Diseño e implementación de un sistema de seguridad integral para un cliente de la empresa CORE IP SAS.

YEISON MONSALVE SANCHEZ

Informe de trabajo de grado como requisito para optar al título de:
Ingeniero de Telecomunicaciones

Tutor
Luis Alejandro Fletscher Bocanegra, Phd
Profesor Facultad de Ingeniería

Jose Gerardo Toro
Director de Ingeniería CoreIP SAS

Universidad de Antioquia
Facultad de Ingeniería
Ingeniería de Telecomunicaciones
Medellín, Antioquia, Colombia
2022

Resumen

En este informe se evidencia el proceso de implementación de un sistema integral de seguridad de red, conformado por varios softwares y herramientas, que son sincronizados para una mayor protección y estabilidad del despliegue. Inicialmente se describe el contexto actual de las soluciones de ciberseguridad en el entorno empresarial, posteriormente se establece el diseño de la topología de red tanto física como lógica, diseñada con equipos de la marca Fortinet, que en la actualidad es una empresa líder en la implementación de Firewalls. Más adelante se encuentra de manera detallada el proceso de implementación y despliegue, donde además se describen varios conceptos claves para entender el proceso llevado a cabo, finalmente, se presentan las conclusiones donde se evidencia la importancia de los pasos a seguir para garantizar un avance seguro en todo el proceso de implementación de la infraestructura de red solicitada por el cliente.

Introducción

La ciberseguridad es un factor cada vez más importante en la vida de las personas y de las empresas, sobre todo en los tiempos actuales con el impacto tecnológico y económico que trajo consigo la cuarentena por la pandemia del COVID-19. Esta situación exigió a las organizaciones una extensión del lugar de trabajo por fuera de las áreas locales, un cambio en la modalidad que las llevó a adoptar forzosamente el home office. Para estos casos se hace necesario la implementación de protocolos de protección en los sistemas y equipos de cada uno de los colaboradores de la organización, tanto de aquellos que están en las instalaciones de la empresa como de aquellos que trabajan en casa u otros lugares, esto con el propósito de eliminar los riesgos potenciales en la totalidad de la red y proteger completamente la información almacenada localmente y en la nube.

En la actualidad, el software y el hardware se han convertido en herramientas fundamentales de las organizaciones, sin embargo, son armas de doble filo porque representan tanto una ventaja empresarial como un riesgo de cibercrimen, ya que se pueden presentar ataques como espionaje industrial, hacking, virus, leaking de información, etc. Lo que crea la necesidad de protección, más aún cuando las empresas se posicionan como competidores fuertes en los mercados, ya que se hacen más atractivas a delincuentes cibernéticos, por lo tanto entre mayor sea el crecimiento mayor será la necesidad de reforzar las medidas de seguridad para evitar los tipos de ataques ya mencionados.

Gracias a la evolución considerable de las técnicas para afrontar los diversos ataques informáticos, hoy se encuentran en el mercado diferentes herramientas de seguridad de hardware y software, las cuales ayudan a reforzar la seguridad informática en las organizaciones, algunas de estas herramientas son, antivirus, firewalls, antimalware y antispam. Por otra parte, está la figura del administrador del área de TI, quien se debe encargar de generar alertas y advertencias, enviando comunicados a los responsables de los equipos o servicios que se vean afectados, realizando el adecuado tratamiento de incidentes,

estudio y análisis de los eventos, con el objetivo de determinar las causas de la aparición de dichas amenazas. Cabe destacar que las amenazas o ataques no provienen únicamente desde afuera, también existen amenazas y ataques que se generan o provienen del interior de las organizaciones, es decir, desde la propia infraestructura tecnológica que posee la empresa.

Los clientes de la empresa CORE IP SAS tienen la misma preocupación y es por esto que el objetivo del presente proyecto es implementar un nuevo diseño en el esquema de seguridad de uno de los clientes corporativos (por cuestiones de confidencialidad no se revela el nombre del cliente). Esta implementación se convertirá en la base estructural de nuevos protocolos de seguridad, con una infraestructura tecnológica sólida, robusta e integrable, utilizando la tecnología de Fortinet, que permitirá realizar monitoreos y auditorías de seguridad periódicas, analizar los riesgos de delito informático y establecer medidas preventivas.

Objetivo general

Desplegar una solución de seguridad integral de red para un cliente corporativo de la empresa CORE IP SAS, mediante la integración de software y herramientas del proveedor Fortinet.

Objetivos Específicos

Identificar las necesidades y requerimientos de la empresa cliente, a nivel de redes y enrutamiento para el levantamiento de información de cara al despliegue del sistema a diseñar.

Diseñar la solución para la seguridad integral del cliente, mediante la integración de software y hardware del fabricante de ciberseguridad Fortinet.

Apropiar las funcionalidades y herramientas de los equipos Fortinet durante la implementación de la solución para la seguridad integral del cliente.

Realizar pruebas y validar el funcionamiento de los diferentes componentes desarrollados en cada etapa del proyecto, tanto en entorno local como en la nube.

Marco Teórico

Dentro del proyecto se utilizarán diferentes herramientas que permitirán realizar el correcto despliegue y desarrollo para la seguridad integral del cliente. A continuación, se definirán algunas de ellas, ya que es importante para tener claridad en el trabajo.

Infraestructura de red [1]

La infraestructura de red la constituyen todos los recursos de una red que hacen posible la conectividad, gestión, operación, comunicación de red interna o externa (internet), todos los componentes de la red determinados entre hardware y software, sistemas y dispositivos. Permite la información y comunicación entre usuarios, servicios, aplicaciones y procesos, todo lo que esté involucrado en la red, desde servidores hasta enrutadores inalámbricos, se une para formar la infraestructura de red de un sistema. La infraestructura de red permite una comunicación y un servicio efectivo entre usuarios, aplicaciones, servicios, dispositivos, etc.

