MEJORA DE ACCESO Y SEGURIDAD: INTEGRACIÓN Y OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE RED ENTRE SEDES.

JUAN MANUEL CAICEDO CASTAÑO
82201919898

UNIVERSIDAD DE MANIZALES
FACULTAD DE CIENCIAS E INGENIERÍA
PROGRAMA DE INGENIERIA DE SISTEMAS Y TELECOMUNICACIONES
MANIZALES
2024

MEJORA DE ACCESO Y SEGURIDAD: INTEGRACIÓN Y OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE RED ENTRE SEDES.

JUAN MANUEL CAICEDO CASTAÑO

Trabajo de grado presentado como opción parcial para optar
al título de
INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES

Asesor Temático / Presidente de proyecto
Diego Fernando Gonzalez Delgado
Ingeniero Electrónico, Especialista en Redes de Datos, Master en Seguridad Informática.

UNIVERSIDAD DE MANIZALES
FACULTAD DE CIENCIAS E INGENIERÍA
PROGRAMA DE INGENIERIA DE SISTEMAS Y TELECOMUNICACIONES
MANIZALES
2024

RESUMEN

El proyecto se centra en la integración de una de las sedes en Latinoamérica de la organización, ubicada en Perú, a la infraestructura tecnológica de la Sede Principal en Colombia a través del uso de firewalls en cada sitio. La motivación principal es mejorar la gestión de la red, facilitar el acceso a los servicios digitales y fortalecer la seguridad de los datos en todas las sedes internacionales. Se identificó que el acceso a los servicios se realizaba mediante VPN, lo que generaba ciertas limitaciones y riesgos en términos de seguridad en su uso constante.

La propuesta comprende en adquirir un Canal de Internet Empresarial de Fibra Óptica en cada ubicación, seguido de la configuración de IP Fija en los firewalls mediante SD-Wan e IPSec VPN, para eliminar la dependencia de la conexión de cada usuario mediante VPN con protocolo SSL. Se llevará a cabo una configuración detallada de las políticas de seguridad y enlaces en los dispositivos de protección de todas las sedes para garantizar una integración coherente y segura con una arquitectura de tecnología centralizada y robusta para el fácil acceso a sus servicios de red.

Se espera que, mediante estas acciones, se optimice el acceso a los recursos de red y se fortalezcan las medidas de seguridad en todas las sedes. Esto facilitará una colaboración más eficiente y segura entre las ubicaciones, así como una administración y monitoreo más eficiente de los usuarios y equipos, promoviendo una mejora significativa en la gestión y seguridad de la infraestructura tecnológica.

PALABRAS CLAVES: Directorio Activo, Firewalls, IPSec, SD-Wan, Seguridad, VPN.

ABSTRACT

The project focuses on the integration of one of the Latin American offices of company, located in Peru, to the technological infrastructure of the main headquarters in Colombia through the use of firewalls at each site. The main motivation is to improve network management, facilitate access to digital services and strengthen data security in all international headquarters. It was identified that access to services was done through VPN, which generated certain limitations and risks in terms of security in its constant use.

The proposal involves acquiring a Fiber Optic Business Internet Channel at each location, followed by the configuration of Fixed IP in the firewalls through SD-Wan and IPSec VPN, to eliminate the dependency of each user's connection through VPN with SSL protocol. Detailed configuration of security policies and bindings on protection devices at all sites will be carried out to ensure consistent and secure integration with a centralized and robust technology architecture for easy access to its network services.

These actions are expected to optimize access to network resources and strengthen security measures at all sites. This will facilitate a more efficient and secure collaboration between locations, as well as a more efficient administration and monitoring of users and equipment, promoting a significant improvement in the management and security of the technological infrastructure.

KEY WORDS: Active Directory, Firewalls, IPSec, SD-Wan, Security, VPN.

Contenido

Lista de Figuras

Lista de Anexos

INTRODUCCIÓN

En el entorno empresarial actual, la integración de sucursales a nivel internacional representa un desafío constante, especialmente en lo que respecta a la gestión de redes y la seguridad de la información. En este contexto, el presente proyecto surge como respuesta a la necesidad de consolidar una infraestructura tecnológica sólida y segura entre la Sede Principal en Colombia y la nueva sede en Perú con el fin de que se puedan contar de forma centralizada con la aplicación de políticas de seguridad, controles y recursos que se encuentran en la arquitectura de red de la sede principal, fortaleciendo y optimizando la integridad de los datos en todas las sedes.

Las buenas prácticas de la industria revelan la importancia de establecer una infraestructura de red sólida y segura en entornos empresariales multinacionales. Asimismo, la práctica ha evidenciado la necesidad de implementar medidas de seguridad efectivas para proteger la información sensible, disminuir vulnerabilidades, mitigar incidentes y riesgos garantizando la continuidad operativa.

Este proyecto tiene relevancia práctica para mejorar la eficiencia y seguridad de operatividad de la organización y contribuirá al avance del campo de estudio de la seguridad informática y la gestión de redes en entornos multinacionales. Al destacar la importancia de la aplicación de políticas a los recursos (usuarios o equipos) en el Directorio Activo promoviendo el intercambio de mejores prácticas de seguridad en el ámbito empresarial.

Si bien se espera lograr una integración segura y eficiente, es posible que surjan desafíos técnicos durante la implementación. Además, la naturaleza dinámica del entorno tecnológico podría requerir ajustes continuos en las políticas de seguridad y la configuración de redes para mantener la efectividad a lo largo del tiempo.

1. ÁREA PROBLEMÁTICA

La cifra de incidencias cibernéticas denunciadas, con un promedio de 1 denuncia cada 8 minutos, en Colombia durante el 2022 creció un 20.5% con respecto al año 2021, según indica la Cámara Colombiana de Informática y Telecomunicaciones. Por otro lado, lo anterior obedece principalmente a las débiles estrategias de ciberseguridad implantadas por los responsables de estas organizaciones, ya sea por no destinar recursos económicos a herramientas de mitigación de riesgos cibernéticos o por simple desconocimiento de las amenazas que día a día crecen en el sector TI.

