PROPUESTA DE SOLUCIÓN DE SEGURIDAD BASADA EN FORTINET

Presentado por:

John Deavid Santos Parada

Tutor:

Angela Tatiana Zona Ortiz, PhD

UNIVERSIDAD SANTO TOMÁS

Facultad de Ingeniería de Telecomunicaciones

Bogotá D.C., 2024

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

1. PRESENTACIÓN DEL PROYECTO

En el marco de la realización de la pasantía dentro de la empresa Sonda de Colombia se plantea la propuesta de red SD-WAN con equipos Fortinet, con la finalidad de que la red sea más eficaz respecto al tráfico y solucione problemas de vulnerabilidades de seguridad como proteger las redes empresariales contra amenazas cibernéticas como malware, virus, ataques de denegación de servicio (DDoS), intrusiones, filtrado de contenido web, entre otros para la empresa Camanchaca. La empresa Sonda de Colombia presta servicios para la solución de problemas de seguridad y optimización de redes de comunicaciones, utilizando soluciones de Fortinet para empresas de diferentes sectores.

Por otro lado, la empresa Camanchaca, una de las empresas pesqueras más importantes de Chile cuenta con tres principales áreas de negocio: Cultivo de Salmon, pesca industrial, cultivo de Mejillones y Abalones. Recientemente también servicios logísticos. La empresa cuenta con 3600 empleados, exporta a 60 países y tiene ventas anuales por 640 millones de dólares. Dentro de chile la empresa cuenta con 18 ubicaciones distintas en el país, entre lugares remotos, desde oficinas comerciales y de ventas hasta centros de producción, plantas de manufactura y centros logísticos. De esta distribución parten los distintos retos de la empresa en materia de conectividad, seguridad y cumplimiento.

1.1 Caso de negocio

Esta empresa está conectada a una red MPLS con un tráfico enrutado a la oficina principal en la ciudad de Santiago, cuenta con 18 oficinas, algunas de ellas se conectan con esta oficina principal y se encuentran separadas a más de 3.000 kilómetros.

Por otra parte, para algunas de las ubicaciones remotas se establece una conectividad a través de enlaces por satélite, lo que genera mayor costo y no brinda la confianza necesaria para él envió de los datos más importantes de la compañía. Es de gran importancia para la empresa tener más control y visibilidad del tráfico de red sobre el ancho de banda y a su vez tener más seguridad.

La empresa pesquera chilena requiere:

1. Mejorar el rendimiento de la red, debido a que solo cuenta con un canal dedicado para el trafico en su red, en este caso MPLS
2. Segmentar el tráfico de la red para brindar prioridad a datos y activos más relevantes en la compañía, dirigiendo por diferentes caminos el trafico
3. Mejorar la visibilidad de los logs que se generan en la red, debido a que actualmente la empresa no cuanta con la visibilidad completa de la red, no monitorea el tráfico, ni genera constantes análisis de seguridad, a demás de ello con el manejo de esta información mejora el tiempo de control de los riesgos y se pueden genera valiosos informes para la empresa
4. Mejorar la seguridad. En la actualidad la seguridad de la red cuenta con pocas herramientas, la mayoría de los filtros se encuentran en la sede central de Santiago,

generando falta de control de acceso, de actualización de software, de cifrado de datos, entre otras. Por lo que se requiere mayor control en sobre la infraestructura.

1.2 Justificación

Para la empresa Camanchaca es importante mejorar tanto la seguridad como el tráfico de sus datos por medio de una utilización eficaz de la red, gracias a dispositivos que brinden el balanceo y la seguridad esperada para la compañía. Esto con el objetivo de tener control de los datos y el flujo a través de la red, además implementar más acciones de seguridad que ayuden a la protección de los datos o activos importantes de la empresa.

1.3 Objetivos

Plantear una solución SD-WAN para segmentar y balancear el tráfico de red MPLS de la empresa Camanchaca, utilizando equipos FortiGate para las distintas sedes de la empresa, con un equipo FortiAnalyzer que brinde información respectiva al tráfico.

1. Caracterizar cada uno de los puntos de la red MPLS de la red de la empresa. A nivel del máximo de dispositivos y el ancho de banda.
2. Establecer diferentes alternativas que permitan la mejora de la conectividad, seguridad y cumplimiento de la empresa.
3. Elegir la solución que soporte el tráfico requerido mediante la caracterización anterior.

2 CONTEXTO EN SOLUCIONES FORTINET

Para plantear alternativas de solución basada en productos Fortinet se requiere de conocimientos básicos. Estos conocimientos se han generado a partir de una serie de certificaciones como lo son: NSE1, NSE2, NSE3 y NSE4. A continuación se describe cada una de dichas certificaciones con su contenido.

2.1 NSE 1 (Information Security Awareness)

La certificación NSE 1 busca la concientización de los aspectos relacionados con la seguridad de la información. La certificación presenta las actuales ciber amenazas que enfrentan las compañías y personas del común en su día a día, además brinda consejos para la protección de la información. A continuación, se presenta (¿Quién? ¿Por qué? Y ¿cómo?) realizan los ataques de ciber seguridad y las estrategias clave para mantenerse seguro en internet.

1. ¿Quién está detrás de los ataques?
   I. Explorador: Busca la manera de engañar a las personas, normalmente por medio de fishing.
   II. Hacker: Atacan objetivos con los que no están de acuerdo (indignación política, social o moral)
   III. Ciber terrorista: Intimidan enemigos, infunden terror para causar caos. (se infiltran en sistemas para robar o exponer datos de un objetivo).
   IV. ciber criminal: roban dinero, datos de tarjetas de crédito, información personal de las personas con la finalidad de pedir un rescate
   V. Ciber soldados: grupo financiado en pro del país

2. ¿Cuáles son los motivos?
   I. Los atacantes buscan infiltrarse en sistemas, para robar información o causar daños en el mismo con la finalidad de robar datos, exponer información, dañar la reputación de compañías, generalmente con la finalidad de ganar dinero o desacreditar a personas o empresas.

3. ¿Cómo se realizan algunos de estos ataques?
   I. Los atacantes buscan vulnerabilidades, fallas de software, firmware o hardware que se puedan usar para realizar acciones no autorizadas. Lo que se busca es identificar las superficies de ataque para reducir la magnitud y el riesgo del ataque.
   Algunos de los malware que se pueden encontrar son: (virus, gusanos, botnets, troyanos, DDoS y ransomwere)
   II. Otra de las formas en que se pueden generar estos ataques es por medio de la ingeniería social, la cual busca engañar usuarios haciéndoles creer que lo que ven es cierto, atrayéndolos por medio de engaños.

4. Estrategias clave para mantenerse seguro en internet
   I. Estar alerta

- Ingeniería social: El atacante se gana la confianza y se aprovecha de ello para que se revele información.
- Juice Jacking: Son puestos de carga inseguro que instalan malware al conectarse.
- Phishing: Son correos electrónicos dañinos que contienen malware o se usan para el robo de la información.
- Ransomware: Malware que impide acceso a sistemas y piden dinero para recuperar los datos.
- Spear Phishing, whaling, fraude del CEO y ataques por email tipo BEC: Son mensajes fraudulentos con los que los atacantes buscan ganar dinero

II. Seguridad de los Móviles
- Proteger la red WIFI, que es puerta principal por donde acceden a los dispositivos y verificar bien el nombre de la red a la que se vaya a conectar.
- No usar puertos de carga en cualquier lugar, lo mejor es fomentar el uso de power bank.

2.2 NSE 2 (The Evolution of Cybersecurity)

En la certificación NSE 2 se contempla la evolución de la ciberseguridad y se enseñan los tipos de productos de seguridad desarrollados por los proveedores de seguridad. La finalidad de estos productos es hacer frente a las problemáticas presentes en redes y organizaciones. Entre los productos desarrollados por los proveedores de seguridad se encuentran:

1. Seguridad SASE (Secure access service edge): Esta en una Tecnología que combina la red y la seguridad como servicio para proporcionar acceso seguro a las redes empresariales actuales, con el objetivo de satisfacer las necesidades de acceso dinámico y seguro de las organizaciones. Esta solución proporciona capacidades de red y de seguridad integradas, ofreciendo:
   I. Rutas optimizadas para todos los usuarios y acceso a todas las nubes, lo que mejora el rendimiento y la agilidad.
   II. Seguridad certificada de nivel empresarial para la fuerza laboral móvil.
   III. seguridad homogénea para todos los bordes.
   IV. Administración consolidada de las operaciones de seguridad y red.