1. **Centralización del tráfico**

El crecimiento inorgánico, las fusiones y nuevas adquisiciones pueden confundir aún más la infraestructura de la red. Como resultado, una empresa puede terminar con múltiples herramientas separadas que monitorean y administran una gran red híbrida. Mantener una visibilidad total en toda la infraestructura de red permite descubrir puntos ciegos y establecer una infraestructura de seguridad de red sólida. Esto es clave tanto para la supervisión del rendimiento como para la detección de amenazas de todas las fuentes lo que posibilita remediarlas más rápidamente.

2. **Filtrado de los datos correctos durante el tráfico.**

Los datos duplicados pueden representar del 50% al 66% del tráfico de la red. La eliminación de datos duplicados es fundamental cuando se trata de la eficacia de las soluciones de seguridad de red. Los proveedores de seguridad deben gestionar todos los datos que necesitan procesar. A mayor cantidad, más tediosa es la gestión, por tanto, enviar el tipo correcto de datos a la herramienta adecuada es un aspecto crítico de las redes de infraestructura, para esto, se realiza el filtrado de tráfico inteligente que permitiría, por ejemplo, que el tráfico de correo electrónico se envíe a las herramientas de seguridad del correo electrónico, mientras se descarta el tráfico de video.

3. **Amenazas contra la ciberseguridad**

Actualmente se encuentra una cantidad considerable de amenazas cibernéticas que ponen en riesgo la estabilidad y protección de la información de las personas y organizaciones, algunas de estas amenazas son:

- Anexos a mensajes enviados por correo electrónico infectados con virus.
- El intercambio de códigos de virus.
- Firewalls mal configurados.

- Ataques a la disponibilidad de los recursos de información existentes en la red (bancos de datos o software disponibles para ser descargados por los usuarios).
- Alteración de páginas web.
- El "repudio" y las estafas asociadas al comercio electrónico.
- Las vulnerabilidades de los sistemas operativos y la desactualización de los “parches" concernientes a su seguridad.
- Rotura de contraseñas.
- Suplantación de identidades.
- Acceso a paginas pornograficas, terroristas, etc.
- Robo y la destrucción de información.
- Pérdida de tiempo durante el acceso a sitios ajenos a la razón social de la entidad.
- Herramientas de hacking y cracking ofrecidas como freeware.

Fortinet [2]

Fortinet es una empresa multinacional de Estados Unidos con sede en Sunnyvale, California. Se dedica al desarrollo y la comercialización de software, dispositivos y servicios de ciberseguridad, como firewalls, antivirus, prevención de intrusiones y seguridad en dispositivos de usuario, entre otros. Es la cuarta compañía de seguridad de redes más grande por volumen de ingresos.

1. **Seguridad perimetral con FortiGate**

Fortinet con sus equipos FortiGate trae la nueva generación de dispositivos de seguridad en tiempo real Unified Threat Management (UTM) o Gestión Unificada de Amenazas. Una solución integral de seguridad, con equipos que pueden mitigar las amenazas de seguridad de manera casi independiente. Estos equipos se basan en el principio de detener en tiempo real los ataques de contenido, del tráfico que entra y sale de los accesos principales de una red corporativa.
FortiGate incluye una serie de funciones de seguridad como firewalls de nueva generación (NGFW), prevención de intrusiones, filtrado web y protección frente a malware o correo no deseado.

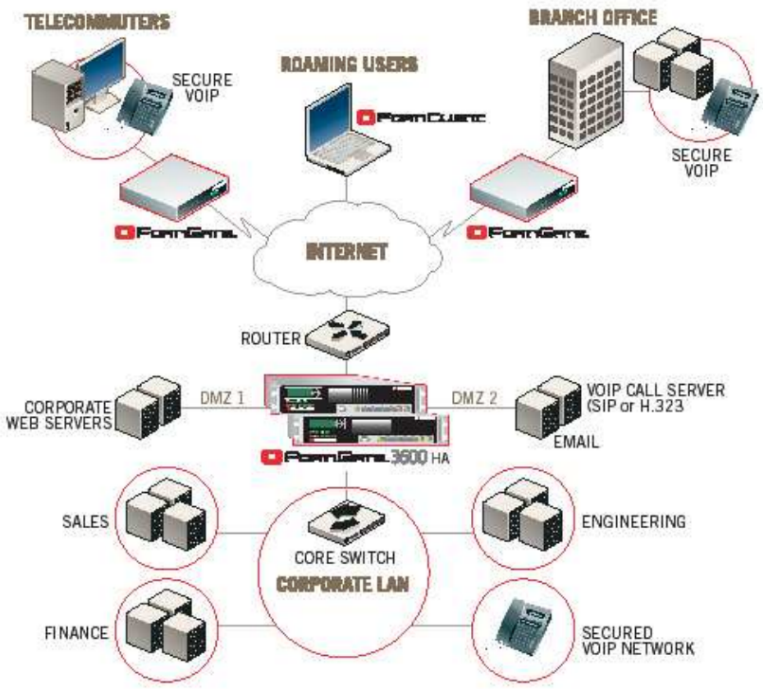

Figura 1: Ambiente de red corporativa con seguridad basada en Fortinet [3]

La figura 1 muestra que Fortinet basa su seguridad en un sistema centralizado, donde el equipo ocupa la parte perimetral de la red. Dependiendo de las posibilidades económicas del cliente corporativo, se puede adoptar sistemas de alta disponibilidad, es decir, más de un equipo de seguridad perimetral, en línea.
Al interior de los equipos FortiGate, se maneja una compleja solución basada en hardware, donde se proveen los siguientes servicios: Antivirus, Firewall, IPS e IPsec-VPN. Cada uno de estos servicios de seguridad es ejecutado en tiempo real, ya que el procesamiento es directo en hardware y gestionados a través de un sistema operativo que permite la configuración de cada uno de los parámetros que implican los servicios antes mencionados.
Cuentan con certificación internacional por la ICSA Labs que garantiza tanto los servicios como la compatibilidad con otros fabricantes. El sistema operativo de FortiGate cuenta con la capacidad de configurar y ejecutar otro tipo de servicios como AntiSpyWare, Traffic Shaping (QoS), Anti-Spam, Dominios Virtuales, Filtrado de Contenido.
Cabe señalar que estos equipos serán óptimos en su funcionamiento, siempre y cuando estén a cargo de técnicos calificados en seguridad en redes de datos. Caso contrario cualquier solución por más sofisticada que sea, sin un adecuado manejo y administración, será tanto o más deficiente como los primeros sistemas de seguridad para redes de datos.

