Universidad Nacional de Ingeniería

Área de Conocimiento de Tecnología de la Información y Comunicación

Renovación de infraestructura de redes y de telecomunicación con la arquitectura Secure Access de la marca Fortinet en una entidad bancaria

Trabajo Monográfico para optar al título de Ingeniero Electrónico

Elaborado por:

Br. Maxell Josué Diaz García
Carnet: 2012-41140

Br. Gerald Antonio Gadea Gómez
Carnet: 2012-42079

Tutor:

Ing. Jaime Álvarez Calero

23 de junio de 2025
Managua, Nicaragua

Área de Conocimiento de
Tecnología de la Información
y Comunicación
SECRETARIA DE ÁREA ACADÉMICA

F-8:CARTA DE FINALIZADO PLAN DE ASIGNATURA

El Suscrito Secretario del **ÁREA DEL CONOCIMIENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN** hace constar que:

DÍAZ GARCÍA MAXELL JOSUÉ

Carné: **2012-41140** Turno: **Diurno** Plan de Asignatura: **97-15** de conformidad con el Reglamento Académico vigente en la Universidad, ha aprobado todas las asignaturas correspondientes a la carrera de **INGENIERÍA ELECTRÓNICA,** en el año 2018 y solo tiene pendiente la realización de una de las formas de culminación de estudio.

Se extiende la presente **CARTA DE FINALIZADO PLAN DE ASIGNATURA,** a solicitud del interesado en la ciudad de Managua, a los dos dias del mes de diciembre del año dos mil veinte y cuatro.

Atentamente,

Ing. Cedrick Elksnherr DallaTorre Morales
SECRETARIO DE ÁREA ACADÉMICA

SECRETARÍA ACADÉMICA DE DACTIC · REPÚBLICA DE NICARAGUA · DACTIC

Móvil: (505) 8588 8333

Recinto Universitario Simón Bolívar
Avenida Universitaria.
Managua, Nicaragua.
Apdo: 5595

www.uni.edu.ni

SO POR SISTEMA DE REGISTRO ACADEMICO EL 02-dic-2024

Área de Conocimiento de
Tecnología de la Información
y Comunicación
SECRETARIA DE ÁREA ACADÉMICA

F-8:CARTA DE FINALIZADO PLAN DE ASIGNATURA

El Suscrito Secretario del **ÁREA DEL CONOCIMIENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN** hace constar que:

GADEA GOMEZ GERALD ANTONIO

Carné: **2012-42079** Turno: **Diurno** Plan de Asignatura: **97-15** de conformidad con el Reglamento Académico vigente en la Universidad, ha aprobado todas las asignaturas correspondientes a la carrera de **INGENIERÍA ELECTRÓNICA,** en el año 2018 y solo tiene pendiente la realización de una de las formas de culminación de estudio.

Se extiende la presente **CARTA DE FINALIZADO PLAN DE ASIGNATURA,** a solicitud del interesado en la ciudad de Managua, a los dos días del mes de diciembre del año dos mil veinte y cuatro.

Atentamente,

Ing. Cedrick Elksnherr Dalla[illegible] Morales
SECRETARIO DE ÁREA ACADÉMICA

Móvil: (505) 8588 8333

Recinto Universitario Simón Bolívar
Avenida Universitaria.
Managua, Nicaragua.
Apdo: 5595

www.uni.edu.ni

Managua 06 de Mayo del 2025

Msc:
Claudia Ben avidez Rugama
Directora DACTIC Su
despacho:

Estimada Msc Benavidez:

Por este medio avalo que el trabajo monográfico para optar al título de Ingeniero Electrónico denominado "Renovación de infraestructura de redes y de telecomunicación con la arquitectura Secure Access de la marca Fortinet en una entidad bancaria" cumple con las normativas establecidas por la UNI, por lo que está listo para someterlo a una defensa. Este trabajo fue desarrollado por los bachilleres: Maxell Josué Díaz García, carnet: 2012-41140 y Gerald Antonio Gadea Gómez carnet:
2012-42078. egresados de la carrera Ingeniería Electrónica.
Agradezco su atención.

Atentamente:

Jaime Alvarez Calero
Profesor Titular DACTIC
Tutor

Área de Conocimiento de
Tecnología de la Información
y Comunicación

Managua, 30 de octubre 2024

Br. Maxell Josué Díaz García ***2012-41140***
Br. Gerald Antonio Gadea Gómez ***2012-42079***
Egresados Programa académico Ingeniería Electrónica

Sus manos.-

Estimados Bachilleres:

Reciban cordiales saludos y éxito en sus actividades.

De acuerdo a carta recibida con fecha 24 de octubre, en donde hacen solicitud de cambio de tutor del tema monográfico titulado: ***"Renovación de infraestructura de redes y de telecomunicación con la arquitectura SECURE ACCESS de la marca FORTINET en una entidad bancaria"****, tomando en consideración las justificaciones expuestas en la misma, tengo a bien comunicarles que se les autoriza dicho cambio, nombrando como Tutor al* ***Ing. Jaime Álvarez Calero*** *para dar continuidad con el proceso de su trabajo monográfico.*

No omito manifestar que deberán entregar a más tardar, el 30 de enero del 2025, el documento para predefensa.

Esperando el cumplimiento con respecto al tiempo establecido, les reitero mis saludos.

Atentamente,

Msc. Claudia Lucía Benavidez Rugama
Directora Área de Conocimiento de
Tecnología de la Información y Comunicación

CC Ing. Jaime Álvarez Calero – Tutor
MSc. Cedrick Elksnherr DallaTorre Parrales – Secretario académico.
Archivo.

Móvil: (505) 8588 8333

Recinto Universitario Simón Bolívar
Avenida Universitaria.
Managua, Nicaragua.
Apdo: 5595

www.uni.edu.ni

Área de Conocimiento de
Tecnología de la Información
y Comunicación

Managua, 15 de Julio 2024

Bachilleres
Darryl Jareth Gómez Avilés 2009-29634
Estudiante egresado de la carrera de ingeniería Electrónica
Sus manos.-

Estimado bachiller:

Reciba cordiales saludos de mi parte y deseándole el mejor de los éxitos en sus actividades diarias.

En respuesta a su misiva, en donde solicita darse de baja como integrante del grupo de trabajo monográfico con el tema: ***"Renovación de Infraestructura de redes y Telecomunicación con la Arquitectura Secure Access de la marca Fortinet en una entidad Bancaria"****, por sus justificaciones y con el visto bueno del Tutor* ***Ing. Juan Manuel Martínez Toribio*** *tengo a bien informarles que se le autoriza la baja, quedando conformado el equipo de trabajo para desarrollar dicho tema por:*

Br. Maxell Josué Díaz García Carnet 2012-41140
Br. Gerald Antonio Gómez Avilés Carnet 2012-42079

Sin más a que hacer referencia, les reitero mis saludos.

Atentamente,

MSc. Claudia Benavidez Rugama
Directora Área de Conocimiento de
Tecnología de la Información y la Comunicación

Cc. Br. Maxell Josué Díaz García Carnet 2012-41140
Br. Gerald Antonio Gómez Avilés Carnet 2012-42079
Ing. Juan Manuel Martínez Toribio – *Tutor*
MSc. Cedrick Elksnherr DallaTorre Parrales – Secretario académico.
Archivo DACTIC.

Móvil: (505) 8588 8333

Recinto Universitario Simón Bolívar
Avenida Universitaria.
Managua, Nicaragua.
Apdo: 5595

www.uni.edu.ni

Decanatura | FEC

Universidad Nacional de Ingeniería
Recinto Universitario "Simón Bolívar"
Facultad de Electrotecnia y Computación
Decanatura
DF-05-2023-59

Managua, 22 de mayo del 2023.

Bachilleres.
Maxell Josué Diaz García 2012-41140.
Gerald Antonio Gadea Gómez 2012-42079.
Darryl Jareth Gómez Avilés 2009-29634.
Egresados de la Carrera de Ingeniería Electrónica.

Estimados Bachilleres:

El suscrito Decano de la Facultad de Electrotecnia y Computación, a través de la presente autoriza de manera formal la inscripción de la Monografía Titulada **"RENOVACIÓN DE INFRAESTRUCTURA DE REDES Y DE TELECOMUNICACIÓN CON LA ARQUITECTURA SECURE ACCESS DE LA MARCA FORTINET EN UNA ENTIDAD BANCARIA".** Para optar al Título de Ingeniero Electrónico, para tal efecto se nombra como Tutor de la Monografía al **Ing. Juan Martínez.**

Así mismo le solicito proceda a la **Inscripción de dicho Tema Monográfico** en secretaria Académica de la facultad, con la finalidad de darle control y seguimiento, de acuerdo a los reglamentos establecidos.

Se les recuerda que, según la normativa para los trabajos monográficos, a partir de la fecha de inscripción tiene 12 meses para defender dicho trabajo.

Sin más a que referirme y deseándoles mucho éxito en la culminación de esta etapa, me despido.

Atentamente,

Msc. Augusto César Palacios Rodríguez
Decano UNI-FEC

C/c: Ing. María Lourdes Montes. Secretaria Académica.
Ing. Juan Martínez Toribio. Jefe de Dpto. de Electrónica.
Ing. Juan Martínez Toribio. Tutor.
Archivo.

Teléfono: (505) 2270 5126

Recinto Universitario Simón Bolívar
Avenida Universitaria.
Managua. Nicaragua.
Apdo: 5595

augusto.palacios@fec.uni.edu.ni
www.fec.uni.edu.ni

DEDICATORIA

A Dios, por ser la fuente inagotable de sabiduría, fortaleza y guía en cada paso de nuestras vidas. A Él dedicamos nuestros logros, nuestras metas cumplidas y este importante proyecto que representa el cierre de una etapa fundamental.

A nuestras familias, pilares inquebrantables que, con su amor, paciencia y apoyo incondicional, nos motivaron a superar los desafíos del camino universitario. Gracias por creer en nosotros incluso en los momentos de mayor dificultad.

A nuestros docentes, en especial a quienes guiaron este proceso, por compartir su conocimiento con entrega, por ser inspiración profesional y humana, y por motivarnos a ir más allá de lo técnico, comprendiendo la importancia de soluciones sólidas, seguras y responsables en el ámbito de las telecomunicaciones.

Dedicamos este trabajo también a los futuros ingenieros que, como nosotros, encontrarán en los desafíos tecnológicos la oportunidad de aportar a la transformación digital de nuestro país. Que este esfuerzo sea una referencia de compromiso, calidad y responsabilidad profesional.

Con profundo respeto y gratitud,

Maxell Josué Díaz García

Gerald Antonio Gadea Gómez

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a todas las personas que contribuyeron de manera significativa en la realización de este trabajo de tesis. Sus apoyos incondicionales fueron fundamentales para culminar esta etapa de mi vida académica.

En primer lugar, quiero agradecer a mis padres, hermanos, pareja e hijo, no puedo expresar con palabras cuánto significan para mí. Su amor, apoyo y sacrificio a lo largo de mi educación son el cimiento de mi éxito. Esta tesis es también un tributo a su constante aliento y apoyo. Gracias por creer en mí y estar a mi lado en cada paso del camino.

De manera especial quiero agradecer a mi asesor, Cristhian Alberto Narváez Morazán, por su triple rol como asesor, jefe y amigo, quien desafió mis límites, tanto como jefe y como amigo, tu orientación y apoyo fueron esenciales para completar este trabajo de investigación, tu guía experta a lo largo de este proyecto fueron esenciales para el éxito, tu conocimiento, dedicación, comprensión y flexibilidad para equilibrar mis responsabilidades laborales con mis estudios académicos me permitieron alcanzar los objetivos de esta tesis de una manera que no habría sido posible sin tu ayuda.

En resumen, esta tesis no habría sido posible sin el apoyo y la colaboración de todas estas personas, así como también la ayuda y trabajo de mis compañeros de grupo. Cada uno de ustedes desempeñó un papel crucial en este logro, y les estoy eternamente agradecido. ¡Gracias!

Maxell Josué Díaz García.

AGRADECIMIENTO

Mi agradecimiento se extiende hasta el lector que se detuvo a leer los agradecimientos porque significa que de una u otra forma le intereso nuestro trabajo, porque creyó y se tomó el tiempo, tiempo que fue invertido educacionalmente por nuestros profesores los que muchas veces tuvieron una que otra decepción pero igualmente estamos agradecidos por que eso me ayudo a valorar más la vocación y también agradecer por todos esos amigos que se hicieron en el camino que aportaron de maneras indirectas o directas en esta monografía, son incontables y no podría mencionarlos a todos, por las personas que ya no están y siguen brindando su apoyo.

Infaltable el agradecimiento a la familia, siempre fueron un refugio y agradecer por el apoyo de mi madre que me dio más que la vida, mi padre que aun después de la vida me sigue apoyando.

Finalmente, sin restarle merito a la universidad que sirvió de escenario para que tantas buenas oportunidades se dieran, así como también sirvió como hogar para mí. Siempre estaré agradecido.

Gerald Antonio Gadea Gómez.

RESUMEN

A través de este documento se proporciona una visión de los aspectos a tener en cuenta durante el proceso de renovación de una infraestructura de red, centrándose especialmente en la modernización de la red. Se abordo la alineación con los objetivos del documento con los de la institución, asegurando que este cambio en infraestructura contribuya directamente a cumplir con las metas y aspiraciones propuestas. Además, se subrayan los beneficios tangibles que aportaron a la entidad bancaria, tales como mejoras en la eficiencia, la seguridad, la accesibilidad y continuidad de los sistemas. Se explica cómo cada uno de los conocimientos adquiridos se aplicó de manera práctica en esta mejora tecnológica.

Lo propuesto y aceptado por la entidad bancaria luego de una licitación pública, es una solución que combino seguridad, capacidad y velocidad de transmisión, además de dar simpleza y facilidad de gestión a los nuevos equipos, con equipos de la marca Fortinet, con la infraestructura llamada Secure Access, la cual se basa en una administración de red y gestión de amenazas unificada en una plataforma, pero que a su vez sea extensible hasta la raíz de los posibles riesgos, desde los enlaces de internet hasta las conexiones de los dispositivos finales de la institución.

ÍNDICE

1. Introducción

El crecimiento y normalización del uso de las TIC se ha expandido en casi todo giro de negocio convencional y no convencional, permitiendo la rápida expansión e inclusión de nuevos servicios que lleguen a nuevos nichos de mercados, llegando masivamente a los usuarios.

En el caso de los servicios que prestan las entidades bancarias se ven afectadas por la era digital y el cambio dinámico de la infraestructura de las comunicaciones, pero con esto se expone un problema evidente, el cual es que a medida que dichos servicios se ramifican y se expanden se vuelve una necesidad que la infraestructura en la que estos servicios conviven sea lo suficientemente robusta y segura para soportar la demanda cada vez más exigente de los mismos.

En Nicaragua, toda entidad que quiera prestar algún servicio bancario necesita aprobación de la Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF), esta se encarga de alinear a dichas entidades con los requisitos estándares aprobados y revisados para que los servicios bancarios estén seguros y disponibles mediante el uso de las TIC.

En el presente documento se muestra como a partir de una necesidad de incremento en los servicios, se solicitó y se realizó un cambio de infraestructura tecnológica de red a una entidad bancaria, tomando en cuenta los lineamientos establecidos por la SIBOIF y las buenas prácticas estandarizadas en el uso de las TIC y recomendaciones del fabricante de las soluciones que componen la nueva infraestructura implementada.