En un entorno empresarial globalizado e internacional, la expansión de operaciones hacia múltiples ubicaciones internacionales plantea desafíos significativos en términos de gestión de redes y seguridad de la información. La nueva sede de Perú necesita integrarse de manera segura a la arquitectura de red de la sede principal, para garantizar un acceso eficiente a los servicios y así proteger la confidencialidad de los datos.

La problemática se concentra específicamente en la necesidad de establecer una conexión segura y efectiva a la infraestructura tecnológica de forma bidireccional entre sucursales internacionales. Esta delimitación considera que la infraestructura de red actual no proporciona una integración adecuada, ya que se está estableciendo una conexión vía VPN SSL a los servicios de la compañía, lo que afecta la eficiencia operativa y aumenta el riesgo de exposición a amenazas cibernéticas en los dispositivos que no se encuentran integrados en el dominio.

¿Cómo habilitar el acceso a los servicios de red de la organización ubicada en Colombia, desde la nueva sede ubicada en Perú mediante el canal de internet?

¿Cómo realizar la configuración en los dispositivos de seguridad de red y monitorear desde Colombia los equipos conectados a la red en Perú?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollar e implementar una infraestructura de red robusta y segura, específicamente diseñada para integrar de manera efectiva la nueva sede de Perú en la arquitectura de tecnología de la sede principal en Colombia, con el fin de optimizar el acceso a los sistemas de información, servicios y fortalecer las medidas de seguridad para proteger la confidencialidad y la integridad de los datos entre sedes a nivel internacional.

2.2 OBJETIVOS ESPECÍFICOS

- Diseñar la arquitectura de red utilizando dispositivos de seguridad y monitoreo.
- Establecer el mecanismo de comunicación entre ambas sedes, para establecer conexiones seguras y controladas con la infraestructura tecnológica.
- Configurar el Canal de Internet Empresarial de Fibra Óptica adquirido en la sede de Perú en el firewall, asegurando una conectividad estable para facilitar la integración en la red corporativa de la Sede Principal en Colombia.
- Implementar políticas y controles de seguridad en los dispositivos Firewall para el monitoreo de tráfico y gestión de usuarios y equipos.
- Realizar prueba piloto de la infraestructura de red implementada para verificar su funcionalidad, estabilidad y seguridad antes de la puesta en marcha completa.

3. JUSTIFICACIÓN

Este proyecto introduce una innovadora solución para abordar los desafíos de integración de redes y seguridad en un entorno empresarial multinacional. A diferencia de las prácticas anteriores que podrían haber implicado soluciones ad hoc o dependencia de conexiones VPN, esta iniciativa se centra en la implementación de Firewalls e infraestructura de red específicamente diseñada para garantizar una integración segura y eficiente en la arquitectura tecnológica.

En primer lugar, la centralización, la gestión de vulnerabilidades y monitoreo de tráfico entrante y saliente y la navegación de usuarios y equipos permitirá un mayor control y protección de datos confidenciales, fortaleciendo la seguridad de la información. La implementación de IPSec VPN y políticas de seguridad robustas en los firewalls simplificará el control de accesos no autorizados, permisos y roles de usuarios y segmentación de red.

El proyecto optimizará el acceso a los recursos de red para los usuarios en Perú, eliminando la dependencia de VPN y facilitando la comunicación entre los equipos e infraestructura tecnológica de Colombia y Perú.

El proyecto beneficia directamente a la organización cómo sede principal y a la sede de Perú involucrada en la integración. El área de Infraestructura experimentará un alivio significativo al contar con una arquitectura de red robusta y segura que facilite la gestión de recursos y garantice la protección de los datos empresariales. Además, la empresa en su conjunto se verá favorecida con una mejora en la eficiencia operativa y una reducción en el riesgo de exposición a amenazas cibernéticas.

4. MARCO REFERENCIAL

Las redes privadas virtuales (VPN) se han convertido en una herramienta esencial para las empresas que necesitan acceder a recursos de red de forma segura a través de redes públicas como Internet. IPsec es un protocolo de seguridad de capa de red que se utiliza comúnmente para crear VPN seguras. La criptografía desempeña un papel fundamental en la seguridad de las VPN con IPsec, protegiendo la confidencialidad, integridad y autenticidad de los datos transmitidos.

Las funciones de hash se utilizan para crear un resumen único de un mensaje, conocido como valor hash o huella digital. Los valores hash se utilizan para verificar la integridad de los datos, es decir, para garantizar que los datos no hayan sido alterados durante la transmisión. Las funciones de hash comunes utilizadas en IPsec incluyen (Secure Hash Algorithm) SHA-256 y (Advanced Encryption Standard) AES-128. La configuración de este protocolo de cifrado se encuentra en el ***ANEXO B. Configuración de Firewalls.pdf***

Beneficios de las VPN con IPsec:

Las VPN con IPsec ofrecen una serie de beneficios, que incluyen:

- **Confidencialidad**: Los datos transmitidos a través de una VPN con IPsec se cifran, lo que protege la confidencialidad de la información.
- **Integridad**: Las funciones de hash se utilizan para verificar la integridad de los datos, lo que garantiza que los datos no hayan sido alterados durante la transmisión.
- **Autenticación**: Los protocolos de autenticación se utilizan para verificar la identidad de las partes que se comunican en una VPN.

En la actualidad no se evidencia información documentada pública acerca de la integración de redes de 2 sucursales a nivel internacional mediante Firewalls, SD-WAN Zones e IPSec, evidenciándose únicamente el uso que se le puede dar a estas tecnologías y posibles configuraciones a realizar.