2. FortiClient

El software de VPN FortiClient brinda una conexión segura a los dispositivos o usuarios que se encuentran fuera de la red local. Es un producto de seguridad de endpoint para PC de escritorio, teléfonos y otros dispositivos.

3. FortiGuard + FortiMail

Los productos antispam de FortiGuard y de seguridad de mensajería FortiMail integran capacidades avanzadas para proteger contra amenazas versátiles como suplantación de identidad, malware, ransomware y ataques BEC (Business Email Compromise).

4. **FortiManager + FortiAnalyzer**

FortiAnalyzer es uno de varios sistemas de censado y análisis que brinda funciones de generación de informes para los productos de Fortinet, incluidos registro de eventos, informes de seguridad y análisis de amenazas. FortiManager es un software de seguridad de centros de datos que permite administrar cualquier equipo diseñado por Fortinet conectado a la red desde un punto central. Los equipos de Fortinet son capaces de integrarse con cualquier herramienta o centro de datos que se desee proteger virtualmente ya sea localmente o en la nube.

Metodología

Para el desarrollo del trabajo se siguió la metodología definida a continuación, en cada una de las fases estipuladas se desarrolla una etapa importante del proyecto que contribuye al objetivo final.

Fase 1. Evaluación de la infraestructura actual.

En esta etapa se evaluó la infraestructura de red lógica y física que se encontraba instalada, realizando copias de seguridad, diseños de topología de red e integración de los dispositivos.

Actividad 1.1 Se identificaron los dispositivos de red a los cuales se le realizó un backup de las configuraciones.

Actividad 1.2 Se realizó la evaluación de infraestructura de red, tanto física (diagrama de conexiones y cableado estructurado) como lógica (diagrama de Vlans, políticas de firewall y direccionamiento IP).

Actividad 1.3 Se evaluaron de manera detallada los requerimientos del cliente para la implementación de la seguridad integral de red.

Fase 2. Diseño, Implementación y despliegue inicial.

Implementación del FIREWALL (NGFW) FORTIGATES HA.

En esta fase se implementó la instalación del equipo FortiGate 600E, para esto se realizó el reconocimiento del equipo FortiGate 200E, el cual se encontraba en producción y estaba ubicado en el centro de datos. Se exploraron todas las configuraciones, servicios y conexiones, las cuales se adaptaron en los nuevos equipos para su instalación.

Actividad 2.1. Se realizó la Instalación y configuración del firewall FortiGate para su puesta en operación.

Actividad 2.2. Se definió la estructura de red con la nueva configuración del firewall FortiGate, esta configuración contiene nuevas políticas de seguridad, migración de servicios y creación de VDOMS.

Actividad 2.3. Se realizó verificación de información, configuración de equipos y continuidad de estabilidad, con lo cual se procedió a realizar el armado de HA (Alta Disponibilidad) entre los firewalls FortiGate.

Fase 3: Despliegue e Integración (CAMBIO DE EQUIPOS CONECTIVIDAD SWITCH).

En esta fase se realizó el reconocimiento de la topología de red anterior y se analizó la configuración del equipo Cisco 4507R+E, el cual estaba en producción y ubicado en el centro de datos. Con la información suministrada del equipo Cisco 4507R+E y una verificación rigurosa en sitio, se mapean las conexiones físicas y lógicas de la red, dichas conexiones se migraron a los Switches de Fortinet.

Actividad 3.1. Se realizó reconocimiento de Topología Lógica, creación de mapa de Red, Vlans y Segmentación de Red.

Actividad 3.2. Se realizó la migración de Switch Core Cisco 4507R+E a los equipos FortiSwitch Core 148F PoE.

Actividad 3.3. Se llevó a cabo la configuración en el firewall FortiGate 600E y en los FortiSwitch 148F, para realizar varias pruebas de conexión y verificación de red.

Actividad 3.4. Se realizó la implementación de los servicios, puesta a punto y estabilización de Red Capa 3.

Actividad 3.5. En cada punto de Acceso se cambiaron los Switches Cisco catalyst 2960X por los FortiSwitch 148F PoE, adecuando cada acceso y proporcionando una topología de red más estable.

Fase 4: Despliegue e Integración (FortiAPs: CAMBIOS DE EQUIPOS CONECTIVIDAD WIRELESS)

En esta fase se realizó el reconocimiento de la topología de red física anterior y se procedió a la instalación de los equipos de conectividad wireless FortiAp, además se realizaron las pruebas de los componentes desarrollados de acuerdo con los lineamientos establecidos.

Actividad 4.1. Se realizaron las adecuaciones e instalaciones físicas para los equipos.

Actividad 4.2. Se evaluaron diferentes estudios y análisis en sitio de los FortiAp para su configuración y adaptación en los diferentes lugares físicos dentro de la empresa.

Actividad 4.3. Se llevó a cabo un control de implementación de los FortiAp, en el cual se verificaban los mapas de calor en sitio, permitiendo generar un ambiente de pruebas controlado.

Actividad 4.4. Se realizó la integración security fabric. En esta etapa se implementó una integración de todos los equipos utilizados en la red, tanto física como lógica, esta función proporcionó respuestas automáticas que permitían remediar las amenazas detectadas en cualquier lugar de la red extendida.