El propósito con este cambio de la infraestructura propuesta es que además de que cumpla con los requisitos de la SIBOIF, sino que también tenga capacidad de crecimiento y mejoras a implementar, una infraestructura totalmente robusta y modular que permita cambios sin afectación perceptible por los usuarios/clientes, escalabilidad tanto en manejo de los datos como en crecimiento de hardware.

2. Objetivos

2.1 Objetivo General

Rediseñar la infraestructura de red y telecomunicaciones de la entidad Bancaria utilizando tecnología Fortinet para cumplir con los requerimientos tecnológicos de la SIBOIF.

2.2 Objetivos Específicos

- Establecer una conexión entre los equipos Fortinet (Fortigate y Fortiswitch) a través de Fortilink logrando la administración de estos.

- Configurar la conexión entre los equipos Fortinet (Fortigate y Fortiswitch) a través de Fortilink para administración eficiente y cumplimiento de estándares de seguridad.

- Realizar configuración de redundancia entre los equipos a través de MCLAG-ISL/ICL (Multi-Chasis Link Aggregation Group - Inter Switch link/Inter Chassis Link).

- Hacer uso de la infraestructura Secure Access mediante la red ya establecida y las políticas definidas por la entidad bancaria adaptando la configuración actual de los equipos cisco a los equipos Fortinet.

3. Justificación

La entidad bancaria, surge con el propósito de brindar servicios financieros enfocados en fomentar la actividad económica y productiva del país. El énfasis en apoyar a las PYME de los sectores económicos prioritarios, los cuales atribuyen en el desarrollo del país. En resumen, promueve el crecimiento de pequeñas y medianas empresas, también se está proyectando nuevos mercados para el público en general el cual, al ser un mercado con mayor alcance, surge como una necesidad de la entidad bancaria una expansión proporcional de sus productos y servicios que sean accesibles para este nuevo sector del rubro, derivada de esta decisión fue imprescindible realizar una renovación de la infraestructura así como también las plataformas de red que actualmente posee a una que pueda soportar los servicios previstos a implementar por dicha entidad bancaria.

Debido a la diversificación del tipo de negocio y el nicho del mismo cambia, haciendo necesario la aprobación del ente regulador del sector bancario conocido como Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF), la cual la entidad bancaria deberá cumplir con los siguientes requerimientos:

- Soporte de Hardware y Software de los equipos de telecomunicaciones.
- Plataforma con alta disponibilidad para la continuidad de los servicios.
- Seguridad en las plataformas.

Existe en la entidad bancaria una infraestructura de red compuesta por switches planos y switches capa tres de la marca Cisco, la cual ya el soporte caduco, por consiguiente, como parte de auditorías y mejores prácticas exigidas a las entidades bancarias estos cambios son imperativos, aunado esto se adjudicó un proyecto de ampliación de público objetivo que este banco ofrece.

El ente regulador SIBOIF constantemente está realizando sus auditorías a las entidades bancarias bajo su “*norma sobre gestión de riesgo tecnológico”*, bajo la cual la entidad bancaria al encontrarse en el incumplimiento con algunos de los

artículos de la normativa, ha tomado la decisión por actualizar su infraestructura de seguridad informática, la cual le permite estar dentro de los estándares establecidos, de igual manera esto le permite ampliar y mejorar sus servicios.

"Arto. 18. Administración de hardware y comunicaciones. - La entidad debe administrar adecuadamente el hardware, las redes y las líneas de comunicación de misión crítica, considerando al menos lo siguiente:

a) Realizar estudios de capacidad y desempeño del hardware y las líneas de comunicación, que permitan determinar en forma oportuna, necesidades de ampliación de capacidades o actualizaciones de equipos.

g) Mantener actualizados los contratos de proveedores, diagramas de red y comunicaciones, diagramas de distribución física, inventarios, configuración técnica y cualquier otra información requerida."[1]

Estos requerimientos citados en su "*norma sobre gestión de riesgo tecnológico"* por parte de la SIBOIF. La entidad bancaria dentro la variedad de opciones para cumplir con la normativa ha optado como solución la arquitectura basada en Secure Access de la marca Fortinet. La cual es la más optima y le permite una escalabilidad que favorece su crecimiento y desarrollo para el lanzamiento de los nuevos productos y servicios que desea brindar entre los cuales incluye tarjetas de crédito y débito, cuentas de ahorro y equipararse a entidades del mismo rubro.

[1] (Superintendencia de Bancos y de Otras Instituciones, (SIBOIF), 2007)

4. Marco Teórico

En esta sección se abordan los conceptos relacionados a los términos, siglas y acrónimos mencionados en documentos.

4.1 Glosario técnico.

4.2 Virus informático.

Un virus es un pequeño programa que infecta las computadoras sin el conocimiento o permiso de sus operadores. Está catalogado también como un mecanismo parásito, puesto que ataca a los archivos o sectores de "boot" (arranque) y se replica para continuar su esparcimiento, 2 de modo que provoca no solo la pérdida de información, imágenes y videos, sino también la de tiempo en la reinstalación de los sistemas operativos, entre otros daños incluso más graves. (Manson, 2010)

4.3 Antivirus

Los antivirus informáticos son piezas de software de aplicación cuyo objetivo es detectar y eliminar de un sistema computarizado los virus informáticos. Es decir, se trata de un programa que busca poner remedio a los daños causados por estas formas invasivas de software, cuya presencia en el sistema no suele ser detectable sino hasta que se evidencian sus síntomas, tal y como los virus biológicos. (Etecé, 2021)

4.4 Firewall.

Un Cortafuegos o Firewall es un dispositivo de hardware o una aplicación de software diseñado para proteger los dispositivos de red de los usuarios externos de la red y/o de aplicaciones y archivos maliciosos, gestionándolo de acuerdo a unas determinadas políticas de configuración. Entre sus funciones se destacan los bloqueos de paquetes que se originan en determinado rango de IP, puertos y direcciones de correo, entre otros. También se utiliza como herramienta de

defensa (contra virus, gusanos y spam), de análisis forense y del comportamiento de sistemas y redes. (MARTÍNEZ MOLINA, PACHECO MENESES, & ZÚÑIGA SILGADO, julio-diciembre, 2009)

4.5 Switch

Un conmutador de red (Switch) es un dispositivo físico que funciona en la capa de enlace de datos del modelo de interconexión de sistemas abiertos (OSI), capa 2. Recibe paquetes enviados por dispositivos que están conectados a sus puertos físicos y los reenvía a los dispositivos Los paquetes están destinados a alcanzar. Los conmutadores también pueden funcionar en la capa de red (capa 3) donde se produce el enrutamiento.

Los conmutadores son un componente común de las redes basadas en Ethernet, canal de fibra, modo de transferencia asíncrono (ATM) e InfiniBand, entre otros. Sin embargo, la mayoría de los conmutadores actuales utilizan Ethernet. (Shaw, 2022)

4.6 Malware.

El malware describe aplicaciones o códigos maliciosos que dañan o interrumpen el uso normal de los dispositivos de punto final. Cuando un dispositivo se infecta con malware, puede experimentar acceso no autorizado, datos comprometidos o bloqueo del dispositivo a menos que pague un rescate. Las personas que distribuyen malware, conocidas como ciberdelincuentes utilizan dispositivos infectados para lanzar ataques, por ejemplo, para obtener credenciales bancarias, recopilar información personal que pueda venderse, vender acceso a recursos informáticos o extorsionar información de pago de las víctimas.

4.7 Antimalware

el software antimalware es un tipo de programa diseñado para prevenir, detectar y eliminar cualquier programa malicioso que afecte la estabilidad y el funcionamiento de un dispositivo. Es fundamental que este software de seguridad realice correctamente sus tareas de detección y eliminación de las amenazas. (ciberseguridadtips.com, 2022)

4.8 Dynamic Host Configuration Protocol (DHCP)

El Protocolo de configuración dinámica de host (DHCP) se utiliza para asignar dinámicamente direcciones de Protocolo de Internet (IP) a cada host en la red de su organización. En este significado de DHCP, un host puede referirse a cualquier dispositivo que permita el acceso a una red. Algunos ejemplos incluyen computadoras de escritorio y portátiles y dispositivos personales, entre otros. DHCP garantiza que a todos estos dispositivos se les asigne una dirección IP. (Fortinet, 2023)

4.9 IP

El protocolo de Internet, conocido por sus siglas en inglés IP, es el protocolo principal de la familia de protocolos de Internet y su importancia es fundamental para el intercambio de mensajes en redes informáticas. El protocolo no orientado a la conexión, publicado en 1974 por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE) y especificado como estándar en RFC 791, fue concebido principalmente para garantizar el éxito en el envío de paquetes de un emisor a un destinatario. Para este fin, el protocolo de Internet establece un formato que determina el tipo de descripción que tienen estos paquetes de datos. (www.ionos.es, 2018)

4.10 High Aviability (HA)

La alta disponibilidad (HA) es la capacidad de un sistema para operar continuamente sin fallar durante un período de tiempo designado. HA trabaja para garantizar que un sistema cumpla con un nivel de rendimiento operativo acordado. En tecnología de la información (TI), un estándar de disponibilidad muy difundido pero difícil de lograr se conoce como disponibilidad de cinco nueves, lo que significa que el sistema o producto está disponible el 99,999 % del tiempo. (Lutkevich, 2021)

4.11 High Aviability Active -Active.

Un clúster activo-activo generalmente se compone de al menos dos nodos, ambos ejecutando activamente el mismo tipo de servicio simultáneamente. El objetivo principal de un clúster activo-activo es lograr el equilibrio de carga. El equilibrio de carga distribuye las cargas de trabajo entre todos los nodos para evitar que un solo nodo se sobrecargue. Debido a que hay más nodos disponibles para atender, también habrá una mejora notable en el rendimiento y los tiempos de respuesta. (Villanueva, 2022)

4.12 High Aviability Active -Pasive.

Al igual que la configuración de clúster activo-activo, un clúster activo-pasivo también consta de al menos dos nodos. Sin embargo, como implica el nombre "activo-pasivo", no todos los nodos estarán activos. En el caso de dos nodos, por ejemplo, si el primer nodo ya está activo, el segundo nodo debe estar pasivo o en espera. El servidor pasivo sirve como una copia de seguridad que está lista para tomar el control tan pronto como el servidor activo (primario) se desconecta o no pueda servir. (Villanueva, 2022)

4.13 Cuenta de ahorro

Una cuenta de ahorros es un producto financiero ofrecido por el Banco que te permite ahorrar tu dinero de forma segura. Tradicionalmente, la cuenta de ahorros es el producto más usado para que puedas ahorrar y disponer de tu dinero de forma rápida. (www.scotiabankcolpatria.com, s.f.)

4.14 Tarjetas de crédito

Una tarjeta de crédito es un documento de material plástico o metal emitido por un banco o institución especializada a nombre de una persona, que podrá utilizarla para efectuar compras sin tener que pagar en efectivo y pudiendo, además, llevar el pago de los productos a períodos futuros. (Economipedia, 2016)

4.15 Tarjetas de debito

La tarjeta de débito, también conocida como dinero electrónico o de plástico, es un instrumento financiero emitido por un banco o caja de ahorros que permite al cliente acceder al saldo que dispone en su cuenta corriente asociada a la tarjeta. (Economipedia, 2016)

4.16 Préstamos personales

Un préstamo personal es un contrato por el que la entidad financiera adelanta una cantidad de dinero (principal) a otra persona llamada prestatario, con la obligación de que devuelva el principal y abone además unos intereses pactados y los gastos derivados de la operación. (www.finanzasparatodos.es, 2010)

4.17 Modelo OSI

Este modelo de referencia proporciona una base común para la coordinación del establecimiento de normas a efectos de la interconexión de sistemas, y permite considerar en perspectiva las normas existentes dentro del modelo de referencia general. Identifica asimismo las esferas en las cuales se pueden establecer y mejorar normas y proporciona una referencia común para mantener la compatibilidad entre todas las normas conexas. El texto se elaboró conjuntamente con la ISO/CEI, y el objetivo primordial de esta revisión es introducir ese texto conjunto, en el cual se incluye el concepto de transmisión sin conexión, además de cierto número de mejoras técnicas y de redacción. (International Telecommunication Union (ITU), 1994)

4.18 Power over Ethernet (PoE)

Power over Ethernet (o PoE) suministra alimentación eléctrica, utilizando los cables de red CATx. Al no ser necesario realizar conexiones de cables eléctricos, hace que con la utilización de dispositivos PoE se consiga un ahorro económico en materiales y tiempo de instalación. Además, es una solución para aplicaciones remotas, puesto que no requiere ninguna toma de corriente eléctrica cercana. Sin embargo, el factor limitante siempre ha sido la potencia que pueda suministrar.

(BlackBox, s.f.)

4.19 Router

Un Router (enrutador) recibe y envía datos en redes informáticas. Los enrutadores a veces se confunden con concentradores de red (network hubs), módems o conmutadores de red (network switches). Sin embargo, los enrutadores pueden combinar las funciones de estos componentes y conectarse con estos dispositivos para mejorar el acceso a Internet o ayudar a crear redes comerciales. (Cisco, 2019)

4.20 Stacking Cisco

El apilamiento (Stacking) permite a los usuarios expandir la capacidad de su red sin la molestia de administrar varios dispositivos. Los switches apilables (Stackable switches) se pueden agregar o quitar de una pila según sea necesario sin afectar el rendimiento general de la pila. Dependiendo de su topología, una pila puede continuar transfiriendo datos incluso si falla un enlace o una unidad dentro de la pila. Esto hace que el apilamiento sea una solución efectiva, flexible y escalable para expandir la capacidad de la red. (Cisco, 2020)

4.21 Throughput

El rendimiento es una medida de cuántas unidades de información puede procesar un sistema en un período de tiempo determinado. Se aplica ampliamente a sistemas que van desde diversos aspectos de sistemas informáticos y de red hasta organizaciones.

Las medidas relacionadas de la productividad del sistema incluyen la velocidad con la que se puede completar una carga de trabajo específica y el tiempo de respuesta, que es la cantidad de tiempo entre una única solicitud interactiva del usuario y la recepción de la respuesta. (Burke, 2022)

4.22 Unified Threat Management (UTM)

La gestión unificada de amenazas, que comúnmente se abrevia como UTM, es un término de seguridad de la información que se refiere a una sola solución de seguridad y, por lo general, a un único producto de seguridad que ofrece varias funciones de protección en un solo punto en la red. Un producto UTM generalmente incluye funciones como antivirus, antispyware, antispam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Algunas unidades también ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, network address translation) y compatibilidad para redes privadas virtuales (VPN, virtual private network). El atractivo de la solución es su sencillez. Las empresas que utilizan servicios de proveedores o productos diferentes para cada tarea de seguridad ahora pueden reunirlos todos en una sola solución, con asistencia de un único equipo o segmento de TI, y ejecutarlos desde una sola consola. (Kaspersky, 2017)

4.23 Wide Area Network (WAN)

Una red de área amplia (también conocida como WAN) es una gran red de información que no está vinculada a una sola ubicación. Las WAN pueden facilitar la comunicación, el intercambio de información y mucho más entre dispositivos de todo el mundo a través de un proveedor de WAN. las redes de área amplia son una forma de redes de telecomunicaciones que pueden conectar dispositivos desde múltiples ubicaciones y en todo el mundo. Las WAN son las formas más grandes y expansivas de redes informáticas disponibles hasta la fecha. (CompTIA, s.f.)