2. Seguridad SD-WAN (Red de área extensa definida por software): Una solución SD-WAN mejora el aprovechamiento de las redes WAN y la conectividad de múltiples nubes, esto con la finalidad de brindar rendimiento de alta velocidad a las aplicaciones de borde de la WAN. Además de esto se tiene un control centralizado con el cual se puede definir la ruta adecuada para el tráfico, lo que garantiza acceso rápido y fácil a las aplicaciones en la nube critica de la empresa. La SD-WAN permite:
   I. Tener un uso efectivo de la WAN.
   II. Rendimiento mejorado al dirigir de la mejor manera el tráfico por el mejor enlace.

III. El uso de túneles IPsec directos entre sitios lo que genera menor latencia entre sitios y menor carga en los Hubs.
IV. Reducción de costos.

3. Seguridad de EndPoint: Generalmente los dispositivos finales son el foco de violaciones de seguridad por los atacantes, por lo que la protección de los EndPoint se encarga de descubrir riesgos en el punto final, supervisar y evaluar el nivel de peligro. El sistema detecta la amenaza, la contiene y elimina automáticamente.
   La protección en los puntos finales genera reducción de la exposición de la red por medio de la eliminación de los puntos que aumenten el nivel de riesgo, esto se logra gracias a EPP (EndPoint protection platform) que se encarga de detener el malware antes de ejecutarse, lo que genera seguridad para detectar, autoriza y protege los dispositivos de almacenamientos externos y EDR (EndPoint detection and response) encargado de detectar y e investigar actividades sospechosas para responder a ellas.

4. Firewall . Es una solución de seguridad encargado de proteger la red del tráfico no deseado, estos firewalls bloquen el malware entrante basado en reglas previamente programadas, estas reglas pueden impedir a los usuarios de la red el acceso a sitios o programas determinados.
   En la actualidad se utilizan los NGFW (firewall de nueva generación) el cual ofrece rendimiento de seguridad potenciado por IA e inteligencia de amenazas, estos firewalls brindan una visibilidad completa, seguridad y convergencia en redes.

5. SOAR (Security orchestation, automation and responce). Unifica las herramientas de seguridad en flujos de trabajo que se ejecutan automáticamente, lo que lo hace más eficiente al automatizar procesos repetitivos manuales, centraliza el proceso de respuesta ante incidentes y optimiza la operación.
   Por medio de la orquestación y respuesta se proporcionan datos de ¿Qué? ¿Cuándo? Y ¿Quién? genero el incidente. Luego se realiza una investigación donde se establecen los pasos para realizar la solución y mitigación de la amenaza.
   La optimización de la operación se realiza gracias a los manuales de estrategias o flujos de trabajo, los cuales ejecutan tareas repetitivas. Gracias a las respuestas veloces y unificadas, se generan menores probabilidades de error y una carga de trabajo reducida par los analistas.

6. NAC (Network acces control). Esta solución está encargada de permitir el acceso de los dispositivos a la red, crea perfiles de dispositivos conectados, es capaz de habilitar permisos a la red dependiendo de la funcionalidad. El NAC tiene la visibilidad completa de la red, esto genera un buen control y rendimiento, todo esto integrado en el marco de la seguridad.

7. SandBox. Con el aumento de los ciber ataques y la sofisticada forma de ejecutarlos es más probable que una amenaza traspase la seguridad y genere una violación de datos. Esta solución es un entorno seguro que limita las acciones de una aplicación.

Para las compañías es necesario adoptar el sandboxing como una de sus estrategias de seguridad esenciales para que ayude a combatir las amenazas desconocidas.

8. SIEM (security information and event management). Los sistemas de gestión de eventos de seguridad recopilan y normalizan alertas y eventos de registros de la red de una organización y de sus dispositivos de seguridad, los almacena en una ubicación central segura. Analiza datos históricos y en tiempo real para identificar posibles incidentes de seguridad, también analiza el comportamiento de usuarios y entidades todo estos por medio del aprendizaje automático. El SIEM compone el NOC (Network operation center) y el SOC (Security operation center).

9. WAF (Web aplication firewall). Es el encargado de proteger aplicaciones web esenciales de la empresa frente a ataques dirigidos a vulnerabilidades conocidas y desconocidas. Es dirigido al tráfico del protocolo de transferencia de hipertexto (HTTP), este WAF se ubica entre los usuarios externos de una aplicación web para realizar un análisis de toda la comunicación.

10. Filtro de contenido WEB. Es una Aplicación que examina las páginas web para determinar si hay contenido para bloquear total o parcialmente, esta aplicación permite establecer reglas para distintos tipos de usuarios (Niños y adultos) o en organizaciones permite o bloque el tráfico a los trabajadores dependiendo de las reglas establecidas. El filtro de contenido WEB es la primera línea de defensa contra ataques en la red.

2.3 NSE 3 (Fortinet Product Awareness)

El objetivo de la certificación NSE 3 es generar conocimiento de los productos clave de Fortinet y describir los problemas de ciberseguridad que solucionan. Estos se organizan basados en los pilares de Fortinet Security Fabric que son Redes basadas en la seguridad, acceso de confianza cero, seguridad en la nube adaptativa, y operaciones de seguridad. A continuación, se describen los productos para cada pilar de Fortinet:

1. Redes basadas en la seguridad: Permite la innovación digital a través de la convergencia de redes y seguridad en un solo sistema integrado que puede expandirse a cualquier borde. Los productos de Fortinet para este pilar son:
   I. FortiGate: Es el firewall de nueva generación de Fortinet, resuelve problemas como superficie de ataque ampliadas, incapacidad de detectar y contener ataques, visibilidad y control limitados y por último realiza trabajos con productos puntuales de mayor complejidad.
   Este producto realiza control de aplicaciones, prevención de intrusiones, filtrado URL, sandboxing inspección SSL y tiene una tecnología de antivirus que protege contra los últimos virus, spyware y otras amenazas a nivel de contenido.
   II. FortiAP: Es el punto de acceso seguro de Fortinet para dispositivos inalámbricos, esta solución ofrece una gestión unificada con el fin de simplificar operaciones y asegurar la aplicación y en cumplimiento de las políticas uniformes.

III. FortiManager: Es un dispositivo o VM que administra otros dispositivos, como FortiGate, FortiAP, FortiExtender y FortiSwitch. Proporciona una gestión centralizada impulsada por la automatización de estos dispositivos desde una sola consola para una administración y visibilidad completas de sus dispositivos de red a través de herramientas de aprovisionamiento y automatización optimizadas.
IV. FortiSASE: Es la solución de Fortinet Secure Access Service Edge (SASE). SASE simplifica la WAN y la seguridad al entregar ambos como un servicio en la nube directamente a la fuente de conexión
V. FortiSwitch: Es un conmutador de red seguro, diseñado y producido por Fortinet, ofrece una amplia oferta de conmutadores que pueden escalar desde la configuración minorista más pequeña hasta el centro de datos.

2. Acceso de confianza cero: Es una filosofía de seguridad de la red que establece que las amenazas siempre están presentes, ya sea dentro o fuera de la red
   I. FortiAuthenticator: Es un producto de administración de identidad para la empresa, que brinda autenticación y autorización sólidas a la red cableada e inalámbrica. Brinda acceso seguro a los usuarios, tanto internos como externos, a las aplicaciones y los recursos de la red, con la opción de usar varios tokens de autenticación de dos factores de Fortinet y que no son de Fortinet (como RSA). También puede utilizar certificados X.509 para requisitos de autenticación más estrictos, más comúnmente vistos en instituciones financieras y de atención médica.
   II. FortiClient: brinda protección, cumplimiento y acceso seguro en un solo cliente modular ligero. Este se ejecuta en un EndPoint como lo son los dispositivos móviles o computadores portátiles.
   III. FortiNAC: solución de acceso a la red la cual permite a los usuarios una mejor visibilidad de todos los dispositivos en todas las redes, principalmente es necesaria para 3 cosas:
   IV. Dar visibilidad para descubrir e identificar lo que hay en la red
   V. Control, para que se pueda hacer algo con lo que encontrado
   VI. Una solución NAC debe continuar vigilando la red para que, si ocurre un incidente, pueda tomar medidas automáticas.

