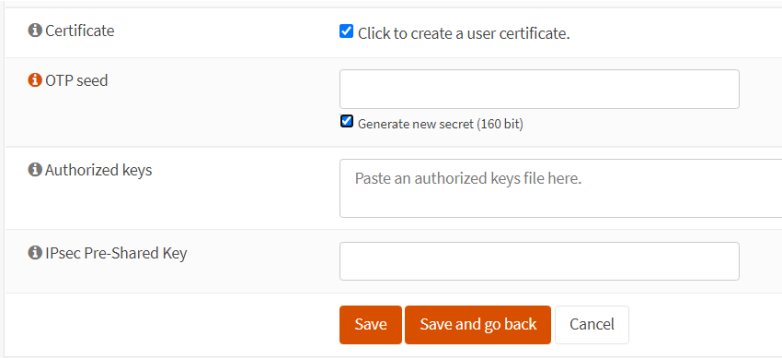

Ilustración 30: Creación de usuario 2

Al dar clic en SAVE se dirigirá al formulario de configuración del respectivo certificado de usuario:

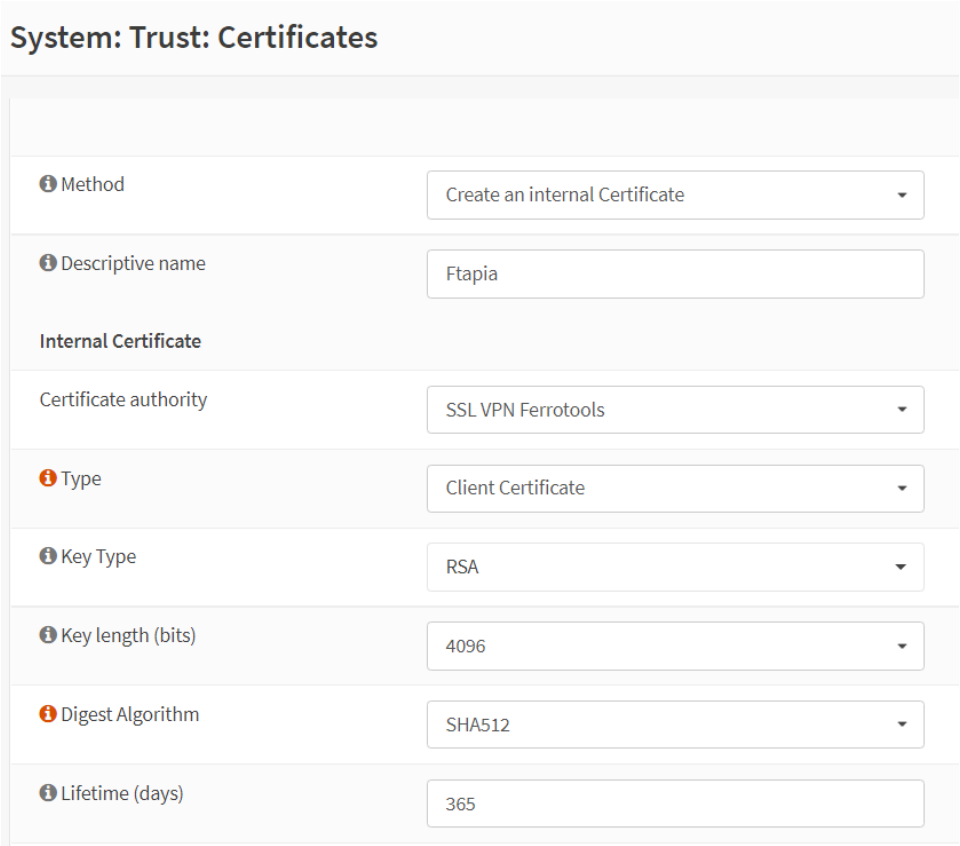

Ilustración 31: Creación de certificado de usuario

Ahora se debe configurar el servidor SSL OpenVPN ingresando al menú VPN ▸ OpenVPN ▸ Servers y aplicando la siguiente configuración:

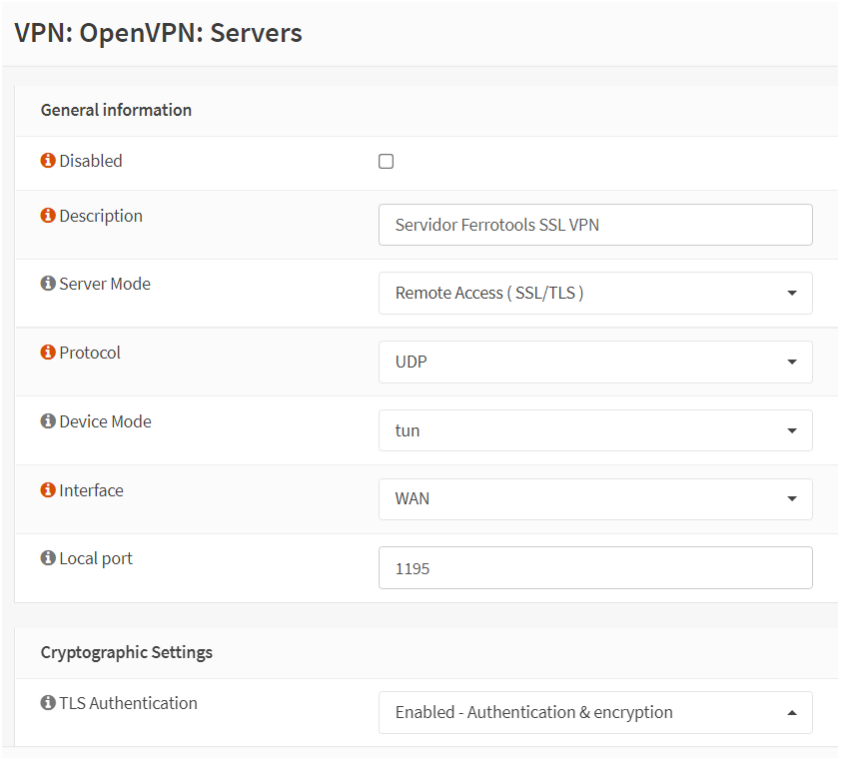

Ilustración 32: Creación servidor ssl 1

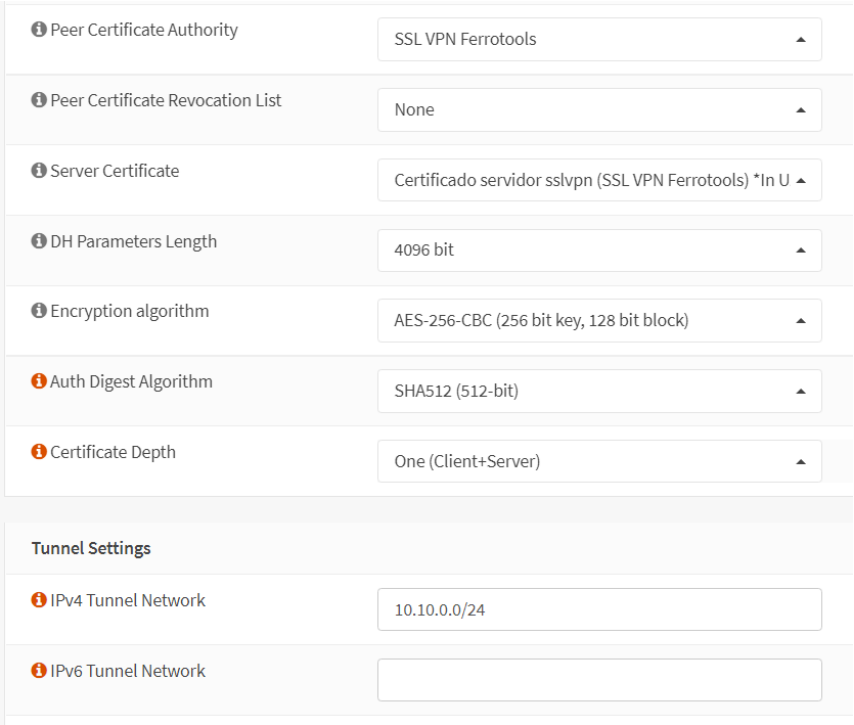

Ilustración 33: Creación servidor ssl 2

También se debe aplicar unas reglas en el firewall para permitir la comunicación entre los equipos remotos y los equipos locales, para esto se debe acceder al menú Firewall ‣ Rules y aplicar la siguiente configuración:

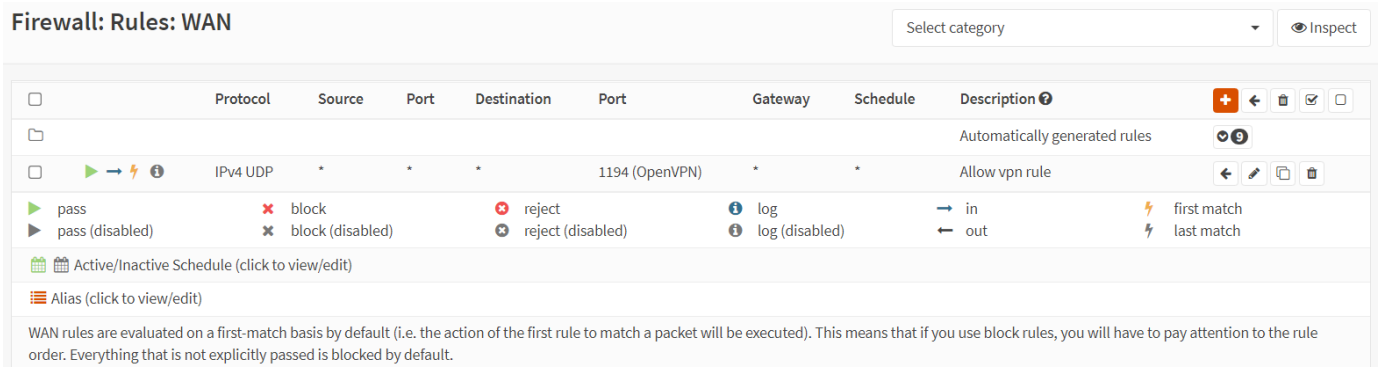

Ilustración 34: Reglas firewall WAN

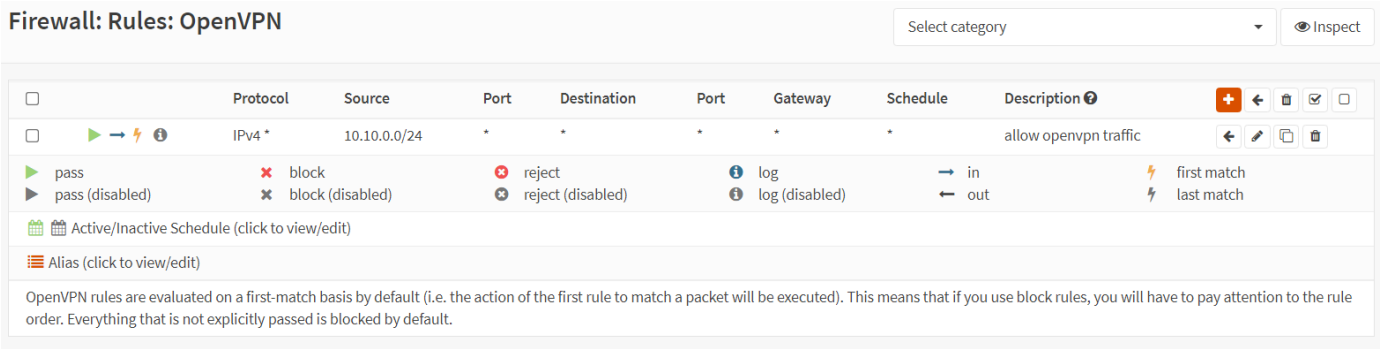

Ilustración 35: Reglas firewall OpenVPN

Finalmente se tendrá que realizar la exportación del archivo de configuracion de OpenVPN de cada usuario ingresando al menú VPN ‣ OpenVPN ‣ Client Export

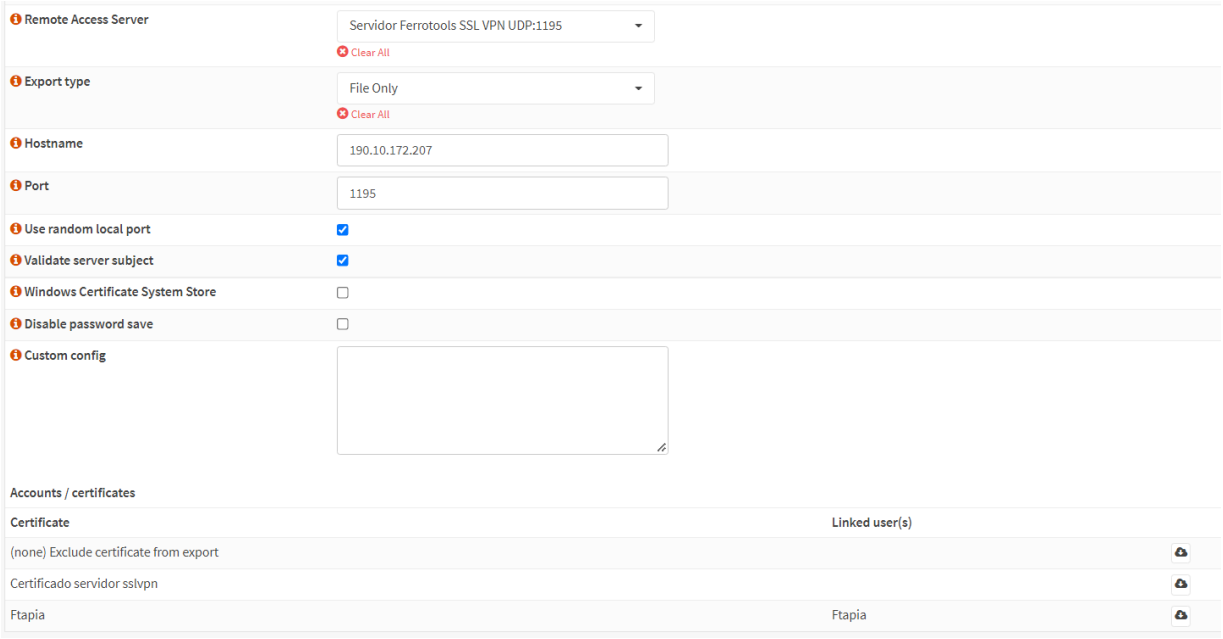

Ilustración 36: Exportación archivo de configuración

5.1.5 Instalación del cliente OpenVPN en equipo del usuario

Para la instalación del cliente que permite la conexión de openvpn se necesita descargar el instalador de la páginaoficial de OpenVPN.