4.24 Multi Chassis Link Aggregation Inter Chassis Link (MC-LAG ICL)

Un grupo de agregación de enlaces (LAG) proporciona redundancia a nivel de enlace. Un LAG multichasis (MCLAG) proporciona redundancia a nivel de nodo al agrupar dos modelos de Fortiswitch para que aparezcan como un único switch en la red. Si alguno de los switch falla, el MCLAG sigue funcionando sin interrupciones, lo que aumenta la capacidad de recuperación de la red y elimina

los retrasos asociados con el protocolo de árbol de expansión “Spanning Tree Protocol (STP)”. (FORTINET, 2023)

4.25 Multi Chassis Link Aggregation Inter Switch Link (MC-LAG ISL)

Este protocolo actúa de la misma manera que (MC-LAG ICL) pero este permite que los switchs se comuniquen a dos o más switchs con (MC-LAG ICL) sin crear una tormenta de broadcast en la red. (FORTINET, 2023)

4.26 Link Aggregation Control Protocol (LACP)

Protocolo de agregación de enlaces (LACP) es un protocolo utilizado entre dispositivos de red para agrupar automáticamente enlaces entre los dispositivos y es compatible con la agregación de enlaces. Una vez que configura una interfaz agregada con LACP habilitado, los paquetes LACP se transmiten a otros dispositivos conectados directamente (como conmutadores y enrutadores), que crearán los enlaces agregados necesarios (si también están habilitados para LACP).

Los enlaces agregados en otros dispositivos de red deben crearse manualmente en esos dispositivos si LACP está deshabilitado en la interfaz agregada que crea, o si un dispositivo de red no es compatible con LACP. Solo admite el modo activo; el modo pasivo LACP no es compatible. (FORTINET, s.f.)

4.27 Intrusion Prevention Sistem (IPS)

Sistema de prevención de intrusiones es la tecnología de seguridad de la red que monitorea constantemente el tráfico de la red para identificar amenazas. Bajo el significado general de IPS, la tecnología IPS también es un sistema de prevención de detección de intrusos (IDPS). (FORTINET, s.f.)

4.28 Virtual Routing Redundance Protocol (VRRP)

El Protocolo de redundancia de enrutador virtual (VRRP) es un protocolo de red informática que permite la asignación automática de enrutadores de Protocolo de

Internet (IP) disponibles a los hosts participantes. Esto aumenta la disponibilidad y confiabilidad de las rutas de enrutamiento a través de selecciones automáticas de puerta de enlace predeterminada en una subred IP. (FORTINET, 2022)

4.29 Hot Stand-By Routing Protocol (HSRP)

Hot Standby Router Protocol (HSRP) es un protocolo de enrutamiento de redundancia que establece la tolerancia a fallas predeterminada y un marco para la conmutación por error de la puerta de enlace de la red principal. HSRP está diseñado para redes de área local (LAN) de difusión o multiacceso y es compatible con la inaccesibilidad del tráfico del Protocolo de Internet sin interrupciones. (techopedia., 2011)

4.30 Open Short Path First (OSPF)

Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado de enlace que se usa comúnmente en redes de grandes empresas con conmutadores L3, enrutadores y firewalls de múltiples proveedores. Puede detectar rápidamente fallas en los enlaces y converge el tráfico de red sin bucles de red. También tiene funciones para controlar qué rutas se propagan, lo que permite tablas de enrutamiento más pequeñas y proporciona un mejor equilibrio de carga en enlaces externos en comparación con otros protocolos de enrutamiento. (FORTINET, 2023)

4.31 Access List (ACL)

Una lista de control de acceso (ACL) es una lista de bloqueo específica y granular que se utiliza para bloquear paquetes IPv4 e IPv6 en una interfaz específica según los criterios configurados en la política de ACL. (FORTINET, 2023)

4.32 Software Defined WAN (SDWAN)

SD-WAN es un enfoque definido por software para administrar redes de área amplia (WAN). Consolida las conexiones de transporte físico, o subyacentes, y monitorea y equilibra la carga del tráfico a través de los enlaces. Las redes de

superposición de VPN se pueden construir sobre las capas subyacentes para controlar el tráfico en diferentes sitios. (FORTINET, 2023)

4.33 Fortilink

FortiLink es una tecnología clave de apoyo de Fortiswtich, que permite que sus puertos se conviertan en extensiones del appliances de seguridad de FortiGate. Cuando se conecta a través de FortiLink. La administración centralizada a través de FortiGate simplifica la implementación y el aprovisionamiento de Fortiswtich con autodescubrimiento sin intervención, VLAN con un solo clic y la asignación de políticas de seguridad. (Pachón, 2019)

4.34 Virtual Domain (VDOM)

Los VDOM o virtual domain es una funcionabilidad que ofrece Fortinet gratuitamente en sus dispositivos Fortigate tanto en equipos appliance como virtuales, esta función nos permite crear instancias de Fortigate, cada instancia es opera de manera independiente tanto de administración como de reglas de acceso, rutas, VPNs y UTM.

Consiste en dividir de manera lógica el dispositivo con el fin de tener varios Fortigate que operen en diferentes modos en el mismos hardware o máquina virtual, permite segmentar flujos de tráfico de diferentes redes y poder separar la administración de los usuarios de seguridad. (DAVID ALEJANDRO TORRES JOSE FELIPE ZAMBRANO, 12/06/2020)

4.35 Secure Access Fortinet

Los FortiSwitch se integra directamente en FortiGate, lo que permite que la administración del conmutador y la seguridad del puerto de acceso se gestionen desde el mismo "panel único". Independientemente de cómo los usuarios y los dispositivos están conectados a la red (por cable, inalámbrica o VPN), para tener visibilidad y control completos sobre la seguridad y el acceso a su red. (FORTINET, 2017)

5. Diseño Metodológico.

5.1 Método de Investigación.

Se empleó una metodología cuantitativa, que permite validar el funcionamiento del diseño propuesto y comprobar que la solución cumple con los requisitos establecidos por la SIBOIF.

5.2 Tipo de investigación.

La investigación realizada en este trabajo monográfico es del tipo aplicada debido a que su propósito principal es la búsqueda de solución de un problema practico. El proyecto consiste en mejorar y robustecer la seguridad informática de una entidad bancaria, partiendo en primera instancia que la infraestructura anterior se encontraba fuera de soporte por parte del fabricante que en este caso es la marca CISCO, debido a esto el ente regulador tiene como normativas la actualización constante de la infraestructura de protección de redes y telecomunicación.

5.3 Etapa de análisis

Esta etapa se inició con la reunión entre los representantes de telecomunicaciones y sus respectivos administradores, con el objetivo de determinar los alcances del proyecto, la necesidad institucional y las expectativas que se derivan del mismo. A partir del diagnóstico realizado, que incluyó la identificación de una arquitectura de red previa y la revisión de los modelos de los equipos existentes, se propusieron mejoras estructurales mediante el diseño de una nueva arquitectura tecnológica. Esta propuesta incluye equipos y configuraciones específicas que permitirían implementar eficientemente las mejoras, aportando un valor agregado significativo a la solución planteada.

En la evaluación de soluciones de seguridad perimetral, es clave considerar no solo el costo inicial, sino el costo total de propiedad (TCO), que incluye licencias, soporte y capacidad de integración. La tabla 1 muestra una comparativa orientada a los requerimientos del sector financiero.

Tabla 1, Comparativa de las diferentes tecnologías

Proveedor	Precio Aproximado (USD)	Costo de Licenciamiento	Ventajas	Consideraciones
Fortinet	$2,000 - $3,000	Múltiples funciones de seguridad con una única licencia.	Alto rendimiento, integración UTM, SD-WAN sin costos extra.	Enfoque en integración con soluciones Fortinet.
Cisco	$1,500 - $2,500	Licencias adicionales para IPS, VPN y filtrado web.	Amplia compatibilidad con entornos empresariales.	Dependencia de licencias para seguridad avanzada.
Palo Alto Networks	$500 - $700	Costos adicionales por su tecnología	Detección de amenazas avanzadas.	Modelo basado en suscripción.
Check Point	$1,000 - $1,500	Licenciamiento basado en paquetes de seguridad.	Seguridad robusta con segmentación granular.	Puede requerir módulos adicionales.
Juniper Networks	$600 - $1,200	Licencias para IPS y filtrado de contenido.	Buen rendimiento en redes complejas.	CLI más técnica, curva de aprendizaje alta.
Sophos	$1,500 - $2,000	Licenciamiento por servicios como Sandstorm.	Integración con soluciones de endpoint.	Mayor costo si se requieren funciones avanzadas.
SonicWall	$2,000 - $3,000	Licencias requeridas para filtrado avanzado y protección ATP.	Opciones flexibles para medianas empresas.	No tan optimizado para grandes entornos bancarios.
WatchGuard	$1,500 - $2,500	Suscripciones para funciones avanzadas.	Gestión centralizada y facilidad de configuración.	Costo adicional por servicios completos.

5.4 Infraestructura previa a la renovación

Previo al proceso de migración, la infraestructura tecnológica de la entidad se basaba en soluciones de Cisco, destacando el uso de **Cisco Identity Services Engine**. La topología implementada incluía un total de 22 dispositivos, de los cuales 19 habían quedado fuera de soporte por parte del fabricante: los modelos **Catalyst 2960** desde el 31 de octubre de 2019, y los **Catalyst 3750** desde el 31 de mayo de 2021. Esta condición impedía el cumplimiento de los requisitos técnicos establecidos por la **SIBOIF**.

La arquitectura respondía a un diseño jerárquico tradicional de tres capas (Core, Distribución y Acceso), estructurado en una configuración en cascada. En el núcleo se encontraban tres switches **Cisco Catalyst 3750**, dos de ellos en configuración *stacking* en el sitio principal y uno en modo *standalone* en el sitio alterno. En las capas de distribución y acceso operaban 19 **Catalyst 2960**, con puntos clave de redundancia para garantizar alta disponibilidad y seguridad. La red contaba con firewalls perimetrales con inspección DPI, segmentación por servicios y autenticación interna.

El diseño de esta arquitectura se ilustra en la **Figura 1**, donde se detalla la disposición y funcionalidad de los componentes principales.

5.5 Arquitectura de Red

- **Core**: Implementado con switch de alto rendimiento en alta disponibilidad (HSRP/VRRP) para la redundancia. Se encargaba de la gestión del tráfico y el enrutamiento entre segmentos internos y externos.

- **Distribución**: Contaba con firewalls perimetrales y sistemas de prevención de intrusiones (IPS) basados en soluciones propietarias, separando la red corporativa, la red de servicios bancarios y los entornos de desarrollo.
- **Acceso**: Conectividad segmentada para sucursales a través de enlaces MPLS y VPNs seguras, con autenticación 802.1X para el control de acceso en oficinas internas.

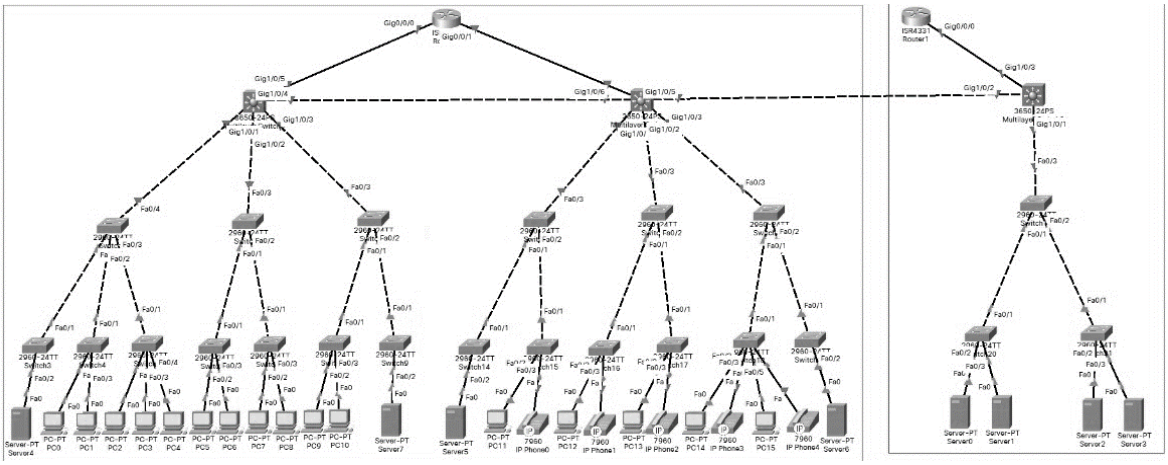


Figura 1, **Infraestructura de red previa a la renovación.**

5.6 Limitaciones Identificadas

- **Gestión Fragmentada**: Cada solución (firewalls, IPS, VPN, filtrado web) operaba en plataformas separadas, lo que dificultaba la administración centralizada y la respuesta rápida ante incidentes.

- **Costos Elevados**: El modelo de licenciamiento para funcionalidades avanzadas (SD-WAN, inspección SSL, análisis de comportamiento) implicaba costos recurrentes significativos, limitando la escalabilidad de la infraestructura.

- **Inspección de Tráfico Cifrado**: La capacidad de inspección SSL/TLS en la plataforma de seguridad tenía un impacto notable en el rendimiento, lo que requería invertir en hardware adicional o balancear la carga de análisis.

- **Expansión de Red**: La adopción de nuevos servicios digitales y la migración hacia entornos híbridos en la nube estaban limitadas por una arquitectura que dependía de hardware físico y configuraciones estáticas.

5.7 Análisis de pros y contras

Para tomar una decisión fundamentada, se realizó un análisis entre Cisco y Fortinet, dos de los principales proveedores de soluciones de seguridad y networking. Este análisis consideró aspectos críticos como rendimiento, integración, facilidad de gestión, costos y escalabilidad. La tabla resultante permitió visualizar con claridad las fortalezas y debilidades de cada solución en el contexto específico del banco.

Tabla 2, pros y contras de arquitecturas.

Criterio	Fortinet	Cisco
Rendimiento	Alto rendimiento con procesadores ASIC dedicados.	Buen rendimiento, pero depende más del software.
Costo	Generalmente más económico en términos de hardware y licenciamiento.	Más costoso, especialmente en licencias y mantenimiento.
Facilidad de uso	Interfaz más intuitiva y fácil de configurar.	Curva de aprendizaje más pronunciada, requiere más experiencia.
Seguridad	Soluciones de seguridad integradas con FortiGuard y UTM.	Seguridad robusta con enfoque en segmentación y detección avanzada.
Integración	Mejor integración con su propio ecosistema Fortinet.	Mayor compatibilidad con entornos empresariales y multi-vendor.

Escalabilidad	Buena escalabilidad, pero más enfocada en medianas empresas.	Más escalable para grandes empresas y entornos corporativos.
Soporte	Soporte eficiente, pero a veces limitado en documentación.	Soporte sólido con una amplia comunidad y documentación extensa.
Popularidad	En crecimiento, especialmente en PYMEs.	Amplia adopción en empresas y gobiernos.

Si bien la red del banco estaba diseñada bajo estándares de seguridad y redundancia adecuados, las limitaciones en escalabilidad, gestión centralizada y costos operativos, representaban desafíos en su evolución tecnológica. La modernización mediante soluciones de seguridad integradas, automatización y SD-WAN optimizada podría mitigar estas barreras y mejorar la eficiencia operativa.

5.8 Etapa de diseño.

Se procedió con el diseño de la arquitectura de red a implementar y dimensionar los equipos necesarios para la misma.

En esta etapa se determinó el diseño de la arquitectura final en la institución, así como la forma y tipos de conexión de los nuevos equipos, los protocolos a configurar, las configuraciones que se deben de migrar y las que se deben desechar.

5.9 Infraestructura propuesta.

La nueva infraestructura implementada en la entidad bancaria fue diseñada para cumplir con los requisitos regulatorios y respaldar la evolución de los servicios institucionales. La solución se fundamenta en tecnología Fortinet, elegida por su capacidad para permitir una migración segura, limpia y sin comprometer la continuidad operativa.