Adicional, dentro del Marco Referencial se da contexto y explicación a detalle de los distintos elementos y tecnologías usadas, las cuales fueron esenciales para la ejecución y desarrollo del proyecto:

4.1 FORTIGATE

FortiGate es una solución de seguridad de red desarrollada por Fortinet, una empresa líder en ciberseguridad. Se trata de un dispositivo o un conjunto de dispositivos que funcionan como un firewall de próxima generación (NGFW). Y brindan una amplia gama de funcionalidades para proteger las redes contra amenazas y ataques cibernéticos. Se puede ver en la figura 1.[1]

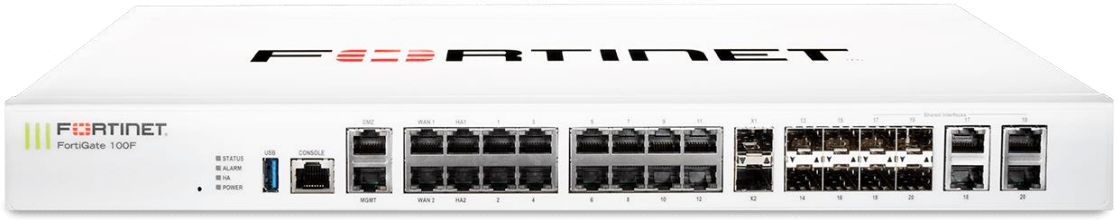

Figura 1. FortiGate 100F

4.1.1. Características funcionales del FortiGate.

- **Control de aplicaciones:** Permite crear políticas rápidamente para permitir, denegar o restringir el acceso a aplicaciones o categorías completas de aplicaciones.
- **Prevención de intrusiones:** Protege contra intrusiones en la red mediante la detección y el bloqueo de amenazas antes de que lleguen a los dispositivos de red.
- **Antivirus:** Efectivo contra virus, software espía y otras amenazas a nivel de contenido.
- **Filtrado de URL:** Bloquea el acceso a sitios web maliciosos, pirateados o inapropiados.
- **Sandboxing:** Es una solución avanzada de detección de amenazas para protegernos identificando malware previamente desconocido.
- **Inspección SSL:** Obtén visibilidad del tráfico cifrado y previene el malware.

[1] Qué es FortiGate - Bits empresa de ti mexico. (2023, July 5). Bits Empresa de Ti Mexico.

FortiGate y SD-WAN

Los equipos Fortigate vienen con capacidades SD-WAN integradas. Esto significa que los clientes obtienen funcionalidades muy avanzadas (como es el caso de SD-WAN) sin complejidad y sin costo adicional. FortiGate SD-WAN es rico en características e incluye todas las funciones típicas de SD-WAN, por mencionar algunos ejemplos:

- Application Steering.
- WAN Path Control.
- Aprovisionamiento Zero Touch.

Para las organizaciones que están migrando a aplicaciones en la nube, FortiGate SD-WAN proporciona acceso directo a Internet para reducir la latencia y aumentar el rendimiento de las aplicaciones. Para que esto sea posible, Fortinet proporciona visibilidad en más de 3000 aplicaciones. Luego, se puede priorizar el tráfico crítico para el negocio proporcionando un alto rendimiento de las aplicaciones.

Por último, es importante mencionar que FortiGate ofrece el mejor rendimiento de VPN IPSEC de la industria, asegurando el rendimiento de las aplicaciones lo cual es un requisito fundamental para SD-WAN.[2]

4.2 ROUTER.

Un router es un dispositivo que proporciona Wi-Fi y que generalmente está conectado a un módem. Envía información desde Internet a los dispositivos personales, como computadoras, teléfonos o tablets. Los dispositivos conectados a Internet de tu casa conforman la red de área local (LAN). Después de que el módem obtiene información de Internet, el router distribuye estos datos a los dispositivos personales. Se puede ver en la Figura 2.[3]

[2] Garza, A. (2022, February 15). ¿Qué es y cómo es que funciona un Firewall FortiGate? Quanti.
[3] ¿Qué es un router? - Ayuda de Google Nest. (2019). Google.com.

Figura 2. Router Inalámbrico Smart Wi-Fi de doble banda AC1200+ Linksys

4.2.1 Características Router Inalámbrico.

El Router inalámbrico Smart Wi-Fi de doble banda AC1200+ Linksys, EA6350 lleva la velocidad inalámbrica de próxima generación a todos sus dispositivos. Provisto de USB 3.0 y cuatro (4) puertos Gigabit junto con la tecnología Inalámbrica-AC más reciente, la AC1200+ está optimizada para admitir todos los dispositivos cableados y Wi-Fi®. Valiéndose de la doble banda hasta N300 Mbps + AC867 Mbps, el tráfico de datos puede fluir de forma rápida. El router incluye las siguientes características clave:

- **Hasta 2,8 veces más rápido que la tecnología Inalámbrica-N:** Doble banda simultánea hasta N300 Mbps (2.4 GHz) + AC867 Mbps (5 GHz) para las aplicaciones multimedia intensas.
- **Puerto USB 3.0:** Los puertos USB 3.0 y Gigabit Ethernet aseguran el máximo streaming de multimedia y la rápida transferencia de fotos, vídeos, archivos de datos o la conexión de dispositivos en su red. USB 3.0 es 10 veces más rápido que USB 2.0.
- **Linksys Smart Wi-Fi:** Permite a los usuarios monitorizar y controlar una red doméstica desde cualquier lugar y en cualquier momento. También les permite a los usuarios priorizar dispositivos o sitios web, obtener el control parental para restringir el acceso a contenidos inapropiados, monitorizar la actividad de la red, ACTIVAR o

DESACTIVAR el acceso Wi-Fi y crear redes de invitados protegidas con contraseñas seleccionadas.