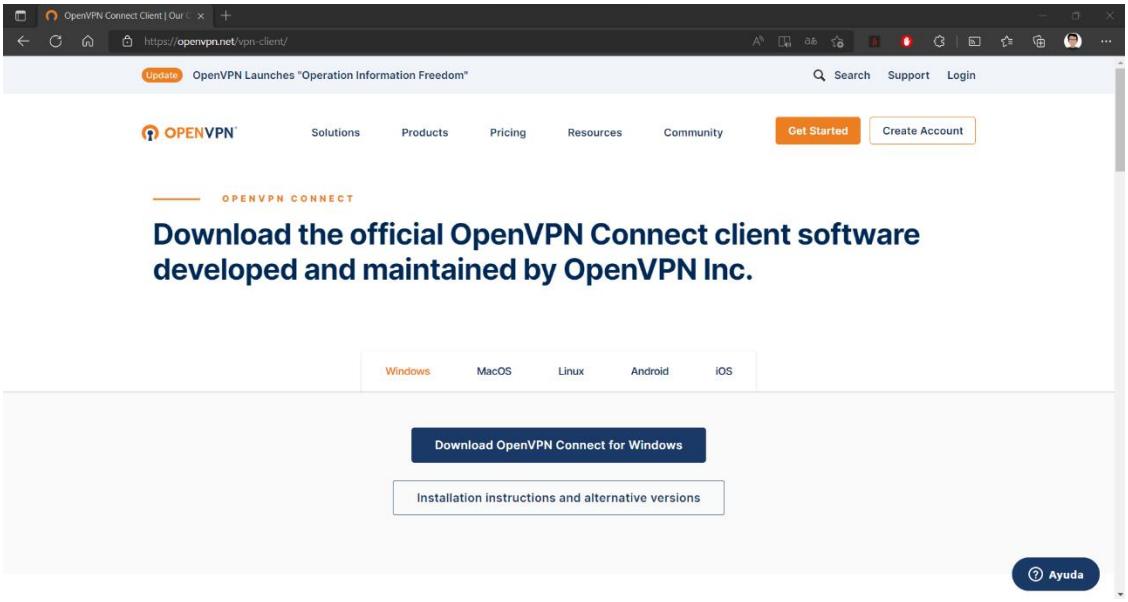

Ilustración 37: Página web de openvpn

En Windows se debe ejecutar openvpn-install-3.3.6.2752 con permisos de administrador, es importante descargar la versión adecuada para el sistema operativo del usuario.

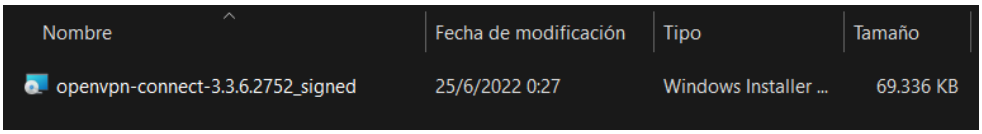

Ilustración 38: Instalador de openvpn

Después de ejecutar el instalador se genera la ventana de bienvenida para la instalación de OpenVPN,Se presiona siguiente para continuar.

Ilustración 39: Ventana de instalación OpenVPN

Se acepta el acuerdo de Licencia

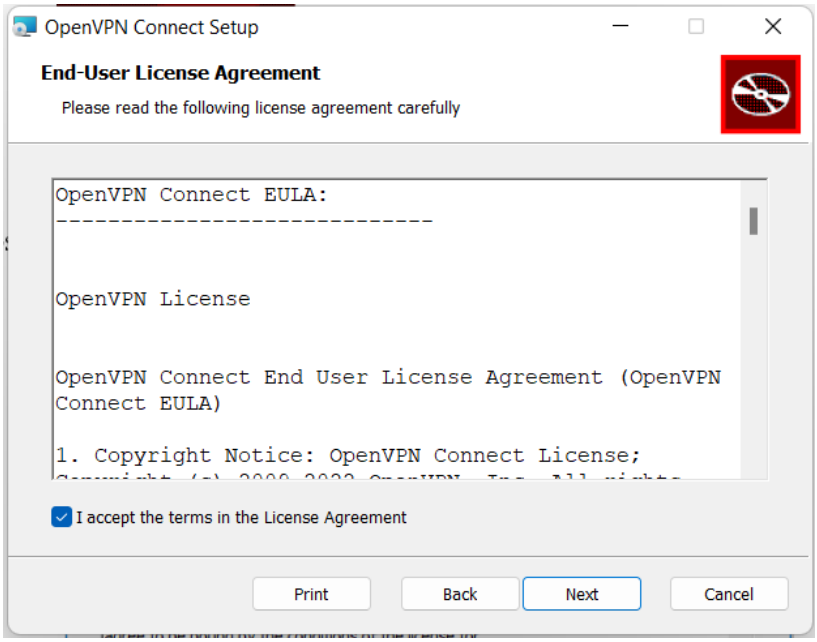

Ilustración 40: Acuerdo de licencia

Iniciará el proceso de instalación:

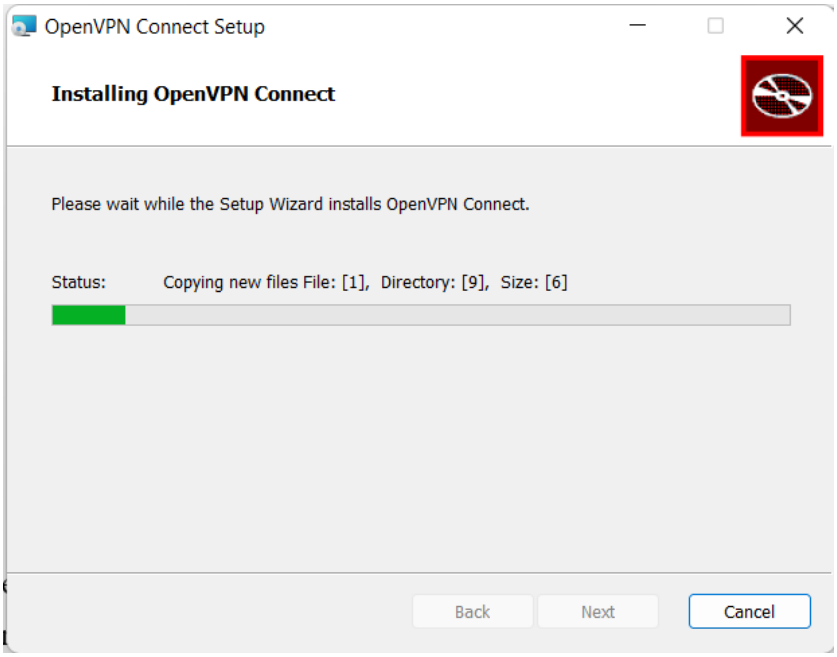

Ilustración 41: Instalación OpenVPN

Una vez completada la instalación se iniciará el Programa donde se tendrá que configurar la conexión al servidor VPN.

Ilustración 42: Ventana principal OpenVPN

Se debe abrir el archivo de configuración del usuario que se exportó desde el servidor VPN.

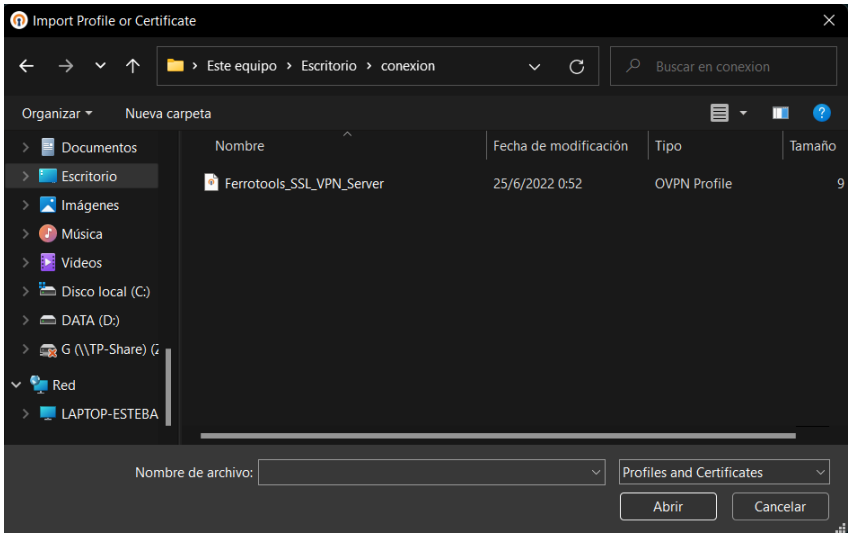

Ilustración 43: selección de archivo de configuración

Una vez seleccionado el archivo de configuración se presentará la siguiente pantalla donde se dará clic en conectar para iniciar la conexión a la VPN.

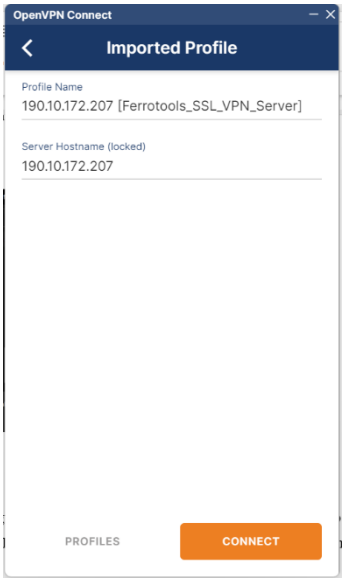

Ilustración 44: Pantalla de conexión

Una vez establecida la conexión se presenta la siguiente pantalla la cual indica los datos de la conexión.

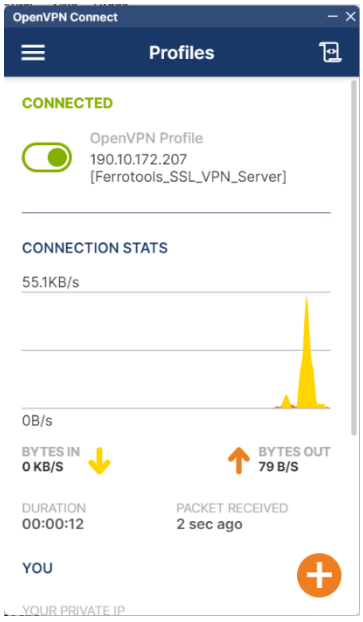

Ilustración 45: Ventana de conexión exitosa

En el panel de control de dispositivos de red aparecerá una nueva tarjeta de red con el nombre TAP, la cual se activará y desactivará cada vez que conecte o desconecte de la VPN.

Ilustración 46: Adaptador TAP virtual

En la parte inferior derecha se puede observar un icono nuevo con el logo de openVPN que indica la conexión activa.

Ilustración 47: icono de conexión OpenVPN

Con esto se concluye la instalación y respectiva configuración de OpenVPN, tanto en el servidor como en el equipo del usuario.

5.2 Instalación y configuración de VoIP

Para la configuración de la central telefónica VoIP se decidió utilizar Issabel ya que permite realizar este proceso manera sencilla, para esto es necesario descargar la imagen ISO del sistema para posteriormente instalarlo ya sea en un equipo físico como puede ser un servidor o un equipo de escritorio, o también se lo puede hacer en una máquina virtual, para este trabajo se decidió utilizar una máquina virtual, ya que de esta forma se puede ahorrar recursos y realizar las pruebas de una mejor manera, a continuación se detalla el proceso de instalación de Issabel en la máquina virtual y la respectiva configuración para el funcionamiento de las llamadas.

Primero se procede a descargar la imagen ISO desde la página web oficial de issabel.

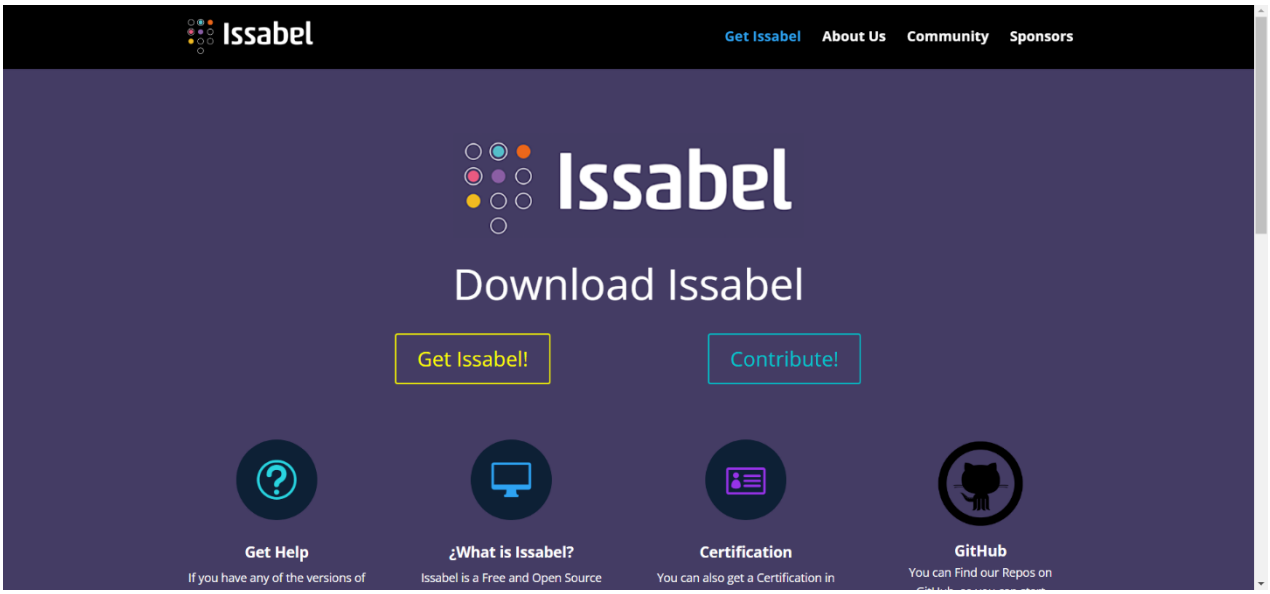

Ilustración 48: Pagina Web Oficial Issabel

Una vez descargada la imagen ISO se puede iniciar con la instalación del sistema como se muestra a continuación:

Ilustración 49: Pantalla instalación Issabel 1

Ilustración 50: Pantalla de selección de idioma

Una vez seleccionado el idioma se debe realizar la selección del idioma del teclado, así como seleccionar la versión de issabel que se va a instalar y el disco donde se va a instalar el sistema.