La topología está conformada por tres FortiGate 200F, responsables de la

inspección del tráfico hacia Internet. La arquitectura continúa con dos FortiGate 600D en alta disponibilidad (HA), que actúan como controladores de switches. En la capa de distribución se implementan FortiSwitch 1048E, conectados a FortiSwitch 448E-FPOE y 448E en la capa de acceso. Esta estructura jerárquica, enfocada en seguridad, escalabilidad y redundancia, se ilustra en la Figura 2, donde se detallan los componentes y su disposición dentro del diseño propuesto.

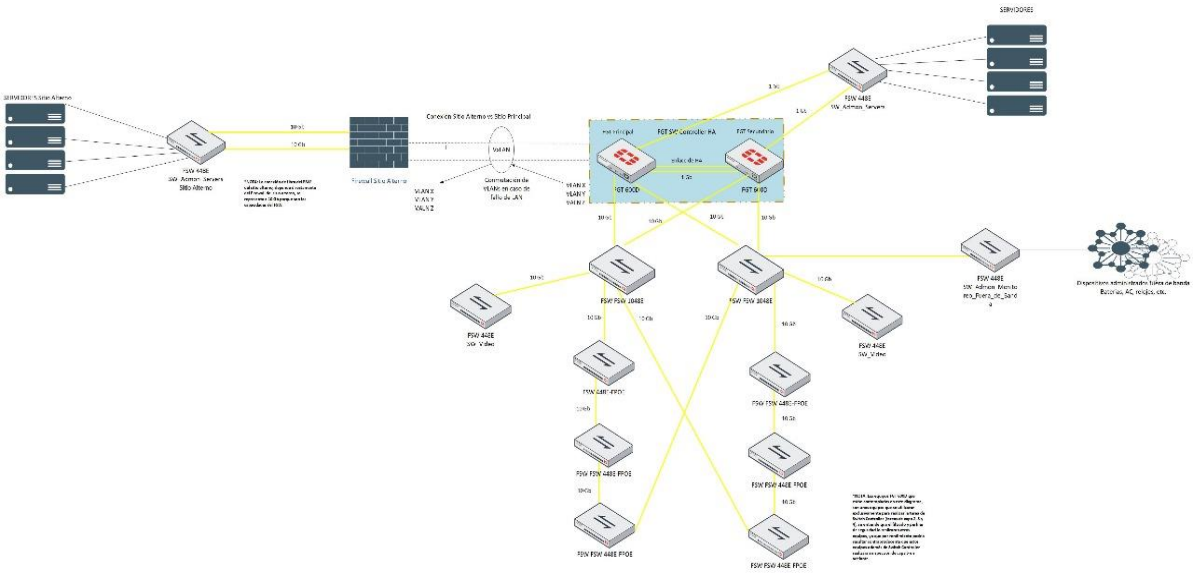


Figura 2, **Diagrama de Infraestructura Propuesta.**

A diferencia de la red anterior, el nuevo esquema mejora la administración, centraliza la gestión, reduce los costos operativos y fortalece la seguridad general. La implementación de SD-WAN optimiza la conectividad entre sucursales, eliminando la dependencia de enlaces dedicados costosos y mejorando la eficiencia operativa.

Como complemento al diseño técnico, se presenta una evaluación financiera de la inversión en infraestructura de red, que considera la adquisición de hardware,

licenciamiento y contratos de soporte. Esta información se resume en la Tabla 2, como parte del análisis integral para asegurar una conectividad segura, escalable y altamente disponible, en cumplimiento con los estándares de seguridad y eficiencia exigidos por la industria financiera.

Tabla 3, **Costos de los Equipos.**

Componente	Función Principal	Cantidad	Precio Unitario (USD)	Costo Total de Adquisición (USD)	Precio Anual de Soporte (USD)
FortiGate 200F	Seguridad y filtrado de tráfico en el sitio alterno	3	$5,861	$17,583	$2,164
FortiGate 600D	Firewall perimetral y switch controller en HA en el sitio principal	2	$10,128	$20,256	$3,450
FortiSwitch 1048E	Switches de distribución de alto rendimiento	2	$21,641	$43,282	$2,164
FortiSwitch 448E	Switches de acceso para conectividad de usuarios	5	$2,402	$12,010	$240
FortiSwitch 448E-FPOE	Switches de acceso con PoE para dispositivos como cámaras y teléfonos IP	6	$5,835	$35,010	$584
Total, Inversión				**$128,141**	
Total, Costo Soporte Anual					**$22,574**
Costo Total inversión más soporte					**$150.715**

6. Etapa de desarrollo.

6.1 Configuración de equipos Fortigate 600D en Alta disponibilidad.

Los equipos Fortigate son los que actúan en realidad como equipo Core de la red, bajo su mando tendrá los demás equipos Fortiswitch que comprenden la densidad de puertos para la conexión de todos los usuarios y los equipos que se van a encargar de realizar el enrutamiento en capa 2 y capa 3 del modelo OSI.

Debido a su criticidad, estos equipos deben de constar con un sistema de alta disponibilidad para ser tolerantes a fallos, el cual debe permitir el paso del tráfico en caso de alguna falla y/o caída de alguno de sus miembros y que esta caída no sea notada por el usuario final, este sistema de clúster constara de dos equipos Fortigate 600D en alta disponibilidad en modo activo-activo, que compartirán sesiones y tendrán de manera obligatoria la misma cantidad de conexiones en los mismos puertos, ya que a nivel de red estos dos equipos se verán y comportarán como uno solo.

Para mantener la coherencia y orden del tráfico que estos equipos van a procesar, se configurará uno de ellos como equipo Máster, un equipo que tendrá el control del clúster y que responderá las peticiones de red, el otro equipo estará como equipo esclavo que estará procesando una minoría de tráfico y que a nivel de red no contestará ninguna petición.

Además de contar con un equipo máster, también se configurarán unos sensores de actividad de puertos apuntando a puertos claves en la interconexión de los equipos Fortigate y los equipos Fortiswitch, el cual tiene como objetivo detectar cuando hay falla en alguno de estos puertos, si la falla se de los puertos se da en

el equipo configurado cómo Máster se realiza un cambio de roles, en el cual el equipo Máster pasa a ser el esclavo y el esclavo el master (Con el supuesto que los puertos del equipo esclavo están funcionando en óptimas condiciones), de tener una caída en el equipo esclavo, se levanta una alerta para revisión y en caso de caerse todos los puertos, tendremos cómo resultado una caída total de la red, es un caso muy remoto pero se debe
tomar en cuenta.

6.2 Configuración de equipos Fortigate 600D como controladores de Fortiswitch.

Como parte final en la configuración de los Fortigate 600D, tenemos la activación de la característica de controlador de switch, esta característica permite al Fortigate comportarse como una consola unificada que administra todos los switches que se conecten a él, cabe destacar que esta característica solo es compatible con los switches de la misma marca, denominados Fortiswitch.

Ser configurarán unos puertos en modo Fortilink que es el protocolo propietario que tiene Fortinet para administrar sus equipos vía Fortigate, una vez configurados estos puertos, se crean sobre estos puertos todas las VLANs que la entidad tiene y las nuevas que necesite, ya que este será el canal por donde pasara toda la comunicación que vendrá desde los usuarios finales, creadas las VLAN con sus IDs, su direccionamiento y sus nombres, se procede a trabajar sobre el enrutamiento necesario sobre las mismas.

Estos puertos son de alta importancia y necesitan ser monitoreados por parte de los sensores de Alta Disponibilidad para poder reaccionar automáticamente en caso de algún problema con las mismas.

Una vez creadas, se procede a conectar los primeros Fortiswitch que son

conocidos como Fortiswitch Core, los cuales se encargaran de recoger las conexiones de los usuarios, una vez conectados el Fortilink los detecta y se procede a autorizarlos en el Fortigate para que puedan ser administrados y reciban la configuración del Fortigate por medio del Fortilink.

6.3 Configuración de equipos Fortigate 600D con VRRP.

Además de la configuración de alta disponibilidad estos equipos tendrán configuración de enrutamiento avanzado con protocolo de VRRP para controlar el enrutamiento en caso de caída entre el centro de datos principal y el secundario, se configura por cada red (sea VLAN o un CIDR) una IP virtual que comparten dos equipos, en este caso el Fortigate del sitio principal y el Fortigate del sitio alterno, además de esta IP virtual se configura una IP del mismo segmento a cada equipo y se le asigna una prioridad, misma que va a definir cuál de los equipos va estar enrutando tráfico (si el de sitio principal o alterno).

Además de esto se configura un sensor para tener un parámetro de cambio, en caso de que el sensor no sea capaz de llegar a un destino específico, automáticamente cambia las prioridades de VRRP y el tráfico se empezará a enrutar por donde indique la nueva prioridad, este enrutamiento está dedicado al uso de Internet, por lo tanto el sensor tendrá como destino el DNS de Google y tendrá como prioridad el internet del sitio principal, si se deja de llegar al DNS de Google por el sitio principal, cambiará las prioridades y enviará todo el tráfico de internet al sitio alterno.

6.4 Configuración de equipos Fortigate 600D con OSPF

Siguiendo con el enrutamiento se tendrá configurado el protocolo OSPF para dar a conocer a través de toda la red interna las redes de las sucursales y demás servicios internos de la entidad, este protocolo enruta dinámicamente las redes declaradas en su configuración y se las envía a sus compañeros que se

encuentren configurados con los mismos parámetros y que se crean como vecinos OSPF en la misma configuración.

En el caso de la entidad se necesitan que tres equipos Fortigate sean vecinos OSPF, para compartirse rutas de sucursales, servicios y acceso a Internet, de los cuales ya hay dos configurados, el tercer equipo es el clúster de equipos Fortigate 600D, por lo tanto para mantener la coherencia entre el tráfico y las rutas y evitar pérdidas de paquetes y colisiones, se configurará una métrica conocida como costo en el OSPF, para indicar que equipo es el preferido/principal y que equipos estarán como secundarios.

6.5 Configuración de equipos Fortiswitch Core con MCLAG-ICL.

Luego de tener listo los equipos Fortigate, se configuran los equipos Fortiswitch, con la característica MCLAG – ICL, la cual permite tener un mismo equipo físico conectado a dos equipos físicos diferentes sin ocasionar un bucle de capa 2, ni perdidas de paquetes, esta característica se configura únicamente en los equipos Fortiswitch Core y se realiza una sola vez, esta configuración también permite que los equipos estén en alta disponibilidad sin comprometer la coherencia y funcionalidad de la red.

Cabe destacar que esta característica se expande automáticamente hacia los equipos Fortiswitch que se conecten a estos equipos sin configurar nada más, además de esto esta configuración es única para los equipos de la marca Fortinet.

6.6 Configuración de equipos Fortiswitch Core.

Una vez configurado el MCLAG-ICL, se conectan los Fortiswitch Core a los Fortigate 600D en los puertos configurados con Fortilink, una vez hecho esto y autorizados los Fortiswitch Core, la configuración realizada en los Fortigate y el

Fortilink automáticamente pasa al Fortiswitch y procedemos a realizar las asignaciones de VLANs en los puertos ya sea de manera Troncal y de Acceso.

Parte de las configuraciones adicionales luego de la asignación de VLAN es el modo de los puertos, ya sea que se utilice un conjunto de puertos físicos como uno solo puerto lógico en un Fortiswitch Core en modo LACP o un conjunto de puertos físicos como uno solo puerto lógico en dos Fortiswitch Core en modo MC-LAG, esto va a depender de lo que la entidad necesite conectar a dichos puertos.

6.7 Integración de equipos Fortiswitch Acceso.

Una vez realizada la configuración en los Fortiswitch Core, se procede a realizar la integración de los Fortiswitch que van a recoger las conexiones de los usuarios finales, en esta etapa la configuración de estos equipos es aplicar MCLAG-ISL y básicamente conectar a los Fortiswitch Core, aprobar en el Fortigate y luego asignar las VLANs y crear los conjuntos de puertos que se necesiten.

6.8 Secure Access.

Tras la configuración inicial de los equipos descritos previamente, se establece una arquitectura de red con administración centralizada desde el **FortiGate 600D**, lo cual permite un control unificado de los dispositivos **FortiSwitch** conectados mediante **FortiLink**. Este enfoque facilita la implementación de una arquitectura **Secure Access**, que integra políticas de seguridad de forma homogénea en toda la red de acceso.

Para lograr la funcionalidad completa de *Secure Access*, se deben asociar políticas de inspección directamente desde el FortiGate 600D a las **VLANs** previamente configuradas. Estas políticas mínimas comprenden funciones

esenciales de seguridad, como **prevención de intrusos (IPS)** y **antivirus**, que son aplicadas en el firewall perimetral y automáticamente heredadas por todos los **FortiSwitches** administrados por el controlador.
Este modelo garantiza que cada punto de acceso a la red desde el núcleo hasta el borde esté protegido bajo un mismo esquema de políticas, evitando configuraciones manuales individuales y reduciendo significativamente los riesgos asociados a brechas de seguridad o errores operativos.

La lógica de funcionamiento y la propagación automática de estas políticas a través de los puertos FortiLink se detalla en la **Figura 2**, donde se visualiza la relación jerárquica entre los dispositivos y la distribución de las funciones de seguridad en cada segmento de la red.

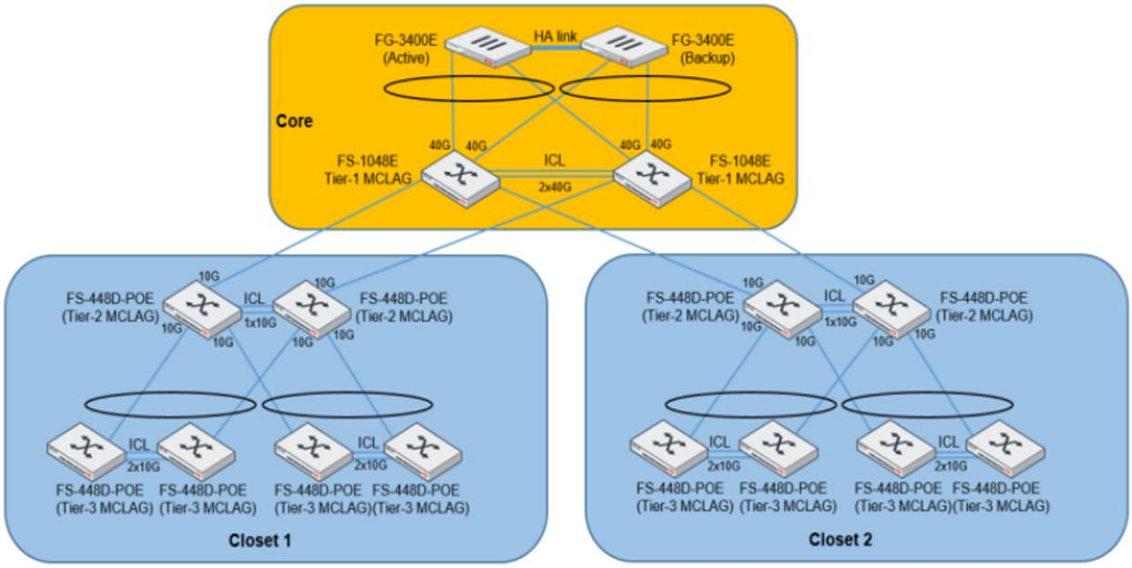


Figura 3, **Diagrama de Topología Secure Access.**

Esta estructura permite no solo una mejor administración y visibilidad, sino también una respuesta más ágil ante amenazas, alineándose con los estándares de seguridad exigidos en el sector financiero.

