Universidad Nacional de Ingeniería

Área de Conocimiento de Tecnología de la Información v Comunicación

“Propuesta de Diseño de una Arquitectura de Interconexión de Redes para una Pyme y sus Sucursales, para mejorar la Eficiencia Operativa y la Seguridad de Datos”

Trabajo Monográfico para Optar al Título de Ingeniero en Telecomunicaciones

Elaborado por:

Br. Jeycob Josué García Ruíz
Carnet: 2018-0805I

Br. Kimberling Tatiana Jarquin Vanegas
Carnet: 2018-0826I

Tutor:

Ing. Marlovio José Sevilla Hernández

10 de febrero de 2026
Managua, Nicaragua

Dedicatoria

A Dios sobre todas las cosas, por ser la fuente inagotable de nuestra fortaleza y por iluminar nuestro camino con su guía. A Él agradecemos profundamente su amor inmenso e incondicional, que nos sostuvo firmemente a lo largo de los momentos más difíciles de esta travesía.

A nuestras familias, por ser el pilar fundamental de nuestra formación profesional, por sus sacrificios, y por el aliento constante que nos motivó a no rendirnos y a esforzarnos por la excelencia.

A nuestros profesores que han sido un gran apoyo y especialmente a nuestro tutor, gracias por compartir su conocimiento, correcciones y siempre guiarnos en el mejor camino, gracias a sus consejos y dedicación hemos culminado exitosamente nuestro trabajo

Finalmente, queremos agradecer a todas las personas que nos apoyaron durante nuestra carrera, a nuestros amigos y compañeros de clase, y con profundo cariño, a aquellos seres queridos que partieron antes de ver culminada esta meta, pero cuyo amor y enseñanzas siguen siendo una inspiración en nuestras vidas.

Jeycob J. García Ruiz

Kimberling T. Jarquín Vanegas

Agradecimiento

Primeramente, a Dios por ser la clave de nuestro éxito, por habernos permitido culminar esta etapa profesional, nos ha dado fortaleza y ha sido nuestro guía en nuestras vidas.

A nuestros amados padres, por su amor incondicional, su sacrificio constante y por ser nuestro pilar fundamental e inspiración. Gracias por impulsarnos a alcanzar nuestros sueños y por creer en nosotros incluso más de lo que nosotros mismos lo hicimos.

Finalmente, al distinguido Tutor Marlovio José Sevilla Hernández, por su invaluable orientación académica, su paciencia ejemplar y sus sabias recomendaciones que iluminaron el camino de la investigación. Su apoyo profesional y personal ha sido verdaderamente fundamental para la consecución y el éxito de este trabajo monográfico.

Jeycob J. García Ruíz

Kimberling T. Jarquín Vanegas

Resumen

Este trabajo monográfico, titulado "Propuesta de Diseño de una Arquitectura de Interconexión de Redes para una Pyme y sus Sucursales", del cual se propuso un diseño técnico que mejore la eficiencia operativa y la seguridad de datos de una empresa, para que esté sea utilizado como una base para desarrollo de interconexión de futuras Pymes, brindando una propuesta robusta y segura. La investigación es de tipo aplicada con un enfoque cuantitativo, basándose en el análisis de datos medibles como la cantidad de usuarios, el cálculo de ancho de banda y los costos del equipamiento para evaluar la viabilidad técnica de la propuesta.

Como resultado, se desarrolló un diseño técnico jerárquico (**Three-Tier** para casa matriz y **Two-Tier** para sucursales) que utilizó túneles **VPN IPSec (ADVPN)** y segmentación por **VLANs**, estableciendo una base robusta y escalable que optimizó la eficiencia operativa y garantizó la protección de datos para organizaciones en el entorno local.

Además de ello se desarrollaron otros puntos con el objetivo de solidificar las bases de la propuesta; como lo es la localización y evaluación de los sitios, garantizando el tipo de tecnología y cobertura con la que cuentan las zonas, una tabla comparativa con modelos de equipo de comunicaciones que ofrecen diferentes marcas; con el fin de concretar la selección de la mejor opción para realizar la propuesta, además de ello se llevó a cabo la presentación de los costos del equipamiento y servicios a contratar. Agregando el desarrollo del cálculo de ancho de banda; para cálculos del consumo de la infraestructura propuesta y de esta manera conocer la capacidad del servicio a contratar a las empresas de telecomunicaciones.

Palabras claves

Casa matriz (CM), sucursal Masaya, sucursal León, EVE-NG, Three Tier, Two Tier, evaluación de proveedores de internet (ISP), FortiGate, Access Point, Switch core, Switch de acceso, VPN, ADVPN.

Índice del contenido

Índice de figura

Índice de Tabla

Índice de formulas

1. Introducción

El crecimiento de las nuevas tecnologías está transformando el panorama empresarial en Nicaragua, especialmente para las pequeñas y medianas empresas (Pymes) que buscan expandirse y consolidarse en los mercados cambiantes, y que representan gran parte del sector del mercado nicaragüense, generando una gran cantidad de empleos. Por lo tanto, la comunicación efectiva es fundamental para estas empresas, y el alcance de este proyecto monográfico se centró en proponer un modelo de infraestructura de interconexión jerárquico y robusto para una PYME y sus sucursales, garantizando así un mayor alcance y flexibilidad en sus procesos productivos, y sirviendo como modelo replicable para futuras Pymes en el entorno local.

La interconexión de redes entre sucursales es crucial para muchas Pymes en Nicaragua y en todo el mundo. Debido a que permite una comunicación eficiente y segura entre diferentes ubicaciones, lo que facilita la colaboración y la coordinación de actividades comerciales para lograr una buena operatividad, es por ello que las empresas suelen recurrir a soluciones tecnológicas, como redes privadas virtuales (VPN), conexiones de fibra óptica, redes de área amplia (WAN) o soluciones basadas en la nube, es por esto la importancia de garantizar la seguridad de estas conexiones mediante el uso de cifrado y medidas de protección contra intrusiones. Esta monografía proporcionará una guía valiosa para mejorar la comunicación interna y externa, por lo tanto, se abordó el desafío de proponer un diseño escalable con el fin de optimizar la interconexión de redes para una pyme y sus sucursales, ya que estas se encuentran en gestión de nuevas propuestas competitivas en los diferentes tipos de mercados en donde se desarrollan, donde un diseño eficiente y seguro de la red permite confidencialidad de información, garantizando la integridad y disponibilidad de acceder de forma oportuna a los servicios de datos para el usuario autorizado.

2. Objetivos

Objetivo General

- Diseñar una arquitectura de red e interconexión para una pyme y sus sucursales con el fin del mejoramiento de la eficiencia operativa y la seguridad de datos.

Objetivo Específicos

- Determinar tecnología y los equipos de red adecuados para el soporte de la interconexión y su escalabilidad.
- Realizar estudio técnico del diseño de la arquitectura de red.
- Validar el funcionamiento de la red mediante el software EVE-NG.

3. Justificación

Cabe resaltar que a medida que evolucionan las redes también surge la necesidad de diseñar una red que cumpla con las expectativas del usuario y se debe de tomar en cuenta al realizar la arquitectura de la red cuatro características primordiales como lo son: tolerancia a fallas, escalabilidad, calidad de servicio y seguridad. Por lo tanto, es importante tener una red bien diseñada y correctamente interconectada. Un diseño deficiente puede generar grandes problemas en el rendimiento, como pueden ser la vulnerabilidad de seguridad y dificultades en la gestión de la red. Es por ello, que en esta investigación se basó en una propuesta de diseño integral y eficiente en donde se garantiza a interconexión robusta y segura, aprovechando las mejores prácticas en el diseño de redes de computadora y la experiencia en certificaciones Cisco.

Para este proyecto monográfico, se propuso una pyme que posee dos sucursales, esto con el objetivo de lograr una propuesta de diseño que sea escalable para empresas y futuras pymes que desean estar a la vanguardia del mercado local e internacional ya que una correcta segmentación, una infraestructura de red robusta y escalable es fundamental debido a que esto permite una comunicación eficiente y fluida entre los empleados y los sistemas de la empresa, lo que mejora la productividad y la colaboración, ya que la ausencia de QOS y segmentación de la red resulta en una latencia de transacciones de ventas. Además, una red robusta garantiza la seguridad de los datos y la protección contra amenazas cibernéticas. Por último, una infraestructura escalable permite adaptarse fácilmente al crecimiento y a las necesidades cambiantes del negocio sin comprometer el rendimiento ni la seguridad.

Una buena elección de proveedor de servicios de telecomunicaciones adecuado es crucial para garantizar una interconexión de redes confiable y eficiente. Algunos de los factores a considerar al seleccionar un proveedor de servicios incluyen la calidad de la infraestructura de red, la cobertura geográfica, la confiabilidad del servicio, el soporte técnico ofrecido y el costo de estos. Cabe mencionar que el diseño propuesto no es solo un costo, sino una inversión que habilita el crecimiento futuro y minimiza los riesgos.

4. Marco Teórico

4.1 Red Informática

Una red informática es un conjunto de dispositivos que se encuentran interconectados entre sí a través de un medio, estos intercambian información y comparten recursos.

Son sistemas de comunicación en la que distintos dispositivos actúan de emisor y receptor de manera alterna. Forman parte de una red informática los dispositivos, los medios de conexión, la estructura y el modo de funcionamiento de las redes, la información y los recursos compartidos. [1]

4.2 Dispositivos Intermedios

Los dispositivos intermedios conectan los dispositivos finales individuales a la red. Pueden conectar múltiples redes individuales para formar una red interna. Los dispositivos intermedios proporcionan conectividad y garantizan el flujo de datos en toda la red.

Los dispositivos intermedios usan la dirección del dispositivo final de destino, junto con información sobre las interconexiones de la red, para determinar la ruta que los mensajes deben tomar a través de la red. En la figura, se muestran algunos ejemplos de los dispositivos intermediarios más comunes. [2]

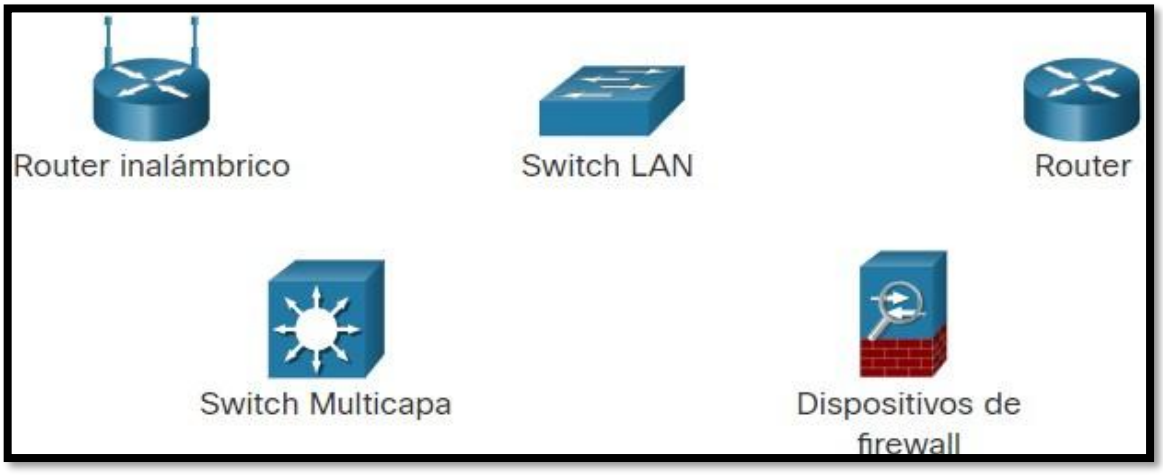

Figura No. 1 Dispositivos Intermedios [2]

4.3 ¿Qué es la topología de red?

La topología de red se representa normalmente mediante un dibujo de líneas y objetos que refleja la topología física y lógica general.

Hay dos tipos diferentes de topologías de red: La topología de red física es la ubicación de diversos componentes de una red. Los diferentes conectores representan los cables de red físicos y los nodos representan los dispositivos de red físicos (como los switches). La topología de red lógica ilustra, en el nivel más alto, cómo fluyen los datos dentro de una red. [3]

4.3.1 Topología de árbol

Pueden enlazarse varios dispositivos en una topología de árbol como si fueran ramas. Estas topologías se utilizan mucho para enlazar equipos en el sistema de una empresa. En esta topología, existe una conexión única entre dos elementos cualquiera vinculados, con un enlace recíproco que forma una estructura típica de padre e hijo. En los sistemas informáticos, este tipo de topología también se conoce como topología de bus en estrella, ya que combina las características de una topología de bus y de estrella. Este tipo de diseño resulta más eficaz en casos concretos, como la comunicación entre dos redes distintas. El modelo de red requiere el uso de varios nodos, como el intermedio, la raíz y el principal.

En una topología de malla completa, las computadoras de una red de área local están interconectadas con todas las demás computadoras de la misma red. En una topología de malla parcial, no todas las computadoras, sino unas pocas, están interconectadas con otras a las que se comunican constantemente. [4]

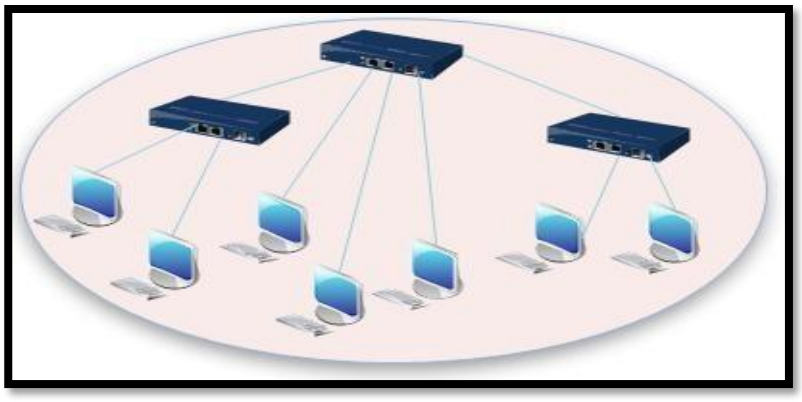

Figura No. 2 Topología en árbol.[4]

4.4 Acceso empresarial (y doméstico): Ethernet y Wifi

En los campus universitarios y corporativos, y cada vez más en entornos domésticos, se utiliza una red de área local (LAN, Local Área Network) para conectar un sistema terminal al router de frontera. Aunque existen muchos tipos de tecnologías LAN, Ethernet es con mucho la tecnología de acceso predominante en las redes corporativas, universitarias y domésticas.

En un entorno de LAN inalámbrica, los usuarios inalámbricos transmiten/reciben paquetes hacia/desde un punto de acceso que está conectado a la red empresarial (probablemente utilizando Ethernet cableada), que a su vez se conecta a la red Internet cableada.

Habitualmente, los usuarios de una LAN inalámbrica deben encontrarse a unas pocas decenas de metros del punto de acceso. Actualmente, el acceso mediante LAN inalámbrica basada en la tecnología IEEE 802.11, más coloquialmente conocido como WiFi, podemos encontrarlo por todas partes: universidades, oficinas, cafés, aeropuertos, domicilios e incluso en los aviones. [4]

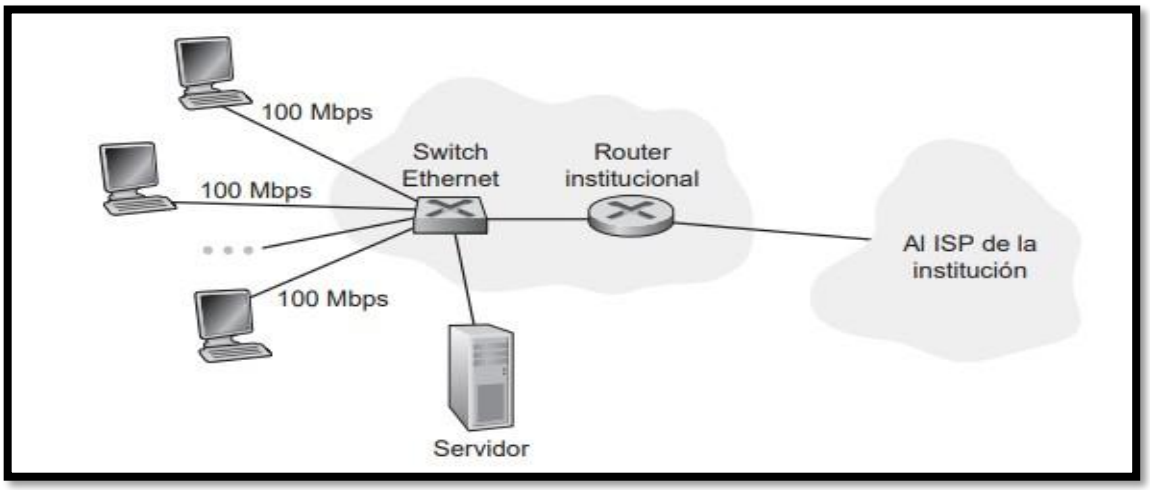

Figura No. 3 Acceso a Internet utilizando tecnología Ethernet. [5]

4.4.1 Las redes de área local (LAN)

Una LAN es una infraestructura de red que proporciona acceso a usuarios y dispositivos finales en un área geográfica pequeña. Normalmente, una LAN se utiliza en un departamento dentro de una empresa, un hogar o una red de pequeñas empresas. Las LANS tienen características específicas:

- Las LANS interconectan terminales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus.
- Por lo general, la administración de las LAN está a cargo de una única organización o persona.
- Las LANS proporcionan ancho de banda de alta velocidad a dispositivos finales internos y dispositivos intermedios, como se muestra en la figura. [7]

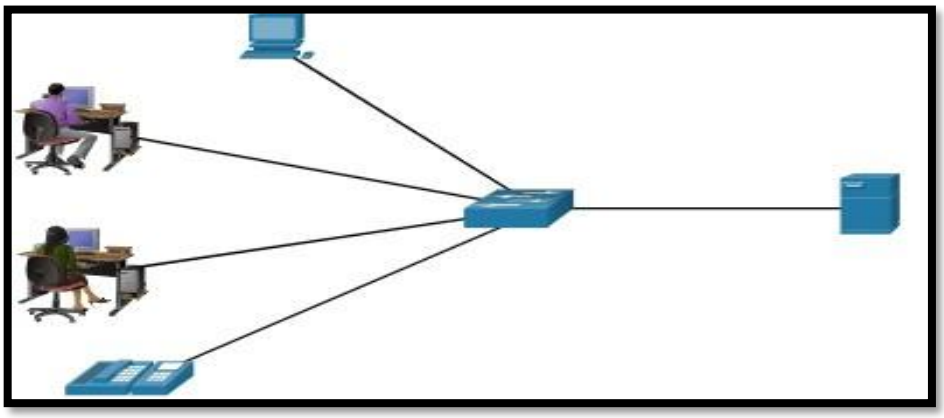

Figura No. 4 Estructura de una red LAN. [2]

4.4.2 Redes WAN

La figura muestra una WAN que interconecta dos LAN. Una WAN es una infraestructura de la red que abarca un área geográfica extensa. Las WAN generalmente son administradas por proveedores de servicios (SP) o proveedores de servicios de Internet (ISP).

Las WANS tienen características específicas:

- Las WAN interconectan LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, estados, provincias, países o continentes.
- Por lo general, la administración de las WAN está a cargo de varios proveedores de servicios. • Normalmente, las WAN proporcionan enlaces de velocidad más lenta entre redes LAN. [2]

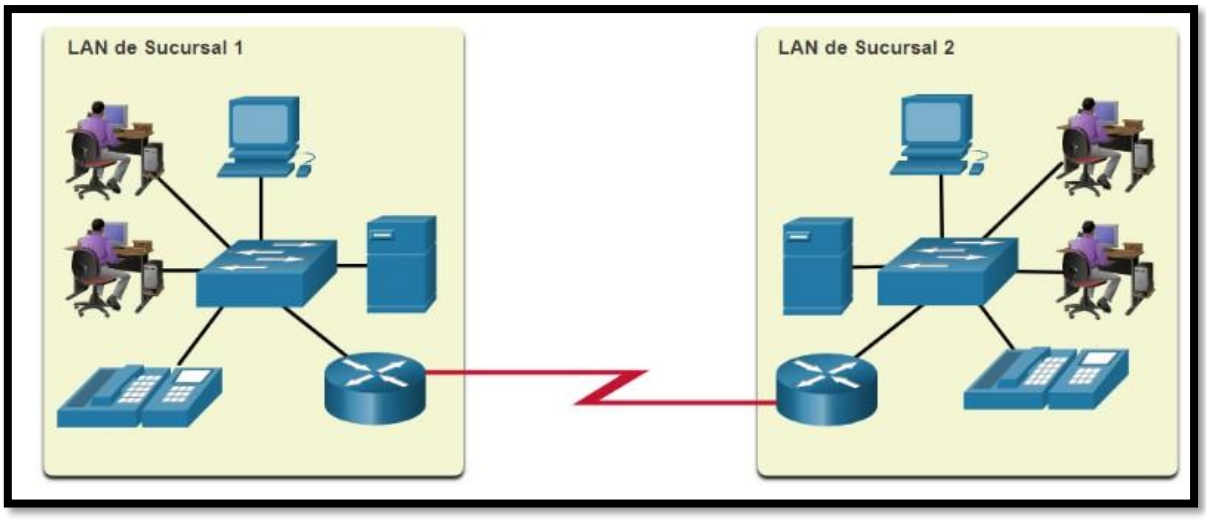

Figura No. 5 Estructura de una red WAN. [2]

4.5 Estructura de Protocolos

4.5.1 DNS el servicio de directorio de Internet

Sistema de nombres de dominio (DNS, Domain Name System) de Internet. DNS es (1) una base de datos distribuida implementada en una jerarquía de servidores DNS y (2) un protocolo de la capa de aplicación que permite a los hosts consultar la base de datos distribuida. [6]

4.5.2 Dirección IP

Las direcciones IP son únicas para cada máquina. Para ser precisos, cada dirección es única para cada una de las interfaces de red IP de cada máquina. Si una máquina dispone de más de una interfaz de red, necesitará una dirección IP para cada una, las direcciones IP tienen una longitud de 32 bits (4 bytes).

Para lograr que no haya ninguna dirección igual, Internet dispone de una organización denominada Internet Network Information Center o InterNIC que se dedica a esta tarea. En la actualidad, esta entidad delega la responsabilidad de la asignación de direcciones a entidades regionales. Las direcciones se asignan por grupos o redes, no individualmente.

Los tipos de redes que tienen cabida en Internet se distinguen por la cantidad de estaciones que pueden soportar, y son los siguientes: [5]

1) Las redes de clase A reservan el primer byte como identificador de red y los tres restantes como identificadores de estación. El primer bit del primer byte vale 0,

por tanto, en Internet sólo puede haber 128 redes de clase A (con 224 estaciones cada una como máximo). Hace mucho tiempo que ya no queda ninguna para asignar.

2) Las redes de clase B tienen 16 bits para cada campo; los dos primeros bytes del identificador de red valen 1 & 0, por lo tanto, hay 16.384 (214) redes de, como mucho, 65.536 estaciones. De clase B no queda ninguna para asignar.

El único objetivo de esta notación es la legibilidad humana. No se puede perder nunca de vista que una dirección IP son 32 bits.

3) Las redes de clase C utilizan los primeros 24 bits para el identificador de red, de los cuales los tres bits iniciales del primer octeto están fijados en 110 para indicar la clase. Los 8 bits restantes (el último octeto) son para el identificador de estación (*host*). Una vez que se conoce una dirección, es fácil saber si corresponde a una red de clase A, B o C, examinando los bits iniciales del primer octeto.

Tabla 1 Segmento de red.

Clase	Direcciones Disponibles		Cantidad de Redes	Cantidad de Hosts	Aplicación
	Desde	Hasta			
A	0.0.0.0	127.255.255.255	128	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes Medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	No aplica	No aplica	Multicast
E	240.0.0.0	255.255.255.255	No aplica	No aplica	Investigación

La clase A está pensada para grandes empresas o corporaciones, con muchos terminales por identificar; la clase B, para corporaciones medianas; la clase C, para entornos mucho más pequeños; la clase D está destinada al tráfico Multicast IP, y la clase E está destinada a investigación. [5]

4.6 Subnetting

Subneteo es la acción de tomar un rango de direcciones IP, donde todas sean locales unas con otras y dividirlas en diferentes rangos, o subredes (subnets), donde las direcciones IP de un rango serán remotas de las otras direcciones.

Para determinar cuántos hosts se tiene en un rango IP, se tiene que definir la porción de host que tenemos, ejemplo: 200.10.50.212 y 255.255.255.248,

Establecemos que la red es 200.10.50.208 y la porción de host es 4. Se explicará el proceso que se llevó para obtener dicho resultado en la red 200.10.50.208.

Tabla 2 Subnetting.

N	7	6	5	4	3	2	1	0
2_n	128	64	32	16	8	4	2	1
Bit	1	1	0	1	0	0	0	0
/	/24	/23	/22	/21	/20	/19	/18	/17

La red que nos dieron es la 200.10.50.212 y su máscara de red es 255.255.255.248, convertimos a binario nuestro cuarto octeto los cuales serán 212 y 248, el valor que resulte de esa sumatoria determinara el cuarto octeto de nuestra nueva red.

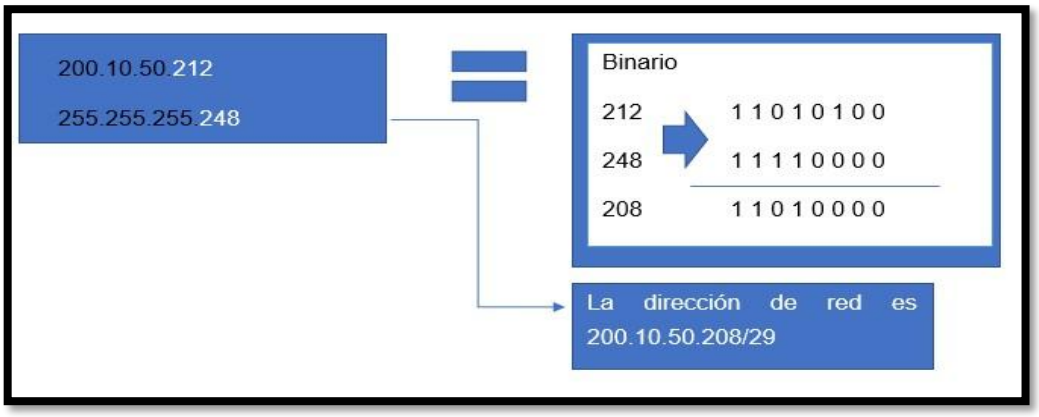

Figura No. 6 Conversión y sumatoria binaria. [5]

Se observa en la imagen anterior, la sumatoria binaria de los últimos cuatro octetos de la red y su máscara para obtener la nueva dirección de red, en otras palabras; tenemos 3 octetos para porción de red y uno para la porción de host. Ahora que hemos determinado la cantidad de hosts bits que tenemos, es 6 host, es decir 6 direcciones IP posibles. Tipo de clase C. [7]

4.7 Protocolo de configuración dinámica de hosts (DHCP)

El protocolo de configuración dinámica de hosts (DHCP) es un estándar TCP/IP que utiliza un servidor central para gestionar direcciones IP y otros datos de configuración para toda una red. Un servidor

DHCP responde a las peticiones de los clientes, asignándoles propiedades de forma dinámica. [8]

4.7.1 Definiciones y conceptos de transmisión de datos

Se entiende por transmisión de datos al movimiento de información codificada, de un punto o más puntos, mediante señales eléctricas, ópticas, electrópticas o electromagnéticas.

Este requerimiento, originado en las organizaciones gubernamentales, industriales, comerciales, bancarias, empresariales, militares, etc., ha nacido por la necesidad de poner a disposición de ellas en un punto remoto la capacidad de proceso de un ordenador, ubicado en un punto que podríamos llamar central.

Este punto puede estar dentro de la propia organización, próximo o alejado del ordenador central. La diferencia importante reside en la distancia y la geografía del problema a considerar, pues en función de estos parámetros, puede ser necesario o no el uso de redes de comunicaciones. [9]

4.8 VPN según necesidades empresariales

Una empresa u organización normalmente implementa una VPN para satisfacer las necesidades de comunicación dentro de la organización (intranet), comunicación con otras organizaciones (extranet) y acceso de usuarios desde dispositivos móviles, computadoras en casa u oficinas remotas.

Las soluciones que cubren estas necesidades abarcan la gran mayoría de topologías y tecnologías que los proveedores de servicios VPN ofrecen. La diferencia se encuentra en el nivel de seguridad que maneja cada tipo de implementación.

En el caso de la intranet, el tráfico enviado suele no estar bien protegido por los hosts finales o los firewalls con los que cuenten. Por lo tanto, la solución VPN para este tipo de comunicación debe ofrecer altos niveles de aislamiento y seguridad. Además, el servicio debe contar con calidad de servicio (QoS) garantizada para procesos críticos.

Por dichas razones, una organización no suele optar por utilizar la red de Internet, pues no se puede contar con calidad de servicio de extremo a extremo, aislamiento o seguridad que las conexiones dentro de la empresa requieren.

Los usuarios remotos acceden a la red corporativa desde ubicaciones desconocidas y no fijas. Esto produce problemas de seguridad entre los extremos del enlace, que se resuelven aplicando tecnologías de encriptación o contraseñas de un solo uso.

Por lo tanto, el nivel de seguridad requerido para estas redes, llamadas VPDN (Virtual Private Dial-up

Network), es significativamente menor que para redes Intranet. Actualmente, la mayoría de servicios VPDN son implementados sobre IP, ya sea a través de Internet o a través del backbone de un proveedor. [10]

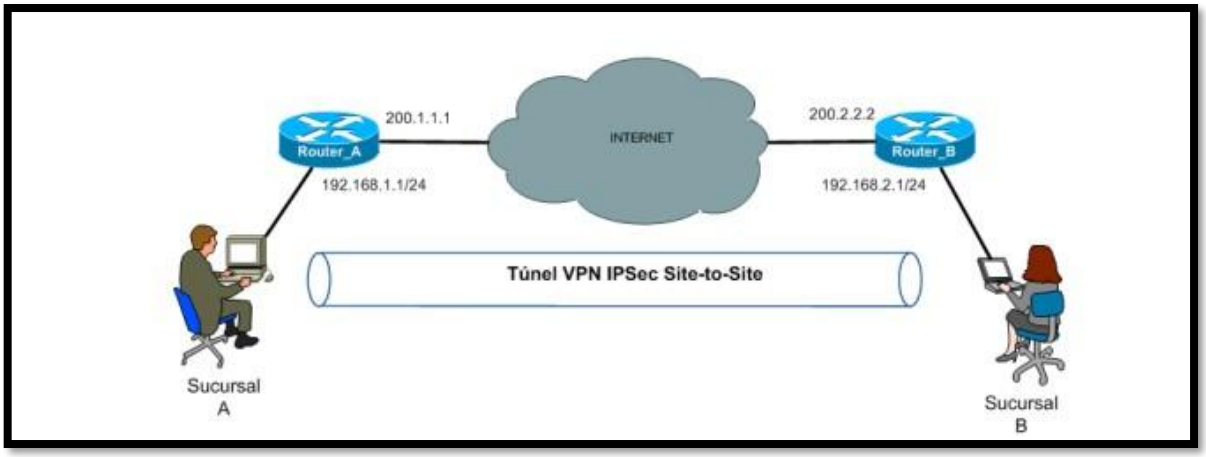

Figura No. 7 Visualización de una red VPN. [10]

4.9 Protocolo de seguridad

La autenticación, autorización y contabilidad (AAA) es un marco de seguridad que controla el acceso a los recursos informáticos, hace cumplir las políticas y audita el uso. La seguridad AAA y sus procesos combinados desempeñan un papel importante en la gestión de redes y la ciberseguridad mediante la selección de usuarios y el seguimiento de su actividad mientras están conectados.

TACACS+ separa los procesos de autenticación y autorización, y esto lo diferencia de RADIUS, que los combina. Además, TACACS+, como RADIUS, cifra sus paquetes AAA. [11]

4.10 Modelo OSI

El modelo OSI, de siete capas, es un modelo conceptual que caracteriza y estandariza la manera en la que los diferentes componentes de software y hardware involucrados en una comunicación de red deben dividir la mano de obra e interactuar entre sí. En la siguiente figura podrá ver los nombres y funciones básicas de cada una de las capas. [12]

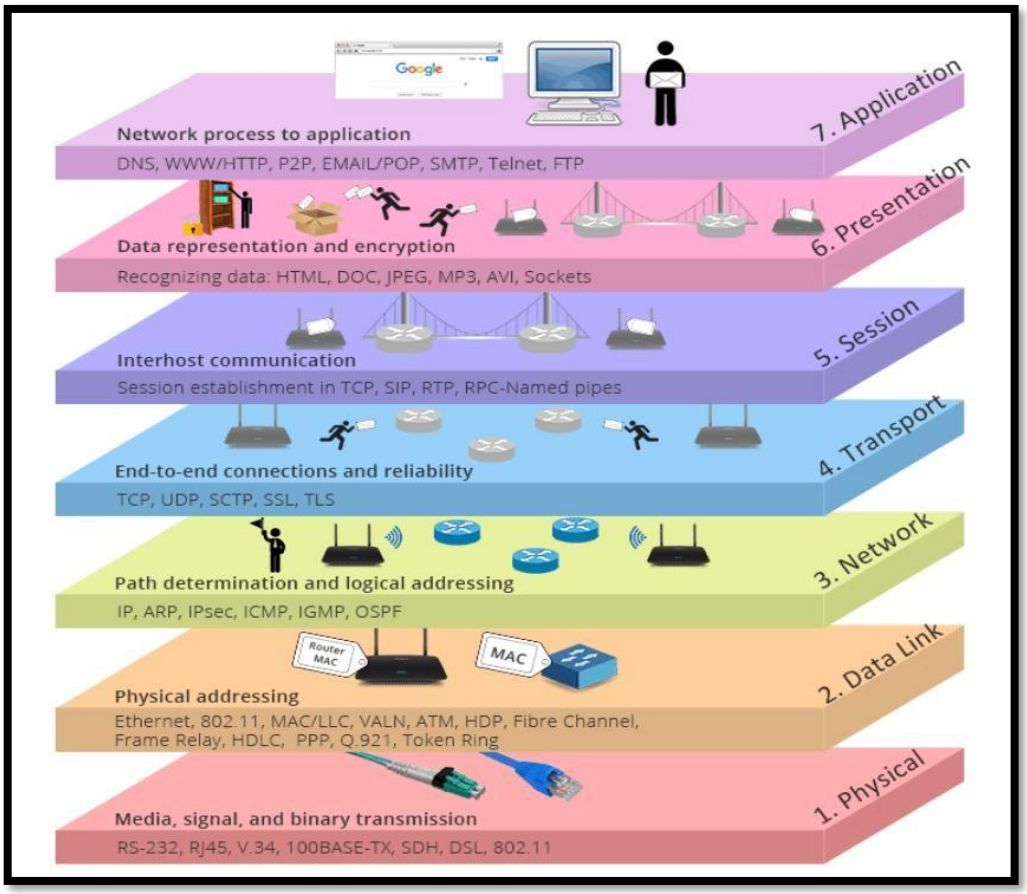

Figura No. 8 Modelo OSI. [12]

4.11 Beneficios de la interconexión de redes para las Pymes

La demanda de la conectividad de calidad y segura se ha convertido en una de las principales preocupaciones en los mercados actuales, es por ello que la interconexión de sucursales de Pymes en Nicaragua a través de una red puede proporcionar una serie de beneficios significativos para estas empresas:

- **Comunicación eficiente:** Esto facilita la coordinación de actividades comerciales, la resolución de problemas y la toma de decisiones en tiempo real.

- **Acceso a información centralizada:** Esto mejora la coherencia de la información y evita duplicaciones o inconsistencias.
- **Mayor productividad:** Al facilitar la comunicación y el acceso a la información, las redes interconectadas pueden aumentar la productividad de las sucursales.

La experiencia de los clientes es uno de los pilares fundamentales de la información digital, creando nuevos desafíos y de esta manera se procura desarrollar soluciones que beneficien a los consumidores, así como al mismo tiempo que se garantiza la seguridad de los datos empresarial.

4.12 EVE-NG

Es una solución de virtualización de red de muy completa que permite crear, configurar y gestionar topologías de red complejas en un entorno virtualizado. Proporciona una solución de virtualización de red completa que combina tecnologías como VirtualBox, VMware, Docker y KVM para permitir a los usuarios crear y gestionar entornos de red virtuales.

Además, EVE-NG ofrece una gran cantidad de características y funcionalidades que hacen que sea fácil de usar y personalizar para cualquier necesidad determinada. Algunas de estas características son: Múltiples protocolos y tecnologías de red como IPv4, IPv6, OSPF, MPLS, VXLAN, etc. [13] EVE-NG se publica actualmente como archivos OVF e ISO. Un OVF es un formato virtual abierto para la máquina virtual. También se puede instalar directamente en el hardware físico, sin virtualización mediante el uso de una imagen ISO. Estado actual: v5.0.1-22 (5 de marzo de 2024). [14]

Tabla 3 Requerimientos para EVE-NG.

Requerimientos mínimos del sistema:	**Configuración del sistema recomendada:**
Sistema operativo: Windows 10 64-bit CPU: doble núcleo a 2,0 GHz RAM: 4 GB o superior Video: AMD Radeon 5450 o NVIDIA GeForce 420 o superior con al menos 1024 MB de VRAM	Sistema operativo: Windows 10 de 64 bits CPU: Intel I7-7700 o AMD Ryzen 7 1700 a 3,6 GHz o superior RAM: 4 GB o superior Vídeo: NVIDIA Geforce GTX 1060, AMD Radeon RX 580 o superior con al menos 4 GB de VRAM

5. Análisis y presentación de resultados

5.1 Diseño metodológico

La presente monografía se orientó al desarrollo de una propuesta de diseño de red para pequeñas y medianas empresas (pymes) y sus sucursales, con el propósito de garantizar una interacción segura y eficiente por parte de los usuarios, dentro de una arquitectura que ofrezca alta escalabilidad y disponibilidad en todo momento. Una red segura debe fundamentarse en cuatro pilares esenciales: tolerancia a fallas, escalabilidad, calidad de servicio y seguridad.

El tipo de investigación de la monografía es aplicada debido a que tiene como finalidad proponer una solución práctica orientada a un problema real: el diseño de una arquitectura de red e interconexión para una pyme y sus sucursales. Este tipo de investigación busca generar conocimientos que puedan ser utilizados directamente para mejorar la eficiencia operativa y la seguridad de los datos, cumpliendo con los requerimientos tecnológicos, cabe destacar que el enfoque de la investigación es de tipo cuantitativo ya que se basa en análisis de datos medibles relacionados con la infraestructura de red, cálculo de ancho de banda, la cantidad de usuarios y dispositivos, los costos de implementación de los servicios y equipos. Estos datos permiten evaluar objetivamente la viabilidad técnica y operativa de la arquitectura propuesta.