Ilustración 51: pantalla de instalación de Issabel 2

Ilustración 52: Selección de idioma del teclado

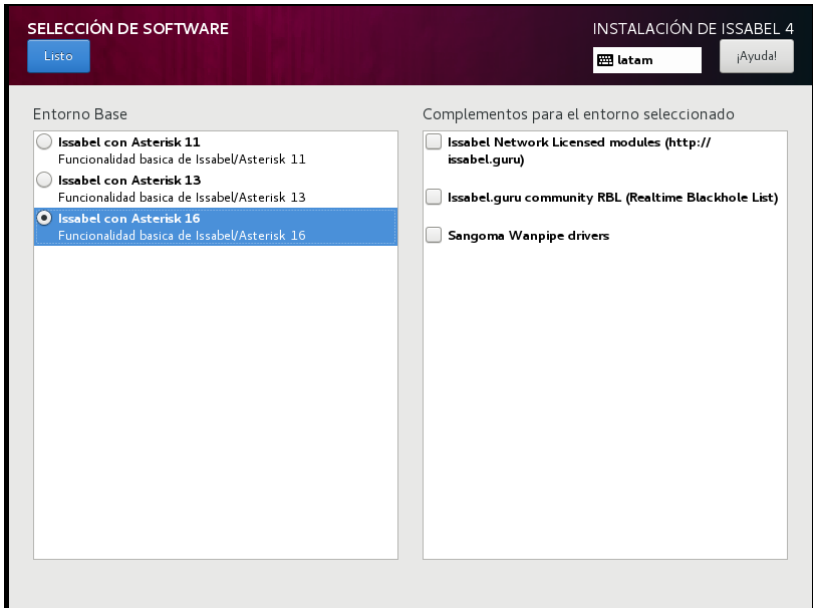

Ilustración 53: Selección de versión de Issabel a Instalar

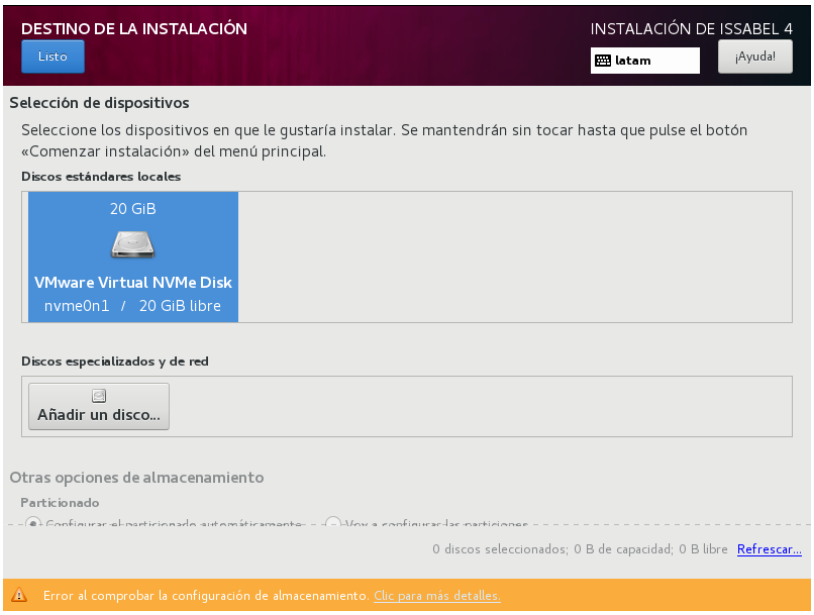

Ilustración 54: Selección de disco destino instalación

A continuación, se debe configurar una contraseña para el usuario ROOT y esperar que termine el proceso de instalación.

Ilustración 55: Pantalla de configuración usuario Root

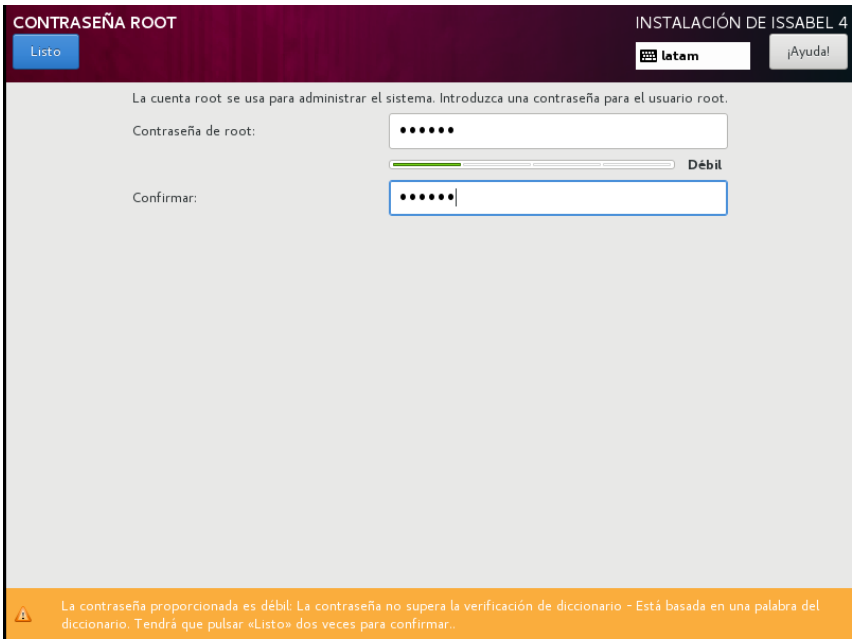

Ilustración 56: Pantalla de configuración contraseña root

Cuando termine el proceso de instalación se debe configurar una contraseña para la base de datos del sistema y para el usuario administrador.

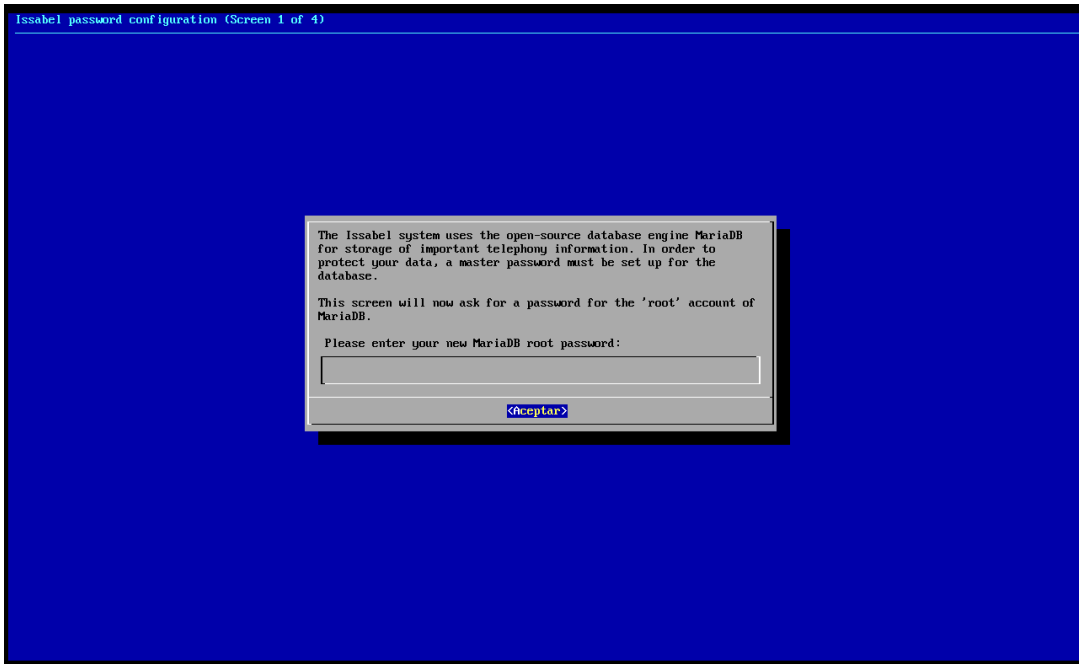

Ilustración 57: Configuración contraseña base de datos

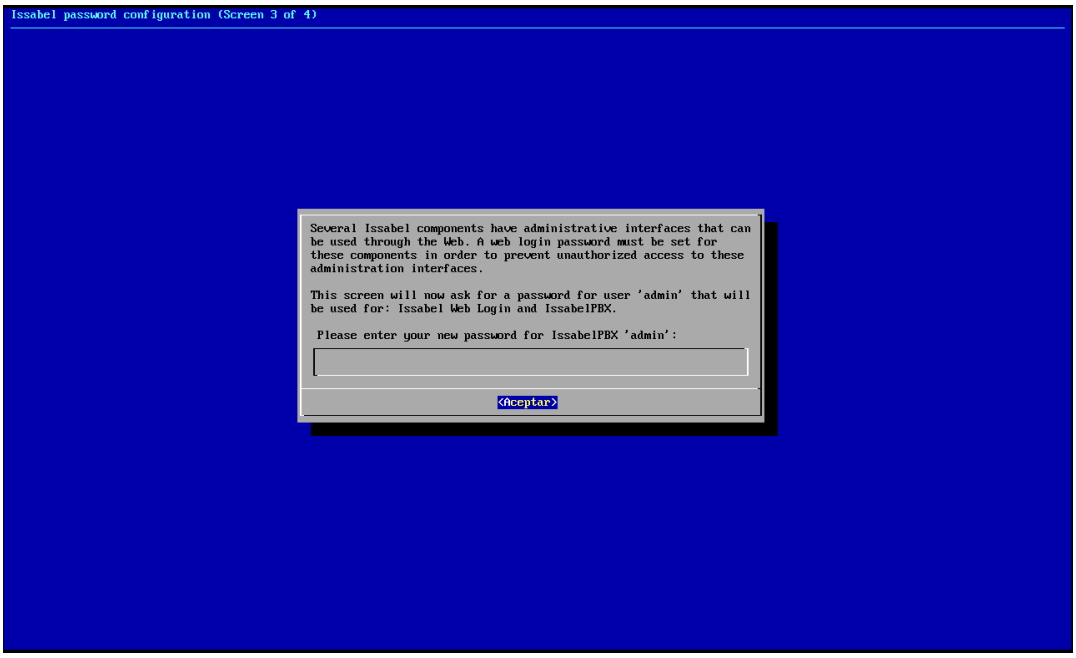

Ilustración 58: Configuración contraseña administrador

Una vez configuradas las contraseñas se podrá ingresar como usuario root desde el servidor o mediante la interfaz gráfica de Issabel ingresando con el navegador a la IP asignada al mismo.