6.9 Etapa de Implementación.

En esta etapa se detallan los pasos a seguir en la instalación de Fortiswitches (De diferentes modelos) de manera que estos equipos sean administrados desde un mismo punto (Fortigate) y que la implementación y administración, tanto de nuevos como de ya implementados equipos sea más rápida, intuitiva y eficiente que con otras tecnologías.

6.10 Preparación de Fortigate.

Debido a la arquitectura y configuración ya existente en la entidad bancaria, se decidió tomar como punto de partida un clúster de equipos FGT 600D que tienen configurado un sistema de dominio virtuales (VDOMs).

Teniendo esto en cuenta se procedió a crear el VDOM que se denomina como: SW-CORE:

```
FGT-MASTER # config system global
FGT-MASTER (global) # set vdom-mode multi-vdom
FGT-MASTER (global) # end
FGT-MASTER # config vdom
FGT-MASTER (vdom) # edit "SW-Core"
FGT-MASTER (SW-Core) # next
FGT-MASTER (vdom) # end
```

En este VDOM tendremos las configuraciones como si de un FGT físico se tratara, acá haremos toda la configuración para que el FGT reciba a los FSW, el siguiente paso es el Fortilink.

6.11 Configuración de Fortilink.

FortiLink es el canal de comunicación utilizado por el FortiGate (FGT) para

administrar los FortiSwitch (FSW). A través de este enlace, se distribuye su configuración hacia los switches. El primer paso es asignar las interfaces físicas al nuevo VDOM denominado SW-CORE, establecerán la conexión de gestión entre el FGT y los FSW con los siguientes comandos:

```
FGT-MASTER # config system global
FGT-MASTER (global) # end
FGT-MASTER # config system interface
FGT-MASTER (interface) # edit "port17"
FGT-MASTER (port17) # set vdom "SW-CORE"
FGT-MASTER (port17) # next
FGT-MASTER (interface) # edit "port18"
FGT-MASTER (port18) # set vdom "SW-CORE"
FGT-MASTER (port18) # next
FGT-MASTER (interface) # end
```

Posteriormente, dentro del VDOM SW-CORE, se procede a crear la interfaz lógica FortiLink:

```
FGT-MASTER # config vdom
FGT-MASTER (vdom) # edit "SW-CORE"
FGT-MASTER (SW-CORE) # config system interface
FGT-MASTER (interface) # edit "Fortilink"
FGT-MASTER (Fortilink) # set vdom "SW-CORE"
FGT-MASTER (Fortilink) # set fortilink enable
FGT-MASTER (Fortilink) # set ip 169.X.X.X 255.255.255.0
FGT-MASTER (Fortilink) # set allowaccess ping fabric
FGT-MASTER (Fortilink) # set type aggregate
FGT-MASTER (Fortilink) # set member "port17" "port18"
FGT-MASTER (Fortilink) # set description "Fortilink SW Core"
FGT-MASTER (Fortilink) # set alias "Fortilink SW Core"
FGT-MASTER (Fortilink) # set lldp-reception enable
FGT-MASTER (Fortilink) # set lldp-transmission enable
FGT-MASTER (Fortilink) # set snmp-index 29
FGT-MASTER (Fortilink) # set fortilink-split-interface disable
FGT-MASTER (Fortilink) # set swc-first-create 127
FGT-MASTER (Fortilink) # next
FGT-MASTER (interface) # end
FGT-MASTER (SW-CORE) # next
FGT-MASTER (vdom) # end
```

En esta arquitectura, se asignan los puertos 17 y 18 del FGT para conectar con los FSW de nivel Data Center, permitiendo la alta disponibilidad (HA) mediante enlaces cruzados entre los equipos.

Para que la conexión de los FSW gestionados sea completamente automática, es necesario que el FGT les asigne direcciones IP mediante DHCP. Esto se logra configurando un servidor DHCP vinculado a la interfaz Fortilink, como se muestra a continuación:

```
FGT-MASTER # config system dhcp server
FGT-MASTER (dhcp server) # edit 1
FGT-MASTER (1) # set dns-service local
FGT-MASTER (1) # set ntp-service local
FGT-MASTER (1) # set default-gateway 169.X.X.X
FGT-MASTER (1) # set netmask 255.255.255.0
FGT-MASTER (1) # set interface "Fortilink"
FGT-MASTER (1) # config ip-range
FGT-MASTER (ip-range) # edit 1
FGT-MASTER (1) # set start-ip 169.X.X.X
FGT-MASTER (1) # set end-ip 169.X.X.X
FGT-MASTER (1) # next
FGT-MASTER (ip-range) # end
FGT-MASTER (1) # set vci-match enable
FGT-MASTER (1) # set vci-string "FortiSwitch" "FortiExtender"
FGT-MASTER (1) # next
FGT-MASTER (dhcp server) # end
```

6.12 MCLAG-ICL.

Para continuar con la configuración de la administración de los FortiSwitch (FSW), es crucial implementar un paso adicional que involucra la definición de la arquitectura de alta disponibilidad. Esta configuración debe ser aplicada directamente en los FSW, teniendo en cuenta que es fundamental distinguir entre dos tipos de FSW:

- ***FSW Core:*** *Son dispositivos de alto rendimiento diseñados para proporcionar conmutación rápida en centros de datos con grandes volúmenes de tráfico. En el caso específico de la ENTIDAD BANCARIA, estos equipos se conforman por un par de FSW 1048E en el Sitio Principal (SP) y un par de FSW 1024E en el Sitio Alterno (SA).*

- ***FSW Acceso:*** *Son equipos dedicados a gestionar las conexiones de los usuarios y otros dispositivos, actuando como puntos de acceso a la red.*

La configuración de MCLAG-ICL se implementa en los FSW Core, ya que no se requerirá una capa adicional de FSW debido a que todos los dispositivos de acceso estarán conectados directamente a los FSW Core.

Esta configuración se realiza a través de la interfaz de línea de comandos (CLI), comenzando con la preparación de los puertos de Fortilink en los FortiGate (FGT). Los siguientes comandos son utilizados para establecer dicha configuración:

```
# En el Switch Core 1 (SW-CORE-1)
SW-CORE-1 # config switch-controller managed-switch
SW-CORE-1 (managed-switch) # edit FS1E48T419000051
SW-CORE-1 (FS1E48T419000051) # config ports
SW-CORE-1 (ports) # edit port18
SW-CORE-1 (port18) # set lldp-profile default-auto-mclag-icl
SW-CORE-1 (port18) # end
SW-CORE-1 (FS1E48T419000051) # end
# En el Switch Core 2 (SW-CORE-2)
SW-CORE-2 # config switch-controller managed-switch
SW-CORE-2 (managed-switch) # edit FS1E48T419000052
SW-CORE-2 (FS1E48T419000052) # config ports
SW-CORE-2 (ports) # edit port17
SW-CORE-2 (port17) # set lldp-profile default-auto-mclag-icl
SW-CORE-2 (port17) # end
SW-CORE-2 (FS1E48T419000052) # end
```

Con estos pasos, los puertos Fortilink en los FortiGate estarán preparados para recibir las conexiones de los FSW Core. A continuación, se configura directamente

en los FSW, asignando los puertos de interconexión entre ellos con los siguientes comandos:

```
# Configuración de los puertos entre los Switches Core (SW_Core_1 y SW_Core_2)
SW-CORE-1 # config switch auto-isl-port-group
SW-CORE-1 (auto-isl-port-group) # edit SW_Core_1
SW-CORE-1 (SW_Core_1) # set members port25
SW-CORE-1 (SW_Core_1) # set members port26
SW-CORE-1 (SW_Core_1) # next

SW-CORE-2 # edit SW_Core_2
SW-CORE-2 (SW_Core_2) # set members port25
SW-CORE-2 (SW_Core_2) # set members port26
SW-CORE-2 (SW_Core_2) # next
SW-CORE-2 (auto-isl-port-group) # next
SW-CORE-2 (auto-isl-port-group) # end
```

Con estos ajustes, los puertos estarán habilitados para la comunicación entre los **FSW Core**, lo que evitará la creación de un bucle **L2** en la red. Este proceso establece la base para conectar los demás **FSW** y garantiza que la arquitectura de red operará de manera eficiente y sin inconvenientes.

Con esto, finalizamos la configuración de **MCLAG-ICL**. Para mayor claridad y referencia visual, consulte la **Figura 3**, la cual ilustra la configuración de red resultante y los vínculos entre los dispositivos.

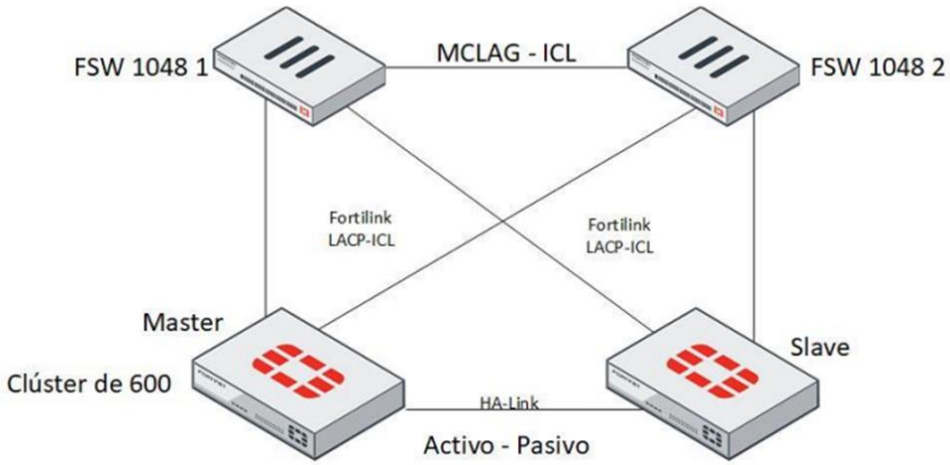


Figura 4, **Diagrama de Arquitectura MCLAG-ICL**

6.13 VLANS

Posteriormente, se procede con la configuración de las interfaces **VLAN** dentro del **FortiGate**, necesarias para garantizar la conectividad lógica de las distintas redes internas. En este caso, las interfaces están asociadas al **VDOM SW-CORE** y se integran mediante la interfaz física **FortiLink**.

Estas interfaces están diseñadas con funcionalidades de alta disponibilidad, empleando **VRRP** (Virtual Router Redundancy Protocol), que permite asegurar continuidad en el direccionamiento IP en caso de fallos. A continuación, se detalla un ejemplo de configuración correspondiente a una VLAN típica, utilizando nombres representativos y valores ficticios para preservar la confidencialidad:

```
FGT-MASTER # config system interface
FGT-MASTER (interface) # edit "VLAN_30"
FGT-MASTER (VLAN_30) # set vdom "SW-CORE"
FGT-MASTER (VLAN_30) # set dhcp-relay-service enable
FGT-MASTER (VLAN_30) # set ip 192.168.30.2 255.255.255.0
FGT-MASTER (VLAN_30) # set allowaccess ping
FGT-MASTER (VLAN_30) # set description "VLAN_30 - Usuarios Administrativos"
FGT-MASTER (VLAN_30) # set device-identification enable
FGT-MASTER (VLAN_30) # set vrrp-virtual-mac enable
FGT-MASTER (VLAN_30) # config vrrp
FGT-MASTER (vrrp) # edit 3
FGT-MASTER (3) # set vrgrp 1000
FGT-MASTER (3) # set vrip 192.168.30.1
FGT-MASTER (3) # set priority 150
FGT-MASTER (3) # set adv-interval 10
FGT-MASTER (3) # set start-time 5
FGT-MASTER (3) # next
FGT-MASTER (vrrp) # end
FGT-MASTER (VLAN_30) # set role lan
FGT-MASTER (VLAN_30) # set snmp-index 36
FGT-MASTER (VLAN_30) # set color 2
FGT-MASTER (VLAN_30) # set dhcp-relay-ip "192.168.30.10"
FGT-MASTER (VLAN_30) # set interface "Fortilink"
FGT-MASTER (VLAN_30) # set vlanid 30
FGT-MASTER (VLAN_30) # next
```

```
FGT-MASTER (interface) # end
```

Esta configuración permite que la VLAN esté habilitada para DHCP Relay, tenga visibilidad SNMP, pueda ser accedida vía ping para pruebas de conectividad, y que se integre correctamente al plano de alta disponibilidad mediante VRRP.

Además, el parámetro *set interface "Fortilink"* vincula la VLAN a la interfaz troncal que conecta con los FSW Core, lo cual es fundamental dentro del esquema centralizado de administración y segmentación de red definido en el diseño general.

6.14 Integrando Fortiswitchs

Una vez creado el FortiLink y configuradas las interfaces correspondientes, se procede con la integración física y lógica de los FortiSwitch (FSW) al FortiGate (FGT). Esta etapa permite establecer la administración centralizada de los switches desde el controlador embebido en el FGT. La conexión se realiza mediante los puertos designados del equipo, que serán definidos dentro del interfaz FortiLink.

Para habilitar esta funcionalidad en el plano de control, es necesario activar el Switch Controller globalmente en el sistema, y luego configurar la interfaz de tipo FortiLink, que operará como troncal de administración y transporte hacia los switches.

A continuación, se presenta la secuencia de comandos correspondiente:

```
GT-MASTER # config system global
FGT-MASTER (global) # set switch-controller enable
FGT-MASTER (global) # end
FGT-MASTER # config system interface
FGT-MASTER (interface) # edit "fortilink"
FGT-MASTER (fortilink) # set fortilink enable
FGT-MASTER (fortilink) # set fortilink-split-interface enable
```

```
FGT-MASTER (fortilink) # set ip 10.10.10.1 255.255.255.0
FGT-MASTER (fortilink) # set member "port15"
FGT-MASTER (fortilink) # set auto-auth-extension-device enable
FGT-MASTER (fortilink) # next
FGT-MASTER (interface) # end
```

Con esta configuración, el FGT queda preparado para descubrir automáticamente los FSW conectados a través del puerto físico especificado (en este caso, port15). Además, al habilitar *auto-auth-extension-device*, se facilita el proceso de autenticación automática de los switches, simplificando el aprovisionamiento.

Este proceso también puede realizarse desde la interfaz gráfica de usuario (GUI), como se ilustra en la, donde se visualiza la habilitación del Switch Controller, la creación del FortiLink y la asociación de interfaces físicas.

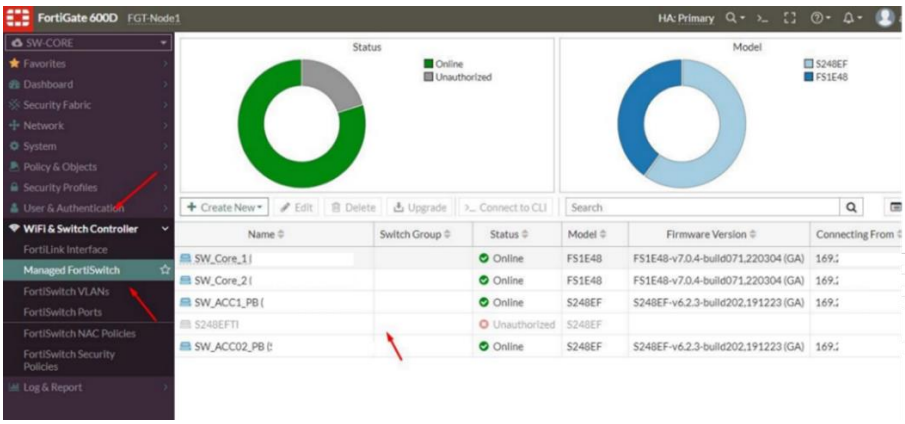


Figura 5, **Configuración de FortiLink desde GUI.**

6.15 Configuración de puertos de FSW

Una vez que se han creado las VLANs y los FortiSwitch (FSW) están correctamente integrados y administrados por el FortiGate (FGT) a través de FortiLink, el siguiente paso es la asignación de dichas VLANs a los puertos físicos de los switches.