Previo a nuestro diseño de interconexión de la pyme y sus sucursales, se planteó el siguiente esquema de trabajo basado en la metodología seleccionada, cabe

destacar que desarrollamos en los siguientes apartados a detalle cada uno de los puntos que a continuación se nombran:

1. Estado de la red actual y sus debilidades.
2. Propuesta de diseño de la arquitectura de red.
3. Direccionamiento de red.
4. Localización y evaluación de sitios.
5. Evaluación de proveedores de internet.
6. Propuesta de equipos y costos.
7. Estimación de ancho de banda.
8. Simulación.

5.2 Propuesta de diseño de la Arquitectura de Red:

En este punto se planteó el desarrollo de una arquitectura de red sólida y escalable que integre la pyme y sus sucursales de manera eficiente y segura, utilizando herramientas de software como lo son: Drawio y EVE-NG para simulaciones y pruebas.

Actualmente con el avance de la tecnología en los diferentes sectores empresariales, la infraestructura de red juega un papel fundamental no solo apoyando las operaciones diarias de las PYMES, sino que también sirve como un habilitador clave para la innovación, el crecimiento continuo y la competitividad en un mercado globalizado y digitalmente transformado. Es fundamental invertir en una infraestructura de red adecuada para aprovechar al máximo las oportunidades que ofrece la tecnología moderna.

Las redes nos permiten realizar conexiones de dos o más ordenadores, de tal forma que son capaces de compartir los recursos de la empresa tales como impresoras, archivos, aplicaciones, software, base de datos, servidores, así como el acceso a escritorios virtuales y sesiones de trabajo, ya que facilitan la productividad, la eficiencia, la optimización del uso de recursos al permitir que múltiples usuarios accedan y utilicen dispositivos y datos compartidos de manera simultánea, reduciendo costos operativos al eliminar la necesidad de replicar recursos para cada usuario o equipo de manera individual.

Como se ha mencionado existen diferentes tecnologías de redes en donde según su aplicación y alcance geográfico se clasifican en redes de área local como lo son LAN, WAN, MAN, entre otras, en donde el uso de esta brinda una solución a las diferentes problemáticas de interconexión entre una empresa y sus filiales.

En este trabajo monográfico se decidió centrar el proyecto en una propuesta de diseño de una arquitectura de interconexión de redes para una pyme, en donde se propuso interconectar una sede central y sus sucursales. Las cuales se encuentran ubicadas en los siguientes departamentos: Casa matriz Managua, sucursal 1 León y sucursal 2 Masaya. Haciendo uso de la tecnología VPN (Redes Privadas Virtuales) para establecer conexiones seguras y cifradas entre la central y cada una de las sucursales, realizando una simulación de funcionalidad de la interconexión mediante el emulador EVE-NG.

Posterior se comenzó con el proceso de diseño de la arquitectura de red, en el cual se especificaron los requerimientos que se tuvieron que tomar en cuenta al momento del diseño, ya que se planteó una propuesta que se adapte a los requerimientos de las PYMES que deseen expandirse a un mercado más globalizado y competitivo, de tal forma que dicho proyecto sirva como guía para una futura implementación en empresas de cualquier tipo de rubro comercial, tomando en cuenta las mejores prácticas de diseño de una arquitectura de interconexión de red.

Retomando lo mencionado con respecto a la división de las sucursales que se han abordado en el transcurso del proyecto monográfico, se realizó como primer paso un esquema de trabajo específico por cada sucursal en donde se plantearon las diferentes áreas de trabajo y puestos que ocupan en dicha empresa. Cabe mencionar que al ser el departamento de Managua la casa matriz esta cuenta con una mayor cantidad de áreas de trabajo, lo que conlleva a una mayor cantidad de trabajadores (usuarios).

5.2.1 Tablas organizativas de las áreas

Los esquemas que se estarán presentando a continuación fueron realizados en orden jerárquicos haciendo uso de la herramienta Drawio, el cual facilitó la agregación de los puestos de trabajo por cada una de las sucursales.

5.2.1.1 Tablas Organizativas de Casa Matriz

Mediante las tablas de casa matriz Managua, la cual actualmente cuenta con un total de 10 áreas y 22 trabajadores en total, estarán distribuidos de la siguiente manera:

- Tabla organizativa de la Gerencia General en la Casa Matriz, distribución de cargos y usuarios.

Tabla 4 Distribución de Cargos y Usuarios área 1.

Área 1:	**Gerencia General**
Cantidad de Usuarios:	1
Cargo Desempeñado:	Gerente General

- Tabla organizativa de la Sub-Gerencia general en la casa Matriz, distribución de cargos y usuarios.

Tabla 5 Distribución de Cargos y Usuarios área 2.

Área 2:	**Sub-Gerencia**
Cantidad de Usuarios:	1
Cargo Desempeñado:	Sub Gerente

- Tabla organizativa de Recursos Humanos en la casa Matriz, distribución de cargos y usuarios.

Tabla 6 Distribución de Cargos y Usuarios área 3.

Área 3:	**Recursos Humanos**
Cantidad de Usuarios:	2
Cargo Desempeñado:	Gerente de RH
Cargo Desempeñado:	Auxiliar de RH

- Tabla organizativa de la Gerencia de Tecnología de la Información en la casa Matriz, distribución de cargos y usuarios.

Tabla 7 Distribución de Cargos y Usuarios área 4.

Área 4:	**Gerencia de Tecnología de la Información**
Cantidad de Usuarios:	5
Cargo Desempeñado:	Gerente de TI
Cargo Desempeñado:	Infraestructura y Seguridad
Cargo Desempeñado:	Analista de base de datos

Cargo Desempeñado:	Desarrollador Web
Cargo Desempeñado:	Desarrollador Web

- Tabla organizativa del área Auditoria en la casa Matriz, distribución de cargos y usuarios.

Tabla 8 Distribución de Cargos y Usuarios área 5.

Área 5:	**Auditoria**
Cantidad de Usuarios:	2
Cargo Desempeñado:	Auditor Interno
Cargo Desempeñado:	Auditor Externo

- Tabla organizativa del área Marketing y Publicidad en la casa Matriz, distribución de cargos y usuarios.

Tabla 9 Distribución de Cargos y Usuarios área 6.

Área 6:	**Marketing y Publicidad**
Cantidad de Usuarios:	3
Cargo Desempeñado:	Gerente de Marketing
Cargo Desempeñado:	Diseñador Grafico
Cargo Desempeñado:	Creador de Contenido

- Tabla organizativa del área de Contaduría en la casa Matriz, distribución de cargos y usuarios.

Tabla 10 Distribución de Cargos y Usuarios área 7.

Área 7:	**Contaduría**
Cantidad de Usuarios:	1
Cargo Desempeñado:	Contador

- Tabla organizativa del área Dirección Jurídica en la casa Matriz, distribución de cargos y usuarios.

Tabla 11 Distribución de Cargos y Usuarios área 8.

Área 8:	**Dirección Jurídica**
Cantidad de Usuarios:	2
Cargo Desempeñado:	Abogado
Cargo Desempeñado:	Asistente Legal

- Tabla organizativa del área que ocupara el puesto de Gerencia de Ventas en la casa Matriz.

Tabla 12 Distribución de Cargos y Usuarios área 9.

Área 9:	Gerencia de Ventas
Cantidad de Usuarios:	3
Cargo Desempeñado:	Gerente de Ventas
Cargo Desempeñado:	Especialista Técnico
Cargo Desempeñado:	Especialista Técnico

- Tabla organizativa del área que ocupara el puesto de Gerencia de Atención al Cliente en la casa Matriz.

Tabla 13 Distribución de Cargos y Usuarios área 10.

Área 10:	Gerencia de Atención al Cliente
Cantidad de Usuarios:	2
Cargo Desempeñado:	Gerente de SAC
Cargo Desempeñado:	Especialista Técnico SAC

5.3 Flujograma de casa matriz

En la siguiente imagen se muestra el flujograma empresarial, se ilustra de manera visual las áreas de la organización de la casa Matriz Managua, el cual es fundamental para comprender la estructura a nivel administrativo de la empresa, optimizando la eficiencia y coordinación entre los diferentes departamentos de trabajo.

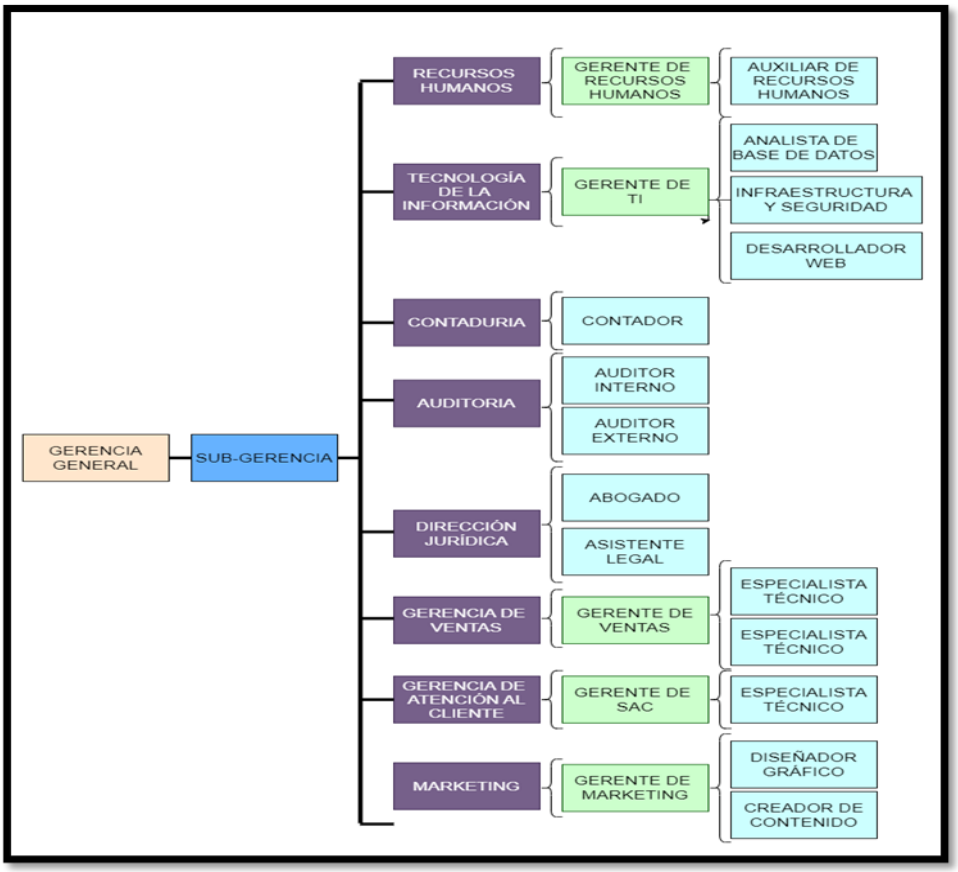

Figura No. 9 Flujograma de la empresa casa matriz Managua.

5.4 Tablas Organizativas sucursales Masaya y León

A continuación, se presentan las tablas organizativas de las 2 sucursales, en donde la primera sucursal está ubicada en el departamento de León y la segunda sucursal ubicada en el departamento de Masaya, las cuales actualmente cuentan con 5 áreas, lo que conlleva a un total de 6 trabajadores por sucursal que desempeñan los siguientes puestos para el correcto funcionamiento operativo de las mismas.

Tabla 14 Distribución de Cargos y Usuarios en área 1 para ambas sucursales.

Área 1:	**Gerencia de Sucursal**
Cantidad de Usuarios:	1
Cargo Desempeñado:	Jefe de Sucursal

Tabla 15 Distribución de Cargos y Usuarios área 2 para ambas sucursales.

Área 2:	**Gerencia de Ventas**
Cantidad de Usuarios:	2
Cargo Desempeñado:	Especialista Técnico
Cargo Desempeñado:	Especialista Técnico

Tabla 16 Distribución de Cargos y Usuarios área 3 para ambas sucursales.

Área 3:	**Gerencia de Atención al Cliente**
Cantidad de Usuarios:	1
Cargo Desempeñado:	Especialista Técnico SAC

Tabla 17 Distribución de Cargos y Usuarios área 4 para ambas sucursales.

Área 4:	**Soporte Técnico**
Cantidad de Usuarios:	1
Cargo Desempeñado:	Técnico en TI

Tabla 18 Distribución de Cargos y Usuarios área 5 para ambas sucursales.

Área 5:	**Gerencia de Finanzas**
Cantidad de Usuarios:	1
Cargo Desempeñado:	Auxiliar Contable

5.4.1 Flujograma de las sucursales Masaya y León.

En este enunciado se observa el flujograma de las sucursales de Masaya y León, el cual es de gran ayuda para entender los procedimientos internos de las áreas de la empresa y de esta manera optimizar la gestión empresarial.

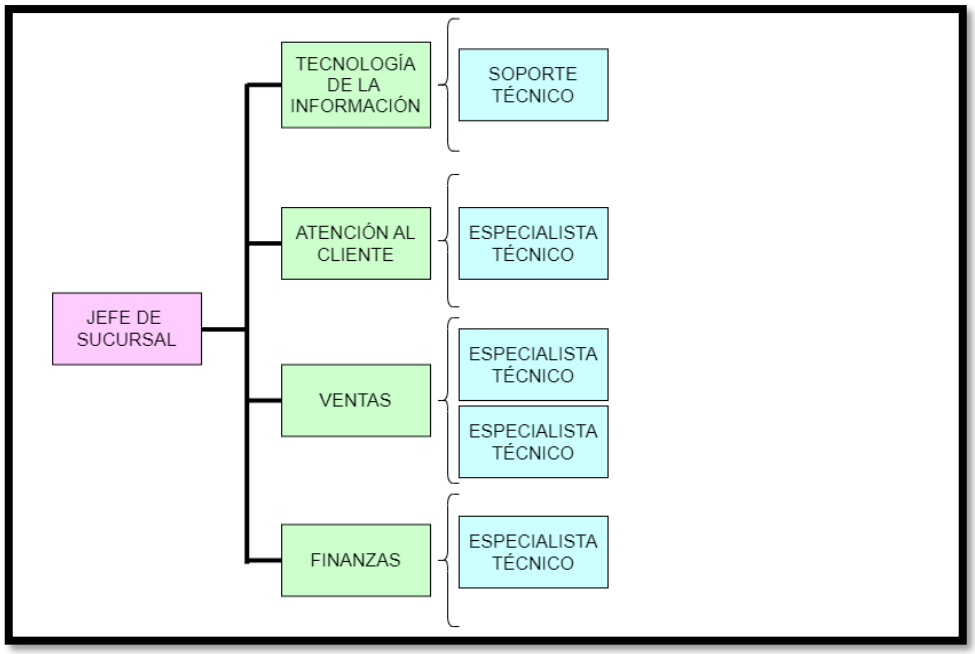

Figura No. 10 Flujograma de las sucursales Masaya y León.

5.5 Estado actual de la pyme y sus mejoras

En la actualidad, la pyme objeto de estudio presento importantes limitaciones en su infraestructura de red, las cuales afectan directamente su eficiencia operativa y la protección de la información. Entre las principales deficiencias identificadas se encontró la ausencia de mecanismos adecuados de seguridad de red, la inexistencia de una correcta segmentación de la red, así como la dependencia de un único proveedor de servicios de Internet, lo que incrementa el riesgo de interrupciones en la conectividad. Asimismo, la empresa no dispone de equipos de red robustos que le permitan escalar su infraestructura y responder de manera eficiente a una posible expansión en el mercado local o internacional, acorde al rubro en el que desee desempeñarse.

En respuesta a estas necesidades, la presente propuesta plantea el diseño de una arquitectura de interconexión de redes que incorporó la selección de equipos robustos y escalables, la implementación de una adecuada segmentación de red, el fortalecimiento de la seguridad de los datos y la provisión de alta disponibilidad del enlace a Internet mediante la utilización de más de un proveedor de servicios, con el objetivo de garantizar continuidad operativa, mayor seguridad y un crecimiento sostenible de la organización.

5.6 Infraestructuras de red lógicas

Las arquitecturas de redes lógicas juegan un papel fundamental en la configuración y operación de infraestructura de comunicaciones modernas, estas estructuras definidas por software permiten realizar el diseño, gestión y optimización de las redes, de manera flexible y eficiente, ya que ayudan a satisfacer las necesidades empresariales y tecnológicas cambiantes del entorno digital actual.

Se procedió a explicar más detalladamente en los siguientes enunciados como está dividida la estructura de red lógica por capas, para posteriormente mostrar de manera gráfica la estructura de red lógica a nivel general.

5.6.1 Infraestructura de red lógica a nivel de Capa

Al dividir la red en capas, cada una puede concentrarse en realizar una tarea específica o extraer características particulares de los datos. Esto facilita el diseño general de la red, ya que cada capa puede optimizarse independientemente y luego integrarse en un sistema unificado. Esto no solo hace que sea más fácil mantener y actualizar la red, sino que también facilita el diagnóstico y la solución de problemas, ya que cada capa puede ser evaluada por separado.

Por lo tanto, se trabajó en la jerarquía de la arquitectura de red con dos diseños principales de jerarquía: Three-Tier (tres capas) y Two-Tier (dos capas).

La elección entre un diseño de dos capas y un diseño de tres capas depende de varios factores, incluyendo el tamaño y complejidad de la red, los requisitos de rendimiento y disponibilidad, así como el presupuesto disponible para la implementación y mantenimiento. Ambos diseños tienen sus propias ventajas y desventajas, y la elección correcta dependerá de las necesidades específicas y los objetivos de la red en cuestión.

5.6.2 Diseño Three Tier

Este diseño consta de tres capas principales: la capa de acceso (Access Layer), la capa de distribución (Distribution Layer) y la capa de núcleo (Core Layer).

Este diseño es recomendado cuando se espera con el tiempo un crecimiento de la red de una empresa, porque de esta manera la capa de distribución está

destinada para conectar a múltiples dispositivos, aunque es importante mencionar que no es recomendable realizar la conexión de múltiples dispositivos a un solo bloque de distribución, ya que se convierte en el único punto de falla de la red.

1. Capa de Acceso: Es la primera capa de cara a los equipos de clientes finales tales como computadoras, cámaras, impresoras, etc; esta conecta equipos inalámbricos, así como cableados. Esta capa también se espera que provea calidad de servicios y políticas de confianza, siendo la capa de acceso el primer punto de defensa en la arquitectura de seguridad y primer punto de negociación entre los dispositivos y la infraestructura de red.

2 Capa de Distribución: La capa de distribución juega un rol importante porque actúa como un servicio y controla la frontera entre la capa de acceso y la capa de core, ofreciendo enrutamiento entre la capa de distribución y el Core. Proporciona conectividad y políticas de servicio para el tráfico que fluye dentro de un único bloque de acceso-distribución para tráfico entre nodos.

Capa de Núcleo (Capa Core): Esta capa está diseñada para estar siempre disponible, ofreciendo un alto nivel de redundancia en el enlace, no se implementa ninguna política compleja de servicios. Sirve como un agregado para todos los demás componentes de la red de la empresa.

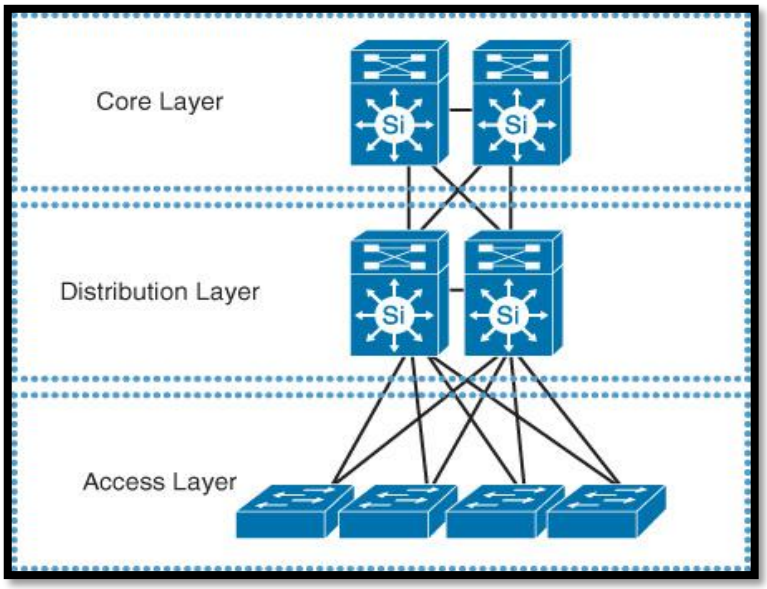

Figura No. 11 Diseño Three Tier. [15]

5.6.2.1 Diseño Two Tier

El modelo Two Tier es recomendado en redes de campus pequeños, cura red tiene algunos departamentos de trabajo en distintos pisos de un mismo edificio. Se debe de considerar escalabilidad futura, expansión y factores que permita la operación eficiente. Este modelo ofrece una solución costo efectiva, al concentrar 2 capas y sus funciones en menos equipos.

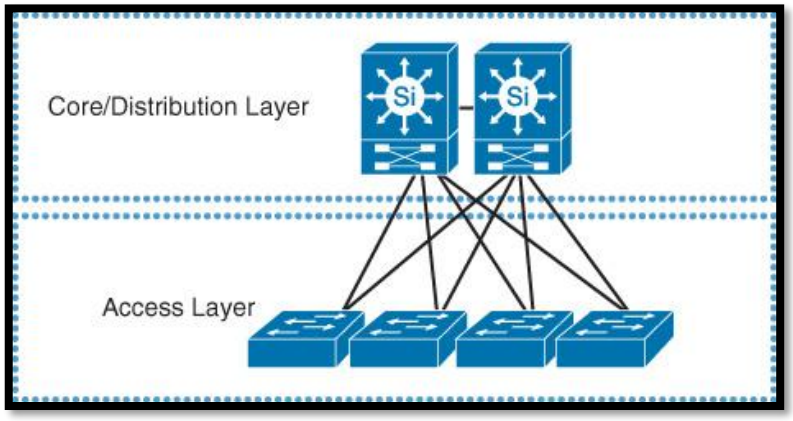

Figura No. 12 Diseño Two Tier. [15]

5.6.3 Infraestructura de red lógica de la casa matriz

Esta estructura de red lógica se diseñó para la casa matriz con el modelo de Three Tier que fue explicado enunciados anteriores, la casa matriz está conformada por la capa de núcleo, la capa de Core de distribución y la capa de acceso.

En la siguiente figura se representó una nube la cual será el enlace que se contrate con los proveedores de internet, se necesita tener dos proveedores para que se brinde una mayor redundancia, teniendo un enlace primario y un enlace secundario, explicando un poco mejor la capa de núcleo se requiere de dos equipos FortiGate para que sea el que reciba el servicio de internet contratado, los FORTINET tendrán una conexión redundante es decir que se prevé que si uno de los dos equipos falla el otro equipo asuma la responsabilidad y finalmente optimiza el tiempo de convergencia al fallar uno de los nodos.

En la siguiente capa, se realizó la conexión del equipo Core con los dos FORTINET de la capa anterior siempre trabajando la redundancia de la red, Sin embargo, es importante destacar que el propósito del Core es el de aislar las fallas y proporcionar conectividad al backbone, por lo cual aislar la capa de distribución y

Core en dos módulos separados crea una clara delineación para cambios que afecten las estaciones finales, data center, WAN y otras partes de la red.

La capa de Core de distribución dependiendo del alcance económico de la empresa en la que se vaya implementar esta práctica se recomienda trabajar con dos equipos Core para una mayor flexibilidad de la red, pero en este caso se trabajó con un solo equipo Core debido a que se tomó como referencias pymes que no cuentan con muchos recursos para implementar dicho diseño con dos Core.

La capa de acceso tiene un enfoque de seguridad física que está conectada al Core de distribución, siendo esta la conexión con los equipos de los usuarios finales que se conectan a la red a nivel de capa dos mejor conocidos como switch de acceso, que estará conectado por medio de cableado a los Access Point que brindaran el acceso a internet de forma inalámbrica.

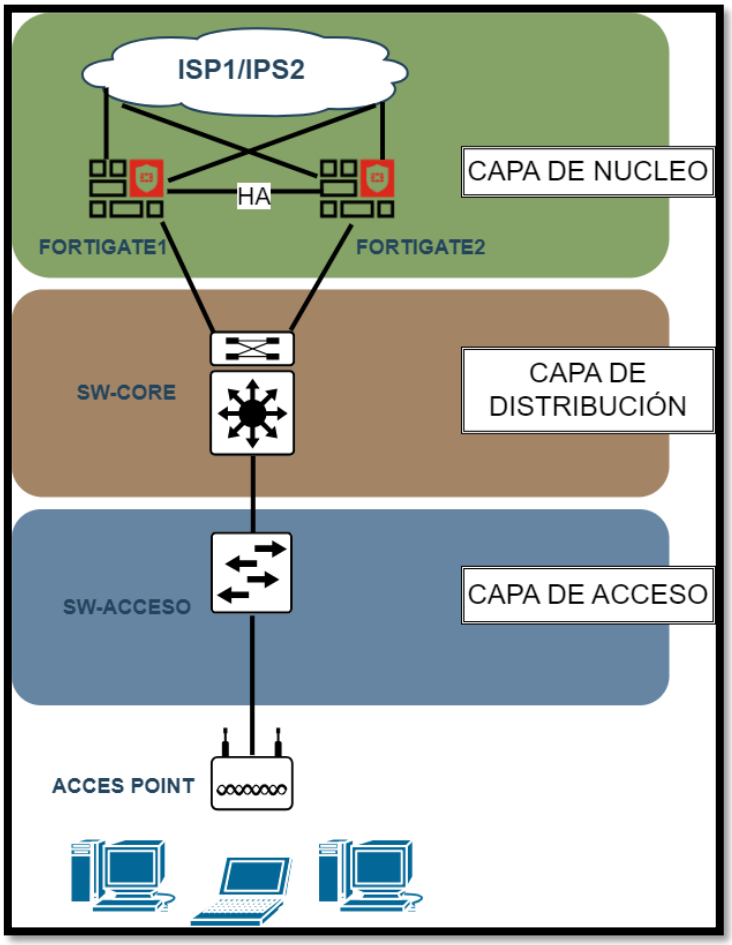

Figura No. 13 Diseño Three Tier Casa Matriz.

5.6.4 Infraestructura de red lógica de las sucursales

Como mejor practica para la conexión de las sucursales, se escogió el diseño de two tier para ambas sucursales, dicha conexiones se explicará a continuación.

La sucursal de Masaya y León utilizara el diseño de two tier, cada sucursal tendrá su propia salida a internet para que realicen su navegación de forma directa sin tener que acceder a los mismos servicios de navegación de la casa matriz. La capa de Core de distribución la asume el equipo FORTINET que se encargara de recibir el enlace de internet que brinde el proveedor de servicios y al mismo tiempo se encargara del enrutamiento a la capa de acceso donde estará conectado el switch por medio de la conexión que se realice con el Access Point para proveer internet a los usuarios finales.

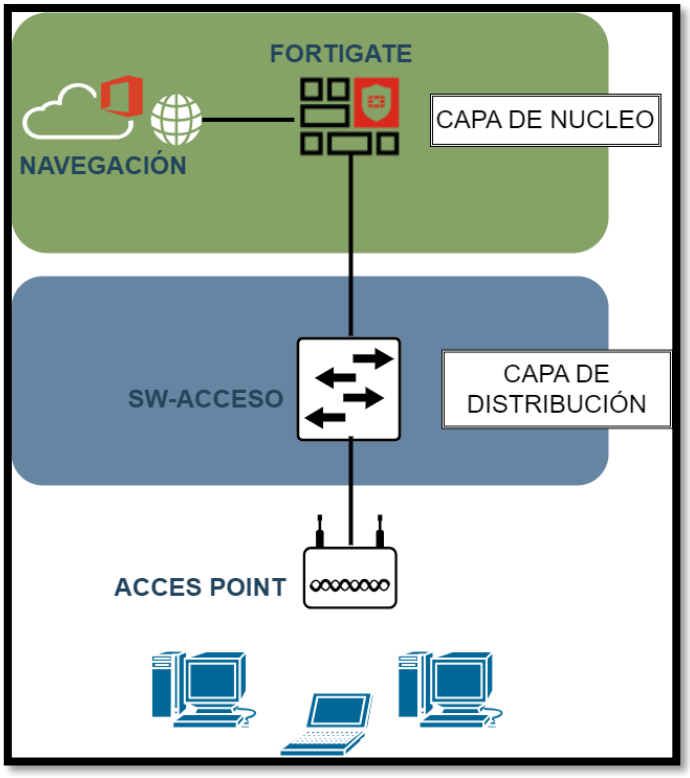

Figura No. 14 Diseño Two Tier para las sucursales.

5.6.4.1 Infraestructura de red lógica a nivel General

Se procedió a detallar la estructura de red lógica General, la cual fue realizada haciendo uso del software libre Draw.io, en donde se muestran las conexiones de los equipos comunicación y seguridad perimetral e interconexión de la casa matriz

hacia sus sucursales. Esta estructura fue elaborada para tener una mayor comprensión de cómo está conformado a nivel lógico, permitiendo la visualización de la interconexión de las sucursales las cuales se encuentran ubicadas en diferentes puntos geográficos del país.

En la sucursal de Masaya, se utilizó el diseño de two tier, debido a la conexión que tiene la sucursal para acceder a los servicios de la casa matriz, por medio de un túnel de VPN.

Igualmente, la sucursal de León se trabajó con el diseño de two tier, en el bloque de la parte superior derecha se observan los equipos que conforman la infraestructura de red de dicha sucursal, la primera capa es la de Core de distribución que se encarga del enrutamiento de la red, para una mayor redundancia de la LAN, la conexión del Core con la capa del switch de acceso para los dispositivos finales de la red de la sucursal.

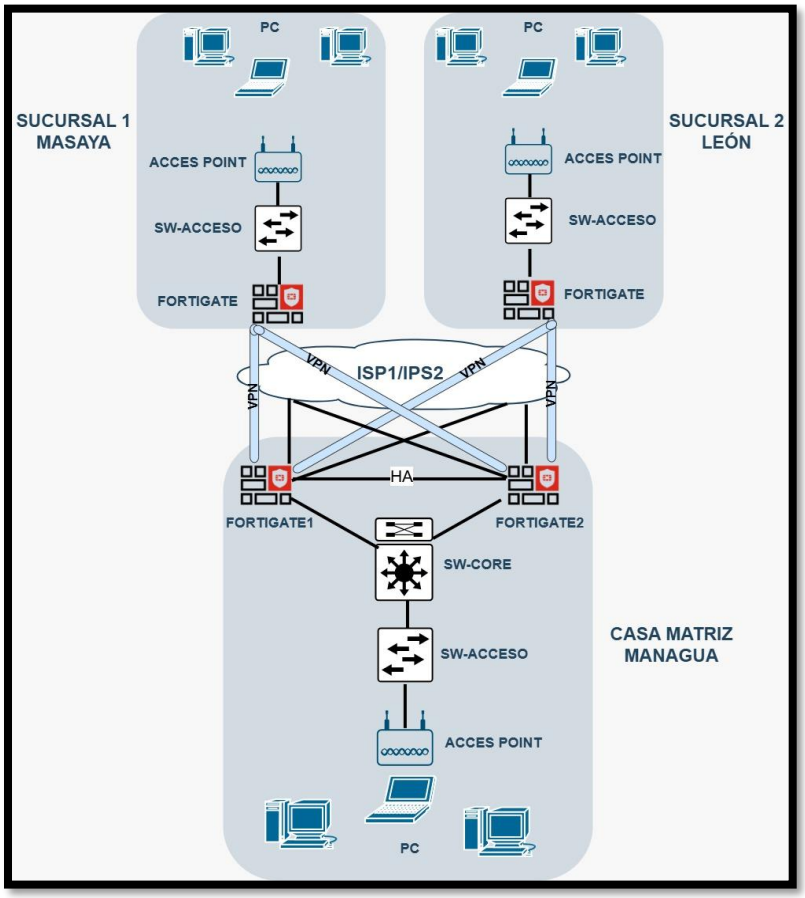

Figura No. 15 Diseño de infraestructura general de la pyme.

5.7 Plano de oficinas casa matriz

En esta figura se muestra el plano de la sede central, Casa matriz que como se comentó anteriormente se encuentra ubicada en el departamento de Managua. En esta oficina al ser la principal, se cuenta con más cantidad de áreas de trabajo, por lo tanto, mayor cantidad de personal y equipos. Siendo más específicos son diez áreas de trabajo desplegadas en diez oficinas diferentes, cada una orientada a un área específica, contando con un total de 22 trabajadores sólo en esta sede.

Con respecto a los equipos, esta cuenta con un total de 22 computadoras distribuidas en todo el personal, además de esto posee un centro de datos, donde se encuentran conectados y configurados los equipos de red encargados de realizar la interconexión entre las sucursales, entre ellos se encuentran: Dos equipos FORTINET, un Switch-Core, un Switch de Acceso y un Access Point.

Figura No. 16 Plano de oficinas Casa Matriz.

5.7.1 Plano de oficinas sucursal Masaya

En esta figura se muestra la sucursal que se encuentra ubicada en el departamento de Masaya, la cual cuenta con una menor cantidad de áreas de trabajo en comparación con la Sede Central Managua, teniendo un total de cinco áreas de trabajo y un total de 6 trabajadores.

Con respecto a los equipos, esta sucursal cuenta con seis computadoras y un centro de datos en donde se encuentran: 1 FORTINET, 1 Switch de Acceso y 1 Access Point.

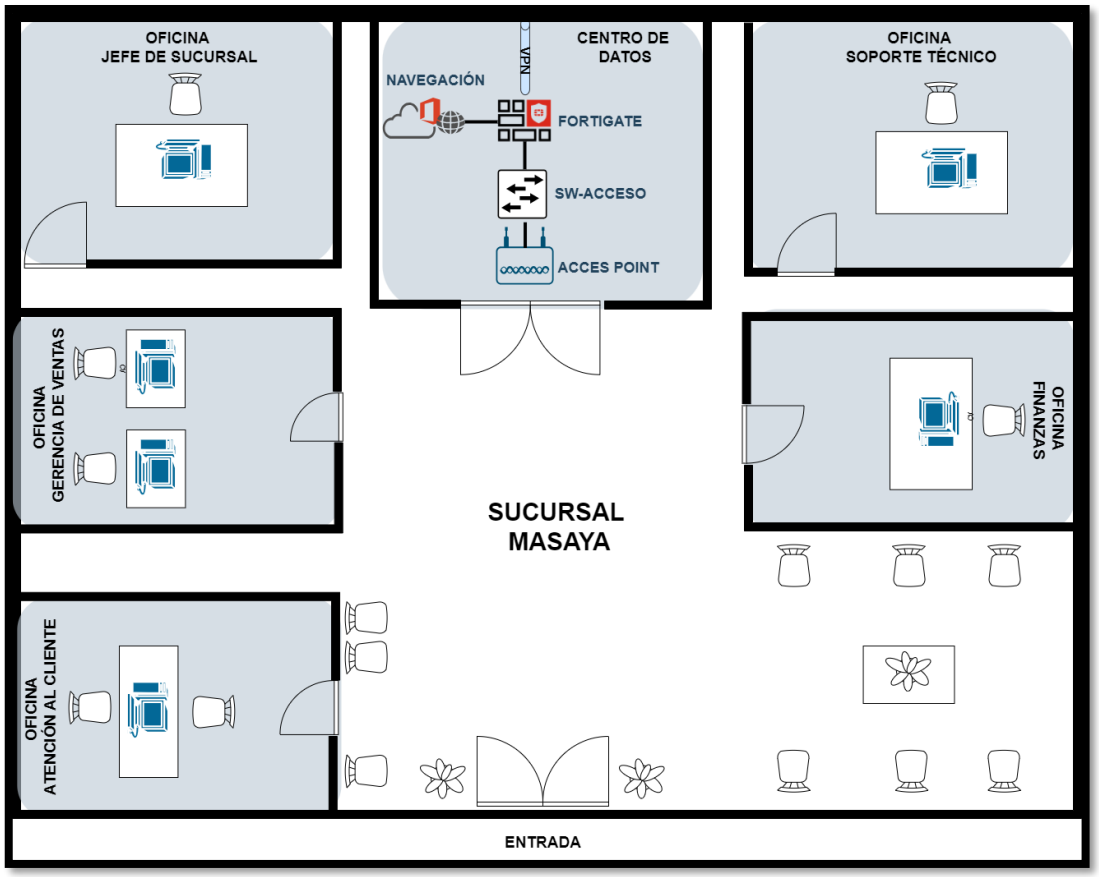

Figura No. 17 Plano de oficinas sucursal Masaya.

5.7.2 Plano de oficinas sucursal León

En la siguiente figura se muestra representación de la oficina de la sucursal que se encuentra ubicada en el departamento de León municipio de León, en donde se observa que esta cuenta con 5 áreas de trabajo lo que conlleva a un total de 6 trabajadores.

Con respecto a los equipos, esta oficina posee un total de 6 computadoras distribuidas en todo el personal de la sucursal, además de que esta cuenta con un centro de datos en el cual se encuentran interconectados los siguientes equipos, tales como: 1 FORTINET, 1 Switch de Acceso y 1 Acces Point.

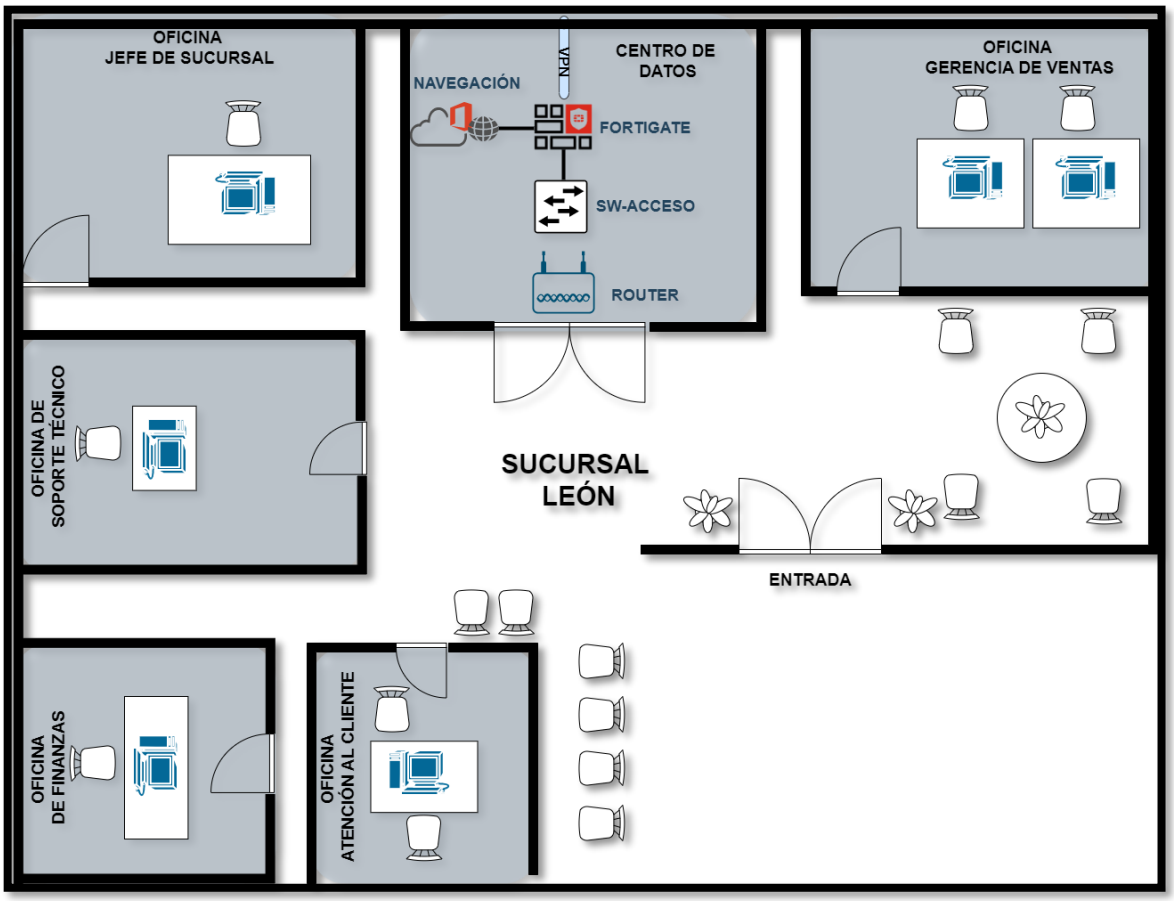

Figura No. 18 Plano de oficinas sucursal León.