- **IEEE 802.11a/b/g/n**
- **Puertos Gigabit Internet y Ethernet**
- **Compatible con DLNA® v1.5**
- **Compatible con IPv6 CPE**[4]

4.3 IP PÚBLICA FIJA.

La dirección IP fija que se le asigna a un equipo nunca cambia, ya sea en Internet (IP fija pública) o en una red doméstica o empresarial (IP fija privada). Esta es asignada por el proveedor del servicio de internet y es entregada al usuario para su administración y seguridad, lo que le permite configurar servidores en Internet para servicios de correo, FTP, VPN, etc. y dirigirlo al dominio que quiera (@nombredelaempresa), evitando actualizar el Servidor.[5]

4.4 CANAL DE INTERNET FIBRA OPTICA.

Estos enlaces de comunicación de alta velocidad están formados por cables que contienen hebras de vidrio más finas que un cabello humano las cuales transmiten información -como señales de teléfono, televisión e Internet- en forma de pulsos de luz infrarroja. Gracias a su rápida capacidad de transferencia de datos, también pueden utilizarse para sistemas de inteligencia artificial (IA) para coches o drones, para gestionar la seguridad en las obras y zonas de trabajo, y para garantizar una rápida prestación de servicios sanitarios y públicos fundamentales. Figura 3.

4.4.1. Las ventajas del cable de fibra óptica son numerosas:

Potencia, alcance, velocidad, durabilidad, fiabilidad y seguridad. Estas ventajas permiten hacer la transición hacia ciudades, empresas y hogares totalmente digitalizados, creando un modo de vida más sostenible y circular. A continuación, te mostramos las **ventajas de la fibra óptica** en detalle:

[4] Introducción al Router inalámbrico Smart Wi-Fi de doble banda AC1200+ Linksys EA6350. (2019). Linksys.com.
[5] ¿Qué es una dirección IP fija? | Empresas. (2020). Tigo CO.

- Resiliencia. Los cables de fibra óptica son **resistentes a los cambios de temperatura** y a las condiciones meteorológicas adversas. Son más **ligeros, finos y robustos** que los cables de cobre, y es menos probable que se rompan o se dañen.
- También son más **seguros**, porque es muy difícil interceptar sus transmisiones. No les afectan las interferencias electromagnéticas, que pueden perturbar las señales.
- Los cables de fibra óptica **pueden transportar señales hasta 40 kilómetros** sin que se deteriore la señal, mientras que la distancia máxima que alcanzan los cables de cobre es ligeramente inferior a un kilómetro.
- Las redes de fibra óptica tienen una baja latencia. En otras palabras, son rápidas. Esta rápida transferencia de datos permite implantar **sistemas de IA** de auto-conducción para coches o drones, telemedicina, seguridad nacional o gestionar la seguridad en obras y zonas de trabajo, por citar algunos ejemplos.
- La transmisión y los juegos mejoran. La mayor capacidad de albergar datos de las redes de fibra óptica significa que no se sobrecargan tan fácilmente como las redes de cable de cobre, por lo que es más rápido descargar y transmitir tus películas favoritas. Y la estabilidad de la fibra significa que el videojuego no se interrumpirá en el momento más inoportuno.
- Viviendas inteligentes. Las redes de fibra óptica son lo suficientemente robustas como para dar servicio a tu oficina en casa, transmitir tus películas favoritas y conectarse a dispositivos del Internet de las Cosas (IoT por sus siglas en inglés) como termostatos, alarmas y electrodomésticos.[6]

[6]Red de fibra óptica: ventajas y definición | Enel X. (2024). Enel X.

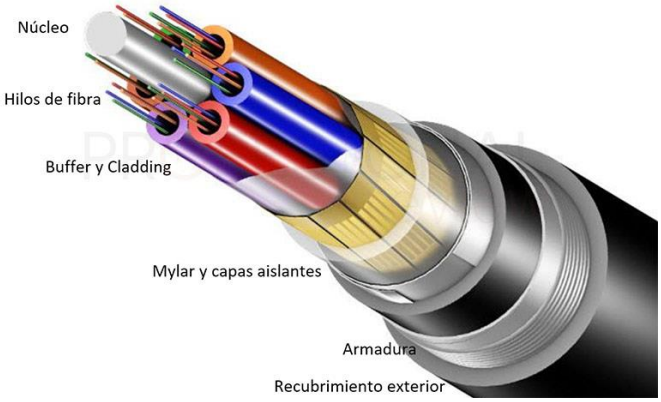

Figura 3. Fibra Óptica

4.5. ANTECENDENTES.

Según la publicación realizada por SISSA Monitoring Integral en su red social LinkedIn (2023). "La integración de redes de datos consiste en conectar diferentes sistemas y aplicaciones en una red, permitiendo que se comuniquen entre sí y compartan datos de forma más rápida y segura. En otras palabras, la integración de redes de datos se refiere al proceso de interconectar distintas redes individuales en una sola red integrada y coherente. Este proceso puede incluir la integración de redes de diferentes marcas y tecnologías, así como la unificación de redes físicas y lógicas, a fin de mejorar la eficiencia y la flexibilidad de las redes de datos para la reducción de los costos y el mejoramiento de los servicios que se ofrecen".[7]

Según la documentación publicada por Fortinet (2023) "Para soportar SD-WAN con IPsec VPN, la configuración del túnel IPsec VPN de todos los túneles IPsec que son miembros de la misma zona SD-WAN en el mismo VDOM (Virtual Domain) debe enviar tráfico al mismo FPM (Flexible Packket Matching). Esto significa que la configuración de ipsec-tunnel-slot del túnel IPsec debe incluir un FPM específico".[8]

De acuerdo con el artículo escrito por Núria Emilio (2023) "La optimización del acceso a recursos de red y la implementación de políticas de seguridad en dispositivos FortiGate son pasos

[7]SISSA Monitoring Integral. (2023, 25 de abril). Integración de redes de datos: solución esencial para la eficiencia y rentabilidad de tu organización, LinkedIn
[8] SD-WAN with multiple IPsec VPN tunnels | FortiGate-7000E Administration Guide. (2024). Fortinet.com.