3. Seguridad en la nube adaptativa: Permite el uso eficaz de los recursos, el equilibrio de carga dinámico y la visibilidad de la experiencia del usuario de la aplicación.
   I. FotiADC: Solución que mejora la escalabilidad, rendimiento y seguridad de las aplicaciones que estén alojadas en la nube o en instalaciones físicas. Proporciona la aceleración de aplicaciones, equilibrio de carga y seguridad WEB inigualables, incluye aceleración WAF, IPS, SSL, equilibrio de carga de enlaces y autenticación de usuario en una solución.
   II. FortiMail: solución integral de seguridad informática contra las amenazas de correo electrónico, protege de suplantación de identidad, ramsomwere, ataques de día cero y ataques de compromiso electrónico comercial (BEC).

III. FortiWEB: es un firewall de aplicaciones web que protege las aplicaciones web críticas para el negocio de los ataques dirigidos a vulnerabilidades conocidas y desconocidas.

4. Operaciones de seguridad: permiten la administración centralizada, la automatización y orquestación de redes y el análisis de Security Fabric.
   I. FortiNDR: dispositivo que utiliza inteligencia artificial y otros análisis para identificar actividades sospechosas, cubriendo tanto el tráfico de red como el análisis basado en archivos, y contiene amenazas de manera adaptativa mientras protege la red de nuevas amenazas.
   II. FortiAnalyzer: recopila, almacena y analiza automáticamente los historiales de todos los dispositivos de Fortinet. Es capaz de administrar grandes volúmenes de registros y buscar eventos específicos utilizando diversos criterios de búsqueda. Entre los beneficios que proporciona están:
      - Aumenta la seguridad al proporcionar herramientas integrales para automatizar la visibilidad del Security Fabric.
      - Reduce la complejidad al aprovechar FortiView y una sola consola para brindar visibilidad nativa dentro de la consola elegida.
      - Reduce el costo total de propiedad al escalar hasta más de 10 000 dispositivos de estructura de seguridad con una consola de visibilidad sin invertir dinero adicional en herramientas de administración de registros de terceros
      - Automatiza el cumplimiento al proporcionar informes de cumplimiento preconstruidos con informes, personalización y programación de nivel empresarial. Como resultado, estos beneficios no solo diferencian a FortiAnalyzer de otros proveedores de administración central, sino que brindan una razón convincente por la cual FortiAnalyzer debe implementarse con FortiGate.
   III. FortiDetector: Combina la noción de honeypot con análisis de amenazas y mitigación de amenazas en uno. Específicamente, FortiDeceptor crea señuelos para atraer a los atacantes e inspecciona su comportamiento para generar inteligencia de amenazas precisa para bloquear ataques externos e internos antes de que ocurra un daño significativo.
   IV. FortiEDR: Se encarga de Predecir y prevenir ataques mediante la reducción de la superficie de ataque y la prevención de malware, Detectar y desactivar amenazas con detección y desarme en tiempo real, por último, Responder, investigar y buscar con la ayuda de la remediación orquestada y la investigación forense.
   V. FortiSandbox: Es la solución sandbox multinivel de Fortinet para detectar amenazas y acelerar el análisis de estas. Los CISO adoptan el sandboxing como un componente esencial de sus estrategias de seguridad para ayudar a combatir amenazas previamente desconocidas.
   VI. FortiSIEM: Es el Core del equipo de operaciones de seguridad, detecta y responde rápidamente amenazas gracias a su aprendizaje automático. FortiSIEM es la única plataforma de operaciones de seguridad que cuenta con una base de datos de gestión de configuración (CMDB) completamente integrada.

VII. FortiSOAR: diseñado para capacitar a los equipos SOC para acelerar su proceso de respuesta a incidentes y lograr la máxima eficiencia. Remedia la entrada de una avalancha de alertas, procesos manuales repetitivos y aumenta las tareas llenando los vacíos donde los recursos son limitados.

2.4 NSE 4 (Security Driven Networking)

La certificación NSE 4 estudia las políticas de firewall, Fortinet security fabric, autenticación de usuario y como proteger la red usando perfiles de seguridad como lo son: IPS, antivirus, filtrado web, control de aplicaciones, entre otros. La finalidad es proporcionar una sólida comprensión de como implementar seguridad básica de la red.La certificación se divide en dos partes principales, que son: FortiGate infrastructure y FortiGate security. A continuación, se expone la composición de cada una de las partes principales.

1. FortiGate infrastructure:
   I. Enrutamientos: FortiGate es compatible con IPV4 e IPV6, este dispositivo realiza el enrutamiento para el tráfico de firewall y del tráfico de salida local, se encarga de determinar el siguiente salto para la dirección de destino. Este siguiente salto puede ser el destino u otro enrutador a lo largo del camino. FortiGate mantiene dos tablas de enrutamiento con la información RIB (Base de información de enrutamiento) y FIB (Base de información de reenvío). Donde RIB contiene las rutas activas “Las mejores rutas”, ya sea conectadas, estáticas dinámicas y la FIB se compone principalmente de entradas RIB, se usa para la búsqueda de rutas las cuales son visibles solo a través de la CLI (Comand line interface).

   Entre las rutas se encuentran:

   - Ruta estática: Esta ruta se configura manualmente por el administrador. Cuando un paquete tiene un destino que esté dentro de un rango específico lo envía a través de una interfaz de red especifica hacia un enrutador especifico.
   - Ruta estática con direcciones con nombre: Son direcciones de firewall configurados para IP, mascara de red o FQDN. Estas rutas pueden ser usadas como destinos para rutas estáticas.
   - Ruta dinámica: En este modelo, las rutas se aprenden automáticamente, FortiGate intercambia rutas con enrutadores adyacentes, para este modelo de rutas no es necesario configurar rutas manuales, es un método útil para redes grandes. También acepta protocolos de enrutamiento dinámicos como RIP, OSPF, BGP e ISIS.
   - Ruta especifica: Para este modelo se deben proporcionar las coincidencias más generales que en las rutas estáticas, como lo son (Protocolo, dirección de fuente, Puertos de origen y puertos de destino).

   Con FortiGate se puede implementar una SD-WAN segura, que se encarga de controlar el y tráfico de salida, gracias a estas redes se puede generar un uso

efectivo de la WAN, mejora el rendimiento de la aplicación y reduce los costos para las compañías.

II. Dominios virtuales: Los dominios virtuales dividen FortiGate en múltiples dispositivos lógicos y dominios de seguridad. Se emplean políticas de seguridad independientes, tablas de enrutamiento, configuraciones de VPN entre otras. Por defecto FortiGate admite hasta 10 VDOMS.
Con el modo multi-VDOM se pueden crear múltiples VDOM que funcionen como múltiples unidades independientes, FortiGate cuenta con dos modos multi-VDOMS (Admin VDOM y Traffic VDOM). Existen tres casos de uso para el modo multi-VDOM, los cuales son, Managmente, Independent y Meshed.
La administración de la VDOM solo es posible a través de la cuenta Admin o Super-admin, desde ellas se pueden realizar las configuraciones y las copias de seguridad. Lo que concierne a los enlaces entre VDOMS, se pueden realizar entre diferentes VDOM, el soporte varía dependiendo el modo de operación, ya sea NAT a NAT, NAT a transparente o viceversa.

III. FortiGate single sing-On: FSSO es un agente de software que permite a FortiGate identificar usuarios de la red para políticas de seguridad o para acceso VPN en implementaciones avanzadas. El FSSO se puede trabajar en tres modos:
   - Modo agente DC: Al autenticarse los usuarios, proporcionan sus credenciales, el agente DC ve el evento y de inicio de sesión y lo envía al agente recolector, este agente se encarga de agregar todos los inicios de sesión y envía a FortiGate (Nombre de usuario, Nombre del Host, dirección IP y los grupos de usuario), por último, FotiGate aprende del agente recopilador quien es el usuario, la dirección IP y algunos grupos de AD de los usuarios de ese miembro.
   - Modo de sondeo basado en agentes recopiladores: Para este modo se debe instalar un agente recopilador en un servidor Windows, el agente recopilador sondea cada DC en busca de elementos de inicio de sesión de usuarios. Este modo requiere una instalación menos compleja y reduce el mantenimiento continuo.
   - Modo sin agentes: Este modo no requiere de un agente DC externo ni agente cobrador, en este caso FortiGate recopila los datos directamente, lo que brinda más CPU y RAM requerida por FortiGate souport.