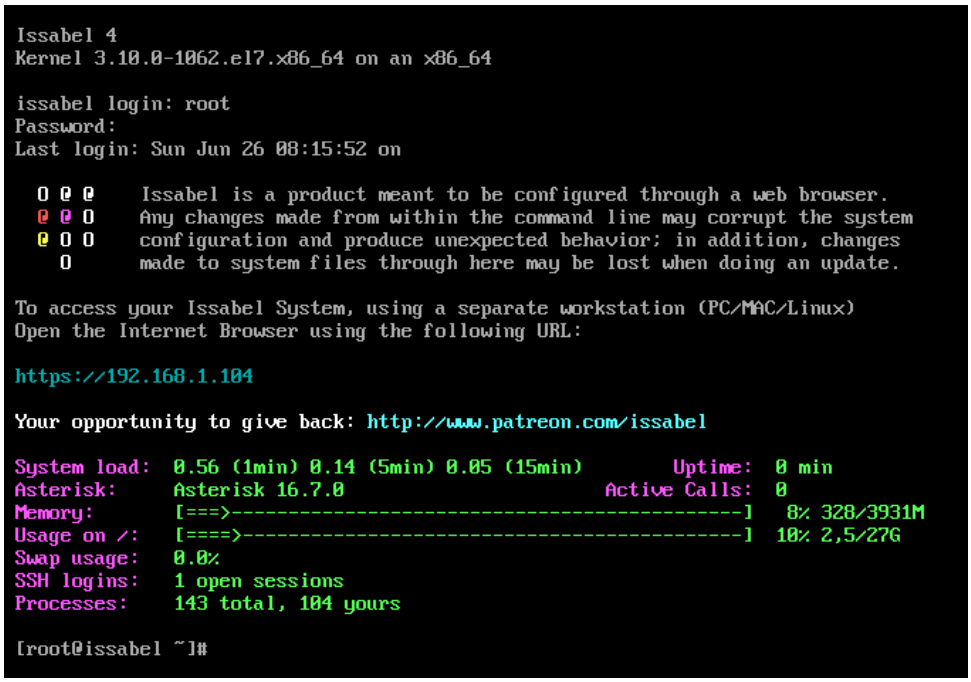

Ilustración 59: Pantalla servidor Issabel

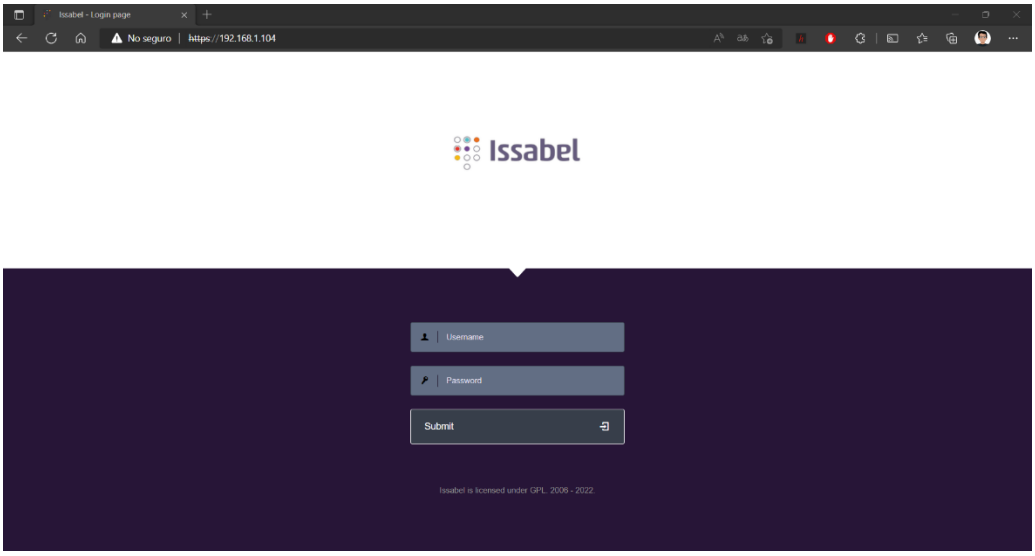

Ilustración 60: Interfaz gráfica web Issabel

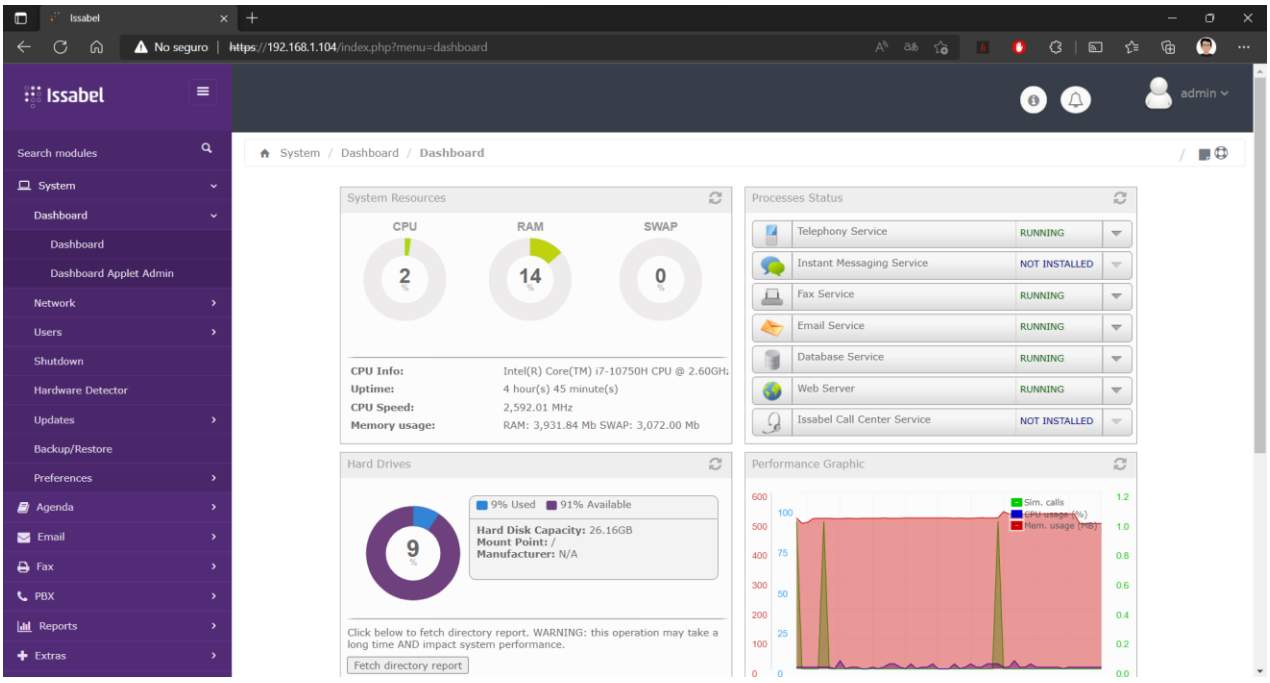

Ilustración 61: menú principal Issabel

Ahora se procederá a configurar las extensiones SIP para cada uno de los usuarios y realizar la configuración del software en el equipo del usuario para que pueda realizar llamadas.

Para configurar las extensiones se accede al menú PBX ‣ configuración PBX ‣ Extensiones, y crear cada número de extensión con su respectiva contraseña.

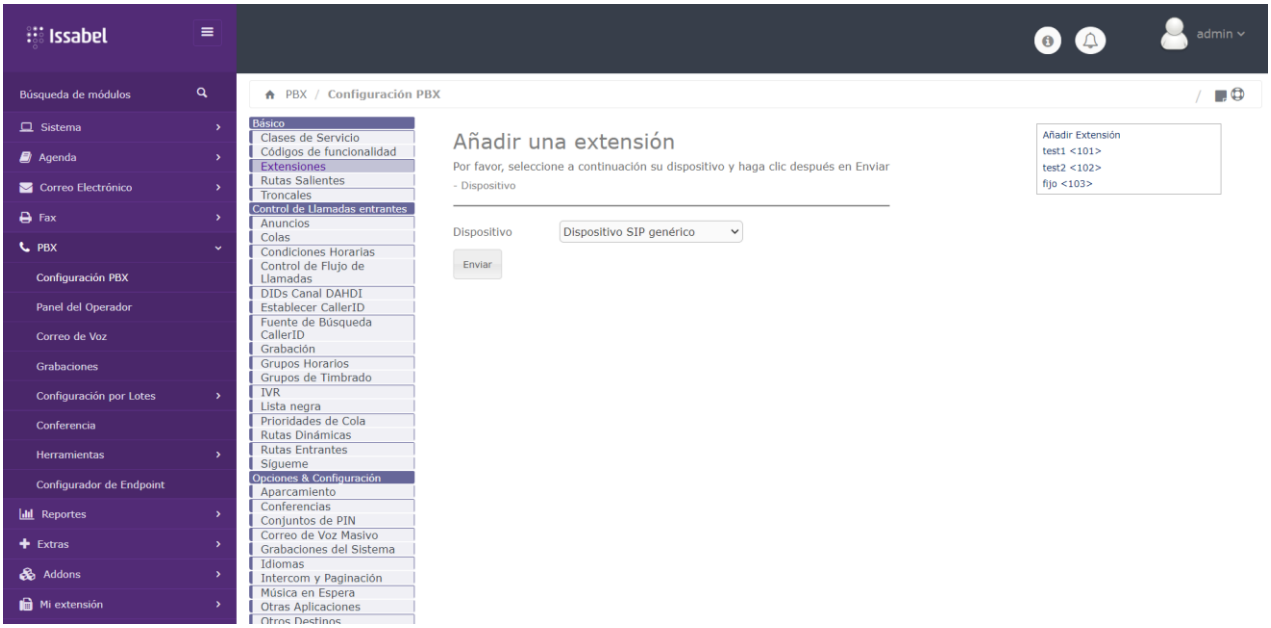

Ilustración 62: menú de configuración de Extensiones

5.2.1 Instalación y configuración de softphone en equipo usuarios

El software elegido para ser utilizado como softphone es Linphone, ya que es gratuito, permite la configuración de las extensiones SIP de manera sencilla y además funciona en distintas plataformas.

Para realizar la instalación del software se debe descargar de su web oficial en el caso de sistemas de escritorio, o desde la tienda de aplicaciones del smartphone donde se vaya a configurar, a continuación, se detalla la configuración dentro del sistema Windows, la configuración en un smartphone es prácticamente la misma.

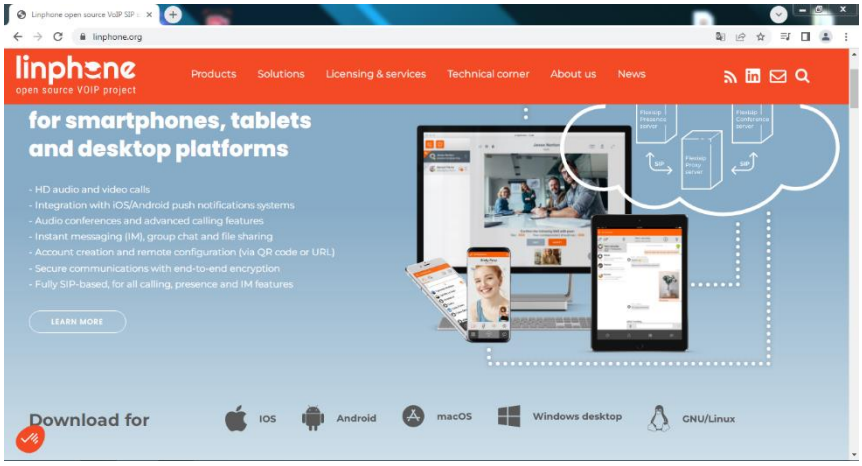

Ilustración 63:Pagina web oficial de Linphone

Una vez descargado el archivo se lo ejecuta y se sigue los pasos de instalación que se indique.

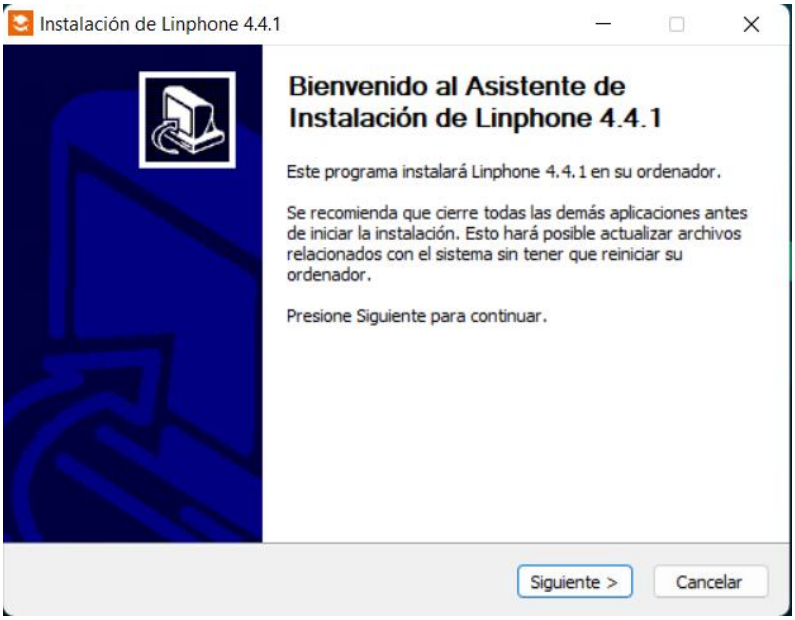

Ilustración 64: Instalación Linphone 1

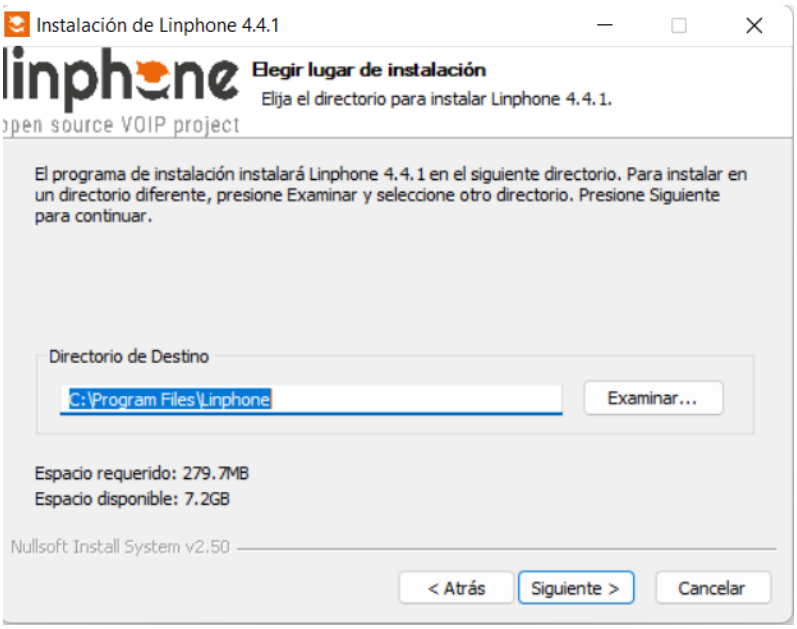

Ilustración 65: Instalación Linphone 2

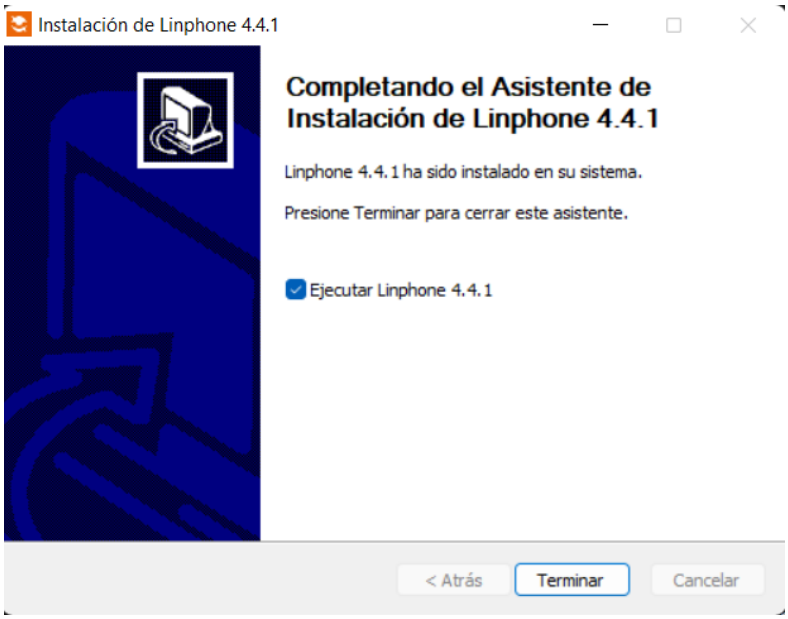

Ilustración 66: Instalación completa Linphone

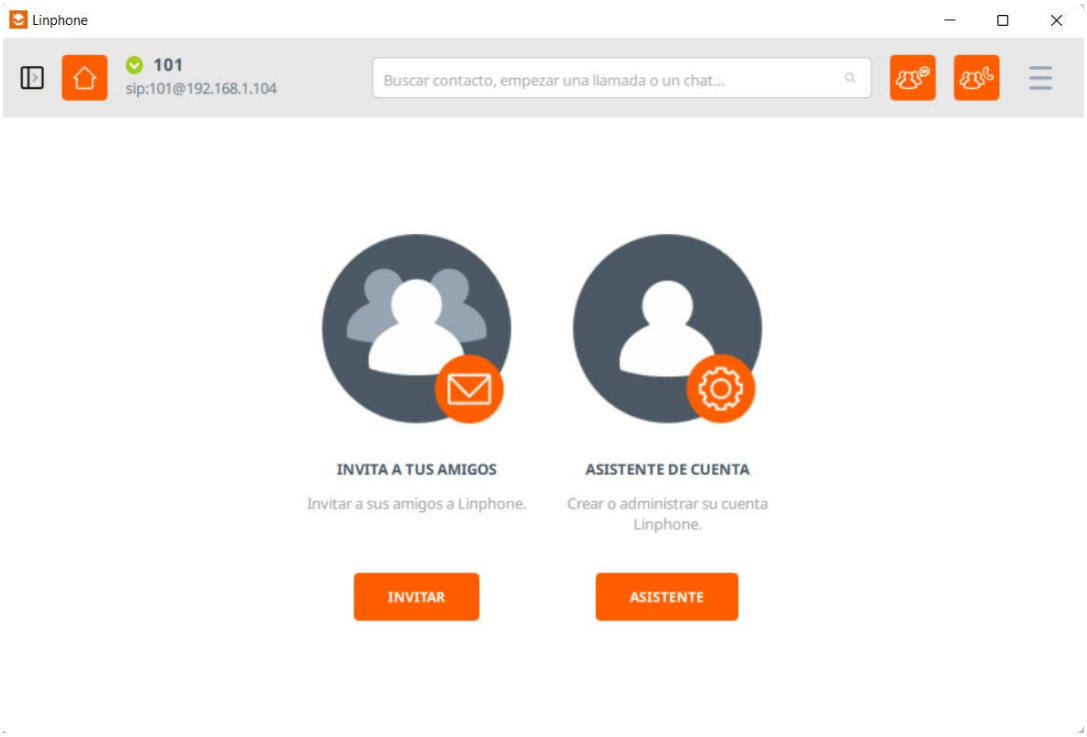

Ilustración 67: Ventana principal Linphone

Para realizar la configuración de la extensión se debe iniciar el asistente de configuración, seleccionar cuenta SIP e ingresar la extensión, contraseña e IP del servidor Issabel.