cruciales para lograr una integración segura y eficiente en el Directorio Activo. Esto contribuye a una gestión más efectiva de usuarios y equipos en todas las ubicaciones".[9]

Cómo indica un blog escrito por Kelsey Kinzer (2023) "La integración de redes de datos es un factor elemental para cualquier organización dada la cantidad de datos que se generan y se procesan en las empresas y distintas organizaciones, la cual aumenta de manera acelerada. La información es uno de los activos más importantes de una organización y, por lo tanto, debe gestionarse de manera efectiva y segura. ". [10]

Según lo escrito por IBM "La configuración adecuada de un firewall es esencial para mantener a las organizaciones protegidas contra la fuga de datos y los ataques cibernéticos. Las políticas de firewall, basadas en el tipo de red (pública o privada), permiten bloquear o permitir el acceso, evitando posibles ataques de piratas informáticos o programa maligno. Es crucial que las características predeterminadas no comprometan la seguridad, ya que el 99 % de las violaciones del firewall se deben a configuraciones erróneas".[11]

Con base en la documentación proporcionada por IBM "FortiGate ofrece una SD-WAN segura rápida, escalable y flexible para empresas cloud, sensibles a la seguridad y globales. La solución Fortinet Secure SDWAN (red de área amplia definida por software) permite a las empresas transformar y proteger todos los bordes de WAN".[12]

Gracias a la publicación realizada por TrendMicro Las medidas de seguridad de red son los controles de seguridad que usted añade a sus redes para proteger la confidencialidad, la integridad y la disponibilidad. Estos controles continúan evolucionando, pero hay muchos conocimientos básicos que son fácilmente accesibles. Cuesta cierto esfuerzo mantener a los atacantes fuera de su red. Los firewalls, proxies y gateways trabajan con ese objetivo. Es peligroso dar por hecho que

[9] Emilio, N. (2020, November 10). La integración de datos: la solución para cualquier empresa moderna. Bismart.com; Bismart.
[10] Kinzer, K. (2023, April 10). Una guía para la autenticación de Active Directory - JumpCloud. JumpCloud Spanish.
[11] ¿Qué es la seguridad de red? | IBM. (2024). Ibm.com.
[12] IBM Documentation. (2023, March 31). Ibm.com

esos dispositivos son suficientes para mantener a los atacantes completamente fuera de su red. Los hackers siempre encuentran la forma".[13]

Según lo escrito en el blog de Internexa por parte de Zapata Giraldo, CM "La tecnología de fibra óptica utiliza finas hebras de vidrio o plástico para transmitir datos a la velocidad de la luz, lo que habilita navegar por internet a velocidades ultrarrápidas y con mayor capacidad de ancho de banda que solo es posible alcanzarlas usando esta tecnología o medio de transmisión. Esto significa que su empresa puede disfrutar de videoconferencias sin interrupciones, transferencias de archivos más rápidas y colaboración en línea ininterrumpida". [14]

Según la documentación por parte de Microsoft Learn (2023) "La seguridad se integra en Active Directory mediante la autenticación de inicio de sesión y el control de acceso a los objetos del directorio. Con un único inicio de sesión de red, los administradores pueden administrar los datos del directorio y la organización a través de su red, y los usuarios de red autorizados pueden tener acceso a los recursos en cualquier parte de la red. La administración basada en directiva facilita la administración de incluso las redes más complejas".[15]

Según lo que indica Jiménez Artiles, Onil[2] **"**Los sistemas SD-WAN contribuyen a optimizar la infraestructura conectiva. Y de esta forma mejorar los servicios que brindan las empresas. Lo que se traduce en mejor experiencia de uso por parte de los empleados en las empresas que interactúan con sistemas que necesitan conexiones a Internet por su parte los consumidores reciben servicios con mayor calidad".[16]

De acuerdo con lo escrito por Calderón Rodríguez, C. "Las AES Soporta tallas de clave y bloque de 128, 192 6 256 bits. El número de fases depende de los tamaños de bloque y clave. Las operaciones básicas que usa son: sustitución de byte –permutación no lineal-, desplazamiento de

[13] ¿Cuáles son las medidas de la seguridad de red? (2024). Trend Micro.
[14] Mario, C. (2023, August 24). Internet de fibra óptica para tu empresa. Lo que debes saber. Internexa.com; INTERNEXA S.A
[15] iainfoulds. (2023, March 9). Introducción a Active Directory Domain Services. Microsoft.com.
[16] Jiménez Artiles, Onil (2020). Optimización de enlaces WAN utilizando software Defined Networks. [Trabajo de grado, Ingeniería en Tecnologías de la Información y la Comunicación]. Santo Domingo: Universidad Iberoamericana (UNIBE).

fila desplazamiento cíclico de bytes, mezcla de columna transformación lineal y suma de clave en cada ronda una clave es derivada de la principal por medio de la función de reparto de la clave. La longitud de esta clave coincide con la del bloque de cifrado". [17]

Se evidencia en el trabajo realizado por Condori Vásquez, G. el cual es un proyecto similar al que estoy llevando a cabo, entendiendo que "Estos últimos años se viene ya se están imponiendo las redes definidas por software SD-WAN al mercado, que permite un despliegue más rápido, ágil, menos costoso y no tan complejo ya que estos utiliza un entorno más amigable son redes que aprovechan el poder de la digitalización para simplificar su gestión y aumentar la velocidad de la ejecución de las aplicaciones.". [18]

[17] Calderón Rodríguez, C. (2001). Implementación de una VPN (Virtual Private Network) usando el estándar IPSEC. http://hdl.handle.net/10251/32198
[18] Condori Vásquez, G. (2022). Diseño e implementación De Una Red Sd-wan Para La Optimización De La Red Corporativa De Una Cadena De Electrodomésticos. https://hdl.handle.net/20.500.12867/7116

5. METODOLOGÍA

5.1 TIPO DE TRABAJO

Este proyecto comprende la integración de redes y seguridad en un entorno multinacional, desde la planificación de la arquitectura tecnológica y topología, hasta las pruebas de conectividad, controles de acceso a sistemas y recursos sin necesidad de conexión VPN.