IV. ZTNA: Con zero trust network Access la identidad se establece a través de certificados de cliente, esta confianza se establece entre:
   - FortiClient: Proporciona información de punto final (información de dispositivo, usuarios registrados y postura de seguridad), además obtiene el certificado de cliente de fortiClient EMS.
   - FortiClient EMS: Emite y firma el certificado de cliente, sincroniza el certificado con FortiGate y utiliza reglas de etiquetado para etiquetar puntos finales.

V. SSL VPN: Para acceder a una VPN SSL hay dos modos:

- Modo túnel: Este modo requiere que FortiClient se conecte a FortiGate para agregar un adaptador de red virtual llamado FortiSSL. FortiGate establece el túnel, establece una dirección virtual al cliente desde un grupo de direcciones reservadas, donde todo el tráfico esta encapsulado con SSL/TLS, un punto a favor del modo túnel es que cualquier aplicación de red IP en el cliente puede guiar el tráfico a través del túnel, pero requiere la instalación de un cliente VPN.
- Modo web: este es el modo más simple, solo se debe conectar al portal de FortiGate SSL VPN desde cualquier navegador, es fácil el acceso a los recursos utilizados de la red, pero entre las desventajas con las que cuenta este modo son, primero se genera una interacción con la red interna exclusivamente mediante el navegador y segundo, admite un número limitado de protocolos.

VI. Ipsec VPN: Conjunto de protocolos estándar neutrales usado para unir dos LAN físicamente distintas, generalmente brindan autenticación para verificar la identidad de ambos extremos, integridad de datos (HMAC) para demostrar que no se manipularon los datos encapsulados y confidencialidad (Cifrado) para asegurarse que solo el destinatario previsto pueda leer el mensaje.

VII. Alta disponibilidad: Sincroniza dos de cuatro dispositivos FortiGate para formar un clúster con fines de redundancia y rendimiento, cuenta con dos modos de operación que son:

- Activo-Pasivo: Se sincroniza la información de operación (configuración, sesiones, entradas FIB, etc.) con los dispositivos secundarios. EL FortiGate principal es el único FortiGate que procesa activamente el tráfico, los dispositivos secundarios permanecen en modo pasivo, monitoreando el estado del dispositivo. Si se detecta un problema en el FortiGate principal, uno de los dispositivos secundarios asume la función principal.
- Activo-Activo: En este modo todos los miembros del clúster pueden procesar el tráfico, es decir que el FortiGate principal puede distribuir sesiones a los dispositivos secundarios. El FortiGate principal debe transmitir paquetes de saludo para el descubrimiento y monitoreo de miembros, sincronizar los datos relacionados con la operación y distribuir sesiones a dispositivos secundarios.

2. FortiGate security:

I. Autenticación de firewall: Por medio de FortiGate se realiza la autenticación de usuarios y grupos de usuarios. El usuario debe autenticarse ingresando las credenciales validad, FortiGate aplica políticas y perfiles de firewall para permitir o denegar accesos. Entre los métodos de autenticación se encuentran:

- Autenticación local: Es una autenticación básica (Nombre de usuario y contraseña), se puede integrar con la autenticación de doble factor.
- Autenticación basada en servidor: Se usa cuando varios FortiGate necesitan autenticar a los mismos usuarios.
- Autenticación doble factor: esta autenticación se establece entre la contraseña más algo que tenga un token o un certificado.

II. Registro y monitoreo: El propósito de los registros es monitorear el tráfico de la red, localizar problemas, establecer líneas base y más. Estos registros se pueden almacenar localmente en FortiGate o externamente en FortiAnalyzer. Entre los tipos de registros se encuentran:
    - Registro de tráfico: Registra información del flujo de tráfico, forward (tráfico aceptado o rechazado por FortiGate), local (tráfico hacia y desde las direcciones IP de administración de FortiGate) y sniffer (tráfico por el rastreador).
    - Registro de eventos: Agregar o modificar una configuración del dominio, como información de operaciones como actualizaciones automáticas de FortiGuard y registros de inicio y cierre de sesión de usuario.
    - Registros de seguridad: registra ataques e intentos de intrusión, los divide en diferentes niveles de prioridad (0-Emergencia, 1-Aerta, 2-Critico, 3-Error, 4-advertencia, 5-Notificacion y 6-Depurar)
III. Operaciones con certificados: Se usan certificados digitales para mejorar la seguridad:
    - Inspección: Genera dinámicamente certificados para realizar inspección SSL completa, FortiGate puede inspeccionar certificados para garantizar que sean confiables y válidos.
    - Privacidad: utiliza certificados y claves privadas para establecer conexión SSL con otros dispositivos.
    - Autenticación: Los usuarios certificados por una autoridad de certificación de confianza pueden autenticarse para acceder a la red.
    - Certificado digital: Documento digital producido y firmado por una CA
IV. Control de aplicaciones: Detecta aplicaciones generalmente que consumen mucho ancho de banda, luego toma decisiones adecuadas como monitorear, bloquear o aplicar modelo de tráfico. En el perfil de control de aplicaciones se permite filtrar el tráfico en función de:
    - Categorías: Se agrupan aplicaciones similares, puede ver formas de control para la categoría y puede configurar acciones para categorías definidas
    - Anulación de aplicaciones: Permite configurar acciones para firmas o aplicaciones especificas
    - Filtrar anulaciones: Es la forma más flexible de crear categorías de aplicaciones según el comportamiento, la popularidad, el protocolo, el riesgo, etc.
V. Antivirus: Para la elección del motor de escaneo se debe tener en cuenta que si lo que se quiere es mejorar el rendimiento se debe hacer con la inspección de flujo, pero si la prioridad es la seguridad realizar la inspección basada en proxi. Las técnicas de detección para el antivirus son:
    - Escaneo o análisis de antivirus: detecta y elimina amenazas en tiempo real, evita la propagación de amenazas y preserva la reputación de cliente de su IP publica

- Escaneo Grayware: utiliza firmas grayware, detecta y bloquea programas no solicitados y se aplican acciones de antivirus.
- Escaneo IA Aprendizaje automático

VI. Security fabric: Es una plataforma de Fortinet impulsado por la inteligencia artificial, permite la protección, detección y respuesta automatizadas junto con la visibilidad consolidada en las soluciones de Fortinet y un amplio ecosistema de más de 500 soluciones de terceros.

En conclusión, con las certificaciones de Fortinet se generaron conocimientos tanto básicos en seguridad, como específicos de los equipos y dispositivos de Fortinet. Se profundizó en características de los equipos y diferentes formas de integración entre ellos. De manera que se tiene la capacidad para plantear diferentes alternativas de solución a problemáticas o requerimientos establecidos por diferentes clientes.

Esto permite abordar soluciones SD-WAN, protección de EndPoint y dispositivo, seguridad de red, seguridad de aplicaciones, acceso seguro y con la ayuda de la inteligencia artificial (IA) la prevención y detección de amenazas.

Finalmente aclarar que, para la selección de los equipos, son necesarias las certificaciones NS3 y NS4, debido a que en la primera se introducen los productos clave y los problemas de ciberseguridad, se complementa con la segunda que plasma la infraestructura requerida para el desarrollo y consolidación de las diferentes soluciones.

3 CARACTERIZACIÓN DE RED MPLS DE LA EMPRESA CAMANCHACA

La empresa Camanchaca es una de las empresas pesqueras más importantes de chile, con un recorrido de más de 55 años en el mercado, emplean alrededor de 3600 empleados, exporta a 60 países y tiene ventas anuales por 640 millones de dólares.

Camanchaca cuenta con un total de 18 sedes. En la Tabla 1Tabla 1 Caracterización de la red MPLS de la empresa , se muestran 3 tipos de sedes para la empresa Camanchaca de Chile, a saber, tipo A, B y C. Estas sedes se dividen por la cantidad de ancho de banda y número de usuarios máximo en cada una.

La empresa cuenta con:

- 3 sedes tipo A, de las cuales se contempla un máximo de 500 usuarios y 1.2Gbit/s de ancho de banda, para la red MPLS que tiene implementada pagan 2.000 USD.
- 9 sedes tipo B, en las cuales se cuenta con un máximo de 200 usuarios y 900 Mbit/s de ancho de banda, el costo estimado de la red MLPS con la que cuentan está alrededor de 1600 USD.
- 6 sedes tipo C, en las que alberga un máximo de 50 usuarios y 500Mbit/s de ancho de banda, el costo estimado de la red MPLS implementada es alrededor de 1100 USD.