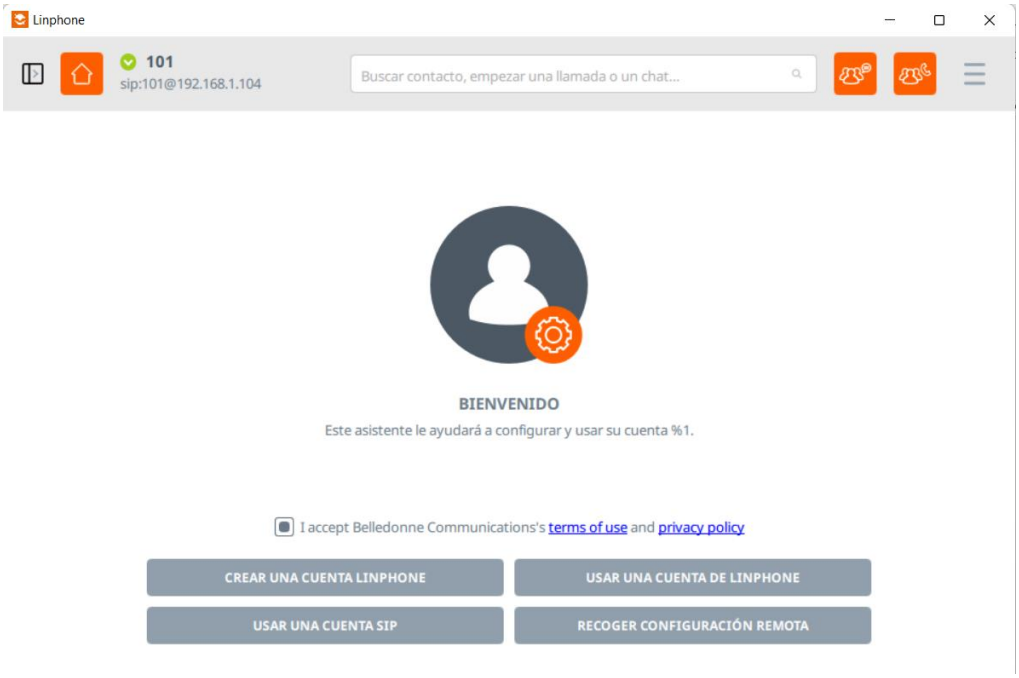

Ilustración 68:Configuración SIP Linphone

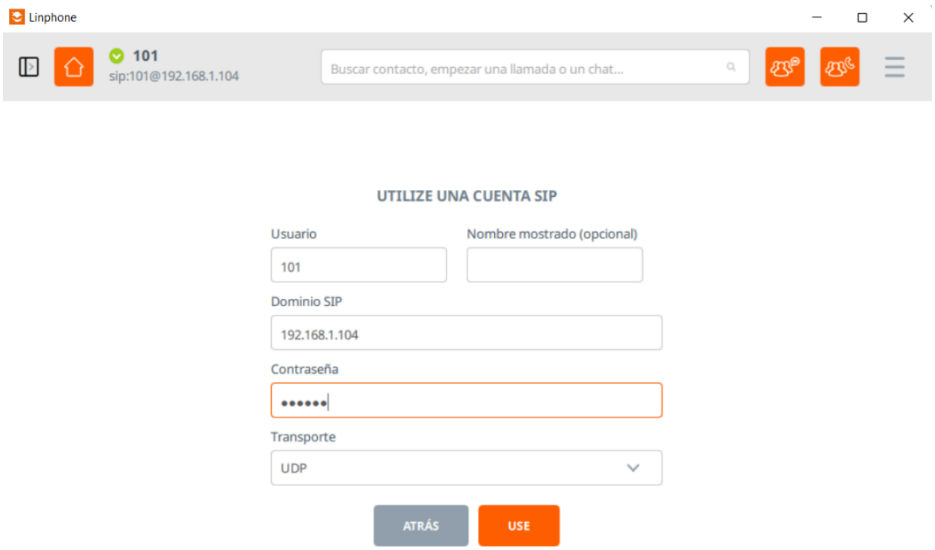

Ilustración 69: SIP Linphone

Una vez configurado Linphone, se podrá realizar llamadas entre las extensiones creadas, es decir cada usuario podrá comunicarse con el resto de los usuarios solamente marcando la correspondiente extensión.

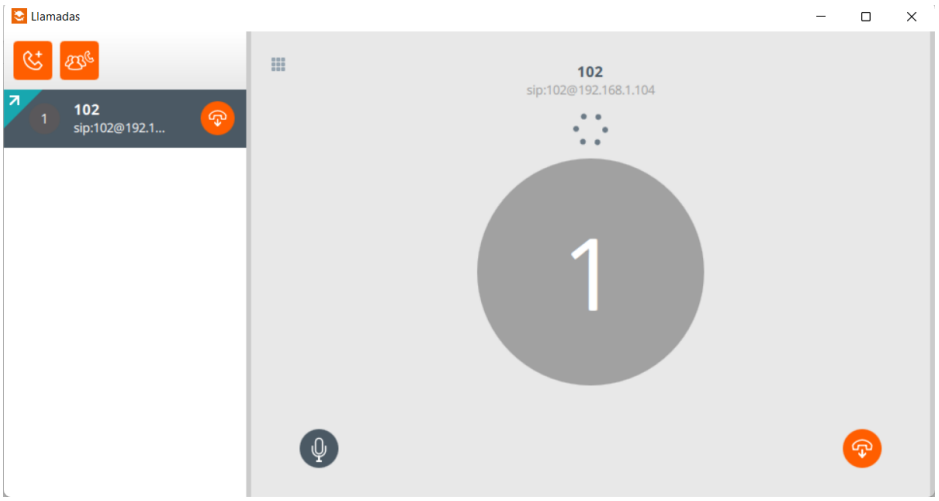

Ilustración 70: llamada realizada con Linphone

CAPÍTULO 6

6.1 EVALUACIÓN DE LA RED IMPLEMENTADA

6.1.1 Pruebas de funcionamiento

Verificación de conectividad

Cuando se encuentre instalado el Cliente OpenVPN en el equipo del usuario se habrá creado una nueva conexión de red con un controlador TAP, el cual si no existe una conexión VPN activa debe mostrarse desconectado como se muestra a continuación:

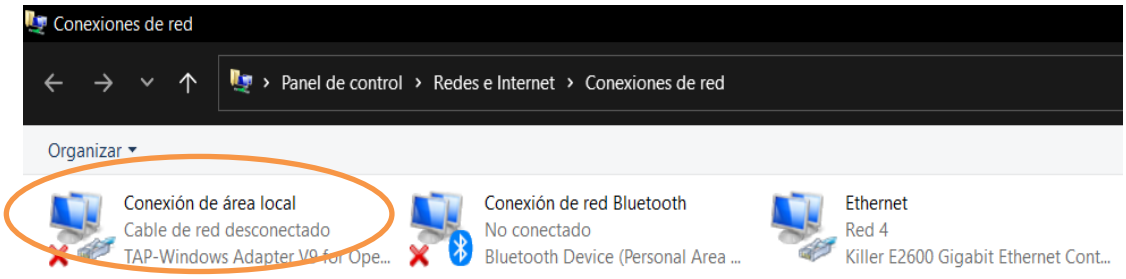

Ilustración 71: conexión de red TAP

Para activar la conexión VPN se debe ejecutar el aplicativo OpneVPN y activar la conexión.

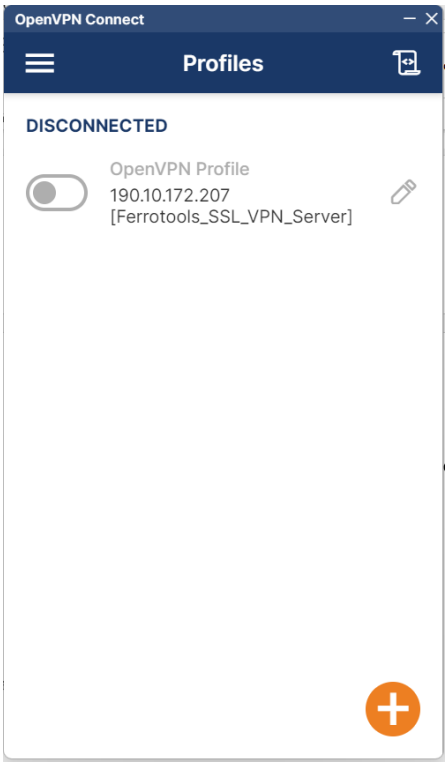

Ilustración 72: Conexión OpenVPN

Se podrá abrir un registro que muestra el proceso de conexión como se muestra a continuación:

Ilustración 73: Log de conexión VPN

A continuación de detalla los datos que muestra el log de conexión:

En la ilustración 74 se puede observar la versión de OpenVPN, y de sistema operativo cliente.

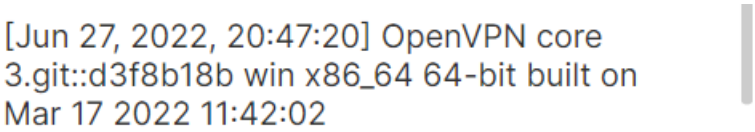

Ilustración 74: Log de openvpn

A través de la ilustración 75 se visualiza la dirección IP del servidor, el puerto que utiliza (1194) y el protocolo de conexión (UDP o TCP).

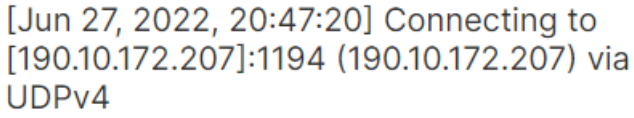

Ilustración 75: Log de conexión OpenVPN

La configuración del túnel de conexión.

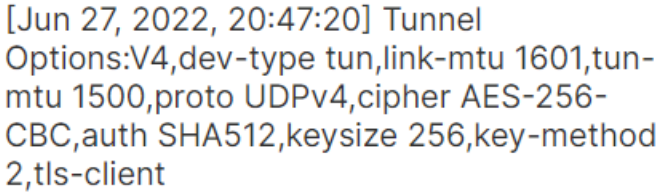

Ilustración 76: Túnel de conexión VPN

Conexión SSL.

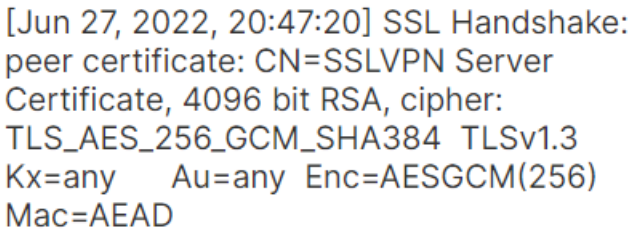

Ilustración 77: Conexion SSL

Asignación de dirección IP dentro de la VPN.

```
[Jun 27, 2022, 20:47:20] CAPTURED
OPTIONS:
Session Name: 190.10.172.207
Layer: OSI_LAYER_3
Remote Address: 190.10.172.207
Tunnel Addresses:
  10.10.0.10/30 → 10.10.0.9 [net30]
Reroute Gateway: IPv4=0 IPv6=0 flags=[
IPv4 ]
Block IPv6: no
Add Routes:
  192.168.1.0/24
  10.10.0.1/32
Exclude Routes:
DNS Servers:
Search Domains:
```

Ilustración 78: Asignación de IP

Una vez establecida de manera correcta la conexión de OpenVPN, se muestra la siguiente ventana con información de la conexión.

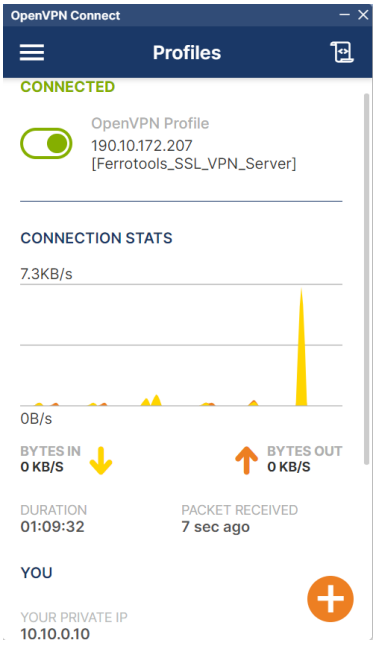

Ilustración 79: conexión exitosa VPN

De esta manera el equipo del usuario estará conectado a la red de la empresa lo que le permitirá utilizar los servicios de esta.

6.1.2 Pruebas de conexión

Se realiza una prueba de ping desde el equipo remoto hacia un equipo que se encuentre en la red local de la empresa, para esto primero se realiza una prueba sin tener la conexión VPN activa.