En él se incluirán aspectos de las disciplinas de Tecnologías de la Información, Seguridad Informática y Gestión de Proyectos.

5.2 PROCEDIMIENTO

El proyecto se realizará en 3 fases, así:

5.2.1 Fase 1. Planeación del diseño para la integración y optimización de la infraestructura de red entre sedes.

Esta fase tiene como objetivo definir los protocolos que se usarán para la configuración, como se autenticarán los usuarios y que cifrado se usara en IPSec. Figura 5.

Actividad 1. Definir de los protocolos de cifrado de datos. Cómo implementación de buenas prácticas, el cifrado de la información del IPSec VPN Tunnel se dará mediante los protocolos **SHA256** generando hashes únicos cómo seguridad criptográfica y **AES-128** para el cifrado y descifrado de los datos en tráfico.

Actividad 2. Diseñar la arquitectura de comunicación de red entre sedes. Se define y diseña la siguiente topología de red, la cual es un diseño que permite la comunicación entre ambas infraestructuras tecnológicas y el acceso de los distintos servicios mediante la SD-Zones e IPSec VPN.

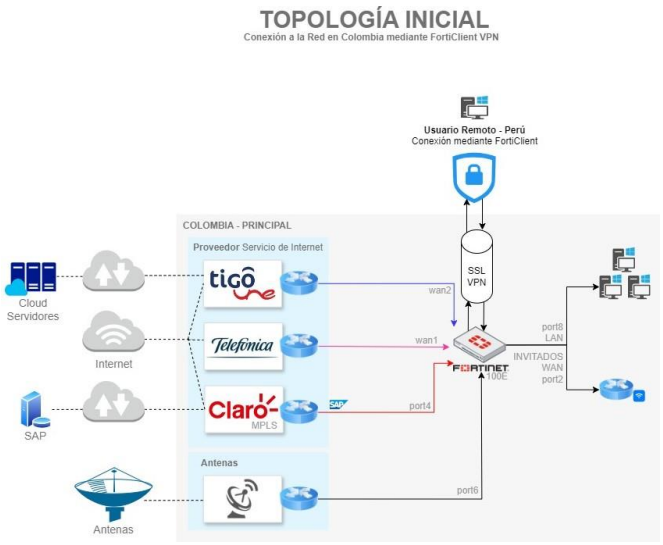

Figura 5. Anterior Topología de Red – FortiClient VPN SSL.

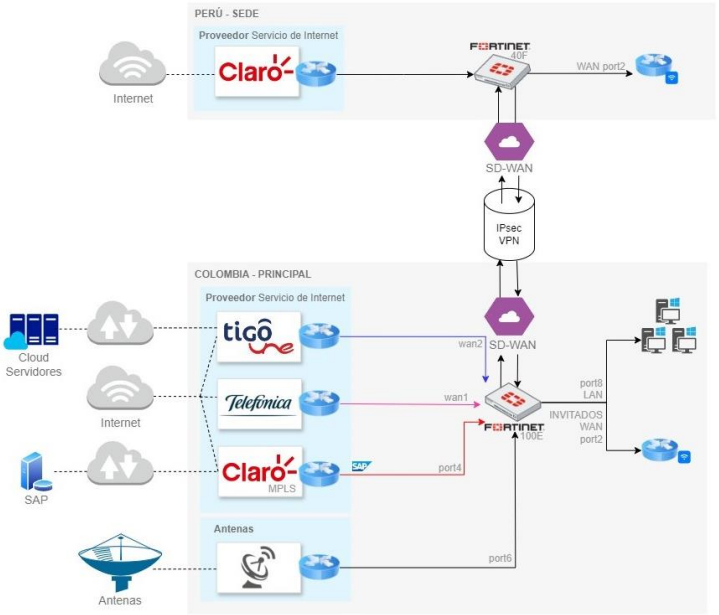

Figura 6. Arquitectura de Red – Sedes Colombia y Perú.

5.2.2 Fase 2. Garantizar la conectividad entre sucursales.

Esta fase implica la configuración del Canal de Internet Empresarial - Fibra Óptica y su correcto despliegue cómo segmento de red, monitoreando su latencia y velocidad de carga y descarga para no saturar el tráfico. Comprendiendo así las actividades:

- **Actividad 1. Instalación y configuración.** Verificar el despliegue de la Fibra Óptica en la sede de Perú realizando pruebas de conectividad, medir la precisión en la velocidad de subida y descarga de datos, latencia (ping) de la conexión. Posterior se validan los datos de IP Pública, Mascara de red, Puerta de Enlace y DNS del servicio. Figura 6.

Figura 7. Conexión entre el Firewall y Canal de Internet.

5.2.3. Fase 3. Configurar el segmento de red y demás dispositivos.

La configuración del FortiGate, un dispositivo de seguridad de red es crucial para garantizar la protección de una red empresarial y el acceso seguro a los servicios de red configurados en nuestros servidores en Colombia. Así se pro

- **Actividad 1. Acceder al Firewall.** Realizar la conexión del Firewall a través de un navegador web e iniciar con la configuración de los parámetros cómo definición del segmento de red, dirección IP, mascara de subred y la contraseña de administrador de acceso al dispositivo.

- **Actividad 2. Configurar el Firewall y la interfaz de red.** Configurar los parámetros del Canal de Internet y su interfaz de red con la información brindada por el proveedor cómo la Dirección IP Pública Fija, Máscara de subred, Puerta de Enlace y definir los puertos de conectividad LAN, WAN, DMZ.