Esta configuración se realiza desde el FGT utilizando comandos en CLI, dentro del contexto del Switch Controller. Para este ejemplo, se tomará como referencia el switch identificado como *"FS1E48T421000948",* el cual ha sido renombrado como *"SW_Core_1"* dentro de la gestión centralizada. A continuación, se muestra el procedimiento:

```
FGT-MASTER # config switch-controller managed-switch
FGT-MASTER (managed-switch) # edit "FS1E48T421000948"
FGT-MASTER (SW_Core_1) # set name "SW_Core_1"
FGT-MASTER (SW_Core_1) # set fsw-wan1-peer "Fortilink"
FGT-MASTER (SW_Core_1) # set fsw-wan1-admin enable
FGT-MASTER (SW_Core_1) # set poe-detection-type 3
FGT-MASTER (SW_Core_1) # set version 1
FGT-MASTER (SW_Core_1) # set max-allowed-trunk-members 48
FGT-MASTER (SW_Core_1) # set dynamic-capability
0x00000000000000000003fff3dfd9df7
FGT-MASTER (SW_Core_1) # config ports
FGT-MASTER (ports) # edit "Trunk_Uplink_37"
FGT-MASTER (Trunk_Uplink_37) # set vlan "default.29"
FGT-MASTER (Trunk_Uplink_37) # set allowed-vlans "Loopback" "VLAN_2"
"VLAN_3" "VLAN_4" "VLAN_5" "VLAN_6" "VLAN_7" "VLAN_8" "VLAN_9"
"VLAN_10" "VLAN_11" "VLAN_12" "VLAN_16" "VLAN_17" "VLAN_20"
"VLAN_40" "VLAN_44" "VLAN_45" "VLAN_50" "VLAN_66" "VLAN_76"
"VLAN_100" "VLAN_101" "VLAN_102" "VLAN_103" "VLAN_104" "VLAN_105"
"VLAN_106" "VLAN_110" "VLAN_116" "VLAN_120" "VLAN_130" "VLAN_172"
"VLAN_175" "VLAN_179" "VLAN_180" "VLAN_200" "VLAN_302" "VLAN_380"
"VLAN_500" "VLAN_VOZ" "VLAN_VRRP"
FGT-MASTER (Trunk_Uplink_37) # set type trunk
FGT-MASTER (Trunk_Uplink_37) # set stp-state disabled
FGT-MASTER (Trunk_Uplink_37) # set packet-sampler enabled
FGT-MASTER (Trunk_Uplink_37) # set sample-direction rx
FGT-MASTER (Trunk_Uplink_37) # set mac-addr xx:xx:xx:xx:xx:xx
FGT-MASTER (Trunk_Uplink_37) # set members "port37"
FGT-MASTER (Trunk_Uplink_37) # next
FGT-MASTER (ports) # end
FGT-MASTER (SW_Core_1) # next
FGT-MASTER (managed-switch) # end
```

Esta configuración asigna múltiples VLANs a un puerto de tipo trunk (en este caso, port37), lo cual es común en enlaces de distribución o troncales hacia otros dispositivos de red. También se habilitan características adicionales como la

captura de paquetes (packet-sampler) y la desactivación del protocolo STP, típicamente gestionado a nivel central.

Este procedimiento también puede visualizarse y aplicarse mediante la interfaz gráfica de FortiGate, como se muestra en la siguiente Figura.

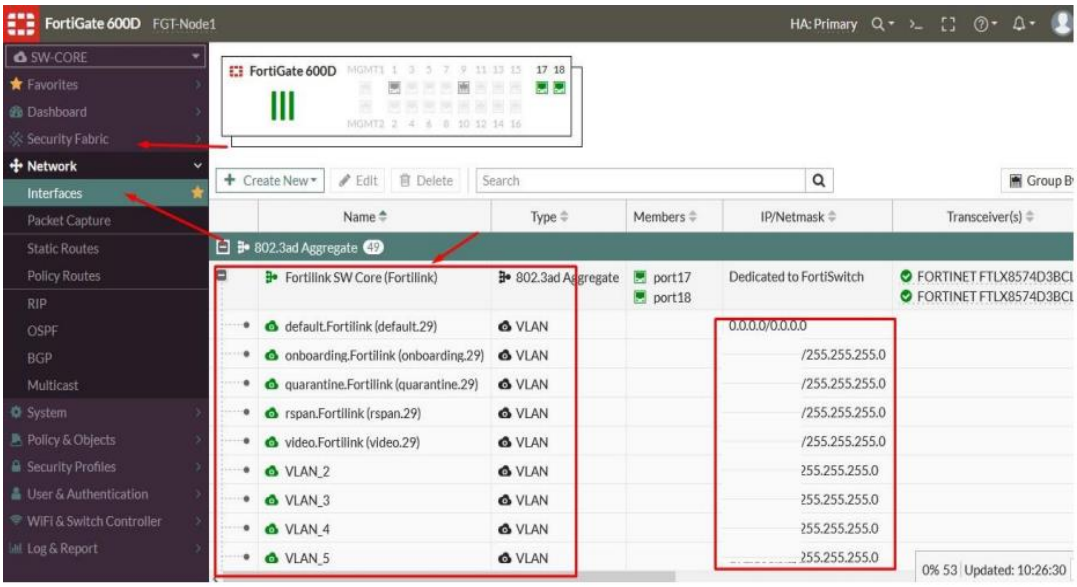


Figura 6, **Asignación de VLANs a puertos físicos desde GUI**.

6.16 TRUNK - LACP

El protocolo LACP (*Link Aggregation Control Protocol*) permite agrupar dos o más interfaces físicas de un mismo FortiSwitch en una interfaz lógica tipo *aggregate*, con el fin de aumentar el ancho de banda disponible y garantizar redundancia a nivel de capa 2.

Esta configuración es útil en escenarios donde se requiere alta disponibilidad y balanceo de carga hacia equipos con múltiples enlaces físicos. A continuación, se presenta el procedimiento CLI desde el FortiGate:

```
FGT-MASTER # config switch-controller managed-switch
```

```
FGT-MASTER (managed-switch) # edit "FS1E48T421000948"
FGT-MASTER (FS1E48T421000948) # config system interface
FGT-MASTER (interface) # edit "LAG_PORTCHANNEL_1"
FGT-MASTER (LAG_PORTCHANNEL_1) # set type aggregate
FGT-MASTER (LAG_PORTCHANNEL_1) # set member "port5" "port6"
FGT-MASTER (LAG_PORTCHANNEL_1) # next
FGT-MASTER (interface) # end
FGT-MASTER (FS1E48T421000948) # end
```

Se debe tomar en cuenta que LACP solo permite la agregación de puertos dentro de un mismo FSW. Para enlaces entre múltiples switches físicos, se debe aplicar una configuración **MCLAG**.

6.17 Configuración de Trunk – MC-LAG

Como parte del rediseño de infraestructura orientado a garantizar alta disponibilidad y resiliencia en la capa de acceso, se implementa **MC-LAG** (*Multi-Chassis Link Aggregation Group*). A diferencia de LACP tradicional, esta tecnología permite la agregación de enlaces entre interfaces ubicadas en diferentes FortiSwitches, ofreciendo redundancia tanto de interfaces como de equipos, sin introducir bucles de capa 2.

Esta solución resulta crítica en entornos como centros de datos o infraestructuras bancarias, donde se requiere mantener continuidad de servicio incluso ante fallos físicos en uno de los switches agregados.

Se establece la configuración desde el FortiGate en la interfaz gráfica como aparece la figura 6 y mediante los siguientes comandos:

```
FGT-MASTER # config switch-controller managed-switch
FGT-MASTER (managed-switch) # edit "FS1E48T421000948"
FGT-MASTER (FS1E48T421000948) # config switch interface
FGT-MASTER (interface) # edit "MCLAG_Trunk_1"
FGT-MASTER (MCLAG_Trunk_1) # set mclag 1
```

```
FGT-MASTER (MCLAG_Trunk_1) # set description "MCLAG Trunk Interface"
FGT-MASTER (MCLAG_Trunk_1) # set mode active
FGT-MASTER (MCLAG_Trunk_1) # set mclag-port "SW_Core_1_port25"
FGT-MASTER (MCLAG_Trunk_1) # set mclag-port "SW_Core_2_port25"
FGT-MASTER (MCLAG_Trunk_1) # next
FGT-MASTER (interface) # end
FGT-MASTER (FS1E48T421000948) # end
```

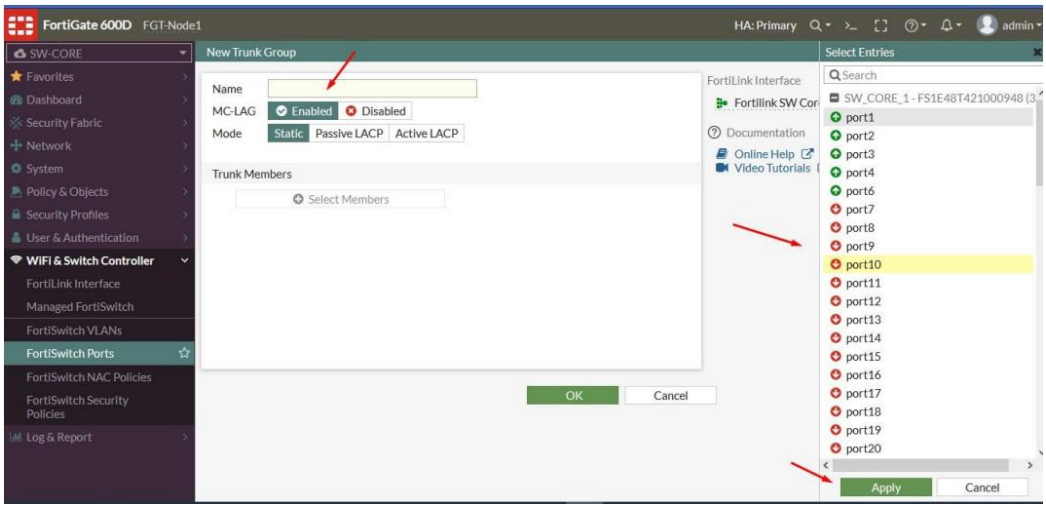


Figura 7, **Habilitación MC-LAG en Puertos.**

La implementación de MC-LAG, junto con FortiLink y LACP, completa el diseño de una arquitectura conmutada resiliente, alineada con los objetivos de continuidad operativa y segmentación eficiente de red definidos para la nueva infraestructura del banco.

6.18 Routing

En ruteo del FGT se configura igual, tenemos en la arquitectura de la entidad bancaria una configuración especial, tenemos OSPF configurado y VRRP. Para configurar estos protocolos, tenemos que habilitar el enrutamiento avanzado en el FGT.

6.19 Open Short Path First (OSPF)

Se implementa el protocolo de enrutamiento dinámico Open Shortest Path First (OSPF). Esta tecnología permite la redistribución eficiente de rutas entre los nodos principales del sistema: los dispositivos FortiGate ubicados en el Sitio Principal (SP), el Sitio Alterno (SA) y el núcleo central (Core).

La implementación de OSPF permite la convergencia automática de rutas, reduciendo la intervención manual ante cambios topológicos y garantizando alta disponibilidad en la comunicación entre las diferentes sedes de la institución.

La configuración se realiza mediante los siguientes comandos CLI:

```
FGT-CORE # config router static
FGT-CORE (static) # edit 6
FGT-CORE (6) # set status disable
FGT-CORE (6) # set dst 192.168.16.0 255.255.255.0
FGT-CORE (6) # set gateway 192.168.16.1
FGT-CORE (6) # set device "VLAN_16"
FGT-CORE (6) # next
FGT-CORE (static) # end
```

Una vez desactivada la ruta estática, se procede a la configuración de OSPF para redistribuir rutas conectadas y estáticas, y para publicar las redes internas:

```
FGT-CORE # config router ospf
FGT-CORE (ospf) # set distance-external 1
FGT-CORE (ospf) # set distance-inter-area 1
FGT-CORE (ospf) # set default-information-metric-type 1
FGT-CORE (ospf) # set default-metric 1
FGT-CORE (ospf) # set distance 1
FGT-CORE (ospf) # set router-id 192.168.0.1
FGT-CORE (ospf) # config area
FGT-CORE (area) # edit 0.0.0.0
FGT-CORE (area) # next
FGT-CORE (ospf) # end
FGT-CORE (ospf) # config ospf-interface
```

```
FGT-CORE (ospf-interface) # edit "OSPF"
FGT-CORE (OSPF) # set interface "VLAN_16"
FGT-CORE (OSPF) # next
FGT-CORE (ospf-interface) # end
FGT-CORE (ospf) # config network
FGT-CORE (network) # edit 1
FGT-CORE (1) # set prefix 192.168.16.0 255.255.255.0
FGT-CORE (1) # next
FGT-CORE (network) # end
FGT-CORE (ospf) # config redistribute "connected"
FGT-CORE (connected) # set status enable
FGT-CORE (connected) # set metric 1
FGT-CORE (connected) # set metric-type 1
FGT-CORE (connected) # end
FGT-CORE (ospf) # config redistribute "static"
FGT-CORE (static) # set metric 1
FGT-CORE (static) # set metric-type 1
FGT-CORE (static) # end
FGT-CORE (ospf) # end
```

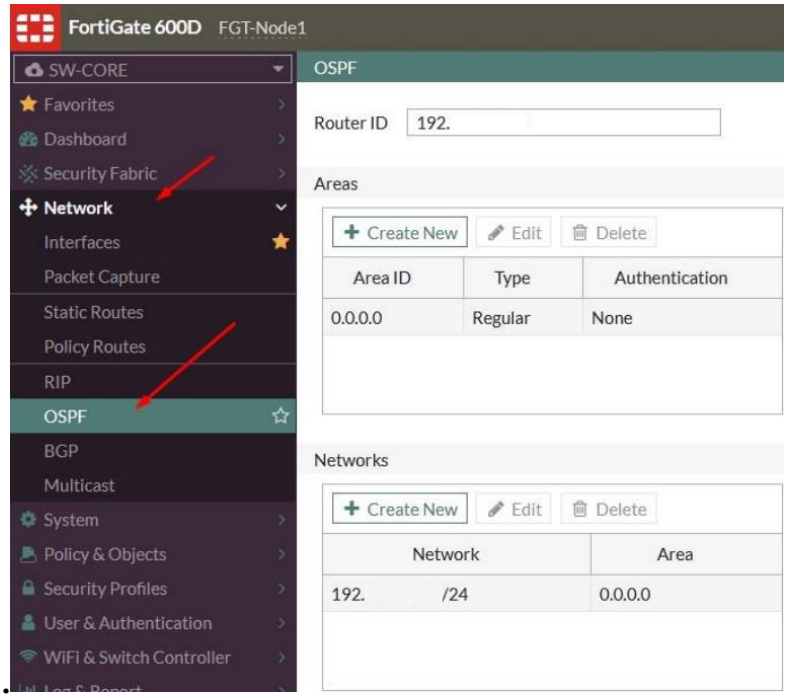


Figura 8, **Configuración de OSPF en FortiGate a través de CLI.**

Se configuramos los datos necesarios, y en el caso particular de la entidad

bancaria, las rutas se redistribuyen por medio de la VLAN 16.