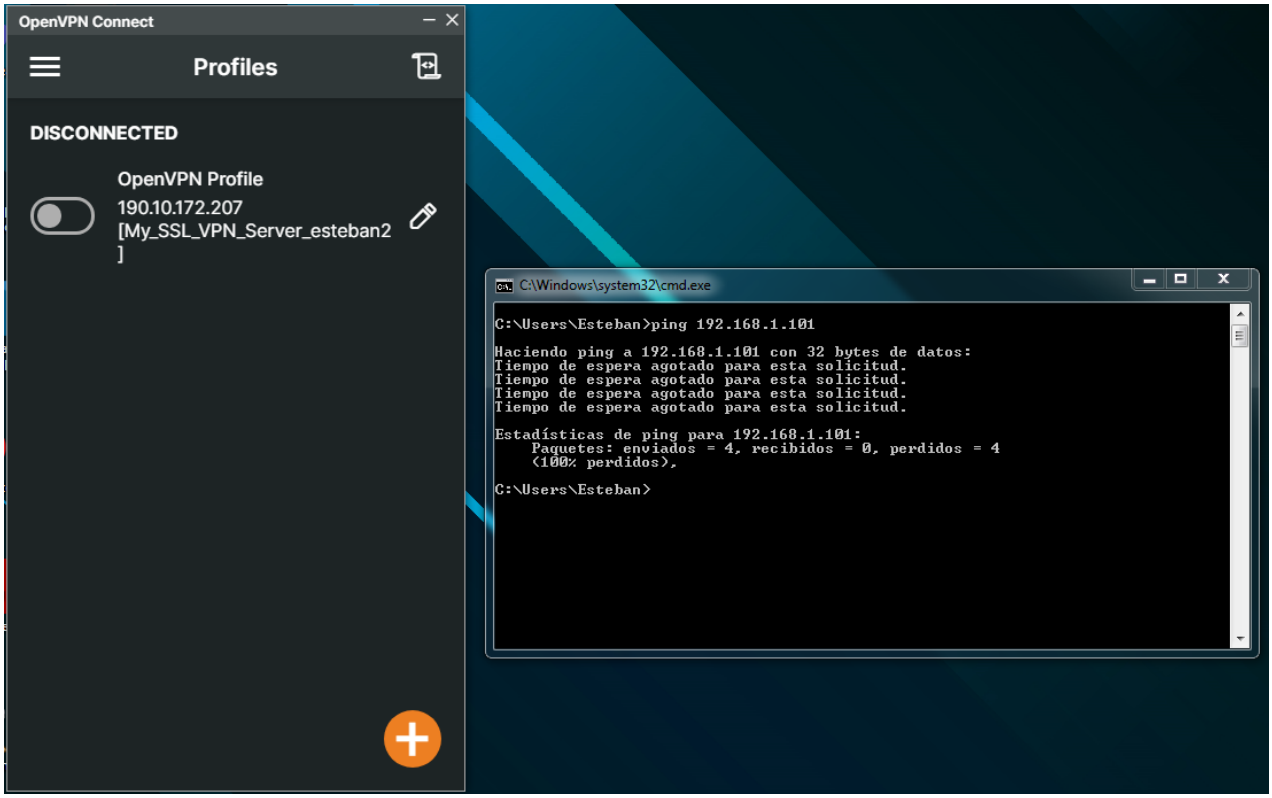

Ilustración 80: Prueba ping sin vpn

Como se puede ver en la ilustración 80, no se tiene respuesta del equipo al que se hace ping, el cual se encuentra dentro de la red de la empresa.

Ahora se realiza la misma prueba, pero con la VPN conectada para comprobar que exista conexión a la red de la empresa.

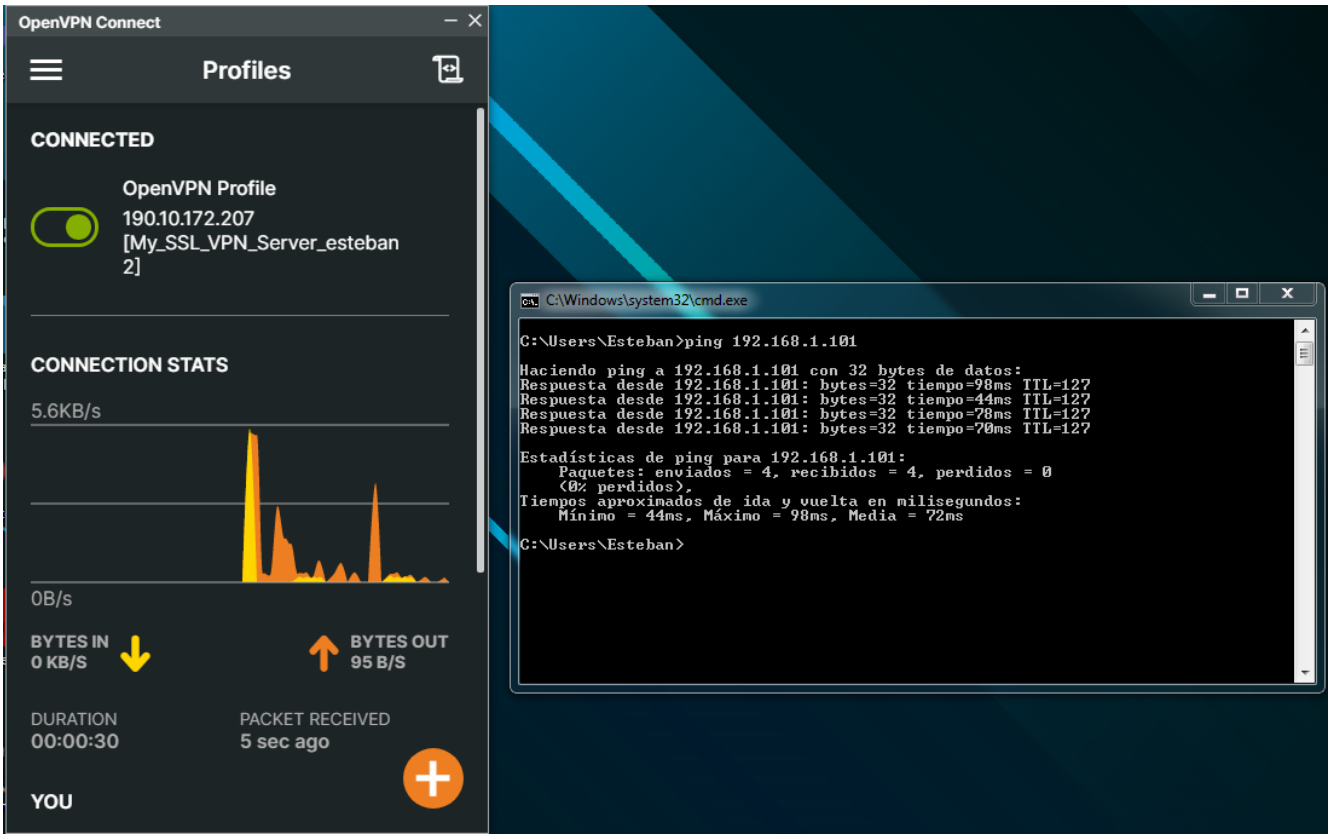

Ilustración 81: Prueba ping con VPN

Como se observa en la ilustración 81, se recibe respuesta del equipo al que se está realizando ping con la VPN conectada, por lo tanto, existe una conexión exitosa del equipo remoto.

Para revisar cual es la ruta que siguen los paquetes al hacer ping al equipo que se encuentra dentro de la red de la empresa se realiza un tracert.

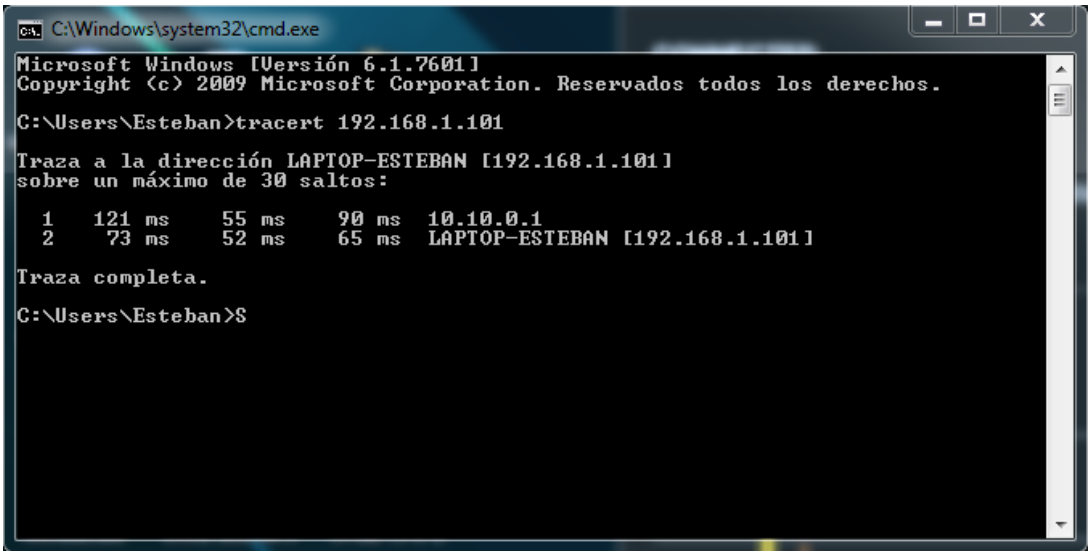

Ilustración 82: Tracert hacia el equipo local

Como se observa en la ilustración 82 al ejecutar el comando tracert para ver la ruta que siguen los paquetes desde el equipo remoto hasta que llegan al equipo que se encuentra dentro de la red local de la empresa, los paquetes pasan por el Gateway de la VPN para llegar al equipo en la red local.

6.1.3 Pruebas de acceso a red local y uso de servicios

Se evidencia que mediante la conexión VPN se pueda conectar remotamente al equipo local mediante el uso de VNC.

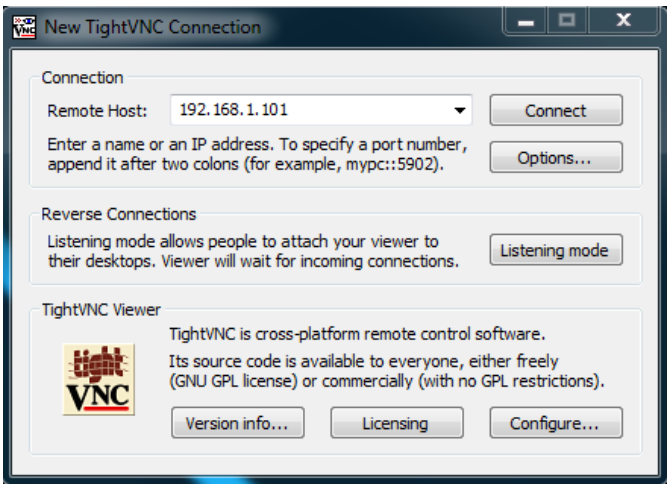

Ilustración 83: Conexión remota VNC

En la ilustración 84 se comprueba que a la conexión VPN permite la conexión remota a través de VNC a los equipos que se encuentra en la red local de la empresa.

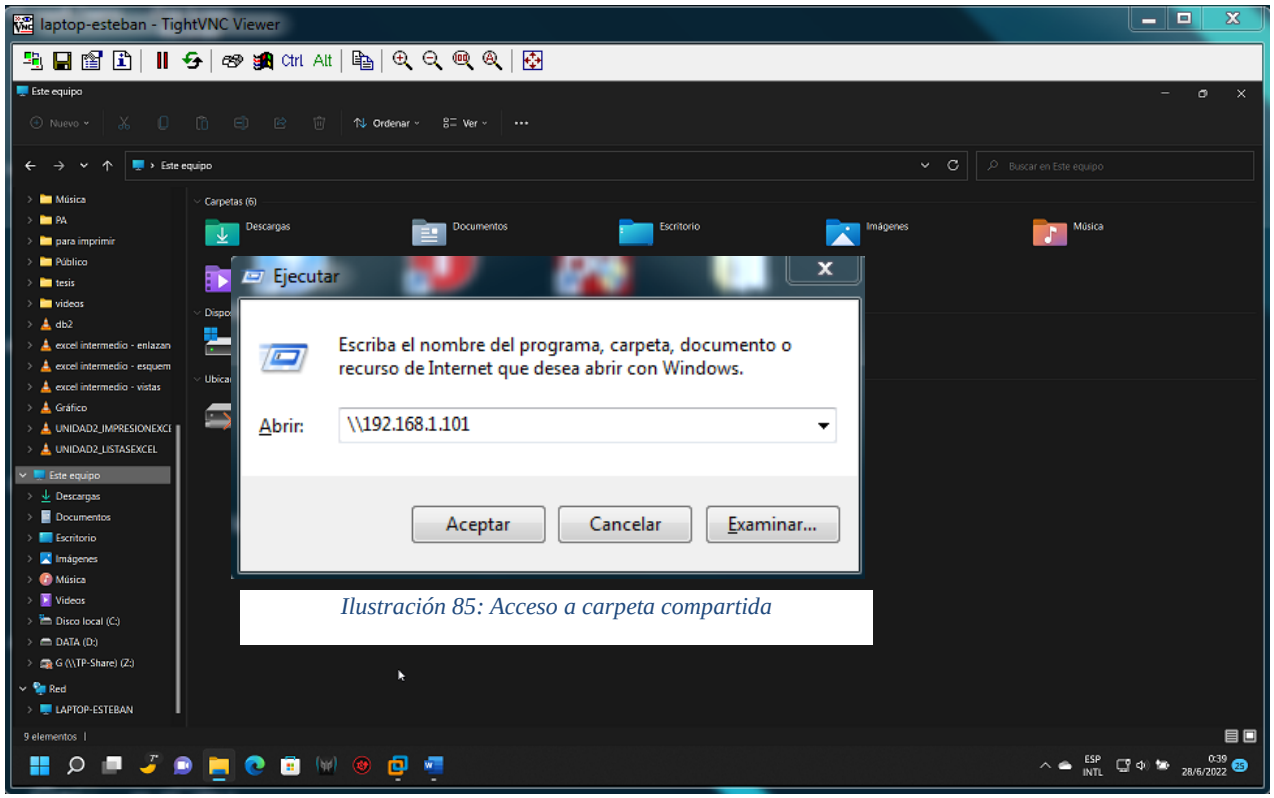

Ilustración 85: Acceso a carpeta compartida

Ilustración 84: Conexión VNC

Se demuestra que se puede acceder a las carpetas compartidas que se encuentran en el equipo 192.168.1.101 ubicado en la red local de la empresa, para lo cual es necesario abrir la ventana de ejecución de comandos y escribir la IP del equipo al que se desea ingresar como se muestra en la ilustración 85.

Como se puede ver en la ilustración 86 se tiene acceso sin problemas a las carpetas compartidas a través de la conexión VPN.