Resultados y análisis

La implementación de la estructura de red está compuesta por la integración de diferentes herramientas que permiten realizar el correcto despliegue y desarrollo para la seguridad integral de red del cliente, está integración se realiza inicialmente por los switches SD-WAN, a los cuales se conectan los Firewall FortiGate, estos son la puerta de ingreso hacia toda la red interna; Conectados a los firewall se encuentran los switches Core FortiGate, a estos se conectan los switches de acceso para la distribución tanto física como lógica de la infraestructura de red, los routers wifi o Wireless Access Points van conectados a los switches de acceso.

Para dar desarrollo a esta implementación, inicialmente se evaluó la infraestructura física y lógica anterior, con el fin de determinar los principales cambios y despliegues a implementar, para esto se realizaron visitas a las instalaciones del cliente, para verificación de la infraestructura actual y revisión de conexiones en equipos para conocer su configuración y contenido, teniendo en cuenta toda la información recolectada, posteriormente se realizó el diseño físico y lógico de la infraestructura de red, con sus respectivas observaciones y recomendaciones de mejora con el fin de brindar al cliente una solución integral para su red.

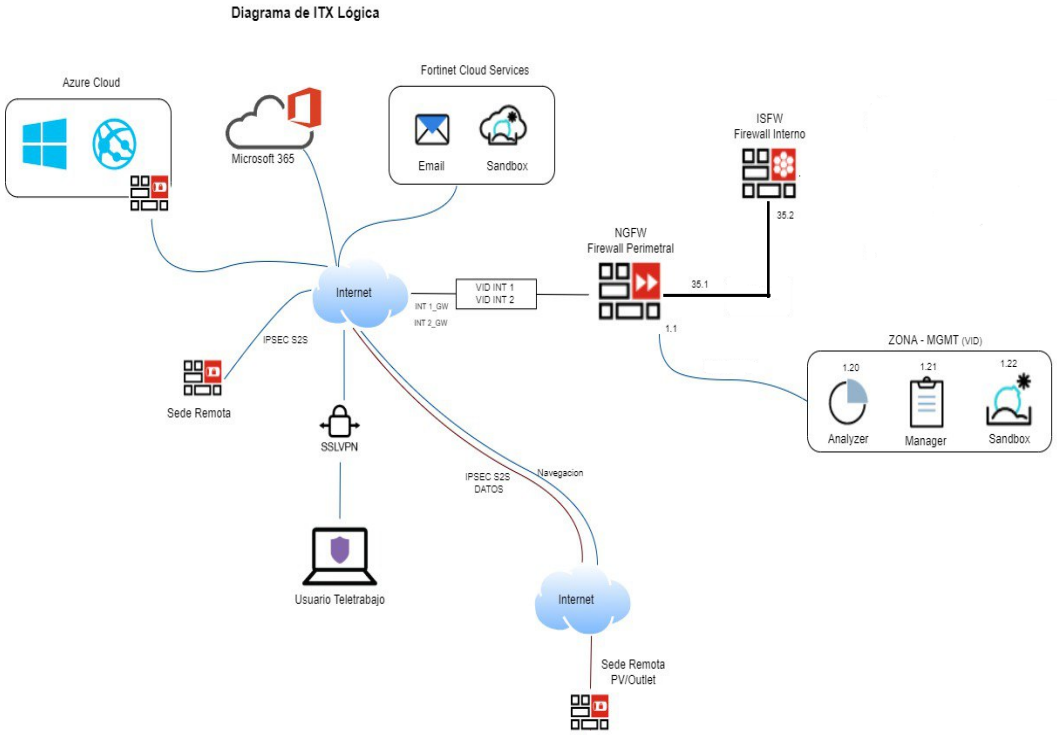

Figura 2. *Topología lógica de red.*

En la figura 2 se evidencia el diagrama lógico diseñado, el cual muestra las herramientas que se van a utilizar para la red del cliente, estas herramientas se sincronizan entre ellas para alertar y evitar cualquier amenaza en la red. El sistema principal es el Firewall Fortigate, el cual analiza todo el tráfico entrante y saliente de la red, también tenemos otros softwares como el Fortimail el cual protege los correos electrónicos de amenazas existentes, por otra parte, están los servicios en la nube, para estos tenemos Firewall que se integran con estas herramientas y están sincronizado al Fortigate principal. Otro punto importante son las conexiones remotas de los usuarios y sedes externas, para esto se crean unas VPNs, sincronizando los equipos al Firewall principal y protegiendo todo el tráfico de datos de los usuarios.