6.20 Virtual Router Redundancy Protocol (VRRP)

Para la redundancia entre el (Sitio Principal) SP y (Sitio Alterno) SA, se ocupó el VRRP, esto lo que hace configurar una misma VLAN, con dos IPs diferentes y una IP flotante, en la cual al IP flotante es la que se configura en los clientes como puerta de enlace, el protocolo se encarga de según las métricas definidas para enrutar, cual camino debe de usar si el (Sitio Principal) SP o el (Sitio Alterno) SA.

Esta configuración se hace por únicamente por CLI en el FGT, en este documento, pondremos el ejemplo de una VLAN de la entidad bancaria tanto en (Sitio Alterno) SA como en (Sitio Principal) SP, las demás VLANs se configuran igual.

Las opciones más importantes de VRRP son las siguientes:

- ***Set vrgrp:*** Se crea un grupo el cual va a obedecer a un link-probe que en el caso de entidad bancaria apunta a Google, esto lo que hace es que si en el equipo que tenemos configurado el VRRP como primario se corta la conexión a Internet, inmediatamente le manda al equipo de SA el tráfico de internet.

- ***Set vrip:*** La IP virtual que va a funcionar como puerta de salida en las VLANs.

- ***Set priority***: Con este definimos cuál de los sitios es el primario, el de mayor valor en este campo, es el que será el primario para enrutar, siempre y cuando la conexión de internet no se interrumpa o si configuramos en el VRRP como primario el de (Sitio Alterno) SA.

- ***Set vrdst:*** Es el destino Link-Probe que el equipo estará chequeando para saber si mantener el primario o secundario para enrutar.

Sitio Principal:

```
FGT-SP (global) # config system interface
FGT-SP (interface) # edit "VLAN_2"
FGT-SP (VLAN_2) # set vdom "SW-CORE"
FGT-SP (VLAN_2) # set dhcp-relay-service enable
FGT-SP (VLAN_2) # set ip 192.168.X.X 255.255.255.0
FGT-SP (VLAN_2) # set allowaccess ping
FGT-SP (VLAN_2) # set description "VLAN_X"
FGT-SP (VLAN_2) # set device-identification enable
FGT-SP (VLAN_2) # set vrrp-virtual-mac enable
FGT-SP (VLAN_2) # config vrrp
FGT-SP (vrrp) # edit X
FGT-SP (X) # set vrgrp X
FGT-SP (X) # set vrip 192.168.X.1
FGT-SP (X) # set adv-interval 15
FGT-SP (X) # set priority 150
FGT-SP (X) # set vrdst 8.8.8.8
FGT-SP (X) # set start-time 10
FGT-SP (X) # next
FGT-SP (vrrp) # end
FGT-SP (VLAN_2) # set role lan
FGT-SP (VLAN_2) # set snmp-index 68
FGT-SP (VLAN_2) # set dhcp-relay-ip "192.168.X.X"
FGT-SP (VLAN_2) # set interface "Fortilink"
FGT-SP (VLAN_2) # set vlanid X
FGT-SP (VLAN_2) # next
FGT-SP (interface) # end
```

Sitio Alterno:

```
FGT-SA (global) # config system interface
FGT-SA (interface) # edit "VLAN_X"
FGT-SA (VLAN_X) # set vdom "SW-CORE_SA"
FGT-SA (VLAN_X) # set dhcp-relay-service enable
FGT-SA (VLAN_X) # set ip 192.168.X.X 255.255.255.0
FGT-SA (VLAN_X) # set allowaccess ping
FGT-SA (VLAN_X) # set description "VLAN_X"
FGT-SA (VLAN_X) # set device-identification enable
FGT-SA (VLAN_X) # set vrrp-virtual-mac enable
FGT-SA (VLAN_X) # config vrrp
FGT-SA (vrrp) # edit X
FGT-SA (X) # set vrgrp X
```

```
FGT-SA (X) # set vrip 192.168.X.1
FGT-SA (X) # set adv-interval 15
FGT-SA (X) # set priority 150
FGT-SA (X) # set vrdst 8.8.8.8
FGT-SA (X) # set start-time 10
FGT-SA (X) # next
FGT-SA (vrrp) # end
FGT-SA (VLAN_X) # set role lan
FGT-SA (VLAN_X) # set snmp-index 68
FGT-SA (VLAN_X) # set dhcp-relay-ip "192.168.X.X"
FGT-SA (VLAN_X) # set interface "Fortilink"
FGT-SA (VLAN_X) # set vlanid X
FGT-SA (VLAN_X) # next
FGT-SA (interface) # end
```

6.21 Etapa de Evaluación.

En esta etapa se realizarán pruebas de las configuraciones realizadas en los FortiGate, integrando un FortiSwitch en un segmento de red que no esté en producción, con el fin de validar que las configuraciones y políticas en el FortiGate son enviadas de forma automática al autorizar la interfaz del FortiGate. A su vez, se realizarán pruebas de tráfico con endpoints. Una vez que estas pruebas sean satisfactorias, se procederá a la migración paulatina de la infraestructura total y a asignarle las VLANs correspondientes al área.

Se implementarán pruebas funcionales y de integración para asegurar que la comunicación entre los equipos mediante FortiLink se establece correctamente, permitiendo una administración centralizada y la aplicación coherente de políticas de seguridad en toda la red. Estas pruebas se llevarán a cabo en un entorno controlado, replicando las condiciones operativas de la entidad bancaria, para identificar y mitigar posibles conflictos de configuración o incompatibilidades antes de su implementación en el entorno de producción.

Además, se evaluará la capacidad del sistema para manejar el tráfico de red esperado, incluyendo la segmentación mediante VLANs y la priorización de

servicios críticos, como transacciones financieras y comunicaciones internas. Se utilizarán herramientas de monitoreo para analizar el rendimiento de la red, la latencia y la capacidad de respuesta de los dispositivos integrados. Esta evaluación exhaustiva garantizará que la nueva infraestructura cumpla con los estándares de seguridad y eficiencia requeridos por la entidad bancaria.

Una vez completadas las pruebas y validaciones, se documentarán los resultados y se procederá con la migración gradual de la infraestructura existente, asegurando una transición sin interrupciones y minimizando el impacto en las operaciones diarias de la entidad.

7. Conclusiones y Recomendaciones.

7.1 Conclusiones.

La infraestructura de red implementada en la entidad bancaria, basada en tecnología Fortinet, ofrece una solución robusta para las necesidades de seguridad, administración y disponibilidad en el entorno bancario. La transición desde dispositivos Cisco hacia Fortinet se realizó de manera controlada, asegurando la continuidad operativa y minimizando el riesgo de interrupciones.

La integración de FortiLink entre FortiGate y FortiSwitch permite una administración centralizada, mejorando la gestión de VLANs y asegurando la aplicación uniforme de políticas de seguridad. Esto optimiza los tiempos de respuesta ante incidentes y reduce los errores operativos.

La solución MCLAG con enlaces ISL/ICL garantiza la redundancia de los dispositivos de red, asegurando la disponibilidad continua del servicio ante fallos. Además, las pruebas en un entorno no productivo validan la correcta propagación de configuraciones y la operatividad de los enlaces, lo que permite proceder con la migración total de forma segura.

En resumen, la infraestructura implementada no solo cumple con los objetivos del proyecto, sino que también establece una base sólida para futuros requerimientos y ampliaciones tecnológicas, asegurando la protección de los recursos digitales críticos de la entidad bancaria.

7.2 Recomendaciones.

Capacitar al personal técnico de TI de la entidad bancaria en la administración y operación de la arquitectura Secure Access de Fortinet, asegurando así un manejo adecuado de las nuevas funcionalidades implementadas, especialmente en lo referente a la gestión de VLANs, configuración de políticas de seguridad y control de accesos.

Actualizar periódicamente el firmware de los dispositivos Fortinet, siguiendo las recomendaciones del fabricante, con el objetivo de mantener la infraestructura protegida ante nuevas vulnerabilidades, mejorar la compatibilidad entre dispositivos y garantizar la estabilidad operativa de la red.

Ampliar gradualmente la integración de otros servicios críticos del banco a la infraestructura Fortinet, como sistemas de monitoreo CCTV, autenticación biométrica o servicios de nube híbrida, para aprovechar las ventajas de escalabilidad, segmentación y protección que ofrece la arquitectura Secure Access.

Documentar todos los cambios, configuraciones y procedimientos realizados durante la migración e implementación, creando una base de conocimiento interna que sirva como referencia para futuras intervenciones, auditorías o ampliaciones del sistema de red.

Evaluar periódicamente la infraestructura mediante auditorías de red y pruebas de penetración, para verificar la efectividad de las políticas de seguridad implementadas, identificar áreas vulnerables y mantener los niveles de ciberseguridad requeridos por el sector bancario.

8. Bibliografía

BlackBox. (s.f.). *BlackBox*. Obtenido de Blackbox.com: https://www.blackbox.com/es-es/insights/black-box-explica-old/redes/que-es-poe-power-over-ethernet

Burke, J. (noviembre de 2022). *www.techtarget.com*. Obtenido de https://www.techtarget.com/searchnetworking/definition/throughput#:~:text=Throughput%20is%20a%20measure%20of,and%20network%20systems%20to%20organizations.

Ciberseguridadtips.com. (26 de agosto de 2022). *ciberseguridadtips.com*. Obtenido de https://ciberseguridadtips.com/definicion-de-antimalware/#Antimalware_definicion

Cisco. (28 de 08 de 2019). *Cisco*. Obtenido de Cisco: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html

Cisco. (18 de 08 de 2020). *Cisco*. Obtenido de Cisco: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350x-series-stackable-managed-switches/smb5252-what-is-stacking.html

CompTIA. (s.f.). *CompTIA*. Obtenido de CompTIA: https://www.comptia.org/content/guides/what-is-a-wide-area-network

DAVID ALEJANDRO TORRES JOSE FELIPE ZAMBRANO. (12/06/2020). *MANUAL DE CONFIGURACIÓN DE VDOM EN FORTIGATE, MODERNIZACION TECNOLÓGICA DE LA INFRAESTRUCTURA DE LOS SERVICIOS DE*

SEGURIDAD PERIMETRAL PARA LA RED CORPORATIVA. Bogota, Colombia. Obtenido de https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/4411/Roncancio_Torres_David_Alejandro_Anexo_C_2020.pdf?sequence=5&isAllowed=y

Economipedia. (11 de 01 de 2016). *economipedia, Tarjeta de credito*. Obtenido de https://economipedia.com/definiciones/tarjeta-de-credito.html

Economipedia. (31 de 01 de 2016). *Economipedia, Tarjeta de debito*. Obtenido de https://economipedia.com/definiciones/tarjeta-de-debito.html

Etecé, E. (05 de agosto de 2021). *Antivirus informático.* (E. Equipo editorial, Ed.) Obtenido de https://concepto.de/antivirus-informatico/

FORTINET. (23 de 02 de 2017). Obtenido de SECURE ACCESS SOLUTION: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SG-SAA-Enterprise-Network.pdf

FORTINET. (07 de 06 de 2022). *Community Fortinet VRRP configuration and debug.* Obtenido de VRRP configuration and debug: https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-VRRP-configuration-and-debug/ta-p/197015

FORTINET. (31 de 05 de 2022). *FORTINET DOCUMENT LIBRARY.* Obtenido de FortiOS 7.0.5 Administration Guide: https://docs.fortinet.com/document/fortigate/7.0.5/administration-guide/19246/sd-wan

FORTINET. (31 de 05 de 2022). *FORTINET DOCUMENT LIBRARY.* Obtenido de FortiOS 7.0.5 Administration Guide:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/e4a593af-8913-11ec-9fd1-fa163e15d75b/FortiOS-7.0.5-Administration_Guide.pdf

FORTINET. (03 de marzo de 2023). *docs.fortinet.com-Guía de administración de FortiOS*. Obtenido de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/541164a8-66d4-11ed-96f0-fa163e15d75b/FortiOS-7.2.4-Administration_Guide.pdf

FORTINET. (28 de 02 de 2023). *FORTINET DOCUMENT LIBRARY-FortiSwitchOS 7.2.3 Administration Guide—Standalone Mode.* Obtenido de https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a5cb2173-7e2e-11ec-a0d0-fa163e15d75b/FortiSwitch-7.0.4-FortiSwitch_Devices_Managed_by_FortiOS_7.0.pdf

Fortinet. (2023). *www.fortinet.com/cyberglossary*. Obtenido de www.fortinet.com/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp

FORTINET. (s.f.). *help.fortinet.com*. Obtenido de LACP: https://help.fortinet.com/fadc/4-0-0/html-e/Content/Quick_Start/Link_Aggregation.htm

FORTINET. (s.f.). *www.fortinet.com,Definición del sistema de prevención de intrusiones*. Obtenido de https://www.fortinet.com/resources/cyberglossary/what-is-an-ips

International Telecommunication Union (ITU). (Julio de 1994). *itu Committed to connecting the world*. Obtenido de www.itu.int: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=2820&lang=es

Kaspersky. (04 de 12 de 2017). *Kaspersky*. Obtenido de Latam Kaspersky: https://latam.kaspersky.com/resource-center/definitions/utm

Lutkevich, B. (01 de abril de 2021). *https://www.techtarget.com/*. Obtenido de https://www.techtarget.com/searchdatacenter/definition/high-availability

Manson, L. M. (06 de mayo de 2010). *monografias.com*. Obtenido de https://www.monografias.com/trabajos/estudiovirus/estudiovirus

MARTÍNEZ MOLINA, K. J., PACHECO MENESES, J., & ZÚÑIGA SILGADO, I. (julio-diciembre, 2009). *Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas).* Obtenido de https://www.redalyc.org/articulo.oa?id=553756879003

Pachón, C. (01 de julio de 2019). *www.nsit.com.co - Fortilink*. Obtenido de https://www.nsit.com.co/secure-access-fortiswtich-y-fortiap-ventajas-de-seguridad/#:~:text=%C2%BFFortiLink%3A%20Qu%C3%A9s%20es%3F,appliances%20de%20seguridad%20de%20FortiGate.

Shaw, K. (04 de 10 de 2022). *networkworld*. Obtenido de networkworld: https://www.networkworld.com/article/3584876/what-is-a-network-switch-and-how-does-it-work.html

Superintendencia de Bancos y de Otras Instituciones, (SIBOIF). (19 de septiembre de 2007). *NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO.* Obtenido de Resolución Nº CD-SIBOIF-500-1-SEP19-2007: https://www.superintendencia.gob.ni/sites/default/files/documentos/normas/cd-siboif-500-1-sep19-2007_-_nrt_2015.pdf

Techopedia. (18 de agosto de 2011). *www.techopedia.com, Hot Standby Router Protocol (HSRP)*. Obtenido de https://www.techopedia.com/definition/15679/hot-standby-router-protocol-hsrp

Villanueva, J. C. (25 de octubre de 2022). *https://www-jscape-com.translate.goog Clúster de alta disponibilidad activo-activo frente a activo-pasivo*. Obtenido de https://www-jscape-com.translate.goog/blog/active-active-vs-active-passive-high-availability-cluster?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=rq#:~:text=Overview,%2Dactive%20and%20active%2Dpassive

www.finanzasparatodos.es. (16 de abril de 2010). *www.finanzasparatodos.es*. Obtenido de https://www.finanzasparatodos.es/es/productosyservicios/productosbancariosfinanciacion/prestamospersonales.html

www.ionos.es. (10 de septiembre de 2018). *IP* . Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/internet-protocol-definicion-y-fundamentos/

www.scotiabankcolpatria.com. (s.f.). *Qué es una Cuenta de Ahorros - Scotiabank Colpatria*. Obtenido de https://www.scotiabankcolpatria.com/personas/cuentas-e-inversion/mas-informacion/definicion-cuenta-ahorro#:~:text=Una%20cuenta%20de%20ahorros%20es,tu%20dinero%20de%20forma%20r%C3%A1pida.