5.8 Localización y Evaluación de Sitios

Para llevar a cabo este apartado fue de suma importancia la utilización del método aplicativo cuantitativo, porque se realizó una investigación del tipo de tecnología con respecto a la cobertura que se ofrece en la zona en donde se encuentran ubicada tanto la Sede Central, como sus sucursales.

El Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR) es el «Ente Regulador» de los servicios de telecomunicaciones y servicios postales, una institución estatal, la cual tiene como funciones la normación, regulación, planificación, técnica, supervisión, aplicación y el control del cumplimiento de las leyes y normas que rigen la instalación, interconexión, operación y prestación de los servicios de telecomunicaciones y servicios postales. [16]

Por lo antes mencionado se procedió a realizar la evaluación y ubicación de los sitios en donde se encuentran ubicada la Cede Central y las sucursales, este procedimiento se elaboró haciendo uso de del software libre de escritorio de Google Earth, ya que este no facilito en gran manera la demostración de la ubicación; además de las coordenadas exactas de estas mismas, las cuales se procedieron a documentar y demostrar mediante figuras en los apartados siguientes.

Figura No. 19 Ubicación globalizada de la pyme y sucursales

5.8.1 Sucursal del departamento de Managua

Ubicación: La casa matriz de la pyme queda ubicada en el departamento de Managua municipio de Managua, específicamente en el Km 8.5 carretera a Masaya, de la entrada principal a las sierritas de santo Domingo 200 mts al oeste. Además de esto se procedió a obtener las coordenadas geográficas las cuales son: 12°05'31"N 86°14'21"W, obtenidas haciendo uso del software Google Earth.

Figura No. 20 Ubicación de Sede Central PYME departamento de Managua.

5.8.2 Sucursal del departamento de Masaya

Ubicación: La sucursal de Masaya se encuentra ubicada, de la Iglesia San Jerónimo Masaya, 2 cuadras al oeste 1 cuadra al sur. Las coordenadas son las siguientes: 11°58'40"N 86°05'59"W, igualmente obtenidas mediante el software Google Earth.

Figura No. 21 Ubicación de Sucursal del departamento de Masaya.

5.8.3 Sucursal del departamento de León

Ubicación: La pyme sucursal León se encuentra ubicada en del parque San Juan 2 cuadras al norte enfrente al café Gourmet, oficina esquinera; las coordenadas son las siguientes: 12°26'32.4"N 86°52'33.7"W. Estas de igual forma obtenidas haciendo uso del software Google Earth.

Figura No. 22 Ubicación de Sucursal del departamento de León.

5.8.4 Evaluación de Proveedores de Internet

Se continuó a revisar mediante la página de TELCOR, a los encargados de proveer servicios de telecomunicaciones en Nicaragua, de esta manera se inició una investigación más exhaustiva de los detalles de servicios que ofrece cada uno de estos, lo que conllevo a la delimitación y selección de 3 proveedores de servicios seleccionados, esto tomando en cuenta diferentes parámetros evaluados como lo son: precio, cobertura, calidad y fiabilidad, lo que conllevo a determinar selección de los siguientes proveedores, los cuales son: CLARO, TIGO y ENATREL, la evaluación que se llevó a cabo se presenta a continuación de forma detallada, además de haciendo uso de imágenes de referencias.

5.8.4.1 Departamento de Managua

En el departamento de Managua es donde se encuentra ubicada la sede central Pyme, así que se empezó a realizar una investigación en la página de TELCOR, para obtener información de los servicios tecnológicos a los cuales se tiene acceso en esta zona, con respecto a los 3 proveedores de servicios que fueron anteriormente seleccionados.

- **Proveedor CLARO departamento Managua**

En la siguiente figura obtenida por TELCOR muestra mediante un mapa la ruta de fibra óptica de CLARO, en esta se observa que un nodo sale de villa fontana hasta Masaya, teniendo cobertura en el sector de las sierritas de santo domingo, zona donde se encuentra ubicada la sede central.

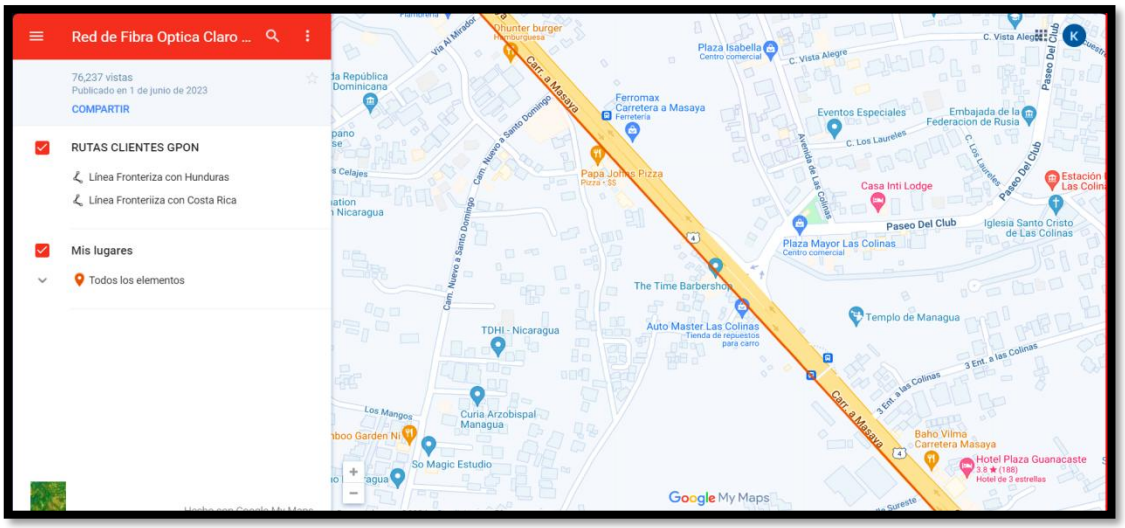

Figura No. 23 Ruta de F.O CLARO cerca de la casa matriz Managua. [17]

- **Proveedor ENATREL departamento Managua**

En la siguiente figura se observa la ruta de la fibra óptica de ENATREL que sale del nodo Centroamérica hacia el sitio Ticuantepe, teniendo cobertura en el sector de las sierritas de santo domingo, se señala la ubicación del edificio de la sede central, la línea morada es la ruta del hilo de fibra óptica.

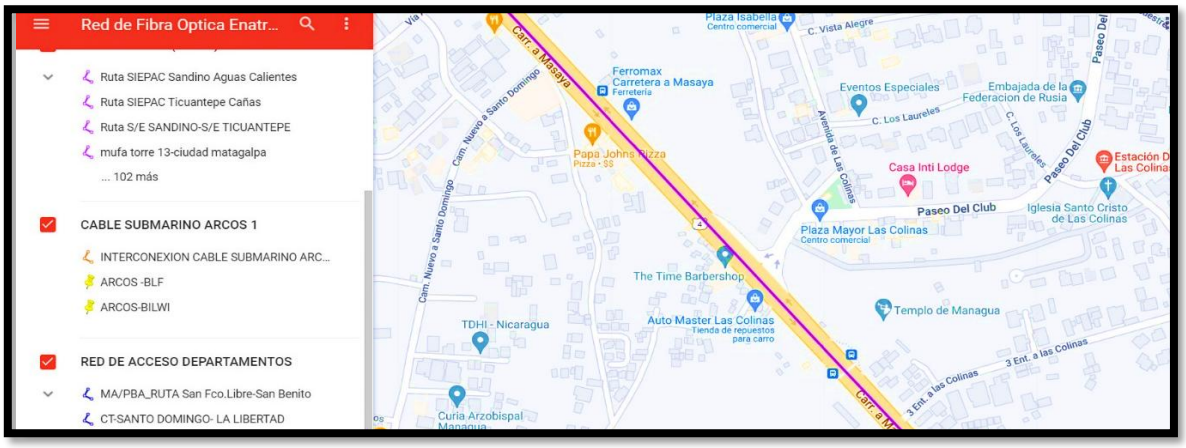

Figura No. 24 Ruta de F.O ENATREL cerca de la casa matriz Managua. [17]

- **Proveedor TIGO departamento Managua**

En la figura se muestra el mapa de cobertura de fibra óptica brindado por la página oficial de TELCOR, en este se observa como el proveedor de servicios Tigo, cuenta con mayor cantidad de hilos de fibra que pasan por la zona, los cuales se encuentra representados por las líneas de color azul.

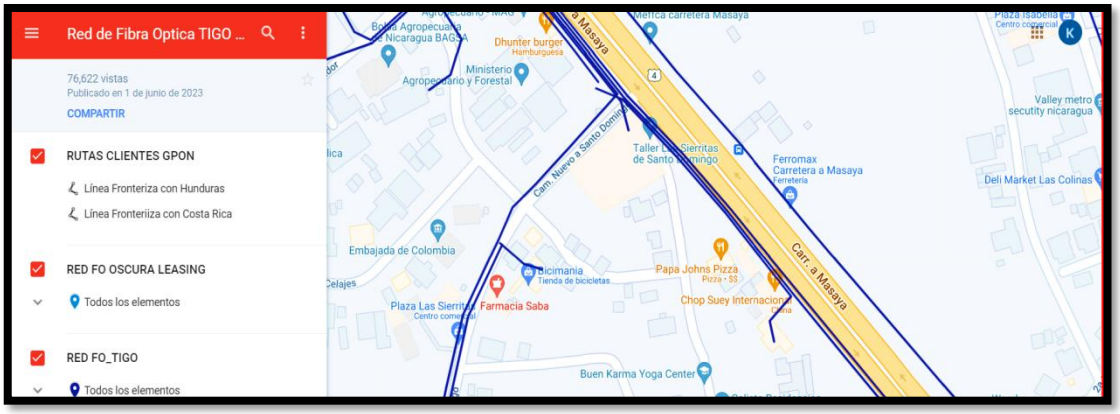

Figura No. 25 Ruta F.O de TIGO cerca de la casa matriz Managua. [17]

- **Acceso a Internet Departamento De Managua**

En la siguiente figura obtenida de un apartado de la página de TELCOR, en el cual se muestra la cobertura de acceso a internet a nivel nacional, por lo tanto, en el estudio de campo se centró en el departamento de Managua en donde se encuentra ubicada la Casa Matriz, donde se logra observar la presencia de diversos proveedores de internet que tienen presencia en este departamento. Donde se confirmó que se cuenta con la presencia de los proveedores anteriormente seleccionados.

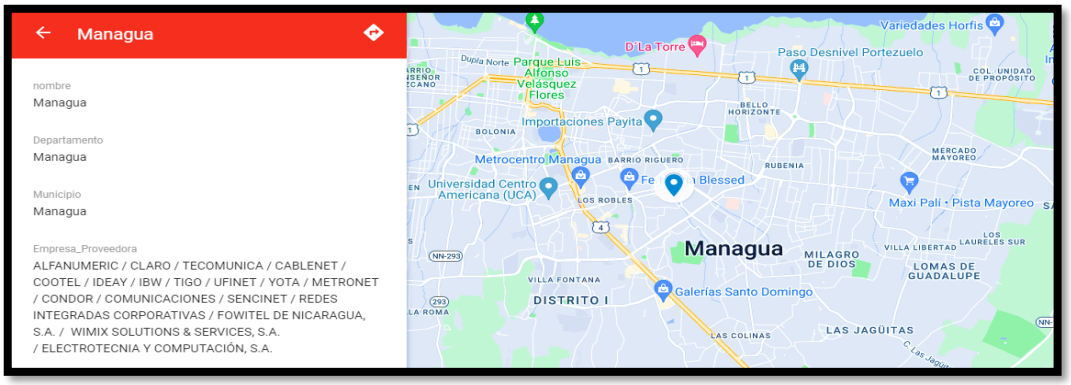

Figura No. 26 Cobertura de acceso de internet cerca de la casa matriz. [17]

5.8.5 Departamento de Masaya

- **Proveedor CLARO departamento Masaya**

Se dio inicio a realizar de igual forma la investigación en la página de TELCOR, con respecto a la sucursal ubicada en el departamento de Masaya, en donde se observa que se tiene acceso a un hilo de fibra en la zona donde se encuentra ubicada la sucursal. Este hilo de fibra se encuentra representado mediante la línea de color naranja.

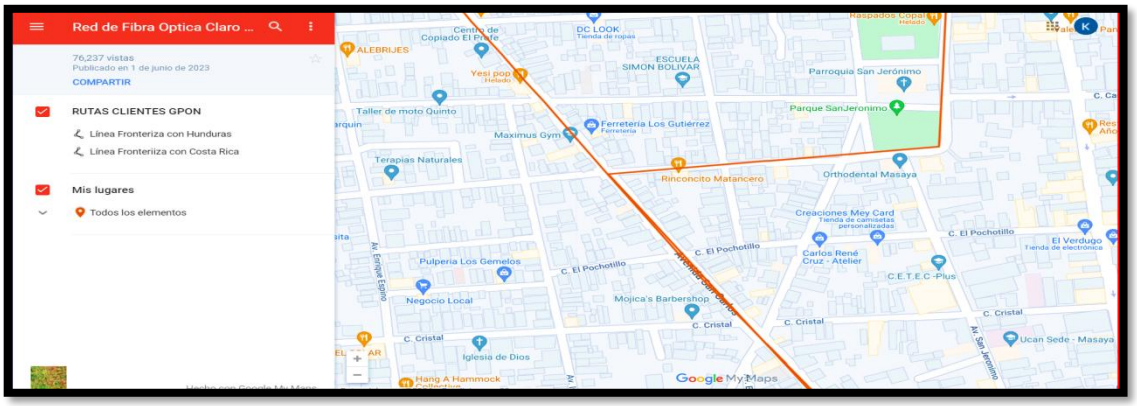

Figura No. 27 Ruta de F.O CLARO cerca de la sucursal de Masaya. [17]

- **Proveedor ENATREL departamento Masaya**

Con respecto al proveedor de servicios de ENATREL, se logró observar en la figura que no se cuenta con un hilo de fibra que pase por la zona donde se encuentra ubicada la sucursal de Masaya, y el hilo más cercano es el que tiene la ruta del parque los Leones a la Alcaldía de Masaya en donde pasa un cable de fibra óptica ADSS Monomodo Core de 48 hilos, representado por una línea morada.

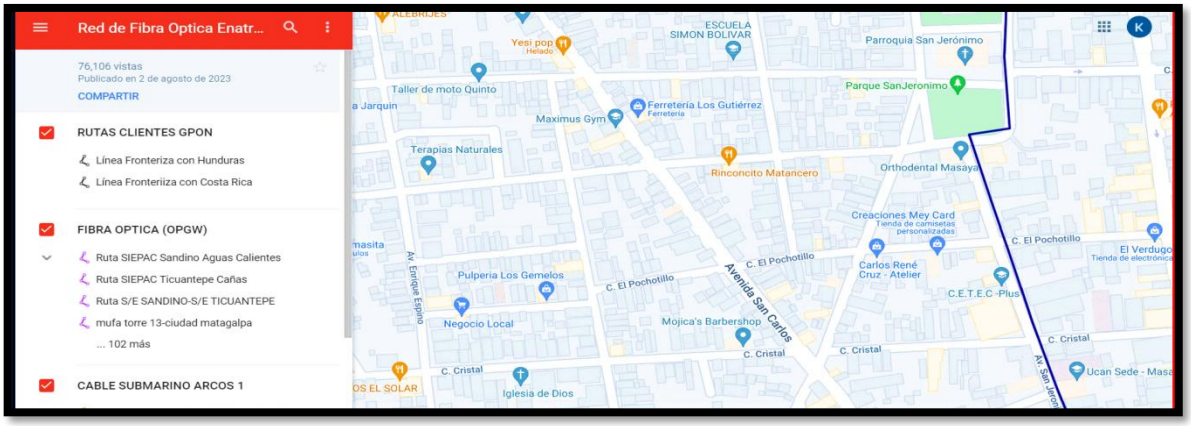

Figura No. 28 Ruta de F.O ENATREL cerca de la sucursal de Masaya. [17]

- **Proveedor TIGO departamento MASAYA**

En la siguiente figura obtenida con respecto al proveedor de servicios Tigo en el mapa de TELCOR se muestra que estos no cuentan con ningún hilo de fibra en la zona central del Sector de la sucursal y el hilo de fibra más cercano únicamente pasa por la carretera Masaya-Managua, el cual se encuentra alejado por varios kilómetros de donde se encuentra ubicada esta sucursal.

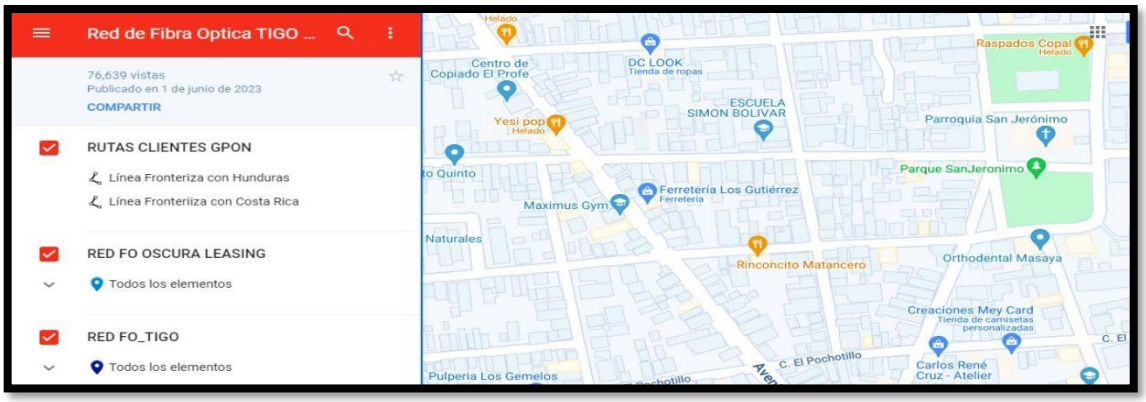

Figura No. 29 Ruta de F.O CLARO cerca de la sucursal de Masaya. [17]

- **Acceso a Internet Departamento De Masaya**

En esta figura se observa que en el departamento de Masaya cuenta con diferentes proveedores de servicio, cabe mencionar que a comparación del departamento de Managua; este cuenta con una menor cantidad empresas de acceso a internet, pero de igual forma este cuenta con la presencia de los proveedores de servicios anteriormente seleccionados.

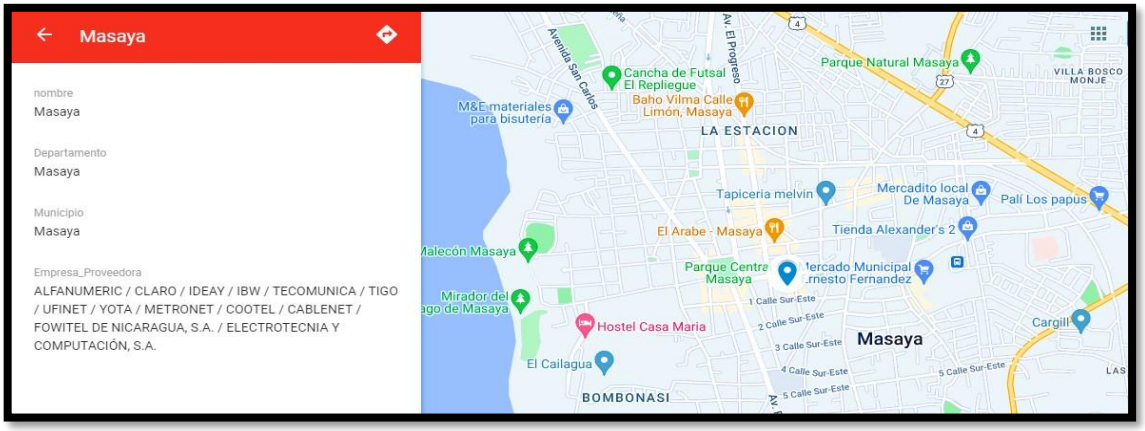

Figura No. 30 Cobertura móvil departamento de Masaya. [17]

5.8.6 Departamento de León

- **Proveedor CLARO departamento León**

En la figura se logra observar como el proveedor de servicio de la empresa Claro, posee un hilo de fibra óptica el cual pasa exactamente por la calle en donde se encuentra ubicada la sucursal del departamento de León, este se encuentra representado mediante una línea de color naranja.

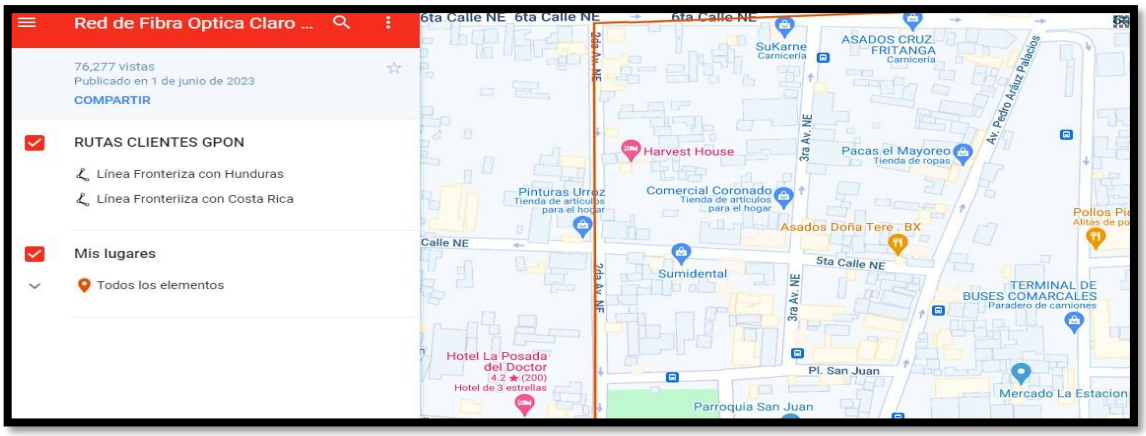

Figura No. 31 Ruta de F.O CLARO cerca de la sucursal de León. [17]

- **Proveedor ENATREL departamento León**

De igual forma, haciendo uso del mapa de fibra por proveedores brindado por la página de TELCOR, se demuestra como el proveedor de servicios ENATREL, posee un hilo de fibra que pasa por la calle donde se encuentra ubicada la sucursal de León, el cual se encuentra representado por una línea de color morado.

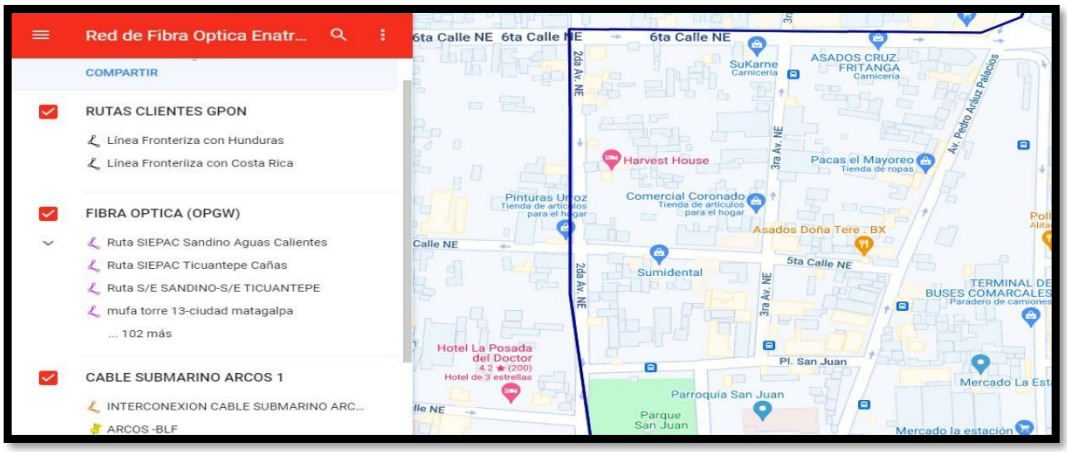

Figura No. 32 Ruta de F.O ENATREL cerca de la sucursal de León. [17]

- **Proveedor TIGO departamento León**

En la siguiente figura se mostró como de igual forma el proveedor de servicios de la empresa Tigo, cuenta con un hilo de fibra que pasa por la zona en donde se encuentra ubicada la sucursal de este departamento. Este está representado por una línea de color celeste.

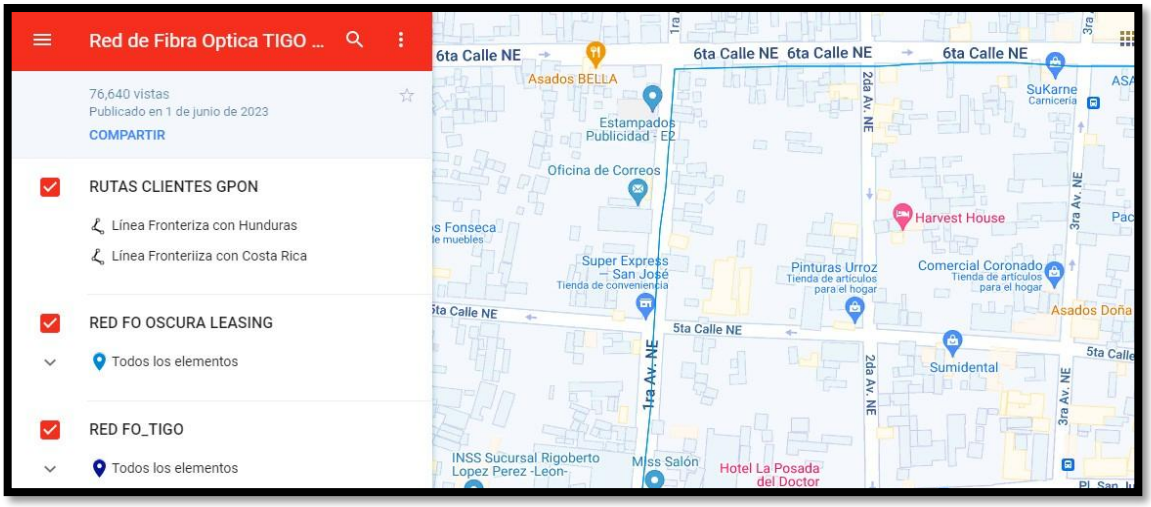

Figura No. 33 Ruta de F.O TIGO cerca de la sucursal de León. [17]

- **Acceso a Internet Departamento De León**

En la siguiente figura se determina que el departamento de león, igualmente cuenta con proveedores de servicio que brindan el acceso a internet, haciendo presencia, de igual forma los tres proveedores de servicio anteriormente seleccionados como lo son las empresas de telecomunicaciones: Claro, Tigo y ENATREL.

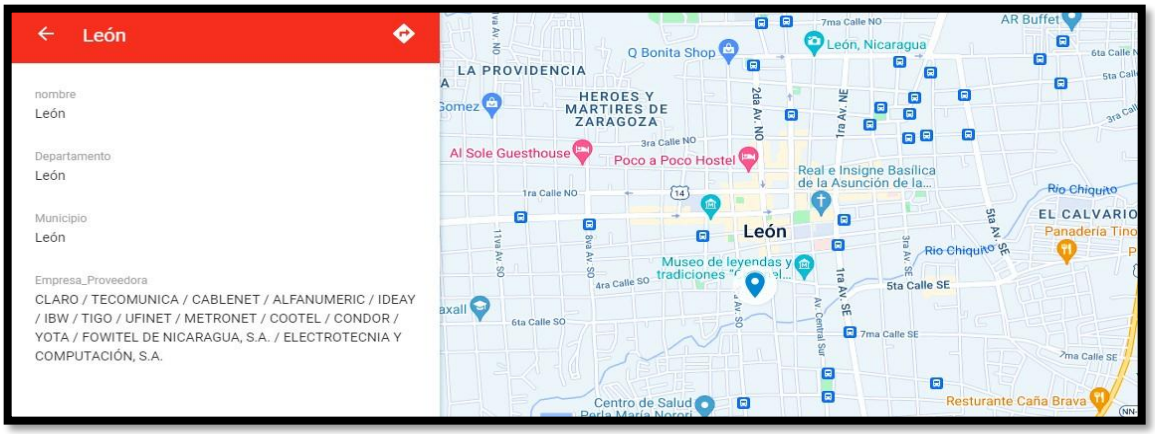

Figura No. 34 Cobertura móvil cerca de la sucursal de León. [17]

5.9 Propuesta de Equipos

Luego de haberse realizado las investigaciones anteriores y tomando en cuenta todos los datos obtenidos; se procedió con la propuesta de equipos de red, los cuales fueron específicamente escogidos tomando en cuenta las características y capacidades de estos, este proceso se realizó con el fin de garantizar que los equipos luego seleccionados cumplan con las funciones requeridas y el objetivo de garantizar una red segura, robusta y escalable de la interconexión de la sede central con sus sucursales.

Para este paso, se tomaron en cuenta tres marcas de proveedores de equipos de redes, los cuales son: FORTINET, Cisco, Aruba y Ubiquiti Unifi, esto para realizar y brindar propuestas que seas viables y den solución al diseño de interconexión de la pyme, haciendo uso tanto de equipos robustos y costosos como también de equipos un poco menos robustos y económicos y de esta manera brindar una variedad en la solución que se adapte tanto a las necesidades como a la economía de la pyme.

5.9.1 Equipos Propuestos en Sucursal Central Managua

Se inició detallando los equipos propuestos de la sucursal ubicada en el departamento de Managua, para realizar la propuesta de diseño de interconexión de la red. Para esta sucursal al ser la sede central, se tomó en cuenta datos anteriormente mencionados ya que esta sucursal cuenta con la mayor cantidad de áreas de trabajo, por consiguiente, más trabajadores; lo que conlleva a una mayor cantidad de dispositivos conectados a la red, incrementando el flujo y demanda de esta misma.

Es por ello que se realizó la selección de los siguientes equipos, ya que estos cumplen con los requisitos necesarios para cumplir con el objetivo y las funciones establecidas además de brindar estabilidad en la red y escalabilidad a tiempo futuro.

5.9.1.1 Propuesta de Equipo Firewall para Casa Matriz

Para realizar la selección de la mejor opción del equipo a proponer como Firewall de la casa matriz, se elaboró una tabla comparativa de las tres marcas seleccionadas las cuales son FortiGate, Ubiquiti y Cisco, cada una con un modelo especifico donde se buscó que las características de sus interfaces de cada uno de estos cumplan con las necesidades requeridas de la casa matriz.

Tabla 19 Precio de Equipos Firewall Casa Matriz.

Precio de Equipos Firewall		
Fortigate: 60F	**Ubiquiti Unifi: Dream Machine (UDM)**	**Cisco: ASA 5506X**
C$ 35, 000 a 40,000	C$ 30,000 a 40,000	C$ 35,000 a 40,000

Tabla 20 Cuadro comparativo Firewall.

Firewall – Casa Matriz		
Marcas		
FortiGate	**Ubiquiti UniFi**	**Cisco**
Modelo: 60F	**Modelo: Dream Machine (UDM)**	**Modelo: ASA 5506X**
Especificaciones Este firewall proporciona un conjunto completo de funciones de seguridad, lo que lo hace ideal para entornos exigentes. Su interfaz es fácil de configurar y cuenta con una línea de comandos para administradores avanzados. • 1 Puerto USB • 1 Puerto de Consola • 2 Puertos RJ45 WAN 10/100/1000Mbps • 1 Puerto RJ45 DMZ 10/100/1000Mbps • 2 Puertos RJ45 Fortilink 10/100/1000Mbps • 5 Puertos RJ45 LAN **Consumo energético:** • Tensión de alimentación: 12 V DC, 3 A. • Consumo de potencia (promedio / máximo): aproximadamente 17 W / 18.5 W.	**Especificaciones** Sencillo y accesible, ideal para pequeñas y medianas empresas que buscan una solución integrada. • Combina el nuevo sistema operativo UniFi con un swith de 8 puertos. • UniFi Protect NVR con soporte estándar para HDD de 3.5. • Switch de 8-puertos Gigabit con 1 Gbps RJ45 y 10G SFP+ LAN. IP/IDS, DPI. **Consumo energético:** • Consumo máximo de energía: 26 W. Rango de tensión soportado: 100-240 V AC	**Especificaciones** Robusto y versátil, diseñado para empresas que requieren un alto nivel de seguridad y gestión compleja. • Rendimiento de firewall 750 Mbit/s • Rendimiento IP/IDS 125 Mbit/s • Número máximo de conexiones de firewall 50000 • Número máximo de conexiones firewall por segundo 5000. **Consumo energético:** • Consumo máximo de energía 60 W.

5.9.1.2 Propuesta de equipo Switch de Acceso - Casa Matriz

Se realizó una investigación de diferentes modelos de Switches de acceso, con respecto a las tres marcas planteadas anteriormente. Estos modelos fueron seleccionados, tomando en cuenta sus especificaciones de la interfaz del equipo, con el objetivo de que cumplan con los requerimientos de las necesidades de la sucursal.

Tabla 21 Precios de equipos.

PRECIOS DE EQUIPOS SWITCH DE ACCESO		
CISCO: C9200L-48P-4x	**ARUBA: 2540 48G POE+ 4SFP+**	**UBIQUITO UNIFI: PoE+ Administrable de 48 puertos**
C$ 150,000 a 200,000	C$ 60,000 a 100,000	C$ 50,000 a 70,000

Tabla 22 Cuadro comparativo SW-L2.

Switch de Acceso – Casa Matriz		
MARCAS		
CISCO	**ARUBA**	**UBIQUITI UNIFI**
Modelo: C9200L-48P-4x	**Modelo: 2540 48G POE+ 4SFP+**	**Modelo: Switch PoE+ Administrable de 48 puertos**
Especificaciones • 48 puertos PoE+ apilables de 10/100/1000 Mbps (Ethernet). • 4 puertos SFP28 (10G) para conexiones de fibra. • Sistema operativo Cisco IOS XE. • Protección contra ataques como DHCP Snooping y Dynamic ARP Inspection. • Soporte para VLANs, VTP, STP y Rapid PVST+. **Consumo energético:** ·Presupuesto máximo de alimentación PoE Activa de 1440 W para los 48 puertos en modo PoE+. Un consumo base estimado de 70 a 80 W (sin PoE activa)	**Especificaciones** • 48 puertos de 10/100/1000 Mbps (RJ-45). • 4 puertos SFP+ para conectividad de fibra óptica de 10 Gbps. • Protección contra ataques como DHCP snooping y Dynamic ARP Inspection. • Especialmente útil para entornos que necesitan un alto presupuesto de PoE y una gestión de red simplificada. **Consumo energético:** Presupuesto de alimentación PoE+: hasta 370 W para los puertos PoE+.	**Especificaciones** • 48 puertos RJ-45: 10/100/1000 Mbps (Ethernet), todos soportan PoE. • 4 puertos SFP+: 10 Gbps para conexiones de fibra. • Soporta IEEE 802.3at (PoE+) y IEEE 802.3bt (PoE++), permitiendo hasta 60W por puerto. **Consumo energético:** ·Consumo máximo excluyendo la salida PoE: 45 W. Consumo máximo incluyendo la salida PoE: 240 W.

5.8.1.3 Equipo Switch Core Casa Matriz

De igual forma se realizó un cuadro comparativo de los modelos de equipos propuestos de las tres marcas: Cisco, Aruba y Ubiquiti. Siempre tomando en cuenta que los modelo cuenten con características similares en sus interfaces con el objetivo de que cumplan con las necesidades de la red de la casa matriz.

Tabla 23 Precios de equipos switch core.

PRECIOS DE EQUIPOS SWITCH CORE		
CISCO: C9300L-48P-E	**ARUBA: 3810M**	**UBIQUITI: USW-Pro-48-POE**
C$ 20,000 a 40,000	C$ 20,000 a 30,000	C$ 40,000 a 60,000

Tabla 24 Cuadro comparativo SW-L3.

Switch de Core – Casa Matriz		
MARCAS		
CISCO	**ARUBA**	**UBIQUITI**
Modelo: C9300L-48P-E	**Modelo: 3810M**	**Modelo: USW-Pro-48-POE**
Especificaciones • Capacidad de switching: Hasta 176 Gbps. • Capacidad de reenvío: Hasta 130 Mpps. • Soporta up to 1.2 Tbps en configuraciones apiladas. • 48 puertos de 10/100/1000 Mbps (RJ-45). • 4 puertos SFP+ (10G). • Ideal para entornos empresariales donde se requiere alta disponibilidad, **Consumo energético**: • Consumo estimado de PoE inactivo es de 60.40 W. Consumo estimado de PoE activos es de: 505 W.	**Especificaciones** • Capacidad de switching: Hasta 128 Gbps. • Capacidad de reenvío: Hasta 95 Mpps. • 48 puertos de 10/100/1000 Mbps (RJ-45) en el modelo estándar. • Módulos intercambiables que permiten la inclusión de puertos SFP/SFP+ adicionales. **Consumo energético:** • La fuente 250 W) para versiones sin PoE. • La fuente PoE+ permiten hasta 370 W de PoE.	**Especificaciones** • 48 puertos RJ-45: 10/100/1000 Mbps (Ethernet) que soportan PoE+ (802.3af/802.3at). • 2 puertos SFP: Para conectividad de fibra óptica. • Presupuesto total de PoE: Hasta 500W • Soporta VLANs, Spanning Tree Protocol (STP) y Link Aggregation Control Protocol (LACP). • Capacidad de switching: Hasta 70 Gbps. **Consumo energético:** • Consumo máximo (Con la salida PoE inactiva): 60 W. Consumo máximo total (incluyendo la salida PoE Activas): 660 W.