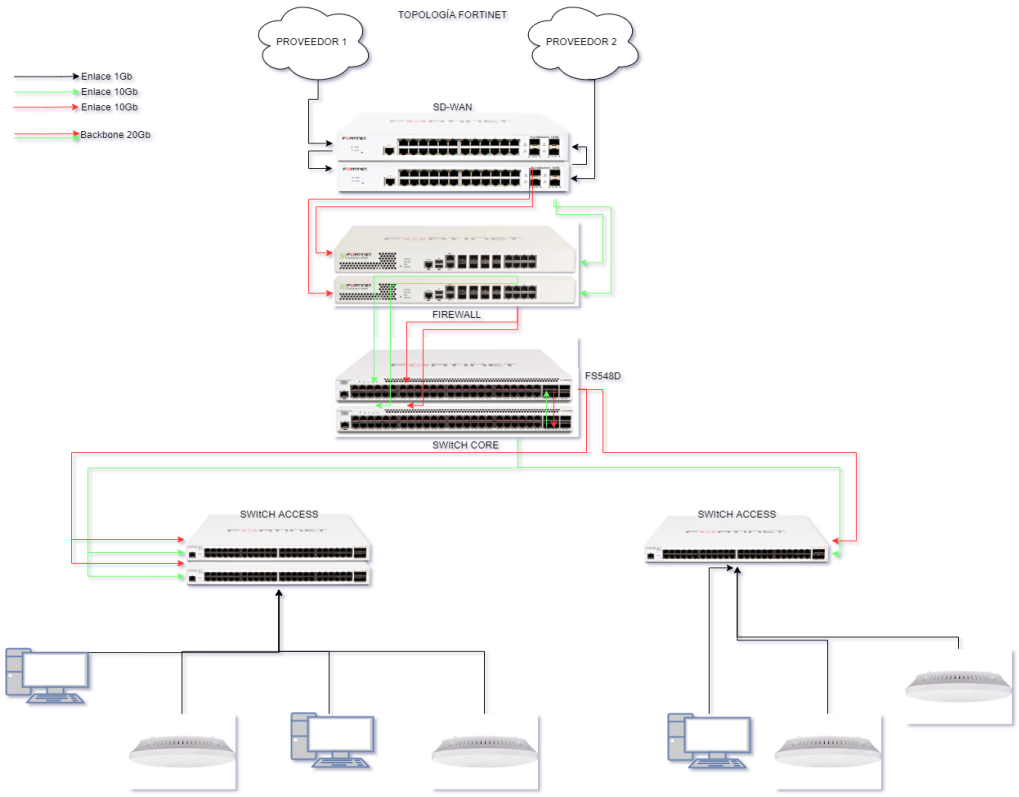

Figura 3. *Topología física de red.*

En la figura 3 se evidencia el diagrama físico diseñado, el cual detalla la estructura de las conexiones de la red y la velocidad de conexión entre equipos.

Respecto a la topología de red física es importante explicar con más detalle el desarrollo de cada una de las conexiones físicas, ya que permite entender algunas configuraciones internas realizadas a los equipos para su funcionamiento y sincronización con las demás herramientas.

SD-WAN:

Una solución SD-WAN de Fortinet permite a los usuarios de la red conectarse a cualquier aplicación de la nube, además determina de forma inteligente qué ruta satisface mejor los requerimientos de una aplicación específica, para enrutar el tráfico por la ruta ideal de la WAN y mejorar su rendimiento. La SD-WAN brinda un mayor control y mejor administración de los servicios de red, lo cual proporciona un mejor rendimiento en la capa de aplicación de las políticas de servicios, garantizando una óptima productividad de esta.

Dentro de las ventajas de la implementación del SD-WAN tenemos, la disminución de los costos de circuitos mediante el uso de banda ancha (DIA, LTE), el aumento en la agilidad de la red al simplificar el control de toda la WAN, la automatización de operaciones mientras las plantillas simplifican el flujo de trabajo de TI, y la centralización de toda la red WAN para una administración, implementación y control de cambios simplificados.

A continuación, se muestra la instalación de los switches SD-WAN en el centro de datos

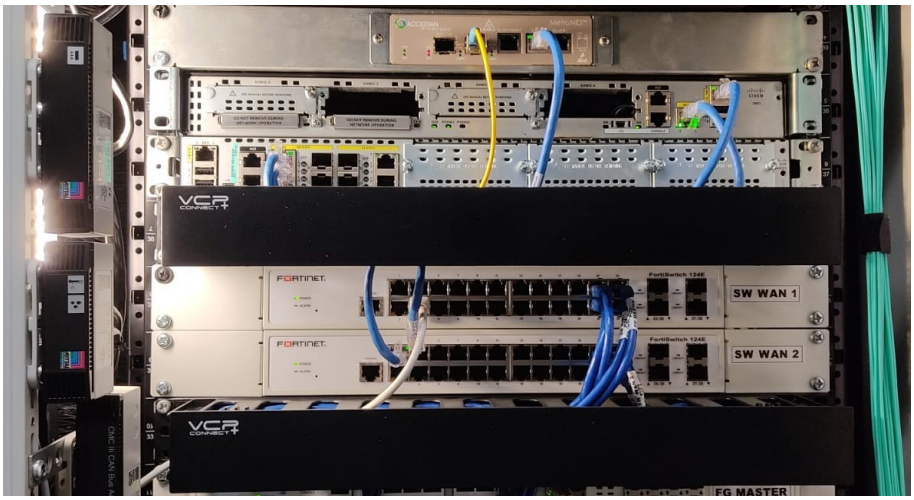

Figura 4. *SD-WAN Conexión física.*

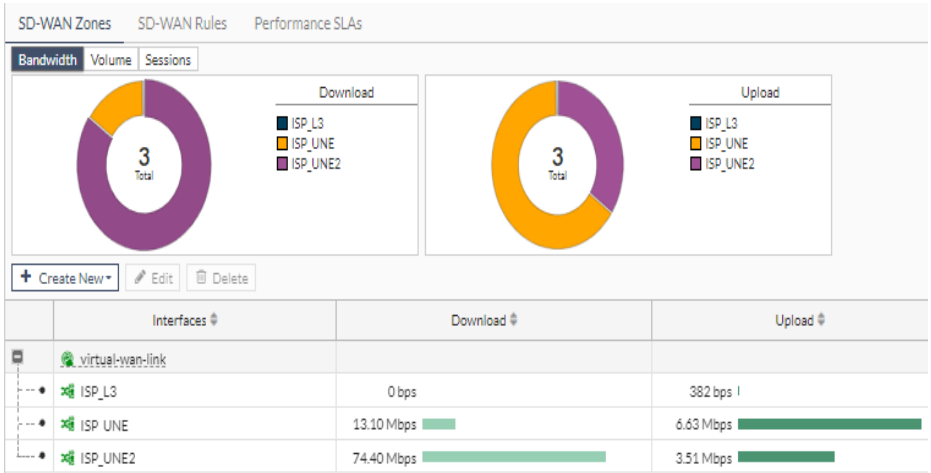

Figura 5. *SD-WAN Configuración.*

FortiGate Firewall:

El principal objetivo de los firewall es brindar protección a la red, prevenir ataques, intrusiones y amenazas que pongan en riesgo la información de las organizaciones, lo que lo vuelve una herramienta necesaria para la protección de datos en la actualidad, para el desarrollo de la implementación de la infraestructura de red en la empresa cliente, los firewall son una de las herramientas más importantes, ya que nos permiten garantizar la seguridad de la red posterior al proceso de implementación y despliegue, con esto el cliente tendrá sus redes seguras de amenazas externas e internas.