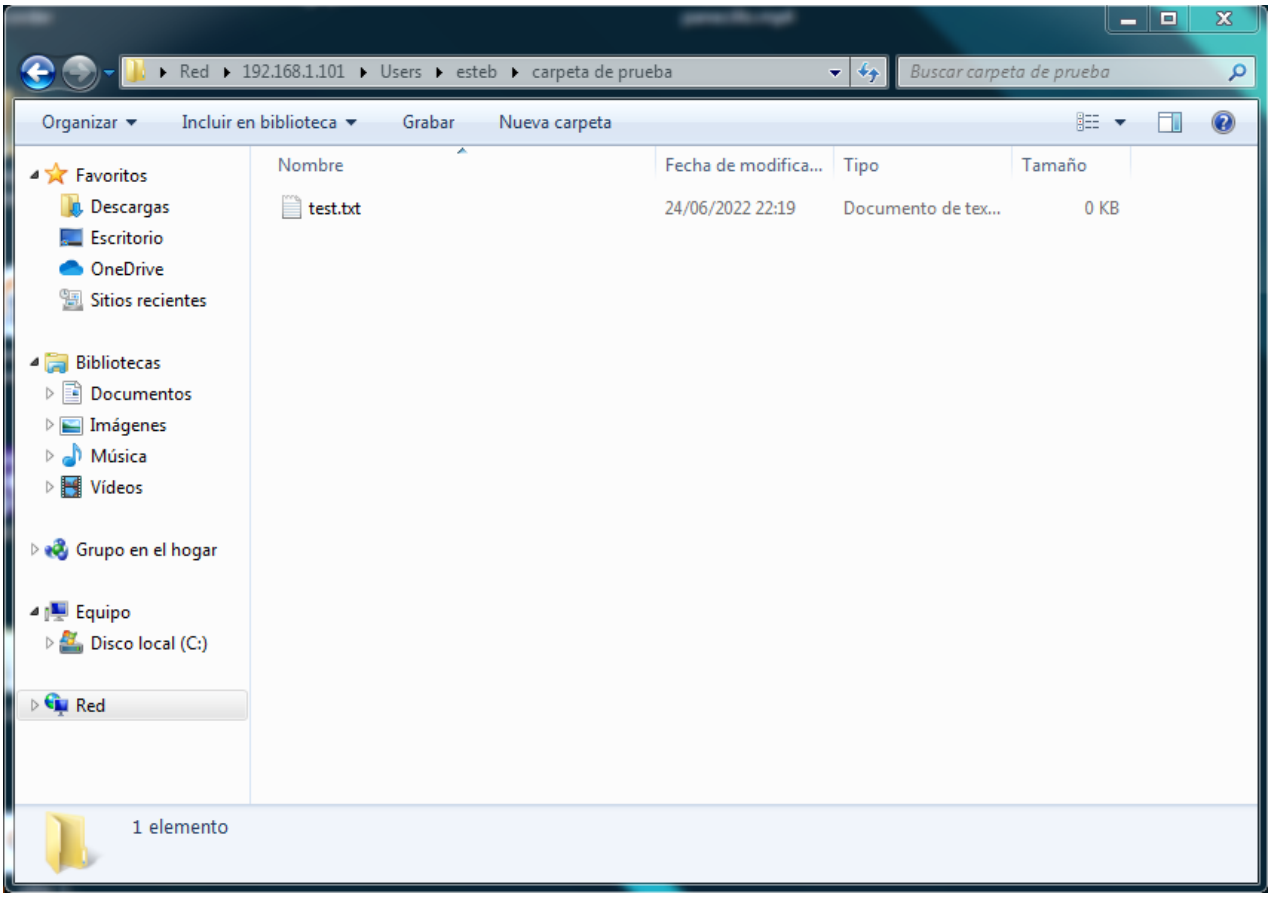

Ilustración 86: Conexión correcta a carpetas compartidas

6.1.4 Pruebas de conexión VoIP a través de VPN

Se comprueba que se pueda conectar al servidor VoIP Issabel de manera remota haciendo uso de OpenVPN y que se pueda realizar llamadas.

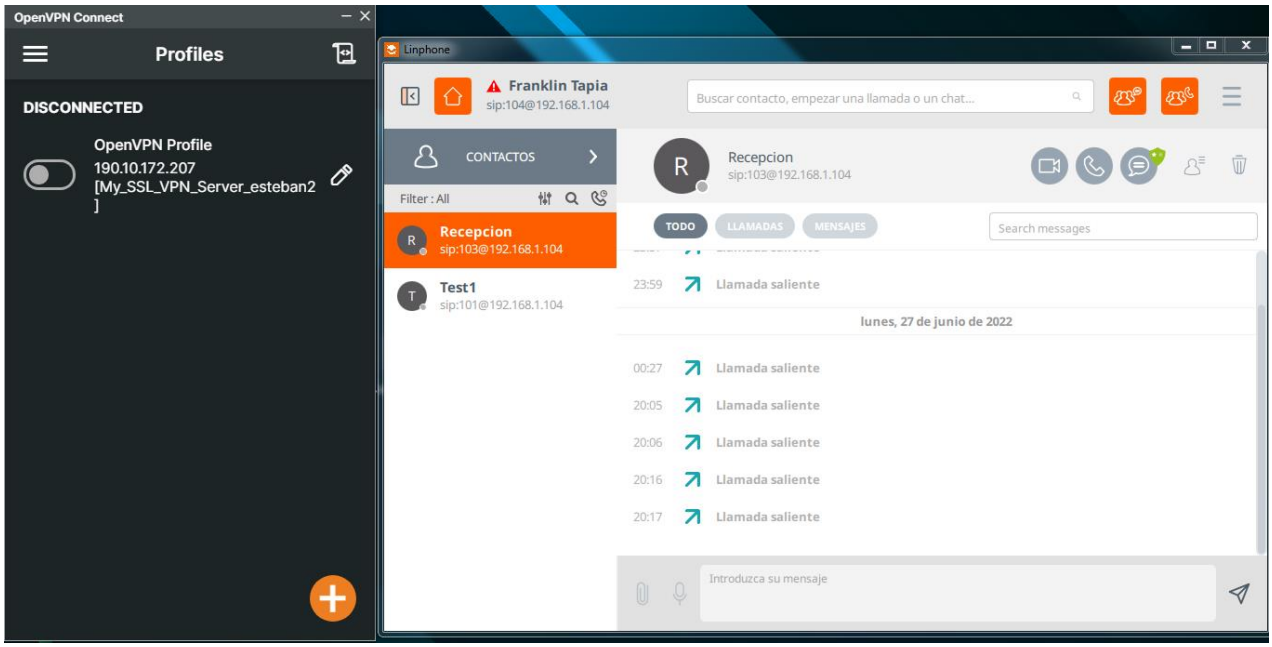

Ilustración 87: Prueba conexion VoIP

Como se observa en la Ilustración 87, cuando la VPN esta desconectada el Software VoIP es incapaz de conectarse al servidor Issabel de VoIP.

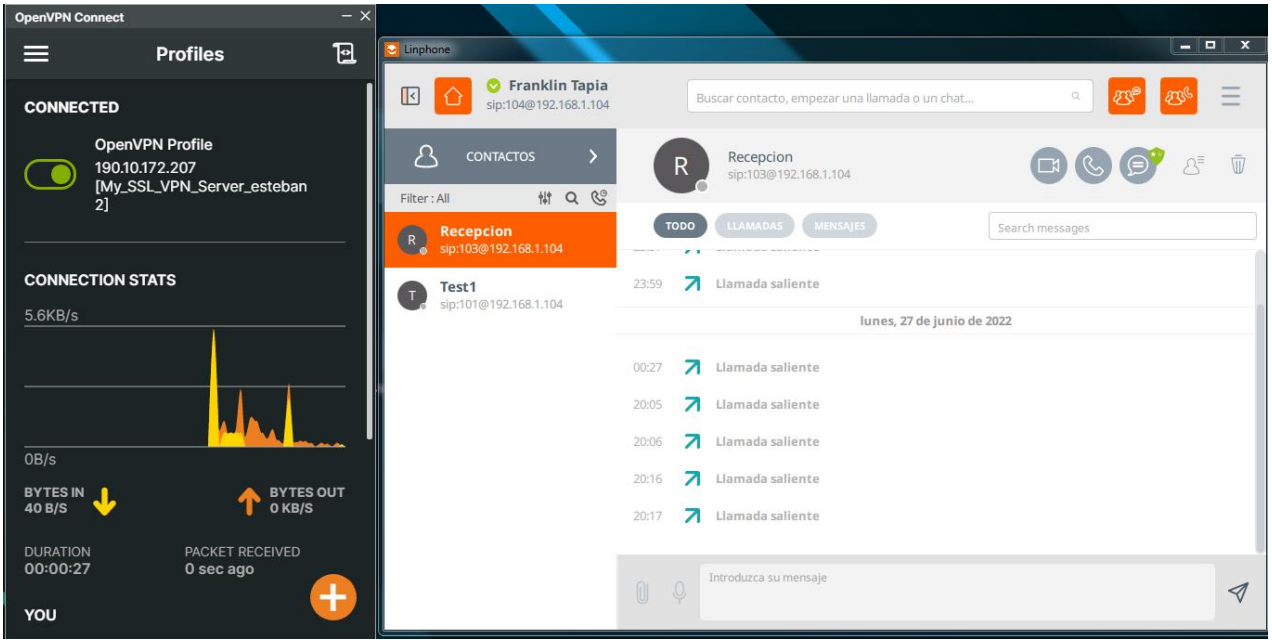

Ilustración 88: Conexión correcta VoIP

En la ilustración 88 se observa que una vez la VPN es conectada la conexión con el servidor

VoIP es exitosa, a continuación, se realiza una llamada de prueba para verificar que se pueda realizar llamadas.

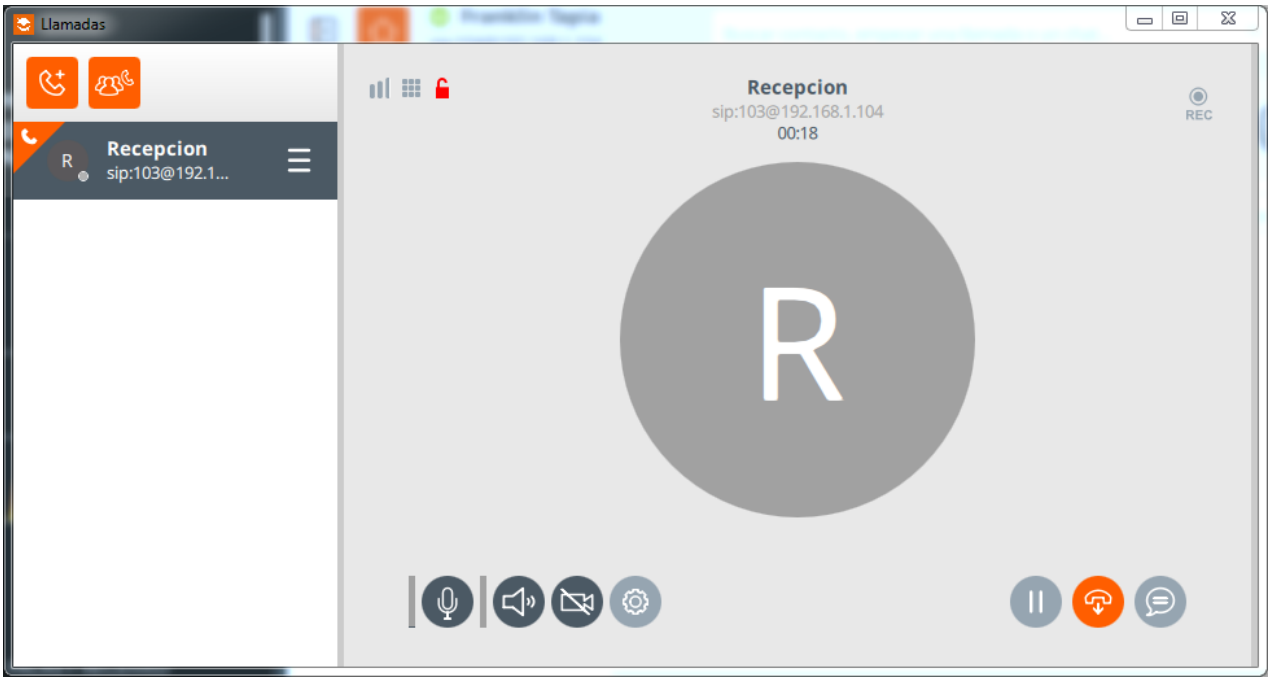

Ilustración 89: Llamada de prueba

En la ilustración 89 se puede ver que la llamada se realiza con éxito y existe comunicación correcta con el receptor de la llamada.

6.2 Evaluación del funcionamiento de la vpn

6.2.1 Análisis de tráfico de la red VPN

Para poder realizar el análisis de tráfico, se debe tener establecida la conexión con el servidor OpenVPN.

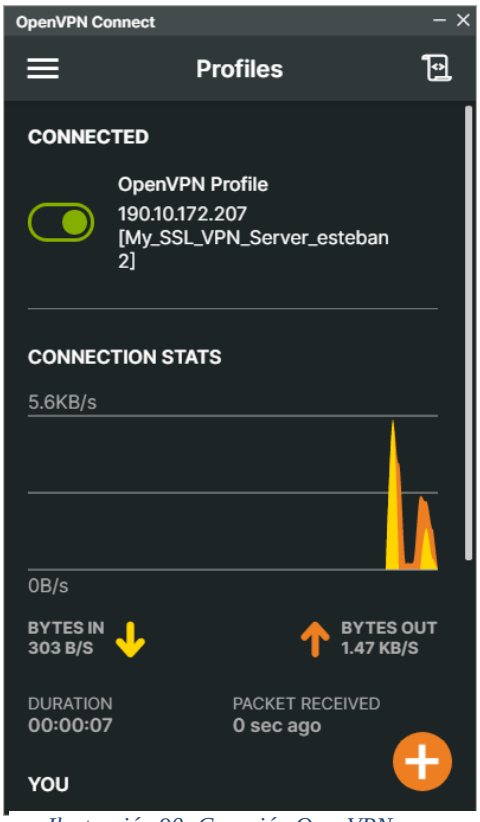

Ilustración 90: Conexión OpenVPN para Pruebas

Mediante ilustración 91 se puede ver la prueba de ping realizada hacia uno de los equipos de la red local, el resultado de la prueba muestra que se envió un total de 901 paquetes, de los cuales se recibieron 899 y se perdieron 2, esto indica que la conexión en general estable con pérdida de unos pocos paquetes, pero esto no afecta en su funcionamiento.

```
Respuesta desde 192.168.1.101: bytes=32 tiempo=67ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=287ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=86ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=93ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=123ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=98ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=105ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=95ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=78ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=214ms TTL=127
Respuesta desde 192.168.1.101: bytes=32 tiempo=100ms TTL=127

Estadísticas de ping para 192.168.1.101:
    Paquetes: enviados = 901, recibidos = 899, perdidos = 2
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 58ms, Máximo = 985ms, Media = 103ms
Control-C
^C
```

Ilustración 91: Prueba de paquetes

6.2.2 Prueba de encriptación

Para completar el proceso de conexión del cliente al servidor OpenVPN, este realiza varios pasos, entre ellos están la autenticación, proceso en el cual se establece los parámetros del cifrado a utilizar, en la ilustración 92 se observa que el cifrado que será utilizado es AES-256 con 256 bits, el cual garantiza un alto grado de cifrado.