- **Actividad 3. Implementar políticas de seguridad y controles en el firewall.** Establecer políticas de Firewall para controlar el tráfico de red entrante y saliente, configurar la conectividad entre los FortiGates de las sedes mediante SD WAN Zones permitiendo agrupar los segmentos lógicos y aplicar políticas específicas a los distintos grupos configurados.

- **Actividad 4. Verificar conectividad del Firewall.** Validar que respondan los servicios de red desde Perú sin necesidad de estar conectados a la VPN, esta validación se debe realizar directamente en la red wifi del Canal de Internet Fibra Óptica contratado. Adicional, asegurar la conexión al servidor de dominio configurado con el AD y funcional en la red.

También se valida mediante PING la visibilidad de los servicios de red que están en el otro segmento de Colombia desde Perú, verificando la latencia.

5.2.4. Fase 4. Realizar prueba piloto con la integración de un equipo al dominio.

Integrar equipos de computación a un dominio es un proceso común en entornos empresariales, donde se utiliza un servidor de dominio para centralizar la administración de usuarios, políticas de seguridad y recursos compartidos en una red.

- **Actividad 1. Validar versión del Sistema Operativo.** Realizar la verificación de la versión del Sistema Operativo Windows, ya que para integrar los equipos al Dominio debe estar legalizado en su versión PRO.

En caso de que se identifique que el Sistema Operativo esté en la versión Home, se debe adquirir la licencia para la legalización de la versión PRO para actualizarlo.

- **Actividad 2. Configuración de Dominio.** Integrar al Dominio el equipo de cómputo e iniciar sesión con el usuario correspondiente creado en el Directorio Activo de la Sede Principal en Colombia. Para hacer este proceso se debe estar conectado a la red wifi la cual tiene acceso a los servicios.

- **Actividad 3. Instalación de Software Corporativo.** Instalar los aplicativos y sistemas de información corporativos que solo se accede dentro de la red.

- **Actividad 4. Verificar aplicación de políticas.** Una vez integrado al Dominio, el dispositivo deberá contar con las políticas del Directorio Activo, cómo, por ejemplo, cambio de contraseña periódica, fondo de pantalla corporativo, bloqueo de pantalla por inactividad, ente otras.

El desarrollo de las actividades de la Fase 2, Fase 3 y Fase 4 se encuentran en el ***ANEXO B. Configuración de Firewalls.***

6. RESULTADOS

La implementación exitosa de una infraestructura de red segura y eficiente, basada en Firewalls y el despliegue de una configuración detallada de políticas de seguridad, evidencia que la integración efectiva de la Sede de Perú en la infraestructura tecnológica de la Sede Principal de Colombia permite asegurar un acceso óptimo a los servicios, sistemas de información, establecer conexión con el servidor de dominio y proteger los datos empresariales en un entorno multinacional.

Al término del proyecto, obtiene una serie de resultados concretos que demuestren la efectividad y el éxito de la integración y optimización de la infraestructura de red entre sedes. Entre estos resultados finales se incluyen:

- Establecimiento de una conexión segura y eficiente entre las sedes de Colombia y Perú, garantizando la confidencialidad e integridad de los datos transmitidos mediante el uso de protocolos de cifrado robustos como SHA256 y AES-128.

- Despliegue exitoso del Canal de Internet Empresarial - Fibra Óptica en la sede de Perú, con una conectividad confiable y velocidades de carga y descarga óptimas, verificadas mediante pruebas de latencia y velocidad.

- Configuración efectiva del Firewall, asegurando la protección de la red empresarial contra amenazas externas, la aplicación de políticas de seguridad coherentes con los estándares del sector y el monitoreo y control de tráfico de red.

- Integración exitosa de equipos de cómputo al dominio, permitiendo el acceso seguro a los recursos corporativos y la aplicación de GPO configuradas en el Directorio Activo, junto a la administración de usuarios y dispositivos conectados.

- Validación de la operatividad de los servicios de red desde Perú sin necesidad de estar conectados a la VPN con protocolo SSL.

Estos resultados finales representan la culminación de un proyecto que busca mejorar la conectividad, seguridad y eficiencia de la infraestructura de red empresarial, brindando un entorno tecnológico más robusto y preparado para satisfacer las necesidades operativas de la organización.

8. CONCLUSIONES

El presente proyecto ha permitido abordar de manera efectiva los desafíos de integración de redes y seguridad en un entorno multinacional. A través de la implementación de una infraestructura de red sólida y segura, basada en Firewalls FortiGate y una cuidadosa configuración de políticas de seguridad, se ha logrado garantizar la integración eficiente de una nueva sede ubicada en Perú en el Directorio Activo de la organización.

Durante la ejecución del proyecto, se ha enfatizado la importancia de una planificación minuciosa desde el área de TI. Además, se ha destacado la necesidad de brindar capacitación adecuada al personal para garantizar el manejo adecuado de la nueva infraestructura en la nueva sede.

La implementación de esta solución ha derivado en beneficios concretos, como una optimización del acceso a servicios y sistemas de información, la no dependencia de una VPN para el acceso a estos recursos, mejora en la eficiencia operativa y una reducción del riesgo de ciberataques. Asimismo, se ha fortalecido la comunicación y cooperación entre las sedes de Colombia y Perú, fomentando un entorno laboral más cohesionado y seguro a nivel de red.

En conclusión, el proyecto ha logrado cumplir con sus objetivos de manera satisfactoria, ofreciendo una solución efectiva a los desafíos identificados en términos de integración de redes y seguridad. Estos resultados subrayan la importancia de invertir en infraestructuras tecnológicas sólidas y seguras para garantizar el éxito empresarial en un entorno globalizado y digitalizado.

REFERENCIAS

[1] O. ADEYINKA. (2008) Analysis of problems associated with IPsec VPN Technology. University of East London, UK.

[2] A. LAGUIDI, A. HAYAR. (2012) Secure HeNB network management Based VPN IPSec. University Hassan II Casablanca, Francia.