Tabla 1 Caracterización de la red MPLS de la empresa Camanchaca

Tipo de sede	**A**	**B**	**C**
N° Sedes	3	9	6
N° Usuarios/sede	500	200	50
BW	1.3 Gbit/s	900 Mbit/s	500 Mbit/s
MPLS (USD)	2.000	1.600	1.100

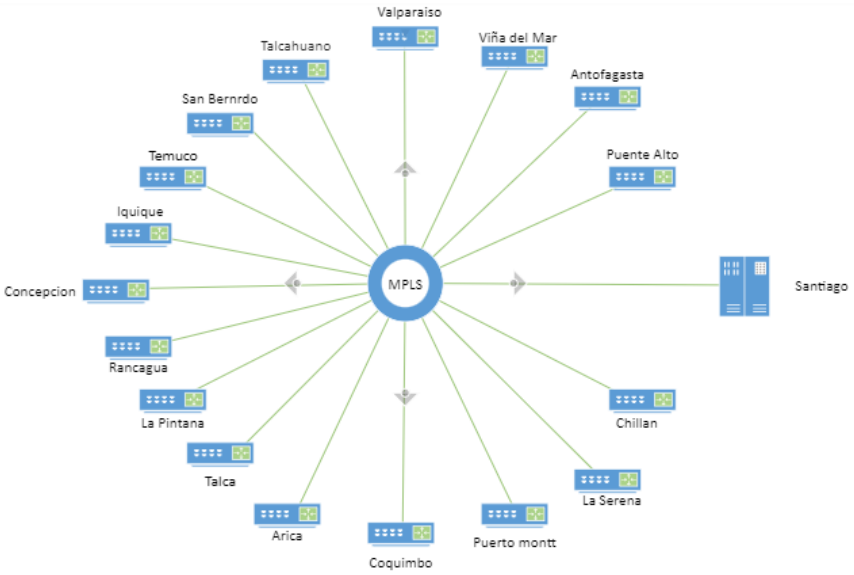

Figura 1 topología de la red MPLS de la empresa Camanchaca

En la Figura 1 se muestra la topología de la red MPLS con la que cuenta actualmente la empresa Camanchaca, se evidencia que las sedes se encuentran conectada a una red central, en este caso a la sede que se encuentra ubicada en la ciudad de Santiago.

Partiendo de los datos contemplados en la Tabla 1 la cual contiene la caracterización y los requerimientos estipulados por la empresa, se plantean posibles alternativas de solución, con la finalidad de escoger la mejor opción basado en tres criterios: presupuesto, topología propuesta, tiempo de implementación.

4 ALTERNATIVAS DE SOLUCIÓN PARA LA EMPRESA CAMANCHACA

En el presente capítulo se presentan las posibles alternativas de solución para la problemática de la empresa camanchaca. Estas soluciones son parcialmente distintas, ya sea por la topología, por ser una solución hibrida (Solución diseñada entre equipos cableados (hardware) y software) o por el nivel de seguridad que genera en la empresa cada una de las alternativas. En esta sección también se muestran los presupuestos y se realiza un análisis para cada una de las soluciones planteadas o alternativas.

Tabla 2 Listado de equipos disponibles para el planteamiento de alternativas

Equipo	Imagen	Características	Capacidad
FortiGate 600F		IPsec VPN Throughput	55 Gbps
		Threat Protection	10.5 Gbps
		Max IPsec Tunnels	50
		SSL Inspection Throughput (IPS, avg. HTTPS)	9 Gbps
		Zero Trust Network Access (ZTNA)	SI
FortiGate 200F		IPsec VPN Throughput	13 Gbps
		Threat Protection	3 Gbps
		Application Control Throughput	13 Gbps
		SSL Inspection Throughput	4 Gbps
		Zero Trust Network Access (ZTNA)	SI
FortiGate 80F		IPsec VPN Throughput	6.5 Gbps
		Threat Protection	900 Mbps
		Application Control Throughput	1.8 Gbps
		SSL Inspection Throughput	715 Mbps
		Zero Trust Network Access (ZTNA)	SI
FortiAnalyzer 3510G		GB/DAY	5000
		Analytic Sustained Rate (logs/sec) *	60000
		Collector Sustained Rate (logs/sec) *	90000
		Devices/VDOMs (Maximum)	10000

Cada una de las alternativas planteadas cuenta con un orquestador, que es el cerebro de la red SD-WAN, encargado de Automatización, optimización, gestión y análisis de la red, estas

alternativas tienen como base los equipos mostrados en la Tabla 2. Lo que diferencia las alternativas es que el número de equipos a utilizar o la topología de la red varían.

Partiendo de la Tabla 1 donde se identifica cada uno de los tipos de sedes, el tráfico y el ancho de banda de estas, se establece que:

- Para las sedes tipo A, con mayor tráfico de usuarios y ancho de banda, se asigna un FortiGate 600F.
- Para las sedes tipo B se asigna un FortiGate 200F
- Para las sedes tipo C, con menor tráfico y ancho de banda, el equipo correspondiente es un FortiGate 80F.

El control y visualización del tráfico de la red se realiza por medio de un solo equipo, en este caso un FortiAnalizer 3510G, que cumple con el número de registros por día para el tráfico con contemplado que actualmente es máximo 3600 GB/Log día y el equipo es capaz de soportar hasta 5000 GB/log día.

4.1 Alternativa N°1

La Figura 2 muestra la topología planteada para la alternativa N°1, donde se interconectan todas las sedes a través de una red MPLS e internet. Las sedes están divididas según el tipo, donde a las sedes tipo A se le asigna un FortiGate 600F, las sedes tipo B FortiGate 200F y las sedes tipo C FortiGate 80F dando cobertura a la totalidad de las sedes.

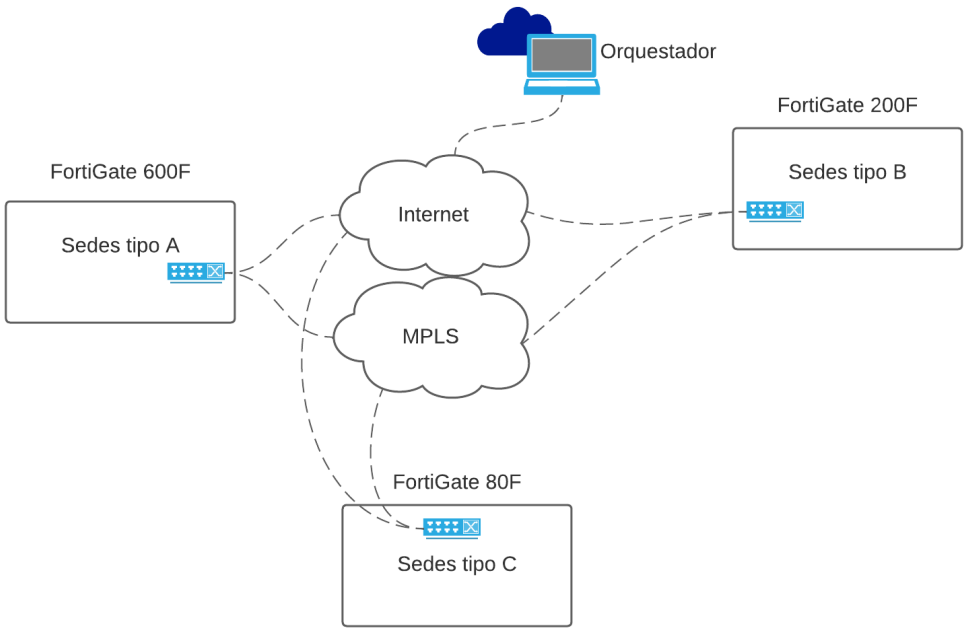

Figura 2 topología de red para la alternativa de solución N°1

La Alternativa N°1 cuenta con un despliegue de equipos en la totalidad de las sedes de la empresa, contemplando 3 equipos FortiGate 600F, 9 FortiGate 200F y 6 FortiGate 80F con la totalidad de los equipos en cada una de las sedes se puede unificar el control y monitoreo de ellos. Los equipos físicos cuentan con ventajas sobre los virtuales, como lo son:

- Rendimiento, ya que los equipos FortiGate físicos suelen tener un rendimiento superior en comparación con una solución virtual, ya que están diseñados para procesar grandes volúmenes de tráfico de red de forma eficiente
- Seguridad, los equipos FortiGate físicos vienen con hardware especializado para la seguridad de la red, lo que proporciona una capa adicional de protección contra amenazas cibernéticas en cuestión de fiabilidad al ser un dispositivo físico, un equipo FortiGate tiene menos probabilidades de sufrir interrupciones o problemas técnicos en comparación con una solución virtual que depende de la infraestructura de hardware.