Dentro de los servicios de firewall de FortiGate encontramos:

- **FortiGuard Antivirus:** Es una solución diseñada específicamente para proteger las redes de la empresa y los dispositivos. FortiGuard Antivirus aprovecha las tecnologías de seguridad proactivas y las actualizaciones permanentes para garantizar que las amenazas avanzadas se detecten y pongan en cuarentena de inmediato.
- **FortiGuard IPS:** los NGFW de FortiGate brindan a las organizaciones capacidades de protección contra intrusiones a través del servicio FortiGuard IPS. Capaz de detectar ataques de día cero, ransomware, malware avanzado y otras amenazas maliciosas, permitiendo que los equipos de seguridad detecten y bloqueen rápidamente las intrusiones en la red.
- **Control de aplicaciones de FortiGuard:** permite a las empresas controlar fácilmente el uso de aplicaciones y cumplir con los requisitos de cumplimiento, al mismo tiempo que mejora su postura de seguridad general, también brinda a los usuarios visibilidad en tiempo real de las aplicaciones que se ejecutan en la red, así como las tendencias de uso a lo largo del tiempo.
- **Filtrado web de FortiGuard:** protege la información de la empresa, evitando que los empleados de esta accedan a contenido web malicioso o sitios web sospechosos que podrían poner en riesgo la red de la empresa.

A continuación, se observa la conexión física implementada del Fortigate 600E y la configuración establecida de los firewalls en la empresa cliente.

Figura 6. *FIrewall FortiGate Conexión física.*

Name	So...	Destinat...	Schedule	Service	Action	N...	Security Profiles	Log	Bytes
LAN (port1) → virtual-wan-link 15									
Win Update	Tie...	Microso... Microso... Microso... Microso...	always	Internet ...	ACCEPT	...	WEB default SSL SSL Inspection H...	All	0 B
Sin Internet x PC	PC...	all	always	ALL	DENY			All	0 B
wolkvox	all	IP_Wol...	always	ALL	ACCEPT	...	SSL no-inspection	All	11.80 GB
TeamsRoomYanetL	Pol... TC...	all	always	ALL	ACCEPT	...	AV default SSL certificate-inspec...	All	1.33 GB
Office365-ADco...	co... co... co... ma...	all	always	ALL	ACCEPT	...	AV default SSL certificate-inspec...	All	457.81 MB
SinRestriccion	IBM Se... Ja... An...	all	always	ALL	ACCEPT	...	AV default WEB W_Sin_Restriccion SSL SSL Inspection H...	All	153.12 GB

Figura 7. *Políticas de seguridad Firewall FortiGate.*

Switches de Acceso:

Los switches de acceso son una extensión del firewall Fortigate que permiten identificar que usuario o dispositivo se conectan a la red, además son configurados de tal forma que la red quede segmentada con el propósito de simplificar la implementación y el aprovisionamiento de los servicios. Es importante destacar que mediante la integración de los Fortiswitch y el Fortigate se puede trabajar a una velocidad de red mayor y más estable, además se pueden desarrollar políticas de seguridad más específicas, ya que el funcionamiento de manera integrada es más eficiente.

A continuación, se puede observar el proceso de instalación y configuración de los Fortiswitch en la empresa cliente