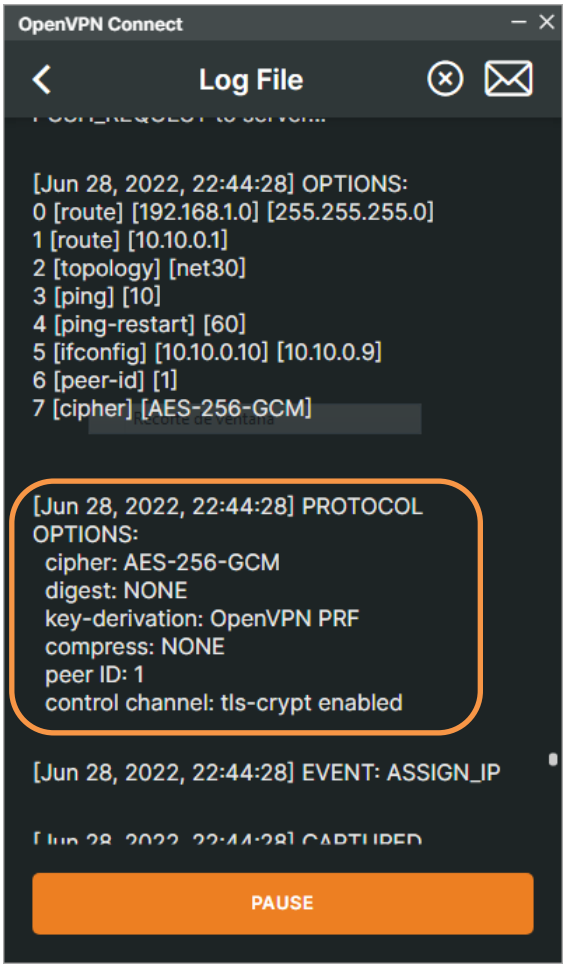

Ilustración 92: Detalle protocolo de encriptación

Se utilizará la herramienta WireShark Network Analizer para validar que se realice la encriptación al momento de establecer la conexión VPN.

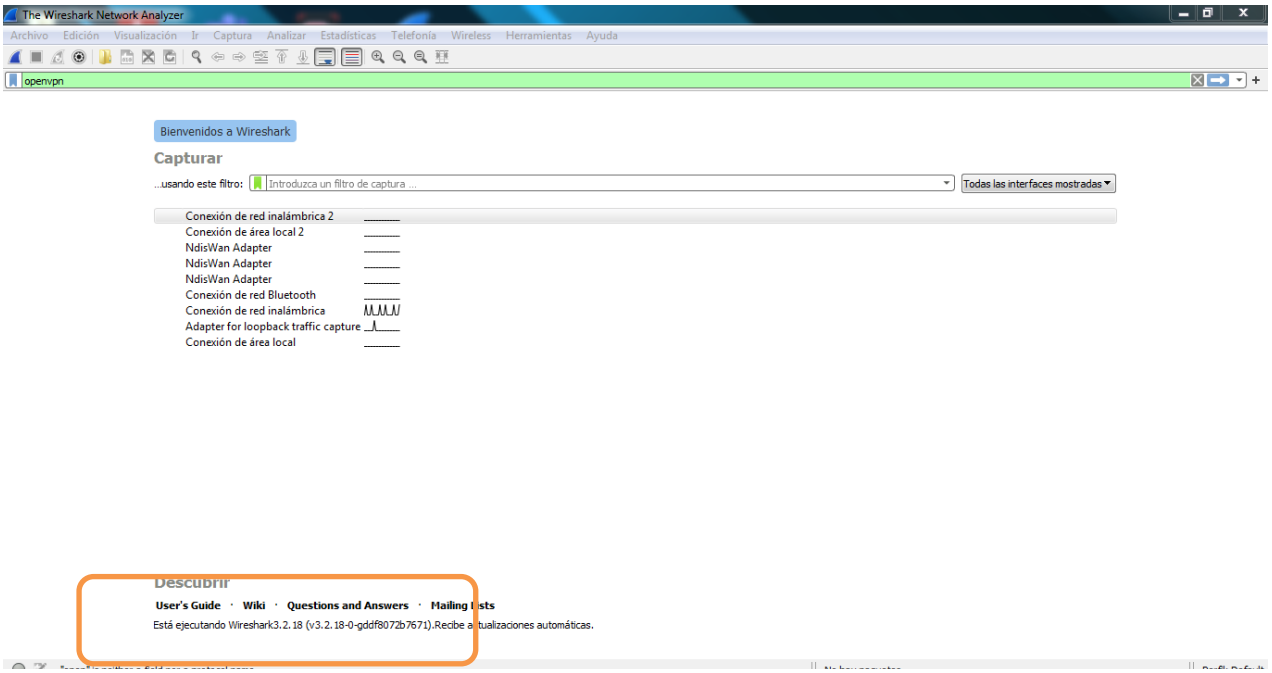

Ilustración 93: Selección de red a analizar

Como se muestra en la ilustración 93, para realizar la validación se aplica filtro de búsqueda digitando OpenVPN, esto nos mostrara únicamente los paquetes del protocolo OpenVPN, a continuación, se selecciona un paquete de la lista para visualizar la información que este contiene, en la sección de datos se puede observar que la información esta encriptada.

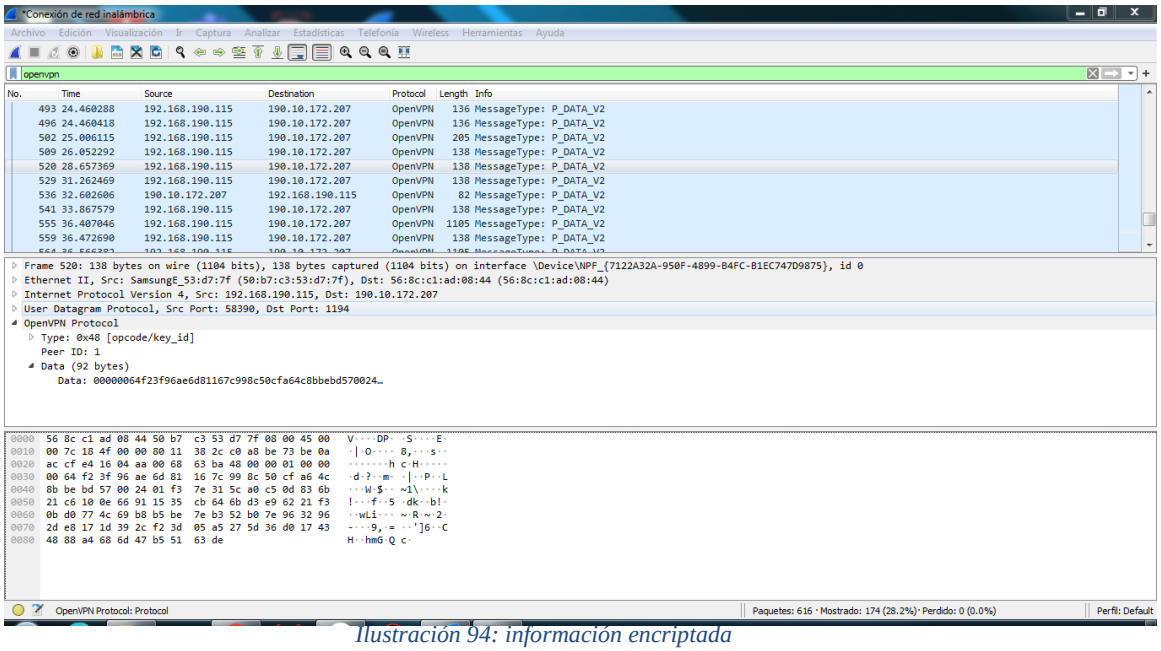

Ilustración 94: información encriptada

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Luego de que se establecieron los requisitos y recursos que dispone la empresa, se utilizara la conexión a internet por fibra óptica de 100Mbps como medio para la conexión VPN, adicionalmente, la infraestructura de red local con la que se cuenta actualmente es adecuada para la implementación de la red privada virtual, y será necesario la actualización de los componentes del equipo que será utilizado como servidor VPN.

Luego de haber revisado los conceptos teóricos necesarios y analizado las diferentes tecnologías y herramientas que existen para realizar la implementación de la VPN, se concluyó que se debe utilizar un sistema operativo orientado al uso como firewall y basado en Linux OPNSense, y utilizar OpenVPN como herramienta para la creación de la red VPN.

Concluida la instalación y configuración de OPNSense en el equipo servidor se concluye que la implementación de la red privada virtual es exitosa y se capacitara al personal encargado del manejo del sistema para su uso correcto.
Las pruebas realizadas para evaluar el correcto funcionamiento de la VPN, prueba de perdida de paquetes, prueba de acceso remoto, prueba de encriptación y prueba de conexión VoIP, arrojan resultados positivos, por lo que la red tiene un apropiado funcionamiento y una adecuada seguridad.

La implementación de la VPN permite a los empleados de la empresa que requieran acceso remoto puedan realizar su trabajo de manera sencilla, y siendo necesario únicamente que cuenten con un computador o smartphone y conexión a internet, para acceder a los servicios como carpetas compartidas y llamadas VoIP, para lo cual se capacitara al personal para el uso correcto de las herramientas.

La implementación de la VPN y VoIP se a realizado con un costo mínimo, ya que se hizo uso de hardware con el que a empresa ya contaba, solo fue necesario mejorarlo, y al uso de herramientas y software libre, el cual no requiere de la adquisición de licencias.

Recomendaciones

Adquirir un equipo con características similares al utilizado como servidor VPN para su uso como servidor VoIP cuando la empresa decida realizar el cambio del antiguo PBX con el que cuenta actualmente.

Realizar la creación de un usuario en el servidor VPN para cada equipo que utilice el empleado como puede ser para un equipo laptop y para su smartphone, lo que facilita la eliminación del usuario si el empleado decide retirarse de la empresa.

Hacer uso de auriculares para el uso de las llamadas VoIP desde el ordenador o hacer uso de su smartphone para el uso de la VoIP a través de la aplicación Linphone y la conexión VPN desde el dispositivo móvil.

Realizar la desactivación del firewall de Windows en el equipo del empleado en caso de que existan problemas con la conexión VPN para garantizar el correcto funcionamiento.

BIBLIOGRAFÍA

3cx.es. (2021). *¿Qué alternativas existen para PBX IP basadas en SIP?* Obtenido de https://www.3cx.es/voip-sip/ejemplos-centralitas-ippbx/

3cx.es. (2021). *¿Qúe son los Teléfono SIP/teléfonos VoIP?* Obtenido de https://www.3cx.es/voip-sip/telefono-voip/

Adeva, R. (2021). *Todo sobre Linux, El sistema operativo de codigo abierto*. Obtenido de ADSLZone: https://www.adslzone.net/reportajes/software/que-es-linux/)

Barrera. (2020). Implementacion de un sistema de alta disponibilidad de un enlace vpn para una entidad financiera.

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-

Carrillo. (2016). Propuesta de implementacion de un entorno de vpn empresarial en la electro oriente s.a.

Castellano, J. (2017). *Características protocolos VPN (OpenVPN, SSTP, L2TP, IKEv2 y PPTP)*. Obtenido de Solvetic.com: https://www.solvetic.com/page/recopilaciones/s/seguridad/caracteristicas-protocolos-vpn-openvpn-sstp-l2tp-ikev2-pptp#:~:text=OpenVPN%20permite%20a%20los%20usuarios,hash%20SHA1%20de%20160%20bits.&text=Dentro%20de%20sus%20principales%20caracter%C3%ADsticas,

Castillo, J. A. (2020). *Que es OpenVPN y que caracteristicas nos da en las redes privadas virtuales*. Obtenido de https://www.profesionalreview.com/2020/04/05/openvpn-que-es/

dasoft. (2021). *Que es IssabelPBX*. Obtenido de https://www.dasoft.com.do/noticias/blog/que-es-issabelpbx/

desconocido. (2021). *¿Que es voz sobre ip(voip)?* Obtenido de https://www.3cx.es/voip-sip/voz-sobre-ip/

Díaz Llatance, M. A. (2015). *Diseño de una red privada virtual para interconectar las sucursales de la empres Terracargo*. Obtenido de http://repositorio.unprg.edu.pe/handle/UNPRG/462

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

Fernandez, L. (2022). *Los Mejores Firewalls open-source para proteger tu red*. Obtenido de https://www.redeszone.net/tutoriales/seguridad/mejores-firewall-open-source-proteger-red/

Group, I. (2020). *Que es un firewall y como funciona*. Obtenido de https://idgrup.com/firewall-que-es-y-como-funciona/#:~:text=Un%20firewall%2C%20tambi%C3%A9n%20llamado%20cortafueg

os,ordenadores%20de%20una%20misma%20red.

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

IBM. (2021). *IBM Docs*. Obtenido de https://www.ibm.com/docs/es/i/7.1?topic=security-virtual-private-networking

IZA, L. M. (2021). *Estudio para la implementacion de una red VPN utilizando herramientas de software libre*. Obtenido de Repositorio Puce: http://repositorio.puce.edu.ec/bitstream/handle/22000/18899/MTI%20TESIS_Quishpe%20Iza%20Luis%20Marcelo_2021-03-29.pdf?sequence=1

Jota Fonseca, R. C. (2018). *diseño de una red privada virtual (vpn) con seguridad L2PT para la empresa laboratorios expofarma s.a*. Obtenido de https://repository.ucc.edu.co/handle/20.500.12494/6193

Linuxito. (2018). *Mejorado la seguridad de un servidor Open VPN con autenticacion TLS*. Obtenido de https://www.linuxito.com/seguridad/1070-mejorando- la-seguridad-de-un-servidor-openvpn-con-autenticacion-tls

Luz, S. D. (2022). *RedesZone*. Obtenido de Configura pfsense para proteger tu hogar o empresa con este firewall: https://www.redeszone.net/tutoriales/seguridad/pfsense-firewall-profesional-configuracion/

Martin Portillo, L. &. (2015). *Diseño e implementacion de un sistema de voz sobre ip basado en la plataforma elastix*. Obtenido de http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAS7511pdf.pdf

OpenVPN. (2015). *OpenVPN Comunity*. Obtenido de https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn

Pomar Pascual, R. (2019). *Impleentacion 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.* Obtenido de https://dspace.unl.edu.ec/jspui/bitstream/123456789/17159/1/Quezada%20Lozano%2C%20Henry%20Daniel.pdf

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

Robine, C. (2021). *¿Qué es la Voz sobre IP y cuáles son sus ventajas?* Obtenido de aircall: https://aircall.io/es/blog/voip-es/que-es-la-voz-sobre-ip-y-cuales-son-sus-

ventajas/#%C2%BFComo_funciona_la_voz_sobre_IP

Robine, C. (2021). *¿Qué es un Softphone y qué ventajas tiene?* Obtenido de aircall.io: https://aircall.io/es/blog/call-center/que-es-un-softphone/

Rosepac. (2021). *IPFire: la distribucionde linux perfecta para crear cortafuegos e inolementar firewall*. Obtenido de https://ciberninjas.com/so-linux-ipfire-redes

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

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

Zapata, M. A. (2016). *Evaluacion de parametros de calidad de servicio (QoS) para el diseño de una red VPN con MPLS.* Obtenido de http://repositorio.puce.edu.ec/handle/22000/12327