Se plantea la arquitectura SD-WAN que mejora el tráfico de la red al segmentarlo y priorizar su distribución. Para finalizar, gracias al FortiAnalyzer se cuenta con una visibilidad completa de la red, centralización de log y reportes, además de mejorar la eficiencia operativa, gracias al control a la visión total de la red, pues los administradores pueden evidenciar y solucionar de manera más eficaz, ya que minimiza el tiempo de inactividad.

Basados en la descripción anterior, las facilidades y teniendo en cuenta que es una solución completa y totalmente basada en equipos de hardware, se valora la topología para la alternativa de solución N°1 con un puntaje de 10/10.

En la **Error! Reference source not found.** se presenta el presupuesto de la alternativa de solucion N°1. Para esta alternativa de solución se contempla un equipo físico por cada sede para un total de 18 dispositivos con un costo total de 114.345 USD, por otro lado el costo de la instalación es de 14.100 USD. Esta solución ofrece un soporte por 3 años, luego de este periodo es necesario volver a comprar una suscripción para el soporte.

Tabla 3 Presupuesto alternativa 1

Rubro	Descripción	Unidad	precio unitario	Cantidad	Total (USD)
Equipo	Equipo FortiGate 600F se implementará en 3 sedes tipo A	unidad	$ 18.423	3	$ 55.269
Equipo	Equipo FortiGate 200F se implementará en 9 sedes tipo B	unidad	$ 5.544	9	$ 49.896
Equipo	Equipo FortiGate 80F se implementará en 6 sedes tipo C	unidad	$ 1.530	6	$ 9.180

Recurso humano	Mano de obra para el despliegue de toda la solución	Mes	$ 4.300	3	$ 12.900
				TOTAL	$ 127.245

El presupuesto de la alternativa N°1 es de 127.245 USD presupuestando todos los equipos y el recurso humano necesario para el despliegue. El tiempo que tardaría el despliegue de esta solución es de 3 meses.

4.2 Alternativa N°2

Para la alternativa de solución N°2 se contempla el mismo despliegue de infraestructura que la alternativa N°1, el factor diferencial en este caso es dividir la implementación de los equipos en dos fases para disminuir costos:

- En la primera fase de la implementación se contempla equipar 7 FortiGate para las sedes más relevantes de la empresa, las que requieren mayor prioridad por el flujo y capacidad de atención a usuarios.
- La segunda fase se establece con las sedes con menor demanda con un total de 11 FortiGate, estas no dejan de importar porque se tiene que reforzar la seguridad debido a que quedan vulnerables para cualquier ataque, además al momento de administrar los dispositivos se transforma en una forma menos sencilla y eficaz

Al implementar en dos fases se busca primero optimizar y priorizar algunas de las sedes criticas para la empresa. De esta manera, se identifica y especifica el tráfico, los logs y se puede dirigir dicho tráfico de manera eficiente, así la misma red se vuelve más eficiente y se agilizan procesos. Se prevé que al término de 9 meses este completa la implementación de las dos fases.

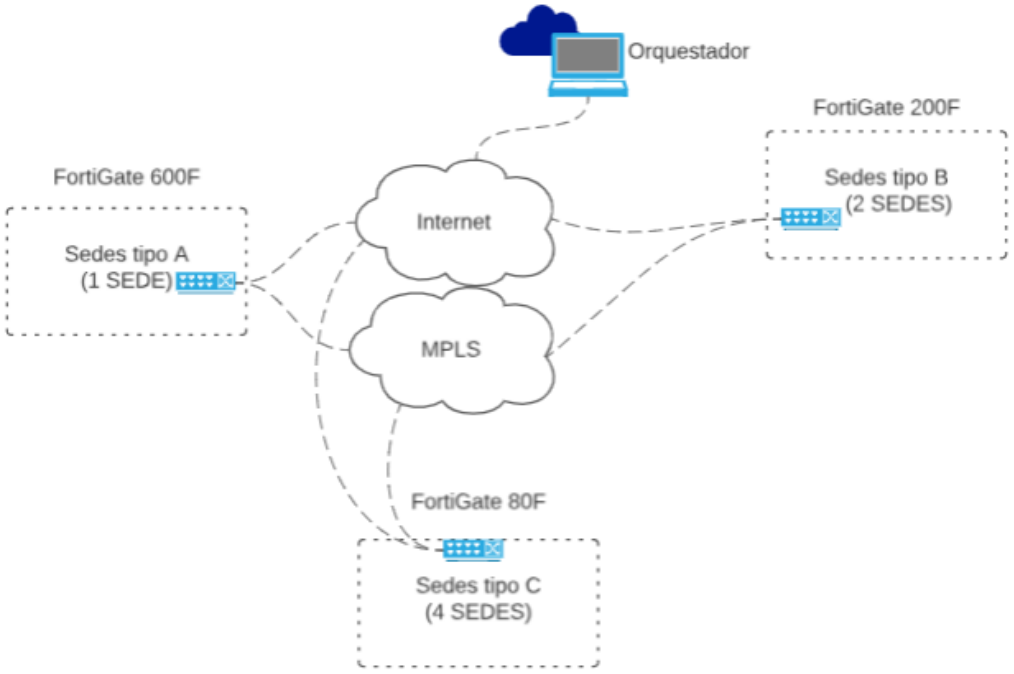

Figura 3 Topología fase 1, Alternativa 2

En la Figura 3 se contempla la topología para la solución de la fase 1 de la alternativa N°2 aquí se plantea la instalación de 7 equipos, distribuidos entre 1 FortiGate 600F, 4 FortiGate 200F y finalmente 2 FortiGate 80F, estos distribuidos en las sedes críticas de la empresa, donde se encuentra mayor flujo y potencial te ataque.

En la **Error! Reference source not found.** se encuentra el presupuesto para la alternativa dos en su fase 1, esta contempla implementar equipos en las sedes que es más necesario para luego de un tiempo invertir en el resto de las sedes. El precio de todos los equipos es de 43.659 USD y la implementación para los equipos en sus respectivas sedes es de 5.800 USD. El precio total de la fase 1 es de 43.659 USD. Es importante aclarar que este precio es solo para la primera fase, esta es una solución viable si la empresa no cuenta con el presupuesto para realizar una implementación completa para cada una de las sedes. Es importante aclarar que esta solucion ofrece un soporte por 3 años, Por lo que es necesario al termino de ello volver a comprar una suscripcion para el soporte. La fase 1 tardara 3 meses en ser implementada.

Tabla 4 Presupuesto fase 1 alternativa2

Rubro	Descripción	Unidad	precio unitario	Cantidad	Total (USD)
Equipo	Equipo FortiGate 600F se implementará en 1 sedes tipo A	unidad	$ 18.423	1	$ 18.423
Equipo	Equipo FortiGate 200F se implementará en 2 sedes tipo B	unidad	$ 5.544	2	$ 11.088

Equipo	Equipo FortiGate 80F se implementará en 4 sedes tipo C	unidad	$ 1.530	4	$ 6.120
Recurso humano	Mano de obra para el despliegue de toda la solución	Mes	$ 3.500	1	$ 3.500
				TOTAL	$ 39.131

En la Figura 4 se contempla la topología para la alternativa de solución N°2 en su fase 2. Se plantea la instalación de 11 equipos, los cuales son el restante de equipos para el resto de las sedes de la empresa. Estos equipos están distribuidos entre 2 FortiGate 600F, 5 FortiGate 200F y finalmente 4 FortiGate 80F, con el despliegue de esta fase se completa la implementación de la alternativa 2.