5.9.1.4 Propuesta de Equipo Access Point Casa Matriz

También se realizó una tabla comparativa de tres modelos de Access Point, continuando con las mismas marcas anteriormente seleccionadas, con la finalidad de seleccionar la mejor, para propuesta de la casa matriz.

Tabla 25 Precios de equipos AP.

PR ⁝CIOS DE EQUIPOS ACCESS POINT		
CISCO: 9120	**ARUBA: JX945A**	**UBIQUITI: 2X2 WI-FI 6 1.5 GBPS**
C$ 40,000 a 60,000	C$ 10,000 a 15,000	C$ 10,000 a 20,000

Tabla 26 Cuadro comparativo AP.

Access Point – Casa MatrizD2:F6		
MARCAS		
CISCO	**ARUBA**	**UBIQUITI UNIFI**
Modelo: 9120	**Modelo: JX945A**	**Modelo: 2×2 Wi-Fi 6 1.5 Gbps**
Especificaciones • Tecnología: Wi-Fi 6 (802.11ax) • Bandas: Doble banda (2.4 GHz y 5 GHz). • Antenas: Múltiples antenas para mejorar la cobertura y el rendimiento. • Soporta PoE+ (802.3at). • Capacidad de IoT y soporte para un gran número de dispositivos conectados. **Consumo energético:** • Con PoE+ activo: el consumo máximo es 25.5 W. Con “PoE inactivo” (sin energía suficiente): el consumo operativo baja a 13.4 W	**Especificaciones** • Tecnología: Wi-Fi 6 (802.11ax) • Bandas: Doble banda (2.4 GHz y 5 GHz) • Velocidad: Hasta 2.4 Gbps en total (con 4x4 MU-MIMO en 5 GHz). • Soporta WPA3,802.1X. • Diseño compacto, fácil de instalar en varios entornos. **Consumo energético:** • Consumo máximo alimentado por fuente de corriente continua (DC) directa: ≈ 11 W. En modo inactivo (idle), el consumo cae a ≈ 3.7 W con PoE o ≈ 2.6 W con DC.	**Especificaciones** • Conectividad: 2x2 MIMO • Velocidad máxima: Hasta 1.5 Gbps • Radios: • 5 GHz: MU-MIMO y OFDMA • 2.4 GHz: MIMO • Puertos: 1 x 10/100/1000 Mbps Ethernet • Alimentación: PoE (Power over Ethernet) • Antenas: Antena interna de alta ganancia **Consumo energético:** • Este equipo realiza un consumo máximo en Poe activo de 12 W.

5.9.2 Equipos Propuestos Sucursal Masaya y León

Para realizar una buena selección de marcas y modelos de equipos tanto de la sucursal León como de Masaya, igual se elaboró un cuadro comparativo tomando siempre las marcas anteriormente seleccionadas para la casa matriz, esto con el fin de garantizar una correcta infraestructura de la red.

5.9.2.1 Propuesta de equipo FIREWALL para ambas sucursales

Tabla 27 Equipos de Firewall.

PRECIOS DE EQUIPOS FIREWALL		
FortigGate 40F	**UBIQUITI UNIFI: EDGErOUTER 6 POE PASIVO 24 V**	**CISCO: CATALYST 9800L**
C$ 40,000 a 55,000	**C$ 25,00 a 30,000**	**C$ 40,000 a 60,000**

Tabla 28 Cuadro comparativo Firewall para ambas sucursales.

Firewall– Masaya y León		
MARCAS		
FORTINET	**UBIQUITI UNIFI**	**CISCO**
Modelo: FortiGate 40F	**Modelo: EdgeRouter 6 PoE Pasivo 24 V**	**Modelo: Catalyst 9800-L**
Especificaciones • CPU: SoC de seguridad de FORTINET. • Memoria: 4 GB de RAM. • Almacenamiento: 32 GB de almacenamiento flash. • Rendimiento de Firewall: Hasta 5 Gbps • Rendimiento de IP: Hasta 2 Gbps • Rendimiento de Antivirus: Hasta 1.5 Gbps • Rendimiento de VPN (IPSec): Hasta 1.6 Gbps • 2 puertos WAN • 8 puertos LAN • 1 puerto de gestión • 1 puerto de consola **Consumo energético:** El consumo energético máximo es de 13.4 W	**Especificaciones** • CPU: Quad-Core de 1 GHz • Memoria: 1 GB de RAM • Almacenamiento: 256 MB de almacenamiento. • Rendimiento de Firewall throughput: 1 Gbps. • 5 puertos Gigabit Ethernet (10/100/1000 Mbps) • 1 puerto SFP (1 Gbps) • Soporte para PoE pasivo (24V) en puertos 1-4 **Consumo energético:** Con PoE inactivo un consumo promedio de 13 a 16 W. Con PoE activo: de 30 a 80 W, dependiendo de equipos conectados	**Especificaciones** • CPU: Procesador de arquitectura de 64 bits • Memoria: 4 GB de RAM (opcional hasta 16 GB) • Almacenamiento: 8 GB de almacenamiento interno. • 2 puertos de red 10/100/1000 Mbps • 2 puertos SFP (1 Gbps) • 1 puerto USB • 1 puerto de gestión (RJ-45) • 1 puerto de consola (RJ-45) • Funciones avanzadas de seguridad y control de acceso. **Consumo energético:** El consumo promedio de este equipo es de entre 60 a 70 W.

5.9.2.2 Propuesta de equipo Switch de Acceso para ambas sucursales

Para la selección del modelo propuesto del switch de acceso, también se creó una tabla comparativa de las características de las interfaces de estos, pero esta vez adaptados a las necesidades de la red de las sucursales.

Tabla 29 Switch de Acceso Masaya y León.

Switch de Acceso – Masaya y León		
MARCAS		
CISCO	**ARUBA**	**UBIQUITI UNIFI**
Modelo: C9200-24P-4X-E	**Modelo: Switch 2540 24G POE+ 4SFP+**	**Modelo: PoE UniFi capa 2 Administrable de 26 puertos**
Especificaciones • Número de puertos: 24 puertos Ethernet 10/100/1000 (Gigabit) • Puertos PoE: 24 puertos PoE+ (802.3at) • Capacidad de conmutación: Hasta 128 Gbps • Rendimiento de reenvío: Hasta 95.2 Mpps (millones de paquetes por segundo) • Puertos SFP: 4 puertos SFP+ (10G) • Características de software: Cisco IOS XE, incluye capacidades de automatización y seguridad avanzadas • Apilamiento: Soporta apilamiento de hasta 8 switches • Dimensiones: 1U (altura estándar de rack) • Alimentación: Soporte para red de energía (PoE) y redundancia de alimentación • Gestión: Acceso a través de CLI, SNMP, o GUI basada en web **Consumo energético:** Con PoE inactivo su consumo es de: 50 w. Con PoE activo su consumo aproximado es de 420 W.	**Especificaciones** • Número de puertos: 24 puertos Ethernet 10/100/1000 (Gigabit) • Puertos PoE: 24 puertos PoE+ (802.3at) • Capacidad de conmutación: 56 Gbps • Rendimiento de reenvío: Hasta 41.66 Mpps • Puertos SFP: 4 puertos SFP+ (10G) • Características de software: ArubaOS con gestión basada en web y CLI • Apilamiento: Soporta apilamiento de hasta 8 switches • Alimentación: Soporte para redundancia de alimentación • Gestión: Acceso a través de la interfaz gráfica de Aruba Central o CLI. **Consumo energético:** Consumo con puertos inactivos es de 36.8 W. Con cantidad de puertos total activos es de 370 W.	**Especificaciones** • Número de puertos: 24 puertos Ethernet 10/100/1000 (Gigabit) + 2 puertos adicionales (usualmente SFP/SFP+) • Puertos PoE: 24 puertos PoE+ (802.3at o 802.3af) • Capacidad de conmutación: Varía según el modelo, típicamente alrededor de 56 Gbps • Gestión: Controlado a través de la aplicación UniFi Network Controller • Dimensiones: 1U (altura estándar de rack) • Alimentación: PoE pasivo o estándar, según el modelo • Características adicionales: VLAN, QoS, soporte para IGMP snooping y funcionalidades avanzadas de red. **Consumo energético:** Consumo de equipo con PoE inactivos es de 25 W. Consumo de equipo con PoE activo es de 120 W.

5.9.2.3 Propuesta de equipo Access Point para ambas sucursales

En la siguiente tabla se desarrolló la comparación de las características de las interfaces de los tres marcas y modelos propuestos de Access point para ambas sucursales.

Tabla 30 Precios de equipos Access Point.

PRECIOS DE EQUIPOS ACCESS POINT		
CISCO: 9115AXI-B	**ARUBA: JX945A**	**UBIQUITI UNIFI: 2*2 WI-FI 6 1.5 GBPS**
C$ 20,000 A 30,000	C$ 10,000 a 15,000	C$ 25,000 a 30,000

Tabla 31 Access Point – Masaya y León.

MARCAS		
CISCO	**ARUBA**	**UBIQUITI UNIFI**
Modelo: 9115AXI-B	**Modelo: JX945A**	**Modelo: 2×2 Wi-Fi 6 1.5 Gbps**
Especificaciones • Interfaces de red:1 puerto Ethernet 10/100/1000 Mbps (RJ45): Para conectividad de red. • 1 puerto USB: Para funciones de almacenamiento o conectividad adicional. • 1 puerto de consola (RJ45): Para la gestión y configuración del dispositivo. • Wi-Fi 6 (802.11ax): Soporta bandas de 2.4 GHz y 5 GHz. **Consumo energético:** Consumo del equipo con PoE activos es de 20.4 W. Consumo del equipo con PoE inactivos es de 13 W.	**Especificaciones** • Tecnología: Wi-Fi 6 (802.11ax) • Bandas: Doble banda (2.4 GHz y 5 GHz) • Velocidad: Hasta 2.4 Gbps en total (con 4x4 MU-MIMO en 5 GHz). • Soporta PoE+ (802.3at) y PoE++ (802.3bt) • Diseño compacto, fácil de instalar en varios entornos. **Consumo energético:** Consumo de equipo con PoE activos es de 13 W. Consumo de equipo con PoE inactivos es de 3.7 W. Consumo mediante alimentación DC directa es de 11 W.	**Especificaciones** • Conectividad: 2x2 MIMO • Velocidad máxima: Hasta 1.5 Gbps • Radios: • 5 GHz: MU-MIMO y OFDMA • 2.4 GHz: MIMO • Puertos: 1 x 10/100/1000 Mbps Ethernet • Alimentación: PoE (Power over Ethernet) • Antenas: Antena interna de alta ganancia. **Consumo energético**: Consumo del equipo con PoE activos es de 13.5 W. Consumo del equipo con PoE inactivos es de 4 W.

5.10 Estudio Técnico

Selección de proveedores de Internet

En el marco de una investigación detallada previamente realizada a través de la página de TELCOR, se analizó el acceso a internet ofrecido por tres de las principales empresas de telecomunicaciones del país: Claro, Tigo y ENATREL. Este análisis contempló aspectos como la cobertura y fiabilidad asociados a los servicios brindados por cada proveedor.

Con base en los resultados obtenidos y en función de las necesidades específicas de conectividad de nuestra empresa y sus sucursales, se procedió a hacer selección de proveedor de internet ideal para nuestra casa matriz y las dos sucursales, buscando optimizar tanto la eficiencia operativa como la calidad del servicio.

5.10.1 Selección de Proveedor Casa Matriz

Tomando como referencia la información obtenida en la plataforma oficial de TELCOR, se valoró a los proveedores existentes en las zonas en donde se encuentra ubicada la oficina central, ubicada en el departamento de Managua, en el cual se determinó que las tres empresas proveedoras de servicios de telecomunicaciones seleccionadas cuentan con presencia en este departamento.

Dado a los requerimientos de la red y el acceso a la zona del tipo de tecnología propuesto en la sede central, se concluyó que en esta sucursal la mejor opción para la contratación de servicios de telecomunicaciones son las empresas de CLARO y ENATREL. Esta selección se realizó basándose en la investigación anteriormente desarrollada; ya que como se pudo observar estas empresas son las que poseen la disponibilidad de hilos de fibra más cercanos a las ubicaciones de todas las sucursales. Además de que estas empresas brindan: cobertura, calidad y fiabilidad, lo que las hace ideales para el desarrollo de esta propuesta de diseño.

5.10.2 Selección de Proveedor Sucursal Masaya y León

Por lo antes mencionado se llegó a la delimitación de la selección del proveedor de servicios de Telecomunicaciones el cual será la empresa **CLARO**, ya que esta

cuenta presencia a nivel nacional y mayor variedad y accesibilidad de tecnologías incluyendo las zonas donde se encuentran ubicadas las oficinas en los departamentos de Masaya y León.

Cabe mencionar que esta empresa cuenta con parámetros importante a tomar en cuenta al momento de realizar una contratación, como lo son: precio, calidad y accesibilidad.

5.10.3 Selección de tecnología

En la actualidad, la tecnología avanza a un ritmo vertiginoso, ofreciendo soluciones innovadoras que transforman tanto el ámbito empresarial como el cotidiano, por lo tanto, es necesario que la selección de la tecnología, trabaje como una herramienta clave para mejorar la eficiencia, reducir costos y optimizar procesos en una amplia gama de industrias. Esta propuesta de tecnología tiene como objetivo explorar las ventajas y beneficios que puede aportar. Al haber seleccionado esta tecnología, las empresas no solo podrán mantenerse a la vanguardia, sino también lograr una ventaja competitiva significativa en un mercado cada vez más exigente.

Es por ello que luego de haber realizado un estudio con respecto al proveedor seleccionado y la cobertura que poseen en las zonas donde se encuentran ubicadas tanto la sede central como sus sucursales se determinó que para realizar la interconexión entre sucursales y que se brinde una alta eficiencia en el flujo de información a través de la red, la tecnología ideal sería el uso de fibra óptica.

Se hizo selección de la tecnología de Fibra Óptica, debido a que luego de hacer uso de la página oficial de TELCOR, está facilitó los puntos de cobertura, que ofrecen los diversos proveedores de servicios de telecomunicaciones en Nicaragua, en donde mostró mediante mapas de rutas de fibras y tablas informativas de los departamentos con sus respectivos municipios y la tecnología a la que se tiene acceso en la zona, esto demostró que las zonas en donde se encuentran ubicadas tanto la casa matriz como las dos sucursales tienen acceso a nodos de fibra óptica.

Además, esta tecnología esta ofrece una velocidad de transmisión de datos significativamente superior en comparación con otras tecnologías, garantizando

una comunicación rápida y sin interrupciones, incluso para transferencias de grandes volúmenes de información. Esto brinda una mayor eficiencia operativa y en la optimización de procesos que dependen de una conectividad constante.

Además de lo antes mencionado; cabe mencionar que la fibra óptica es más fiable y resistente a las interferencias electromagnéticas, lo que asegura una señal estable y de alta calidad en todo momento, minimizando tiempos de inactividad.

Es importante recalcar que nuestra propuesta se basa en una red escalable, por lo tanto, a largo plazo, esta tecnología también es más ampliable, lo que permite adaptarse fácilmente al crecimiento de la empresa, soportando futuras ampliaciones de red sin pérdida de rendimiento. Por estas razones, la fibra óptica es la opción ideal para garantizar una interconexión robusta, rápida y flexible entre la sede central y sus sucursales, asegurando la competitividad y continuidad operativa de la empresa.

5.10.4 Selección de Equipos de Red

En el proceso de selección de los equipos para propuesta de implementación de la interconexión de la red, se optó por soluciones tecnológicas que garantizan un rendimiento óptimo, alta fiabilidad y escalabilidad a largo plazo. Los equipos elegidos han sido cuidadosamente seleccionados tras un exhaustivo análisis de sus especificaciones técnicas, compatibilidad con la infraestructura propuesta y la capacidad de adaptarse al crecimiento futuro de la empresa.

Estos dispositivos, provenientes de fabricantes líderes en el sector, ya que estos están diseñados para ofrecer una conectividad rápida y estable, asegurando que las operaciones de la sede central y sus oficinas puedan realizarse sin interrupciones.

Además, la facilidad de gestión, el soporte técnico y las características avanzadas de seguridad incorporadas en cada uno de los equipos aseguran no solo una implementación exitosa, sino también una operación continua y protegida frente a posibles amenazas cibernéticas. En este sentido, los equipos seleccionados representan la mejor opción para garantizar la eficiencia y competitividad de la red,

consolidando una infraestructura robusta que será capaz de satisfacer las demandas presentes y futuras de la empresa.

5.10.4.1 Selección de Equipo FortiGate – Casa Matriz

Luego de realizar la comparación de las marcas y modelos de equipos propuestos para desarrollar las funciones de un Firewall en la Casa Matriz, se evaluaron cada una de las características que estos ofrecen y se eligió: el FORTINET 60F ya que es una decisión estratégica que proporciona una solución de seguridad integral y eficiente, adecuada para organizaciones que valoran tanto la protección avanzada como la facilidad de uso. Su capacidad de adaptación y rendimiento lo convierte en una opción ideal en un entorno empresarial cada vez más complejo y desafiante.

Cabe resaltar que este equipo será proporcionado por el proveedor de servicios al momento de contratar el enlace de internet ya que requiere de licencia y soporte, el uso de dos FORTINET es que estos fueron destinados uno para un enlace primario y el otro para un enlace secundario ambos proveedores de internet deben instalar mismo equipo para tener HA alta disponibilidad y que si un enlace llegara a fallar el otro equipo del proveedor pueda asumir la carga y operar con normalidad.

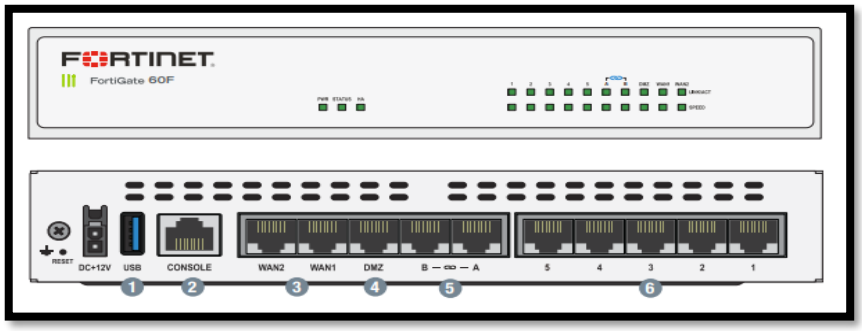

Figura No. 35 Equipo FORTINET modelo FortiGate 60F para casa matriz. [18]

5.10.4.2 Selección de Equipo Switch de Acceso – Casa Matriz

Luego de haber realizado una búsqueda de modelos de switch de accesos de diferentes marcas y revisar cada una de sus especificaciones y características,

llegamos a la decisión de proponer el siguiente modelo de switch de Acceso el cual es de la marca Cisco, más específicamente el modelo: C9200L-48P-4X, ya que este es la solución ideal para la estructura de red de la empresa, ofreciendo 48 puertos PoE+ que permiten alimentar dispositivos como teléfonos IP y cámaras de seguridad sin complicaciones.

Además de que su capacidad de escalabilidad asegura que la red pueda crecer sin problemas, mientras que las avanzadas características de seguridad, como Cisco TrustSec, protegen la información crítica del negocio. Con 4 puertos SFP+ de 10 Gigabit, garantiza una conectividad de alta velocidad para enlaces ascendentes, y su compatibilidad con Cisco DNA facilita la gestión y el monitoreo de la red. Con la fiabilidad y el soporte de Cisco, este switch es una inversión estratégica que asegura un rendimiento robusto y continuo para la empresa.

Figura No. 36 Switch de cisco modelo C9200L-48P-4X. [19]

5.10.4.3 Selección de Equipo Switch Core – Casa Matriz

Luego de la elaboración de la tabla comparativa de las características de las interfaces de los modelos de equipos propuestos, de las tres marcas anterior mente seleccionadas para la propuesta de un equipo core; que cumpliera con las características y capacidades necesarias para realizar la conectividad de la red de la Casa Matriz. Se concluyó que una buena propuesta de este sería el: Switch Core de la marca Cisco modelo C9300-48P-E

Este es la mejor elección para la estructura de red de la empresa, ya que combina un rendimiento excepcional con una escalabilidad sin igual. Con 48 puertos PoE+ y capacidades avanzadas de apilamiento, este modelo proporciona una gestión eficiente de dispositivos conectados, como teléfonos IP y puntos de acceso. Su arquitectura de software flexible, basada en Cisco IOS XE, permite implementar actualizaciones y nuevas funciones sin interrupciones, asegurando que la red esté

siempre a la vanguardia. Además, cuenta con robustas características de seguridad y soporte para Cisco DNA, lo que facilita una administración simplificada y una visibilidad integral de la red. Al optar por el C9300-48P-E, garantiza una infraestructura de red fiable, segura y lista para crecer junto con la empresa.

Figura No. 37 Switch Core marca Cisco modelo C9300L-48P-E. [20]

5.10.4.4 Selección de Equipo Access Point – Casa Matriz

Siguiendo con la estructura anteriormente planteada, se procedió a realizar una tabla comparativa de equipos, para la propuesta de Access Point, en el cual luego de esta, se seleccionó un equipo de la marca CISCO, específicamente el modelo Catalyst 9120AXP-B, debido a que este es implementado para realizar instalaciones interiores empresariales de forma profesional, de esta manera logrando cumplir con las necesidades y demanda a la que estará expuesta la red de la sucursal central.

Este modelo es ideal para la estructura de red de la empresa, ya que ofrece un rendimiento excepcional en entornos de alta densidad y movilidad. Equipado con tecnología Wi-Fi 6, proporciona velocidades de conexión más rápidas y una capacidad de manejo de dispositivos mucho mayor, lo que es esencial para satisfacer las demandas de usuarios y dispositivos conectados. Su diseño robusto incluye características avanzadas de seguridad, como Cisco Umbrella y Cisco Secure Network Analytics, garantizando una protección integral para su red. Además, la integración con Cisco DNA permite una gestión intuitiva y analítica de la red, facilitando la optimización del rendimiento y la resolución de problemas.

Figura No. 38 Access Point Catalyst 9120AXP-B. [21]

5.10.4.5 Selección de Equipo FortiGate – Sucursal Masaya y León

El equipo seleccionado que se propuso para la conexión de red que se realizara dentro de las sucursales de Masaya y León, es el FortiGate encargado de mantener disponibilidad y seguridad del enlace de internet, el modelo de FortiGate propuesto para ambas sucursales es el: FortiGate Cisco 40F.

Este modelo es la solución ideal para la seguridad de la red de la empresa, ya que combina un alto rendimiento con una amplia gama de funciones de ciberseguridad en un solo dispositivo. Con su tecnología de inspección de tráfico de alta velocidad y capacidades avanzadas de firewall, el FortiGate 40F protege la infraestructura contra amenazas emergentes y ataques cibernéticos, asegurando la continuidad del negocio. Además, incluye funciones de prevención de intrusiones, filtrado de contenido y VPN, lo que le permite mantener un entorno seguro y eficiente para todos los usuarios. Su integración con FortiOS proporciona una gestión centralizada y fácil de usar, permitiendo una rápida implementación y adaptación a las necesidades cambiantes de la empresa. Al elegir el FortiGate 40F, se está asegurando una defensa robusta y escalable que resguardará los datos y recursos críticos, preparándola para enfrentar los desafíos del futuro digital.

Figura No. 39 FortiGate 40 F para sucursales. [22]

5.10.4.6 Selección de Equipo Switch de Acceso – Sucursal Masaya y León

Para propuesta de Switch de acceso implementado en ambas sucursales, luego de realizar un cuadro comparativo de las marcas y los diferentes modelos propuestos, se seleccionó el modelo C9200L-24P-4X-E de la marca CISCO, ya que este cumple con las características necesarias para satisfacer las demandas de las necesidades para el correcto funcionamiento de la red en estas sucursales. El modelo C9200L-24P-4X-E es el ideal para la estructura de red de la empresa, ya que ofrece un equilibrio excepcional entre rendimiento, seguridad y escalabilidad. Este modelo permite alimentar dispositivos como teléfonos IP y cámaras de seguridad sin necesidad de fuentes de alimentación adicionales, optimizando la infraestructura existente. Su capacidad de apilamiento y conectividad con 4 puertos SFP+ de 10 Gigabit garantizan un rendimiento ágil y una expansión sencilla a medida que su empresa crece. Además, incluye características avanzadas de seguridad y gestión a través de Cisco DNA, lo que facilita el monitoreo y la administración de la red de manera intuitiva. Al optar por el C9200L-24P-4X-E, se está invirtiendo en una solución robusta y confiable que asegura la continuidad y eficiencia operativa de la empresa.

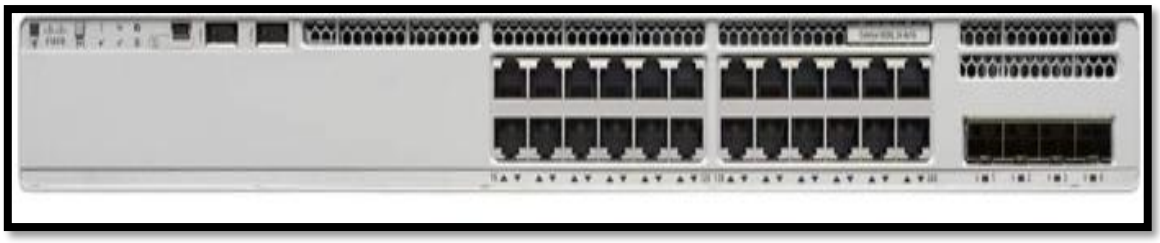

Figura No. 40 Switch de acceso C9200-24P-4X-E [23]

5.10.4.7 Selección de Equipo Access Point – Sucursal Masaya y León

Como propuesta de equipo Access Point para la conexión interna de ambas sucursales, se procedió a realizar tabla comparativa de marcas y modelos de AP que cumplieran y brindaran soluciones a las necesidades de requerimientos de la red, es por ello que se seleccionó y un equipo de la marca CISCO, específicamente el modelo Catalyst 9115AXI-B.

El modelo Catalyst 9115AXI-B de Cisco es perfecto para la estructura de red de la empresa, ofreciendo una conectividad Wi-Fi 6 de última generación que garantiza un rendimiento superior y una capacidad excepcional en entornos de alta densidad. Diseñado para manejar un gran número de dispositivos simultáneamente, este punto de acceso asegura que los empleados y clientes disfruten de una experiencia de red rápida y fluida.

Su robusta seguridad integrada, que incluye protección avanzada contra amenazas y segmentación del tráfico, resguarda la información crítica de su negocio. Además, su compatibilidad con Cisco DNA facilita la gestión y el análisis de la red, permitiendo una administración proactiva y optimizada.

Figura No. 41 Access point C9115 AXI-B. [24]

5.11 Cálculos del Ancho de Banda

En esta monografía, se analizó las necesidades de interconexión de una Pyme y sus sucursales, considerando tanto los usuarios en la sede central como en las sucursales. La oficina central cuenta con 22 usuarios, mientras que cada sucursal tiene 6 usuarios. El cálculo del ancho de banda necesario para garantizar un flujo de datos eficiente se basa en varios factores, entre los cuales destacan los servicios que los usuarios requieren para realizar sus tareas diarias.

Uno de los aspectos fundamentales en este análisis es la estimación del consumo de internet por parte de las computadoras de los usuarios. En este sentido, se ha determinado que cada computadora requiere ciertos servicios básicos de acceso a internet, como: correo electrónico (GMAIL), la paquetería office 365, navegación web, acceso a aplicaciones en la nube, y otros servicios de comunicación y colaboración, como videoconferencias (Microsoft Teams) o plataformas de trabajo compartido (Drive), antivirus, software CRM (Gestión de relaciones con clientes), software de diseño gráfico (Adobe Photoshop), herramientas para el manejo de base de datos, etc.

Además de los servicios previamente mencionados, se ha considerado la utilización de otros **softwares** específicos que las computadoras deberán ejecutar para facilitar el desarrollo de las actividades laborales. Entre estos se incluyen programas especializados en **contabilidad y finanzas,** los cuales permiten gestionar la información financiera de la empresa, realizar registros contables y generar reportes financieros. Asimismo, se contempla el uso de **herramientas de gestión de proyectos**, que son fundamentales para organizar, planificar y supervisar el avance de tareas y proyectos dentro de la empresa, asegurando la eficiencia y el cumplimiento de plazos establecidos.

5.11.1 Estimación del consumo Casa Matriz

- Estimación de ancho de banda PC

Con base en los servicios mencionados anteriormente, podemos estimar el consumo de ancho de banda necesario por usuario en la Pyme. Dependiendo de las necesidades específicas de cada usuario y de la frecuencia con la que se utilicen estas herramientas, el **ancho de banda total** para cada empleado puede variar. Sin embargo, es razonable estimar que se recomienda que cada equipo de cómputo para cada usuario de Pyme necesita un promedio de entre **300 kbps a 512kbps** de ancho de banda para cubrir todos estos servicios y garantizar una experiencia fluida en la red.

Es por ello que para estimar el cálculo del ancho de banda de la sede Central la cual cuenta con 22 usuarios, se seleccionó para cada PC un promedio de consumo de 512kbps, esto con el objetivo de cubrir las necesidades operativas y garantizar un rendimiento adecuado en el entorno empresarial. El cual se detalla a continuación:

Fórmula No. 1 Calculando ancho de banda sede Central.

$$\mathrm{BW} = \mathrm{Dispositivos} * \mathrm{Consumo}$$

$$\mathrm{BW\ PC} = 22\ * 512\mathrm{kbps} = 11{,}264\mathrm{kbps}$$

- **Conversión del ancho de banda de Computadora de Kbps a Mbps:**

Fórmula No. 2 Convirtiendo de ancho de banda de Kbps a Mbps.

$$\mathrm{MB} = \mathrm{Kbps} * 0.001$$

$$MB = 11{,}264Kbps * 0.001 = 11Mbps$$

- **Estimación del ancho de banda Servidores:**

Un servidor tiene un consumo aproximado de 3072 Kbps, lo cual nos indicó el siguiente calculo:

Fórmula No. 3 Calculando ancho de banda servidores.

$$BW = Dispositivos * Consumo$$

$$BW = 2 * 3072 = 6{,}144\mathrm{kbps}$$

- **Convirtiéndolo en Mbps, se estima que el consumo de 2 servidores para la casa matriz de la siguiente manera:**

Fórmula No. 4 Convirtiendo ancho de banda servidores en Mbps.

$$\mathrm{MB} = \mathrm{Kbps} * 0.001$$

$$\mathrm{MB} = 6{,}144\mathrm{Kbps} * 0.001 = 6.14\mathrm{Mbp}$$

- **Estimación de ancho de banda Teléfonos:**

Un teléfono IP tiene un consumo nominal promedio de 80Kbps por 1 llamada, lo cual nos indicó el siguiente calculo:

Fórmula No. 5 Calculando ancho de banda teléfono.

$$\mathrm{BW} = \mathrm{D}ispositivos * Consumo$$

$$\mathrm{BW} = 6 * 90\mathrm{Kbps} = 540\mathrm{Kbps}$$

- **Convirtiéndolo en Mbps, se estima que el consumo de 6 teléfonos para la casa matriz de la siguiente manera:**

Fórmula No. 6 Convirtiendo ancho de banda teléfonos en Mbps.

$$\mathrm{MB} = \mathrm{Kbps} * 0.001$$

$$\mathrm{MB} = 540\mathrm{Kbps} * 0.001 = 0.54\mathrm{Mbps}$$

- **Estimación del ancho de banda para cámaras**

Tomando en cuenta una estimación de los equipos de seguridad, como lo son las cámaras para resguardar la integridad de la pyme, se tiene destinado un total de 8 cámaras IP HD para la central

Fórmula No. 7 Calculando ancho de banda cámaras.

$$BW = Dispositivos * Consumo$$

$$\mathrm{BW} = 8 * 1500\mathrm{Kbps} = 12000\mathrm{Kbps}$$

- **Estimación del ancho de banda para cámaras en Mbps:**

Fórmula No. 8 Convirtiendo ancho de banda cámaras en Mbps.

$$\mathrm{MB} = \mathrm{Kbps} * 0.001$$

$$\text{MB} = 12000\text{Kbps} * 0.001 = 12\ \text{Mbps}$$

- **Estimación del ancho de banda para Impresoras**

Se realizaron los cálculos para impresora de las sucursales, en donde se estimó que una impresora consume un total de 115 Kbps, dando los siguientes resultados:

Fórmula No. 9 Calculando ancho de banda impresoras casa matriz.

$$BW = Dispositivos * Consumo$$

$$BW = 4 * 115\text{Kbps} = 460\text{Kbps}$$

- **Estimación del ancho de banda para impresoras en Mbps:**

Fórmula No. 10 Convirtiendo ancho de banda impresoras en Mbps.

$$\text{MB} = \text{Kbps} * 0.001$$

$$\text{MB} = 460\text{Kbps} * 0.001 = 0.46\text{Mbps}$$

5.11.2 Estimación de consumo sucursal Masaya y León

- Para 1 PC

Luego de haber realizado los cálculos para la pyme Casa Matriz, se inició a realizar los cálculos necesarios para estimar el ancho de banda tanto de la sucursal de Masaya como la de León, cabe mencionar que ambas sucursales cuentan con la misma cantidad de equipos (usuarios), por consiguiente, los resultados calculados del consumo del ancho de banda con respectos a los equipos (PC) son iguales para ambas sucursales:

Fórmula No. 11 Calculando ancho de banda PC ambas sucursales.

$$BW = Dispositivos * Consumo$$

$$\text{BW PC} = 6\ * 512\text{kbps} = 3.072\text{kbps}$$

- **Convirtiéndolo del ancho de banda de Computadora de Kbps a Mbps:**

Fórmula No. 12 Cálculo ancho de banda PC en Mbps.

$$\text{MB} = \text{Kbps} * 0.001$$

$$\text{MB} = 3.072\text{Kbps} * 0.001 = 3\text{Mbps}$$

Luego de realizados los cálculos para las PC de ambas sucursales, se procedió a realizar el cálculo de ancho de banda para otros equipos como: Teléfonos, impresoras y cámaras. Cabe mencionar que se estimó que ambas sucursales cuentan con el mismo número de estos equipos, al igual que con las computadoras.

De igual forma como se mencionaba anteriormente estos equipos no fueron incluidos en la propuesta de la estructura de red de casa matriz ni de las sucursales, pero de igual forma se decidió estimar el consumo de estos, con el objetivo de un cálculo de ancho de banda más acertado y que sirviera como guía al momento que se retome para una futura implementación.

- **Estimación de ancho de banda Teléfonos:**

Un teléfono IP tiene un consumo nominal promedio de 80Kbps por 1 llamada, lo cual indicó el siguiente calculo:

Fórmula No. 13 Calculando ancho de banda teléfono sucursales.

$$BW = Dispositivos * Consumo$$

$$\mathrm{BW} = 3 * 90\mathrm{Kbs} = 270\mathrm{Kbps}$$

- **Convirtiéndolo en Mbps, se estima que el consumo de 3 teléfonos para ambas sucursales de la siguiente manera:**

Fórmula No. 14 Convirtiendo ancho de banda teléfonos de sucursales en Mbps.

$$\mathrm{MB} = \mathrm{Kbps} * 0.001$$

$$\mathrm{MB} = 270\mathrm{Kbps} * 0.001 = 0.27\mathrm{Mbps}$$

- **Estimación de ancho de banda Cámaras**

Tomando en cuenta una estimación de los equipos de seguridad, como lo son las cámaras para resguardar la integridad de la pyme, se tiene destinado un total de 4 cámaras IP para las sucursales. En donde se estima que una consume 432 kbps.

Fórmula No. 15 Calculando ancho de banda cámaras de sucursales en Mbps.

$$BW = Dispositivos * Consumo$$

$$\mathrm{BW} = 4 * 1500\mathrm{Kbps} = 6000\mathrm{Kbps}$$

- **Estimación del ancho de banda para cámaras en Mbps:**

Fórmula No. 16 Convirtiendo ancho de banda cámaras de sucursales en Mbps.

$$\mathrm{MB} = \mathrm{Kbps} * 0.001$$

$$\mathrm{MB} = 6000\mathrm{Kbps} * 0.001 = 6\ \mathrm{Mbps}$$

- **Estimación del ancho de banda para Impresoras**

Se realizaron los cálculos para impresora de las sucursales, en donde se estimó que una impresora consume un total de 115 Kbps, dando los siguientes resultados:

Fórmula No. 17 Calculando ancho de banda impresoras ambas sucursales.

$$BW = Dispositivos * Consumo$$

$$\mathrm{BW} = 2 * 115\ \mathrm{Kbps} = 230\ \mathrm{Kbps}$$

- **Estimación del ancho de banda para Impresoras en Mbps:**

Fórmula No. 18 Convirtiendo ancho de banda impresoras de sucursales en Mbps.

$$\mathrm{MB} = \mathrm{Kbps} * 0.001$$

$$\mathrm{MB} = 230\mathrm{Kbps} * 0.001 = 0.23\mathrm{Mbps}$$

Luego de haber realizado todos los cálculos correspondientes para el total estimado del ancho de banda tanto de la Cede Central como las sucursales, dieron los siguientes resultados:

Total, de ancho de Banda para sucursal León: Luego de realizar la sumatoria del consumo de todos equipos, dio un resultado de 6.85 Mbps, a este resultado se le aplico un porcentaje de 5% como medida de prevención; siendo este un margen de error. Dando como resultado final un total de Ancho de Banda de **7.19 Mbps** para la sede de León.

Total, de ancho de Banda para sucursal Masaya: Después de sumar el consumo de todos los equipos, se obtuvo un total de 6.85 Mbps. A este valor se le agregó un 5% adicional como medida preventiva, para cubrir posibles márgenes de error. De este modo, el resultado final del ancho de banda para la sucursal de sede Masaya fue de **7.19 Mbps.**

Total, de ancho de Banda para Casa Matriz: Se realizó la sumatoria de todos los equipos con respecto al consumo estimado, dando un total de 21 Mbps, cabe mencionar que como se estaba realizando una propuesta de interconexión, la oficina central es la que cuenta con los servidores a los que se conectaran las sucursales mediante el uso de VPN, es por ello que a este dato se le debe de sumar el total de ambas sucursales obteniendo un total de 35.84 Mbps, al cual de igual forma se le tiene que emplear un porcentaje de margen de error; al ser la sede central se decidió aplicar un 20%, dando un total de ancho de banda para la Sede Central de **43.008 Mbps.**

El ancho de banda propuesto fue dimensionado a partir de un análisis detallado de los requerimientos estimados de una pyme o futuras pymes, considerando la cantidad de usuarios, los servicios de red implementados y el consumo promedio de los dispositivos seleccionados. La infraestructura fue diseñada bajo criterios de

optimización y eficiencia, evitando el sobredimensionamiento de recursos de la red. Asimismo, los equipos elegidos presentan un bajo consumo de ancho de banda, lo que garantiza un funcionamiento adecuado dentro del ancho de banda estimado para la sede central y sucursales técnicamente viable y acorde a la capacidad operativa y financiera de las pymes.