Figura 8. *FortiSwitch Conexión física.*

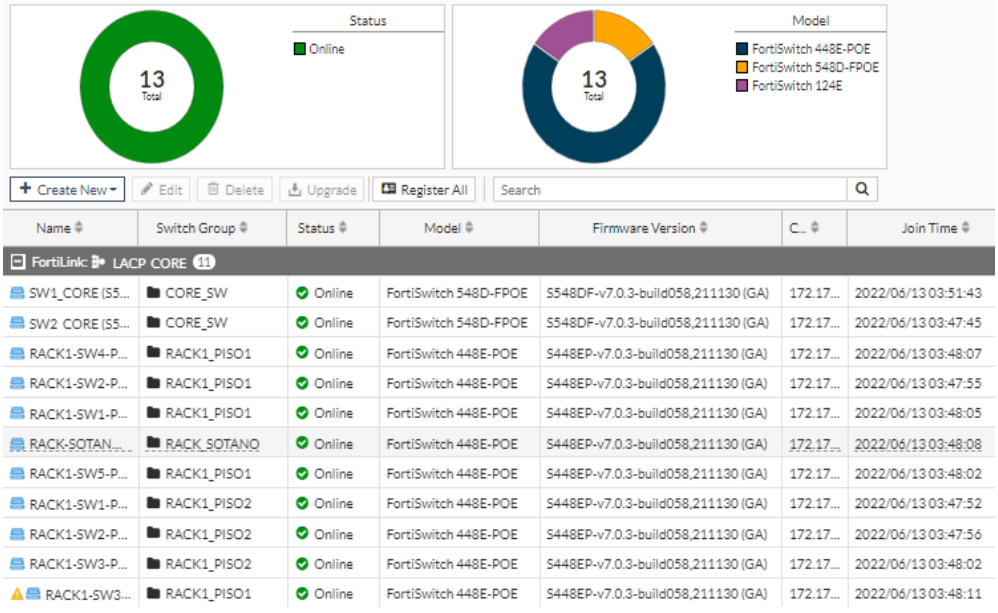

Figura 9. *FortiSwitch Configuración.*

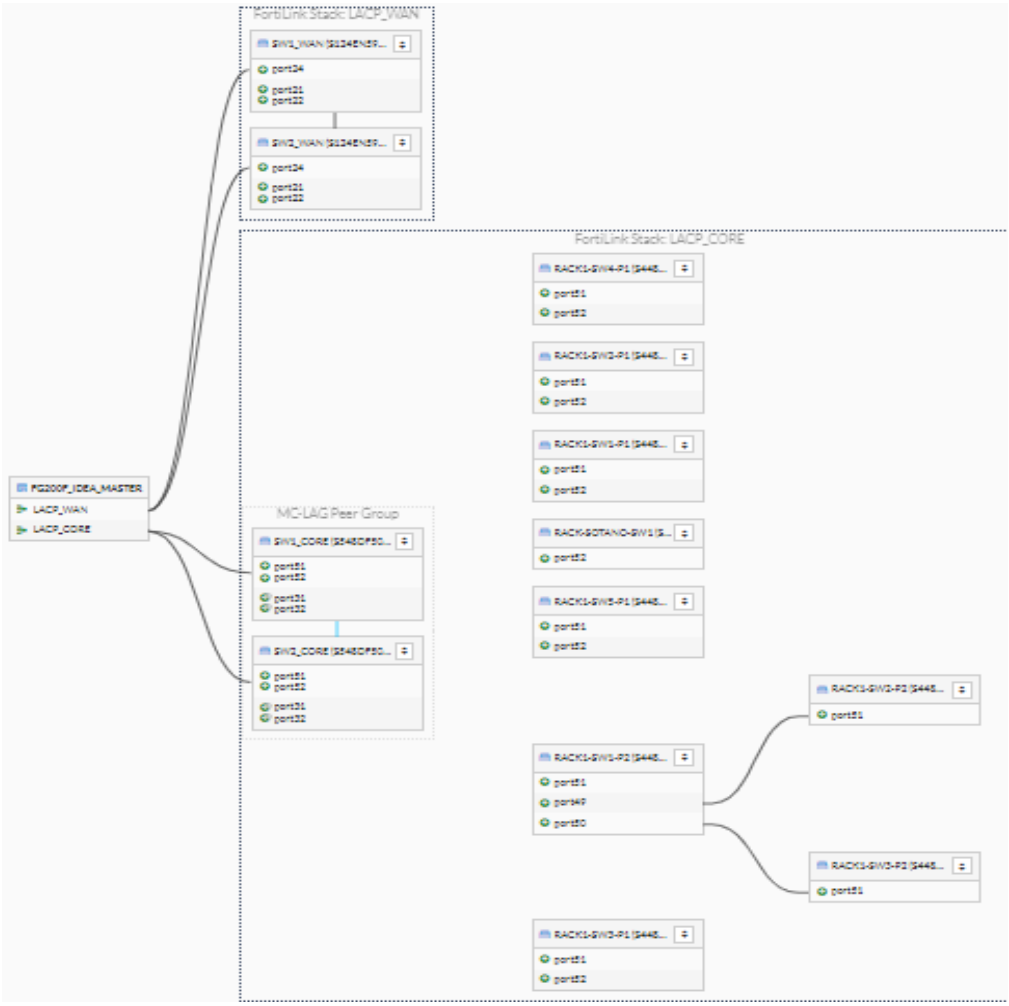

Figura 10. *FortiSwitch Conexión lógica.*

Wireless Access Points (Puntos de acceso inalámbrico):

Los wireless access point brindan acceso a la red de forma inalámbrica, permitiendo administrar el acceso a los mismos para evitar posibles amenazas de seguridad, actualmente un gran número de usuarios cuentan con dispositivos tecnológicos que se integran en el ámbito empresarial, por lo que se hace importante prestar atención a estas conexiones para mitigar el riesgo de amenazas desde dispositivos que no se tienen controlados. Es importante aclarar que estos dispositivos se integran con el Fortigate, permitiendo una extensión de las políticas establecidas y el control de los usuarios que acceden a estos puntos de red.

En la siguiente imagen se muestra un access point, su configuración y mapa de calor y ubicación física.