En la **Error! Reference source not found.** se presenta el presupuesto de la alternativa 2 en la fase 2, aquí se puede encontrar el resto de los equipos a utilizar. El precio de los equipos es de 79.986 USD, la implementación de estos equipos tiene un valor de 9.300 USD y finalmente el valor total de esta última fase es de 70.686 USD. Es importante aclarar que esta solucion ofrece un soporte por 3 años, Por lo que es necesario al termino de ello volver a comprar una suscripción para el soporte. La segunda fase quedara implementada 6 meses despues de la primera fase, para que asi quede completa toda la implementacion al termino de 9 meses

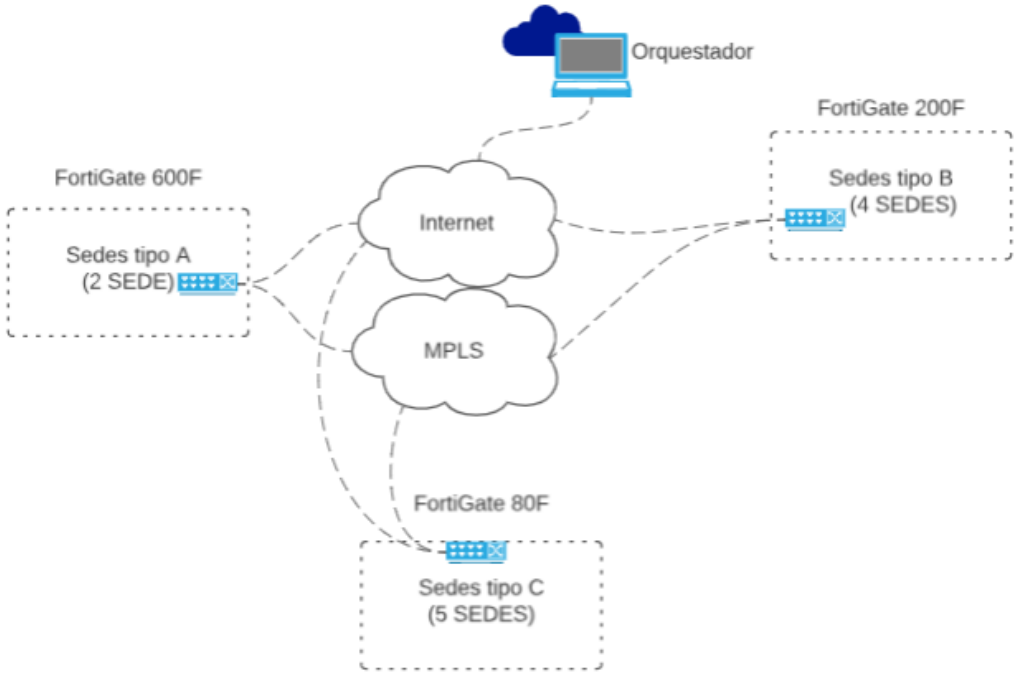

Figura 4 Topología fase 2, alternativa 2

Tabla 5 Presupuesto fase 2 alternativa 2

Rubro	Descripción	Unidad	precio unitario	Cantidad	Total (USD)
Equipo	Equipo FortiGate 600F se implementará en 3 sedes tipo A	unidad	$ 18.423	2	$ 36.846
Equipo	Equipo FortiGate 200F se implementará en 9 sedes tipo B	unidad	$ 5.544	5	$ 27.720
Equipo	Equipo FortiGate 80F se implementará en 6 sedes tipo C	unidad	$ 1.530	4	$ 6.120
Recurso humano	Mano de obra para el despliegue de toda la solución	Mes	$ 3.850	2	$ 7.700
				TOTAL	$ 78.386

En definitiva, el costo total de esta alternativa es 117.517 USD, y su implementación es de 9 meses. Es importante resaltar que para la selección de alternativas se tiene en cuenta para la alternativa 2 la fase 1 y la fase 2. La valoración de la topología es de 7/10.

4.3 Alternativa N°3

Para la Solución N°3 se plantea una implementación hibrida, se plantea en la sede principal un equipo FortiGate 600F y para el resto de las sedes una licencia de FortiSASE FC4-10EMS05-547-02-DD que soporta desde 2000 hasta 9999 usuarios. Esta licencia provee protección a usuarios cerrando brechas de seguridad y simplificando operaciones, desde una sola consola se puede gestionar la puerta de enlace web segura, acceso a la red de confianza cero, agente de seguridad de acceso a la nube, firewall como servicio y la SD-WAN segura.

En la Figura 5 se encuentra la topología de red para la alternativa de solución N°3, en esta topología se evidencia que la sede principal va a tener un equipo físico, el cual es un FortiGate 600F, el resto de las sedes cuentan con la licencia de FortiSASE, por esta combinación es que la alternativa N°3 es Hibrida.

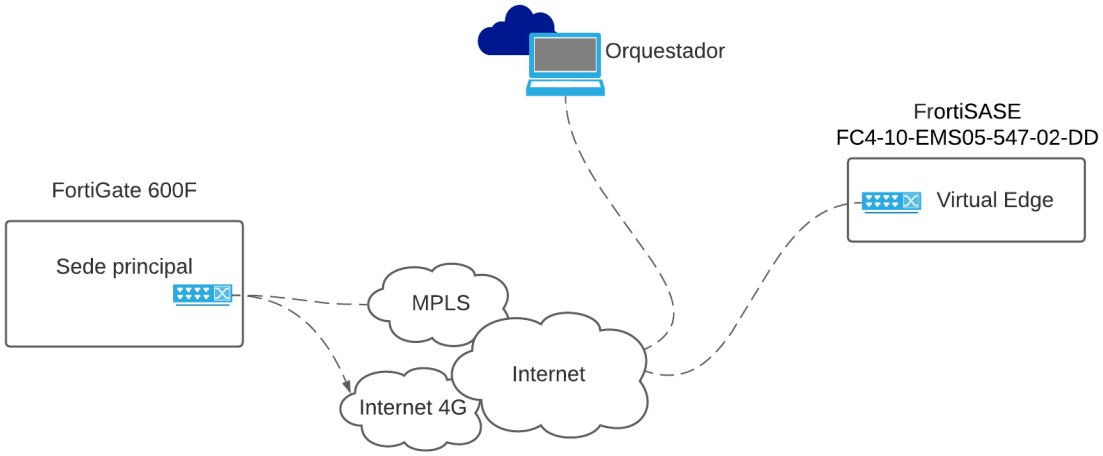

Figura 5 topología alternativa de solución N°3

Las ventajas de tener una red hibrida son la capacidad en flexibilidad y escalabilidad, combinación de un equipo Fortigate virtual con un equipo físico permite a las organizaciones adaptarse rápidamente a cambios en sus necesidades de red, tanto en términos de capacidad como de funcionalidades. Por esto, se plantea el equipo físico, en la sede central ubicada en Santiago, debido a que tiene un mayor rendimiento y capacidad de procesamiento. Al contar con un equipo físico que soporta la carga pesada de procesamiento de datos, se mejora el rendimiento y la capacidad del firewall virtual para gestionar un mayor volumen de tráfico de red de manera eficiente. Esta alternativa mejora evita la implementación de equipos en cada una de las sedes, facilita actualizaciones, no tiene límites de crecimiento, cuenta con alta disponibilidad y eficiencia. Basados en la descripción anterior se le da una calificación de 8/10 a la topología puesto que cumple con

los requerimientos, pero puede congestionarse y ser un poco menos eficiente que tener todos los quipos físicos.

Tabla 6 Presupuesto alternativa 3

Rubro	Descripción	Unidad	precio unitario	Cantidad	Total (USD)
Equipo	Equipo FortiGate 600F se implementará en 3 sedes tipo A	unidad	$ 18.423	1	$ 18.423
software	Licencia de FortiSASE a 3 años	Mes	$ 8,67	36	$ 312
	Virtualizar el servidor en la nube	Mes	$ 108,33	36	$ 3.900
Recurso humano	Mano de obra para el despliegue de toda la solución	Mes	$ 900	1	$ 900
				TOTAL	$ 23.535

En la **Error! Reference source not found.** se presenta el presupuesto para la alternativa de solución N°3. Está cuenta con el precio del firewall FortiGate 600F para la sede principal el cuales de 18.423 USD y la instalación de este equipo es de 1.500 USD, es de aclarar que el soporte de este equipo es para 3 años, al término de este tiempo se requiere comprar un licenciamiento para ello. Se evidencia el costo de la suscripción de FortiSASE por 3 años el cual es de 312 USD y Finalmente se puede encontrar el precio de virtualizar en la nube por 3 años el cual es de 3.900 USD. El precio total de esta alternativa contando con soporte, mantenimiento y licenciamiento por 3 años es de 24.235 USD. El tiempo para la implementación de esta solución es de 1 mes.