Se recomienda contratar el siguiente ancho de banda para la PYME, para que cubrir y exceder el consumo calculado, ofreciendo un margen de seguridad adicional.

Tabla 32 Ancho de banda.

Ancho de Banda		
Casa Matriz	**Sucursal Masaya**	**Sucursal León**
45Mbps	10Mbps	10Mbps

La recomendación de 10 Mbps para cada sucursal (6 usuarios) se basa en un enfoque de contención de costos y una evaluación del riesgo de congestión, asumiendo que el uso es más ligero y que el tráfico crítico (como bases de datos) se concentra en la Oficina Central.

5.12 Costos de equipamientos

Casa Matriz – Managua

Presupuesto Estimado para la Contratación de Enlace de Fibra Óptica, con FortiGate 60F para una PYME en Managua.

Enlace de Fibra Óptica de 45 Mbps (Proveedor Claro y ENATREL)

Descripción del Servicio de Fibra Óptica

El enlace de fibra óptica de 45 Mbps proporcionado por el proveedor de servicio ya sea Claro y ENATREL, es un servicio de acceso a internet de alta velocidad, que utiliza tecnología de fibra óptica para garantizar una conexión rápida y estable, ideal para pequeñas y medianas empresas (PYMEs). Este servicio ofrece un ancho de banda adecuado para realizar actividades comerciales, operaciones en la nube, videoconferencias y transferencias de archivos de tamaño medio.

Tabla 33 Desglose costos enlace de internet sede central.

Concepto	Rango de costo	Frecuencia	Nota	Proveedor
Servicio de internet fibra óptica (45Mbps)	$150 - $250	Mensual	Varía según el proveedor, duración y tipo de contrato.	CLARO/ENATREL
Instalación	$150 - $150	Único	Depende de la ubicación, infraestructura y complejidad del tendido.	CLARO/ENATREL
ONT (Optical Network Terminal)	$50 - $150	Único (en caso que aplique)	Generalmente incluido, pero puede requerirse un costo extra por equipo específico.	CLARO/ENATREL

Conclusiones y recomendaciones del enlace de internet

Para la implementación de un enlace de fibra óptica de 45 Mbps en una PYME en Managua, el presupuesto mensual estimado es de $150 a $250 USD. Es importante que la empresa se comunique directamente con los proveedores de internet Claro y ENATREL para obtener una cotización exacta del servicio de fibra óptica y confirmar los precios de instalación, así como también con los costos de contratación de equipos Fortinet para obtener precios actualizados y detalles de la licencia FortiGuard.

Además, se recomienda negociar condiciones favorables de mantenimiento y soporte técnico de estos equipos, ya que se le sumaran estos costos al presupuesto mensual antes estimado.

Sucursal Masaya y León Descripción del Servicio de Fibra Óptica

El servicio de fibra óptica de 10 Mbps ofrecido por los proveedores Claro y ENATREL proporciona acceso a internet de alta velocidad, utilizando tecnología de fibra óptica para asegurar una conexión estable y confiable. Es una opción adecuada para pequeñas empresas o entornos laborales con un uso moderado de internet, como la navegación web, el envío de correos electrónicos, las videoconferencias y la transferencia de archivos de tamaño ligero a medio.

Tabla 34 Desglose costos enlace de internet sucursales.

Concepto	Rango de costo	Frecuencia	Nota	Proveedor
Servicio de internet fibra óptica (10Mbps)	$80 - $150	Mensual	Precio estimado para un servicio de menor ancho de banda en zonas fuera de la capital, para cada sucursal.	CLARO/ENATREL
Instalación	$80 - $120	Único	Despliegue de la infraestructura de FO en cada sucursal.	CLARO/ENATREL
ONT (Optical Network Terminal)	$40 - $100	Único (si aplica)	Costo estimado del Terminal de Red Óptica para cada sucursal.	CLARO/ENATREL

Cabe mencionar que ambos proveedores, Claro Nicaragua y ENATREL, ofrecen precios similares para los servicios de fibra óptica en Nicaragua, Ambos incluyen mantenimiento básico y soporte técnico dentro de su tarifa mensual. Sin embargo, Claro podría incluir servicios de seguridad adicionales como las licencias de FortiGuard dependiendo del plan contratado, mientras que ENATREL no incluye estas licencias y los costos adicionales por servicios de seguridad deben ser contratados por separado. La instalación puede ser gratuita o tener un costo adicional dependiendo de la ubicación, pero generalmente ENATREL tiene un costo de instalación más alto en algunos casos.

Además, esto Claro ofrece licencias adicionales para protección de red. Por otro lado, ENATREL el costo de instalación es un factor clave, o si ya tienes un sistema de seguridad independiente en tu red.

Tabla 35 Costo de servicios.

Costo de servicio de internet			
Ubicación	**Ancho de banda**	**Costo mensual**	**Instalación (único)**
Managua	45Mbps	C$250.00	C$150.00
Masaya	10Mbps	C$150.00	
León	10Mbps	C$150.00	
Total		**C$550.00**	**C$150.00**

5.13 Propuesta de Tabla de Direccionamiento y Segmentación de Red

El enfoque adoptado, asignó a cada sede un rango de direcciones IP independiente, lo que eliminó la posibilidad de superposición y simplificó la administración de la red. Esta segmentación redujo el riesgo de conflictos de IP y permitió un mayor control del tráfico interno, al definir qué dispositivos o departamentos podían comunicarse entre sí.

Tomando en cuenta los requerimientos de la red de la empresa se dividió en 6 subredes dentro de casa matriz, cabe resaltar que se utilizó un bloque de direccionamiento de clase C el cual es más apropiado para redes medianas y pequeñas, también se valoró que la conexión entre el router principal y el router secundario se manejara por medio de un enrutamiento diferente con la finalidad de que cada uno conociera su vía alterna en caso de que se vea afectado el enlace del router principal.

Presentamos el esquema de direccionamiento IP para una empresa con las características que mencionamos anteriormente, cabe resaltar que según las necesidades específicas del cliente se debe realizar el plan de direccionamiento.

5.13.1 Direccionamiento IP para routers del proveedor

Retomando el enunciado anterior las IP públicas proporcionadas por el ISP son suficientes, para la configuración de la VPN no necesitamos un direccionamiento diferente a menos que tengamos múltiples servicios que requieran IP adicionales, por lo tanto, la dirección IP pública que se tiene asignada en la casa matriz y sus

dos sucursales sirven para establecer la conexión de VPN site-to-site y para acceso remoto de empleados o usuarios externos.

5.14 Asignación de VLANS para 10 áreas de trabajo en casa matriz.

La asignación de VLANS es importante para tener un enfoque de una red bien segmentada y segura, manteniendo el control adecuado del tráfico de cada área de trabajo. Sé procedió a realizar el direccionamiento.

5.14.1 Creación de VLANS y direccionamiento para sucursal Masaya

La sucursal de Masaya, cuenta con un total de 6 trabajadores y son 5 puestos de trabajo, se solicitó que se crearan 4 VLANS, pero para ello se debía ajustar la subred original. El diseño se implementó mediante subneteo y VLANs para la asignación precisa de IPs estáticas a los usuarios. Este enfoque optimizó los recursos, asegurando que la red fuera funcional y adaptable a futuras necesidades.

5.14.2 Creación de VLANS y direccionamiento para Sucursal León

La filial ubicada en el departamento de León, cuenta con un total de 6 trabajadores y son 5 puestos de trabajo, se solicitó que se crearan 4 VLANS, pero para ello se debía ajustar la subred original, cabe mencionar que ambas sucursales tienen el mismo requerimiento

5.15 Instalación de EVE-NG

EVE-NG es un **software de emulación y virtualización de redes** que se instala en un servidor o computadora para crear y ejecutar simulaciones de redes. Permite a los profesionales de redes crear topologías complejas de manera virtual y probar diferentes escenarios sin necesidad de hardware físico.

Puedes instalar EVE-NG en bare metal o en un emulador, pero la instalación en bare metal es preferible para obtener el máximo rendimiento y estabilidad. Instalarlo en un hipervisor (emulador) como VMware o VirtualBox es una opción viable y más común para pruebas de escritorio, aunque la ejecución puede estar limitada por el rendimiento del hipervisor subyacente.

5.16 Simulación de la infraestructura de Red propuesta

Se utilizó del software EVE-NG para validar el funcionamiento de la red, llevando a cabo pruebas exhaustivas para garantizar la estabilidad y el rendimiento esperado.

En la siguiente imagen podemos observar la topología de nuestra PYME

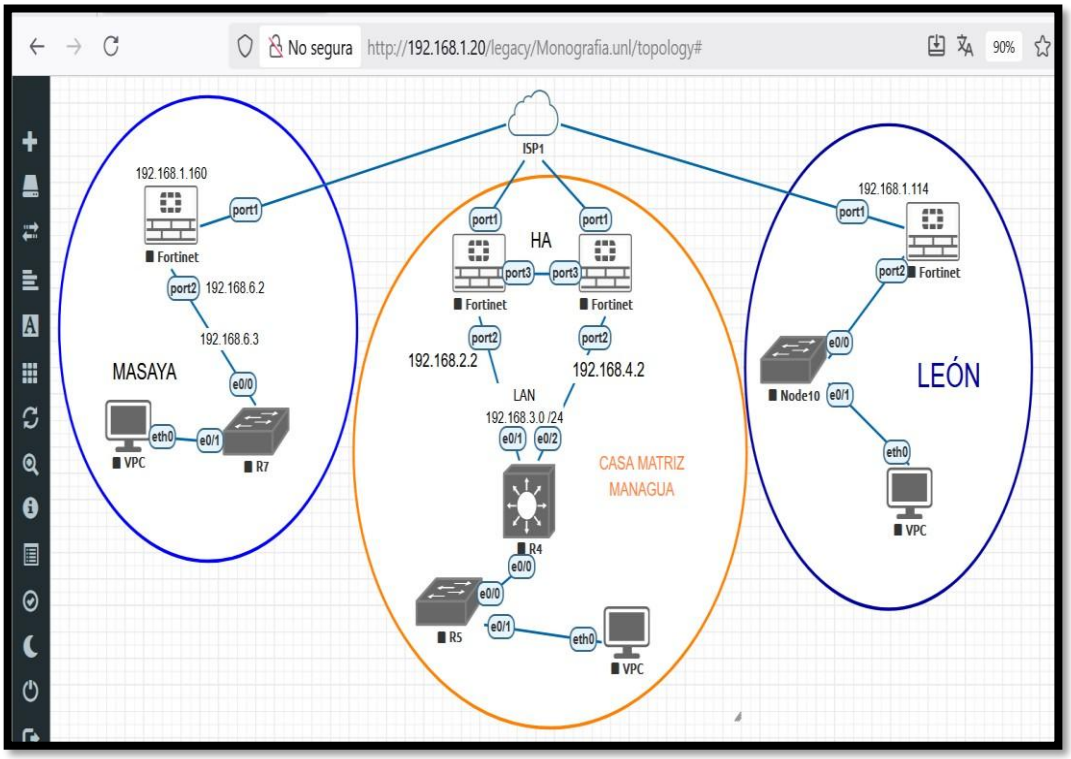

Figura No. 43 Interconexiones de las Pyme.

1. Se ingresa primeramente al equipo Fortinet para la configuración la interfaz 2 para la conexión LAN de casa matriz.

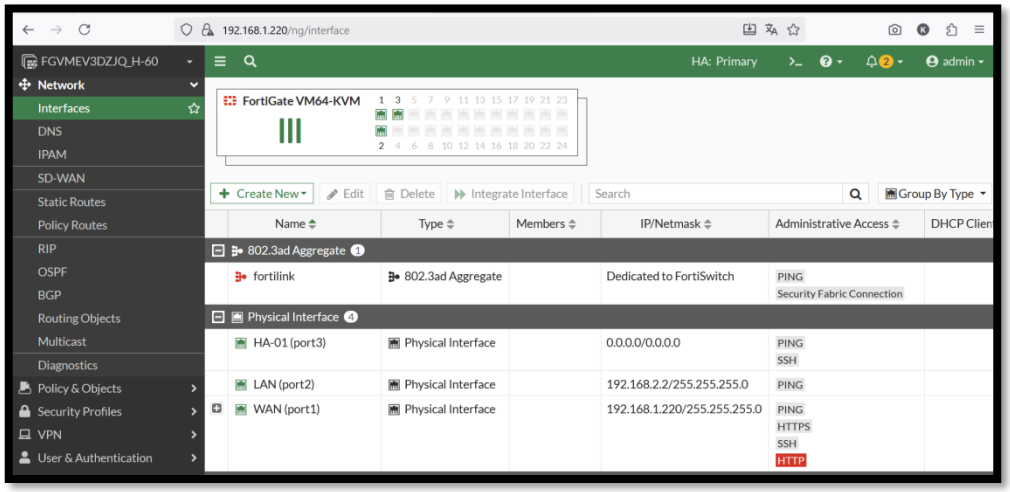

Figura No. 42 Interfaces del FORTINET.

2. Se ingresó al Fortinet para la creación de rutas estáticas ISP1 CM.

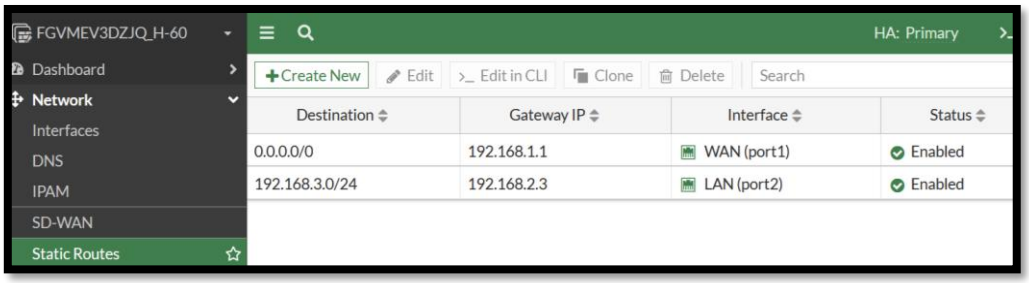

Figura No. 43 Rutas estáticas ISP1 CM.

3. Se ingresó al Fortinet para la creación de rutas estáticas ISP2 CM.

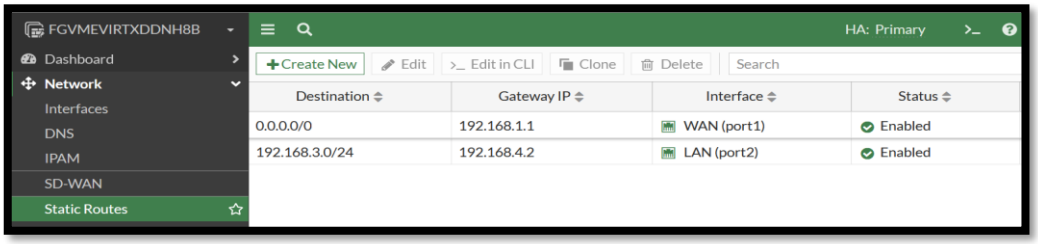

Figura No. 44 Rutas estáticas ISP2 CM.

4. Se ingresa mediante consola a la imagen de simulación del switch capa 3 para configuración de Switch Core casa matriz.

```
interface Ethernet0/0
 description !Conexion LAN!
 ip address 192.168.3.1 255.255.255.0
!
interface Ethernet0/1
 description !Conexion-Fortinet1!
 ip address 192.168.2.3 255.255.255.0
!
interface Ethernet0/2
 description !Conexion-Fortinet2!
 ip address 192.168.4.2 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.2.2 track 1
ip route 0.0.0.0 0.0.0.0 192.168.2.2
ip route 0.0.0.0 0.0.0.0 192.168.4.1 100
ip route 8.8.8.8 255.255.255.255 192.168.2.2 name SLA/TEST
!
ip sla 1
 icmp-echo 8.8.8.8 source-interface Ethernet0/1
 frequency 5
ip sla schedule 1 life forever start-time now
!
!
```

Figura No. 45 Configuración Switch Core

5. Realizando prueba de conectividad desde el SW-CORE de casa matriz.

```
SW-CORE>ena
SW-CORE#ping 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CORE#ping 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CORE#ping 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/1 ms
SW-CORE#ping 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SW-CORE#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4 ms
SW-CORE#ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SW-CORE#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 51/52/56 ms
SW-CORE#
```

Figura No. 46 Prueba de conectividad SW-CORE.

6. Realizando prueba de salida del switch core casa matriz por el ISP1

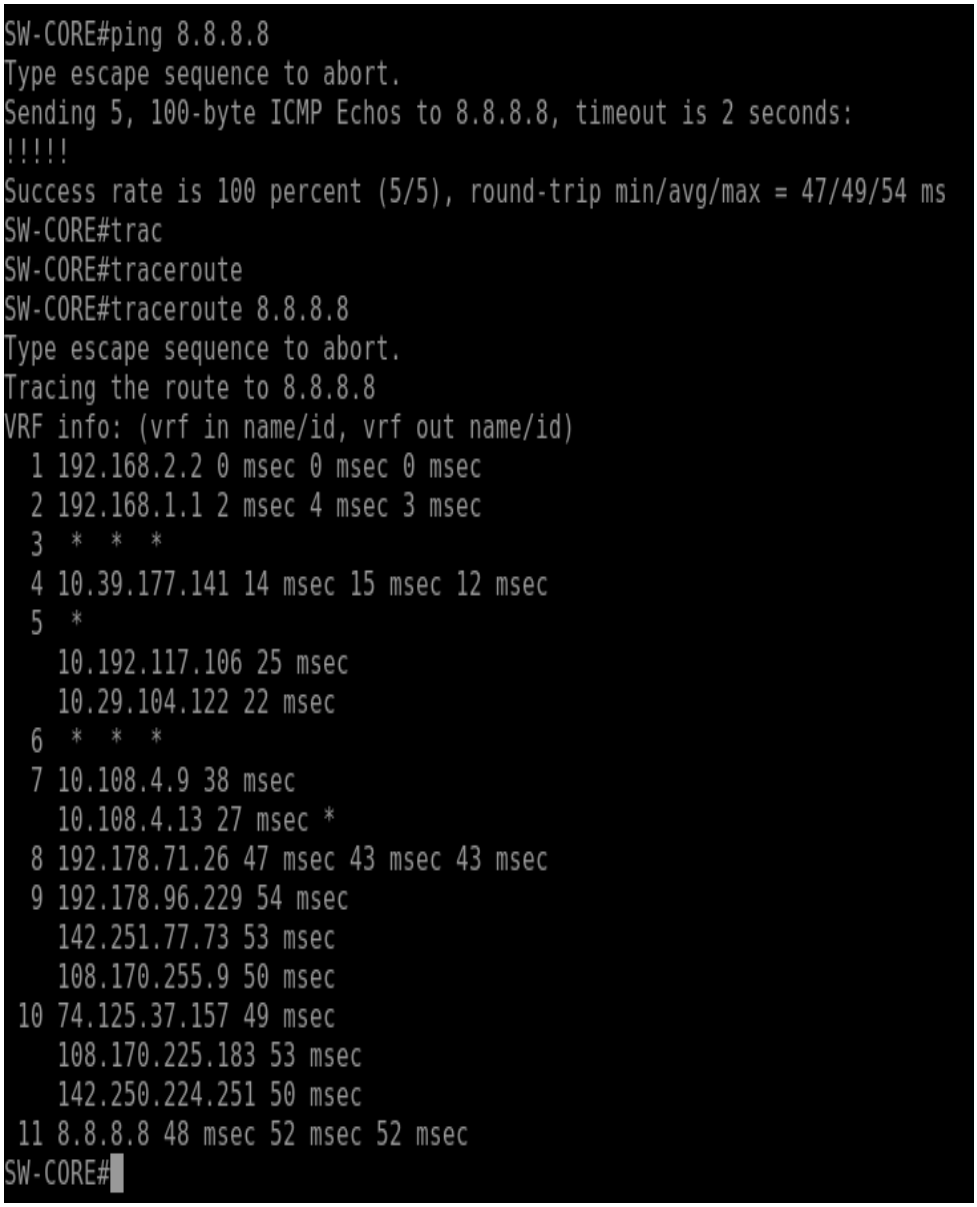

Figura No. 47 Prueba de navegación SW-CORE por el ISP1

7. Se realizo pruebas de conectividad utilizando el Proveedor de Servicios de Internet 2 (ISP2). Para dirigir el tráfico por esta nueva vía, fue necesario modificar la ruta de salida en el switch de capa de distribución, indicándole que utilizara la ruta del ISP2 para su tráfico.

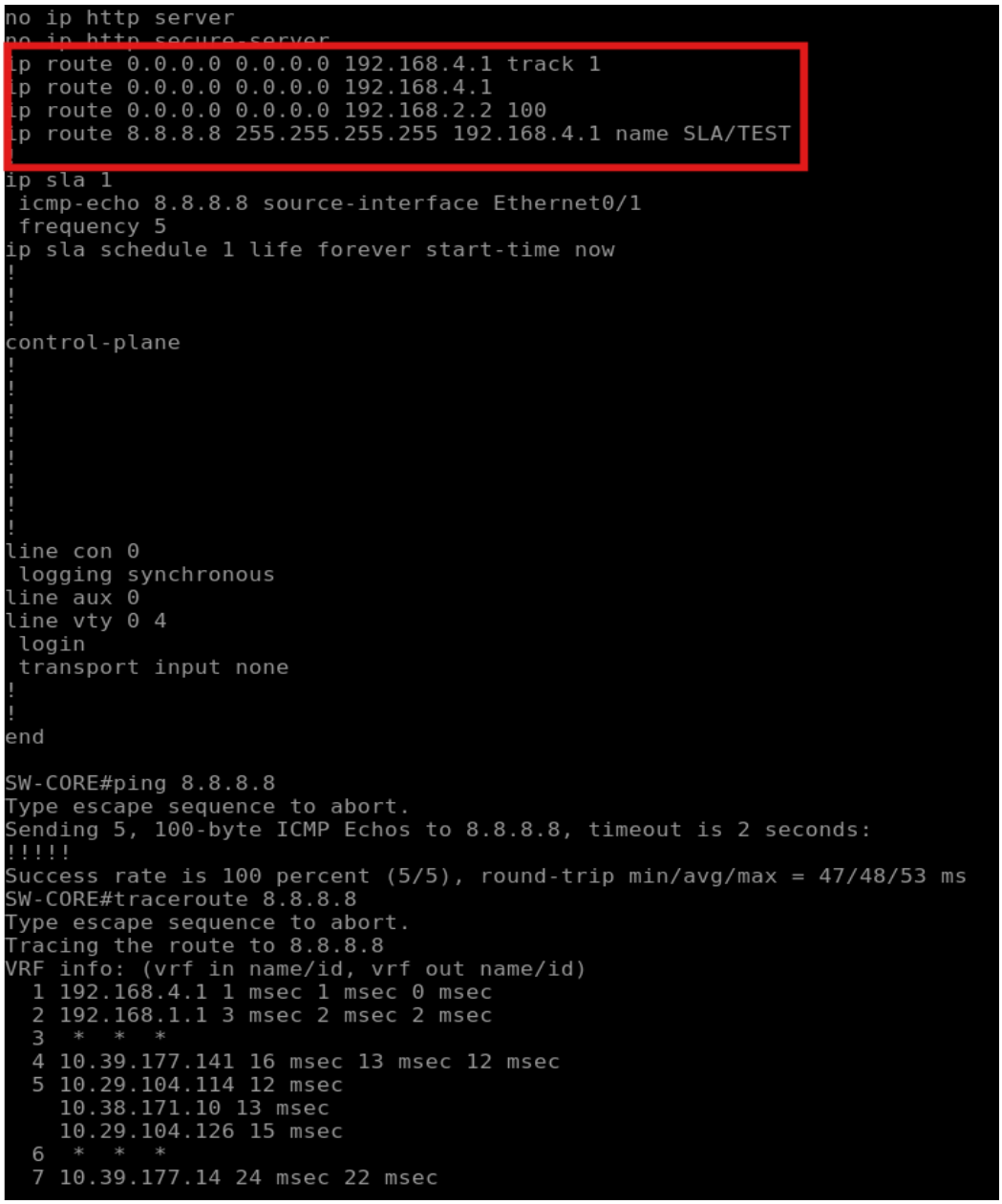

Figura No. 48 Prueba de navegación SW-CORE por el ISP2.

7. Configuración de la PC en EVE-NG y prueba de conectividad con los equipos a nivel LAN y navegación a Google

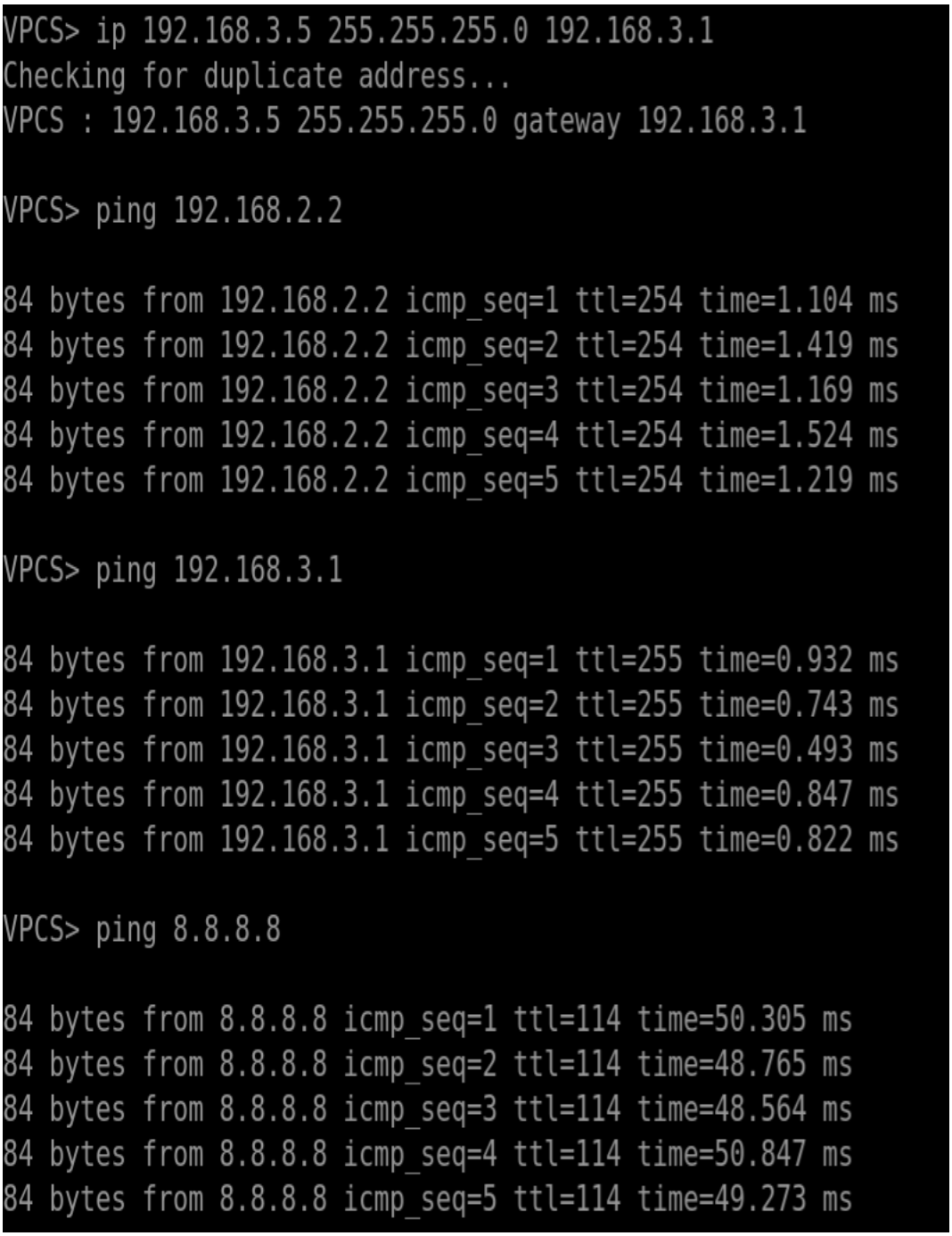

Figura No. 48 Prueba de navegación VPCS CM.

8. Ingresamos al Fortinet para crear desde la plantilla IPSEC WIZARD de VPN, indicamos que el FORTINET de casa matriz (CM) será el HUB

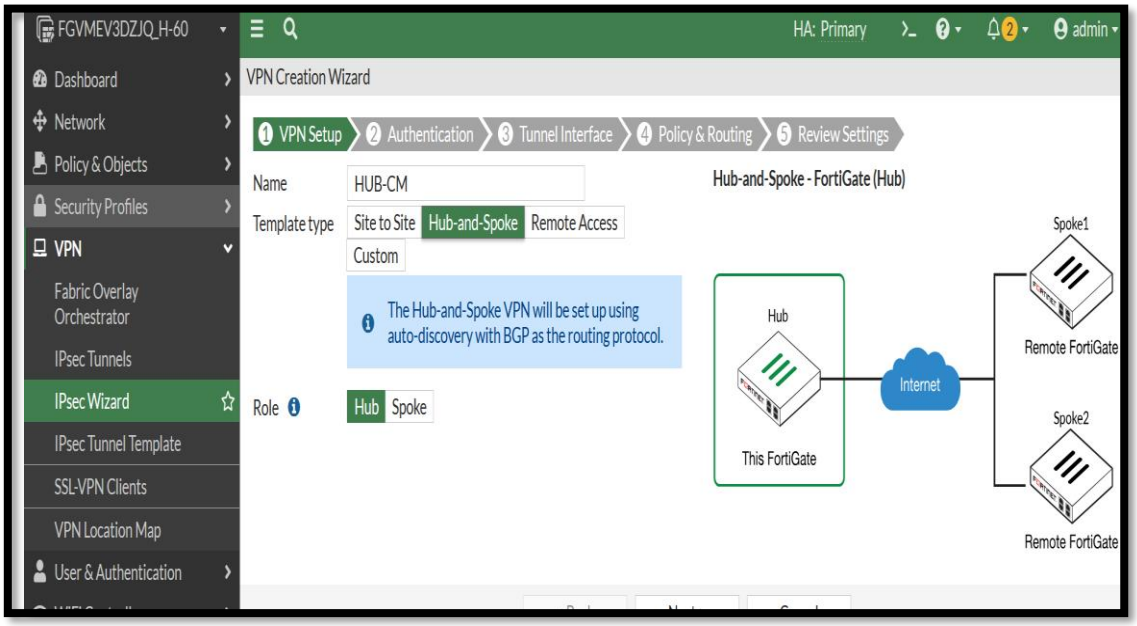

Figura No. 49 Creación HUB FORTINET CM

9. Se indicó que el tráfico del Hub se deberá enrutar mediante dos Spoke que son nuestras dos sucursales.

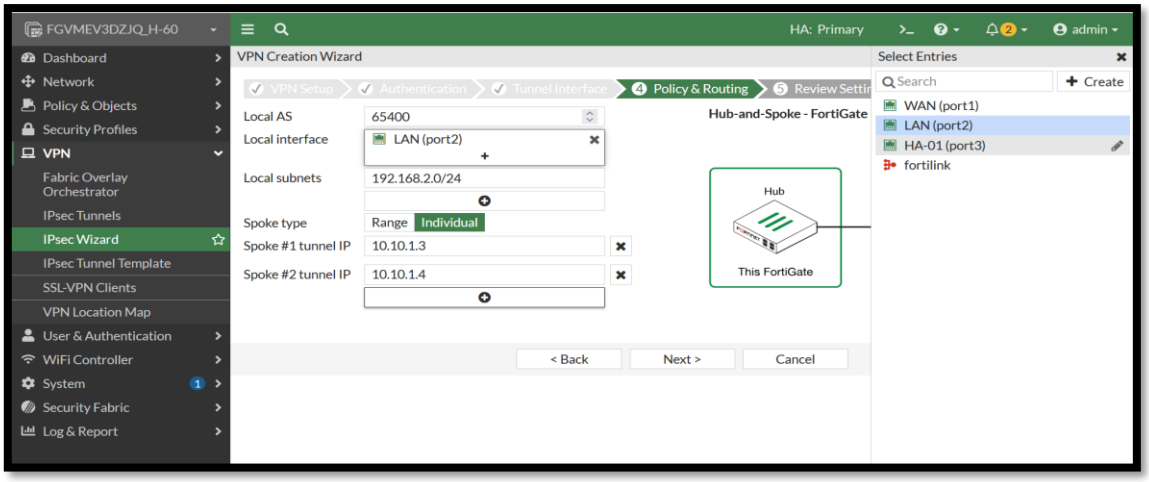

Figura No. 50 Creando Políticas y Rutas HUB FORTINET CM.

10. Indicó que el túnel desde casa matriz fue creado exitosamente y comparte la PSK con la que levantó el túnel de los otros extremos para la encriptación.

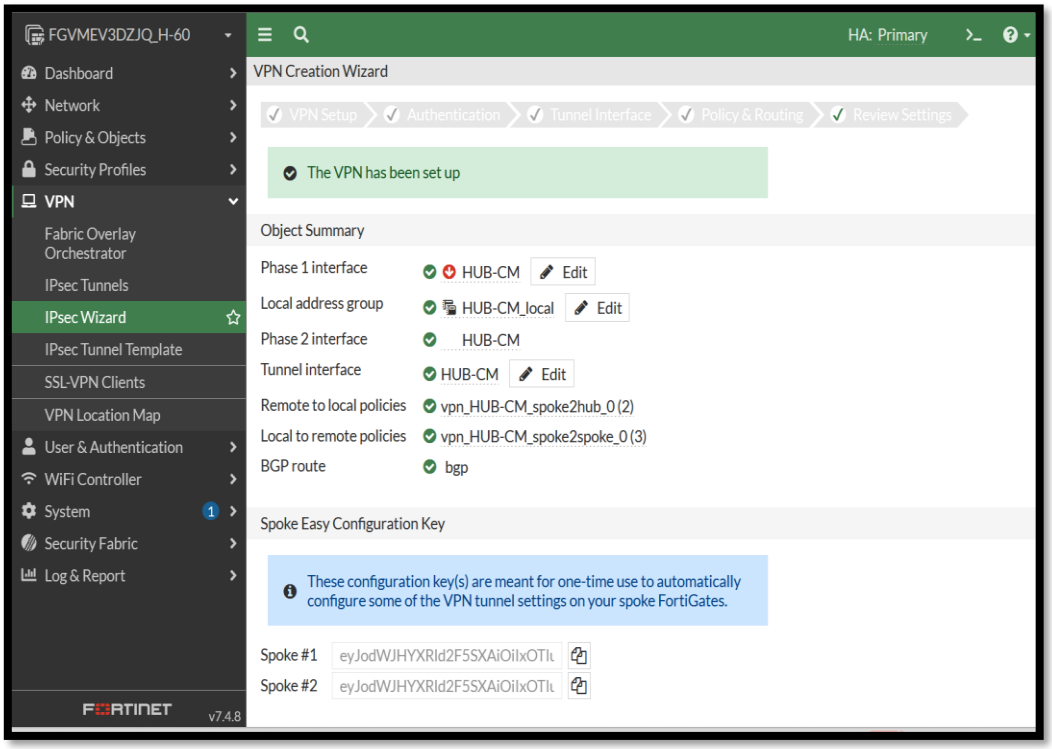

Figura No. 51 Creación de túnel VPN HUB exitosa.

11. Configuración de túnel VPN en Masaya utilizando el método de IPSEC HUB AND SPOKE Masaya. Se aplicó la llave creada por el FORTINET HUB.

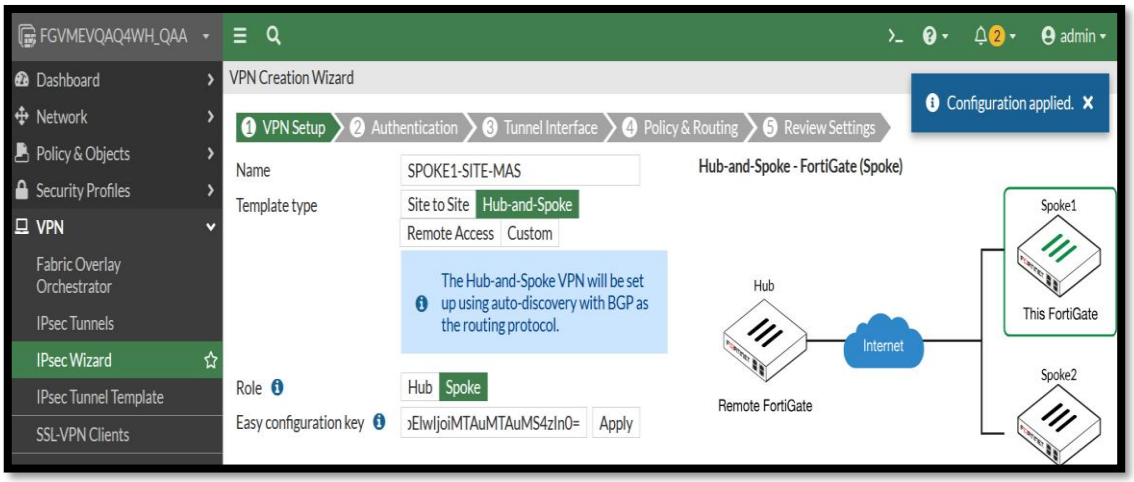

Figura No. 52 Creación túnel VPN SPOKE1.

12. Se configura el puerto por donde se van a interconectar y la contraseña admin1 que fue la que se agregó también en el FORTINET de CM

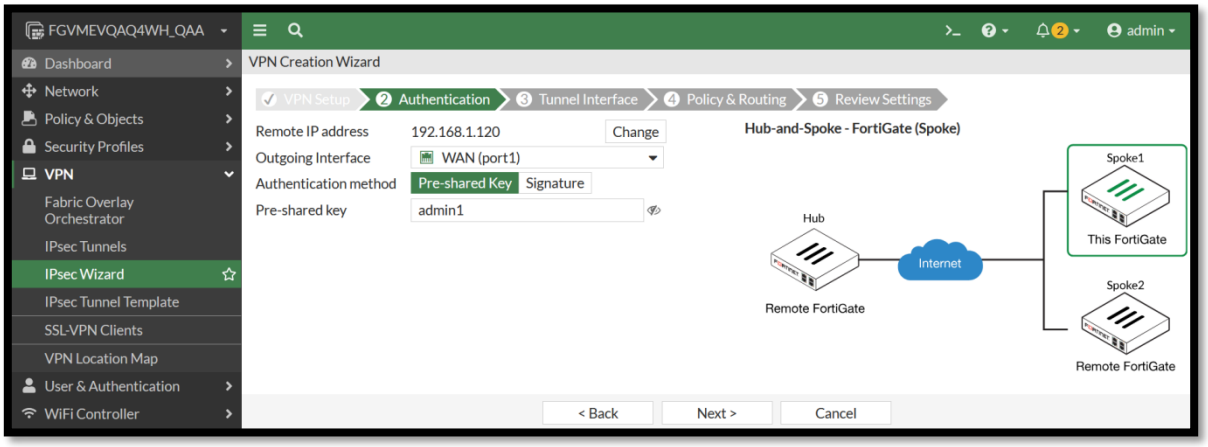

Figura No. 53 Interfaces de conexión SPOKE1.