Tablas de Etapa de Análisis

Tabla A

Proveedor	Precio Aproximado (USD)	Costo de Licenciamiento	Ventajas	Consideraciones
Fortinet	$2,000 - $3,000	Múltiples funciones de seguridad incluidas con una única licencia.	Alto rendimiento, integración UTM, SD-WAN sin costos extra.	Enfoque en integración con soluciones Fortinet.
Cisco	$1,500 - $2,500	Licencias adicionales para IPS, VPN y filtrado web.	Amplia compatibilidad con entornos empresariales.	Dependencia de licencias para seguridad avanzada.
Palo Alto Networks	$500 - $700	Costos adicionales por Threat Prevention y WildFire.	Detección de amenazas avanzadas.	Modelo basado en suscripción.
Check Point	$1,000 - $1,500	Licenciamiento basado en paquetes de seguridad.	Seguridad robusta con segmentación granular.	Puede requerir módulos adicionales.
Juniper Networks	$600 - $1,200	Licencias necesarias para IPS y filtrado de contenido.	Buen rendimiento en redes complejas.	CLI más técnica, curva de aprendizaje alta.
Sophos	$1,500 - $2,000	Licenciamiento por servicios como Sandstorm (sandboxing).	Integración con soluciones de endpoint.	Mayor costo si se requieren funciones avanzadas.
SonicWall	$2,000 - $3,000	Licencias requeridas para filtrado avanzado y protección ATP.	Opciones flexibles para medianas empresas.	No tan optimizado para grandes entornos bancarios.

WatchGuard	$1,500 - $2,500	Suscripciones para funciones avanzadas.	Gestión centralizada y facilidad de configuración.	Costo adicional por servicios completos.

Tabla B

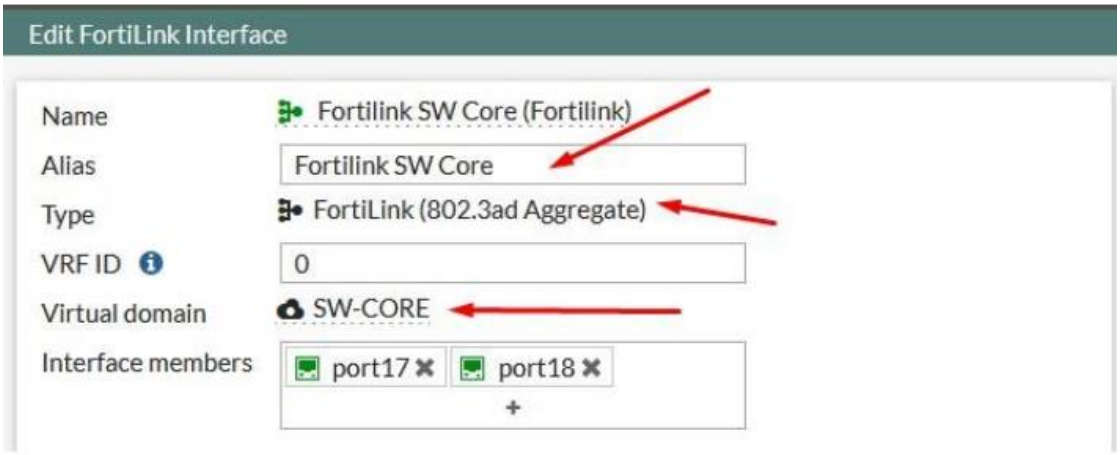
Criterio	Fortinet	Cisco
Rendimiento	Alto rendimiento con procesadores ASIC dedicados.	Buen rendimiento, pero depende más del software.
Costo	Generalmente más económico en términos de hardware y licenciamiento.	Más costoso, especialmente en licencias y mantenimiento.
Facilidad de uso	Interfaz más intuitiva y fácil de configurar.	Curva de aprendizaje más pronunciada, requiere más experiencia.
Seguridad	Soluciones de seguridad integradas con FortiGuard y UTM.	Seguridad robusta con enfoque en segmentación y detección avanzada.
Integración	Mejor integración con su propio ecosistema Fortinet.	Mayor compatibilidad con entornos empresariales y multi-vendor.
Escalabilidad	Buena escalabilidad, pero más enfocada en medianas empresas.	Más escalable para grandes empresas y entornos corporativos.
Soporte	Soporte eficiente, pero a veces limitado en documentación.	Soporte sólido con una amplia comunidad y documentación extensa.
Popularidad	En crecimiento, especialmente en PYMEs.	Amplia adopción en empresas y gobiernos.

Tabla C

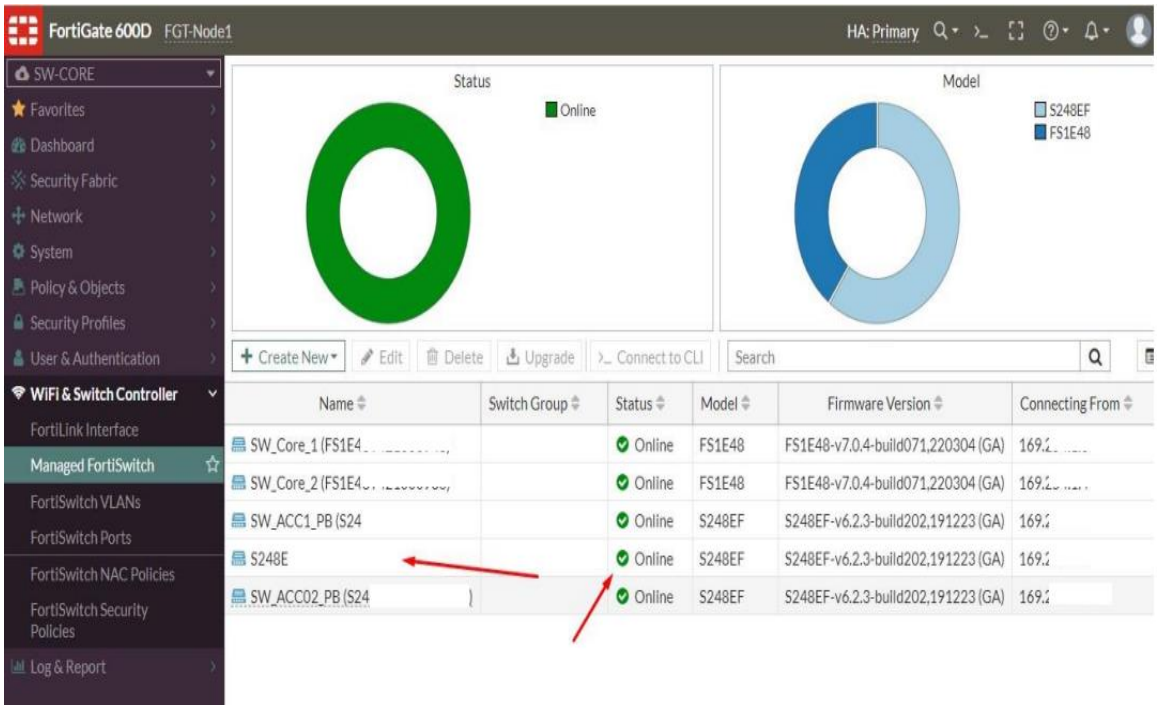
Componente	Función Principal	Cantidad	Precio Unitario (USD)	Costo Total de Adquisición (USD)	Precio Anual de Soporte (USD)
FortiGate 200F	Seguridad y filtrado de tráfico en el sitio alterno	3	$5,861	$17,583	$2,164
FortiGate 600D	Firewall perimetral y switch controller en HA en el sitio principal	2	$10,128	$20,256	$3,450
FortiSwitch 1048E	Switches de distribución de alto rendimiento	2	$21,641	$43,282	$2,164
FortiSwitch 448E	Switches de acceso para conectividad de usuarios	5	$2,402	$12,010	$240
FortiSwitch 448E-FPOE	Switches de acceso con PoE para dispositivos como cámaras y teléfonos IP	6	$5,835	$35,010	$584
Total, Inversión				**$128,141**	
Total, Costo Soporte Anual					**$22,574**
Costo Total inversión más soporte					**$150.715**

Anexos

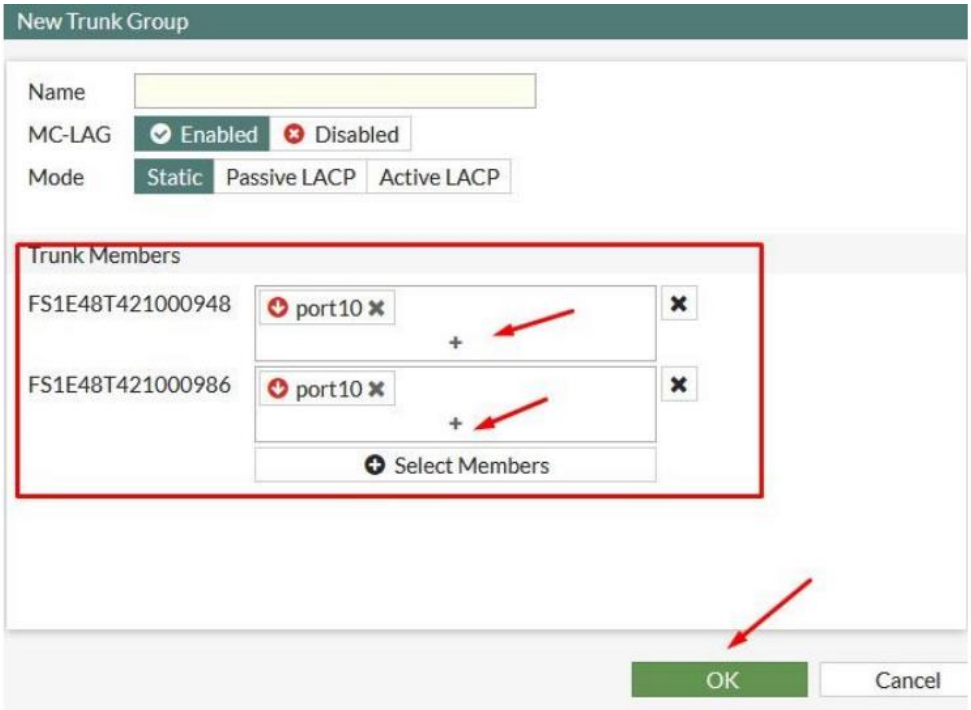
Anexo A: Creación de interface Fortilink en Fortigate para los Switch Core.



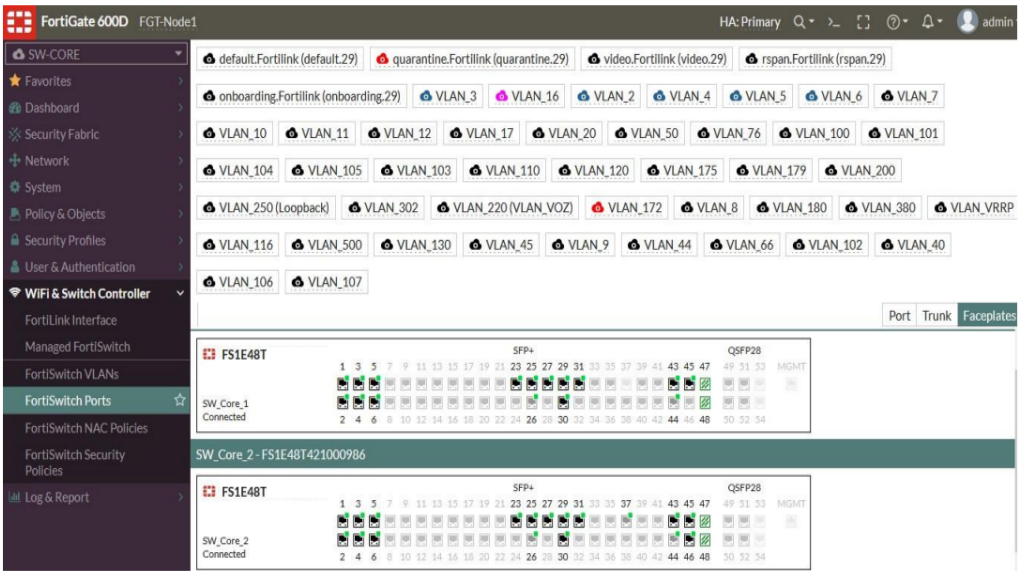
Anexo B: Fortiswitch autorizado.



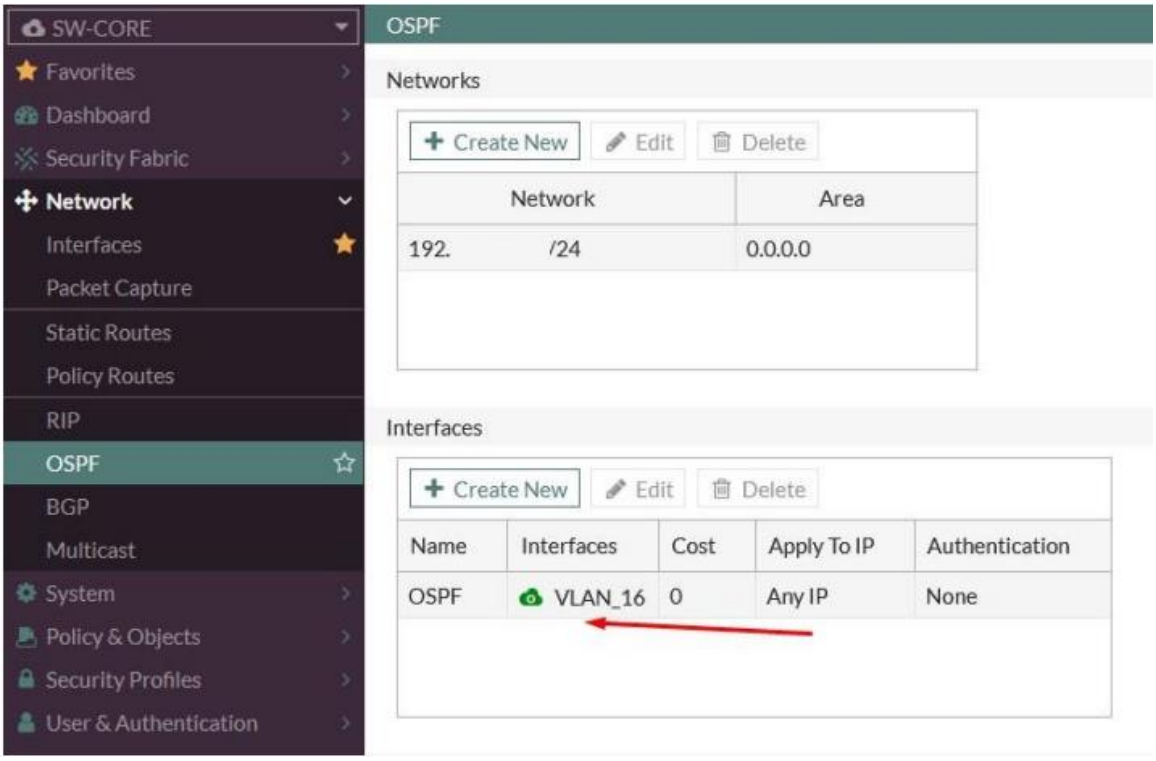
Anexo C: Agregar puerto de los miembros del troncal a crear.



Anexo D: VLAN permitidas en los troncales creados.



Anexo E: Redistribución de las rutas por medio la VLAN asignada.



Anexo F: ubicación en los racks.