[3] G. CHICA. (2012) Estudio y Análisis de la Viabilidad de la Implementación de Tecnología PLT (Power Line Telecommunications) en Colombia, en el Ámbito de la Transmisión de Datos Sobre Redes de Baja Tensión, Departamento de ingeniería de Sistemas e Industrial, Universidad Nacional de Colombia, Colombia.

[4] Seedup Growth hacking. (2023, July 5). Qué es FortiGate - Bits empresa de ti mexico. https://bits.com.mx/que-es-fortigate

[5] Garza, A. (2022, February 15). ¿Qué es y cómo es que funciona un Firewall FortiGate? Quanti. https://quanti.com.mx/articulos/conociendo-el-firewall-fortigate/

[6] ¿Qué es un router? - Ayuda de Google Nest. (2019). Google.com. https://support.google.com/googlenest/answer/6274087?hl=es-419#:~:text=Un%20router

[7] Introducción al Router inalámbrico Smart Wi-Fi de doble banda AC1200+ Linksys EA6350. (2019). Linksys.com. https://www.linksys.com/ve/support-article/?articleNum=141018

[8] Tigo CO. (2020) ¿Qué es una dirección IP fija?. Empresas. https://ayuda.tigo.com.co/hc/es/articles/8944709230483--Qu%C3%A9-es-una-direcci%C3

[9] Enel X. (2024). Red de fibra óptica: ventajas y definición. https://corporate.enelx.com/es/question-and-answers/advantages-of-fiber-optic

[10] SISSA Monitoring Integral. (2023, 25 de abril). Integración de redes de datos: solución esencial para la eficiencia y rentabilidad de tu organización, LinkedIn https://www.linkedin.com/pulse/integraci%C3%B3n-de-redes-datos-soluci%C3%B3n-esencial-para-la-eficiencia/

[11] FortiGate-7000E Administration Guide. (2024). SD-WAN with multiple IPsec VPN tunnels Fortinet.com. https://docs.fortinet.com/document/fortigate/7.4.2/fortigate-7000e-administration-guide/761182/sd-wan-with-multiple-ipsec-vpn-tunnels

[12] Emilio, N. (2020, November 10). La integración de datos: la solución para cualquier empresa moderna. Bismart.com; Bismart. https://blog.bismart.com/importancia-integracion-datos

[13] Kinzer, K. (2023, April 10). Una guía para la autenticación de Active Directory - JumpCloud. JumpCloud Spanish. https://jumpcloud.com/es/blog/active-directory-authentication

[14] IBM. (2024). ¿Qué es la seguridad de red? https://www.ibm.com/mx-es/topics/network-security

[15] IBM Documentation. (2023, Marzo 31). Ibm.com. https://www.ibm.com/docs/es/tncm-p/1.4.3?topic=packs-configuring-fortinet-sd-wan-technology-pack

[16] Trend Micro. (2024). ¿Cuáles son las medidas de la seguridad de red? https://www.trendmicro.com/es_es/what-is/network-security/network-security-measures.html

[17] Mario, C. (2023, Agosto 24). Internet de fibra óptica para tu empresa. Lo que debes saber. Internexa.com; INTERNEXA S.A. https://blog.internexa.com/es/internet-de-fibra-optica-internexa

[18] Microsoft Learn. (2023, Marzo 9). Introducción a Active Directory Domain Services. Microsoft.com. https://learn.microsoft.com/

[19] Jiménez Artiles, Onil (2020). Optimización de enlaces WAN utilizando software Defined Networks. [Trabajo de grado, Ingeniería en Tecnologías de la Información y la Comunicación]. Santo Domingo: Universidad Iberoamericana (UNIBE). http://repositorio.unibe.edu.do/jspui/handle/123456789/389

[20] Yupanqui C., Marcionila G., Diaz M., Mariela C. (2021) Implementación de sd-wan y túnel vpn ipsec para redundancia de comunicaciones hacia servicios internos y externos en agencia Accha de una entidad financiera. Universidad Nacional Tecnológica de Lima Sur.

[21] Calderón Rodríguez, C. (2001). Implementación de una VPN (Virtual Private Network) usando el estándar IPSEC. http://hdl.handle.net/10251/32198

ANEXOS

ANEXO A. Nueva topología de red - solución SD-WAN Zones con IPSec.
La figura "*Nueva topología de red – Solución SD-WAN Zones con IPSec.jpeg*" muestra la topología de red propuesta para el proyecto de integración de la sede en Perú con la Sede Principal en Colombia. Esta topología ha sido diseñada para garantizar una integración coherente y segura en el Directorio Activo, así como para optimizar el acceso a los recursos de red y fortalecer las medidas de seguridad en todas las sedes internacionales.
Imagen realizada por Juan Manuel Caicedo Castaño el 15 de marzo de 2024

ANEXO B. Anterior topología de red - FortiClient VPN SSL.
La figura "*Anterior topología de red - FortiClient VPN SSL.jpeg*" representa la configuración de la infraestructura de red anterior a la implementación de la nueva solución. Se evidencia que incluye una conexión VPN SSL a los servicios de la compañía, aumentando el riesgo de exposición de amenazas cibernéticas al no controlar el tráfico ni controles de seguridad mediante un firewall.
Imagen realizada por Juan Manuel Caicedo Castaño el 4 de mayo de 2024.

ANEXO C. Solución y proceso de configuración de los Firewall.
El anexo "Configuración de Firewalls.pdf" proporciona un resumen del proceso detallado que se siguió para llevar a cabo la implementación del proyecto de integración de sedes en el Directorio Activo de la Sede Principal en Colombia. El objetivo principal de este anexo es proporcionar una visión general del flujo de trabajo y las actividades que se llevó a cabo para alcanzar los objetivos establecidos.
Documento realizado por Juan Manuel Caicedo Castaño el *17 de marzo de 2024.*