13. Validación que el túnel fue creado para sucursal de Masaya

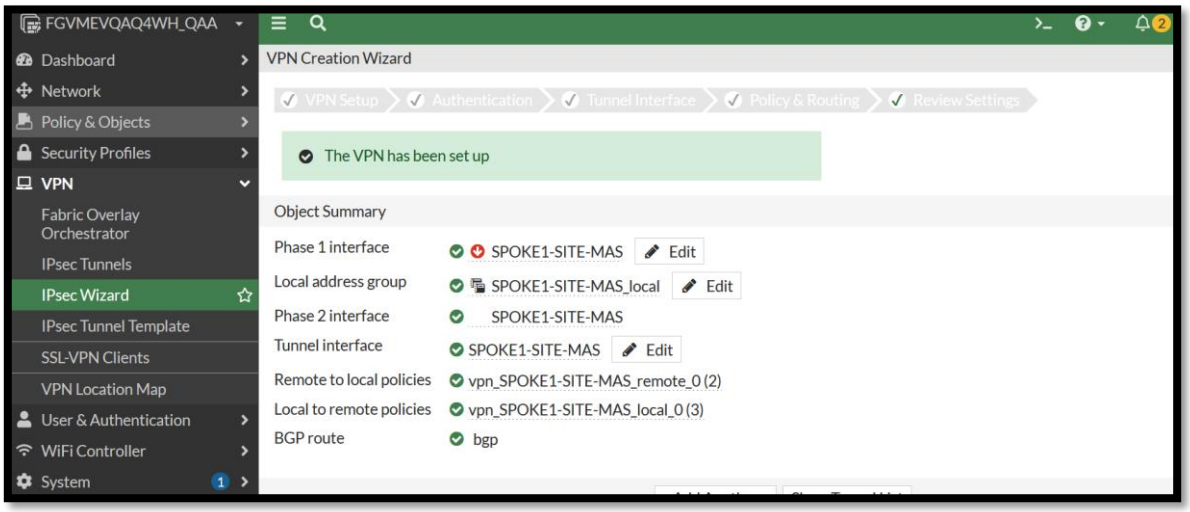

Figura No. 54 Creación de túnel VPN SPOKE1 exitosa.

14. Ingresando al Fortinet para validar que ambos extremos el túnel están activos.

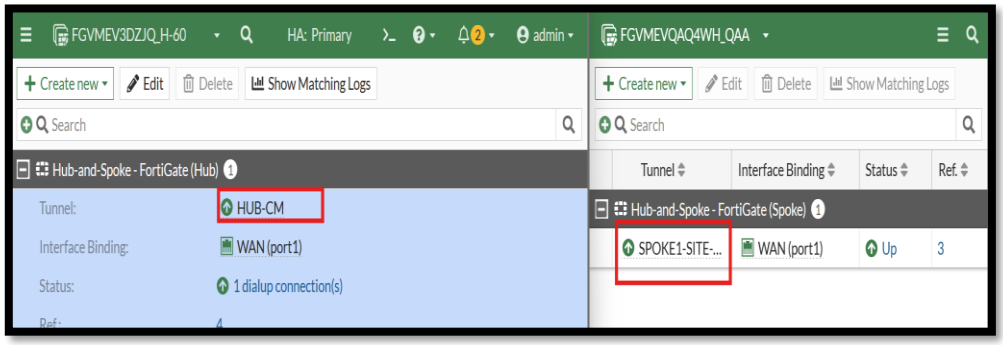

Figura No. 55 Validación de túnel HUB-SPOKE.

15. Se crearon las políticas de CM para permitir el tráfico del túnel de VPN.

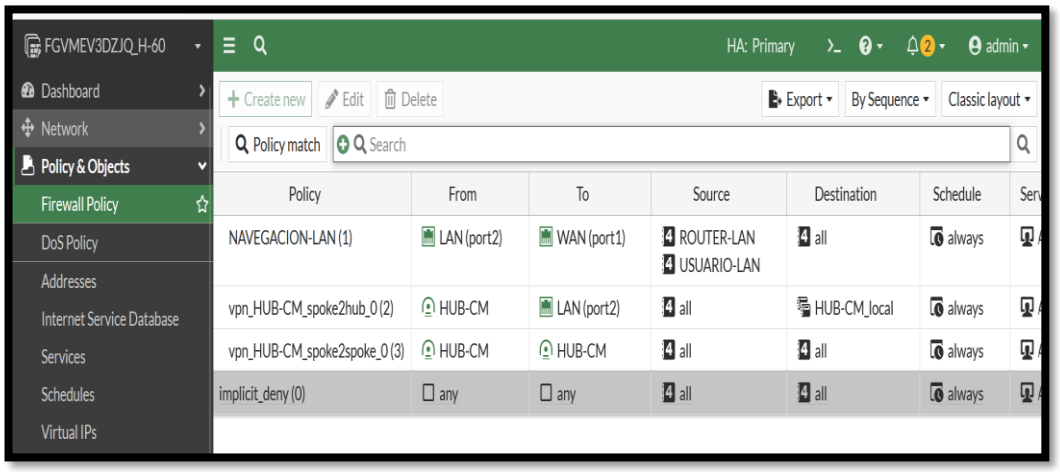

Figura No. 56 Políticas del túnel VPN FORTINET CM

16. Ingresamos vía consola al switch de acceso (switch L2) sucursal Masaya.

```
interface Ethernet0/0
 switchport access vlan 2
 switchport mode access
!
interface Ethernet0/1
 switchport access vlan 2
 switchport mode access
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Vlan2
 ip address 192.168.6.10 255.255.255.0
!
ip default-gateway 192.168.6.2
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.6.2
!
```

Figura No. 57 Configuración Switch Masaya

17. Realizando la validación de conectividad desde el switch de la sucursal Masaya mediante la línea de consola el switch L2.

```
Switch#ping 192.168.6.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 50/51/55 ms
Switch#
```

Figura No. 58 Prueba de conectividad switch Masaya

18. Ingresamos por medio de consola a la PC de simulación para la validación de la conectividad desde la PC de la sucursal Masaya

```
VPCS> ip dhcp
DDORA IP 192.168.6.3/27 GW 192.168.6.2

VPCS> ping 192.168.6.2

84 bytes from 192.168.6.2 icmp_seq=1 ttl=255 time=0.418 ms
84 bytes from 192.168.6.2 icmp_seq=2 ttl=255 time=0.726 ms
84 bytes from 192.168.6.2 icmp_seq=3 ttl=255 time=0.850 ms
84 bytes from 192.168.6.2 icmp_seq=4 ttl=255 time=0.602 ms
84 bytes from 192.168.6.2 icmp_seq=5 ttl=255 time=0.565 ms

VPCS> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=115 time=53.504 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=115 time=53.801 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=115 time=52.494 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=115 time=56.189 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=115 time=52.734 ms
```

Figura No. 59 Prueba de conectividad VPCS Masaya

19. Creación del túnel de VPN de la sucursal de León, utilizando el mismo método de Hub and Spoke, se aplicó la llave creada por el HUB y dar la opción de siguiente.

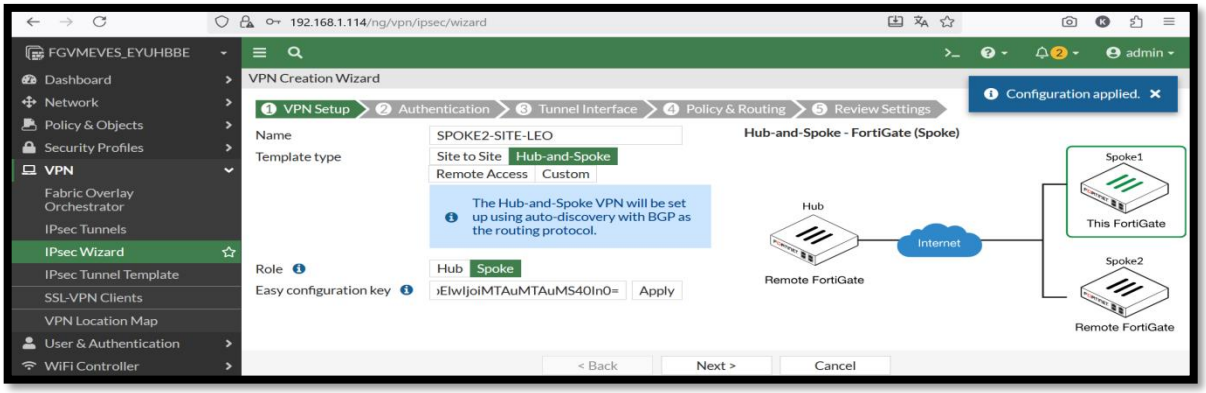

Figura No. 60 Creación túnel VPN SPOKE2

20. Validación de que fue creada de forma correcta el túnel de VPN de León

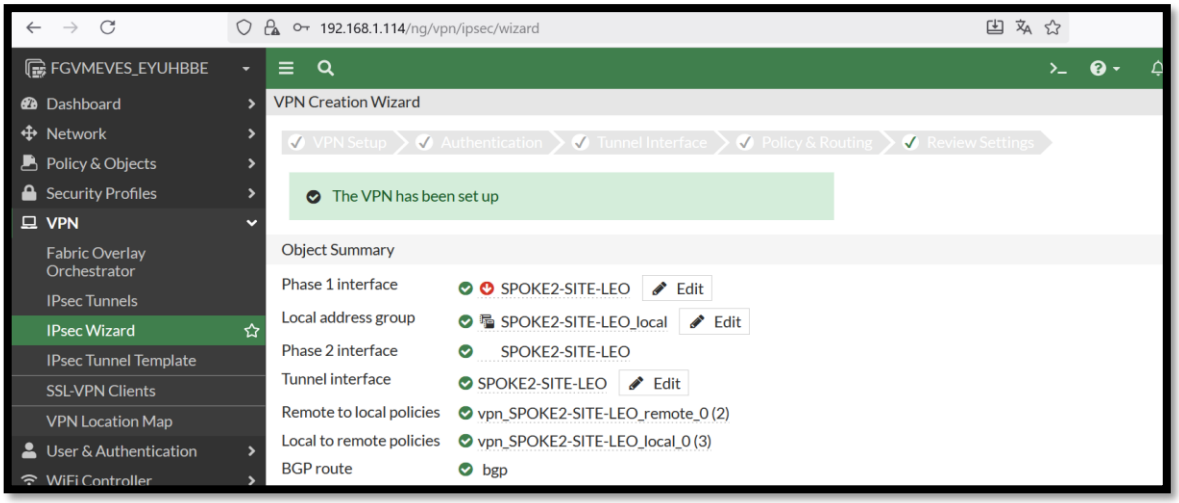

Figura No. 61 Creación de túnel VPN SPOKE2 exitosa

21. Indica que el túnel está activo de León hacia Casa matriz

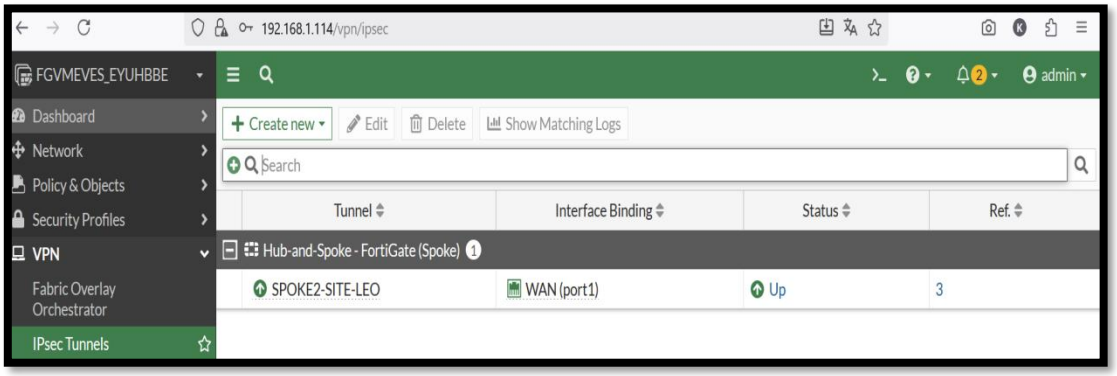

Figura No. 62 Validación de túnel León a CM

22. Ingresando mediante consola para la configuración del switch de León.

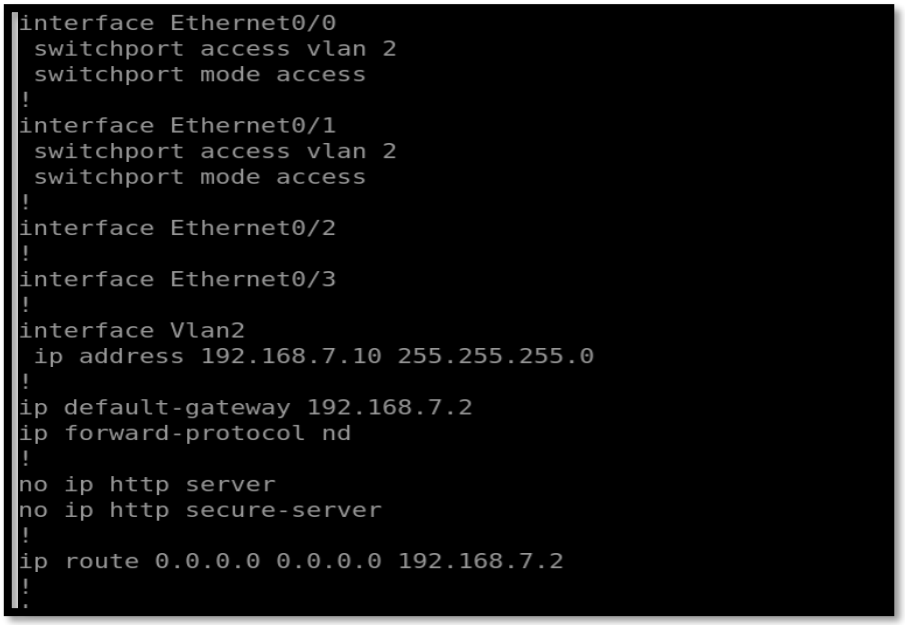

Figura No. 63 Configuración Switch León

23. Ingresando mediante consola para la validación de conexión del switch de León.

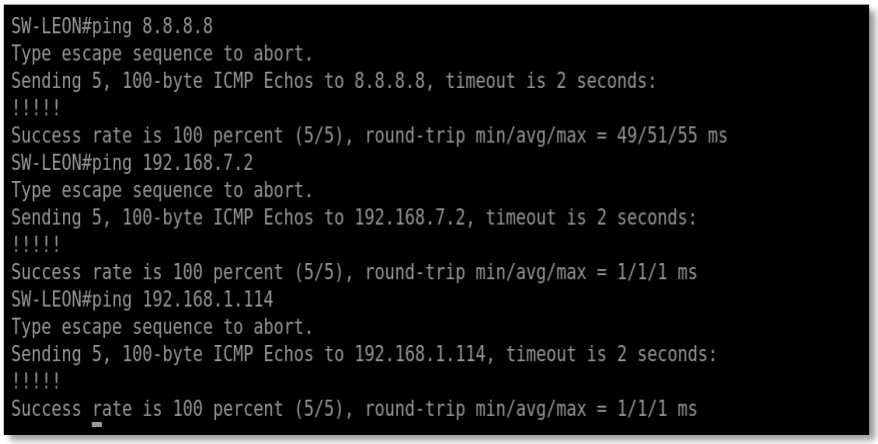

Figura No. 64 Prueba de conectividad switch León.

24. Prueba de conexión desde la PC de León

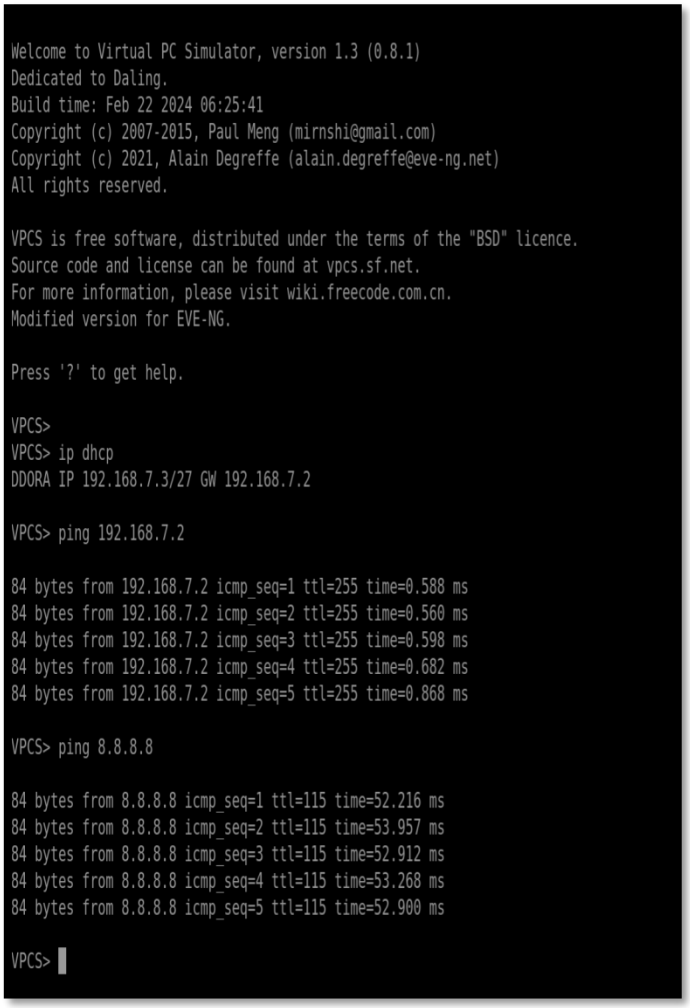

Figura No. 65 Prueba de conectividad VPCS León

5.17 Evaluación y Ajustes

La fase de evaluación se centró en la validación continua del diseño de red propuesto, utilizando los resultados de las pruebas de conectividad y funcionalidad en el entorno simulado de la PYME y sus sucursales.

Para llevar a cabo la simulación fue necesario utilizar el modo de prueba permanente para Fortigate (sin licencia), debido que una de las limitantes de trabajar con esta marca es la licencia para interactuar con la GUI del equipo, se trabajó con la versión 7.4.8 una de las actuales.

Esta decisión se tomó para mitigar una limitante inherente en el entorno de prueba: el periodo de prueba gratuita estándar de FortiGate (típicamente 15 días), ya que implicaba que las configuraciones avanzadas, las políticas de seguridad y todo el progreso del diseño se perderían, forzando una reprocesamiento constante del avance.

Modo de prueba permanente para FortiGate-VM

La licencia permanente de evaluación para máquinas virtuales (VM) reemplaza el período de evaluación de 15 días de FortiGate-VM. Esta licencia se aplica a todas las instancias de nube privada (VMware ESXi, KVM, etc.) y a todas las instancias de nube pública con licencia propia (BYOL).

Al iniciar una nueva máquina virtual FortiGate, puede elegir iniciar sesión en FortiCare para activar la versión de prueba de la máquina virtual o cargar una nueva licencia.

Las limitaciones de la licencia de evaluación de la máquina virtual incluyen lo siguiente:

- Máximo de una copia de evaluación gratuita por cuenta de FortiCare
- Solo se admite el funcionamiento con cifrado bajo, excepto para el acceso a la administración de la interfaz gráfica de usuario y las comunicaciones con FortiManager.
- Máximo de 1 CPU y 2 GB de memoria
- Máximo de tres interfaces, políticas de firewall y rutas
- Sin sujetador de FortiCare
- Sin número para FortiGuard

- Se permiten dos dominios virtuales (VDOM). Al usar el modo multi-VDOM, la raíz de VDOM debe ser de tipo administrador y el otro puede ser un VDOM de tráfico. Consulte Tipos de VDOM.

Para obtener la licencia de prueba permanente de la máquina virtual de Forticare, se realizó el siguiente proceso:

1. Se registró los correos en la página de soporte FORTINET para acceder, se ingresó el correo y damos CLI en crear cuenta.

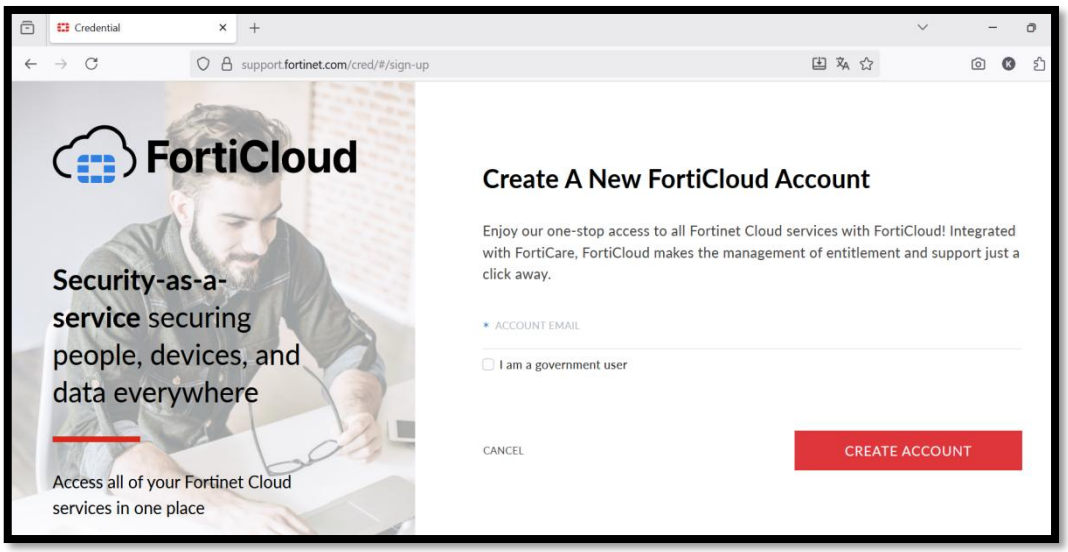

Figura No. 66 Registrando cuenta en FORTINET.

2. Se completaron los datos y confirmación que la cuenta fue creada correctamente, este procedimiento se realiza por cada uno de los FORTINET a utilizar en la simulación

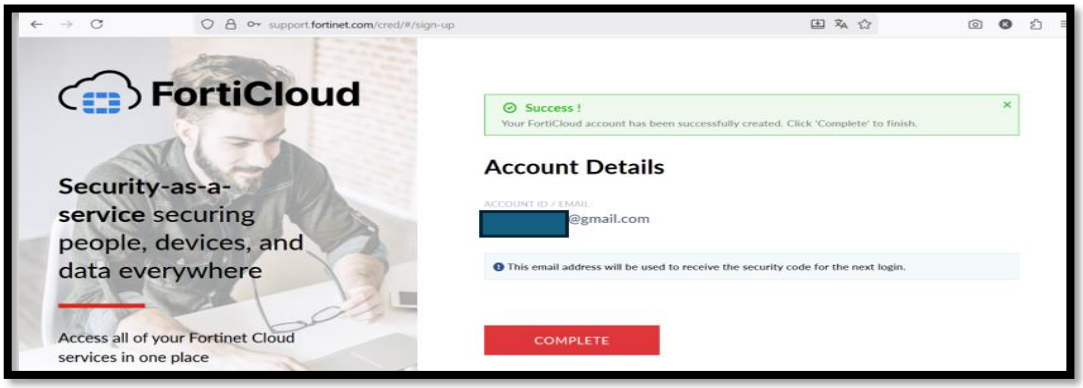

Figura No. 67 Registro exitoso de la cuenta FORTINET

3. Una vez completado esa parte de la cuenta de soporte con FortiGate, se debe ingresar vía web al equipo con la IP que brinda en su interfaz 1, pueden observar la imagen del paso que se realizó y aceptamos los cambios que se aplicaron.

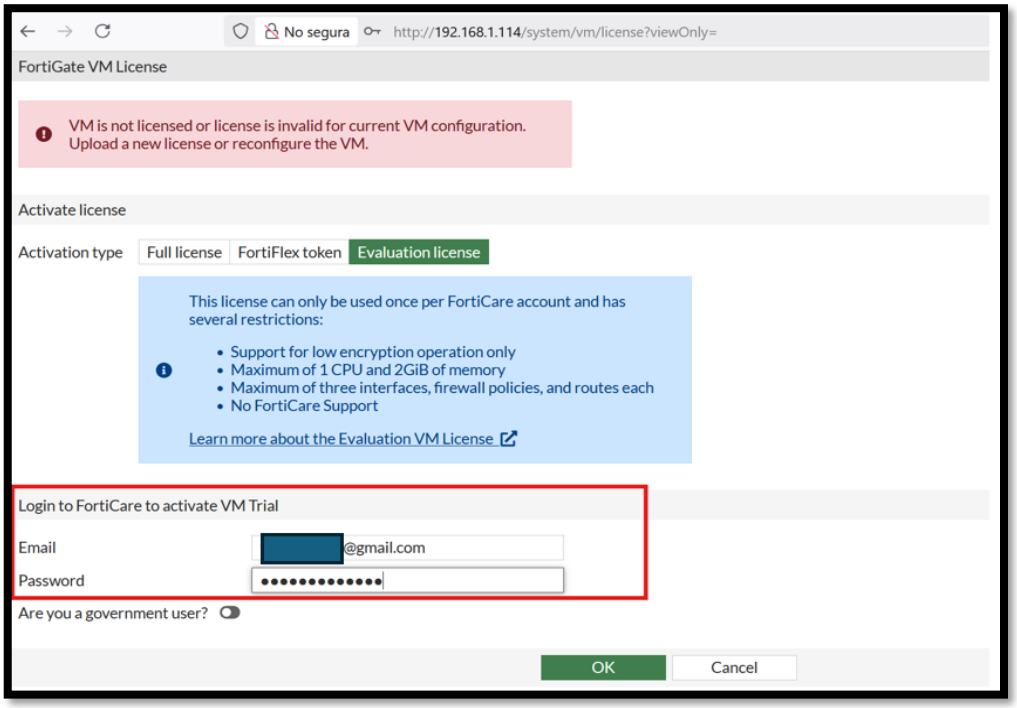

Figura No. 68 Ingresando la cuenta en la GUI para activar licencia de prueba.

4. Después que se manda a reiniciar para aplicar cambios y de esa forma se obtuvo la licencia de prueba permanente.

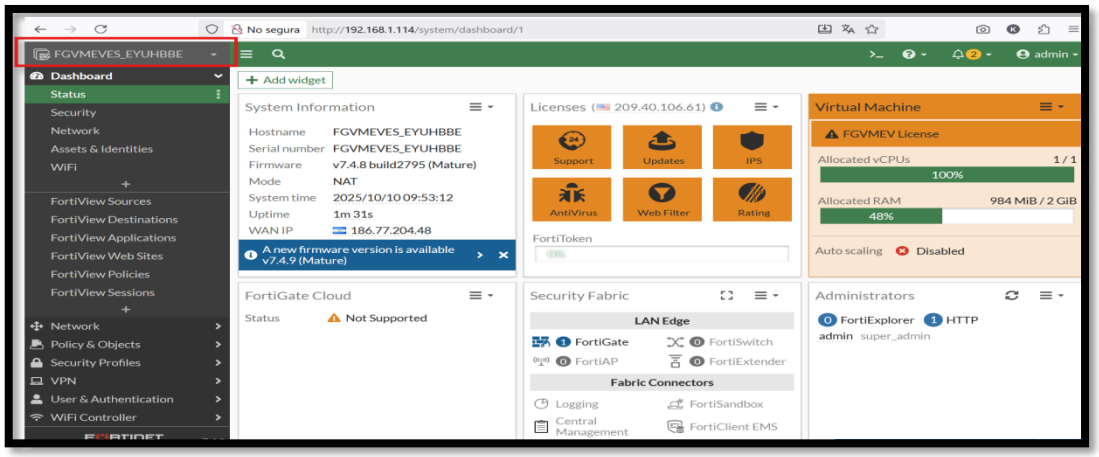

Figura No. 69 Validación de la licencia de prueba permanente

5.18 Realización de ajustes

Según sea necesario para optimizar aún más la eficiencia operativa y la seguridad de datos

1. Validación de BGP de CM y sus sucursales se encuentran debidamente operativas y seguro el tráfico compartido mediante IPSEC.

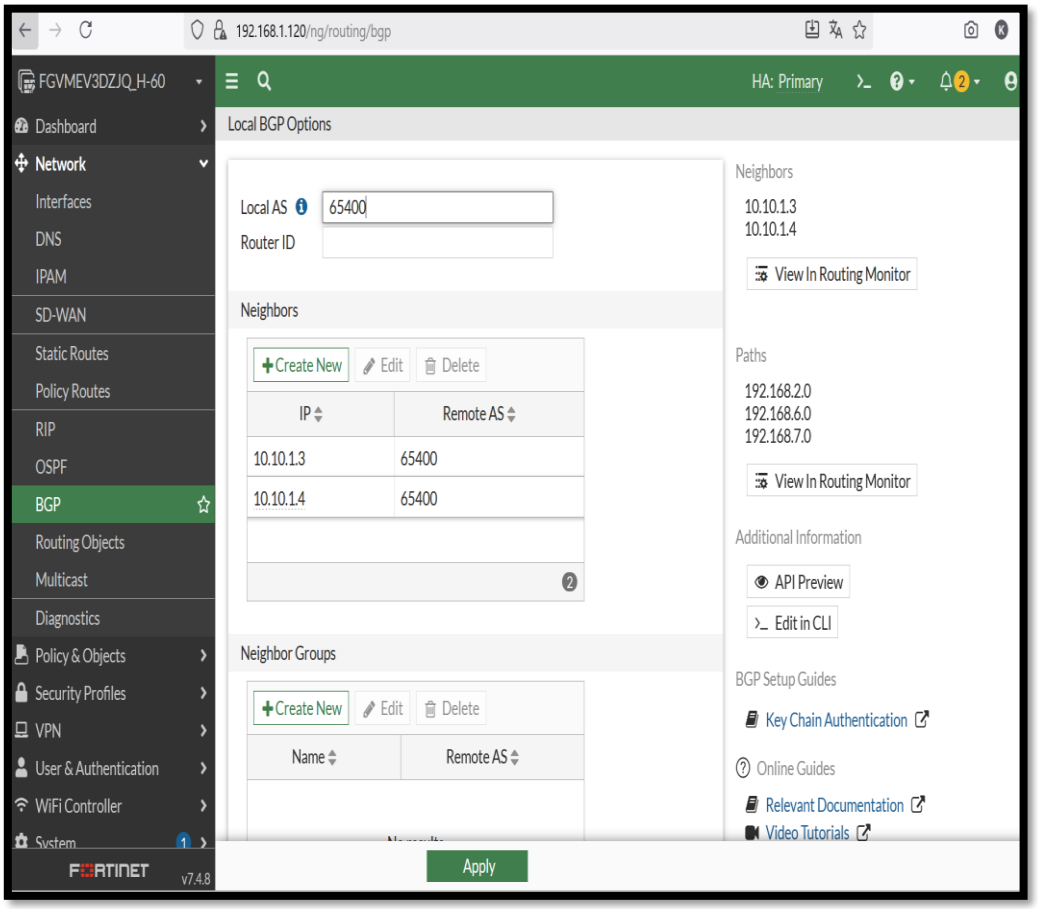

Figura No. 70 Validación de BGP HUB-SPOKE1-SPOKE2.

2. Se concluye que con la capa de seguridad la cual fue establecida y activa por el túnel SPOKE1-SITE-MAS y SPOKE2-SITE-LEO, culminando la negociación satisfactoriamente y garantizando que todo el tráfico transmitido por el enlace WAN esté encriptado y autenticado. Además, la capa de control fue validada, confirmándose que la interfaz de túnel virtual HUB-CM (10.10.1.1) está correctamente configurada para funcionar como un endpoint (punto final) BGP.

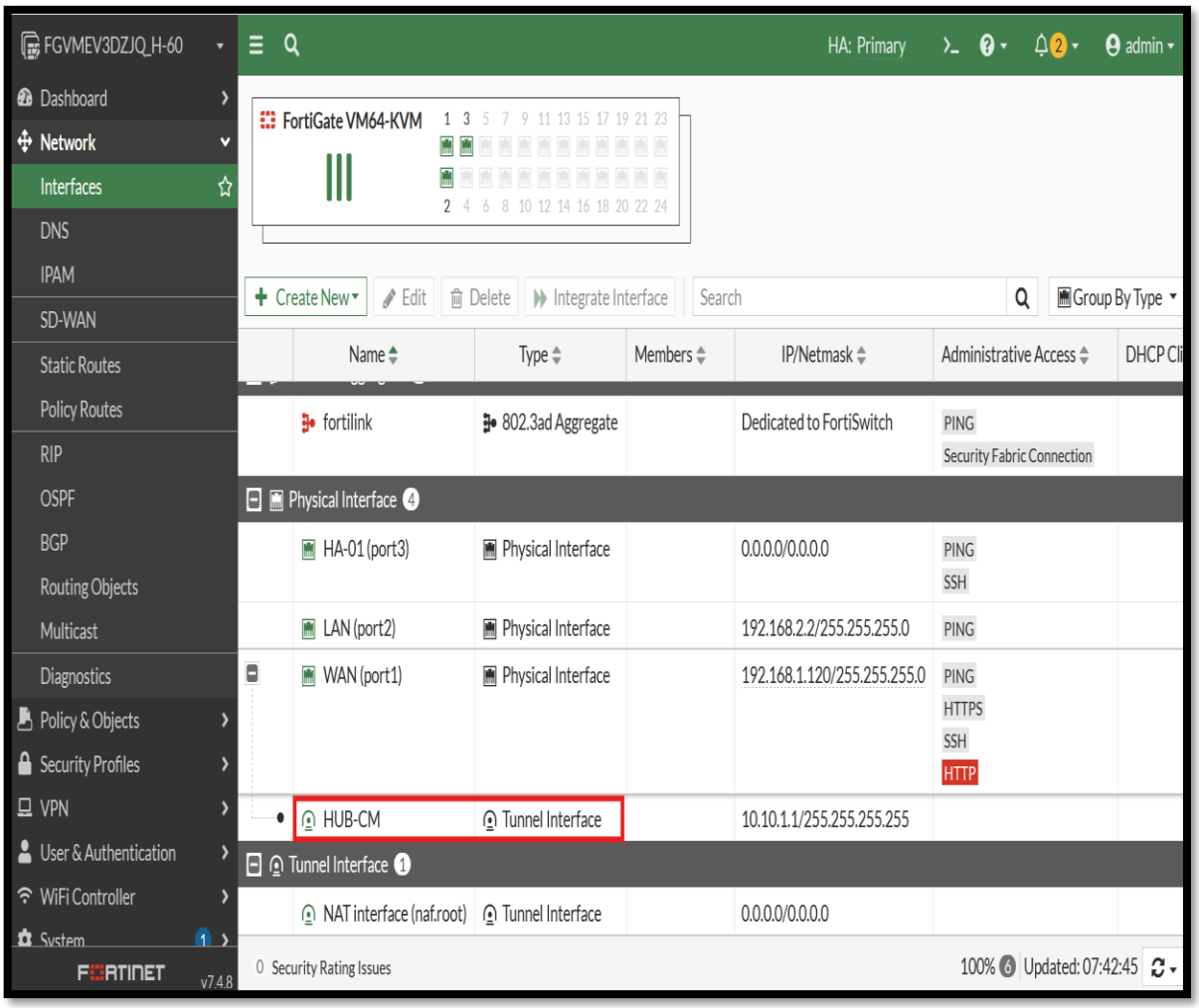

Figura No. 71 Validación de la interfaz WAN de FORTINET CM.

6. Conclusión

El presente trabajo monográfico ha culminado con la satisfacción del objetivo principal. La elaboración de una propuesta de diseño de arquitectura de red e interconexión para una PYME y sus dos sucursales, enfocada en la eficiencia operativa y seguridad de los datos. Este apartado detalla la consecución de los resultados y aborda los desafíos técnicos superados durante la fase de validación.
Para determinar la tecnología y equipos de red adecuados de la seguridad perimetral y segmentación la solución clave fue la integración de equipos *Firewall* **FortiGate** en la capa perimetral y el uso riguroso de la segmentación de red mediante VLANs.
Esta segmentación no solo reduce la asignación de direcciones IP por grupos de usuarios, también aplican políticas de seguridad específicas entre ellos y así asegurar la idoneidad de los equipos de red, tanto en casa matriz como para las sucursales.
Se realizó comparaciones entre los tres principales proveedores de internet que operan en Nicaragua, en donde se seleccionaron dos proveedores (principal y secundario) que cumplan con todas las características necesarias para realizar la interconexión de forma segura y escalable, se recomendó un segundo proveedor para respaldo garantizando la operatividad y disponibilidad de red de la PYME.
Con respecto a la simulación se logró establecer y validar la comunicación mediante la validación del software EVE-NG, la conexión segura entre la Casa Matriz y sus sucursales a través de túneles VPN IPSec creando un ADVPN. Esto garantiza que la información sensible transmitida a través de la red pública de Internet mantenga su confidencialidad e integridad, es un requisito indispensable para la continuidad operativa.
Durante la validación práctica del diseño en el entorno de emulación **EVE-NG**, donde se utilizaron imágenes de máquinas virtuales de FortiGate (FortiGate VM), se encontró una limitación técnica importante en la configuración de Firewalls.
La interfaz gráfica de usuario (GUI) de las versiones virtuales o comunitarias de los equipos FortiGate mostró inestabilidad y restricciones notables al intentar configurar múltiples sub-interfaces de VLAN en 3 interfaz física, y al establecer las complejas

políticas de enrutamiento y VPN. Esto se manifestaba en la no aplicación de cambios, reafirmando que el diseño es técnicamente implementable con equipos físicos de producción.

También se demostró la capacidad de utilizar herramientas de bajo nivel como la CLI para sortear las limitaciones del entorno de laboratorio de EVE-NG, asegurando la fiabilidad del modelo de red desarrollado, esperamos que sea de su agrado y que pueda servir como una guía para pymes que deseen expandirse haciendo uso de las tecnologías de redes, además de ejemplo para los futuros ingenieros en telecomunicaciones o a fines.

Por otra parte, los estudios técnico, económico y operativo confirmaron la viabilidad y la madurez del diseño. El cálculo de ancho de banda estima la selección de enlaces de interconexión, mientras que el estudio económico presentó una estimación de costos transparente y razonable, alineada a la capacidad de inversión de una PYME.

7. Recomendaciones

En esta fase es necesario que se adopten las mejores prácticas de seguridad para la pyme, cuando se implemente esta guía de pasos que se brindó de la interconexión de una Pyme y sus sucursales.

1. Aplicar Filtrado por aplicación

Este perfil se utiliza en las políticas de Firewall para controlar y monitorear el tráfico según el tipo de aplicación, independientemente del puerto que utilice (lo que se conoce como control de aplicaciones de capa 7).

Cabe resaltar que lo deben de ajustar según sus necesidades.