5 SELECCIÓN DE SOLUCIÓN FORTINET PARA EMPRESA CAMANCHACA

Para la selección de la alternativa se hará una toma de decisiones pondera, para lo cual, lo primero que se hace es definir los siguientes tres criterios:

- Tiempo (meses): es el plazo para el despliegue de la topología dentro de la empresa.
- Presupuesto (USD): es el costo total del despliegue de la topología dentro de la empresa.
- Topología (puntaje): es el nivel de cumplimiento técnico de la topología propuesta frente a los requerimientos de la empresa expuestos en el caso de negocio. Este puntaje se valorará sobre un máximo de 10 puntos.

La empresa espera que estos criterios sean maximizados o minimizados en la solución que desean seleccionar. Para esto se define para cada criterio:

- Tiempo: Para la empresa Camanchaca es importante reforzar su seguridad y el tráfico de la red en el MENOR tiempo posible, por ello es mejor la alternativa de solución que represente el menor tiempo de despliegue.
- Presupuesto: A pesar de no estar limitados presupuestalmente, la empresa Camanchaca prefiere elegir una alternativa buena técnicamente, pero con el MENOR presupuesto.
- Topología: La prioridad la empresa Camanchaca es que la alternativa cumpla en la MEJOR medida los requerimientos, es decir; que brinde la seguridad necesaria, segmente el tráfico de la red, mejorar el rendimiento de la red y tener visibilidad y control desde un solo dispositivo.

Así que los criterios a maximizar (MEJOR) se normalizaran según la ecuación (1) y los criterios a minimizar (MENOR) según la ecuación (2)

$$\frac{Valor\ Alternativa}{Max\ Valor\ de\ las\ alternativas} \quad \text{Ecuación 1}$$

$$1 - \frac{Valor\ alternativa}{Max\ valor\ de\ las\ alternativas} \quad \text{Ecuación 2}$$

La Tabla 7 muestra el resumen de los valores de cada una de las alternativas para cada uno de los criterios, como lo es el presupuesto, el tiempo y la topología. Estos valores se normalizarán según si el criterio se maximiza o minimiza, según las ecuaciones 1 y2. Para posteriormente ser ponderados y poder hacer una evaluación de las alternativas de manera comparada (Tabla 8).

Tabla 7. Valoración de las alternativas

Alternativas	N1	N2	N3
Presupuesto (USD)	127.245	117.517	23.535
Tiempo (meses)	3	9	1
Topología (puntaje)	10	7	8

Teniendo en cuenta que los tres criterios no tienen la misma importancia en la toma de decisiones de la empresa, se realiza una ponderación de estos teniendo en cuenta que lo más importante es que la solución cubra los requerimientos propuestos la topología tiene una ponderación de 50%, el segundo criterio en importancia sería el tiempo de implementación y se ponderara con un 35%, y finalmente, pero aun tenido en cuenta el presupuesto se pondera en un 15%.

La Tabla 8 muestra la evaluación de las alternativas, de modo que para cada alternativa se puede observar el valor del criterio, la normalización de este valor y su valor ponderado. La evaluación de cada alternativa es entonces la suma de los valores ponderados de su valor para cada criterio.

Tabla 8 Evaluación de alternativas

VALORACION Y NORMALIZACION DE CRITERIOS POR ALTERNATIVA		PRESUPUESTO 15%	TIEMPO 35%	TOPOLOGIA 50%	EVALUACION
alternativa 1	Valor	127.245	3	10	0,76
	Normalización	0,00	0,75	1,00	
	Ponderación	0,00	0,26	0,50	
alternativa 2	Valor	117.517	12	7	0,36
	Normalización	0,08	0,00	0,70	
	Ponderación	0,01	0,00	0,35	
alternativa 3	Valor	23.535	1	8	0,84
	Normalización	0,82	0,92	0,80	
	Ponderación	0,12	0,32	0,40	

La selección de la solución se basó en el tiempo del despliegue, la eficiencia y eficacia de la topología al momento de cumplir con los requerimientos, y el presupuesto, teniendo en cuanta un peso ponderado para cada uno de estos criterios diferente. Entonces, la alternativa de solución con mayor calificación es la alternativa N°3, con una calificación de 0,84, 8 puntos por encima de la alternativa N°1 donde la valoración es de 0,76 y la alternativa N°2 que se valoró con 0,36 siendo la alternativa con menor calificación presente pues es la que mas tiempo toma y la de menor calificación en topología.

La alternativa seleccionada presenta una solución de una red hibrida, que consta de un software fortiSASE instalado en cada una de las sedes excepto en la oficina principal que se

encuentra ubicada en Santiago, esta sede cuenta con un equipo FortiGate 600F. Esta alternativa de solución no solo es la que tarda menos tiempo en realizar el despliegue de sus equipos por su facilidad al instalar el software y la solo un equipo físico como lo es el FortiGate 600F, sino que brinda el mejor precio respecto a las otras alternativas de solución. Por último, pero no menos importante, la topología planteada para la alternativa de solución N°3 está planteada para una red SD-WAN que no solo dirigirá de manera efectiva, brindado prioridad al trafico deseado por la empresa, protección en cada una de las sedes respecto a la ciberseguridad y teniendo un monitoreo constante del trafico de la empresa, generando análisis e informes que van a ayudar al desarrollo de la empresa

6 CONCLUSIONES

1. La alternativa de solución N°3 plantea una solución SD-WAN capaz de segmentar y balancear el tráfico de red MPLS de la empresa Camanchaca, utilizando equipos FortiGate para las distintas sedes de la empresa, con un equipo FortiAnalyzer que brinde información respectiva al tráfico, basado en la caracterización de la red.
2. Se identifico que la Empresa camanchaca cuenta con tres tipos de sede, Estas sedes se dividen por la cantidad de ancho de banda y número de usuarios máximo en cada una, tipo A que cuenta con un máximo de 500 usuarios y 1.2Gbit/s de ancho de banda, tipo B que cuenta con un máximo de 200 usuarios y 900 Mbit/s de ancho de banda y sedes tipo C, en las que alberga un máximo de 50 usuarios y 500Mbit/s de ancho de banda.
3. Se plantearon 3 diferentes alternativas de solución que se diferencian principalmente por la topología, por ser una solución hibrida (Solución diseñada entre equipos cableados (hardware) y software) o por el nivel de seguridad que genera en la empresa cada una de las alternativas.
4. El control de los datos y el flujo a través de la red se logró gracias a el equipo FortiAnalyzer, que principalmente es capaz de Monitoreo del tráfico de red, Análisis de amenazas, Generación de informes y Gestión de eventos y registros
5. Tras el paso por la empresa SONDA DE COLOMBIA S.A se generaron conocimientos como ingeniero preventa, potencializando habilidades blandas como pensamiento crítico, pensamiento creativo, trabajo en equipo, resolución de problemas, gestión del tiempo, comunicación, entre otras.

REFERENCIAS

1. “¿Qué es la SD-WAN? Una WAN definida por software básica | Fortinet”. Fortinet. [En línea]. Disponible: https://www.fortinet.com/lat/products/sd-wan1/what-is-sd-wan
2. “Seguridad para endpoints | Elimine violaciones de seguridad | Fortinet”. Fortinet. [Enlínea]. Disponible: https://www.fortinet.com/lat/resources/cyberglossary/endpoint-protection
3. “Firewall de próxima generación (NGFW) | Fortinet”. Fortinet. [En línea]. Disponible: https://www.fortinet.com/lat/products/next-generation-firewall
4. “What is SIEM? How does it work? | Fortinet”. Fortinet. [En línea]. Disponible: https://www.fortinet.com/resources/cyberglossary/what-is-siem
5. “Firewall de aplicación web (WAF) & Protección de API | Fortinet”. Fortinet. [En línea]. Disponible: https://www.fortinet.com/lat/products/web-application-firewall/fortiweb#:~:text=El%20Firewall%20de%20aplicaciones%20web,a%20vulnerabilidades%20conocidas%20y%20desconocidas.
6. “Controladores de entrega de aplicaciones | Fortinet”. Fortinet. [En línea]. Disponible: https://www.fortinet.com/lat/products/application-delivery-controller/fortiadc#:~:text=FortiADC%20proporciona%20aceleración%20de%20aplicaciones,usuarios%20en%20todo%20el%20mundo.