Figura 11. *FortiAps Conexión física.*

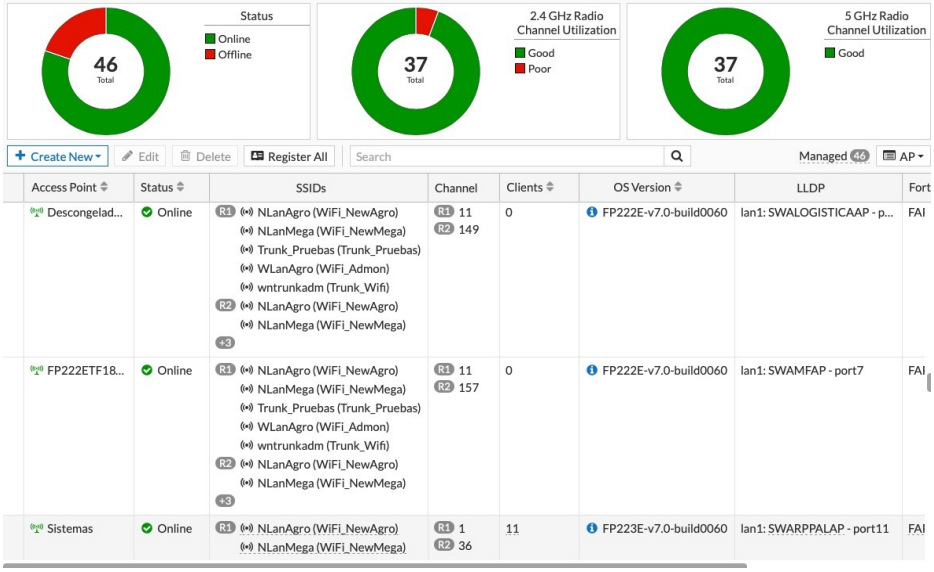

Figura 12. *FortiAps Configuración.*

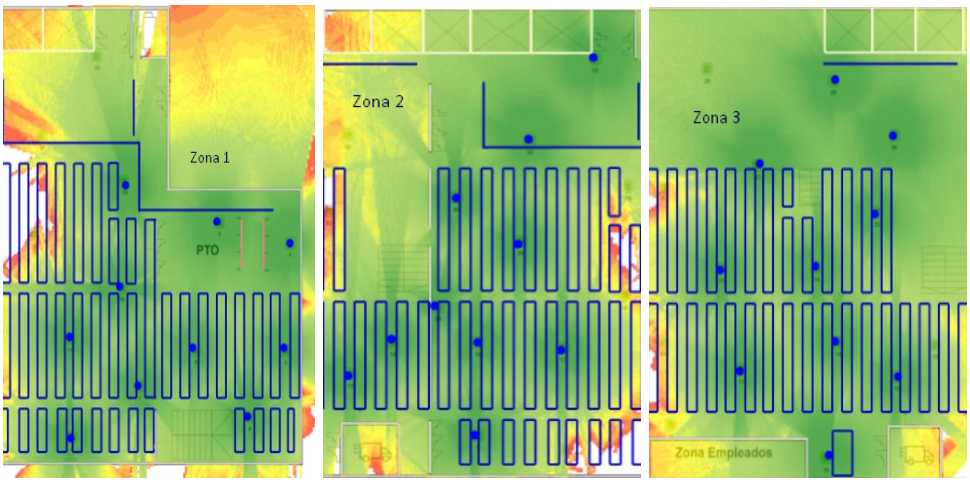

Figura 13. *Mapa de calor FortiAps* y *ubicación física.*

Conclusiones

De acuerdo a lo abordado en este documento, se puede concluir que, el diseño e implementación de un sistema de seguridad integral de red, requiere herramientas de hardware y software, que cuenten con características como: modernidad, eligiendo las versiones más vigentes y estables de cada una; compatibilidad, que permita la adaptación a la infraestructura de red de la empresa y que pueda convivir con las diferentes versiones de sistemas operativos, reduciendo costos de licencias y soporte permanente; seguridad, adquiriendo herramientas que brinden respaldo y garanticen la completa integración de red de forma segura.

En el despliegue de la solución de seguridad integral de red para la empresa cliente de Core IP SAS, se desarrolló toda una infraestructura que tuvo como principio la seguridad, la cual se basó en la utilización de los equipos adquiridos de la empresa Fortinet, los cuales proporcionan tranquilidad gracias a sus estándares de seguridad y su fácil administración desde el área de TI.

En el desarrollo de la implementación se realizaron algunas modificaciones al diseño inicial, ya que, aunque hubo un proceso riguroso para el diseño y despliegue, fue necesario ejecutar modificaciones de acuerdo con las necesidades que surgieron en el proceso de implementación de los equipos y requerimientos específicos del cliente.

En mi participación en el proyecto, al interior de la Empresa Core IP SAS trabajé en el área de desarrollo y despliegue de infraestructura, diseñando y programando los componentes que hacen parte de la correcta implementación del proyecto, aplicando los conocimientos adquiridos en mi formación académica. De manera complementaria también se realizaron varios cursos integrales para el crecimiento personal y profesional.

Para establecer una correcta administración de los recursos humanos, la empresa Core IP SAS tiene un diseño de jerarquía de cargos con sus respectivos roles y responsabilidades,

con el fin de garantizar un óptimo desempeño en el cumplimiento de los objetivos y el desarrollo de las funciones, permitiendo un flujo apropiado de todos los procesos. A través de determinados niveles jerárquicos, que se encuentran interrelacionados entre sí, estableciendo canales de comunicación, líneas de autoridad, supervisión y auditoría.

Referencias Bibliográficas

Diseño y simulación de una infraestructura de red segura. (2017, April 19). ddd-UAB. Obtenido de: https://ddd.uab.cat/record/173864.

Fortinet. (n.d.) (2022). Wikipedia. obtenido de: https://es.wikipedia.org/wiki/Fortinet#Productos.

FORTINET. (n.d.) (2022). Fortinet Resources and Documents. Fortinet. Obtenido de: https://www.fortinet.com/resources.

Group, I., (2022). Ataques BEC, ¿sabes lo que son? Obtenido de: https://www.itdigitalsecurity.es/reportajes/2018/03/ataques-bec-sabes-lo-que-son.

Joseph Pacotaype, R. (2018, diciembre 16). Metodología integral para evaluar el rendimiento de firewalls. Obtenido de: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/38180/Pacotaype_HR.pdf?sequence=2&isAllowed=y.

LEAL MENDIVELSO, J. A. (2020, diciembre 23). Diseño técnico de la implementación de centro de respuesta a incidentes de seguridad informática cyber security de Colombia LTDA. https://repository.unad.edu.co/handle/10596/38716.

López Fierro, J., (2022). Estudio y propuesta de diseño para la arquitectura de seguridad perimetral de campus, caso de estudio data center para el Municipio del Distrito Metropolitano de Quito. Repositorio.puce.edu.ec. Obtenido de: http://repositorio.puce.edu.ec/handle/22000/12582?show=full.

Network Security Solutions for Enterprise. (n.d.). Fortinet. Obtenido de: https://www.fortinet.com/solutions/enterprise-midsize-business/network-security.

ORTIZ OSORIO, M. (2021, noviembre 27). Importancia de las buenas prácticas en ciberseguridad en el trabajo remoto de entidades públicas de Colombia en época de pandemia. Obtenida de: https://repository.unad.edu.co/handle/10596/44501.

¿Qué es una infraestructura de red? (2021, March 13). Tecnología Mix. Obtenido de: https://www.tecnologiamix.com/que-es-una-infraestructura-de-red/.

Rodríguez Limones, M. F. (2021, noviembre 10). Diseño de implementación de un sistema de seguridad gestionada con SD-WAN para una red MPLS que provee servicios de internet y datos para la universidad Politécnica Salesiana. Obtenido de: http://201.159.223.180/bitstream/3317/17647/1/T-UCSG-POS-MTEL-207.pdf.