- Vimeo y Vimeo.Video.Play: Se permite el uso para subir o reproducir videos. Esto lo vemos implementado en la pyme para el área de marketing.
- Root.Certificate.URL: Para que la certificación al momento de la navegación permita Https.
- Google.Analytics: Se permite el uso ya que es fundamental si la PYME tiene un sitio web o aplicación que requiere enviar métricas.

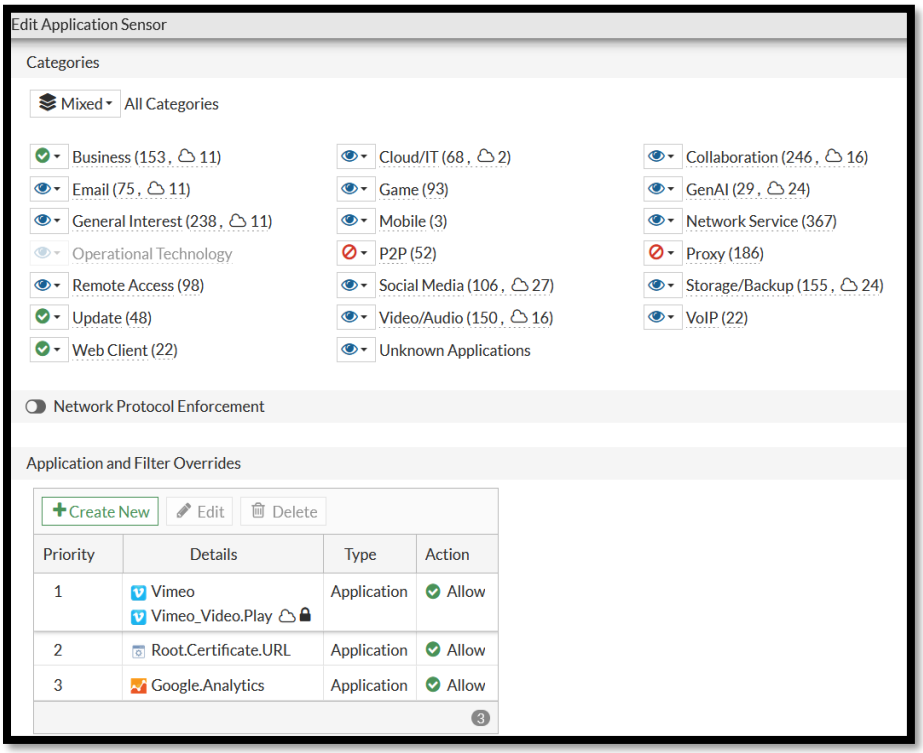

Figura No. 72 Filtrado por aplicación.

2. Aplicar Filtrado WEB

Este perfil de seguridad lo pueden llenar según los privilegios que deseen otorgar al colaborador, ya sea categorizado por puesto de trabajo o de forma general.

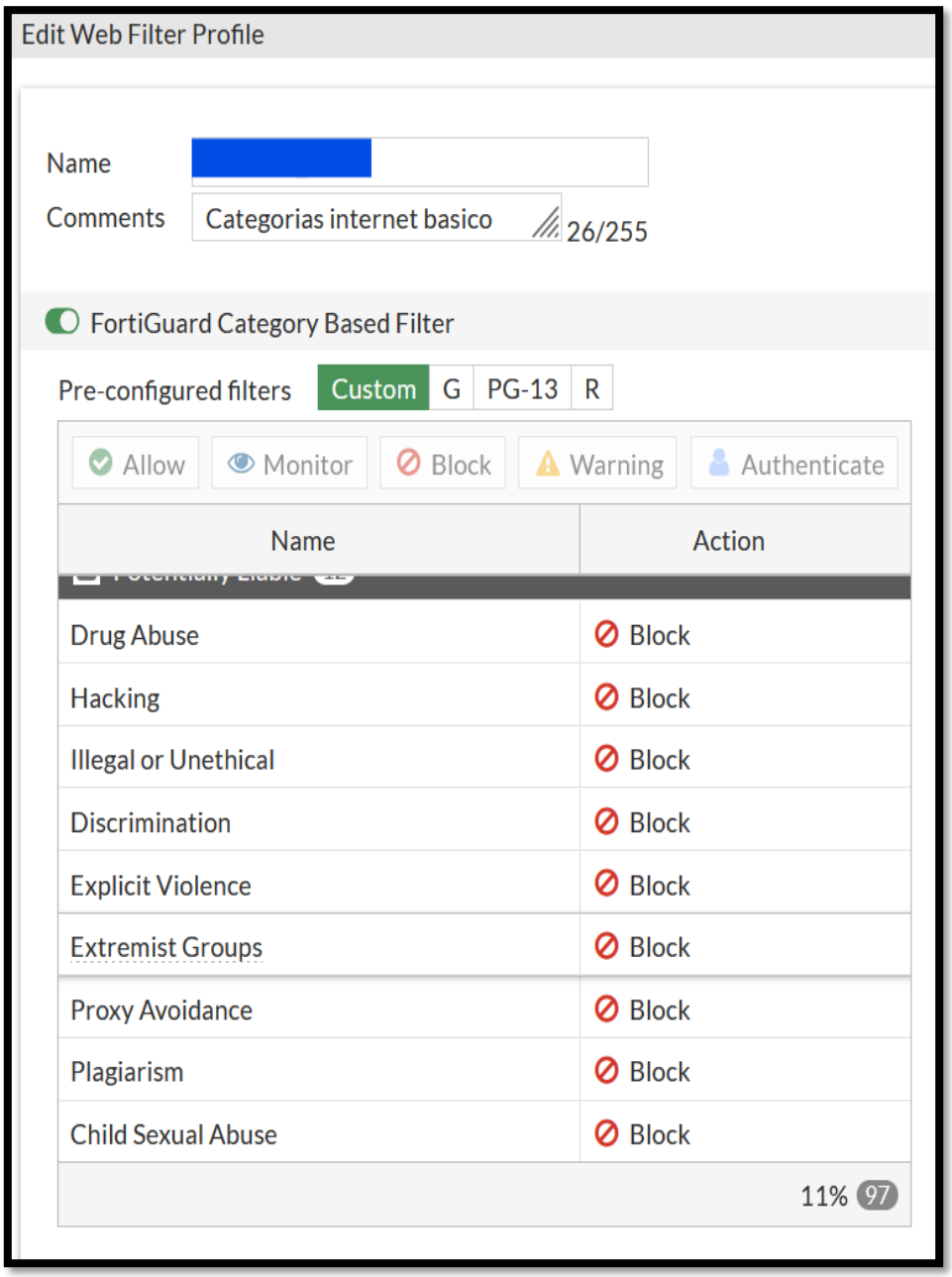

Figura No. 73 Filtrado web.

3. **Aplicar Antivirus**

Ya viene por defecto configurado, solo es necesario habilitarlo.

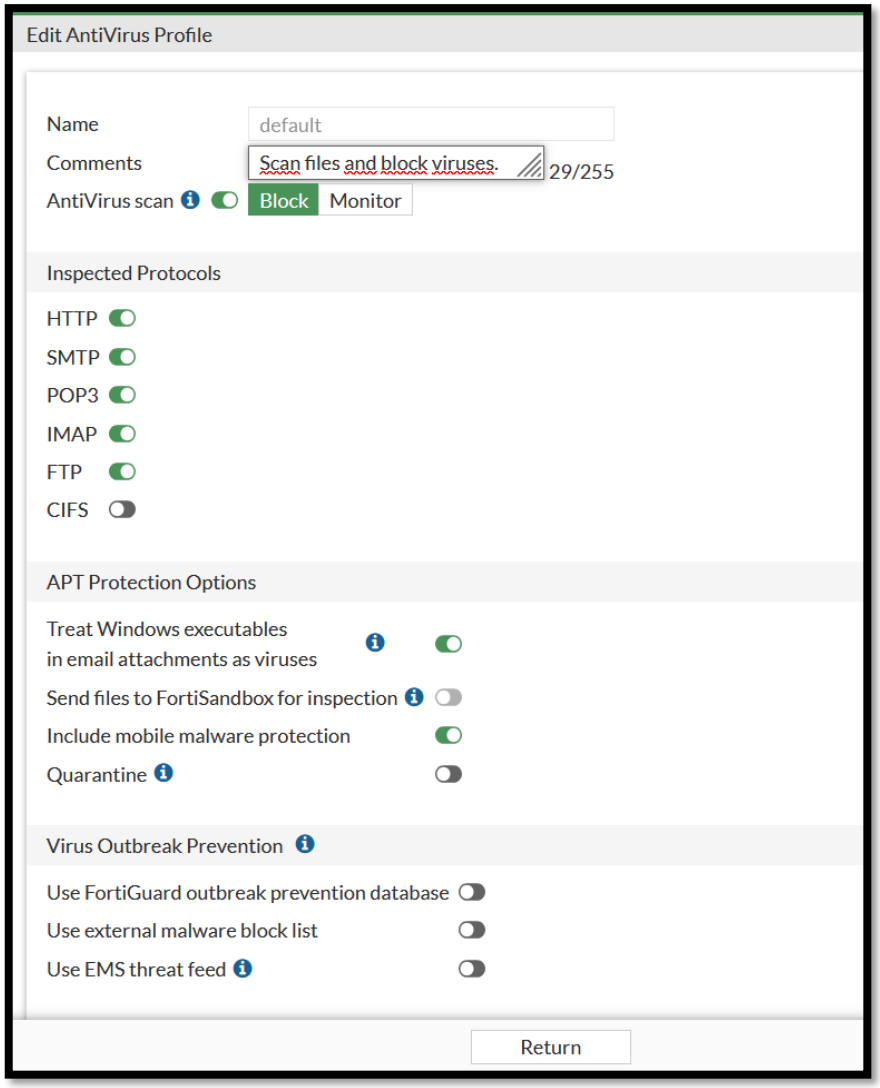

Figura No. 74 Antivirus.

4. **Aplicar políticas que restrinja el tráfico a WhatsApp web, redes sociales, YouTube.**
5. **También se recomienda utilizar ACL en los equipos de distribución y acceso.**

8. Bibliografía

[1] Implika, «¿Qué son las redes informáticas y cómo funcionan?,» Implika, 2024. [En línea]. Available:

https://www.implika.es/blog/que-son-redes-informaticas. [Último acceso: 14 marzo 2024].

[2] Cisco, «Cisco Acadey,» CCNA 1 V7, 2023. [En línea]. Available: https://lms.netacad.com/course/view.php?id=2173930. [Último acceso: 2 2024 marzo].

[3] Aruba, «"HPE Aruba Networking",» ¿QUÉ ES LA TOPOLOGÍA DE RED?, 2024. [En línea].

Available: https://www.arubanetworks.com/es/faq/que-es-la-topologia-de-red/.

[Último acceso: 17 marzo 2024].

[4] Wondershare, «Wondershare,» "Guia completa de la topolgia de redes con ejemplos y planillas gratuitos", 2024. [En línea]. Available: https://www.edrawsoft.com/es/network-topologies.html. [Último acceso: 17 marzo 2024].

[5] José María Barceló Ordinas, Jordi Íñigo Griera, Ramon Martí Escalé, Enric Peig Olivé, «Redes de computadoras,» Fundació per a la Universitat Oberta de Catalunya Primera edición: marzo, 2004. [En línea]. Available: https://libros.metabiblioteca.org/server/api/core/bitstreams/2deaa017-ef04-4f73866c-9a81f23ad1c0/content. [Último acceso: 18 marzo 2024].

[6] J. F. Kurose y K. W. Ross, «Redes de computadoras. Un enfoque descendente Madrid,» Pearson

S.A 7ma edición, 2017. [En línea]. Available:

https://elhacker.info/manuales/Redes/Redes_de_computadoras_Un_enfoque_descendente_James_Kurose_Keith_Ross_2017.pdf. [Último acceso: 18 marzo 2024].

[7] B. O. Bayas, E. S. Mena y J. M. Oviedo, «Fundamentos de redes,» Editorial Grupo

Compás,Guayaquil, Ecuador, 2018. [En línea]. Available:

https://www.researchgate.net/publication/358105030_Libro_de_Fundamentos_de_REDES. [Último acceso: 18 marzo 2024].

[8] IBM, «Redes Protocolo de configuración dinámica de hosts (DHCP),» Copyright IBM Corporation

1998,2014 IBM Versión 7.2 Impreso en España, [En línea]. Available: https://www.ibm.com/docs/es/ssw_ibm_i_72/rzakg/rzakgpdf.pdf. [Último acceso: 25 marzo 2024].

[9] Julio Johnny Regalado Jalca, Vicente Fray Romero Castro, Marieta Del Jesús Azua Menéndez, Galo Roberto Parrales Anzules, Yanina Holanda Campozano Pilay, Angel Leonardo Pin Pin, «Redes de computadoras,» Editorial Área de Innovación y Desarrollo, S.L Primera edición, 2018. [En línea].

https://books.google.com.ec/books?id=rElVDwAAQBAJ&printsec=copyright&hl=es #v=onepage&q&f=f alse. [Último acceso: 23 marzo 2024].

[10] V. R. Martel Velasquez, «Diseño de una red de comunicación VPN sobre internet para un

Distribuidor,» Tesis para optar título e Ingeniero de Redes y Comunicaciones, Universidad Peruana de

Ciencias Aplicadas (UPC), 3 abril 2019. [En línea]. Available:

https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625693/Martel_V v.pdf?sequence=1 &isAllowed=y. [Último acceso: 15 abril 2024].

[11] Fortinet, «¿Qué es la seguridad de autenticación, autorización y contabilidad (AAA)?, Fortinet Cyberglossary (Ciberglosario),» Copyright © 2025 Fortinet, [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/aaa-security. [Último acceso: 13 agosto 2024].

[12] Sheldon, «FS.COM,» Comunidad FS, 21 06 2021. [En línea]. Available: https://community.fs.com/es/article/tcpip-vs-osi-whats-the-difference-between-the-two-models.html.

[Último acceso: 18 11 2024].

[13] J. Climent Fornés, «Virtualización de redes con el emulador EVE-NG,» Trabajo Fin de Grado en

Ingeniería de Tecnologías y Servicios de Telecomunicación, UNIVERSITAT POLITÈCNICA DE

VALÈNCIA, 2023. [En línea]. Available: https://riunet.upv.es/bitstream/handle/10251/197658/Climent%20-%20Virtualizacion%20de%20redes%20con%20el%20emulador%20EVENG.pdf?sequence=1&isAllowed=y. [Último acceso: 31 marzo 2024].

[14] EVE-NG Ltd, «EVE-NG: The Emulated Virtual Environment,» EVE-NG Ltd 2025, [En línea]. Available: https://www.eve-ng.net. [Último acceso: 23 julio 2024].

[15] Marwan Al-shawi, Dustin R. Schuemann, y Andre Laurent, «Enterprise Campus Network Virtualization,» CCDE Study Guide, Cisco Press, 2024. [En línea]. Available: https://www.ciscopress.com/articles/article.asp?p=2448489. [Último acceso: 23 julio 2024].

[17] TELCOR, « Mapas de Cobertura de Servicios de Telecomunicaciones “Red de Fibra Óptica”,» mapas interactivos , 1 Junio 2023. [En línea]. Available: https://telcor.gob.ni/mapas-de-coberturas-detelecomunicaciones-telcor/. [Último acceso: 31 agosto 2024].

[18] Fortinet, «FortiGate 60F – Firewall Fortinet FG-60F,» Ecosistema Ciberseguridad, [En línea]. Available: https://ecosistemaciberseguridad.com/es/pr/fortigate/fortigate-60f-firewall-fortinet-FG..60F7?srsltid=AfmBOoovaO7QwGUUCX_jXPK7R_r2JZ9qrBe988MI576-i_FfoEqjSWu6. [Último acceso: 14 diciembre 2024].

[19] Cisco, «Hoja de datos: Cisco Catalyst 9200 Series Switches,» Switch-Wifi.com, 2020. [En línea]. Available: https://switch-wifi.com/wp-content/uploads/2020/12/Hoja-de-datos-Cisco-Catalyst-9200Series-Switches.pdf. [Último acceso: 13 diciembre 2024].

[20] Cisco, «C9300-48P-E – Cisco Switch Catalyst 9300,» Tetop, [En línea]. Available: https://tetop.co.ke/product/c9300-48p-e-cisco-switch-catalyst-9300/. [Último acceso: 18 diciembre 2024].

[21] CiscoAP, «Cisco Catalyst 9120AX Series Access Points Data Sheet,» Cisco , 29 noviembre 2023. [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-

9120axseries-access-points/datasheet-c78-742115.html. [Último acceso: 17 diciembre 2024].

[22] Fortinet, «FortiGate FG-40F – Firewall de seguridad de red,» Amazon México, [En línea]. Available:

https://www.amazon.com.mx/dp/B084FFFFP9. [Último acceso: 18 diciembre 2024].

[23] C. Systems, «Switch Cisco C9200L-24T-4X-E,» A Computer Service, [En línea]. Available: https://www.acomputerservice.com.pe/cisco/976-switch-cisco-catalyst-9200l-24-puertos101001000mbps-poe-c9200l-24t-4x-e.html. [Último acceso: 18 diciembre 2024].

[24] Cisco Systems, «Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Data Sheet,» Cisco, 29 noviembre 2023. [En línea]. Available:

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheetc78-741988.html. [Último acceso: 18 diciembre 2024].

[25] Fortinet, «FortiGate 60F Series Data Sheet,» AVFirewalls.com, [En línea]. Available:

https://www.avfirewalls.com/datasheets/fg-60f-series.pdf. [Último acceso: 13 diciembre 2024].

[26] CiscoC9200l, «C9200L-48P-4X-E-Datasheet,» Router-Switch.com, [En línea]. Available: https://www.router-switch.com/pdf2html/pdf/c9200l-48p-4x-e-datasheet.pdf. [Último acceso: 13 diciembre 2024].

[27] Cisco, «Hoja de datos: Cisco Catalyst C9300-48P-E,» Router-Switch.com, [En línea]. Available: https://bcms.barghchi.com/storage/uploads/2023/05/ سو -پورت-سیسکو48بیچ--C9300-48P-E.pdf. [Último acceso: 17 diciembre 2024].

[28] Fortinet, «FortiGate/FortiWiFi 40F Series – Data Sheet,» Fortinet, [En línea]. Available: https://www.fortinet.com/resources/data-sheets/fortigate-fortiwifi-40f-series. [Último acceso: 18 diciembre 2024].

[29] Cisco Systems, «Cisco Catalyst C9200L-24P-4X-E Datasheet,» Router-Switch.com, [En línea]. Available: https://www.router-switch.com/pdf2html/pdf/c9200l-24p-4x-e-datasheet.pdf. [Último acceso:

18 diciembre 2024].

[30] Cisco Systems, «Cisco Catalyst C9115AXI-B Datasheet,,» Router-Switch.com, [En línea]. Available: https://www.router-switch.com/pdf2html/pdf/c9115axi-b-datasheet.pdf. [Último acceso: 18 diciembre 2024].

9. Anexo

Datasheet del equipo Forti60F el cual fue seleccionado para la propuesta de FortiGate de la casa Matriz, en donde se especifican las características de este equipo:

System Performance — Enterprise Traffic Mix	
IPS Throughput [2]	1.4 Gbps
NGFW Throughput [2, 4]	1 Gbps
Threat Protection Throughput [2, 5]	700 Mbps
System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps
Firewall Latency (64 byte UDP packets)	4 µs
Firewall Throughput (Packets Per Second)	9 Mpps
Concurrent Sessions (TCP)	700,000
New Sessions/Second (TCP)	35,000
Firewall Policies	5,000
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	500
SSL-VPN Throughput	900 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	750 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	400
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55,000
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps
CAPWAP Throughput (HTTP 64K)	15 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiSwitches Supported	16
Maximum Number of FortiAPs (Total / Tunnel Mode)	30 / 10
Maximum Number of FortiTokens	500
Maximum Number of Registered FortiClients	200
High Availability Configurations	Active / Active, Active / Passive, Clustering

Figura A. 1 Datasheet FortiGate 60F. [25]

Datasheet del equipo C9200L-48P-4XE, para complementar la información de las especificaciones de la interfaz de este:

Model	C9200L-48P-4X-E
Downlinks total 10/100/1000 or PoE+ copper ports	48 ports full PoE+
Uplink configuration	4x 10G fixed uplinks
Default primary AC power supply	PWR-C5-1KWAC
Fans	Fixed redundant
Software	Network Essentials
Stacking bandwidth	80 Gbps
DRAM	2 GB
Flash	4 GB
Switching capacity	176 Gbps
Forwarding rate	261.9 Mpps
Chassis Dimensions	1.73 x 17.5 x 11.3 in 4.4 x 44.5 x 28.8 cm

Figura A. 2 Datasheet switch L2-C9200L-48P-4X. [26]

Datasheet del equipo Switch Modelo C9300-48P-E, esto con el fin de brindar información más de talladas de las características de la interfaz que posee, el cual está plasmada en la siguiente figura.

C9300-48P-E Specification	
Part Number	C9300-48P-E
Product Description	Catalyst 9300 48-port PoE+, Network Essentials
Total 10/100/1000 or Multigigabit copper ports	48 POE+
Default AC power supply	715W AC
Available PoE power	437W
Cisco StackWise-480	Yes
Cisco StackPower	Yes
Default power supply	PWR-C1-715WAC-P/2
Switching capacity	256 Gbps on 48-port Gigabit Ethernet model
Stacking bandwidth	480 Gbps
Total number of MAC addresses	32,000
Total number of IPv4 routes (ARP plus learned routes)	32,000 (24,000 direct routes and 8000 indirect routes)
IPv4 routing entries	32,000
IPv6 routing entries	16,000
Multicast routing scale	8000
QoS scale entries	5120
ACL scale entries	5120
Packet buffer per SKU	16 MB buffer for 24- or 48-port Gigabit Ethernet models
FNF entries	64,000 flow on 24- and 48-port Gigabit Ethernet models
DRAM	8 GB
Flash	16 GB
VLAN IDs	4000
Total Switched Virtual Interfaces (SVIs)	2000
Jumbo frames	9198 bytes
Total routed ports per 9300 Series stack	208

Figura A. 3 Datasheet switch Core C9300L-48P-E. [27]

Datasheet del equipo, esto para brindar mayor información de las especificaciones de la interfaz del equipo:

Software	• Cisco Unified Wireless Network Software Release 8.9.x or later • Cisco IOS XE Software Release 16.11 with AP Device Pack, or later
Supported wireless LAN controllers	• Cisco Catalyst 9800 Series Wireless Controllers • Cisco 3500, 5520, and 8540 Series Wireless Controllers and Cisco Virtual Wireless Controller
802.11n version 2.0 (and related) capabilities	• 4x4 MIMO with four spatial streams • Maximal Ratio Combining (MRC) • 802.11n and 802.11a/g beamforming • 20- and 40-MHz channels • PHY data rates up to 890 Mbps (40 MHz with 5 GHz and 20 MHz with 2.4 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) • 802.11 Dynamic Frequency Selection (DFS) • Cyclic Shift Diversity (CSD) support
802.11ac	• 4x4 downlink MU-MIMO with four spatial streams • MRC • 802.11ac beamforming • 20-, 40-, 80-, and 160-MHz channels • PHY data rates up to 3.47 Gbps (160 MHz with 5 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) • 802.11 DFS • CSD support
802.11ax	• 4x4 downlink MU-MIMO with four spatial streams • Uplink/downlink OFDMA • TWT • BSS coloring • MRC • 802.11ax beamforming • 20-, 40-, 80-, and 160-MHz channels • PHY data rates up to 5.38 Gbps (160 MHz with 5 GHz and 20 MHz with 2.4 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) • 802.11 DFS • CSD support
Integrated antenna	Flexible radio (either on 2.4 GHz or on 5 GHz) • 2.4 GHz, peak gain 4 dBi, internal antenna, omnidirectional in azimuth • 5 GHz, peak gain 5 dBi, internal antenna, omnidirectional in azimuth Dedicated 5-GHz radio • 5 GHz, peak gain 5 dBi, internal antenna, omnidirectional in azimuth
External antenna (sold separately)	• Cisco Catalyst 9120AXE Access Points are certified for use with antenna gains up to 6 dBi (2.4 GHz and 5 GHz) • Cisco Catalyst 9120AXP Access Points) are certified for use with antenna gains up to 13 dBi (2.4 GHz and 5 GHz) with the AIR-ANT2513P4M-N= antenna • Cisco offers the industry's broadest selection of antennas, delivering optimal coverage for a variety of deployment scenarios • Supports Self-Identifiable Antennas (SIA) on one RP-TNC port • For more details, see the Catalyst 9120AX Series Deployment Guide.
Smart antenna connector	• Available on the 9120AXE and 9120AXP only • Compact multi-RF connector with DART interface • Requires the AIR-CAB002-DART-R= 2 ft smart antenna connector when used with antennas with RP-TNC connector • Required when running the flexible radio as either a second 5-GHz serving radio or a Wireless Security Monitoring radio

Figura A. 4 Datasheet Access point C9120. [21]

Datasheet del equipo el cual seleccionamos para propuesta de FortiGate de las sucursales de Masaya y León, en donde se adjuntó esta figura para brindar más detalles del sistema y características de la interfaz del equipo

System Performance — Enterprise Traffic Mix	
IPS Throughput [2]	1 Gbps
NGFW Throughput [2, 4]	800 Mbps
Threat Protection Throughput [2, 5]	600 Mbps
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	5 / 5 / 5 Gbps
Firewall Latency (64 byte, UDP)	2.97 µs
Firewall Throughput (Packet per Second)	7.5 Mpps
Concurrent Sessions (TCP)	700 000
New Sessions/Second (TCP)	35 000
Firewall Policies	2000
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	250
SSL-VPN Throughput [6]	490 Mbps
Concurrent SSL-VPN Users [6] (Recommended Maximum, Tunnel Mode)	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	320
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000
Application Control Throughput (HTTP 64K) [2]	990 Mbps
CAPWAP Throughput (HTTP 64K)	3.5 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiSwitches Supported	8
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8
Maximum Number of FortiTokens	500
High Availability Configurations	Active-Active, Active-Passive, Clustering

Figura A. 5 Datasheet FORTINET 40F. [28]

Datasheet para brindar mayor información de este, la figura de la tabla de especificaciones es la siguiente.

Model	C9200L-24P-4X-E
Downlinks total 10/100/1000 or PoE+ copper ports	24 ports full PoE+
Uplink configuration	4x 10G fixed uplinks
Default primary AC power supply	PWR-C5-600WAC
Fans	Fixed redundant
Software	Network Advantage
Stacking bandwidth	80 Gbps
DRAM	2 GB
Flash	4 GB
Switching capacity	128 Gbps
Forwarding rate	190.4 Mpps
Chassis Dimensions	1.73 x 17.5 x 11.3 in 4.4 x 44.5 x 28.8 cm

Figura A. 6 Datasheet Switch Modelo C91200-24P-4X-E. [29]

Datasheet donde se refleja mayor información de las características de la interfaz del equipo seleccionado, la cual es la siguiente:

C9115AXI-B Specification	
Description	Cisco Catalyst 9115AX Series Access Point, Internal antenna; Wi-Fi 6; 4x4:4 MIMO, B Domain
Software	• Cisco Unified Wireless Network Software Release 8.9 or later • Cisco IOS ® XE Software Release 16.11 or later
Supported wireless LAN controllers	• Cisco Catalyst 9800 Series Wireless Controllers • Cisco 3500, 5520, and 8540 Series Wireless Controllers and Cisco Virtual Wireless Controller
802.11n version 2.0 (and related) capabilities	• 4x4 MIMO with four spatial streams • Maximal Ratio Combining (MRC) • 802.11n and 802.11a/g beamforming • 20- and 40-MHz channels • PHY data rates up to 890 Mbps (40 MHz with 5 GHz and 20 MHz with 2.4 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) • 802.11 Dynamic Frequency Selection (DFS) • Cyclic Shift Diversity (CSD) support
802.11ac	• 4x4 downlink MU-MIMO with four spatial streams • MRC • 802.11ac beamforming • 20-, 40-, 80-, and 160-MHz channels • PHY data rates up to 3.47 Gbps (160 MHz with 5 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) • 802.11 DFS • CSD support
802.11ax	• 4x4 downlink MU-MIMO with four spatial streams • Uplink/downlink OFDMA • TWT • BSS coloring • MRC • 802.11ax beamforming • 20-, 40-, 80-, and 160-MHz channels • PHY data rates up to 5.38 Gbps (160 MHz with 5 GHz and 20 MHz with 2.4 GHz) • Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) • 802.11 DFS • CSD support
Integrated antenna	• 2.4 GHz, peak gain 3 dBi, internal antenna, omnidirectional in azimuth • 5 GHz, peak gain 4 dBi, internal antenna, omnidirectional in azimuth

Figura A. 7 Datasheet Access point C9115. [30]

Tablas de direccionamiento para la PYME

Tabla A.1 direccionamiento de red Casa Matriz.

DIRECCIONAMIENTO CASA MATRIZ					
NO. SUBRED	**RED**	**MASCARA**	**GATEWAY**	**VLAN**	**DESCRIPCION**
1	192.168.3.0	255.255.255.224	192.168.3.1	2	EQUIPOS
2	192.168.3.32	255.255.255.224	192.168.3.33	3	USUARIOS
3	192.168.3.64	255.255.255.224	192.168.3.65	4	GTI
4	192.168.3.96	255.255.255.224	192.168.3.97	5	AP
5	192.168.3.128	255.255.255.224	192.168.3.129	6	IMPRESORA
6	192.168.3.160	255.255.255.224	192.168.3.161	7	CCTV

Tabla A. 2 Enrutamiento utilizado en la topología.

ENRUTAMIENTO FORTINET CM CON SW-CORE					
SUBRED	**GATEWAY**	**MASCARA**	**INTERFAZ-FORTINET**	**ISP**	**INTERFAZ SWCORE**
192.168.1.0	192.168.1.120	255.255.255.0	PUERTO 1(WAN)	ISP1	N/A
192.168.1.0	192.168.1.220	255.255.255.0	PUERTO 1(WAN)	ISP2	N/A
192.168.2.0	192.168.2.2	255.255.255.0	PUERTO 2(LAN)	ISP1	ETHERNET 0/1
192.168.4.0	192.168.4.1	255.255.255.0	PUERTO 2(LAN)	ISP2	ETHERNET 0/2
ENRUTAMIENTO FORTINET MASAYA Y SWITCH					
SUBRED	**GATEWAY**	**MASCARA**	**INTERFAZ**	**CONEXIÓN**	
192.168.1.0	192.168.1.114	255.255.255.0	PUERTO 1(WAN)	ISP	
192.168.6.0	192.168.6.2	255.255.255.224	PUERTO 2(LAN)	ISP HACIA SWITCHACCESSO	
ENRUTAMIENTO FORTINET LEON Y SWITCH					
SUBRED	**GATEWAY**	**MASCARA**	**INTERFAZ**	**CONEXIÓN**	
192.168.1.0	192.168.1.160	255.255.255.0	PUERTO 1(WAN)	ISP	
192.168.7.0	192.168.7.2	255.255.255.224	PUERTO 2(LAN)	ISP HACIA SWITCHACCESSO	

Tabla A. 3 Asignación de VLAN por área Casa matriz.

AREA	VLAN	SUBRED	IP GATEWAY	RANGO	MASCARA
1,2,3	3	192.168.3.32	192.168.3.33	192.168.3.40-62	255.255.255.224
4	4	192.168.3.64	192.168.3.65	192.168.3.71-192.168.3.94	255.255.255.224
5,6,7	5	192.168.3.96	192.168.3.97	192.168.3.104-192.168.3.126	255.255.255.224
8,9,10	6	192.168.3.128	192.168.3.129	192.168.3.134-192.168.3.158	255.255.255.224

Tabla A. 4 Direccionamiento Sucursal Masaya.

DIRECCIONAMIENTO SUCURSAL MASAYA				
No. SUBRED	**RED**	**MASCARA**	**GATEWAY**	**VLAN**
1	192.168.6.0	255.255.255.224	192.168.6.2	2
2	192.168.6.32	255.255.255.224	192.168.6.33	3
3	192.168.6.64	255.255.255.224	192.168.6.65	4
4	192.168.6.96	255.255.255.224	192.168.6.97	5
5	192.168.6.128	255.255.255.224	192.168.6.129	6

Tabla A. 5 Asignación de VLANs en sucursal Masaya.

ÁREA	VLAN	SUBRED	IP GATEWAY	RANGO DE DIRECCIONAMIENTO POR DHCP	MASCARA
1,2	3	192.168.6.32	192.168.6.33	192.168.6.39-192.168.6.62	255.255.255.224
3	4	192.168.6.64	192.168.6.65	192.168.6.70-192.168.6.94	255.255.255.224
4,5	5	192.168.6.96	192.168.6.97	192.168.6.104-192.168.6.126	255.255.255.224

Tabla A. 6 Direccionamiento Sucursal León.

DIRECCIONAMIENTO SUCURSAL LEÓN				
NO. SUBRED	**RED**	**MASCARA**	**GATEWAY**	**VLAN**
1	192.168.7.0	255.255.255.224	192.168.7.1	2
2	192.168.7.32	255.255.255.224	192.168.7.33	3
3	192.168.7.64	255.255.255.224	192.168.7.65	4
4	192.168.7.96	255.255.255.224	192.168.7.97	5
5	192.168.7.128	255.255.255.224	192.168.7.129	6

Tabla A. 7 Asignación de VLANs en sucursal León.

AREA	**VLAN**	**SUBRED**	**IP GATEWAY**	**RANGO DE DIRECCIONAMIENTO POR DHCP**	**MASCARA**
1,2	3	192.168.7.32	192.168.7.33	192.168.7.39- 192.168.7.62	255.255.255.224
3	4	192.168.7.64	192.168.7.65	192.168.7.70- 192.168.7.94	255.255.255.224
4,5	5	192.168.7.96	192.168.7.97	192.168.7.104- 192.168.7.126	255.255.255.224

Instalación en EVE-NG modo Bare Metal

Se instala un sistema operativo base (como Ubuntu Server) directamente en el hardware, en lugar de hacerlo dentro de una máquina virtual. Los pasos clave incluyen descargar la imagen ISO del sistema operativo, crear una unidad USB de arranque, arrancar desde ella y seguir el instalador para seleccionar el idioma, configurar el almacenamiento (a menudo sobrescribiendo todo el disco), crear una cuenta de usuario y habilitar SSH para la gestión remota.

Figura A. 8 Requisitos de Nuestro Servidor.

Figura A. 9 Bare Metal Options.

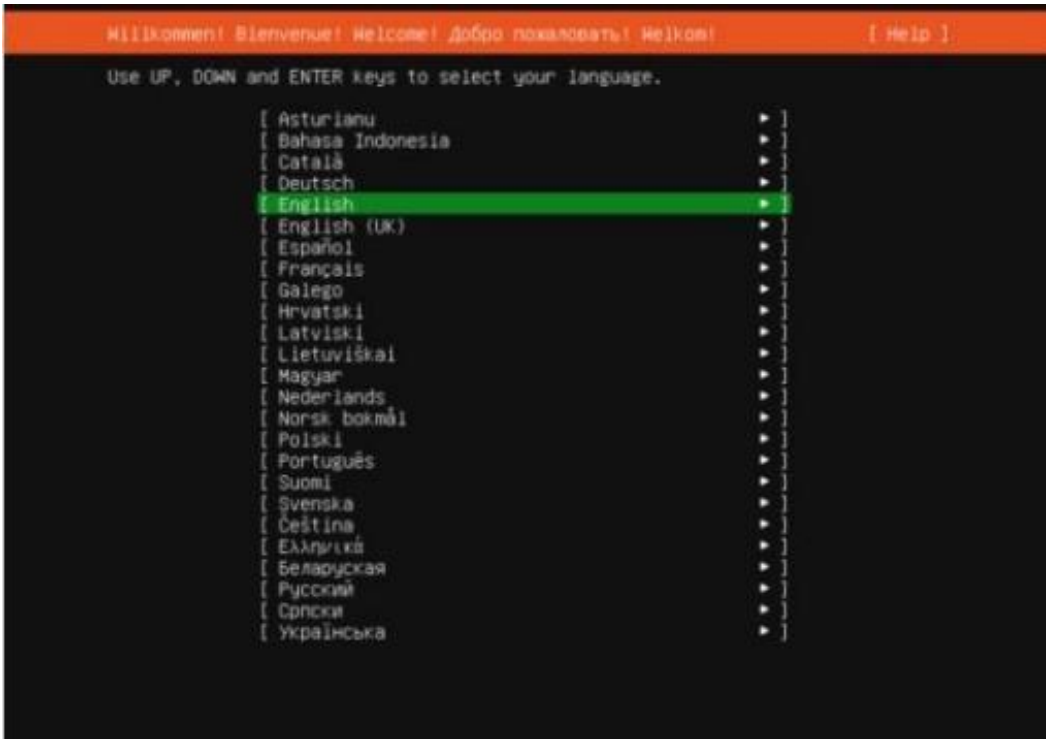

Figura A. 10 Seleccionar Idioma.

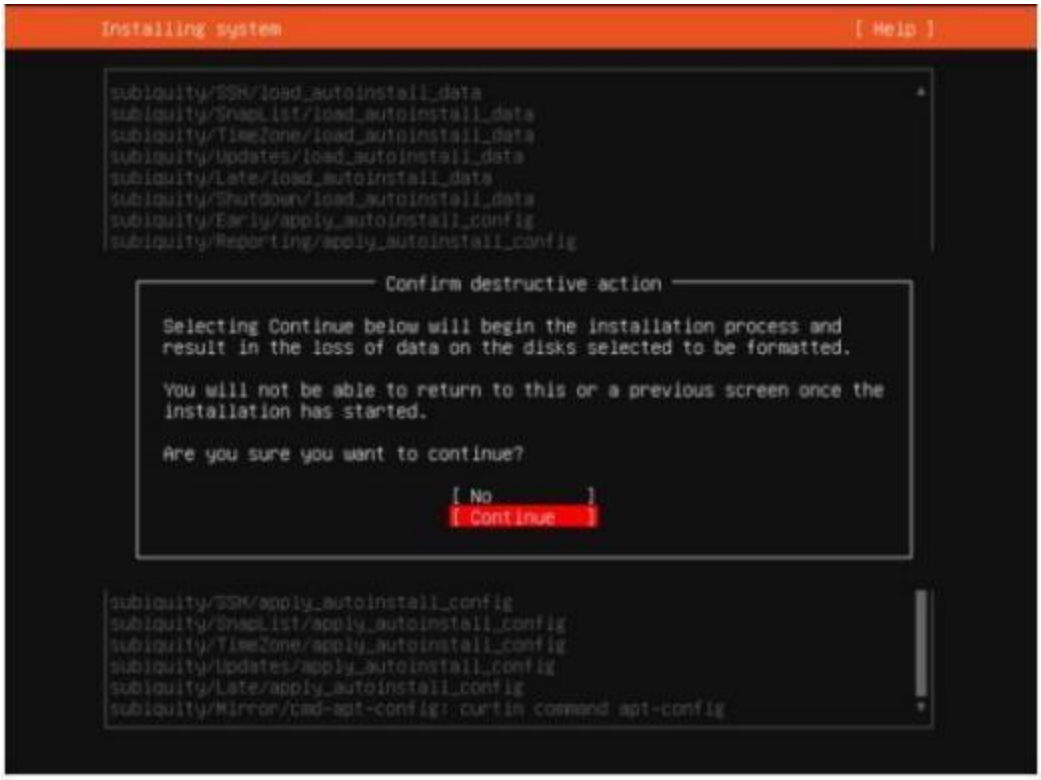

Figura A. 11 Instalación EVE-NG.

Figura A. 12 Iniciando EVE-GN.

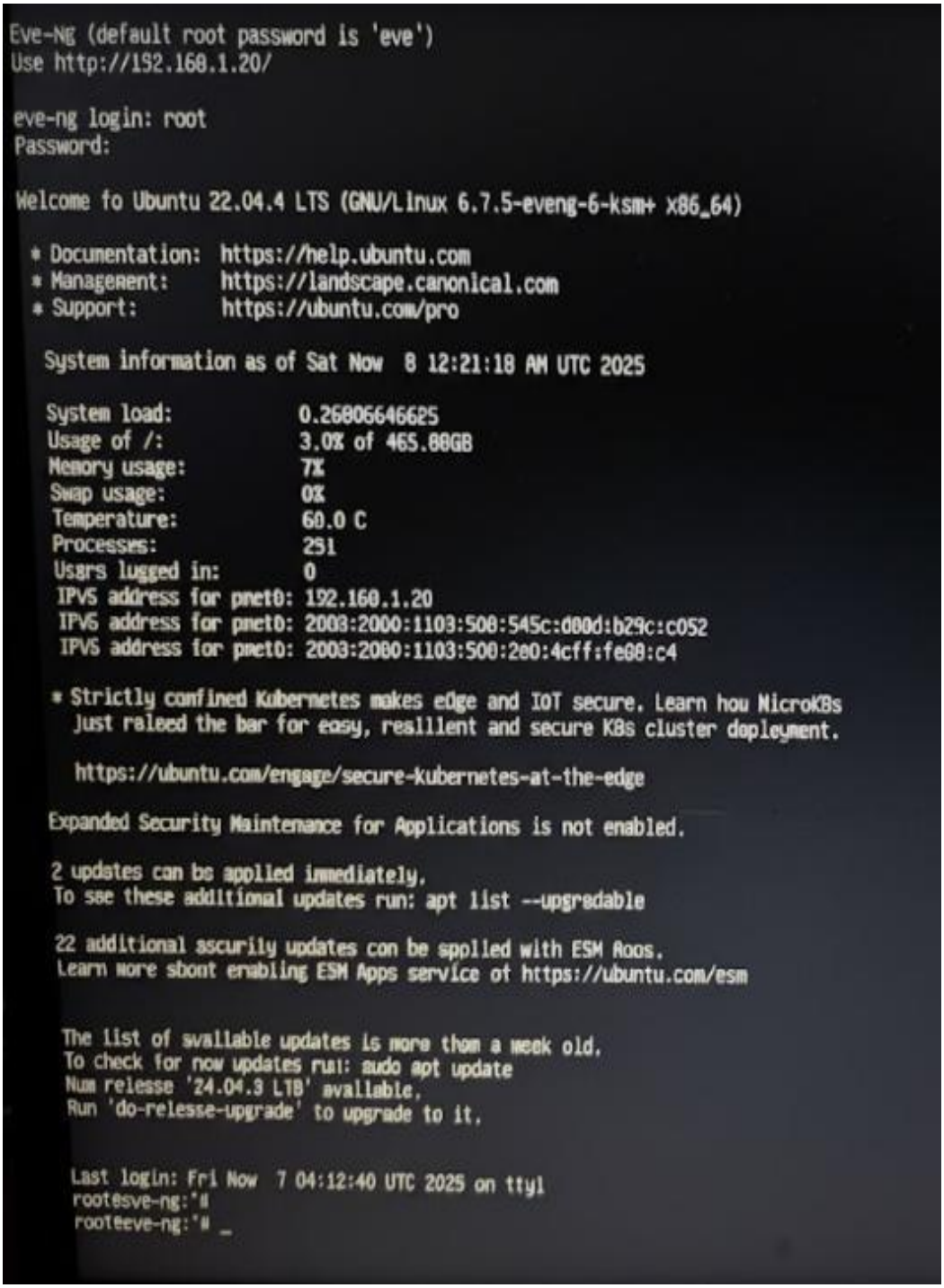

Figura A. 13 Iniciar sesión EVE-NG.

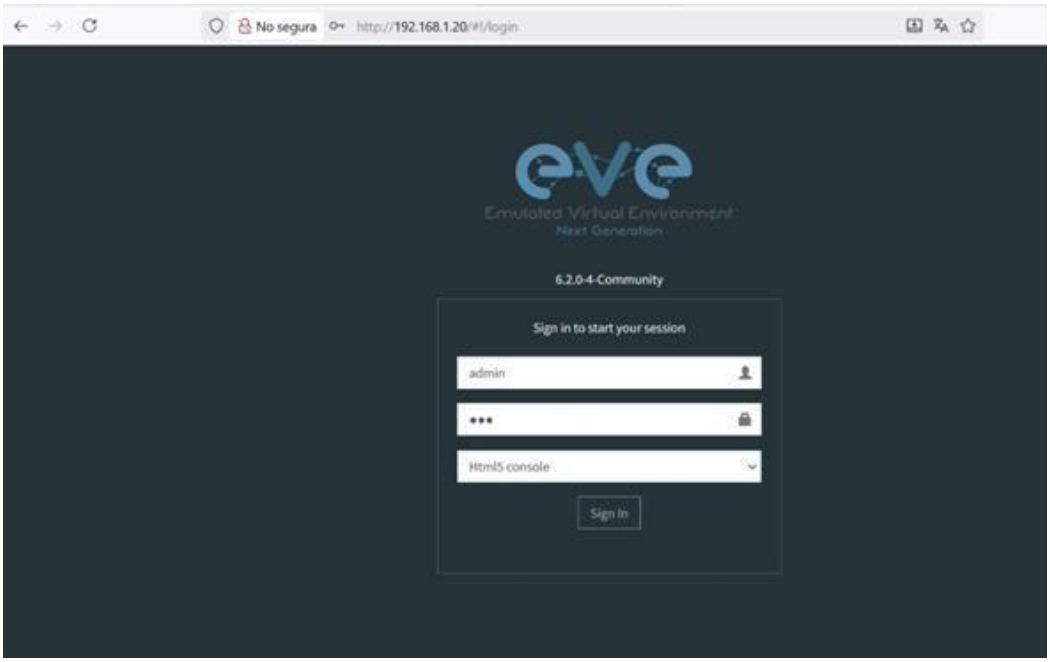

Figura A. 14 Iniciar sesión en HTMl5 console.

Se ingresa mediante PUTTY con conexión SSH a la CLI del servidor donde se está ejecutando el software EVE-NG.

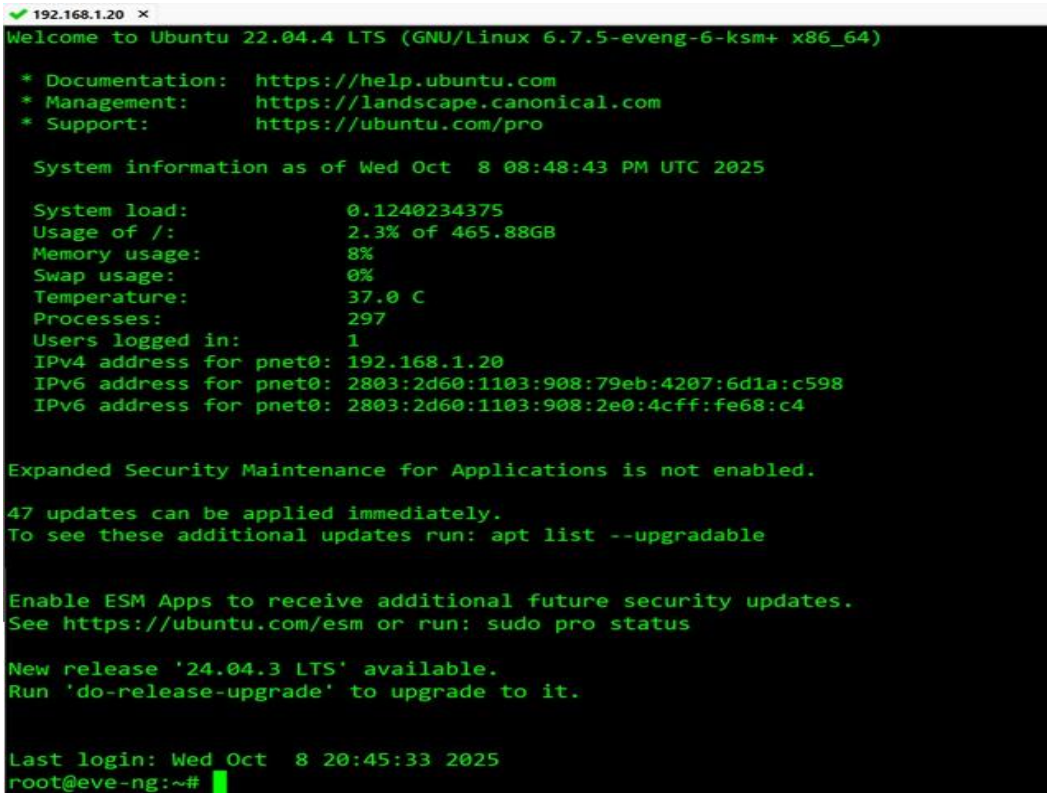

Figura A. 15 Inicio por SSH.

Figura A. 16 Se agrego imagen de FORTINET.

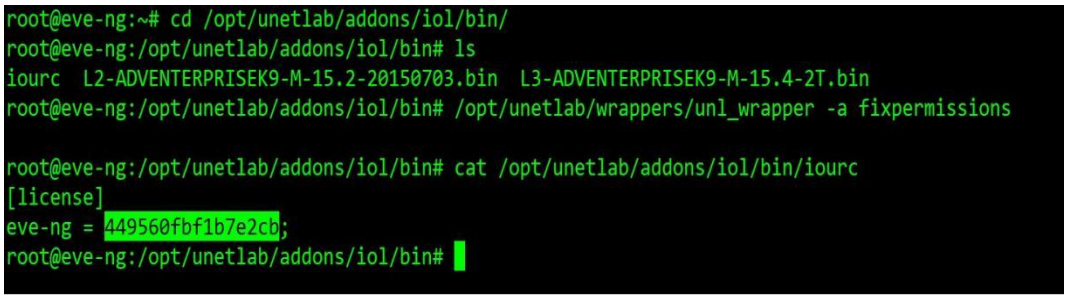

Figura A. 17 Creamos directorio en EVE-NG imagen IOL.

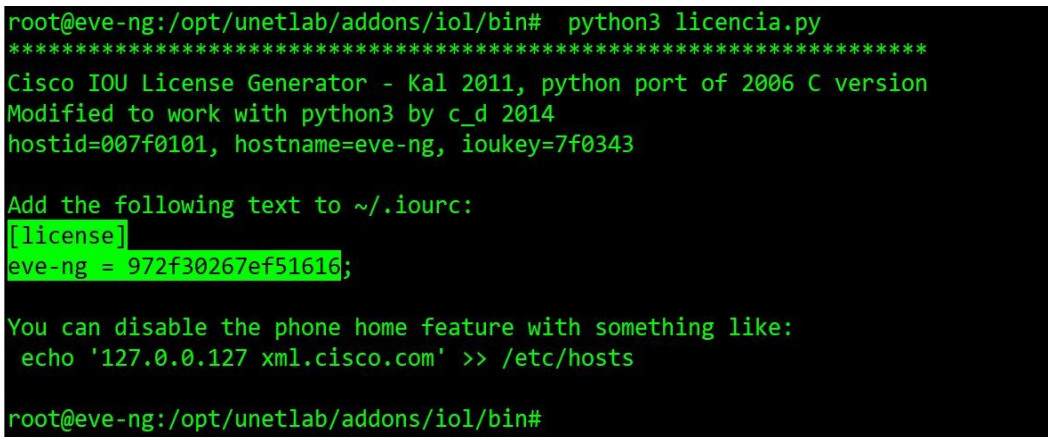

Figura A. 18 Activamos licencia equipo IOL.

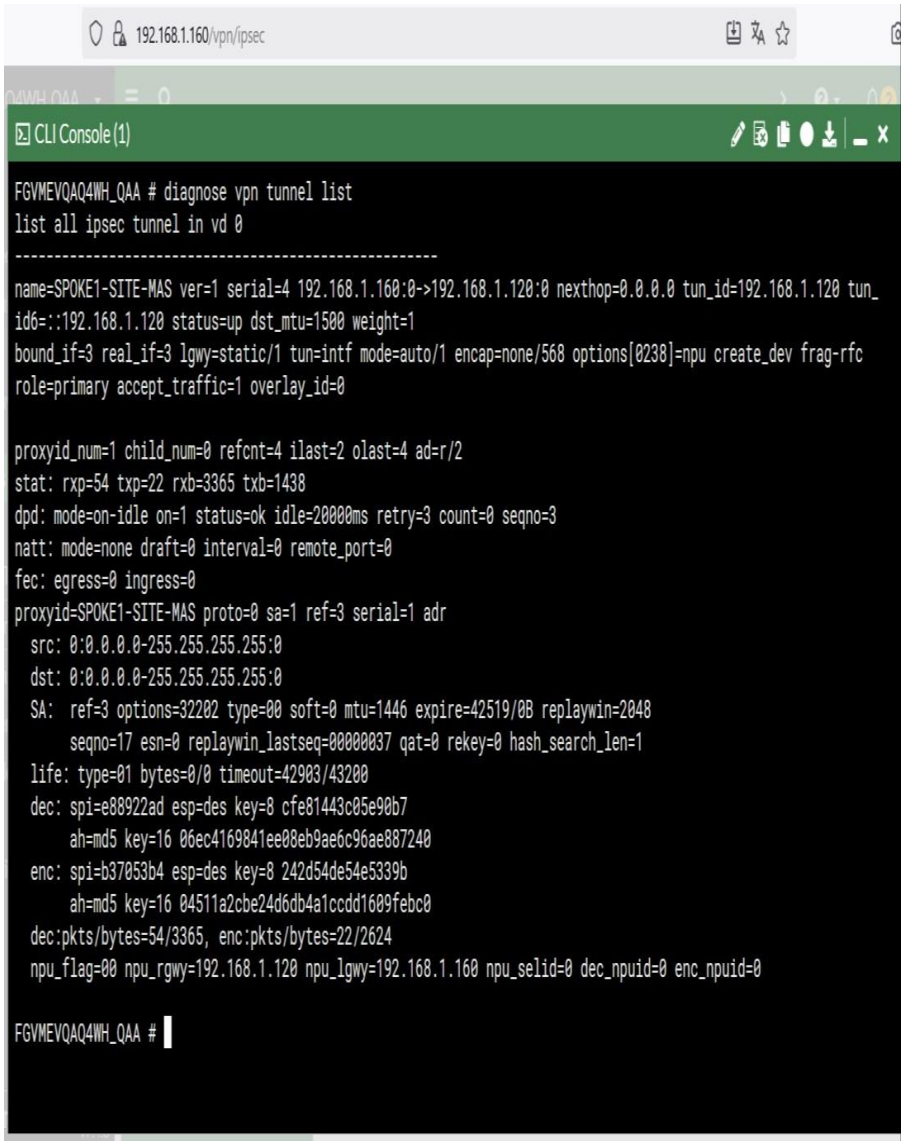

Figura A. 19 Validación por medio de CLI del estado túnel Masaya.

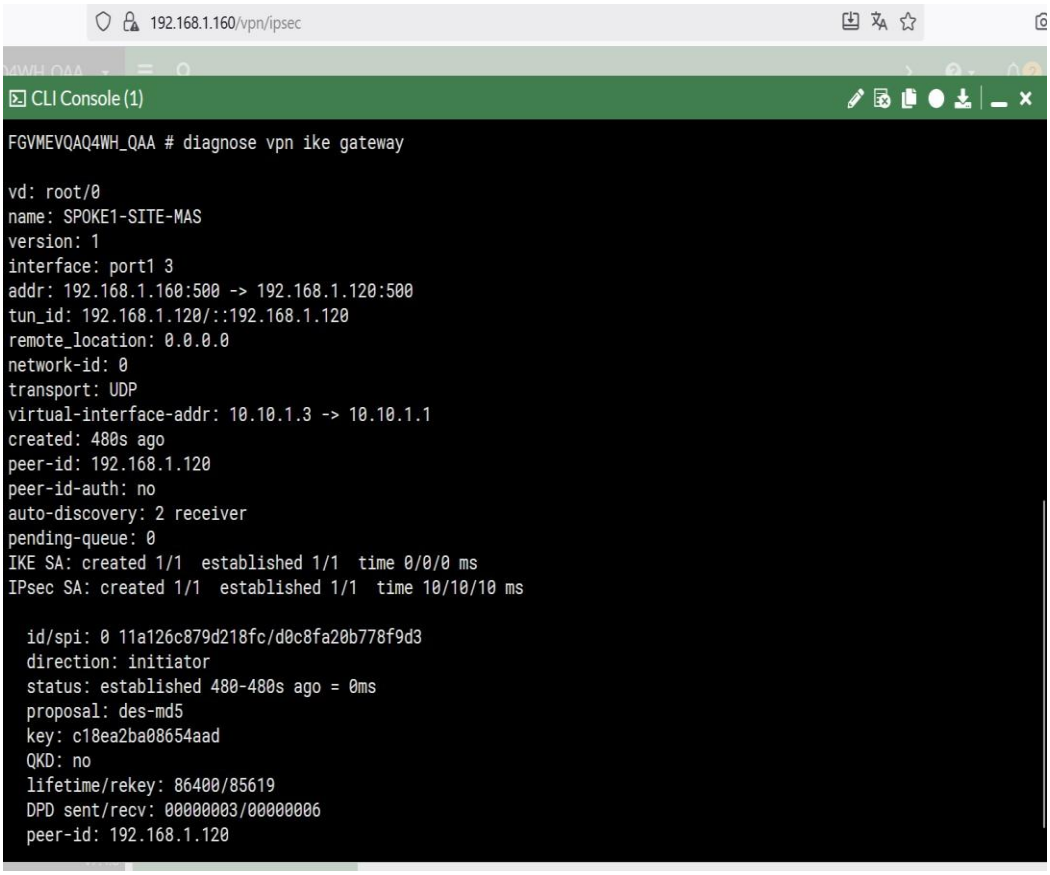

Figura A. 20 Validación de la operatividad túnel SPOKE1-HUB.

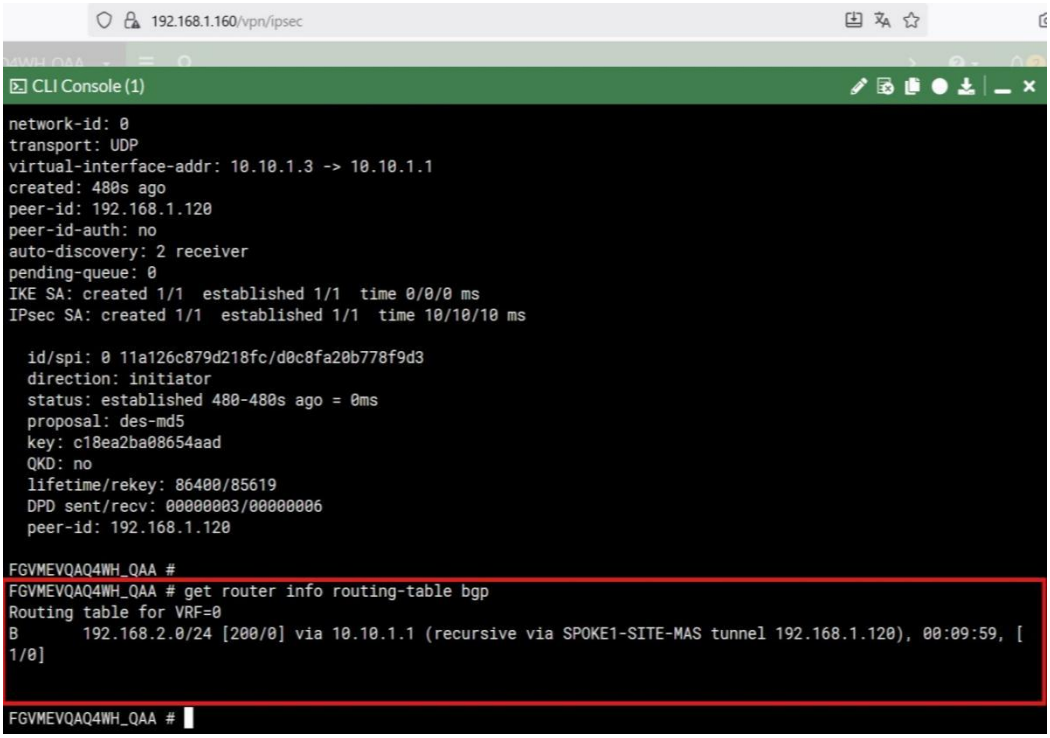

Figura A. 21 Validación de BGP sucursal Masaya.

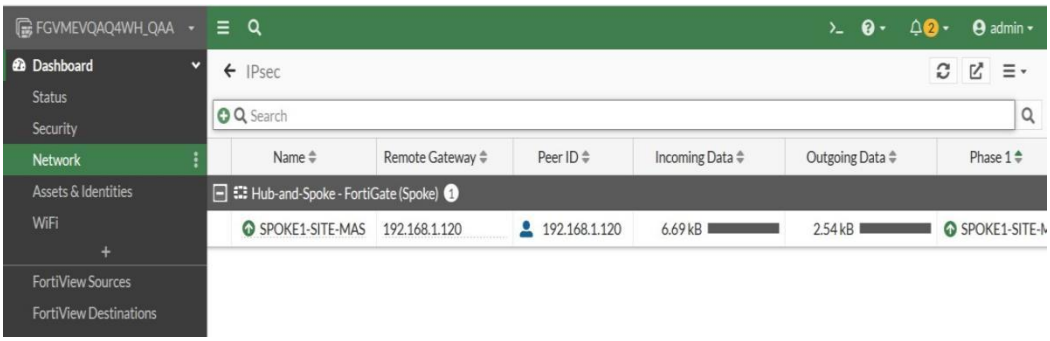

Figura A. 22 Validación del estado de túnel VPN Masaya.

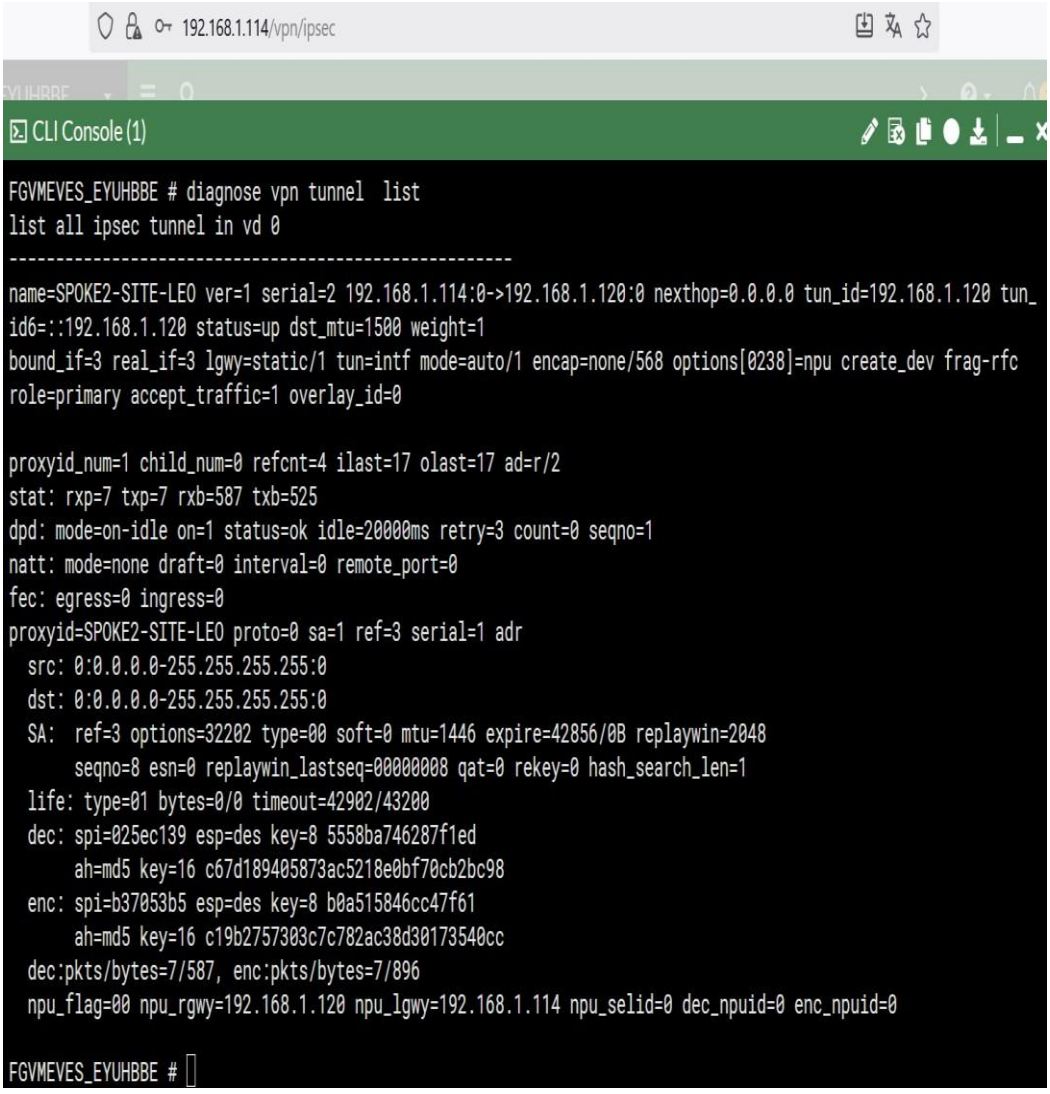

Figura A. 23 Validación de estado túnel León.

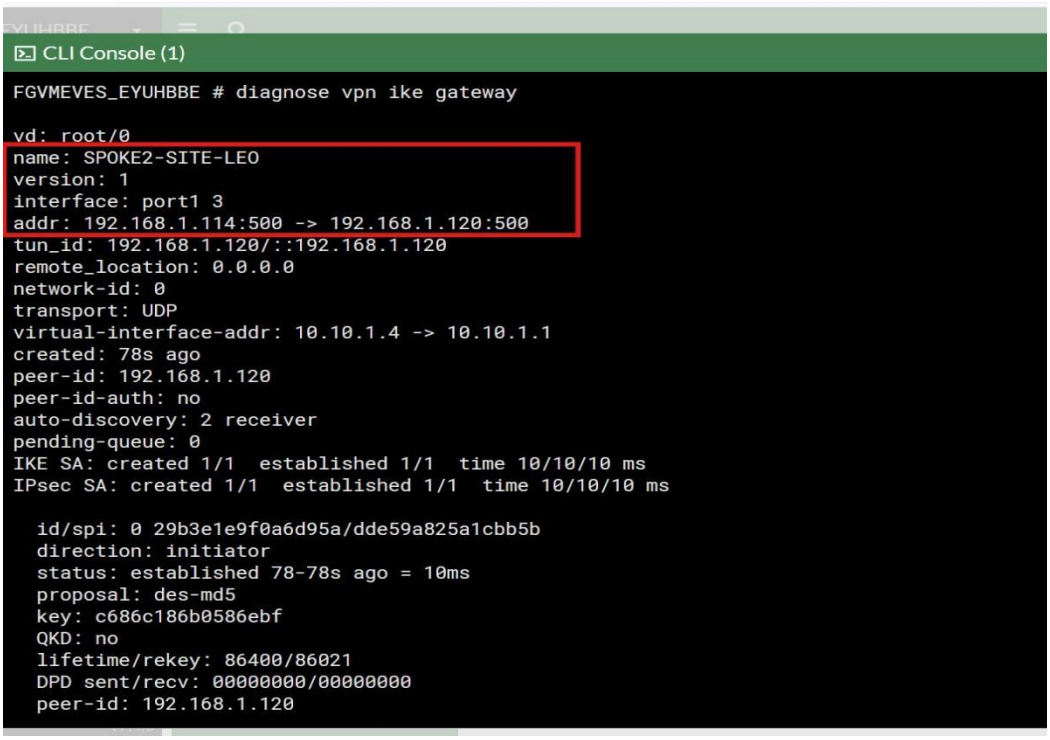

Figura A. 24 Validación de conexión SPOKE2--HUB.

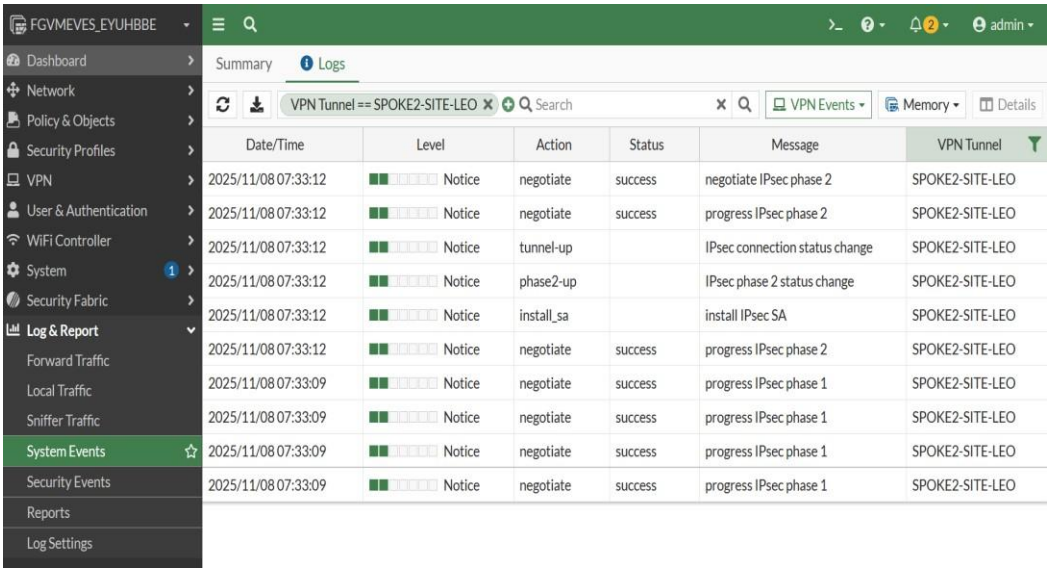

Figura A. 25 Log de tráfico túnel VPN SPOKE2.

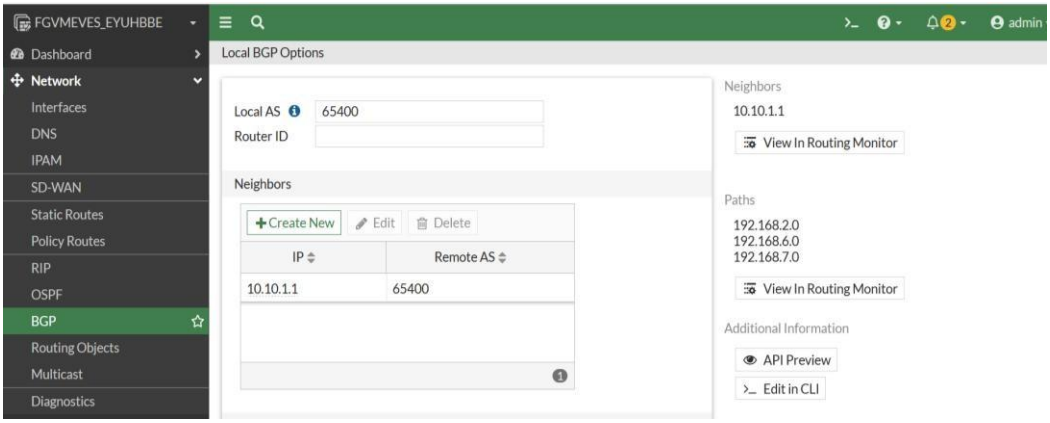

Figura A. 26 Validación de BGP SPOKE2-HUB.

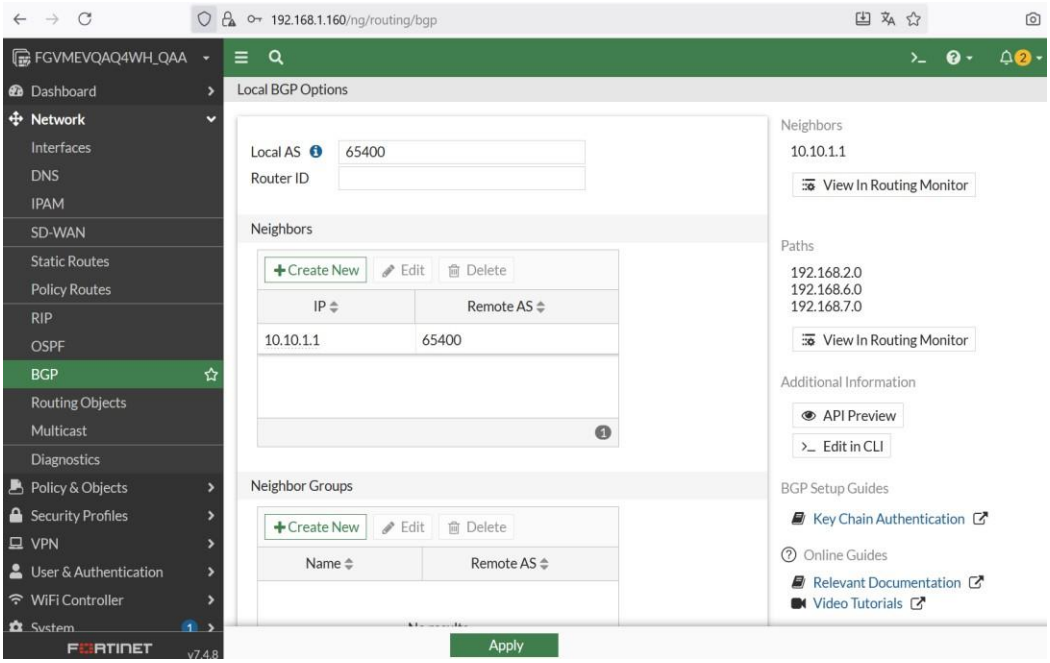

Figura A. 27 Validación de BGP SPOKE1-HUB.

Cronograma de actividades

CRONOGRAMA DE ACTIVIDADES			
Descripción	**Duración**	**Fecha Inicio**	**Fecha Fin**
Cronograma Protocolo UNI	**361 días**	**Lunes 4/3/2024**	**Viernes 28/2/2025**
Fase 1: INVESTIGACIÓN	**11 días**	**Lunes 4/3/2024**	**Viernes 15/3/2024**
Planteamiento de propuesta de diseño a desarrollar para una pyme y sus sucursales	**2 días**	**Lunes 4/3/2024**	**Miércoles 6/3/2024**
Búsqueda de información para propuesta de diseño	**4 días**	**Jueves 7/3/2024**	**Lunes 11/3/2024**
Organización de información recopilada	**3 días**	**Martes 12/3/2024**	**Viernes 15/3/2024**
Fase 2: ELABORACIÓN DEL PROTOCOLO	**52 días**	**Lunes 18/3/2024**	**Jueves 9/5/2024**
Delimitación del tema	**2 días**	**Lunes 18/3/2024**	**Miércoles 20/3/2024**
Revisión de literatura	**5 días**	**Jueves 21/3/2024**	**Jueves 28/3/2024**
Elaboración de portada y redacción de introducción	**3 días**	**Viernes 29/3/2024**	**Miércoles 3/4/2024**
Selección de antecedentes Nacionales	**2 días**	**Jueves 4/4/2024**	**Lunes 8/4/2024**
Selección de antecedentes Internacionales	**2 días**	**Martes 9/4/2024**	**Jueves 11/4/2024**
Redacción de la justificación del protocolo	**2 días**	**Viernes 12/4/2024**	**Lunes 15/4/2024**
Pruebas y delimitación del software a utilizar	**6 días**	**Martes 16/4/2024**	**Miércoles 24/4/2024**
Delimitación de objetivo general y específicos	**1 día**	**Jueves 25/4/2024**	**Viernes 26/4/2024**
Realización de Marco Teórico	**5 días**	**Lunes 29/4/2024**	**Viernes 3/5/2024**
Redacción de diseño metodológico	**1 día**	**Lunes 6/5/2024**	**Martes 7/4/2024**
Creación de cronograma de actividades	**1 día**	**Miércoles 8/4/2024**	**Jueves 9/5/2024**
Fase 3: ENTREGA DE PROTOCOLO	**21 días**	**Viernes 10/5/2024**	**Viernes 31/5/2024**
Entrega a revisión del protocolo al tutor	**6 días**	**Martes 16/5/2024**	**Lunes 20/5/2024**
Entrega final de protocolo a DACTIC	**6 días**	**Jueves 23/5/2024**	**Viernes 31/5/2024**

Fase 4: ANALISIS Y PROPUESTA	**66 días**	**Lunes 3/6/2024**	**Jueves 8/8/2024**
Propuesta de diseño de la arquitectura de la red en Drawio	10 días	Lunes 3/6/2024	Lunes 17/6/2024
Selección de equipos y Tecnologías.	10 días	Miércoles 19/6/2024	Miércoles 3/7/2024
Estudio Técnico	10 días	Jueves 4/7/2024	Jueves 18/7/2024
Costos de equipamiento	15 días	Viernes 19/7/2024	Viernes 9/8/2024
Fase 5: DISEÑO Y PREPARACIÓN	**49 días**	**Lunes 12/8/2024**	**Martes 1/10/2024**
Propuesta de tabla de direccionamiento	20 días	Lunes 12/8/2024	Lunes 9/9/2024
Propuesta de segmentación de la Red	15 días	Martes 10/9/2024	Martes 1/10/2024
Fase 6: SIMULACIÓN	**82 días**	**Martes 2/10/2024**	**Lunes 23/12/2024**
Validación del diseño de la red en el software de simulación EVE-NG	60 días	Martes 2/10/2024	Lunes 23/12/2024
Fase 7: ELABORACIÓN DE DOCUMENTO FINAL	**32 días**	**Lunes 6/1/2025**	**Viernes 7/2/2025**
Redacción de documento final con respecto a la propuesta planteada	24 días	Lunes 6/1/2025	Viernes 7/2/2025
Fase 8 (FINAL): PRESENTACIÓN DE DEFENSA MONOGRAFICA	**11 días**	**Lunes 17/2/2025**	**Viernes 28/2/2025**
Presentación de documento final	9 días	Lunes 17/2/2025	Viernes 28/2/2025